Preventive and Corrective Protection for Mobile Ad Hoc Network Routing Protocols

Ricardo Staciarini Puttini[1], Ludovic Mé[2], and Rafael Timóteo de Sousa Jr.[1]

[1] University of Brasilia, Department of Electrical Engineering, CP 4386,
70919-970 Brasília, Brazil
{puttini, desousa}@unb.br
[2] École Supérieure d'Électricité – Supélec, BP 81127
35511 Cesson-Sévigné Cedex, France
{ludovic.me}@supelec.fr

Abstract. In this paper we describe vulnerabilities and possible protections for mobile ad hoc networks (MANET) routing protocols. Vulnerability and adversary models are built to describe impersonation, fabrication and modification attacks. A security model is proposed, considering both preventive and corrective protection. The basic preventive protection consists of a certificate-based authentication mechanism, which is designed as a MANET authentication extension (MAE) that provides authentication for all routing protocol messages. Corrective protection consists of an intrusion detection and response service (IDS). Certification service and IDS are both provided in a distributed and self-organized manner. Intrusion response is mainly defined in terms of interaction between certification service and IDS. The proposed vulnerability analysis and security design are detailed and validated using the Optimized Link State Routing (OLSR) Protocol.

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, combining both preventive and corrective security services.

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], which is designed to be self-organized and fully localized. An intrusion detection and response system (IDS) provides the corrective solution feeding the certification service with information about misbehaving nodes, which are eliminated from the network by certification revocation. The proposed model is completely developed for protection of the Optimized Link State

Routing (OLSR) Protocol[1]. 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: Section 2 discusses related work. In section 3, we discuss the vulnerability and adversary models defined in our proposal. Section 4 is devoted to description of the security model. Section 5 details the development of the proposed solution for protection of the OLSR. Section 6 describes the implementation and results obtained from experimentation. Finally, section 7 concludes the paper with our final remarks.

2 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 similar to ours [2,3,4]. Alternative 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 [5] or directly from mobility, allowing local security associations only [6]. As a general rule, these solutions are not tolerant to the presence of malicious or compromised nodes in the MANET.

On the other hand, research results on intrusion detection in MANET have only started to appear. Also, published intrusion detection approaches do not address intrusion response yet. This is the case for [7,8], where basic MANET IDS architectures have been proposed and preliminary results were presented. An intrusion detection strategy to deal with non-cooperative nodes in ad hoc networks is presented in [9]. However, there isn't any notion of collaborative security services in this approach.

The work in [10] proposes 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.

3 Vulnerability and Adversary Models

3.1 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

[1] OSPF, AODV, TBRPF and DSR routing protocols are specified in experimental RFCs, which are available from IETF at http://www.ietf.org/html.charters/manet-charter.html.

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.

Each node in MANET keeps local routing information in order to provide the routing service. Nodes use routing protocol messages so share such local routing information. We define an "adversary" as any node announcing erroneous routing information in fabricated, modified and/or impersonated routing protocol messages. Also, a "target" is any node accepting and using this erroneous information.

We admit that modified/fabricated messages have valid syntax. Adversaries may exploit any message defined as mandatory for the routing protocol. If a message is fabricated, the adversary should either masquerade as some node that is already present in the network or use any unallocated network address.

3.2 Adversary Model

Although it might seems that the MANET routing protocol vulnerabilities considered here are quite similar to those from classical routing protocols [11], exploitation of such vulnerabilities are quite different in the MANET, given the particular features of these networks [12]:

- promiscuous nature of the wireless link (adversary may promiscuously listen to wireless transmissions);
- non-centralized, peer-to-peer communication model/lack on infra-structure (adversary may communicate directly with any node within the transmission range of its wireless interface); and
- mobility and dynamic network topology (adversary may move with limited speed to gather information about other nodes or to escape from intrusion detection).

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. Any broken node may be either used to launch routing protocol attacks or may be impersonated. As there is no way to distinguish between these situations, we do not differentiate compromised nodes from adversaries, from the security point of view. Neither do we differentiate insider from outsider adversaries.

4 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 security 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. 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 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 (section 2.2), 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 compromised nodes, excluding them from the routing service. This is accomplished 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 [8]. Fig. 1 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.

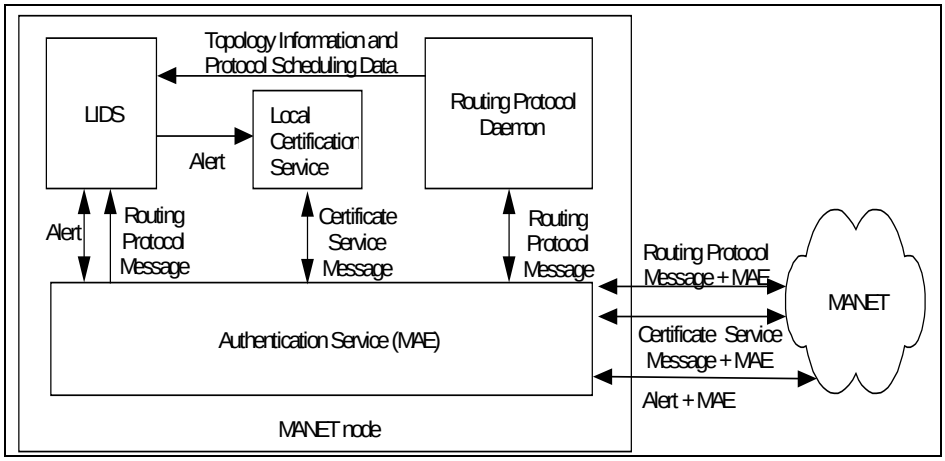

Fig. 1. Routing Protocol Protection Model

Whenever a node is broken, an adversary becomes able to impersonate the compromised node and may fabricate/modify not only routing protocol messages but, also, certificate service messages and alerts (IDS message). 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.

Given that collaboration is done by means of authenticated messages (certificate services and IDS messages are also authenticated with 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, 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 the parameter k.

4.1 MANET Certification Service

The design of self-organized certification services in MANET has been discussed in a few recent papers [1,13], which are based on a distributed certification authority (DCA) trust model. The CA secret key (K_{CA}) is used to sign certificates for all nodes in the MANET. A certificate signed with K_{CA} can be 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 [1]. Each MANET node holds a private-key-share (SK_{CA}) 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 K_{CA}, however, is not recoverable by any node. Counter-certificate issuing does certificate revocation, which must also be signed with K_{CA}. Our proposal is based on [1], with improvements in certification policy specification, local certificate management and multiple DCA support[14].

4.2 Authentication in MANET 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 message syntax unchanged, differently from previous work [2-4].

Authentication Objects: MAE is composed by authentication objects. At least one (mandatory) authentication object should be present in the MAE and alternatively contains a message authentication code (MAC) object, which is computed as a hash-function applied to the data being authenticated keyed with a private-key-shared team key, or a digital signature (DS) object. MAC/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 (keeping additional authentication data related to protection of mutable fields in the packet/message of AODV and DSR) and sequence number (for reply protection) [14].

Mutable Fields: In DSR and AODV, MANET routing protocols there are messages that progressively change while they are forwarded by intermediate nodes in the path between message source and destination. While it is desirable that this mutable information should also be protected, such protection usually implies in increasing the authentication information size each time the message is forwarded. This is not surprising as the information contained in the message is due to all nodes that have previously forwarded it and, each of them should be authenticated in general. Some methods to protect typical mutable information (e.g. hop count, IP address based routing trace, etc.) have been proposed [15] and may be used in our design.

4.3 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) [4] 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 [5]. RREP messages could be simply signed by the target of the route discovery (e.g. the node originating the RREP message).

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	Authentication 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	proactive	link-state	Hello, Topology Control	DS
TBRPF	proactive	link-state	Hello, Topology Update	DS

4.4 Collaborative Intrusion Detection and Response

Present intrusion detection concerns are usually divided in three main processes: data collection, detection algorithm design and alert management. A simple IDS model consists of three modules: Sensor, Analyzer and Manager, each of them being related with one of the intrusion detection processes. More precisely, a Sensor collects data from a data source, an Analyzer processes the collected data for detecting signs of events that might have security concerns and the Manager stands for the management interface of whole process, besides of doing alert correlation and response initiation.

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 described above should be executed in a distributed and cooperative manner [7,8]. 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.

Fig. 2 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.

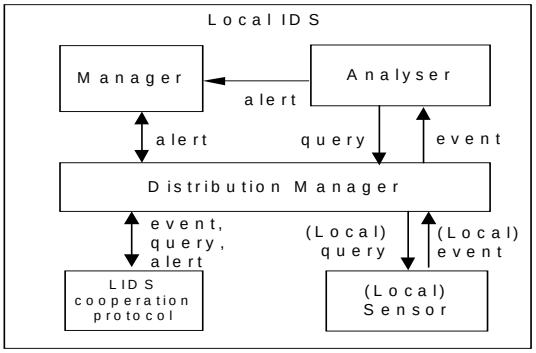

Fig. 2. LIDS Architecture

4.5.1 Sensor: Data Sources

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.

4.5.2 Analyzer: Intrusion Detection Algorithm

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. In misuse IDS, attack signature should be supplied for each attack (or class of attacks) that must be detected. Attack signatures can be generally described by patterns that become observable when the attack is launched. In the case of modification, fabrication and impersonation attacks against the routing protocol, these patterns correspond to anomalies in the scheduling of the routing protocol or inconsistencies in the routing information advertised simultaneously by different nodes.

4.5.3 Collaboration in the Intrusion Detection

The Distribution Manager 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.

4.5.4 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.

Redundancies in the MANET should compensate for the nodes that are not cooperating in the detection and response processes. Indeed, it will be shown that it is possible for more than one single node to track and detect the same attack. If any combination of k nodes in the network detects an attack coming from the same adversary, the adversary's certificate will be revoked.

5 OLSR Vulnerability and Protection Analysis

5.1 OLSR Background

OLSR operates as a table driven proactive routing protocol, which means that it is based on the regular exchange of network topology information between nodes. The topological information is used for updating the routing table of participating nodes

by means of a link-state routing algorithm. The routing metric is always hop-distance. Thus, the protocol gives minimum hop distance routing when the network is in a stable state. Optimization over a pure link state algorithm is obtained by reducing the size of control messages and minimizing flooding of control traffic, which is executed only by some selected nodes called MPR (Multi Point Relays). OLSR communicates using a unified packet format for all data related to the protocol. Each packet is carried in UDP and contains one or more OLSR messages.

The nodes use HELLO messages to detect and update their neighbor set. Each node periodically broadcasts HELLO messages, containing information about heard neighbor interfaces and their link status. The link status may either be "symmetric" (link has been verified to be symmetrical), "heard" (link is asymmetrical), "MPR" (node is selected as MPR, link must also be symmetric) or "lost" (neighbor have moved away). HELLO messages are periodically broadcasted from each node to all 1-hop neighbors and emitted on each MANET interface of the node. These messages are not relayed to other nodes.

Each node in the network independently selects its own MPR set among his "symmetric" neighborhood. The MPR set must be computed by a node in such a way that, through the neighbors in the MPR set, it can reach all symmetric 2-hop neighbors, which are not at the same time symmetric neighbors of the node.

For provision of routes to faraway nodes, each node maintains topological information about the network. This information is acquired by means of OLSR topology control (TC) messages and is used for routing table updates. Nodes that have been selected as MPR by other nodes periodically generate the TC messages, which contain the list of all selector nodes (MS). TC messages are flooded to the whole network by the MPR nodes. A "Message Sequence Number" field is used to avoid duplicated message processing.

5.2 OLSR Vulnerabilities

The attacks being described here rely on the fabrication of OLSR HELLO and TC messages or on modification of OLSR TC messages. All attacks basically have denial-of-service (DoS) effects. Table 2 summarizes the attack identification following the vulnerability model described in section 3.

Table 2 – OLSR Attack Identification

Attack	**OLSR Message**	**Disrupted Information**	**Message Originator Identification**	**Attack Signature**
Fabrication	HELLO	Neighbor List		Inconsistency in routing information
Fabrication + Impersonation	HELLO	Link-status	IP address of target node	Anomaly in the scheduling
Fabrication	TC	MS list		Inconsistency in routing information
Modification + Impersonation	TC	Sequence Number	IP address of target node	Anomaly in the scheduling

5.3 OLSR Message Authentication

None of the OLSR messages (e.g. HELLO, TC, MID, HNA and FRR) has any mutable fields in the message data. However, each message has a message header, which contains a "hop count" and a "time to live" mutable fields. HELLO and FRR messages are broadcasted only in the originator neighborhood, while TC, MID and HNA messages are flooded in the whole network. Given that these fields are not used in the routing table calculation but only in the flooding algorithm (which is robust by itself, provided that there are redundancies in the network topology), no additional protection is required for authentication of the mutable fields. Thus, OLSR MAE consists of a single digital signature, authenticating all fields in message data and in the message header, except from the "hop count" and "time to live" fields, which must be zeroed for the digital signature computation.

5.4 OLSR Intrusion Detection

OLSR intrusion detection is accomplished by implementation of Sensor and Analyzer modules that must, respectively, collect information related to the attacks and analyze the information searching for occurrences of patterns representing signatures for each one of the attack. Whenever detecting an attack, the Analyzer generates the respective alert and pass it to both Manager and Distribution Manager modules, which will collaborate with other nodes to provide the intrusion response. The collected information (Sensor) consists of all HELLO and TC routing messages and some topological information maintained by the routing daemon.

Information analysis (Analyzer) is done whenever a new HELLO or TC message arrives and consists in the identification of the attack signature as described bellow:

- Attack 1: This attack can be characterized by identification of inconsistency in routing information from different HELLO messages. Nodes that hear HELLO messages from both the attacker and correct nodes announced in the fake message will detect the attack by verification of inconsistencies in these messages.
- Attack 2: This attack can be characterized by the anomaly in the scheduling of routing messages related to the reception of both correct and spoofed messages with the same originator information and advertising the link type of some neighbor as "lost" and as "symmetric" in the same HELLO_INTERVAL period.
- Attack 3: This attack can be characterized by the presence of inconsistencies in the routing information advertised simultaneously by different nodes. Fake TC message are flooded in the network and these messages will eventually arrive at the nodes being advertised as MS and at their neighbors. These nodes detects the attack, as advertised nodes don't have the adversary in their neighbor set.
- Attack 4: This attack can be characterized by the anomaly in the scheduling of routing messages. The actual originator node and its neighbors, which receive both correct and modified TC messages, can detect the attack by verifying the occurrence of TC messages from the same originator, advertising the same MS set but with different "message sequence number", during the same TC_INTERVAL period.

6 Implementation and Results

The MAE and the local certification service were implemented along with the available implementation of OLSR v.3. The openssl library was used for the cryptography routines. The LIDS was coded separately, and mobile agents were used for collaborative intrusion detection [8]. Attacks described above were implemented by using the tcpdump packet capture library (libpcap).

The developed platform was tested in an experimental MANET with 10 nodes running on Linux/Intel laptops with IEEE802.11b cards. Two of them are playing the role of adversary nodes. The number of nodes in service coalition was fixed to k = 3 in all experiments. Certification renewal was required at each 60 minutes.

6.1 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 72 bytes, for an RSA key of 512 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 analyzed indirectly by evaluation of RSA signature generation and verification. In the MAE 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 (512-bits key) were averaged in a Pentium III (900MHz, 128M RAM, running Red Hat Linux with kernel 2.4.7) to 9ms and 2.6ms, 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.

6.2 Security Evaluation

Attacks have been successful in corrupting routing when authentication was disabled for the routing protocol. All four attacks were played by two adversary nodes. Attack effects were analyzed for this topology in three different scenarios: (1) with no pro-

tection at all; (2) with only preventive protection (authentication); and (3) with both preventive and corrective (IDS) protections.

In the first scenario, routing disruption was readily obtained and persisted while the adversaries continued to send the fake messages. In the second scenario, the adversaries needed to have a valid certificate to authenticate messages, in order to successfully realize the attacks. This is equivalent of the compromising of some MANET node. If the attacks were played with valid authentication information, the same results that have been observed in scenario 1 for the routing disruption were observed. Finally, in the third scenario, the attack effects on routing disruption were completely mitigated, all the attacks being detected, with no false negatives, by at least 3 nodes (neighbors from the adversaries nodes) that had collaborated to isolate both the adversaries.

Another important issue concerns the choice for the k parameter. Clearly, there is a tradeoff between security and performance/availability in this choice. If k is choose to be lesser then the neighborhood size, all services are locally provided. However, if there are compromised nodes it is possible that there isn't enough correct nodes in the neighborhood for local intrusion detection. In our experiments, we have chosen k = 3 because our neighborhood size is 5, so even in the presence of 2 compromised nodes (the maximum number of compromised nodes allowed in this security solution), we shall have at least 3 correct nodes (the minimum number of nodes required to detect the attack).

The initial certificate distribution in our experiments was done out-of-band but certification renewal automatically executed at each 60 minutes. As long as the correct nodes detects both misbehaving nodes, these cannot renew their certificates.

7 Extension to Other MANET Routing Protocols

OLSR and TBRPF messages do not have any mutable fields that are directly used by the routing algorithm, and so, the authentication data in the MAE for these protocols is a single digital signature. MAE for AODV and DSR must provide additional data to authenticate the mutable fields of these protocol messages, such as additional digital signature (signed by nodes modifying and forwarding the original message [2]) or hash chains [3,4].

LIDS design must be carried out for considering the particular features and vulnerabilities of each MANET routing protocol. More specifically, attack signature should be identified for each routing protocol vulnerability. Nevertheless, the IDS architecture should be effective in any case.

8 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. B. Dahill, K. Sanzgiri, B. N. Levine, C. Shields and E. Royer, "A secure routing protocol for ad hoc networks". In the Proceedings of the 2002 IEEE International Conference on Network Protocols (INCP 2002), Nov. 2002.
3. 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.
4. M. Guerrero and N. Asokan, "Securing Ad Hoc Routing Protocols", in the Proceedings of 2002 ACM Workshop on Wireless Security (WiSe'2002), in conjunction with the ACM MOBICOM2002, September, 2002.
5. 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.
6. 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.
7. Y. Zhang and W. Lee – Intrusion detection in wireless ad hoc networks. Proc. of 6th Annual Int. Conf. on Mobile Computing and Networking, pp. 275-283, 2000.
8. 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.
9. K. Bradley, S. Cheung, N. Puketza, B. Mukherjee and R. Olsson - Detecting disruptive routers: a distributed network monitoring approach, Proceedings of the IEEE Symposium on Security and Privacy, pp. 115 –124, 1998.
10. H. Yang, X. Meng and S. Lu, "Self-Organized Network Layer Security in Mobile Ad Hoc Networks", in the Proc. of ACM Workshop on Wireless Security (WiSe 2002), 2002.
11. F. Wang, F. Wu – On the vulnerabilities and Protection of OSPF Protocol. Proceedings of 1998 International Conference on Computer Communications and Networks, 1998.
12. S. Corson and J. Marker – Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation consideration. RFC 2501 (informational), IETF, 1999.
13. L. Zhou and Z. J. Haas. Securing ad hoc networks. IEEE Network Magazine, 13(6):24-30, November/December 1999.
14. R. Puttini, L. Me, R. de Sousa, "MAE – MANET Authentication Extension for Securing Routing Protocols", in Proc. of the 5th IFIP Int. Conf. on Mobile and Wireless Communications Networks (2003).
15. Y.C. Hu, A. Perrig, D. Johnson, "Efficient Security Mechanisms for Routing Protocols", Proceedings of the 2003 IETF Network and Distributed System Security Symposium (NDSS 2003), 2003.