Combining Certification-based Authentication and Intrusion Detection to Secure Manet Routing Protocols

Ricardo Puttini[1], Rafael de Sousa[1], Ludovic Mé[2]
[1]Departamento de Engenharia Elétrica - Universidade de Brasília
Campus Universitário Darcy Ribeiro – Asa Norte – Brasília – DF – BRAZIL
[2]École Supérieure d'Électricité - Supélec - Campus de Rennes
Avenue de la Boulaie - BP 81127 - 35511 Cesson-Sévigné Cedex – France
e-mail: puttini@unb.br, desousa@unb.br, ludovic.me@supelec.fr

Abstract **: In this paper we describe a new mobile ad hoc networks (Manet) routing protocol security design that combines a certificate-based authentication service with intrusion detection. Certification service and IDS are both designed to have distribution, collaboration and self-organization features. Intrusion response is defined in terms of interaction between certification service and IDS. The proposed vulnerability analysis and security design are validated using the Optimized Link State Routing (OLSR) Protocol. Performance results, obtained from actual implementation of the security services, are presented, in order to establish the feasibility of the proposed solutions.**

1. Introduction

In this paper we propose a new security model for protection of MANET routing protocol. The salient features in our design are:

- Combination of both preventive and corrective protection;
- Self-organized conception of security services, in the sense that security services are provided collaboratively, without assumption on any centralized entity;
- Fully localized solutions, restricting communication overheads within nearby nodes; and
- Robustness in the presence of node compromising, allowing the security solution to be tolerant to presence of compromised nodes.

As a basic preventive solution, a digital certificate based authentication service is proposed for the routing protocol messages. The companion certificate services are also proposed, as an extension to [1], and designed to be self-organized and fully localized. An intrusion detection and response system (IDS) provides the corrective solution feeding the certificate services with information about misbehaving nodes, which are eliminated from the network by certification revocation. Both certificate services and IDS are designed to be robust even in the presence of compromised nodes.

The proposed model is completely developed for protection of the Optimized Link State Routing (OLSR) Protocol [2]. Validation of the proposed model is obtained from actual implementation of security services for the OLSR.

The rest of this paper is organized as follows: In section 2, we discuss the vulnerability and adversary models. Section 3 is devoted to description of the security model. Section 4 details the development of the proposed solution for protection of the OLSR. Section 5 describes the implementation and results obtained from experimentation. Section 6 discusses related work and section 7 concludes the paper with our final remarks.

2. Vulnerability and Adversary Models

2.1. Vulnerability Model

Attacks against routing protocols are usually related to the insertion of erroneous routing information, attempting to disturb the routing algorithm. This is the case for modification (malicious modification of routing protocol messages), impersonation (masquerading as another node) or fabrication (generation of false routing messages) attacks. Combinations of these basic operations are also possible and provide a broader range of attacks. There are also some cases where passive eavesdropping vulnerabilities may also be considered (e.g. in military application, where the routing protocol messages can reveal information about geographical positioning of the nodes). Additionally, trivial attacks based in resource consumption and non-cooperation are possible in all ad hoc routing protocols. In this paper, we focus on vulnerabilities related to impersonation, modification and fabrication of routing protocol messages.

2.2. Adversary Model

Although it might seems that the MANET routing protocol vulnerabilities considered here are quite similar to those from classical routing protocols, exploitation of such vulnerabilities are quite different in the MANET, given the particular features of these networks:

- promiscuous nature of the wireless link (nodes are able to monitor neighbors behavior);
- non-centralized, peer-to-peer communication model (e.g. lack on infra-structure); and
- mobility (dynamic network topology).

An adversary may readily exploit these features in many different ways. Thus, an adversary may:

- promiscuously listen to wireless transmissions coming from its neighbors in order to learn about the local routing information kept by them;

– communicate directly with any node within the transmission range of its wireless interface;
– move away (with limited speed) to gather information about other (far away) nodes.

Moreover, unlike classical routers, which provide only limited service with careful protection, MANET nodes have a non-negligible probability of compromise due to vulnerabilities related to OS, software bugs, backdoors, viruses, etc. Also, a mobile node without adequate physical protection is also prone to being captured. Although we do not elaborate on such vulnerabilities, we admit that an adversary may be able to compromise or capture a mobile node. We do not restrict the consequences of a node break-in. Thus, during break-in, any secret information (including private or shared keys) stored locally may be exposed to the intruder.

3. Security (Protection) Model

MANET context imposes strong requirements in the protection model. The MANET requirements considered in our security model are:

– Mobility: nodes in a MANET may, at any time, disappear from, appear into or move within the network. Therefore, availability of an individual node cannot be assured and services cannot rely on a central entity.
– Locality: the error prone nature of the wireless links and the limited bandwidth requires that security services must be provided collaboratively by nearby nodes, most often by 1-hop neighbor nodes.
– Intrusion Tolerance: security solution should be robust in the existence of compromised nodes in the network, given the non-negligible probability for node break-ins.

To cope with mobility of the MANET nodes, we do not assume in our design the existence of any centralized entity in the network. Instead, we take the self-organized approach by adopting fully localized mechanisms and relying on the collaboration for the provision of the security services.

Self-organization is illustrated in Figure 1. An autonomous instance of each security service must be active in each MANET node. These instances are generally called Local Service (L-Service). A L-Service collaborates with L-Services from nearby nodes (usually in the neighborhood), by means of some collaboration protocol. This sense of self-organization is exactly the same used in the very conception of the MANET routing service, the L-Service being represented by the MANET routing protocol daemon, which is autonomously executed in each MANET node, the collaboration protocol being represented by the MANET routing protocol.

In our design, protection of the routing protocol includes both preventive and corrective security services. A certificate-based authentication service for

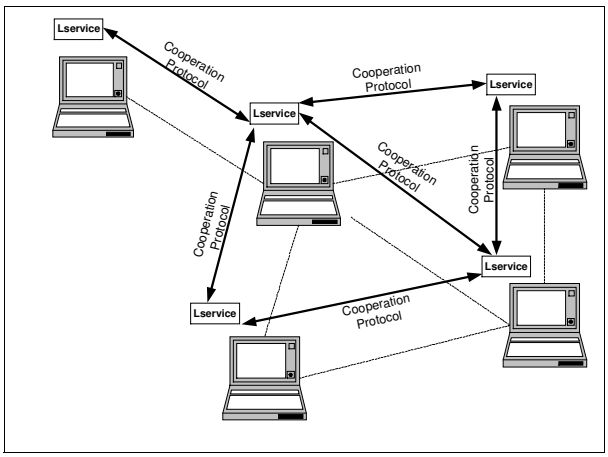

Figure 1 – Model for self-organized services

the routing protocol messages is considered as a basic preventive solution. The authentication service aims to avoid an attack to be generated from a non-authenticated node. However, according to the presumed adversary model, attacks are still possible in two situations: (1) an authenticated node (e.g. certificate holder) starts to behave maliciously; or (2) a MANET node has been compromised and the authentication secret (e.g. private key) from that node has been exposed.

The corrective security service is provided in terms of an intrusion detection and response system (IDS). Intrusion response consists mainly in the isolation of malicious/compromised nodes, excluding them from the routing service. This is accomplished basically by means of certificate revocation.

Certification services and intrusion detection and response should be provided in a self-organized and distributed manner by a Local Certification Service (L-Cert) and a Local IDS (LIDS) instances [3]. Figure 2 illustrates the proposed protection model.

Basically, routing protocol, certification service and IDS (alert) message exchanges must be authenticated with a MANET authentication extension (MAE), which is appended to each message and provides the authentication information. Authentication is based on the certification service and uses asymmetric cryptography primitives. Each node in the MANET must hold a valid certificate, binding the node's identity to its public key.

In order to maintaining the robustness of the security solution in the presence of compromised nodes, security services in our system are designed to have k-by-n security, in the sense that any certification service or intrusion response must be collaboratively provided by, at least, k nodes, where n is the total (non-fixed) number of nodes in the network. Thus, for compromising a security service, an adversary must break into k different nodes. Correct nodes running the LIDS must detect the attacks against the routing protocol and isolate the compromised node (by revoking its certificate) before that an adversary can compromise k nodes, breaking the collaborative security system.

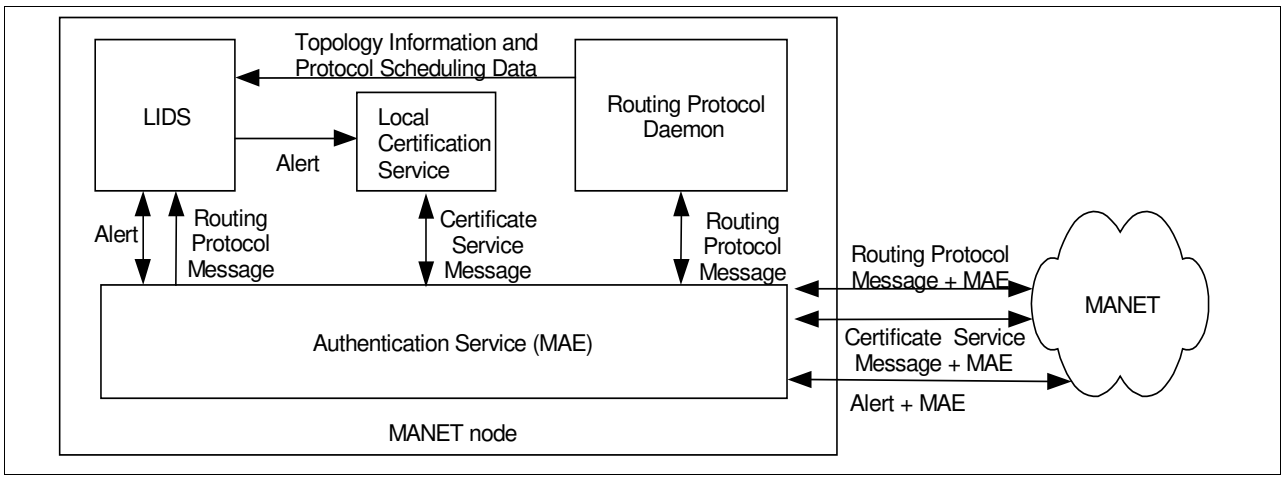

Figure 2 – Routing Protocol Protection Model

Given that collaboration is done by means of authenticated messages (certificate services and IDS messages are all authenticated using MAE), isolating a node is equivalent to revoking the node's certificate. An indirect revocation mechanism is related to certification expiration. Thus, security can be improved if we require that certificates must be renewed from time to time. Certificates are issued with constrained certificate expiration time. Each node having a valid certificate must request for a new certificate, before the current certificate has expired. Nodes that are not well behaving should not have their certificates renewed.

Finally, locality requirement states that collaboration should be designed to restrict communications among L-Services (e.g. local certificate services and LIDSes) around nearby nodes, usually in the local neighborhood. This is an important requirement as it relates to the scalability of the overall solution. Considering the locality requirement stated above, k becomes an important parameter and should be related to the average size of neighborhoods in the network. If a node has k or more neighbors, IDS and certification services can be fully provided in the local neighborhood. Thus, the security solution is scalable, in the sense that security services are run locally, provided a convenient choice for parameter k.

3.1. MANET Certification Service

The design of self-organized certification services in MANET has been discussed in a few recent papers [1,4], which are based on a distributed certification authority (DCA) trust model. The CA secret key (KCA) is used to sign certificates for all nodes in the MANET. A certificate signed with KCA can be readily verified with the well-known system public key. The distribution of the CA capabilities is achieved by sharing the secret key among network nodes by means of threshold cryptography techniques. Each MANET node holds a private-key-share (SKCA) and any k (a system wide constant, usually related to the average number of neighbors) of such private-key-share holders can collective function as a CA. The KCA, however, is not recoverable by any node. Counter-certificate issuing does certificate revocation, which must also be signed with KCA.

Our proposal is based on [1], with the following improvements [5]: (1) Certification issuing and renewal in [1 follows some pre-established rule. In our design, instead of having such a fixed rule, we propose a set of policy configurable options for issuing of new certificates, certificate renewal, private-key-share issuing and updating. This policy may be used to enforce that new certificate and SKCA issuing in the DCA following strictly the same identity verification that an equivalent centralized CA, avoiding multiple identity faking attacks (sybil attacks) [6]. This identity check can be adapted to the MANET context, using the notion of communities, for example [7]. (2) Approaches described in [1] do not specify how valid certificates are acquired and stored in each node. Also, local Certification Revocation Lists (CRL) are progressively built by accumulating counter-certificates that are flooded in the network. However, synchronization of newly arrived nodes (which must initialize their empty CRL) is left unspecified. We propose a set of policy configurable options for distribution and localized maintenance of valid certificates and certificate revocation list. (3) Designs from [1] are based on a single DCA. We extend the model to supporting multiple DCA and trust path constructions.

3.2. Authentication for Securing Routing Protocols

The authentication service considered in our model is provided by a MANET authentication extension (MAE), which is appended to each routing protocol message or packet. This MAE contains all the authentication information required to correctly assure authenticity and integrity to the message or packet being protected. Our objective is to design such extension in a flexible and adaptable way, so that it could be used to secure different MANET routing protocols. The idea is to preserve the routing protocol syntax unchanged, differently from previous work.

Authentication Objects: MAE is composed by authentication objects. At least one (mandatory) authentication object should be present in the MAE and alternatively contains a digital signature (DS) object. DS authenticates all the non-mutable fields of a routing protocol packet/message. Additional authentication objects are used to provide optional

services. Currently defined options are signer certificate (using to carry the certificate of the MAE signer within the message), hash chains information (protection of the mutable fields) and sequence number (reply protection) [5].

3.3. MAE for DSR, AODV, OLSR and TBRPF

OLSR and TBRPF are proactive link-state routing protocols whose message don't have mutable fields in the routing messages that are actually used by the respective routing protocol algorithm. MAE for securing OLSR and TBRPF is simply built with a single authentication object containing MAC or digital signature (DS).

AODV have mutable fields in route request (RREQ) and route reply (RREP). These fields are hop count metrics that are changed every time the packet is processed and forwarded by nodes between the message source and destination. A hash chain object (HC) [12] is included and updated each time these fields change (e.g. each time the message is processed and forward). Such protection avoids that an attacker could decrement the hop count. Route error (RERR) messages are signed only by the node forwarding them. Route reply acknowledgments (RREP-ACK) have no mutable fields and are only authenticated by the message originator.

Securing DSR is quite more complex, although limited security can be achieved by combining the mandatory authentication object with a hash chain object implementing a per-hop hashing schema in RREQ messages. This will avoid an attacker from faking of the initiator node and from removing correct IP address in the route list [14]. RREP messages could be simply signed by the target of the route discovery. Table 1 illustrates the main features of each MANET routing protocol and MAE requirements for each of them.

Table 1 – MAE for MANET routing protocols

Routing Protocol	Routing Discovery	Routing Algorithm	Relevant Messages	Auth. Objects
DSR	on-demand	source-routing	RREQ	DS+HC
			RREP	DS
AODV	on-demand	distance-vector	RREQ	DS+HC
			RREP	DS+HC
			RERR	DS
			RREP-ACK	DS
OLSR[**Erro! A origem da referência não foi encontrada.**]	proactive	link-state	Hello, TC	DS
TBRPF	proactive	link-state	Hello, TU	DS

3.4. Authentication and Certification Policy Issues

MAE and certification service specifications are provided with a set of configurable options that should be used to define a security context that is adapted to the security requirements of the MANET security policy. Figure 3 below summarizes all the authentication and certification policy parameters considered in our design. See [5] for further details.

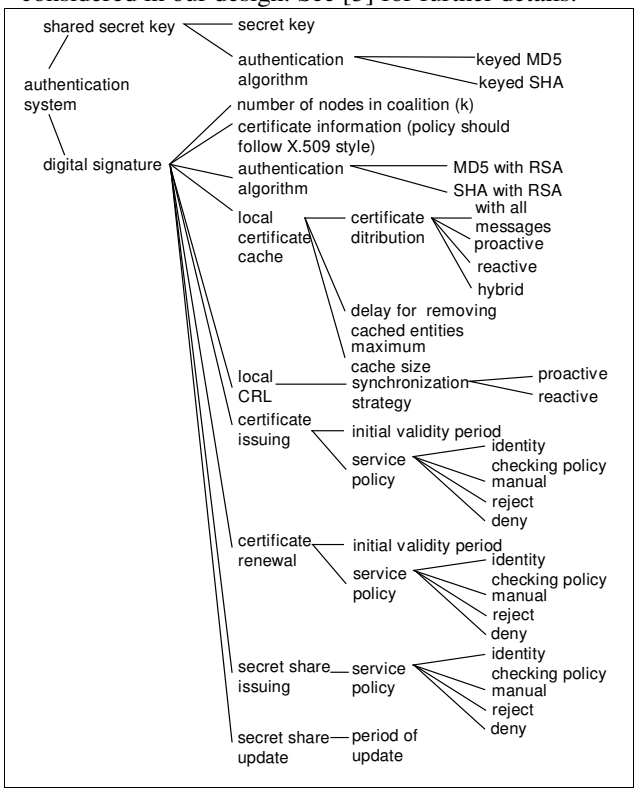

Figure 3 – Authentication Policy Parameters

3.5. Collaborative Intrusion Detection and Response

Given the lack of centralization, the mobility of the nodes and the wireless nature of link connections in the MANET environment, some (if not all) of the tasks required for the intrusion detection process must be executed in a distributed and cooperative manner [3,9]. To active these objectives, the MANET-adapted IDS is designed with the following features: (1) each MANET node runs an autonomous instance of a local IDS (LIDS); (2) each LIDS is functionally complete, in the sense that it may execute the whole detection process (e.g. data collection, detection algorithm execution and alert management); (3) LIDS collaborate with each using a mechanism that takes into account the restrictions resulting from the MANET context; e.g. limited bandwidth or poor connectivity.

Figure 4 shows the proposed architecture for the LIDS. Besides of the basic IDS functional modules (e.g. Sensor, Analyser and Manager), Distribution Manger and LIDS Cooperation Protocol are also included in the architecture, in order to cope with the distribution and cooperation requirements.

Sensor: In our process, the data collected for intrusion detection consists of all routing protocol messages, which are obtained from the authentication service. The sensor also maintains information about the neighborhood topology and the protocol message scheduling, which are used to extract information from a new received message that could be relevant to the detection process.

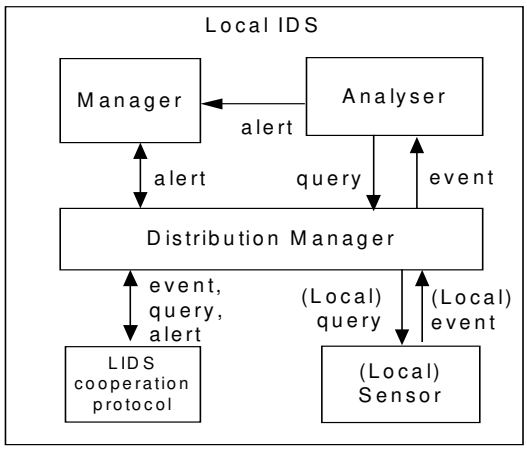

Figure 4 – LIDS Architecture

Analyzer: The Analyzer processes the events according to some defined detection strategy. At least two detection methodologies are currently in discussion: misuse and anomaly detection. Misuse detection relates to the identification of patterns (e.g. event sequences) that characterizes a known attack type, which are called attack signatures. Alternatively, anomaly detection consists in characterizing the normal system behavior and detecting deviations from this normal pattern. In our model, we use the misuse intrusion detection strategy. The principal advantage of the misuse approach relates to the possibility of identification of the attack type being detected and even, in some cases, the identification of the attack source. This last feature is required in our design, as intrusion detection is used to identify misbehaving nodes that must be isolated.

Distribution Manager: This module receives all IDS messages (e.g. event, query and alert), either if the message was locally generated or received from remote nodes, and decides if the message should be consumed locally or if it should be dispatched to a remote node. The IDS Cooperation protocol module implements the communication aspects of the cooperation. Data collection is always local but relevant events may be communicated to other remote nodes in order to help them in the intrusion detection processing. Also, if a LIDS needs to know about an event that may be occurring in a remote node, it can query the remote node by sending a query message.

Collaboration in the Intrusion Response: As a general rule, each node must monitor the behavior of neighbor nodes. LIDS executes this monitoring. If an adversary launches an attack against the routing protocol, correct neighbors receiving the faked routing protocol message may possibly detect the attack. The nodes detecting the attack collaborate with its neighbors to provide intrusion response by signing an accusation (alert) against the detected adversary. This alert is also sent to the local certification service, which signs a partial counter-certificate for the adversary. Partial counter-certificates are flooded in the network. Correct nodes may collect alerts from different nodes detecting and attack. A node collecting, at least, k accusations against the same adversary will also sign a partial counter-certificate for it, even if the node haven't detect any attack coming from that adversary by itself.

4. Implementation and Results

The MAE and the local certification service were implemented along with the available implementation of OLSR v.3. The developed platform was tested in an experimental MANET with 10 nodes running on Linux/Intel laptops with IEEE 802.11b cards. Two of them are playing the role of adversary/compromised nodes. Figure 4 shows a sample topology for the network during experimentation. Note that in this topology, any correct MANET node (e.g. A, B, C, D, E, F, G, H) has neighbor set with minimum size of 3 neighbors. Thus, the number of nodes in certification service coalition was fixed to k = 3 in all experiments. Certification renewal was required at each 60 minutes.

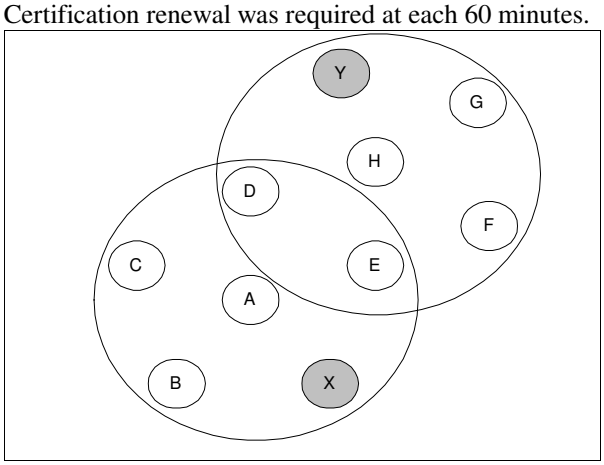

Figure 4 – Experimental Topology

4.1. IDS Design

Sensor: In the present implementation, intrusion detection is exclusively based in data collected from the Management Information Base (MIB), maintained locally in each ad hoc network node by an SNMP agent. Data is extracted directly from the local MIB by simple SNMP queries. The use of this data source is doubled justified. First, because raw data and raw data retrieving has standardized format and process respectively given by the MIB format, which is coded in ASN1, and the SNMP. Moreover, these standard are extensively implemented and adopted in a variety of platforms, providing good portability for the IDS designed in such way. Second, MIB information describes entities of different layers of the node architecture. The Local Sensor is simply a software module that can execute local SNMP queries to the SNMP agent. It should be noted that SNMP is exclusively used in the local host, avoiding the principal shortcomings of the SNMP architecture (e.g. data unreliability and security flaws).

Concerning MIB data collection, high level queries are defined and mapped into respective MIB variables to be queried. Mapping between queries and MIB variables to be evaluated is supplied in the configuration file providing query specification. When scheduled by the Distribution Manager, the query is mapped into the respective query in the Event

Abstractor. The resulting raw data corresponds to the value(s) of the queried MIB variables at the moment of the query execution. Data collection is accomplished by explicitly querying the data source. Two types of queries may be used: queries that are executed only once, which are trigged by a transition in the finite state machine, and queries that are executed periodically.

Analyzer: The IDS Kernel module implements a misuse intrusion detection strategy. Attack signatures should be supplied for all attacks that are aimed to be detected. Signatures are described as finite state diagrams (FSD), which are composed by a finite number of states with defined transitions between then. Each transition is executed as a consequence of one event being triggered. Whenever passing from one state to another (e.g. in a transition), an appropriate action can be activated, which may result in generation of one or more messages among: (1) new (more specific) queries, (2) new events (3) a detection state message (e.g. containing information about the current state in the FDS) or (4) an alert, the last one in case of positive attack detection. Event triggering is related to some particular entity (nodes or service) that has been targeted by an attack (target). The LIDS detecting the attack, which is not placed in the node targeted in the attack, is always signaled in the event/alert generation. Whenever possible, the target of the attack and the entity that originates the attack (attacker) is also signaled by the detection procedure.

Alert Management: The current implementation realizes only a simple alert correlation. The idea is to aggregate multiple alerts generate from different nodes detecting the same attack in a group alert. Whenever a node detects an intrusion, generates an alert and share this alert (by means of mobile agents) with all other nodes participating in the detection process or with its neighbors (if the node have detected the intrusion locally). The nodes caches the alerts generated locally and those received from other cooperating peers. Any node collecting k alerts from different nodes, referring to the same attack can generate a group alert, which is flooded in the network and used for certificate revocation. Alert cache policy is simple timeout, e.g. received/generated alerts are cached during t (a time parameter) seconds. It can be easily shown that such type of group alerts have an improved rate of false positives. Group alerts can be used in attack response (elimination of the node originating the attack from the network).

4.2. Computational and Network Performance Considerations

Overhead of the proposed protocols has been preliminarily evaluated through our experiments with the OLSR implementation. Considering the network overhead, a MAE transmitted without certificates have a fixed size of 136 bytes, for an RSA key of 1024 bits. Average size of OLSR messages depends on the network size and density. For example, in a 100 nodes MANET, which are uniformly distributed over a 1000m x 1000m area and having a transmission range of 200 m, the average size of a HELLO message is 64.26 bytes (each node having an average neighborhood of 12.56 nodes). The high overhead represented by the MAE is due to the use of asymmetric cryptography. In our experiments the message size observed were comparatively smaller, because our real MANET had only 10 nodes. In any case, an OLSR packet containing a HELLO or TC message and a certificate loaded MAE do not oversize the 512-byte packet limit of the OLSR implementation. LIDS network overhead were limited to alert propagation during detection of any attack in the neighborhood of the node detecting the attack.

Computational overhead of the authentication service was evaluated indirectly. The most expensive operation in MAE generation and verification is RSA signature and verification, respectively. In the verification process, two signatures may be verified, if the MAE signer certificate is not cached and must be validated. Time for executing a RSA signature generation and verification (1024-bits key) were averaged in a Pentium III (900MHz, 128Mbytes de RAM, running Red Hat Linux with kernel 2.4.7) to 4.6ms and 12ms, respectively. The normal OLSR packet processing (packet reception) was estimated in 2.5ms. Storage requirements of our proposal are mainly related to certificate cache storage (as CRL can not oversize k, a small constant). If all certificates in the 100 nodes MANET being simulated were locally cached, a 26kbyte cache is due, which is perfectly reasonable. Memory and CPU usage for both the MANET routing protocol daemon (which also implements both authentication and certification services) and for the LIDS process were evaluated. The routing protocol daemon have demonstrated to be by far more resource-consuming than the LIDS process. These evaluations were done in the 10 nodes experimental MANET, which is a short-sized network. However, we believe that these results should not change significantly in larger networks, given the localized design of the security solutions adopted.

5. Related Work

Most of the current research in MANET security is devoted to provision of preventive protection for the routing protocol, usually by means of an authentication service [11,12]. As a general rule, these solutions are not tolerant to the presence of compromised nodes in the MANET. Alternatives approaches are based in the establishment of security associations between nodes, allowing the use of symmetrical cryptography instead of public key cryptography. These associations may be derived from node synchronization such as in [14] or directly form mobility, allowing local security associations only [15]. However, in this approaches we do not have a clear solution for revocation of compromised nodes.

On the other hand, research results on intrusion detection in MANET have only started to appear. Also, most of intrusion detection approaches do not address intrusion response yet. This is the case for [9,3], where

basic MANET IDS architectures have been proposed and preliminary results were presented. The work in [8] is claimed to be an intrusion-tolerant security solution for the AODV protocol. However, the designed solution doesn't incorporate any preventive (authentication) protection. Instead, only a simple neighbor verification mechanism is used. Unfortunately, this mechanism is based in an erroneous assumption that MAC address cannot be spoofed. Moreover, the intrusion detection mechanism limited only to RREP message flooding, which do not generalize to accomplish all the attacks described in terms of fabrication, modification and impersonation of other routing protocol messages.

6. Conclusions

We have presented in this paper a novel security model for MANET networks that incorporates both preventive and corrective protections. The security services designed in our proposal are self-organized and have shown to restrict communication and processing overhead among sets of few nearby nodes. In our approach, vulnerability analysis considers the intrusion detection by defining attack signatures due to anomalies in topology and routing protocol scheduling. The security solution uses both preventive and corrective protections and security services are designed to be self-organized. Finally, the usage of the same authentication service (MAE) for both routing protocol and security service messages was successful, providing some insights for future research on the preventive protection of the security service messages.

REFERENCES

[1] J. Kong, P. Zerfos, H. Luo, S. Lu and L. Zhang, "Providing robust and ubiquitous security support for MANET," IEEE ICNP 2001, 2001.

[2] T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot - Optimized Link State Routing Protocol - IETF Internet Draft, MANET working group, version 11, Jul. 2003.

[3] Puttini, R; Percher, JM; Me, L, Camp, O; de Sousa, R. "A Modular Architecture for a Distributed IDS for Mobile Ad Hoc Networks". Lecture Notes on Computer Science vol. 2669, Springer-Verlag, pp. 91-113, 2003.

[4] L. Zhou and Z. J. Haas. Securing ad hoc networks. IEEE Network Magazine, 13(6):24--30, November/December 1999.

[5] R. Puttini, L. Me, R. de Sousa, "MAE – MANET Authentication Extension for Securing Routing Protocols", 5th IEEE Int. Conf. on Mobile and Wireless Communications Networks, Oct. 2003.

[6] Douceur, J. – The Sybil Attack. 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), February 2002.

[7] L Feeney, B. Ahlgren, A. Westerlund, "Spontaneous Networking: An Application-oriented Approach to Ad Hoc Networking. IEEE Communications Magazine, pp. 176-181, June 2001.

[8] H. Yang, X. Meng and S. Lu, "Self-Organized Network Layer Security in Mobile Ad Hoc Networks", in the Proceedings of ACM Workshop on Wireless Security – 2002 (WiSe'2002), 2002.

[9] Y. Zhang and W. Lee – Intrusion detection in wireless ad hoc networks. Proceedings of 6th Annual International Conference on Mobile Computing and Networking, MOBICOM 2000, ACM, ACM Press New York, pp. 275-283, 2000.

[10] B. Dahill, K. Sanzgiri, B. N. Levine, C. Shields and E. Royer, "A secure routing protocol for ad hoc networks". In the Proc. 2002 IEEE International Conference on Network Protocols, Nov. 2002.

[11] P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan 2002.

[12] M. Guerrero and N. Asokan, "Securing Ad Hoc Routing Protocols", in the Proceedings of 2002 ACM Workshop on Wireless Security (WiSe'2002), 2002.

[13] Y.C. Hu, A. Perrig, D. Johnson, "Efficient Security Mechanisms for Routing Protocols", Proceedings of the 2033 IETF Network and Distributed System Security Symposium (NDSS 2003), 2003.

[14] Y. C. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure On-demand routing protocol for ad hoc networks", in the Proceedings of ACM MobiCom 2002, Sep. 2002.

[15] S. Capkun, J.P. Hubaux, L. Buttyán, "Mobility helps security in ad hoc networks", Proceedings of the fourth ACM international symposium on Mobile ad hoc networking & computing (MobiHoc 2003), pp. 46-56, 2003.