Layered Security Design for 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

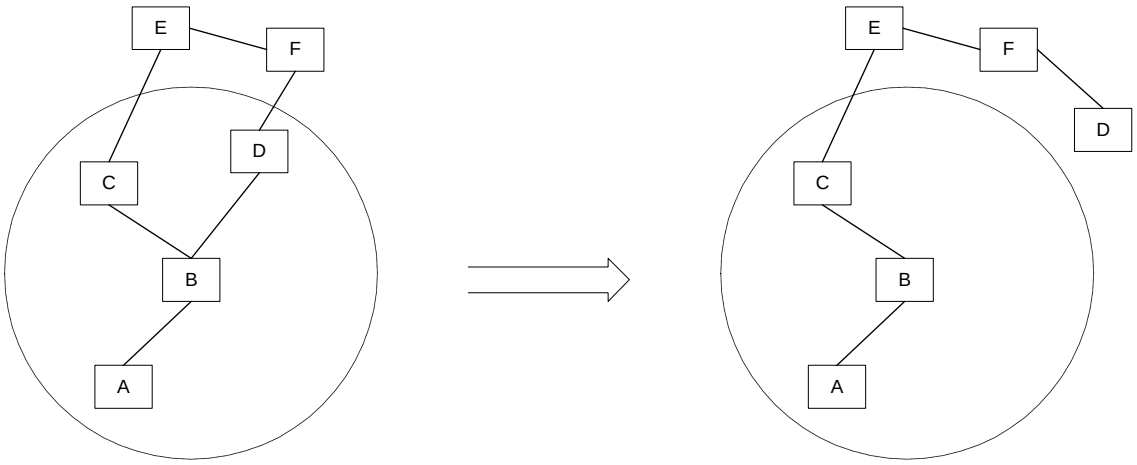
Abstract

When security of a given network architecture is not properly designed from the beginning, it is difficult to preserve confidentiality, authenticity, integrity and non-repudiation in practical networks. Unlike traditional mobile wireless networks, ad hoc networks rely on individual nodes to keep all the necessary interconnections alive. In this article we investigate the principal security issues for protecting mobile ad hoc networks at the data link and network layers. The security requirements for these two layers are identified and the design criteria for creating secure ad hoc networks using multiple lines of defense against malicious attacks are discussed.

Keywords: mobile ad hoc networks, security, link and network layers, authentication.

1. Introduction

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. Nodes communicate with 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) [7].



(a) **(b)**

Figure 1 - Topology changes in MANET

A simple MANET example is illustrated in Figure 1. Here it is shown how mobility in ad hoc networks causes changes in the network topology. Initially, the network has the topology shown in Figure 1 (a) but when node D moves out of the radio range of node B, the network topology changes to the one in Figure 1 (b). When node D moves out of node B's radio range, link is broken. Nevertheless, the network remains connected since node B can reach node D though nodes C, E, and F.

So far, applications of mobile ad hoc networks have been visualised mainly for crisis solutions (e.g., in the battlefield or in rescue operations). In these applications, all the nodes of the network belong to a single authority (e.g. a single military unit or a rescue team). With the progress of technology, however, it is becoming possible to deploy MANET for civilian applications as well [4, 5, 24]. Examples include networks of cars and provision of communication facilities in remote areas. In these networks, the nodes do not necessarily belong to a single authority. In addition, these networks could be larger, have a longer lifetime, and they could be completely self-organizing, meaning that the network could be run solely by the operation of the end-users.

Since ad hoc networks can be deployed rapidly, sensitive applications raise important security issues. Security requirements in ad hoc networks are different from those of fixed networks. While the security requirements are the common ones, namely availability, confidentiality, integrity, authentication and non-repudiation, they are considered differently for ad hoc networks due to system constraints in mobile devices (i.e. low power microprocessor, small memory and bandwidth, short battery life) and frequent network topology changes.

In this article, we focus on the key attributes related to the security of ad hoc networks. We seek to identify the security issues and attacks in such networks and also examine secure protocols found in the data link and network layers. We also propose a layered security design that uses multiple lines of defence against malicious attacks and other network faults. In particular, section 2 mentions the security goals and types of attacks that exist in ad hoc networks. Sections 3 and 4 present the security aspects of link and network layer security protocols and their challenges to secure MANET. Section 5 describes the layered security design and discusses how challenge-response and zero knowledge cryptographic protocols can be applied. Finally, section 6 concludes with comments on the unexplored security areas for MANET.

2. Securing ad hoc networks

Security in ad hoc networks is difficult to be achieved due to their nature. The vulnerability of the links, the limited physical protection of each of the nodes, the sporadic nature of connectivity, the dynamically changing topology, the absence of a certification authority and the lack of a centralized monitoring or management point make security goals difficult to achieve [7]. In order to identify critical security points in ad hoc networks, it is necessary to examine the security requirements and the types of attacks from the ad hoc network perspective.

2.1. Security Requirements

Security requirements depend very much on the kind of application the mobile ad hoc network is to be used and the environment in which it has to operate. For example, a military MANET will have very stringent requirements in terms of confidentiality and resistance to the denial of service attacks (DoS). Similar to other practical networks,

MANET security goals include availability, authenticity, integrity, confidentiality and non-repudiation.

Availability can be considered as the key value attribute related to the security of networks. It ensures that the service offered by the node will be available to its users when expected and also guarantees the survivability of network devices despite DoS attacks [4, 5, 24]. Possible attacks include adversaries who employ jamming to interfere with communication on physical channels, disrupt the routing protocol, disconnect the network and bring down high-level services [3, 10, 13].

Authentication ensures that the communicating parties are the ones claim to be and that the source of information is assured [1, 4, 5, 24]. Without authentication, an adversary could gain unauthorized access to resources and to sensitive information and possibly interfere with the operation of other nodes [9, 11, 14, 21].

Integrity ensures that no one can tamper with the transferred content [1, 4, 5, 24]. The communicating nodes want to be sure that the information comes from an authenticated node and not from a node that has been compromised and send out incorrect data. For example, message corruption because of radio propagation impairment or because of malicious attacks should be avoided.

Confidentiality ensures the protection of sensitive data so that no one can see the transferred contents [1, 4, 5, 24]. Leakage of sensitive information, such as in military environment, could have devastating consequences. However, it is pointless to attempt to protect the secrecy of a communication without first ensuring that one is talking to the right node.

Non-repudiation ensures that the communicating parties cannot deny their actions [1, 4, 5, 24]. It is useful for the detection and isolation of malicious nodes. When node A receives an erroneous message from node B, non-repudiation allows node A to accuse node B using this message and to convince other nodes that node B has been compromised.

2.2. Types of Attacks

Similar to other wireless networks, ad hoc networks are susceptible to ***passive*** and ***active*** attacks [1, 4, 5, 24]. 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 target to cause congestion, propagate incorrect routing information, prevent services from working properly or shut them down completely [12, 14, 26].

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 perform passive attacks with the aim of saving battery life for their own communications are considered to be *selfish* [9, 12]. A selfish node affects the normal operation of the network by not participating in the routing protocols or by not forwarding packets as in the so called *black hole attack* [18, 25].

Compromised nodes can interrupt the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information and by impersonating other nodes. Recent research studies have also brought up a new type of

attack that goes under the name of *wormhole attack* [19, 20, 25, 27]. In the latter, two compromised nodes create a tunnel (or wormhole) that is linked through a private connection and thus 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 [10].

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 [10, 19, 21].

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* [15] that result in erroneous and bogus routing messages.

DoS is another type of attack, in which the attacker injects a large amount of junk packets into the network. These packets consume a significant portion of network resources and introduce wireless channel contention and network contention in ad hoc networks [4, 5, 24].

The described attacks identify critical security threats in ad hoc networks. The security challenges that arise in the main operations related to ad hoc networking are found in the data link and network layers.

3 Security Challenges in the Data Link Layer

The Open Systems Interconnection Reference Model (OSI Model or OSI Reference Model for short) is a layered abstract description for communications and computer network protocol design, developed as part of the Open Systems Interconnect initiative. The data link layer is second level of the seven-level OSI model and is the layer of the model which ensures that data is transferred correctly between adjacent network nodes. The data link layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the physical layer [17]. However, the main link layer operations related to ad hoc networking are ***one hop connectivity*** and ***frame transmission*** [18]. Data link layer protocols maintain connectivity between neighbouring nodes and ensure the correctness of frames transferred.

It is essential to distinguish the relevance of security mechanisms implemented in the data link layer with respect to the requirements of MANET. In the case of mobile ad hoc networks, there are ***trusted*** and ***non-trusted*** environments [1, 4, 5, 14, 24]. In a *trusted* environment the nodes of the ad hoc network are controlled by a third party and can thus be trusted based on authentication. Data link layer security is justified in this case by the need to establish a trusted infrastructure based on logical security means. If the integrity of higher layer functions implemented by the trusted nodes can be assured, then data link layer security can even meet the security requirements raised by higher layers including routing and application protocols.

In *non-trusted* environments, on the other hand, trust in higher layers like routing or application protocols cannot be based on data link layer security mechanisms. The only relevant use of the latter appears to be node-to-node authentication and data integrity as required by the routing layer. Moreover, the main constraint in the deployment of existing data link layer security solutions (i.e. 802.11 and Bluetooth) is the lack of support for automated key management which is mandatory in open environments where manual key installation is not suitable.

The main requirement for data link layer security mechanisms is the need to cope with the lack of physical security on the wireless segments of the communication infrastructure. The data link layer can be understood as a means of building a 'wired equivalent' security as described by the objectives of WEP of 802.11. Data link layer mechanisms like the ones provided by 802.11 and Bluetooth basically serve for access control and privacy enhancements to cope with the vulnerabilities of radio communication links. However, data link security performed at each hop cannot meet the end-to-end security requirements of applications neither on wireless links protected by IEEE 802.11 or Bluetooth nor on physically protected wired links.

Recent research efforts have identified vulnerabilities in WEP and several types of cryptographic attacks exist due to misuse of the cryptographic primitives [16]. The IEEE 802.11 protocol is also weak to DoS attacks where the adversary may exploit its binary exponential back-off scheme to deny access to the wireless channel from its local neighbours. In addition, a continuously transmitting node can always capture the channel and cause other nodes to back off endlessly thus triggering a chain reaction from upper layer protocols (e.g. TCP window management) [2, 16].

Another DoS attack is also applicable in IEEE 802.11 with the use of the NAV field, which indicates the channel reservation, carried in the request to send/clear RTS/CTS frames. The adversary may overhear the NAV information and then intentionally introduce a 1-bit error into the victim's link layer frame by wireless interference [2, 16].

Link layer security protocols should provide peer-to-peer security between directly connected nodes and secure frame transmissions by automating critical security operations including node authentication, frame encryption, data integrity verification and node availability.

4 Security Challenges in Network layer

The network layer is the third level of the seven level OSI model. The network layer addresses messages and translates logical addresses and names into physical addresses. It also determines the route from the source to the destination computer and manages traffic problems, such as switching, routing, and controlling the congestion of data packets [17].

The main network operations related to ad hoc networking are ***routing*** and ***data packet forwarding*** [3, 8]. The 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.

In attacking routing protocols, the attackers can extract traffic towards certain destinations in compromised nodes and forward packets along a route that is not optimal. The adversaries can also create routing loops in the network and introduce network congestion and channel contention in certain areas. There are still many active research efforts in identifying and defending more sophisticated routing attacks [25, 26, 27, 28].

In addition to routing attacks, the adversary may launch attacks against packet forwarding operations. Such attacks cause the data packets to be delivered in a way that is inconsistent with the routing states. For example, the attacker along an established route may drop the packets, modify the content of the packets, or duplicate the packets it has already forwarded [14]. DoS is another type of attack that targets packet-forwarding protocols and introduces wireless channel contention and network contention in ad hoc networks [4, 5, 24].

Routing protocols can be divided into proactive, reactive and hybrid protocols depending on the routing topology [21]. *Proactive protocols* are either table-driven or distance-vector protocols. In such protocols, the nodes periodically refresh the existing routing information so every node can immediately operate with consistent and up-to-date routing tables [21].

On the contrast, *reactive or source-initiated on demand protocols* do not periodically update the routing information [10]. Thus, they create a large overhead when the route is being determined, since the routes are not necessarily up-to-date when required. *Hybrid protocols* make use of both reactive and proactive approaches. They typically offer the means to switch dynamically between the reactive and proactive modes of the protocol [10].

Current efforts towards the design of secure routing protocols are mainly focused on reactive routing protocols, such as dynamic source routing (DSR) or ad-hoc on-demand distance vector (AODV) [6, 22], that have been demonstrated to perform better with significantly lower overheads than the proactive ones since they are able to react quickly to topology changes while keeping the routing overhead low in periods or areas of the network in which changes are less frequent. Some of these techniques are briefly described in the next paragraphs.

Secure routing protocols currently proposed in the literature take into consideration active attacks performed by compromised nodes that aim at tampering with the execution of routing protocols whereas passive attacks and the selfishness problems are not addressed. For example, the secure routing protocol (SRP) [3, 8], which is a reactive protocol, guarantees the acquisition of correct topological information. It uses a hybrid key distribution based on the public keys of the communicating parties. It suffers, however, from the lack of a validation mechanism for route maintenance messages [14, 23].

Another reactive secure ad hoc routing protocol ARIADNE, which is based on DSR, guarantees point-to-point authentication by using a message authentication code (MAC) and a shared secret between the two parties [8, 26]. The ARAN secure routing protocol [8] detects and protects against malicious actions carried out by third parties and peers in the ad hoc environment. It protects against exploits using modification, fabrication and impersonation but the use of asymmetric cryptography makes it a very costly

protocol in terms of CPU usage and power consumption. The wormhole attack is surpassed with the use of another protocol [8].

SEAD, on the other hand, is a proactive protocol based on the destination sequenced distance vector protocol (DSDV) [28] that deals with attackers who modify routing information. It makes use of efficient one-way hash functions rather than relying on expensive asymmetric cryptography operations. SEAD does not cope with the wormhole attack and the authors propose, as in the ARIADNE protocol, to use a different protocol to detect this particular threat [8, 28].

5 Layered Security Design

The existing proposals in ad hoc networks are typically attack-oriented since they first identify several security threats 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 newly attacks.

When the security of a given network architecture is not properly designed from the beginning, then the above mentioned security goals are difficult to achieve during network deployment. It is essential, therefore, to design secure ad hoc networks that will result in multiple lines of defence against both known and unknown security threats. This design is what we call layered security design.

In the layered security design, we take into consideration not only malicious attacks but also other network faults due to misconfiguration, extreme network overload, or operational failures. All such faults, whether caused by attacks or by misconfiguration, share some symptoms from both the network and end-user perspectives, and should be handled by the security mechanisms. In addition, the overall system has to be robust and it should not be affected against the breakdown of any individual line of defence.

Network Layer Operations Routing / Data Packet Forwarding	**Post-secure (Prevention / Reaction)** Node-to-Node Authentication & Key Agreement Data Integrity, Confidentiality Non-repudiation of data	Network Security Mechanisms
Link Layer Operations One-hop Connectivity / Frame Transmission	**Pre-secure (Detection)** Node-to-Node Authentication & Key Agreement Frame Integrity, Confidentiality Node Availability	Link Security Mechanisms

Table 1 - Layered Security

As mentioned in section 3 and also shown in Table 1, link layer operations involve *one-hop connectivity* and *frame transmission*, whereas network layer operations include *routing* and *data packet forwarding*. These operations comprise of link security and network security mechanisms that integrate a protocol securization process (Figure 2) which consists of ***pre-secure*** and ***post-secure*** sessions. The *pre-secure* session attempts to detect security threats through various cryptographic techniques, whereas the *post-secure* session seeks to prevent such threats and react accordingly.

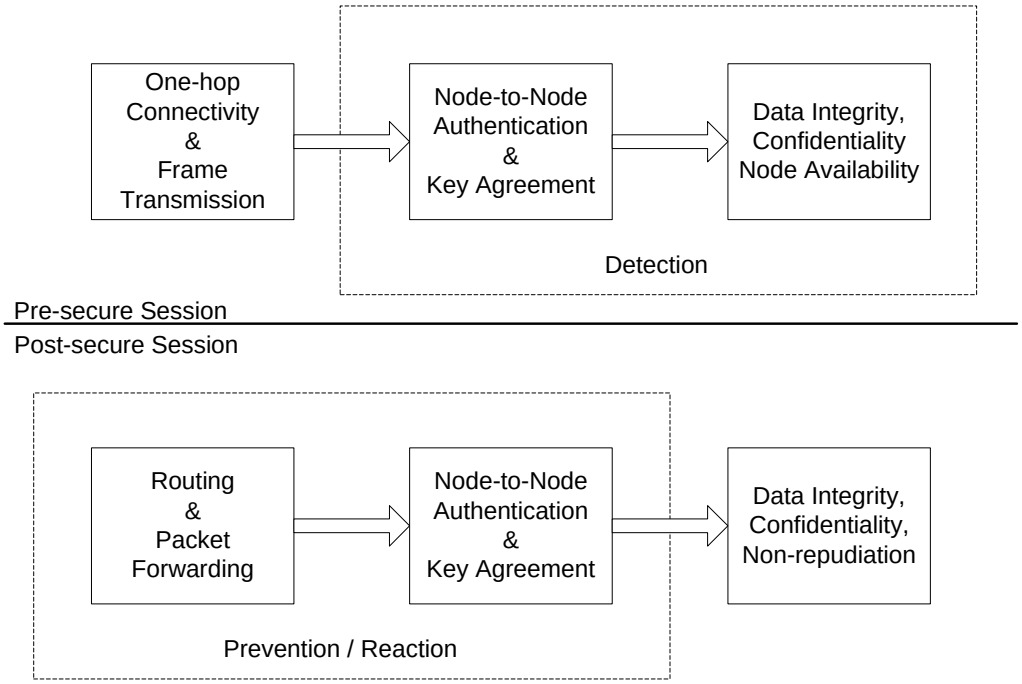


Figure 2 – Protocol Securization Process

The layered security mechanisms should include prevention, detection and reaction operations to prevent intruders from entering the network. They should discover the intrusions and take actions to prevent persistent adverse effects. The prevention process can be embedded in secure routing and packet forwarding protocols to prevent the attacker from installing incorrect routing states at nodes.

The detection process exploits ongoing attacks through identification of abnormal behaviour by malicious or selfish nodes. Such misbehaviour can be detected in the pre-secure session either by node-to-node authentication or by node availability mechanisms as illustrated in Figure 3. Once the attacker is detected, reaction operations reconfigure routing and packet forwarding operations. The adjustments can range from avoiding this particular node in route selection to expelling the node from the network.

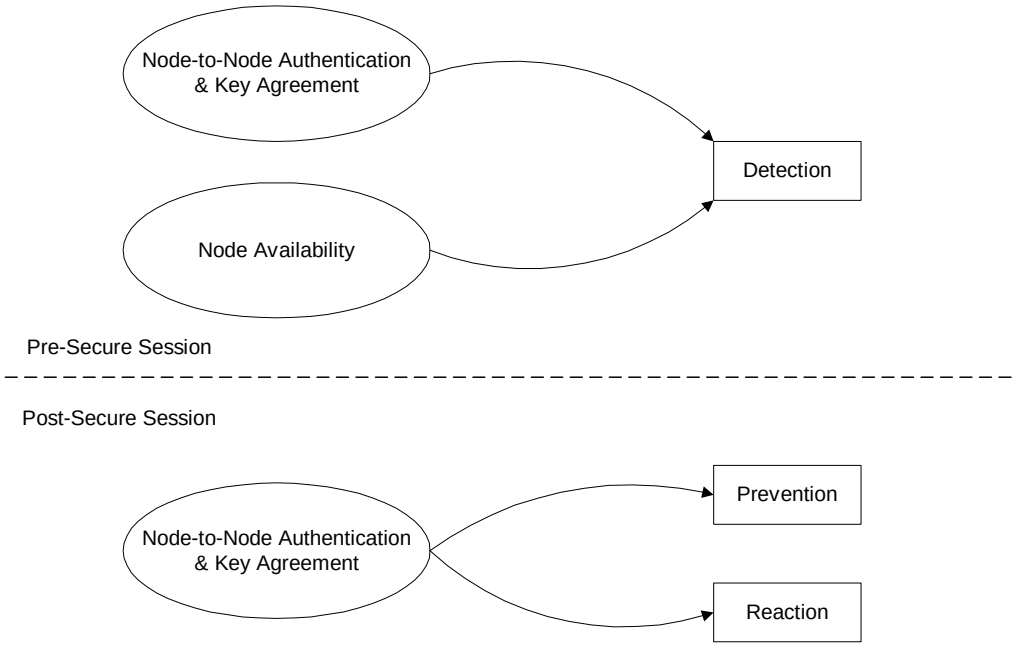


Figure 3 – Interaction of Prevention-Detection-Reaction Mechanisms

5.1. Pre-secure Session

The layered security design adapts cryptographic methods to offer multiple protection lines to communicating nodes. When one or more nodes are connected to a MANET, the first phase of node-to-node authentication and key agreement procedure takes place. At this early stage, it is necessary to be able to determine the true identity of the nodes which could possibly gain access to a secret key later on. Let us consider the MANET of Figure 4 with the authenticated nodes A, B, and C.

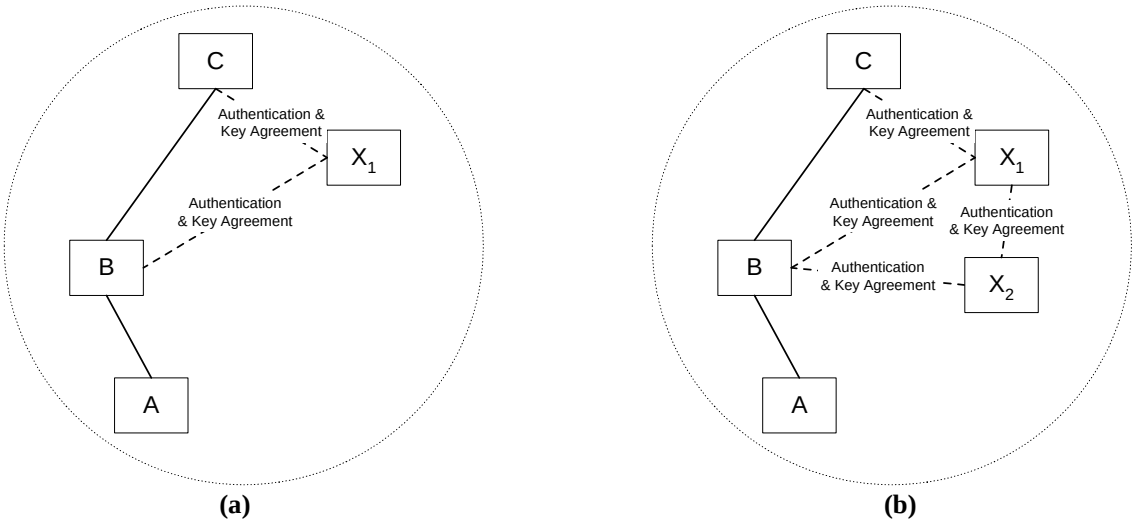


Figure 4 – New Nodes in MANET

As illustrated in Figure 4 (a), when node X_1 enters the MANET, it will be authenticated by both nodes that will exchange routing information later on in the post-secure session (i.e. B and C). When two nodes e.g. nodes X_1 and X_2 enter the MANET simultaneously, they will both be authenticated by valid nodes. Even though we refer to nodes entering simultaneously there will always be a small time difference in their entrance to the network. Therefore, node X_1 will enter slightly before node X_2. In this case node X_1 gets authenticated first by nodes B and C, making node X_1 a valid node and upon entrance of node X_2, nodes B and X_1 will authenticate node X_2. 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 and key agreement 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 and key agreement scheme can be considered as a “good” candidate at the pre-secure session. Such a scheme is preferable to a computationally secure authentication and key agreement 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 and key agreement can be achieved with a zero knowledge protocol, similar to the protocol described in [17] 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 4 (a) for example, node X_1 can prove its identity to nodes B and C ensuring that specific discrete logarithms (i.e. $y_1=\beta_1^{x1}$ and $y_2=\beta_1^{x2}$ to the bases β_1 and β_2) satisfy a linear equation (i.e. $\lambda_1 x_1 + \lambda_2 x_2 = b \pmod q$ for integers λ_1 and λ_2) [17]. In this example, node X_1 sends to nodes B and C some logarithms. Nodes B and C respond with the parameters of the logarithms and finally node X_1 responds with a resulting proof that satisfies a known linear equation. Following the same procedure, nodes B and C can prove their identity to node X_1.

The node-to-node authentication and key agreement procedure found in the pre-secure phase can detect whether an authenticated node has been compromised. This can be done when a random secret number has been injected and shared between the nodes. The range of the exchanged random secret can be checked by the node. This will probably enable or disable traffic to be forwarded to nodes that fail to authenticate.

The random secret can take part in the generation of the encryption key that takes place at the post-secure session. Such random information can also be used to determine node availability. When the authentication and key agreement phases have been completed, frames can be encrypted and data integrity can be achieved using state-of-the-art existing cryptographic algorithms.

5.2. Post-secure Session

When routing information is ready to be transferred, the second phase of the authentication and key agreement process takes place. Authentication carries on in the available nodes starting one-hop at a time from the source to destination route. While nodes in the source to destination path are authenticated, they also agree on an encryption key, also referred to as session key, which will be used to encrypt their traffic. Similar to the pre-secure session, data confidentiality and integrity can be achieved using well-known cryptographic algorithms. Moreover, non-repudiation can be attained with cryptographic techniques, such as digital signatures, message authentication codes (MAC) and hash functions.

In this second phase of the authentication and key agreement, strong authentication is necessary since the actual data are ready to be sent. Challenge-response protocols can be applied to identify users through verification of their knowledge of a shared secret. Such protocols are based on symmetric and/or asymmetric key techniques. When symmetric schemes are applied, the nodes share a symmetric key k and mutual authentication between nodes B and X_1 (see Figure 4a) can be achieved in the following way:

$$\begin{aligned} &B \leftarrow X_1 : r_1 && (1)\\ &B \rightarrow X_1 : E_k(r_1, r_2, B) && (2)\\ &B \leftarrow X_1 : E_k(r_2, r_1) && (3) \end{aligned}$$

where E is a symmetric encryption algorithm and r_1, r_2 are random numbers.

Node X_1 generates a random number and sends it to node B. Upon reception of (1), node B encrypts the two random numbers and its identity and sends message (2) to node X_1. Then, node X_1 checks for its random number, constructs (3) and sends it to node B. Upon reception of (3), node B checks that both random numbers match these ones used earlier. The encryption algorithm in the above mechanism may be replaced by MAC, which is efficient and affordable for low-end devices, such as sensor nodes. However, MAC can be verified only by the intended receiving node, making it ineligible for broadcast message authentication.

When asymmetric key techniques are applied, nodes own a key pair and mutual authentication between nodes X_1 and C (Figure 4a) can be achieved in the following way:

$$X_1 \rightarrow C : P_C(r_1, A) \quad (1)$$
$$X_1 \leftarrow C : P_{X1}(r_1, r_2) \quad (2)$$
$$X_1 \rightarrow C : r_2 \quad (3)$$

where P is a public key encryption algorithm and r_1, r_2 are random numbers.

Nodes A and B exchange random numbers in messages (1) and (2) that are encrypted with their public keys. Upon decrypting messages (1) and (2), nodes B and A achieve mutual authentication by checking that the random numbers recovered agree with the ones sent in messages (3) and (2) respectively. Note that the public key encryption algorithm can be replaced by digital signatures.

Digital signatures though involve much more computational overhead in signing, decrypting, verifying and encrypting operations. They are also less resilient against DoS attacks since an attacker may launch a large number of bogus signatures to exhaust the victim's computational resources for verifying them. Each node also needs to keep a certificate revocation list or revoked certificates and public keys of valid nodes.

In many cases, routing messages are typically propagated through multiple paths and redundant copies of such messages can be used by compromised nodes. The authentication and key agreement procedure found in the post-secure phase can prevent and react to compromised nodes. This can occur by using the random information that has been injected and agreed upon at the pre-secure session.

The above mentioned layered security solution poses grand yet exciting research challenges. The structuring process steps of layered security design (Figure 2) can be expanded into a "process framework", as illustrated in Figure 5.

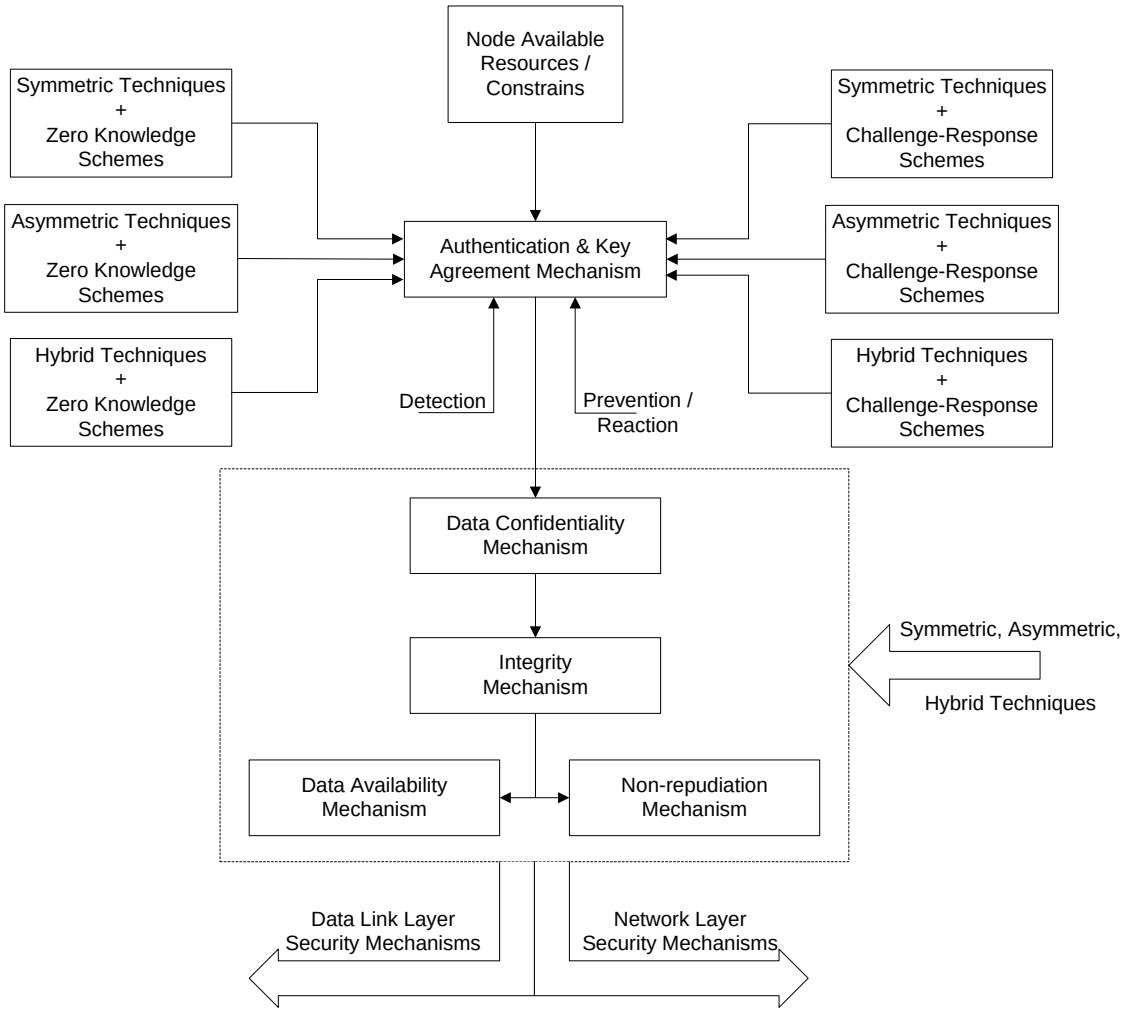


Figure 5 – Process Framework for Layered Security Design

A node has to properly select security mechanisms that fit well into its own available resources, deployment cost and other complex constraints. It expects best effort from each component. It is necessary to identify the systems principles of how to build such link and network security mechanisms that will explore their methods and learn to prevent, detect and react to threats accordingly.

For example, if it is our intention to build security mechanisms at the data link layer then it can be seen in Figure 5 that the authentication and key agreement mechanism can be based on symmetric, asymmetric and/or hybrid techniques to identify nodes. The identification procedure can apply zero knowledge schemes. Such authentication mechanism should also integrate detection methods. The data confidentiality, integrity and node availability mechanisms can be based on symmetric, asymmetric or hybrid techniques.

Likewise, the security mechanisms at the network layer consist of an authentication and key agreement mechanism that will be based on symmetric, asymmetric and/or hybrid techniques to identify nodes; an identification procedure that follows challenge-response schemes and integrates prevention and reaction methods; and data confidentiality integrity, and node availability mechanisms that can apply symmetric, asymmetric or hybrid techniques.

Evaluating the layered security design also offers new research opportunities. The effectiveness of each security operation and the minimal number of fences the system has to build to ensure a certain degree of security assurance should be evaluated through a combination of analysis, simulations, and measurements.

6 Conclusions

Security is an issue that it is more sensitive in MANET than 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 key management mechanisms, on the other side, are explored less than routing protocols. Moreover, the least explored research area relates to link security protocols.

Since mobile ad hoc networks can be formed, merged together or partitioned into separate networks on the fly, the need for more sophisticated security measures arises. Therefore, security requirements, such as authenticity, confidentiality, integrity and non-repudiation should focus on both link and network layers. In this article, we explored the security requirements in a layered approach, in which prevention, detection and reaction mechanisms should be available. Integrating cryptographic mechanisms in the pre-secure and post-secure sessions will help to create multiple lines of defence and further protect ad hoc networks from malicious attackers.

Designing such cryptographic mechanisms, which are efficient in terms of both computational and message overhead, is the main research objective in the area of authentication and key management for ad hoc networks. In wireless sensing for instance, designing efficient cryptographic mechanisms for authentication and key management in broadcast and multicast scenarios poses a great challenge.

Once the authentication and key management infrastructure is in place, data confidentiality and integrity issues can be tackled by using existing and efficient symmetric algorithms since there is no need to develop any special integrity and encryption algorithms for ad hoc networks.

7 Acknowledgements

This work has been partially supported by the Hellenic Ministry of Education and Religious Affairs through “Pythagoras” research project.

References

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

[2] A. Stubblefield, J. Ioannidis, and A. Rubin, “Using the Fluhrer, Martin, and Shamir Attack to break WEP”, *NDSS*, 2002.

[3] B. Dahill et al., “A Secure Routing Protocol for Ad Hoc Networks”, *IEEE ICNP*, 2002.

[4] B. Schneier, *Secret and Lies, Digital Security in a Networked World*, Wiley, 2000.

[5] C. Kaufman, R. Perlman, and M. Speciner, *Network security: private communication in a public world*, Prentice-Hall, Inc., 1995.

[6] C. Perkins et al., “Ad Hoc On-Demand Distance-Vector Routing (AODV)”, *IETF draft*, 2001.
[7] C. Perkins, *Ad Hoc Networking*, Addison-Wesley, 2000.
[8] E.M. Royer and C.-K. Toh, “A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks”, *IEEE Personal Communications Magazine*, pp. 46-55, 1999.
[9] F. Stajano and R. J. Anderson, “The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks”, *Proceedings of the 7th International Workshop on Security Protocols*, p.172-194, 1999.
[10] 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*, USA, 2001.
[11] J. Kong et al., “Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks”, *IEEE ICNP*, Riverside, USA, 2001.
[12] L. Blazevic et al., “Self-Organization in Mobile Ad-Hoc Networks: the Approach of Terminodes”, *IEEE Communications Magazine*, June 2001.
[13] 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, 2000.
[14] L. Zhou and Z.J. Haas, “Securing Ad Hoc Networks”, *IEEE Network Magazine*, 1999.
[15] N. Asokan and P. Ginzboorg, “Key agreement in ad hoc networks”, *IEEE Computer Communications*, 23, 1627-1637, 2000.
[16] N. Borisov, I.Goldberg, and D. Wagner, “Intercepting Mobile Communications: The insecurity of 802.11”, *ACM MOBICON*, 2001.
[17] N. Komninos, *Security Architecture for Future Communication Systems*, PhD Thesis, Lancaster university, 2003.
[18] 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, 2003.
[19] 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.
[20] P. Papadimitratos , Z. J. Haas, “Secure Link State Routing for Mobile Ad Hoc Networks”, *Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops)*, 2003
[21] 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)*, San Antonio, 2002.
[22] S. Bhargava and D.P. Agrawal, “Security Enhancements in AODV Protocol for Wireless Ad Hoc Networks”, *Vehicular Technology Conference, 2001*, vol. 4, pp. 2143-2147, 2001.
[23] S. Marti et al., “Mitigating routing misbehavior in mobile ad hoc networks”, *Proceedings of the 6th annual international conference on Mobile computing and networking*, p.255-265, Boston, Massachusetts, United States, 2000.
[24] W. Stallings, *Cryptography and Network Security (2nd ed.): Principles and Practice*, Prentice-Hall, Inc., 1998.
[25] 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.
[26] Y. Hu, A. Perrig, and D. Johnson, “Ariadne: A Secure on-demand Routing Protocol for Ad Hoc Networks”, *ACM WiSe*, 2002.

[27] Y. Hu, A. Perrig, and D. Johnson, “Packet Leashes: A Defence against wormhole Attacks in Wireless Networks, *IEEE INFOCOM*, 2002.
[28] Y. Hu, D. Johnson, and A. Perrig, “Sead: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks”, *IEEE WMCSA*, 2002.