4-Way Handshaking Protection for Wireless Mesh Network Security in Smart Grid

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

Abstract—Wireless mesh/sensor networks offer various unique features such as self-configuration, ease of installation, scalability, and self-healing, which make them very attractive for deployment in various smart grid domains, such as Home Area Networks (HAN), Neighborhood Area Networks (NAN), and substation/plant-generation local area networks for real-time monitoring and control. Their main drawback is that they are more exposed to cyber-attack as data packets have to be relayed on a hop-by-hop basis. This paper presents a dynamically updating key distribution strategy, together with a message protection scheme in support of 4-way handshaking. For the 4-way handshaking, we propose a hash based encryption scheme to secure the unprotected message exchanges during the handshaking process. This is aimed at improving the resiliency of the network in the situation where an intruder carries a denial of service attack. We then evaluate the security of the proposed scheme against cyber-attack, as well as network performance in terms of delay and overhead.

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

I. INTRODUCTION

Wireless Local Area Networks (WLAN) can be deployed in various smart grid domains [1]-[2] where a wire line infrastructure does not exist. These networks offer a cost effective solution when compared with other wired or wireless options. Fig. 1 shows a possible deployment of WLAN in various smart grid domains, which includes a Home Area Network (NAN), Neighborhood Area Network (NAN), and Substation Area Network (SAN). To improve the coverage area these networks can extend to mesh networks to overcome their limited transmission range. Currently, mesh networks that are based on the IEEE 802.11s [3] and IEEE 802.15.4g smart utility network (SUN) [4]-[5], have been extensively considered for smart grid systems. For neighborhood area networks (NAN), [6] proposes a multigate mesh network that is based on the IEEE 802.11s standard. In this approach, a combination of packet scheduling and multichannel frequency assignment is used. This combination is mainly utilized to solve the bottleneck problem under blackout conditions when a system expects to receive extensive power outage notifications and exchanges.

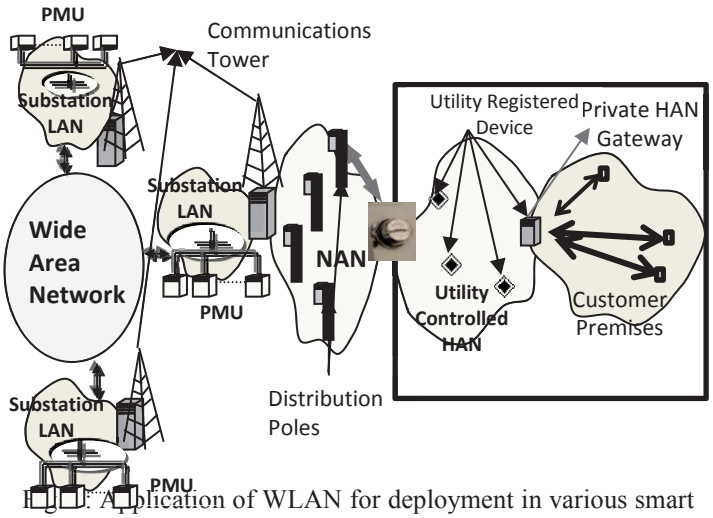

Fig. 1. Application of WLAN for deployment in various smart grid domains.

Fig. 1 also shows an example of a Substation Area Network (SAN). SAN may consist of a number of Phasor Measurement units (PMUs) that are communicating with the Phasor Data Collector (PDC) located at the gateway connected to the backbone network. A PMU is GPS synchronized to generate high-precision, common time, date packets. These packets need to be transmitted reliably with low delay to the final destination (e.g., super PDC) via the local PDC for archiving, monitoring, or control. While single hop WLAN technologies may be considered as a viable option in the absence of any wired or wireless infrastructure, their mesh extension would require thorough investigation with respect to latency and reliability. Nonetheless, mesh networks 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, and self-healing are amongst other important features. Despite these advantages, a major drawback of multi-hop mesh networks is that they are more exposed to cyber attack 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 Points (MPs).

So far, there has been a significant amount of work on mesh network security protocols, namely network vulnerability

against cyber attack [7]-[15]. For more information about existing security protocols [13] and [14] provide a survey of security requirements for mesh networks. For IEEE 802.11 WLAN networks, the newly adopted IEEE 802.11s standard was recently released for mesh networks [3]. This standard supports Simultaneous Authentication of Equals (SAE) as its default security protocol. SAE is based on a single password shared by all nodes in the network. Although an attacker may not be able 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. An alternative approach to SAE is a protocol known as Efficient Mesh Security Association (EMSA) [16]. Through the use of a mesh key hierarchy EMSA is capable of establishing link security between two MPs in a wireless mesh network. Since both protocols deploy a 4-wayhandshaking, the network can become vulnerable to a Denial of Service (DoS) attack. In particular, through eavesdropping an intruder can easily block the 4-way handshake by forging the unprotected Message-1 [17] or the defective Message-3 that an MP receives from the Mesh Authenticator (MA). To enhance network protection against such attacks, we had considered a periodic key refreshment and distribution strategy to further protect the network security against a denial of service attack [15]. While the periodic key updating approach can significantly improve the overall security of mesh networks [15], in the 4-way handshaking process Message-1 and Message-3 remain vulnerable to DoS attacks. Therefore, in this paper our main objective is to develop an efficient 4-way handshaking protection scheme. The proposed scheme is capable of improving the security of mesh networks for their deployment in various smart grid domains (see Fig. 1).

The paper is organized as follows: In Section II we provide a brief overview of EMSA and its implementation in a mesh network, followed by the key refreshment strategy in Section III. In section III, after introducing a Denial of Service (DoS) attack model by an intruder during a 4-way handshaking process, we propose a hash based encryption scheme that is aimed at protecting the so-called Message-1 and Message-3. Finally, in Section V we present the results for a mesh network in terms of delay and overhead.

II. Dynamic Mesh Key Distribution Strategy

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) accessing 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) [11], or making all packets to be routed to itself. To securely maintain operation of the network over the long haul, we developed a strategy that is capable of dynamically changing the key information periodically and/or in situations where an active attack has been detected. Before describing the key refreshment strategy, the following provides a brief description of the mesh security protocol namely, EMSA.

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. EMSA services, for instance, are based on providing an efficient establishment of link security between two MPs through the use of a mesh key hierarchy [16]. In the case of a multigate network structure [6] 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 points) [6]. The MKD derives keys to create a mesh key hierarchy. In this network, the master gateway is responsible for creating and distributing a mesh key hierarchy to its local gateways and subsequently to all the MPs after each stage of the authentication process. In other words, the master gateway stores all MP's authentication information. 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. 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 now 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 Key Distribution Key (KDK) for communication between the supplicant node (e.g., gateway) and the Master gateway. It is used for all communications between the mesh authenticator 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 EAPOL authentication. This is referred to as the “Subsequent Authentication” in [16]. The process of link establishment and authentication will continue until every node 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 [6].

III. Periodic Key Refreshment Strategy

In this strategy all the key materials will be updated at regular intervals. This is achieved by initiating EAP

authentication and 4-way handshaking to derive a new set of keys before expiration of the existing key materials.

In EMSA, for instance, the lifetimes of the PMK-MKD and KDK should not be more than the lifetime of the MSK. Also, 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 [16]. As soon as the key lifetime expires, each key holder deletes their respective derived keys. 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 attack.

Therefore, to securely maintain operation of the network over the long haul, we developed a strategy that is capable of dynamically changing the key information periodically and/or in situations where an active attack has been detected. In the absence of any reliable detection scheme, the system can update the key materials seamlessly, hence eliminating network disruption.

Under these conditions, all the key materials, together with MSK, will be updated periodically. For EMSA, MAs refresh the MSK with MKD through EAP authentication. Such updates may take place at regular intervals. Therefore, during each MSK lifetime, also referred to as a MSK session, multiple PTK/GTK updates can be performed before expiration of the MSK. This would consequently result in generating a new PTK/GTK through 4-way handshaking. It is important to point out that updating the key materials before expiration will result in maintaining the existing routes in the network; otherwise it would become necessary to carry out a fresh routing and association process of the involved MPs. This would consequently cause a significant delay in re-establishing the network.

IV. Proposed Security-Improved 4-way handshaking

Protecting the confidentiality and integrity of data packet exchanges would require designing a highly reliable association and authentication processes in order to prevent an adversary to originate fake messages that can interrupt the network during the 4-way handshaking process. For example, as shown in Fig. 2, after acquiring PMK-MA, the MA and supplicant will begin a 4-Way handshake. It is reasonable to assume that the PMK key (derived after EAP) is known only to the authenticator and the supplicant.

As stated in [17], attacks are expected to occur 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, to deny the authenticator and supplicant from deriving PTK keys. The intruder is assumed to be able to forge other MPs' MAC addresses, eavesdrop, and forge received messages. Fig. 2 shows the abstract messages that are exchanged in a 4-way

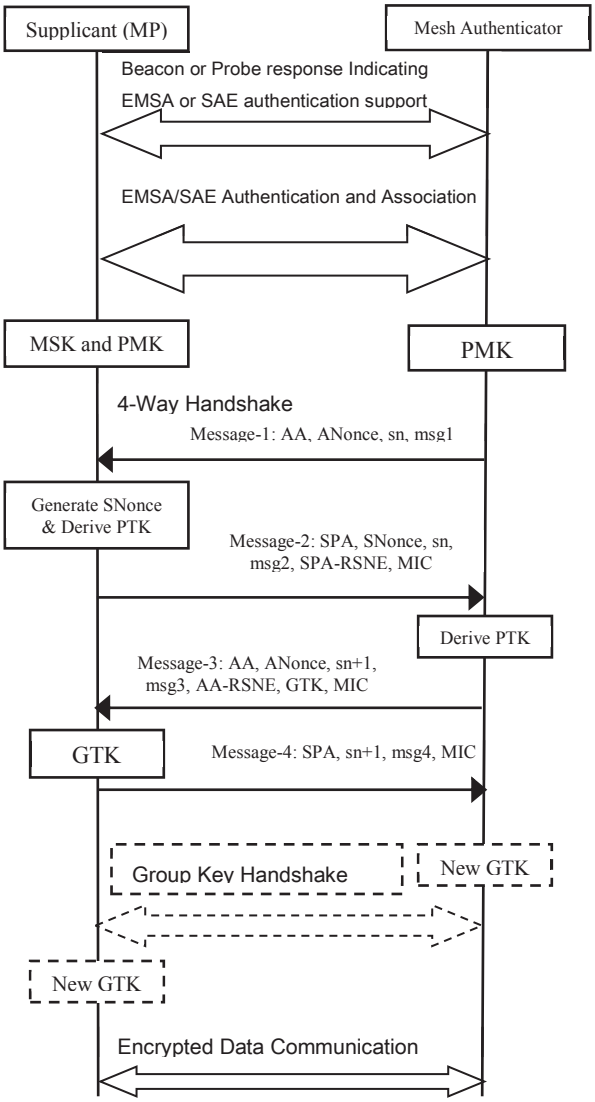

Fig. 2: Establishment of Robust security network association (RSNA), where the dashed group key handshake is optional.

handshake, In this figure 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]. MIC is used to prevent attackers from tampering the message without detection. Robust Security Network Element (RSNE) indicates RSN capabilities, authentication, and cipher key selection.

DoS Attack on Message-1

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. Subsequently, 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. 3, where an intruder eavesdrops Message-1 from the authenticator and sends a forged Message-1 with a new ANonce to the supplicant after Message-2. Consequently, the supplicant has to generate a new PTK' after receiving a forged Message-1.

Obviously, this PTK' would be inconsistent with the one in the authenticator and hence terminates the 4-way handshaking process. One solution to this one-message DoS attack is to store two temporary PTKs (TPTKs) 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-message 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 PTKs, in order to complete the 4-way handshaking with a legitimate authenticator. Unfortunately, this multiple-message DoS attack can exhaust the supplicant's memory and, more importantly, cause a significant delay if the intruder floods huge numbers of forged Messages-1 to the supplicant.

DoS Attack on Message-3

After receiving Message-3, the supplicant verifies the Robust Security Network Element (RSNE) by comparing it with the RSNE previously received (either in the Beacon or Probe Response Frame in Fig. 2). If the two RSNEs are not identical, the supplicant terminates the 4-way handshake and disassociates from the corresponding mesh authenticator. As indicated in Fig. 4, an intruder can carry out a DoS attack on Message-3 by forging a Message-3 with faked AA RSNE', msg3' and MIC'. This clearly indicates that it is not difficult for the intruder to extract and derive the correct AA, Anonce and sn+1 information from the eavesdropped Message-1., It is quite possible that the intruder is able to construct and send a faked Message-3 earlier than the MA without requiring any MIC computation. When the supplicant receives the forged Message-3 with correct AA, Anonce and sn+1, it will check the sn+1 and then verify the AA RSNE' [18]. Since the faked RSNE' is not a match with what it received before, the supplicant will abort the 4-way handshake and disassociate from the MA.

To enhance the resiliency of the 4-way handshaking, we propose a one-way hashing scheme to protect both Message-1 and Message-3 against any cyber attack. For this purpose, the MA uses one-way hash functions, such as SHA-1 [19] and SHA-2 [20], to construct secure authentication.

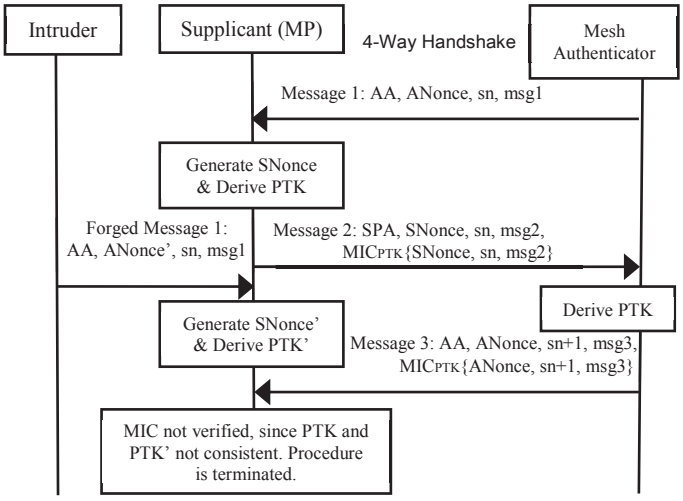

Fig. 3: The DoS attack on the Message-1 of the 4-way handshaking

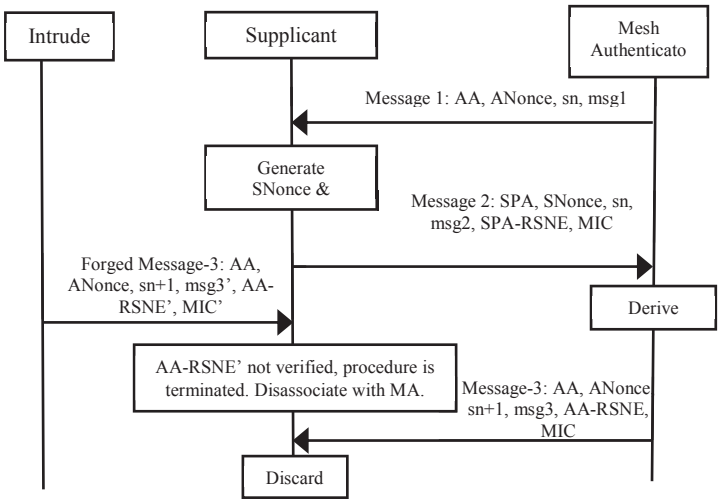

Fig. 4: The DoS attack on the Message-3 of the 4-way handshaking

Specifically, for Message-1, the MA uses *ANonce, sn, msg1* and *PMK* as input of the one-way hash function to derive a hashed value hash (*ANonce, sn, msg1, PMK*) and insert it in Message-1. Note that, since a one-way function is used to encrypt the PMK information, it is computationally impossible to derive the PMK from message-1. In other words, once the supplicant receives the one way hashing-secured Message-1, it uses the *ANonce, sn, msg1* from the received Message-1 together with its own PMK to compute the hashed value. It then compares it with that included in Message-1 to verify it. Indeed, without the PMK information, the intruder is unable to derive the correct hashed value by using a new ANonce. Please note that the employed one-way hashing function is a low complexity algorithm, in the order of $O(1)$.

As mentioned earlier, the one-way hashing scheme has also been used for Message-3 to avoid DoS attacks. Similarly, the MA uses *ANonce, sn+1, AA RSNE* and PMK as input to derive

a hashed value: *hash (ANonce, sn+1, AA RSNE, PMK)* and insert it in Message-3, as shown in Fig. 4. As soon as the supplicant receives Message-3, it then checks and compares the hashed value before verifying *AA RSNE*. Again, the intruder is unable to construct a correct hashed value: *hash(ANonce, sn+1, AA RSNE', PMK)* by using a different AA RSNE' within a relatively short period of time.

Thanks to the key-refreshment strategy proposed in Section III, the PMK, PTK and GTK are periodically updated. We can therefore utilize the updated key materials in the one-way hashing authentication mechanism to better protect Message-1 and Message-3.

V. Simulation Results

To assess the delay and overhead of the key refreshment strategy we used a mesh routing model for NAN. This simulation model consists of one gateway and 16 nodes (e.g., meters). The 16 nodes are wirelessly connected to the gateway which is connected to the backbone network. As in [6] the maximum data-rate for each node is 2 Mbps, while the gateway are assumed to have unlimited bandwidth. 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.

In Fig. 5, we assess the security performance for EMSA with and without a periodical key-refreshment scheme. When the EMSA scheme 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 authentication. It can be seen from Fig. 5 that in terms throughput the EMSA scheme can achieve a slightly worse performance than the Non-Security system when periodic key refreshment is applied. Without periodical updating, the EMSA scheme achieves the worst performance. Obviously, re-initiation of the EMSA authentication after the keys' expiration will halt the data transmission temporarily and cause more overhead.

In Fig. 6, we construct a DoS attack scenario where an intruder eavesdrops and spoofs neighbors' messages. The simulation results in Fig. 6 demonstrate the extent of the damage caused by the DoS attacks on Message-1 and Message-3. However, after employing one-way hashing protection for Message-1 and Message-3, the systems' performances remain unaffected. In this simulation, PMK, PTK and GTK are dynamically updated every 200 seconds. In Table 1, we provide the average end-to-end delay of the RSNA establishment delays caused by DoS attacks on Message-1 and Message-3 and compare them with that of the One-way hashing scheme. It can be seen from Table I that One-way hashing protection is capable of effectively defeating DoS attacks on Message-1 and/or Message-3. The attack on Message-3 causes more delay than that on Message-1, since the failure of AA RSNE verification results in the disassociation between the supplicant MP and the MA.

VI. Conclusion

In this paper we present a combination of a key refreshment strategy and a 4-way handshaking protection scheme to enhance key distribution in a wireless multihop network. We first assessed the impact of the periodical refreshment strategy on the delay and overhead. We then applied a one-way hashing scheme to improve network protection against cyber attack. This included a denial of service (DoS) attack by an intruder during 4-way handshake message exchanges. In particular, we applied the encryption scheme to message-1 and message-3.

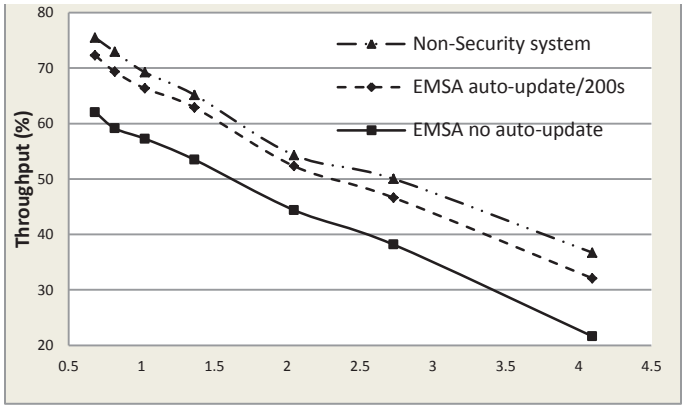

Fig. 5: Throughput performance of the proposed periodic-key-update EMSA scheme, where the beacon interval is 0.8 second and the MSK/MPMK lifetime is 200 seconds.

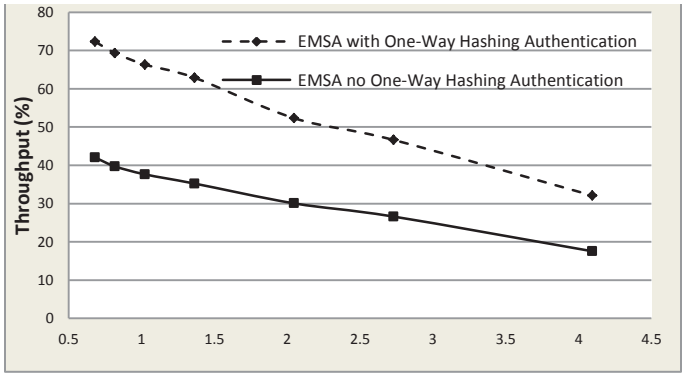

Fig. 6: Throughput performance of the proposed One-way hashing scheme when encountering DoS attacks.

Table I. Average end-to-end delay of the RSNA establishment of the attacked MPs, with and without the protection of the proposed one-way hashing scheme

	No Protection when DoS Attacks on Message-1	No Protection when DoS Attacks on Message-3	One-way hashing protection when DoS Attacks on Message-1 & Message-3
Average end-to-end delay of the RSNA establishment	3.486 s	16.534 s	0.2715 s

VII. REFERENCES

[1] Xi Feng, S. Misra, G. Xue, D. Yang, "Smart Grid — The New and Improved Power Grid: A Survey," IEEE Communications Surveys & Tutorials, Issue 4, PP. 994-980, 2012.

[2] SZ Islam, N Mariun, H Hizam., M. L. Othman, M. A. M. Radzi, M. Hanif, and I. Z. Abidin, "Communication for Distributed Renewable Generations (DRGs): A review on the penetration to Smart Grids (SGs)," 2012 IEEE International Conference on Power and Energy (PECon), pp. 870-875, Dec. 2012.

[3] 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.

[4] IEEE Std. 802.15.4g-2012, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) - Amendment 4: Physical Layer Specifications for Low Data Rate Wireless Smart Metering Utility Networks, March 2012.

[5] ZigBee Alliance, ZigBee Specification: ZigBee Document 053474r172008

[6] 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.

[7] X. Wang and P. Yi, "Security Framework for Wireless Communications in Smart Distribution Grid", IEEE Transactions on Smart Grid, vol. 2, Issue 4, pp. 809-818, Dec. 2011.

[8] 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.

[9] Y. Zhang, L. Wang, W. Sun, R. C. Green and M. Alam, "Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids", IEEE Transactions on Smart Grid, vol. 2, Issue 4, pp. 796-808, Dec. 2011.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] H. Gharavi and Bin Hu, "Dynamic Key Refreshment for Smart Grid Mesh Network Security," Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES.

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

[17] 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.

[18] IEEE 802.11 Standard Working Group, Standard for Information Technology – Telecommunications and Information Exchange Between Systems – LAN/MAN Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ANSI/ IEEE Std 802.11, first ed., 1999.

[19] FIPS PUB 180-1, Secure Hash Standard, SHA-1, http://www.itl.nist.gov/fipspubs/fip180-1.htm

[20] FIPS PUB 180-2, Secure Hash Standard, SHA-2, http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html