



## City Research Online

### City, University of London Institutional Repository

---

**Citation:** Komninos, N., Vergados, D. D. and Douligeris, C. (2007). Multifold node authentication in mobile ad hoc networks. *International Journal of Communication Systems*, 20(12), pp. 1391-1406. doi: 10.1002/dac.882

This is the unspecified version of the paper.

This version of the publication may differ from the final published version.

---

**Permanent repository link:** <https://openaccess.city.ac.uk/id/eprint/2508/>

**Link to published version:** <http://dx.doi.org/10.1002/dac.882>

**Copyright:** City Research Online aims to make research outputs of City, University of London available to a wider audience. Copyright and Moral Rights remain with the author(s) and/or copyright holders. URLs from City Research Online may be freely distributed and linked to.

**Reuse:** Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

# Multifold Node Authentication in Mobile Ad-Hoc Networks

Nikos Komninos<sup>(a, b)</sup>, Dimitrios D. Vergados<sup>(a)</sup> and Christos Douligeris<sup>(c)</sup>

<sup>(a)</sup> Department of Information and Communication Systems Engineering, University of the Aegean, GR-832 00, Karlovassi, Samos, Greece  
Email: {komninos; vergados}@aegean.gr

<sup>(b)</sup> Algorithms & Security Group, Athens Information Technology, GR-190 02, Peania Greece  
Email: nkom@ait.edu.gr

<sup>(c)</sup> Department of Informatics, University of Piraeus, GR-18534, Piraeus Greece  
Email: cdoulig@unipi.gr

## Abstract

*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. In this article we propose a multifold node authentication approach for protecting mobile ad hoc networks. The security requirements for protecting data link and network layers are identified and the design criteria for creating secure ad hoc networks using multiple authentication protocols are analysed. Such protocols, which are based on zero knowledge and challenge response techniques, are presented through proofs and simulation results.*

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

## 1. Introduction

Unlike traditional mobile wireless networks, ad hoc networks do not rely on a fixed infrastructure but on each other to keep the network connected. Such networks are also referred to as mobile ad hoc networks (MANET) [7]. Unlike networks using dedicated nodes to support basic functions like packet forwarding, routing, and network management, in ad hoc networks those functions are carried out by all available nodes [6, 7].

So far, applications of MANETs have been proposed 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 possible to deploy MANET for civilian applications as well [4, 7, 23]. 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-organized, meaning that the network could be run by the operation of the end-users.

Since ad hoc networks can be deployed rapidly and several sensitive applications are investigated in this environment, important security issues are raised. The security requirements in ad hoc networks are different than the ones used for 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, small battery life) and frequent network topology changes in the network.

In this article, we seek to identify the security issues and attacks in MANETs and also examine the adaptation of cryptographic protocols in the data link and network layers. A multifold node authentication approach is proposed which implements multiple lines of defense against malicious attacks. Section 2 discusses the security challenges and attack types that exist in ad hoc networks. It also presents the security mechanisms implemented at the link and network layer with respect to the requirements of MANET.

Section 3 describes the multifold node authentication approach and discusses how challenge-response and zero knowledge cryptographic protocols can be applied. Section 4 presents a timing analysis of specific zero knowledge and challenge response protocols to compare the execution time for one-hop multifold authentication. Furthermore, section 5 concludes with remarks and comments on the unexplored security areas for MANET.

## 2. Security Challenges in Mobile 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 data authenticity, integrity, and confidentiality difficult to achieve [7].

Similar to other wireless networks, ad hoc networks are susceptible to *passive* and *active* attacks [1, 4, 7, 23]. 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 have as target to cause congestion, propagate incorrect routing information, prevent services from working properly or shut them down completely [11, 12, 13, 25].

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*. 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* [11, 12, 13, 17, 23].

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* [10, 18, 19, 23, 26]. In the latter, two compromised nodes create a tunnel (or wormhole) that is linked through a private connection and thus they manage to 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.

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, 18, 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* that result in erroneous and bogus routing messages [14].

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 consume a significant portion of network resources, and introduce wireless channel contention and network contention in ad hoc networks [4, 7, 23].

## **2.1. Security Issues in the Data Link Layer**

It is essential to distinguish the relevance of security mechanisms implemented in the data link layer with respect to the requirements of MANET. Two different environments can be identified in which the security mechanisms can potentially be deployed: *802.11* or *Bluetooth* [17] and *mobile ad hoc networks*.

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 is then completely justified as a means of building a 'wired equivalent' security as stated by the objectives of wireless equivalent privacy (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 either where 802.11 or Bluetooth protects wireless links or on physically protected wired links.

The existence of several types of cryptographic attacks due to misuse of the cryptographic primitives have identified vulnerabilities in WEP. The 802.11 protocol is vulnerable to DoS attacks where the adversary may exploit its binary exponential back-off scheme to deny access to the wireless channel from its local neighbors. In addition, a continuously transmitting node can always capture the channel and cause other nodes to back off endlessly which can trigger a chain reaction from upper layer protocols (e.g. TCP window management) [2, 15].

Another DoS attack is also applicable in 802.11 with the use of the network allocation vector (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, 15].

In the case of mobile ad hoc networks, there are *trusted* and *non-trusted* environments. In the *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 [1, 4, 7, 13, 23].

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.

Regardless of the type of environment, the main operations of each layer should be investigated for its protection. The main link layer operations are *one hop connectivity* and *frame transmission* [17]. 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.

## 2.2. Security Issues in the Network layer

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 attacks related to 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 active research efforts in identifying and defending more sophisticated routing attacks [9, 23, 25, 26, 26].

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 [13]. DoS is another type of attack that targets packet-forwarding protocols and introduce wireless channel contention and network contention in ad hoc networks [4, 7, 23].

Current efforts towards the design of secure routing protocols are mainly focused on reactive routing protocols, such as in dynamic source routing (DSR) or ad-hoc on demand distance vector (AODV) [6, 21]. Reactive routing protocols have been demonstrated to perform better with significantly lower overheads than proactive protocols since they are able to react quickly to topology changes while keeping routing overhead low in periods or areas of the network in which changes are less frequent. Some of these are briefly described in the next few paragraphs.

Current secure routing protocols 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 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 [13, 22].

Another reactive secure ad hoc routing protocol ARIADNE [8, 25], which is based on [6], guarantees point-to-point authentication using a keyed message authentication code (MAC). Next, the ARAN [8] secure routing protocol 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 to use in terms of CPU and energy usage.

SEAD [26], on the other hand, is a proactive protocol based on the destination sequenced distance vector protocol 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 [8]. SEAD does not cope with the wormhole attack and the authors propose, as in the ARIADNE protocol, to use a different protocol to detect the threat [8, 26].

### **3. Multifold Node Authentication**

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 newborn attacks. It is essential, therefore, to design secure ad hoc networks that will result in multiple lines of defense against both known and unknown security threats.

As mentioned in section 2 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 the link and the network security mechanisms that can integrate a multifold node authentication approach consisting of two phases. The operations of either link or network layer can enable one of the two phases to take place. In phase-one, for example, the node authentication procedure attempts to determine the true identity of the communicating nodes through a non-interactive zero knowledge protocol. Likewise, in phase-two the authentication procedure seeks again the identities of the communicating nodes through a challenge-response protocol.

It is essential to mention that 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 at the first phase. 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 at this early stage [1, 4]. Therefore, authentication can be achieved with a zero knowledge protocol, similar to [16] that provide such characteristics.

The idea of such cryptographic protocols is that they allow a claimant, a node in 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 the protocol. In such protocols, nodes must exchange multiple messages, also referred to as interactive, where proof is probabilistic rather than absolute. However, interactive zero protocols are not suitable for wireless environments since they exchange multiple messages and result to 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 the second phase of the authentication, node authentication is essential before routing information is ready to be sent. A computationally secure authentication scheme is preferable than a provably secure authentication scheme because it requires the use of a symmetric or asymmetric key encryption algorithm. It is necessary to use an encryption algorithm to authenticate nodes since it is the last procedure before information is exchanged between communicating nodes. Thus, the security in multifold node authentication will not rely only on the apparent intractability of a single computational problem. A challenge-response protocol can be chosen where users and nodes can prove their identities by demonstrating knowledge of a shared secret known to be associated with them.

### 3.1. First Phase

The multifold node authentication design adopts 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 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 1 with the authenticated nodes A, B, and C.

As illustrated in Figure 1a, when node X1 enters the MANET, it will be authenticated by both nodes that will exchange routing information later on in the second phase (i.e. B and C). When two nodes e.g. X1 and X2 enter the MANET simultaneously (Figure 1b), 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. When X1 enters slightly before X2, then X1 gets authenticated first by nodes B and C, making X1 a valid node and next X2 gets authenticated by nodes B and X1.

When two or more nodes are simultaneously connected to a MANET (e.g. Figure 1b) there will still be a fraction of time that X1, for example, will enter the network first and will be authenticated. Once X1 and X2 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.

In Figure 1a for example, X1 can prove its identity to B and C ensuring that the discrete logarithms,  $y_1 = \alpha_1^{x_1}$  and  $y_2 = \alpha_2^{x_2}$ , to the bases  $\alpha_1, \alpha_2$ , satisfy the linear Equation 1,

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

for integers  $k_1, k_2$  and prime number  $p$  [16].

In the protocol, X1 first computes  $y_3 = \alpha_3^{x_3}$ ,  $y_4 = \alpha_4^{x_4}$  and solves Equation 2, for integers  $x_3, x_4$ .

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

Then, as shown below,

$$B, C \leftarrow X1 : y_5 = \alpha_1^{x_3}, y_6 = \alpha_2^{x_4} \quad (M1)$$

$$B, C \rightarrow X1 : H(\alpha_1, \alpha_2, y_1, y_2, k_1, k_2, b, y_5, y_6) = y_7 \quad (M2)$$

$$B, C \leftarrow X1 : y_8 = x_3 - y_7 \cdot x_1 \pmod{p}, y_9 = x_4 - y_7 \cdot x_2 \pmod{p} \quad (M3)$$

X1 sends  $y_5$  and  $y_6$  to B and C. Upon reception of message (M1), B and C compute  $y_7$  with one way hash function and sends message (M2) to X1. Next, X1 checks the validity of (M1), constructs message (M3) and sends  $y_8, y_9$  to B and C.

X1 convinces B and C that he/she knows the discrete algorithms of  $y_1$  and  $y_2$  to the bases  $\alpha_1$  and  $\alpha_2$ , 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 B and C, will always succeed in constructing a valid proof by first reconstructing  $y_{10} = \alpha_1^{y_8} \cdot y_1^{y_7}$ ,  $y_{11} = \alpha_2^{y_9} \cdot y_2^{y_7}$ , 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.

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

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

$$\begin{aligned} y_{10} &= \alpha_1^{y_8} \cdot y_1^{y_7} = \alpha_1^{x_3 - y_7 \cdot x_1} \cdot \alpha_1^{x_1 \cdot y_7} = \alpha_1^{x_3} = y_5 \\ y_{11} &= \alpha_2^{y_9} \cdot y_2^{y_7} = \alpha_2^{x_4 - y_7 \cdot x_2} \cdot \alpha_2^{x_2 \cdot y_7} = \alpha_2^{x_4} = y_6. \end{aligned}$$

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, B and C calculate  $y_{12}$  and compares 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  $\alpha_1, y_1$  and  $\alpha_2, y_2$  which implies the knowledge of  $x_1$  and  $x_2$ , the discrete logarithms  $y_1, y_2$  to the bases  $\alpha_1, \alpha_2$ , but this contradicts the assumption that the cheating E does not know  $x_1$  and  $x_2$ .

Furthermore, B and C verify whether the response  $y_8$  and  $y_9$ , satisfies Equation 3. Thus,

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

and validates the identity of X1.

### 3.2. Second Phase

When routing information is ready to be transferred, the second phase of the multifold node authentication takes place. Authentication carries on in the available nodes starting with one-hop at a time from the source to destination route. While nodes in the source to destination path are authenticated, they can also agree on a secret key, which will be used to encrypt their traffic.

Based on the zero knowledge protocol of section 3.1, integers  $x_1$  and  $x_2$  are known to all nodes and can be used here as a shared secret key. Hence, when symmetric techniques are applied mutual authentication between B and X1 (see Figure 1a) can be achieved based on ISO/IEC 9798-2:

$$B \leftarrow X1 : r_1 \quad (M1)$$

$$B \rightarrow X1 : E_{x_1}(r_1, r_2, B) \quad (M2)$$

$$B \leftarrow X1 : E_{x_2}(r_2, r_1) \quad (M3)$$

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

Node X1 generates a random number and sends it to B. Upon reception of (M1), B encrypts the two random numbers and its identity and sends message (M2) to X1. Next, X1 checks for its random number and then constructs (M3) and sends it to B. Upon reception of (M3), B checks that both random numbers match those 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.

On the other hand, when asymmetric key techniques are applied, nodes own a key pair and mutual authentication between X1 and C (Figure 1a) can be achieved by using the modified Needham-Schoeder public key protocol [1] in the following way:

$$X1 \rightarrow C : P_C(r_1, X1) \quad (M1)$$

$$X1 \leftarrow C : P_{X1}(r_1, r_2) \quad (M2)$$

$$X1 \rightarrow C : r_2 \quad (M3)$$

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

$X1$  and  $C$  exchange random numbers in messages (M1) and (M2) that are encrypted with their public keys. Upon decrypting messages (M1) and (M2),  $C$  and  $X1$  achieve mutual authentication by checking that the random numbers recovered agree with the ones sent in messages (M3) and (M2) respectively. Note that the public key encryption algorithm can be replaced by an elliptic curve cryptosystem (ECC) or digital signatures.

Digital signatures, however, involve much more computational overhead in signing, decrypting, verifying and encrypting operations. They are 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.

#### 4. Implementation Results

The multifold authentication solution poses grand yet exciting research challenges. Since a mobile communication system expects a best effort performance from each component, MANETs have to properly select authentication mechanisms for their nodes that fit well into their own available resources. 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 and react to threats accordingly.

The analysis presented in this section targets to compare the execution time of well known authentication protocols for the purposes of multifold authentication. The described protocols in sections 3.1 and 3.2 were simulated following the MANET infrastructure of Figure 1a. The zero knowledge and challenge-response authentication protocols were simulated in an OPNET network simulator, whereas the encryption algorithms were implemented in a digital signal processor (DSP). The testbed consisted of an IBM compatible PC, in which OPNET was installed, and two parallel 36303 Motorola DSPs (66MHz), in which encryption and decryption were performed.

Symmetric, asymmetric and elliptic curve cryptosystems were implemented to offer a complete analysis of the authentication protocols of section 3.2. The advanced encryption standard (AES), RSA, and Menezes-Vanstone cryptosystems were used as symmetric, asymmetric key and elliptic curve algorithms respectively. The key size was based on X9.30 standard specifications.

As illustrated in Table 2 and as specified in the current draft of the revision of X9.30, for reasonable secure 128-bit AES, 2048-bit and 224-bit are the "appropriate" key sizes for RSA, when the Chinese Remainder Theorem (CRT) is used, and for ECC, respectively [1, 27, 28]. Note that in the results of Table 2, the AES key setup routine is slower for decryption than for encryption; for RSA encryption, we assume the use of a public exponent  $e = 65537$  while ECC uses an optimal normal base curve [1, 4].

Table 3 shows the time it is required for a node to be authenticated, when a combination of cryptographic protocols is used in the first and second phase. For example, when a node enters a MANET, it can be authenticated by a zero knowledge protocol similar to the one in section 3.1. It is not recommended, however, for nodes to follow exactly the

same authentication procedure in phase two when routing information is ready to be transferred. This is because the authentication procedure that was successful once is most likely to succeed again without increasing security.

Notice that when exactly the same authentication procedure is deployed in both phases, the total execution time is faster (i.e. 42.82ms, 96.44ms, 340.28ms and 290.34ms) than the execution time of combined cryptographic techniques (i.e. 129.26ms, 383.10ms and 33.16ms). Considering that the authentication procedure that was successful once is most likely to succeed again without increasing security, a combination of zero knowledge and challenge-response authentication techniques appears to be a recommended option when link and network layers operations are taking place.

In such circumstances, the decision of whether to use zero knowledge with symmetric or asymmetric key techniques can be determined by timing analysis and therefore node resources. Note that, no consideration was taken regarding to the physical connection link between DSPs and the PC in the total timing and different implementation will yield to different results. In addition, the zero knowledge and challenge-response total execution time was considered for one-hop connectivity. In the case of broadcast messaging, packets were dropped by the neighboring nodes in a table-driven routing protocol without affecting the execution time of the authentication procedure. Moreover, no timing differences were observed in different network loads.

The analysis presented in Table 3 evaluates multiple authentication fences in MANETs and offers new application opportunities. The effectiveness of each authentication operation and the minimal number of fences the system has to pose to ensure some degree of security assurance was evaluated through simulations analysis and measurement in principle.

Even though the results of this section were obtained by specific zero knowledge and challenge-response protocols useful information can be drawn. MANET security designers are able to determine whether to use multiple authentication techniques or not. They can also decide on which combination of zero knowledge and challenge-response technique to apply on their applications.

## **5. Concluding Remarks**

Security of MANET has become a more sophisticated problem than security of 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, whereas 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, security becomes more sophisticated. Security requirements, such as authenticity should focus on the operations of both link and network layers. In this article, we explored the security issues of MANETs and integrated cryptographic mechanisms in the first and second phase that helped to design multiple lines of defense and further protect ad hoc networks against malicious attacks.

Designing such cryptographic mechanisms as zero knowledge and challenge-response protocols, which are efficient in the sense of both computational and message overhead,

is the main research objective in the area of authentication and key management for ad hoc networks. For instance in wireless sensing, designing efficient cryptographic mechanisms for authentication and key management in broadcast and multicast scenarios may poses a challenge. The execution time of specific protocols was examined and useful results were obtained when multiple lines of defence were applied.

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.

#### **4 Acknowledgements**

This research work was 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". The author Komninos was with the Dept. of Information and Communication Systems Engineering at the University of Aegean, when this research work was performed. We are also grateful to the anonymous reviewers for their comments and suggestions that helped to improve the quality of the paper.

## 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. Perkins and E. Royer, "Multicast Ad Hoc On-Demand Distance-Vector Routing (MAODV)", *IETF draft*, 2000.
- [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, "The Resurrecting Duckling - What Next?", *Revised Papers from the 8th International Workshop on Security Protocols*, p.204-214, 2000.
- [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. Zhou and Z.J. Haas, "Securing Ad Hoc Networks", *IEEE Network Magazine*, 1999.
- [14] N. Asokan and P. Ginzboorg, "Key agreement in ad hoc networks", *IEEE Computer Communications*, 23, 1627-1637, 2000.
- [15] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The insecurity of 802.11", *ACM MOBICON*, 2001.
- [16] N. Komninos, *Security Architecture for Future Communication Systems*, Ph.D. Thesis, Lancaster University, 2003.
- [17] 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.
- [18] 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.
- [19] 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.
- [20] 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.

- [21] 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.
- [22] 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.
- [23] 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.
- [24] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure on-demand Routing Protocol for Ad Hoc Networks", *ACM WiSe*, 2002.
- [25] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against wormhole Attacks in Wireless Networks, *IEEE INFOCOM*, 2002.
- [26] Y. Hu, D. Johnson, and A. Perrig, "Sead: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", *IEEE WMCSA*, 2002.
- [27] ANSI X9.30, *Public Key Cryptography for the Financial Services Industry: The Digital Signature Algorithm (DSA)*, 1999.
- [28] ANSI X9.31, *Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*, 1998.

# Figures

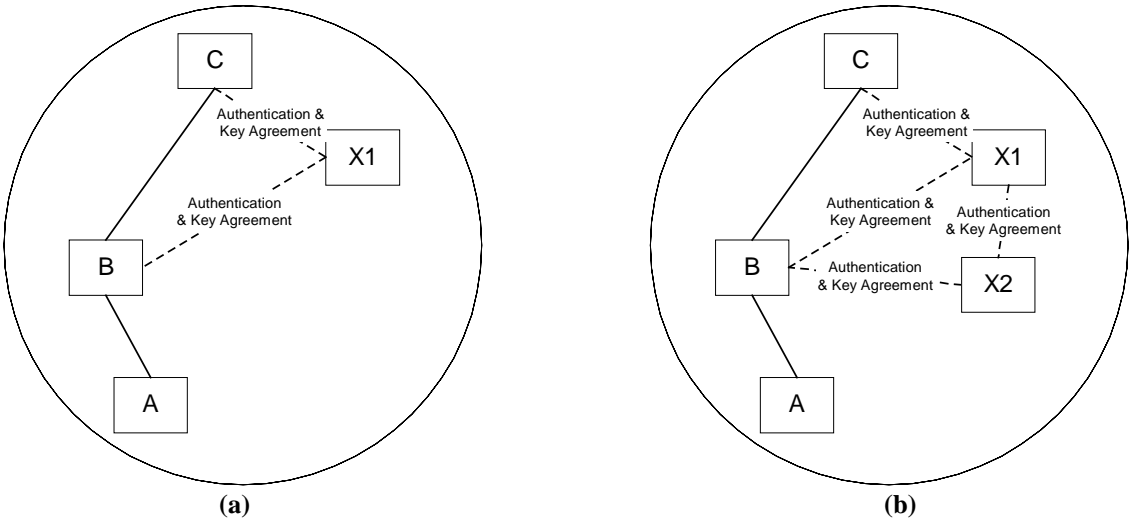


Figure 1 – New Nodes in MANET

# Tables

<b>Network Layer Operations</b> Routing / Data Packet Forwarding	<b>First Phase</b> Node-to-Node Authentication (Zero Knowledge Protocol)	Network Security Mechanisms
<b>Link Layer Operations</b> One-hop Connectivity / Frame Transmission	<b>Second Phase</b> Node-to-Node Authentication (Challenge-Response Protocol)	Link Security Mechanisms

Table 1 – Security in Data Link and Network Layers

Cryptographic Algorithms	Key Length	Encryption (500-bit)	Decryption (500-bit)
AES	128-bit	20ms	23ms
RSA (with CRT)	2048-bit	50ms	120ms
ECC Menezes-Vanstone	224-bit	72ms	68ms

Table 2 – Timing Analysis of Encryption Algorithms for Specific Key Size

<b>Two-Phase Authentication</b>	<b>First Phase</b>	<b>Second Phase</b>	<b>Total</b>	<b>Remarks</b>
2 x Zero Knowledge (ZK) (Section 3.1)	(ZK) 21.41 ± 2ms	(ZK) 21.41 ± 2ms	42.82 ± 5ms	Not Recommended
2 x ISO/IEC 9798-2 (AES) (Section 3.2)	(9798-2-AES) 43.22 ± 2ms	(9798-2-AES) 43.22 ± 2ms	96.44 ± 5ms	Not Recommended
2 x Needham-Schroeder (NS-RSA) (Section 3.2)	(NS-RSA) 170.14 ± 2ms	(NS-RSA) 170.14 ± 3ms	340.28 ± 5ms	Not Recommended
2 x Needham-Schroeder (NS-ECC) (Section 3.2)	(NS-ECC) 145.17 ± 3ms	(NS-ECC) 145.17 ± 2ms	290.34 ± 5ms	Not Recommended
ZK & 9798-2-AES	(ZK) 64.63 ± 2ms	(9798-2-AES) 64.63 ± 2ms	129.26 ± 5ms	Recommended
ZK & NS-RSA	(ZK) 191.55 ± 2ms	(NS-RSA) 191.55 ± 2ms	383.10 ± 5ms	Recommended
ZK & NS-ECC	(ZK) 166.58 ± 2ms	(NS-ECC) 166.58 ± 2ms	333.16 ± 5ms	Recommended

**Table 3 – Timing Analysis of Multifold Node Authentication**