Secure, Intuitive and Low-Cost Device Authentication for Smart Grid Networks

Erman Ayday
School of Electrical and Comp. Eng.
Georgia Institute of Technology
Atlanta, GA 30332, USA
eayday@gatech.edu

Sridhar Rajagopal
Samsung Telecommunications America
1301 East Lookout Dr.
Richardson, TX 75082, USA
srajagop@sta.samsung.com

***Abstract*- Security concerns about the Smart Grid are becoming more prevalent as the deployment of grid becomes more widespread. In this paper, we propose secure and intuitive device authentication techniques for the Smart Grid enabled Home Area Networks (HANs). We assume a distributed architecture for the HAN which consists of the smart appliances, the smart meter and the gateway. In this architecture, the operating schedules of the appliances are controlled by the gateway based on the pricing and control messages from the smart meter. We propose three different authentication mechanisms for devices in the HAN: 1) between the gateway and the smart meter, 2) between the smart appliances and the HAN, and 3) between the transient devices and the HAN. We show that the adversarial behavior during the authentication of devices such as the man-in-the-middle and impersonation attacks are prevented using the proposed device authentication mechanisms by extensive use of collaboration between different parties. Eventually, we provide secure and intuitive device authentication mechanisms (that require minimum or no user effort) for various parts of the HAN with low computation and communication overheads.**

I. Introduction

A Smart Grid is an intelligent monitoring system which delivers electricity from suppliers to consumers and keeps track of all electricity flowing in the system by overlaying the electricity distribution grid with an information and net metering system. It organizes the operating schedules of the appliances so that the consumers use their most power consuming appliances when the power is least expensive, and similarly these appliances are turned off during the peak times.

The Smart Grid is formed by many sub-networks such as the Home Area Network (HAN), service providers, transmission, distribution, bulk generation, operations and market. In this paper, we focus on the HAN part of the Smart Grid with a distributed architecture which consists of the smart appliances, the smart meter, the gateway and a user interface (UI) which is either directly or remotely (via the Internet) connected to the gateway. In this architecture (illustrated in Fig. 1), smart appliances (SAs) directly communicate (wirelessly) with the gateway and they either directly or indirectly (via the gateway) communicate with the smart meter (SM) using a HAN protocol such as Zigbee [1]. Further, operating schedules of the SAs are controlled by the gateway based on the pricing and control messages from the SM. User can manually control the operating schedules of the SAs anytime using a physical UI or a web application.

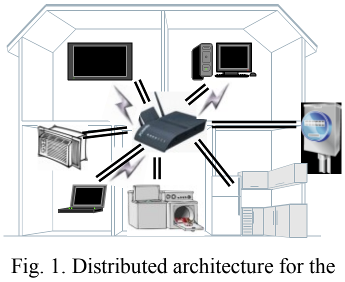

Fig. 1. Distributed architecture for the HAN.

The task of providing security services for the Smart Grid is not trivial due to its large scale deployment, the legacy devices, scattered field devices, and its heterogeneous architecture [2]. An attacker may launch a wide range of attacks including man-in-the-middle (MITM), impersonation, eavesdropping, message forgery, packet dropping, and noise injection. Impacts of these attacks can be as serious as blackouts.

In this work, we focus on device authentication for the HAN part of the Smart Grid. Even though there are also other crucial security requirements for the Smart Grid such as privacy, message authentication, data integrity and data availability, they all require securely authenticated devices as a basis. Further, the HAN is the only part of the grid for which the Utility has no direct control. Therefore, it is the most vulnerable part of the Smart Grid.

Device authentication for the HAN has its own particular challenges. During the authentication between the SM and the gateway or between the SAs and the HAN, the attacker can take control of the gateway or SAs by initiating a man-in-the middle (MITM) attack. Similarly, during the authentication between the transient devices (such as plug-in hybrid electric vehicles - PHEVs) and the HAN, the attacker can initiate an impersonation attack and cause the victim to be overcharged in his electric bill. All these security problems can be addressed by using secure device authentication mechanisms that are resilient to the aforementioned attacks.

Our main goal is to develop secure authentication mechanisms that will be resilient to aforementioned attacks. Further, we propose intuitive authentication mechanisms, so that a high level of security can be provided in every HAN independent of user effort. We note that a security mechanism is only as strong as its weakest link. Therefore, counting on the user effort for the strength of a security mechanism indeed introduces more vulnerability to the scheme since not all the users will be able to follow the security procedures properly. Even if a single user fails to follow the security procedures, the attacker can use that weak link to get into the system and might threaten all the other users (even if they followed the procedures properly).

The main contributions of this work are summarized in the following.

- We propose three different authentication mechanisms between the devices in the HAN: 1) between the gateway and the SM, 2) between the SAs and the HAN, and 3) between the transient devices and the HAN.
- The proposed device authentication algorithms are resilient against insider attackers performing serious attacks such as

MITM or impersonation during the authentications of the devices.

- Proposed authentication algorithms are intuitive and require no user effort.
- The proposed algorithms have low computational and communication overheads. Therefore they are applicable for a typical Smart Grid network that includes millions of appliances with limited computational power and memory.

A. Related Work

Currently the most popular HAN protocol Zigbee [1] proposes five potential device authentication schemes for the devices in the HAN. However, the proposed schemes either need user effort to provide security or they are impractical for a typical Smart Grid enabled HAN. The other popular HAN protocol, Wi-Fi, introduced Wi-Fi protected setup [3] for the secure establishment of the HAN. Wi-Fi protected setup offers four choices for the customer to add a new device to the HAN. However, these methods are either not secure (require user effort, and hence, reveal secret material to users or subject to MITM attack) or not practical for a typical Smart Grid enabled HAN. Another HAN protocol INSTEON [4] utilizes device authentication either by pressing the buttons of devices (which is vulnerable to MITM attack) or by sending special messages including device IDs which are written on the devices (and hence, vulnerable to attacks). Different from INSTEON, in the Z-Wave protocol [5] each home has a unique home ID and the privacy of communication within each home is provided by using this unique ID. Therefore, it is likely that the attacker can compromise any home by just capturing its unique ID.

Several technical works in the literature have focused on securing Smart Grid networks in general. In [6-8] the security challenges of Smart Grid networks are discussed and identified. [9] proposed using public key infrastructure (PKI) and trusted computing for the security of Smart Grid enabled HANs. However, we do not foresee that all the appliances in the HAN will have a strong processor to perform PKI operations [10]. In [11], authors addressed the impact of the blackhole attack on data availability during the multi-hop routing between the SMs and the Utility. [12] introduced a policy based encryption system for the data sharing problem in the electric grids. Further, in [13], authors proposed a conceptual layered framework for protection of the Power Grid automation systems against cyber attacks. Finally, [14] discussed the strategy for security checks and authentications for command requests of operations in the host area electric power system (AEPS) and in the interconnecting AEPSs. Different from the existing work, in this work we develop secure, intuitive and low-cost device authentication mechanisms for the Smart Grid enabled HANs.

II. Secure Device Authentication Mechanisms For Smart Grid Enabled Home Area Networks

A typical Smart Grid network may include millions of devices which should be globally reachable to control the network, and hence, they all should have unique IDs [1]. Therefore, we assume that IPv6 is used and every device has a unique IP address (which can also be represented as the unique ID of every device). Indeed, it is also stated in [15] that IPv6 will enable new revenue-yielding service opportunities such as Smart Grid networks.

We further assume that all devices in the HAN (SAs, SM and the gateway) are able to perform symmetric key encryption and decryption[1] to provide confidentiality during the device authentication process. Further, every device shares a pair-wise key with the center of trust (cloud or Utility). Therefore, the confidentiality of all messages between the gateway, the SM, the SA and the cloud are cryptographically provided using these pair-wise keys. Furthermore, all messages include a message authentication code (MAC) to provide message integrity. Finally, we assume that the gateway is connected to the cloud (the trust center which is the Utility in our case) via the Internet, land line a cell phone or the Advanced Metering Infrastructure (AMI). To facilitate future references, we listed the frequently used notations and cryptographic tools in Table 1.

TABLE 1
NOTATIONS AND CRYPTOGRAPHIC TOOLS.

ID_G	Unique ID of the gateway (IP_G, unique IP of the gateway, can be used as its ID).
ID_M	Unique ID of the SM (IP_M, unique IP of the SM, can be used as its ID).
ID_A	Unique ID of the SA (IP_A, unique IP of the SA, can be used as its ID).
ID_T	Unique ID of the transient device - TD (IP_T, unique IP of the TD, can be used as its ID).
$K_{G,U}$	Pair-wise key between the gateway and the Utility.
$K_{M,U}$	Pair-wise key between the SM and the Utility.
$K_{A,U}$	Pair-wise key between the SA and the Utility.
$K_{T,U}$	Pair-wise key between the TD and the Utility.
$K_{G,M}$	Pair-wise key between the gateway and the SM.
$K_{A,G}$	Pair-wise key between the SA and the gateway.
$K_{A,M}$	Pair-wise key between the SA and the SM.
$K_{T,G}$	Pair-wise key between the TD and the gateway.
$K_{T,M}$	Pair-wise key between the TD and the SM..
$E_{Ki,j}(X)$	Symmetric encryption algorithm using the pair-wise key between i and j.
$MAC(K_{i,j}, X)$	Message Authentication Code (MAC) algorithm using the pair-wise key between i and j.

A. Authentication between the gateway and the smart meter

Since manufacturers or the Utility have no physical control on the devices in consumers' homes, a compromised gateway may give serious damages to the network by initiating a MITM attack during the authentication of a legitimate gateway to a legitimate SM. After a successful attack, the attacker can send incorrect pricing/control messages to the legitimate gateway and cause serious problems such as blackouts by shutting down all the appliances. Moreover, the power demand can be dramatically reduced and increased by using compromised meters. Therefore, we propose a secure and intuitive authentication mechanism that is resilient to MITM attacks. The steps of the proposed authentication process are illustrated in Fig. 2.

The gateway and the SM exchange authentication request and acknowledgement messages between each other to initiate the process. Then, they both send an authentication request message to the trust center (cloud/Utility). Once the cloud receives the authentication requests from both devices, it maps the ID of the SM (ID_M) to its location from its database (the cloud can map the ID of a SM to its actual location due to billing issues).

[1] Use of Advanced Encryption Scheme (AES) with at least 128-bits long keys is recommended and enabled by Zigbee [1].

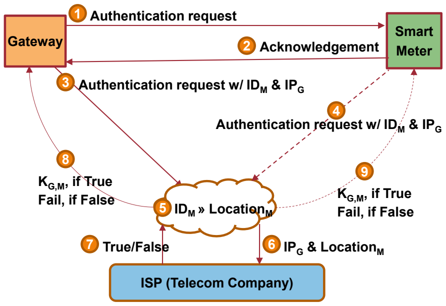

Fig. 2 Authentication mechanism between the gateway and the SM.

The cloud should make sure that it authenticates the correct gateway to the correct SM. Hence, we propose to collaborate with the 3rd party service providers such as ISPs or telecommunication companies (depending on the type of gateway-cloud connection) to pair the gateway and the SM based on their locations. If the gateway is connected to the cloud via the Internet (the land line, a cell phone or the AMI), the ISP (telecommunication company) will be able to identify its location from its unique IP (from the calling number). Assuming the gateway-cloud connection is via the Internet, the cloud forwards the IP of the gateway (IP_G) along with the location of the SM to the ISP. The ISP processes these two inputs and sends a "True" message if the location of the gateway matches the SM's location. Otherwise, a "False" message is sent back to the cloud which causes the process to be terminated. If the cloud receives a "True" message from the ISP, it pairs the gateway with the SM, creates a pair-wise key between them ($K_{G,M}$) and sends the following message to the gateway.

$$\left\{\begin{array}{l} \mathrm{E}_{\mathrm{K_{G,U}}}(K_{G,M}, ID_M), \\ \mathrm{MAC}(\mathrm{K_{G,U}}, \mathrm{E}_{\mathrm{K_{G,U}}}(K_{G,M}, ID_M)), \mathrm{IP}_G \end{array}\right\} \qquad (1)$$

Similarly, the cloud sends the following message to the SM.

$$\left\{\begin{array}{l} \mathrm{E}_{\mathrm{K_{M,U}}}(K_{G,M}, ID_G), \\ \mathrm{MAC}(\mathrm{K_{M,U}}, \mathrm{E}_{\mathrm{K_{M,U}}}(K_{G,M}, ID_G)), \mathrm{ID}_M \end{array}\right\} \qquad (2)$$

After the gateway and the SM authenticate (1) and (2), they both decrypt the encrypted parts using the keys they share with the cloud to obtain the pair-wise keys that they will use to create a secure channel between each other. Once they establish the secure channel, they can securely negotiate on a key exchange protocol between each other.

The proposed authentication mechanism is resilient to MITM attacks, as the attacker cannot forge a gateway with IP address pointing the user's actual location. The attacker may initiate a MITM attack using a compromised gateway; however, this attack will fail during the verification at the 3rd party service provider. We note that IP spoofing is not possible during the authentication of the gateway to the SM since all the messages between the gateway and the cloud are encrypted by the pair-wise key between them ($K_{G,U}$). Therefore, even if an attacker spoofs the IP of the actual gateway (which is located in the home), he cannot generate the messages encrypted by the correct key.

B. *Authentication between the Smart Appliances and the HAN*

Since the SA has no direct connection to the cloud, it has to communicate with the gateway or the SM during the authentication process (communication between the SA and the SM can be either direct or via the gateway). If the SA is authenticated to the HAN via the gateway, the MITM attack is a potential threat. A compromised gateway-SA pair may give serious damages to the network by initiating a MITM attack during the authentication of the SAs to the HAN. After a successful attack, the attacker can send incorrect control messages to the SA and incorrect sensor readings to the gateway, affecting the operating schedules of the appliances and causing wrong alarms at the gateway. Therefore, we propose to use a collaborative authentication (by using the collaboration of the SM and the gateway) model to combat the attacker. The steps of this authentication process are illustrated in Fig. 3.

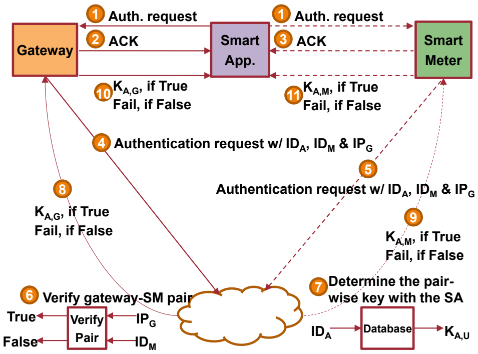

Fig. 3. Authentication mechanism between the SA and the HAN.

We assume that the SM and the gateway are already authenticated to each other (and the cloud) by using the mechanism described in Section II.A. After the initial authentication request-ACK exchange between the SA, the SM and the gateway, both the gateway and the SM send authentication requests (for the SA) to the cloud. The cloud verifies that the messages are coming from a paired gateway and SM (as discussed in Section II.A). If the messages are not coming from a valid gateway-SM pair, the cloud terminates the authentication process by sending "Fail" messages to the parties. Once the gateway-SM pair is verified, the cloud maps the ID of the SA (ID_A) to the pair-wise key ($K_{A,U}$) between the SA and the cloud (this key is used for end-to-end encryption between the cloud and the SA). Further, it creates two pair-wise keys between the gateway and the SA ($K_{A,G}$), and between the SM and the SA ($K_{A,M}$) for them to establish a secure channel between each other. Then, it sends the following message to the gateway.

$$\left\{\begin{array}{l} \mathrm{E}_{\mathrm{K_{G,U}}}\left\langle\begin{array}{l} \mathrm{E}_{\mathrm{K_{A,U}}}(K_{A,G}, ID_G), \mathrm{MAC}(\mathrm{K_{A,U}}, \\ \mathrm{E}_{\mathrm{K_{A,U}}}(K_{A,G}, ID_G)), K_{A,G} \end{array}\right\rangle, \\ \mathrm{MAC}(\mathrm{K_{G,U}}, \mathrm{E}_{\mathrm{K_{G,U}}}\left\langle\begin{array}{l} \mathrm{E}_{\mathrm{K_{A,U}}}(K_{A,G}, ID_G), \\ \mathrm{MAC}(\mathrm{K_{A,U}}, \\ \mathrm{E}_{\mathrm{K_{A,U}}}(K_{A,G}, ID_G)), K_{A,G} \end{array}\right\rangle), \mathrm{IP}_G \end{array}\right\} \qquad (3)$$

Similarly, the cloud sends the following message to the SM.

$$\left\{\begin{array}{l} \mathrm{E}_{\mathrm{K_{M,U}}}\left\langle\begin{array}{l} \mathrm{E}_{\mathrm{K_{A,U}}}(K_{A,M}, ID_M), \mathrm{MAC}(\mathrm{K_{A,U}}, \\ \mathrm{E}_{\mathrm{K_{A,U}}}(K_{A,M}, ID_M)), K_{A,M} \end{array}\right\rangle, \\ \mathrm{MAC}(\mathrm{K_{M,U}}, \mathrm{E}_{\mathrm{K_{M,U}}}\left\langle\begin{array}{l} \mathrm{E}_{\mathrm{K_{A,U}}}(K_{A,M}, ID_M), \\ \mathrm{MAC}(\mathrm{K_{A,U}}, \\ \mathrm{E}_{\mathrm{K_{A,U}}}(K_{A,M}, ID_M)), K_{A,M} \end{array}\right\rangle), \mathrm{ID}_M \end{array}\right\} \qquad (4)$$

After the gateway and the SM authenticate (3) and (4), they both decrypt the encrypted parts using the keys they share with the cloud to obtain the pair-wise keys that they will use to create a secure channel between the SA. We note that neither the gateway not the SM can decrypt the parts of (3) and (4) which are encrypted by the pair-wise key between the cloud and the SA ($K_{A,U}$). Further, they cannot modify these encrypted parts without being detected due to the attached MACs (which are created using $K_{A,U}$). Therefore, the gateway sends the following message to the SA.

$$\left\{\begin{aligned} &\mathrm{E}_{\mathrm{K_{A,U}}}(K_{A,G}, ID_G), \\ &\mathrm{MAC}(\mathrm{K_{A,U}}, \mathrm{E}_{\mathrm{K_{A,U}}}(K_{A,G}, ID_G)), \mathrm{ID}_A, \mathrm{ID}_G \end{aligned}\right\} \tag{5}$$

Likewise, the SM sends the following message to the SA.

$$\left\{\begin{aligned} &\mathrm{E}_{\mathrm{K_{A,U}}}(K_{A,M}, ID_M), \\ &\mathrm{MAC}(\mathrm{K_{A,U}}, \mathrm{E}_{\mathrm{K_{A,U}}}(K_{A,M}, ID_M)), \mathrm{ID}_A, \mathrm{ID}_M \end{aligned}\right\} \tag{6}$$

SA initially verifies the integrity of (5) and (6). Then, it decrypts the encrypted parts using the pair-wise key it shares with the cloud. Therefore, the SA authenticates the gateway and the SM, and it also obtains the pair-wise keys generated by the cloud. Once the SA establishes a secure channel with the gateway and the SM (using $K_{A,G}$ and $K_{A,M}$), it can securely negotiate on a key exchange protocol with them.

Assuming an insider attacker cannot utilize a legitimate SM-gateway pair while attacking (as it is not a practical attack scenario due to the limitations of the SMs); the proposed authentication mechanism is resilient to MITM attacks since the cloud does not verify the process that is not initiated by a paired gateway-SM pair. Therefore, even if the attacker tries to initiate a MITM attack, he will fail during the verification of the SM-gateway pair at the cloud and the authentication attempt will be terminated by the cloud.

C. Authentication between the Transient Devices and the HAN

The best example for a transient device (TD) is a PHEV which can be charged either at user's own HAN (referred to as the home HAN including home gateway) or at a visiting location (visiting HAN). TDs such as PHEVs consume high power while being charged. Therefore, when they are used at a visiting HAN, the power usage is billed to the user. Hence, device impersonation attack becomes a critical challenge. By impersonating a transient device, the attacker may have his own power usage billed to another (victim) user (actual owner of the impersonated device). Therefore, the cloud should make sure that the TD is not being impersonated before it verifies the authentication process between the TD and the visiting HAN.

We assume that the TD can communicate with its home gateway anytime (even when it is mobile). The steps of the authentication process are shown in Fig. 4.

TD initiates the authentication process by sending the following authentication request to the visiting gateway and the visiting SM.

$$\left\{\mathrm{Auth\ Req}, \mathrm{ID}_T, \mathrm{ID}_M^T, \mathrm{M}\right\} \tag{7}$$

where

$$\mathrm{M} = \left\{\mathrm{E}_{\mathrm{K_{TU}}}(ID_T, Seq.No), \mathrm{MAC}(\mathrm{K_{T,G}}, \mathrm{E}_{\mathrm{K_{T,G}}}(ID_T, Seq.No))\right\} \tag{8}$$

and *Seq. No* is the sequence number of the message between the TD and its home gateway. The TD notifies the visiting HAN that it is already authenticated to a HAN by including the ID of its home SM (ID^T_M) in the authentication request message. Moreover, the authentication request message of the TD also includes a part, M in (8), which is encrypted by the pair-wise key between the TD and its home gateway ($K_{T,G}$). This encrypted part is forwarded from the visiting HAN to the cloud and from the cloud to the home gateway for the verification of the home gateway. After learning that the TD is already authenticated to another HAN, the visiting gateway will give a manual entry option to the user about the duration of the authentication, and hence, the user manually enters the duration of the authentication (T) via the UI. After its authentication period is expired, the TD is automatically removed from the visiting HAN.

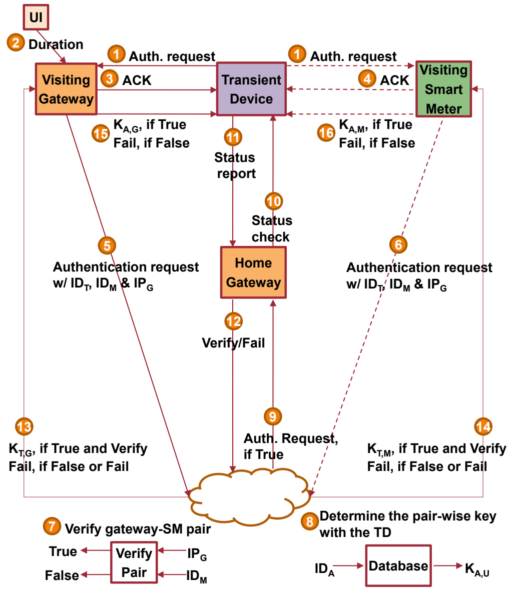

Fig. 4. Authentication mechanism between the TD and the HAN.

After responding to this authentication request by sending ACK messages, both the visiting gateway and the visiting SM send authentication requests (for the TD) to the cloud. The visiting gateway includes ID^T_M and T to the message so that the cloud can contact with the home HAN of the TD and also know how long the TD will be a part of the visiting HAN. The cloud verifies that the authentication request messages are coming from a paired gateway and SM (as discussed in Section II.B). If this verification fails, the cloud immediately sends a "Fail" message to the visiting HAN and terminates the process. Otherwise (if the verification succeeds), the cloud maps the ID of the TD (ID_T) to the pair-wise key ($K_{T,U}$) between the TD and the cloud and forwards the following part of the authentication request message (which is encrypted by the pair-wise key between the TD and its home gateway) to the home gateway of the TD to prevent the impersonation attacks.

$$\left\{\mathrm{E}_{\mathrm{K_{HG,U}}}(\mathrm{M}), \mathrm{MAC}(\mathrm{K_{HG,U}}, \mathrm{E}_{\mathrm{K_{HG,U}}}(\mathrm{M}))\right\} \tag{9}$$

where $K_{HG,U}$ is the pair-wise key between the home gateway of the TD and the cloud.

We propose using one-time keys between any TD and its home gateway (different pair-wise key at each session) to combat the impersonation attack. Therefore, the TD generates and uses a different pair-wise key whenever it communicates with its home gateway. Further, the generated key depends on the time of communication so that it becomes hard to predict future keys once the older keys are captured by the attacker. Further, the TD uses sequence numbered messages when it communicates with its home gateway as in (8). Therefore, even if the attacker captures the current pair-wise key between the TD and its home gateway (which will expire in the next communication session), he cannot predict the sequence number of the next message, and hence, will be detected if he sends a message to the home gateway with an incorrect sequence number.

Once the home gateway receives (9), it makes sure that the TD is indeed at the visiting HAN from which the cloud received the authentication request messages. The home gateway initially verifies that the message M sent by the TD via the MAC attached to it and the sequence number of the message. If either of these is incorrect, the home gateway terminates the process and sends a “Fail” message back to the cloud as a feedback (which will eventually terminate the authentication process). Otherwise (if both the message and the sequence number are verified), the home gateway sends a “status check” message to the TD to figure out if it is actually trying to authenticate with any particular visiting HAN[2].

If the TD sends a “status report” (as a response to the “status check” from its home gateway) and verifies its authentication attempt to the particular visiting HAN, then the home gateway sends a “Verify” message to the cloud. Otherwise, if the TD does not verify its authentication attempt, a “Fail” message is sent from the home gateway to the cloud. We note that by sending these status messages between the home gateway and the TD, the proposed mechanism can immediately detect and prevent the attacker even if he both captures the current pair-wise key between the TD and its home gateway, and guesses the sequence number of the next message correctly. If the cloud receives a “Fail” message from the home gateway, it immediately terminates the authentication process. Otherwise, if the home gateway sends a “Verify” message, it creates two pair-wise keys between the visiting gateway and the TD ($K_{T,G}$), and between the visiting SM and the TD ($K_{T,M}$). Next, the cloud sends the following message to the visiting gateway.

$$\left\{\begin{array}{l} \mathrm{E}_{\mathrm{K_{G,U}}}\left\langle\begin{array}{l} \mathrm{E}_{\mathrm{K_{T,U}}}(K_{T,G}, ID_G), \mathrm{MAC}(\mathrm{K_{T,U}}, \\ \mathrm{E}_{\mathrm{K_{T,U}}}(K_{T,G}, ID_G)), K_{T,G} \end{array}\right\rangle, \\ \mathrm{MAC}(\mathrm{K_{G,U}}, \mathrm{E}_{\mathrm{K_{G,U}}}\left\langle\begin{array}{l} \mathrm{E}_{\mathrm{K_{T,U}}}(K_{T,G}, ID_G), \\ \mathrm{MAC}(\mathrm{K_{T,U}}, \\ \mathrm{E}_{\mathrm{K_{T,U}}}(K_{T,G}, ID_G)), K_{T,G} \end{array}\right\rangle), \mathrm{IP}_G \end{array}\right\} \quad (10)$$

Similarly, the cloud sends the following message to the visiting SM.

$$\left\{\begin{array}{l} \mathrm{E}_{\mathrm{K_{M,U}}}\left\langle\begin{array}{l} \mathrm{E}_{\mathrm{K_{T,U}}}(K_{T,M}, ID_M), \mathrm{MAC}(\mathrm{K_{T,U}}, \\ \mathrm{E}_{\mathrm{K_{T,U}}}(K_{T,M}, ID_M)), K_{T,M} \end{array}\right\rangle, \\ \mathrm{MAC}(\mathrm{K_{M,U}}, \mathrm{E}_{\mathrm{K_{M,U}}}\left\langle\begin{array}{l} \mathrm{E}_{\mathrm{K_{T,U}}}(K_{T,M}, ID_M), \\ \mathrm{MAC}(\mathrm{K_{T,U}}, \\ \mathrm{E}_{\mathrm{K_{T,U}}}(K_{T,M}, ID_M)), K_{T,M} \end{array}\right\rangle), \mathrm{ID}_M \end{array}\right\} \quad (11)$$

The visiting gateway and the visiting SM both decrypt the encrypted parts of (10) and (11) using the keys they share with the cloud to obtain the pair-wise keys that they will use to create a secure channel between the TD. Then, the visiting gateway sends the following message to the TD.

$$\left\{\begin{array}{l} \mathrm{E}_{\mathrm{K_{T,U}}}(K_{T,G}, ID_G), \\ \mathrm{MAC}(\mathrm{K_{T,U}}, \mathrm{E}_{\mathrm{K_{T,U}}}(K_{T,G}, ID_G)), \mathrm{ID}_T, \mathrm{ID}_G \end{array}\right\} \quad (12)$$

Likewise, the visiting SM sends the following message to the TD.

$$\left\{\begin{array}{l} \mathrm{E}_{\mathrm{K_{T,U}}}(K_{T,M}, ID_M), \\ \mathrm{MAC}(\mathrm{K_{T,U}}, \mathrm{E}_{\mathrm{K_{T,U}}}(K_{T,M}, ID_M)), \mathrm{ID}_T, \mathrm{ID}_M \end{array}\right\} \quad (13)$$

The TD decrypts the encrypted parts using the pair-wise key it shares with the cloud. Therefore, the TD authenticates the visiting gateway and the visiting SM, and it also obtains the pair-wise keys generated by the cloud. Once the TD establishes a secure channel with the visiting gateway and the visiting SM (using $K_{T,G}$ and $K_{T,M}$), it can securely negotiate on a key exchange protocol with them.

The proposed mechanism is resilient against impersonation attacks. Even if the attacker impersonates a victim device, captures the current key between the victim and its home gateway, and guesses the sequence number of the next message correctly, he will be detected due to the status messages between the TD and its home gateway.

We note that the status messages between the TD and its home HAN is only possible with the assumption that the TD can communicate with its home gateway anytime. Assuming the TD does not have such a stable connection, even though it is not very likely, the attacker can capture the current pair-wise key and predict the sequence number of the next message. This type of an attack cannot be detected immediately; however, it will be detected when the TD is connected to a HAN (either its home HAN or a visiting HAN). The authentication mechanism for this case is the same as before, only with the exception of the status messages between the TD and its home gateway.

III. Conclusion

In this paper, we propose three secure and intuitive authentication mechanisms for the HAN part of the Smart Grid networks. We show that the proposed authentication mechanisms are resilient to adversarial behavior including MITM and impersonation attacks which cause serious damages to the grid. Further, the proposed mechanisms have low computation and communication overheads. Hence, they can be easily implemented to the devices in a typical HAN.

References

[1] Zigbee Alliance, “ZigBee smart energy profile™ 2.0 technical requirements document”, available online: http://www.zigbee.org.

[2] Cisco, “Securing the Smart Grid”, available online: http://www.ciscosystemsnetwork.net/web/strategy/docs/energy/SmartGridSecurity_wp.pdf, 2009.

[3] Wi-Fi Alliance, “Introducing Wi-Fi protected setup”, available online: http://www.wi-fi.org/wifi-protected-setup, 2007.

[4] INSTEON, “Developer’s guide”, available online: http://www.insteon.net.

[5] Z-Wave, “http://www.z-wave.com”.

[6] H. Khurana, R. Bobba, T. Yardley, P. Agarwal and E. Heine, “Design principles for Power Grid cyber-infrastructure authentication protocols”, in proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS '10), 2010.

[7] M. Amin, “Challenges in reliability, security, efficiency, and resilience of energy infrastructure: toward smart self-healing electric power grid”, Power and Energy Society General Meeting: Conversion and Delivery of Electrical Energy in the 21st Century, July 2008.

[8] H. Khurana, M. Hadley, N. Lu and D. A. Frincke “Smart-Grid security issues”, IEEE Security and Privacy, vol. 8, no. 1, pp. 81-85, 2010.

[9] A.R. Metke and R. L. Ekl, “Security technology for Smart Grid networks”, IEEE Transactions on Smart Grid, vol. 1, no. 1. (June 2010), pp. 99-107.

[10] C.Valli, “The not so smart, Smart Grid - potential security risks associated with the deployment of Smart Grid technologies”, in proceedings of the 7th Australian Digital Forensics Conference, 2009.

[11] C. Bennett and S. Wicker, “Decreased time delay and security enhancement recommendations for AMI smart meter networks”, in proceedings of IEEE Innovative Smart Grid Technologies (ISGT), 2010.

[12] R. Bobba, H. Khurana, M. AlTurki, and F. Ashraf. “PBES: a policy based encryption system with application to data sharing in the power grid”, in proceedings of the 4th International Symposium on Information, Computer, and Communications Security (ASIACCS ’09), 2009.

[13] D. Wei, Y. Lu, M. Jafari, P. Skare and K. Rohde. “An integrated security system of protecting Smart Grid against cyber attacks”, in proceedings of the 1st IEEE PES Conference on Innovative Smart Grid Technologies, 19-21 Jan. 2010.

[14] A. Hamlyn, H. Cheung, T. Mander, L. Wang, C. Yang and R. Cheung, “Computer network security management and authentication of smart grids operations”, Power and Energy Society General Meeting: Conversion and Delivery of Electrical Energy in the 21st Century, July 2008.

[15] Cisco, “Cisco carrier-grade IPv6 (CGv6) solution, 2009.

[2] Since the TD can communicate with its home gateway anytime, we assume that the TD keeps sending periodic synchronization messages to its home gateway while it is mobile (i.e., not connected to a HAN).