View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by City Research Online

Komninos, N., Vergados, D. D. & Douligeris, C. (2007). A two-step authentication framework for Mobile ad hoc networks. China Communications Journal, 4(1), pp. 28-39.

CITY UNIVERSITY LONDON

City Research Online

Original citation: Komninos, N., Vergados, D. D. & Douligeris, C. (2007). A two-step authentication framework for Mobile ad hoc networks. China Communications Journal, 4(1), pp. 28-39.

Permanent City Research Online URL: http://openaccess.city.ac.uk/2512/

Copyright & reuse

City University London has developed City Research Online so that its users may access the research outputs of City University London's staff. Copyright © and Moral Rights for this paper are retained by the individual author(s) and/ or other copyright holders. All material in City Research Online is checked for eligibility for copyright before being made available in the live archive. URLs from City Research Online may be freely distributed and linked to from other web pages.

Versions of research

The version in City Research Online may differ from the final published version. Users are advised to check the Permanent City Research Online URL above for the status of the paper.

Enquiries

If you have any enquiries about any aspect of City Research Online, or if you wish to make contact with the author(s) of this paper, please email the team at publications@city.ac.uk.

A Two-Step Authentication Framework in Mobile Ad-Hoc Networks

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

*Algorithms & Security Group, Athens Information Technology, 19002 Peania Greece, nkom@ait.edu.gr
**Dept. of Information and Communication Systems Engineering,
University of the Aegean, 83200 Samos Greece, vergados@aegean.gr
***Dept. of Informatics, University of Piraeus, 18534 Piraeus Greece, cdoulig@unipi.gr

Abstract— The lack of fixed infrastructure in ad hoc networks causes nodes to rely more heavily on peer nodes for communication. Nevertheless, establishing trust in such a distributed environment is very difficult, since it is not straightforward for a node to determine if its peer nodes can be trusted. An additional concern in such an environment is with whether a peer node is merely relaying a message or if it is the originator of the message. In this paper, we propose an authentication approach for protecting nodes in 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 several authentication protocols are analyzed. Protocols based on zero knowledge and challenge response techniques are presented and their performance is evaluated through analysis and simulation.

Index Terms— ***Authentication steps, link and network layers, ad hoc networks.***

I. Introduction

AD hoc networks are composed of nodes that do not depend on a fixed infrastructure. These networks are often wireless with mobile nodes. Examples of ad hoc networks can be found in a range of environments, such as military battlefields, emergency missions, sensor networks, and even virtual classrooms. These networks all require a certain level of security that is network function dependent [7, 8]. For example, a military network might be concerned about sensitive intelligence that could affect lives or an entire operation, while a transportation sensor network may be concerned only with the possible disclosure of proprietary data.

This research work was completed when the author was with the University of Aegean. 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".

N. Komninos is with the Athens Information Technology, 19002 Peania, Greece (phone: +30-6682801; fax: +30-6682703; e-mail: nkom@ ait.edu.gr).

D. Vergados is with University of Aegean, 83200 Samos, Greece (e-mail: vergados@aegean.gr).

C. Douligeris is with the University of Piraeus, 18534 Piraeus, Greece (e-mail: cdoulig@unipi.gr).

Mobile ad hoc networks (MANET) [8] face many challenges. Aside from the many forms of protocol attacks that menace a fixed wired network, wireless nodes may also be easier to compromise physically. In addition, ad hoc networks can be highly dynamic since wireless nodes are free to move around. Furthermore, wireless nodes have limited battery life and computational power to cope with these challenges. To compound these problems, the lack of a fixed infrastructure in ad hoc networks causes nodes to rely more heavily on peer nodes, even though establishing trust in such a distributed environment is very difficult [5, 8, 27].

The criteria for protecting ad hoc networks encompass both physical entity security and data security (authentication, integrity, confidentiality, non-repudiation). Availability is another very significant concern. For example, a robust network should not lose connectivity when a small number of nodes leave the network or become unresponsive. Access control must also be considered to prevent unauthorized access.

In this paper, the authentication aspect of ad hoc network security is addressed. A particularly difficult problem in wireless communication is peer identification. The invisible node attack and the less threatening wormhole attacks leverage the fact that it is very difficult for a receiving node to determine if the received message was originated, or was relayed without change, from a neighbor [16]. This fact greatly complicates peer identification.

In this article, we first identify the main security issues and the most prominent attacks in MANET and then we examine the adoption of cryptographic protocols in the data link and network layers. A two-step authentication approach is proposed to implement multiple lines of defense against malicious attacks. This procedure is evaluated and the most promising protocols for such an environment are identified.

This paper is organized as follows. After this introduction, 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 presents current works in the authentication research area. Section 4 describes the two-step authentication procedure and discusses how challenge-response and zero knowledge cryptographic protocols can be applied. Section 4 presents a timing analysis

of some zero knowledge and challenge response protocols to compare the execution time for one-hop two-step authentication. Section 5 concludes with remarks and comments on the unexplored security areas for MANET.

II. Security Issues in the Operational Layers of Mobile Ad Hoc Networks

The vulnerability of the wireless links in a mobile ad hoc environment, 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, and, thus, security, difficult to achieve [7].

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 the Wireless Equivalent Privacy protocol (WEP) of 802.11. If one want to study the security of the data link layer with respect to the requirements of MANET, it is essential to distinguish the associated environment of operation. Two different environments can be identified which in turn identify the security mechanisms that can be potentially deployed: 802.11 or Bluetooth networks [19] and mobile ad hoc networks.

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.

Several types of cryptographic attacks due to the misuse of the cryptographic primitives exploit inherent 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, a situation which can trigger a chain reaction from upper layer protocols (e.g. TCP window management) [3, 18].

Another DoS attack in 802.11 exploits the network allocation vector (NAV) field, which indicates 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 [3, 18].

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 meet the security requirements raised by higher layers including routing and application protocols [2, 5, 8, 15, 27].

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.

Nevertheless, regardless of the type of environment, the main operations of each layer should be investigated for its protection. Since the main link layer operations are one-hop connectivity and frame transmission [20], 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.

The main network operations related to ad hoc networking are routing and data packet forwarding [4, 9]. 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 exist several active research efforts in identifying and defending more sophisticated routing attacks [12, 26, 29, 30].

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 may drop the packets along an established route, 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 [5, 8, 27].

Current efforts towards the design of secure routing protocols are mainly focused on reactive routing protocols, such as in the dynamic source routing (DSR) or in the ad-hoc on demand distance vector (AODV) protocols [7, 24]. It has been shown that reactive routing protocols 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 protocols 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 [4, 9], 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 [15, 25].

Another reactive secure ad hoc routing protocol ARIADNE [9, 29], which is based on [7], guarantees point-to-point authentication using a keyed message authentication code (MAC). The ARAN [9] 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 [30], 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. 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 [9, 30].

III. Related Work

Authentication has been explored less than routing protocols, despite the fact that several authentication mechanisms for ad-hoc wireless networks have already been proposed. Zhou and Hass [16] identified the vulnerability of using a centralized certification authority (CA) for authentication in ad-hoc networks and proposed a method with multiple CAs based on Threshold Cryptography [2]. These multiple CAs have secret shares of a Certificate Authority Signing Key (CASK) while there are no CAs that individually know the whole complete CASK. The multiple CASK can be known only when more than a certain number of m CAs collaborate. Therefore, this method can support network security against up to m−1 collaborative compromised nodes. While Zhou and Hass's method improves the robustness of the authentication system, it depends on the offline authority which elects n CAs ($n \geq m$) during the bootstrapping phase. Furthermore, it has poor availability because if n−m+1 CAs have been compromised, the uncompromised m−1 CAs that are left can not provide authentication services anymore.

Kong et al. [14] proposed another authentication method based on threshold secret sharing [16]. After the bootstrapping phase, a new node can join the network at any time and through self-initialization it can obtain its own secret share of CASK with the help of m local neighbor nodes. Even though this approach enhances scalability and availability, it still depends on an offline authority during the bootstrapping phase. Capkun et al. [25] proposed an authentication method and asserted that mobility helps the security. The key idea is that if two nodes are in the vicinity of each other, they can establish a security association (SA) by exchanging appropriate cryptographic material through a secure channel with a short transmission range. However, this direct solution takes a long time because it requires a node to encounter every node that it wants to communicate with.

Some of the proposals related to the authenticity of ad-hoc networks are based on anonymity schemes. ANODR [14] is based on an on-demand with identity free routing protocol using a symmetric cryptography with a 'trapdoor boomerang onion' (TBO) approach, similar to the onion routing protocol used by Chaum in [9]. The trapdoor mechanism consists of sending cryptographically secured messages which may be opened only by the intended party. In [10] the low performance of the protocol in highly mobile networks was pointed out.

In the MASK [27] protocol both a proactive and a reactive approach are applied simultaneously. A priori anonymous links are established with all neighboring nodes using a symmetric cryptography and a trusted authority. The path discovery process is conducted in an on-demand manner. Mutually authenticated nodes participate in the end-to-end communication. Already established paths may consist of several multipath channels. Nevertheless, the source and destination nodes become unauthenticated. In SDAR [1] the communication between the source and the destination is based on a public key cryptography. Additionally, the destination node shares a symmetric session key with each intermediate node and uses them to secure the discovery path process. This protocol takes advantage of both onion and on demand routing. Messages in SDAR are large and strongly depend on the number of hops. Nevertheless, SDAR is the first anonymous protocol for mobile ad-hoc networks that introduces a trust management system. However, this system supports only three levels of permissible reputation limiting therefore its efficiency.

IV. Two-Step Authentication

The existing proposals in ad hoc networks are typically attack-oriented since they first identify several security threats and then they 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 mentioned in section 2, 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 two-step authentication procedure consisting of two steps. The operations of either link or network layer can enable one of the two steps to take place. In step-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 step-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 MANET. 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 step. 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 the one proposed in [16], that provides such characteristics.

The basic idea behind the operation 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. 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. MANET are suitable for non-interactive zero knowledge protocols where nodes do not need to exchange multiple messages to prove their identity.

In the second step 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 an 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 two-step 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.

1. First Step

The two-step 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 step 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.

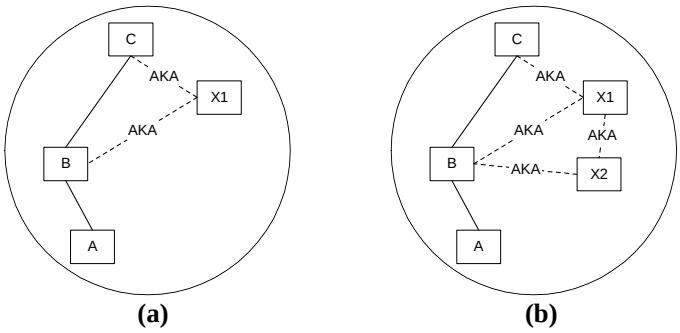

Figure 1 – Authentication of New Nodes in MANET

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 step (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, a provably secure scheme can be applied. X1 proves its identity to B and C by ensuring that the discrete logarithms, $y_1 = a_1^{x1}$ and $y_2 = a_2^{x2}$, to the bases a_1, a_2, satisfy the linear Equation 1:

$$k_1 \cdot x_1 + k_2 \cdot x_2 = b \ (mod\ p) \qquad (1)$$

for integers k_1, k_2 and prime number p [19].

In the protocol, X1 first computes $y_3 = a_3^{x3}$ and $y_4 = a_4^{x4}$ and then solves Equation 2, for integers x_3, x_4:

$$k_1 \cdot x_3 + k_2 \cdot x_4 = 0 \ (mod\ p) \qquad (2)$$

Then, as shown below:

B,C ← X1: $y_5 = a_1^{x3}$, $y_6 = a_2^{x4}$ (M1)
B,C → X1: $H(a_1, a_2, y_1, y_2, k_1, k_2, b, y_5, y_6) = y_7$ (M2)
B,C ← X1: $y_8 = x_3 - y_7 \cdot x_1 \ (mod\ p)$, $y_9 = x_4 - y_7 \cdot x_2 \ (mod\ p)$ (M3)

X1 sends y_5 and y_6 to B and C. Upon reception of message (M1), B and C compute y_7 with a one way hash function and send message (M2) to X1. Next, X1 checks the validity of (M1), constructs message (M3) and sends y_8 and 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 a_1 and a_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 $y_{10} = a_1^{y8} \cdot y_1^{y4}$, $y_{11} = a_2^{y9} \cdot y_2^{y7}$, and then checking whether y_7 is equal to y_{12}, for $H(a_1, a_2, y_1, y_2, k_1, k_2, b, y_{10}, y_{11}) = y_{12}$, and whether Equation 3 is valid:

$$k_1 \cdot y_8 + k_2 \cdot y_9 = - y_7 \cdot b \ (mod\ p) \qquad (3)$$

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

$$y_{10} = a_1^{y8} \cdot y_1^{y7} = a_1^{x3 - y7 \cdot x1} \cdot a_1^{x1 \cdot y7} = a_1^{x3} = y_5$$
$$y_{11} = a_2^{y9} \cdot y_2^{y7} = a_2^{x4 - y7 \cdot x2} \cdot a_2^{x2 \cdot y7} = a_2^{x4} = y_6.$$

Thus,

$$y_{12} = H(a_1, a_2, y_1, y_2, k_1, k_2, b, y_{10}, y_{11}) = H(a_1, a_2, y_1, y_2, k_1, k_2, b, y_5, y_6) = y_7$$

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

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 a_1, y_1 and a_2, y_2 which implies the knowledge of x_1 and x_2, the discrete logarithms y_1, y_2 to the bases a_1, a_2, but this contradicts the assumption that the cheating intruder 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:

$$\begin{aligned} k_1 \cdot y_8 + k_2 \cdot y_9 &= k_1 \cdot (x_3 - y_7 \cdot x_1) + k_2 \cdot (x_4 - y_7 \cdot x_2) \\ &= k_1 \cdot x_3 - k_1 \cdot y_7 \cdot x_1 + k_2 \cdot x_4 - k_2 \cdot y_7 \cdot x_2 \\ &= k_1 \cdot x_3 + k_2 \cdot x_4 - y_7 \cdot (k_2 \cdot x_1 - k_2 \cdot x_2) \\ &= - y_7 \cdot b \ (mod\ p) \end{aligned}$$

and the identity of X1 is validated.

2. *Second Step*

When routing information is ready to be transferred, the second step of the two-step authentication takes place. Authentication carries on in the available nodes starting with one-hop distances 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:

$$\begin{aligned} &B \leftarrow X1 : r_1 && (M1) \\ &B \rightarrow X1 : E_{x1}(r_1, r_2, B) && (M2) \\ &B \leftarrow X1 : E_{x2}(r_2, r_1) && (M3) \end{aligned}$$

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

Node X1 generates a random number and sends this number to B. Upon reception of (M1), B encrypts the two random numbers and its identity and sends message (M2) to X1. Then, X1 checks for its random number, 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 the 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:

$$\begin{aligned} &X1 \rightarrow C : Pc(r_1, X_1) && (M1) \\ &X1 \leftarrow C : P_{X1}(r_1, r_2) && (M2) \\ &X1 \rightarrow C : r_2 && (M3) \end{aligned}$$

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 by digital signatures. Digital signatures, however, involve a higher 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 as the user tries to verify these signatures. Each node also needs to keep a certificate revocation list or the revoked certificates and public keys of valid nodes.

V. IMPLEMENTATION RESULTS

The two-step authentication solution poses grand yet exciting research challenges. Since a mobile communication system expects a best effort performance from each component, MANET 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 compares the execution time of well known authentication protocols to achieve two-step authentication. The described protocols in sections 4.1 and 4.2 were simulated following the MANET infrastructure of Figure 1a. We have considered the simplest MANET structure where a newly -entering mobile node is authenticated by only two neighbouring nodes. Additional tests were carried out for mobile nodes that have three and four neighbouring nodes. The results depended on the number of neighbouring nodes in a proportional way and, thus, they are not presented in this paper.

The zero knowledge and challenge-response authentication protocols were simulated in the OPNET Modeler / Wireless network simulator, whereas the encryption algorithms were implemented in a digital signal processor (DSP). The testbed consisted of an IBM compatible personal computer (PC), in which OPNET was installed, and two parallel 36303 Motorola DSPs (66MHz), in which the encryption and the decryption were performed. The PC and the DSPs communicated through a parallel port.

The OPNET Modeler / Wireless suite has a large set of standard communication protocols, along with number of models for simulating the wireless channel. Individual components are updated and interchanged, allowing us to select mobility, application and channel models that are appropriate for any given MANET scenario. Moreover, the proposed protocols can be easily replaced with models of traditional protocols, allowing us to easily perform comparative simulation analyses.

Symmetric, asymmetric and elliptic curve cryptosystems were implemented to offer a complete analysis of the authentication protocols that were described in section 3.2. As a symmetric key algorithm, the advanced encryption standard (AES) cryptosystem was applied; as an asymmetric key algorithm the Rivest, Shamir, Adleman (RSA) cryptosystem was implemented; and as an elliptic curve the Menezes-Vanstone cryptosystem [2] was deployed. The key size was based on the X9.30 standard specifications.

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 1 – Timing Analysis of Encryption Algorithms for Specific Key Size

As illustrated in Table 1 and as specified in the current draft of the revision of X9.30, for reasonable secure 128-bit key of 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 [2, 31, 32]. The processing times presented in Table 1 are computed in the DSPs. Note that 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 [2, 5]. The processing times are related only to the second phase of the authentication procedure, where an encryption algorithm is applied in ISO/IEC 9798-2 protocol.

Two-Step Authentication	First Step	Second Step	Total	Remarks
2 x Zero Knowledge (ZK) (Section 3.1)	(ZK) 21.41 ± 2ms	(ZK) 21.41 ± 2ms	42.82 ± 5ms	NR
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	NR
2 x Needham-Schroeder (NS-RSA) (Section 3.2)	(NS-RSA) 170.14 ± 2ms	(NS-RSA) 170.14 ± 3ms	340.28 ± 5ms	NR
2 x Needham-Schroeder (NS-ECC) (Section 3.2)	(NS-ECC) 145.17 ± 3ms	(NS-ECC) 145.17 ± 2ms	290.34 ± 5ms	NR
ZK & 9798-2-AES	(ZK) 64.63 ± 2ms	(9798-2-AES) 64.63 ± 2ms	129.26 ± 5ms	R
ZK & NS-RSA	(ZK) 191.55 ± 2ms	(NS-RSA) 191.55 ± 2ms	383.10 ± 5ms	R
ZK & NS-ECC	(ZK) 166.58 ± 2ms	(NS-ECC) 166.58 ± 2ms	333.16 ± 5ms	R

Table 2 – Timing Analysis of two-step Node Authentication

Table 2 shows the time 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 presented in section 3.1. It is not recommended, however, for nodes to follow exactly the same authentication procedure in phase two when the routing information is ready to be transferred, because the authentication procedure that is successful once is most likely to succeed again without providing a significant increase in security.

Notice that when exactly the same authentication procedure is deployed twice in phase one and phase two, the total execution time is faster (i.e. 2xZK=42.82ms, 2xAES=96.44ms, 2xRSA=340.28ms and 2xECC=290.34ms)

than the execution time of the combined cryptographic techniques (i.e. ZK & AES = 129.26ms, ZK & RSA = 383.10ms and ZK & ECC = 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 with asymmetric key techniques can be determined by the timing analysis. Notice that no consideration was given to the physical connection link between the DSPs and the PC in the total timing. A 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 purpose of the simulation analysis, which is presented in Table 2, is to evaluate multiple authentication fences in MANET and offer new application opportunities. The effectiveness of each authentication operation and the minimal number of fences the system has built to ensure some degree of security assurance was evaluated through simulations analysis and measurements.

The results of this section were obtained by specific zero knowledge and challenge-response protocols. MANET security designers can use these results to determine whether to use multiple authentication techniques or not. The timing analysis of Table 2 directs security designers to overcome the single point of failure in an ad hoc network when two-step authentication is implemented. They can also choose which combination of zero knowledge and challenge-response technique to apply in their particular applications. However, we should also take into consideration that the two-step authentication procedure adds extra overhead to the network, an overhead that must be evaluated vis as vis the specific application and the environment the MANET operates in.

VI. Concluding Remarks

The security of MANET has become a considerably more sophisticated problem than the problem of 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 MANET and integrated cryptographic mechanisms in the first and second step 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 pose 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.

References

[1] A. Boukerche, "An Efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc network", *IEEE Computer Communications*, Vol. 28, Iss. 10, 2005, pp. 1193-1203

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

[3] A. Stubblefield, J. Ioannidis, and A. Rubin, "Using the Fluhrer, Martin, and Shamir Attack to break WEP", NDSS, 2002.

[4] B. Dahill et al., "A Secure Routing Protocol for Ad Hoc Networks", IEEE ICNP, 2002.

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

[6] C. Perkins and E. Royer, "Multicast Ad Hoc On-Demand Distance-Vector Routing (MAODV)", *IETF draft*, 2000.

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

[8] C. Perkins, *Ad Hoc Networking*, Addison-Wesley, 2000.

[9] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms", *Communications of the ACM*, 24(2):84-88, February 1981.

[10] 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.

[11] F. Stajano, "The Resurrecting Duckling - What Next?", *Revised Papers from the 8th International Workshop on Security Protocols*, p.204-214, 2000.

[12] 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.

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

[14] J. Kong, X. Hong, "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks", in proc. of the 4th ACM MobiHoc, 2003, pp. 291 - 302.

[15] L. Blazevic et al., "Self-Organization in Mobile Ad-Hoc Networks: the Approach of Terminodes", *IEEE Communications Magazine*, June 2001.

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

[17] N. Asokan and P. Ginzboorg, "Key agreement in ad hoc networks", *IEEE Computer Communications*, 23, 1627-1637, 2000.

[18] N. Borisov, I.Goldberg, and D. Wagner, "Intercepting Mobile Communications: The insecurity of 802.11", *ACM MOBICON*, 2001.

[19] N. Komninos, D. Vergados, and C. Douligeris, "Layered Security Design for Mobile Ad-Hoc Networks", *Computers & Security (Elsevier)*, Volume 25, Issue 2, pp. 124-134, 2005

[20] 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.
[21] 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.
[22] 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
[23] 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.
[24] 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.
[25] S. Capkun, J. P. Hubaux, L. Buttyan, "Mobility Helps Security in Ad Hoc Networks", *Proceedings of the ACM MobiHoc*, 2003, pp. 46 – 56.
[26] 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.
[27] 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.
[28] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure on-demand Routing Protocol for Ad Hoc Networks", *ACM WiSe*, 2002.
[29] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against wormhole Attacks in Wireless Networks", *IEEE INFOCOM*, 2002.
[30] Y. Hu, D. Johnson, and A. Perrig, "Sead: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", *IEEE WMCSA*, 2002.
[31] ANSI X9.30, *Public Key Cryptography for the Financial Services Industry: The Digital Signature Algorithm (DSA)*, 1999.
[32] ANSI X9.31, *Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*, 1998.

BIOGRAPHIES

Nikos Komninos received his B.Sc. degree in Computer Science & Engineering from the American University of Athens, Greece in 1998, his M.Sc. degree in Computer Communications & Networks from Leeds Metropolitan University, UK in 1999 and his Ph.D. degree in Communications Systems from Lancaster University, UK in 2003. Dr. Komninos has several years of R&D experience in the academia and industry working on the evaluation, analysis and development of practical secure communication systems including encryption algorithms, hash functions, digital signatures, security infrastructures and cryptographic protocols. He has also led the development of practical security applications in both software (i.e. Windows) and hardware devices (i.e. FPGAs, CPLD and Smart cards). His main technical interests lie in the areas of authentication, key agreement, intrusion and detection in ad hoc networks, design and evaluation of efficient encryption algorithms, attack analysis of cryptographic protocols and transport / network layer security protocols. Dr. Komninos is also the Guest Editor in the special issue on Advances in Ad Hoc Network Security for the International Journal of Computer Research, Reviewer in several Journals and member of various international societies.

Dimitrios D. Vergados was born in Athens, Greece in 1973. He is a Lecturer in the University of the Aegean, Department of Information and Communication Systems Engineering. He received his B.Sc. in Physics from the University of Ioannina and his Ph.D. in Integrated Communication Networks from the National Technical University of Athens, Department of Electrical Engineering and Computer Science. His research interests are in the area of Communication Networks (Wireless Broadband Networks, Sensor - Ad-hoc Networks, WLANs, IP, MIP, SONET Networks), Neural Networks, GRID Technologies, and Computer Vision. He participated in several projects funded by EU and National Agencies and has several publications in journals, books and conference proceedings. Dimitrios D. Vergados is a member of the IEEE. He is also Guest Editor and Reviewer in several Journals and member of International Advisory Committees of International Conferences.

Christos Douligeris received the Diploma in Electrical Engineering from the National Technical University of Athens in 1984 and the M.S., M.Phil. and Ph.D. degrees from Columbia University in 1985, 1987, 1990, respectively. He held positions with the Department of Electrical and Computer Engineering at the University of Miami, where he reached the rank of associate professor.. He is currently an associate professor at the department of Informatics, University of Piraeus, Greece and an associate member of the Hellenic Authority for Information and Communication Assurance and Privacy. He has served in technical program committees of several conferences. His main technical interests lie in the areas of security and performance evaluation of high speed networks, neurocomputing in networking, resource allocation in wireless networks and information management, risk assessment and evaluation for emergency response operations. He was the guest editor of a special issue of the IEEE Communications Magazine on ''Security for Telecommunication Networks'' and he is preparing a book on ''Network Security'' to be published by IEEE Press/ John Wiley. He is an editor of the IEEE Communications Letters, a technical editor of IEEE Network, Computer Networks (Elsevier), International Journal of Wireless and Mobile Computing (IJWMC) and the Euro Mediterranean Journal of Business (EMJB).