

# On the Vulnerabilities and Protection of Mobile Ad Hoc Network Routing Protocol

*Authors*

**Keywords:** MANET, routing protocol, security, authentication, IDS

## **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, which is one of the IETF candidates for a MANET routing protocol standard. OLSR attack definition and signature identification, OLSR authentication protection and OLSR IDS design are discussed, as well. Preliminary 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:

- (1) Combination of both preventive and corrective protection;
- 2) Self-organized conception of security services, in the sense that security services are provided collaboratively, without assumption on any centralized entity;

- (3) Fully localized solutions, restricting communication overheads within nearby nodes; and

- (4) 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 [1,2], and designed to be self-organized and fully localized. An intrusion detection and response system (IDS) provides the corrective solution, providing 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 [3]. 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**

Several MANET routing protocols have been proposed [4]. Among those considered to standardization by the IETF MANET working group (WG) in the IETF, none directly addresses security services. Also, there is no single standard yet and it seems that more than one routing protocol may be accepted. At the date this paper

was written, the status of all routing protocol proposals was Internet Draft. Recently, the MANET WG have scheduled four routing protocol proposals to pass through the next step in the standardization process (e.g. publication as Experimental RFC). Table 1 below shows the particular features of each one of these routing protocols.

**Table 1 – Features of MANET routing protocols**

Routing Protocol	Routing Discovery	Routing Algorithm	Relevant Messages
AODV [5]	on-demand	distance-vector	Route Request, Route Reply*, Route Error
DSR [6]	on-demand	source-routing	Route Request, Route Reply
OLSR [3]	proactive	link-state	Hello, Topology Control
TBRPF [7]	proactive	link-state	Hello, Topology Update

A complete vulnerability and protection analysis should address the particular features of each routing protocol. Proceeding with such detailed analysis on each routing protocol can be a very extensive work. Instead, we believe that it is possible to specify vulnerability and protection models that could be applied to some (if not all) of the proposed MANET routing protocols.

## 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.

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<sup>1</sup>.

## 2.2 Adversary Model

Although it might seem that the MANET routing protocol vulnerabilities considered here are quite similar to those from classical routing protocols [8], exploitation of such vulnerabilities are quite different in the MANET, given the particular features of these networks [9]:

- promiscuous nature of the wireless link (nodes are able to monitor neighbors behavior)<sup>2</sup>;
- non-centralized, peer-to-peer communication model (e.g. lack on infra-structure); and
- mobility (dynamic network topology).

<sup>1</sup> We admit that only network (IP) addresses are used to identify the message originator, for the purpose of the routing protocol. While masquerading as another MANET node, an adversary doesn’t need to spoof both network and MAC addresses. We do not rely on network address translation for identification of masqueraded packets.

<sup>2</sup> Link layer access is required for any node participating in a MANET. Should the link layer service uses any kind of authentication and/or encryption (e.g. WEP in IEEE 802.11 networks), a node participating in the MANET must be able to authenticate himself and/or to encrypt/decrypt link layer frames. We do not elaborate on link layer security issues.

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 [2]. 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 (see note 1), we do not differentiate compromised nodes from adversaries, from the security point of view. Neither do we differentiate insider from outsider adversaries.

Note that, if any authentication is required for the routing protocol messages, an adversary must compromise a node and impersonate it in order to generate any attack against the routing protocol.

Finally, we admit that multiple attackers can coexist in the network and may collaborate on the purpose of system break-ins.

### 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 security services cannot rely on a central entity.

- **Intrusion Tolerance<sup>3</sup>:** security solution should be robust in the existence of compromised nodes in the network, given the non-negligible probability for node break-ins.
- **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.

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.

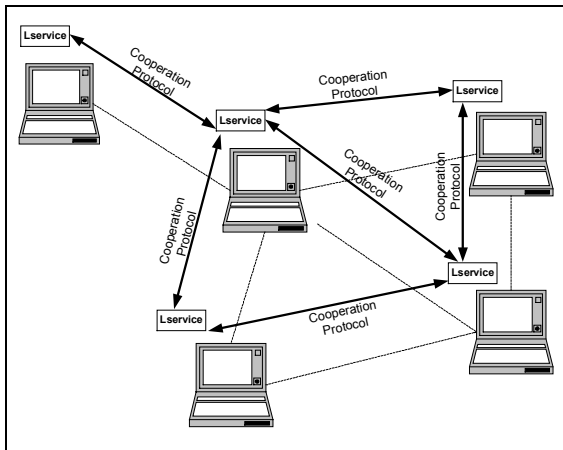
Self-organization is illustrated in Figure 1. An autonomous instance of each security service must be active in each MANET node. These instances are generally called Local Service (L-Service). A L-Service collaborates with L-Services from nearby nodes (usually in the neighborhood), by means of some collaboration 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, and 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

---

<sup>3</sup> We use “intrusion tolerance” in the sense that our security model is robust even in the presence of some compromised nodes in the network.



**Figure 1 – Model for self-organized services**

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 malicious/compromised nodes, excluding them from the routing service. This is accomplished basically by means of certificate revocation.

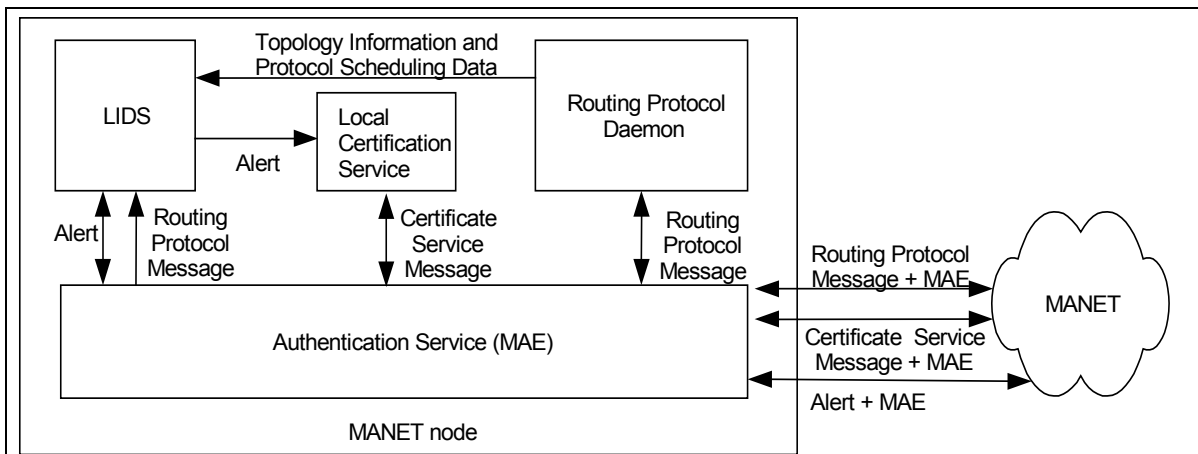
Certificate services (issuing, renewal, revocation and validation) and intrusion detection and response should be provided in a self-organized and distributed manner by a Local Certification Service and an local IDS (LIDS) instances [10]. Figure 2 illustrates the proposed protection model.

Basically, routing protocol, certificate 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 certificate 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.

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 at least k different nodes.

Correct nodes running the LIDS should detect the attacks against the routing protocol<sup>4</sup> and isolate the compromised node (by revoking its certificate) before that an adversary can compromise k nodes, breaking the collaborative security system.

<sup>4</sup> As stated above, the attack can also be executed against the local certification service or the LIDS. We do not elaborate in the detection on these attacks, at this moment.



**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 consists 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 (certificate renewal service, which is provided by any other  $k$  nodes), 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 the parameter  $k$ .

When trying to compromise other nodes, an attacker should act incorrectly in the behalf of the compromised node (impersonation).

### 3.1 MANET Authentication Extension

For prevention against modification, impersonation and fabrication attacks, the authentication service should provide both integrity and authenticity protection to the routing protocol messages.

Concerning the authentication service, nodes are identified by means of a digital certificate and authentication uses asymmetric cryptography primitives, such as RSA. In such design, each node has a private/public key pair and the digital certificate is used to bind the node's identity and public key. Note that network addresses (IP) are not used as the node's identity, in the concerns of the authentication service. Using certificates to

bind IP address and public key seems to be a non-realistic approach, as roaming nodes can change his IP address even dynamically or randomly.

A MANET authentication extension (MAE) is appended to each message being authenticated. MAE contains all the information needed to authenticate the information supplied in the message. Specially, MAE contains a digital signature, which is computed as a function of the message fields and the private key of the node signing it (message originator). Such digital signature readily provides authentication for all non-mutable fields of the routing protocol message<sup>5</sup>.

Certificates are even publicly distributed in the MANET and cached in each node or attached to the messages along with the digital signature (e.g. included in the MAE).

### 3.2 Collaborative Certification Service

The design of a certification service to be used with the MAE authentication service is discussed in this section.

Conventional PKI based certification systems [11] are not adequate to MANET, given the absence of central entities in the network. The unreliable and bandwidth constrained communication channel and the restricted computational resources available in MANET nodes impose additional performance requirements on the certification service design. Furthermore, MANET is self-organized in nature and MANET certification service should be likewise designed.

In our design, certification services are provided in a distributed and collaborative manner. Certification services are based in a distributed certification authority (DCA) trust model [1,2,12]. The CA secret key (SK) is used to sign certificates for all nodes in the MANET. A certificate signed with SK can be readily verified with the well-known system public key (PK). The distribution of the CA capabilities is achieved by sharing the

---

<sup>5</sup> If a routing protocol message has mutable fields that are directly used by the routing algorithm, the information supplied in these fields must also be authenticated and the MAE encapsulates the data used to authenticate the mutable fields along with the digital signature authenticating all non-mutable fields. Authentication of mutable fields in the routing protocol messages is out of the scope of this paper.

secret key among network nodes by means of threshold cryptography techniques [13]. Each MANET node  $n_i$  holds a secret share ( $SS_i$ ) and any  $k$  (a system wide constant, usually related with the average number of neighbors) of such secret share holders can collectively function as a CA. The SK, however, is not recoverable by any node. Thus, the system is said to be  $k$ -by- $n$  secure.

Certification revocation is done by counter-certificate issuing, which must also be signed with SK. Certification revocation lists (CRL) are kept locally at each node.

Collisions of  $k$  secret share holders are dynamically established to provide three basic services: (1) certificate signature (used in issuing, renewing and revoking certificates); (2) issuing of new secret shares (used to initialize arriving nodes); and (3) secret share update (which is realized periodically to avoid that an intruder could have unlimited time to progressively compromise different MANET nodes, breaking the system trust after compromising the  $k^{\text{th}}$  node). This last service is directly related with intrusion tolerance, in the sense that the overall system security is conditioned to a distributed intrusion detection mechanism that should be able to track and isolate misbehaving nodes from the network, before that an adversary could compromise  $k$  nodes.

Our proposal is adapted from [1,2]. Certificate issuing, renewal and revocation, as well as secret share issuing and updating are directly taken from them, while node initialization, local certificate cache and CRL and usage with multiple DCA are proposed in this paper.

### 3.2.1 Basic Certification Services

Basic certifications services include certificate issuing, renewal and revocation.

#### **Certificate Issuing and Certificate Renewal**

Technically, there is no difference between certificate issuing and renewal, but the policies for doing such services are specified separately. Whenever a node needs to receive a new certificate, he locally prepares a certificate request, which must contain the node's identity information and his public key. If the node is requesting a certificate renewal, the old (but not expired) certificate is also sent with the certification request. Any secret share holder receiving the certification request may answer the request. If a valid certificate is found along with

the certification request, the request is treated as a certificate renewal. Otherwise, the request is viewed as a new certificate-issuing request. The appropriate policy for issuing the new certificate is applied accordingly. If the node decides to answer the certification request, it signs the certification request with his secret share, generating a partial certificate request (as the signed certificate is not yet signed with SK), which should be unicasted back to the requester. Whenever  $k$  valid partial certificates are received, the requester can compute his new certificate. The reader interested in cryptography details should refer to [14].

In our approach, different policies are specified for certificate renewal and certificate issuing. Any node receiving a certificate renewal request will decide to sign the certificate for that node only if it hasn't detect any misbehavior for that node (e.g. by mean of the LIDS). Policy for certification issuing is discussed in section 3.2.3.

#### **Certificate Revocation and CRL**

The certificate revocation is done by signing a counter-certificate with SK. Counter-certificate data must include the identification of the certificate being revoked (e.g. the certificate serial number) and the revoking time. The decision for signing a counter-certificate should be taken in two different cases: self-revocation and intrusion detection revocation.

Self-revocation is done when any node decides to revoke his own certificate (e.g. due to the exposure of its private key). To do that, the node broadcasts a self-signed counter-certificate in his neighborhood. Any node receiving a self-signed counter-certificate generates a partial counter-certificate by signing the original counter-certificate with their SS.

Intrusion detection revocation relates to intrusion reaction. When a node detects a misbehaving node, he creates a partial counter-certificate for the compromised node by signing a counter-certification with its secret share. When  $k$  different nodes have detected the same node as a misbehaving one,  $k$  partial counter-certificates should have been generated.

In both self-revocation and intrusion detection revocation, the partial counter-certificates being generated are immediately flooded into the network. Any node receiving  $k$  partial counter-certificates can recover the SK signed counter-certificate, which is also flooded in the network. Any node receiving/recovering a signed counter-

certificate must store the certificate in his local CRL.

Counter certificates are maintained in the CRL while the current time ( $t_{now}$ ) is lesser than the revoked certificate expiration time ( $t_{exp}$ ), e.g.  $t_{now} < t_{exp}$ .

### 3.2.2 *Secret Share Issuing*

Secret share issuing process is used to initialize the nodes that do not have a secret share, but holds a valid certificate. The SS issuing proceeds in 6 steps of communication:

- (1) The uninitialized node broadcasts the service request along with his certificate.
- (2) Secret share holders decide if the certification policy authorizes to serve the requested service and, if so, these nodes unicast back to the requester a service request acknowledgement, along with their certificates.
- (3) The uninitialized node selects  $k$  nodes with valid certificates among all answering nodes to form a  $k$ -nodes coalition and then broadcasts the service request along with the coalition information.
- (4) Each coalition member selects a random nonce for each other members if his public key is lower than the other one. Each nonce is encrypted with the public key of the uninitialized node, which will act as a router for the  $k-1$  nonces being generated.
- (5) The requester routes encrypted nonces to intended receivers.
- (6) Each coalition member decrypts all nonces, computes a shuttled partial secret share and then unicasts it back to the requester, which will be able to recover the secret share after collecting partial secret shares for all nodes in the coalition.

Once more, the reader should refer to [14] for the cryptography details.

### 3.2.3 *Node Initialization*

A node will be able to authenticate a message using the MAE only if it holds a valid certificate (and associated private key). Also, a node will be able to participate in the collaborative certification service only if it holds a secret share. Thus, any node wanting to participate in our security solution

must be initialized with a valid certificate and a valid SS.

One possible solution consists in requiring the nodes to be initialized by a trusted centralized CA (*dealer*). The centralized CA proceeds with node identity verification (which may involve some kind of out-of-band procedures) and both certificate and SS issuing. The certificate issuing policy is very important to the overall security solution, as an adversary may exploit permissive policies for obtaining digital certificates and SS.

According to our distributed certification service approach, whenever there is, at least,  $k$  initialized nodes in the network, these nodes may collaboratively provide the certification services for initializing other arriving nodes. Thus, the centralized CA (*dealer*) is required only in the bootstrap of the network, for initializing the first  $k$  nodes. Note that each node providing certification services to node initialization (e.g. partial certificate/SS issuing) must apply the same policy of the centralized CA for verification of the requester identity (same out-of-band procedures). If identity verification is not assured, an adversary can compromise the overall system security by forging multiple identities and recovering  $k$  different SS (sybil attack [15]).

### 3.2.4 *Secret Share Update*

Secret shares in the network should be updated proactively to limit the time available to an adversary for compromising of  $k$  nodes. Thus, for compromising SK, one intruder should be able to compromise  $k$  nodes during the time between two consecutive secret share updates. The algorithm being used in our model is the parallel secret share update from [2].

### 3.2.5 *Local Certificate Cache and CRL*

Some local data should be permanently stored in each node participating in the certification service. These data includes: the node's private key and certificate, valid certificates for each trusted CA, a secret share (if any) along with a secret share version and a PK encrypted polynomial for secret share update along with an update version.

Each node also dynamically maintains: a table with (cached) valid certificates, a table with revoked certificates (local CRL) and a table with partial counter-certificates. Table entries should be automatically removed when  $t_{now} < t_{exp}$ . Valid certificate table entries are maintained during a

maximum period of ( $t_{out}$ ), after last usage. The valid certificate table can also have a maximum number of entities. Whenever this number is achieved, the entry with earlier expurgating time are removed to free room for new entries being placed in the table. Entries in the partial counter-certificate table must also be removed if the certificate from the signer is revoked (e.g. the counter-certificate might have been issued by a compromised node).

### 3.2.6 Usage with Multiple DCA

Nodes trusting and being trusted by more than one CA should apply for certificate and secret shares from each CA. Such nodes can be used as proxies between two groups of nodes in the network trusting in different CAs, which are both trusted by the proxy node. Alternatively, a cross trust relation between the nodes trusting in two different CAs (e.g. CA1 and CA2) can be established if there are, at least,  $k$  nodes trusting both CAs. This is simply done by generating a certificate for CA1 and a certificate for CA2 that are signed by  $k$  secret shares from CA2 and CA1, respectively. The CAs certificates generated in this processes should be flooded in the network, finalizing the cross trust relation establishing. Establishing of cross trust relation is also controlled by the certification policy.

### 3.3 Collaborative Intrusion Detection and Response

Present intrusion detection concerns are usually divided in three main processes: data collection, detection algorithm design and alert management [16].

The requirement specification from the IETF Intrusion Detection Exchange Format Working Group (IDWG)<sup>6</sup> proposes an IDS model consisting of three modules: Sensor, Analyzer and Manager, each of them being related with one of the intrusion detection processes [16]. 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.

<sup>6</sup> Official charter can be found at: <http://www.ietf.org/html.charters/idwg-charter.html>

The IDWG model also defines messages (or data flows) exchanged by these elements. Thus, activities monitored by the Sensor in the data source may be mapped in events, which are passed to the Analyzer, where they are submitted to the detection algorithm. When the Analyzer finds events with relevant security concerns, alerts are generated to the Manager.

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 [10,18]. 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 3 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 modules are also included in the architecture, in order to cope with the distribution and cooperation requirements.

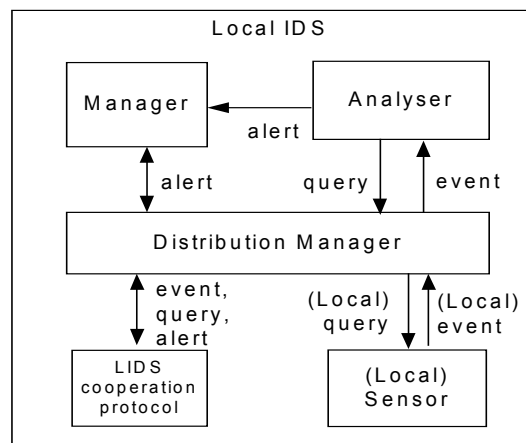


Figure 3 – LIDS Architecture

#### 3.3.1 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.

### 3.3.2 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 [19]. 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. If such attack signatures are available, the IDS can be designed as a monitoring system that identifies occurrences of patterns during the routing protocol operation, associated with attacks.

### 3.3.3 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.

### 3.3.4 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.

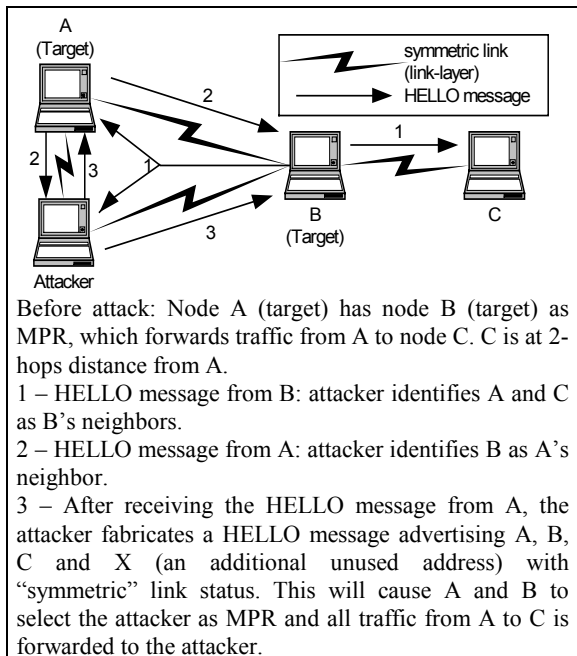
## 4 OLSR Vulnerability and Protection Analysis

### 4.1 OLSR Background

The status of the OLSR specification is Internet Draft [3]. 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 a UDP datagram 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),



**Figure 4 – Routing Disruption by Fabrication of HELLO Messages**

“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.

#### 4.2 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 2.1.

##### 4.2.1 Attack 1: Routing Disruption by Fabrication of HELLO Messages

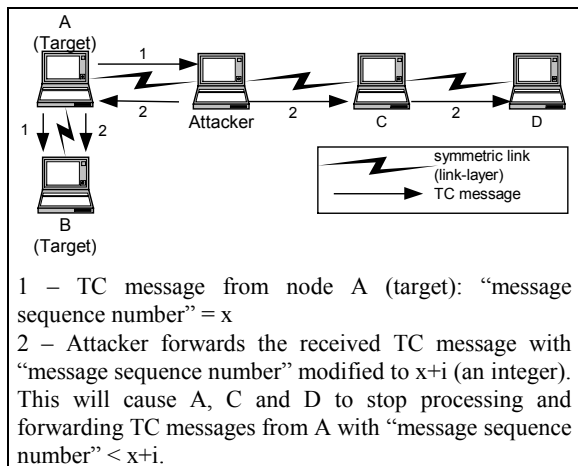
In this attack, showed in Figure 4, the adversary

**Table 2 – OLSR Attack Identification**

Attack	OLSR Message	Routing Information Disrupted	Originator Identification in Disrupted Message	Attack Signature	Attack Example
Fabrication	HELLO*	Neighbor List		Inconsistency in routing information	Section 4.2.1
Fabrication + Impersonation	HELLO*	Link-status	IP address of target Node	Anomaly in the scheduling	Section 4.2.2
Fabrication	TC**	MS list		Inconsistency in routing information	Section 4.2.3
Modification + Impersonation	TC**	Sequence Number	IP address of target node	Anomaly in the scheduling	Section 4.2.4

\*HELLO messages are sent only to 1-hop neighbors, and modification attacks do not apply to such messages.

\*\*TC messages are flooded into the network.



**Figure 6 – Routing Disruption by Modification of TC Messages**

fabricates a HELLO message advertising all nodes previously announced in any HELLO message received by the adversary, along with one additional unused address, with “symmetric” link status. This should cause target nodes to select the attacker as MPR. Traffic going from/through the target toward nodes that are not direct neighbors is forward to the adversary node.

*4.2.2 Attack 2: Routing Disruption by Fabrication+Impersonation of HELLO Messages*

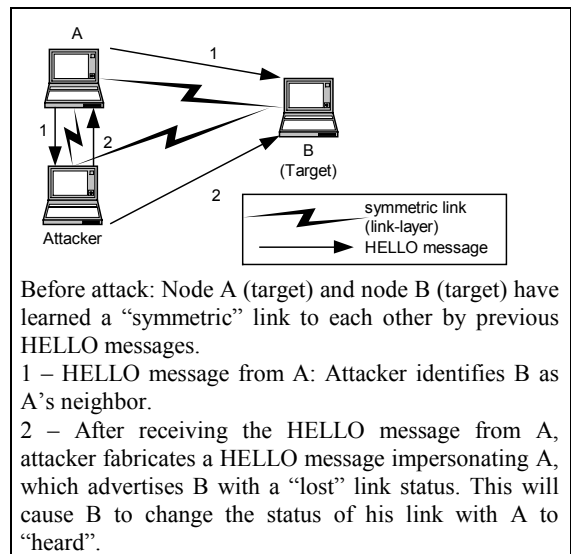
Figure 5 illustrates this attack, where one attacker should generate a spoofed HELLO message after receiving a correct HELLO message, advertising all nodes announced in correct message with “lost” link status. The node being impersonated is the same node that originated the correct message. When receiving the faked HELLO message, all nodes that have their address advertised in the message would have the status of the link with the target changed to “heard” and would stop routing traffic through this link.

*4.2.3 Attack 3: Routing Disruption by Fabrication of TC Message*

In this attack (Figure 7), the attacker fabricates a TC message advertising faraway nodes as part of his MS set. This should cause targets to choose routing to these faraway nodes through the attacker.

*4.2.4 Attack 4: Routing Disruption by Modification of TC Message*

In this attack (Figure 6), the attacker changes the “message sequence number” of a TC message,



**Figure 5 – Route Disruption by Fabrication + Impersonation of HELLO Messages**

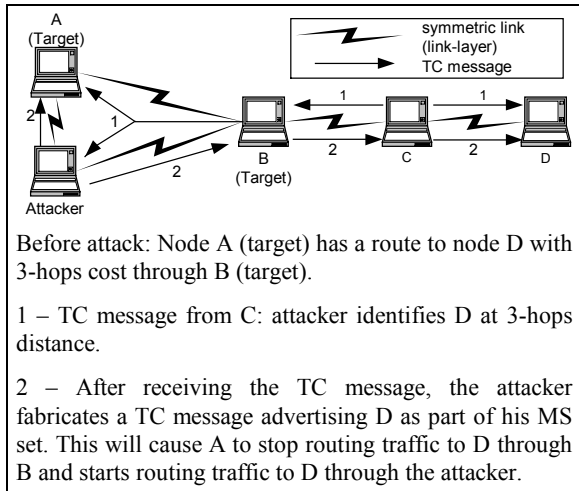
before forwarding it. The “message sequence number” in the modified message is obtained by adding the advertised “message sequence number” with some integer value. Such attack would stop the processing and forwarding of TC messages from the node advertised as originator in the TC message in the whole network<sup>7</sup>.

**4.3 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

<sup>7</sup> A “fight back” strategy is not defined in the OLSR draft and the modification of only one TC message can disturb the routing protocol for a long time. We suggest that some kind of “fight back” should be included in the processing of TC messages when a node receives a TC message with its own address advertised as originator and a “message sequence number” greater than the present “message sequence number” used by the node. This would be similar to the OSPF “fight back” strategy [8].

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.



**Figure 7 – Routing Disruption by Fabrication of TC Messages**

#### 4.4 OLSR Intrusion Detection

OLSR intrusion detection is accomplished by implementation of Sensor and Analyzer modules that must, respectively, collect information related to the attacks described in section 4.2 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 (e.g. 1-hop and 2-hop neighbor tables).

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

- Attack 1: This attack can be characterized by identification of inconsistency in routing information from different HELLO messages. Nodes that can hear HELLO messages from both the attacker and some other node that is not heard by the attacker can 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” (or “MPR”) 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. As the fake TC message should be flooded in the network, this message will eventually arrive at the nodes being advertised as MS and at their neighbors, as well. These nodes can detect the attack, as advertised nodes do not 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.

## 5 Implementation and Results

The MAE and the local certification service were implemented along with the available implementation of OLSR v.3. The *openssl* library<sup>8</sup> was used for the cryptography routines. The LIDS was coded separately, and mobile agents were used for collaborative intrusion detection [20]. Attacks described above were implemented by using the *tcpdump* packet capture library (*libpcap*)<sup>9</sup>.

The developed platform was tested in an experimental MANET with 10 nodes, 2 of them playing the role of adversary/compromised nodes. Figure 8 shows a sample topology for the network

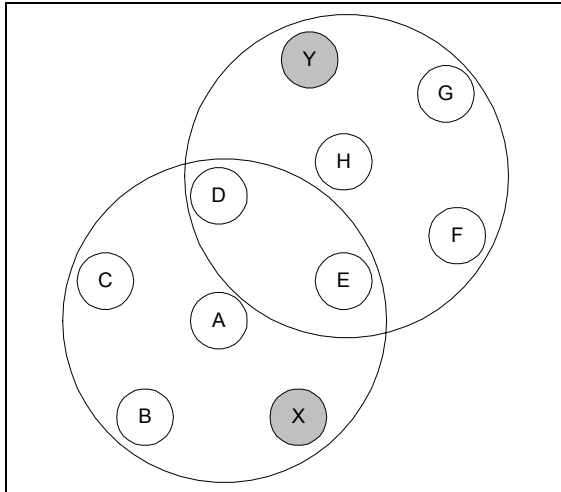
<sup>8</sup> Information on openssl can be found in <http://www.openssl.org>

<sup>9</sup> Information on tcpdump and libpcap can be found in <http://www.tcpdump.org>.

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.

Attacks have been successful in corrupting routing when authentication was disabled for the routing protocol. All four attacks were played by the adversary nodes X and Y. Attack effects were analyzed for this topology in three different scenarios: (1) with no protection at all; (2) with only preventive protection (authentication); and (3) with both preventive and corrective (IDS) protections.

Table 3 summarizes the observed attack effects in the correct node A suffering attacks from X.



**Figure 8 – Experimental Topology**

<b>Table 3 – Effects on A / Attacks from X</b>				
<b>Attack</b>	<b>Message generated</b>	<b>MPR set before attack</b>	<b>MPR set during attack</b>	<b>Nodes detecting the attack*</b>
1	Hello, with B,C,D,E,F,H ,Z = “sym”	E	X	A,B,E
2	Hello, with B,C,D,E = “lost”, spoofing E	E	D	A,B,E
3	TC, with F,G,H	E	E,X	A,D,F, G,H
4	TC from E, with	E	D	A,B,C,D, E,F,G,H

	modified NS			
--	-------------	--	--	--

\* only in the 3rd scenario

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, any of the attacks being detected for, at least, 3 nodes that had collaborated to isolate both the adversaries.

### 5.1 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 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 (512-bits key) were averaged in a

Pentium III (900MHz, 128Mbytes de 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.

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.

## 5.2 Extension to Other MANET Routing Protocols

OLSR [3] and TBRPF [7] 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 [5] and DSR [6] 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 [21]) or hash chains [22,23].

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.

## 6 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 [21, 22,23]. As a general rule, these solution are not tolerant to the presence of 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 [18,20], where basic MANET IDS architectures have been proposed and preliminary results were presented.

An intrusion detection and response strategy to deal with non-cooperative nodes in ad hoc networks is presented in [24]. However, there isn't any notion of collaborative security services in this approach.

The work in [17] 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.

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.

## 7 Conclusions and Future Work

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.

Let us finish with some concluding remarks on future work:

Mobility analysis was only carried out in theory. Simulations are being carried out on this issue, specially in the concerns of false positive (a node moves/fails/leaves and temporary topology inconsistency is detected) and false negatives (an attacker moves to avoid it certificate for being revoked) in the intrusion detection, due to mobility.

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] H. Luo, P. Zerfos, J. Kong, S. Lu and L. Zhang, "Self-securing Ad Hoc Wireless Networks", in the Proceeding of Seventh IEEE International Symposium on Computer and Communications (ISCC'02), 2002.
- [3] T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot - Optimized Link State Routing Protocol - IETF draft, MANET working group, version 8, March 2003.
- [4] Y. Chun, L. Qin, L. Yong and Shi MeiLin – Routing protocols overview and design issues for self-organized network. Proceedings of IEEE International Conference on Communication Technology - ICCT 2000, Vol., pp. 1298-1303, 2000.
- [5] C. E. Perkins, E. M. Royer, and S. R. Das. Ad hoc on-demand distance vector (AODV) routing. IETF INTERNET DRAFT, MANET working group, version 13, Feb. 2003.
- [6] D. B. Johnson et al, "The dynamic source routing protocol for mobile ad hoc networks (DSR)", INTERNET DRAFT, MANET working group, version 8, Feb. 2003.
- [7] R. Ogier, M. Lewis, F. Templin and B. Bellur, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)", INTERNET DRAFT, MANET working group, <draft-ietf-manet-tbrpf-06.txt>, November 2002.
- [8] F. Wang, F. Wu – On the vulnerabilities and Protection of OSPF Protocol. Proceedings of 1998 International Conference on Computer Communications and Networks, 1998.
- [9] S. Corson and J. Marker – Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation consideration. RFC 2501 (informational), IETF, 1999.
- [10] *Reference anonymized for the review process.*
- [11] R. Housley; W. Ford; W. Polk and D. Solo - Internet X.509 Public Key Infrastructure: Certificate and CRL Profile - RFC 3280, IETF Network Working Group, April 2002.
- [12] L. Zhou and Z. J. Haas. Securing ad hoc networks. IEEE Network Magazine, 13(6):24--30, November/December 1999.
- [13] A. Shamir – How to Share a Secret. Communications of the ACM, 22(11):612-613, 1979.
- [14] H. Luo and S. Lu, "Ubiquitous and robust authentication services for ad hoc wireless networks," UCLA Computer Science Technical Report 200030, Oct. 2000.
- [15] Douceur, J. – The Sybil Attack. 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), February 2002.
- [16] Wood and Erlinger – Intrusion detection message exchange requirements. IETF Internet Draft, June 2002.
- [17] 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), in conjunction with the ACM MOBICOM2002, September, 2002.
- [18] Y. Zhang and W. Lee – Intrusion detection in wireless ad hoc networks. Proceedings of 6<sup>th</sup> Annual International Conference on Mobile Computing and Networking, MOBICOM 2000, ACM, ACM Press New York, pp. 275-283, 2000.
- [19] H. Debar, M. Dacier and A. Wespi - A revised taxonomy for intrusion-detection systems, IBM Research Report, Zurich, 1999.
- [20] *Reference anonymized for the review process.*
- [21] 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.
- [22] 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.
- [23] 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.
- [24] 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.