Securing End-to-End Wireless Mesh Networks Ticket-Based Authentication.

Rushdi A. Hamamreh
Computer Engineering Department, Faculty of Engineering
Al-Quds University
Al-Quds, Palestine
rushdi@eng.alquds.edu

Anas M. Melhem
Computer Engineering Department, Faculty of Engineering
Al-Quds University
Al-Quds, Palestine
amelhem@eng.alquds.edu

Abstract—**Hybrid wireless mesh network (WMN) consists of two types of nodes: Mesh Routers which are relatively static and energy-rich devices, and Mesh Clients which are relatively dynamic and power constrained devices. In this paper we present a new model for WMN end-to-end security which divide authentication process into two phases: Mesh Access Point phase which based on asymmetric cryptography and Mesh Client phase which based on a server-side certificate such as EAP-TTLS and PEAP.**

Keywords-component; Hybrid mesh; network security; end-to-end authentication; server mobile; mobile router

I. INTRODUCTION

Wireless networks have grown rapidly for the past years due to recent developments, easy installation and low setup cost as compared to wired networks [1]. Wireless Mesh Network (WMN) is a promising new technology which is adopted as the wireless internetworking solution for the near future due to their self-healing, self-configuring and self-optimizing capabilities [16]. The most commercial form of WMN is called hybrid mesh networks [2], shown in Figure 1. Hybrid mesh networks consist of two types of wireless nodes: **Mesh_Routers/Access_Point (MAP)** and **Mesh_Clients (MC)**. Mesh Routers are relatively static and energy-rich devices that have multiple wireless network interfaces. On the other hand Mesh Clients are relatively mobile and power constrained devices such as notebook, Smartphone, and smart pad [17].

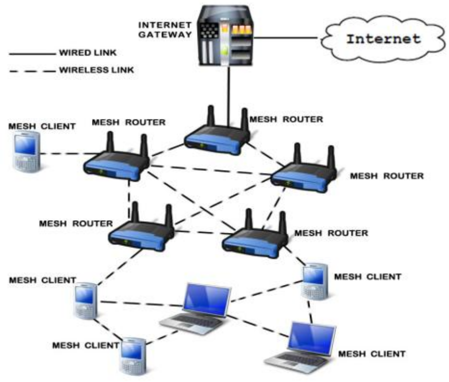


Figure 1. Hybrid wireless mesh network.

II. ROUTING IN WMN

The routing protocols used for WMNs can be categorized into two types: **Reactive** and **Proactive** [13][14][18]. In reactive routing protocols, the routes are established only when required, generally via flooding of Route Request packets in the network. While, in proactive routing protocols the routes are established before actual usage, through periodical exchanges of connectivity information. Both protocols have their individual advantages. Reactive protocols focus on minimizing control packet overhead such as Ad hoc On Demand Distance Vector (AODV) [3], Dynamic Source Routing (DSR) [4],Temporally-Ordered Routing Algorithm (TORA) [5] etc. while the proactive protocols attempt to minimize the route establishment delays such as OLSR [4], DSDV [5].

However, since these routing protocols have been designed for relatively homogenous MANETs, they will not provide optimum security for hybrid WMNs. An important security goal of a wireless mesh network is to protect the end-to-end communication between the device and its home network, in particular to protect the application content from being eavesdropped or modified during its transmission.

III. RELATED WORK

A. KAMAN

Kerberos Assisted Authentication in Mobile Ad-hoc Networks [6] uses multiple Kerberos servers for distributed authentication and load distribution. In Kaman only the users know the secret key or passwords and the servers know a cryptographic hash of these passwords. All Kaman servers share a secret key with each other server. In Kaman all servers periodically, or on-demand, replicate their databases with each other. Kaman uses an election based server selection mechanism.

B. TAODV

Ticket Based Ad-hoc On Demand Distance Vector [7] is a ticket-based security protocol foe WMNs that is based upon the AODV protocol, which is a cross layer protocol which works at network layer but also provides security for data exchange

DOI: 10.5176_2010-2283_1.2.64

and avoids transfer of ARP messages for finding MAC addresses of source and destination.

C. Secure Extension to the OLSR protocol

Use The Secure Extension to the OLSR protocol [8] has only provides integrity and not confidentiality by signing each OLSR control packet with digital signature for authenticating the message. The digital signature is based on symmetric keys [19]. All OLSR control traffic is signed for every hop. This doesn't provide end-to-end signatures.

IV. Our proposed model

Our proposed model aims to achieve an end-to-end authentication in WMN. In order to achieve such goal we have divided the authentication way into two phases: the **MAP phase** in which a new MAP conducts the network, and the **MC phase** is when a new MC conducts the network.

At the **MAP phase**, we consider that MAP is energy rich devices so we can use asymmetric cryptographic [19] in contrary to MC devices in the second part of the authentication, server-side certificate such as EAP-TTLS and PEAP.

A. MAP Phase

During the setup phase when a Router/MAP connects to the WMN it has to follow the following steps: (1) MAP sends its details including the type (1 for MAP / 0 for MC) and MAC address to an Authentication Server (AS). (2) AS will send key generation mechanism back to the MAP after checking MAC address in a stored list. (3) MAP will generate its public and secret keys, and then sends its public key ($PK_{\mathbf{MAP}}$) to the AS. Then AS also generates a secret key ($K_{\mathbf{MAP}}$)for new MAP and itself on the basis of public key of MAP and its secret key by using Fixed Diffie-Hellman key exchange protocol. (4) AS generates a ticket for new MAP with required info (MAP ID, IP, issue time, expiration time etc.) $\mathbf{ticket}_{\mathbf{MAP}}$ and sign it with its private key. Then, after signing, AS will encrypt that ticket with the shared secret key and then forward this encrypted ticket to new MAP. After receiving encrypted ticket, new MAP will first generate a shared secret key on the basis of AS's public key and its secret key (as AS generated) and then will decrypt the ticket. For future communication (route discovery request/reply) MAP will use this ticket.

(1) MAP $\rightarrow$ AS: Type|| MAC|| $N_{\mathbf{once}}$
(2) AS $\rightarrow$ MAP: key generation mechanism|| $N_{\mathbf{once}}$
(3) MAP $\rightarrow$ AS: PK_{MAP} || N_{once}
(4) AS $\rightarrow$ MAP: $\{\boldsymbol{ticket}_{\mathbf{MAP\text{-}AS}}\}K_{MAP}$ || N_{once}

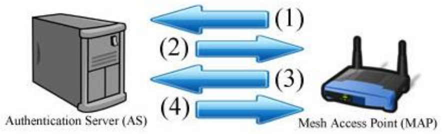


Figure 2. MAP phase

B. MC Phase

When a new MC connects to the WMN the AS ask for credentials such as user name or ID number and password (via PAP, CHAP, or MD5 challenges) [9]. In this phase server-side certificate such as EAP-TTLS and PEAP can be used. After successful authentication, the mobile node will receive a secret key that shares with the authentication server (AS).

C. MAP –to- MAP Authentication

As we mentioned before MAP depends on proactive protocols such as OLSR in order to build routing table through periodical exchanges of connectivity information, when an MAP discover a new neighboring MAP, a secure route must be established. In order to have a secure route between MAPs, the first MAP sends it identifier and the identifier of destination second MAP to the AS, which in turn looks up both MAPs in its database in order to verify the validity of both clients.

MAP1 $\rightarrow$ AS: $\{ID_{\mathbf{MAP1}}, ID_{\mathbf{MAP2}}\}\ K_{\mathbf{MAP1}}||\boldsymbol{ticket}_{\mathbf{MAP1\text{-}AS}}\ ||N_{\mathbf{once}}$

AS sends $\boldsymbol{ticket}_{\mathbf{MAP2}}$ $\{K_{\mathbf{MAP1\text{-}AS}}, K_{\mathbf{MAP12}}, ID_{\mathbf{MAP1}}, T\}$ in which $K_{\mathbf{MAP12}}$ is the secret shared key between two MAPs and T is the lifetime of that key, this ticket will be sent to MAP1 along with the Authenticator which provides MAP1 with the shared key and proof that this is the right shared key to use with MAP2 at this time.

AS $\rightarrow$ MAP1: $\boldsymbol{ticket}_{\mathbf{MAP2}}$ || $ID_{\mathbf{MAP1}}$ || $\{K_{\mathbf{MAP12}}$, lifetime, $N_{\mathbf{once}}$, $ID_{\mathbf{MAP2}}\}K_{\mathbf{MAP1}}$

MAP1 decrypts Authenticator in order to validate its information and then creates a new message with a fresh **timestamp**, this message contains both identifiers in addition to $\boldsymbol{ticket}_{\mathbf{MAP2}}$ and encrypted values that express MAP2 identifier with the fresh timestamp. And then send this message to MAP2.

MAP1 $\rightarrow$ MAP2: $\boldsymbol{ticket}_{\mathbf{MAP2}}$ || $ID_{\mathbf{MAP1}}$, $ID_{\mathbf{MAP2}}$ ||**timestamp**

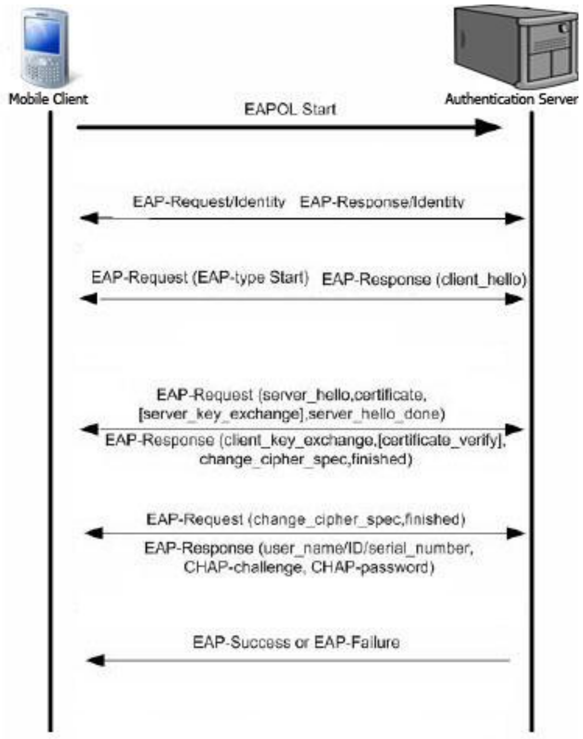

Mobile Client
Authentication Server
EAPOL Start
EAP-Request/Identity
EAP-Response/Identity
EAP-Request (EAP-type Start)
EAP-Response (client_hello)
EAP-Request (server_hello,certificate,
[server_key_exchange],server_hello_done)
EAP-Response (client_key_exchange,[certificate_verify],
change_cipher_spec,finished)
EAP-Request (change_cipher_spec,finished)
EAP-Response (user_name/ID/serial_number,
CHAP-challenge, CHAP-password)
EAP-Success or EAP-Failure

Figure 3. MC phase

After receiving this message MAP2 decrypts ***ticket***$_{\mathbf{MAP2}}$ with $K_{\mathbf{MAP2}}$ to obtain $K_{\mathbf{MAP12}}$ which in turn used to get the encrypted values, then MAP2 validates timestamp and local time comparing the life time sent from MAP1. In case the verification succeeded, MAP2 send a new encrypted message with $K_{\mathbf{MAP12}}$, this message contains the timestamp sent before by MAP1 and a new key instead of $K_{\mathbf{MAP12}}$ called **subkey** used as a shared key between two clients in their communications. When the message received MAP1 decrypts it and verifies timestamp. If the verification succeeded, MAP1 knows that MAP2 received the previous message

MAP2 → MAP1: {**timestamp**, **subkey**}$K_{\mathbf{MAP12}}$

a) MAP1 → AS: {$ID_{\mathbf{MAP1}}$, $ID_{\mathbf{MAP2}}$ } $K_{\mathbf{MAP1}}$||***ticket***$_{\mathbf{MAP1\text{-}AS}}$ ||$N_{\mathbf{once}}$
b) AS → MAP1: ***ticket***$_{\mathbf{MAP2}}$ || $ID_{\mathbf{MAP1}}$ || {$K_{\mathbf{MAP12}}$, lifetime, $N_{\mathbf{once}}$, $ID_{\mathbf{MAP2}}$}$K_{\mathbf{MAP1}}$
c) MAP1 → MAP2: ***ticket***$_{\mathbf{MAP2}}$ || $ID_{\mathbf{MAP1}}$, $ID_{\mathbf{MAP2}}$ ||**timestamp**
d) MAP2 → MAP1: {**timestamp**, **subkey**}$K_{\mathbf{MAP12}}$

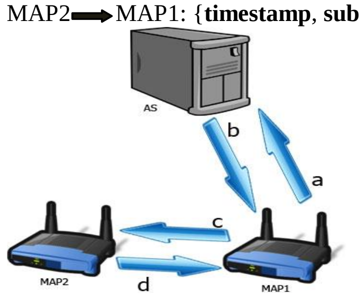


Figure 4. MAP-to-MAP authentication.

D. *Client–to-Client Authentication*

For Client–to-Client Authentication, our proposed model uses EAP authentication with a modified version of a scheme known as a four-pass Kerberos protocol [10][15].

When a new MC connects to the WMN it approves itself to the Authentication Server (AS) in order to get a secret key shared with the AS in addition to a unique identifier ID.

Whenever an MC wants to establish a secure connection with another MC it approaches the AS and follows the protocol as following steps:

In the first Client MC1, sends its identifier and the identifier of destination client MC2 to the AS, which in turn looks up both MCs in its database in order to verify the validity of both clients.

MC1 → AS: $ID_{\mathbf{MC1}}$ || $ID_{\mathbf{MC2}}$ || $N_{\mathbf{once}}$

AS sends ticketMC2 which contains KMC12 and the lifetime of that key, this ticket will be sent to MC1 along with the Authenticator which provides MC1 with the shared key and proof that this is the right shared key to use with MC2 at this time.

AS → MC1: ***ticket***$_{\mathbf{MC2}}$ || $ID_{\mathbf{MC1}}$ || {$K_{\mathbf{MC12}}$, lifetime, $N_{\mathbf{once}}$, $ID_{\mathbf{MC2}}$}$K_{\mathbf{MC1}}$

MC1 decrypts Authenticator in order to validate its information and then creates a new message with a fresh **timestamp**, this message contains both identifiers in addition to ticketMC2 and encrypted values that express MC2 identifier with the fresh timestamp. And then send this message to MC2.

MC1 → MC2: ***ticket***$_{\mathbf{MC2}}$ || Authenticator

After receiving this message MC2 decrypts ***ticket***$_{\mathbf{MC2}}$ with $K_{\mathbf{MC2}}$ to obtain $K_{\mathbf{MC12}}$ which in turn used to get the encrypted values, then MC2 validates timestamp and local time comparing the life time sent from MC1.

In case the verification succeeded, MC2 send a new encrypted message with $K_{\mathbf{MC12}}$, this message contains the **timestamp** sent before by MC1 and a new key instead of $K_{\mathbf{MC12}}$ called **subkey** used as a shared key between two clients in their communications. When the message received MC1 decrypts it and verifies timestamp. If the verification succeeded, MC1 knows that MC2 received the previous message in proper form and decrypt the shared key correctly.

MC2 → MC1: {**timestamp**, **subkey**}$K_{\mathbf{MC12}}$

a) MC1 → AS: $ID_{\mathbf{MC1}}$ || $ID_{\mathbf{MC2}}$ || $N_{\mathbf{once}}$
b) AS → MC1: ***ticket***$_{\mathbf{MC2}}$ || $ID_{\mathbf{MC1}}$ || {$K_{\mathbf{MC12}}$, lifetime, $N_{\mathbf{once}}$, $ID_{\mathbf{MC2}}$}$K_{\mathbf{MC1}}$
c) MC1 → MC2: ***ticket***$_{\mathbf{MC2}}$ || Authenticator
d) MC2 → MC1: {**timestamp**, **subkey**}$K_{\mathbf{MC12}}$

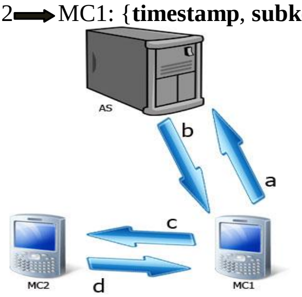


Figure 5. Client-to-Client authentication.

We have to notice that all routes between MAP's are all secured through MAP-to-MAP authentication steps, so that when MC1 send a message to MC2 this message will be encrypted by the shared secret key **subkey** between every single MAP pair, this will provide both node–to–node and end-to-end security.

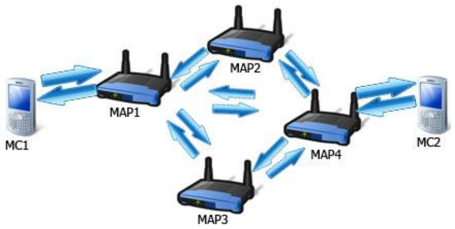


Figure 6. end-to-end security.

E. *Server Election*

Due to wireless network nature, and because our proposed model depending on server side authentication; we used an election based mechansim in order to overcom the nonavilability of one or more server. In order to intiate election process [6] has define the following three conditions (1) when the number of servers increases or decreases. (2) when the server lifetime expiers (3)when a server fails the optional availability check mechanism.

Servers periodically use secure BEACON and ECHO packets to discover the availability of other servers [6].in the case the server is in non-availabilty situation, the election procedure intiates. Server elecation process based on factors such as connectivity, processing ability, RAM capacity, and network topology such as wireless transmission range, geographical position, or the lifetime expiration of a server. these factors reflect *Server Ability Degree* (SAD) [11] which takes into account static factors such as RAM capacity, and dynamic factors such as network topology.

We are defined the following factors in order to calcutate SAD, (1) CPU ability.(2)RAM capacity. (3)hop count; AS is prefearable to has central position to all APs in the network, this position is given by the mean distance between this server and all APs in the network. (4)Server ticket's lifetime. The weights assigned to each of these criteria are $w_1=3$ for CPU ability criterian, $w_2=1$ for RAM capacity criterian, $w_3=2$ for hop count criterian, and $w_4=4$ for ticket's lifetime criterian.

The equation for calculating SAD is:

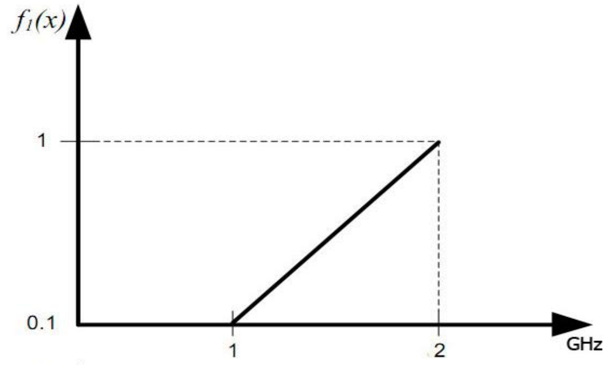
$$\text{SAD}(AS_j) = w_1*c_1 + w_2*c_2 + w_3*c_3+\ldots+w_nc_n \qquad (1)$$

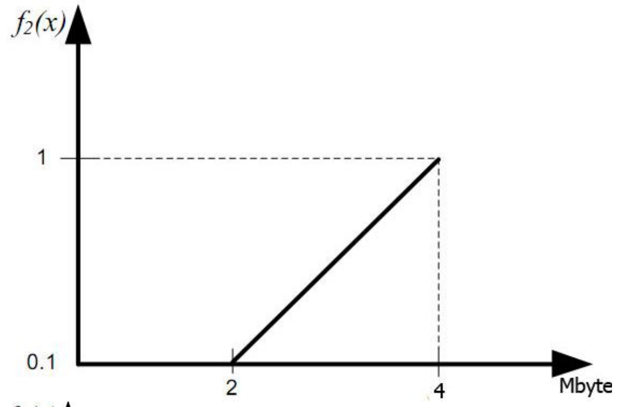
After calculating SAD for every server, the highset value server will be upgraded to be the Authentication server.

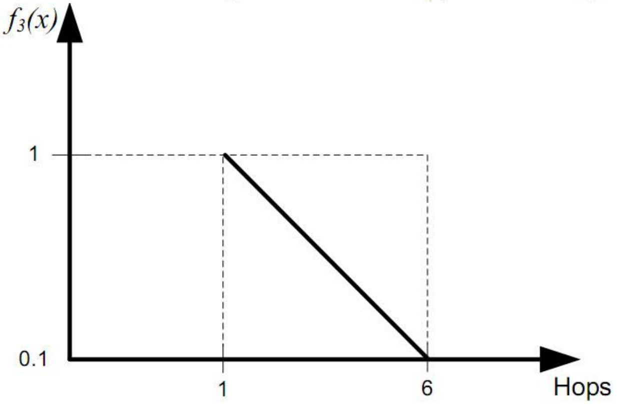
F. Database Riplecation

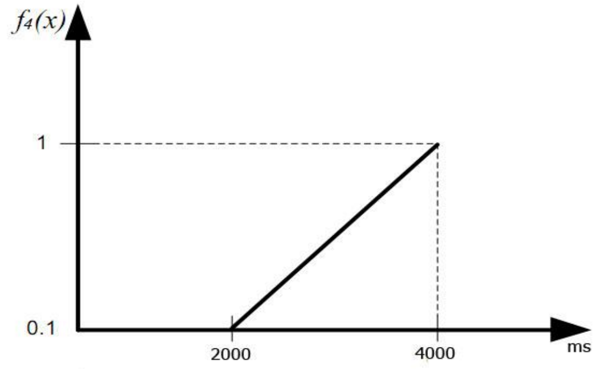
Regular database replication maintains authentication mechanism and server election procedure. Periodically replications protect server from being captured or compromised. Also it does maintain database updated with all added, modified, and revoked accounts since last replicate. Since WMN contains MCs that work as routers and by noticing that these devices are energy-poor devices, we recommend using a distributed replication scheme called *Distributed Adaptive Service Replication* (*DAR*) [12]. DAR aims to improve service availability with reasonable energy consumption across the network. In order to dynamically place service replicas in appropriate nodes, DAR divides the whole network into disjoint zones with diameters at most 2 hops, selects a node with minimum moving speed in each zone as a zone head, and constructs a virtual backbone network connecting all zone heads. Each replication has a sequence replication number in order to maintain global consistency of the database as described in KAMAN Replication Repository[6]

Server1 $\longrightarrow$ Server2: {Seq# || time || Database} $K_{\mathbf{AS12}}$
Seq#: Replication Sequence Number.
time: the time of executing this replica.
$K_{\mathbf{AS12}}$: shared secrete key between two Database.









V. CONCLUSION

In this paper we present a new model for securing end-to-end wireless mesh network with ticked based-authentication. This model divides the authentication process into two phases: MAP phase and MC phase. In the first phase Our proposed model authenticate MAP using asymmetric cryptography [19] depending on MAP's MAC address, this phase ensure securing all network path by establishing ticket based route between every single MAP pair. While in the second phase the authentication process done by proving the new MC itself to the AS using credentials, these credentials will be a username or ID and a password. This is required since the MC doesn't have any certificate yet. Then AS use a server-side certificate such as EAP-TTLS and PEAP in order to authenticate the new MC. This is a secure method that saves MC battery since it is constrained power devices. Our proposed model uses a modified version of a scheme known as a four-pass Kerberos protocol in MAP-to-MAP authentication and MC-to-MC authentication. By doing this we ensure providing secure node-to-node routes for all routes in the network in addition to the end-to-end security message that cannot be decrypted without the secret key at the receiver MC. With reasonable consuming to the battery at MC side.

VI. References

[1] A. A. Pirzada, anad M. Portmann, "High Performance AODV Routing Protocol for Hybrid Wireless Mesh Networks", Proceedings of the 2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking&Services (MobiQuitous), p.1-5, August 06-10, 2007

[2] I. F. Akylidiz, X. Wang and W. Wang, "Wireless Mesh Network: A Survey' in Computer Network ans ISDN Systems", Volume 47, Issue 4, March 2005

[3] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc On demand Distance Vector (AODV) Routing", IETF RFC 3561, July 2003.

[4] S. Hamma, E. Cizeron, H. Issaka, and J.-P. Guèdon, "Performance Evaluation of Reactive and Proactive Routing Protocol in IEEE 802.11 Ad hoc Network" in the proceedings of SPIE, Next-Generation Communication and Sensor Networks 2006, Volume 6387, October 2006.

[5] J. Broch, D. A. Maltz, D. B. Johnson, Y –C. Hu, and J. Jetcheva, "A Performance Comprison of Multi-Hop Wireless Ad Hoc Network Routing Protocols" in the proceedings of the Fourth Annual International Conference on Mobile Computing and Networking (MobiCom`98), Oct, 1998, pp: 85-97.

[6] A.A. Pirzada and C. McDonald, "Kerberos Assisted Authentication in Mobile Ad Hoc Networks," Proc. 27th Australasian Computer Science Conf. (ACSC), vol. 26, pp. 41-46, 2004.

[7] Qazi, S.; Yi Mu; Susilo, W.; , "Securing wireless mesh networks with ticket-based authentication," Signal Processing and Communication Systems, 2008. ICSPCS 2008. 2nd International Conference on , vol., no., pp.1-10, 15-17 Dec. 2008.

[8] A. Hafslund, A. Tønnesen, J. Andersson, R. Rotvik, Ø Kure "Secure Extension to OLSR" Currently under review for the OLSR Interop and Workshop, 2004.

[9] Bhakti, M.A.C.; Abdullah, A.; Jung, L.T.; , "EAP-based Authentication with EAP Method Selection Mechanism: Simulation Design," Research and Development, 2007. SCOReD 2007. 5th Student Conference on , vol., no., pp.1-4, 12-11 Dec. 2007

[10] D. W. Carman, P. S. Kruus and B. J.Matt, "Constraints and Approaches for DistributedSensor Network Security," dated September 1, 2000.NAI Labs Technical Report.

[11] Y.M.; Senouci, S.-M.; Agoulmine, N.; , "P-SEAN: A Framework for Policy-based Server Election in Ad hoc Networks," Network Operations and Management Symposium, 2006. NOMS 2006. 10th IEEE/IFIP , vol., no., pp.271-281, 3-7 April 2006.

[12] Ahmed, A.; Yasumoto, K.; Shibata, N.; Kitani, T.; Ito, M.; , "DAR: Distributed Adaptive Service Replication for MANETs," Wireless and Mobile Computing, Networking and Communications, 2009. WIMOB 2009. IEEE International Conference on , vol., no., pp.91-97, 12-14 Oct. 2009

[13] M. S. Azad, F. Anwar, M. A. Rahman, A. H. Abdalla, A. U. Priantoro, O. Mahmoud, "Performance Comparison of Proactive and Reactive Multicast Routing Protocols over Wireless Mesh Networks", Vol. 9 No. 6 pp. 55-62, June 2006.

[14] A. jmal, M.M.; Mahmood, K.; Madani, S.A.; , "Efficient routing in wireless mesh network by enhanced AODV," Information and Emerging Technologies (ICIET), 2010 International Conference on , vol., no., pp.1-7, 14-16 June 2010

[15] P. Langendoerfer, and K. Piotrowski, More Privacy in Context-aware Platforms: User Controlled Access Right Delegation using Kerberos, Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers, Tenerife, Spain, December 16-18, 2005

[16] Stephan Miry, Asad Amir Pirzada and Marius Portmannz "HOVER: Hybrid On-demand Distance Vector Routing for Wireless Mesh Networks" Proceedings of the thirty-first Australasian conference on Computer science - Volume 74, Wollongong, Australia, 2008.

[17] Ping Yi; Tianhao Tong; Ning Liu; Yue Wu; Jianqing Ma; , "Security in Wireless Mesh Networks: Challenges and Solutions," Information Technology: New Generations, 2009. ITNG '09. Sixth International Conference on , vol., no., pp.423-428, 27-29 April 2009

[18] Mbarushimana, C.; Shahrabi, A.; , "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad Hoc Networks," Advanced Information Networking and Applications Workshops, 2007, AINAW '07. 21st International Conference on , vol.2, no., pp.679-684, 21-23 May 2007

[19] R. A. Hamamreh, and M. Farajallah, "Design of a Robust Cryptosystem Algorithm for Non-Invertible Matrices Based on Hill Cipher" IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.5, May 2009.

Rushdi A. Hamamreh received his M.S. degree in computer engineering from the Saint Petersburg State Technical University in 1998 and his Ph.D. in Distributed Information Systems and Networks Security from the Saint Petersburg State Technical University in 2002. He is currently an assistant professor of computer engineering at the Al-Quds University, Jerusalem and the head of computer engineering department. His research and teaching interests include design and development multiagent systems, Networks Security and Routing Protocols.

Anas Melhem received his B.S. degree in Electrical Engineering from Palestine Technical University, in 2005. Currently he is pursuing his M.S. degree in Computer and Electronic Engineering as well as working as a technical engineer in Palestine. His research interests include wireless network security.