Improved Security with Intrusion Detection through 4 Way Handshake of DoS Attack in WMN

Sandeep Shivhare[1] , Madhuvan Dixit[2]

[1] *(PG Scholar, CSE),* [2]*A.P. (Dept of CSE)*

MITS, Bhopal

Abstract: ***The IEEE 802.11s standard has been designed to enhance security in Wireless Mesh Networks. The Extensible Authentication Protocol (EAP) and 4-way handshake aims to provide mutual authentication between supplicant and authentication server, and then derive the Pair-wise Master Key (PMK) in smart grid network. In the 4-way handshake the supplicant and the authenticator use PMK to derive a fresh pair-wise transient key (PTK). The PMK is not used directly for security while assuming the supplicant and authenticator have the same PMK before running 4-way handshake. The EAP and 4-way handshake phases have been analyzed with a proposed framework using NS2 tool. In the analysis, we have found a new Denial-of-Service (DoS) attack in the 4-way handshake. The attack prevents the authenticator from receiving message 4 after the supplicant sends it out. This attack forces the authenticator to re-send the message 3 until time out and subsequently to de-authenticate supplicant. The proposed improvements to the 4-way handshake to avoid the Denial-of-Service attack.***

Keywords: Wireless Mesh Network, Pair-wise Transient Key, Denial-of-Service, 4-way handshake.

1. Introduction

Wireless mesh networks (WMNs) offer improved utility and lower infrastructure costs than conventional wireless networks because, like mobile ad hoc networks (MANETs), they use multi-hop routing. This routing strategy extends the wireless service area and enables the network's self-healing and self-organizing properties. A WMN is distinct from MANETs in that it uses multiple radios and relies on a high-speed back-haul network itself, often wireless that optimizes network performance and provides gateways to the wired Internet and other wireless services. Early adopters of wireless mesh technology include community networks, which can provide low-cost Internet access to whole neighborhoods by buying inexpensive wireless mesh routers from companies such as Meraki. WMNs are also appealing in the developing world, as evidenced by the One Laptop per Child project's XO laptop, which is designed for educational use and implements a wireless mesh network using hardware and software that conforms to the IEEE 802.11 standard but has extensions to support wireless mesh networking. With millions of units in projected XO sales, IEEE 802.11 use for mesh networking is set to expand rapidly. The IEEE formed the 802.11 Task Group "s" (TGs) in 2004 to prepare a standards amendment to meet the requirements for WMNs. The standards amendment, which will be known as 802.11s, is expected to be ratified in the last quarter of 2009, and efforts are already under way to integrate it into the GNU/Linux kernel. WMNs need robust security protocols to ensure secure operation. The protocols should ensure the confidentiality, integrity, and authenticity of network traffic and preserve the availability of communications. A more comprehensive set of requirements might also address the problems of intrusion detection and location privacy.

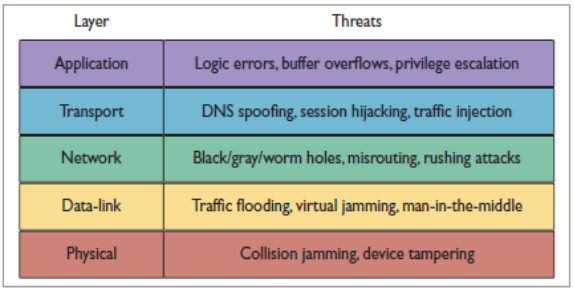

Figure 1: Wireless Mesh Network Security Risks

2. Literature Review

Wireless mesh networks (WMN) function as regular wireless networks, but with significant differences. Mesh networks decentralize the infrastructure required to maintain a network by making each node, or computer, pull double-duty as a user and a router of Internet traffic.(G. Satyavathy, S. Ananthi; 2016)

Mobile ad hoc networks (MANETs) are dynamic mobile networks that can be formed in the absence of any pre-existing communication infrastructure. In addition to node mobility, a MANET is characterized by limited resources such as bandwidth, battery power, and storage space. (Mieso K. Denko; 2015)

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), and substation/plant-generation local area networks. (Bin Hu, Hamid Gharavi; 2014)

In Smart Grid, the communication network plays a significant role. Wired communication adopted to ensure robustness of the backbone for power transmission

network but it does not provide any flexibility. (S. K. Saranya, Dr. R. Karthikeyan; 2014)

The IEEE 802.11i standard has been designed to enhance security in wireless networks. The EAP-TLS handshake aims to provide mutual authentication between supplicant and authentication server, and then derive the Pair-wise Master Key (PMK). (Abdullah Alabdulatif, Xiaoqi Ma; 2013)

It provides a survey of possible solutions for intrusion detection system (IDS) against DoS attacks. In a Denial of Service (DoS) attack, legitimate users are prevented from access to services or network resources. (Anurag Kumar, Akshay Kumar, Anubha Dhaka, Garima Chaudhary; 2013)

3. Denial-of-Service Attack in WMN

The number of Denial of Service (DoS) attack on the Internet has risen sharply in the last several years. Service providers are routinely expected to prevent, monitor and mitigate these types of attacks which occur daily on their networks. This section discuss the most common types of DoS attacks seen on the Internet and ways that service providers can prevent or mitigate damages from the attack threats. DoS attacks have become more sophisticated in the last several years as the level of attack automation has increased. Sample and fully functional attack software is readily available on the Internet. Precompiled and ready to use programs allow novice users to launch relatively large scale attacks with little knowledge of the underlying security exploits. The advent of remote controlled networks of computers used to launch attacks has changed the landscape and methods that a service provider must use. In the past year, Black Hats have taken theoretical optimizations in worm propagation and applied them to the fastest spreading worm today.

4. Problem Identification

When a nodes encounter under DoS attacks. Such nodes exhibit one or more of the following behavior:

Packet Drop- Simply consumes or drops the packet and does not forward it.

Battery Drained- A malicious node can waste the battery by performing unnecessarily operations.

Buffer Overflow- A node under attack can fill the buffer with fake updates so that genuine updates cannot be stored further.

Bandwidth Consumption- Whenever a malicious node consumes the bandwidth so that no other legitimate node can use it.

Malicious Node Entering- A malicious node can enter in the network without authentication.

Stale Packets- This means to inject stale packets into the network to create confusion in the network.

Delay- Any malicious node can purposely delay the packet forward to it.

Node Not Available- An intruder can isolate the node from taking part in any operation so as to create delays when the source node chooses another alternative path.

Stealing Information- Information like the content, location, sequence number can be stolen by the malicious node to use it further for attack.

Session Capturing- When two legitimate nodes communicate malicious node can capture their session so as to take some meaningful information.

Link Break- This can result in restricting the two legitimate nodes from communicating if the malicious node is between them.

Message Tampering- A malicious node can tamper the content of the packets.

Denying from Sending Message- Any malicious node may deny from sending messages to other legitimate nodes.

5. Proposed Methodology

The algorithm of proposed method is as follows:

Step 1: Firstly we create an IDS node in which we set AODV as a routing protocol.

Step 2: Then after the creation, our IDS node check the network configuration and capture lode by finding that if any node is in its radio range and also the next hop is not null, then capture all the information of nodes.

Step 3: Else nodes are out of range or destination unreachable.

Step 4: With the help of this information IDS node creates a normal profile which contains information like type of packet, in our case (protocol is AODV, pkt type TCP, UDP, CBR), time of packet send, receive and threshold.

Step 5: After creating normal profile and threshold checking is done in the network i.e. if network load is smaller than or equal to maximum limit and new profile is smaller than or equal to maximum threshold and new profile is greater than or equal to minimum threshold then there is no any kind of attack present.

Step 6: Else there is an attack in the network and find the attack.

Step 7: For doing it compare normal profile with each new trace value i.e. check packet type, count unknown packet type, arrival time of packet, sender of packet, receiver of

packet. And after detection of any anomaly in that parameters then block that packet sender node (attacker node).

Step 8: Now perform authentication scheme through 4-way handshake with GTK. In WMN, any two nodes consider as supplicant (Mesh Point) and Mesh Authenticator (MA). MA sends message-1 to MP with information (AA, ANonce, sn, msg1) where, these information parameter are MAC address of authenticator, pseudo or random number of authenticator, serial number and indicator of different message types, respectively.

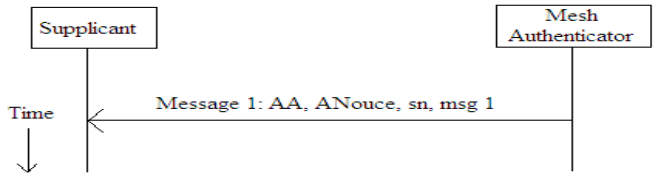

Figure 2: Message 1 delivered from Supplicant to MA

Step 9: Generate new SNouce (random number for authentication) and drive GTK (Group Transient Key), then send message-2 to authenticator with following information.

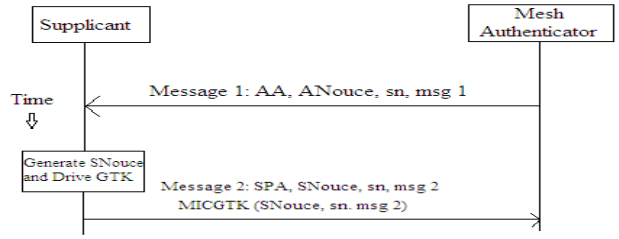

Figure 3: Message 2 delivered from Supplicant to MA

Step 10: If DoS attack perform by intruder after receiving message 1 from MA, where an intruder eavesdrops on 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 GTK after receiving the forged Message-1. Obviously, this GTK would be inconsistent with the one in the authenticator, hence causing a termination of the 4-way handshaking process. For resolving this problem perform step 1 to 7 and then perform again authentication process.

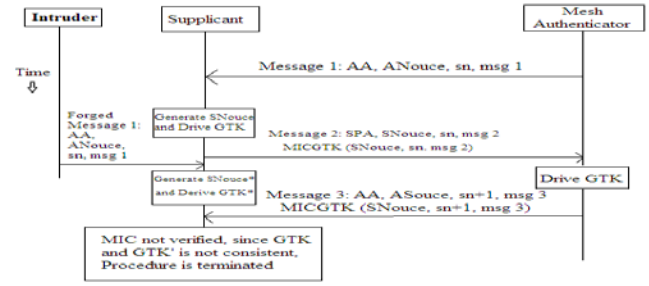

Figure 4: DoS attack on Message 1

Step 11: If DoS attack not perform on message 1 then message 3 send by MA after receiving message 2.

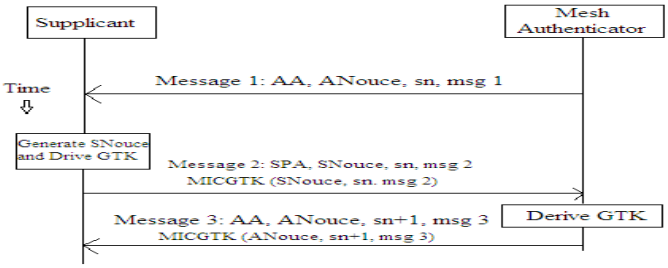

Figure 5: DoS attack does not on Message 1

Step 12: Finally, confirmation message-4 send by supplicant.

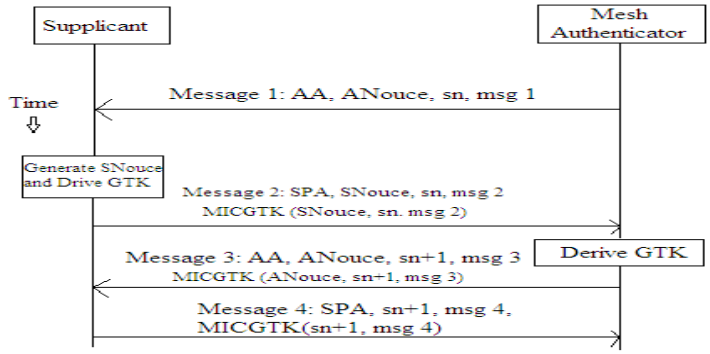

Figure 6: 4-Way Handshaking

6. Simulation/Experimental Results

For implement proposed method, we have use VMWare 10.0.1 workstation version for installing Ubuntu 12.0.4 LTS version and nsallinone-2.35.tar.gz file. Now extract tar file of NS2 in virtual machine. The simulation process has been started with three cases, which is as follows. The simulation has been started through following command

>ns sample.tcl

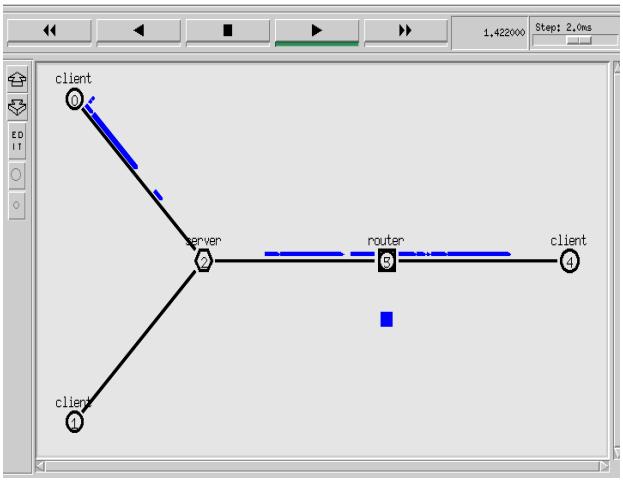

Figure 7: Simulation without attacker

When attack case has been arise then following command is used.

>ns dos.tcl

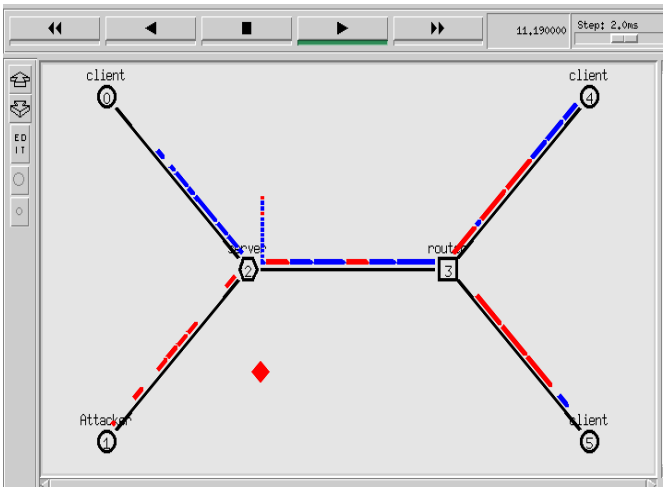

Figure 8: Simulation in attacker case

When attack case has been prevent through proposed scheme then following command is used.

>ns proposed.tcl

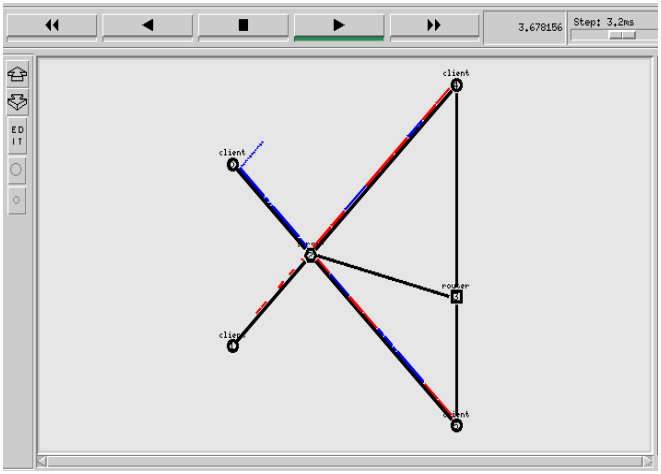

Figure 9: Simulation in after resolve attacker case

Comparison analysis has been performed on the basis of performance parameters.

Sim. Time	DoS Attack Case				Normal Case				Attack Prevention Through IDS-4WH			
	Drop Packets	Thr.	PDR	Avg. EED	Drop Packets	Thr.	PDR	Avg. EED	Drop Packets	Thr.	PDR	Avg. EED
5	177	0.76	79.62	26.92	160	0.98	42.26	16.26	114	0.82	58.69	19.22
10	492	0.98	180.5	25.46	361	1.56	117.43	15.82	263	1.25	139.73	23.32
15	750	1.12	276.9	23.45	648	1.65	205.08	14.73	553	1.35	215.41	20.55
20	1051	1.22	374.8	22.22	998	1.73	298.77	20.31	892	1.39	317.82	21.12
25	1336	1.34	474.1	27.41	1232	1.85	361.82	25.39	1031	1.44	419.21	26.39

Table 1: Comparative Result Analysis

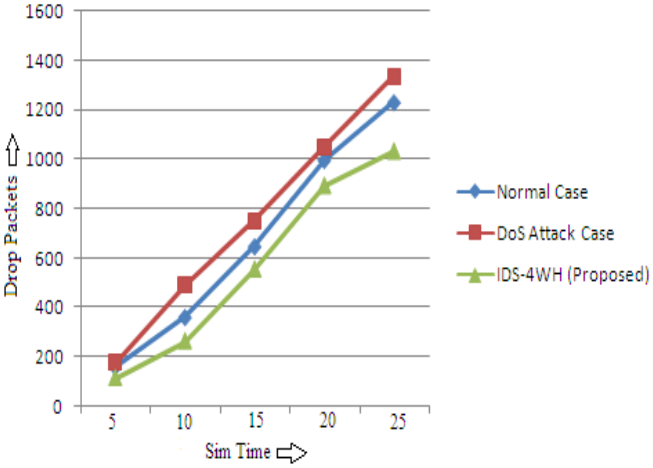

Figure 10: Analysis of Drop Packets in Normal Case, DoS Attack Case and Proposed IDS-4WH

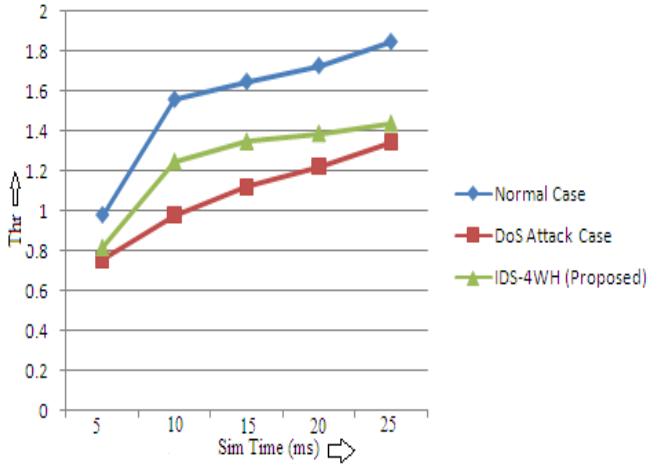

Figure 11: Analysis of Throughput in Normal Case, DoS Attack Case and Proposed IDS-4WH

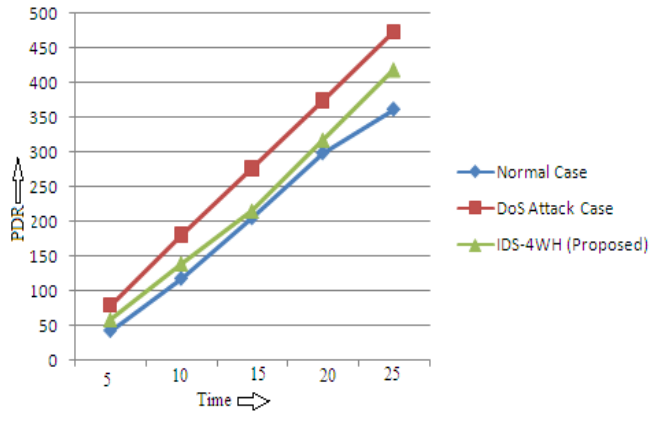

Figure 12: Analysis of PDR in Normal Case, DoS Attack Case and Proposed IDS-4WH

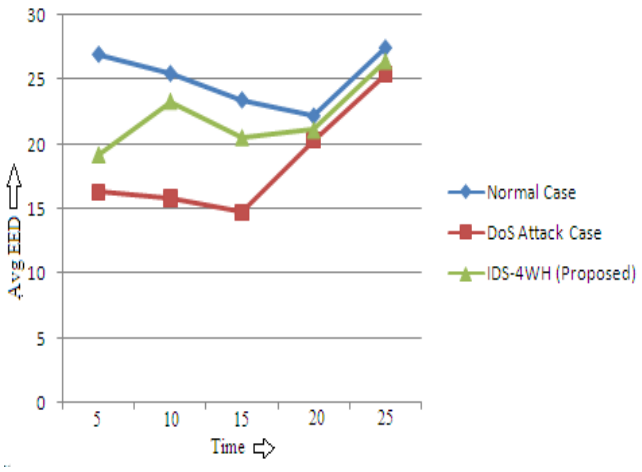

Figure 13: Analysis of Avg. EED in Normal Case, DoS Attack Case and Proposed IDS-4WH

7. Conclusion and Future Scopes

In Wireless Mesh Networks, the proposed method improve throughput, PDR in DoS attack case. Throughput is increase by 19.51%, PDR is increase by 35%. Reduce rate of drop packet and also reduce average end to end delay time. Therefore improves the QoS in WMN through detecting malicious node.

(1) The work can be extended to study the robustness of Wireless Ad Hoc Networks for all types of protocols.

(2) A study can be conducted on the relationship between the average detection delay and the mobility of the nodes.

(3) More types of attacks including group attacks can be studied and their relations to the vulnerability of the protocols can be ascertained.

(4) A complete system can be designed to implement intruder identification.

(5) A complete approach can be developed that considers more parameters such as the available queue length and the delay on a path during the route determination. In order to avoid traffic fluctuation, randomness can be introduced into route determination.

8. References

[1] Bin Hu and Hamid Gharavi, "Smart Grid Mesh Network Security Using Dynamic Key Distribution With Merkle Tree 4-Way Handshaking", IEEE TRANSACTIONS ON SMART GRID, VOL. 5, NO. 2, MARCH 2014.

[2] X. Feng, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," IEEE Commun. Surveys Tuts., no. 4, pp. 994–980, 2012.

[3] S. Z. 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)," in Proc. IEEE Int. Conf. Power Energy (PECon), Dec. 2012, pp. 870–875.558 IEEE TRANSACTIONS ON SMART GRID, VOL. 5, NO. 2, MARCH 2014.

[4] 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: ESSMesh Networking, IEEE P802.11s/D1.0, IEEE 802.11s Task Group, Nov. 2006.

[5] 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, IEEE Std. 802.15.4g-2012, Mar. 2012.

[6] ZigBee Alliance, ZigBee Specification: ZigBee Document 053474r172008.

[7] H. Gharavi and B. Hu, "Multigate communication network for smart grid," Proc. IEEE, vol. 99, no. 6, pp. 1028–1045, Jun. 2011.

[8] X.Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 809–818, Dec. 2011.

[9] K. Ren, S. Yu, W. Lou, and Y. Zhang, "PEACE: A novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 2, pp. 203–215, 2010.

[10] 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 Trans. Smart Grid, vol. 2, no. 4, pp. 796–808, Dec. 2011.

[11] J. Mišic and V. B. Mišic, "Wireless sensor networks for clinical information systems: A security perspective," in Proc. IEEE Int. Conf. Distrib. Comput. Syst. Workshops (ICDCS), Jul. 4, 2006.

[12] A. Prathapani, L. Santhananr, and P. D. Agrawal, "Intelligent honey pot agent for blackhole attack detection in wireless mesh networks," in Proc. IEEE 6th Int. Conf. Mobile Adhoc Sensor Syst. (MASS'09), pp. 753–758.

[13] B. He and S. D. P. Agrawal, "An identity-based authentication and key establishment scheme for multi-operator maintained wireless mesh networks," in Proc. IEEE 7th Int. Conf. Mobile Adhoc Sensor Syst (MASS), 2010, pp. 71–87.

[14] H. Gharavi and B. Hu, "Dynamic key refreshment for smart grid mesh network security," in Proc. IEEE PES Innov. Smart Grid Technol. (ISGT), 2013.

[15] "Efficient mesh security and link establishment," doc: IEEE 802.11-06/1470r3:, Nov. 2006.

[16] C. He and J. C. Mitchell, "Analysis of the 802.11i 4-way handshake," in Proc. 2004 ACM Workshop Wirel. Security (WiSe'04), pp. 43–50.

[17] Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control, IEEE Std. 802.1X-2004, Dec. 2004.

[18] 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, IEEE 802.11 Standard Working Group, 1999, 1st ed.

[19] Z. Bai and Y. Bai, "4-way handshake solutions to avoid denial of service attack in ultra wideband networks," in Proc. 3rd Int. Symp. Intell. Inf. Technol. Appl., Nov. 2009, vol. 3, pp. 232–235.

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

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

[22] R. C.Merkle, G. Brassard, Ed., "A certified digital signature (subtitle: That antique paper from 1979)," in Proc. CRYPTO 1989, Santa Barbara, CA, USA, 1990, vol. 435, Lecture Notes on Computer Science, pp. 218–238, Springer.

[23] M. S. Islam, Y. J.Yoon, M.A.Hamid, and C. S.Hong, "A secure hybrid wireless mesh protocol for 802.11s mesh network," in Proc. Int. Conf. Comput. Sci. Its Appl., Part I (ICCSA'08), pp. 972–985.

[24] L. Santhanam, B. Xie, and D. P. Agrawal, "Secure and efficient authentication in wireless mesh network using merkle trees," in Proc. Int. Conf. Comput. Sci. Its Appl., Part I (ICCSA'08), pp. 972–985.

[25] M. Szydlo, "Merkle tree traversal in log space and time," in Proc. Eurocrypt 2004, vol. 3027, Lecture Notes on Computer Science, pp. 541–554.

[26] B. Blanchet, "An automatic security protocol verifier based on resolution theorem proving (invited tutorial)," in Proc. 20th Int. Conf. Automated Deduction (CADE'05).

[27] A. Egners and U. Meyer, "Wireless mesh network security: State of affairs," in Proc. IEEE 35th Conf. Local Comput. Netw. (LCN), 2010, pp. 997–1004.