UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UMA PROPOSTA DE UM MODELO DE CONFIANÇA COMPUTACIONAL PARA GRUPOS EM SISTEMAS DISTRIBUÍDOS

ROBSON DE OLIVEIRA ALBUQUERQUE

ORIENTADOR: RAFAEL TIMÓTEO DE SOUSA JÚNIOR

TESE DE DOUTORADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPGENE.TD - 029/2008
BRASÍLIA, DF: AGOSTO / 2008.

UNIVERSIDADE DE BRASILIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UMA PROPOSTA DE UM MODELO DE CONFIANÇA COMPUTACIONAL PARA GRUPOS EM SISTEMAS DISTRIBUÍDOS

ROBSON DE OLIVEIRA ALBUQUERQUE

TESE DE DOUTORADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASILIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE DOUTOR.

APROVADO POR:

RAFAEL TIMÓTEO DE SOUSA JÚNIOR, Dr., ENE/UnB
(ORIENTADOR)

ANDERSON CLAYTON ALVES NASCIMENTO, Dr., ENE/UnB
(EXAMINADOR INTERNO)

PAULO HENRIQUE PORTELA DE CARVALHO, Dr., ENE/UnB
(EXAMINADOR INTERNO)

RICARDO STACIARINI PUTTINI, Dr., ENE/UnB
(EXAMINADOR INTERNO – SUPLENTE)

JACIR LUIZ BORDIM, Dr., CIC/UnB
(EXAMINADOR EXTERNO)

BRASILIA, 08 DE AGOSTO DE 2008.

FICHA CATALOGRÁFICA

ALBUQUERQUE, ROBSON DE OLIVEIRA.
Uma proposta de um modelo de confiança computacional para grupos em sistemas distribuídos [Distrito Federal], 2008.
xv, 171p., 210 x 297 mm (ENE/FT/UnB, Doutor, Engenharia Elétrica, 2008).
Tese de Doutorado – Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica.

1. Sistemas distribuídos	2. Sistemas Multi-Agentes
3. Segurança da Informação	4. Confiança Computacional
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

ALBUQUERQUE, ROBSON DE O. (2008). Uma proposta de um modelo de confiança computacional para grupos em sistemas distribuídos. Tese de Doutorado, Publicação PPGENE.TD - 029/2008, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 186p.

CESSÃO DE DIREITOS

AUTOR: Robson de Oliveira Albuquerque

TÍTULO: Uma proposta de um modelo de confiança computacional para grupos em sistemas distribuídos.

GRAU: Doutor ANO: 2008

Robson de Oliveira Albuquerque
QNM 38 Conjunto U casa 13
CEP: 72.145-821, Taguatinga, Brasília - DF
Tel. 55 – 61 – 3307-2308 ext. 238 / robson@redes.unb.br

Dedico este trabalho:

Aos meus pais. Seus exemplos e orientações me trouxeram até aqui.

Às minhas filhas – Mariana, Maria Eduarda e Ana Clara. Vocês me deram um novo sentido à vida. Sou grato por tudo que me ensinaram, me ensinam e me ensinarão.

Á Sheyla. Meu compromisso com você é muito maior do que eu posso imaginar ou expressar através de palavras.

Aos meus irmãos, Amauri e Elon. Que nossa união permaneça. Que nossos atos sejam em prol do nosso bem estar comum.

Aos meus amigos. Este trabalho é fruto da colaboração de vários deles. Que nossa amizade continue sempre a crescer.

"Quem desiste não alcança o resultado esperado."

Robson de Oliveira Albuquerque

AGRADECIMENTOS

Às minhas filhas pelos sorrisos diários, pelos questionamentos que tanto me fazem refletir na simplicidade das coisas e na felicidade duradoura. E que por vezes me fazem esquecer das dificuldades e arranjar forças para continuar lutando.

À minha família. O apoio de todos foi fundamental.

À Sheyla por não ter desistido e não me deixar desistir.

Aos meus amigos e amigas, que de uma forma ou de outra, contribuíram para minhas conquistas e fazem parte deste trabalho.

A toda equipe do LabRedes, onde tenho o prazer de ser um facilitador, acompanhar seu desenvolvimento e poder contribuir para seu sucesso, além de ter aprendido muito mais do que ensinado.

Aos alunos de quem tive o prazer de ser orientador e dos trabalhos que realizamos juntos. Isto é uma parte um trabalho construído por diversas mãos e não só as minhas.

Aos professores com quem tive o prazer de aprender, de trocar idéias e de contribuir de alguma forma para o avanço da ciência e tecnologia.

Aos meus companheiros de trabalho diário que aturaram inúmeras dúvidas e questionamentos, muitas vezes sem nem entender o que eu queria ou precisava.

Em especial, agradeço ao Prof. Dr. Rafael. Isto é fruto de nosso esforço constante na área acadêmica.

Sobretudo agradeço a Deus!

Meus sinceros agradecimentos.

RESUMO

UMA PROPOSTA DE UM MODELO DE CONFIANÇA COMPUTACIONAL PARA GRUPOS EM SISTEMAS DISTRIBUÍDOS

Autor: Robson de Oliveira Albuquerque
Orientador: Rafael Timóteo de Sousa Junior
Programa de Pós-graduação em Engenharia Elétrica
Brasília, 08 de agosto de 2008

A representação da confiança e da reputação em sistemas computacionais é um desafio em sistemas distribuídos. Nesses sistemas, a aplicação da confiança e da reputação busca contribuir com a segurança da informação, de forma a dar uma garantia mínima de realizar transações seguras sem uma autoridade central de controle. Nessa perspectiva, a confiança e a reputação se tornaram objeto de pesquisas científicas tanto do ponto de vista teórico quanto prático em MANET (*mobile ad hoc networks*), sistemas *peer-to-peer* (P2P) e grids computacionais, entre outros domínios. Em conseqüência, diversos trabalhos foram apresentados na tentativa de resolução dos problemas decorrentes da aplicação da confiança e da reputação. Entretanto, não há um consenso em torno do tema, principalmente porque existem muitos modelos distintos, muitas vezes complementares, que tratam de problemas envolvendo a aplicação da confiança e da reputação. Uma das questões ainda em aberto consiste das situações em que os sistemas distribuídos se destinam à interoperação ou ao interelacionamento entre grupos de entidades, contexto em que a confiança e a reputação são promissoras como fatores de escalabilidade, desempenho e garantia de transações. Para tais situações, esta tese apresenta uma proposta de um modelo de confiança para grupos em sistemas distribuídos, visando solucionar alguns pontos em aberto, especificamente no que se refere à representação da confiança entre grupos através de um modelo matemático, além do consenso quanto à confiança intra-grupo considerando questões de identidade dos participantes e à definição de líderes. Este trabalho, além de ter base na revisão da literatura sobre confiança e da reputação, que se encontra apresentada na tese, é também voltado para a demonstração prática dos conceitos propostos com a aplicação das definições de confiança e reputação em sistemas distribuídos, considerando a formação de grupos, o que é realizado através da implementação do modelo de confiança proposto para grupos em sistemas distribuídos baseados em P2P e sistemas de agentes de software, envolvendo simulações de serviços de um grid computacional. Esse ambiente experimental permite demonstrar alguns resultados da confiança em grupos segundo o modelo apresentado em termos de reusabilidade.

ABSTRACT

A PROPOSAL OF A COMPUTATIONAL TRUST MODEL FOR GROUPS IN DISTRIBUTED SYSTEMS

Author: Robson de Oliveira Albuquerque
Director: Rafael Timóteo de Sousa Junior
Programa de Pós-graduação em Engenharia Elétrica
Brasília, 08 august 2008

The representation of trust and reputation in computational systems is a challenge in distributed systems. In such systems, the application of trust and reputation tries to contribute with the information security area in order to guarantee secure transactions without a central control authority. Considering this approach, trust and reputation has become research interest in scientific theory and practical implementations in mobile ad hoc networks (MANET), peer-to-peer (P2P) systems, computational grids, and others research areas. As consequence, several research works have been published in order to try to solve specific problems considering the application of trust and reputation in distributed systems, but without a common consensus in the subject. One reason for this problem is because there are a lot of different models, sometimes complementary, that deals with trust and reputation and its application scenarios in distributed systems. Some open issues regarding trust and reputation consists in situations that in distributed systems there are the necessity of interaction in groups, particularly in its representation considering a mathematical model, besides the consensus in trust inside a group regarding the identification of its members and a unique leader, preferentially chosen using trust and reputation criteria. This thesis moreover based in the literature review about trust and reputation herein presented, also shows some practical results considering a proposed group trust model in distributed systems using trust and reputation approach. The results are shown considering P2P networks and software agent systems simulating a computational grid. The experimental environment allowed the demonstration of some results in group trust following the definition of the presented model in terms of reusability.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE ACRÔNIMOS

ACL	Agent Communication Language
CA	Certification Authority / Autoridade Certificadora
CIA	Centralized Indexing Architecture
CP	Candidato Proposto
DIFA	Distributed Indexing with Flooding Architecture
DIHA	Distributed Indexing with Hashing Architecture
DTM	Dynamic Trust Metric
DyTR	Dynamic Trust-based Resources
FIPA	Foundation for Intelligent Physical Agents
GCP	Green Card Protocol
GKA	Group Key Agreement
HPC	High Performance Computing
JXTA	Justapose – Framework P2P da Sun Technologies
MANET	Mobile Ad Hoc Network
MITD	Man In The Middle
MPP	Massively Parallel Computing
OLSR	Optimized Link State Routing protocol
P2P	Peer-to-Peer
RADE	Role based Agent Development Framework
RBF	Reputation Based Feedback
REGRET	Reputation Based Model for Gregarious Societies
SN	Social Networks
SSL	Secure Socket Layer
TGDH	Tree-Based Group Diffie-Hellman
TLS	Transport Layer Security
TRAVOS	Trust and Reputation Model for Agent-based Virtual Organizations
XML	Extensible Markup Language

1 INTRODUÇÃO

Este trabalho propõe um mecanismo para calcular a confiança em situações de grupos em sistemas distribuídos. Para tanto elabora a proposta de um modelo que possibilita o cálculo da confiança em grupos mediante observações de reputação de seus integrantes.

A confiança computacional é objeto de estudo de diversos autores como ([1], [2], [3], [4], [5]), e tem aplicação em diversas áreas ([6], [7], [8], [9], [10]). Nas áreas de conhecimento da computação e da engenharia de redes de comunicação, a linha de fronteira entre as conceituações de confiança é extremamente tênue e às vezes se confunde com outras definições fora destes campos de conhecimento. Assim, os aspectos que tratam da definição da confiança serão tratados e referenciados e, na medida do possível, tentar-se-á manter os limites conceituais.

Entretanto, o foco deste trabalho é a aplicação da confiança em sistemas distribuídos em situações que envolvam grupos de entidades. Para atingir este objetivo, são revisados os conceitos de confiança, de reputação, sua aplicação e seus modelos em sistemas distribuídos, além de citar alguns problemas e necessidades observadas no estudo aprofundado do tema. Como uma tentativa de solução de alguns desses problemas, se define uma proposta baseada em um modelo de confiança para grupos e é realizada sua conseqüente implementação. Além disso, são tratados os temas inerentes à avaliação da efetividade desse modelo proposto.

Vale ressaltar também problemas relativos à identificação de entidades em sistemas distribuídos. Este ponto é básico no tratamento da confiança computacional porque se deve confiar e gerar valores de confiança em uma entidade que apresente uma identidade correta, dando uma perspectiva clara na identificação de nodos. Relacionado a este ponto específico foi realizado um estudo com um protocolo de identificação para sistemas distribuídos, dando uma idéia mínima de requisitos de identificação. Entretanto, a sua aplicação é extremamente complexa e deixa margem para a criação de um trabalho específico para o estudo dos problemas de identificação de nodos.

Entre outras aplicações, a confiança computacional é usada para se conhecer e avaliar com quais entidades se deve interagir. De maneira simplificada, a confiança é um conceito que pode auxiliar na autenticação, que sofre diversos ataques em ambientes tecnológicos conforme citado em [11] e [12].

A partir do momento em que percepções individuais das entidades são armazenadas e as opiniões propagadas, passa-se a ter informações disponíveis, não apenas sobre o que acontece no sistema, mas também sobre como as iterações estão atendendo às expectativas das entidades, refletindo a dinâmica comportamental dos membros do grupo, o que complementa e reforça a autenticação. Dessa forma, há interesse em tratar as variáveis que influenciam o cálculo da confiança em um ambiente distribuído.

Mas, também é importante considerar que entidades maliciosas existem em ambientes colaborativos e distribuídos [11], fazendo com que a preocupação com a segurança da informação seja um aspecto de interesse. Até mesmo porque a presença de administradores de sistemas não pode ser garantida todo o tempo para realizar a verificação de requisitos de segurança (disponibilidade, integridade, não-repúdio etc.), acarretando a necessidade de um máximo de automatização destas tarefas.

Outro ponto que merece uma atenção especial é que não existe nos sistemas reais uma autoridade legítima única. Os sistemas computacionais cobrem domínios sob o controle de múltiplas autoridades administrativas, logo são operados dentro de múltiplos domínios administrativos diferentes (que normalmente envolvem áreas geográficas distintas). O uso de autoridades certificadoras nem sempre é adequado à solução desse problema em sistemas distribuídos [13] porque não se pode garantir certificação cruzada todo o tempo, e muito menos certificados para todos os elementos (serviços, usuários, estações etc.) que fazem parte de um ambiente distribuído com domínios de gerência diferentes, sem um enorme esforço gerencial e administrativo, além de muitas vezes ser uma solução ineficiente.

Assim, em sistemas distribuídos, o emprego da confiança é complexo porque envolve uma variedade de situações e aplicações ([6], [8], [11], [14], [18]). De maneira geral, há requisitos acerca da quantidade e dos tipos de variáveis utilizadas, tornando a análise e tratamento da confiança em ambientes computacionais uma tarefa árdua. Quanto maior a quantidade de variáveis envolvidas, maior a complexidade do tratamento do problema e conseqüentemente maior a dificuldade da elaboração de um modelo que atenda o máximo de ambientes e situações possíveis.

Em conseqüência, muitos autores ([1], [3], [9], [11], [14], [15], [16], [17]) colocam a aplicação da confiança dentro de um cenário específico. Como as soluções apontadas por tais autores tratam de criação de modelos e a sua aplicação dentro de um cenário específico, não se pode com certeza afirmar que exista um modelo global, que seja amplamente adotado como o mais completo, e que atenda às diversas disciplinas da tecnologia da informação.

Na aplicação da confiança em sistemas distribuídos, a revisão bibliográfica aponta que os modelos pesquisados e referenciados são utilizados em aplicações P2P, agentes de software, grids computacionais e redes ad hoc. Em tais domínios de aplicação, existem interesses na extensão do conceito de confiança, de modo que relações de confiança possam ser estabelecidas envolvendo não apenas entidades individuais, mas também grupos de entidades. Entretanto, o assunto da confiança em grupos ainda é relativamente pouco pesquisado, tendo poucas referências disponíveis ([3], [18]), e que não complementam e nem fornecem soluções para sistemas distribuídos em uma perspectiva mais ampla.

Nesse contexto, o presente trabalho procura desenvolver o estado da arte da representação de confiança voltada para grupos em sistemas computacionais distribuídos. Por exemplo, uma organização detentora um cluster e outra que possua um grid podem estabelecer uma relação de confiança para alcançar um objetivo em comum, sem que sejam conhecidos todos os elementos que as compõem, contudo, desde que sejam disponibilizadas informações de confiança sobre tais elementos.

A possibilidade de ataques com múltipla identidade [12] e a formação de coalizão de atacantes [13] para atacar um sistema e levá-lo a uma situação de inutilidade é um dos vários problemas que uma solução de confiança em grupos pode tentar evitar. Nesse sentido, o uso de técnicas de identificação única, sem o uso de autoridade central de controle [19], é um mecanismo fundamental para evitar problemas de ataques e intrusos em sistemas distribuídos. Contudo o problema da confiança na identificação de uma entidade é de solução não-trivial.

Estes e outros problemas envolvem o uso de técnicas de segurança da informação e modelos adequados, para que se garanta o sigilo e a autenticidade da comunicação sem o uso de certificação digital através de autoridades certificadoras centralizadas, como forma de garantia de identificação única de um nodo ou de um grupo [11].

É importante citar que as técnicas requerem a integridade das mensagens trocadas no estabelecimento da confiança, até mesmo porque estas mensagens e seu conteúdo se tornam ponto chave no tratamento da segurança da informação. Então, um modelo de confiança em grupos deve suportar uma proteção mínima contra ataques do tipo man-in-the-middle ([12], [13]), além de prover garantias de disponibilidade do sistema.

De maneira geral, esta discussão inicial apresenta o foco principal deste trabalho com enfoque na confiança, na sua aplicação em sistemas distribuídos e nas observações do seu uso em grupos. A seguir algumas limitações que envolvem os conceitos apresentados são brevemente discutidas.

1.1 LIMITAÇÕES DAS SOLUÇÕES DE CONFIANÇA COMPUTACIONAL

Conforme já visto, a confiança computacional é uma área de estudo em que estão sendo realizadas pesquisas a fim de se definir um modelo que possa ser aplicado não só em ambientes computacionais distribuídos ([1], [2], [3], [9], [11], [12], [13], [14], [15], [20]), mas também em outras áreas de conhecimento que fazem uso da tecnologia da informação ([4], [6], [7], [8]).

Devido à complexidade e à variedade de sistemas, ambientes, modelos matemáticos, modelos de gestão da confiança e da reputação, entre outros, não foi possível levantar um único modelo que seja considerado largamente aceito pela comunidade científica, seja nas implementações de sistemas utilizados atualmente para representar sistemas distribuídos, seja por parte da indústria ou ao menos pelos grandes fabricantes de sistemas e serviços de tecnologia da informação. Desta maneira, os esforços acabam sendo pontuais para sanar determinados problemas em determinados ambientes ([1], [3], [9]).

No que se refere à certificação digital, trata-se de uma técnica que com alguns problemas porque não é possível criar, manter e gerenciar uma autoridade certificadora centralizada ([1], [2], [3], [13]) para todas as entidades envolvidas em um ambiente distribuído, dado que múltiplos domínios são criados, dificultando a certificação cruzada e até mesmo a gerência dos recursos de certificação.

Além disso, os sistemas distribuídos são muito dinâmicos, com entrada e saída de nodos a todo o momento, tornando inviável criar uma associação direta de um certificado digital à identidade a um nodo ou a um serviço na rede e ainda assim garantir a escalabilidade do sistema.

Em uma análise mais detalhada, não é possível afirmar que existe um consenso sobre o uso de autoridades certificadoras em sistemas distribuídos ([1], [3], [13]), principalmente por ser inviável administrativamente de se fazer a certificação cruzada de todas as autoridades certificadoras necessárias de todos os usuários que se juntam a um grid ou a uma rede P2P, dado a complexidade técnica, e também de legislação internacional sobre o tema.

Na literatura referenciada acima, os temas de agentes de software, grids computacionais e sistemas P2P são objetos de pesquisas na tentativa de sistematizar e buscar uma solução para os problemas em sistemas computacionais distribuídos, bem como ambientes para a aplicação das teorias relativas à confiança.

Entretanto, as soluções encontradas e referenciadas envolvem o uso da confiança e da reputação apenas no relacionamento 1:1 (de um nodo para um único outro nodo), ou no

máximo para um grupo muito restrito de nodos ([3], [18]), dentro de um ambiente extremamente controlado. O relacionamento de um nodo para um grupo (1:N) ou de um grupo para outro grupo distinto (M:N), apesar de ser citado como necessário em várias situações ([3], [4], [18]), não foi observado como tema de pesquisas nos domínios da confiança e reputação até o momento da finalização deste trabalho.

Especificamente no que se refere à reputação, as questões (relacionamentos, informações sociais, nível de confiança, reputação etc.) relativas à opinião de um nodo sobre um grupo, a opinião de um grupo sobre outro grupo e vice-versa, também são pouco abordadas e estão a merecer maior aprofundamento da pesquisa.

Vale notar que, na tradição da área de pesquisa sobre confiança computacional, as propostas de trabalhos em geral englobam conceitos tipicamente humanos para o uso em sistemas computacionais, incluindo conceitos de sociedade, comunidade e organizações, que são abordadas na tentativa de inspirar as soluções na perspectiva de expansão do uso da confiança e da reputação em sistemas distribuídos.

Nessa linha de raciocínio, a criação de sociedades de nodos P2P, comunidades de agentes de software, organizações virtuais de grids, entre outros temas, apesar de ter grande interesse em sistemas distribuídos, acaba esbarrando nos conflitos quanto às definições básicas, nos impedimentos da segurança da informação, na falta de consenso por parte dos autores quanto aos modelos que tratam da confiança nestes ambientes e à implementação de tais modelos.

Em outras palavras, as dificuldades começam com as deficiências sobre a confiança e seu uso como solução para problemas complexos, apresentando uma interface relativamente simples para os usuários e mecanismos eficientes de gerência automatizados.

Assim, continua ainda em aberto o atendimento das referidas comunidades, sociedades e organizações, com a criação de modelos capazes de fazer a representação da confiança e da reputação, em especial com modelos que sejam capazes de fazer o tratamento de grupos e dos relacionamentos envolvendo grupos.

Nesse sentido, há trabalhos que vêm apontando algumas direções a serem exploradas. Wang [18] propõe o uso de um ambiente baseado em peer-to-peer que utiliza informações de reputação e confiança e sugere o uso de grupos, entretanto o trabalho não é conclusivo para outros ambientes e não trata explicitamente a necessidade da confiança em grupos ou comunidades em sistemas distribuídos.

Já a pesquisa realizada por Patel [3] é voltada para organizações virtuais para grids através do uso de agentes de software. Entretanto o trabalho não explora a confiança aplicada

a um grupo ou comunidade, apesar de citar a sua importância e necessidade no contexto de sistemas distribuídos. Assim, Patel [3], embora proponha um modelo extensível para sistemas distribuídos (demonstrado neste trabalho), não aborda a confiança para um grupo, uma comunidade ou uma sociedade de agentes em uma organização virtual e considera que os modelos desse tipo são considerados ainda no estado da arte da aplicação de confiança em tais ambientes.

Vale enfim comentar que as redes sociais (*social networks*) ([4], [6], [7]) têm sido objeto de estudo correlacionado às comunidades de agentes, entretanto o uso de informações sociais de grupos não é totalmente explorado pelas referências estudadas. E, da mesma forma que a confiança e a reputação em grupos, não foi possível levantar um modelo que fosse capaz de fazer o tratamento de informações sociais, através de grupos, voltadas para comunidades de agentes, ou sociedades com P2P que tratem da aplicação de conceitos de confiança e reputação.

1.2 MOTIVAÇÃO

Apesar de ser comum a idéia de representação de grupos ou de criação de uma comunidade, os modelos de confiança estudados e revisados não focam integralmente a representação da confiança voltada para grupos ou comunidades virtuais.

Conforme já visto, a representação da confiança e da reputação ocorre em uma perspectiva de um para um (1:1), dentro de um contexto específico. Também nos modelos pesquisados e referenciados, a confiança e a reputação não são tratadas diretamente para grupos ou comunidades, mesmo sendo constatada a necessidade de que ocorram de uma entidade individual de um para um grupo (1:N) ou de um grupo para outro grupo (M:N).

A realização de uma pesquisa detalhada visando a criação e a validação de um modelo que trate da confiança em grupos é um aspecto motivacional forte porque abre um leque de discussões sobre segurança da informação e a possibilidade de resolução de problemas atuais em sistemas distribuídos ([3], [15], [20]).

Além disso, possibilita uma contribuição ao tema através de uma revisão bibliográfica atualizada, de uma implementação do modelo proposto e das análises decorrentes da implementação e dos resultados obtidos.

1.3 OBJETIVOS DO TRABALHO

Tendo sido apontados os pontos em que existe uma área promissora de ser explorada através de pesquisas e análises experimentais, além de manter o foco na confiança em ambientes computacionais distribuídos, os objetivos deste trabalho podem ser resumidos em:

a. Desenvolvimento de uma proposta de um modelo que possa representar a confiança em um grupo em sistema distribuído;
b. Implementar o modelo proposto em um ambiente controlado, de forma a permitir à realização de simulações que validem a proposta em termos de critérios como a disponibilidade, auxiliada por critérios de confiança e reputação;
c. Tratar aspectos de segurança para a garantia da troca de informações seguras dentro de uma comunidade, entre nodos pares ou organizações virtuais, evitando a possibilidade de ataques contra identidade de nodos, informações maliciosas e *man-in-the-middle*.

Assim, o principal objetivo deste trabalho, observando o estado da arte da confiança em sistemas distribuídos, consiste na elaboração de um modelo computacional para a confiança e a reputação em sistemas distribuídos, envolvendo agentes de software e sistemas P2P, que seja capaz de representar ou mapear a confiança voltada para grupos ou comunidades.

Não obstante, outros objetivos adicionais podem ser citados:

a. Revisão bibliográfica sobre confiança e reputação envolvendo sistemas distribuídos, bem com a sua representação através de modelos que tratem a confiança de um para um (1:1), um para um grupo (1:N) e de grupo para grupo (M:N).
b. Implementação do modelo em linguagem e padrões abertos.

1.4 ORGANIZAÇÃO DA TESE

O capítulo 2 objetiva uma revisão dos conceitos principais abordados, incluindo principalmente a confiança e a reputação, além dos temas de interesse nos domínios de sistemas distribuídos (redes sociais, grids, agentes de software etc.) e fazer a correlação da aplicação da confiança e da reputação em tais ambientes.

Já o capítulo 3 apresenta a teoria que envolve a revisão e análise de modelos de confiança e reputação.

No capítulo 4 tem-se a proposta do modelo de confiança para grupos através de uma representação matemática e alguns dos problemas decorrentes de consenso na confiança.

As principais considerações sobre a implementação e sobre os ambientes de testes para agentes de software e sistemas P2P são tratadas no capítulo 5.

As análises dos resultados experimentados do trabalho são tratadas no capítulo 6, apontando variáveis sobre o comportamento de nodos em situações normais, e situações de comportamento malicioso e da representação de valores de confiança e reputação em grupos.

O capitulo 7 conclui esta pesquisa, sinalizando algumas perspectivas possíveis, o fechamento dos resultados obtidos e os caminhos futuros que podem ser seguidos para a seqüência deste trabalho.

2 APLICAÇÃO DA CONFIANÇA EM SISTEMAS DISTRIBUÍDOS

Este capítulo tem como foco a revisão dos principais conceitos de confiança, da reputação e suas aplicações em alguns sistemas computacionais distribuídos. Desta forma, com o intuito de abranger o tema em um cenário amplo e ao mesmo tempo, ser possível a separação dos conceitos, assuntos correlatos e de assuntos similares, foi realizado uma divisão dos assuntos em tópicos específicos. Considerando um tratamento mais abrangente, aspectos da confiança voltados para o comportamento humano, para a sociedade e a sua representação serão abordados.

Na primeira parte o enfoque será dado na confiança propriamente dita, explicando sua importância, suas características, suas aplicações e seu enfoque no cenário computacional (os termos, de uma forma ou de outra, serão discutidos e tratados no decorrer de todo o trabalho). A seguir, a reputação será definida de forma a descrever suas características e do seu relacionamento com o confiança.

A confiança aplicada a Grids e as suas revisões serão apontadas como o próximo tópico, onde o conceito de Grid computacional será introduzido. Vale ressaltar que a explicação detalhada de um grid computacional não é o enfoque deste trabalho, mas sim da aplicação da confiança no mesmo.

O tópico seguinte trata da confiança em P2P, e da mesma forma que o grid computacional, aspectos introdutórios e de uso da tecnologia em si serão citados. Entretanto, para o aprofundado do assunto, as referências servem como guia para que os interessados possam buscar maiores informações.

Confiança em agentes de software é o assunto na sessão seguinte. Como o foco de implementação direta deste trabalho envolve agentes de software, será dada uma atenção especial ao tema, tentando explicar o máximo de conceitos inerentes de agentes e a sua aplicação no contexto deste trabalho.

Alguns aspectos da aplicação da confiança voltado para redes MANET serão abordados na seqüência. Este tópico se deve à similaridade de conceitos envolvendo redes distribuídas e os seus cenários de aplicação com certificação digital, entretanto, da mesma forma que Grids e P2P, será a aplicação da confiança em MANET o assunto com um maior detalhamento.

As redes sociais serão abordadas na próxima sessão. O tratamento das redes sociais está voltado para os requisitos da criação de grupos ou comunidades e as suas principais características.

Por fim uma síntese do capítulo.

2.1 DEFINIÇÃO DE CONFIANÇA

A confiança continua sendo um item de questionamento de vários pesquisadores ([7] [8], [10]). As respostas sobre sua definição são muitas e variadas porque depende do contexto e da conseqüente análise. Este trabalho tenta abordar a confiança de acordo com os principais conceitos estudados e a revisão de autores que canalizaram esforços para a sua explicação.

As principais definições de confiança voltadas para o aspecto humano se baseiam nas relações entre pessoas, transparecendo de forma clara a relação entre confiança e o sentimento de segurança ([7], [8]). Segundo o Dicionário Aurélio da Língua Portuguesa [21], "Confiança: (S.) 1. Segurança íntima de procedimento 2. Crédito, fé 3. Boa fama 4. Segurança e bom conceito que inspiram as pessoas de probidade, talento, discrição etc. 5. Esperança firme 6. Familiaridade 7.(Pop) Atrevimento, petulância 8.(Bras) Atos libidinosos; licença 9.(Bras/RS) Empregado (ou outra pessoa) de confiança." A confiança então pode ser analisada como uma esperança firme em alguém ou em alguma coisa, considerando um sentimento de segurança, de certeza e tranqüilidade.

Para a explicação mais detalhada da confiança, dividiu-se o tratamento do assunto sob dois aspectos. O primeiro trata a confiança na perspectiva humana e o segundo no cenário computacional – foco principal desta pesquisa.

2.1.1 Confiança sob o aspecto humano

O sentimento de conforto e segurança faz com que todos os dias, o homem tome decisões baseadas na confiança que ele possui sobre determinada coisa, inclusive fazendo co-relações. Por exemplo, se uma pessoa está com algum problema de saúde e vai a um consultório médico é porque confia que o médico irá lhe auxiliar no problema, e assume o custo e a responsabilidade pela ação tomada. Em um pequeno paralelo, considerando uma situação normal, um ser humano não procura um psicólogo para resolver um problema de fratura.

Agora, imagine que uma pessoa escolheu um médico que esteja dentro dos seus padrões de confiança e dentro do consultório, ele comece a fazer perguntas voltadas para sua situação financeira, sobre seus bens materiais e não se importasse com a sua dor em si ou com o seu problema de saúde. Certamente, o grau de confiança depositado neste médico diminuiria até mesmo porque as perguntas nada têm a ver com a sua visita ou o contexto da consulta. Agora imagine que o diagnóstico do médico não fizesse sentido dado o problema em si. Por exemplo, você sente a sua cabeça doer e ele diz que seu problema está na cor da camiseta que está usando porque não combinou com sua aparência física.

Uma pessoa resolve confiar ou não em um procedimento ou em outra pessoa quando não possui informações completas e necessárias para realizar uma interação e para isso usa outros recursos, tais como o histórico da pessoa e sua reputação na sociedade, para definir se uma relação de confiabilidade deve ser estabelecida, ou se é possível de ser.

Desta forma, a confiança no aspecto humano está relacionada com o sentimento de segurança voltada para um determinado contexto, para a satisfação de uma expectativa de uma solução que seja provável de ser resolvida ([7], [8]). O processo de confiar em alguém é um resultado de várias análises que em conjunto gera a definição de confiança.

Em outras palavras, dentro de um contexto e da situação em si, é esperado que uma solução seja dada de acordo com uma expectativa criada pelo agente que precisa resolver um determinado problema. No caso de auxílio de outro agente, é gerado da mesma forma uma expectativa de solução, e se o problema for resolvido conforme a expectativa, a confiança aumenta. Caso contrário, o sentimento de que não foi atendido, ou que ocorreu uma traição da nossa expectativa, ou ainda da nossa confiança, geralmente é o primeiro sinal perceptível.

Normalmente o sentimento de traição da confiança envolve a avaliação do contexto e ainda de informações externas à situação propriamente dita (opiniões, relações, informações adversas, vivência, entre outros). Nos seres humanos, a construção da confiança é um processo que tarda porque envolvem muitas situações vivenciadas, entretanto, a perda da mesma é quase que imediata. Isso, sob o aspecto humano, faz com que a sua reconquista pode simplesmente não ocorrer ou ser extremamente trabalhosa, logo a aquisição da confiança é complexa e a sua perda é quase que instantânea.

A confiança então é um conceito abstrato, difícil de ser explicado com uma única verdade, mas que está presente em todos os dias da vida de um ser humano.

2.1.2 Confiança sob o aspecto computacional

Nas revisões de confiança, diversos autores ([3], [5], [9]) fizeram seu tratamento dentro de um aspecto em específico, alguns deles envolvendo a psicologia e sendo considerados como os precursores dos modelos computacionais atuais.

A definição que é comumente a mais aceita ([3], [4], [9], [10]) quando se trata da confiança aplicada a um conceito matemático e conseqüentemente no cenário computacional, é a dada por Gambetta [7], que são reforçadas por Lamsal [8]. Esta definição cita que a confiança é um nível particular de probabilidade subjetiva, na qual um agente acredita que outro agente realizará uma ação em particular, que está sujeita a uma verificação e que influencia na própria ação do agente em si.

A confiança ainda é definida por Gambetta [7] como o conceito social mais importante que auxiliam seres humanos a cooperar em seu ambiente social e está presente em todas as iterações humanas. Esta definição ainda é suportada por Dagsputa [10] e reforçada por Lamsal [8].

De uma forma geral, sem a confiança (em outros seres humanos, agentes, organizações etc.) não existe cooperação e conseqüentemente não existe uma sociedade, segundo Gambetta [7]. De maneira análoga, a confiança pode ser tratada como uma probabilidade de comportamento de que um agente realize uma determinada ação esperada por outro agente.

Em uma melhor análise, um agente pode fazer a verificação da execução de uma ação solicitada (se estiver dentro de sua capacidade), e dentro de um contexto que a realização da ação esperada afetará a própria ação do agente em si (envolvendo uma tomada de decisão).

Assim, se alguém é confiável, significa que existe uma probabilidade alta o suficiente de que esta pessoa irá executar uma ação, considerada benéfica de alguma forma, para que seja considerada a cooperação com ela. Em uma situação contrária, simplesmente acredita-se que a probabilidade é baixa o suficiente para que a cooperação seja evitada.

Estendendo a discussão neste trabalho, a confiança será tratada com um nível de probabilidade na qual um agente ou um grupo, acredita que outro agente ou grupo realizará uma ação em particular, sujeita a uma verificação e que influencia nas ações decorrentes.

O estudo de Gambetta [7] ainda propõe que a confiança tenha uma relação com a cooperação, de tal forma que a cooperação tenha uma importância com a aquisição da confiança. Se a confiança é unilateral a cooperação não pode obter sucesso. Por exemplo, se só existe a desconfiança entre dois agentes, então não pode existir nenhuma cooperação entre

eles, logo não podem realizar uma operação em conjunto para uma solução de um problema. Então de maneira análoga, se existe um alto nível de confiança, é muito provável que exista uma alta cooperação entre os agentes para a solução de um problema particular.

O trabalho realizado por Marsh [9] envolve um estudo abrangente sobre confiança relacionando as suas definições no comportamento do ser humano, tanto em cenários sociais, quanto psicológicos, fazendo também referências às definições de Gambetta [7]. Neste trabalho, considerado um dos primeiros na área de representação da confiança na computação, afirma que a confiança, possui um escopo que é passível de representação matemática e logo pode ser implementável em um sistema computacional.

Segundo o trabalho de Marsh [9], a definição de Gambetta [7], gera um conceito que varia de uma desconfiança (0) para uma confiança total (1). Logo a confiança será relevante se existir uma possibilidade de desconfiança, traição, saída ou desistência.

Figura 2-1 – Variação da confiança segundo Marsh [9].

A possibilidade de desconfiança, traição, saída e desistência são critérios que devem ser considerados na construção da confiança porque são aspectos importantes na análise de uma expectativa de comportamento. Esta definição aponta ainda que seja provável que uma confiança total faça com que a cooperação funcione porque simplesmente não existe a desconfiança. O problema neste caso é que uma decepção muito forte possa ser gerada caso alguma coisa saia fora do contexto para a solução do problema em si, fazendo com que os valores de confiança sejam completamente modificados.

Como a confiança é um objeto de avaliação subjetiva, a sua formalização requer uma série de preceitos, inclusive na percepção do mundo pelo agente porque a sua avaliação dependerá do contexto, do problema, da sua visão, entre outros fatores. Esta situação nos leva a acreditar que em uma mesma situação observada por agentes diferentes, um agente venha a ter uma percepção que eleve o seu grau de confiança enquanto outro agente a diminua.

De uma forma geral, a confiança no aspecto computacional envolve situações onde é necessário que o agente gere a sua própria confiança (definido como confiança direta). Por exemplo, o agente necessita resolver um problema e a partir das suas próprias inferências gera um valor de confiança de acordo com a sua percepção. Em uma situação em que o agente faça

o cálculo baseado em situações de relacionamento e recomendações, a confiança é dita como indireta.

A confiança então, dentro de um contexto determinado, é passível de representação matemática e no capítulo 3, será feito uma revisão dos principais modelos de confiança e reputação.

2.1.3 Aspectos que influenciam na confiança

Segundo Lamsal [8], a revolução causada pela Web em conseqüência da Internet, permitiu a evolução dos conceitos de comunicação, em que não existe mais a necessidade de interação direta. Como conseqüência principal não se precisa confiar tanto nas pessoas conforme na situação de interação direta. Esta situação é verdadeira quando se trata apenas do aspecto da comunicação porque não precisamos interagir diretamente, mas ainda se precisa da confiança, principalmente nos dispositivos eletrônicos que são utilizados para que essa interação ocorra, além dos meios de comunicação e nas trocas de mensagens.

Outro fator que influência nos aspectos de confiança envolve a recomendação, que pode ser entendida como uma apresentação de um agente a outro através de um terceiro agente. Por exemplo, é normal que conheçamos pessoas durante a nossa vida. Uma pessoa que necessite da indicação de alguém para auxílio em algum tipo de problema ou situação, tende a perguntar a outras pessoas que já confia, sobre o seu conhecimento sobre uma terceira pessoa.

Baseado nas intenções e na resposta se pode inferir se vamos confiar ou não no agente recomendado. Essa confiança ainda leva em consideração o quanto se confia no agente que fez a recomendação, na confiança ou na reputação do agente recomendado e até mesmo na capacidade do agente em auxiliar no problema ou na situação em questão.

Vale à pena ressaltar que quanto maior se torna a cadeia de recomendação a tendência é que o valor da confiança seja menor, simplesmente pela forma que a confiança é percebida. Por exemplo, quem me disse foi um amigo do meu amigo do meu vizinho.

A confiança também envolve uma relação de custo x benefício [9]. A decisão de confiança pode ser assinalada quando alguma coisa está em jogo que pode ter algum tipo de valia para o agente. Neste ponto, se a cooperação for considerada, a relação de custo x benefício fica mais clara, mas também pode tornar-se um problema.

Em outras palavras. Se a cooperação for importante na análise do agente para gerar uma informação em que possa ser pesado o custo x benefício, é preciso ser definido o que

deverá ser levado em conta em termos de cooperação, de tempo e sob quais circunstâncias. De uma forma ou de outra, a quantidade de variáveis no ambiente o torna complexo, necessitando de que certas definições devem ser consideradas para simplificar a confiança.

Marsh [9] e Gambetta [7], levam em consideração a competição fazendo um paralelo com a cooperação. Por exemplo, em determinados setores, como a economia, o monopólio é visto por um lado negativo e deve ser evitado, aumentando a competição e em conseqüência gerando melhores oportunidades e o direito de escolha. Já na segurança das pessoas, a cooperação entre forças policiais é inquestionável e a concorrência deve ser evitada para se combater o crime com maior eficiência. A confiança então também deve encontrar um ponto de equilíbrio que envolva a cooperação e a competição, evitando simplesmente assumir um dos extremos.

O risco também influencia na confiança envolvendo a cooperação ([3], [7], [9]). Neste caso, o risco pode ser definido com uma expectativa de que a cooperação não vá evoluir, ou simplesmente não será benéfica dada a "experiência" do agente no contexto em questão. Neste caso o agente é capaz de inferir através de mecanismos próprios e de colaboração para chegar a uma conclusão de avaliação do risco, caso a cooperação venha dar errado.

Outros fatores que influenciam a confiança envolvem o contexto, informações terceiras sobre a confiança e a apresentação de uma entidade.

2.1.3.1 Contexto

De maneira geral, a representação da confiança é aplicada seguindo um modelo de um para um (1:1), onde se segue o foco em que uma entidade A comunica-se com outra entidade B e se cria um relacionamento simples, unidirecional e dentro de uma situação ou contexto. A entidade A pode comunicar-se com outras entidades ao mesmo tempo, e ainda se mantêm a perspectiva de 1:1, entretanto, dentro de outros contextos. A Figura 2-2 ilustra esta situação.

No detalhamento da figura, suponha que a entidade A seja um nodo de um grid computacional, um nodo de uma rede P2P ou um agente de software para a realização de uma tarefa específica. De uma forma ou de outra (através de informações emitidas na rede ou buscadas em alguma base de referência), a entidade A resolve relacionar-se com B para a solução de um problema específico. De posse das informações necessárias ou por inferência própria, A entra em contato com B para saber se B pode auxiliá-lo ou não na solução de seu problema. À medida que a interação ocorre no tempo, A pode aumentar ou diminuir seu grau de confiança em B.

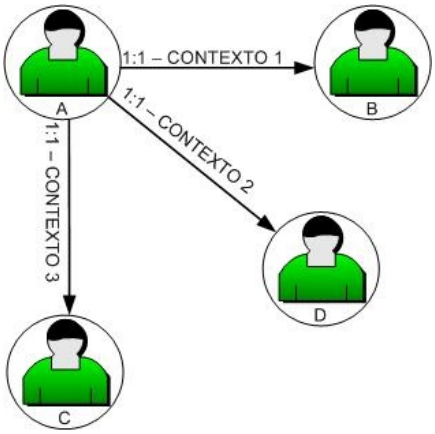


Figura 2-2 – Relacionamento 1:1 dentro de um contexto.

Nesta situação, e na maior parte dos casos do mundo real, nada impede que A se relacione com outros nodos para a conclusão de sua tarefa, ou até mesmo para a solução de novos problemas. Observado as considerações da confiança, A adquire ou perde a confiança em B dentro do contexto 1, e também adquire ou perde a confiança em C e D dentro dos contextos 3 e 2 respectivamente. O(s) contexto(s) para A, pode(m) envolver uma série de variáveis (definição do problema, quando ocorreu, em que situação se deu a comunicação, se esta foi positiva ou negativa etc.).

Vale ressaltar que esta é a perspectiva de A e somente A. Para B, C e D, os dados e os contextos podem ser outros. Isto nos dá uma idéia da opinião de A sobre B, C, ou D, no contexto específico. Considerando este cenário, A pode criar uma base de conhecimento representada pelo contexto e com quem se relacionou. A Tabela 2-1 representa a possibilidade desta base de conhecimento.

Tabela 2-1 – Base de Conhecimento de A.

Entidade	Contexto	Variáveis
B	1	X, Y, Z, N
C	3	P, Q, R, N
D	2	J, Y, P, N

2.1.3.2 Informações terceiras

No tratamento da confiança, existe a perspectiva de que uma entidade A solicite informação de uma entidade B a uma entidade C. Imagine que a entidade A, da situação anterior, precise de uma informação sobre uma entidade que ele ainda não se relacionou

(entidade E). A pode perguntar para os nodos dentro da sua rede de relacionamentos se algum deles conhece a entidade E, e qual a opinião sobre a mesma (variáveis da base de conhecimento). Em um resumo simples, esta perspectiva fornece uma idéia da reputação de E.

Na situação anterior, A conhece B, C e D, mas não conhece E. A entidade A pode disparar uma pergunta sobre E para B, C e D, e aguardar a resposta. Se alguma das entidades conhecerem E, esta retornará a informação para A relatando a sua opinião sobre E. A entidade A, de posse das opiniões sobre E, pode inferir sobre o comportamento de E dentro de uma determinada perspectiva. Vale ressaltar que nesta perspectiva não são considerados problemas da segurança da informação. A Figura 2-3 ilustra esta situação.

De posse das informações obtidas através de C e D, a entidade A pode realizar seu cálculo de confiança, baseado em um modelo, e a partir do resultado obtido, tomar uma decisão de relacionamento, que define se A irá se relacionar ou não com E, dentro do contexto de A. O mesmo é válido na perspectiva de E.

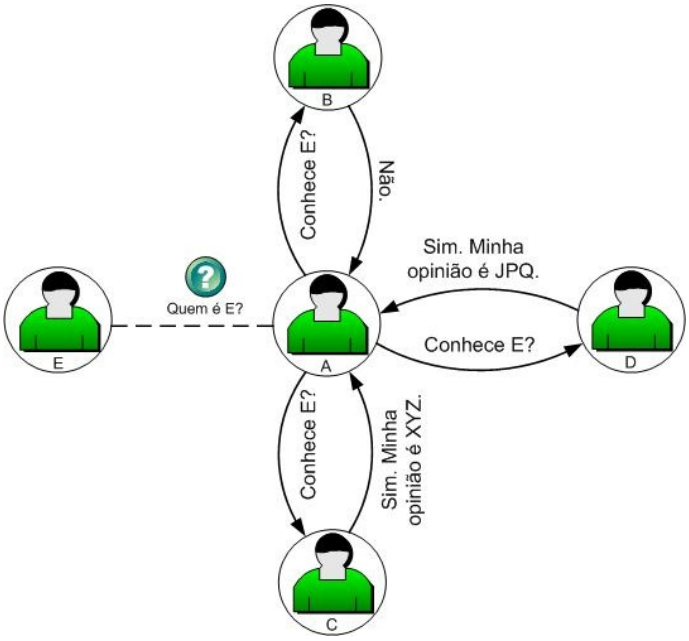


Figura 2-3 – Representação da aquisição de informações terceiras.

2.1.3.3 Apresentação de uma entidade

Nas situações de relacionamento com valores de confiança, alguns autores ([3], [4], [9]) sugerem a idéia de uma apresentação formal de uma entidade para outra, a partir de uma terceira entidade. Em determinadas situações, uma entidade A pode apresentar a entidade B para a entidade C, onde A e C já possuem certo grau de confiança entre si. Neste tipo de

situação assume-se que existe certo diálogo entre as entidades, em que a necessidade de apresentação de uma entidade pode auxiliar outra entidade na resolução de um problema. Esta situação inverte o papel da busca de informações por uma entidade. A Figura 2-4 ilustra esta situação.

Seguindo os exemplos anteriores, para a solução de um determinado problema, a entidade E é apresentada para a entidade A pela entidade C, que já possui uma opinião formada sobre E e a informa para A, que por sua vez, de posse da informação fornecida por C (de quem já possui certo grau de confiança), pode tomar a decisão de relacionar-se com E. Vale observar que neste processo, A pode ou não aceitar a oferta de relacionar-se com E já que não existe uma obrigação formal para tal, dado que A é autônomo. A também pode considerar não ser vantajoso se relacionar com E em um determinado contexto (por exemplo, A pode estar sobrecarregado de tarefas). A ainda pode buscar mais informações sobre E para auxiliá-lo no seu processo decisório, voltando à situação de informações terceiras.

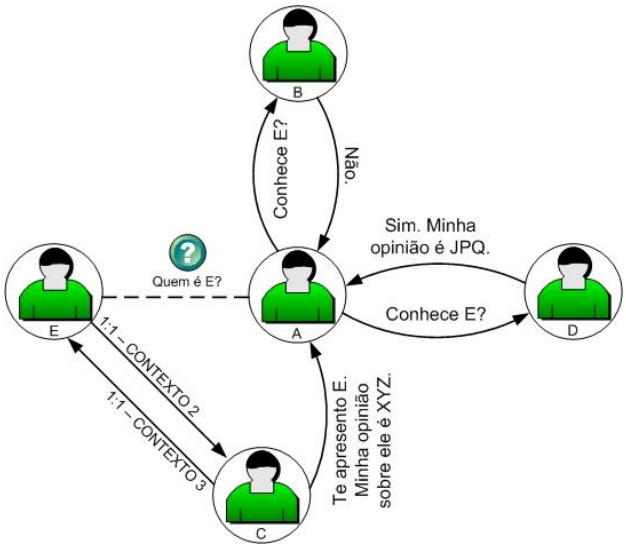


Figura 2-4 – Apresentação de uma entidade.

2.1.4 Resumo das características da confiança

A partir das considerações de confiança apresentadas até o momento, algumas características particulares podem ser assumidas. A Tabela 2-2 a seguir, sintetiza essas características iniciais.

Para Patel [3] a visão de confiança é modular, dados as suas várias características. Logo é calculada seguindo uma série de observações e implicações que versão desde a confiança adquirida unicamente pelo agente, como a confiança calculada baseado em

situações passadas e obtidas em um contexto social através de organizações e relacionamentos.

Tabela 2-2 – Características básicas da confiança.

Característica	Exemplo
A confiança é relativa a um determinado contexto ou situação	A pode confiar em B para lhe oferecer uma carona. Mas A não confia em B o suficiente dirigir seu carro.
A confiança tem um aspecto direcional.	A pode confiar em B, entretanto B pode não confiar em A.
A confiança é passível de ser mensurada	A pode confiar mais em B do que confia em C.
A confiança possui aspecto temporal e evolutivo	A confiança que A tem em B pode aumentar ou diminuir conforme A e B interagem.
A confiança pode ser influenciada por uma recomendação	A que já confia em B, passa a ter certa confiança em C, que por sua vez lhe foi apresentado por B.
A confiança não é transitiva	Se A confia em B e B confia em C, não significa dizer que A confia em C.

É importante ressaltar que a transitividade da confiança pode existir em determinados casos, já que algum critério de confiança é utilizado quando se considera relacionamentos entre entidades. Em outras palavras, algum indicativo ou valor de confiança pode ser passado entre A e B para que A confie em C.

2.2 REPUTAÇÃO

A reputação envolve um aspecto fundamental da confiança ([7], [8], [10]). Para Patel [3], a reputação pode ser definida em um cenário em que não se possui informação o suficiente para realizar a inferência de que um agente é ou não confiável, e para alcançar este valor de inferência, o agente questiona sobre a opinião de outros agentes. De posse da opinião de terceiros, o agente então realiza o seu cálculo de reputação a partir de suas próprias informações, que é baseado em seus valores de confiança e nas informações obtidas dos terceiros (seu grau de confiança nos mesmos). Uma vez obtidas as informações necessárias, o agente avalia o contexto da situação em si, sendo capaz de chegar a um valor de reputação.

Dagsputa [10] afirma que a confiança é baseada na reputação e que a reputação deve ser adquirida com base no comportamento através do tempo, entretanto, em circunstâncias bem entendidas. No seu trabalho, a confiança pode ser definida no sentido de expectativas corretas que influenciam na escolha de conduta de um agente antes mesmo que este possa monitorar as ações de outros agentes.

Conforme a confiança, a reputação também é adquirida com o tempo. Para Dagsputa [10], a reputação deve ser pública. Além disso, é baseada na atribuição de uma probabilidade

de distribuição sobre vários tipos de situações que um agente pode ser, ter ou estar. Em outras palavras, um agente pode ter várias funções e sua reputação ser distribuída conforme os seus vários papéis desempenhados nestas várias funções.

A reputação raramente é do tipo “tudo ou nada” ([3], [9]). Apesar disso, a reputação pode levar tempo para ser adquirida e pode ser perdida muito rapidamente, dependendo da criticidade da situação e da avaliação realizada.

O cálculo dos valores de reputação geralmente é feito fazendo uso de informações passadas ([3], [4]), adquiridas com o tempo e ainda através da opinião ou de uma imagem formulada por terceiros (ou uma comunidade) que é tornada pública.

Em um cenário mais amplo, a reputação é uma opinião (avaliação social) de um determinado público em sentido de uma pessoa, agente, grupo de pessoas ou agentes ou uma organização, além de ser um fator importante em vários aspectos e ser fundamental para a confiança. Alguns modelos de reputação serão tratados e revisados no capítulo 3, ampliando a discussão.

2.3 GRIDS COMPUTACIONAIS E CONFIANÇA

Até este ponto, a confiança voltada para o aspecto computacional, é algo mensurável, baseada em um contexto, evolui com o tempo e tem relacionamento direto com a reputação. Como exemplo do uso direto em sistemas distribuídos, a confiança pode ser aplicada em grids computacionais.

Para uma melhor distribuição do assunto, primeiro se define os Grids Computacionais e a seguir, alguns exemplos de confiança aplicada nesse ambiente.

2.3.1 Definição de grid computacional

Existem diversas definições para um grid computacional. A maior parte delas derivadas de outras definições ou até mesmo com um caráter evolutivo. A seguir são citadas algumas das definições revisadas.

Segundo a IBM [22], um grid envolve a habilidade de obter acesso a aplicações e dados, capacidade de processamento, armazenamento, e um conjunto de outros recursos computacionais na Internet, através do uso de um conjunto de padrões abertos e diversos protocolos. De uma forma mais específica, um grid é um tipo de sistema distribuído e paralelo que possibilita o compartilhamento, seleção e agregação de recursos distribuídos através de

múltiplos domínios administrativos baseados na disponibilidade, capacidade, performance, custo e qualidade de serviço dos usuários de seus recursos computacionais.

Com o uso da Internet como plataforma básica de comunicação, um grid é um conjunto de recursos computacionais geograficamente distribuídos ([22], [24], [25], [26]). Isto implica então que um Grid também é um *framework* conceitual, ao invés de simplesmente um recurso físico, que está associado com requerimentos de prover recursos computacionais flexíveis através de uma plataforma externa a um domínio administrativo.

Um grid normalmente é criado para resolução de problemas de recursos (ciclos de CPU, periféricos, dados, softwares, armazenamento etc.), onde normalmente estes recursos estão caracterizados por sua disponibilidade fora de um domínio administrativo, gerando um novo domínio administrativo (também denominado como Organização Virtual [3]), com características próprias de políticas administrativas de uso, acesso, segurança, entre outros. Em resumo, a maior parte dos grids computacionais pode ser comparada com a Figura 2-5.

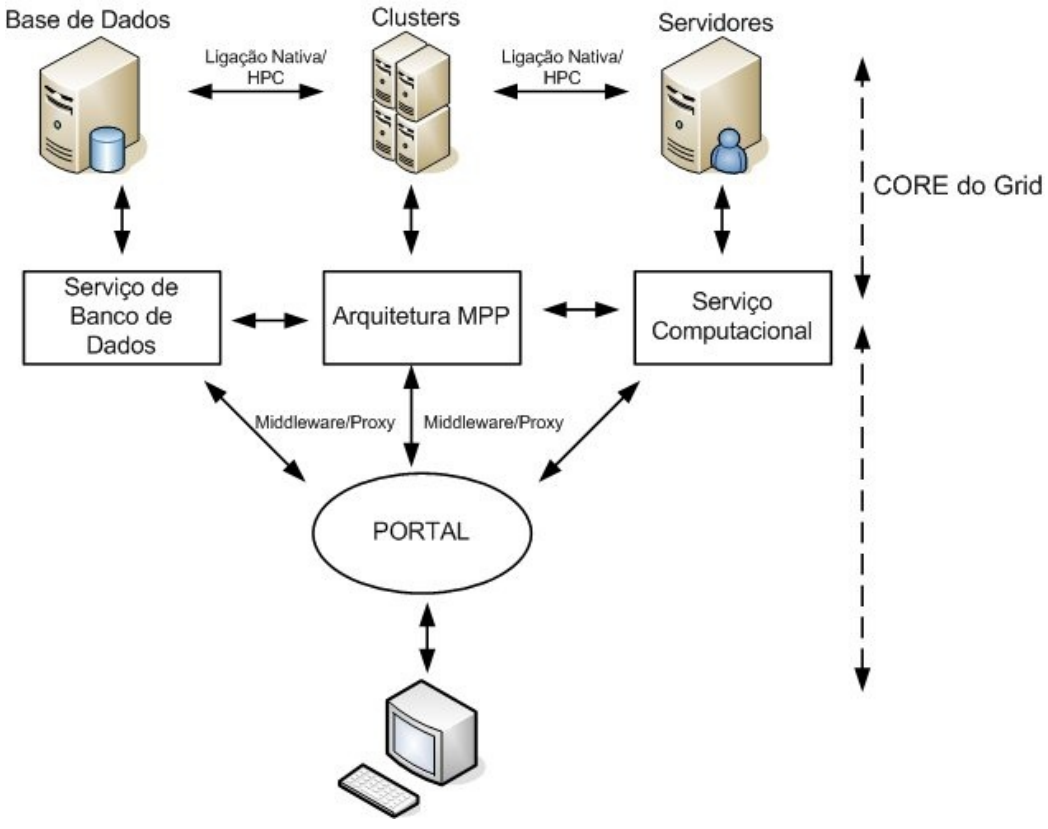


Figura 2-5 – Grid computacional multicamadas

Segundo Fox *et al.* [23], um grid envolve o uso de um conjunto de ferramentas e tecnologias que permite aos usuários acesso simplificado aos recursos e aplicações. Para os

usuários, normalmente aparece uma interface Web, que permite acesso a uma plataforma de desenvolvimento de n camadas ou simplesmente como um shell, dando acesso e permissões a diversas funcionalidades, como se fosse um típico shell Unix.

Voltado para a parte do Core do Grid, a ligação entre os dispositivos é realizada de maneira nativa como, por exemplo, através de um middleware específico ou através de protocolos próprios para HPC (High Performance Computing). Nesta camada do Grid existe a ligação de diversos dispositivos oferecendo diversos tipos de recursos. De maneira intermediária, fazendo a ligação entre o Core do Grid e o ambiente do Grid propriamente dito, existem os serviços associados.

A arquitetura MPP (Massively Parallel Processing) [23] permite o uso de recursos massivos de forma paralela em ambientes computacionais distribuídos. Em outras palavras, permite a agregação de várias CPUs geograficamente distribuídas em diversos componentes de hardware, dando a impressão de uma CPU gigante, trabalhando de forma paralela ou individual, dependendo do tipo de trabalho a ser processado ou realizado.

A interface de conexão ou gerência do ambiente permite que os usuários ou os administradores realizem as suas tarefas específicas. Este “portal” é a maneira que os usuários possuem para submeter seus trabalhos ao Grid e aos administradores em fazer as configurações e a manutenções do ambiente. E para permitir a maior transparência e independência possível de plataformas, são usados middlewares e proxys como camada intermediária de conexão.

No trabalho de Ferreira *et al.* [24], um grid computacional é considerado como a computação distribuída em um próximo nível evolucionário. Ainda explica que o objetivo é criar uma espécie de ilusão de um computador virtual, extremamente potente e grande, auto gerenciado, formado através da interligação de diversos sistemas heterogêneos compartilhando uma variação de combinações de recursos.

Para Pernas e Dantas [27], ambientes baseados em um grid computacional podem compartilhar serviços e recursos em uma larga escala, além de estarem sendo considerados como uma solução efetiva para a execução de aplicações distribuídas, alcançando um nível alto de performance e disponibilidade por várias organizações. Entretanto, Pernas e Dantas [27] citam que o uso de um grid computacional pode ser uma tarefa complexa para um usuário comum porque demanda um conhecimento prévio de pré-requisitos de acesso de uma organização virtual.

A existência de um Grid é possível através da padronização de processos de comunicação entre sistemas heterogêneos (similar ao que aconteceu com a Internet e a pilha

de protocolos TCP/IP), além do constante aumento da capacidade de processamento das máquinas e do aumento da largura de banda nos diversos canais de comunicação disponíveis atualmente. Esta combinação de fatores, associado à padronização de camadas e processos, permitiu a evolução dos conceitos de computação distribuída e computação paralela para o que atualmente é conhecido como grid computacional.

Na Internet existem diversos modelos de grids disponíveis, da mesma forma que através de ferramentas adquiridas por fornecedores de sistemas. Segundo a pesquisa realizada, o modelo mais completo aceito (até o fechamento deste trabalho) é o Globus Toolkit [25].

O Globus Toolkit [25] é um sistema livre e aberto utilizado para construir sistemas grid e de aplicações que fazem uso do Grid. É mantido por uma comunidade de organizações e de pessoas desenvolvendo tecnologias fundamentais "por trás" do Grid. Esta comunidade é amplamente conhecida como Globus Alliance [25].

OurGrid [26] é outro grid conhecido. Em resumo, trata-se de um projeto brasileiro, e que pode ser usado para rodar qualquer aplicação em que as suas tarefas não necessitam de comunicar-se entre si durante a sua execução (simulações, data mining, buscas, entre outras).

De forma a sintetizar o conceito e a demanda, a surgimento da tecnologia grid teve como principal fundamento a necessidade de expansão de processamento utilizando a capacidade de equipamentos considerados ociosos relacionados com seus recursos de hardware ([25], [26]). Como resposta para este problema surgiu o Grid computacional, de tal forma que uma tarefa possa ser distribuída em uma rede para ser executada pelo melhor equipamento ou conjunto de equipamentos disponíveis de acordo com os requisitos necessários da aplicação.

Definições mais aprofundadas sobre Grids podem ser encontradas nas referências ([3], [22], [23], [24], [25], [26]).

2.3.2 Confiança em grids computacionais

A complexidade de gerência de um Grid, dos seus usuários, de seus aspectos técnicos, de troca de dados e de informações envolve requisitos de segurança da informação ([3], [22], [24]). As tentativas para cobrir essa lacuna versam desde o uso de SSL/TLS [28], autoridades certificadoras (CA), técnicas criptográficas, entre outros, até a criação de modelos de comunicação para os nodos em uma rede, envolvendo middlewares e arquiteturas complexas.

Ainda existem lacunas a serem preenchidas nos problemas que tratam da confiança em sistemas distribuídos. Patel [3] cita a necessidade de solução de problemas de intra-domínios

em organizações virtuais e muitas delas voltadas diretamente para o tratamento da confiança nesses ambientes.

Problemas como a junção de grids, adoção de novos nodos na rede, gerência e submissão de tarefas a nodos "desconhecidos", comportamento de nodos no grid etc., necessitam mais detalhamento do que simplesmente adicionar um canal de comunicação seguro, provido por técnicas já conhecidas de criptografia, o que garantiria a confidencialidade da comunicação, mas não necessariamente a identidade do nodo [19]. Dessa maneira, diversos esforços da confiança foram voltados para grids e seu tratamento relacionado com a confiança, sendo que alguns desses esforços são citados a seguir.

Basney *et al.* [29], realizou um trabalho voltado para a extensão da segurança em Grids para suportar aspectos dinâmicos e aspectos organizacionais cruzados. A idéia versa sobre a adição de facilidades para permitir o estabelecimento de confiança entre partes distintas, que para tal, foi apresentado um modelo denominado de linguagem PeerTrust (*PeerTrust language*).

De uma forma mais sistêmica, o trabalho de Basney *et al.* [29], trata de como estender a infra-estrutura de segurança do Grid para prover melhor suporte para aspectos dinâmicos de atividades específicas, adicionando facilidades para o estabelecimento de confiança entre as partes envolvidas em um Grid.

O esforço realizado no trabalho de Basney *et al.* [29] vislumbra alguns princípios simples. Em um Grid, uma grande quantidade de recursos está disponível. Entretanto, não é desejável dar esses recursos a quem quer que seja, até mesmo porque não existe uma confiança mútua nos usuários e nas organizações para acesso a tais recursos. Estes princípios versam sobre a autonomia de cada entidade em gerenciar seus próprios recursos, fazendo com que o acesso aos mesmos será disponibilizado a quem tiver os mecanismos de confiança estabelecidos.

Em uma análise sobre essa distribuição de recursos (máquinas, sistemas, memória, CPU etc.), o problema não é simplesmente resolvível com a emissão de certificados digitais porque não existe nenhuma obrigação de um Grid confiar em certificados digitais emitidos por outra CA de outro grid. Isto nos leva ao problema de certificação digital cruzada, onde o usuário deverá gerenciar diversos certificados digitais diferentes para os diversos recursos diferentes no Grid, ou seja, o usuário deve apresentar diversas identidades para o acesso aos recursos disponíveis, que por sua vez, também podem ter seus certificados digitais.

Fica claro que o gerenciamento e a manutenção de uma quantidade de certificados distribuídos em um grid não permitem a escalabilidade e nem a flexibilidade, bem como a

facilidade de gerência que um grande Grid precisa para controlar o acesso aos seus recursos. Isto porque a autorização depende de propriedades, além da simples apresentação de uma identidade.

Considerando o problema de certificação digital em Grids, Olson *et al.* [1], levantou o questionamento sobre que tipo de confiança pode ou se deve ter em um certificado digital emitido por uma CA sem auditoria ou vetada, mesmo sendo gerenciada por pessoal técnico capacitado e bem-intencionado. Entretanto, apesar de apontar o problema, não elucida uma maneira clara de solução do mesmo, apenas exemplificando uso de certificados e papéis da CA.

O problema de certificação digital distribuída acaba ganhando um tratamento maior quando a escalabilidade e flexibilidade entram novamente em cena, além da facilidade de gerência. Isto porque fazer o manejo correto voltado para autorização e autenticação em grandes Grids, implica em possuir um grande conjunto de identidades expressas através de certificados (para usuários, serviços, estações, servidores etc.), dificultando sensivelmente a gerência de segurança de certificados (emissão, validação, controle, revogação, checagem etc.). Da mesma maneira também é necessário um grande número de contas de usuários, forçando de uma forma ou de outra, uma gerência centralizada, o que a princípio contradiz a filosofia de computação distribuída em Grid.

No trabalho proposto por Wang *et al.* [15], existe a sinalização de um modelo de confiança que possa ser aplicado a Grids, através de uma proposta de gerência de semântica de conteúdo. A proposta está entrelaçada através de algumas definições abrangendo variáveis relacionadas com nível de confiança, honestidade, recomendações, segurança, tempo etc., contudo o modelo não diz como adquirir o nível de confiança e muito menos define o que seria honestidade dentro do modelo.

De acordo com Papilo e Freisleben [14], em Grids é importante o gerenciamento de confiança entre entidades envolvidas em um ambiente colaborativo. Assim, foi proposto um modelo para esta gerência onde a confiança é calculada baseada na confiança da entidade propriamente dita, na sua confiança em outras entidades e na confiança de outros sobre si mesmo. Para a realização desta tarefa, Papilo e Freisleben [14], usaram as funcionalidades providas por redes Bayesianas (Bayesian Networks [30]), com o intuito de calcular e designar valores para determinadas entidade, além de avaliar suas capacidades em cenários distintos, observando o comportamento voltado para Grids como organizações virtuais.

Para Tran *et al.* [31], a confiança em Grid significa competência em entrega ou realização de serviços, de tal forma que a confiabilidade de um nó é função do seu

comportamento no grid. Diferentes nós possuem diferentes graus de confiança em um determinado nó, que muda com o tempo.

Existe a proposta de um modelo no trabalho de Tran *et al*. [31] para calcular a confiança em Grids, que é baseada no comportamento dos nodos, que por sua vez é dividido em bom, normal, má e maliciosa. De acordo com o tipo de comportamento do nodo, é possível realizar um cálculo de confiança baseado nas iterações dos nodos e com o auxílio de informações providas por entidades terceiras. Após estas informações terem sido calculadas, se pode chegar a um valor que mede a confiança de um nodo em outro e ainda uma possibilidade de avaliar e calcular a reputação.

Thompson *et al.* [2], sinaliza a base de um mecanismo de confiança entre entidades partes com o uso de certificação digital, contudo não aborda assuntos envolvendo relacionamentos de confiança entre autoridades certificadoras, suas autoridades de registro ou ainda entre as entidades e os provedores de recursos.

Fazendo uma análise simples do exposto até o momento, considerando as principais características dos grids computacionais, torna-se difícil criar ou definir estabelecimentos de confianças fixos, até mesmo porque uma relação de confiança possui um tempo de vida limitado e não deve sobrecarregar a execução de tarefas no Grid.

É importante ressaltar que o estabelecimento de confiança não deve ter uma intervenção manual, como por exemplo, uma equipe de administração da rede. Ela deve ser automatizada e independente, até mesmo porque usuários que se conectam a um Grid, além de buscar serviços e recursos, também podem oferecê-los. E dentro deste cenário, também podem definir quais são os seus próprios critérios de segurança, englobados pela política de segurança do Grid. Além disso, como a infra-estrutura de um Grid ultrapassa as fronteiras individuais de uma organização, novamente entra em foco a necessidade do estabelecimento de regras ou mecanismos de confiança. Até mesmo porque a execução de uma tarefa ou solicitação de outro recurso pode estar fora do Grid local, sendo necessária a comunicação com outro Grid.

Segundo a análise realizada por Ferreira e Schulze [32], três itens devem ser considerados em uma proposta de infra-estrutura de segurança para o Grids: integração, interoperabilidade e relacionamento de confiança. Isto torna a necessidade de confiança como um pré-requisito para a escalabilidade de Grids, organizações virtuais e a distribuição de identidades.

Li *et al.* [34] apresentou um trabalho com o objetivo de mostrar um modelo de confiança de dois níveis (ou camadas) e seus correspondentes algoritmos de métricas de

avaliação de confiança, elevando a segurança em infra-estrutura de um Grid. No modelo elaborado, existe um mecanismo de avaliação integrada de confiança para suportar serviços seguros e transparentes através de domínios seguros, sendo projetada uma implementação para adequar o esquema de confiança com o foco na segurança de uma infra-estrutura de um Grid.

Os dois níveis da arquitetura de Li *et al.* [34] são o domínio (nível mais inferior) e a organização virtual (nível mais superior). Esta estrutura surgiu devido ao fato dos recursos de segurança e gerência em um mesmo domínio (intra-grid) e fora do domínio (extra-grid ou em uma organização virtual) serem diferentes, concluindo que domínios e organizações virtuais precisam adotar modelos de confiança diferentes.

De uma forma geral, a confiança em Grids envolve diversos modelos e teorias que devem ser aplicadas e desenvolvidas com o intuito de resolver as questões que tratam da comunicação e da segurança entre nodos em um Grid e entre Grids.

2.4 P2P E CONFIANÇA

Redes P2P também são classificadas como um ambiente distribuído ([35], [36]). Como complemento do tratamento da confiança aplicada a sistemas distribuídos, este tópico trata diretamente de algumas definições de P2P e de confiança aplicada a P2P. Na seqüência, primeiro se apresentam as principais definições de P2P, e no tópico seguinte algumas revisões sobre a aplicação da confiança em tais ambientes.

2.4.1 Definição de P2P

Atualmente, existem diversas referências ([35], [36], [39], [40]) que tentam fazer uma definição e uma classificação de redes P2P. Basicamente, um sistema pode ser definido como Peer-to-Peer (P2P) se as entidades envolvidas na rede que compõe o sistema compartilham uma parte de seus próprios recursos (normalmente de hardware - processamento, armazenamento, banda passante etc.). Neste tipo de sistema, tais recursos são necessários para o provimento de serviços e conteúdo, que são ofertados na rede (compartilhamento de arquivos, espaços de colaboração mútua, entre outros).

Em uma situação normal em sistemas P2P, os serviços e recursos podem ser acessados por todas as entidades participantes na rede sem necessidade de passar por alguma entidade

intermediária. Observa-se então que os participantes são provedores de recursos e ao mesmo tempo podem demandar acesso aos mesmos recursos que oferta.

Para Rocha [35], apesar de algumas confusões de conceitos envolvendo redes P2P e arquitetura cliente-servidor, a definição é clara porque nas redes cliente-servidor, uma entidade provê o serviço e a outra consome o serviço. Isto gera uma diferença básica da arquitetura cliente-servidor tradicional porque em P2P, a entidade pode funcionar tanto como cliente (fazendo requisições de serviços) como servidor (servindo serviços a outras entidades) e já na arquitetura tradicional cliente-servidor, a entidade só pode funcionar como uma de cada vez.

Stoica *et al.* [36] observa os sistemas e as aplicações P2P como distribuídas sem qualquer forma de controle centralizado ou hierarquia organizacional, de tal forma que o software que está sendo executado em cada nó é equivalente em funcionalidade. Em um primeiro momento, pode-se afirmar que redes e sistemas P2P possuem aspectos técnicos em comum que envolve a sua auto-organização, a adaptabilidade e a escalabilidade, em que todos os nós possuem capacidades e responsabilidades idênticas. Assim, a rede se organiza e depende da participação voluntária dos nodos, contribuindo com os recursos sob qual a infra-estrutura é construída.

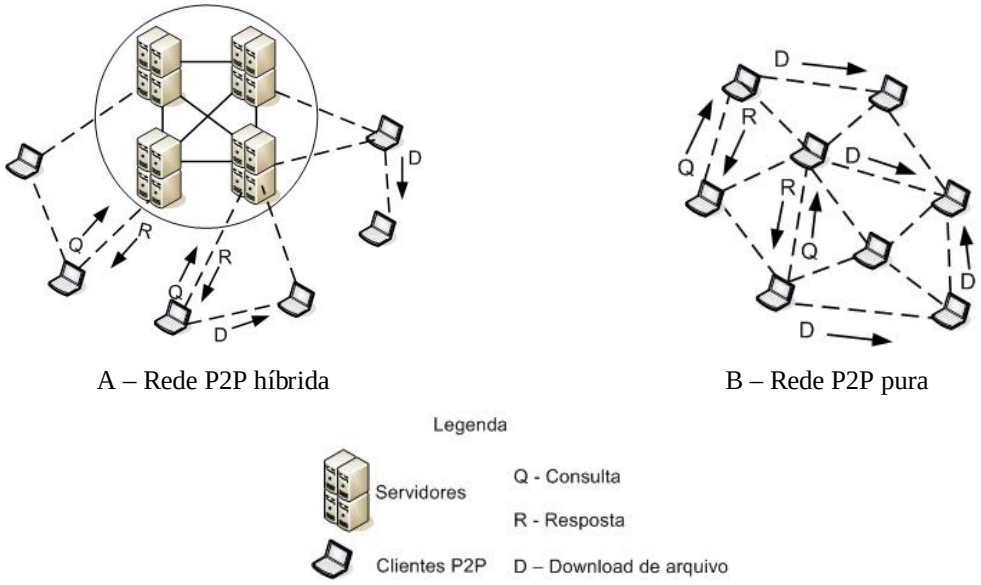
Ge *et al.* [37] fez uma classificação de redes P2P dividindo-as em três grupos distintos, denominados de CIA (*Centralized Indexing Architecture*), DIFA (*Distributed Indexing with Flooding Architecture*) e DIHA (*Distributed Indexing with Hashing Architecture*). A Tabela 2-3 resume as características da classificação proposta por Ge *et al.* [37].

Tabela 2-3 – Classificação de sistemas P2P segundo Ge *et al. [37]*.

Classificação	Descrição
CIA	Contêm um servidor central ou um cluster de servidores que é responsável por responder os pedidos de busca e realizar todas as tarefas de manutenção da infra-estrutura. O principal exemplo e precursor desta arquitetura foi o NAPSTER [38].
DIFA	Caracterizada pela completa descentralização de seu funcionamento. Os mecanismos de busca e manutenção da infra-estrutura estão distribuídos pela rede, onde cada nó é responsável por manter a listagem dos seus próprios arquivos, e responder quando receber uma busca para um arquivo.
DIHA	Arquitetura, que conforme a DIFA, também possui uma característica totalmente descentralizada. A principal diferença entre as redes DIFA e DIHA está no mecanismo de busca. Na DIHA, cada nó é responsável por um subconjunto do espaço total de índices, onde o nó que entra na rede recebe um espaço do conjunto dos índices dos arquivos. Ao sair da rede, esta deverá designar estes índices para outro nó. As buscas são direcionadas para o nó correto que é o responsável pelo respectivo índice dentro do espaço de índices.

Schollmeier [39] realiza outra classificação de redes P2P, a dividindo basicamente em redes puras e redes híbridas. Uma arquitetura do tipo híbrida (representado pela Figura 2-6 A) não é inteiramente distribuída, dependendo de um elemento central (servidor de algum tipo de dado centralizado) para o seu funcionamento. Já uma rede P2P Pura (representado pela Figura 2-6 B) é aquela que possui uma arquitetura inteiramente distribuída e não necessita de um elemento central para o seu funcionamento.

Fazendo-se uma comparação com a proposição de Ge *et al.* [37], os modelos DIFA e DIHA encontram-se dentro da classificação de uma rede P2P pura, enquanto que redes do tipo CIA são Híbridas.



A – Rede P2P híbrida

B – Rede P2P pura

Figura 2-6 – Redes P2P hibrida e pura segundo Schollmeier [39]

Segundo a classificação de Schollmeier [39], nas redes puras, os nodos são responsáveis por todas as transações entre si (roteamento, autenticação, controle sobre as seções, manutenção de bases de dados), além de gerenciarem todas as informações que sejam relevantes para a aplicação que se utilize dessa rede. Por sua vez, nas redes híbridas existem servidores centrais responsáveis pela execução de tarefas consideradas como críticas (indexação de informação, aspectos voltados para a segurança - integridade dos dados, segurança no processo de transferência, dentre outras funções).

Devido ao constante aumento dos recursos de processamento e de largura de banda atualmente disponíveis, os sistemas P2P obtiveram um impulso extra, fazendo com que diversas aplicações usem a sua arquitetura. Como exemplo de aplicações que envolvem P2P cita-se compartilhamento de arquivos, processamento distribuído, webcaching, disseminação

de conteúdo, backup distribuído, telefonia IP, banco de dados descentralizados, serviços de mensagens instantâneas (Instant Messaging), jogos, entre outros.

Para uma melhor explicação sobre a arquitetura P2P, que inclusive é objeto da implementação de parte do modelo proposto neste trabalho, o framework JXTA [40] será explicado no capítulo 5.

2.4.2 Confiança em P2P

No tratamento da confiança aplicado a redes P2P existem diversos pesquisadores ([5], [16], [41], [42], [43]) e desenvolvedores que canalizaram esforços para o desenvolvimento de soluções neste tipo de sistema distribuído.

Duma *et al.* [16] sinalizam que um dos desafios fundamentais em redes e sistemas P2P está relacionado com os riscos de interação e colaboração com entidades desconhecidas e que podem ser potencialmente maliciosas. Apontam que os sistemas atuais de reputação não são capazes de reagir adequadamente a mudanças rápidas de comportamento de entidades pares. Como possível solução, um trabalho de métrica de confiança que satisfaça estas necessidades é proposto [16], sendo capaz de identificar e punir mudanças bruscas no comportamento de entidades pares, além de verificar possíveis oscilações do comportamento, indicando a possibilidade de que uma ação maliciosa possa ocorrer.

No estudo realizado por Suryanarayana e Taylor [5], os sistemas P2P que não regulamentam a entrada de novos nodos na rede estão sujeitos a riscos elevados porque podem se sujeitar ao recebimento de informações espúrias e terem nodos atuando como sendo outros nodos na rede (manipulação de identidades).

Isto implica que cada peer precisa analisar as informações recebidas pelo outro peer para determinar o nível de confiança tanto da informação quanto do remetente. Observando estes pontos, Suryanarayana e Taylor [5] levantaram os questionamentos voltados para a necessidade de gerenciamento de confiança, e apontam que os nodos devem ser responsáveis por avaliar a informação recebida por outros nodos para comprovar sua confiabilidade e também avaliar, de certa forma, o comportamento dos outros nodos.

Para Suryanarayana e Taylor [5] tanto a reputação quanto a confiança devem ter características que são consideradas importantes no contexto de sistemas e ambientes P2P. Estas características estão sintetizadas na Tabela 2-4.

Suryanarayana e Taylor [5] ainda fazem uma classificação da gerência de confiança voltada para a reputação e a dividem em três categorias. A primeira foi definida como sendo

baseado em credencias, onde os requisitantes de serviços não podem ser totalmente confiáveis enquanto que os provedores de serviço e o seu serviço podem ser. Na segunda classificação, definida como sendo baseada em reputação, a confiança deve ser adquirida pelas iterações do próprio nodo e também podendo ser através de informações dadas por terceiros. Na terceira, denominada de redes sociais (*social networks*), a confiança é mensurada através de relacionamentos entre os nodos e os vários papéis desempenhados pelos mesmos em suas comunidades. Idéia apoiada por Patel [3].

Tabela 2-4 – Características de reputação e confiança [5]

Característica	Justificativa
Controle local	Inclui valores de confiança e reputação, bem como outras informações e recursos. É usado para distinguir mecanismos de confiança que trocam valores locais dos que não trocam.
Valores de confiança e reputação	Representam a confiança que um peer tem em outro, através de valores que podem ser discretos ou contínuos.
Tipo de reputação	Indica o tipo de reputação utilizado por um modelo de confiança. São utilizados três tipos: reputação positiva, reputação negativa ou uma combinação dos dois.
Verificação de assinatura	Usada para distinguir modelos de confiança que usam explicitamente verificação de credencial para estabelecer a autenticidade do emissor da mensagem.
Anonimato	Utilizada para proteger a identidade dos peers, a fim de protegê-los de ações maliciosas. Essa propriedade ignora as relações de confiança entre os peers.
Custo de largura de banda	A troca de mensagens entre os peers resulta em muito tráfego sendo gerado simultaneamente, que acarreta em um aumento na utilização da banda. Reduzir esta utilização é um objetivo muito importante para qualquer modelo de confiança.
Custo de armazenamento	Utilizado em modelos de confiança que necessitam que os peers armazenem informação acerca de outros peers. Este custo aumenta linearmente com o número de peers.
Tolerância à falhas	Representa a habilidade do modelo de confiança de se adaptar à natureza transiente do sistema (mudanças de topologia).
Escalabilidade	Remete à habilidade de um modelo de confiança de se adaptar a um aumento do número de peers.
Confiabilidade	Refere-se à habilidade de um modelo de confiança em determinar corretamente a extensão da confiança nos outros peers baseado em experiências passadas e/ou em informações recebidas de outros peers. A confiabilidade também é determinada pela tolerância à falhas do modelo.

Por fim, Suryanarayana e Taylor [5] indicaram um modelo de gerência de confiança, envolvendo questões de segurança e armazenamento, ambos voltados para tecnologias que necessitam de princípios envolvendo a confiança e reputação. Nesse sentido, modelaram a confiança em categorias, cada uma tratando de aspectos próprios envolvendo sistemas P2P.

Diversos aspectos voltados para a confiança em sistemas P2P também foram mapeados no trabalho realizado por Aberer e Despotovic [41], afirmado que os métodos existentes estão focados em reputação, envolvendo propriedades semânticas de um modelo de confiança. Nesse sentido, Aberer e Despotovic [41] citam que os modelos descritos não são escaláveis. Para solucionar a questão criam um método descentralizado que permite aos nodos alcançar um nível de confiança baseado no cálculo da reputação, com valores mensurados através de iterações realizadas com outros agentes.

De uma forma geral, o proposto por Aberer e Despotovic [41] define que a gerência de confiança baseia-se na análise de transações passadas e recentes dos agentes, criando assim uma idéia de reputação de um agente na rede e até mesmo um contexto histórico de iterações entre determinados nodos.

Envolvendo esquemas de justiça relacionada ao uso de sistemas P2P, Ngan *et al.* [42] relata que os usuários em redes P2P não se vêm obrigados a fornecer uma contrapartida pelo uso de recursos, até mesmo porque os conseguem "gratuitamente". E também questionam sobre a definição ou criação de mecanismos de hierarquia dentro de uma rede P2P, de tal forma que um mecanismo de confiança não pode ser baseado em nenhum critério que dependa de "importância" de um nodo sobre outro. Este ponto é questionável devido à criação de organizações virtuais, simulando o comportamento de uma sociedade ou de uma comunidade, na qual de uma forma ou de outra existe a figura de um líder ou um grupo que exerce a liderança. O enfoque dado por Ngan *et al.* [42] não pode ser estendido neste contexto se for necessário para a organização do grupo, e até mesmo se for necessário segundo requisitos de confiança para um grupo ou uma comunidade virtual, a identificação do grupo (uma espécie de rótulo do grupo) e não apenas um único nodo na rede.

Nelson e Pitigoi-Aron [43] citam a elaboração de diversos modelos de confiança voltados para P2P e apontam a falta de critérios que facilitem a implementação de tais modelos em sistemas reais. E como uma proposta inicial de solução, desenvolveram um modelo de confiança em redes P2P baseado em certificação digital capaz de trocar informações sobre confiança, entretanto não demonstram resultados práticos do trabalho realizado.

Um fato importante a ser considerado em um modelo de segurança em redes está relacionado com a certificação digital. O principal problema é que não se pode ter uma autoridade certificadora centralizada em redes distribuídas, de acordo com a análise realizada em de Sousa *et al.* [13], porque todos os aspectos de gerenciamento não são alcançáveis em redes descentralizadas.

Além disso, somente a associação de um certificado a uma entidade não garantirá que essa entidade não possa gerar um par de chaves que a substitua em determinado momento, até mesmo porque não existe certificação cruzada nestas situações, não tendo como ser verificado determinados detalhes (assinatura, emissão dos certificados etc.). É importante ressaltar que uma autoridade certificadora em redes distribuídas é altamente complexa em termos de utilização em ambientes reais por motivos já explicados em de Sousa *et al.* [13]. Desta forma um outro modelo que garanta a segurança em sistemas distribuídos deve ser pensado, e a confiança se propõe a preencher parte desta lacuna.

Com o intuito de resolver problemas de descentralização em redes P2P, Aberer *et al.* [44], produziram informações voltadas sobre o sistema P-GRID. Em um dos vários assuntos abordados, a questão da confiança e da reputação é tratada como sendo um foco importante em redes distribuídas voltados para identidade de nodos. No modelo proposto por Aberer *et al.* [44] foi desenvolvido uma base individual sobre as iterações passadas envolvendo diversos nodos com que já foi estabelecido algum tipo de contato. Além disso, também foi endereçado o problema de opiniões externas sobre um determinado nodo. Em outras palavras, um mecanismo de coleta de opiniões e cálculo da reputação para redes P2P com a implementação do P-GRID.

Num breve relato do trabalho de Cáceres *et al.* [45], existe uma tendência de sistemas de agentes inteligentes ou agentes de software de serem amplamente integrados em redes P2P (também denominado pelo autor como IP2P). A finalidade é a garantia do espalhamento de requisições de serviços em nome do usuário em várias infra-estruturas de transmissão distintas e ainda garantir a confiança do serviço que por ventura envolva uma variedade de provedores.

Conforme as revisões bibliográficas discutidas brevemente, a confiança esta sendo amplamente discutida em redes P2P. Todavia, ainda não existe um consenso de sua aplicação e utilização como um todo. Isto permite que sejam feitas algumas análises iniciais.

Primeiramente, um modelo de confiança em P2P serve para alavancar problemas conhecidos que não são resolvidos com simples certificados digitais ([3], [5], [13]). No entender deste trabalho e da pesquisa realizada, um modelo de comunicação através de certificação digital não garantirá a identidade de um nodo ou um serviço porque é muito difícil de se conseguir alcançar alguns requisitos de identidade em redes distribuídas através certificação cruzada. Entretanto, está claro que alguma forma de criptografia para a troca de mensagens deve ser pensada para evitar ataques como o Sybil [12] e ainda ter a garantia do sigilo da comunicação.

Em segundo lugar, um modelo de confiança deve ter a idéia da representação da reputação, entre outros requisitos, associado à aquisição, tratamento, gerenciamento e processamento da confiança. E como as redes P2P são altamente distribuídas e fracamente acopladas em termos de disponibilidade de um ou outro nodo (não se sabe se um nodo estará na rede ou não no momento em que se precisa dele), a garantia de se comunicar com o nodo certo requer que critérios de confiança sejam estabelecidos previamente, a fim de evitar a manipulação de identidade.

Estendendo a discussão, os mecanismos de avaliação da confiança por ventura adquiridos, deve evoluir com o passar do tempo e com as iterações que por ventura, venham a ocorrer. Assim a confiança em redes P2P agrega valor ao entendimento e aplicação da confiança em ambientes computacionais distribuídos.

2.5 AGENTES DE SOFTWARE E CONFIANÇA

Nos diversas referências pesquisadas percebe-se que a confiança e a reputação trabalham muitas vezes de forma complementar e outras vezes de forma individual. Agentes de software é outro exemplo de sistemas distribuídos que tratam de aplicar a confiança e serve como base de implementação de modelos e estudos práticos. Nos tópicos a seguir, explica-se um pouco sobre agentes de software e na continuação sobre a aplicação da confiança neste cenário.

2.5.1 Definições de agentes de software

A definição de agentes de software é motivo de discussão, não se tendo uma conclusão única para a definição do termo [46], até mesmo devido à área e variedade de abrangência do uso de agentes. A definição adequada de agentes de software faz um forte paralelo com os conceitos aplicados em agentes inteligentes. Desta forma a definição depende do seu nível de abrangência em um determinado sistema, das modificações no ambiente e da reatividade do agente no ambiente, ou seja, para se definir um agente software e se é ou não inteligente, é necessário definir primeiro o seu ambiente de atuação e as suas respectivas reações.

Os agentes de software dotados de certa inteligência são objetos de pesquisa na área de inteligência artificial ([46], [47]). Entretanto, é dependente de sistemas de redes pelo fato de necessitarem de mecanismos de troca de informação, abrindo ainda mais o leque de ligação com outras áreas. Esta troca de informações é necessária para os agentes criarem a sua base de

conhecimento, de onde, através de análises, o agente deverá buscar informações e reagir a uma determinada situação, permitindo o agente se adequar ao seu ambiente ou executar determinada tarefa.

Neste ponto, um paralelo com a confiança é apropriado porque todo o conhecimento de confiança e reputação adquirido tem de ser armazenado, o que complementa a base de conhecimento do agente, e ainda considerando a perspectiva de organizações sociais, a confiança e a reputação podem ser definidas tanto no comportamento humano quanto no ambiente computacional como uma forma de habilidade social que está relacionada com a segurança que se deseja obter [3] [9].

Em ambientes reais, é esperado que um agente de software possua algumas funcionalidades comparadas ao comportamento humano [47]. Essas características envolvem a adaptabilidade ao meio, independência, criatividade, reação, entre outros. Isto implica que um agente deve executar uma tarefa delegada por um usuário e não sofrer o comando direto do usuário para e durante a execução da tarefa.

Nas décadas de 70 e 80, o uso de agentes era restrito a apenas um computador ou uma rede homogênea [9]. Com o avanço da internet e do poder de processamento existente atualmente, o seu uso passou a ser muito mais difundido, de forma que agentes adquiriram novas características que os tornaram capazes de realizar tarefas mais complexas baseados em seu conhecimento e aprendizado (base de conhecimento adquirida). Assim um agente deve possuir conhecimento necessário, e aprender o mínimo necessário para a execução das tarefas as quais foi submetido, sem interferência humana, e retornar o produto do trabalho realizado ao usuário.

2.5.1.1 Classificação de agentes

Segundo Morreale [47], agentes devem possuir cinco características que os diferencia de um software convencional: autonomia, reatividade, aprendizado, cooperação e mobilidade. Ainda segundo Morreale [47], a autonomia, o aprendizado e a cooperação são características que se sobressaem sobre as demais, e classifica um agente como sendo básico (se implementar pelo menos uma das três características), avançado (se implementar duas das três características) e ideal (se implementar as três).

As melhores definições de agentes estão relacionadas a um sistema computacional que depende do ambiente e que possua as características de autonomia, habilidade social, reatividade, iniciativa, entre outros, e com um objetivo bem definido [48]. Em alguns casos é necessário saber como um agente executa suas tarefas para alcançar o seu objetivo.

Agentes de software são classificados de acordo com o agrupamento de características que possuem em comum. De acordo com Nwana [48], agentes podem ser classificados de acordo com cinco critérios diferentes. A primeira classificação diz respeito à mobilidade (móvel ou estático). A segunda classificação define agentes como reativos ou deliberativos (modelo interno representando o raciocínio). A terceira classificação de agente corresponde ao conceito dos atributos primários e ideais que um agente deve possuir ou exibir (autonomia, cooperação, aprendizagem). Até este nível de classificação é possível definir agentes em quatro grandes grupos: agentes colaborativos, agentes de aprendizagem colaborativos, agentes de interface e agentes de software inteligentes. A Figura 2-7 ilustra esta divisão de acordo com os atributos primários de um agente.

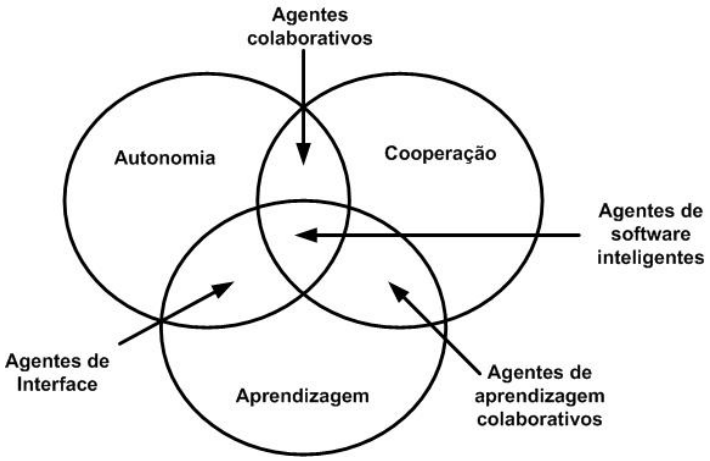


Figura 2-7 – Divisão de agentes segundo atributos primários [48]

2.5.1.2 Agência

Segundo Wooldridge e Jennings [46], uma forte definição de agência está relacionada ao comportamento de agentes, seja ele conceitualizado ou implementado, associado a conceitos aplicados aos seres humanos. Esta definição ainda está associada a pesquisas em áreas de inteligência artificial, que prevê noções mentais aos agentes como conhecimento, crença, intenção e obrigação.

As necessidades fundamentais para implementação de agentes baseados em software estão relacionadas com a representação do conhecimento, a forma com que é manipulado o conhecimento e a sua troca (porções de modelos mentais) entre agentes, comunidades de agentes e seres humanos. E todos estes aspectos podem de uma forma ou de outra estarem relacionados com a confiança e a reputação, influenciando diretamente no comportamento dos agentes.

Quando se trata do comportamento dos agentes de software, o grau de autoridade e autonomia que lhe é outorgado também pode ser definido como agência. Esta por sua vez pode ser mensurada de forma qualitativa, de acordo com a interação entre o agente e outras entidades no sistema no qual atua ([46], [48]). Esta atuação pode ser através de interação com aplicações, base de dados informacionais, bem como outros agentes.

Uma vez que o ambiente no qual um agente está inserido se torna mais imprevisível ou inovador, é necessário que o agente incorpore mais agência. Esta incorporação faz com que o agente atualize seu estado de modelos "mentais" através de estímulos do ambiente ou através de decisões internas, como por exemplo, através da influência da confiança e da reputação.

Na maior parte do desenvolvimento dos modelos de inteligência aplicados à construção de agentes de software, as abordagens mais bem sucedidas estão orientadas à solução de problemas muito bem delimitados ([47], [49]). Problemas relacionados à execução de atividades rotineiras, complexas e colaborativas nas áreas de engenharia, gerência e manufatura têm obtido sucesso no uso de agentes inteligentes [49]. Outras aplicações práticas de agentes inteligentes tem sido a construção de assistentes de comunicação pessoal, capazes de cuidar de detalhes como organizar correio eletrônico, realizar filtragem de informações, organizarem agendas de compromissos, gerenciar reserva de hotéis e passagens etc.

Ainda de acordo com Wooldridge e Jennings [46], outras características associadas à agência dizem respeito a sua mobilidade, veracidade, benevolência e racionalidade. Desta forma, agência está relacionada com a capacidade de autonomia e autoridade, influenciadas pelo ambiente e características associadas à inteligência que um agente deve possuir.

2.5.1.3 Linguagem de comunicação

Agentes necessitam tanto de modelos de representação quanto de comunicação. O modelo de representação está mais voltado à ontologia ([27], [50]), que diz respeito à especificação de como interpretar objetos, conceitos e demais entidades que supostamente existem em alguma área de interesse e o relacionamento existente entre eles. Por sua vez os modelos de comunicação estão voltados para o modelo mental de um agente (intenções, crenças, desejos etc.) dentro de um domínio de uma comunidade de agentes [46]. Este modelo de comunicação é conhecido como linguagem de comunicação de agentes ou *agent communication language* (ACL). Sua função é prover primitivas de linguagem que um agente implementa em um modelo de comunicação (enviar mensagens, solicitar informação, avisar, responder, requerer, comandar etc.).

Nos conceitos de confiança e reputação uma ACL é de fundamental importância porque toda a troca de informação e de gerenciamento de grupos é derivada de uma linguagem formal de comunicação [49], definida entre agentes. Em outras palavras, para se haver comunicação no ambiente de agentes, eles devem falar o mesmo "idioma". A aquisição da confiança e seus respectivos passos requerem que um modelo de comunicação exista e que tenha os requisitos de segurança mínimos de confidencialidade, integridade e disponibilidade.

2.5.2 Confiança em agentes de software

A confiança aplicada a agentes de software pode resolver problemas de iterações dos usuários e a formação de comunidades virtuais com "afinidades" em comum, sendo estas atividades realizadas por sistemas de agentes em nome do usuário final ([3], [9]). Isto de uma forma ou de outra cria uma "sociedade" com afinidade similar, o que facilita a busca de informações e a interação na rede. O agente pode até mesmo agir em nome do usuário, seguindo ordens previamente estabelecidas, forçando em determinados casos a uma tomada de decisão por parte do componente de software, e se necessário extrapolar a sociedade formada ou se manter dentro dela.

Para se alcançar este nível de capacidade de decisão, os requisitos funcionais de um agente devem ser bem elaborados e possuir os "modelos mentais" que façam com que o agente, por si só, aprenda em seu ambiente. Considerando este aspecto de capacidade de aprendizagem, é possível inferir que existe um problema de segurança e de confiança ([3], [7]), porque em tais ambientes não é possível que o agente saiba que a informação recebida seja verdadeira, se não possuir mecanismos de como verificá-la. Isto implica que através de algum instrumento, o agente tenha a garantia de que a informação recebida não foi manipulada por uma entidade maliciosa. Ou até mesmo por uma entidade que estaria se passando por outra, com o intuito de prejudicar a comunicação ou a troca de informações no ambiente em si. Desta forma, um agente deve ser capaz de fazer interpretações para evitar que dados infundados sejam utilizados.

Partindo desse pressuposto, é necessária a definição de métricas capazes de assegurar uma comunicação com requisitos de segurança e de confirmação da informação em tais ambientes. E ainda de manter um registro histórico dos fatos ocorridos para auxiliar nas definições de confiança e de reputação em sistemas de agentes distribuídos, sem mencionar o sigilo da comunicação, que é útil em determinados casos.

Agentes de software são capazes de realizar tarefas dotadas de certa complexidade em redes de computadores [51]. Tais sistemas utilizam camadas de comunicação seguindo uma linguagem definida, uma base de conhecimento e uma rotina de execução de tarefas. É importante ressaltar que a automação de tarefas com uso de agentes de software envolve uma série de detalhamentos sobre o que é a "inteligência" do agente e o seu "limite" de conhecimento. Tais problemas são comumente assinalados e estudados na literatura voltados para requisitos de inteligência artificial ([46], [47], [48]), seguidos de modelos de comunicação ([49], [50]). Isto permite que agentes de software possam desempenhar um papel importante em sistemas distribuídos. Entretanto, é importante considerar que nestes ambientes, o modelo deve ser escalável, capaz de atender demandas heterogêneas com uma variedade de serviços, middleware, sistemas operacionais, entre outros, e sem um controle central.

Com o foco em segurança da informação através do uso de sistemas multi-agentes, Poggi *et al.* [17], apresentou um modelo embasado em certificação digital com o intuito de gerenciar as regras em relações de confiança em agentes de software. O modelo prevê o seu uso dentro de uma sociedade de agentes colaborativos, sob uma determinada infra-estrutura, e cita que a importância de um modelo de segurança que envolva agentes de software deve ser robusto e flexível, com a finalidade de auxiliar no desenvolvimento da confiança e das iterações entre os agentes.

Considerando aspectos de confiança, existe a necessidade de que os agentes de software sejam capazes de criar e analisar iterações entre si com o intuito de realizar um determinado serviço ou atender uma determinada solicitação do usuário, até mesmo porque isto auxilia nas definições de valores e métricas de confiança e reputação ([3], [17]).

No trabalho proposto por Zhang e Xu [52], foi desenvolvido o conceito de RADE (*Role-based agent development framework*) a fim de permitir o maior reuso de sistemas multi-agentes e aumentar a robustez destes sistemas. Além disso, de desenvolver de forma geral mecanismos de planejamento/agendamento e de colaboração/cooperação entre agentes. Tal modelo é novo e ainda não está incorporado em frameworks de agentes, necessitando um melhor estudo e detalhamento do tema. Até o momento da conclusão desta pesquisa, tal modelo não estava explicitamente disponível para ser testado.

Segundo Poggi *et al.* [53], aplicações baseadas em agentes requerem delegação de tarefas para alcançar determinados objetivos e requerem cooperação com entidades, muitas vezes necessitando de direitos de acesso, o que aponta para uma infra-estrutura de segurança distribuída. Em seu trabalho realizaram uma análise de princípios de gerencia de confiança e

de certificação digital através de agentes com a plataforma JADE [54], e como poderiam ser aplicados em sistemas multi-agente.

Vale ressaltar neste ponto que em ambientes em que a confiança é necessária ou está inserida, conforme já sinalizado anteriormente por ([3], [12], [13], [49]), a certificação digital trará auxílio na confidencialidade e na integridade da informação. Entretanto as questões que envolvem a identificação única em uma rede distribuída não podem ser mapeadas através de certificação digital, porque qualquer um pode gerar um par de chaves e assumir uma identidade, favorecendo claramente técnicas como o ataque sybil [12]. Além disso, conforme já citado, a certificação digital distribuída e cruzada não permite determinadas situações sob aspectos de escalabilidade e gerência ([13], [19]).

Para Ramchurn *et al.* [55], agentes autônomos que fazem parte de ambientes abertos podem quebrar contratos, indicando que a confiança tem um papel importante nestes modelos computacionais para a determinação de com quem interagir e como as iterações se conduziram. Seguindo esta linha de raciocínio, foi desenvolvido um modelo de confidência e reputação, usando conjuntos fuzzy, guiando agentes através de avaliações de iterações passadas e estabelecendo novos contratos de cooperação.

Questões que envolvem agentes de software e confiança também são áreas de estudo e de pesquisa de diversos autores em diversas áreas abrangendo os temas da confiança e da reputação, conforme a revisão de alguns trabalhos neste tópico. No capítulo 3 serão apontados e revisados modelos de confiança e reputação usados em sistemas distribuídos com o uso de agentes de software.

2.6 REDES MANET E CONFIANÇA

Devido as suas características (ausência de controle centralizado, rede amplamente distribuída, entre outros), as Redes MANET [56] são utilizadas em diversas áreas do conhecimento. Dados seus aspectos técnicos, estudos que tratam da confiança computacional também são aplicados nesse tipo de tecnologia.

2.6.1 Definições de redes MANET

Existem diversas pesquisas e grupos trabalhando atualmente com enfoque em MANET [56]. Segundo as definições realizadas por Amvame-nze [57], Mobile Ad hoc NETwork (MANET) são redes sem fio nas quais os nodos móveis têm possibilidade de

trocarem informação sem o auxílio de uma rede infra-estuturada. A literatura aponta que essas redes também podem ser conhecidas como redes espontâneas, em que os nodos se comunicam diretamente entre eles, ponto a ponto.

Devido à ausência de infra-estrutura física cabeada, o que facilita a implementação de sistemas específicos para roteamento, serviço de nomes, entre outros, nas MANETs os serviços de roteamento são estabelecidos de maneira cooperativa, de tal forma que cada nó integrante de uma rede MANET é capaz de atuar como um possível roteador. Assim, se for o desejo de um nó estabelecer um canal de comunicação com outro nó, fora do seu alcance (relacionado com a área de cobertura de rádio freqüência), este pode encaminhar seus pacotes com o auxílio dos nodos vizinhos até que os pacotes cheguem ao nó de destino.

Em uma MANET, os nodos podem entrar e sair de uma área de cobertura de outros nodos continuamente e a qualquer momento. Isto resulta que a adesão dos nodos com uma MANET é mantida dinamicamente, o que gera mudanças freqüentes e normalmente imprevisíveis no ambiente e na topologia da rede devido à mobilidade.

Desta forma as MANETs podem ser consideradas redes móveis com características de salto múltiplos em que a conectividade entre os nodos é assegurada através de um protocolo de roteamento colaborativo, normalmente dividido em pró-ativo ou reativo ([13], [57]).

2.6.2 Confiança em redes MANET

Devido a sua característica de ser distribuída, não se ter controle direto sobre entrada e saída de nodos, não ter nenhum mecanismo de gerência centralizado, as redes MANETs também possuem aspectos em que a aplicação da confiança aparece como um requisito para auxiliar a identificação de nodos e auxiliar nos mecanismos de controle e aumento da segurança ([13], [55], [58], [59]).

Li [58] voltou a aplicação da confiança para redes MANET [56], onde se criou um modelo de confiança aplicado à decisões de roteamento neste tipo de redes. A idéia principal foca que um nodo *n1* é capaz de julgar se outro nodo *n2* pode ser de confiança. Esta inferência é realizada através de uma capacidade que o nodo *n1* tem de “formar uma opinião” sobre o nodo *n2* e decidir se pode comunicar-se com ele. O modelo ainda estende a discussão prevendo que o nodo *n1* pode requerer provas por outras maneiras de *n2* que é confiável.

Gligor [59] também cita a importância de confiança em redes Ad Hoc e em outras tecnologias. Segundo Gligor [59], o estabelecimento da confiança deve ser baseado em avaliação dinâmica de uma evidência assinada sobre um nodo (localização, identidade,

atributos de configuração, entre outros) e não apenas em relacionamentos definidos estaticamente segundo um protocolo de roteamento. Isto implica que o tempo ou a localização do nodo não pode antecipar e prever um relacionamento de confiança (devido à mobilidade da rede), tornando esta questão incerta. A extensão do problema indica ainda que o estabelecimento dinâmico de relações de confiança deve ser capaz de detectar relacionamentos não desejáveis, assegurando uma maior confiabilidade ao nodo em si.

De Sousa *et al.* [13] reforça a necessidade da confiança envolvendo MANET, e estende a discussão para aspectos tratando de auto-configuração, autenticação e certificação. Os problemas tratados neste cenário questionam a certificação distribuída como forma de se garantir a segurança da rede e por conseqüência a confiança aplicada aos nodos. Segundo o trabalho realizado por de Sousa *et a*l. [13] a análise do problema de confiança requer que sejam discutidos outros aspectos que envolvam não somente autenticação ou auto-configuração, porque neste ponto a certificação distribuída é baseada em limiares de informação utilizando o esquema criptográfico proposto por Shamir [60].

Na análise dada por de Sousa *et al.* [13], um determinado valor K deve ser distribuído entre um grupo de N nodos, que deve se juntar para gerar novas assinaturas de certificados. O problema, quando observado sob o prisma de MANET, é que não existe a garantia da reunião de N nodos de acordo com a necessidade de assinatura. O tamanho de K também influencia na segurança porque se o valor de K for muito pequeno computacionalmente e se N – 1 nodos forem comprometidos, o valor de K é descoberto facilmente. E também não se tem a garantia de que N nodos seja um número bom ou não, dado as características da MANET, influenciando diretamente na real aplicação e utilização do modelo.

Ainda dentro desta análise, um modelo de coalizão, baseado em certificação distribuída (segredo de assinatura compartilhado), pode ser prejudicado com o ataque Sybil proposto por Douceur [12]. O princípio básico deste ataque versa que *n* identidades falsas podem ser geradas por um único atacante, de forma que o relacionamento parecerá ser realizado a várias entidades, onde na verdade, existe apenas um nodo, com *n* disfarces.

O trabalho realizado por Adnane *et al.* [61], mostra os tipos diferentes de relações de confiança em MANET utilizando informações de roteamento do protocolo OLSR. Ainda aponta o processo de construção da confiança, permitindo assim a análise de requisitos para a confiança no protocolo OLSR e tratando os ataques como traições às relações de confiança. A análise do trabalho permite apontar indicadores para que nodos que usam o OLSR possam ter um comportamento de proteção contra ataques e maus comportamentos quando trabalhando efetivamente com relacionamentos de confiança.

Para Hughes *et al.* [62], sistemas dinâmicos de recursos baseados em confiança (DyTR - *The Dynamic Trust-based Resources*) geram uma noção dinâmica de confiança para recursos em redes Ad Hoc. A idéia da DyTR determina a quantidade de entidades confiáveis com o passar do tempo baseado em eventos e controla os recursos da rede de acordo com os níveis corrente da confiança. Para uma abordagem dinâmica da quantidade de confiança, a proposta envolve o uso de modelos sócio-cognitivos de confiança, que aborda conceitos essenciais das características de confiança em uma sociedade humana.

Diversos modelos da aplicação da confiança computacional utilizados em MANET podem ser estendidos, com o devido respeito dos delimitadores de objetivo, para outras áreas de sistemas distribuídos.

2.7 REDES SOCIAIS

Uma rede social é definida como uma estrutura social feita de entidades (indivíduos ou organizações) que estão ligadas normalmente por algum tipo específico de relações (valores, idéias, amizade, comércio, gostos, objetivos comuns, entre outros) [63]. A análise de uma rede social observa relacionamentos sociais entre as entidades e suas respectivas ligações, e as pesquisas em vários campos acadêmicos demonstram que redes sociais trabalham em diversos níveis ([63], [64]). E isto auxilia na determinação de como problemas são resolvidos, além de indicar como organizações funcionam e o nível de sucesso que entidades individuais conseguem alcançar em seus objetivos.

Sabater e Sierra [65] fizeram uma revisão apontando diversas linhas de interesse voltadas para os aspectos de confiança e também referenciaram a reputação como ponto focal dentro de uma “sociedade” em redes de computadores. Sabater e Sierra [65] citam que a ciência da computação está em outro paradigma que envolve computação por redes e computação distribuída, além de tratar de aspectos envolvendo agentes autônomos e sistemas multi-agente.

Este raciocínio é suportado também por outro trabalho de Sabater e Sierra [4], indicando a necessidade do tratamento de ambientes computacionais através do auxilio de redes sociais. Para Sabater e Sierra [4], o uso de iterações diretas prévias é provavelmente a melhor maneira de realizar o cálculo da reputação. Entretanto, em sistemas multi-agentes a quantidade de iterações em função da demanda pode ser escassa e para solucionar este problema, propõem um modelo auxiliado por redes sociais, aproveitando vantagem de relações sociais entre agentes.

Para Gaston e desJardins [6], a topologia é um fator chave em uma estrutura de uma rede social, indicando que a natureza de uma rede social possui um efeito significativo na performance do sistema com um todo. Assim, sugerem que encontrar uma boa estrutura para a rede, em domínios particulares de aplicação, tem um fator crítico na modelagem de sistemas multi-agentes.

Seguindo a mesma linha de análise, o trabalho de Bowman e Hexmoor [32] avalia preferências para colaboração entre grupos de agentes em uma rede social, defendendo a idéia que a colaboração de agentes afeta nos resultados da construção da sociedade de agentes.

Levando a idéia para a web, Wang e Emurian [66] fizeram um levantamento sobre comércio eletrônico e voltaram a aplicação de conceitos de confiança para aplicações *on-line* e afirmam que se a confiança for aplicada em mercados abertos na web, existe uma forte tendência de aumentar o número de consumidores.

O fundamento da afirmação está relacionado com as atitudes dos consumidores e fornecedores que seriam capazes de liberar informações mais sensíveis porque existe uma crença que o ambiente onde são tratadas as negociações é confiável e por implicação direta, também é seguro, formando uma rede de negociação. Dessa forma, se consumidores e fornecedores se sentem confortáveis em relação a um negócio, ambos têm as garantias de que necessitam associados às definições de confiança, em conseqüência estariam propícios a realizar mais negócios. Neste ponto, a afirmação vai contra a garantia de segurança *on-line* envolvendo apenas certificação digital e autoridades certificadoras, porque os modelos baseados em certificação digital geralmente são estáticos, enquanto que a confiança é dinâmica e evolutiva [7] [8] [10].

No contexto deste trabalho, redes sociais estariam voltadas para questões do estabelecimento e formação de grupos, bem como técnicas de análise decorrentes do comportamento dos agentes quando aplicado um modelo de confiança. Além disso, é possível avaliar o que o agente deveria ser capaz de fazer, após os critérios definidos na confiança em si, e a sua posterior avaliação, gerando resultados específicos da aplicação das técnicas de confiança e do modelo propriamente dito.

2.8 SÍNTESE DO CAPITULO

Em uma primeira perspectiva, observa-se que a confiança e a reputação envolvem um grande nível de complexidade, de variáveis e de situações específicas, quando observada sob o prisma em sistemas distribuídos. É nestes cenários complexos que, tanto a confiança

computacional quanto a reputação, estão sendo pesquisadas e referenciadas nas áreas de engenharia e de computação. Esta complexidade abrange diversas características, mapeamentos e definições na tentativa de se alcançar um modelo que seja abrangente e que possa ser considerado ideal. Entretanto, devido a suas características particulares e dentro das situações específicas em que os modelos são criados e conseqüentemente testados, a sua expansão para outros ambientes é um processo complexo devido à quantidade de variáveis associadas.

Desta forma, as questões que trabalham e necessitam da confiança computacional, suas dependências e relações, formam o escopo deste capítulo. Que por sua vez, abrange a aplicação do conceito em redes distribuídas. A confiança e a reputação não podem ser consideradas como uma solução única para problemas de segurança ([3], [9], [13]). Segundo as revisões, a confiança e a reputação se tornam complementos de outras soluções, que por sua vez agregam valor as discussões dos diversos problemas em sistemas distribuídos, e conseqüentemente da segurança da informação.

Como síntese, a revisão bibliográfica deste capítulo apontou diversos mapeamentos possíveis que envolvem a confiança e em conseqüência a reputação.

O capítulo seguinte trata de diversos modelos de confiança e reputação, apontando características necessárias para a elaboração de um modelo que atinja o pré-requisito de trabalhar a confiança em grupos.

3 REVISÃO DE MODELOS DE CONFIANÇA E REPUTAÇÃO

Conforme observado no capítulo anterior, a confiança é uma área de pesquisa, que além dos seus aspectos próprios, também está voltada para a solução de problemas que envolvem a segurança da informação em diversos ambientes computacionais. Quando seu conceito é aplicado em um sistema, seja real ou simulado, é necessária a transformação do conceito em um modelo implementável, normalmente matemático, que seja capaz de gerar um valor pela qual se mensura a confiança. O mesmo equivale para a reputação.

3.1 TIPOS DE CONFIANÇA

Um dos pontos principais deste tópico é fazer uma revisão analítica de alguns modelos de confiança, referenciados pelos diversos autores pesquisados durante a elaboração deste trabalho. Esta revisão tem como principal objetivo a identificação e agregação de características previamente pesquisadas, consideradas como argumentos positivos, para a geração de um modelo de confiança que seja capaz de fazer a representação da confiança em grupos. Além disso, também é importante identificar as características que não são desejáveis em um modelo de confiança. De forma que seja possível à criação de um modelo robusto, com características aceitas comumente em diversas arquiteturas, seguro a partir do ponto de vista dos requisitos de segurança e principalmente, passível de implementação em ambiente de software.

Os tópicos seguintes auxiliam na geração de requisitos iniciais que um modelo de confiança para grupos deve ter.

3.1.1 Confiança direta

No trabalho de Beth *et al.* [67], foi proposto um modelo para representação da confiança direta, através de um sistema que se comunica através de *links*. Segundo Beth *et al.* [67] a confiança direta pode ser definida segundo a expressão:

$$A_{confia} x^{seq} B_{valor} V_{(p)} \qquad \text{eq. 3-1}$$

Uma relação de confiança direta existe se A sabe que todas as experiências com B são positivas, voltadas para a classe de confiança X, e *seq* é a seqüência de agentes que mediaram

as experiências com exceção de A e B. *V* é o valor de uma relação de confiança, que é estimado pela probabilidade de que B se comporte bem quando sendo confiável. Este valor é baseado no número de experiências positivas de B que A conhece.

Então, segundo Beth *et al.* [67], assumindo que *p* seja o número de experiências positivas de B que A conhece, e voltadas para a classe de confiança x, então o valor destas experiências (V_z) pode ser calculado conforme a fórmula:

$$V_{z(P)} = 1 - a^{\,p} \qquad \text{eq. 3-2}$$

Este valor reflete a probabilidade de que B seja mais confiável que o valor de limiar α, fundado nas informações de que A possui sobre B. Esta relação de confiança está voltada para a expectativa de que B será confiável para A dentro de uma perspectiva da execução de uma única tarefa. A situação envolve uma correta definição do valor de limiar (α), que deve ser bem mensurado para que as estimativas sejam seguras o suficiente.

O modelo de confiança direta proposto por Patel [3], trabalha com a idéia de apresentação de valores específicos utilizando uma visão probabilística. Neste modelo a confiança está diretamente ligada com uma alta probabilidade de que uma entidade executará uma ação em particular que está relacionado com o cumprimento de determinadas ações durante uma interação. A probabilidade neste caso é extremamente subjetiva porque só pode ser assumida por um ponto de vista individual da entidade, fundamentado em suas experiências pessoais. Mais detalhes sobre este modelo no tópico seguinte.

3.1.1.1 TRAVOS

O modelo de confiança explorado na implementação no contexto deste trabalho é uma modificação e extensão do TRAVOS (*Trust and Reputation Model for Agent-based Virtual Organizations*) [3] porque engloba uma revisão e um mapeamento de diversos outros modelos de confiança e reputação. Patel [3] modela o ambiente no qual o TRAVOS é aplicado como um sistema multi-agente formado por n agentes, e denota o conjunto de todos os agentes como $\mathrm{A} = \{a_1, a_2, ..., a_n\}$.

Vários pares de agentes $\{a_x, a_y\} \subseteq \mathrm{A}$ podem interagir uns com os outros, governados por contratos que especificam as obrigações de cada agente em relação a seu parceiro de interação. Uma interação entre a_1 e a_2 é considerada bem sucedida por a_1 se a_2 cumpre suas obrigações. Pela perspectiva de a_1, a avaliação de uma interação entre a_1 e a_2 é resumida em

uma variável binária, O_{a_1,a_2}, onde $O_{a_1,a_2}=1$ indica uma interação bem sucedida para a_1 com a_2 e $O_{a_1,a_2}=0$, uma interação mal sucedida. Uma avaliação de uma interação observada no tempo t é denotada como $O^t_{a_1,a_2}$, e o conjunto de todas as avaliações observadas de um tempo t_0 a t, como $O^{t_0:t}_{a_1,a_2}$.

Em qualquer ponto no tempo t, o histórico de interações entre agentes a_1 e a_2 é guardado como valores ordenados, $\Re^t_{a_1,a_2}=\left(m^t_{a_1,a_2},n^t_{a_1,a_2}\right)$, onde o valor de $m^t_{a_1,a_2}$ é o número de interações bem sucedidas de a_1 com a_2 no tempo t, enquanto $n^t_{a_1,a_2}$ é o número de interações mal sucedidas de a_1 com a_2 no tempo t.

A tendência de um agente a_2 cumprir ou não com as obrigações para com o agente a_1 é governada por seu comportamento. O comportamento de a_2 em relação à a_1, denotado por B_{a_1,a_2}, é modelado como o valor esperado de O_{a_1,a_2}.

Cada agente mantém um nível de confiança em cada agente presente no sistema. O nível de confiança de um agente a_1 em um agente a_2, é denotado por t_{a_1,a_2}. Especificamente, o nível de confiança calculado utilizando somente as interações do próprio agente com outro é conhecido como confiança direta, denotado por $t^{\,d}_{a_1,a_2}$. Por outro lado, o nível de confiança calculado utilizando somente opiniões capturadas por outros é conhecido como reputação, denotado por $t^{\,r}_{a_1,a_2}$. A confiança calculada da combinação de experiência direta com opiniões de terceiros é conhecida como confiança combinada, denotada por $t^{\,c}_{a_1,a_2}$.

Outra métrica utilizada nesse modelo de confiança é a confidência, que consiste em uma métrica que representa a acuidade do valor de confiança calculado por um agente, dado o número de observações que são utilizadas para o cálculo dessa confiança. A confidência de a_1 na sua avaliação de a_2 é denotado por g_{a_1,a_2}.

No cálculo da confiança direta, é realizada uma abordagem probabilística baseada nas experiências individuais de um agente no papel daquele que confia. Se o agente a_1 tem informações completas sobre o agente a_2, a probabilidade de a_2 cumprir com suas obrigações é expressa por B_{a_1,a_2}, de acordo com a_1. Entretanto, geralmente, não se assume que haja informação completa. Assim, a confiança direta $t^{\,d}_{a_1,a_2}$ em um tempo t é definida como o valor esperado de B_{a_1,a_2}, dado um conjunto de avaliações $O^{1:t}_{a_1,a_2}$ de interações observadas.

$$t^{d}_{a_1,a_2} = \mathrm{E}\left[\mathrm{B}_{a_1,a_2} \mid O^{1:t}_{a_1,a_2}\right] \qquad \text{eq. 3-3}$$

O valor esperado de uma variável aleatória contínua depende da função densidade de probabilidade (PDF) utilizada para modelar a probabilidade que a variável terá um determinado valor. Nas análises Bayesianas [30], a família beta de PDFs é comumente utilizada como uma distribuição prévia para variáveis aleatórias que possuem valores contínuos no intervalo [0,1].

A fórmula geral para distribuições beta é dada pela eq. 3-4. Essa fórmula possui dois parâmetros, a e b, os quais definem o formato da função densidade quando plotada.

$$f(b \mid a, b) = \frac{b^{a-1}(1-b)^{b-1}}{\int U^{a-1}(1-U)^{b-1} dU} \qquad \text{eq. 3-4}$$

onde $a, b > 0$

Utilizando-se dessa função, é possível calcular o valor da confiança direta. Primeiro, é preciso encontrar o valor de a e b. Assumindo previamente, antes de interagir, que todos os valores possíveis de B_{a_1,a_2} são iguais, os valores iniciais de a e b são $a = b = 1$. Baseando-se em técnicas padronizadas, considerando as observações realizadas nas interações, esses parâmetros podem ser calculados adicionando o número de interações bem sucedidas ao valor inicial de a e o número de interações mal sucedidas a b.

$$\hat{a} = m^{1:t}_{a_1,a_2} + 1 \text{ e } \hat{b} = n^{1:t}_{a_1,a_2} + 1 \qquad \text{eq. 3-5}$$

onde t é o tempo de avaliação

Vale ressaltar que a utilização na notação com acento circunflexo ($\hat{a}$ e $\hat{b}$) é para indicar que os valores dos parâmetros da distribuição beta são estimados baseados na evidência do que é observado.

Assim, o valor final de $t^{d}_{a_1,a_2}$ é calculado aplicando a equação padrão para o valor esperado de uma distribuição beta.

$$t^{d}_{a_1,a_2} = \frac{\hat{a}}{\hat{a} + \hat{b}} \qquad \text{eq. 3-6}$$

Pela eq. 3-4 e pela eq. 3-6 pode-se deduzir que o valor da confiança direta e a distribuição mudam conforme um agente ganha experiência interagindo com o outro agente, o que promove a modificação do formato da curva de distribuição, visto que o valor dos parâmetros é alterado com o tempo.

Sabendo como calcular a confiança direta, é possível criar um agente de confiança direta (DTA – Direct Trust Agent), que avalia a confiabilidade somente pela confiança direta depositada no confiado. Assim, para esse caso, toda a confiança de a_1 em a_2 é igual à confiança direta, $t_{a_1,a_2} = t^{d}_{a_1,a_2}$.

O DTA tem a vantagem de saber que a informação utilizada para calcular a confiança é verdadeira, pois foi o próprio agente que participou das interações e as avaliou. A limitação desse agente é que, na ausência de interações com determinado agente, o DTA não possui a capacidade de calcular o valor de confiança. A continuação da explanação sobre o modelo TRAVOS está no item 3.2.4.

3.1.2 Confiança indireta

Não existe claramente um consenso sobre a definição de confiança indireta porque diversos autores ([3], [4], [9], [11], [20]) a citam, e às vezes, fazem um paralelo com outras dependências. De maneira geral, a confiança indireta pode ser tratada como o conhecimento das capacidades e confiabilidade de um nodo por meio de nodos terceiros.

Patel [3] descreve a reputação como uma forma de se alcançar a confiança indireta. Associado a esta situação define ainda que a reputação possa ser vista como um conceito multifacetado em que uma única entidade pode ter diferentes valores de reputação, cada uma para um contexto específico.

Em uma análise mais detalhada, isto leva a um problema de consenso da confiança porque os valores associados serão extremamente distintos em cada nodo, envolvendo situações de histórico e em conseqüência do tempo, além do serviço associado e do contexto em si da comunicação. Isto gera a análises de valores distintos sobre uma mesma situação por parte das entidades, sendo necessária a definição de um limite de valores observados. Até mesmo porque como cada nodo é independente em termos básicos de seu comportamento, cada nodo cria a sua própria estrutura de confiança de acordo com seus conhecimentos e de suas iterações individuais com outros nodos. E como para formar uma opinião conta com informações de outros nodos sobre um nodo terceiro, a definição de um valor de confiança,

quando comparado com de outro nodo gera valores distintos, tornando o processo de definição de consenso mais complexo.

3.1.3 Confiança Situacional

Para Marsh [9], a confiança tem diversos aspectos. E esse autor, visando o seu esclarecimento, apresentou um formalismo que fornece uma ferramenta para uma discussão mais precisa sobre como mensurar a confiança através de aspectos práticos envolvendo definição e implementação de um modelo que pode ser utilizado por agentes artificiais para a tomada de decisões baseada em confiança. De maneira resumida, Marsh [9] explica a confiança através de uma divisão de classes conforme a Tabela 3-1.

Tabela 3-1 – Tipos de confiança segundo Marsh [9].

TIPO DE CONFIANÇA	DESCRIÇÃO
Básica	É um valor que indica a disposição de um agente a confiar. Esse valor é calculado baseado no histórico de interações do agente e é representado por Tx, para um agente X. Pode ter seu valor variando entre [-1,1).
Geral	É o valor que indica o quanto um agente X confia em um agente Y, é dado por Tx(Y), com o valor entre [-1,1), sendo 0 um valor neutro.
Cega	Pode-se ter um valor -1 para total desconfiança, mas, aqui, não é aceito o valor 1 para total confiança, pois como diz o nome 'Confiança cega' quer dizer que se confia sem uma observação ou analise da situação. E para que a haja confiança é necessário que haja considerações e avaliações no contexto em que se vai confiar. Logo, confiança cega não é confiança' e logo não pode ser tratada no formalismo proposto por Marsh.
Não confiar e desconfiar	A diferença entre não confiar e desconfiar, ou seja, valor 0 e valor -1. Zero pode significar que x nem conhece y ou que x confiava em y, mas o valor de sua confiança foi reduzido devido a suas ações.
Situacional	Mais uma vez os valores variam entre [−1, +1). Considerando que a confiança é nas pessoas e não em suas ações. A visão de confiança situacional estende essa visão de confiança, dizendo que confiança é em pessoas em determinadas situações.

Considerando a confiança básica, a geral e a situacional, na visão de Marsh [9], a situacional é a mais importante em situações de cooperação. A condição básica é que uma vez que confiança situacional estiver acima de um determinado valor a cooperação acontecerá. Nesse sentido, para o cálculo da confiança computacional T devem ser levados em consideração vários aspectos, como por exemplo, a importância e a utilidade.

Seguindo estes pontos, e considerando os fatos de uso de agentes nas proposições de confiança no trabalho de Marsh [9], afirma-se que seus agentes são basicamente agentes de confiança. Então se leva em conta a confiança que A tem em B, por conhecimentos de

experiências anteriores, o que permite a definição da fórmula de confiança situacional, sem considerar variável temporal, apresentada por:

$$T_A(B,a) = U_A(a) \times I_A(a) \times \hat{T_A}(B) \qquad \text{eq. 3-7}$$

onde $T_A(B,a)$ é a confiança que A tem em B em uma situação a , $U_A(a)$ é a utilidade da situação a para A, $I_A(a)$ é a importância para A da situação e $\hat{T_A}(B)$ é a confiança média que A tem em B.

Em uma primeira análise, a fórmula mostra alguns erros que formalizar confiança pode trazer. Por exemplo, assumir valores negativos gera problemas na computação da mesma, o que pode levar a situações indesejáveis.

Em outra análise, percebe-se que quanto maior a importância, maior será o valor da confiança situacional, e de maneira análoga, para uma situação menos importante menor será a confiança situacional, podendo se chegar á 0 (zero) quando a importância for 0 (zero). Em conseqüência, o valor zero de importância pode levar o limiar de cooperação a zero. Isto em uma maneira prática leva a definição de que o agente no modelo irá cooperar se a importância for zero.

Pensando em uma forma de estender o problema voltado para a confiança situacional, comparando-se com as pessoas De maneira geral, pessoas confiáveis são mais propensas a confiar em outras pessoas. O contrário também é verdadeiro, onde pessoas não confiáveis tendem a não confiar em outras pessoas (acreditam que os outros agirão da mesma forma que elas). Então se houver uma maneira de saber o quanto os outros confiam em nós podemos estimar se eles são confiáveis ou não, e de maneira simplificada saberíamos pelo menos que não somos tão confiáveis quanto pensávamos ser.

Apesar de ser relativamente simples, temos o problema de tentar saber o quanto os outros confiam em nós. Em uma conclusão prévia, a resposta é que não há como saber. Até mesmo porque se uma pergunta ocorre nesse sentido, não existe a garantia de que a resposta será verdadeira, o que é mais sensível ainda em ambientes em que a confiabilidade é mensurada como baixa.

Então, para Marsh [9] isto leva a crer que no caso de agentes, se eles fossem tão transparentes que se pudesse saber se confiam em nós, eles seriam tão transparentes que não seria necessário o estabelecimento de confiança. Ainda assim, Marsh [9] apresenta uma

extensão da confiança situacional dada por uma estimativa de quão confiável A é aos olhos de B, denotada por:

$$T_A(B,a) = (U_A(a) + T_A(\hat{B})) \times (I_A(a) \times T_B(\hat{A}))^A \qquad \text{eq. 3-8}$$

onde $T_B(\hat{A}))^A$ representa o quão confiável A é no ponto de vista de B. Isto implica que a estimativa de A sobre a opinião de B é importante e logo a estimativa de A sobre a estimativa de B a respeito de A também tem a sua importância, de tal forma que se leva a uma recursividade que não possui muito sentido em uma aplicação real.

3.1.4 Políticas de confiança

Este tipo de modelo, também conhecido como *policy based trust*, pode ser caracterizado pela situação em que a fonte de um recurso requer uma autenticação do nodo que está solicitando o recurso. Em uma explicação mais detalhada, nesse tipo de esquema um nodo *A* solicita uma determinada informação ou serviço a outro nodo B, chamado de fonte. O nodo B exige uma credencial de A para determinar sua identidade, basicamente para saber se ele é quem diz ser e se tem privilégios para acessar a informação ou serviço que ele solicitou.

Desta forma, se as credenciais fornecidas por A estiverem de acordo com o que B tem armazenado, A terá acesso ao serviço solicitado, caso contrário, o acesso solicitado será negado. Dependendo do sistema utilizado, pode ser guardada a informação de que A fez uma tentativa de acesso que foi recusada. Se A tiver várias tentativas de acesso negadas em um curto espaço de tempo, outras medidas podem ser tomadas. Estas medidas também variam muito do sistema em si, mas pode variar desde um período de quarentena até o banimento do nodo em relação ao serviço.

3.1.5 Confiança cognitiva

Castelfranchi e Falcone [68] concordam com a definição de confiança dada por Gambetta [7] onde aponta a confiança basicamente como uma estimativa, ou simplesmente uma crença. Entretanto, geram uma discussão da confiança não só como um dimensionamento de predição, mas levando em consideração o aspecto de dimensão da competência.

Em outras palavras, segundo Castelfranchi e Falcone [68], seria como ignorar o significado de que A faz quando decide por confiar em B (eu confio em B), onde existe a decisão em si e uma ação por parte de A para que confie em B.

O tratamento dado ainda questiona aspectos da confiança proposto por Gambetta [7] porque não diz concretamente de que é feita a avaliação e nem o seu embasamento concreto, de tal maneira que a probabilidade subjetiva não envolve muitas crenças e parâmetros que são importantes na consideração social da confiança.

Assim propõe um modelo em que um agente A confia em um agente B sobre uma determinada ação, gerando um estado G. A confiança desta forma é vista como um estado mental ou uma atitude que resulta na ação de delegação de parte dos planos de A para B. Para tanto existe a divisão do trabalho em dois componentes diferentes. O primeiro aponta uma característica da entidade confiada (confiança interna) e a segunda aponta uma avaliação sobre a probabilidade e consistência de fatores externos, obstáculos e oportunidades, entre outros fatores externos (confiança externa).

Castelfranchi e Falcone [68] tratam que a confiança, segundo uma visão cognitiva, requer três aspectos – crença, desejo e intenção. Apesar de o modelo tratar aspectos importantes que envolvem a confiança em si serem válidos, a aplicação e implementação direta de tais circunstancias são complexas. A afirmação leva em consideração o fato de que é difícil fazer uma tradução de aspectos da teoria cognitiva para uma aplicação direta, em situações reais utilizando ambientes computacionais.

Para Johnson e Grayson [69] a confiança cognitiva envolve a confidência. Ela nasce de um conhecimento acumulado que permite fazer predições com algum nível de confidência de que uma entidade em específico cumprirá suas obrigações. Neste caso, o conhecimento é adquirido mediante observação do comportamento da entidade em questão e das informações de reputação dada por outros relacionamentos, que se forem consideradas importantes, uma interação inicial será meramente uma oportunidade de confirmar ou não as percepções já conhecidas através da confiança. Neste caso, a confiança cognitiva se transforma em definitiva em apenas uma ou poucas iterações. Apesar de a confiança cognitiva ser direcionada por um conhecimento, o fato de se necessitar confiar presume um conhecimento incompleto, porque se um estado de certeza completa em um parceiro é atingido, o risco é eliminado e a confiança é um ponto redundante.

Segundo Dunn [70], a confiança cognitiva é importante no estabelecimento de relações em negócios. Para tanto conduziu um experimento de como uma entidade confiante calcula a confiança em uma entidade confiável. Seu estudo considerou que a confiança

cognitiva é medida como resultado da confiabilidade perceptível por parte da entidade confiante na entidade confiada, de que esta executará uma determinada tarefa em função de um tempo aceitável. E os resultados revelaram que a consistência do comportamento passado na entidade confiada é o elemento mais importante na produção da confiança cognitiva em um relacionamento social.

3.1.6 Modelo de confiança em ambientes de grid

No trabalho proposto por Tran *et al*. [31], a confiança em Grid pode ser entendida como uma competência na entrega ou realização de serviços. A confiabilidade de um nodo é função do seu comportamento e diferentes nodos possuem diferentes graus de confiança em um determinado nodo. E esta situação é variável de acordo com o tempo.

Em um detalhamento do seu estudo, leva-se a situação de que existem dois tipos de confiança em ambientes de Grid. A primeira está relacionada com a confiança de provedor, que mede se o nodo irá alocar recursos de modo a entregar o serviço conforme prometido. Já a segunda refere-se a confiança de consumido, que mede se o nodo utilizará o serviço requisitado de forma acordada e adequada. Então, de uma forma ou de outra, classifica-se a confiança em direta ou indireta, sendo que a direta diz respeito ao conhecimento do nodo baseado em experiências diretas. Já a indireta, ao conhecimento das capacidades e confiabilidade de um nodo por meio de nodos terceiros (reputação). E afirma que uma combinação ponderada dessas duas define a confiança total. A partir destas afirmações, trabalha com a concepção de um modelo de confiança que trata o comportamento do nodo classificado em 4 categorias, conforme descrito na Tabela 3-2.

Tabela 3-2 – Classificação de confiança por comportamento segundo Tran *et al*. [31]

Comportamento	Confiança como Provedor	Confiança como Consumidor	Nota
Good (G)	Excelente qualidade de serviço	Código de qualidade, rápida execução	2
Normal (N)	Qualidade de serviço esperada	Execução normal do código	1
Bad (B)	Serviço com atraso ou resultado incorreto	Código lento, alta utilização, instruções repetitivas	-1
Malicious (M)	Interfere no código, não executa	Código prejudicial, instruções não autorizadas	$-\infty$

Logo a formalização da confiança em uma rede aberta pode ser dada como uma estimativa de confiança de um através de

$$T_{ij} = 1 - a^{n} \qquad \text{eq. 3-9}$$

onde T_{ij} é a confiança que o nodo i tem em j, n é o valor acumulado das notas que i deu para j e a é a taxa de aprendizado (atribuído por um valor entre 0 e 1). Com o crescimento do valor de confiança, T_{ij} se aproxima de 1, e n começa com 0 (reflete nenhuma interação entre os nodos). Seguindo esta descrição, Tran ***et al.*** [31] traça que a confiança direta como provedor é definida por

$$T_{ij}^{P} = 1 - a^{S_P} \qquad \text{eq. 3-10}$$

e a confiança direta como consumidor é dada através de

$$T_{ij}^{C} = 1 - a^{S_C} \qquad \text{eq. 3-11}$$

já a confiança indireta computada por

$$R_{ij} = \frac{\left(\sum_{t=1}^{k} T_{it} * T_{tj} \right)}{K} \qquad \text{eq. 3-12}$$

onde se assume que S_P = valor acumulado como provedor e que S_C = valor acumulado como consumidor. A fórmula da confiança indireta envolve somente um nível visto que há a interposição de um nodo.

A discussão da confiança se estende ainda voltada para o conceito de troca justa (***Fair Trading***). De forma simplificada se assume apenas dois tipos de serviço no Grid: serviço computacional e o de armazenamento. De tal forma que a contribuição computacional é dada por $G_{com} = h_{com} * N_i$, e a contribuição de armazenamento é expressa por $G_{stg} = h_{stg} * V_S$, onde h = notas dos serviços consumidos, N_i = número de instruções e V_S = volume do storage. G_{stg} e G_{com} podem ser convertidas uma na outra por $G = G_{com} + \partial * G_{stg}$, onde ∂ = fator de conversão.

Ainda no modelo, é definido um mecanismo de contribuição direta e de contribuição indireta, de tal forma que Q_{ij} é a contribuição direta de j em i, e Q_{ij} é dado por $Q_{ij} = G_{ij} - G_{ji}$. A contribuição direta mostra se o avaliador deve ao avaliado baseado nas interações passadas.

A contribuição indireta indica a quantidade relativa de contribuição do avaliado. E considera que as recomendações dos diversos nodos têm peso diferente, dependendo da confiança depositada no nodo que está passando a informação. A confiança indireta pode ser expressa por

$$P_{ij} = \left(\sum_{t=1}^{k} T_{it} * Q_{tj} \right) \qquad \text{eq. 3-13}$$

onde P_{ij} representa a contribuição indireta do nodo j sob a perspectiva do nodo i, e k é o número de recomendações. Utilizando a confiança direta como ponderador, neutraliza-se o efeito de informação falsa de um grupo de nós desonestos.

Segundo Tran *et al.* [31], o modelo elaborado resolve alguns problemas de controle de acesso no Grid, e a sua justificativa é dada porque preserva a descentralização do Grid e a autonomia dos nodos ao mesmo tempo em que habilita e encoraja interação entre nodos honestos. Depois, o modelo de confiança ajuda a distinguir nodos bons, ruins, maliciosos pela confiabilidade e contribuição. E estendendo a discussão, privilégios apropriados de acesso podem ser designados de acordo com essa classificação. Além disso, as notas de contribuição do trabalho incentivam o compartilhamento de recursos e serviços, enquanto guarda a confiabilidade destes serviços, e que sem grandes modificações, esse modelo também pode ser aplicado a outras aplicações descentralizadas, como P2P.

3.2 MODELOS DE REPUTAÇÃO

A reputação no cenário computacional, segundo as revisões de trabalhos correlatos sobre confiança, indica que a mesma pode ter um forte componente na influencia do cálculo da confiança ([3], [7], [9], [10], [65]). Isto permite que a confiança esteja interligada com a reputação na geração de valores de confiança e que tais valores sejam objeto não só da percepção da imagem de uma entidade, mas também de avaliação própria por parte de quem tem interesse em algum tipo de interação em um ambiente distribuído

Dando seqüência nas definições e na representação em um cenário computacional, os tópicos seguintes revisam alguns modelos de reputação.

3.2.1 REGRET

REGRET é um modelo de reputação criado por Sabater e Sierra ([4], [65]) utilizado em sociedade de agentes que possuem uma tendência de formar grupos com outros agentes do mesmo tipo e de certa forma “apreciar” sua companhia, que segundo os autores podem ser comparadas com sociedades gregarious ([4], [65]). A reputação nestas sociedades é vista como “uma opinião ou visão de um sobre alguma coisa”, e normalmente é um conceito construído levando-se em conta o tempo considerado em uma interação direta com outras entidades. Ou o tempo gasto para obter essa informação através de opiniões de outros membros da sociedade, e de certa forma, avaliar a informação.

Comparando-se este tipo de sociedade em um cenário computacional, equivale a observação de que um determinado agente pode ter um excelente comportamento para prestar um determinado serviço e um comportamento indesejado na prestação de outro serviço. Isto permite situar os diferentes tipos de reputação e a maneira que são ou podem ser combinadas como uma definição de uma dimensão ontológica da reputação. Esta dimensão é formada em adição por outros dois tipos, a dimensão social (formada pela experiência adquirida interagindo com o grupo) e a dimensão individual (formada por iterações diretas com uma entidade na sociedade) [65].

A representação de um diálogo ou interação entre agentes no modelo REGRET é definido por um contrato inicial, que direciona os termos e condições de uma transação entre duas entidades e o resultado atual da transação. Inicialmente, ele contém variáveis comuns, que representam os atributos da transação que são conhecidos e aceitos por ambas as partes na comunicação. O contrato estipulado também contém variáveis que tratam da expectativa de que partes da transação são assumidas de serem finalizadas por uma das entidades e que estão relacionadas diretamente com a subjetividade do comportamento de uma entidade.

O resultado desta expectativa aponta que uma única transação formará um contrato diferente para cada uma das entidades envolvidas. Isto gera uma impressão por parte da entidade através da avaliação subjetiva sobre um determinado aspecto do contrato, que segundo o modelo, é definido por uma tupla (*a, b, o,* ∂ *, t, W*) que contém identificadores das entidades envolvidas na transação (*a,b*), o contrato *o* relacionado com a transação, a variável ∂ da parte do contrato que é julgada, o tempo *t* que a impressão foi gravada e *W* com um valor de limiar entre [-1,1] associado com o atributo do contrato sendo avaliado, através do ponto de vista do agente. *W* representa a avaliação subjetiva por parte do agente voltado para uma variável específica do contrato (armazenado em um banco de dados), que é utilizado para estimar e avaliar a reputação de outras entidades.

Para a elaboração da reputação subjetiva de um agente a partir de um atributo específico do contrato, pode ser recolhido um subconjunto de informações, a partir de um determinado padrão vindo de um conjunto de impressões armazenado na base de impressões. Um valor atual é calculado por uma média de fatores de impressão por um determinado peso, vindo do subconjunto encontrado a partir de uma pesquisa realizada pelo agente. E quanto mais recentes forem as impressões, maior será a relevância no valor final da reputação. A confidência do valor de reputação calculado pode ser gerada considerando a combinação do número de impressões usadas para o cálculo e a variância dos valores médios das impressões utilizadas.

Apesar dos vários pontos positivos do REGRET, segundo análise realizada por Patel [3], o modelo não endereça um aspecto que pode ser importante na questão de uma "mentira estratégica", principalmente quando se tratar de sociedades altruísticas. Este tipo de comportamento tem por objetivo ganhar algum tipo de vantagem em uma competição na sociedade formada, por exemplo, melhorar sua imagem, ganhar mais destaque, entre outros. Além disso, o modelo pode ser suscetível a ruídos em razão da maneira de como os valores das impressões são pesadas e somadas.

Existem ainda outros modelos de reputação que seguem a mesma linha do REGRET, como o FIRE [71], o CREDIT [72], e o *Distributed Reputation Management* [73]. Entretanto, apresentam-se como uma variação do REGRET, complementando alguns pontos do modelo, ou apontam os mesmos requisitos para o cálculo da confiança.

É importante observar que não existe um consenso aberto sobre qual modelo é mais eficiente ([3], [65]). O que existe são definições de aplicações dos modelos dentro de uma linha de problema, ou seja, os modelos funcionam muito bem para a linha de problema para qual foi criada. Contudo, o contexto do problema e a sua delimitação influenciam diretamente na escolha de um modelo de reputação para um determinado ambiente.

3.2.2 Reputação baseada em feedback

Também conhecido como *Reputation Based Feedback* (RBF), é um esquema muito utilizado em sites de e-commerce, onde como principais exemplos, citam-se o e-Bay [74] e o Mercado Livre [75]. Seu esquema de funcionamento é o de avaliações das transações anteriores, que estão disponíveis para quem pretende fazer uma transação nova com um determinado usuário cadastrado no sistema. Essas avaliações normalmente são classificadas em positivas, se a interação ou a negociação foi concluída com sucesso e ambas as partes se consideram satisfeitas. Em neutras, se alguma das partes não possui uma opinião formada sobre a outra parte, ou negativas se na avaliação de alguma de uma das partes indica que a outra parte não cumpriu com o acordo pré-estabelecido.

Na RBF, o esquema de funcionamento é tratado em um ambiente em que um usuário A possui um perfil através do qual outros usuários podem avaliar se A é confiável ou não, utilizando da classificação acima. Em uma análise simples, somente este tipo de avaliação permite a geração de informações falsas. Por exemplo, o próprio usuário A pode criar diferentes usuários na rede, ou ainda trabalhar juntamente com outros usuários mal intencionados, e gerar avaliações positivas em seu favor, aumentando sua boa reputação na

rede, ou ainda gerar avaliações negativas para outros usuários, prejudicando a reputação dos mesmos. A Tabela 3-3 apresenta um resumo das classificações utilizadas na RBF.

Tabela 3-3 – Resumo das classificações em RBF

Avaliação	Descrição
Positiva	Negociação concluída com sucesso e há satisfação nos dois lados da transação
Neutra	Não existe uma opinião formada sobre a transação ou seu valor não representa ganho ou perda de reputação
Negativa	Não houve cumprimento do acordo por uma das partes

Este tipo de modelo funciona em uma arquitetura híbrida, onde há uma base de dados central para guardar as avaliações. Em uma rede totalmente descentralizada, existem sistemas que implementam o RBF através de protocolos como o DMRep [41] , EigenRep [76], Dynamic Trust Metric [77] e outros. Vejamos alguns deles a seguir.

3.2.2.1 DMRep

No DMRep [41] as avaliações são armazenadas de forma distribuída e redundante utilizando um esquema como o P-GRID [44]. No tratamento da reputação no DMRep, se *p* e *q* efetuam uma transação e *p* avalia *q* como malicioso, essa informação será enviada a outros nodos aleatoriamente segundo o formalismo

$$insert(a_1; key(p); c(p,q)) \qquad \text{eq. 3-14}$$

onde a_1 é um nodo aleatório, *key* é o identificador do nodo *p* e *c* (*p,q*) é a avaliação negativa na transação de *q* com *p*. Tendo *p* dado uma avaliação negativa de *q*, é provável que *q* dê também uma avaliação negativa sobre *p*, assim um terceiro nodo qualquer *r* não terá certeza sobre a confiabilidade de *q*.

Para se ter uma idéia melhor sobre a reputação de *q* o nodo *r* envia mensagens para outros nodos aleatoriamente perguntando sobre avaliações anteriores em transações envolvendo *q* segundo

$$query(a_i; key(q)) \qquad \text{eq. 3-15}$$

com objetivo de obtenção de uma avaliação mais precisa. Ao receber as respostas, o nodo *r* calcula uma média ponderada de acordo com o nível de participação dos nodos respondentes e avalia se deve ou não confiar em *q*.

No caso do DMRep as avaliações de nodos com grande participação positiva em transações na rede têm peso maior que as de nodos com baixa participação ou nodos novos, e a aleatoriedade na distribuição das avaliações e a redundância destas é o ponto chave do esquema. O ponto forte do modelo é a total descentralização, além de ser relativamente eficiente em redes com grande número de nodos, contudo não se pode afirmar que seja robusto porque a geração da opinião pode ser forjada realizando coalizão de nodos.

3.2.2.2 EigenRep

O objetivo deste modelo [76] é identificar nodos maliciosos por meio da atribuição de valores de confiança de acordo com o comportamento de cada nodo em transações anteriores. Para realizar tal procedimento, cada nodo *i* guarda um valor C_{ij} para cada outro nodo *j* com quem ele já manteve algum tipo de relação, onde C_{ij} representa um valor local de confiança. O valor de confiabilidade do nodo *i* dado por "toda a rede" é representado por T_i.

Como cada nodo, em uma situação normal, possui poucas experiências com outro determinado nodo, é importante obter a opinião a partir de outros nodos sobre aquele com quem se pretende realizar uma transação. Este valor pode ser expresso por T_{ik} obtido através de

$$T_{ik} = \sum_j C_{ij} C_{jk} \qquad \text{eq. 3-16}$$

onde *j* equivale a outros nodos conhecidos, C_{jk} é a opinião do nodo *j* sobre o nodo *k* e C_{ij} é a opinião do nodo *i* sobre do nodo *j*, que é um fator que pondera a opinião de cada outro nodo de acordo com a concepção de *i* a seu respeito. O nodo *i* calcula T_{ik} para todos os nodos da rede formando um vetor local de valores t_i expresso por

$$\begin{pmatrix} T_{i1} \\ \dots \\ T_{ik} \\ \dots \\ T_{iN} \end{pmatrix} = \begin{pmatrix} C_{11} & \dots & C_{k1} & \dots & C_{N1} \\ \dots & \dots & \dots & \dots & \dots \\ C_{ik} & \dots & C_{kk} & \dots & C_{Nk} \\ \dots & \dots & \dots & \dots & \dots \\ C_{1N} & \dots & C_{kN} & \dots & C_{NN} \end{pmatrix} \begin{pmatrix} C_{i1} \\ \dots \\ C_{ik} \\ \dots \\ C_{iN} \end{pmatrix} \qquad \text{eq. 3-17}$$

Ou, simplificando, por

$$T_i^w = C^T c_i^v \qquad \text{eq. 3-18}$$

onde, repetindo o procedimento se chega a

$$T_i^v = \left(C^T\right)^n c_i^v \qquad \text{eq. 3-19}$$

Com o valor n grande, se converge para um mesmo vetor para todos os nodos (autovetor) da matriz C. Esse vetor é chamado de Vetor de Reputação Global (*Global Reputation Vector*), que indica a confiabilidade que a rede inteira tem em um determinado nodo.

Para que o EigenRep [76] seja eficaz contra grupos de nodos maliciosos é necessário que existam nodos pré-confiados (como os nodos criadores da rede). Quando nodos inativos ou novos na rede aparecem no cálculo do C_{ij} é assumido o valor de um nodo pré-confiado, aumentando a dependência do esquema nesses nodos.

3.2.3 Métrica de confiança dinâmica

Na proposta de métrica de confiança dinâmica, também conhecida como *Dynamic Trust Metric* (DTM), Duma *et al.* [77], propõem um modelo capaz de detectar mudanças no comportamento dos nodos com certa rapidez, o que segundo os autores, não era conseguido por outros modelos de confiança baseada em reputação.

Segundo Duma *et al.* [77], em alguns modelos de reputação leva-se um tempo relativamente grande até se detectar um comportamento malicioso. Isto porque todo o histórico das iterações de determinando nodo é levado em consideração no cálculo do seu valor de confiança e não há diferenças nos pesos das iterações mais recentes ou mais antigas. Dessa forma, se um nodo que sempre teve uma boa avaliação de suas iterações (o que equivale a uma boa reputação), começar a agir de forma maliciosa, ou ainda oscila constantemente seu comportamento (parte do tempo é malicioso e parte do tempo não), a rede como um todo demorará a detectar essa mudança de comportamento, o que pode resultar em situações indesejáveis.

Outro problema que é relativamente sensível nos modelos de *Reputation Based Feedback* (RBF) é que avaliações positivas e negativas têm o mesmo peso, de tal forma que uma avaliação boa anula uma má. Em geral isso não é uma boa alternativa porque se leva

muito tempo para se adquirir um bom nível de confiança, mas rapidamente essa confiança pode ser destruída.

Para solucionar esses problemas, o DTM apresenta uma métrica que leva em consideração três fatores. O primeiro fator é de curto prazo (*Short Term Trust Factor*) ou simplesmente *st*, o segundo fator é de longo prazo (*Long Term Trust Factor*) ou *lt* e o terceiro é o fator de penalidade (*Penalty Factor*) ou *pf*.

Esses três fatores são utilizados para o cálculo de um vetor de confiança (*trust vector*), sendo que cada fator é ponderado por um peso diferente no cálculo da reputação. O próprio vetor de confiança, por sua vez, é ponderado pelas avaliações locais de um nodo e por avaliações de outros nodos. O *st* é calculado mediante

$$st_{n+1}(a,b) = st(a,b) + art(a,x)(e_{n+1}(x,b) - st_n(a,b))$$
$$\text{se } e_{n+1}(x,b) - st_n(a,b) \geq -e \text{ ou} \qquad \text{eq. 3-20}$$
$$st_{n+1}(a,b) = st(a,b) + brt(a,x)(e_{n+1}(x,b) - st_n(a,b))$$

Baseado nesses pontos, foram estabelecido fatores que correspondem a sensibilidade positiva (a) e a sensibilidade negativa (b) e variam entre [0,1]. Se $a = b = 0$, o sistema não é sensível a mudanças rápidas, porém se $a = b = 1$, o sistema será bastante sensível às iterações recentes.

Isto gera um problema porque se o sistema estiver muito sensível ($a = b = 1$) e o nodo tiver uma avaliação negativa (por erro ou por ter sofrido um ataque), sua reputação pode ser bastante prejudicada, mesmo que ele tenha um histórico de reputação muito bom, garantindo a possibilidade de calculo do fator de curto prazo (*st*). E da mesma forma um nodo malicioso pode conseguir aumentar sua confiabilidade agindo de forma correta e recebendo uma avaliação positiva, desde que consiga um alto grau de iterações.

O fator de longo prazo (*lt*) indica como é o comportamento histórico do nodo, o que fornece certa estabilidade para o cálculo da confiança. Então, se um nodo malicioso, que começou a agir corretamente, não terá seu grau de confiança elevado abruptamente, devido a seu histórico. E um nodo que tem um histórico de boa reputação, poderá recuperar sua reputação após sofrer uma mudança de comportamento repentina (por ataque ou erro). O fator *lt* é calculado por

$$lt_{n+1}(a,b) = \frac{w_s(n+1)}{(n+1)}\left[\frac{n}{w_s(n)} lt_n(a,b) + rt(a,x_i)e_{n+1}(x_i,b)\right] \qquad \text{eq. 3-21}$$

O fator de Penalidade (*fp*) é utilizado para punir nodos que apresentam comportamento malicioso oscilatório. Os nodos que forem punidos terão mais dificuldades para aumentar sua reputação, por força que devem ter mais avaliações positivas do que necessitavam anteriormente. Para o cálculo do fator *fp* é definido um acumulador macc, que recebe o valor resultante da diferença entre a confiança investida e a experiência atual.

$$macc_{n+1} = macc_n(a,b) + r(a,x)(t_n(a,b) - e_{n+1}(x,b))$$
$$\text{se } t_n(a,b) - e_{n+1}(x,b) > e \text{ ou} \qquad \text{eq. 3-22}$$
$$macc_{n+1} = macc_n(a,b)$$

sendo que o fator de penalidade é dado por

$$fp_n(a,b) = \frac{macc_n(a,b)}{c + macc_n(a,b)} \qquad \text{eq. 3-23}$$

E finalmente se pode realizar a combinação de fatores, gerando uma métrica de confiança combinada. Inicialmente se relaciona *st* e *lt* considerando o pior dos dois casos, dado por

$$t_n(a,b) = \min(st_n(a,b), lt_n(a,b)) \qquad \text{eq. 3-24}$$

Combinando este dado com o *fp*

$$lt_n(a,b) = lt_n(a,b)(1 - fp_n(a,b)) \text{ para } lt \text{ e}$$
$$a = a(1 - fp_n(a,b)) \text{ para } st \qquad \text{eq. 3-25}$$

De acordo com os resultados obtidos no trabalho de Duma *et al.* [77], o *Dynamic Trust Metric* se mostrou eficiente na detecção rápida de mudança de comportamento e na forma de punição de nodos maliciosos, considerados como problemas que os outros métodos apresentam.

3.2.4 Reputação no modelo TRAVOS

Para o correto entendimento desta parte é importante revisar o modelo de confiança direta (item 3.1.1.1). Segundo o modelo de Patel [3], a maneira mais confiável de prever o comportamento de um agente é segundo a avaliação do histórico de interação direta com esse

agente. Entretanto, existem casos em que a interação ainda não ocorreu e ainda assim será preciso estimar o nível de confiança no agente com o qual se deseja interagir. Neste caso, a reputação se apresenta como uma métrica para avaliação do agente. Essa métrica envolve consultar outros nodos que estiveram em contato com esse agente no passado para colher informações de confiança. O histórico de interações de a_3 com a_2 no tempo t pode ser representado por

$$\Re^t_{a_3,a_2} = \left(m^t_{a_3,a_2}, n^t_{a_3,a_2}\right) \qquad \text{eq. 3-26}$$

De maneira análoga, a opinião de a_3 com relação à a_2 é dada por

$$\hat{\Re}^t_{a_3,a_2} = \left(\hat{m}^t_{a_3,a_2}, \hat{n}^t_{a_3,a_2}\right) \qquad \text{eq. 3-27}$$

Em geral se nota que $\Re^t_{a_3,a_2} \neq \hat{\Re}^t_{a_3,a_2}$ no modelo, pois a opinião provida não é imparcial (possui a tendência positiva ou negativa de alterar o que seria de fato resultado da interação), e caso o opinante seja honesto, $\Re^t_{a_3,a_2} = \hat{\Re}^t_{a_3,a_2}$.

O agente a_1 deve calcular o valor de reputação $t^{\,r}_{a_1,a_2}$ em relação à a_2 pelas opiniões coletadas de outros agentes. As interações bem sucedidas e as mal sucedidas precisam ser enumeradas e somadas resultando nos valores de N_{a_1,a_2} e M_{a_1,a_2}, os quais serão utilizados para calcular os parâmetros da distribuição beta utilizado no modelo. Esses parâmetros servirão para o cálculo da reputação (eq. 3-30).

$$N_{a_1,a_2} = \sum_{k=0}^{p} \hat{n}_{a_k,a_2}\ ,\ M_{a_1,a_2} = \sum_{k=0}^{p} \hat{m}_{a_k,a_2}\ , \qquad \text{eq. 3-28}$$

onde p = número de reportes

$$\hat{a} = M_{a_1,a_2} + 1 \text{ e } \hat{b} = N_{a_1,a_2} + 1 \qquad \text{eq. 3-29}$$

$$t^{\,r}_{a_1,a_2} = \frac{\hat{a}}{\hat{a} + \hat{b}} \qquad \text{eq. 3-30}$$

A Figura 3-1 mostra a distribuição beta para opiniões providas por três agentes diferentes e a distribuição resultante da combinação dessas opiniões. Pela análise desse gráfico, é possível perceber que, considerando as opiniões separadas, a distribuição resultante

da combinação possui menos variância, o que significa que o agente tem mais confidência no valor de confiança obtido pela distribuição da combinação.

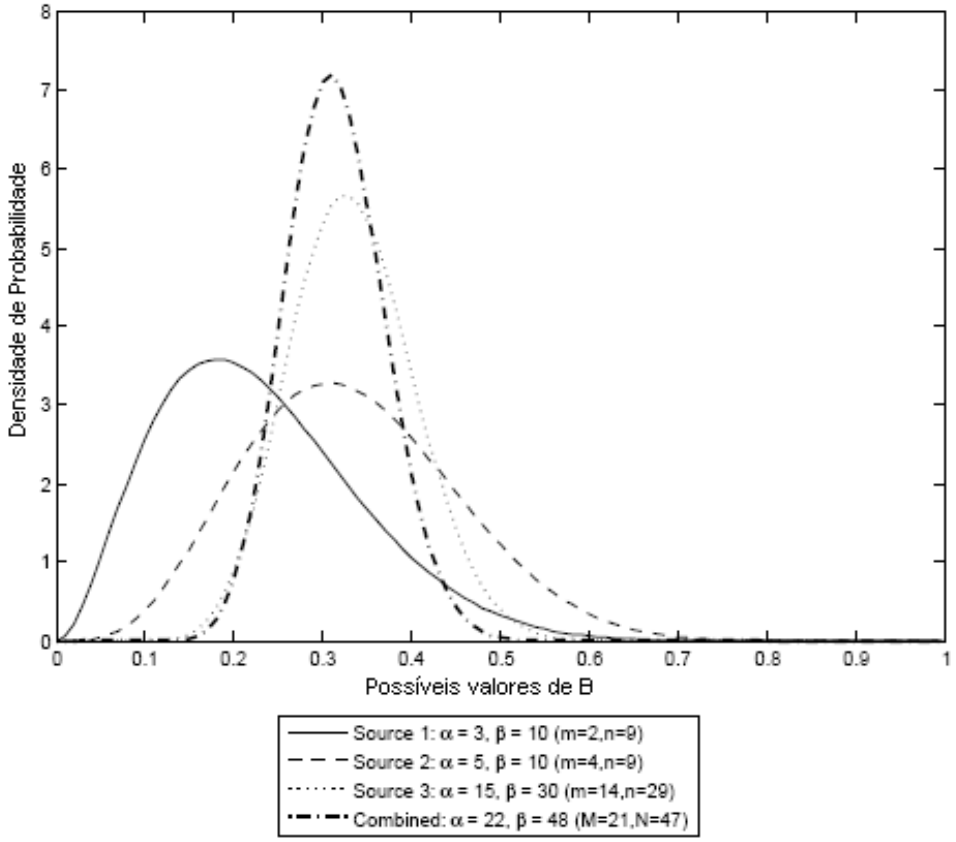


Figura 3-1 – Três opiniões separadas e a reputação calculada com a combinação delas [3]

Sabendo como calcular a reputação, é possível criar o agente de reputação (RTA – Reputation Trust Agent), que avalia a confiabilidade pelas informações coletadas de terceiros. Assim, para esse caso, toda a confiança de a_1 em a_2 é igual à reputação, $t_{a_1,a_2} = t^{r}_{a_1,a_2}$. Esse modelo do cálculo de reputação resolve o problema de não ter informações sobre o agente com o qual se deseja interagir, o que inviabilizaria o cálculo de confiança.

Se for considerado que o comportamento de um agente é sempre o mesmo, independente do agente com o qual está interagindo e que aquele que provê a reputação está sempre dizendo a verdade, o valor de confiança resultante será o mesmo, se for calculado tanto com base nas informações de terceiros ou na própria experiência direta com o agente. Entretanto, na prática, não é o que acontece. Então, o modelo precisa prever a existência de opiniões inconsistentes ou imprecisas.

Opiniões imprecisas não são somente resultado de ação maliciosa, mas podem ser causadas pela existência de informações incompletas no agente que provê essa opinião.

Assim, é importante que o agente que está coletando as informações de confiança possa avaliar a probabilidade de precisão daquela opinião dada. Dessa forma, a solução é ajustar ou ignorar as opiniões não confiáveis antes da combinação delas no valor total de reputação.

A probabilidade de precisão é uma métrica que representa o quanto o agente acredita que a opinião de determinado nodo é precisa, dados os resultados das interações passadas nas quais o mesmo nodo forneceu opiniões semelhantes. Assim, o primeiro passo para barrar opiniões imprecisas é guardar o histórico de opiniões providas e o resultado da interação na qual a opinião foi requerida.

As opiniões gravadas são representadas como $\hat{\Re}^t$. Todos os valores possíveis de $\hat{\Re}^t$ são divididos em faixas predefinidas, de acordo com o valor esperado $\mathrm{E}_{\hat{\Re}^t}$ resultante da distribuição beta obtida de $\hat{\Re}^t$ (eq. 3-31). Essas faixas possuem um limiar máximo ($bin_{\max}$) e um mínimo ($bin_{\min}$), sendo $\hat{\Re}^t$ pertencente a essa faixa. O histórico de opiniões H é representado por um conjunto de tuplas na forma (a_3, a_2, $bin_{\min}$, $bin_{\max}$, $\hat{\Re}^t_{a_3,a_2}$, $O^t_{a_3,a_2}$).

$$\mathrm{E}_{\hat{\Re}^t} = \frac{a}{a+b}, \text{ onde } a = \hat{m}^t + 1 \text{ e } b = \hat{n}^t + 1 \qquad \text{eq. 3-31}$$

O segundo passo para barrar opiniões imprecisas é calcular a probabilidade da opinião $\hat{\Re}^t_{a_3,a_2}$ provida por um agente específico ser precisa. Denota-se por $r^t_{a_1,a_3}$ a precisão da opinião provida por um opinante a_3 de acordo com a visão de a_1 no tempo t.

Para o cálculo dessa probabilidade, é necessário calcular o valor esperado de $\hat{\Re}^t_{a_3,a_2}$ para que seja possível determinar a faixa na qual essa opinião se encaixa, encontrando o seu limiar. Com isso, obtém-se um subconjunto, h, de H que contém todas as tuplas que coincidem com (a_3, - , $bin^{\hat{\Re}^t_{a3,a2}}_{\min}$, $bin^{\hat{\Re}^t_{a3,a2}}_{\max}$, - , -), representando opiniões anteriores de a_3 similares a $\hat{\Re}^t_{a_3,a_2}$. O conjunto h é utilizado para determinar os parâmetros a e b de uma distribuição beta que representa o comportamento atual de a_2, na perspectiva de a_1, em todas as situações nas quais o opinante a_3 provê uma opinião parecida com $\hat{\Re}^t_{a_3,a_2}$.

a = número de tuplas em h (onde $O_{a_x,a_y} = 1$) + 1

b = número de tuplas em h (onde $O_{a_x,a_y} = 0$) + 1

Dessa forma, a probabilidade de precisão $r^{t}_{a_3,a_2}$ é definida com a área abaixo da distribuição beta produzida utilizando h, delimitada pelos limites da faixa pertencente a $\hat{\Re}^{t}_{a_3,a_2}$.

$$r_{a_1,a_3} = \frac{\int_{bin_{\min}^{\hat{\Re}^{t}_{a_3,a_2}}}^{bin_{\max}^{\hat{\Re}^{t}_{a_3,a_2}}} (\mathrm{B}_{a_1,a_2})^{a-1}\left(1-\mathrm{B}_{a_1,a_2}\right)^{b-1} d\mathrm{B}_{a_1,a_2}}{\int_0^1 U^{a-1}(1-U)^{b-1} dU} \qquad \text{eq. 3-32}$$

Se o opinante a_3 tem falado sempre a verdade e provido opiniões precisas, com o passar do tempo o pico da curva da distribuição beta estará na faixa que $\hat{\Re}^{t}_{a_3,a_2}$ está presente, resultando em um elevado valor para $r^{t}_{a_3,a_2}$, conforme pode ser observado pela Figura 3-2.

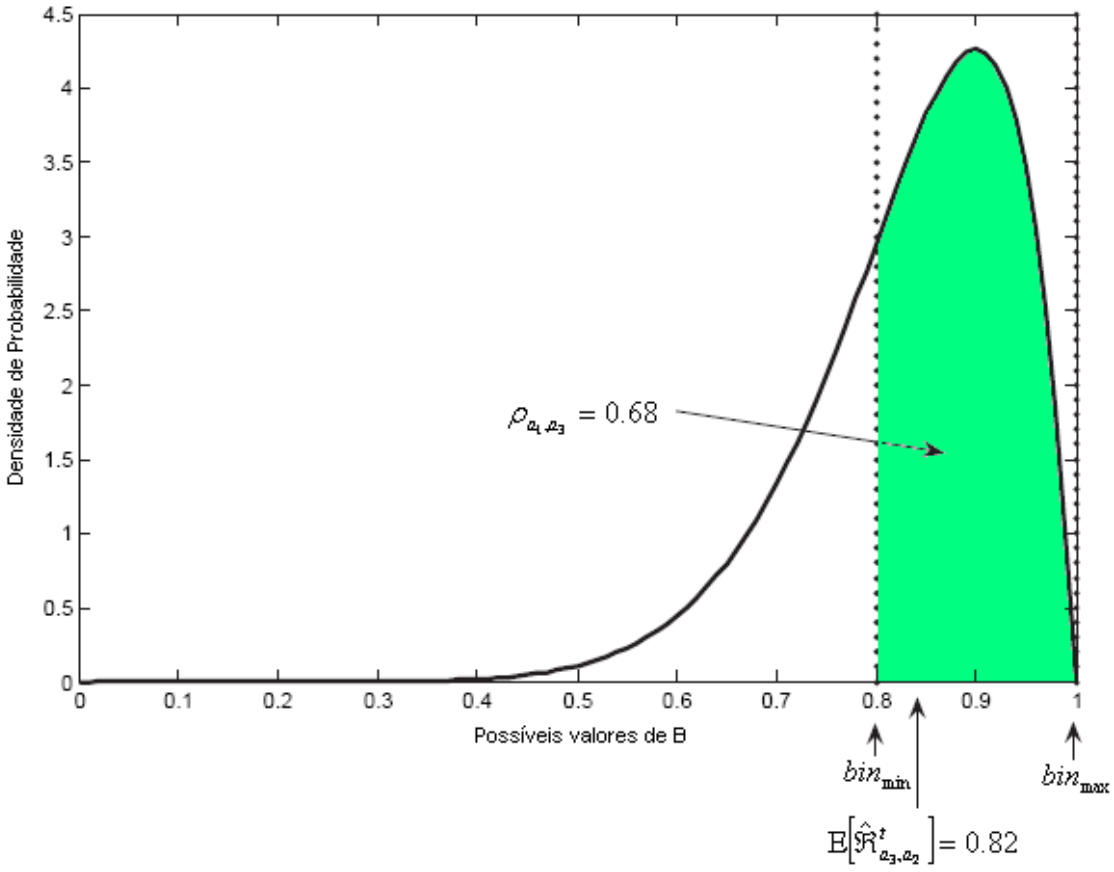


Figura 3-2 – Curva da distribuição beta demonstrando o alto valor de r obtido quando o opinante fornece opiniões precisas e honestas [3]

Por outro lado, se o agente opinante a_3 mente de forma constante e provê opiniões imprecisas, o pico da distribuição beta não estará na faixa na qual se encontra $\hat{\Re}^t_{a_3,a_2}$, resultando em um baixo valor para $r^t_{a_3,a_2}$. Esse comportamento pode ser observado pela Figura 3-3.

O último estágio para barrar opiniões imprecisas é reduzir seu impacto na reputação de um nodo. Para tal, é preciso avaliar as propriedades da distribuição beta, analisando o efeito do acréscimo de novas opiniões na combinação final. O desvio da curva contribui para a confidência da distribuição da combinação.

O modelo utilizado visa diminuir a distância entre o valor esperado $\mathrm{E}_{\hat{\Re}^t}$ e a variância $s^{\,2}_{\hat{\Re}^t}$ (da distribuição da opinião) e a distribuição uniforme ($a = 1$ e $b = 1$). Denota-se o valor esperado da distribuição uniforme como $\mathrm{E}_{uniforme}$ e sua variância como $s^{\,2}_{uniforme}$.

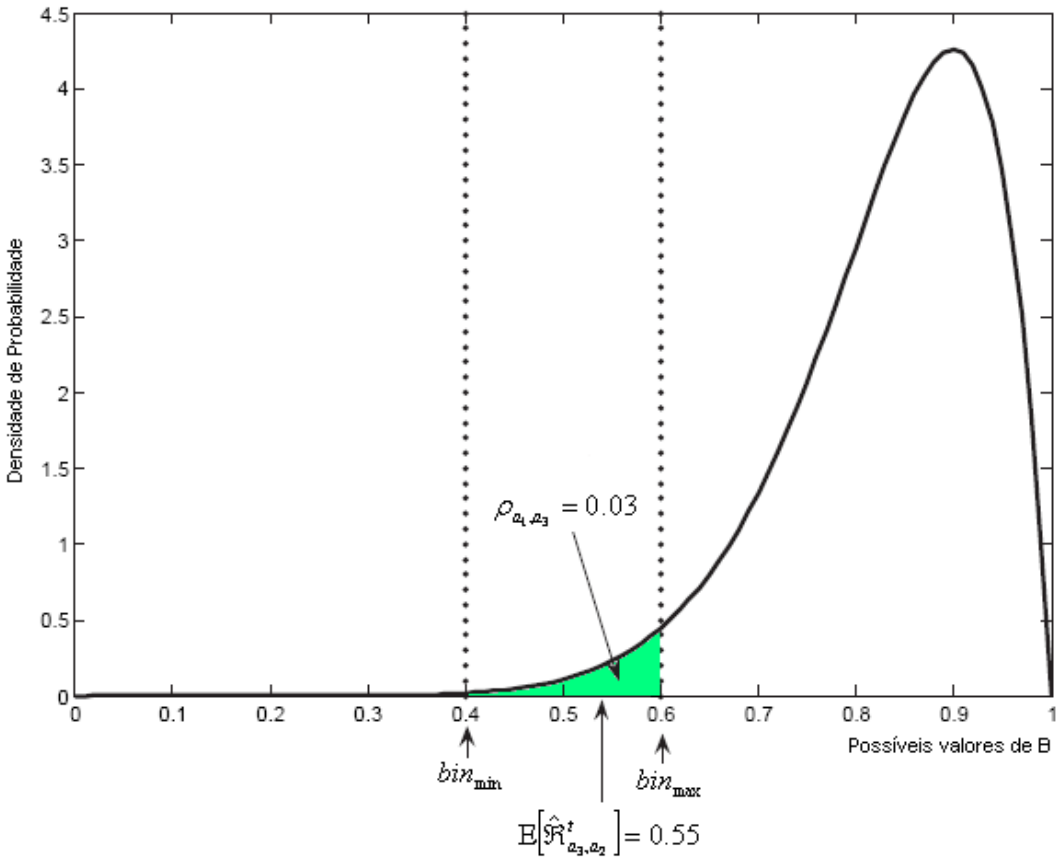


Figura 3-3 – Curva da distribuição beta demonstrando o baixo valor de r obtido quando o opinante fornece opiniões imprecisas e desonestas [3]

Considerando um agente a_3 que provê opinião para a_1 sobre a_2, a eq. 3-33 e a eq. 3-34 mostram essa redução de distância. A barra presente acima da letra (por exemplo, $\overline{a}$) refere-se à distribuição ajustada.

$$\overline{\mathrm{E}}_{\hat{\Re}^t_{a_1,a_3}} = \mathrm{E}_{uniforme} + r_{a_1,a_3}.\left(\mathrm{E}_{\hat{\Re}^t_{a_1,a_3}} - \mathrm{E}_{uniforme}\right) \qquad \text{eq. 3-33}$$

$$\overline{s}^{2}{}_{\hat{\Re}^t_{a_1,a_3}} = s^{2}{}_{uniforme} + r_{a_1,a_3}.\left(s^{2}{}_{\hat{\Re}^t_{a_1,a_3}} - s^{2}{}_{uniforme}\right) \qquad \text{eq. 3-34}$$

Para combinar os valores das opiniões obtidas, além de ajustar todas as distribuições das opiniões, é necessário ajustar os parâmetros da distribuição beta e os valores de $\hat{m}^t$ e $\hat{n}^t$ que formam a opinião.

$$\overline{a} = \frac{\left(\overline{\mathrm{E}}_{\hat{\Re}^t_{a_1,a_3}}\right)^2 - \left(\overline{\mathrm{E}}_{\hat{\Re}^t_{a_1,a_3}}\right)^3}{\left(\overline{s}_{\hat{\Re}^t_{a_1,a_3}}\right)^2} - \left(\overline{\mathrm{E}}_{\hat{\Re}^t_{a_1,a_3}}\right) \qquad \text{eq. 3-35}$$

$$\overline{b} = \frac{\left(1-\overline{\mathrm{E}}_{\hat{\Re}^t_{a_1,a_3}}\right)^2 - \left(1-\overline{\mathrm{E}}_{\hat{\Re}^t_{a_1,a_3}}\right)^3}{\left(\overline{s}_{\hat{\Re}^t_{a_1,a_3}}\right)^2} - \left(1-\overline{\mathrm{E}}_{\hat{\Re}^t_{a_1,a_3}}\right) \qquad \text{eq. 3-36}$$

$$\overline{m}_{a_3,a_2} = \overline{a} - 1 \qquad \text{eq. 3-37}$$

$$\overline{n}_{a_3,a_2} = \overline{b} - 1 \qquad \text{eq. 3-38}$$

3.2.4.1 Confidência

A confidência g_{a_1,a_2} é uma métrica que mede a probabilidade do valor atual B_{a_1,a_2} estar dentro de um nível de erro aceitável e sobre t_{a_1,a_2}, que é calculada pela equação por

$$g_{a_1,a_3} = \frac{\int_{t_{a_1,a_2}-e}^{t_{a_1,a_2}+e} (\mathrm{B}_{a_1,a_2})^{a-1}\left(1-\mathrm{B}_{a_1,a_2}\right)^{b-1} d\mathrm{B}_{a_1,a_2}}{\int_0^1 U^{a-1}(1-U)^{b-1} dU} \qquad \text{eq. 3-39}$$

Sua representação é dada na Figura 3-4. O nível aceitável de erro e influencia quão confidente é um agente, dado o mesmo número de observações.

Com a inserção desse conceito na implementação de um agente CTA (C*ombined Trust Agent*), ocorre alteração no cálculo de confiança. O agente a_1 calcula t_{a_1,a_2} baseado na sua experiência direta com a_2. Se o valor de t_{a_1,a_2} tiver uma confidência correspondente g_{a_1,a_2} abaixo de um valor mínimo predeterminado, denotado por q_g, a_1 buscará a opinião de outros agentes sobre a_2 de modo a obter uma confidência acima desse valor.

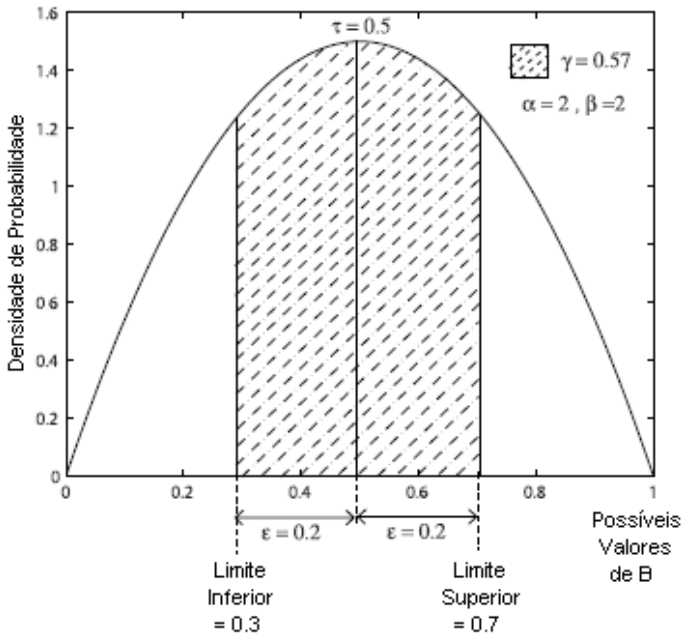


Figura 3-4 – Confidência é a área abaixo da distribuição beta cercada pelo limite superior e inferior, calculado pela adição e subtração do erro e obtido do valor de confiança t [3]

3.2.5 Combinação de Confiança direta e reputação no TRAVOS

Utilizando a distribuição beta para modelar o comportamento de um agente, é possível combinar as informações obtidas por experiência direta com as opiniões coletadas por outros agentes. Conforme apresentado anteriormente, o histórico de interações diretas entre os agentes a_1 e a_2 é representada por $\Re^t_{a_1,a_2} = \left(m^t_{a_1,a_2}, n^t_{a_1,a_2}\right)$ e as opiniões coletadas de outros nós por $\hat{\Re}^t_{a_3,a_2} = \left(\hat{m}^t_{a_3,a_2}, \hat{n}^t_{a_3,a_2}\right)$.

Assim, para combinar a opinião pessoal com a reputação, é preciso enumerar todas as opiniões, como apresentado pela eq. 3-28. Obtidas todas as informações, é possível calcular os parâmetros da distribuição beta e o nível de confiança combinada $t^c_{a_1,a_2}$.

$$\hat{a} = M_{a_1,a_2} + \overline{m}^{t}_{a_1,a_2} + 1 \text{ e } \hat{b} = N_{a_1,a_2} + \overline{n}^{t}_{a_1,a_2} + 1 \qquad \text{eq. 3-40}$$

$$t^{c}_{a_1,a_2} = \frac{\hat{a}}{\hat{a} + \hat{b}} \qquad \text{eq. 3-41}$$

Sabendo como calcular a combinação de confiança direta e reputação, é possível criar um agente de confiança combinada (CTA – *Combined Trust Agent*). Assim, para esse agente, o nível de confiança total é igual ao nível de confiança combinada, $t_{a_1,a_2} = t^{c}_{a_1,a_2}$.

A vantagem desse método é que ele utiliza tanto informações pessoais do agente como evidências externas obtidas de outros agentes. A desvantagem é que, mesmo com a combinação, poderá haver alguns agentes que exercerão influência no cálculo de confiança provendo informações imparciais, tanto para o lado negativo quanto para o positivo. Essa limitação pode ser contornada concedendo ao agente a habilidade de determinar a confidência presente em suas observações e somente buscar opiniões de terceiros se esse nível não for suficiente.

3.3 SÍNTESE DO CAPÍTULO

O principal objetivo deste capítulo foi fazer uma revisão de modelos de confiança e reputação aplicados a ambientes computacionais distribuídos e de certa maneira auto-organizados. Isto permitiu citar diversos autores e modelos referenciados por diversos trabalhos. Além disso, foi possível fazer uma análise mais detalhada de como gerar e calcular a confiança em diversos aspectos de um ambiente distribuído. Assim, o mapeamento de confiança de um para um (1:1) é bastante comum e já aplicado em outros cenários conforme pode ser explicado segundo os modelos revisados.

Entretanto, o problema de confiança em grupos (1:N) ou (M:N) ainda não foi amplamente discutido, apesar de já ter sido citado como necessidade em diversos trabalhos de confiança anteriores a este.

4 PROPOSTA DE UM MODELO DE CONFIANÇA PARA GRUPOS

Este capítulo trata de alguns conceitos para a aplicação da confiança e propõe um modelo de como fazer seu cálculo na situação de grupos.

Alguns aspectos de segurança (integridade, confidencialidade, disponibilidade) também serão tratados para que o modelo de confiança seja capaz de gerar e trocar informações que representem a confiança em grupos, sem necessariamente criar um modelo demasiado complexo em seus aspectos técnicos. Até mesmo porque isto torna a implementação um verdadeiro problema de codificação, devido a requisitos extremamente complicados e, às vezes, até desnecessários.

Além disso, determinados problemas importantes na formação de grupos, processos de votação, os problemas de consenso e diversos outros assuntos correlatos são referenciados de maneira a se obter o maior conjunto de informações possíveis para a representação de um modelo de confiança que englobe o detalhamento necessário para grupos e algumas características sobre consenso.

4.1 CONSIDERAÇÕES INICIAIS

Em sistemas distribuídos, uma das principais formas de se adquirir a confiança envolve situações dos nodos, cujas ações passadas ou fatos históricos, possam influenciar na tomada de decisão para o cálculo e a geração da confiança. Entretanto, outros aspectos influenciam esta situação porque um nodo que não tenha nenhum tipo de interação prévia com outro nodo não poderá usar nenhum valor, porque, neste caso, ele simplesmente não o terá.

De posse de algumas considerações, tais como os dados prévios sobre confiança, a identificação do nodo, além de outros atributos iniciais, incluso ainda a necessidade de resolução de algum tipo de problema em específico, um determinado nodo em um ambiente distribuído pode tomar uma decisão de confiar ou não em outro nodo para a resolução de um determinado problema de forma colaborativa.

Pois bem, é comum a formação de grupos de nodos nas redes ([32], [41], [46], [47], [51]). Grids, MANET e P2P são exemplos claros deste tipo de formação, conforme citado nos capítulos anteriores. Agentes de software também são capazes de formar uma comunidade de agentes, gerando uma idéia de grupos.

Na formação de grupos devem ser tratados os aspectos que envolvem as situações de como que determinado nodo (1) ou um grupo de nodos (M) possa confiar em outro grupo de nodos (N). A Figura 4-1 ilustra este esquema.

A idéia pretende alcançar a resposta de como uma entidade A pode confiar em um grupo Y, na qual desconhece parcial ou totalmente os seus membros, entretanto necessita dos serviços oferecidos pelo grupo Y. De maneira análoga visa preencher a lacuna de como o grupo X pode confiar no grupo Y dada à necessidade de solução de algum problema cujo grupo Y possa auxiliar. Nesta consideração inicial, existem problemas que precedem ao tratamento para uma possível solução. Alguns deles são discutidos no decorrer do texto e nos tópicos seguintes.

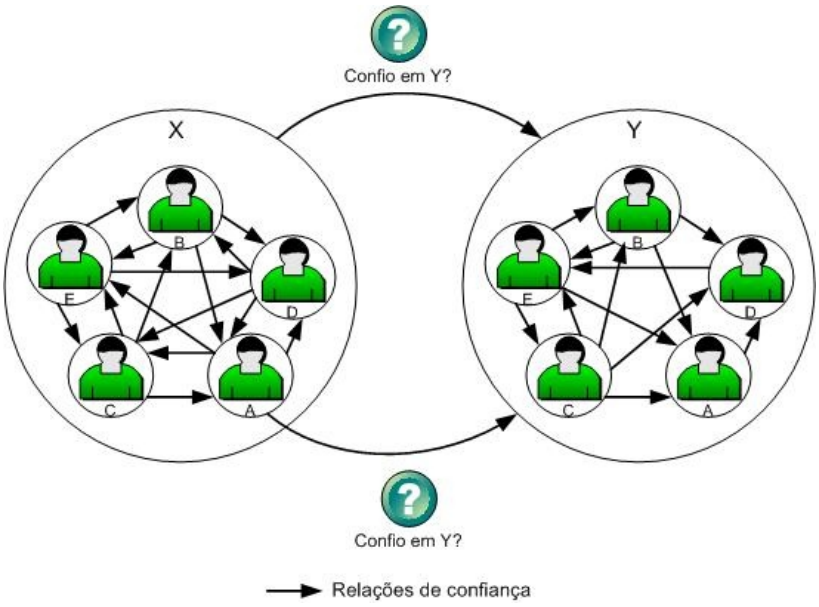


Figura 4-1 – Relações de confiança de 1:N e de M:N

Para de Sousa Jr. *et al.* [19], a gestão da confiança em redes espontâneas auto-organizadas é um mecanismo que visa reduzir a complexidade do controle de acesso e da autorização de operações, permitindo tratar a descentralização estrutural dessas redes, a dinâmica da entrada e saída dos usuários, a mobilidade (considerando redes móveis) e a possibilidade de um grande número de entidades participantes.

Isto leva ao ponto em que nessas redes espontâneas, o próprio subsistema de controle da rede, assim como as aplicações, constitui sistema distribuído que, sem possuir uma estrutura fixa previamente determinada e sem contar com um controle central, se organiza de maneira autônoma para prover uma estrutura de comunicação e de processamento para as

entidades participantes. Tais características são comuns a redes móveis ad-hoc, grids computacionais, sistemas peer-to-peer, comunidades de agentes etc.

No caso de redes sociais, a idéia parte de um pré-suposto da formação de "comunidades" ou "ambientes sociais" virtuais dentro de uma infra-estrutura tecnológica baseada em uma rede de comunicação. Seguindo o tratamento da Figura 4-1, o relacionamento de A com B, C, D e E é um tipo de rede social, em que A dentro de sua perspectiva, relaciona-se com B, C, D ou E para atingir um objetivo específico. O mesmo é válido na perspectiva de B, C, D e E para seus respectivos relacionamentos. Então, estes relacionamentos geram uma idéia de grupo ou comunidade virtual, que tem um tempo de formação finito, com um objetivo em comum e com ação limitada dentro do seu objetivo.

Em Grids, a formação destas comunidades virtuais é mais complexa porque depende de outros requisitos que não só um agente ou um nodo, entretanto, o princípio de funcionamento é o mesmo. Em um Grid pode existir um conjunto de nodos que saibam resolver um determinado tipo de problema ou que ofereçam um determinado serviço, formando assim um grupo ou uma comunidade para alcançar a solução de um problema específico.

Em outra perspectiva, considere que dentro de uma comunidade de agentes, encontra-se um determinado conjunto finito de agentes capazes de fazer processamento de imagens. Este conjunto de agentes forma uma pequena comunidade especialista, podendo ser comparada inclusive com um pequeno cluster. Considere ainda que dentro ou fora desta comunidade, exista um determinado agente com um problema de renderização de uma imagem, que sozinho não será capaz de realizar a sua tarefa em tempo hábil. Este agente, sabendo da existência deste grupo de agentes especialistas, pode solicitar ao grupo ou à comunidade que o auxiliem na execução da sua tarefa. Ainda assim ainda é necessário responder como confiar na comunidade de agentes da qual não possui nenhuma informação. Isto requer a definição de um modelo capaz de representar a definição de confiança e reputação na perspectiva de 1:N.

Considere outro exemplo. O grupo P do Grid A precisa de informações ou de um serviço do grupo Q do Grid B, mas alguns nodos do grupo P já sabem que alguns nodos do grupo Q não possuem um grau de confiança aceitável e nem a reputação também é considerada boa. Entretanto, como a imagem ou a representação de confiança e de reputação do grupo Q pode ser mais forte, quando comparada com a confiança individual de seus membros, o grupo P pode comunicar-se com o grupo Q. Isto, da mesma forma que a anterior,

requer um modelo de confiança capaz de fazer a representação de confiança e reputação de na perspectiva de M:N.

Fazendo um paralelo com o mundo real, a representação de grupos, empresas, comunidades, sociedades, entre outros, passam a idéia de que possa existir a confiança de relacionamento com tais grupos, ou seja, fazem as demais pessoas a acreditar e a confiar em uma imagem do grupo, associada à resolução de algum tipo de problema. Neste caso, os grupos, empresas, comunidades, sociedades, entre outros, são compostos por vários membros (N).

Aprofundando esta situação, se uma determinada pessoa tem um problema e sabe que a empresa A consegue resolvê-lo, esta pessoa tende a procurar a empresa A para auxiliá-lo no seu caso. Se a empresa executa um bom serviço, a pessoa fica satisfeita e aumenta seu grau de confiança na empresa e no serviço executado (contexto). Entretanto, se a empresa (ou pessoa que representa a empresa) não realiza o serviço a contento, a pessoa não fica satisfeita e também diminui a confiança que já poderia ter ou adquirir sobre a empresa. E ainda passar a sua opinião para outros, gerando uma reputação negativa para a empresa. Isto é um exemplo da necessidade de representação de 1:N.

Agora suponhamos que não uma pessoa, mas uma empresa X, necessita dos serviços fornecidos por outra empresa Y. Tanto X quanto Y possuem boa reputação e boa aceitação na execução de seus serviços, através de opiniões sobre as mesmas. Se Y realiza o serviço a contento para X, mas X não cumpre a sua parte do acordo, a imagem de X será má vista por Y, mas a de Y será bem vista para X. Isto gera uma representação de M:N.

Da mesma forma que a representação da confiança e da reputação de 1:1, a representação de 1:N e de M:N ocorre dentro de um contexto, entretanto, o que está em observação não é mais a situação de um nodo em particular, mas sim de um grupo ou uma comunidade (N) perante a um (1) nodo ou a outro grupo (N).

Assim, conforme visto na revisão do capítulo 3, os modelos atuais e as referências pesquisadas, não abrangem as situações de 1:N e M:N, envolvendo agentes e suas comunidades, P2P e suas redes e nem Grids, não se tendo um modelo que trate da representação da confiança na perspectiva de um grupo.

4.1.1 Requisitos de um modelo confiança computacional

Patel [3] apontou diversos pontos importantes e que são necessários na formação de um modelo de confiança. Os seus requisitos envolvem basicamente funcionalidades ou

aspectos que devem ser tratados em um modelo de confiança. Tais aspectos estão resumidos na Tabela 4-1.

Tabela 4-1 – Requisitos gerais de um modelo de confiança segundo Patel [3]

#	Requisito	Descrição
1	Ser escalável	Não deve sofrer em performance e ser restrito ao número de entidades que participam em seu processo, ou seja, deve ser escalável.
2	Ser descentralizado	Deve ser robusto e continuar seu funcionamento, mesmo em situações de falhas na rede.
3	Fazer distinção entre entidade e ambiente.	Deve ser capaz de fazer a distinção entre o papel de uma entidade e o papel do ambiente que percebido pela entidade, principalmente pelas características não determinísticas de uma rede que normalmente deverá estar inserido.
4	Calcular confiança direta	Deve permitir um agente realizar o cálculo de um nível de confiança para um agente de interação potencial, baseado em experiências passadas que já teve com este agente potencial.
5	Calcular a reputação	Caso não tenha experiência prévia, o modelo deve ser capaz de permitir que o agente faça o cálculo do nível de confiança para um agente de interação potencial baseado nas opiniões de outros agentes.
6	Encontrar reputação	Oferecer mecanismos que permitam a identificação de fontes de opiniões em potencial, além dos protocolos para tal objetivo.
7	Incentivar provimento de opiniões	Para a realização do requisito #5, o agente deve prover razões para que outros agentes dêem sua opinião sobre outro agente.
8	Ajustar opiniões	Prover mecanismos de ajustar as opiniões de outros agentes (confiabilidade) de tal forma que não seja enganado por opiniões falsas.
9	Guardar histórico de iterações	De acordo com a necessidade de novos cálculos de níveis de confiança, o agente deve manter uma base com o histórico de situações passadas com outros agentes e a respectiva opinião sobre o fato ocorrido.
10	Usar informações sociais	Em determinadas organizações, o uso de informações sociais se torna fonte de informações que pode auxiliar no cálculo da confiança.
11	Valor de confiança dinâmico	O valor da confiança deve ser ajustável de acordo com a opinião formada do agente sobre outro. À medida que a opinião muda, o valor de confiança também deverá ser mudado, dependendo da situação em si.
12	Consenso no nível de confiança	Deve permitir que um grupo de agentes alcance um consenso sobre o nível de confiança em um determinado indivíduo interno ou externo ao grupo.
13	Nível de confiança do grupo	Em alguns casos é necessário avaliar ou se ter um nível de confiança de um grupo ou de seus membros dentro do grupo.
14	Troca efetiva de opiniões	Deve prover forma que permita os agentes trocarem informações de maneira eficiente e rapidamente.
15	Distribuir informações sobre confiança	Dado o requerimento #2, as informações sobre confiança não podem ficar guardadas unicamente em um ponto central.
16	Dependente de contexto	Permitir que os agentes troquem informações sobre um contexto em si e os níveis de confiança obtidos de forma que possam avaliar o contexto e o nível de confiança que foi obtido.

Apesar dos avanços realizados por Patel [3], seu trabalho não permitiu alavancar os requisitos de número 12 e 13 e apenas menciona poucas idéias de um trabalho futuro. Além disso, levando em consideração tais informações, é importante avaliar que os aspectos de identificação e de segurança, que normalmente estão ligados durante a apresentação de uma identidade, sejam corretamente tratados até mesmo para se ter a garantia da criação de um grupo com membros confiáveis, ou pelo menos facilmente identificáveis.

4.2 CONFIANÇA EM GRUPOS

Considerando uma perspectiva computacional, o tratamento de grupos pode ser exercido através da representação da liderança ([20], [79], [80], [81], [82]). As entidades, através de algum mecanismo de votação ou consenso, podem fazer com que um membro M seja o líder para assumir a representação de um grupo G e esta informação pode ser publicada em um canal de broadcast qualquer (página, informação, mensagens etc.).

Considerando processos de votação normais, o fato de um nodo obter um maior número de votos, não necessariamente o faz o melhor líder, apenas o mais votado segundo algum critério (consenso parcial). O consenso total envolveria a definição de critérios próprios para o tratamento do problema de tal forma que qualquer entidade saberia e aceitaria a eleição de um líder, que seria considerado capaz de representar o grupo, o que em um sistema distribuído não é tarefa trivial de ser implementada.

4.2.1 Representantes por um grupo

Dentro de uma perspectiva inicial, o problema da representação com o foco na confiança exige um tratamento diferenciado porque existem alguns critérios que podem ser assumidos, quando se pondera sobre um grupo. Considere o seguinte exemplo. Quando você (entidade A) necessita de ir a uma instituição financeira – um Banco (entidade G) – normalmente é porque deseja resolver algum tipo de problema que necessite da intervenção ou do auxílio de G. No processo de chegada ou de tratamento com G, normalmente A é atendido por um membro (M) que integra G, ($M \in G$), sendo que M possui determinados poderes de representação de G. Entretanto, em situações normais, A não escolhe M. M de uma forma ou de outra, já está disponível para A, até mesmo porque uma das funções de M é ser interface de comunicação com G ($A \overset{\rightarrow}{\leftarrow} M \overset{\rightarrow}{\leftarrow} G$).

Ocorre que muitas das vezes M não conhece A e não tem como verificar nem se A é confiável ou não. O mesmo ocorre na perspectiva de A, que por uma necessidade específica precisa de algum tipo de serviço de G. Neste processo, o que é normal é a verificação das credenciais de cada um. M solicita determinada identidade de A, até mesmo para saber se M pode ou não atender a demanda de A. Após essa verificação, M passa a inserir e tratar os dados necessários em G. Neste ponto, a apresentação de identidades não chega a ser um critério de segurança razoável, porque a falsificação de identidades é um problema comum em redes.

Estendendo a discussão, em determinadas situações, A não é atendido só por M. Pode ser atendido por mais de uma entidade (M_1, M_2, M_3, ..., M_n), e que do mesmo jeito que M, fazem parte de G. Isto é $G = \{M_1, M_2, M_3, ..., M_n\}$, onde seus integrantes possuem poderes para fazer a representação de G. Até este ponto a complexidade é tratada porque A simplesmente "entende e aceita" que a única forma de atender sua necessidade de serviço que tem em G é utilizar M ou M_1, M_2, M_n. Quando comparada com uma perspectiva humana, esta situação é extremamente comum.

Agregue-se então o ponto de vista computacional. A é uma entidade na rede que necessita de serviços de G e só pode se comunicar através de M (ou M_1, M_2, M_n), mas não possui nenhum indicativo de confiança sobre G ou até mesmo sobre M. E agreguem-se quais os critérios que M pode demonstrar para A de que é um representante legítimo de G. Ou ainda quais os critérios que G levaria em consideração para atender as solicitações de A, de acordo com sua representação (M ou M_1, M_2, M_n).

Sob o ponto de análise de A com M, fica claro que o processo é de 1 para 1 (1:1), mas não fica claro sob este mesmo ponto de vista de que M, sem uma identidade válida, é o representante de G, até mesmo porque A não deseja M, mas sim G. Isto faz com que a comunicação sob o ponto de vista de A seja de 1 para N (1:N), onde N representa as várias entidades para que se comunique com G.

Na perspectiva humana, G não precisa informar para A que M é o seu representante, até mesmo porque A conhece G através de algum mecanismo de difusão de informação. Neste ponto, A perspectiva de representação de G é mais tranqüila porque se assume uma série de outros valores, por exemplo, a interpretação que A faz de M em relação a G, a imagem e o julgamento que A faz de M, a necessidade em si de A, entre outros. É importante ressaltar que estes aspectos são voltados a sentimentos e análises puramente humanas, tornando a codificação destes problemas uma tarefa complexa.

4.2.2 Problemas envolvidos na confiança em grupos

A identidade do nodo tem uma forte influência nos aspectos que envolvem a confiança em grupos. Esta influência depende principalmente de critérios que sejam capazes de fazer com que um nodo seja reconhecido na rede através de alguma identidade, de preferência única, e que não possa ser falsificada facilmente. Estes critérios visam à proteção de um nodo contra outro nodo malicioso, capaz de gerar várias identidades e fazer se passar por outros nodos, como o que é proposto no ataque sybil [12].

Quando se considera as questões de confiança no processo de identificação de um determinado nodo em uma rede, ou até mesmo na formação de um determinado grupo, o problema de confiança requer conhecimentos passados, determinados tipos de interação, aquisição de informações sociais para auxílio no cálculo da confiança, entre outros, além de algum mecanismo próprio de atribuição de identidades.

Com o foco na liderança, a decisão de quem é o líder do grupo ou o ponto de contato para a representação do grupo, em uma situação ideal, exige um consenso por parte dos nodos, que devem utilizar algum processo cuja decisão implique na eleição de um representante ou até mesmo um grupo de representantes. Este problema envolve o tratamento de um líder que seja capaz de fazer a representação do grupo e ser o responsável pelos valores de confiança do grupo.

O problema da definição de confiança envolve aspectos fundamentais, como já apontados por Patel [3]. A questão do tratamento da confiança para grupos é que necessita de novas definições, basicamente no cálculo da confiança para grupos e o tratamento do consenso na confiança, ambos sem uma solução específica em sistemas distribuídos. Isto porque o conceito de confiança voltada para grupos, apesar de ser uma necessidade, exige soluções não triviais. Outro ponto focal deve-se a diversidade de recursos computacionais existentes, trabalhando com características próprias e às vezes sem interoperabilidade (Grids, agentes de software, P2P, Ad Hoc etc.). Uma das maneiras de solução destes pontos é através da criação de modelos seguindo alguns delimitadores, que normalmente são difíceis de mensurar porque depende do ambiente e das suas características próprias. Até mesmo porque a quantidade de variáveis analisada, normalmente é muito grande.

Ainda observando a questão da confiança para grupos, o problema necessita da geração de um consenso da confiança. De acordo com as referencias consultadas, é um problema que não pode ser mapeado simplesmente assumindo a diretiva de que “se você confia, eu também confio”. Até mesmo porque isso é uma das características da não

transitividade da confiança (se A confia em B, e B confia em C, A não necessariamente confia em C).

Além do consenso, outro problema que pode influenciar na confiança é a formação dos próprios grupos. Exemplificando esta situação, se um nodo quiser entrar em um determinado grupo porque acredita que possui certa afinidade com o grupo em questão, de uma forma ou de outra, ele teria que ser “aceito” pelo grupo. Mas, em determinados casos, para a sua saída não é necessário um “aviso prévio”, mesmo sendo esta a situação ideal, em que os demais nodos seriam informados sobre a sua saída. Em redes distribuídas, a saída de um nodo da rede não pode ser facilmente prevista, porque a quantidade de variáveis envolvidas torna a saída de um nodo de um determinado grupo em uma situação de quase adivinhação.

O comportamento do nodo também influência na sua permanência ou até mesmo na sua junção com um determinado grupo. Se alguma entidade já conhecer previamente o nodo (sua reputação) e seu comportamento passado for taxado como negativo (comportamento ruim), a sua entrada em um grupo pode ser bloqueada, a fim de evitar problemas facilmente previsíveis (ataques, informações espúrias, desinformação etc.). Além disso, existem diversos outros problemas voltados para os aspectos de segurança (autenticação, confidencialidade, distribuição de informações etc.), ataques conhecidos em redes e sistemas distribuídos, bem como outras situações que podem influenciar neste processo, com o intuito de prejudicar uma comunicação em um grupo ou simplesmente a impedir.

Os pontos de segurança devem ser considerados porque a confiança trata de valores que são trocados em uma rede de comunicação. Esses valores são computados individualmente, considerando aspectos da experiência da entidade em si, de contexto e de aspectos históricos de uma transação ocorrida. A reputação também faz uma forte diferença na análise e na formação da confiança por parte de outras entidades, gerando valores que podem ser agregados, ou simplesmente uma informação com que pode se levar a uma tomada de decisão em um processo de comunicação dentro de uma rede. Então uma informação falsa computada influencia nos valores de confiança e reputação.

4.3 LIDERANÇA EM GRUPOS

Conforme citado anteriormente, existem diversos problemas para o tratamento de grupos em redes distribuídas, espontâneas e auto-organizadas.

No tratamento da confiança, a formação de grupos por determinado interesse é um aspecto relativamente comum. Basta observar a criação de comunidades de agentes, sistemas P2P, coalizão de nodos para um objetivo, Grids com organizações virtuais, entre outros. Entretanto, é importante responder como escolher um líder em uma situação em que não se tem nenhum critério de confiança atribuído, ou nem todos confiam diretamente no líder que por ventura possa existir. Ou ainda, aprofundando alguns pontos específicos da confiança, existem situações onde não se confia ou não se sabe definir o líder de um contexto do grupo (liderança em um subgrupo), e isto deve ser tratado em sistemas distribuídos quando o foco é a confiança, a reputação e o consenso.

Observando estes aspectos, os tópicos abaixo tentam evoluir o conceito do tratamento da confiança levando em consideração pontos na formação de líderes e algumas de suas características.

A formação da liderança em grupos segue duas linhas de criação. A primeira diz respeito ao processo através do qual o líder é eleito segundo um processo de contagem de votos. Já o segundo diz respeito ao processo que envolve a aquisição de consenso.

4.3.1 Liderança computacional

A formação do grupo necessita de entidades que se juntem em torno de um interesse comum, tornando-se membros de um grupo. E este grupo necessita da figura de um líder, ou seja, o responsável pelas tomadas de decisão que envolve o grupo como um todo, e até mesmo para ser o responsável por agregar as questões para o cálculo da confiança em grupos.

No aspecto computacional, a representação da liderança normalmente é feita pela eleição em comum de um nodo. A partir deste momento o nodo eleito por algum mecanismo (normalmente por votação) é responsável pelo tratamento e processamento de informações que refletem a sua posição de liderança no grupo. O processo de liderança em si, envolve envio de mensagens, solicitação de informação, controle de entrada de novos membros, entre outras situações.

Considerando o consenso no aspecto da liderança, para se alcançá-lo em sistemas distribuídos, é necessária antes a criação de um processo que garanta a liderança de um grupo. O problema envolve a elaboração de acordos sobre um determinado problema ou uma determinada situação. Os nodos devem então gerar valores onde concordam ou discordam sobre o assunto tratado. O desafio neste ponto envolve o recolhimento de informações na rede

mesmo com a presença de falhas, de forma a auxiliar no mecanismo de elaboração de escolha da liderança do grupo.

Para Gupta *et al.* [78] o problema de eleição de um líder só pode ser resolvido se e somente se existir um processo eficiente de descobrimento de falhas. Tal situação requer um sistema de monitoração perfeito que suspeite o tempo todo sobre eventuais falhas, o que por si só, é um processo complexo e muito difícil de ser alcançado em sistemas muito grandes.

Da mesma forma que a confiança, alguns pontos da liderança depende de um contexto. Em um grupo que possui muitas funcionalidades ou é capaz de executar diversos serviços, o melhor líder para a situação X não necessariamente o torna o melhor líder, no mesmo grupo, para a situação Y. Na perspectiva da confiança, isto cria um problema de que em determinados grupos possa existir mais de um líder no grupo para cada contexto ou de serviços do grupo. Por exemplo, o líder L_1 é responsável pelo contexto C_1, já o líder L_2 é responsável pelo contexto C_2 e o líder L_n pelo contexto C_n. De maneira geral, esta situação implica que uma liderança geral L pode ter um ou mais representantes de liderança por contexto, $L = \{L_1, L_2, ..., L_n\}$.

Em uma situação mais evoluída, o representante do grupo possui habilidades o suficiente para representar o grupo nos vários contextos.

Entretanto, em sistemas distribuídos, o ponto focal do problema voltado para a confiança é que um Líder L pode não ser capaz de representar o grupo em todos os contextos. Apenas naquilo que o grupo o considera capaz de representação, o que normalmente necessita de um processo de decisão e não apenas votação. Uma das maneiras de se resolver este problema é através do correto mapeamento do consenso e dos aspectos de liderança.

4.3.2 Votação

O processo de votação está diretamente relacionado com a escolha de uma alternativa dentro de várias. Considerando a sua representação, a votação é um modelo do tipo “perde ou ganha”, em que a maior parte se preocupa com um número ou um conjunto deles que é usado para se ganhar o processo, do que o assunto propriamente dito que necessita de uma votação.

O principal aspecto no processo de votação é de que ele não leva em consideração informações individuais (necessidade ou sensação – por exemplo, a confiança). Em sua essência é um método quantitativo e não qualitativo de tomada de decisão.

Em uma comparação com um ambiente computacional, a votação seria o ato de eleger um nodo para a representação de um determinado grupo, entretanto, critérios e aspectos da

confiança em si, do contexto da situação, não são considerados. Por exemplo, em um processo de votação dentro de um grupo de nodos, sendo que por algum motivo qualquer, o nodo A ou o nodo B são os concorrentes, ganhará o que obtiver o maior número de votos. Em uma rede de comunicação, esse processo pode ser simplesmente por envio de mensagens de broadcast com o respectivo voto. Entretanto, é importante ressaltar que isso não deixa a representação da votação muito transparente quando se tem vários contextos em uma situação, o que seria necessário uma votação para cada contexto.

Em uma perspectiva mais analítica, suponha que um nodo A confia no nodo B e vota nele para a situação W. O nodo A sabe, através de seus aspectos históricos, decisões, necessidades ou até mesmo "bom-senso", que o nodo B é o melhor representante no contexto W. Isto quer dizer que o nodo A confia no nodo B para a situação W.

Contudo, o nodo A também sabe que no contexto Y, o nodo B não pode ser seu representante, muitas vezes até mesmo porque não possui ou não sabe de nada do nodo B que lhe transmita esta confiança, ou simplesmente porque não confia no nodo B no contexto Y.

Considerando o exemplo acima, o problema descrito não pode ser resolvido com um simples processo de votação. Um grupo envolvido em um consenso pode utilizar outras formas de decisão (individual, compromisso, regras majoritárias etc.) quando for apropriado, e um grupo que adota um modelo de consenso usará esse processo para qualquer item que envolva situações em específico onde existe a necessidade de escolha de uma figura representativa em um contexto.

Bhaskar *et al.* [79], propôs um modelo de eleição de um líder de grupo. O ponto chave de sua proposta reside em que todos os membros do grupo concordem em um mesmo líder. E para a conformidade da liderança, o líder envia periodicamente mensagens de broadcast através de uma rede de comunicação. A mensagem serve como prova de que o líder está ativo e operante na rede para os demais membros do grupo. No modelo de Bhaskar *et al.* [79], a idéia reside em alguns conjuntos de mensagens definidas como INIT (define a existência e o correto funcionamento de um nodo líder), IREPLY (reposta dos nodos a mensagem INIT) e IGROUP (mensagem criada pelo líder do grupo em função das respostas de IREPLY que é enviada a todos os nodos do grupo).

O trabalho de Bhaskar *et al.* [79], apesar de permitir a troca de informações de nodos em um grupo, não deixa claro como é o processo de formação de um grupo, simplesmente assumindo que já existe tal grupo. Também não sinaliza de forma clara o processo de escolha de um líder. Simplesmente assume que um nodo é líder e que este deve enviar mensagens de INIT.

Conforme explicado anteriormente, o processo de escolha de um líder baseado em critérios de confiança não pode depender exclusivamente de um processo de votação. É necessário definir como o líder é eleito pelo grupo e principalmente o seu contexto de representação, até mesmo porque um grupo pode ter diversas funções, oferecer e requisitar diversos serviços.

4.3.3 Consenso

No tratamento de questões que envolvem a confiança em grupos e a sua representação, o consenso se torna necessário. Assim, um modelo de confiança para grupos tem como pré-requisito a capacidade de os nodos trabalhem dentro de um limiar de consenso da confiança.

O consenso pode ser definido como um processo de decisão que envolve um determinado grupo. No aspecto humano, é um método pelo qual um conjunto de pessoas chega a um determinado acordo comum. Neste processo são recolhidas informações e idéias de todos os participantes (ou da maior parte), sintetizadas para um nível de entendimento comum, até que se chegue a uma decisão final aceita por todos. Através do consenso se obtêm o crescimento de uma comunidade e da confiança, além de se alcançar melhores soluções.

Em uma situação em que é necessário o consenso não significa dizer que todos acreditam que a decisão tomada é a melhor possível. Significa que dentro da situação, o grupo "sente" que nenhuma posição ou necessidade foi mal interpretada ou que não foi levada em consideração. Contudo, todos crêem que a melhor solução para o problema foi apontada, ou porque funciona, ou porque a coletividade, através da elaboração e formulação de proposta, encontra uma solução melhor, quando comparada a uma solução individualizada.

Através do consenso, o grupo trabalha as diferenças e alcançam uma posição satisfatória que é dividida entre todos. Contudo, também é possível que a visão de um membro seja forte o suficiente para influenciar todo o grupo.

O consenso, quando comparado com a votação, geralmente é um processo que toma mais tempo e requer maiores habilidades dos membros, o que implica em um maior consumo de recursos antes de uma tomada de decisão. O ponto forte nesta colocação é que se cria uma coalizão mais forte para a decisão em si, o que normalmente facilita a tomada de decisão de uma forma mais criativa. Até mesmo porque existe a capacidade de novas experiências e novos processos, e em conseqüência, a resolução de novos conflitos.

Para o consenso ser considerado como uma experiência positiva é necessário que o grupo tenha valores comuns, alguma habilidade em processos de grupos e na resolução de

conflitos ou uma visão de comprometimento, que permite que a solução seja alcançada De maneira mais facilitada. Outro ponto forte é o comprometimento com o grupo em si e tempo o suficiente para que todos participem do processo.

Inicialmente, para a formação do consenso uma proposta é discutida com o intuito de se alcançar uma decisão comum. Em uma situação normal, esta proposta é modificada diversas vezes e segue-se acrescentado novos pontos através de mais discussão, ou simplesmente se abandona a idéia porque parece que não existe uma saída plausível ou em um tempo hábil. Durante este processo a articulação de idéias é importante e existe a responsabilidade de quem não está de acordo com uma proposta, de fazer soluções alternativas.

É importante no processo de se alcançar o consenso que todos envolvidos sejam capazes de contribuir por vontade própria, através de suas próprias palavras e que sejam entendidas por todos os membros do grupo. Neste ponto, a coerção ou acordos são substituídos por outras soluções, que normalmente envolvem a criatividade e compromisso com a síntese. Uma vez que uma proposta seja entendida por todos e não existe nenhuma nova mudança solicitada, um facilitador pode perguntar se existe alguma objeção. Se esta não existir, se cria o processo de consenso e todos no grupo devem ficar cientes do que foi decidido.

As dificuldades em se alcançar o consenso envolvem basicamente a ausência de suporte, algumas ressalvas ou reservas, posição de não interferir, simplesmente bloquear o processo ou sair da proposta e não tomar nenhum partido. O problema neste ponto é que se vários membros do grupo não concordam com o assunto em si, não podem expressar sua opinião a favor de uma solução. Isto gera um impasse que deverá ser tratado de outra forma ou simplesmente abandonando a idéia e gerando-se uma nova. Ou no pior dos casos, partir para um processo de votação.

4.3.3.1 Regras básicas para o consenso

Para se alcançar o consenso em um processo decisório é necessário o tratamento de algumas regras básicas. Um determinado facilitador deve deixar o grupo à parte de uma decisão que precisa ser tomada e ajuda o grupo nos eventuais passos que devem ser tomados para se alcançar um acordo, mantendo o processo em movimento até que se chegue a um consenso com a participação de todos. É importante ressaltar que o facilitador não decide o problema, ele simplesmente arranja o encontro onde a decisão deve ser tomada. Ainda, se o facilitador tem algum interesse direto no problema, também não pode estar envolvido na

condução do processo para não direcionar e nem influenciar na discussão do assunto e conseqüentemente na decisão do grupo. Como o facilitador não é um representante oficial do grupo (líder), este por ser eleito por um processo de votação simples.

Considerando uma perspectiva humana do consenso, em determinados processos, o facilitador por ser ajudado por um auxiliar ou observador. Sua função é assistir e comentar as opiniões individuais e do grupo, bem como os níveis de participação. Uma terceira entidade (Secretário) também pode estar envolvida no processo como tomador de anotações ou memorizar as decisões tomadas, organizar o tempo de decisão de cada item e a agenda a ser discutida, até mesmo porque o tempo possui um aspecto importante neste tipo de processo.

4.3.4 Consenso com teoria dos generais bizantinos

Lamport *et al.* [80] apresentou um procedimento clássico para alcançar consenso sob falhas arbitrárias em sistemas síncronos. Este procedimento ficou amplamente difundido e conhecido como o algoritmo dos generais bizantinos, apresentado em 1982. O algoritmo garante consenso por troca de mensagens para qualquer tipo de falha quando o número total de nodos for maior ou igual a 3 vezes mais 1 o número de faltosos (3m +1, onde m equivale aos nodos falhos, que na teoria é denominado de traidores). Além disso, também é assumido que a) toda mensagem enviada é recebida corretamente, b) o receptor sabe quem enviou a mensagem, c) a ausência de uma mensagem pode ser detectada (por exemplo, através de um timeout).

Segundo Lamport *et al.* [80], sistemas tolerantes a falhas precisam suprir duas necessidades primárias para usarem o consenso. A primeira é de que os nodos possuam um algoritmo que lhes garanta estarem tomando decisões sobre o mesmo plano de ação. A segunda é que uma pequena quantidade de nodos maliciosos não pode fazer com que a decisão tomada pelos nodos bons seja errônea. Para garantir a primeira necessidade, todos os nodos bons devem receber os mesmos dados. Essa é uma necessidade difícil de ser atendida porque um nodo malicioso pode enviar mensagens diferentes para cada nodo do grupo. Ainda sobre a primeira necessidade, se um nodo é bom, o valor enviado por ele tem de ser transmitido a todos os outros, e estes, por sua vez, devem associar a cada mensagem recebida o identificador do nodo que a enviou.

Existem alguns problemas envolvidos no consenso da confiança usando as questões dos generais bizantinos. Uma delas é que não se pode prever corretamente, sem uma autoridade central de controle um mecanismo que garanta a identidade de um nodo na rede, já

que na perspectiva de sistemas distribuídos, a autoridade central é um ponto de discórdia. Além disso, a troca de mensagens com a solução de Lamport *et al.* [80] é exponencial, tornando a quantidade de mensagens e o tratamento das mesmas um verdadeiro problema de quantidade de mensagens entre todos os nodos na rede. Por fim, também foi mostrado no trabalho de Lamport *et al.* [80], que o consenso é impossível em sistemas assíncronos com falhas arbitrárias, o caso de alguns sistemas distribuídos.

De maneira geral, a aplicação da teoria dos generais bizantinos em sistemas distribuídos grandes pode se tornar um problema de codificação, em função da quantidade de mensagens que devem ser trocadas entre os membros de um grupo. Além disso, o tratamento da confiança necessita de mecanismos de troca de mensagens criptografadas para não se modificar mensagens enviadas. Isto aponta a questão para um problema de criação eficiente de um mecanismo que garanta o sigilo da comunicação dos membros de um ambiente distribuído sem a necessidade de uma autoridade central de controle.

4.4 MODELO DE CONFIANÇA PARA GRUPOS

Tendo em vista os problemas da confiança em grupos, o ponto principal deste tópico é tratar as diversas informações necessárias para se gerar, na medida do possível, um modelo para confiança em grupos e uma representação básica do consenso.

Para fins de elaboração de um modelo, considere que um grupo pode ser definido como uma coleção de entidades reunidas com um objetivo ou afinidades em comum (capazes de realizar atividades), com contextos afins (oferecimento e busca de serviços em comum), e que cada uma tenha um valor de confiança e/ou de reputação umas sobre as outras. Este valor de confiança ou de reputação pode ser adquirido usando qualquer modelo de confiança ou de reputação que levem em consideração alguma interação. A extensão da interação gera a avaliação de confiança e reputação por contexto.

No que se refere ao consenso, o tratamento de pré-requisitos implica diretamente que em um grupo, cujos membros não são capazes de tomar decisões em comum, estes não são capazes de tomar uma decisão que indique um consenso. Assim, considerando os problemas de consenso e de confiança para grupos, a eleição de um líder em um grupo que tenha que levar em conta tais situações, requer um modelo que agregue valor nas discussões e aponte uma proposta de solução para a confiança em grupos e para o consenso da na perspectiva de confiança.

4.4.1 Pré-requisitos de consenso para grupos

Inicialmente, para se alcançar um consenso na liderança, os nodos devem concordar no mínimo, em um limiar de confiança, até mesmo para que sejam capazes de fazer uma análise e escolherem um representante (ou um determinado conjunto de nodos com essa função). De maneira geral, os nodos devem trabalhar com algum tipo de valor de confiança e de serem capazes de calculá-lo e difundi-lo, de tal maneira que se consiga uma comparação de dados de confiança.

No que diz respeito ao consenso, os nodos que possam estar envolvidos no processo de escolha da representação do grupo, devem ser capazes de trocar informações sobre consenso e a definição de um determinado limiar de confiança, atribuído segundo requisitos de segurança. Isto implica que quanto maior o limiar de confiança para o consenso, maior seria a segurança de comunicação porque o nodo não trocaria informações com outros nodos que não estivessem dentro do limiar estabelecido, isolando nodos considerados não confiáveis.

Além disso, esta representação deve levar em consideração alguns fatores básicos, e que seja de preferência encontrado em cada nodo participante, até mesmo porque a formação do grupo também deve seguir alguns critérios ou afinidades para a sua própria criação.

Para a formação de um líder de grupo, o mecanismo de votação não permite que a confiança seja diretamente utilizada porque o único ponto em si é que o nodo deve dar um voto em algum outro nodo. E isto contradiz os aspectos considerando as questões de confiança já abordadas, fazendo com que estes pontos não sejam levados em consideração.

Desta maneira, o melhor tratamento para o processo de eleição de um líder deve ser através de consenso porque cada participante pode expressar sua opinião. Isto faz com que os valores de confiança sejam considerados e a opinião de um nodo não passa a ser restrita a um voto, mas a uma opinião segundo algum critério que auxilie a tomada de decisão da escolha de um líder.

Conforme se percebe nas referências apontadas e já discutidas nos capítulos 2 e 3, a confiança pode representada por um valor V que mensura a expectativa de que um determinado nodo N irá se comportar bem em um contexto C. À medida que se consegue mais interação na rede, mais informações são usadas para o cálculo da confiança. De uma forma geral, a confiança pode ser representada por

$$t = V_c^n \qquad \text{eq. 4-1}$$

onde t é a confiança, V_c^n o valor da confiança de um nodo *N* no contexto *C*.

Normalmente, V varia entre 0 (representando a desconfiança total) e 1 (representando a confiança cega). Apesar de possível, a confiança cega não é desejável porque simplesmente não se pode confiar totalmente em qualquer nodo em qualquer contexto, uma vez que nodos podem mudar de comportamento de acordo com a necessidade, variando muito o grau de expectativa que se pode gerar em um determinado contexto. Este problema já não acontece na desconfiança total porque pode ser considerada como o início de uma situação de confiança, em que não se conhece um determinado nodo.

Assim, a variação da confiança deve ser entre 0 e $1-a$, onde a representa um limiar de confiança que impede um nodo de alcançar a confiança cega, de tal maneira que um nodo sempre deve estar com um grau de "desconfiança" em relação a uma interação. a deve variar conforme a importância ou expectativa de uma interação bem sucedida.

Desta forma, para a avaliação da confiança é importante que os nodos sejam capazes de fazer um julgamento que gera uma "desconfiança", indiferente do conhecimento prévio do nodo sobre o parceiro de interação.

4.4.2 Representação do consenso na liderança em grupos

Para se resolver o problema de candidatos à liderança, vale ressaltar que inicialmente, qualquer nodo pode ser um líder em potencial do grupo. O pré-requisito necessário é que o nodo tenha qualquer valor de reputação no contexto a ser observado para o processo de escolha do líder. Além disso, conforme já citado nas questões de consenso, outras entidades podem anunciar o nodo de sua preferência para ser seu representante de acordo com o contexto.

Considerando esta definição, qualquer modelo que seja capaz de representar valores de confiança e de reputação pode ser utilizado porque o que é importante neste ponto de vista é que os valores de confiança e de reputação sejam expressos dentro de um contexto. Além disso, a troca de valores de confiança e de reputação devem ser computadas e difundidas, de maneira que uma confiança final possa ser alcançada sobre um nodo em todos os contextos em que esteja inserido. Isto gera uma possibilidade de que o nodo com o melhor valor de reputação visto pelos demais, possa ser eleito como o líder.

Outro ponto a ser tratado é que os nodos possam ser capazes de inferir se um valor de confiança é ou não considerado aceitável, gerando um limiar de confiança. Se o nodo ultrapassa um determinado limiar dentro de um conjunto de valores observados, ele é capaz de julgar o nodo sobre um determinado grau de confiança. Esse grau de confiança pode variar de acordo com uma avaliação quantitativa (o nodo confia muito em outro, confia pouco em outro, não tem critérios suficientes para opinar, confia o suficiente para opinar etc.).

Desta forma, se um nodo A deseja saber se o nodo B, em relação ao grupo é ou não confiável, pode comparar seu valor de confiança com o valor de reputação média fornecido por todos os outros nodos do grupo. Esta aproximação é possível porque uma vez que A dispõe de valores de confiança calculados por ele para se chegar a uma idéia de confiança em B, A pode comparar seus resultados com a informação de reputação de outros nodos para saber se B é ou não confiável.

Para que esta situação aconteça, o nodo A e os demais nodos membros do grupo devem trocar informações sobre seus valores de confiança e o contexto analisado. Como referência inicial para um contexto *C*, a Tabela 4-2 ilustra possíveis valores para se chegar a valores de comparação de confiança ou reputação, considerando valores entre 0 e 1.

Tabela 4-2 – Valores de referencia para consenso na confiança.

Valor	Descrição	Decisão
0	Nenhuma confiança/reputação no contexto *C*	Sem opinião
[0, 0.29[	Confiança/reputação baixa no contexto *C*	Não confio
[0.3, 0.59[	Confiança/reputação média no contexto *C*	Não confio
[0.6, 0.89[	Confiança/reputação alta no contexto *C*	Confio
[0.9, 0.99[	Confiança/reputação muito alta no contexto *C*	Confio

A comparação de valores de confiança e reputação com valores de referencia permite um nodo gerar uma opinião comum sobre um determinado nodo, dando uma idéia de consenso da confiança de um nodo sobre outros, dentro de um determinado grupo. No caso da Tabela 4-2, um nodo confia em outro de $t \geq 0.6$.

Além disso, é importante ressaltar que os valores de confiança devem seguir um tratamento que envolva a confiança final de um nodo sobre outro em um contexto, porque dentro de um único contexto podem ser geradas várias iterações, auxiliando no cálculo da confiança. Além disso, um nodo que tenha mais de um contexto deve ser capaz de fazer a confiança final de um nodo sobre outro. Por exemplo, o nodo A possui o contexto *i* e *j*. Um nodo B que tenha os mesmos contextos de A, deve ser capaz de calcular um valor de confiança final para o contexto *i* e para o contexto *j*. Uma vez computados esses valores, a

confiança final do nodo A no ponto de vista do nodo B é computado observando os valores de todos os contextos em questão, neste caso a partir de *i* e *j*.

De posse deste valor de confiança final, os nodos podem opinar na indicação de um líder de acordo com os melhores valores de confiança que possui, ou opinar sobre a concordância de um líder já indicado. Isto é possível através da comparação de valores para um contexto ou para uma tabela de referência que represente o limiar do consenso de confiança, indiferente do contexto.

Para que este mecanismo funcione, cada entidade deve conhecer todos os contextos que o grupo é capaz de trabalhar, formando-se grupos por afinidade. No melhor dos casos, os nodos podem eleger um único nodo como líder e os demais nodos opinarem se concordam ou não segundo seus valores de confiança.

4.4.3 Protocolo de representação do consenso na liderança

Considerando os aspectos da liderança e do consenso para se eleger um líder, as informações de referência sobre o consenso e um método de comparação de valores são pré-requisitos no processo da liderança de um grupo, seguindo definições dentro de um conjunto mínimo de valores de confiança.

Na definição de procedimentos para a escolha de um líder de um grupo, podem ocorrer basicamente duas situações. A primeira é que pode existir um líder para um determinado contexto para um conjunto de nodos. A segunda é que se pode ter um líder geral para o grupo observando os vários contextos em si.

É desejável se ter apenas um único líder no grupo para evitar confusão de representantes e, além disso, evitar confusão nas determinações de valores de confiança do grupo.

4.4.3.1 Protocolo para líder de contexto

Para o caso de um líder de grupo em um contexto *C*, um protocolo prévio pode ser dado através dos seguintes passos:

1. Um nodo no grupo deve realizar a escolha do candidato proposto (CP) indicando o nodo de sua preferência no grupo através do seu maior valor de confiança do contexto C;

2. Enviar essas informações para os demais nodos que conhece no grupo, esperando uma resposta. A mensagem pode ser do tipo - M = {(identidade do CP, confiança no contexto C)};
3. Cada nodo que recebe essa informação deve gerar seu valor de confiança final do contexto C sobre o CP, comparar seus valores de confiança com o limiar de confiança para saber se confia ou não e enviar uma resposta;
4. A resposta deve ser enviada a todos os membros do grupo da forma: a) aceito (valor 1), b) Não tenho opinião formada (neutralidade – valor 2), c) não aceito (valor 3);
5. O formato da mensagem de resposta é do tipo – Resposta assinada R = {[identidade do CP, confiança no contexto C, Valor (1,2 ou 3)]}**;**
6. Se a resposta contiver o valor 3, o nodo pode sugerir o líder de sua preferência para o contexto C baseado em um valor de confiança maior do que o que foi recebido. A mensagem deve ser do tipo M = {(identidade de outro CP), confiança no contexto C)} para o nodo que enviou a solicitação de um líder e para os demais nodos do grupo;
7. Um terceiro nodo recolhe as respostas. Se a quantidade de respostas de aceite for maior do que N/2 + 1, onde N representa o total de membros do grupo, significa que a maior parte dos nodos concorda sobre o líder proposto (CP), chegando-se a um consenso básico através da coleta de opiniões dos nodos. Este nodo então envia uma mensagem do tipo M = {Líder = identidade do CP};
8. Se N/2 + 1 confirmarem esta mensagem, então CP deixa de ser candidato e passa a ser líder L no contexto C (L_c);
9. Se o nodo que enviou uma solicitação de um líder tiver a sua proposta não aceita porque outro nodo tem um valor de confiança maior no contexto C, este deve votar no novo candidato porque um valor de confiança maior de outro nodo significa que o CP já é confiável no contexto por aspectos históricos, observados por outros nodos;
10. Se N/2 + 1 respostas de valor 1 (aceita) não for alcançado, o processo deve ser reiniciado, indicando que não houve consenso, usando o mesmo CP ou outro nodo candidato deve ser escolhido;
11. Se não houver outro CP o processo deve ser abandonado porque não há consenso sobre valores de confiança no grupo;

Desta forma, o CP que tiver a maior quantidade de valores de referência de confiança de acordo com um contexto pode ser considerado o líder dos demais nodos no mesmo contexto. Neste caso, se considera que a maior parte dos nodos concorda que o CP possui valores próximos de confiança em cada nodo membro em função das mensagens (aceita, neutro ou não aceita). Considerando estes passos, é possível gerar um líder para o contexto C, com o mínimo de consenso.

Exemplificando a situação proposta, seja C_{fs} um contexto para compartilhamento de arquivos. O nodo que tiver os melhores valores de confiança no contexto C_{fs}, comparado com valores de referência previamente estabelecidos, observando o consenso do grupo, pode ser considerado o líder para representação do grupo no contexto C_{fs}. Assim todos os nodos, após a troca de informações, saberão que os demais nodos do grupo já possuem uma opinião formada sobre o nodo líder do contexto C_{fs}. É importante ressaltar que este protocolo estabelece o nodo será o líder se e somente se a maior parte do grupo (N/2 +1) esteja de acordo com a eleição do candidato proposto. O líder então pode enviar mensagens para o grupo segundo a proposta de Braskar *et al.* [79].

4.4.3.2 Protocolo para líder geral

Para o caso de um líder de geral do grupo é importante considerar primeiro um processo de consenso nos vários líderes de contexto que possam existir. Um protocolo prévio para liderança geral com consenso pode ser dado através dos seguintes passos:

1. Eleger um facilitador por votação simples;
2. Facilitador deve verificar se existe mais de um líder de contexto;
3. Se existir, recolher a identificação de todos os líderes de contexto;
4. Se existir só um líder de contexto, o facilitador anuncia o único líder de contexto como o líder geral do grupo;
5. Se mais de dois líderes existem, recolher a informação de reputação sobre todos os líderes de contexto;
6. O Facilitador deve comparar todos os valores de reputação dos líderes de contexto;

7. Os dois líderes de contexto com o maior valor de reputação devem ser indicados como o líder geral do grupo e seu substituto (em caso de falha do líder geral);
8. Enviar a mensagem de conformidade da definição de escolha dos líderes para os demais nodos no grupo;
9. Nodos devem comparar as informações sobre a identidade do líder e opinar segundo valores limites de consenso para valores de confiança;
10. Nodos devem responder que receberam a informação da escolha do líder e seu representante e informam a confirmação de concordância com o líder geral. Os que não concordam não devem enviar a mensagem de confirmação;
11. Se N/2 + 1 confirmarem esta mensagem, então o líder e o substituto está confirmado pelo grupo;
12. Se N/2 + 1 respostas não for alcançado, o processo deve ser reiniciado ou abandonado, indicando que não houve escolha do líder;

Desta forma, o líder geral do grupo é aquele que possui o melhor valor de reputação na visão dos membros do grupo.

4.4.4 Representação da confiança

Considerando as várias revisões em sistemas distribuídos, um nodo pode se relacionar diversas vezes com uma ou várias outras entidades para a resolução de um problema. Como a confiança inicial de um nodo sobre outro é calculada em cada interação e em cada contexto específico, a confiança final de um nodo sobre outro em um contexto pode ser dado através de uma média dos valores de cada interação. Vale ressaltar que é importante que se obtenha alguma resposta dentro da interação ou do contexto em si, caso contrário, a confiança começa a sofrer influencias negativas em função das avaliações das expectativas. Assim, a confiança final de cada contexto auxilia na confiança total do nodo. Então, no processo de cálculo de confiança do grupo é importante que todos os nodos conheçam todos os contextos possíveis do grupo.

Vale ressaltar que é comum que um determinando nodo não seja capaz de atuar em um determinado contexto. Esta consideração não impede o nodo de contribuir no processo de cálculo e aquisição da confiança no grupo, e também não o impede de participar na escolha do líder, previamente discutido. Nesta situação, o nodo apenas não poderá opinar no contexto em

si (valor de confiança será 0), mas poderá opinar na confiança final, em função dos contextos que conhece e de que possua alguma referência de interação de confiança.

O cálculo da confiança em grupos pode ser melhor expresso se usar os valores de reputação de seus membros, segundo as definições de confiança e de reputação. Isto porque a confiança do grupo deve levar em consideração a opinião dos membros vistos por seus próprios membros. Isto significa que cada membro avalia os outros membros de maneira individual, em função dos seus conhecimentos na rede e das interações realizadas, e gera seus respectivos valores de confiança e reputação, que por sua vez é repassado para o líder do grupo para que este possa, através do modelo proposto, calcular a confiança do grupo.

Também ocorre que em determinadas situações, um contexto pode ter uma maior importância sobre outro. Por exemplo, a resolução de um problema pode ter um peso maior do que uma interação sobre reputação. Dada esta consideração, o nodo pode atribuir um peso para um contexto, influenciando no cálculo da confiança, se for necessário.

De maneira geral, a confiança de um nodo A em um nodo B em um contexto *c* pode ser representada por

$$t^{c}_{a,b} = V^{b}_{c} \qquad \text{eq. 4-2}$$

onde V^{b}_{c} representa o valor de confiança de B no contexto C visto por A, e $t^{c}_{a,b}$ representa a confiança de A em B no contexto C. Segundo as definições de confiança V^{b}_{c} equivale à expectativa da interação por parte de A em relação a B no contexto C.

Em uma situação normal, os dados das informações de confiança podem ser armazenados através de registros individuais de interação com o nodo em questão, mantendo-se uma coleção de informações distintas sobre cada nodo e o contexto em si. Assim, a confiança final do nodo A sobre o nodo B no contexto C pode ser representada por

$$\bar{t}^{c}_{a,b} = \frac{\sum_{i=1}^{j} V^{b}_{Ci}}{j}, \text{ para j > 0.} \qquad \text{eq. 4-3}$$

onde $\bar{t}^{c}_{a,b}$ representa a confiança final de A em B no contexto C, *j* representa a quantidade de iterações de confiança do nodo A com o nodo B no contexto C.

Como um nodo pode ter diversos contextos, a confiança final de um nodo sobre outro é dado pela soma final dos valores de confiança de todos os contextos, representado por

$$\bar{t}_{a,b} = \frac{\sum_{i=1}^{x} \bar{t}_{a,b}^{i}}{x}, \text{ para x >0.} \qquad \text{eq. 4-4}$$

onde $\bar{t}_{a,b}$ representa a confiança final do nodo A no nodo B, *x* representa a quantidade total de contextos de A com B.

4.4.4.1 Cálculo da confiança no grupo

Considerando que um grupo seja uma coleção de nodos com características de contextos afins e que sejam capazes de calcular tanto os valores de confiança direta e de reputação, a confiança do grupo pode ser expressa através de um mecanismo que considere estes valores. O cálculo da confiança em grupos não pode só usar valores de confiança direta porque estes são dados computados individualmente, sem necessariamente usar a opinião dos nodos uns sobre os outros. Isto faz com que o valor de confiança do grupo seja calculado a partir dos valores de reputação dos membros do grupo, ou seja, a visão dos membros uns sobre os outros.

Desta forma, um valor de confiança do grupo pode ser dado como uma média dos valores de reputação de cada nodo membro do grupo. Isto é viável porque é possível obter os valores de reputação dos membros do grupo com base nas observações individuais de reputação de cada membro. Isto quer dizer que a confiança do grupo é baseada nas avaliações de todos os membros segundo as observações de comportamento de cada nodo.

Uma vez definido o líder de um grupo, este deve recolher os valores de reputação dos membros do grupo. Por exemplo. Considere um grupo com 5 membros N. O líder do grupo pergunta ao nodo membro N_1 sobre a reputação de N_2, N_3, N_4 e N_5. Após essa rodada, o líder pergunta para o nodo membro N_2 sobre a reputação de N_1, N_3, N_4 e N_5. E assim sucessivamente até o ultimo nodo membro do grupo. Além disso, os nodos sabendo quem é o líder, também podem enviar seus valores de reputação sobre os nodos que já conhecerem e que sejam integrantes do grupo, sem necessariamente esperar por uma solicitação do líder.

O líder, por sua vez, de posse de todas as observações de reputação de todos os nodos uns sobre os outros, é capaz de calcular a reputação média de cada nodo do grupo através de

$$\overline{w}_g^n = \frac{\sum_{i=1}^{j} R_i}{j}, \text{ para } j > 0 \qquad \text{eq. 4-5}$$

onde $\overline{w}_g^n$ representa a reputação média do nodo *n* vista pelo grupo *g*, *j* representa a quantidade de nodos integrantes do grupo *g*, e R_i os valores de reputação sobre cada nodo *n* recebido pelo líder.

A reputação R_i é obtida a partir da confiança direta. Isso quer dizer que para um nodo gerar uma opinião, primeiro ele tem que gerar a confiança direta em outro nodo. No caso da implementação proposta, o modelo TRAVOS [3] gera os valores iniciais de confiança, e a reputação R_i é uma observação baseada na confiança direta.

Após realizar o cálculo da reputação média, o líder então é capaz de computar a confiança final do grupo através da soma média de todos os valores de reputação de todos os membros do grupo, dado por

$$\overline{t}_g = \frac{\sum_{i=1}^{x} \overline{w} i_g^n}{x}, \text{ para } x > 0 \qquad \text{eq. 4-6}$$

onde $\overline{t}_g$ é a confiança final do grupo *g*, e *x* representa a quantidade de nodos no grupo.

Após o cálculo da confiança no grupo, o líder pode enviar o valor da representação da confiança do grupo para outras entidades, gerando a representação de confiança do grupo para a entidade na forma de 1:N. O líder ainda pode enviar as informações de confiança para outros líderes de outros grupos gerando a idéia de representação da confiança de M:N.

É importante ressaltar que o viabiliza o cálculo da confiança de grupos são os valores de reputação porque isto representa a visão dos nodos do grupo sobre os demais. O líder, de posse da reputação dos membros segundo as próprias opiniões dos membros, pode gerar um valor de confiança na perspectiva do grupo. Se o líder fizer o cálculo da confiança no grupo usando somente sua visão de confiança nos membros, a confiança no grupo não se torna imparcial, mas apenas a visão do líder sobre os membros. É importante ressaltar que o líder nesta condição não pode ser de maneira nenhuma malicioso, já que ele é o responsável por calcular a confiança do grupo.

4.4.5 Comunicação segura de mensagens no grupo

Como os valores de confiança podem implicar diretamente nas decisões de se interagir ou não com outro nodo, estas mensagens devem ser protegidas. Além disso, aspectos que tratam da troca de informações entre os membros do grupo sem auxílio de uma autoridade certificadora devem ser considerados.

As mensagens de confiança trocadas entre nodos na rede distribuída necessitam de mecanismos eficientes e seguros, até mesmo para que determinados valores de confiança não possam ser amplamente difundidos, sem o mínimo de garantias de que não serão alterados, implicando em tomada de decisões baseada em critérios errados. Isto facilita ações de nodos maliciosos que podem tentar elevar seus valores de confiança com o objetivo de aumentar a quantidade de relacionamentos com outros nodos a fim de desferir algum tipo de ataque ou negação de serviço na rede.

Neste cenário, os trabalhos de Bhaskar *et al.* [79], de Zou [81] e de Cuppens *et al.* [82] propõem mecanismos de troca de mensagens seguras sem o uso de certificação digital centralizada. A premissa é que o grupo já esteja formado, devidamente identificado e que a partir de um determinado ponto, comecem a trocar informações criptografadas.

Além disso, para se evitar problemas de coalizão de nodos, visando a formação de um grupo falso para gerar valores de confiança, e em conseqüência induzir outros nodos ao erro em se comunicar com um grupo falso, é necessário considerações básicas de comunicação. Essas considerações podem inferir que um nodo só deverá se comunicar com um grupo em questão se já tiver realizado pelo menos uma interação positiva com algum membro do grupo em questão, tendo uma opinião de confiança sobre o membro. Se não o tiver, pode ser lançado um desafio, indicado um primeiro contato e auxiliando o nodo a calcular o seu primeiro valor de confiança. Além disso, também deve solicitar algum valor de reputação sobre o nodo em questão a algum membro do grupo ou solicitá-lo na rede.

Bhaskar *et al.* [79] cita que os problemas de segurança em Ad Hoc são mais complexos do que em redes normais e uma das maneiras de tratar estes problemas está no uso de chaves de criptografia simétrica compartilhada com os membros da rede. O principal problema é que estabelecer e manter uma chave de sessão não é uma tarefa trivial em uma rede distribuída. Na tentativa de solução deste problema, fazem um estudo de um protocolo de concordância de chave em grupo GKA (*Group key agreement*) e demonstram detalhes de implementação e de parâmetros que reduzem o trabalho computacional de usar criptografia de chave pública nestas redes.

No contexto do trabalho de Bhaskar *et al.* [79], um protocolo GKA ajuda na derivação de chaves que são compostas da contribuição individual de cada membro em um grupo. Isto garante que a chave resultante é nova para uma determinada sessão e que não é favorável para nenhum participante em nenhuma maneira. Através de um GKA alguns objetivos de segurança podem ser alcançados, resumidos na Tabela 4-3.

Na perspectiva do trabalho de Zou [81], a comunicação segura em grupos é uma área ativa de pesquisa porque uma série de aplicações necessita deste mecanismo. Desta forma, propõem um GKA baseado em uma modificação de um protocolo Tree-based Group Diffie-Hellman (TGDH) para outro, denominado Block-Free Tree-based Group Diffie-Hellman (BF-TGDH). O protocolo proposto possui as características resumidas na Tabela 4-4.

Tabela 4-3 – Objetivos de segurança garantidos por um protocolo GKA.

Objetivo	Descrição
Segredo da chave	A chave só pode se computada somente pelos participantes do grupo
Independência da chave	O conhecimento de qualquer conjunto de chaves não leva ao conhecimento de qualquer outra chave em outro grupo.
Encaminhamento de segredos	Conhecimento de termos longo de segredos não leva ao conhecimento de chaves de grupo passadas.

Tabela 4-4 – Características do *Block-Free Group Tree-based Diffie-Hellman*.

Característica	Descrição
1	Sem bloqueamento durante o processo de recriação da chave e transição da comunicação do grupo sem interrupção.
2	Possui resistência a ataques Man-in-the-middle.
3	Autenticação das mensagens enviadas usando o protocolo de assinatura ElGamal.

Segundo as análises de Zou [81], um sistema de comunicação seguro em grupos deve permitir que os participantes troquem informações entre si de maneira segura, e que entidades que interceptem essas mensagens não sejam capazes de decodificá-las. A base do protocolo proposto por Zou [81] deriva do TGDH que é fundamentado no problema de logaritmos discretos e no princípio de troca de chaves do mecanismo Diffie-Hellman. A idéia básica do BF-TGDH reside no fato de utilizar dois tipos de chaves. A primeira é denominada *front-end key* e a segunda *back-end key*. A *front-end key* pode ser computada por todos os membros do grupo, enquanto que a *back-end key* indica uma chave que o nodo não pode computar. Se um nodo abandona o grupo, os nodos remanescentes passam para a chave de *back-end key* imediatamente, que é computada segundo o funcionamento do TGDH, alterando a chave de sessão.

No trabalho de Cuppens *et al.* [82], é apresentado e analisado um protocolo para gerenciamento de grupos em redes ad hoc grandes e dinâmicas. O protocolo proposto, também baseado no TGDH, é denominado S-TGDH e ajuda no cálculo rápido e eficiente da

chave de grupo em cada nodo de maneira uniforme. A proposta do trabalho de Cuppens *et al.* [82], visa melhorar as questões de processamento das informações de criptografia no grupo por parte dos membros e do compartilhamento do segredo De maneira distribuída sem uma autoridade central. Além disso, remontam que a árvore global criptográfica proposta no TGDH é otimizada. Segundo os autores, o algoritmo proposto provê várias características de segurança bem-conhecidas, tais como autenticação de nodos, resistente a ataques passivos e a ataques conhecidos de chaves, além de outras características.

De maneira geral, um processo de comunicação de mensagens em um grupo pode fazer uso de protocolos como o TGDH e as suas variações para a proteção das informações sobre confiança e reputação. A questão em si remonta nos aspectos de troca de mensagens para o estabelecimento da chave de grupo e a formação dos próprios grupos. Em uma breve análise, as questões de saída dos nodos não são amplamente discutidas nos trabalhos de Bhaskar *et al.* [79], de Zou [81] e de Cuppens *et al.* [82]. Já as questões de entrada dos nodos e o seu comportamento relacionado à distribuição e o processamento das chaves são discutidos e algumas soluções são propostas por todos os trabalhos.

4.5 SÍNTESE DO CAPÍTULO

O principal objetivo deste capítulo foi de propor um modelo capaz de gerar valores de confiança para um grupo. Para tanto, alguns conceitos de liderança, consenso e grupos foram discutidos e colocados através de representações específicas.

Considerando as revisões, analisando e observando o comportamento de modelos de confiança e de reputação, foi possível fazer a elaboração de um mecanismo capaz de calcular a confiança no grupo, segundo os valores de interação de reputação de seus membros. Além disso, as premissas de comunicação segura foram discutidas, citando possíveis soluções para uma comunicação segura em um ambiente distribuído sem uma autoridade central de controle.

De uma forma geral, é possível calcular a confiança de um grupo através de escolhas de líderes de contexto e da escolha de um líder geral. Após esta escolha, o líder, de posse da reputação dos membros do grupo, é capaz de fazer o cálculo médio da confiança no grupo baseado nas informações recebidas.

É importante ressaltar que é necessário considerar os problemas de gerenciamento de identidades em redes distribuídas, evitando situações como o ataque Sybil [12] e diversos outros ataques comuns em redes.

5 CARACTERÍSTICAS DAS IMPLEMENTAÇÕES

Este capítulo trata dos resultados obtidos segundo a elaboração e tratamento dos conceitos nos capítulos anteriores e da análise experimental dos mesmos, demonstrando a viabilidade do conceito proposto para um modelo de confiança para grupos.

A maior parte dos resultados foi coletada usando ferramentas próprias, através de saídas de comandos implementados ou analisados através de comparação de dados. A sua representação, de maneira a simplificar a demonstração dos mesmos, será feita através de tabelas e gráficos e a sua correspondente análise.

A linha de implementação trabalhou basicamente com dois conceitos estudados no decorrer deste trabalho. Primeiramente foi demonstrada a implementação de um modelo de confiança em sistemas distribuídos, utilizando como tecnologia um sistema de agentes de software. Em segundo foi demonstrado o modelo de confiança proposto em redes P2P.

5.1 FERRAMENTAS UTILIZADAS

Para os testes envolvendo um protocolo para identificação foram utilizados algoritmos escritos em linguagem C e C++ em Linux. Já para os sistemas de agentes de software, foi usada as especificações da FIPA (Foundation for Intelligent Physical Agents) [49] e sua implementação através do Jade [54]. Para a demonstração prática para P2P foi utilizado o framework JXTA [40] e um ferramenta que a implementa, denominado JXTA Shell, obtido através do framework do próprio JXTA [40].

5.1.1 FIPA

A FIPA [49], formada inicialmente em 1996 para produzir padrões e especificações para sistemas de agentes heterogêneos, foi incorporada ao IEEE [83] em 2005, agregando valores na elaboração de especificações para uso de agentes de software.

Segundo a própria FIPA, sua principal missão é “a promoção de tecnologias e especificações de interoperabilidade que facilitam o trabalho mútuo fim-a-fim de sistemas de agentes inteligentes em definições comerciais e industriais”. Sendo que seu foco é em agentes inteligentes ou agentes cognitivos (em agentes que possuem um potencial de conhecimento e reações sobre si mesmos e sistemas que eles venham a encontrar).

O núcleo de mensagens da FIPA é baseado na combinação de atos de discurso [84], lógica de predicado e ontologias públicas, de tal maneira que possibilita a oferta de alguns tipos de padrões de interpretação entre agentes. Isto permite que os agentes respeitem o significado pretendido da comunicação, facilitando o processo de tomada de decisão. Esta tecnologia permite primeiramente que sejam adotadas especificações que abrangem arquiteturas de comunicação de agentes entre si. Além disso, permite o tratamento de linguagens de comunicação e conteúdo da linguagem (para expressar as mensagens) e por fim, no uso de protocolos de interação que vão do escopo de mensagens simples até transações completas.

As especificações elaboradas pelos grupos membros da FIPA representaram os primeiros passos em direção da padronização de agentes [46]. É importante ressaltar que as especificações não têm a pretensão de recomendar arquiteturas internas de um agente e nem como deve ser implementado, mas determinam as interfaces necessárias capazes de suportar a interoperabilidade entre sistemas baseados em agentes. São divididas em cinco grandes grupos, conforme a Tabela 5-1.

Tabela 5-1 – Divisão das especificações FIPA.

Grupo	Descrição
Aplicação	Relacionada a exemplos de áreas de aplicações na qual agentes baseados na arquitetura FIPA podem ser desenvolvidos. Representam ontologia e especificações de descrição de serviço para um domínio em particular.
Arquitetura Abstrata	Define, em um nível abstrato, como dois agentes podem se localizar e comunicar se registrando em serviços de diretórios (páginas amarelas) e trocar mensagens.
Comunicação de agentes	Agentes se comunicam entre si através do envio de mensagens. São regidos por três aspectos fundamentais. O primeiro aspecto é a estrutura da mensagem (tupla de valores-chave). O segundo aspecto está relacionado à representação da mensagem e o terceiro, vislumbra o transporte da mensagem.
Gerencia de agentes	Trabalham com o controle e a gerência de agentes em uma mesma plataforma ou em plataformas diferentes. A gerência de agentes preocupa-se com a gerência dos serviços dos agentes e para os agentes, além da gerência da ontologia e da gerência do transporte da mensagem.
Transporte de mensagem de agentes	Engloba três níveis. O primeiro está relacionado ao protocolo de mensagem de transporte que é utilizado para carregar uma mensagem entre dois canais de comunicação de agentes. O segundo trata do serviço de transporte de mensagem (serviço provido por uma plataforma de agente na qual um agente está ligado e suporta o transporte de mensagens FIPA ACL entre agentes em uma mesma plataforma ou em plataformas diferentes). O terceiro nível trata da representação do conteúdo (payload) das mensagens transportadas tanto pelo serviço de transporte de mensagem quanto pelo protocolo de mensagem de transporte.

Em resumo, o foco primário da especificação da arquitetura FIPA é a criação de um mecanismo que permita a troca de mensagens entre agentes com um significado semântico, indiferente de qual protocolo de mensagens, de qual ACL ou de qual linguagem de conteúdo um agente usa. Para que tal objetivo seja alcançado, são necessários vários pontos de interoperabilidade em potencial, que segundo a FIPA inclui: a) um modelo de serviço e descoberta de serviços disponível para agentes e outros serviços; b) interoperabilidade no transporte das mensagens; c) representação de várias formas de ACLs; d) representação de várias formas de conteúdo de linguagens; e) suporte a representação de serviços de diretórios múltiplos; f) de certa forma deve ser possível criar implementações que possam variar em alguns destes tópicos, entretanto, de tal maneira que ainda possam interoperar.

Para uma arquitetura ser compatível com a especificação FIPA é necessário que se tenha algumas propriedades, entre elas, incluir mecanismos para o registro e descoberta de agentes (formação de grupos ou comunidades), além de transferência de mensagens inter-agentes (troca de valores). Tais serviços devem estar explicitamente descritos em termos dos elementos correspondentes na arquitetura FIPA.

5.1.1.1 Jade

Java Agent Develpment Framework [54] ou simplesmente JADE é um ambiente baseado em aplicações voltadas para agentes, compatível com o padrão proposto pela FIPA. O framework JADE simplifica o processo para interação de agentes em sistemas distribuídos, troca de mensagens, formação de grupos, processos de comunicação, entre outros. Uma das vantagens de utilização do JADE no contexto deste trabalho é que se simplifica o desenvolvimento de agentes e ainda se garante um padrão através de um conjunto de serviços e de agentes.

Em uma avaliação mais ampla, o JADE pode ser considerado com um middleware que implementa uma plataforma de agentes e um ambiente de desenvolvimento, podendo ser utilizado diversas interfaces gráficas para o desenvolvimento. O JADE lida com aspectos relacionados à implementação da parte interna de agentes (suas características, inferências, inteligência etc.) e a parte externa (transporte de mensagens, codificação, ciclo de vida etc.). A FIPA ACL é a linguagem de comunicação utilizada pelo JADE.

Relacionado a pontos específicos de desenvolvimento, o framework implementa e disponibiliza um vasto conjunto de ferramentas que auxiliam e simplificam o desenvolvimento de sistemas baseados em agentes. Tais ferramentas podem ser locais ou

distribuídas, de acordo com a necessidade do ambiente e controladas através de uma interface gráfica.

Em relação à arquitetura de comunicação, o JADE oferece um esquema flexível e eficiente de controle de mensagens. Este esquema envolve a criação e o gerenciamento de filas de mensagens ACL privadas para cada agente, e estes por sua vez, podem acessá-las de várias formas: por timeout, bloqueio, votação etc. Como mecanismo de transporte, diversos protocolos podem ser utilizado, por exemplo, o SMTP, o HTTP, o RMI, entre outros.

No ponto de vista de programação, JADE oferece uma série de características que torna o processo de desenvolvimento mais simples e eficiente em termos práticos de utilização e tempo. Estas características estão simplificadas na Tabela 5-2.

Tabela 5-2 – Características de desenvolvimento do Jade.

#	Característica	Descrição
1	Plataforma de acordo com o padrão FIPA	Inclui um sistema de gerencia de agentes, um facilitador de diretório e um canal de comunicação de agentes. Todos habilitados automaticamente na própria plataforma quando se inicia.
2	Plataforma de agentes distribuída	A plataforma permite a criação de agentes distribuídos em uma rede de comunicação, fazendo uso de várias estações e tarefas paralelas podem ser agendadas.
3	Serviço de diretório	Facilidade de uso de serviços de diretório de acordo com o Padrão FIPA
4	Interfaces de auxílio	Interface gráfica para simplificar o registro de serviço de agentes em um ou mais domínios (facilitadores de diretório).
5	Transporte	Mecanismo de transporte e interface para receber e enviar mensagens.
6	Protocolos	Implementação do padrão FIPA para protocolo de transporte de mensagem para diferentes plataformas.
7	Mensagens ACL	Transporte de mensagens ACL leve dentro da plataforma de agentes, o que permite que as mensagens sejam transferidas como objetos e que sejam modificadas para o padrão FIPA quando em plataformas diferentes.
8	Reutilização	Biblioteca de protocolos de interação FIPA
9	Serviço de registro	Registro automático de agentes no serviço de gerência de agentes.
10	Serviço de identificação	Serviço de nomes compatível com o padrão FIPA através de um número único e global para cada agente
11	Controle de ciclo de vida	Interface gráfica para gerência remota do ciclo de vida de agentes e dos repositórios de agentes.
12	Debug	Interface de debug para auxilio ao desenvolvimento de sistemas multi-agentes.
13	Mobilidade	Adoção de características de agentes móveis, permitido a criação de agentes móveis.

De maneira mais abrangente a arquitetura JADE distribuída, pode ser definida através de um ambiente composto por aplicações de agentes que interagem entre si fazendo uso de

uma plataforma de agentes. Para esta interação é necessário um mecanismo de rede e um ambiente mínimo de execução.

5.1.2 JXTA

O JXTA [40] é um framework considerado como um dos mais maduros e completos porque é formado por um conjunto de protocolos P2P simples e de código aberto. Foi desenvolvido com o intuito de possibilitar a comunicação, colaboração e o compartilhamento de recursos de qualquer tipo de equipamento conectado a uma rede. Sua abrangência de uso envolve desde telefones celulares, PDAs e computadores pessoais, até servidores de rede.

Uma rede composta pelo framework JXTA [40] consiste em um grupo de nodos que desenvolvem papéis específicos na rede, porém qualquer nodo pode, em teoria, desenvolver qualquer um dos papéis. Os possíveis papéis que um nodo pode assumir são resumidos na Tabela 5-3.

Tabela 5-3 – Papéis de um nodo com framework JXTA

Papel	Descrição
Edge Peers	Peers simples, podendo ser qualquer dispositivo conectado a rede. Dividido em: Minimal Peers (dispositivos de capacidade limitada, como celulares e PDAs) e Proxy Peers (dispositivos de maior capacidade que funcionam como servidor Proxy para peers que se encontram atrás de firewalls e para Minimal Peers porque estes nodos não possuem IP público ou que mesmo possuindo IP, não têm capacidade de processamento suficiente).
Rendezvous Peers	Peers com maior poder computacional que funcionam como cache guardando informações sobre os peers que estão conectados à rede, tornando o procedimento de descoberta de peers mais rápido.
Relay Peers	Peers que adquirem informações sobre o roteamento. Geralmente essa função é desempenhada por um peer que também é Rendezvous Peer

O JXTA [40] cria uma rede virtual Ad-Hoc sobre as redes existentes, deixando de lado a complexidade existente em cada rede (tipo de equipamento, capacidade de processamento, ambiente de operação etc.) tornando possível a conexão de qualquer nodo da rede, mesmo o nodo estando atrás de um firewall ou de um NAT.

Todas as entidades de uma rede JXTA [40] possuem um ID universal único e são representadas por um documento XML que, além desse ID, contém outras informações da entidade (chamado de *advertisement*). Através da publicação do *advertisement* (envio de dados a outros peers) é que um peer disponibiliza seus serviços ou dados na rede. Assim, cada

peer armazena localmente os *advertisements* de outros peers e o utiliza para estabelecer uma conexão e realizar a transação que desejar com o peer de seu interesse.

Os *advertisements* possuem um prazo de validade a fim de evitar a descrição de entidades que não estão mais conectadas à rede. São definidos seis tipos de *advertisements*:

1. Peer;
2. Peergroup;
3. Pipe – canal virtual de comunicação ponto-a-ponto ou propagate pipe (conexão de 1 para n);
4. Service - serviço oferecido por um Peer ou Peergroup;
5. Content - conteúdo publicado;
6. Endpoint – pontos de conexão de um pipe;

Nas redes JXTA [40] são utilizados seis protocolos básicos para a execução das funções necessárias a uma rede P2P, como por exemplo, a pesquisa por peers, o roteamento, publicação de *advertisement*, entre outras. Esses protocolos são independentes uns dos outros e uma aplicação rodando sobre o JXTA não precisa, necessariamente, utilizar todos os protocolos. A Tabela 5-4 resume os protocolos do JXTA e suas funções.

Tabela 5-4 – Protocolos do JXTA e sua função

Protocolo	Função
Peer Discovery Protocol (PDP)	Protocolo utilizado pelos peers para descobrir recursos na rede por meio dos *advertisements* publicados. Esse protocolo se baseia no envio de uma mensagem multicast na rede local e o envio de requisições aos Rendezvous peers, para a pesquisa em outras redes que não a local.
Peer Resolver Protocol (PRP) –	Envia mensagens de consulta a outros peers e serve de infra-estrutura para outros protocolos como o Peer Information e o Peer Discovery.
Peer Information Protocol (PIP)	Faz a coleta de informações sobre um peer. É útil para monitoramento da rede checando se um determinado peer está on-line e também podendo solicitar o seu *advertisement*.
Rendezvous Protocol (RVP)	Responsável por propagar as mensagens na rede bem como controlar essa propagação e permitir a conexão a serviços disponíveis. Esse protocolo é utilizado como base nos protocolos Peer Resolver e Pipe Binding.
Pipe Binding Protocol (PBP)	É responsável pela conexão de um pipe a seus dois endpoints. Por meio do protocolo Rendezvous envia mensagens para encontrar um endpoint para conectar a um pipe já com um endpoint estabelecido.
Endpoint Routing Protocol (ERP)	Envia mensagens para encontrar informações de roteamento, para troca de mensagens entre dois peers. As rotas encontradas são armazenadas localmente, e incluem informações sobre o Peer remetente, o Peer destinatário e a seqüência ordenada de peers na rota.

Em resumo, o JXTA [40] é uma plataforma contendo várias funcionalidades necessárias à implementação de uma aplicação P2P. No tratamento de questões de segurança criptográfica para troca de mensagens, que possam até envolver a confiança, o framework deixa em aberto a escolha do modelo criptográfico como responsabilidade do usuário.

5.1.2.1 JXTA Shell

O JXTA Shell é uma aplicação construída sobre o framework JXTA [40] e que funciona como uma ferramenta de demonstração da tecnologia, além de possuir um ambiente de desenvolvimento relativamente flexível. O Shell da ferramenta permite que os usuários possam utilizar todas as funcionalidades disponíveis dos protocolos JXTA, implementadas em linguagem Java. Sua utilização é semelhante ao Shell de sistemas Unix, que através de uma linha de comando permite que os usuários possam executar operações P2P. Estes comandos envolvem a manipulação de peers, peer groups e pipes, através de uma sintaxe de execução relativamente simples.

Para se instalar o JXTA Shell (utilizado a versão 2.4.1) primeiramente deve se verificar e certificar de que existe uma Máquina Virtual Java (JRE) versão 1.3 ou superior instalada no sistema. Os arquivos necessários para a instalação podem ser adquiridos através do site do projeto JXTA [40]. Basta fazer o download do arquivo jxta-shell-x.x.x.zip (onde x.x.x indica a versão) e extraí-lo em uma pasta qualquer do sistema.

Relacionado ao conteúdo do pacote do JXTA Shell, existe basicamente os diretórios lib e o Shell. O diretório lib contém as bibliotecas (arquivos JAR) da plataforma JXTA. Já o diretório shell contém o arquivo executável necessário para iniciar a aplicação. Quando executado pela primeira vez, o shell passa a conter um cache com informações de configuração relativas àquele peer. Para executar o JXTA Shell em plataforma Windows, basta clicar no arquivo executável jxta.exe localizado no subdiretório shell. Na primeira execução, é apresentada ao usuário uma tela requisitando informações de configuração. Neste ponto é que algumas informações importantes sobre os nodos P2P são definidas.

Após a configuração de um nodo P2P, a plataforma carrega o JXTA Shell automaticamente, onde é apresentada ao usuário uma tela requisitando as informações de autenticação do nodo, que por sua vez são definidas em um módulo da plataforma denominado Configurator. Por fim, a console do Shell é oferecida ao usuário assim que a autenticação for bem sucedida.

5.2 DESCRIÇÃO DOS AMBIENTES DE TESTES

Para demonstrar os objetivos propostos pelo trabalho, foi necessário definir ambientes capazes de mensurar dados, na expectativa de atingir resultados de acordo com os parâmetros e critérios de informações de confiança. Além disso, os ambientes servem como base para discussões futuras, bem como a evolução da proposta através de novos sistemas distribuídos.

Através da implementação de tais ambientes é possível discutir e evoluir os parâmetros necessários para a confiança em grupo, da análise da geração de situações de confiança onde deve ser necessário um líder, seguindo considerações de contexto, e por fim gerar dados que sirvam para a discussão do problema da confiança para grupos.

No tratamento do problema da confiança em grupos, um pré-requisito fundamental é a identidade dos nodos. Até mesmo porque não se pode criar um ambiente de grupos de agentes de software ou P2P sem antes tratar das identidades dos membros que irão compor o grupo. Esta questão é tratada porque se for possível falsificar uma identidade, será possível fazer a coalizão de nodos e assim gerar problemas voltados para a segurança do ambiente, envolvendo a disponibilidade e integridade dos dados trafegados. Além disso, através de uma coalizão é possível realizar ataques dos tipos previstos pelos formalismos assumidos nas definições do ataque Sybil [12]. Neste ponto em específico é considerada a identidade oferecida pelos próprios ambientes de implementação utilizados.

A confiança pode entrar no cenário de identificação de nodos para automatizar e dar inteligência à rede para que seus membros sejam capazes de resolver seus próprios problemas de relacionamento. Em uma perspectiva de implementação, a confiança pode ser colocada na camada de aplicação das redes distribuídas, dando margem de sua utilização através de módulos específicos de confiança e de reputação, módulos de distribuição da confiança, módulos de aquisição da confiança, entre outros. Isto permite que a aquisição e tratamento de informação de confiança (que é um processo individual) não dependam necessariamente de módulos externos, tais como certificados digitais. Os certificados devem e podem até ser utilizados, mas não como garantia de identificação e muito menos de confiança, mas como garantia de troca de informações assinadas, agregando mais segurança a uma determinada arquitetura.

Como os resultados estão divididos em vários ambientes de testes, e cada um composto por uma arquitetura própria de comunicação em rede local, não é possível fazer uma definição global de uma ambiente de testes para cada arquitetura de implementação. Assim, as descrições dos ambientes são feitas para cada uma das arquiteturas de simulação, utilizando os devidos controles e considerações.

5.2.1 Considerações sobre o ambiente de agentes de software

A parte prática desta etapa do trabalho consistiu em desenvolver agentes de software que tanto possuíssem funcionalidade simulando nodos em um Grid computacional, que fizessem uso de valores de confiança computacional para decidir quanto às suas interações.

O ambiente proposto foi desenvolvido na plataforma JADE e, em seguida, os agentes desenvolvidos foram instanciados para uso. Uma vez que o objetivo foi estudar aspectos de confiança, foi suficiente executar todos os agentes em um mesmo computador, até mesmo porque não foi tratado aspectos de performance.

Os testes foram realizados em um PC Intel Core 2 Duo de 1,66 GHz e 2 GB de memória RAM. O sistema operacional utilizado foi o Windows Vista Home Premium. Maiores detalhes podem ser vistos no Apêndice A deste documento.

Foi implementado o modelo de confiança e reputação TRAVOS [3] para o cálculo da confiança e reputação na perspectiva de 1:1.

Nesta implementação, não foram tratadas questões referentes às identidades dos agentes porque um mecanismo do JADE [54] atribui uma identificação única para cada agente. Dessa forma, o problema da personalização de agentes (agentes que assumem a identidade de outro agente) não fez parte do escopo desta implementação.

Com o intuito de facilitar a explicação são considerados os seguintes pontos:

- A1 é um agente grid que possui uma tarefa, a divide e distribui entre os agentes confiáveis da rede.
- A2 é um agente que recebe uma parte da tarefa para ser executada;
- A3 é um agente que responde para A1 sobre seu passado de interações com A2.

5.2.1.1 Desafio

Quando um agente A1 deseja delegar uma sub-tarefa e não possui informação sobre um determinado agente A2 em sua tabela de interações diretas baseadas em confiança, ele envia um desafio a A2. Com esse recurso, A1 evita ter que confiar em um agente com base exclusivamente nas opiniões fornecidas sobre ele e passa a ter pelo menos uma interação direta para compor o cálculo da confiança combinada (confiança direta mais reputação).

Cabe ressaltar que a falha de A2 ao responder o desafio, não significa que ele não realizará sub-tarefas para A1, até mesmo porque A2 pode ter interagido com outros agentes que fornecerão uma boa reputação sobre ele. Mesmo no caso inicial do sistema, em que

ninguém possui informações sobre ninguém, A2 pode responder positivamente ao desafio de outro agente que repassará uma boa reputação dele para os demais nodos da rede.

O desafio consiste em enviar ao agente desafiado uma matriz e esperar que ele responda com o determinante dessa matriz. Nessa resposta, o agente avaliado também informará qual é o seu processador. O primeiro critério de avaliação do desafio é avaliar se o valor respondido está correto. Para tal, o próprio agente desafiador calcula o determinante da matriz enviada por ele próprio. Uma vez que o valor é correto, o critério seguinte é o tempo de resposta ao desafio. Ele é importante, pois permite identificar se o agente candidato a realizar a tarefa não tem capacidade de processamento suficiente para realizá-la, está ocupado realizando outra tarefa ou até mesmo atrasando a entrega do resultado propositadamente. O agente avaliador consultará uma tabela interna do tipo *<Processador, Tempos de resposta>*, que contém, para cada processador mencionado por algum agente desafiado, um histórico dos últimos 10 tempos de resposta obtidos. Com base nesse histórico, o tempo de resposta do agente desafiado é classificado como aceitável ou não. Se, para um determinado processador, todos os últimos 10 tempos de resposta não estejam preenchidos, se considera que não há dados suficientes para calcular o limiar e se utiliza um limiar pré-determinado.

Esse desafio será considerado uma interação bem sucedida se o valor estiver correto e o tempo de resposta for inferior a um limiar pré-determinado, caso não haja informações sobre o processador. Caso contrário, será utilizado à média somada ao desvio padrão do histórico de tempos de resposta para o processador informado. O resultado do desafio já será armazenado como uma primeira interação pessoal e será usado para o cálculo da confiança.

5.2.1.2 Confiança direta

A cada sub-tarefa realizada por A2 a pedido de A1, este armazena localmente a sua avaliação a respeito dessa interação (contexto). Para facilitar a análise, definimos que a tarefa será um processamento que retornará um valor gastando um determinado tempo. Isso nos possibilita utilizar o tempo de resposta como critério de desempenho. Com base no tempo que um agente gastou para processar a sub-tarefa, a interação é classificada como bem ou mal sucedida. Cada agente guarda esses resultados na forma *<Agente que realizou a tarefa, Quantidade de boas interações, Quantidade de más interações>*.

O método que calcula a confiança direta retorna um valor booleano que indica, com base na fórmula de confidência do modelo TRAVOS [3] se a experiência pessoal do agente é suficiente ou se será necessário buscar por opiniões.

5.2.1.3 Confiança combinada

Utilizando o cálculo da confidência é possível determinar se a quantidade de interações diretas com A2 é suficiente. Caso não seja, A1 perguntará a todos os agentes da rede o resultado de suas interações com A2 para o contexto em questão. Ao receber um pedido de opinião, os agentes questionados informarão a quantidade de boas e más interações que tiveram com A2. Dessa forma, A1 poderá usar esses valores no modelo de confiança que julgar mais adequado, permitindo que cada agente decida como irá calcular seu valor de confiança e adicionando flexibilidade ao Grid.

Considerando que um agente A3 enviou sua opinião a A1, se A1, em outras ocasiões, tiver recolhido a opinião de A3 (histórico de opiniões fornecidas por A3), A1 irá calcular a exatidão da opinião recém obtida com base nesse histórico, que é pessoal de cada agente e obedece à forma *<Agente que forneceu opinião, Opinião fornecida, Avaliação da interação referente à opinião fornecida>*. Nesse momento, todas as opiniões fornecidas são armazenadas nos campos <*Agente que forneceu opinião*> e <*Opinião fornecida*> para posterior conferência.

Após o recebimento de todas as opiniões requisitadas, estas, juntamente com as interações pessoais, serão usadas para calcular a confiança combinada do TRAVOS [3]. Se um agente informa que não teve nenhuma interação, sua opinião é desconsiderada no cálculo da confiança combinada.

5.2.1.4 Tarefa realizada

Quando A1 deseja delegar partes de uma tarefa, ele primeiro pesquisa quais agentes são provedores para essa tarefa. Em seguida, calcula a confiança combinada para cada agente. Apenas os agentes que possuírem um valor de confiança superior a um determinado limiar receberão a tarefa.

As tarefas simuladas no grid são o processamento das operações de multiplicação e soma de matrizes de números inteiros. A distribuição de sub-tarefas consiste em dividir um arranjo de matrizes quadradas de ordem 10 em grupos de 3 e enviar para os nodos confiáveis realizarem a operação solicitada. A quantidade máxima de matrizes no arranjo é 25, pois acima desse valor ocorre uma perda de precisão no resultado.

Para cada operação, são definidos limiares de confiança diferentes. Consideramos que a multiplicação é uma tarefa mais crítica e, por isso, requer um valor de confiança mais

elevado (por exemplo, 0.8). Da mesma forma, definimos um limiar para que a tarefa de soma de matrizes seja delegada a um agente (por exemplo, 0.6).

Após receber o resultado de todos os agentes aos quais delegou sub-tarefas, A1 avalia se o resultado foi satisfatório ou não e armazena essa avaliação em dois locais. O primeiro é sua tabela de interações diretas <*Agente que realizou a tarefa, Quantidade de boas interações, Quantidade de más interações*> e incrementa o campo "*Quantidade de boas interações*" ou "*Quantidade de más interações*", dependendo do resultado. O segundo local é a sua tabela de histórico de opiniões fornecidas <*Agente que forneceu opinião, Opinião fornecida, Avaliação da interação referente à opinião fornecida*>. Essa tabela já possui os campos "*Agente que forneceu opinião*" e "*Opinião fornecida*" preenchidos.

5.2.1.5 Nodos desonestos

Um agente desonesto possui as mesmas funcionalidades que um honesto, porém fornece uma opinião errada sobre outros agentes com o intuito de obter uma maior quantidade de tarefas, visto que estamos simulando um ambiente em que os nodos provedores de um serviço podem cobrar por cada serviço realizado. Assim, quanto mais tarefas um nodo executar, maior será sua receita. Dessa forma, quando a opinião do agente desonesto é solicitada, ele sempre envia como resposta um valor de confiança muito baixo, fazendo com que o agente que solicitou a opinião diminua seu valor de confiança no agente analisado no momento. Ao longo do tempo, se o agente desonesto sempre fornece opiniões negativas sobre outros agentes, porém estes oferecem opiniões positivas sobre aquele, a reputação do agente desonesto será comparativamente maior que a dos agentes honestos, o que diminui a requisição de serviços a esses agentes enquanto aumenta a do nodo desonesto.

5.2.2 Considerações sobre o ambiente para nodos P2P

Voltado para o ambiente P2P, as simulações foram executadas em dois computadores com sistema operacional Windows XP e o JXTA Shell instalado e operacional. Basicamente, cinco *peers* foram instanciados em cada estação. A comunicação das duas máquinas foi feita através de um *switch* camada dois, com portas de velocidade 10/100 kbps. O objetivo desta topologia foi representar o melhor possível a realidade de uma rede, de modo que os tempos de transferência definidos pudessem considerar eventuais atrasos de transmissão. Além disso, todos os peers foram inicializados em uma mesma rede IP, de modo que eles pudessem se comunicar diretamente (sem saltos). Foi utilizado o modelo de confiança e reputação

TRAVOS [3] para o cálculo da confiança e reputação na perspectiva de 1:1. É importante ressaltar que não é considerada a quantidade de mensagens trocadas entre os nodos para avaliação da confiança na rede. Considera-se que uma mensagem enviada chegará ao destino.

5.2.2.1 Nodos maliciosos

O comportamento dos nodos é dado como malicioso se não executam uma tarefa segundo um intervalo de tempo dado ou o arquivo enviado via P2P está corrompido. O cálculo realizado utiliza o parâmetro do tempo de transferência e estabelece uma variável para receber os valores para cada situação. Se o arquivo chegar em até 1s, será considerado dentro do prazo de entrega, se o tempo variar de 1s a 2s significa que o arquivo chegou um pouco atrasado, pois não comprometeu totalmente a confiabilidade do processo; se o tempo de chegada for maior que 2s, o arquivo chegou muito atrasado, e se considera que o peer de origem realizou uma operação maliciosa na rede.

O outro parâmetro utilizado é a integridade do arquivo recebido. Quando o hash é calculado e o arquivo encontra-se íntegro o nodo é classificado como confiável; caso contrário, considera-se que o peer de origem realizou uma operação maliciosa.

5.2.2.2 Comandos desenvolvidos para o JXTA

Novos comandos foram desenvolvidos para o Framework do JXTA Shell para a realização das simulações de calculo da confiança, da reputação e da sua perspectiva na visão de grupos. Detalhes sobre hierarquia, sintaxe e organização destes comandos podem ser visualizados no Apêndice B.

a) trust –init

Comando que realiza a inicialização automatizada e individual de cada peer na rede P2P. Para que o peer realize qualquer operação ou interação na rede é preciso que este comando seja executado, preparando o peer para as futuras comunicações.

b) trust –test

Comando que realiza a transferência de um arquivo para um peer de destino usando o protocolo SFTP. O mesmo comando é responsável por preparar o peer de destino para receber o arquivo e calcular seu hash através do algoritmo MD5 para verificar automaticamente a integridade do arquivo recebido.

c) trust –interaction

Comando que automatiza os testes de confiança na rede. Para cada vez que o comando é acionado, é feita uma interação seqüencial entre todos os peers na rede através do comando trust –test.

d) trust –directtrust

Comando que calcula o coeficiente de confiança direta entre dois peers na rede. Para isso, abre o arquivo "peerTableMN.txt" presente na pasta Tables e retira os coeficientes de confiança M e N para o peer em questão. Este cálculo é baseado somente no histórico das interações entre os dois peers.

e) trust –reputation

Comando que calcula a reputação de um peer específico na rede. Cada vez que o comando é acionado, várias requisições são enviadas por um peer de origem para todos os outros peers na rede, com exceção do peer do qual a reputação foi requisitada.

f) trust –answer

Comando que responde as requisições de reputação dos peers, executado logo após o "trust –reputation" em cada peer que tiver recebido a requisição.

g) trust –combinedtrust

Comando que calcula o coeficiente de confiança combinada entre dois peers na rede, utilizado para calcular o grau de confiança de um peer em outro.

h) trust –grouptrust

Comando que calcula o coeficiente de confiança de um grupo em outro grupo.

5.2.3 Considerações na perspectiva de grupos

Este tópico indica algumas considerações sobre o cálculo da confiança considerando uma visão de membros em um grupo. As questões que envolvem os grupos tratam de um grupo de origem e um grupo de destino e um nodo, que é considerado como o líder para

recolher as informações sobre os dados de reputação, responsável por realizar o cálculo da confiança no grupo e ser um nodo comum integrante do mesmo.

Para fins de demonstração, se considerou dois grupos compostos por 5 agentes em cada grupo. Nestes grupos os agentes interagem entre si e são capazes de gerar opiniões uns sobre os outros. O líder de cada grupo pede para seus membros os valores de reputação para que possa gerar dados sobre a confiança considerando as observações de todos os membros. De posse destes dados, os líderes anunciam entre si os valores de confiança de cada grupo.

Para a visão de grupos é considerado que existe um canal de comunicação seguro entre os nodos e que as mensagens não podem ser alteradas na rede. Além disso, também é considerado que existe uma identidade única em cada ambiente (agentes de software e P2P), e que esta corresponde corretamente a quem se diz ser.

Estas considerações se devem ao fato de não ter sido possível implementar em tempo hábil todas as considerações de eleição de um líder por consenso, conforme parte da proposta de consenso e muito menos de um protocolo de comunicação segura na rede como as propostas de TGDH e suas variações.

5.3 SÍNTESE DO CAPÍTULO

Este capítulo mostra as considerações que são assumidas para a obtenção dos resultados e da conseqüente análise realizada. O estudo da confiança para grupos necessita de critérios bem definidos para a sua aplicação. Esta abordagem tem o intuito de evitar uma quantidade desnecessária de situações, de tal forma que um ambiente tenha uma enorme quantidade de variáveis, gerando uma complexidade que dificulta a obtenção de resultados.

Além disso, como a proposta necessita de valores de confiança direta e de reputação para que a confiança no grupo possa ser calculada, é importante frisar que o modelo de implementção utilizado (TRAVOS [3]) é capaz de gerar os valores de confiança e de reputação na perpectiva de 1:1.

6 RESULTADOS E ANÁLISES

Os resultados são divididos em dois tópicos. O primeiro tópico trata dos resultados e análise para agentes de software. Já o segundo trata da implementação de aspectos da confiança na perspectiva de P2P.

Como forma de aumentar o grau de confiabilidade em uma rede, é necessária a utilização de protocolos que permitam o gerenciamento de identidades, evitando o uso de certificação digital como garantia de identificação única em redes distribuídas. As questões de identificação são complexax para serem tratadas através de uma única análise. Entretanto é importante ressaltar que a utilização de um protocolo de identidade em sistemas distribuídos é uma necessidade e suas características devem ser consideradas para identificação de membros em um grupo em situações onde isto seja necessário e importante.

6.1 CONFIANÇA COM AGENTES DE SOFTWARE

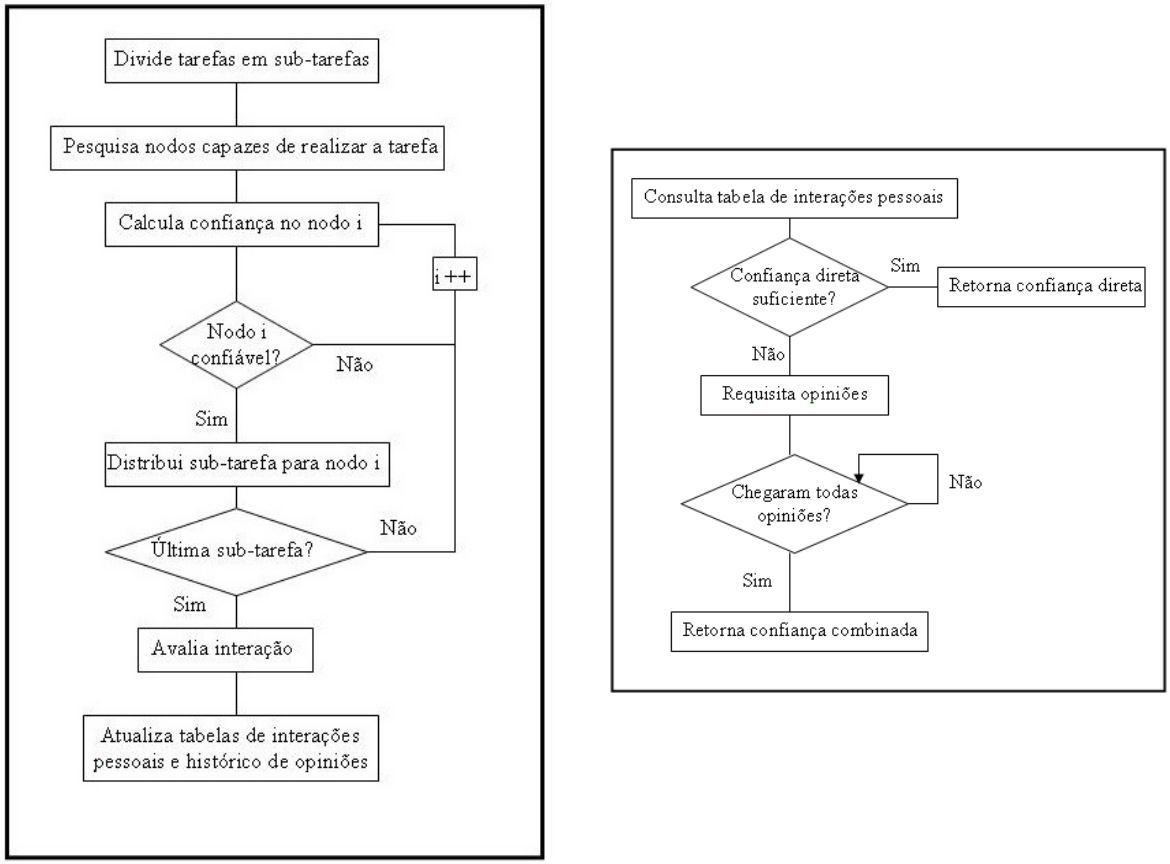
Com o objetivo de fazer o tratamento da confiança em grupos com agentes de software, e para o tratamento e auxilio na identificação de agentes desonestos, foi desenvolvido um conjunto de agentes de software que simulam nodos dentro de um Grid computacional que fazem uso de dados de confiança e reputação para decidir quanto à interação com outros agentes.

É importante ressaltar que o objetivo não é desenvolver uma plataforma Grid completa, com todas as suas camadas e características. Desta forma, optou-se por manter o registro de informações sobre os agentes no Directory Facilitator (DF) do JADE [54]. A Tabela 6-1 demonstra as principais características dos agentes desenvolvidos.

Tabela 6-1 – Características dos agentes simulados

#	Características
1	No momento de sua criação, se registrar no DF como provedor de um determinado serviço;
2	Encontrar todos os agentes disponíveis e/ou os agentes que oferecem determinado serviço
3	Processar desafios enviados por outros agentes
4	Responder questionamento sobre suas interações com outros agentes
5	Receber opiniões de outros agentes e a combinarem com sua própria para chegar a um valor único de confiança, utilizando o modelo de confiança TRAVOS
6	Receber um arranjo de matrizes e retornar a soma ou multiplicação delas

Relacionado com a lógica de implementação, o fluxograma da Figura 6-1a ilustra a seqüência de ações executadas por um agente quando ele possui uma tarefa a ser processada na simulação do Grid, e a Figura 6-1b ilustra a seqüência de passo para calcular a confiança de um nodo i.



a) **b)**

Figura 6-1 – Fluxograma da implementação dos agentes

6.1.1 Resultados experimentados

Para a obtenção de dados para serem analisados, realizou-se simulações do ambiente proposto com 20 agentes. Em primeiro lugar, avaliou-se a quantidade de interações necessárias para que a base de opiniões pessoais se torne suficiente para o cálculo de um valor preciso de confiança. E na seqüência, a quantidade de agentes desonestos no sistema foi variada com o intuito de analisar o impacto de opiniões desonestas no valor de confiança como um todo. Os procedimentos adotados para chegar aos resultados encontrados, bem como suas respectivas análises seguem nos tópicos seguintes.

6.1.2 Desafio

Para encontrar um limiar inicial para o tempo de resposta ao desafio, simulamos um ambiente com 20 agentes que ofereciam um mesmo serviço. No primeiro momento do teste, nenhum deles possuía qualquer informação sobre confiança de outros agentes, e mesmo assim um agente precisava realizar uma tarefa. Devido à falta de informação sobre interações pessoais, ele envia o desafio a todos os agentes do Grid identificados e capacitados para a execução da tarefa.

Para se obter um valor de um tempo médio relacionado com a resposta, se inicializou 20 vezes o ambiente, e seus dados iniciais que foram armazenados em um arquivo para análise. Como característica individual de análise, todos os processadores foram iguais, (apesar dos agentes saberem tratar processadores diferentes). Considerou-se como limiar a média (56 ms) somada ao desvio padrão (23 ms) dos valores da primeira resposta recebida em cada vez que o ambiente foi inicializado. Adotou-se esse critério, pois o primeiro agente a responder ao desafio sempre levava mais tempo que os demais por conta de características próprias do ambiente Jade em relação à identificação e registro dos nodos. Assim, o limiar definido foi de 79 ms, o que para o ambiente de confiança significa que se um agente responder ao desafio levando mais de 79 ms, sua interação será considerada mal sucedida. Também vale ressaltar que este é o limiar para o caso em que o agente desafiador não possua uma tabela completa (com 10 valores) sobre o processador do desafiado. Caso ele possua, o método é o mesmo, porém são utilizados os valores de sua base pessoal de dados.

Para testar a eficiência do critério utilizado, aplicamos o limiar encontrado nos próprios dados amostrados e obtivemos um erro 1,3158%. Nesta aproximação significa que a cada 1000 nodos idôneos que respondem ao desafio, 13 são erroneamente classificados como maliciosos por terem resolvido o desafio em um tempo maior que o esperado.

6.1.3 Confidência

Para cada valor de confiança direta obtido está associado a um valor de confidência. Sendo assim, simulou-se o ambiente Grid para 3, 5, 7 e 10 agentes e observou-se a quantidade de interações necessárias para que um agente passasse a utilizar somente sua tabela de interações pessoais para calcular a confiança em outro agente. Visto que o foco dessa etapa é analisar apenas a confidência, consideramos que todos os agentes do sistema são confiáveis para a realização da tarefa.

Toda vez que um agente A1 precisa avaliar o valor de confiança em um agente A2, A1 calcula o valor de confidência g_{A_1,A_2} na sua avaliação pessoal sobre A2. Definiu-se que um valor adequado para g_{A_1,A_2} no ambiente deveria ser maior que 0,95 (a confiança direta possui no máximo 5% de erro). Assim, enquanto g_{A_1,A_2} for menor que 0,95, A1 incrementa um contador que marca a quantidade de interações realizadas com A2. Quando g_{A_1,A_2} atinge um valor maior que 0,95, o valor do contador contém a quantidade de interações necessárias para que sua base pessoal de informações seja suficiente para o cálculo da confiança e, portanto, é armazenado em um arquivo para análise. Neste arquivo, cada linha possui a quantidade de interações realizadas até o momento em que g_{A_1,A_2} se torna maior que 0,95. Vale notar que esse valor é pessoal para cada agente, ou seja, $g_{A_1,A_2} \neq g_{A_2,A_1}$. Então para um ambiente com N agentes, a quantidade de linhas do arquivo gerado será um arranjo de N dois a dois. Na Tabela 6-2 estão os valores das médias de interações até que g atingisse um valor maior que 0,95.

Tabela 6-2 – Resultados obtidos para o valor de confidência

Quantidade de agentes	***Quantidade média de interações***
3	7,333
5	7,350
7	7,595
10	7,086

Na Tabela 6-2 tem os valores das médias de interações, e até que g atinja o limiar definido estão entre 7 e 8 iterações. Em uma pequena análise, este valor pode parecer relativamente pouco, entretanto, considerando que um sistema distribuído com vários agentes, e com muitos confiáveis, um nodo pode levar uma quantidade de tempo considerável para realizar essa quantidade de interações com um mesmo agente. Uma vez que a divisão da tarefa gera nove sub-tarefas quando um nodo as distribui, no máximo nove nodos são contemplados. Normalmente, esses nodos são os que primeiro se registraram no DF e satisfazem o limiar de confiança adotado. Como na primeira etapa da simulação se considera todos os nodos confiáveis, em um ambiente com mais de 10 nodos, apenas os 9 primeiros recebem sub-tarefas. Desta maneira, considerando que os valores da Tabela 6-2 não demonstraram discrepâncias, considerou-se desnecessário uma simulação para uma quantidade maior de agentes.

6.1.4 Distribuição de tarefas

Inicialmente, foi necessário encontrar um tempo de resposta que seja aceitável na realização de uma tarefa. Para tal ponto, simulou-se o ambiente com todos os nodos confiáveis, onde cada um dos 20 estabelecidos nodos enviou partes da tarefa para cada agente. Esta operação foi repetida 20 vezes e o tempo gasto para receber cada resultado foi armazenado. De maneira análoga ao tempo de resposta ao desafio, considerou-se como limiar o tempo médio de resposta somado ao desvio padrão. Para tarefas do tipo soma o limiar foi de 38ms e para as do tipo multiplicação o limiar foi 33ms. Assim como na análise do tempo de resposta média ao desafio, se armazenou os tempos de resposta das tarefas em arquivo para análise.

Após a definição dos critérios de avaliação de uma interação bem sucedida, se deu continuidade à simulação, que consistiu de um único agente delegando 10 vezes seguidas uma tarefa para um Grid de 20 agentes. Na simulação os nodos são capazes de realizar dois tipos de operações com matrizes (soma e multiplicação), e para as simulações, os agentes alternavam aleatoriamente entre esses dois tipos de operação (relembrando que o limiar de confiança para soma é 0,6 e para multiplicação é 0,8). A cada opinião fornecida, o seu respectivo valor de exatidão era armazenado em um arquivo log para posterior análise, seguindo a forma de uma tabela do tipo <*Agente que avalia, Agente que forneceu opinião, Agente que está sendo avaliado*>. Também a cada resultado de tarefa recebido, a tabela de interações pessoais do agente que requisitou a tarefa era armazenada em outro arquivo de log.

Analisou-se a exatidão da opinião dos agentes para o caso de todos os agentes serem honestos e para 1, 2, 5 e 10 agentes desonestos. No caso do agente desonesto, ao fornecer uma opinião, este sempre envia como resposta 5 interações bem sucedidas e 35 mal sucedidas, o que equivale a um valor de confiança de aproximadamente 0,142857, de tal forma que isto prejudica a reputação do agente alvo da requisição.

Para cada quantidade de agentes desonestos, se escolheu os agentes que melhor ilustravam o caso retratado e utilizaram-se suas informações de confiança para a construção de gráficos que demonstram a variação da opinião fornecida e sua respectiva exatidão. Maiores detalhes sobre os dados podem ser encontrados no Apêndice A.

6.1.5 Análise com todos agentes honestos

A meta foi identificar o comportamento do sistema em um ambiente ideal para comparação com o caso de um ambiente real, onde podem existir nodos desonestos. Nessa análise, todas as sub-tarefas são realizadas com sucesso e todas as opiniões são verdadeiras, o que reflete as tabelas pessoais dos agentes opinadores. Assim, foram simulados 20 agentes, cada um tendo que realizar 10 tarefas. Outra meta era confirmar que quanto mais um agente interage com o sistema, mais sua tabela de interações pessoais se torna próxima à situação real do sistema em um dado instante.

Dada a grande quantidade de interações, escolheu se um agente que tivesse se comportado de forma mais ilustrativa. Pelas respectivas tabelas de interações pessoais (Apêndice A), verificamos que os agentes 0, 16 e 17 se enquadraram nesta situação, já que interagiram várias vezes com outros agentes. Considerando que r depende apenas do passado de opiniões, se analisou as opiniões que o Agente16 forneceu ao Agente0 sobre o Agente17.

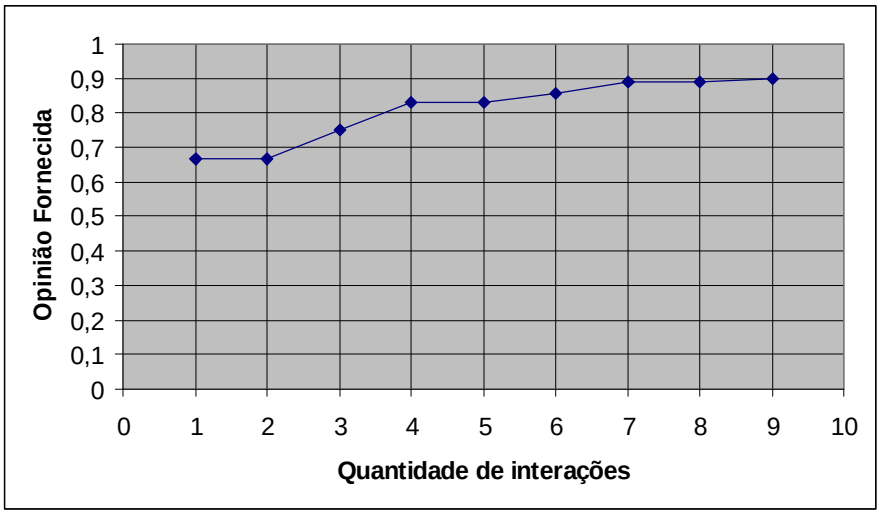


Figura 6-2 – Opiniões fornecidas por um agente honesto que interagiu muitas vezes

A Figura 6-2 mostra a variação da opinião fornecida pelo Agente16 ao Agent0 sobre o Agente17.

Já a Figura 6-3 ilustra a respectiva exatidão das opiniões calculada pelo Agente0. Na primeira interação o valor de r é zero, pois a operação realizada foi de multiplicação, o que seguindo os parâmetros definidos, exige um valor mínimo de confiança de 0,8. Como nenhum nodo conseguiu atingir esse valor, o próprio Agente0 fez toda a tarefa, não recebendo nenhum resultado de interação. O segundo valor de r novamente é zero, entretanto, o Agente0, que requisitou as tarefas, ainda não havia tido uma opinião do Agente16 previamente catalogada.

Ou seja, foi a primeira vez que recebeu uma opinião verificável, e por sua vez, só será utilizada no cálculo do r na próxima vez que ele solicitar a opinião do Agente16.

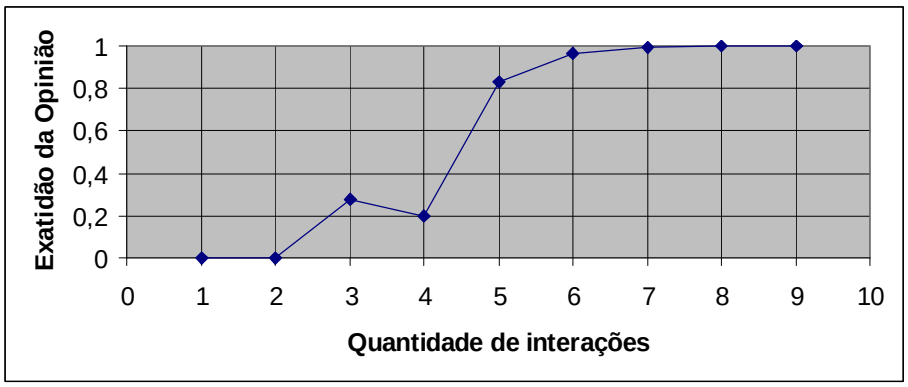


Figura 6-3 – Exatidão das opiniões fornecidas por um agente honesto que interagiu muitas vezes

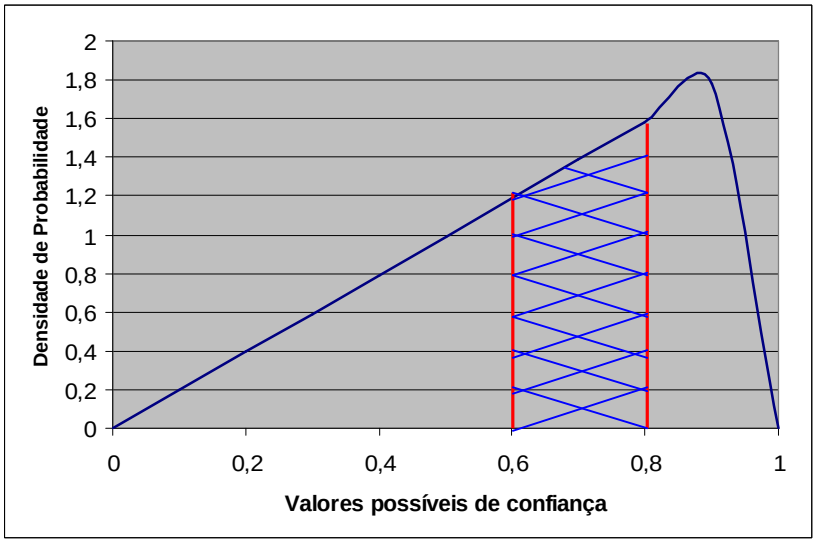


Figura 6-4 – Curva da Densidade de Probabilidade da Confiança de um agente honesto para uma interação bem sucedida e nenhuma má sucedida

Nas terceira e quarta interações, o valor de r para a faixa de opinião [0,6;0,8] é um pouco maior que o da faixa [0,8;1,0]. Com base na tabela pessoal do Agente16, verificou-se que, na terceira interação, a opinião fornecida por ele sobre o Agente17 foi de apenas uma interação bem sucedida. Dessa forma, a curva da sua confiança no Agente17 estava concentrada entre 0,6 e 0,8, como pode ser observado na Figura 6-4.

Após mais algumas interações, devido às tarefas serem bem-sucedidas, a confiança aumenta e a curva afunila-se, deslocando-se para a direita, como ilustrado na Figura 6-5. Isso é perceptível a partir da quinta interação (Figura 6-3), que mostra que a faixa da opinião

fornecida é [0,8;1,0], agora com um maior valor de r associado, que a partir de então se torna crescente (Figura 6-5). Em uma breve análise, quando o agente analisado não teve muitas interações com outros agentes, não se observou o comportamento descrito acima.

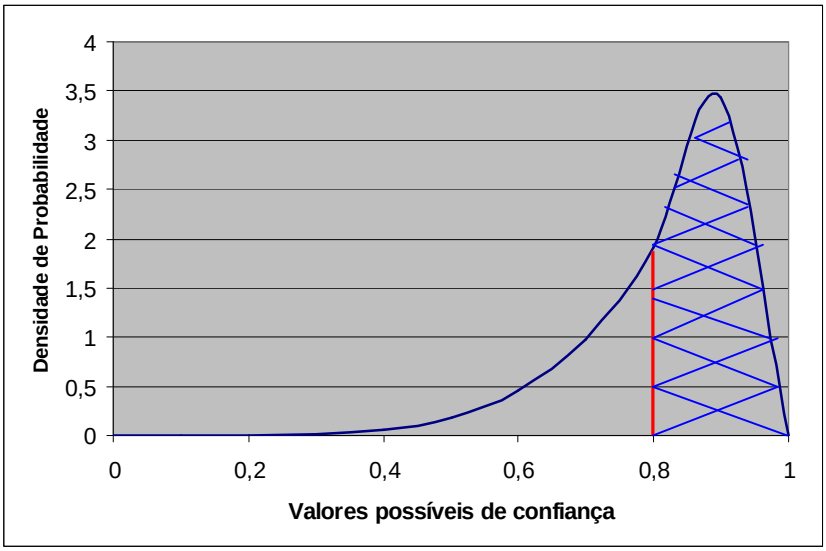


Figura 6-5 – Curva da Densidade de Probabilidade da Confiança de um agente honesto para 5 opiniões bem sucedidas recebidas e nenhuma má sucedida

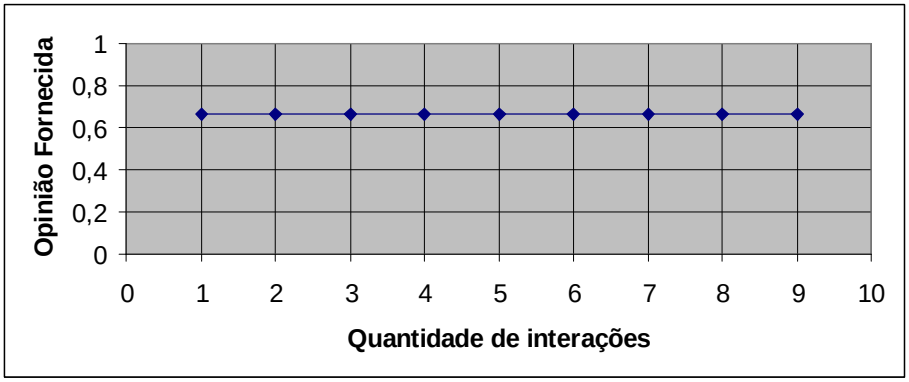


Figura 6-6 – Opiniões fornecidas por um agente honesto que interagiu poucas vezes

A Figura 6-6 ilustra esse caso, no qual o Agente12 não teve uma quantidade suficiente de interações com o Agente11 para oferecer uma opinião que refletisse seu comportamento real, visto que, informava uma opinião que não estava de acordo com os resultados das demais interações com outros agentes.

Por isso, o r do Agente0 no Agente12, de acordo com a Figura 6-7, foi decrescendo continuamente. Esse padrão foi observado em todas as simulações para agentes que tiveram poucas interações. Na Figura 6-6, a opinião fornecida pelo Agente12 é sempre 0,667, o que

reflete uma interação bem sucedida e uma má sucedida. Porém, o histórico de opiniões do requisitante, Agente0, não condiz com a opinião fornecida para a faixa [0,6;0,8], que é a faixa que contém essa opinião.

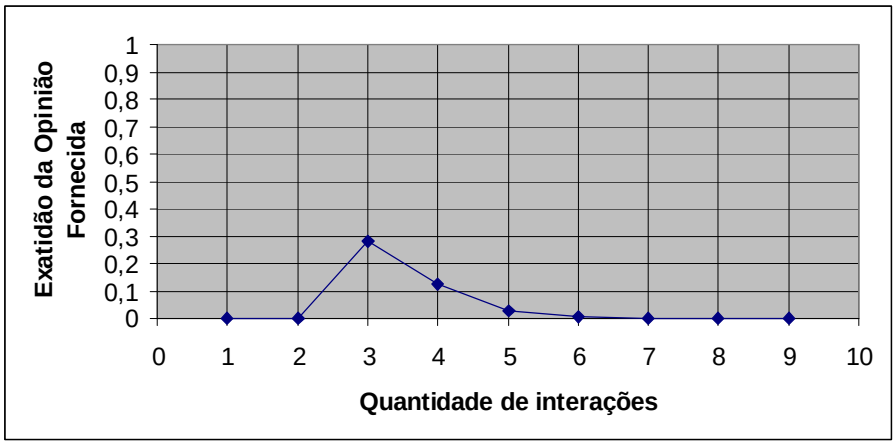


Figura 6-7 – Exatidão das opiniões fornecidas por um agente honesto que interagiu poucas vezes

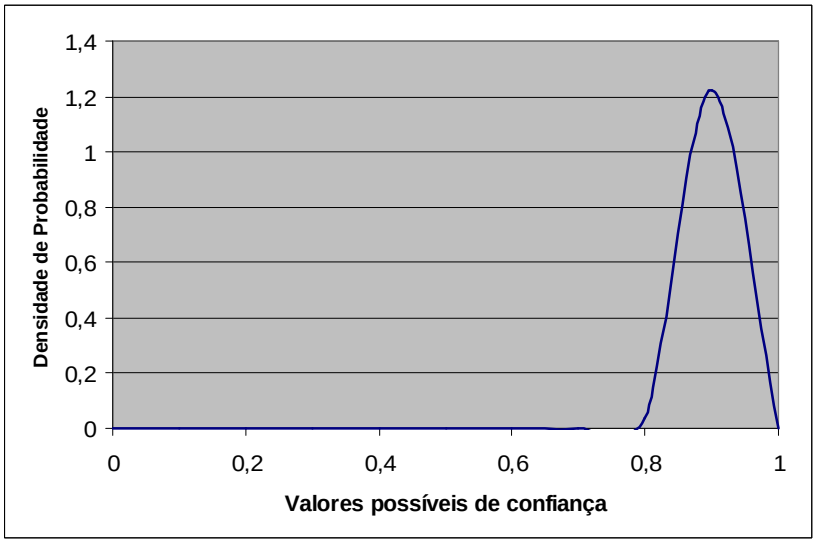


Figura 6-8 – Curva representativa da Densidade de Probabilidade da Confiança para um ambiente onde já ocorreram várias interações

De acordo com a Figura 6-7, após a sexta interação (neste teste todos os agentes realizam a tarefa com sucesso), a quantidade de boas interações torna-se muito maior que a de más interações. E baseado nessa constatação, a Figura 6-8 ilustra a densidade de probabilidade de confiança para um ambiente em que já ocorreram várias interações.

Desta maneira, para o caso em que o Agente12 forneceu uma opinião de 0,667, observamos que a área sob o gráfico limitada pelo intervalo ao qual pertence à opinião fornecida – [0,6;0,8] – é muito pequena, quase nula. Como a exatidão da opinião é

diretamente proporcional a essa área, esta será praticamente desconsiderada, visto que a área analisada tem seu valor de pouca representação.

6.1.6 Análise com agentes desonestos

Os dados a seguir, ilustram os resultados para uma simulação de uma situação real, onde existem agentes desonestos no Grid computacional. Foram realizados testes divididos para 1, 2, 5 e 10 agentes desonestos, em um total de 20 agentes no sistema. Para cada teste, o ambiente foi reiniciado, de forma que as simulações foram independentes, o que não deixa uma relação entre os agentes de uma simulação com outra. Nesta consideração, por exemplo, o Agente0 analisado para um teste com um agente desonesto não é o mesmo Agente0 em outro teste com dois agentes desonestos.

6.1.6.1 Um agente desonesto

Para o caso de um agente desonesto, neste caso o Agente0, dentre 19 agentes honestos, obtivemos o comportamento ilustrado pela Figura 6-9. Para este resultado foram considerados dois agentes específicos, o único agente desonesto do sistema, o Agente0, e um agente honesto que tenha interagido bastante com o ambiente, neste caso o Agente1. Na situação observada, esses agentes constituem os opinadores, ou seja, eles fornecem opinião a um agente sobre um terceiro.

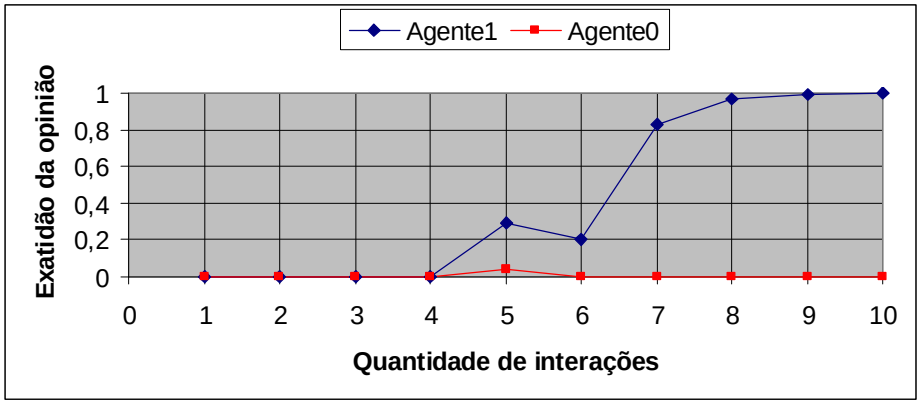


Figura 6-9 – Resultados de um agente honesto (Agente1) e um desonesto (Agente0) em um sistema composto de 1 desonesto e 19 honestos

Na análise dos dados coletados, o Agente12 pede opinião sobre o Agente4 aos agentes Agente0 e Agente1. E também existe uma exatidão associada a essa opinião fornecida, de acordo com o passado de interações do Agente12, o requisitante da opinião. Essa métrica de

exatidão refere-se à conformidade da opinião fornecida em relação ao histórico de opiniões passadas.

Pela análise da Figura 6-9, percebe-se que a precisão da opinião, r , do agente desonesto é extremamente pequena, tendendo a zero, em contraste com o r do agente honesto. Este detalhe, assim como na análise do sistema composto exclusivamente de agente honestos, tende a crescer ao longo do tempo. Isto implica que a opinião fornecida pelo desonesto não influi no cálculo da confiança. Observa-se ainda que na sexta interação, a exatidão da opinião do agente honesto (Agente1) diminui para depois voltar a crescer. Esse fenômeno está relacionado à faixa de opinião fornecida e ao histórico de opiniões no momento daquela interação.

6.1.6.2 Dois agentes desonestos

No caso de dois agentes desonestos, compostos pelos Agente0 e Agente1, dentre outros 18 agentes honestos, se obteve resultados dados pela Figura 6-10. Os dados referem-se ao Agente13 como nodo interessado em realizar uma tarefa, que recebe opiniões sobre o Agente14. As opiniões analisadas foram as fornecidas pelos dois agentes desonestos (Agente0 e Agente1) e um agente honesto para comparação (Agente16).

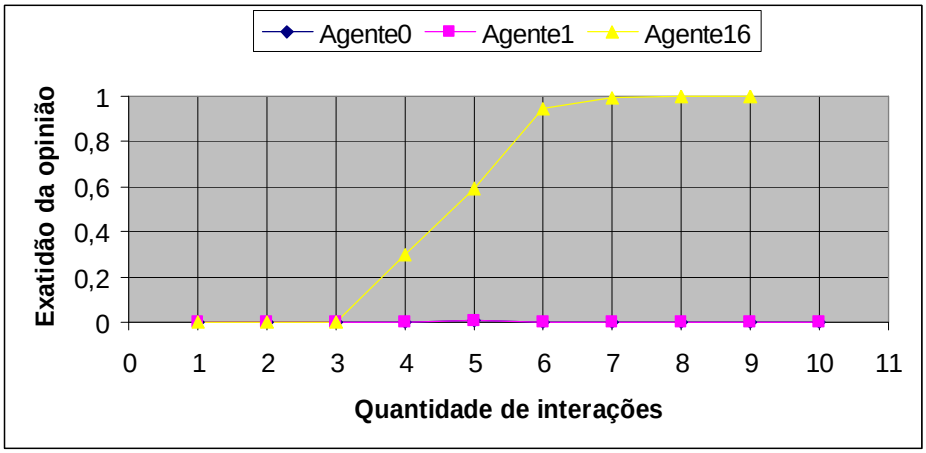


Figura 6-10 – Resultados de um agente honesto (Agente16) e 2 agentes desonestos (Agente0 e Agente1) em um sistema composto de 2 desonestos e 18 honestos

Notamos que o comportamento dos agentes desonestos assemelha-se ao comportamento representado pela Figura 6-9. Na análise dos resultados, os agentes desonestos têm sua opinião praticamente neutralizada, pois o valor da exatidão que as pondera é praticamente nulo. Assim, quando o Agente13 for combinar todos os valores de reputação

recebidos, os fornecidos pelos agentes 0 e 1 têm pouca influência sobre o valor final de confiança. Já o comportamento do nodo honesto (Agente16) apresenta-se crescente, mantendo a tendência até aqui observada.

Observa-se que as curvas dos dois agentes desonestos retratados (Agente0 e Agente1) estão sobrepostas, não sendo possível visualizar diretamente a curva do Agente0.

6.1.6.3 Cinco agentes desonestos

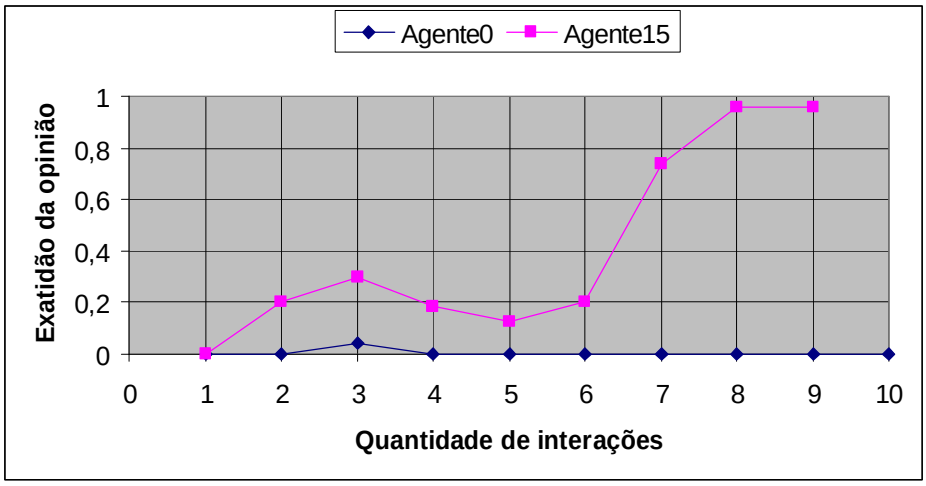


Figura 6-11 – Resultados de um agente honesto (Agente15) e um desonesto (Agente0) em um sistema composto de 5 desonestos e 15 honestos

Neste teste, o ambiente foi composto do Agente0 ao Agente4 sendo desonestos e os outros 15 sendo honestos. Analisaram-se as opiniões fornecidas ao Agente10, sobre o Agente4, por um dos agentes desonestos (Agente0) e por um dos agentes honestos (Agente15), ilustrado pela Figura 6-11. Observa-se na figura que o valor da exatidão da opinião dos agentes desonestos é praticamente zero, enquanto que a opinião do honesto, a longo prazo, tende a um valor próximo de 1. Neste caso, quanto mais o agente honesto (Agente15) realiza interações, mais opiniões são fornecidas que refletem o comportamento do agente alvo das requisições de opinião (Agente4).

É interessante observar que o alvo da requisição, em ambos os casos, é um agente desonesto (Agente4). A princípio seria estranho perceber que a opinião sobre um agente desonesto é positiva e possui uma alta exatidão, quando fornecida por um nodo honesto. Entretanto, nas considerações desta simulação, os agentes desonestos realizam as sub-tarefas solicitadas corretamente. O que os torna indesejáveis na rede é o fato de mentirem a respeito

de suas interações pessoais, com o intuito de diminuir a confiança de outros agentes em seus concorrentes diretos.

6.1.6.4 Dez agentes desonestos

Por fim, foi simulado um Grid de 10 nodos desonestos, compostos dos Agente0 ao Agente9, e 10 agentes honestos, do Agente10 ao Agente19. Analisamos as opiniões fornecidas ao Agente14, sobre o Agente17, por um dos agentes desonestos (Agente5) e pelo agente honesto (Agente18), representados pela Figura 6-12.

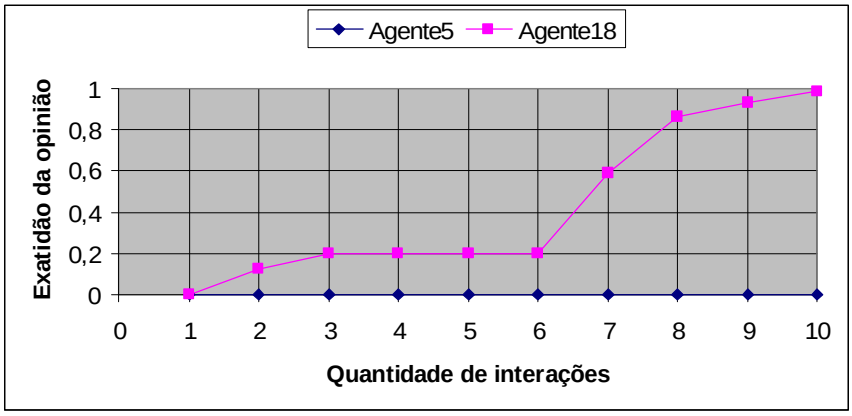


Figura 6-12 – Resultados de um agente honesto (Agente18) e um desonesto (Agente5) em um sistema composto de 10 desonestos e 10 honestos

Do mesmo modo que observado para nos resultados anteriores, o valor de r (exatidão da opinião) para os agentes desonestos (exemplificado aqui pelo Agente5) diminui, tendendo a zero, ao passo que o dos honestos (ilustrado pelo Agente18) aumenta.

6.1.6.5 Comparativo entre os casos de agentes desonestos

A representação dos resultados dos itens a, b, c e d teve por objetivo a análise entre as exatidões de opinião de um agente desonesto com um honesto de maneira que fosse possível avaliar o impacto de opiniões desonestas no valor final da confiança. Esta avaliação foi composta por meio da análise da ponderação da opinião fornecida, que é representada pela exatidão da opinião mencionada. E na seqüência, comparou-se as exatidões de opinião entre um nodo desonesto de cada situação (1, 2, 5 e 10 nodos desonestos de um total de 20 nodos). A

Tabela 6-3 lista os agentes que foram analisados para cada situação.

Tabela 6-3 – Agentes desonestos analisados em cada situação simulada

Descrição do ambiente	Agente analisado
1 agente desonesto e 19 honestos	Agente0
2 agentes desonestos e 18 honestos	Agente0
5 agentes desonestos e 15 honestos	Agente0
10 agentes desonestos e 10 honestos	Agente5

Desta forma, foram compostos os dados das demais análises, gerando os dados representados pela Figura 6-13.

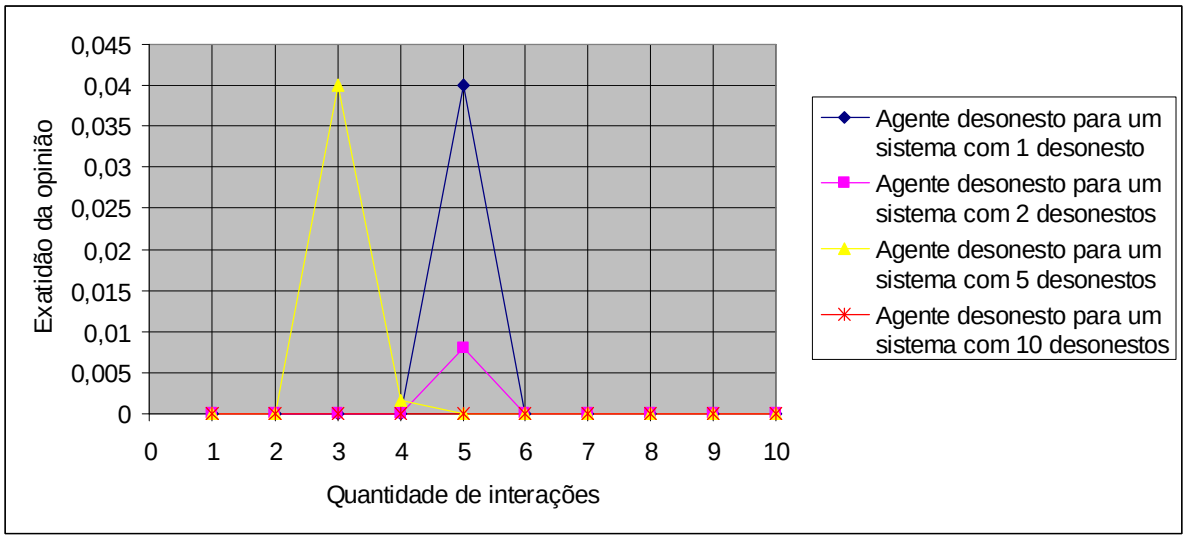


Figura 6-13 – Comparação da variação das exatidões de opinião em função da quantidade de iterações para agentes desonestos nos casos apresentados

Em uma breve análise, constatou-se que as curvas comportam-se de forma semelhante, indicando que o modelo de confiança foi capaz de identificar a opinião de um nodo desonesto, minimizando sua má influência no valor da confiança, independente da quantidade de nodos desonestos na rede. Verificou-se também que mesmo nos picos das curvas equivalem a valores muito baixos de exatidão da opinião (r).

O detalhe destes picos é que ocorrem na primeira vez que o agente requisitante associa um valor de r à opinião fornecida pelo agente desonesto, cuja dimensão ainda não é extremamente pequena, pois, nesse momento, os agentes realizaram poucas interações, possuindo pouca informação para o calculo da confiança. E no ambiente, quanto mais interações ocorrem, mais o valor da confiança de um agente honesto se distancia da opinião fornecida por um agente desonesto. Por isso sua opinião influencia cada vez menos no valor da confiança combinada. Assim, com o decorrer das interações, às informações fornecidas

pelo agente desonesto é associado um valor de exatidão que tende a zero. E de maneira geral, isolando os agentes com estas características dos demais no ambiente.

6.1.7 Resultados na perspectiva de grupos

Este tópico demonstra alguns resultados com a perspectiva de funcionamento dos nodos considerando os valores de confiança e o cálculo da confiança em grupos. Cada grupo é composto de 5 agentes (do agente1 ao agente5). As simulações foram feitas em cinco testes distintos. O primeiro ilustra a situação ideal, em que todos os nodos possuem um bom comportamento e este não muda com o passar do tempo. No segundo teste, existe um nodo malicioso que já inicia o teste como sendo malicioso. O terceiro teste inicia com dois nodos maliciosos. O quarto teste inicia com 3 nodos maliciosos. Nestes testes não é considerado o histórico da comunicação. Por fim o último teste inicia com o nodo 1 mudando seu comportamento em um determinando instante (t=2), o nodo 3 muda seu comportamento no instante t=5 e o nodo 5 muda seu comportamento no instante t=8 e é considerado o histórico da comunicação. Estabeleceu-se que o valor de confiança mínimo para se considerar uma comunicação com o grupo foi de $t \geq 0{,}7$.

6.1.7.1 Com todos os nodos honestos

A Figura 6-14 ilustra o que seria uma situação ideal, em que todos os nodos são honestos e não mudam de comportamento durante o passar do tempo.

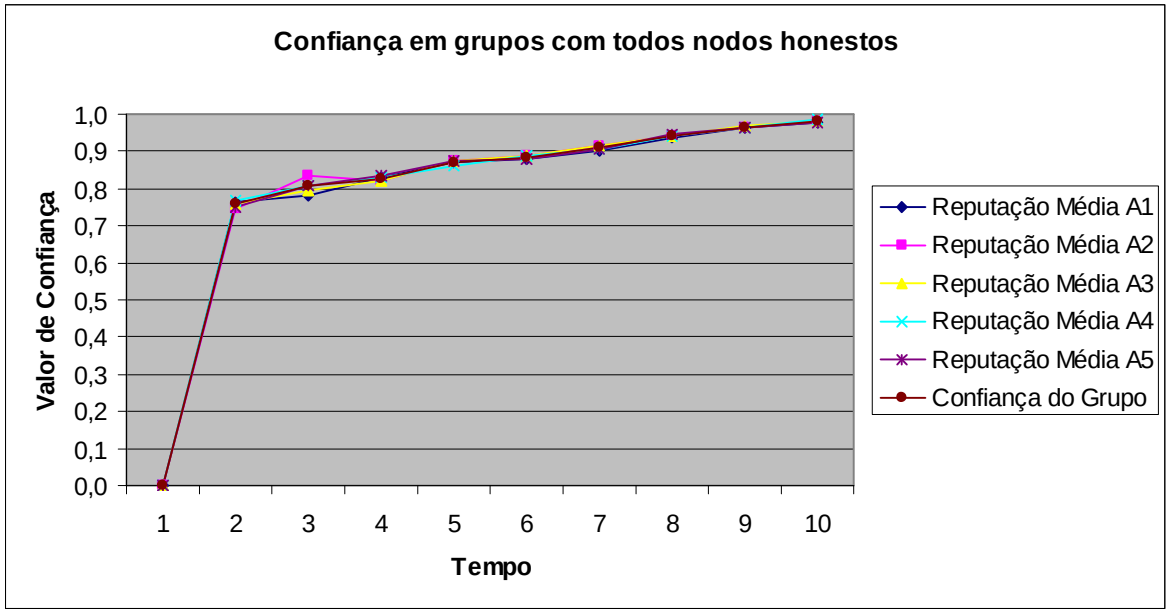


Figura 6-14 – Confiança em grupos na situação ideal

Neste caso, a confiança do grupo segue a perspectiva de comportamento dos seus membros. Todos os nodos iniciam com a confiança igual a zero e seguem realizando interações na rede. Já a partir de t=2 o grupo já é considerado honesto porque todos os nodos realizam as tarefas a contento. E seguem crescendo seus valores de confiança.

6.1.7.2 Com um nodo desonesto no grupo

Para o caso onde existe um agente desonesto e os nodos são capazes de identificá-lo, a situação da perspectiva do grupo muda porque só depois de algumas iterações a mais na rede é que o grupo consegue alcançar um limiar de confiança mínimo estabelecido. A Figura 6-15 ilustra a situação onde existe um nodo malicioso no grupo.

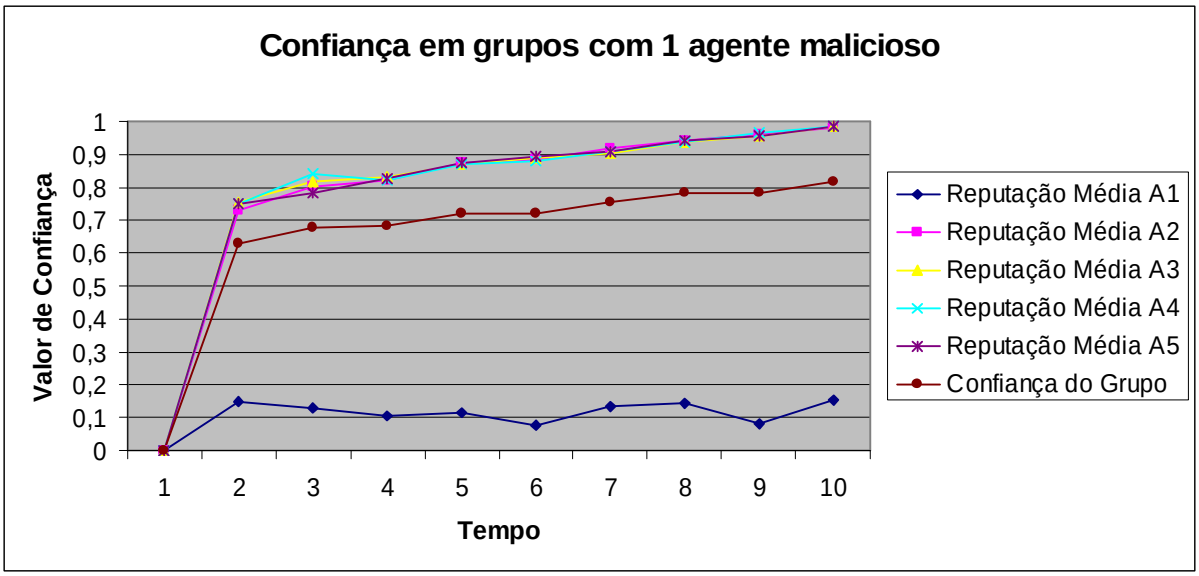


Figura 6-15 – Confiança em grupos com um nodo malicioso

Nesta perspectiva, somente entre o instante t=4 e t=5 é que o grupo pode ser considerado confiável com um de seus membros sendo maliciosos.

6.1.7.3 Com dois nodos desonestos no grupo

Nesta perspectiva, mesmo cerca de 60% dos nodos mantendo seu comportamento bom durante o tempo, a sua representação de confiança não é suficiente para inferir no comportamento do grupo.

A Figura 6-16 ilustra o caso quando existem dois nodos maliciosos em um grupo. Neste caso, até a execução do final do teste, o grupo não é considerado confiável.

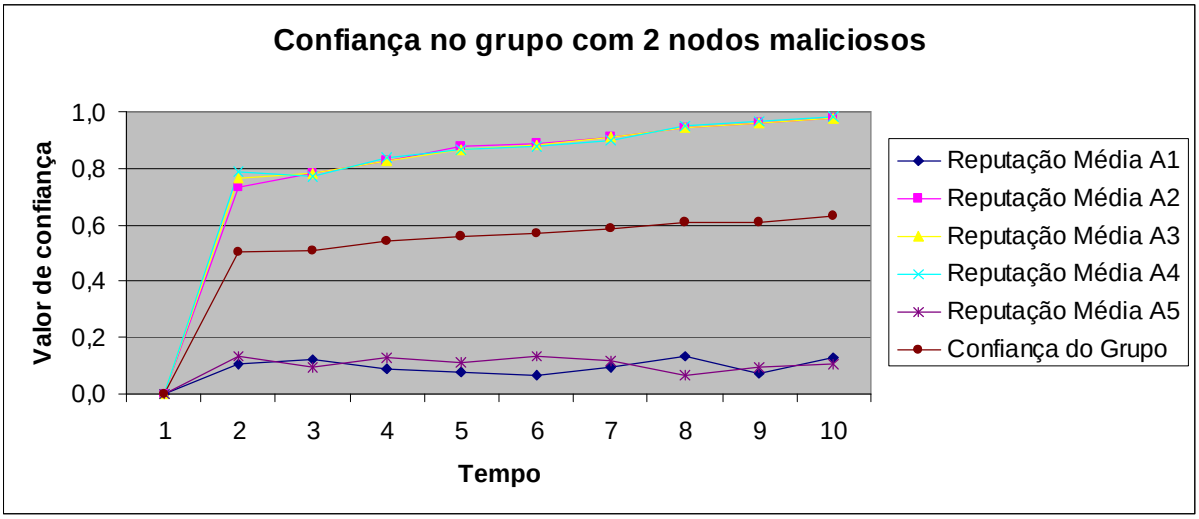


Figura 6-16 – Confiança em grupos com dois nodos maliciosos

6.1.7.4 Com três nodos desonestos no grupo

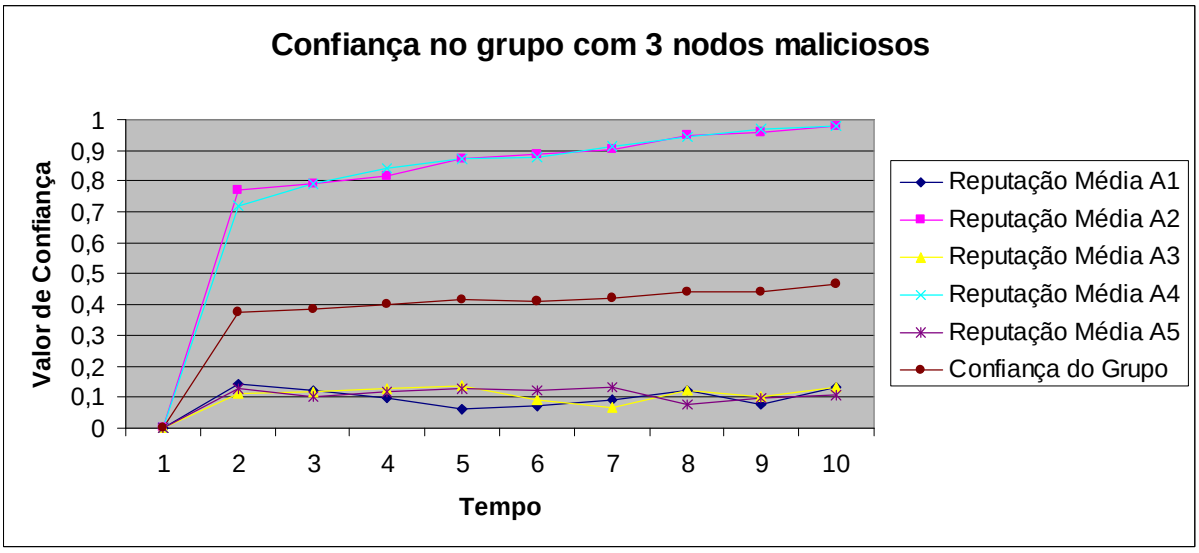


Figura 6-17 – Confiança em grupos com três nodos maliciosos

A Figura 6-17 ilustra a situação onde três nodos no grupo são maliciosos. Neste caso, e conforme o segundo caso, o grupo não é considerado confiável e os dados de confiança dos membros mantêm o valor de confiança do grupo sempre abaixo do mínimo critério estabelecido. Como conseqüência o grupo é considerado como não confiável durante todo o tempo.

6.1.7.5 Com mudança de comportamento dos nodos considerando histórico

Este teste demonstra a questão de um ou alguns nodos mudarem de comportamento no decorrer do tempo. Em outras palavras, simula uma situação real em que um nodo malicioso inicia suas atividades de maneira normal e com o passar do tempo muda repentinamente seu comportamento. O histórico neste caso é considerado até o instante t=10. No caso deste teste, os agentes1, 3 e 5 mudam seu comportamento durante a execução do teste em t=12, t=15 e t=18 respectivamente (considerando o ponto inicial da mudança de comportamento equivale a t=10). A Figura 6-18 ilustra este esquema deste teste.

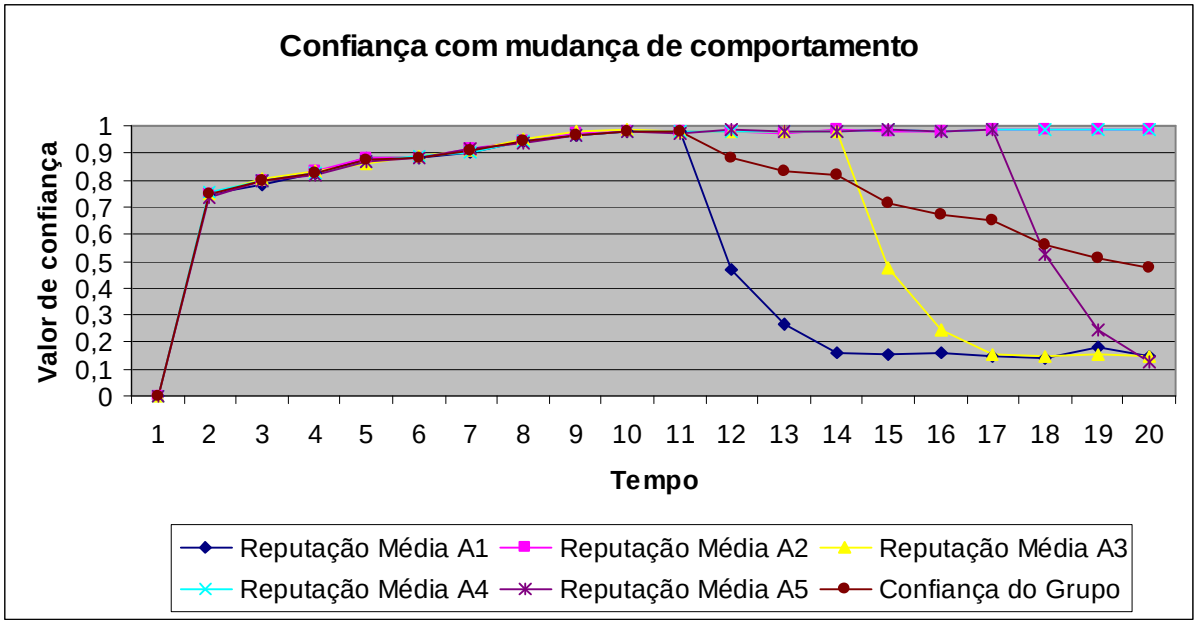


Figura 6-18 – Confiança em grupos com mudança de comportamento

Observando os resultados, a partir do momento que mais de um nodo é malicioso na rede, o grupo deixa de ser confiável. Neste caso isto ocorre entre o instante t=15. Como a confiança em grupo reflete o funcionamento das relações de confiança entre os membros, se um único membro começa a deixar de colaborar corretamente, o grupo é capaz de perceber essa mudança. Assim a confiança do grupo tende a ir baixando à medida que interações ocorrem. E a confiança do nodo em questão tende a ir abaixando até a chegar a um patamar próximo de zero.

Esta característica é percebida nos nodos que também mudam seu comportamento com o passar do tempo. E esse reflexo, segundo o gráfico, é percebido com poucas iterações no grupo porque o agente simplesmente deixa de colaborar segundo o esperado. Além disso, como a reputação conta no cálculo da confiança do grupo, a opinião dos nodos, que são

capazes de detectar a mudança, dizem que determinado agente deixou de agir corretamente. Bem deste ponto em diante, se o grupo deseja manter o seu valor de confiança alto, deverá isolar e remover o nodo do grupo, fazendo com que o valor de confiança volte a representar o comportamento dos membros do grupo.

6.2 CONFIANÇA COM P2P

Para simplificar a análise dos resultados, os testes foram realizados desconsiderando a possibilidade real de que os peers podem mentir sobre sua confiança na rede, ou seja, todos divulgavam seus valores reais de confiança e reputação. Um peer malicioso divulga corretamente seus valores de confiança, mas age de maneira a enviar dados corrompidos ou atrasados, comprometendo os parâmetros iniciais de confiança estabelecidos.

As simulações foram feitas considerando um ambiente ideal, em que todos os peers iniciam seus trabalhos na rede ao mesmo tempo e interagem uns com os outros o mesmo número de vezes. Isto significa que as tabelas de confiança são equivalentes para qualquer peer na rede, ou seja, os peers sempre estarão de acordo quanto a um determinado assunto. O objetivo da inicialização dos peers ao mesmo tempo é mostrar o comportamento das máquinas de acordo com o modelo de confiança escolhido de uma maneira padronizada, evitando que fatores alheios ou não observados pudessem influenciar os resultados.

O parâmetro e utilizado para o cálculo de confidencia foi definido em $e = 0.2$, e indica o nível de erro aceitável de uma observação. O parâmetro de confidencia g, por sua vez, foi definido como $g = 0.95$. Isto significa que, se a confidencia de um peer específico for menor que este valor, este peer precisará requisitar informações de reputação a outros peers na rede. Foi estabelecido um valor de confiança total mínimo de 0.7 para que um peer possa considerar outro peer confiável e resolva continuar interagindo com ele. Para valores menores que 0.7, o peer não é considerado confiável e a troca de informações com ele é terminada. Foram realizadas três simulações distintas. A primeira equivale ao cálculo da confiança sem mudança de comportamento. A segunda com mudança de comportamento dos peers e a terceira no contexto de grupos.

6.2.1 Cálculo da confiança sem mudança de comportamento

Esta simulação foi feita através de uma rede na qual todos os peers possuem um comportamento padrão, ou seja, não mudam de comportamento no decorrer do tempo. Isto

significa que os peers maliciosos já são iniciados como sendo maliciosos (t=0), e mantém o seu comportamento até o final das interações. Neste teste os peers não possuem um histórico de confiança com bons valores e, por isso esta simulação é também considerada como um cálculo da confiança sem histórico.

Nesta simulação foram realizados dois testes, onde o primeiro considera que nenhum peer é malicioso na rede. O segundo considera que 20% dos peers são maliciosos na rede. Como todos os peers são iniciados ao mesmo tempo, os valores de confiança são semelhantes para peers com o mesmo comportamento. É importante relembrar que em uma rede real isto não acontece, gerando valores de confiança distintos para cada peer, conforme percebido no caso dos agentes. Em cada teste foram realizadas dez interações, o que é considerado suficiente para descrever o comportamento da confiança na rede.

6.2.1.1 Nenhum peer malicioso

Esta simulação foi feita como uma base de comparação para todos os outros testes porque não existe nenhum peer malicioso e a rede se comporta de forma ideal. O valor da confiança se inicia com 0 no t=0 e segue aumentando no decorrer do tempo. Os valores de confiança são iguais porque todos os nodos foram iniciados ao mesmo tempo executando a mesma tarefa.

Tabela 6-4 – Confiança direta com nenhum peer malicioso

Peer	t=0	t=1	t=2	t=3	t=4	t=5	t=6	t=7	t=8	t=9	t=10
peer2	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.917
peer3	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.917
peer4	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.917
peer5	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.917
peer6	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.917
peer7	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.917
peer8	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.917
peer9	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.917
peer10	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.917

Peers não maliciosos

A Tabela 6-4 e a Tabela 6-5 são relativas aos dados analisados para o peer1 e equivalem a confiança direta e outra da confiança combinada.

Nesta simulação, que poderia ser considerada um ambiente ideal, caso somente a confiança direta estivesse sendo considerada, todos os peers a partir de t=2 são dados como confiáveis. Segundo as propriedades para a distribuição beta, utilizado no modelo de confiança, esta é crescente, tendo como tendência que o valor aumente até estabilizar próximo a um.

Tabela 6-5 – Confiança combinada com nenhum peer malicioso

Peer	t=0	t=1	t=2	t=3	t=4	t=5	t=6	t=7	t=8	t=9	t=10
peer2	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.917
peer3	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.917
peer4	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.917
peer5	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.917
peer6	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.917
peer7	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.917
peer8	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.917
peer9	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.917
peer10	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.917

Peers não maliciosos

Momento em que a confiança direta é suficiente

Para uma perspectiva de confiança combinada, todos os peers, a partir de t=1, são confiáveis. Este ponto se deve ao fato de que todos os peers respondem a requisição de reputação com valores positivos (no início), o que leva os coeficientes de confiança combinada a crescerem mais rápido do que os coeficientes de confiança direta. Em t=8, ocorre uma queda do coeficiente de confiança porque é neste ponto que a confidência g é maior ou igual ao limiar estabelecido (0.95). A partir deste ponto, as informações de reputação não são mais consideradas e o coeficiente de confiança combinada é igual ao coeficiente de confiança direta.

6.2.1.2 Simulação com 20% dos peers maliciosos

No caso desta simulação, 20% dos peers se comportam de forma maliciosa. Como resultado básico da análise, o valor da confiança diminui sensivelmente para os peers maliciosos e aumenta para os peers normais. A Tabela 6-6 e a Tabela 6-7 são relativas ao peer1, indicando a confiança direta e a confiança combinada. Os valores de confiança são iguais porque todos os nodos foram iniciados ao mesmo tempo executando a mesma tarefa.

No caso desta simulação, se somente a confiança direta estivesse sendo considerada, todos os peers normais (do peer1 ao peer8) seriam considerados confiáveis a partir de t=2. Para o caso dos peers maliciosos (peer9 e peer10), estes são considerados não-confiáveis desde o início porque o coeficiente de confiança foi iniciado como zero, entretanto, durante as interações na rede, o seu comportamento influencia no cálculo da confiança e estes nunca alcançam um valor inicial para serem considerados confiáveis.

Tabela 6-6 – Confiança direta com 20% de peers maliciosos

Peer	t=0	t=1	t=2	t=3	t=4	t=5	t=6	t=7	t=8	t=9	t=10
peer2	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.917
peer3	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.917
peer4	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.917
peer5	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.917
peer6	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.917
peer7	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.917
peer8	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.917
peer9	0.000	0.333	0.250	0.200	0.167	0.143	0.125	0.111	0.100	0.091	0.083
peer10	0.000	0.333	0.250	0.200	0.167	0.143	0.125	0.111	0.100	0.091	0.083

Peers maliciosos
Peers não maliciosos

Tabela 6-7 – Confiança combinada para 20% dos peers maliciosos

Peer	t=0	t=1	t=2	t=3	t=4	t=5	t=6	t=7	t=8	t=9	t=10
peer2	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.917
peer3	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.917
peer4	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.917
peer5	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.917
peer6	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.917
peer7	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.917
peer8	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.917
peer9	0.000	0.091	0.050	0.034	0.026	0.021	0.018	0.015	0.100	0.091	0.083
peer10	0.000	0.091	0.050	0.034	0.026	0.021	0.018	0.015	0.100	0.091	0.083

Peers maliciosos
Peers não maliciosos
Momento em que a confiança direta é suficiente

Percebe-se que o coeficiente de confiança dos peers normais no decorrer do teste é semelhante ao da simulação anterior e que o coeficiente de confiança dos peers maliciosos é decrescente, sendo que esta tendência é diminuir até estabilizar em um valor próximo a zero.

Nesta simulação, todos os peers normais são confiáveis a partir de t=1. No caso dos peers maliciosos, estes já são considerados como não confiáveis desde a primeira interação porque continuam com um coeficiente baixo de confiança.

Este fato se explica porque todos os peers respondem a requisição de reputação dos peers 9 e 10 com valores negativos (o que leva os coeficientes de confiança combinada a decaírem mais rápido do que os coeficientes de confiança direta). Em t=8, ocorre uma queda repentina do coeficiente de confiança dos peers normais e um aumento repentino do coeficiente dos peers maliciosos. E semelhante à análise anterior, isto acontece porque é este o ponto em que a confidência g é maior ou igual ao limiar estabelecido.

Considerando estes resultados, os peers normais (do peer1 ao peer8) são considerados confiáveis e interagem uns com os outros, enquanto os peers maliciosos (peer9 e peer10) são considerados não-confiáveis e são isolados da comunicação da rede, onde nenhum peer normal interage com eles.

No caso desta simulação, fica sinalizado de que não existe possibilidade de que os peers normais confiem nos peers maliciosos, não importando quantos peers maliciosos existam na rede, desde que tenham algumas iterações iniciais. Esta perspectiva ocorre porque os peers já iniciam maliciosos e o não existe histórico de boas interações.

6.2.1.3 Cálculo da confiança com mudança de comportamento

Na tentativa de simular um ambiente mais próximo da realidade, foi conduzido um teste no qual os peers são capazes de mudar o seu comportamento no decorrer do tempo, refletindo um fato mais condizente com redes P2P atuais.

Nesta simulação, todos os peers são iniciados como peers normais no instante t=0. À medida que ocorrem interações, alguns peers mudam o seu comportamento. Neste teste, os peers possuem um histórico de confiança com bons valores no momento em que se tornam maliciosos. E por esta consideração, esta simulação também pode ser denominada de cálculo da confiança com histórico.

Na simulação realizada, um teste em momentos definidos, alguns peers se tornam maliciosos. 20% dos peers (peer9 e peer10) em t=4. Na sequência, 50% dos peers (peer6, peer7, peer8, peer9 e peer10) em t=7. Por fim 70% dos peers (peer4, peer5, peer6, peer7, peer8, peer9 e peer10) em t=10.

Como todos os peers na rede são iniciados ao mesmo tempo, os valores de confiança são semelhantes para peers com o mesmo comportamento. Como ocorrem mudanças na rede, e de maneira a ter melhores resultados para análise do comportamento dos coeficientes de confiança, foi realizado um número maior de interações.

No início desta simulação, não existe nenhum peer malicioso e a rede se comporta de forma ideal. O valor da confiança inicia zerado (t=0) e vai aumentando no decorrer do tempo. A Tabela 6-8 e a Tabela 6-9 são relativas ao peer1 de seus dados de confiança direta e outra da confiança combinada.

Neste caso, se a confiança direta estivesse sendo considerada, todos os peers passam a ser confiáveis a partir de t=2. Na perspectiva do teste para a confiança direta, o comportamento do peer1 ao peer3 é semelhante aos resultados da simulação anterior, uma vez que estes se mantêm íntegros no decorrer de todo o teste.

Tabela 6-8 – Confiança direta com histórico

Peer	t=0	t=1	t=2	t=3	t=4	t=5	t=6	t=7	t=8	t=9	t=10	t=11	t=12
peer2	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.917	0.923	0.929
peer3	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.917	0.923	0.929
peer4	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.833	0.769	0.714
peer5	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.889	0.900	0.909	0.833	0.769	0.714
peer6	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.778	0.700	0.636	0.583	0.538	0.500
peer7	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.778	0.700	0.636	0.583	0.538	0.500
peer8	0.000	0.667	0.750	0.800	0.833	0.857	0.875	0.778	0.700	0.636	0.583	0.538	0.500
peer9	0.000	0.667	0.750	0.800	0.667	0.571	0.500	0.444	0.400	0.364	0.333	0.308	0.286
peer10	0.000	0.667	0.750	0.800	0.667	0.571	0.500	0.444	0.400	0.364	0.333	0.308	0.286

Momento a partir do qual o peer4 e peer5 se tornam maliciosos
Momento a partir do qual o peer6, peer7 e peer8 se tornam maliciosos
Momento a partir do qual o peer9 e peer10 se tornam maliciosos

Tabela 6-9 – Confiança combinada com histórico

Peer	t=0	t=1	t=2	t=3	t=4	t=5	t=6	t=7	t=8	t=9	t=10	t=11	t=12
peer2	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.917	0.923	0.929
peer3	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.917	0.923	0.929
peer4	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.833	0.812	0.745
peer5	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.985	0.900	0.909	0.833	0.812	0.745
peer6	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.846	0.743	0.663	0.598	0.545	0.500
peer7	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.846	0.743	0.663	0.598	0.545	0.500
peer8	0.000	0.909	0.950	0.966	0.974	0.979	0.982	0.846	0.743	0.663	0.598	0.545	0.500
peer9	0.000	0.909	0.950	0.966	0.737	0.596	0.500	0.431	0.378	0.337	0.304	0.277	0.255
peer10	0.000	0.909	0.950	0.966	0.737	0.596	0.500	0.431	0.378	0.337	0.304	0.277	0.255

Momento a partir do qual o peer4 e peer5 se tornam maliciosos
Momento a partir do qual o peer6, peer7 e peer8 se tornam maliciosos
Momento a partir do qual o peer9 e peer10 se tornam maliciosos

Na análise dos dados dos peers 4 e 5, estes também são considerados confiáveis durante todo o teste, embora eles tenham se tornado maliciosos no instante t=10. Este ponto é porque $t \geq 0.7$ e equivale ao limiar estabelecido. Na perspectiva os peers 6, 7 e 8, estes são considerados confiáveis somente até t=8, e os peers 9 e 10 até o instante t=3. Neste ponto, isto acontece porque os peers já possuíam um valor relativamente alto de confiança quando eles se tornaram maliciosos (seu histórico é de bom comportamento), e a rede leva um determinado tempo para se perceber o novo comportamento dos peers, identificando-os como maliciosos. A partir desta situação, o coeficiente de confiança começa a decair, já que o valor de N é incrementado.

Relacionado com a análise do valor da confiança combinada, todos os peers são confiáveis a partir de t=1. O valor da confiança combinada aumenta ou diminui mais rapidamente que o da confiança direta, porque os valores de reputação são considerados. O

ponto em que o confidence g é maior ou igual ao limiar estabelecido (0.95) é diferente em cada conjunto de peers com o mesmo comportamento. Na perspectiva desta análise, o número de interações realizadas não foi suficiente para que esse instante pudesse ser visualizado nos resultados da tabela, já que os peers modificaram o seu comportamento.

O comportamento do peer1 ao peer3 é semelhante ao teste anterior, e eles são considerados confiáveis a partir de t=1. Os peers 4 e 5 são considerados confiáveis durante todo o teste ($t \geq 0.7$), porém o valor da confiança em t=12 é um pouco maior que o da confiança direta. Isto indica que a medida que algumas interações a mais ocorrem, a rede descobre quais peers são maliciosos. Esta percepção é lenta no início porque os valores anteriores de confiança (histórico antes da mudança de comportamento) eram bastante altos, indicando um peer considerado normal e que muda abruptamente de comportamento.

Os peers 6, 7 e 8 também são considerados confiáveis até t=8, com um coeficiente de confiança um pouco maior que o da tabela de confiança direta. Já os peers 9 e 10 são confiáveis até t=4, uma interação a mais que a análise da confiança direta. Levando em consideração a confiança combinada, a rede leva um tempo um pouco maior para se adaptar ao novo comportamento dos peers.

Na perspectiva de uma análise geral, até o instante t=4, todos os peers são confiáveis e interagem entre si. A partir de t=5 (percpeção da rede para mudança de comportamento) os peers 9 e 10 são excluídos da troca de informações e o mesmo acontece com os peers 6, 7 e 8 no instante t=9. Nesta simulação, os peers 4 e 5 são considerados confiáveis ao final deste teste (para t=12). Entretanto, com um número maior de interações, estes seriam excluídos da rede.

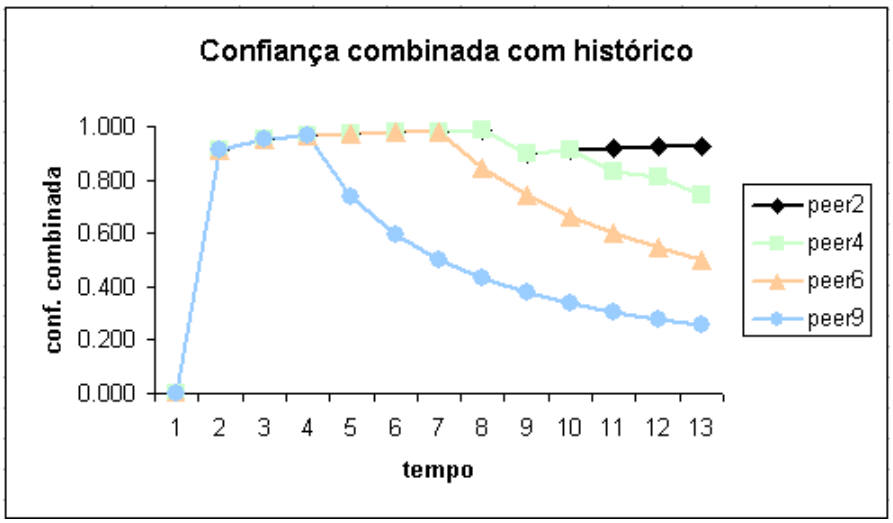


Figura 6-19 – Representação da confiança combinada com histórico

De maneira geral, o comportamento da rede se estabiliza em um ponto no qual somente os peers normais (peer1 ao peer3) são considerados confiáveis e interagem entre si. A Figura 6-19 ilustra através de um gráfico a conduta de um peer de cada conjunto com o mesmo comportamento.

Relacionado com uma análise dos resultados observados, se nota a queda do coeficiente de confiança combinada do peer2 em t=8 (onde $g \geq 0.95$) e a estabilização de seu valor próximo de 1. Nos demais casos, a queda do coeficiente de confiança ocorre no instante em que os peers mudam o seu comportamento, e segue uma tendencia de queda para valores próximos a zero.

6.2.2 Considerações para o cálculo da confiança em grupos

Para ilustrar a representação da confiança em um grupo (1:N e M:N), foram conduzidos alguns testes de maneira a obter resultados com dois focos. O primeiro com mudança de comportamento e o segundo sem esta mudança. Relacionado com a definição dos critérios dos testes, os peers ímpares compõem o grupo de origem, o que equivale ao grupo que requisita valores de confiança. Já os peers pares, equivalem ao grupo de destino, em que confiança é calculada.

Todas as tabelas apresentadas são relativas ao líder do grupo de origem (peer1). Em cada teste foram realizadas doze interações, que foi um número considerado suficiente para descrever o comportamento de um determinado grupo na rede por conta da análise dos resultados com iterações individuais (1:1). E o valor final da confiança do grupo é calculado em cada teste.

Para o cálculo da confiança no grupo existe a figura de um líder. Este líder para fins de simulação foi escolhido de maneira aleatória. Este ponto específico se deve ao fato de que o consenso da confiança e um mecanismo de eleição baseado em consenso não foram devidamente implementados, até mesmo porque necessitam de mais estudos relacionado com a perspectiva de eleição de um líder em grupos considerando critérios de confiança computacional, e não apenas de votação. Além disso é considerado que as mensagens no grupo são consideradas confiáveis e não são alteradas no seu trânsito pela rede.

6.2.3 Confiança no grupo sem mudança de comportamento

Neste teste, não havia nenhum peer malicioso e somente interações normais foram realizadas. Na sequência, os históricos de confiança foram removidos e o teste foi reiniciado com 20% dos peers do grupo sendo maliciosos. A seguir o processo foi repetido para 40% dos peers e por fim para 60% dos peers maliciosos no grupo.

Vale ressaltar que os valores de confiança calculados são referentes ao coeficiente de confiança combinada dos peers pertencentes ao grupo de destino, segundo o peer1. A confiança combinada nesta perspectiva equivale aos valores de reputação que são a parte fundamental para o cálculo da confiança em grupos segundo a proposta de como calcular a confiança em grupos.

6.2.3.1 Nenhum peer malicioso no grupo

Esta simulação foi feita como uma base de comparação para todos os outros testes relacionados à confiança de grupos. Neste caso, não existe nenhum peer malicioso no grupo e a rede se comporta de forma ideal. O valor da confiança se inicia com zero em t=0. E a medida que as iterações ocorrem, seus valores seguem aumentando no decorrer do tempo. Em t=8, a confidência g é maior ou igual ao limiar estabelecido (0.95) e as informações de reputação são consideradas na perspectiva do cálculo da confiança combinada. Neste momento, o líder do grupo de origem (peer1) passa a decidir se o grupo de destino é confiável utilizando critérios de suas próprias interações no grupo.

Como todos os nodos são iniciados ao mesmo tempo, a confiança do grupo é igual à confiança individual de cada peer do grupo, já que todos os integrantes do grupo possuem o mesmo comportamento e que a proposta de confiança para o grupo equivale ao uso de valores de reputação (utilizando dados da confiança combinada). Neste caso, o grupo é considerado bastante confiável e o seu coeficiente tende a estabilizar em um valor próximo de um. A Tabela 6-10 ilustra os resultados obtidos nesta simulação.

Tabela 6-10 – Confiança do grupo com nenhum peer malicioso

destGroup	t=0	t=1	t=2	t=3	t=4	t=5	t=6	t=7	t=8	t=9	t=10	t=11	t=12
peer2	0.000	0.857	0.917	0.941	0.955	0.963	0.968	0.973	0.900	0.909	0.917	0.923	0.929
peer4	0.000	0.857	0.917	0.941	0.955	0.963	0.968	0.973	0.900	0.909	0.917	0.923	0.929
peer6	0.000	0.857	0.917	0.941	0.955	0.963	0.968	0.973	0.900	0.909	0.917	0.923	0.929
peer8	0.000	0.857	0.917	0.941	0.955	0.963	0.968	0.973	0.900	0.909	0.917	0.923	0.929
peer10	0.000	0.857	0.917	0.941	0.955	0.963	0.968	0.973	0.900	0.909	0.917	0.923	0.929
GroupTrust	0.000	0.857	0.917	0.941	0.955	0.963	0.968	0.973	0.900	0.909	0.917	0.923	0.929

Momento em que a confiança direta é suficiente

Confiança do grupo

6.2.3.2 Um peer malicioso no grupo

Neste caso, um peer (equivalente a 20% do grupo estabelecido) se comporta de forma maliciosa. Neste teste, o valor da confiança decai para o peer malicioso e aumenta para os peers normais, e o coeficiente de confiança do grupo, mesmo com um peer malicioso, cresce e tende a estabilizar em um valor próximo de 0.8, já que os demais dos peers do grupo são confiáveis. Na perspectiva deste deste, isto ocorre porque o aumento dos coeficientes dos peers normais supera o decaimento do coeficiente do peer malicioso. Neste caso, como resultado é que o grupo também é considerado confiável ($t \geq 0.7$) embora possua um integrante malicioso.

Tabela 6-11 – Confiança do grupo com um peer malicioso

destGroup	t=0	t=1	t=2	t=3	t=4	t=5	t=6	t=7	t=8	t=9	t=10	t=11	t=12
peer2	0.000	0.857	0.917	0.941	0.955	0.963	0.968	0.973	0.900	0.909	0.917	0.923	0.929
peer4	0.000	0.857	0.917	0.941	0.955	0.963	0.968	0.973	0.900	0.909	0.917	0.923	0.929
peer6	0.000	0.857	0.917	0.941	0.955	0.963	0.968	0.973	0.900	0.909	0.917	0.923	0.929
peer8	0.000	0.857	0.917	0.941	0.955	0.963	0.968	0.973	0.900	0.909	0.917	0.923	0.929
peer10	0.000	0.143	0.083	0.059	0.045	0.037	0.031	0.027	0.100	0.091	0.083	0.077	0.071
GroupTrust	0.000	0.714	0.750	0.765	0.773	0.778	0.781	0.784	0.740	0.745	0.750	0.754	0.757

Peers maliciosos
Momento em que a confiança direta é suficiente
Confiança do grupo

6.2.3.3 Dois peers maliciosos no grupo

Tabela 6-12 – Confiança do grupo com dois peers maliciosos

destGroup	t=0	t=1	t=2	t=3	t=4	t=5	t=6	t=7	t=8	t=9	t=10	t=11	t=12
peer2	0.000	0.857	0.917	0.941	0.955	0.963	0.968	0.973	0.900	0.909	0.917	0.923	0.929
peer4	0.000	0.857	0.917	0.941	0.955	0.963	0.968	0.973	0.900	0.909	0.917	0.923	0.929
peer6	0.000	0.857	0.917	0.941	0.955	0.963	0.968	0.973	0.900	0.909	0.917	0.923	0.929
peer8	0.000	0.143	0.083	0.059	0.045	0.037	0.031	0.027	0.100	0.091	0.083	0.077	0.071
peer10	0.000	0.143	0.083	0.059	0.045	0.037	0.031	0.027	0.100	0.091	0.083	0.077	0.071
GroupTrust	0.000	0.571	0.583	0.588	0.591	0.593	0.593	0.595	0.580	0.582	0.583	0.585	0.586

Peers maliciosos
Momento em que a confiança direta é suficiente
Confiança do grupo

Nesta simulação, dois peers do grupo (o que equivale a 40% do grupo) se comportam de forma maliciosa. E na perspectiva de análise dos dados obtidos, o valor da confiança decai para os peers maliciosos e aumenta para os peers normais. Já o coeficiente de confiança do grupo, com dois peers maliciosos, cresce e tende a estabilizar em um valor próximo de 0.6,

considerando que os demais peers são normais. Neste caso, o aumento dos coeficientes dos peers normais não supera o decaimento dos coeficientes do peers maliciosos e como resultado o grupo não é considerado confiável segundo o limiar estabelecido ($t < 0.7$).

6.2.3.4 Três peers maliciosos no grupo

Neste teste, três peers do grupo (o que equivale a 60%) se comportam de forma maliciosa. Na sequência de execuçao dos testes, o valor da confiança decai para os peers maliciosos e aumenta para os peers normais e o coeficiente de confiança do grupo com três peers maliciosos decai e tende a estabilizar em um valor próximo de 0.4. Da mesma maneira que o teste anterior, o aumento dos coeficientes dos peers normais não supera a queda dos coeficientes do peers maliciosos. Como resultado o grupo também não é considerado confiável ($t < 0.7$).

Tabela 6-13 – Confiança do grupo com três peers maliciosos

destGroup	t=0	t=1	t=2	t=3	t=4	t=5	t=6	t=7	t=8	t=9	t=10	t=11	t=12
peer2	0.000	0.857	0.917	0.941	0.955	0.963	0.968	0.973	0.900	0.909	0.917	0.923	0.929
peer4	0.000	0.857	0.917	0.941	0.955	0.963	0.968	0.973	0.900	0.909	0.917	0.923	0.929
peer6	0.000	0.143	0.083	0.059	0.045	0.037	0.031	0.027	0.100	0.091	0.083	0.077	0.071
peer8	0.000	0.143	0.083	0.059	0.045	0.037	0.031	0.027	0.100	0.091	0.083	0.077	0.071
peer10	0.000	0.143	0.083	0.059	0.045	0.037	0.031	0.027	0.100	0.091	0.083	0.077	0.071
GroupTrust	0.000	0.429	0.417	0.412	0.409	0.407	0.406	0.405	0.420	0.418	0.417	0.415	0.414

Peers maliciosos
Momento em que a confiança direta é suficiente
Confiança do grupo

6.2.4 Confiança no grupo com mudança de comportamento

Na segunda simulação, interações anteriores são consideradas (gerando um histórico dos dados) e os peers passam a ser maliciosos em momentos pré-determinados. Em um primeiro momento o peer10 em t=2 (o que equivale a 20% do grupo). No segundo momento os peers peer8 e peer10 em t=4 (o que equivale a 40% do grupo). E por fim o peer6, peer8 e peer10 em t=7 (60% do grupo). No início deste teste, não existe nenhum peer malicioso e a rede se comporta de forma ideal. O valor da confiança de cada peer se inicia com zero (t=0). E durante a execução do teste, entra em queda para os peers maliciosos e aumenta para os peers normais. O comportamento do peer2 e peer4 é semelhante ao teste anterior (sem mudança de comportamento), e eles são considerados confiáveis a partir de t=1. Já o peer6,

por sua vez, é visto como confiável até o instante t=8. O peer8 até o instante t=4 e o peer 10 somente em t=1.

A partir do cálculo da confiança no grupo, utilizando valores de reputaçao associados aos da confiança combinada de cada peer, o grupo é considerado confiável até t=6. Do instante t=7 a seguir, o grupo deixa de ser considerado confiável e a comunicação do grupo de origem este grupo deixa de ocorrer porque o critério de confiança mínimo não é mais suficiente. Ao final do teste, a confiança do grupo tende a estabilizar em um valor próximo de 0.4 (o que equivale a 40% do grupo ser confiável). E nesta perspectiva, este grupo é isolado e como tal deixa de ser um ponto de troca de informações da rede.

Tabela 6-14 – Confiança do grupo com histórico e mudança de comportamento

destGroup	t=0	t=1	t=2	t=3	t=4	t=5	t=6	t=7	t=8	t=9	t=10	t=11	t=12
peer2	0.000	0.857	0.917	0.941	0.955	0.963	0.968	0.973	0.900	0.909	0.917	0.923	0.929
peer4	0.000	0.857	0.917	0.941	0.955	0.963	0.968	0.973	0.900	0.909	0.917	0.923	0.929
peer6	0.000	0.857	0.917	0.941	0.955	0.963	0.968	0.838	0.700	0.636	0.583	0.538	0.500
peer8	0.000	0.857	0.917	0.941	0.727	0.593	0.500	0.432	0.400	0.364	0.333	0.308	0.286
peer10	0.000	0.857	0.500	0.353	0.273	0.222	0.188	0.162	0.200	0.182	0.167	0.154	0.143
GroupTrust	0.000	0.857	0.834	0.823	0.773	0.741	0.718	0.676	0.620	0.600	0.583	0.569	0.557

Momento a partir do qual o peer6 se torna malicioso
Momento a partir do qual o peer8 se torna malicioso
Momento a partir do qual o peer10 se torna malicioso
Confiança do grupo

A Figura 6-20 ilustra através de um gráfico, o comportamento do coeficiente de confiança combinada (utilizando critérios de reputação) dos peers pertencentes ao grupo de destino. Além disso ilustra o comportamento da confiança do grupo relacionado com as iterações no decorrer do tempo.

Na análise correpondente do gráfico, se nota que o valor da confiança do grupo inicia alto (momento em que todos os peers têm bom comportamento). Na sequência começa a decair a partir do momento em que o primeiro peer do grupo passa a ser malicioso (indicativo de alguma anomalia do comportamento do grupo). Nos instantes seguintes em que os peers mudam de comportamento, o coeficiente do grupo entra em queda mais rapidamente. Considerando os critérios utilizados e os coeficientes de resultados da confiança, se nota que a tendência é de estabilizar em um limiar próximo de 0,4.

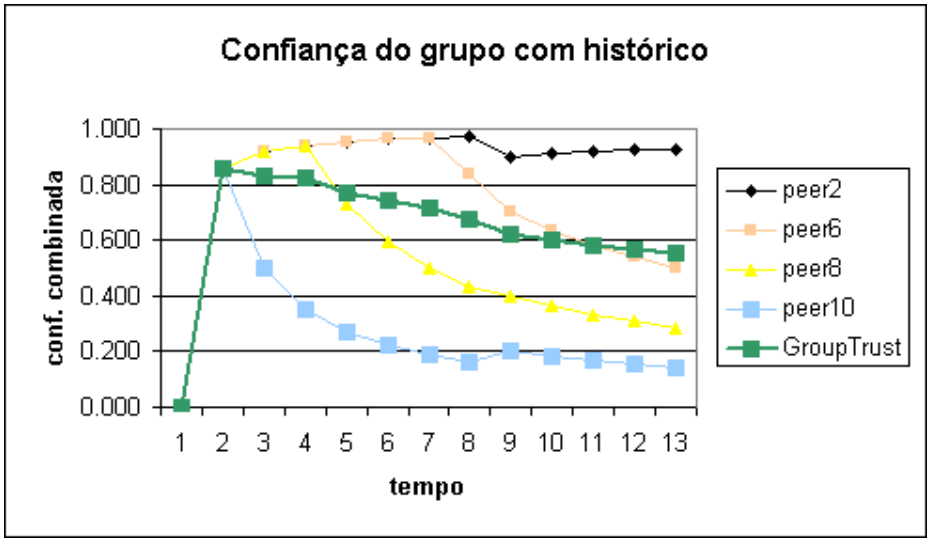


Figura 6-20 – Resultados para confiança em um grupo com histórico

6.3 SÍNTESE DO CAPÍTULO

O objetivo deste capítulo foi demonstrar e analisar os resultados decorrentes da implementação da proposta deste trabalho na perspectiva de grupos e sua aplicação em sistemas distribuídos. Como modelo de sistemas distribuídos foi implementado a proposta em ambientes de agentes de software, simulando um grid em um ambiente com P2P.

Como segunda característica, foi realizada uma implementação da proposta em ambientes com agentes de software, demonstrando alguns pontos de como usar a confiança e a importância de índices de avaliação da confiança.

Como terceira característica foi implementada a proposta em sistemas P2P que, da mesma maneira que os agentes de software, se obteve resultados na perspectiva da confiança e da sua aplicação em sistemas distribuídos.

Dentro de uma perspectiva geral, os resultados demonstram a análise da aplicação da confiança e da reputação em sistemas distribuídos e com a consideração do seu uso em grupos, segundo a proposta do modelo elaborado. Nos resultados, foi possível perceber como o comportamento individual de cada membro influencia na confiança do grupo como um todo porque o coeficiente de confiança do grupo é calculado segundo valores dados pelos coeficientes de confiança individuais de cada peer do grupo.

7 CONCLUSÕES

O eixo articulador do presente trabalho é a elaboração de uma proposta de um modelo de confiança e reputação que possa ser utilizado nas interações envolvendo grupos de entidades em sistemas distribuídos. Além de buscar equacionar a questão central da confiança e da reputação nessa situação, o presente trabalho procura também discutir as questões correlatas cuja solução contribui para o tratamento do tema, o que inclui a questão da identificação das entidades e a proteção das trocas de informação relativas à confiança e à reputação.

Acerca do objetivo focal deste trabalho, se definiu um modelo capaz de utilizar critérios de confiança e reputação para grupos, podendo ser aplicado nas interações entre entidades individuais e grupos (1:N), ou nas interações de grupo para grupo (M:N). Uma das características do modelo aqui proposto é a presença de um líder, entidade que representa um grupo e que deve ser então definida no contexto de um grupo, por intermédio de algum processo de escolha, seleção ou eleição.

O modelo proposto foi objeto de duas implementações que permitiram realizar várias avaliações referentes à sua efetividade e utilidade. A primeira implementação foi feita em ambiente Jade, que se mostrou uma boa opção de implementação de agentes de software para a simulação de ambientes que possam utilizar critérios de confiança e reputação. A segunda implementação foi realizada em JXTA, que apesar de possuir certa instabilidade, pode ser considerado bastante flexível e estruturado, emulando perfeitamente uma rede P2P descentralizada.

Nas duas implementações, foi operacionalizado, como referencial para a análise do modelo aqui proposto, um modelo básico de gerência da confiança (TRAVOS) utilizada para gerar valores de confiança e reputação utilizáveis por entidades individuais, mas não por grupos, ao menos em sua forma inicial. Esse é um modelo que possui vantagens funcionais, por ser portável e poder ser utilizado nas plataformas estudadas de ambientes distribuídos, além de poder ser desenvolvido em qualquer linguagem de programação atual. Tal modelo reage a mudanças de comportamento, permitindo identificar nodos maliciosos. Foram observadas outras características interessantes relacionadas ao modelo. Por exemplo, quando considerado um Grid que foi inicializado há pouco tempo, verificou-se que, quando nenhum nodo na rede possui qualquer informação, isso implica que em uma primeira interação existe

o risco de ser feita com nodo malicioso. Por outro lado, um nodo que ainda não interagiu na rede, recebe informações sobre reputação, mas não possui nenhuma base de interações pessoais para compor a confiança combinada entre sua experiência direta e os dados de reputação, que são informações indiretas sobre a confiança. Para resolver estes dois problemas, a proposta de um desafio anterior à primeira interação cria a possibilidade de avaliar se um nodo pode realizar a tarefa (o desafiante é capaz de verificar se a resposta do desafiado é válida) e ao mesmo tempo cria a base de avaliações pessoais. Além disso, nota-se pelo modelo que quando duas opiniões iguais são combinadas, elas geram uma resultante maior se forem positivas, ou uma menor, se negativas. Essa consideração se deve ao fato de que quanto mais informações coerentes existirem sobre um determinado nodo, mais confiável ele se tornará. Além do que, opiniões divergentes só atrapalham e, por isso, acabam preteridas.

Considerando tal referencial estabelecido nas duas implantações, os diversos experimentos de validação que foram realizados mostraram que a modelo de confiança para grupos aqui proposto mostrou-se capaz de criar a representação da confiança em um grupo, o que pode ser explorado em uma perspectiva de um nodo ou de vários nodos. Vale ressaltar que o modelo, após diversas observações de comportamento, também pode determinar o comportamento de um grupo sendo malicioso em função dos comportamentos individuais de seus membros. Vale notar que, no modelo proposto, no que se refere aos aspectos de liderança, se supõe que o líder é um nodo de bom comportamento e que não irá agir maliciosamente objetivando obter algum tipo de vantagem. Esta consideração coloca em questão a seguinte situação: se um nodo muda de comportamento após certo instante t, e passa a fornecer resultados errados para as tarefas a ele delegadas, com o intuito de prejudicar o nodo que lhe requisita tarefas. Nessa situação, o nodo atingido é o primeiro a perceber essa mudança comportamental e passa a reportar o mau comportamento para os nodos da rede. Porém, no caso de nodos que recebem essa opinião e ainda possuem um bom histórico de interações com o nodo mal comportado (referente ao momento anterior a t), podem não acreditar na opinião recebida. Por isso, um modelo de confiança deve prever um mecanismo para reconhecer a mudança de comportamento de um nodo que evite que as opiniões sinceras sobre um nodo que muda de comportamento sejam interpretadas como opiniões desonestas em função do histórico.

As implementações e os experimentos de validação permitiram também analisar os aspectos correlatos ao tema da proposta central de confiança em grupos. Com a implementação de um modelo de confiança dessa natureza, é possível fazer a avaliação de

diversos outros aspectos em um ambiente distribuído e que estão ligados diretamente com a segurança da informação. Dentre esses, o principal aspecto é o de que a confiança e a reputação, sejam individuais ou em grupos, afetam a disponibilidade. Isto ocorre porque utilizando um critério a mais de análise, o nodo pode decidir garantir ou negar acesso ao recurso solicitado baseado em métricas de confiança. De maneira simplificada seria equivalenta a dizer que se uma entidade não tiver um valor mínimo de confiança estabelecido, mesmo autenticada e autorizada, o recurso ainda será negado mediante fatores relacionados à confiança. Nesse sentido, a questão da autenticação e autorização, que normalmente são utilizadas para os requisitos de disponibilidade de serviços de rede, podem ganhar um reforço extra na avaliação do comportamento e nas questões relacionadas diretamente com a confiança e a reputação (histórico, contexto, limiar de confiança, o que estará disponível em cada limiar etc.).

Como a confiança e a reputação são conceitos abstratos e dependem de uma série de inferências, a aplicação da confiança e da reputação fica evidentemente associada ao comportamento dos nodos e, assim, permite que a disponibilidade seja vista com o auxílio de mais de um critério além da autorização e autenticação. Esse aspecto impacta diretamente na disponibilidade da segurança da informação porque quando um nodo é identificado como não confiável, o acesso ao recurso pode ser negado, mesmo sendo um nodo autenticado e autorizado ao recurso. A mesma avaliação cabe no modelo de confiança de grupos.

Outro ponto que merece análise é a avaliação feita por um modelo de confiança, de que seja capaz de neutralizar a opinião fornecida por um nodo malicioso em uma rede. Estendendo este ponto para o conceito de grupos, escalona-se a solução para auxiliar de maneira mais efetiva os nodos bons que conseguem identificar nodos ruins e isolá-los da comunicação legítima e dos serviços relacionados. Entretanto, essa possibilidade depende de uma correta identificação dos nodos.

Por essa razão, considerando os aspectos de identificação de um nodo na rede, a análise de um protocolo de identificação durante a implementação deste trabalho, permitiu levantar critérios em que somente a possibilidade de apresentação de uma identidade não é um ponto de acordo. Devem existir critérios de verificação da identidade apresentada, de alguma maneira relacionada a um histórico ou a um conhecimento prévio do nodo, por exemplo, considerando a troca de informações passadas em interações que auxiliem a identificar as entidades da comunicação.

Assim, no que é relacionado com o tratamento de critérios da segurança, especificamente de confidencialidade e integridade, verificou-se que existe a necessidade de

implementação de funcionalidades de segurança imprescindíveis ao envio e recebimento de mensagens de confiança e reputação na rede. Isso posto, a proposta do modelo criado alcançou em parte esses objetivos.

Enfim, vale notar que as contribuições da implementação e da revisão de aspectos de confiança e reputação possibilitam o uso deste trabalho como referência para a confiança e a reputação em ambientes distribuídos considerando grupos, além de apresentar uma implementação em padrões abertos.

7.1 TRABALHOS FUTUROS

Como propostas de trabalhos futuros são indicados alguns pontos que podem ser evoluídos.

Existe a necessidade de desenvolver um mecanismo para gerenciar a identidade de um nodo em um ambiente distribuído, porque é complexo averiguar se um nodo é realmente quem ele diz ser sem critérios de uma unidade de controle centralizado. Por exemplo, considerando critérios de confiança e reputação relacionados com a disponibilidade, um nodo com má reputação poderá assumir a identidade de um com boa reputação, burlando a confiança e por fim aumentando suas chances de uso de mais recursos.

Outro ponto em aberto são as considerações sobre o consenso da confiança e da reputação. Os nodos de alguma maneira devem concordar sobre confiar ou não confiar além de limiares previamente definidos. O consenso, assim como a confiança e a reputação, deve ser dinâmico e evoluir com o tempo. Além disso, estabelecer métricas, protocolos e modelos de escolha dos líderes em um grupo.

A comunicação segura entre os membros de um grupo também não foi implementado. Isto indica que existe a possibilidade de avaliar alguns modelos de troca de informações tratando a confidencialidade e integridade sem uma autoridade central de controle em um ambiente distribuído. Esta implementação permitiria a troca de valores de confiança e reputação sem o risco de serem alterados no seu trânsito pela rede, até mesmo porque apesar da confiança e da reputação usarem critérios individuais para seu cálculo, estes devem ser trocados de alguma maneira na rede, existindo a necessidade da integridade e confidencialidade no caminho da rede em um ambiente distribuído.

7.2 PUBLICAÇÕES

1. Albuquerque, Robson de Oliveira; Cohen, Fernanda Fontes; Mota, Jovelina Lima Teixeira; de Sousa Júnior, Rafael Timóteo; “Analysis of a trust and reputation model applied to a computational Grid using software agents”. International Conference on Convergence and Hybrid Information Technology – ICHIT 2008 – August 28th - 29th, Daejeon, Korea. Proceedings with IEEE CS. Paper accepted for publication as a regular paper.

2. de Sousa Júnior, Rafael Timóteo; Albuquerque, R. O. ; Hanashiro, Maíra; Silva, Yamar Aires da; Gondim, Paulo Roberto de Lira. “Towards establishing trust in MANET: an integrated approach for auto-configuration, authentication and certification”. The International Journal of Forensic Computer Science, Brasil, v. 1, p. 33 - 40, 06. November 2006.

3. Albuquerque, Robson de Oliveira; Hanashiro, Maíra; de Sousa Junior, Rafael Timóteo; Abbas, Claudia Jacy Barenco; Villalba, Luis Javier García; “Manet - Autoconfiguration with Distributed Certification Authority Models Considering Routing Protocols Usage”. In: Edudardo Fernández-Medina; Julio César Hernández; Luis Javier García. (Org.). Security in Information Systems - WOSIS 2005. Portugal: INSTICC PRESS, 2005, v. 1, p. 57-66.

4. Albuquerque, Robson de Oliveira; Silva, Tamer Américo da; de Sousa Júnior, Rafael Timóteo; “Ambiente Baseado em agentes de software para o auxílio na detecção e estudo de ataques em redes de computadores”. In: Departamento de Polícia Federal. (Org.). ICCYBER'2004 Proceedings of the 1st International Conference on Cyber Crime Investigation. Brasília: SEGRAF-DPF, 2004, v. 1, p. 156-161.

5. Albuquerque, Robson de Oliveira; de Sousa Júnior, Rafael Timóteo; Hanashiro, Maíra; Silva, Yamar Aires da; Gondim, Paulo Roberto de Lira; “Manet auto configuration with distributed certification authority models considering routing protocols use”. In: Departamento de Polícia Federal. (Org.). ICCyber'2004 Proceedings of the 1st International Conference on Cyber Crime Investigation. 1 ed. Brasília: SEGRAF-DPF, 2004, v. 1, p. 188-195.

6. Albuquerque, Robson de Oliveira; de Sousa jr, Rafael Timóteo; Puttini, Ricardo Staciarini; Silva, Tamer Américo da; “Survivability for a Network Service and Load Balancing using Intelligent Agents Software”. Lecture Notes in Computer Science, Japão, v. 3207, p. 734 - 744, 25. August 2004.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Olson, Doug; Cowles, Robert; Mullen, Shawn; Helm, Mike. “Grid Trust Model for CA Signed Identity Certificates”. Global Grid Forum. Grid Certificate Policy Working Group, July 2000.

[2] Thompson, Mary R.; Olson, Doug; Cowles, Robert; Mullen, Shawn; Helm, Mike. “CA-based Trust Issues for Grid Authentication and Identity Delegation.” Grid Certificate Policy Working Group, June 2003.

[3] Patel, Jigar. “A Trust and Reputation Model for Agent-Based Virtual Organizations”. Thesis of Doctor of Philosophy. Faculty of Engineering and Applied Science. School of Electronics and Computer Science. University of Southampton. January 2007.

[4] Sabater, Jordi; Sierra, Carles. “Reputation and social network analysis in multiagent systems.” Proceedings of The First International Joint Conference on Autonomous Agents & Multiagent Systems, pages 475–482, ACM, Italy, 2002.

[5] Suryanarayana, Girish; Taylor, Richard N. “A Survey of Trust Management and Resource Discovery Technologies in Peer-to-Peer Applications.” Institute for Software Research, University of California, ISR Technical Report # UCI-ISR-04-6, July 2004.

[6] Gaston, Matthew E.; desJardins, Marie. “Social Networks and Multi-agent Organizational Performance”. Department of Computer Science. University of Maryland Baltimore County. Acessado em 20/03/2006. Disponível em www.csee.umbc.edu/~mgasto1/papers/gaston-flairs05.pdf.

[7] Gambetta, Diego. ‘Can We Trust Trust?’, in Gambetta, Diego (ed.) Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford, chapter 13, pp. 213-237, 2000.

[8] Lamsal, Pradip. “Understanding Trust and Security”. Department of Computer Science University of Helsiki, Finland, October 2001. Acessado em 13/02/2006. Disponível em http://www.cs.helsinki.fi/u/lamsal/asgn/trust/UnderstandingTrustAndSecurity.pdf.

[9] Marsh, Stephen Paul. “Formalizing Trust as a Computational Concept”. Department of Computing Science and Mathematics, University of Stirling. Doctorate Thesis. April 1994.

[10] Dasgupta, Partha. ‘Trust as a Commodity’, in Gambetta, Diego (ed.) Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology,

University of Oxford, chapter 4, pp. 49-72, 2000 . Acessado em 15/02/2006. Disponível em http://www.sociology.ox.ac.uk/papers/dasgupta49-72.doc.

[11] Seigneur, Jean-Marc. “Trust, Security and Privacy in Global Computing”. University of Dublin, Trinity College, Doctorate Thesis in Computer Science, March 2005.

[12] Douceur, John R. “The Sybil Attack”. Proceedings of the IPTPS02 Workshop, Cambridge, March 2002.

[13] de Sousa Jr, Rafael Timóteo; Albuquerque, Robson de Oliveira; Hanashiro, Maíra; da Silva, Yamar Aires; Gondim, Paulo Roberto de Lira. “Towards Establishing Trust in MANET: an Integrated Approach for Auto-configuration, Authentication and Certification.” The International Journal of Forensic Computer Science, Volume 1, Number 1, 2006.

[14] Papalilo, Elvis; Freisleben, Bernd. “Towards a Flexible Trust Model for Grid Environments”. Lecture Notes in Computer Science. Springer Berlin/Heidelberg Volume 3270, 2004.

[15] Wang, Li; Wu, Wenli; Li, YingJie; Yu, XueLi. “Content-aware Trust Statement for semantic Grid”. Proceedings of the Second International Conference on Semantics, Knowledge, and Grid. IEEE, 2006.

[16] Duma, C.; Shahmehri, N.; Caronni, G. “Dynamic trust metrics for peer-to-peer systems”. Proceedings on Sixteenth International Workshop on Database and Expert Systems Applications, Pages: 776 – 781, Volume, Issue, August 2005.

[17] Poggi, Agostino; Tomaiuolo, Michele; Vitaglione, Giosuè. “A Security Infrastructure for Trust Management in Multi-agent Systems”. Proceedings of the International Joint Conference on Autonomous Agents and Multiagent Systems. Lecture Notes in Computer Science, volume 3577, pages 162-179, Netherlands 2005.

[18] Wang, Yao; J., Vassileva. “Trust-Based Community Formation in Peer-to-Peer File Sharing Networks”. Proceedings of IEEE/WIC/ACM International Conference on Web Intelligence,. Page(s): 341 – 348. September 2004.

[19] de Sousa Jr, Rafael Timóteo; Albuquerque, Robson de Oliveira; Prado, Ricardo Queiroz; Rodrigues, Guilherme Coelho; Puttini, Ricardo Staciarini. “Emprego do paradoxo do aniversário para estimar o máximo esforço de um ataque bem sucedido contra um protocolo de identificação”. I2TS'2006 - 5th International Information and Telecommunication Technologies Symposium, 2006, Cuiabá, MT – Brazil.

[20] Elser, Benedikt. “Managing Trust in a Distributed Network”. University of Munich, Institute of Informatics. Germany. Approved Thesis. March 2006.

[21] Ferreira, Aurélio Buarque de Holanda. “Novo Dicionário Aurélio da Língua Portuguesa”. Editora: Positivo – Livros. ISBN: 8574724149. 3ª Edição, 2004.

[22] IBM. “IBM Solutions Grid for Business Partners: Helping IBM Business Partners to Grid-enable applications for the next phase of e-business on demand”. Acessado em 17/02/2006. Disponível em http://www-304.ibm.com/jct09002c/isv/marketing/emerging/grid_wp.pdf.

[23] Fox, G., Pierce, M., Gannon, D., Thomas, M. “Overview of Grid Computing Environments”. Global Grid Forum, February 2002.

[24] Ferreira, Luis; Berstis, Viktors; Armstrong, Jonathan; Kendzierski, Mike; Neukoetter, Andreas; Takagi, Masanobu; Bing-Wo, Richard; Amir, Adeeb; Murakawa, Ryo; Hernandez, Olegario; Magowan, James; Bieberstein, Norbert. “Introduction to Grid Computing with Globus.” IBM RedBooks, September 2003.

[25] The Globus Alliance. Acessado em 19/02/2006. Disponível em http://www.globus.org/.

[26] OurGrid. Acessado em 19/02/2006. Disponível em http://www.ourgrid.org/.

[27] Pernas, Ana Marilza; Dantas, Mario. “Grid Computing Environment Using Ontology Based Service”. ICCS 2005 - Lecture Notes in Computer Science ISSN 0302-9743. Volume 3516/2005. Pages 858-861. May 2005.

[28] The OpenSSL project. “OpenSSL: The Open Source toolkit for SSL/TLS.” Acessado em 15/03/2006. Disponível em http://www.openssl.org.

[29] Basney, J., Nejdl, W., Olmedilla, D., Welch, V. and Winslett, M. “Negotiating Trust on the Grid”. University of Illinois and National Center for Supercomputer Applications, 2004, USA.

[30] Jensen, Finn V. “Bayesian Networks and Decision Graphs”. Information Science and Statistics. Springer Verlag. ISBN 0387952594. 2001.

[31] Tran, H.; Watters, P.; Hitchens, M.; Vijay Varadharajan. “Trust and authorization in the grid: a recommendation model. Proceedings of the International Conference on Pervasive Services. Pages: 433 – 436. Volume, Issue, July, 2005.

[32] Bowman, R.S.; Hexmoor, H. “Agent collaboration and social networks”. International Conference on Integration of Knowledge Intensive Multi-Agent Systems. Volume, Issue, Pages: 211-214. April 2005.

[33] Ferreira, E. C., Schulze, B. “Análise da Infra-estrutura de Segurança na Arquitetura Aberta de Serviços de Grid”. Laboratório Nacional de Computação Científica. Março de 2004.

[34] Li, Tieyan; Zhu, HuaFei; Lam, Kwok-Yan. "A Novel Two-level Trust Model for Grid". Lecture Notes on Computer Science in the Fifth International Conference on Information and Communications Security (ICICS), Huhehaote city, China. October 2003.

[35] Rocha, Rafael R. da; "Redes Peer-to-Peer para Compartilhamento de Arquivos na Internet". Grupo de Teleinformática e Automação PEE/COPPE - DEL/POLI. Universidade Federal do Rio de Janeiro – Rio de Janeiro – Brasil. Acessado em 25/03/2006. Disponível em http://www.gta.ufrj.br.

[36] Stoica, Ion; Morris, Robert; Liben-Nowelly, David; Karger, David; Kaashoek, M. Frans; Dabek; Frank; Balakrishnan, Hari. "Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications". In: Proceedings of SIGCOMM 2001.

[37] Ge, Z.; Figueiredo, D. R.; Jaiswal, S.; Kurose, J.; Towsley; D. "Modeling Peer-to-Peer File Sharing Systems". In: Proceedings of INFOCOMM 2003.

[38] Napster Free. Acessado em 26/03/2006. Disponível em http://free.napster.com/.

[39] Schollmeier; Rüdiger. "A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications". Institute of Communication Networks, Technische Universität München. Germany. Acessado em 27/03/2006. Disponível em http://csdl2.computer.org/comp/proceedings/p2p/2001/1503/00/15030101.pdf.

[40] JXTA. "JXTA – Get Connected". Acessado em 30/03/2006. Disponível em http://www.jxta.org.

[41] Aberer, Karl; Despotovic, Zoran. "Managing trust in a peer-2-peer information system". Proceedings of the tenth international conference on Information and knowledge management. Pages: 310 – 317, Atlanta, USA, 2001.

[42] Ngan, T.; Wallach, D.; Druschel, P. "Enforcing Fair Sharing of Peer-to-peer Resources". Second International Workshop on Peer-to-Peer Systems. Berkeley, California. February 2003.

[43] Nelson, Robert and Pitigoi-Aron, Gruia. "P2P Trust Infrastructure". Computer Science Division, University of California, Los Angeles, USA. Acessado em 18/03/2006. http://www.cs.ucla.edu/~rlnelson/trust.pdf.

[44] Aberer, Karl; Cudré-Mauroux, Philippe; Datta, Anwitaman; Despotovic, Zoran; Hauswirth, Manfred; Punceva, Magdalena; Schmidt, Roman. "P-Grid: A Self-organizing Structured P2P System". International Conference on Management of Data/Principles of Database Systems, San Diego, California. June 2003.

[45] Caceres, Cesar; Fernandez, Alberto; Ossowski, Sascha; Vasirani, Matteo. “An Abstract Architecture for Service Coordination in IP2P Environments”. International Workshop on Computer Supported Activity Coordination Artificial Intelligence at International Conference on Enterprise Information Systems, Cyprus. May 2006.

[46] Wooldridge, M.; Jennings, N.R. “Intelligent Agents: Theory and Practice” - Knowledge Engineering Review, October 1994.

[47] Morreale, Patrícia. “Agents on the Move” IEEE Spectrum - April 1998.

[48] Nwana, Hyacinth S.; “Software Agents: An Overview”. Intelligent Systems Research AA&T, BT Laboratories. 2000.

[49] The Foundation for Intelligent Physical Agents. Acessado 25/03/2006. Disponível em: http://www.fipa.org.

[50] Gruber, Thomas R. “A Translation Approach to Portable Ontology Specifications”. Knowledge Acquisition, 5 (2):199-220, 1993.

[51] Silva, Tamer A. da; Albuquerque, Robson de O.; Buiati, Fabio M.; Puttini, Ricardo S.; de Sousa, Rafael T. “A Community of Agents for Trapping Attacks Against Network Services and Redirecting Traffic Attacks to a Honeynet”. International Conferences on Internet Technologies and Applications (ITA 05) ISBN: 0-94688-132-4. Wrexham, North Wales, UK. September 2005.

[52] Zhang, Xiaoqin; Xu, Haiping. “Towards Automated Development of Multi-Agent Systems Using RADE”. “Towards Automated Development of Multi-Agent Systems Using RADE”. Proceedings of the International Conference on Artificial Intelligence. Volume I e II, pages: 44-50, EUA. June 2006.

[53] Poggi, Agostino; Tomaiuolo, Michele; Vitaglione, Giosuè. “Do Agents Need Certificates? Distributed Authorization to Improve JADE Security”. 6th Workshop on Trust, Privacy, Deception and Fraud In Agent Societies. Melbourne 2003.

[54] Telecom Lab. Itália, “Jade - Java Agent DEvelopment Framework”. Acessado em 28/03/2006. Disponível em http://jade.tilab.com/.

[55] Ramchurn, Sarvapali D.; Jennings, Nicholas R.; Sierra, Carles; Godo, Lluis. “A Computational Trust Model for Multi-Agent Interactions Based on Confidence and Reputation”. 6th Workshop on Trust, Privacy, Deception and Fraud in Agent Societies. Melbourne 2003.

[56] IEEE Workgroup - Mobile Ad-hoc Networks (MANET) – Acessado em 13/03/2006. Disponível em http://www.ietf.org/html.charters/manet-charter.html.

[57] Amvame-nze, Georges. “Reconfiguração dinâmica de agentes móveis ipv4 em redes sem fio ad hoc”. Tese de doutorado, publicação ppgene.td - 012/06. Departamento de engenharia elétrica, Universidade de Brasília, Brasília, DF, 147p. 2006.

[58] Xiaoqi, Li. “Trust Model Based Self-Organized Routing Protocol for Secure Ad Hoc Networks”. The Chinese University of Hong Kong - Department of Computer Science and Engineering - Ph.D. - Term Paper. April 2003.

[59] Gligor, Virgil D. “Security of Emergent Properties in Ad-Hoc Networks.” Electrical and Computer Engineering Department - University of Maryland.

[60] Shamir, A. “How to Share a Secret”, Communications of the ACM, v. 22(11), pp. 612-613, 1979.

[61] Adnane, Asmaa; de Sousa Jr., Rafael Timóteo; Bidan, Christophe; Me; Ludovic. “Analysis of the implicit trust within the OLSR protocol”. IFIP Networking – Canada, 2007.

[62] Hughes, Todd; Denny, James; Muckelbauer; P. Andy. “Dynamic Trust Applied to Ad Hoc Network Resources”. Lockheed Martin Advanced Technology Laboratories. Executive Campus. Cherry Hill. USA.

[63] Blythe, Jim; McGrath, Cathleen; Krackhardt, David. “The Effect of Graph Layout on Inference from Social Network Data”. Lecture Notes in Computer Science. Proceedings of Graph Drawing 1995: 40-51. Germany, September 1995.

[64] Social Network References. Acessado em 23/05/2006. Disponível em http://www.socialnetworks.org/.

[65] Sabater, Jordi; Sierra, Carles. “Review on Computational Trust and Reputation Models”. Artificial Intelligence Review (2005) 24:33–60, Springer 2005.

[66] Wang, Ye Diana; Emurian, Henry H. “An overview of online trust: Concepts, elements, and implications.” Information Systems Department, College of Engineering and Information Technology, UMBC, USA, February 2004.

[67] Beth, T.; Borcherding, M.; Klien, B. “Valuation of Trust in Open Networks”. Proceedings of the European Symposium on Research in Computer Security, Brighton, UK. 1994.

[68] Castelfranchi, Cristiano; Falcone, Rino. “Social Trust: A Cognitive Approach”. National Research Council - Institute of Psychology. Unit of "AI, Cognitive Modelling and Interaction". Roma – Italy. Acessado em 25/04/2006. Disponível em http://www.istc.cnr.it/T3/download/Social-trust.pdf.

[69] Johnson, Devon; Grayson, Kent. “Cognitive and affective trust in service relationships”. Elsevier Journal of Business Research 58 (2005) 500– 507.

[70] Dunn, Paul. “The Importance of Consistency in Establishing Cognitive-based Trust: A Laboratory Experiment”. Journal Teaching Business Ethics, Springer Netherlands, ISSN 1382-6891, Volume 4, Number 3, Pages 285-306. August 2000.

[71] Huynh, T. D.; Jennings, N. R.; Shadbolt N. R. “An integrated trust and reputation model for open multi-agent systems”. Autonomous Agents and Multi-Agent Systems, 13(2):119–154, 2006.

[72] Ramchurn S. D. “Multi-Agent Negotiation using Trust and Persuasion”. PhD thesis, Electronics and Computer Science, University of Southampton, UK, 2004.

[73] Yu, B; Singh, M. P. “An evidential model of distributed reputation management”. In AAMAS’02: Proceedings of the first international joint conference on Autonomous agents and multiagent systems, pages 294–301. ACM Press, 2002.

[74] eBay - New & used electronics, cars, apparel, collectibles, sporting goods & more at low prices. Acessado em 30/04/2006. Disponível em http://www.ebay.com.

[75] MercadoLivre Brasil - Onde comprar e vender de Tudo. Acessado em 30/04/2006. Disponível em HTTP://www.mercadolivre.com.br.

[76] Kamvar, Sepandar D.; Schlosser, Mario T.; Garcia-Molina, Hector. “EigenRep: Reputation Management in P2P Networks”. Stanford University. Acessado em 03/05/2006. Disponível em http://home.eng.iastate.edu/~snt/courses/internetalgos/reputation.pdf.

[77] Duma, C; Shahmehri, N.; Caronni, G. “Dynamic trust metrics for peer-to-peer systems”. In Proceedings of Sixteenth International Workshop on Database and Expert Systems Applications, page(s): 776- 781. Agust 2005.

[78] Gupta, Indranil; van Renesse, Robbert; Birman, Kenneth P. “A Probabilistically Correct Leader Election Protocol for Large Groups”. Acessado em 30/06/2006. Disponível em: www.cs.cornell.edu/projects/quicksilver/public_pdfs/Probabilistically%20Correct.pdf.

[79] Bhaskar, Raghav; Mühlethaler, Paul; Augot, Daniel; Adjih, Cédric; Boudjit, Saadi; Laouiti, Anis. “Efficient and Dynamic Group Key Agreement in Ad hoc Networks”. Institut National de Recherche en Informatique et en Automatique – IRIA. Rapport de Recherche N° 5915, Mai 2006.

[80] Lamport, Leslie; Shostak, Robert; Pease, Marshall; “The Byzantine Generals Problem”. ACM Transactions on Programming Languages and Systems (TOPLAS), v.4 n.3, p.382-401, July 1982.

[81] Zou, Xukai. “A block-free TGDH key agreement protocol for secure group communications”. Department of Computer and Information Sciences, Indiana University - Purdue University, Indianapolis, USA. 2008.

[82] Cuppens, Frédéric; Cuppens-Boulahia, Nora; Thomas, Julien. “S-TGDH, secure enhanced group management protocol in ad hoc networks”. ENST Bretagne, Rennes, SERES team. September 2007.

[83] Institute of Electrical and Electronics Engineers. IEEE. Acessado em 30/07/2006. Disponível em http://www.ieee.org.

[84] Searle, J.R. “Speech Acts: An Essay in the Philosophy of Language”. Cambridge University Press, 1969.

[85] Campadello, S. “The Green Card Protocol: an identification protocol for decentralized systems”. In Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks, IEEE Comp. Soc., pp. 647-651, 2006.

[86] Erdelsky, Philip J. “The Birthday Paradox”. Acessado em 06/08/2006. Disponível em http://www.wfgh.com/math/birthday.htm.

[87] Bellare, M.; Kohno, T. “Hash Function Balance and Its Impact on Birthday Attacks”. In C. Cachin e J. Camenisch (Eds.): EUROCRYPT 2004, LNCS 3027, pp. 401–418, 2004.

[88] Stallings, W. “Cryptography and Networks Security – Principles and Practices”. Upper Saddle River, NJ: Pearson Prentice Hall, pp. 82–83. 2006.

[89] IETF RFC 2631 – June 1999 – Diffie-Hellman Key Agreement Method.

[90] IETF RFC 4251 – January 2006 – SSH Protocol Architecture.

APÊNDICES

APÊNDICE A – AGENTES DE SOFTWARE

As tabelas a seguir representam uma situação em que um nodo (*Requisitante*) possui uma tarefa a ser realizada e, para tal, solicita a opinião de outro nodo (*Opinador)* sobre um terceiro (*Alvo da avaliação)*. Elas contêm o valor da opinião fornecida pelo *Opinador* e cada respectivo valor de exatidão associado (r).

Tabela A1 – Resultados para agentes que interagiram muitas vezes

Requisitante	*Opinador*	*Alvo da avaliação*	*Exatidão da opinião (r)*	*Opinião fornecida*
Agente0	Agente16	Agente17	0.0	0.6666666666666666
Agente0	Agente16	Agente17	0.0	0.6666666666666666
Agente0	Agente16	Agente17	0.28000000000006386	0.75
Agente0	Agente16	Agente17	0.19999999999999996	0.8333333333333334
Agente0	Agente16	Agente17	0.8322278587312869	0.8333333333333334
Agente0	Agente16	Agente17	0.9648157090282394	0.8571428571428571
Agente0	Agente16	Agente17	0.992621485844252	0.8888888888888888
Agente0	Agente16	Agente17	0.9984528992675177	0.8888888888888888
Agente0	Agente16	Agente17	0.9996759852961759	0.9

Tabela B2 – Resultados para agentes que interagiram poucas vezes

Requisitante	*Opinador*	*Alvo da avaliação*	*Exatidão da opinião (r)*	*Opinião fornecida*
Agente0	Agente12	Agente11	0.0	0.6666666666666666
Agente0	Agente12	Agente11	0.0	0.6666666666666666
Agente0	Agente12	Agente11	0.28000000000006386	0.6666666666666666
Agente0	Agente12	Agente11	0.12414003550640432	0.6666666666666666
Agente0	Agente12	Agente11	0.02786538929419493	0.6666666666666666
Agente0	Agente12	Agente11	0.005895061966673265	0.6666666666666666
Agente0	Agente12	Agente11	0.0012377193860120548	0.6666666666666666
Agente0	Agente12	Agente11	0.0003245083989564744	0.6666666666666666
Agente0	Agente12	Agente11	0.0003245083989564744	0.6666666666666666

Tabela A3 – Resultados para 1 agente desonesto

Requisitante	*Opinador*	*Alvo da avaliação*	*Exatidão da opinião (r)*	*Opinião fornecida*
Agente12	Agente0	Agente4	0.0	0.14285714285714285

Requisitante	*Opinador*	*Alvo da avaliação*	*Exatidão da opinião (r)*	*Opinião fornecida*
Agente12	Agente0	Agente4	0.0	0.14285714285714285
Agente12	Agente0	Agente4	0.0	0.14285714285714285
Agente12	Agente0	Agente4	0.0	0.14285714285714285
Agente12	Agente0	Agente4	0.04	0.14285714285714285
Agente12	Agente0	Agente4	$5{,}12 \times 10^{-7}$	0.14285714285714285
Agente12	Agente0	Agente4	$6{,}55 \times 10^{-12}$	0.14285714285714285
Agente12	Agente0	Agente4	$8{,}39 \times 10^{-17}$	0.14285714285714285
Agente12	Agente0	Agente4	$2{,}15 \times 10^{-22}$	0.14285714285714285
Agente12	Agente0	Agente4	$2{,}75 \times 10^{-27}$	0.14285714285714285
Agente12	Agente1	Agente4	0.0	0.6
Agente12	Agente1	Agente4	0.0	0.6666666666666666
Agente12	Agente1	Agente4	0.0	0.7142857142857143
Agente12	Agente1	Agente4	0.0	0.75
Agente12	Agente1	Agente4	0.2960000007201369	0.7777777777777778
Agente12	Agente1	Agente4	0.19999999999999996	0.8
Agente12	Agente1	Agente4	0.8322278587312869	0.8181818181818182
Agente12	Agente1	Agente4	0.9648157090282394	0.8333333333333334
Agente12	Agente1	Agente4	0.992621485844252	0.8461538461538461
Agente12	Agente1	Agente4	0.9984528992675177	0.8571428571428571

Tabela A4 - Resultados para 2 agentes desonestos

Requisitante	*Opinador*	*Alvo da requisição*	*Exatidão da opinião (r)*	*Opinião fornecida*
Agente13	Agente0	Agente14	0.0	0.14285714285714285
Agente13	Agente0	Agente14	0.0	0.14285714285714285
Agente13	Agente0	Agente14	0.0	0.14285714285714285
Agente13	Agente0	Agente14	0.0	0.14285714285714285
Agente13	Agente0	Agente14	0.008000000000001723	0.14285714285714285
Agente13	Agente0	Agente14	$4.096000000002763 \times 10^{-9}$	0.14285714285714285
Agente13	Agente0	Agente14	$2.0971520000020394 \times 10^{-15}$	0.14285714285714285
Agente13	Agente0	Agente14	$1.0737418240013663 \times 10^{-21}$	0.14285714285714285
Agente13	Agente0	Agente14	$5.497558138888631 \times 10^{-28}$	0.14285714285714285
Agente13	Agente0	Agente14	$2.8147497671118186 \times 10^{-34}$	0.14285714285714285
Agente13	Agente1	Agente14	0.0	0.14285714285714285

Requisitante	*Opinador*	*Alvo da requisição*	*Exatidão da opinião (r)*	*Opinião fornecida*
Agente13	Agente1	Agente14	0.0	0.14285714285714285
Agente13	Agente1	Agente14	0.0	0.14285714285714285
Agente13	Agente1	Agente14	0.0	0.14285714285714285
Agente13	Agente1	Agente14	0.008000000000001723	0.14285714285714285
Agente13	Agente1	Agente14	$2.0480000000013055 \times 10^{-8}$	0.14285714285714285
Agente13	Agente1	Agente14	$5.2428800000047526 \times 10^{-14}$	0.14285714285714285
Agente13	Agente1	Agente14	$1.3421772800015733 \times 10^{-19}$	0.14285714285714285
Agente13	Agente1	Agente14	$3.4359738368049417 \times 10^{-25}$	0.14285714285714285
Agente13	Agente1	Agente14	$8.796093022222977 \times 10^{-31}$	0.14285714285714285
Agente13	Agente16	Agente14	0.0	0.6666666666666666
Agente13	Agente16	Agente14	0.0	0.6666666666666666
Agente13	Agente16	Agente14	0.0	0.6666666666666666
Agente13	Agente16	Agente14	0.2960000007201369	0.75
Agente13	Agente16	Agente14	0.5904000028803664	0.8
Agente13	Agente16	Agente14	0.9450244776638308	0.8333333333333334
Agente13	Agente16	Agente14	0.992621485844252	0.8571428571428571
Agente13	Agente16	Agente14	0.9990100196168474	0.875
Agente13	Agente16	Agente14	0.9998677011302012	0.875

Tabela A5 - Resultados para 5 agentes desonestos

Requisitante	*Opinador*	*Alvo da requisição*	*Exatidão da opinião (r)*	*Opinião fornecida*
Agente10	Agente0	Agente4	0.0	0.14285714285714285
Agente10	Agente0	Agente4	0.0	0.14285714285714285
Agente10	Agente0	Agente4	0.04000000000000432	0.14285714285714285
Agente10	Agente0	Agente4	0.0016000000000004982	0.14285714285714285
Agente10	Agente0	Agente4	$2,56 \times 10^{-6}$	0.14285714285714285
Agente10	Agente0	Agente4	$3,28 \times 10^{-11}$	0.14285714285714285
Agente10	Agente0	Agente4	$3,28 \times 10^{-11}$	0.14285714285714285
Agente10	Agente0	Agente4	$4,19 \times 10^{-16}$	0.14285714285714285
Agente10	Agente0	Agente4	$1,07 \times 10^{-21}$	0.14285714285714285
Agente10	Agente0	Agente4	$1,07 \times 10^{-21}$	0.14285714285714285
Agente10	Agente15	Agente4	0.0	0.6666666666666666
Agente10	Agente15	Agente4	0.20000000000005594	0.6666666666666666

Requisitante	*Opinador*	*Alvo da requisição*	*Exatidão da opinião (r)*	*Opinião fornecida*
Agente10	Agente15	Agente4	0.2960000007201369	0.7142857142857143
Agente10	Agente15	Agente4	0.1817216030054692	0.7777777777777778
Agente10	Agente15	Agente4	0.12414003550640432	0.7777777777777778
Agente10	Agente15	Agente4	0.19999999999999996	0.8
Agente10	Agente15	Agente4	0.7378560089287955	0.8333333333333334
Agente10	Agente15	Agente4	0.9560196045652225	0.8461538461538461
Agente10	Agente15	Agente4	0.9560196045652225	0.8571428571428571

Tabela A6 - Resultados para 10 agentes desonestos

Requisitante	*Opinador*	*Alvo da Requisição*	*Exatidão da Opinião (r)*	*Opinião*
Agente14	Agente5	Agente17	0.0	0.14285714285714285
Agente14	Agente5	Agente17	$5{,}12 \times 10^{-7}$	0.14285714285714285
Agente14	Agente5	Agente17	$5{,}12 \times 10^{-7}$	0.14285714285714285
Agente14	Agente5	Agente17	$5{,}12 \times 10^{-7}$	0.14285714285714285
Agente14	Agente5	Agente17	$5{,}12 \times 10^{-7}$	0.14285714285714285
Agente14	Agente5	Agente17	$5{,}12 \times 10^{-7}$	0.14285714285714285
Agente14	Agente5	Agente17	$4{,}10 \times 10^{-9}$	0.14285714285714285
Agente14	Agente5	Agente17	$1{,}31 \times 10^{-12}$	0.14285714285714285
Agente14	Agente5	Agente17	$1{,}05 \times 10^{-14}$	0.14285714285714285
Agente14	Agente5	Agente17	$2{,}68 \times 10^{-20}$	0.14285714285714285
Agente14	Agente18	Agente17	0.0	0.75
Agente14	Agente18	Agente17	0.12414003550640432	0.75
Agente14	Agente18	Agente17	0.19999999999999996	0.8333333333333334
Agente14	Agente18	Agente17	0.19999999999999996	0.8333333333333334
Agente14	Agente18	Agente17	0.19999999999999996	0.8571428571428571
Agente14	Agente18	Agente17	0.19999999999999996	0.8888888888888888
Agente14	Agente18	Agente17	0.5904000028803664	0.8888888888888888
Agente14	Agente18	Agente17	0.8657822970266946	0.9
Agente14	Agente18	Agente17	0.9312805725230671	0.9166666666666666
Agente14	Agente18	Agente17	0.988470935247331	0.9166666666666666

APÊNDICE B – NODOS P2P

A figura B1 apresenta a modelagem das funcionalidades adicionadas ao JXTA Shell através de um diagrama de classes.

Figura B1: Diagrama de classes

A classe trust representa a classe principal da implementação do modelo de confiança e reputação, sendo ao mesmo tempo a classe pai das outras classes (test, combinedtrust, answer, reputation, directtrust). Estas classes filhas estendem as funcionalidades da classe trust e são responsáveis pela execução de tarefas específicas do modelo. São mostrados também os métodos pertencentes à classe trust, que estabelecem a comunicação entre as classes.

Os procedimentos realizados com a execução do comando “trust –grouptrust” seguem uma seqüência lógica de acordo com o fluxograma representado pela figura B2.

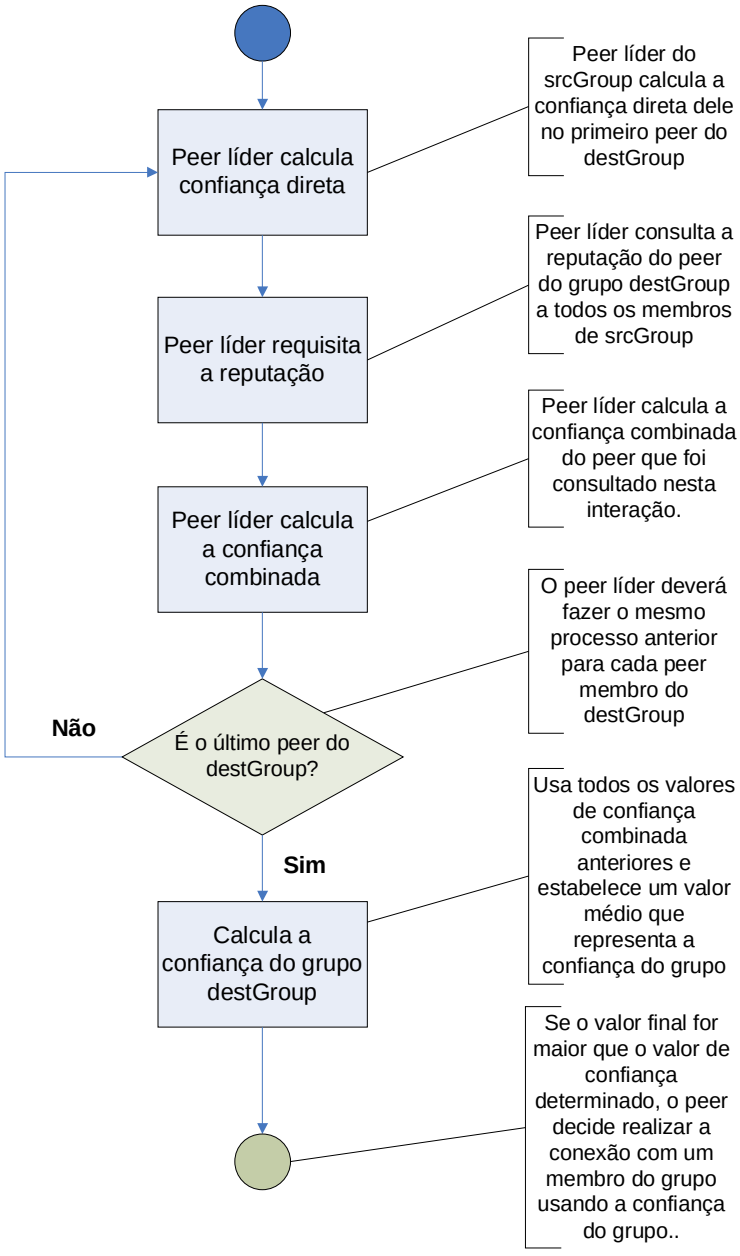


Figura B2 - Fluxograma confiança de grupos

Sobre os comandos implementados no JXTA Shell

a) trust –init

Comando que realiza a inicialização automatizada e individual de cada peer na rede P2P. Para que o peer realize qualquer operação ou interação na rede é preciso que este comando seja executado, preparando o peer para as futuras comunicações. Sintaxe do comando: *JXTA> trust –init peerName.*

peerName representa o peer que será inicializado na rede. Os peers encontrados na rede P2P são mostrados e o processo de registro do peer na rede é iniciado para que possa enviar e receber arquivos via protocolo SFTP. Este comando também por cria um diretório Tables, o qual armazena as tabelas de confiança dos peers.

b) trust –test

Comando que realiza a transferência de um arquivo para um peer de destino usando o protocolo SFTP. O mesmo comando é responsável por preparar o peer de destino para receber o arquivo e calcular seu hash através do algoritmo MD5 para verificar automaticamente a integridade do arquivo recebido. Cada vez que um arquivo é enviado o tempo da transmissão e a velocidade são calculados. Sintaxe deste comando: *JXTA> trust –test srcName destName fileName*.

srcName refere-se ao peer que está enviando o arquivo, *destName* é o peer destinatário e *fileName* é o arquivo que deseja-se enviar. A cada transferência o grau de confiança do peer de origem é testado e seus parâmetros para os cálculos dos valores da confiança e da reputação são atualizados para serem usados pelos próximos comandos. O tempo total de recebimento do arquivo, em milisegundos, é utilizado como parâmetro para realizar uma análise geral da transferência, e juntamente com o resultado do hash, define-se uma interação confiável com o peer de destino.

O cálculo realizado neste programa utiliza o parâmetro do tempo de transferência e estabelece uma variável a para receber os valores para cada situação. Se o arquivo chegar em até 1s, será considerado dentro do prazo de entrega e a variável recebe $a = 1$, se o tempo variar de 1s a 2s significa que o arquivo chegou um pouco atrasado e a variável recebe $a = 0.5$, pois não comprometeu totalmente a confiabilidade do processo; se o tempo de chegada for maior que 2s, o arquivo chegou muito atrasado, e se considera que o peer de origem realizou uma operação maliciosa na rede desencadeando um valor de $a = 0$.

O outro parâmetro utilizado é a integridade do arquivo recebido, e que gera um valor para a variável b. Quando o hash é calculado e o arquivo encontra-se íntegro, $b = 1$; caso contrário, considera-se que o peer de origem realizou uma operação maliciosa e, por isso, $b = 0$. Criou-se uma fórmula para calcular o grau de sucesso C em função de a e b que determina o sucesso que a transação obteve, dado por:

$$C = ((P \times a) + ((1 - P) \times b)) \qquad \text{eq. B1}$$

onde P representa o peso relacionado ao cálculo do hash.

Esta fórmula considera que a integridade do arquivo é mais importante do que o tempo de duração da transferência, exceto o caso em que o arquivo chega muito atrasado. O cálculo foi feito de maneira linear, considerando que os dois parâmetros (tempo e integridade) influem diretamente no resultado final. O valor estipulado foi de $P = 0.75$, que pode ser alterado de acordo com a situação. Assim, as situações que podem ocorrer são dadas pela tabela B1.

Tabela B1 – Parâmetros de tempo e hash

Situação	a	b	C
Arquivo corrompido e no tempo certo	0,00	1,00	0,250
Arquivo corrompido e pouco atrasado	0,00	0,50	0,125
Arquivo corrompido e muito atrasado	0,00	0,00	0,00
Arquivo integro e no tempo estimado	1,00	1,00	1,00
Arquivo integro e um pouco atrasado	1,00	0,50	0,875
Arquivo íntegro e muito atrasado	1,00	0,00	0,750

Para as simulações foi definido que valores para $C \geq 0.8$ resultavam em uma interação bem sucedida, fazendo com que o valor do contrato O fosse um, o que significa que o peer que enviou o arquivo realizou suas obrigações de entrega com qualidade e de forma confiável. Caso contrário, significa que interações são associadas à peers maliciosos.

O comando também cria o arquivo “peerTableMN.txt” (dentro do diretório Tables) contendo os coeficientes de M e N provenientes do cálculo da variável de O. Caso O seja igual a um, a variável M é incrementada; caso contrário, a variável N é incrementada.

c) trust –interaction

Comando que automatiza os testes de confiança na rede. Para cada vez que o comando é acionado, é feita uma interação seqüencial entre todos os peers na rede através do comando

trust –test. Sintaxe deste comando: *JXTA> trust –interaction srcName fileName [destName1 destName2 etc.]*

O argumento *srcName* refere-se ao peer que enviará o arquivo. De acordo com o resultado desta interação, o grau de confiança deste peer será testado. O argumento *fileName* contém o nome do arquivo que será enviado aos outros peers na transação. Os argumentos *destName* referem-se aos peers de destino na transação. Estes são os peers que armazenam os coeficientes de confiança da reputação. A quantidade de argumentos deste comando não é fixa, já que a interação pode ser feita com uma quantidade variável de peers, sendo que o mínimo é um peer e o máximo é a quantidade total de peers na rede menos um (peer de origem).

d) trust –directtrust

Comando que calcula o coeficiente de confiança direta entre dois peers na rede. Para isso, abre o arquivo "peerTableMN.txt" presente na pasta Tables e retira os coeficientes de confiança M e N para o peer em questão. Este cálculo é baseado somente no histórico das interações entre os dois peers. Sintaxe deste comando: *JXTA> trust –directtrust srcName destName.*

O argumento *srcName* refere-se ao peer de origem, o qual está requisitando o valor da confiança. Já o argumento *destName* refere-se ao peer do qual está sendo calculado a confiança. A saída do comando é constituída contém o coeficiente de confiança direta do peer de origem no peer de destino.

e) trust –reputation

Comando que calcula a reputação de um peer específico na rede. Cada vez que o comando é acionado, várias requisições são enviadas por um peer de origem para todos os outros peers na rede, com exceção do peer do qual a reputação foi requisitada. Sintaxe deste comando: *JXTA> trust –reputation srcName destName [otherName1 otherName2 etc.]*.

O argumento *srcName* refere-se ao peer que está requisitando a informação. O argumento *destName* contém o nome do peer cuja reputação foi solicitada. Os argumentos *otherName* referem-se aos peers de destino na transação. Estes são os peers que responderão à requisição com os coeficientes de confiança (M e N). A saída do comando contém o coeficiente de reputação do peer de destino.

f) trust –answer

Comando que responde as requisições de reputação dos peers, executado logo após o "trust –reputation" em cada peer que tiver recebido a requisição. Sintaxe deste comando: *JXTA> trust –answer otherName srcName.*

O argumento *otherName* refere-se ao peer local, que enviará a resposta contendo os coeficientes de reputação. O argumento *srcName* contém o nome do peer que requisitou a informação de reputação.

g) trust –combinedtrust

Comando que calcula o coeficiente de confiança combinada entre dois peers na rede, utilizado para calcular o grau de confiança de um peer em outro. Sintaxe deste comando: *JXTA> trust –combinedtrust srcName destName [otherName1 otherName2 etc.]*.

O argumento *srcName* refere-se ao peer que está requisitando a informação. O argumento *destName* contém o nome do peer cuja confiança combinada foi solicitada. Os argumentos *otherName* referem-se aos peers de destino na transação, que respondem à requisição com os coeficientes de reputação (M e N). A saída do comando contém o coeficiente de confiança combinada do peer de destino.

h) trust –grouptrust

Comando que calcula o coeficiente de confiança de um grupo em outro grupo. Sintaxe deste comando: *JXTA> trust –grouptrust srcGroup srcLeader [srcOtherName1 srcOtherName2 etc.] destGroup [destOtherName1destOtherName2 etc.]*.

O argumento srcGroup é fixo e refere-se ao grupo de origem, que fará o cálculo do coeficiente de confiança do grupo de destino. O argumento srcLeader contém o nome do peer que será designado líder do grupo. Os argumentos srcOtherName referem-se aos outros peers do grupo de origem. O argumento destGroup também é fixo e refere-se ao grupo de destino, do qual a confiança está sendo calculada. Os argumentos destOtherName referem-se aos outros peers do grupo de destino. A saída do comando contém o coeficiente de confiança combinada do grupo de destino.