IJoFCS (2006) **1**, 33-40

e-forensic PRESS

The International Journal of FORENSIC COMPUTER SCIENCE

www.IJoFCS.org

Towards Establishing Trust in MANET: an Integrated Approach for Auto-configuration, Authentication and Certification

Rafael Timóteo de Sousa Jr., Robson de Oliveira Albuquerque, Maíra Hanashiro, Yamar Aires da Silva and Paulo Roberto de Lira Gondim

Abstract - In this paper, we discuss open issues regarding certification, auto-configuration and authentication of routing messages for mobile ad-hoc networks (MANET). We describe and discuss existing models for these operations and highlight their specific problems. Considering routing protocols usage, we propose new solutions based on protocol modifications and distributed certifications that can be integrated to establish trust relationships for MANET operation and utilization.

Key Words: Authentication, distributed certification, mobile ad-hoc networks, routing protocols.

I.INTRODUCTION

WIRELESS networks are defined as computer networks connected through wireless links, such as radio frequencies and infrared rays. Wireless local area networks (WLANs) have arisen with the main purpose of overcoming the limitations imposed by traditional wired networks, thus permitting faster network installations and mobility at lower costs. According to the IEEE 802.11 standard [1], WLANs can be classified as access point-dependent networks (infrastructured) or independent networks (ad-hoc). In an infrastructured WLAN all communications among mobile nodes (MNs) travel through one or more mobile support stations (MSSs) and usually at least one MSS has a direct connection to a wired network. In this situation, MNs cannot communicate to each other directly.

In Ad Hoc WLANs, referred as Mobile Ad Hoc NETworks (MANETs) by the The Internet

Manuscript received October 6, 2006.

R. T. de Sousa, Jr., is with the Networks and Information Systems Security Group, Ecole Superiéure d´Electricité, Rennes 35000 France, on leave from the Electrical Engineering Department, University of Brasília, DF 70910-900 Brazil (corresponding author phone: 55-61-3307-2308; fax: 55-61-3247-6651; e-mail: desousa@ unb.br). He is sponsored by CNPq – Brazil.

R. O. Albuquerque is with the Electrical Engineering Department, University of Brasília, DF 70910-900 Brazil (e-mail: robson@redes.unb.br).

M. Hanashiro is with the Electrical Engineering Department, University of Brasília, DF 70910-900 Brazil (e-mail: maira@redes.unb.br).

Y. A. da Silva is with the Electrical Engineering Department, University of Brasília, DF 70910-900 Brazil (e-mail: yamar@ redes.unb.br).P. R. L. Gondim is with the Electrical Engineering Department, University of Brasília, DF 70910-900 Brazil (e-mail: pgondim@ene.unb.br).

Engineering Task Force (IETF) [1], MNs can communicate with each other directly because there is no MSS. Inside a MANET, MNs do not require any physical infrastructure, and the nodes can move freely because there is no central communication point. A MANET can operate in isolation or as an extension of some preinstalled wired network, which, in this case, requires a communication gateway to connect the attached ad-hoc networks.

MANETs are used mainly when a fixed wired network cannot be installed, or if wired networks are not well-suited. This can be during a natural disaster situation (hurricanes and earthquakes), when rescue teams must setup coordination and communication systems quickly. Other scenarios that require MANETs include battlefield exchange of tactical information among soldiers, police operations, information sharing in business meetings and student interactions in computer-supported classrooms.

MANETs are advantageous because they are quick to install (regardless of location because they require no previous infrastructure nor a fixed base to route messages) and provide fault tolerance (any malfunction or disconnection of a station can be solved with a dynamic reconfiguration of the network), connectivity (if two stations are inside the same area within reach of radio waves, there is a communication channel), mobility and other characteristics.

However, these characteristics impose fragilities that are important in these networks. The IETF Request for Comment (RFC) 2501 [2] explains how these fragilities are related to dynamic topologies, restricted bandwidths and variable link capacities, power save consumption operations and limited physical security. Consequently, MANETs require proper specifications involving certification, authentication, configuration and routing in order to sustain trust relationships in these networks.

In this paper, some proposals [3]–[5] related to certification and auto-configuration are presented and discussed. The problems in these models are emphasized and some solutions are highlighted regarding auto-configuration and the deployment of distributed certification authorities (CA). The integration of these functions is shown to be necessary for MANET to be a trust environment.

II. MANET Routing Protocols

Routing protocols are responsible for finding, establishing and maintaining routes among MNs that must communicate. It is very important for routing protocols in MANET to exchange as few messages as possible to avoid network overhead (bandwidth network usage) and in order to save power. These combined factors are related directly to the performance of the routing protocols. Different techniques have been developed to optimize the time for some routing protocols to create and establish routes. Other protocols were optimized to consume less bandwidth but require more time to establish a specific route.

According to the IETF MANET workgroup [1], there is a desirable quality list that routing protocols must supply with: (a) distributed operation, (b) no routing loops, (c) under demand operations, (d) pro-active operation, (e) security, (f) inactivity period operation and (g) unidirectional link support.

In general, MANET routing protocols can be classified as reactive and pro-active. Pro-active routing protocols store information about routes to every MN in the network. Reactive protocols only create a route when it is requested by an origin node. Four routing protocols are specified by IETF with RFC drafts: (a) Topology Dissemination Based on Reverse-Path Forwarding (TBRPF) [6], (b) Optimized Link State Routing Protocol (OLSR) [7], (c) Ad hoc On-Demand Distance Vector Routing (AODV) [8], and (d) Dynamic Source Routing (DSR) [9]. Drafts (a) and (b) are considered pro-active routing protocols, while (c) and (d) are reactive routing protocols.

The TBRPF creates per hop routing by the shortest path for each destination. Each MN running TBRPF generates a topology information tree database that is saved in a topology table. To minimize network processing, each MN reports only a small portion of its topology table to a neighbor MN. TBRFP uses different combinations and periodical updates to keep every MN informed about its own topology tree. To reach and maintain robustness in highly mobile environments, the protocol allows each MN to send additional information (complete topology tree) to its neighbors.

The TBRPF can be divided into two main modules. The first module, termed “neighbor discovery”, discovers and learns information about neighboring nodes. The second module, called “routing”, performs topology discovery and computes the routes to every destination. Differentiated HELLO messages are used for neighbor discovery and contain only information about a specific neighbor change. This results in

shorter messages for a link state algorithm.

The key concept of the OLSR is the use of multipoint relays (MPRs). MPRs are MNs selected to forward and broadcast OLSR messages, thus constituting a flooding mechanism. MPRs are spread throughout MANET to provide every MN with the partial information about the necessary topologies for computing the best route to every MN in the network. MPRs, combined with local duplicity avoidance, are used to minimize the number of control packets that should be sent in the network. OLSR is projected to work with highly scalable networks where traffic is sporadic and randomly distributed among the MNs. As a pro-active protocol, it is also appropriate for scenarios in which MN pairs change often, because no additional control packet is generated in the network since the routes are maintained and known by all possible destinations.

The AODV is based on the Destination-Sequenced Distance Vector Routing Algorithm (DSDV) protocol. The AODV is classified as distance-vector algorithm and is considered a reactive protocol because a route is created out of necessity. In general, the AODV tries to eliminate the broadcast routing message flooding, which in turn limits its own scalability. The AODV also tries to minimize latency when new routes are requested. Its functions are similar to traditional algorithms, including a feature to facilitate the interconnection with wired networks. Even though it adheres closely to traditional protocols, the AODV allows multicast and unicast traffic; however the protocol shows only one route to every destination, which constitutes a restrictive characteristic.

The DSR is a simple and efficient routing protocol designed for multi-hop MANETs with up to 200 MNs and supports high mobility rates. It allows the network to organize itself and auto-configure without any infrastructure administration. DSR is divided into two main modules called “routing discovery” and “routing maintenance” that work together to permit the MN to discover and maintain updated routes. All aspects of the protocol operate on demand, thus eliminating periodical routing information exchange. This characteristic reduces network bandwidth consumption and saves power. The DSR also permits multiple routes to a specific destination, allows every sender to select and control the used routes, provides loop-free routing information, supports unidirectional links and presents fast convergence when the network topology changes.

Noteworthy is the common characteristic of the four described protocols to ensure that nodes can trust the critical operation of routing. These protocols all require functions for node identification and message authentication, issues that are discussed herein.

III. Message Authentication within Routing Protocols

For the routing infrastructure to be trusted and thus to avoid malfunctioning in MANET, it is necessary to secure the routing messages. An authentication service for routing protocols is proposed in [10] and [11], in which an extension header – the MANET Authentication Extension (MAE) – is prefixed to every message of the routing protocol. All necessary information to authentication is included in the MAE. The main focus of the proposed model was to maintain the routing packets and their messages in unchanged formats, regardless of the specific protocol.

The MAE format includes tree protocol fields. Two of these fields are used to control the MAE itself (the MSG_TYPE field is used to differentiate MAE messages from other routing protocol messages and the MSG_LENGTH field indicates the size of MAE in bytes). The remaining field (AUTH_OBJECTS) carries authentication information, such as message authentication code, signer certificate, hash chains and sequence number. To ensure trust within the MANET, the production and verification of these objects must rely on the correct identification, authentication and certification of nodes, which brings the issue of operating these functions in a fully distributed ad-hoc environment.

IV. Distributed Certification

The MANET characteristics render a centralized certification service ill-suited for these networks. Instead, the distributed certification models present a more appropriate solution. Some existing models [3, 12 and 13] use threshold cryptography theory and pro-active secret key updates based on the Shamir schema [14]. This schema is fully distributed and the service is based on a node coalition approach and uses a cryptographic system that fully obeys the RSA model.

The certification models consider a MANET in which every MN v_i has its RSA key pair $\{sk_i, pk_i\}$, where $sk_i=<d_i,n_i>$ and $pk_i=<e_i,n_i>$ are respectively

the private and public keys to be used in point-to-point transactions.

The distributed certification authority (CA) has a key pair $\{SK,PK\}$, where $SK=<d,n>$ is used to sign all MN certificates. Any certificate in this approach can be verified using the system public key SK that is known by every MN in the network.

According to threshold cryptography, SK is divided in the network. Every MN v_i, besides its own key pair, has the partial key P_{vi}. Any subgroup k of n nodes can work as a CA. However, it is not possible to any MN to know the whole SK, except during the schema initialization.

Threshold cryptography is indicated to MANET as a result of some of its proprieties: (a) the distribution and decentralized control of the keys fits the profile of ad hoc networks, (b) security omnipresence is guaranteed since the secret is fully distributed in the network and intrusion detection is more practical and efficient, (c) the limit k is the balance between the service availability and intrusion tolerance. In other words, a group of adversaries need to destroy $(n-k+1)$ partial key holders to bring the system down (once the network auto-configuration becomes impossible without these nodes) and at least obtain k partial keys to steal the SK.

The system initialization is a critical step and includes choosing carefully the value of k . The lower the k value, the easier it is for an intruder to obtain the secret SK. Inversely, the greater the k value, the higher is the system security level, although this reduces fault tolerance simultaneously, since the closer k is from n, the greater is the probability of $(n-k+1)$ MN leaving the network; an event that would block the certification service.

A certificate generated by a CA is formed by parts of SK coming from a subgroup of k MNs, and is used for certifying a MN public key, as in a normal RSA cryptographic system. Therefore, every MN has its own SK signed certificate, $certi=<v_i,pk_i,T_{sing},T_{expire}>$, comprising the MN identifier v_i, its public key pk_i, the signature date T_{sing} and the certificate expiration date T_{expire} .

Two methods are used to control the certificate validity: (a) implicit certificate revocation stating that every MN must renew its certificate at least every T_{renew} period, where $T_{expire} \leq T_{sing} + T_{renew}$, (b) explicit certificate revocation where a certificate registered in a Certificate Revocation List (CRL) is not valid yet its T_{expire} is valid, which implies that only revoked certificates that did not expire must be in the CRL.

As implemented in [3], this model involves only subgroups, k size, of partial key holders. The basic operations include: (a) secret key negotiation, where the secret key can be obtained by a MN in the system initialization or by using the auto-configuration service (in the first case, both keys and certificates are distributed to MN by a central negotiator before MANET formation; in the second case, an auto initialization algorithm where k MN can provide a partial key to a new MN in the network), (b) secret key update, instead of changing the system key periodically, the operation only changes the partial key with the main purpose of protecting the secret key from breaking. This model supports $k-1$ partial secret breaks because SK is obtained with k keys. If in an update situation there are fewer than k discovered keys, SK is protected and does not need to be changed, (c) the certification service permits that when a MN starts using the certification service, one subgroup of k partial secret key holders (one coalition) is created and every MN v_i generates a partial signed certificate to the requesting MN. This one then generates its certificate by grouping k received certificates that represents a SK signed certificate. This service includes emission, renovation and revocation of certificates, and the setting of a security policy for each step, even before the MANET is formed.

V. Auto-configuration

In order for a MN to communicate in a network it must have a unique identifier, usually the IP address. However, in MANET the topology changes dynamically, thus creating difficulties for centralized administration to distribute IP addresses or any other identifier. This situation leads to a distributed, dynamic and automatic service.

Auto-configuration provides a service that renders MANET more efficient and robust. Even though there are many approaches related to auto-configuration, none has been standardized. A proposed auto-configuration model [4] uses message authentication supported by a distributed CA, according to models such as those presented by Silveira et al. [3], Luo et al. [12] and Kong et al. [13]. The presence of a distributed CA avoids the possibility that any intruder MN can produce messages or even change the messages already created with the purpose of breaking the protocol or rendering the service unavailable. The approach by Buiati [4] requires that the MN is configured

previously with a valid certificate before they can request and join the auto-configuration service. Therefore, for a MN to request an IP address or even respond to a client MN solicitation, that MN must have a valid certificate. The authentication service of the auto-configuration mechanism is supplied using the same MAE described above for routing in MANET, which has all the necessary information to guarantee authenticity, integrity and non-repudiation in all MAE protected messages.

The MAE contains authentication objects which includes a mandatory digital signature (DS) and authenticates all non-mutable fields of auto-configuration messages. The MAE should have one more object that can be the certificate. The message sender DS is obtained with the sender private key because the certificate that accompanies the MAE has the sender public key that can be used to certify the message sender. If the MN certificate is not locally available, MAE can possess a CERT object, which carries with the message the certificate that created and signed the MAE. Additional objects are used to provide additional services that are beyond the protocol auto-configuration approach.

Every NM that is valid and trusted to a specific MANET has an IP address identifying its interface, and a subset of free IP addresses (FIAs) to offer to MN clients that wish to associate to the network. Within a particular MANET, a MN FIA must be distinguished from other MN FIAs to avoid multiple MNs distributing the same IP address. Additionally, every MANET has a unique identifier defined as partition ID (PID), which permits that a MN having the same PID as other MN consider both MN in the same MANET. The PID also helps to distinguish different MANETs that share a specific area, and is a parameter that is necessary to control the fusion of MANETs.

The Dynamic Configuration Distribution Protocol (DCDP) is used to distribute network configuration information such as IP address, network mask and default gateway. The DCDP uses binary division to provide to distinct IP address for MNs in the network. Binary division assures that all MNs receive distinguished IP addresses, thus avoiding IP address conflicts even when two or more MANETs are fused.

As stated by Buiati [4], in order to obtain and associate an IP address the MN must have received its valid certificate. When a MN wishes to join a MANET so that it can obtain an IP address, it broadcasts an ADDR_REQ message using its MAC address as the source address. Any MN belonging to the MANET answers the message with an ADDR_REP that contains a FIA with the largest free IP quantity because a MN can have more than one FIA with different address quantities. The MN can receive more than one answer from the other MNs, and then selects the MN that has the largest FIA by sending a SERVER_POOL message directly to the chosen MN server, thus discarding all other received messages.

The SERVER_POOL message confirms the intention of the requesting MN for obtaining an IP address. The elected MN server then divides its FIA, sending one-half to the MN that requested it and keeping the other half for answering future requests. The requesting MN receives the FIA throughout the IP_ASSIGNED message and stores the free IP addresses in its own FIA, reserving the first IP address for itself (if it possesses more than on FIA, the MN must mark which FIA has its own address). The remaining addresses may be used to answer other MN client requests. The process is completed using an IP_ASSIGNEMENT_OK message to the server MN.

VI. Open Issues and Proposed Solutions

As discussed above, the integration of auto-configuration, certification and authentication is imperative for establishing trust in MANET. The models described, though bringing effective solutions to each of these operations, present open issues to be resolved. A fully distributed MANET certification authority can be created and implemented [3], but it depends and relies on the value of k, which describes the size of a MN group capable of holding the parts that constitute a SK key. During MANET operations this implies directly that MN must be reached so that a MN can have its certificate signed. If k MANET are not reached, the MN cannot join the MANET because it cannot sign its requests. A routing protocol should then be used to reach k MN, thus permitting the certificate signature.

Another problem related to k is its fixed arbitrary value, the definition of which is relative to two empirical heuristics: (a) k cannot have a large value (close to the total number of MNs in the MANET), because this brings a reachability issue and reduces fault tolerance, and (b) k cannot have a very small value (considering the number of MNs in MANET), because this increases the vulnerability of SK. However, the number of nodes in a MANET is possibly highly variable,

thus implying that an adequately defined k value may become inadequate considering that some number of MNs can leave or join the MANET at anytime.

An initial solution is that k may vary as a function of a percentage of the network actual size. However, to be able to modify k dynamically it is important to define a maximum and a minimum value (both related to a percentage of the network size) that should be chosen according to the security constraints of the network. Moreover, these values should be monitored during the MANET operation, whether they are growing or decreasing, given that if a minimum or a maximum value is reached, it is necessary to redefine the limits for k . Given these limits, according to the analyses of the results obtained in [3], the value of k can be defined as an average of the maximum and the minimum sizes.

Still considering that k may vary periodically, the model requires improvements in the CRL because the number of revoked certificates would be much larger once the number of used certificates is fully dependent on k. The more the value of k varies, the more frequent is the emission of revoked certificates and the requests and emissions of new certificates. This generates more traffic in the network, thus forcing the MNs to process new certificates, thereby leading to increased power consumption and a longer CRL list.

Moreover, as MNs enter and leave the network, the dynamic variation of k implies each time to return to the CA initialization stage because the k parts of SK must change. A centralized approach for the process of CA initialization is possible [3], but contradicts the MANET requirement of fully distributed services. A new model of a distributed CA, aware of periodical changes of k, requires a mathematical model for the computation of a new SK in a distributed environment.

Additionally, there is the issue of reaching k MNs for a new node to be accepted in the MANET. These MNs can be reached using routing protocols with the signature based on a previous requested certificate. This problem requires a MN to work as a proxy, acting in other MN's names and representing $k - 1$ MN to sign the certificate request. If a proxy MN already has a valid configuration in the network, it could provide signed certificates even if the $k - 1$ nodes cannot be reached otherwise.

Another approach considers that a temporary IP address can be used to request the certificate signature. This implies that a topology change is required due to the temporary IP chosen by the MN. To solve this problem, a range of IP network address (even in CIDR) could be allocated and announced in the network informing that if a MN wishes to sign a certificate so it can join MANET, it then should use an IP address range reserved to that finality.

In this situation, the OLSR could be used as routing protocol because of its pro-active characteristic, in addition to the information messages, the reserved IP range could be announced by the MPRs. A time-to-live (TTL) should be limited to 2 or 3 hops because it is highly probable that $k - 1$ nodes could be contacted at these distances by routing, thus limiting the certification signature-related traffic. In fact, any pro-active routing protocol could be used in this situation once the routing information is easily created, because the IP range would be well-known in the network.

Although the model by Buiati [4] uses the distributed CA approach implemented by Silveira et al. [3], the routing considerations where not applied there, thus limiting the extent of the proposed auto-configuration model, which assumes that the MN already possesses a valid signed certificate. Another problem in Buiati's model [4] is that the auto-configuration operation assumes that every message sent in the network is a broadcast message. This auto-configuration model does not scale well because in a large MANET the number of messages would increase significantly, creating problems related to unnecessary bandwidth consumption and increasing power consumption by the MNs.

To resolve this specific problem, the protocol should be altered so that only the first message is broadcast to all nearby MNs. In this message, the MAC address of the MN goes with the frame. As the destination MN receives the sender MAC address, the other messages in the communication process can be conducted using unicast addressing, thus avoiding network flooding.

VII. Conclusion

MANET utilization is increasing at a rapid pace, but critical problems remain unresolved. Specific problems related to auto-configuration, routing metrics and distributed certification are increasing as MANET standards are developed.

The approaches by Silveira [3] and Buiati [4] evaluated herein present open issues to be solved. Our proposed solutions consider routing

and other protocol modifications to integrate solutions for auto-configuration, certification and authentication.

An approach such as that proposed by Buiati [4], that relies in a static value k as the number of parts for a group key SK, is not adequate for MANET as the number of MNs cannot be predicted readily. On the other hand, k is defined by considering an expected number of nodes n. As the real n increases or reduces, k cannot vary because the entire process needs to restart to allow the SK secret key creation, which is a centralized process. A new envisioned solution is based on the idea that relies on a fully distributed CA initialization approach so that k can vary according to the requirements of MANET. It is important to note that this model should be validated mathematically, an issue that we are considering for future work.

Silveira et al. [3] contends that the routing metrics required to reach k nodes is not considered because it assumes that all nodes are close to the requesting MN, which in MANET may not be true due to the mobility of nodes. The present paper proposes a solution whereby routing protocols can be used by proxy nodes to reach k MNs in order to produce a signed certificate.

The auto-configuration model, based on broadcast messages during the entire auto-configuration process, should be altered in order to avoid unnecessary bandwidth consumption and power consumption. Once the first message is sent, the MAC address of the sender can be obtained easily, and the consequent communication can continue using unicast messages.

Towards establishing trust in MANET, an integrated approach for auto-configuration, authentication and certification is needed. In this paper we propose solutions for this integration to be obtained effectively, while respecting the specific characteristics of MANET, namely the mobility of nodes, the dynamic of node presence, the particular connectivity and associated restrictions regarding power consumption, restricted bandwidth and limited physical security.

There is evidence that the integration of auto-configuration, authentication and certification results in accrued complexity for MANET nodes, with several factors to be considered and involving mutually dependent operations. Based on discussions of trust in [15], it can be argued that the explicit consideration of trust among nodes is a means for reducing the complexity in the MANET environment.

However, the concept of trust [16] remains an open subject and implies the need for more study in areas such as collecting and distributing information specific to trust, monitoring nodes behavior, storing memories of trust, proving and establishing the reputation of nodes, among other subjects that we are considering for future work.

References

[1] *Wireless LAN media access control (MAC) and physical layer (PHY) specifications*, IEEE Standard 802.11, First edition, 1999.

[2] S. Corson and J. Marker, *Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation consideration*, IETF RFC 2501 (informational), 1999.

[3] F. Silveira and M. Hanashiro, "Serviços de Certificação para Redes Móveis Ad Hoc", final undergraduate project PFG.17/2003. Elect. Eng. Dept., University of Brasília, Brasília, Brazil, 2003.

[4] F. M. Buiati, "Protocolo Seguro para Autoconfiguração de Endereços de Redes Móveis Ad Hoc". M.S. thesis T.180/04. Elect. Eng. Dept., University of Brasília, Brasília, Brazil, 2004.

[5] R. S. Puttini, L. Mé, and R. T. de Sousa Jr., "Preventive and Corrective Protection for Mobile Ad Hoc Network Routing Protocols", *Lecture Notes in Computer Science*, v. 2928, pp. 213-226, 2004.

[6] R. Ogier, M. Lewis, F. Templin, and B. Bellur, *Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)*, IETF Internet Draft, MANET working group, <draft-ietf-manet-tbrpf-06.txt>, November, 2002.

[7] T. Clausen and P. Jacquet, *Optimized Link State Routing Protocol*, IETF Internet Draft, MANET working group, version 11, July, 2003.

[8] C. E. Perkins, E. M. Royer and S. R. DAS, *Ad hoc on-demand distance vector (AODV) routing*, IETF Internet Draft, MANET working group, <draftietfmanetaodv10.txt>, January, 2002.

[9] D. B. Johnson, D. A. Maltz, Y.-C. Hu, and J. G. Jetcheva, *The dynamic source routing protocol for mobile ad hoc networks (DSR)*, IETF Internet Draft, MANET working group, <draft-ietf-manet-dsr-07.txt>, February, 2002.

[10] R. S. Puttini, L. Mé, and R. T. de Sousa Jr., "An Authentication Protocol to MANET". *Recent Advances in Communications and Computer Science*, pp. 208-226, 2003.

[11] F. Buiati, R. S. Puttini, and R. T. de Sousa Jr., "A Secure Autoconfiguration Protocol for MANET Nodes". *Lecture Notes in Computer Science*, v. 3158, pp. 108-121, 2004.

[12] H. Luo and S. Lu, "Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks", Dept. Comp. Science, UCLA, Technical Report TR-200030, 2000.

[13] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for MANET", in *IEEE 9th Int. Conf. Network Protocols*, pp. 251-257, 2001.

[14] A. Shamir, "How to Share a Secret", *Communications of the ACM*, v. 22(11), pp. 612-613, 1979.

[15] S. P. Marsh. "Formalising Trust as a Computational Concept". PhD thesis, Dept. Comp. Science and Math., University of Stirling, 1994.

[16] D. Trcek, "Towards trust management standardization", *Computer Standards & Interfaces*, v. 26, pp. 543–548, 2004.

R. T. de Sousa, Jr., was born in Campina Grande – PB, Brazil, on June 24, 1961. He graduated in Electrical Engineering, Federal University of Paraíba – UFPB, Campina Grande – PB, Brazil, 1984, and got his Doctorate Degree in Telecommunications, University of Rennes 1, Rennes, France, 1988. His field of study is Network Engineering, Management and Security.

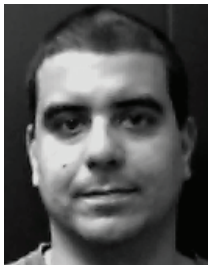
His professional experience includes technological consulting for private organizations and the Brazilian Federal Government. He received the 3rd Telecommunications Telexpo Golden Medal for his work on the management of network services quality. He is a Network-Engineering Professor at the Electrical Engineering Department, University of Brasília, Brasília – DF 70910-900 Brazil. He is with the Networks and Information Systems Security Group, Ecole Superiéure d´Electricité, Rennes 35000 France, on leave from the University of Brasília, and his current research interest is Trust Management for Spontaneous Self-organized Networks.

R. O. Albuquerque was born in Taguatinga – DF, Brazil, on January 30, 1976. He graduated in Computer Science, Catholic University of Brasília, Brasília – DF, Brazil, 1999, and got his Master Degree in Electrical Engineering, University of Brasília, Brasília – DF, 2003. He is pursuing his Doctorate Degree at University of Brasília, Brasília – DF, Brazil, and at Universidad Complutense de Madrid, Madrid, Spain. His field of study is Network and Information Security.

He is a network security specialist and Professor at University of Brasília. His professional experience includes IT consulting for private organizations and the Brazilian Federal Government. His fields of interest and research include Network Management, Network Systems, Software Agents, Wireless Networks and Open Source Software.

M. Hanashiro was born in Mairiporã – SP, Brazil, on June 21, 1980. She graduated in Network Engineering (2003) and is pursuing a Master Degree in Electrical Engineering at the University of Brasília, Brasília – DF, Brazil.

She works for the Brazilian Federal Government. Her fields of interest include Network Engineering and Security and IT Governance.



Y. A. da Silva was born in Brasília – DF, Brazil, on April 22, 1973. He graduated in Electrical Engineering (2000) and is pursuing a Master Degree in Electrical Engineering at the University of Brasília, Brasília – DF, Brazil.

He has been working as a consultant for Siemens, regarding IT Market. His research is focused in Information Security.

P. R. L. Gondim was born in Rio de Janeiro – RJ, Brazil, on February 23, 1957. He graduated in Computer Engineering (1987) and received his Master Degree in Computing and Systems (1992) from Military Engineering Institute, Rio de Janeiro – RJ, Brazil. He obtained his doctor degree in telecommunications at Catholic University (PUC-Rio), Rio de Janeiro – RJ, Brazil, 1998.

He directed master degree dissertations in Computer Science and Communications Networks. He is a professor at the Electrical Engineering Department, University of Brasília, Brasília – DF, Brazil. His research interests include Networks and Wireless Technologies, Information Security, Quality of Service and Interactive Digital Television.