City Research Online

City St George's, University of London

Citation: Komninos, N., Vergados, D. D. & Douligeris, C. (2007). Authentication in a layered security approach for mobile ad hoc networks. Computers & Security, 26(5), pp. 373-380. doi: 10.1016/j.cose.2006.12.011

This is the unspecified version of the paper.

This version of the publication may differ from the final published version. To cite this item please consult the publisher's version.

Permanent repository link: https://openaccess.city.ac.uk/id/eprint/2504/

Link to published version: https://doi.org/10.1016/j.cose.2006.12.011

Copyright and Reuse: Copyright and Moral Rights remain with the author(s) and/or copyright holders. Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge, unless otherwise indicated, 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. For full details of reuse please refer to City Research Online policy.

City Research Online: http://openaccess.city.ac.uk/ publications@citystgeorges.ac.uk

Authentication in a Layered Security Approach for Mobile Ad-Hoc Networks

Nikos Komninos[a, b], Dimitris Vergados[b], Christos Douligeris[c]

(a) Algorithms & Security Group, Athens Information Technology, 19002 Peania Greece, nkom@ieee.org

(b) Department of Information and Communication Systems Engineering, University of the Aegean, 83200 Samos Greece, {komninos, vergados}@aegean.gr

(c) Department of Informatics, University of Piraeus, 18534 Piraeus Greece, 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 investigate authentication in a layered approach, which results to multiple lines of defense for mobile ad hoc networks. The layered security approach is described and design criteria for creating secure ad hoc network using multiple authentication protocols are analysed. The performance of several such known protocols, which are based on challenge-response techniques, is presented through simulation results.

Keywords: authentication, layered security approach, mobile ad hoc networks, authentication protocols, challenge-response techniques.

1. Introduction

A mobile ad hoc network (MANET) is a collection of wireless mobile nodes dynamically forming a temporary network without any existing network infrastructure or centralized administration. 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 [9, 16, 22]. MANET provide an emerging technology for civilian and military applications. However, security in MANET is hard to achieve due to the vulnerability of the link, the limited physical protection of the nodes, and the absence of a certification authority or centralized management point.

The existing security proposals in ad hoc networks are typically attack-oriented [17, 22] 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 new attacks.

When the security of a given network architecture is not properly designed from the beginning, then the security goals (i.e. authenticity, confidentiality, integrity, availability) 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 have called layered security design in [8].

In the layered security design presented in [8], 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 the end-user perspectives, and should be handled by appropriate security mechanisms. In addition, the overall system has to be robust and it should not be critically affected by the breakdown of any individual line of defence.

Authentication can be considered as one of the most important primitives in an ad hoc network. Due to the nature of ad hoc networks and based on the proposed layered security approach, several questions arise. How authentication can be established between neighbouring nodes? Which current authentication protocols are applicable to ad hoc networks? What cryptographic techniques are suitable for such networks? In this article, we seek to identify the security issues related to authentication and also examine the adaptation of challenge-response cryptographic protocols, which are based on symmetric and asymmetric techniques, in a layered security approach. The node authentication methodology implements multiple lines of defence against malicious attacks through the layered approach and is presented with simulation results.

In particular, Section 2 presents related works with emphasis in authentication mechanisms. Section 3 briefly discusses the main operations related to ad hoc networking in the data link and network layers as defined in [8]. Section 4, analyses how authentication can be achieved in a layered approach through well known cryptographic protocols that use symmetric and asymmetric techniques. The operation of well known challenge-response protocols, such as the ISO/IEC 9798-2, 4 and Needham-Schoeder, in a MANET environment is also discussed in detail. Section 5 presents a timing analysis of several challenge-response protocols in order to compare the execution time for one-hop multiple authentications. Section 6 concludes with remarks and comments on the open security issue in MANET.

2. Related Work

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 in ad hoc networks follow a hierarchical approach, with the most explored area being that of secure routing protocols. Authentication on the other side, has been explored less than routing protocols. Despite of that several authentication mechanisms for ad-hoc wireless networks have already been proposed. Zhou and Hass [24] 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 [13]. 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, which can be known only when more than m CAs collaborate. Therefore, this method can support the 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't provide authentication services anymore.

Kong and et. al. [9] proposed another authentication method based on threshold secret sharing [24]. After the bootstrapping phase, a new node can join the network at any time through self-initialization it can obtain its own secret share of CASK with the help of *m* local neighbour nodes. Even though this approach enhances scalability and availability, it still depends on an offline authority during the bootstrapping phase. In addition, Capkun and et. al [4] 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*. Anonymity schemes in mobile ad hoc networks were proposed in [23], [2], and [10]. ANODR [10] is based on an on-demand with identity free routing protocol using a symmetric cryptography with a 'trapdoor boomerang onion' (TBO) approach, similar to onion routing [18] used by Chaum in [3]. The trapdoor mechanism consists of sending cryptographically secured messages which may be opened only by the intended party. In [10] the low performance in highly mobile networks was pointed out.

In the MASK [23] protocol a proactive and a reactive approach are applied simultaneously. A priori anonymous links are established with all neighbouring nodes using a symmetric cryptography and trusted authority. The path discovery process is conducted in an on-demand manner and mutually authenticated nodes participate in the end-to-end communication. Already established paths may consist of several multipath channels however the source and destination nodes become unauthenticated. In SDAR [2] 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 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.

3. Layered Security Design

In [8], we proposed a layered security design that uses multiple lines of defence to protect MANET against attacks and network faults. The idea is based on the security challenges that arise in the main operations related to ad hoc networking that are found in *data link* and *network layers* of the Open Systems Interconnection Reference Model (OSI). In the case of MANET, for example, there are ***trusted*** and ***non-trusted*** environments [15, 16]. 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 the 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.

As mentioned above, the security challenges that arise in the main operations related to ad hoc networking are found in the *data link* and *network layers* of the OSI. The data link layer is the second level of the seven-level OSI model and it 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. However, the main link layer operations related to ad hoc networking are ***one hop connectivity*** and ***frame transmission*** [13, 24]. Data link layer protocols maintain connectivity between neighbouring nodes and ensure the correctness of frames transferred.

The network layer, which is the third level of the seven level OSI model, 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. The main network operations related to ad hoc networking are ***routing*** and ***data packet forwarding*** [14, 15, 16]. 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.

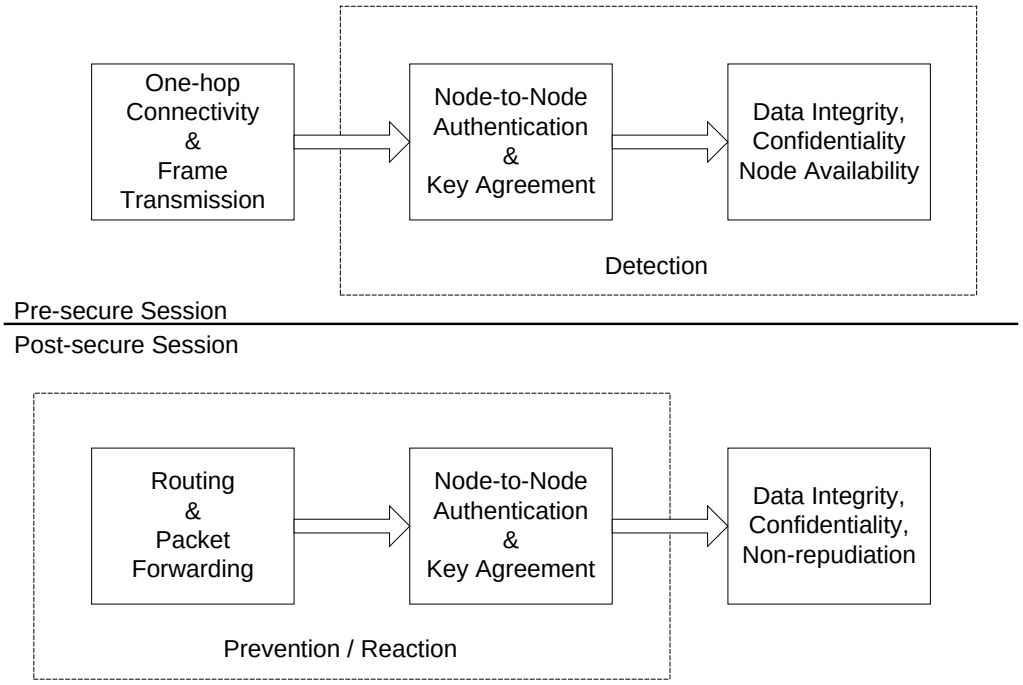

Figure 1 – Protocol Security Process [8]

As illustrated in Figure 1, these operations are comprised of link security and network security mechanisms that integrate a protocol to achieve protocol security process 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. In addition, the layered security mechanisms include prevention, detection and reaction operations to prevent intruders from entering the network. They 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 1. Once the attacker is detected, reaction operations reconfigure routing and packet forwarding operations. These adjustments can range from avoiding this particular node during the route selection process to expelling the node from the network. Independently from the detection, prevention and reaction, both secure sessions can enhance the authentication procedures for node identification in a MANET.

4. Authentication in a Layered Security Approach

As mentioned in section 3, link layer operations involve *one-hop connectivity* and *frame transmission*, whereas network layer operations include *routing* and *data packet forwarding*. These operations are comprised of the link and the network security mechanisms that can integrate a node authentication approach consisting of two phases. The operations of either the link or the 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 challenge-response protocols based on symmetric-key techniques. Likewise, in phase-two the authentication procedure seeks again the identities of the communicating nodes through challenge-response protocols based on public key techniques.

It is essential to mention that there are several authentication protocols available in the literature [9, 24, 13] that can be applied to MANETs. However, it is necessary to use low complexity protocols that will not create extra computational overhead in the wireless network. For example, the idea of cryptographic challenge-response protocols is that one entity (the claimant node in MANET context) “proves” its identity to the neighbouring node by demonstrating knowledge of a secret known to be associated with that node, without revealing the secret itself to the verifying node during the protocol. In some mechanisms, the secret is known to the verifying node, and is used to verify the response; in others, the secret need not actually be known to the verifying node.

In the first phase, the node identification procedure assumes that the secret is known to the verifying node, and this secret is used to verify the response with symmetric techniques. In the second phase of the authentication, the secret is not actually known to the verifying node. Asymmetric techniques can be applied before private information is exchanged between communicating nodes.

4.1. First Phase

The node authentication in the layered security 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 the 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 2 with the authenticated nodes A, B, and C.

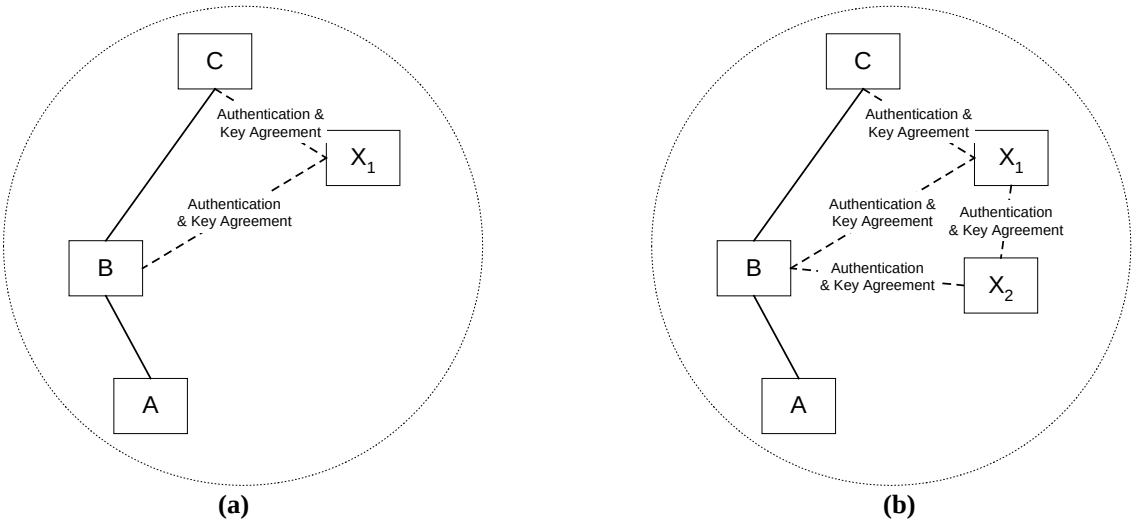

Figure 2 – Addition of New Nodes in a MANET

As illustrated in Figure 2a, 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 2b), 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 then X2 gets authenticated by nodes B and X1.

When two or more nodes are simultaneously connected to a MANET (e.g. Figure 2b) 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. 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. When symmetric techniques are applied the mutual authentication between B and X1 can be achieved based on ISO/IEC 9798-2 [13]:

$$\text{B} \leftarrow \text{X1}: \; r_1 \qquad \text{(M1)}$$
$$\text{B} \rightarrow \text{X1}: \; E_k(r_1, r_2, B) \qquad \text{(M2)}$$
$$\text{B} \leftarrow \text{X1}: \; E_k(r_2, r_1) \qquad \text{(M3)}$$

where E is a symmetric encryption algorithm and r_1 and 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 a message authentication code (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.

The revised three-pass challenge-response mechanism based on a MAC h_k that provides mutual authentication is ISO/IEC 9798-4 [13], also called *SKID3*, and has the following messages:

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

4.2. Second Phase

When routing information is ready to be transferred, the second phase of the node authentication takes place. Authentication carries on in the available nodes starting with one-hop at a time from the source to destination route one-hop at a time. 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. When asymmetric key techniques are applied, nodes own a key pair and the mutual authentication between X1 and C (Figure 2a) can be achieved by using the modified Needham-Schoeder public key protocol [13] in the following way:

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

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 the Menezes-Vanstone elliptic curve cryptosystem (ECC) [13] or by digital signatures. Digital signatures, however, involve much more computational overhead in signing, decrypting, verifying and encrypting operations. They are less resilient against denial of service 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.

5. Implementation Results

The authentication solution in a layered security approach 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 targets to compare the execution time of well known authentication protocols when applied in a layered security approach. The described protocols in sections 4.1 and 4.2 were simulated following the MANET infrastructure of Figure 2a. The implementation results are not affected by the network infrastructure. If the infrastructure changes and a new-entered node must be authenticated by more or less neighbouring nodes the authentication time will remain the same. This is due to the fact that the timing analysis presented in the next few paragraphs involves each node individually.

The 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 sections 4.1 and 4.2. The advanced encryption standard (AES) and message digest version 5 as MAC (MD5-MAC) were implemented as symmetric algorithms and RSA, and Menezes-Vanstone cryptosystems were used as asymmetric key algorithms. The key size was based on X9.30 standard specifications.

Cryptographic Algorithms	**Key Length**	**Encryption (500-bit)**	**Decryption (500-bit)**
AES	128-bit	20ms	23ms
MD5-MAC	128-bit	10ms	10ms
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 AES / MD5-MAC, 2048 bits and 224 bits are the "appropriate" key sizes for RSA, when the Chinese Remainder Theorem (CRT) is used, and for ECC, respectively [13, 19, 20]. Note that in the results of Table 1, 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 [13, 19].

Two-Phase Authentication	First Phase	Second Phase	Total	Remarks
2 x ISO/IEC 9798-4 (MD5-MAC) (Section 4.1)	(9798-4 MD5-MAC) 20.14 ± 2ms	(9798-4 MD5-MAC) 20.14 ± 2ms	40.18 ± 5ms	NR
2 x ISO/IEC 9798-2 (AES) (Section 4.1)	(9798-2-AES) 43.22 ± 2ms	(9798-2-AES) 43.22 ± 2ms	86.44 ± 5ms	NR
2 x Needham-Schroeder (NS-RSA) (Section 4.2)	(NS-RSA) 170.14 ± 2ms	(NS-RSA) 170.14 ± 3ms	340.28 ± 5ms	NR
2 x Needham-Schroeder (NS-ECC) (Section 4.2)	(NS-ECC) 145.17 ± 3ms	(NS-ECC) 145.17 ± 2ms	290.34 ± 5ms	NR
9798-4-MD5-MAC & NS-RSA	(9798-4-MD5-MAC) 20.14 ± 2ms	(NS-RSA) 170.14 ± 2ms	190.28 ± 5ms	R*
9798-2-AES & NS-RSA	(9798-2-AES) 43.22 ± 2ms	(NS-RSA) 170.14 ± 2ms	213.36 ± 5ms	R*
9798-4-MD5-MAC & NS-ECC	(9798-4-MD5-MAC) 20.14 ± 2ms	(NS-ECC) 145.17 ± 2ms	165.31 ± 5ms	R*
9798-2-AES & NS-ECC	(9798-2-AES) 43.22 ± 2ms	(NS-ECC) 145.17 ± 2ms	188.39 ± 5ms	R*

Table 2 – Timing Analysis of Authentication in a Layered Approach

Table 2 shows the time that 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 challenge-response protocol (9798-2- or 9798-4) similar to the ones presented in section 4.1. 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 for the symmetric algorithms (i.e. 40.18ms, 86.44ms, and slower for the asymmetric algorithms (i.e. 340.28ms and 290.34ms) than the execution time of combined cryptographic techniques (i.e. 190.28ms, 213.36ms, 165.31ms and 188.39ms). Considering that the authentication procedure that was successful once is most likely to succeed again without increasing security, a combination of symmetric and asymmetric challenge-response authentication techniques appears to be a recommended (R)* option when link and network layers operations are taking place. In such circumstances, the decision of whether to use challenge-response with symmetric or asymmetric key techniques can be determined by timing analysis and therefore node resources.

In our analysis, no consideration was taken when multiple hops were required to authenticate nodes in different network topologies of the second phase. In such circumstance, it is believed that the multiple authentication will not substantially be affected since only will only be authenticated the end-nodes. Moreover, no consideration was taken regarding the physical connection link between DSPs and the PC in the total timing and it is expected that a different implementation will yield different absolute results but the same comparative discussion. In addition, the 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 2 evaluates multiple authentication fences in MANET 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 for specific 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 which combination of challenge-response technique to apply in their applications.

6. Conclusions

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 integrated cryptographic mechanisms in the first and second phase that helped to design multiple lines of authentication defense and further protect ad hoc networks against malicious attacks.

Designing cryptographic mechanisms such as 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 authentication protocols were applied. This work can be extended to provide authentication for nodes that are several hops away and to compare routing protocols to different authentication mechanisms. Furthermore, it will be interesting to determine how multiple authentication protocols will behave in broadcasting and multicasting scenarios.

Eventually, 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

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

References

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

[2] A. Boukerche, "An Efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc network", Computer Communications, 2004.

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

[4] S. Capkun, J. P. Hubaux, L. Buttyan, "Mobility Helps Security in Ad Hoc Networks", In ACM MobiHoc, 2003

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

[6] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure on-demand Routing Protocol for Ad Hoc Networks", ACM WiSe, 2002.

[7] 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.

[8] N. Komninos, D. Vergados and C. Douligeris, "Layered Security Design for Mobile Ad-Hoc Networks", Computers & Security Journal, to be published by Elsevier, 2005.

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

[10] J. Kong, X. Hong, ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks, ACM MobiHoc 2003.

[11] J. Kong, X. Hong, M. Gerla., Mobility Changes Anonymity: Mobile Ad Hoc Networks Need Efficient Anonymous Routing, IEEE Computer Society, 2005.

[12] 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.

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

[14] 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.

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

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

[17] 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.

[18] M. Reed, P. Syverson, D. Goldschlag, "Proxies for anonymous routing", Proceedings of the 12th Annual Computer Security Applications Conference, IEEE, New York, 1995, pp. 95–104.

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

[20] 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.

[21] W. Stallings, *Cryptography and Network Security (2nd ed.): Principles and Practice*, Prentice-Hall, Inc., 1998.

[22] 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.

[23] Y. Zhang, W. Liu W. W. Lou, “Anonymous Communications in Mobile Ad Hoc Networks”, IEEE INFOCOM 2005
[24] L. Zhou and Z. J. Haas, “Securing Ad Hoc Networks”, IEEE Network Magazine, 1999.