An Enhanced 4-way Handshake for the Neighborhood Area Networks in Smart Grid Systems

Tianhe Shen and Maode Ma

School of Electrical and Electronic Engineering
Nanyang Technological University

Abstract

A smart grid, a new generation of the power grid, has gradually revealed people in the contemporary society its unique advantages, not only in electric distribution, but also in power management. However, security of the smart grid is a gulf that needs to be surmounted before its widespread construction. In this paper, the communication architecture in the smart grid has been investigated to explore the vulnerability in the communication networks. One solution to enhance the security is designed and proposed to protect the system against malicious attacks. Finally, AVISPA is applied to prove the security of the enhanced protocol in smart grid.

Keywords–Smart grid; Neighborhood Area Networks (NANs); Wireless mesh network; IEEE 802.11s; AVISPA

1. Introduction

A smart grid has appeared as a new paradigm of the fast development of wireless technology. The newly developed power grid pushes the frontier of human's life much forward to a new area. Compared to the old power grid, the smart grid system combines information and communication technology with the conventional power distribution system to lower the customers power cost and provide more smart and efficient service. Besides, it tracks all of the electricity flows in the grid to help customers arrange the operating schedules reaching the most efficient power use plan.

The architecture of the communication networks in smart grid have been classified into Home Area Network (HAN), Neighborhood Area Network (NAN), and Wide Area Network (WAN). Due to the complex architecture of the communication networks in smart grid, the security vulnerabilities in the communication networks can be taken used by malicious attacks, which become the most primary threats to the smart grid system.

In order to prevent the various malicious attacks against the communication networks in smart grid, a security system is necessary. Particularly, in the NAN, because of its lack of infrastructure, the security requirement of the mesh network, which implements the NAN, has to be met by a distributed approach to authenticate the mesh points (MPs). This requirement can guarantee the authenticity of the incorporated nodes and the confidentiality of the transmission messages. There are a number of security protocols proposed for the mesh networks. The investigations of security requirements in mesh networks are presented in [1] and [2]. IEEE 802.11s standard [3] has been issued for mesh network included in the IEEE 802.11 wireless LAN networks. One of the most popular protocols in mesh network, simultaneous authentication of equals (SAE) scheme, is supported in this standard. By the SAE scheme, all nodes share the same password to authenticate each other and establish the secure communication channels. However, the security of the SAE scheme is threatened by the eavesdropping and disclosure of the password shared by the nodes. Once the password is known by an intruder, it is easy to be authenticated by other nodes and join the whole network. The confidentiality and integrity of the network cannot be guaranteed. Efficient mesh security association (EMSA) [4] is one of the existing mesh network security protocols using the mesh key hierarchy to establish secure communication channels between the gateway and the MPs in the mesh network. The EMSA scheme is proposed as an alternative mechanism for the SAE scheme.

In this paper, the vulnerability of the EMSA scheme has been explored. Furthermore, a new solution has been designed, named as Message Integrity Code

Embedding (MICE), to overcome the vulnerability with the security enhancement. At last, the security of the proposed protocol has been formally verified by using a protocol verification tool, Automated Validation of Internet Security Protocols and Applications (AVISPA) [5].

In the following, the vulnerability exploration will be presented in Section 2. In Section 3, the proposed MICE scheme will be described and a formal verification is implemented to prove the security of the enhanced protocol in Section 4. Conclusion will be made in the last section.

2. Vulnerability Exploration

Among the mesh secure communication protocols, the EMSA is an alternative mechanism for the SAE, which is supported in IEEE 802.11s standard. In EMSA, 4-way handshake process is one of the most important steps in the entire authentication process to provide authentication and establish the secure communication channels for the Supplicant side, and Authentication side in the mesh network.

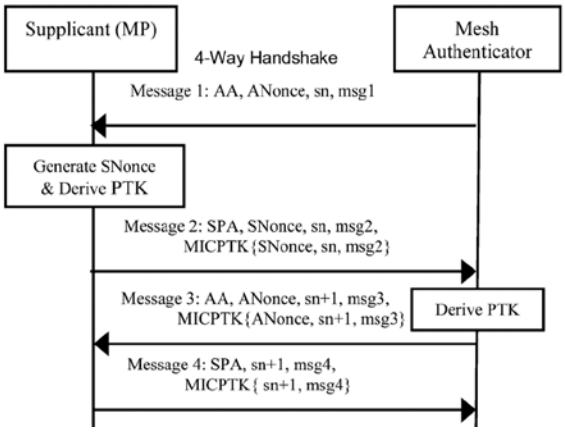

Figure 1 4-way Handshake Procedure

Fig. 1 describes the 4-way handshake procedures in the mesh networks. The two ends of 4-way handshake in the mesh network are the Supplicant, which are the numerous MPs in the network, and the Mesh Authenticator (MA). The MP and the MA starts the 4-way handshake after PMK is generated in the MP and received in the MA side. The MA initiates the 4-way handshake through sending a message containing its medium access control (MAC) address, a fresh random nonce it generated, sequence number, and the indicator of different message type. The MP could also send a request message to start the handshake. After the MP receives the message 1 sent from the MA, it will generate its own random nonce, namely SNonce, and then, derive the PTK. The PTK is calculated from its own PMK, MAC address, and SNonce, combined with the MAC address of the MA and the ANonce sent from the MA in message 1. After the MP generates the PTK, it will respond the MA through sending message 2. The Message Integrity Code (MIC), which is calculated from MP's nonce, sequence number, and indicator of message type with the fresh PTK, is inserted into message 2 to detect if the message is tempered by attackers. With the information including the MP's MAC address and the SNonce, now the MA is able to calculate the PTK. Once it derives the PTK, it sends message 3 to the MP. Then the MP will send message 4 back to acknowledge and close the handshake process. Both message 3 and 4 are protected by the MIC calculated from different information as shown in Fig. 1.

After the handshake procedure, the MP and the MA own their common shared PTK to use to encrypt the future transmission messages. A secure communication channel is then established. Further, the shared secret master key has never been transmitted on the network. The master key would always be keeping secure. After the 4-way handshake process, the MP itself can become a MA after the MKHSH process according to the EMSA protocol.

In the 4-way handshake procedure, since the message 1 is not encrypted, it can be easily tampered with by the attackers. After the MP receives message 1, it immediately has all the necessary information to construct the reply message. In the message 2, the MP calculates the MIC to encrypt the message. The MA would be able to detect the changes by attackers, if any. After that, both of message 3 and 4 are encrypted with the corresponding MICs to permit the MP and the MA to know whether the messages have been tampered with or not.

A vulnerability is found to exist due to the unprotected message 1, by which, an intruder is able to disrupt the 4-way handshake. To be specific, a one-message DoS attack can be performed as shown in Fig. 2. At the beginning of the 4-way handshake, the MA sends message 1 to the MP. Meanwhile, since the message is sending over the unsecure channel without encryption, the intruder would be easily to eavesdrop on this message and forge it.

After the MP receives the message 1, it will generate

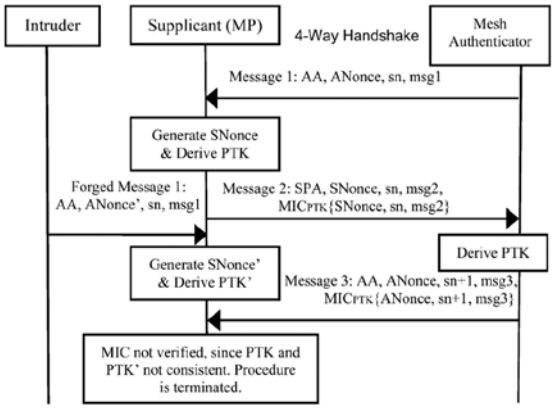

Fig. 2 A One-message DoS Attack

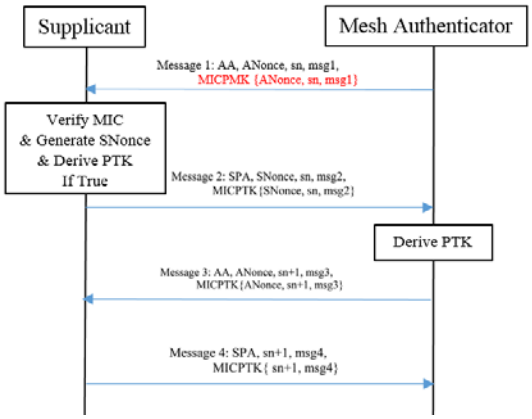

Fig. 3 MIC Inserted into Message 1

a nonce of its own and drives the PTK according to the information in message 1 from the MA. Then, it sends the reply message, message 2, to the MA. While the MP waits for the responds from the MA, it receives a forged message 1 sent from the intruder. The intruder has only changed the nonce in the original message 1. When the MP receives the forged message 1, it will initiate the process again, generate a new fresh nonce and calculate the PTK with the fake ANonce, the new SNonce, the PMK and both of the MAC addresses of the MP and the MA. Thus, the PTK will be different and the MP will store the new PTK and overwrite the old one, which is the same one calculated by the MA based on the message 2.

Now, once the MP obtains the message 3 sent by the MA, it will terminate the process since the PTKs are inconsistent and the MIC in message 3 cannot be verified. Thus, the intruder interrupts the handshake process successfully and the MP and the MA cannot authenticate each other's identities to generate the same PTK for the future transmission.

3. The Proposed Solution

In order to overcome the vulnerability and further to prevent the one-message DoS attacks, we propose a security enhanced 4-way handshake schemed of MICE. The principal idea of the proposed MICE scheme is to embed the MIC into the message 1 to make it protected. The MIC is a short piece of information generated by the cryptography to protect the authenticity and integrity of the sending message.

In the current 4-way handshake procedure, the MP and the MA have shared the same PMK through EAP authentication. Since PMK = PBKDF2 (passphrase, SSID, SSID length, 4096, 256) [6], it is entirely possible to concatenate PMK into a MIC.

The MA can embed a MIC into message 1 to prevent the intruder to forge message 1 and interrupt the process. As shown in Fig. 3, the MA calculates a MIC with ANonce, sn, msg 1 and the PMK. When the MP receives message 1, it could be able to calculate the MIC with using its PMK to verify whether the message has been tampered with or not. Since the intruder does not have the PMK, it cannot forge the message 1 and attack the process. But the receiver would be able to find out whether there is an intruder who has changed the content in the receiving message or not.

The intruder cannot interrupt the process through sending the fake message 1 to the MP. The MP and the MA can authenticate each other and generate the same PTK for future transmission.

4. Formal Verification

In order to formally verify the proposed MICE scheme, we have employed the formal verification tool of the AVISPA over a Linux platform. The AVISPA is an interactive, industrial-strength technology for the analysis of large-scale Internet security-sensitive protocols and applications. The AVISPA consists of four verification and automatic security analysis back-end servers including On−the−fly Model−Checker (OFMC), Constraint-Logic-based Attack Searcher (CL-AtSe), SAT-based Model-Checker (SATMC), and Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP). In this work, we have used both OFMC and CL-AtSe as the back-

end servers. The execution of the AVISPA can generate the results of the verification processes as shown in Fig. 4 and Fig. 5. The results tell that the proposed MICE scheme is logically correct without any major logical defect.

The execution results of AVISPA also show that the MICE is proved to be secure with the ability to prevent an attacker to launch a DoS attack. And the goals of 4-way handshake can be achieved. And all other expecting goals can be achieved. At the end of 4-way handshake, the MP and the MA could be able to authenticate each other's identities and communicate with each other by the new generated PTK. The potential vulnerability in message 1 has been removed by the proposed MICE scheme. The security of the 4-way handshake by the proposed MICE scheme has been verified.

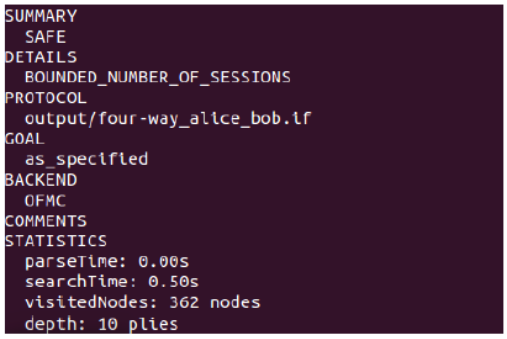

Fig. 4. AVISPA Results on the OFMC Back-end Server

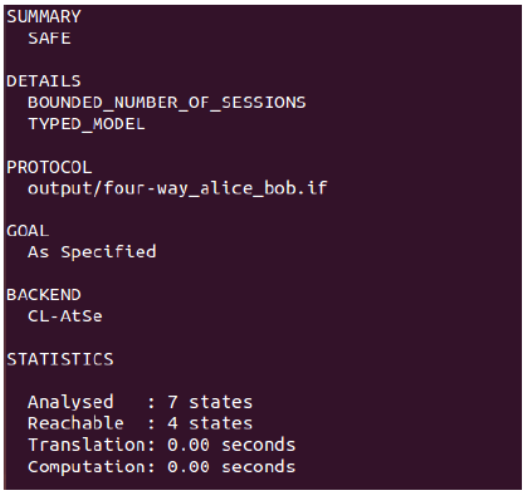

Fig. 5 AVISPA Results on the CL-AtSe Back-end

5. Conclusion

In this paper, we have explored the vulnerability in the 4-way handshake process for the wireless mesh network, which is the implementation of the NAN in smart grid. We have also discussed the impairments to the communication in the NAN when this vulnerability is taken use by an attacker to launch DoS attacks. To overcome this vulnerability, one possible solution of MICE has been proposed to prevent malicious attacks to harm the communication in the NAN. The security functionality of the proposed solutions has been formally verified by using the formal verification tool, AVISPA, to show that the proposed solution has the ability against DoS attacks.

References

[1] A. Prathapani, L. Santhananr, and P. D. Agrawal, "Intelligenthoneypot agent for blackhole attack detection in wireless mesh networks," *Proceedings of IEEE 6th International Conference of Mobile Ad hoc Sensor Systems, MASS'09*, pp. 753–758.

[2] B. He, and S. D. P. Agrawal, "An identity-based authentication and key establishment scheme for multi-operator maintained wireless mesh networks," *Proceedings of IEEE 7th International Conference of Mobile Ad hoc Sensor Systems, MASS'10*, pp. 71–87.

[3] 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, IEEE 802.11s Task Group*, November 2006.

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

[5] http://www.avispa-project.org/

[6] S. Blake-Wilson and A. Menezes, "Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol", *Public Key Cryptography*, Lecture Notes in Computer Science Vol. 1560, 1999, pp. 154-170.