SWMPT: Securing Wireless Mesh Networks Protocol Based on Ticket Authentication

Rushdi A Hamamreh

Al-Quds University

SWMPT: Securing Wireless Mesh Networks Protocol Based on Ticket Authentication

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

Anas M. Melhem
Computer Engineering Department, Faculty of Engineering
Palestine Technical University
Tulkarm, Palestine
amelhem@ptuk.edu.ps

ABSTRACT

Wireless mesh network (WMN) consists of two parts: mesh access points which are relatively static and energy-rich devices, and mesh clients which are relatively dynamic and power constrained. In this paper, we present a new model for WMN end-to-end security which divides authentication process into two phases: Mesh Access Point which is based on asymmetric cryptography and Mesh Client which is based on a server-side certificate such as EAP-TTLS.

General Terms

Algorithms, Performance, Design, Reliability, Experimentation, Security, Standardization, Theory.

Keywords

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

1. INTRODUCTION

Wireless mesh networks have appeared as a promising design model for next generation wireless networks which have grown rapidly due to recent developments such as easy installation and low setup cost when compared to wired networks [1]. WMN is a promising new technology which has been adopted as the wireless internetworking solution for the near future due to their self-healing, self-configuring and self-optimizing capabilities [2]. The most commercial form of WMN is called hybrid mesh networks [3], shown in Figure 1. Hybrid mesh networks contain mesh access points (MAP) and mesh clients (MC). MAPs 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 [4].

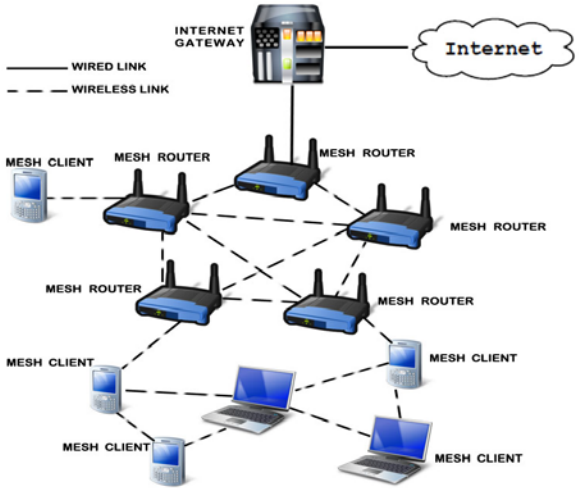

Figure 1. Hybrid Wireless Mesh Network.

The routing protocols used for WMNs can be classified into two types: Reactive Routing Protocols in which routes are established only when required and generally via flooding of Route Request packets in the network, and Proactive Routing Protocols in which routes are established before actual usage through periodical exchanges of connectivity information [5] [6] [7]. Both protocols have their individual advantages. Reactive protocols focus on minimizing control packet overhead such as Ad hoc On Demand Distance Vector (AODV) [8], Dynamic Source Routing (DSR) [9],Temporally-Ordered Routing Algorithm (TORA) [10] etc. while the proactive protocols attempt to minimize the route establishment delays such as OLSR [9], DSDV [10].

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 general, and to protect the application content from being eavesdropped or modified during its transmission in particular.

Copyright ©2011 IJJ: The Research Bulletin of Jordan ACM - ISWSA; ISSN: 2078-7952 (print); 2078-7960 (online)

2. RELATED WORK

2.1 KAMAN

Please Kerberos Assisted Authentication in Mobile Ad-hoc Networks [11] 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.

2.2 TAODV

Ticket Based Ad-hoc On Demand Distance Vector [12] 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 and avoids transfer of ARP messages for finding MAC addresses of source and destination.

2.3 Secure Extension to the OLSR protocol

Use The Secure Extension to the OLSR protocol [13] has only provided 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 [14]. All OLSR control traffic is signed for every hop. This doesn't provide end-to-end signatures.

3. Our Proposed Model

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

At the MAP phase, we aim to use asymmetric cryptographic sine MAP is an energy rich device [14] on the other hand, MC devices in the second part of the authentication use server-side certificate such as EAP-TTLS and PEAP.

3.1 MAP Phase

When a MAP is connected to a WMN during setup stage, it has to do 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 generates a shared secret key ($K_{\mathbf{MAP}}$) for new MAP and AS 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) 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 → AS: Type|| MAC|| $N_{\mathbf{once}}$
(2) AS → MAP: key generation mechanism|| $N_{\mathbf{once}}$
(3) MAP → AS: PK_{MAP} || N_{once}
(4) AS → MAP: {$\boldsymbol{ticket}_{\mathbf{MAP\text{-}AS}}$}$K_{MAP}$ || N_{once}

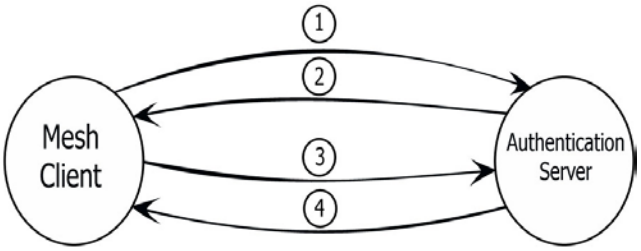

Figure 2. MAP Phase

3.2 MC Phase

When a new MC is connected to the WMN, it has to provide credentials to the AS. These credentials can be user-name/ID-number and password (via PAP, CHAP, or MD5 challenges) [15]. In this phase server-side certificate such as EAP-TTLS can be used. After successful authentication, the mobile node will receive a secret key that shares with the authentication server (AS).

3.3 MAP –to- MAP Authentication

As it has been mentioned, MAP depends on proactive protocols such as OLSR in order to build routing table through periodical exchanges of connectivity information, when a MAP discovers a new neighboring MAP, a secure route must be established. In order to do so, the first MAP sends both its identifier and the identifier of destination MAP to the AS, which in turn looks up both identifiers in its database in order to verify the validity of both clients.

MAP1 → AS: {$ID_{\mathbf{MAP1}}$, $ID_{\mathbf{MAP2}}$} $K_{\mathbf{MAP1}}$|| $N_{\mathbf{once}}$

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

AS → MAP1: $\boldsymbol{ticket}_{\mathbf{MAP2}}$ || $ID_{\mathbf{MAP1}}$ || {$K_{\mathbf{MAP12}}$, times, $N_{\mathbf{once}}$, $ID_{\mathbf{MAP2}}$} KMAP1

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

After receiving this message, MAP2 decrypts $\boldsymbol{ticket}_{\mathbf{MAP2}}$ with $K_{\mathbf{MAP2}}$ to obtain $K_{\mathbf{MAP12}}$ which in turn is used to get the encrypted values, and then MAP2 validates timestamp by comparing it to local time. In case the verification succeeds, MAP2 sends 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 has received the previous message

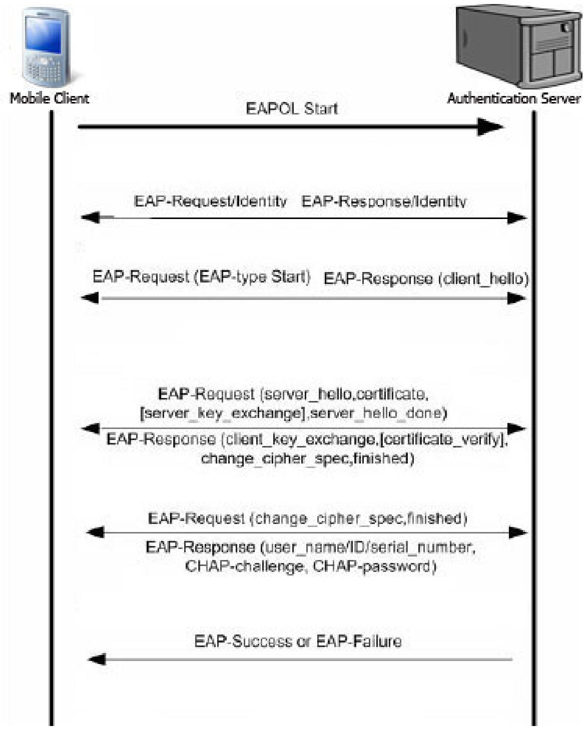
Mobile Client
Authentication Server
EAPOL Start
EAP-Request/Identity
EAP-Response/Identity
EAP-Request (EAP-type Start)
EAP-Response (client_hello)
EAP-Request (server_hello,certificate,
[server_key_exchange],server_hello_done)
EAP-Response (client_key_exchange,[certificate_verify],
change_cipher_spec,finished)
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

a) MAP1 → AS: {ID$_{\mathbf{MAP1}}$, ID$_{\mathbf{MAP2}}$ } K$_{\mathbf{MAP1}}$||***ticket***$_{\mathbf{MAP1}}$||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$_{\mathbf{MAP12}}$

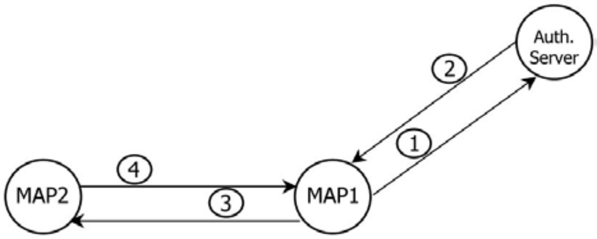

Figure 4. MAP-to-MAP Authentication

3.4 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 [16][17].

When a new MC is connected 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 does the protocol as following steps:

The first Client MC1, sends both its identifier and the identifier of destination client MC2 to the AS which in turn searches for both MCs identifiers 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 ***ticket***$_{\mathbf{MC2}}$ which contains K$_{\mathbf{MC12}}$ and the lifetime of that key, this ticket is sent to MC1 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. It then creates a new message with a fresh timestamp. This message contains both identifiers in addition to ***ticket***$_{\mathbf{MC2}}$ 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 is used to get the encrypted values. Then MC2 validates timestamp and local time comparing the life time sent from MC1.In case the verification succeeds, MC2 sends a new encrypted message with K$_{\mathbf{MC12}}$. This message contains both the **timestamp** sent before by MC1 and a new key called **subkey** instead of K$_{\mathbf{MC12}}$ which is used as a shared key between the two clients in their communications. When the message is received, MC1 decrypts it and verifies timestamp. If the verification succeeds, then MC1 knows that MC2 has 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$_{\mathbf{MC12}}$

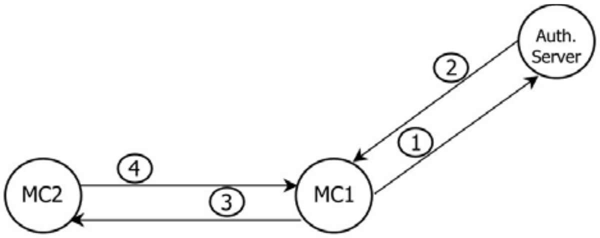

Figure 5. Client-to-Client authentication

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

4. Simulation

We have used ns-2 simulator to simulate our proposed model (THWMP) protocol and to compare it with existing protocols HWMP and SHWMP[19]. We have simulated 50 static mesh nodes in a 1500 x1500 m2 area. We use 5 to 10 distinct source-destination pairs that are selected randomly. Traffic source are CBR (constant bit-rate). Each source sends data packets of 512 bytes at the rate of four packets per second during the simulation period of 900 seconds.

In order to compare HWMP with SHWMP, both protocols were run under identical traffic scenario. Both on-demand and proactive mode were simulated. We consider Packet delivery ratio and End-to-end delay as performance metrics.

As shown in Figure 7, the packet delivery ratio is better in SHWMP for both on demand and proactive mode than that of HWMP. We assume that 10% misbehaving nodes are present in the network. Since the misbehaving nodes participate in the route discovery process, in HWMP sometimes packets are intentionally dropped by the misbehaving nodes. But, in the proposed protocol, misbehaving nodes cannot participate in the route discovery process and thus always achieve a higher packet delivery ratio.

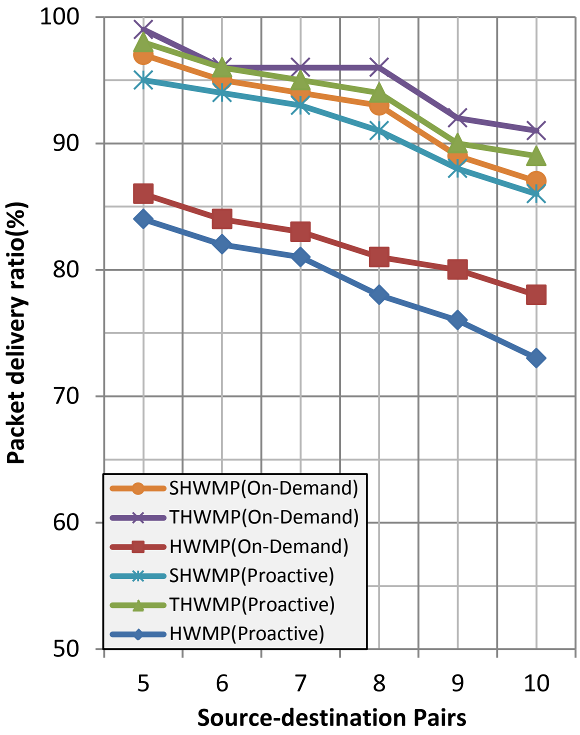

Figure 7. Packet delivery ratio

Figure 8 depicts that the average end-to-end delay of data packets for both protocols are almost equal. We run the simulation using 5 and 10 source-destination pairs, and as the traffic load increases, end-to-end delay also increases. It is also evident that the effect of route acquisition delay on average end-to-end delay is not significant.

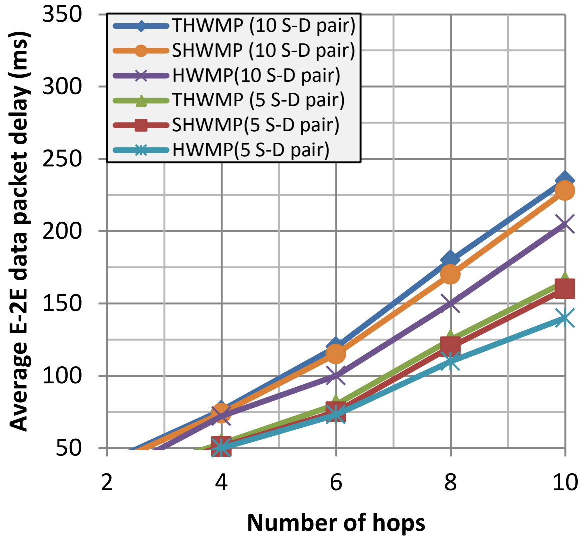

Figure 8. Control overhead

5. Conclusion

In this paper, we presented 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, our proposed model authenticates MAP using asymmetric cryptography [19] depending on MAP's MAC address. This phase ensures the securing of all network paths by establishing ticket based between every single MAP pair. Whereas in the second phase, the authentication process is done by proving the new MC to the AS using preconfigured credentials. This is required because the MC doesn't have any certificate yet. After that, the AS uses a server-side certificate to authenticate the MC. This is a secure method that saves MC battery. Our proposed model uses a modified version of a scheme known as four-pass Kerberos protocol in MAP-to-MAP authentication and MC-to-MC authentication. By doing this, we ensure the providing of a 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. .

6. REFERENCES

[1] A. A. Pirzada, anad M. Portmann, 2007. 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] Stephan Miry, Asad Amir Pirzada and Marius Portmannz, 2008. 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.

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

[4] 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.

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

[6] A. jmal, M.M.; Mahmood, K.; Madani, S.A.; , 2010. 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

[7] Mbarushimana, C.; Shahrabi, A.; , 2007. 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

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

[9] S. Hamma, E. Cizeron, H. Issaka, and J.-P. Guèdon, 2006 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.

[10] J. Broch, D. A. Maltz, D. B. Johnson, Y –C. Hu, and J. Jetcheva, 1998. "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.

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

[12] Qazi, S.; Yi Mu; Susilo, W.; , 2008. 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.

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

[14] R. A. Hamamreh, and M. Farajallah, 2009. 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.

[15] Bhakti, M.A.C.; Abdullah, A.; Jung, L.T.; ,2007. 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

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

[17] P. Langendoerfer, and K. Piotrowski, 2005. 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.

[18] Y.M.; Senouci, S.-M.; Agoulmine, N.; , 2006, 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.

[19] Ahmed, A.; Yasumoto, K.; Shibata, N.; Kitani, T.; Ito, M.; ,2009. 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.

[20] Md. Shariful Islam, Md. Abdul Hamid and Choong Seon Hong, 2009. SHWMP: A Secure Hybrid Wireless Mesh Protocol for IEEE 802.11s *Wireless Mesh Networks, Lecture Notes in Computer Science, 2009*, Volume 5730/2009.

[21] *William Stallings; Cryptography and Network Security: Principles & Practice (5th ed.) Pearson/Prentice* Hall, 2010.