Detecting Unauthorized and Compromised Nodes in Mobile Ad-Hoc Networks

Nikos Komninos*, Dimitris Vergados*, Christos Douligeris**

*Department of Information and Communication Systems Engineering
University of the Aegean,
83200 Samos Greece
komninos@aegean.gr, vergados@aegean.gr

**Department of Informatics
University of Piraeus
18534 Piraeus Greece
cdoulig@unipi.gr

Abstract

Security of mobile ad-hoc networks (MANET) has become a more sophisticated problem than security in other networks, due to the open nature and the lack of infrastructure of such networks. In this paper, the security challenges in intrusion detection and authentication are identified and the different types of attacks are discussed. We propose a two-phase detection procedure of nodes that are not authorized for specific services and nodes that have been compromised during their operation in MANET. The detection framework is enabled with the main operations of ad-hoc networking, which are found at the link and network layers. The proposed framework is based on zero knowledge techniques, which are presented through proofs.

Keywords: mobile ad-hoc networks, authentication, intrusion detection, compromised nodes.

1. Introduction

An ad-hoc network is a collection of nodes that do not need to rely on a predefined infrastructure to keep the network connected. Nodes communicate amongst each other using wireless radios and operate by following a peer-to-peer network model. Such networks are also referred to as mobile ad-hoc networks (MANET) [5]. Unlike networks using dedicated nodes to support basic functions like packet forwarding, routing, and network management, in ad-hoc networks these functions are carried out by all available nodes [11]. Applications of mobile ad-hoc networks range from military tactical operations to civil rapid development such as emergency search-and-rescue missions, data collection/sensor networks, and instantaneous classroom/meeting room applications.

The nature of the wireless and mobile environment makes it vulnerable to an adversary's malicious attacks. Such networks are susceptible to attacks ranging from

passive eavesdropping to active interfering. Unlike wired networks where an adversary must gain physical access to the network wires or pass though several lines of defense at firewalls and gateways, attacks on a wireless network can come from any direction and target all nodes. Therefore MANETs, do not have a clear line of defense, and every node must be prepared for encounters with an adversary directly or indirectly.

In MANETs, nodes are receptive to being captured, compromised, and hijacked since they are units capable of roaming independently. Since tracking down mobile nodes is difficult to achieve, attacks by compromised nodes are far more damaging and much harder to detect. Therefore, nodes and network infrastructure must be prepared to operate in a non-trusting mode. Furthermore, the lack of a centralized authority gives ground to adversaries to exploit new types of attacks and break the required for efficient operations cooperative algorithms.

In this paper, we propose a two-phase detection procedure of nodes that are not authorized for specific services and nodes that have been compromised during their operation in MANET. The detection framework is enabled with the main operations of ad-hoc networking, which are found at the link and network layers. The proposed framework is based on zero knowledge techniques, which are specifically designed to achieve node identification but do not rely on symmetric or asymmetric encryption algorithms, digital signatures, sequence numbers and timestamps. The zero knowledge techniques are presented through proofs.

This paper is organized in the following five sections. Section 2 presents the types of attacks that exist in ad-hoc networks. Sections 3 and 4 discuss the challenges and related work in intrusion detection and present authentication models developed for ad-hoc networks. Section 5 describes the detection framework and discusses how unauthorized and compromised nodes are discovered. Finally, section 6 concludes the paper by presenting on areas that need further study.

2. Attacks in Mobile Ad-Hoc Networks

Similar to other wireless networks, ad-hoc networks are susceptible to ***passive*** and ***active*** attacks [1]. Passive attacks typically involve only eavesdropping of data, whereas active attacks involve actions performed by adversaries such as replication,

modification and deletion of exchanged data. In particular, attacks in ad-hoc networks can cause congestion, propagate incorrect routing information, prevent services from working properly or shut them down completely [2, 8, 14, 17, 29, 30].

Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered to be *malicious*, also referred to as *compromised*, while nodes that just drop the packets they receive with the aim of saving battery life for their own communications are considered to be *selfish* [12, 14]. A selfish node affects the normal operation of the network by not participating in the routing protocols or by not forwarding packets. In addition, a compromised node may use the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept as in the so called *black hole attack* [19, 29].

Compromised nodes can interrupt the correct functioning of a routing protocol by modifying routing information and by fabricating false routing information. Recent research studies have also brought up a new type of attack that goes under the name of *wormhole attack* [26, 27]. In the latter, two compromised nodes create a tunnel (or wormhole) that is linked through a private connection and thus they by-pass the network. This allows a node to short-circuit the normal flow of routing messages creating a virtual vertex cut in the network that is controlled by the two attackers [13, 15].

On the other hand, selfish nodes can severely degrade network performance and eventually partition the network by simply not participating in the network operation. Compromised nodes can easily perform *integrity attacks* by altering protocol fields in order to subvert traffic, denying communication to legitimate nodes and compromising the integrity of routing computations in general. *Spoofing* is a special case of integrity attacks whereby a compromised node impersonates a legitimate one due to the lack of authentication in the current ad-hoc routing protocols [11, 20].

The main result of a spoofing attack is the misrepresentation of the network topology that may cause network loops or partitioning. Lack of integrity and authentication in routing protocols creates *fabrication attacks* [3, 6, 22] that result in erroneous and bogus routing messages.

Denial of service (DoS) is another type of attack, in which the attacker injects a large amount of junk packets into the network. These packets overspend a significant portion of network resources, and introduce wireless channel contention and network contention in ad-hoc networks [4, 5]. In addition, the *routing table overflow attack*, where an attacker attempts to create routes to nonexistent nodes and the *sleep deprivation attack*, where an attacker tries to consume the batteries of a node, are two other types of DoS attacks [10].

3. Intrusion Detection Challenges

When a set of actions that attempt to compromise the integrity, confidentiality, or availability of a mobile node takes place, intrusion prevention techniques, such as encryption and authentication, are usually the first line of defense. However, intrusion prevention alone is not sufficient when systems become more complex and as security is often the after-thought. There are always weaknesses in the systems due to design and programming errors, or various "socially engineered" penetration techniques.

For example, even though exploitable "buffer overflow" security holes, which can lead to an unauthorized root shell, were first reported many years ago they still exist in some recently released system software. Furthermore, as illustrated by the Distributed Denial-of-Services (DDoS) attacks launched against major Internet sites where security measures were in place, the protocols and systems that are designed to provide services are inherently subject to attacks such as DDoS. Intrusion detection can be used as a second wall to protect network systems because once an intrusion is detected, a response must be put into place to minimize damages.

By definition, intrusion detection involves capturing data and reasoning about the evidence in the data to determine whether the system is under attack [2, 19, 21, 22, 24, 29]. The most important difference between fixed networks and MANETs is perhaps that the latter do not have a fixed infrastructure. Compared with wired networks where traffic monitoring is usually done at switches, routers and gateways in a network-based intrusion detection system (IDS), the mobile ad-hoc environment does not have such traffic concentration points and therefore can be categorized as host-based IDS.

While network-based IDS look at all the traffic in a network, host-based IDSs [19, 22, 24] are concerned with what is happening on each individual node. They are able to detect actions such as repeated failed access attempts or changes to critical system files, and normally operate by accessing log files or monitoring real-time system usage. Furthermore, there may not be a clear separation between normalcy and anomaly in a mobile environment. A node that sends out false routing information could be the one that has been compromised, or merely the one that is temporarily out of sync due to volatile physical movement.

There have been several studies on security detection measures for infrastructure based wireless networks, such as [2, 19, 22, 24, 29]. On the prevention side, general approaches such as key generation and management have been used in a distributed manner to ensure the authenticity and integrity of routing information [5, 7, 9, 30].

Zhou and Haas [17] introduced a routing protocol-independent distributed key management service. This approach uses redundancies in the network topology to provide reliable key management. The main idea is to be able to use key sharing even with a maximum threshold ratio of compromised nodes to total nodes.

The difficulties in realizing all these schemes are: first, cryptography is relatively expensive on mobile hosts, where computational capability is comparatively restricted; second, since there is no central authority that can be depended upon, authentication is more difficult to implement; third, these schemes are only useful to prevent intruders from outside (external attacks) and are not useful when an internal node is compromised (internal attack). Since authentication of mobile nodes is mainly achieved with the use of cryptographic techniques, it is essential to design efficient methods to achieve authenticity without the use of encryption algorithms, digital signatures etc.

4. Authentication and Key Management Challenges

Early authentication methods focused on connecting roaming mobile phone users to networks. The network needed to ensure that only valid users have access to its services and the users access a secure facility, as security lapses in a network can lead to permanent damage to a visiting user. The main aim was to establish a session key for confidential communication, mutual authentication and non repudiation [8, 16].

Most access control systems rely on public key management systems to certify an association between an identity and a key in the form of a digital certificate. These certificates contain the public key and the identity along with other details cryptographically signed by a trusted third party. Public key certificates employed by applications are created by Certificate Authorities (CAs). Security requirements for CAs are important with an exploration of the wide range of attacks that can be mounted against CAs [1, 4].

In conventional networks, the two main public-key management solutions are Pretty Good Privacy (PGP) and the X.509 public key infrastructure [1, 4]. PGP has an anarchic organization in contrast to the rigid hierarchy of X.509. In PGP there are some central certificate repositories that are not often used. In X.509 there is a hierarchy of CAs which are responsible for the issuing of certificates and their verification. A node verifies the authenticity of a certificate by using the public key of the CA.

The CA may revoke a certificate and periodically release a Certificate Revocation List (CRL) containing references to the revoked certificates. Delays in the release of a CRL may lead to the acceptance of some revoked certificates by nodes in the network. In ad-hoc networks this approach is difficult to operate as access to a CA cannot be guaranteed at all times to obtain the latest CRL. In PGP a certificate's trustworthiness is assigned by the user using it. The process to estimate the trustworthiness of a certificate may be prolonged and difficult in an ad-hoc network.

The key management approaches for ad-hoc networks try to eliminate the need for a centralized CA. The first approach described in [17] emulates a conventional CA by distributing parts of the secret key on several nodes. A key management scheme has been proposed for ad-hoc networks using threshold cryptography and the public key paradigm. The scheme provides for distribution of parts of the secret key among some special ad-hoc nodes designated as servers. An attacker has to break into a threshold number of servers in order to get access to the secret key of the service. To prevent progressive compromise of servers share refreshing is done periodically. This scheme requires prior communications and coordination between the nodes for setting up the service. In addition, some nodes will have to work more than other nodes. Furthermore,

the requirement for each node to know the public key of all nodes is not feasible if the number of nodes in the ad-hoc network is large.

In the second approach [23] each node authenticates the other by using some prefixed criteria, like the existence of a shared secret among the nodes in the ad-hoc network. Individual nodes in the network use the shared secret to generate their respective keys. One such scheme proposed by DeCleene [3] has a hierarchical framework. Each area in the hierarchy has a controller. These area controllers re-key a node when it moves between different "areas". Another scheme proposed by Kong [12] uses the emulation of certification authority and shared secret model along with a Public Key Infrastructure (PKI) based centralized model. Initially the scheme has an aerial node acting as the centralized node for key distribution. If this aerial node is destroyed the scheme uses threshold cryptography based on secret sharing to emulate a distributed certification authority.

In the last approach a self-organized public-key infrastructure is used. Hubaux [11] proposed a public-key distribution based trust building scheme for ad-hoc networks which is similar to the PGP web of trust concept. The scheme differs from PGP as there are no central certificate directories for distribution of certificates. Instead a user selects a subset of certificates from its repository to disclose to the other user. Both users then merge the received certificates with their own certificates. In order to find the public-key of a remote user the local user makes use of the Hunter Algorithm on the merged certificate repository to build certificate chain(s). A certificate trust chain should lead from the local user certificate to the remote user's certificate. The local user uses the public-key contained in the remote user's certificate.

The plurality of authentication and key management approaches (i.e. [25, 28]) enhance attacks that can target either the identity of a mobile node or the encryption key which is stored or exchanged via some cryptographic protocols.

5 Detection Framework

As mentioned in sections 3 and 4, the existing proposals in ad-hoc networks are either authentication or detection-oriented since they first identify current vulnerabilities and then enhance the existing protocol or propose a new protocol to challenge such threats.

Because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under newborn attacks. As illustrated in Figure 1, the detection framework we propose is related to the main operations of ad-hoc networking which are found at the link and network layers of the Open Systems Interconnection Reference Model (OSI).

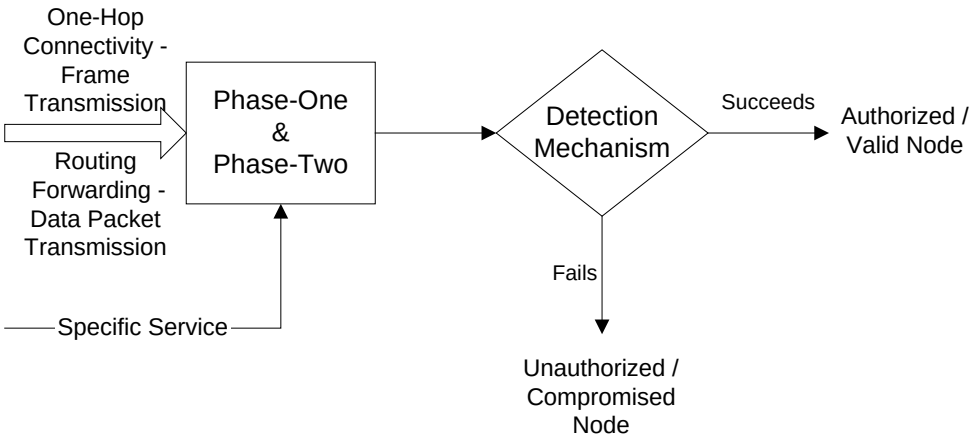


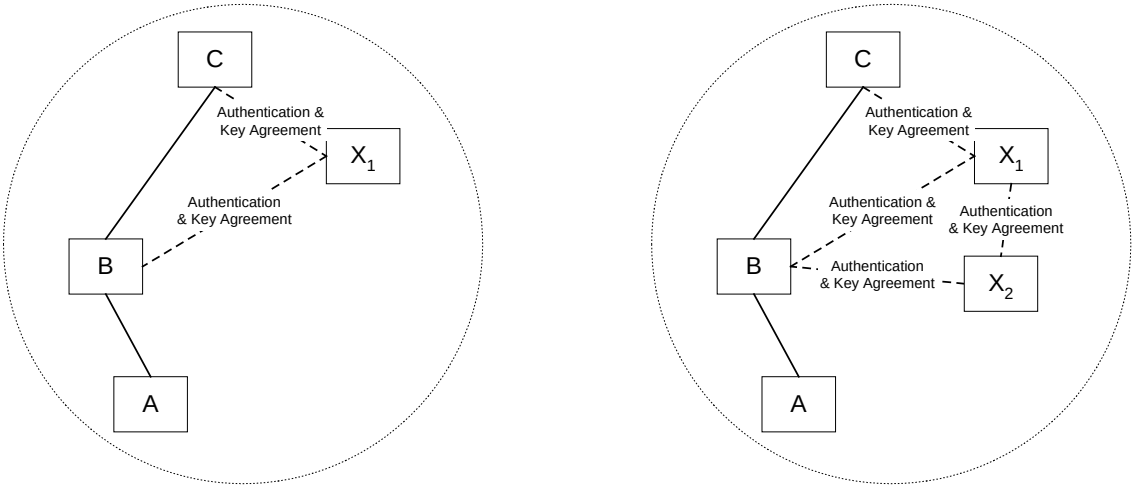
Fig. 1 – Detection Framework

The main operations related to ad-hoc networking are mainly taking place at the link layer with *one-hop connectivity* and *frame transmission* and at the network layer with *routing* and *data packet forwarding* [12, 14, 17]. Data link layer protocols maintain connectivity between neighboring nodes and ensure the correctness of frames transferred whereas routing protocols exchange routing data between nodes and maintain routing states at each node accordingly. Based on the routing states, data packets are forwarded by intermediate nodes along an established route to the destination.

These operations comprise of link security and network security mechanisms that integrate a detection framework which consists of two phases. In phase-one the detection mechanism attempts to determine the true identity of the communicating nodes and thus detects unauthorized nodes through a non-interactive zero knowledge protocol. Likewise, in phase-two the detection mechanism determines whether the communicating nodes have been compromised or not through a non-interactive zero knowledge protocol.

5.1. Detecting Unauthorized Nodes (Phase-One)

When one or more nodes are connected for the first time to a MANET, the detection procedure of an unauthorized node takes place. At this stage, it is necessary to be able to authenticate and thus determine the true identity of the nodes which could possibly gain access to specific applications or services in a MANET. This can be done by an authentication protocol which is suitable for MANETs.



(a) **(b)**

Fig. 2 – New Nodes in MANET

Let us consider the MANET of Figure 2 with the authenticated nodes A, B, and C. As illustrated in Figure 2(a), when node X_1 enters the MANET, it will be authenticated by neighboring nodes B and C. When two nodes, e.g. nodes X_1 and X_2, enter the MANET, they will both be authenticated by neighboring nodes because new routes between nodes will be created as shown in Figure 2(b). For example, node X_1 gets authenticated by the closest nodes B and C, making node X_1 a valid node. Similarly, upon entrance of node X_2, the closest nodes B and X_1 will authenticate node X_2 (Figure 2b). Once nodes X_1 and X_2 have been authenticated by valid nodes, they will also authenticate each other since routing and packet forwarding data will be sent to or received by them.

There are several authentication protocols available in the literature that can be applied to MANETs. However, it is necessary to use non-interactive and low complexity protocols that will not create extra computational overhead in the network. For example, a provably secure authentication scheme can be considered as a “good” candidate in phase-one. Such a scheme is preferable to a computationally secure authentication scheme because its security relies on the apparent intractability of a well known

computational problem (i.e. discrete logarithm problem) and does not necessarily require the use of a symmetric or an asymmetric encryption algorithm. Therefore, authentication can be achieved with a zero knowledge protocol, similar to the protocol described in [18] that provides such characteristics.

The basic concept behind the use of such cryptographic protocols is that they allow a claimant, a node in a MANET context, to demonstrate knowledge of a secret while revealing no information whatsoever of use to the verifying node even if the claimant node misbehaves. In such protocols, nodes must exchange multiple messages, also referred to as interactive, where the proof is probabilistic rather than absolute. However, interactive zero protocols are not suitable for wireless environments since they exchange multiple messages and result in the reduction of network performance. MANETs are suitable for non-interactive zero knowledge protocols where nodes do not need to exchange multiple messages to prove their identity.

In Figure 2 (a) for example, node X_1 can prove its identity to nodes B and C ensuring that the discrete logarithms $y_1 = \alpha_1^{x_1}$ and $y_2 = \alpha_2^{x_2}$ to the bases α_1, α_2, satisfy Equation 1;

$$k_1 \cdot x_1 + k_2 \cdot x_2 = b \pmod{p} \quad \textbf{(1)}$$

for integers k_1, k_2, and prime number p [18].

In the protocol, node X_1 first computes $y_3 = \alpha_3^{x_3}$ and $y_4 = \alpha_4^{x_4}$ then solves Equation 2, for integers x_3, x_4:

$$k_1 \cdot x_3 + k_2 \cdot x_4 = 0 \pmod{p} \quad \textbf{(2)}$$

Next, the following message exchange takes place:

$$\text{B, C} \leftarrow \text{X}_1 : \; y_5 = \alpha_1^{x_3}, \; y_6 = \alpha_2^{x_4} \quad \text{(M1)}$$

$$\text{B, C} \rightarrow \text{X}_1 : \; y_7 = H(\alpha_1, \alpha_2, y_1, y_2, k_1, k_2, b, y_5, y_6) \quad \text{(M2)}$$

$$\text{B, C} \leftarrow \text{X}_1 : \; y_8 = x_3 - y_7 \cdot x_1 \pmod{p}, \; y_9 = x_4 - y_7 \cdot x_2 \pmod{p} \quad \text{(M3)}$$

Node X_1 sends y_5 and y_6 to nodes B and C. Upon reception of message (M1), nodes B and C compute y_7 with a one-way hash function and send message (M2) to node X_1.

Next, node X_1 checks the validity of (M1), constructs message (M3) and sends y_8, y_9 to nodes B and C.

Node X_1 convinces nodes B and C that he/she knows the discrete algorithms of y_1 and y_2 to the bases α_1 and α_2 respectively, and that these logarithms satisfy a linear equation. This can be done by verifying the resulting proof (y_7, y_8, y_9). It can be easily seen that nodes B and C will always succeed in constructing a valid proof by first reconstructing $y_{10} = \alpha_1^{y_8} \cdot y_1^{y_7}$ and $y_{11} = \alpha_2^{y_9} \cdot y_2^{y_7}$, then checking whether y_7 is equal to y_{12}, for $H(\alpha_1, \alpha_2, y_1, y_2, k_1, k_2, b, y_{10}, y_{11}) = y_{12}$, and if Equation 3 is valid:

$$k_1 \cdot y_8 + k_2 \cdot y_9 = -y_7 \cdot b \pmod{p} \qquad \textbf{(3)}$$

First, it can be easily seen that nodes B and C will always succeed in constructing a valid proof since $y_{10} = y_5$ and $y_{11} = y_6$

$$y_{10} = \alpha_1^{y_8} \cdot y_1^{y_7} \overset{y_8, y_1}{=} \alpha_1^{x_3 - y_7 \cdot x_1} \cdot \alpha_1^{x_1 \cdot y_7} = \alpha_1^{x_3} = y_5$$

$$y_{11} = \alpha_2^{y_9} \cdot y_2^{y_7} \overset{y_9, y_2}{=} \alpha_2^{x_4 - y_7 \cdot x_2} \cdot \alpha_2^{x_2 \cdot y_7} = \alpha_2^{x_4} = y_6 .$$

Thus,

$$y_{12} = H(\alpha_1, \alpha_2, y_1, y_2, k_1, k_2, b, y_{10}, y_{11}) = H(\alpha_1, \alpha_2, y_1, y_2, k_1, k_2, b, y_5, y_6) = y_7$$

Hence, nodes B and C calculate y_{12} and compare it with y_7 in message M2.

Second, assume that an intruder E who does not know x_1 and x_2 was able to compute such proofs. Since the one-way hash function y_7 is hard to invert, we can assume that the values y_{10} and y_{11} were fixed before y_7 in message M2 was computed. It also seems necessary that when fixing the values y_{10} and y_{11}, B and C were prepared to compute a proof for many other possible messages. But this means that E could also compute different representations of y_{10} and y_{11} to the bases α_1, y_1 and α_2, y_2 which implies the knowledge of x_1 and x_2, the discrete logarithms y_1, y_2 to the bases α_1, α_2, but this contradicts the assumption that the cheating E does not know x_1 and x_2.

Furthermore, nodes B and C verify whether the responses y_8 and y_9 satisfy Equation 3. Thus,

$$\begin{aligned} k_1 y_8 + k_2 y_9 &\overset{y_8, y_9}{=} k_1 \cdot (x_3 - y_7 \cdot x_1) + k_2 \cdot (x_4 - y_7 \cdot x_2) \\ &= k_1 \cdot x_3 - k_1 \cdot y_7 \cdot x_1 + k_2 \cdot x_4 - k_2 \cdot y_7 \cdot x_2 \\ &= k_1 \cdot x_3 + k_2 \cdot x_4 - y_7 \cdot (k_1 \cdot x_1 + k_2 \cdot x_2) \\ &\overset{Eq.1,2}{=} -y_7 \cdot b \pmod{p} \end{aligned}$$

and validate the identity of node X_1. The successful authentication of node X_1 concludes that the particular node is authorized to specific applications which are carried out in the MANET.

5.2. Detecting Compromised Nodes (Phase-Two)

When routing information and/or data packets are ready to be transferred, phase-two takes place. The detection procedure for compromised nodes carries on in the available nodes starting with one-hop at a time from the source to destination route. Due to the node mobility in ad hoc networks, the route from the source to destination node is subject to change. However, the detection procedure is independent to the mobility of nodes since the routing protocol is responsible for delivering data to nodes. The detection process, followed in phase-two, requires the true identity and compromised status of the communicating nodes. Hence, nodes are authenticated with a zero-knowledge protocol and the compromised status is determined by a local agent that collects and analyses audit data.

The agent, which is embedded to all nodes, knows the user's standard profile, records deviations from this reference and is also familiar with the signatures of known attacks. Even though the agent operations are similar to IDS, the agent has a passive role of gathering and analyzing audit data locally and passing a confidence interval to the neighboring node for further process. The agent can collect and analyze data at regular intervals or provide a continuous service for open environments. Data manipulation determines node identification and compromised status procedure.

5.2.1 Node Identification & Compromised Status Procedure

Let us assume that X_1 was authenticated when it entered the MANET of Figure 2a with the zero knowledge protocol of section 5.1. Similar to section 5.1, when routing

information is ready to be transferred, node X_1 should prove again its identity and compromised status to nodes B and C ensuring that the discrete logarithms, $y_1 = \alpha_1^{x_1 + f(z_1, z_2)}$ and $y_2 = \alpha_2^{x_2 + f(z_1, z_2)}$ to the bases α_1, α_2, satisfy Equation 4:

$$k_1 \cdot x_1 + k_2 \cdot x_2 = f(z_1, z_2) + b \pmod{p} \quad \textbf{(4)}$$

for integers k_1, k_2, b and prime number p [18].

Notice that Equation 4 contains a multivariable function $f(z_1, z_2)$ that determines the compromised status of a node. Such function is defined in Equation 5:

$$f(z_1, z_2) = \begin{cases} k_1 \cdot z_1 + k_2 \cdot z_2 = c \bmod p, \text{for } x_1 \le z_1, z_2 \le x_2 \\ 0, \text{otherwise} \end{cases} \quad \textbf{(5)}$$

for integers k_1, k_2, and prime number p.

The value of $f(z_1, z_2)$ is determined by the local agent. Based on the analysis of data the agent defines a confidence interval where a node is considered to be compromised. The confidence interval can follow a normal distribution as shown in Figure 3. Even though the values of x_1 and x_2 are discrete, the interval is continuous.

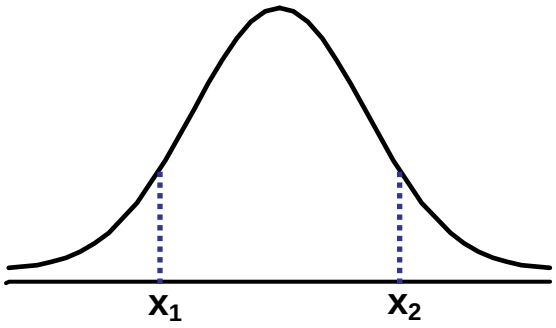


Fig. 3 – Confidence Interval for Compromised Nodes

If the values of z_1 and z_2, which are assigned by the local agent, are found within the interval of x_1 and x_2, then $f(z_1, z_2)$ is defined as $f(z_1, z_2) = k_1 \cdot z_1 + k_2 \cdot z_2 = c \bmod p$. Next, node X_1 proves its valid identity to nodes B and C and routing information is exchanged. On the contrary, if the values of z_1 and z_2 exceed the interval from x_1 to x_2, then $f(z_1, z_2) = 0$. Hence, Equations 1 and 4 are the same. In such a circumstance, node X_1 is considered to be compromised because it proves its identity to nodes B and

C with the procedure mentioned in section 5.1. Therefore, routing information will be considered unreliable and will be discarded by the neighboring nodes B and C.

5.2.2 Validation Procedure

In the validation procedure, node X_1 computes $y_3 = \alpha_3^{x_3}$ and $y_4 = \alpha_4^{x_4}$ and then solves Equation 2, for integers x_3, x_4. Following, exchange of messages takes place afterwards:

$$\text{B, C} \leftarrow \text{X}_1 : \; y_5 = \alpha_1^{x_3}, \; y_6 = \alpha_2^{x_4} \qquad \text{(M1)}$$

$$\text{B, C} \rightarrow \text{X}_1 : \; y_7 = H(\alpha_1, \alpha_2, y_1, y_2, k_1, k_2, c, f(z_1, z_2) + b, y_5, y_6) \qquad \text{(M2)}$$

$$\text{B, C} \leftarrow \text{X}_1 : \; y_8 = x_3 - y_7 \cdot (f(z_1, z_2) + x_1) \pmod{p},$$

$$y_9 = x_4 - y_7 \cdot (f(z_1, z_2) + x_2) \pmod{p} \qquad \text{(M3)}$$

Node X_1 sends y_5 and y_6 to nodes B and C. Upon reception of message M1, nodes B and C compute y_7 with an one-way hash function and send message M2 to node X_1. Next, node X_1 checks the validity of M1, constructs message M3 and sends y_8, y_9 to nodes B and C.

Node X_1 convinces nodes B and C that he/she knows the discrete algorithms of y_1 and y_2 to the bases α_1 and α_2, respectively, and that these logarithms satisfy a linear equation. This can be done by verifying the resulting proof (y_7, y_8, y_9). It can be easily seen that nodes B and C will always succeed in constructing a valid proof by first reconstructing $y_{10} = \alpha_1^{y_8} \cdot y_1^{y_7}$, $y_{11} = \alpha_2^{y_9} \cdot y_2^{y_7}$ and then checking whether y_7 is equal to y_{12}, for $H(\alpha_1, \alpha_2, y_1, y_2, k_1, k_2, c, b, y_{10}, y_{11}) = y_{12}$ and if Equation 6 is valid:

$$k_1 \cdot y_8 + k_2 \cdot y_9 = -y_7 \cdot (f(z_1, z_2) + b) \pmod{p} \qquad \textbf{(6)}$$

for

$$k_1 \cdot f(z_1, z_2) + k_2 \cdot f(z_1, z_2) = 0 \pmod{p}. \qquad \textbf{(7)}$$

First, it can be easily seen that nodes B and C will always succeed in constructing a valid proof since $y_{10} = y_5$ and $y_{11} = y_6$:

$$y_{10} = \alpha_1^{y_8} \cdot y_1^{y_7} \overset{y_8, y_1}{=} \alpha_1^{x_3 - y_7 \cdot (f(z_1, z_2) + x_1)} \cdot \alpha_1^{y_7 \cdot (f(z_1, z_2) + x_1)} = \alpha_1^{x_3} = y_5$$

$$y_{11} = \alpha_2^{\,y_9} \cdot y_2^{\,y_7} \overset{y_9, y_2}{=} \alpha_2^{\,x_4 - y_7 \cdot (f(z_1, z_2) + x_2)} \cdot \alpha_2^{\,y_7 \cdot (f(z_1, z_2) + x_2)} = \alpha_2^{\,x_4} = y_6 .$$

Then,

$$y_{12} = H(\alpha_1, \alpha_2, y_1, y_2, k_1, k_2, c, b, y_{10}, y_{11}) = H(\alpha_1, \alpha_2, y_1, y_2, k_1, k_2, c, b, y_5, y_6) = y_7 .$$

Hence, nodes B and C calculate y_{12} and compare it with y_7 in message M2. Furthermore, nodes B and C verify whether the responses y_8 and y_9, satisfy Equation 6. Thus,

$$\begin{aligned} k_1 y_8 + k_2 y_9 \overset{y_8, y_9}{=}\ & k_1 \cdot (x_3 - y_7 \cdot (f(z_1, z_2) + x_1)) + k_2 \cdot (x_4 - y_7 \cdot (f(z_1, z_2) + x_2)) \\ & = k_1 \cdot x_3 - k_1 \cdot y_7 \cdot f(z_1, z_2) - k_1 \cdot y_7 \cdot x_1 + k_2 \cdot x_4 - k_2 \cdot y_7 \cdot f(z_1, z_2) - k_2 \cdot y_7 \cdot x_2 \\ & = k_1 \cdot x_3 + k_2 \cdot x_4 - y_7 \cdot (k_1 \cdot x_1 + k_2 \cdot x_2) - y_7 \cdot (k_1 \cdot f(z_1, z_2) + k_2 \cdot f(z_1, z_2)) \\ & \overset{Eq.2,4,7}{=} -y_7 \cdot (f(z_1, z_2) + b) \pmod{p}. \end{aligned}$$

Nodes B and C will accept the routing information which is coming from node X_1 since there is a high confidence that it has not been compromised during its operation in MANET. As a result, the communicating nodes are eligible to agree upon a secret key, which will encrypt the actual communication.

6 Conclusions

Security of MANET has become a more sophisticated problem than security in other networks due to the open nature and lack of infrastructure of ad-hoc networks. Current research efforts on ad-hoc networks follow a hierarchical approach, where the most explored area involves secure routing protocols. Authentication and intrusion detection mechanisms, on the other side, are explored less than routing protocols. In this paper we explored the authentication and intrusion detection challenges and proposed a detection mechanism for unauthorized and compromised nodes.

Since mobile ad-hoc networks can be formed, merged together or partitioned into separate networks on the fly, it is essential to be able to determine the identity of the nodes participating in such networks. It is also necessary to be able to verify whether a node has been compromised or not during the operation of a MANET. The proposed detection mechanism, which is enabled with the main operations of link and network layers, makes use of local agents that collect and analyze audit data. Each agent assigns a compromised status based on his data analysis and passes it to the neighbouring nodes for further decisions.

Nodes apply zero knowledge techniques to exchange information and therefore, identify unauthorized and compromised nodes. Our protocols allows a proof of the truth of an assertion, while conveying no information whatsoever about the assertion itself other than its actual truth. The authentication schemes applied in MANETs usually demonstrate knowledge of a secret in a time-variant manner which might nonetheless reveal some partial information about the secret key. Nevertheless, once the authentication infrastructure is in place, data confidentiality and integrity issues can be tackled by using existing and efficient symmetric algorithms since there is no need of developing any special integrity and encryption algorithms for ad-hoc networks.

7 Acknowledgements

This research work is funded by the Ministry of Education and Religious Affairs and co-funded by E.U. (75%) and National Resources (25%) under the Grant "Pythagoras - Research Group Support of the University of the Aegean".

References

[1] A. J. Menezes, S. A. Vanstone, and P. C. Van Oorschot, *Handbook of Applied Cryptography*, CRC Press, Inc., USA, 2001.

[2] A. Mishra, K. Nadkarni, A. Patcha, "Intrusion detection in wireless ad hoc networks", *IEEE Personal Communications*, Vol: 11, Issue 1, Feb 2004 Page(s): 48 – 60.

[3] B. DeCleene et al, "Secure Group Communications for Wireless Networks", *IEEE Military Communications Conference* (MILCOM), October 2001, Virginia (USA).

[4] C. Douligeris and A. Mitrokosta, "DDoS attacks and defense mechanisms: classification and state-of-the-art", *Computer Networks: The International Journal of Computer and Telecommunications Networking*, Vol: 44, Issue 5, 2004, Page(s): 643 – 666.

[5] C. M. Chlamtac and J. J.-N. Liu, "Mobile ad hoc networking: imperatives and challenges", *Ad Hoc Networks*, Vol: 1, July 2003, Page(s): 13 - 64.

[6] C. Perkins et al., "Ad Hoc On-Demand Distance-Vector Routing (AODV)", *IETF draft*, 2001.

[7] D. Watkins and C. Scott, "Methodology for evaluating the effectiveness of intrusion detection in tactical mobile ad-hoc networks" *IEEE Wireless Communications and Networking Conference*, (WCNC), Vol: 1, 21-25 March 2004, Page(s): 622 – 627.

[8] E.C.H. Ngai, M.R. Lyu, R.T. Chin, "An authentication service against dishonest users in mobile ad hoc networks", IEEE Proceedings on Aerospace Conference, Vol: 2, 6-13 March 2004, Page(s): 1275 – 1285.

[9] E.C.H. Ngai, M.R. Lyu, "Trust- and clustering-based authentication services in mobile ad hoc networks", *24th International Conference on Distributed Computing Systems Workshops*, June 2004, Page(s): 582 – 587.

[10] H. Yang, H. Y. Luo, F. Ye, S. W. Lu and L. Zhang, "Security in Mobile Ad Hoc networks: challenges and solutions", *IEEE Wireless Communications*, Vol: 11, February 2004, Page(s). 38 - 47.

[11] J. Hubaux, L. Buttyán, and S. Capkun, "The Quest for Security in Mobile Ad Hoc Networks", *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, Long Beach, CA, USA, Oct. 2001.

[12] J. Kong et al, "Adaptive Security for Multi-layer Ad-hoc Networks", *Special Issue of Wireless Communications and Mobile Computing*, John Wiley InterScience Press, 2002.

[13] J. Kong et al., "Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks", *IEEE ICNP*, Riverside, USA, 2001.

[14] L. Blazevic et al., "Self-Organization in Mobile Ad-Hoc Networks: the Approach of Terminodes", *IEEE Communications Magazine*, June 2001, Page(s) 166 - 173.

[15] L. Buttyán and J. Hubaux, "Enforcing service availability in mobile ad-hoc WANs", *Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing*, Boston, Massachusetts, August 2000.

[16] L. Venkatraman and D.P. Agrawal, "A Novel Authentication Scheme for Ad hoc Networks", *2nd IEEE Wireless Communications and Networking Conference*, Chicago, 2000.

[17] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks", *IEEE Network Magazine*, 1999.

[18] N. Komninos, *Security Architecture for Future Communication Systems*, Ph.D. Thesis, Lancaster University, 2003.

[19] P. Kyasanur and N. Vaidya, "Detection and Handling of MAC Layer Misbehavior in Wireless Networks", *International Conference on Dependable Systems and Networks (DSN'03)*, San Francisco, California, June 2003, Page(s): 173 - 182.

[20] P. Papadimitratos , Z. J. Haas , E. G. Sirer, "Path set selection in mobile ad hoc networks", *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, Lausanne, Switzerland, 2002, Page(s) 1 - 11.

[21] Q. Xue, J. Sun, Z. Wei, "TJIDS: an intrusion detection architecture for distributed network", *IEEE Canadian Conference on Electrical and Computer Engineering, (CCECE)*, Vol: 2, 4-7 May 2003 Page(s): 709 – 712.

[22] S. Bo, W. Kui, U.W. Pooch, "Towards adaptive intrusion detection in mobile ad hoc networks", *IEEE Global Telecommunications Conference* (GLOBECOM), Vol: 6, 29 Nov.-3 Dec. 2004, Page(s): 3551 – 3555.

[23] X. Gang; L. Iftode, "Locality driven key management architecture for mobile ad-hoc networks", *IEEE International Conference on Mobile Ad-hoc and Sensor Systems*, 25-27 Oct. 2004, Page(s): 436 – 446.

[24] X. Yan, L. Ren-Fa, L. Ken-Li, "Intrusion detection using mobile agent in ad-hoc networks", *Proceedings of International Conference on Machine Learning and Cybernetics*, Vol: 6, 26-29 Aug. 2004, Page(s): 3383 – 3388.

[25] Y. Chou-Chen, C. Chia-Meng, C. Ting-Yi, "A routing authentication mechanism for wireless ad hoc networks", *IEEE International Conference on Networking, Sensing and Control*, Vol: 1, 21-23 March 2004, Page(s): 456 – 461.

[26] Y. Hu, A. Perrig, and D. Johnson, “Ariadne: A Secure on-demand Routing Protocol for Ad Hoc Networks”, *ACM MOBICOM*, September 2002, Georgia (USA).

[27] Y. Hu, A. Perrig, and D. Johnson, “Packet Leashes: A Defense against wormhole Attacks in Wireless Networks, *IEEE INFOCOM*, 2002.

[28] Y.-R. Tsai and S.-J. Wang, “Routing security and authentication mechanism for mobile ad hoc networks”, *IEEE 60th Vehicular Technology Conference* (VTC2004), Vol: 7, 26-29 Sept. 2004, Page(s): 4716 – 4720.

[29] Y. Zhang , W. Lee, “Intrusion detection in wireless ad-hoc networks”, *Proceedings of the 6th annual international conference on Mobile computing and networking*, p.275-283, Boston, Massachusetts, United States, 2000.

[30] W. Zhang, R. Rao, G. Cao, G. Kesidis; “Secure routing in ad hoc networks and a related intrusion detection problem” *IEEE Military Communications Conference* (MILCOM), Vol: 2, 13-16 Oct. 2003, Page(s): 735 – 740.