Dynamic Key Refreshment for Smart Grid Mesh Network Security

Hamid Gharavi and Bin Hu
Advanced Network Technologies
National Institute of Standards and Technology
Gaithersburg, USA
Emails: [Gharavi, bhu]@nist.gov

Abstract— This paper presents a dynamically updating key distribution strategy to enhance mesh network security against cyber attacks. The scheme has been applied to two security protocols known as Simultaneous Authentication of Equals (SAE) and Efficient Mesh Security Association (EMSA). The former is based on a password-authenticated key exchange and the latter relies on mesh key holders through the use of a mesh key hierarchy. Since both SAE and EMSA protocols utilize 4-way handshaking, the resiliency of the network in a situation where an intruder carries a denial of service attack has been evaluated. This includes the effect of the proposed dynamic key refreshment strategy on the network delay and overhead performance.

Keywords-Smart Grid, wireless mesh networks, security protocols, EMSA, SAE, security attacks, IEEE 802.11s

I. INTRODUCTION

Distributed mesh sensor networks provide cost-effective communications for deployment in various smart grid domains, such as home area networks (HAN), neighborhood area networks (NAN), as well as Substation/Plant-generation local area networks for real-time monitoring and control. They offer various unique features such as self-configuration, where the network can incorporate a new node into the existing structure In addition, ease of installation, scalability, self-healing are also amongst other important features.

Despite these advantages, a major drawback of mesh networks is that they are more exposed to cyber attacks as data packets have to be relayed on a hop-by-hop basis. For this reason the security of mesh/sensor networks has been a challenging issue in wireless communications. In particular, these networks, due to their lack of infrastructure, would require a distributed approach to authenticate the mesh nodes. So far, there has been a significant amount of work on mesh network security protocols, namely network vulnerability against cyber attacks [1]-[8]. For example [4] studies the risk of denial of service attacks through interference (jamming) at the Physical (PHY) and Medium Access Control (MAC) layers. In [5] the authors explore the use of intelligent agents called Honeypots by generating a dummy Route Request (RREQ) packet to detect and trap attackers. [6] addresses a distributed Security Architecture for mesh routers, as well as a key distribution scheme that supports layer-2 encryption. For more information about existing security protocols [7] and [8] provide a survey of security requirements for mesh networks.

The newly adopted IEEE 802.11s standard was recently released for mesh networks [9]. This standard supports Simultaneous Authentication of Equals (SAE) as its default security protocol. Unlike other protocols where one node will act as an authenticator and the other as the supplicant (e.g. server-client), in SAE either side can function as the "authenticator" to run the protocol as soon as it discovers its peer through Beacons and Probe Responses. SAE is a password based authentication protocol where passwords are used to deterministically compute a secret element in the negotiated group, called a "password element (PWE)" [9]. The derivation of these key materials in SAE is based on a single password shared by all nodes in the network. Although an attacker is unable to determine the password through eavesdropping, disclosure of the password would allow unauthorized nodes to join the network, hence compromising the confidentiality and integrity of the network. Bear in mind that since the MAC address of a node is the only identity, by impersonating other nodes an attacker can access the network. Once an attacker cracks the password or receives it from a legal MP, it cannot be excluded from the network without changing this password in all MPs and restarting the network [10].

An alternative approach to SAE is a protocol known as Efficient Mesh Security Association (EMSA) [11]. Through the use of a mesh key hierarchy EMSA is capable of establishing link security between two MPs in a wireless mesh network. While both SAE and EMSA can be utilized to support IEEE 802.11s mesh networks, they differ in terms of delay overhead, complexity, and resiliency to cyber attacks. Nonetheless, since both protocols deploy a 4-wayhandshaking, the network can become vulnerable to the denial of service attack. Therefore, to enhance the network protection against such attacks, in this paper we present a novel periodic key refreshment and distribution strategy together with the denial of service attack model to access both protocols..

The paper is organized as follows: In Section II after a brief overview of SAE and EMSA, we describe the implementation of SAE and EMSA using a multigate mesh networks followed by introducing the key refreshment strategy, which is presented in Section III. In section IV, we present a denial of service (DOS) attack model by an intruder during a 4-

way handshaking process. Finally, in Section V we present the results in terms of delay and overhead based on the frequent updates of the key materials.

II. MESH SECURITY SYSTEMS

The security of a mesh network relies on its ability to protect the message integrity against malicious attacks. This requires guaranteeing the confidentiality and authenticity of the data packet exchanges, which can be achieved by designing a highly reliable association and authentication processes to prevent an attacker (the adversary) access to the network by originating fake messages to interrupt the network. An example of the latter is a black hole attack where a node can tamper with the routing and prevent packets reaching their intended destinations by sending fake messages (also causing DoS), or making all packets to be routed to itself. In a mesh network the authorization is an important step where a node needs to undergo a process of association in order to access the network. The process consists of peer link establishment and authentication. In the following, we describe the SAE and EMSA protocols for mesh networks.

A. EMSA for Multigate Networks

EMSA services are based on providing an efficient establishment of link security between two MPs in a wireless mesh network through the use of a mesh key hierarchy [11]. For example, in the case of a multigate network structure [12] we assume that the master gateway will act as the mesh authenticator (MA), as well as the mesh key distributor (MKD). Within the MKD domain there are a number of gateways and meters (mesh nodes) [12]. The MKD derives keys to create a mesh key hierarchy. In our network the master gateway is responsible for creating and distributing a mesh key hierarchy to its local gateways and subsequently to all the mesh points after each stage of the authentication process. In other words, the master gateway stores all MP's authentication information. The EMSA operation consists of peer link establishment, followed by EAP (Extensible Authentication Protocol) [13] and 4-way handshaking for the key derivation between every pair of mesh nodes in the network. After Mesh Key Holder Security Handshake (MKHSH) of the EMSA, the authenticated supplicant becomes a mesh authenticator.

At the initial stage the EMSA capability is advertised through beacon and probe response frames using the MKD domain identifier (MKDD-ID) value. This value is received from the MKD during the mesh key holder security handshake. In initial EMSA authentication, an MP carries out its first security association with an MA and establishes mesh key hierarchy for securing future links. This contains communication exchanged between an MP and an MA where a supplicant MP issues an association request frame containing a Peer Link Open IE and the MKDD-IE requests to establish a mesh key hierarchy. The supplication MP is expected to receive an association response frame containing a Peer Link Confirm IE and the information to perform key derivations for establishing link security. If required, the 802.1X authentication occurs next and is followed by an EMSA 4-way handshake.

For example, in the case of a multigate network, prior to the EMSA authentication each gateway (as a supplicant) initiates the link establishment with the master gateway through the Association Request and Association Response frames. This consists of exchanging Peer Link Open and Peer Link Confirm information elements. As soon as the link establishment succeeds, the master gateway begins the authentication process. Under IEEE 802.1X, which also defines EAP over LANs (EAPOL), EAP messages are exchanged between the supplicant (e.g., gateway) and authenticator (e.g., Master gateway). EAP messages from the supplicant are relayed to the authentication server. In our model we assume that the authentication server and master gateway are co-located (otherwise, EMSA should provide a mechanism for secure communications between the master gateway and mesh key holders). This process in 802.11s is referred to as initial authentication. Upon successful authentication, the master gateway and a supplicant gateway will initiate a 4-way handshake that results in deriving PTK (Pairwise Transit Key) for unicast communications and GTK (Group Transit Key) for multicast communications. After 4-way handshaking, the supplicant MP is able to receive the router announcement from the mesh authenticator and then has the route to the mesh key distributor (e.g., the master gateway). Before a supplicant MP (e.g. gateway) becomes an authenticator itself, another set of hierarchical key needs to be established via the Mesh Key Holder Security Handshake (MKHSH). This key, which is referred to as PTK-KD, is derived from the KDK for communication between the supplicant node (e.g., gateway) and the Master gateway. It is used for all communications between the mesh authenticator (see Fig. 2) and mesh key distributor (e.g., Master gateway) when the supplicant becomes a mesh authenticator.

The newly authenticated supplicant gateway then begins to initiate the authentication process for one of its children selected in the routing tree. If the child MP has already been authenticated previously by another neighbor MP (or gateway), the authentication process may consist of only a peer link establishment with 4-way handshaking, but without the need of EAP-OL authentication. This is referred to as the “Subsequent Authentication” in [11]. The process of link establishment and authentication will continue until every MP possesses PTK, GTK and PTK-KD throughout the routing tree. We should point out that the multigate network structure routing tree is constructed according to [12].

B. SAE for Multigate Networks

In SAE, a single shared password is used by all MPs to authenticate each other in the absence of knowledge proof [9]. Unlike EMSA, there is no authentication server involved in SAE.

In SAE the participating pair of MPs can equally initiate the protocol. Indeed, either side may initiate the protocol simultaneously as their messages are independent of each other [9]. In this paper, the parties involved are defined as MP-A and MP-B and identified by their MAC addresses. After discovering a peer through passively monitoring beacons or active probing, MPs initiate the SAE protocol. Prior to the message exchanges, the involved parties will generate the PWE based on the shared password and their MAC addresses. The computation is either based on FFC or ECC. After the generation of the PWE, two random numbers, namely rand and mask, are produced and used with PWE in the following message exchanges. Upon successful SAE authentication, both MP-A and MP-B generate a PMK, which is used in the following 4-way handshake to produce PTK and GTK.

In the case of a multigate network, every pair of MPs will perform SAE authentication after discovering each other and generate PMK keys. Security policy is then negotiated in the following association procedure [9]. Based on the PMK keys, a 4-way handshaking is performed to generate PTK and GTK.

III. Periodic Key Refreshment Strategy

In this strategy all the key materials will be updated at regular intervals. This is achieved by initiating EAP or SAE authentication and 4-way handshaking to derive a new set of keys before expiration of the existing key materials. It should be noted that the lifetime of all keys derived from the MSK in the EMSA protocol, or Master PMK (MPMK) in the case SAE, are bound to the lifetime of the MSK or MPMK. In EMSA, for instance, the lifetimes of the PMK-MKD and KDK should not be more than the lifetime of the MSK. The lifetime of the PTK and PMK-MA should remain the same as that of the PMK-MKD. Similarly, the lifetime of the PTK-KD should be the same as that of the KDK [11]. As soon as the key lifetime expires, each key holder deletes their respective derived keys.

A similar situation occurs in the SAE case where the lifetime of the PMK-R0, PMK-R1, and PTK are bound to the lifetime of the Master PMK (MPMK) from which they are derived. In both cases, upon expiration of the keys' lifetime the corresponding MP's operation will come to an end and will resume only after a successful security process. This can consequently disrupt the operation of the network if the life cycle of the key materials is short. At the same time, if keys remain unchanged over a long period of time (until they expire), the network becomes more vulnerable to cyber attacks.

Therefore, in order to maintain operation of the network over the long haul, we propose a strategy that is based on refreshing the key materials periodically. In this approach, which has been implemented in our testbeds for both EMSA and SAE, MAs will periodically refresh MSK, PMK-MA, PTK, KDK and PTK-KD for EMSA and MPMK, PMK-R0, PMK-R1, and PTK in the case of SAE. Periodical key refreshment should occur before expiration of the key materials. By employing this strategy, the system can update the key materials seamlessly, hence eliminating network disruption. As shown in Fig. 1 for EMSA, MAs refresh the MSK with MKD through EAP authentication T_{EMSA} seconds

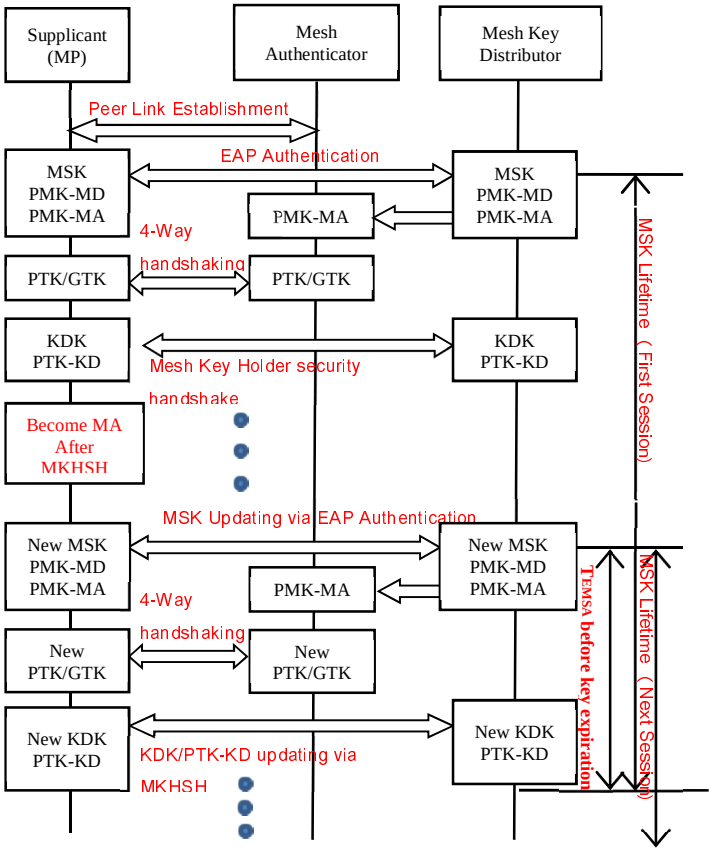

Figure 1: Periodic-Key-Updating Scheme for EMSA

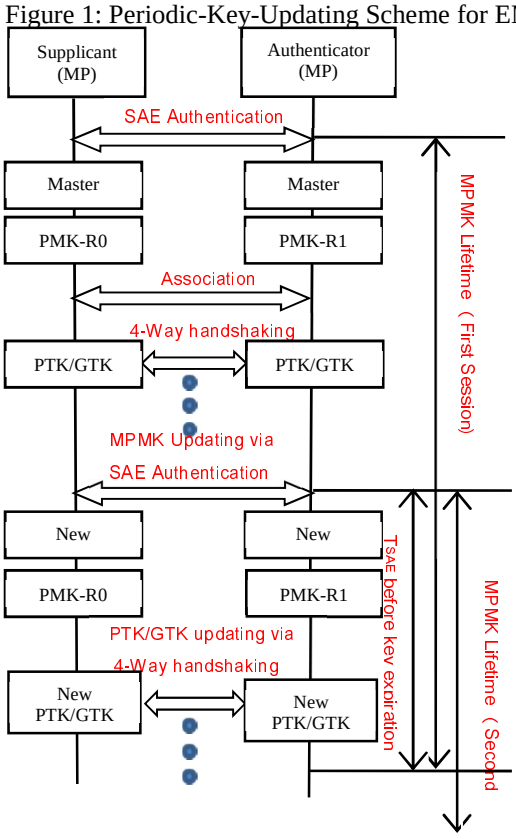

Figure 2: Periodic -Key-Updating Scheme for SAE

before expiration of the current. TEMSA is carefully selected so that the key refreshment can be completed before MSK expiration. Subsequently, based on the newly derived PMK-MKD and PMK-MA, the MAs' neighbors get PMK-MA from the MKD. As a result the PTK/GTK will be changed through 4-way handshaking. In Each MSK lifetime, referred to as a MSK session, multiple PTK/GTK updates will be performed to against cyber attacks and mitigate vulnerability. As shown in Fig. 2, a similar strategy has also been applied to SAE.

IV. SECURITY-IMPROVED 4-WAY HANDSHAKING

The security of a mesh network relies on its ability to protect the message integrity against malicious attack. This requires guaranteeing the confidentiality and authenticity of the data packet exchanges, which can be achieved by designing a highly reliable association and authentication processes to prevent an attacker (the adversary) access to the network by originating fake messages to interrupt the network. For example, as shown in Figs. 1 and 2, after acquiring PMK-MA in EMSA or PMK-R0 and PMK-R1 in SAE, the MA and supplicant will begin a 4-Way handshake. It is reasonable to assume that the PMK key derived after EAP authentication or SAE authentication is secure and known only to the authenticator and the supplicant. As stated in [14], attacks are expected to occur only before the generation of the first PTK because of the Link Layer Data Encryption. Therefore, protecting PTK at all times is vitally important as it is nearly impossible to break the cryptographic functions, unless the integrity of the PTK is compromised. To assess this situation, in our model we assume an intruder is carrying out a DoS attack during the 4-way handshake, in order to deny the authenticator and supplicant from deriving PTK keys. The intruder is assumed to be able to forge other MPs' MAC address, eavesdrop and forge received messages. Without loss of generality the abstract messages are exchanged in a 4-way handshake, as shown in Fig. 3, where SPA and AA, SNonce and ANonce, represent the MAC address and Nonces of the supplicant and authenticator, respectively; sn is the sequence number; msg1, 2, 3, 4 are indicators of different message types; and MIC$_{PTK}${} represents the Message Integrity Code (MIC) calculated for the contents inside the bracket with the fresh PTK [14]. Note that the first message sent from the authenticator to the supplicant MP is not encrypted and tampering with it simply makes the handshake fail. As soon as the supplicant has received message 1, it will have the necessary information (as shown in Fig 2) to construct its reply message. However, the supplicant will encrypt message-2 by computing the MIC over the entire message-2. This would permit the MA to detect whether the message has been tampered with.

Under these conditions, as shown in Fig. 3, Message 1 is highly vulnerable to attack as it is not protected by the MIC field. An intruder can easily block the 4-way handshake by forging Message 1. A one-message DoS attack is depicted in Fig. 4, where the intruder eavesdrops Message 1 from the authenticator and sends a forged Message 1 with a new ANonce to the supplicant after Message 2. The supplicant will generate a new PTK' after receiving forged Message 1. This PTK' is inconsistent with the one in the authenticator and

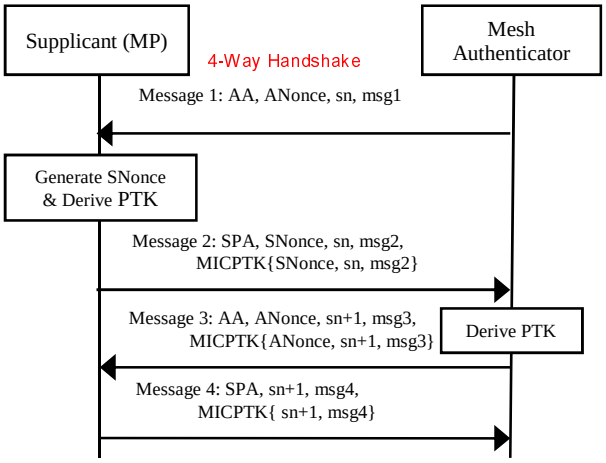

Figure 3: The 4-way handshaking procedure

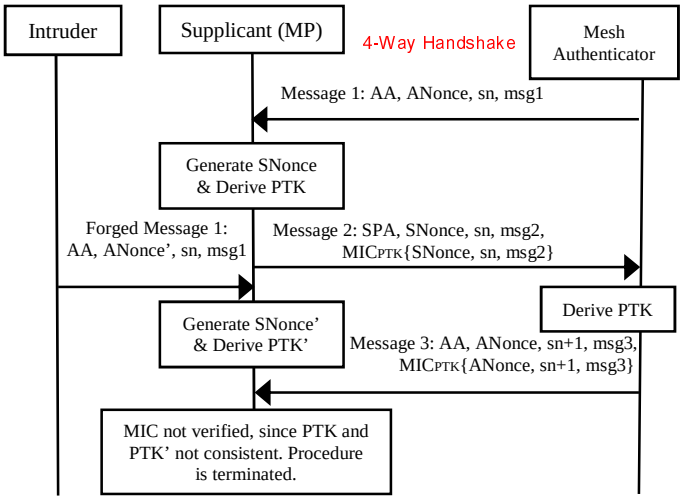

Figure 4: The one-message DoS attack on the 4-way handshaking

hence terminates the following 4-way handshaking steps. A solution to this one-message DoS attack is storing two temporary PTKs (TPTK) and one PTK in supplicant [14], where TPTK is updated when receiving Message 1, while PTK is updated only upon receiving Message 3 with a valid MIC. The MIC in Message 3 is verified by the two TPTKs or PTK. In this way, the one-message DoS attack is defeated.

Nonetheless, the intruder can still attack the supplicant by employing a multiple-messages DoS attack, where multiple forged messages with different Nonces are sent to the supplicant by the intruder. In this case, the supplicant has to store all the received Nonces, TPTKs and PTK, in order to complete the 4-way handshaking with a legitimate authenticator. This multiple-message DoS attack can exhaust the supplicant's memory if the intruder floods huge numbers of forged messages 1 to the supplicant.

In this paper, message 1 authentication in [14] is employed to improve the security properties of EMSA and SAE by preventing the DoS attacks on a 4-way handshaking. Since the

PMK key is known only to both authenticator and the supplicant, it can be used to derive a trivial PTK and then an MIC. In this way, the intruder cannot forge Message 1. Therefore the one-message DoS attack in Fig. 4 and multiple-message DoS attack are avoided. Furthermore, in the key-refreshment schemes proposed in Section III the PMK is periodically and dynamically updated which would further prevent the intruder hacking into the PMK key through replay messages.

V. Simulation Results

In this section, the proposed auto-key-upgrade EMSA and SAE security protocols are investigated using a 3-DAP (3-Gateway) mesh network, as seen in Fig. 5. This network consists of three gateways (DAP-1, DAP-2, and DAP-3) and 36 meters [12].

In the simulation the input data generated at a Variable Bit Rate (VBR), is encapsulated into fixed 512 bytes User Datagram Protocol (UDP) packets. IEEE 802.11b is used in the physical layer and the data-rate is 2 Mbps, while the gateways are assumed to have an unlimited bandwidth. The noise factor is 10.0, as recommended for testing IEEE 802.11b. The path loss factor used in this paper is 2 and the retransmission limit is 7. In the simulations, a set of MSK/MPMK lifetime values, namely 20 seconds, 100 seconds and 200 seconds, is used to study the impact of the overhead caused by periodical key-refreshment schemes. Furthermore, in each MSK/MPMK session, multiple PTK/GTK updates (e.g., 1, 2 and 5 updates) will be performed to mitigate vulnerability.

In Figs. 6 and 7, we assess the security performance for EMSA and SAE with and without a periodical key-refreshment scheme. When the EMSA and SAE schemes refrain from periodical updates, mesh nodes stop communication with each other as soon as the PTK keys expire and this will result in re-initiating EMSA or SAE authentications. It can be seen from Figs. 6 and 7 that the EMSA and SAE schemes achieve a slightly worse performance than the Non-Security system when periodic key refreshment is applied. The EMSA and SAE schemes without periodical updating, obtain the worst performance. Obviously, re-initiation of the EMSA or the SAE authentication after the keys' expiration will halt the data transmission temporarily and cause more overhead. Furthermore, SAE schemes outperform EMSA schemes because of less overhead. Fig. 8 shows that at the selected MSK/MPMK lifetime value, the system performance does not degrade significantly with more frequent key refreshment. This is a price that may be worth paying in order to improve system security. Furthermore, it can be seen from Fig. 8 that there is only slight differences when carrying out different numbers of PTK/GTK updates in each MSK/MPMK session. It is reasonable to draw the conclusion that in our schemes, the overhead resulting from 4-way headshaking is negligible.

In Figs. 9 and 10, we introduced an intruder to the network that eavesdropped and spoofed neighbors' messages. The simulation results in Figs. 9 demonstrate the extent of the damage caused by the DoS attacks. However, after employing Message 1 authentication, the EMSA and SAE systems' performances remain unaffected. In Fig. 10, we assume that an intruder carries out a black hole attack after it passes EMSA

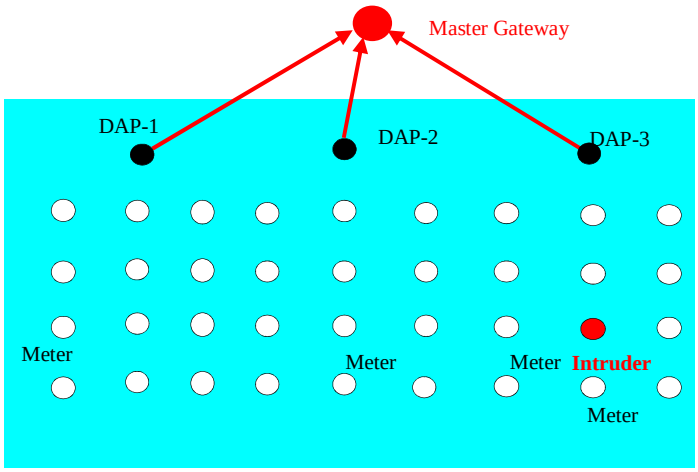

Fig. 5: A Multi gateway (GW) network scenario consisting of 3-DAP and 36 meters where every meter can have separate paths to at lease two of the neighboring DAPs.

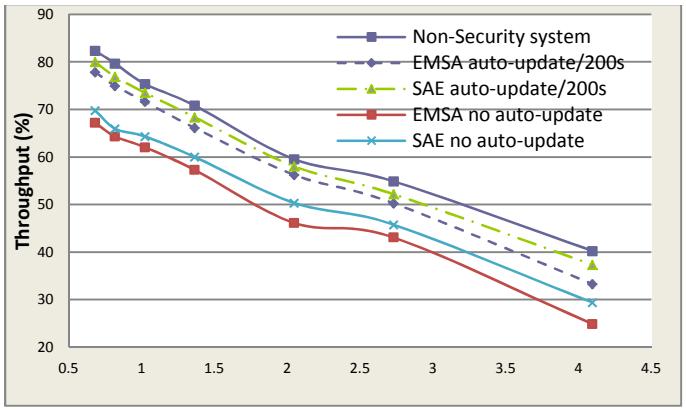

Fig. 6: Throughput performance of the proposed periodic-key-update EMSA and SAE schemes, where the beacon interval is 0.8 second and the MSK/MPMK lifetime is 200 seconds.

authentication or SAE authentication. In SAE, once the intruder cracks the password or receives it from a legitimate MP, it cannot be excluded from the network without changing this password in all MPs and restarting the network [10]. By contrast, the EMSA is capable of removing the intruder from the network with the involvement of authentication server. Fig. 10 demonstrates this advantage of the EMSA over the SAE.

VI. Conclusion

In this paper we first evaluate the performance of different authentication schemes for a multigate mesh network. We then adopt a strategy which is based on periodical refreshment of key materials and investigate its effect on improving network protection against cyber attacks. The results include a denial of service (DoS) attack by an intruder during 4-way handshake message exchanges. Furthermore, the simulation results demonstrate the advantage of EMSA over SAE in that EMSA is capable of excluding an intruder from the network easily thanks to the involvement of the authenticate server.

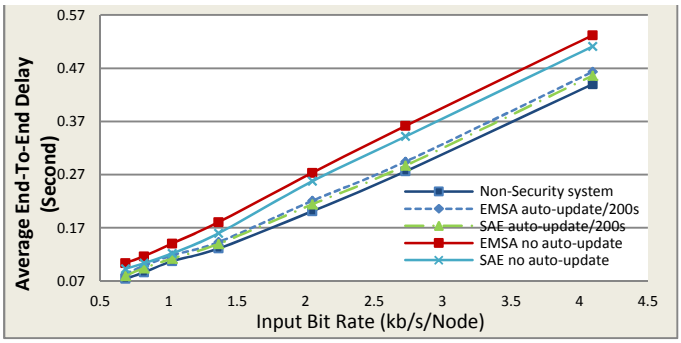

Fig. 7: Delay performance of periodic-key-update schemes.

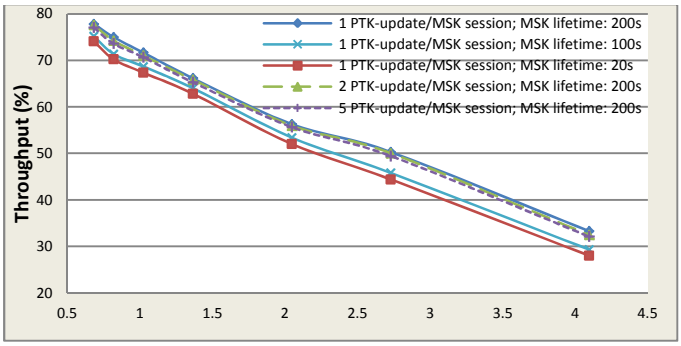

Fig. 8: Throughput performance of the proposed periodic-key-update EMSA with different MSK lifetime and multiple PTK updates per session.

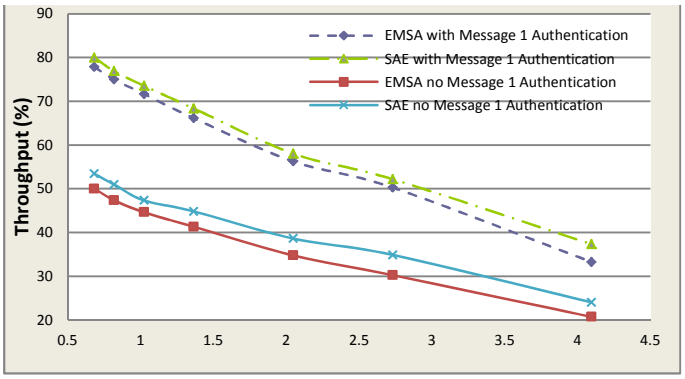

Fig. 9: Throughput performance of the proposed EMSA and SAE schemes when encountering DoS attacks.

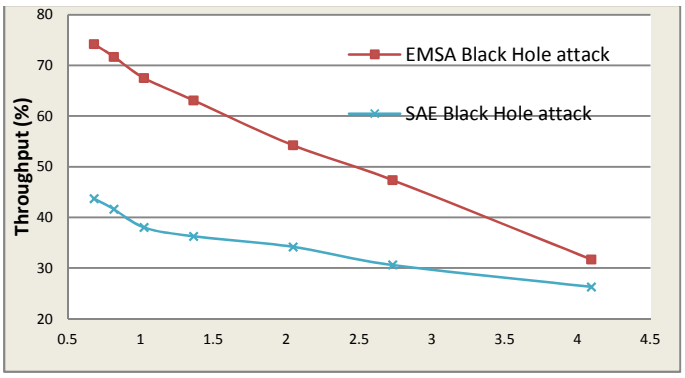

Fig. 10: Performance of the proposed EMSA and SAE schemes when trying to exclude the intruder from the network.

REFERENCES

[1] Kui Ren, Shucheng Yu, Wenjing Lou and Yanchao Zhang, "PEACE: A Novel Privacy-Enhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks", IEEE Transactions on Parallel and Distributed Systems, vol. 21, Issue 2, pp. 203-215, 2010.

[2] L. Lazos and M. Krunz, "Selective jamming/dropping insider attacks in wireless mesh networks", IEEE Network, vol. 25, Issue 1, pp. 30-34, 2011.

[3] S. Glass, M. Portmann and V. Muthukkumarasamy, "Securing Wireless Mesh Networks", IEEE Internet Computing, vol. 12, Issue 4, pp. 30-36, 2008.

[4] J. Mišic, and B. Mišic, Vojislav, "Wireless sensor networks for clinical information systems: A security perspective," IEEE International Conference on Distributed Computing Systems Workshops, ICDCS 2006, July 4, 2006.

[5] A. Prathapani, L. Santhananr, P. D. Agrawal, "Intelligent honeypot agent for blackhole attack detection in wireless mesh networks," IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, MASS '09, p 753-758, 2009, 2009.

[6] F. Martignon and S. Paris, "Experimental study of security architectures for wireless mesh networks," 6th IEEE Annual Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops, SECON Workshops 2009, June 22, 2009 - June 26, 2009.

[7] H. Redwan, K-H Kim, "Survey of security requirements, attacks and network integration in wireless mesh networks," Proceedings of New Technologies, Mobility and Security Conference and Workshops, NTMS 2008.

[8] B. He and SD. P. Agrawal, "An identity-based authentication and key establishment scheme for multi-operator maintained Wireless Mesh Networks, IEEE 7th International Conference on Mobile Adhoc and Sensor Systems (MASS), 2010, pp. 71-87.

[9] IEEE 802.11s Task Group, Draft Amendment to Standard for Information Technology – Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Amendment: ESS Mesh Networking, IEEE P802.11s/D1.0, November 2006.

[10] A. Egners and U. Meyer. "Wireless mesh network security: State of affairs". IEEE 35th Conference on Local Computer Networks (LCN), pages 997–1004, 2010.

[11] doc.: IEEE 802.11-06/1470r3: "Efficient Mesh Security and Link Establishment", November 2006.

[12] H. Gharavi and Bin Hu, "Multigate Communication Network for Smart Grid", THE PROCEEDINGS OF THE IEEE, vol. 99, NO. 6, pp. 1028-1045, June 2011.

[13] IEEE Standard 802.1X-2004: "Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control", December 2004.

[14] Changhua He and John C Mitchell, Analysis of the 802.11i 4-Way Handshake. In WiSe '04: Proceedings of the 2004 ACM workshop on Wireless security, P43—50, 2004.