Improved Security Architectures for Wireless Mesh Networks using Merkle Tree Handshaking

E. Fenil[1] A. Maria Merlyne[2]
[1,2]Department of Information Technology
[1]Assistant Professor
[1,2]Jeppiaar Engineering College

Abstract— *advanced communication architectures help for the success of the smart grid system. An advanced smart grid network should meet and satisfy the future demands of the electric systems in terms of reliability (able to rely on) and latency (existing but not yet developed). The latest wireless technology is a promising network in the field of communication in wide range area networks. It offers higher data rates, lower latency and larger coverage. However there are drawbacks found in the wireless communication. It does not provide security guarantee to the smart grid applications. Therefore, in this project, we propose a merkle-tree based hand shacking scheme, to overcome the disadvantage, which is capable of improving the reliability in terms of security of smart grid network.*

Keywords— Grid Network, Merkle Tree Handshaking, Wireless Mesh Networks

I. INTRODUCTION

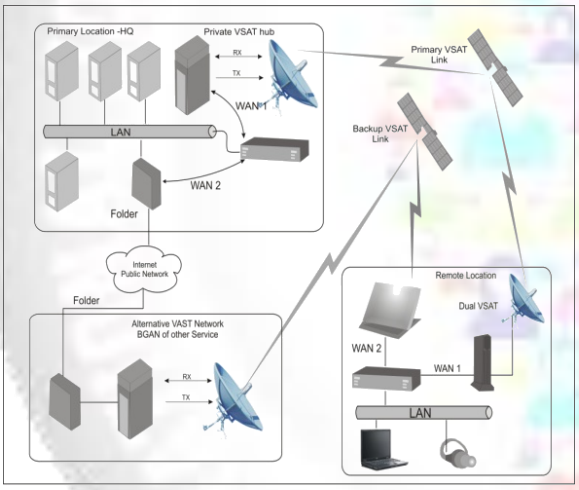

Fig. 1:

The wireless local area network simplifies the communication since the cable makes it complication. There are numerous networks made used. The main purpose of mesh network helps to overcome the limitations of the coverage. Therefore, mesh network considered to be one of the best medium of communication, since it is utilized wireless communication. Packet scheduling and multichannel frequency used to solve bottle neck problem (in the context of wireless communication, the flow of data between nodes or storage fabric designs are impaired or stopped entirely. It can be temporary or permanent until the rectification takes place). The main advantage of WLAN is wireless. It is highly effective for the communication. There is a wide range of coverage without observed communication due to the fact that the wire complicates the communication. Mesh networks has similar benefits such as self-configuration, installation, stability and self-healing. Due to the fact of various benefits the major drawback is "cyber-attack" (it is an offensive maneuver. It is done voluntarily by an individual or by a firm. It is stealing or alters the contents or destroys whole contents. It is serious crime in the field of communication). So it is a demanding and tiresome task of mesh communication.

The major advantage of this network is, it offers a cost effective solution when compared with other wired or wireless options. There are 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. Network vulnerability is made used to counter attack the cyber-attack. Simultaneous Authentication of Equals (SAE) allows having a single password for all the nodes. It provides safety against eavesdropping (listening to the voice messages without the sender's or receiver's knowledge).

Added to SAE, the Efficient Mesh Security Association (EMSA) comes in handy for the same purpose, to establish link security between nodes or MPs. WLAN technologies may be considered as a viable option in the absence of any wired or wireless communication, their mesh extension to the other substation would require thorough investigation with respect to lasting hour of communication and reliability. Security of mesh/sensor networks has been a challenging issue in wireless communications. It does not provide complete security and so, it is liable to eavesdropping. To overcome the thread, there is suggested periodic key refreshment and distribution strategy to protect it. In spite of the periodic key refreshment messages 1 and message 3 remain vulnerable to DoS attack. We shall look into it in the later pages about the preventing from the attacks.

Therefore, the main study or work of this paper is to provide or to develop an efficient 4-way handshaking protection scheme which enables mesh networks a complete firewall against all odds in wireless communication. The organization of the paper:

- Part I: Introduction
- Part II: Birds eye view of SAE and EMSA
- Part III: The implementation of SAE and EMSA
- with key refreshment strategy
- Part IV: 4-way handshaking communication against (DoS). It includes merkle tree and one way hashing for 4-way handshaking effective communication.
- Part V: The end results.

II. MESH SECURITY SYSTEMS

The core advantage of MSS is confidentiality and authenticity of data. It prevents the black hole attacker to hack the data's. MSS is capable of dynamically changing

the key information periodically or in a situation where an active attack has been detected. EMSA for Multigate Networks: The main function of EMSA is the establishment of link security between two MPs. It allows the multiple gateways for every node to access separate path ways. Hybrid wireless mesh protocol is used to implement the network master gateway is the mesh authenticator and key distributor the master gateway is responsible for creating mesh key hierarchy to all the mesh pints. The EMSA becomes the secondary mesh authenticator, due to link establishment.

Hybrid wireless mesh protocol is used to implement the network for EMSA. These are connected wirelessly to the backbone network. The EMSA is capable of producing value. The value is being carried out by MP to MA with security and establishing mesh key hierarchy for securing future link. It contains wireless communication exchange between MP and MA. The additional or supporting MP should receive response frame for establishing link security. The master gateway is the mesh authenticator. The master gateway is responsible for creating and distributing to the local gateways and to its branches. Therefore, the master gateway is responsible to store all the data's as well as distribution at the appropriate time.

Each and every node has link with master gateway. The link leads to authentication of nodes to protect from fake attack. The verified messages are authenticated in authentication server. The successful initial authentication enables PTK (Pair wise Transient Key) for unicast and GTK (Group Transient key) for multicast communication. Domain identifier vale (MKDD-ID) is received from MKD. MP forwards the first security association with MA in order to establish mesh key hierarchy for future safety link. It leads to safe communication between MP and MA.

Based on the security service, a supplicant MP issues connection through Peer Link Open IE to MKDD-IE to establish a continuous mesh key hierarchy Therefore, the MP develops subsequent connection with all the nods. It requires master gateway authentication so as to safeguard the communication. The PTK-KD (Pair wise Transient key for key distribution) becomes a key by which the suppliant MP becomes an authenticator. It is used for all mesh communication when supplicant becomes the authenticator. In this process, the master gateway through the Association Request and Association Response frames establishes link with supplicant master gateways. The secure link guarantees for the master gateway to begin the authentication process between MP and MA. It gives the safety from the cyber-attack. Based on the successful authentication, the master gateway and a supplicant gateway will initiate 4-way handshaking.

The subsequent authentication is initiated by authenticated supplicant. The authentication was completed by an MP than the peer link establishment takes place. The subsequent authentication has a value PMK-MKD name for authenticating the initially generated in EMSA.

They should have corresponding PMK-MA keys, if not, will retrieve the key from MKD for 4-way handshake communication. The same will continue until the source link establishes between the routing trees.

A. SAE for Multiage Networks

SAE for Multigate networks involves MPs for authentication of device. There are MP-A and MPB. MP-A and MP-B can initiate SAE protocols simultaneously. There is an authentication server involved in SAE. Shared password and MAC address will generate PWE. Rand and Mask are used to complete the SAE authentication. This will result in 4-way handshake communication. As mentioned earlier the MPs main task is to be SAE authenticator. It is negotiated with generated MK and GTK.

III. PERIODIC KEY REFRESHMENT STRATEGY

All the soft wares which are used in the wireless communications will be updated at regular intervals. The updating of the keys is done with the help of EAP and SAE. The life time PMKMKD should be less than the MSK life time. Therefore, it will be updated without fail or without any further delay. The PMK-MA should be similar to PMK-MKD. Once, the life time expires the key and their pats deletes by itself. There is no further life span or function of the keys. It is also similar situation with other keys. The keys are bound expire at the appointed time, therefore, keys are required to update periodically. The PMK-R0, PMK-R1 are not life time but carry out the safety work for the appropriate period of time. The validity expires with the function of the keys. It should be updated at an appropriate time in order to protect from cyber-attack also for the smooth running of the communication without any interruption.

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 will guarantee successful communication. EMSA and SAE keys have long lasting life time duration. The key materials should be updated periodically or else it leads to other complications especially to cyber-attacks. All the keys of EMSA and SAE are termed for life time but due to lack of maintenance becomes more vulnerable to cyber-attack. Therefore, to avoid the loss data or communication the periodic key refreshment is recommended for wireless communication without interrupting the communication. This is done automatically without any personal or external intervention. The periodic key refreshment clearly explained through respective diagrams.

IV. SECURITY IMPROVED 4-WAY HANDSHAKING

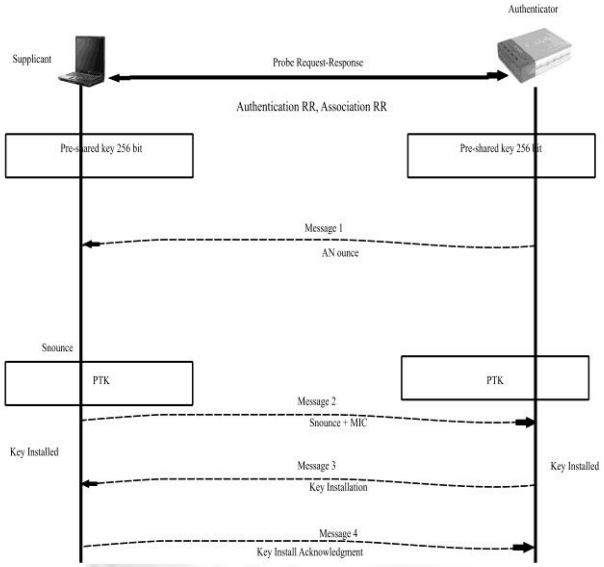

Fig. 2:

4-way handshaking is powerful means of communication. It requires complete protection from fake messages and cyber-attacks. To protect PTK is vitally important because of the heavy importance; it is also prone to hardest attack from all corners. The attack is from DoS; it can destroy MAC addresses, eavesdrop, and forge received messages, in 4-way handshaking communication. Protecting the confidentiality and integrity of data packet exchanges would require designing a highly reliable association and authentication processes in order prevent an adversary to originate fake messages that can interrupt the network during the 4-way handshaking process.

How can we prevent from DoS attack?

Message Integrity Code (MIC) is presented as solution for DoS attack. It is also viable to tampering the messages. Added to MIC, two temporary PTs and one PTK supplicant is necessary to prevent the messages. There is possibility of tampering the reply messages. There is a possibility of tampering the reply messages as well. Therefore, the PTK is generated to prevent the cyber-attacks on reply message. TPTKS and PTKs become necessary tool to complete the 4-way handshaking with legitimate authenticator, to prevent from huge DoS fake attackers. To protect DoS attack, is to store two temporary PTKs, and one PTK in supplicant where TPTK is updates when receiving message-1, while PTK is updated only upon receiving message- 3 with a valid MIC.

This way it would be possible to defeat the DoS attack once the MIC in message-3 is verified by the two TPTKs or PTK. The supplicant has to store all the received nonces, TPTKs and PTKs on order to complete the 4-way handshaking with a legitimate authenticator. 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. Robust Security Network Element (RSNE) becomes guardian of message 3. Since, message 3 is left out from protection. In this case, messages 1, 2, 3, and 4 are safely communicated without tampering. To avoid all attacks and confusions, the proposed solution is merkle-tree based hashing and single hash function. The above mentioned Solutions are employed to protect message 1 and message 3 from cyber-attack. The merkle tree is binary tree with leaf tokens and internal nodes. The merkle tree is m=2H leaf tokens. It is impossible to drive from root of the merkle tree U1234. MA has ANonce, sn, meg1 and PMK as leaf tokens to drive the root U1234. This complicated task of leaf tokens, the intruder finds difficult to reach the root U1234. Merkle tree on way hash function makes it hard for fake or cyber-attack. A pair of synchronized counters has been suggested in to avoid replay attacks. The design and implementation of the synchronized counters, at the expense of increasing overhead, is problematic especially in wireless environments. The most reliable solutions, we propose a merkle- tree based hashing, as well as a single hash function scheme. We apply both to protect message- 1 and message-3. The MA can use one way hash function such as SHA-1 and SHA-2.

However in our implementation we apply SHA-1 to construct secure authentication. Merkle tree is a binary tree consisting of a set of leaf tokens and internal nodes, each of which is the hash of the concatenation of its left and right children nodes. U12=hash (U1//U2 and U1=hash (V1), where // represents the concatenation of two strings. A merkle tree with a height of H has a set of m=2h leaf tokens. More importantly, to prevent further attacks the same merkle tree will not be made used. Instantly MS constructs new or second merkle tree for with m=2H which is referred as φ. For the new message and reply MA will identify authentication tokens corresponding authentication path. The identification takes place between computed root with stored or generated root φ. The identification takes place to prevent any further attacks. Therefore, the merkle trees are able to efficiently store and provide multiple one time authentication tokens to a single root. To prevent any further replay attacks this merkle tree will not be used again. Any situation where 4-way handshaking may have to be executed again, the MA constructs the second merkle tree with m=2h random authentication tokens by recursively computing the root, which is referred to as f in this case. With the help of the second merkle tree the MA then encrypts root f with the PMK information and sends it to the supplicant via message-3 of the first 4-way handshaking.

Merkle trees are able to efficiently store and provide multiple one time authentication tokens to a single root. This will effectively prevent any potential replay attacks. A merkle tree with authentication tokens requires to space and of computational effort. For message 3, AA RSNE made used to protect it. ANOnce, sn + 1, AA RSNE and PMK as leaf tokens to derive a root V1234. The supplicant receives the message 3 and the authentication takes place. Without the PMK information, there is no possibility of cyber-attack. And so, the subsequent takes place with new or generated merkle tree. It provides protection and safety to the message 3. PMK information plays the vital important to protect the message 1, message 3, so also, it is difficult to reach the merkle tree root. Since, the root changes at the new generation of it. The intruder will find difficult to construct correct hashed value to reach the root in order to tamper the message. Once the supplicant receives the one way hashing secured message-1, it will use 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 for verification. Indeed, without the PMK information, the intruder is unable to derive the correct hashed value by using a new ANonce. As mentioned earlier, we have also considered a one way hashing scheme for message-3 to avoid DoS attacks. The MA uses ANonce, sn +1, AARSNE and PMK as input to derive a hashed value: hash and insert it in message-3. As soon as the supplicant receives message-3, it will first check and compare the hashed value before verifying AA RSNE. Again, the intruder is unable to construct a correct hashed value: hash by using a different AA RSNE within a relatively short time frame. The merkle tree has the flexibility to construct the second merkle tree, which we have also considered to further enhance the reliability against reply attacks.

A. Protocol Verification

Proverify is made used to analyze the flaw of the four way handshaking process. Key refreshment strategy at the periodical updates can lessen or prevent the other attacks from the intruder.

B. Binary Exponential Backoff

It helps the datas to be secure in the face of solid collusion. It helps the datas to be stored back in the foundational station from which it is originated. Binary exponential back off is used to transmit the datas in a safer mode so that, it will not cause damage to its originality. Exponential Backoff is an algorithm that uses feedback to multiplicatively decrease the rate of some process in order to gradually find an acceptable rate. The main purpose of using the binary exponential backoff algorithm is for congestion avoidance in or during the data transmission between the nodes or substations of the communication in the wireless security system.

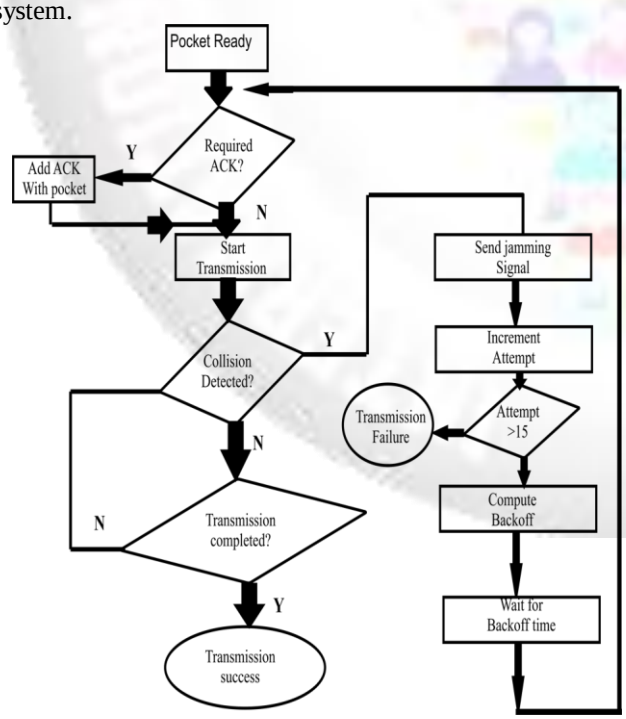

Fig. 3:

If a collision is detected during transmission of a packet, the master gateway and the substations immediately ceases transmission. It transmits jamming signal for all the stations so that, it will not cause further damage or collusion in the transmission of the datas. Brief duration is required to ensure that all stations know that collision has occurred and to reassume the signals or transmission between different stations. After transmitting the jamming signal, the node waits for a quit lot of amount of time and then transmission is resumed. This is to reassure that the data are exchanged safely without any delay or damage to them. The main purpose of using the binary exponential backoff is to achieve stability in the back off scheme. A node will try to attempt to transmit datas repeatedly in the face of repeated collisions which occurred in the process of communication. But after each collision, the mean value of the random delay, is doubled. After every 15 retries (excluding the original try), the unlucky packet is discarded and the node reports an error.

V. CONCLUSION

Evaluation of different authentication schemes for Multigate mesh network. There was a periodic key refreshment strategy to protect from intruder. Introduction of merkle tree for authentication and for safe reply of messages. Proverify is sign of protocol verification pros and cons of EMSA and SAE presented in a gist manner. Finally, the merkle tree based authentication scheme for both protocols.

REFERENCES

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

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

[3] Z. Bai and Y. Bal, "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.

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

[5] 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. "Efficient mesh security and link establishment," doc: IEEE 802. 11-06/1470r3:, Nov. 2006.

[6] 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