Secure Device Authentication Mechanisms for the Smart Grid-Enabled Home Area Networks

Erman Ayday, and Sridhar Rajagopal,

Abstract

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 in which the smart appliances can communicate both with the smart meter and the gateway. Further, operating schedules of the smart 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 proposed mechanisms are resilient against insider attackers performing serious attacks such as man-in-the-middle or impersonation during device authentication. Further, the proposed authentication mechanisms are intuitive and require no (or minimum) user effort.

Index Terms

Smart Grid, security, authentication, home area networks, smart appliances

1 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. The main purpose of the Smart Grid is to control the appliances at consumers' homes to save energy, reduce cost and increase reliability and transparency.

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. We can consider two different architectures for the HAN: 1) *Centralized architecture*, in which all appliances directly or in a multi-hop fashion communicate with the smart meter, and the Utility sends the scheduling information via the smart meter, 2) *Distributed architecture*, in which

- *E. Ayday is with the School of Computer and Communication Sciences, EPFL, Lausanne, Switzerland.*
  E-mail: erman.ayday@epfl.ch
- *S. Rajagopal is with Samsung Telecommunications America, Dallas Telecom Lab.*
  E-mail: srajagop@sta.samsung.com

appliances communicate with the gateway, and gateway does the scheduling based on the pricing information it receives from the meter. Smart meters are typically not capable of organizing and scheduling tens of devices in a HAN due to their computational limitations. This makes the centralized architecture impractical especially for high scale deployments. Therefore, we believe that the distributed architecture will be used by the majority of the users, and hence, in this work, we assume a distributed architecture for the HAN. We note that the work presented can also be applied to HANs with centralized architectures.

A distributed architecture for the HAN (illustrated in Fig. 1) consists of the smart appliances (AC, refrigerator, etc.), the smart meter, the gateway and a user interface (UI) which is either directly or remotely connected to the gateway. In this architecture, smart appliances (SAs) directly communicate 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.

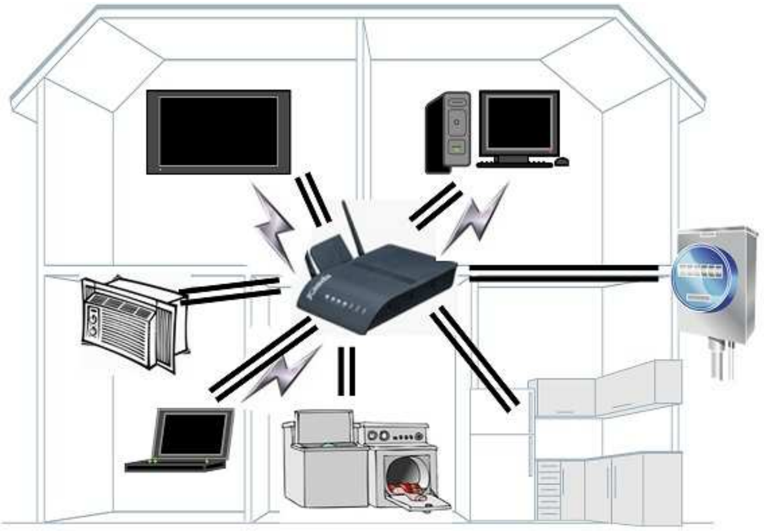

Fig. 1. Distributed architecture for the HAN.

The task of providing security services for the Smart Grid is not trivial due to its large scale deployment (larger than the Internet), the legacy devices (i.e., long lifetime of most network elements), field locations (i.e., millions of scattered field devices), and its heterogeneous architecture (i.e., various types of networks within the grid) [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 [3].

The security of the Smart Grid depends on authentication, authorization, message integrity and privacy mechanisms. Among these security services, device authentication for the HAN part of the Smart Grid is one of the most important challenges. Even though there are also other crucial security requirements 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 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 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.

Our main goal is to develop secure authentication mechanisms that will be resilient to aforementioned attacks. Further, we propose intuitive authentication mechanisms (that require no user effort), 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 SA and the HAN, and 3) between the transient devices and the HAN.
- Proposed authentication algorithms make extensive use of collaboration between different parties in order to provide secure and attack resilient authentication protocols.
- The proposed device authentication algorithms are resilient against insider attackers performing serious attacks such as MITM or impersonation during the authentication of the devices.
- 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.

The rest of this paper is organized as follows. In the rest of this section, we summarize the related work. In Section 2, we present the proposed device authentication mechanisms. Later, in Section 3, we show the attack resiliency of the proposed mechanisms by conducting a security analysis. Finally, in Section 4, we conclude the paper.

1.1 Related Work

Existing HAN protocols support security only up to a certain level. One of the popular HAN protocols, Zigbee [1], uses the IEEE 802.15.4 protocol. Zigbee enabled devices can handle 128-bits security for confidentiality and message integrity. Further, they can handle advanced encryption scheme (AES). The designers of the protocol propose 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. Further, IEEE 802.15.4 protocol has known vulnerabilities about access control lists (ACLs), key management and new user authentication [4]. Another popular HAN protocol, Wi-Fi, is also widely deployed to many homes. Wi-Fi alliance introduced Wi-Fi protected setup [5] for the secure establishment of the HAN. Wi-Fi protected setup offers four choices to the customer in order 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 [6] is mostly used for the lights and the security systems in the home. In INSTEON, device authentication is utilized 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, Z-Wave protocol [7] is mostly used for remote controls, smoke detectors and security sensors. In Z-Wave, 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 [8]–[12] the security challenges of Smart Grid Networks are discussed and identified. [13] 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 [14]. In [15], authors addressed the impact of the blackhole attack on data availability (during the multi-hop routing between the SMs and the Utility). They proposed using a dedicated path during the network discovery phase to combat this attack. Bobba et al. introduced a policy based encryption system for the data sharing problem in the electric grids in [16]. Further, in [17], authors proposed a conceptual layered framework for protection of the Power Grid automation systems against cyber attacks. Finally, in [18] Hamlyn et al. 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.

2 Secure Device Authentication Mechanisms for Smart Grid Enabled Home Area Networks

2.1 Assumptions

A typical Smart Grid network may include millions of devices. All these devices should be globally reachable in order to control the network, and hence, they all should have unique IDs [1]. One option to provide unique IDs to the devices in such large scale deployments is to utilize IPv6. Therefore, we assume that IPv6 is used, and hence, every device has a unique IP address (this IP address can also be represented as the unique ID of every device). Indeed, it is also stated in [19] that IPv6 will enable new revenue-yielding service opportunities such as Smart Grid networks. We note that Zigbee currently uses 64-bit MAC address (EUI-64 Identifier) for the unique ID. However, we do not foresee that this addressing will be sufficient for the future large scale deployment of the grid. 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 preserve the confidentiality during the device authentication process. Further, every device shares a pair-wise key with the center of trust (Utility) [1]. Furthermore, the confidentiality of all messages between the gateway, the SM, the SA and the Utility are

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

cryptographically provided using the pair-wise keys. Moreover, all messages include a message authentication code (MAC) to provide message integrity. To facilitate future references, we listed the frequently used notations and cryptographic tools in Table 1.

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

TABLE 1
Notations and cryptographic tools.

2.2 Authentication between the Gateway and the Smart Meter

We assume that the SM is already installed by the Utility; the user can easily purchase the gateway from any consumer electronics store and the gateway should be authenticated with the SM with no user effort once it is plugged in. We further assume that the gateway is connected to the Utility (the trust center) via the Internet (if a broadband connection is available), land line, a cell phone or the Advanced Metering Infrastructure (AMI). We believe that the gateway with Utility connection can be a popular architecture and will be used by the majority of the users. Even though it is a rare situation, we also consider the case when the gateway has no connection to the Utility in Appendix A.

We propose an intuitive authentication mechanism that is resilient to MITM attacks. Since manufacturers or Utility companies 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.

The details of the mechanism are discussed below. Further, the steps of the proposed authentication process are also illustrated in Fig. 2. We note that the numbers on the figure are the sequence numbers of the messages and they are not related to the message numbers used throughout the text.

The gateway initiates the process as soon as it is plugged in by sending the following authentication request message to the SM.

$$\{\mathrm{AuthReq}, \mathrm{IP_G}\}. \tag{1}$$

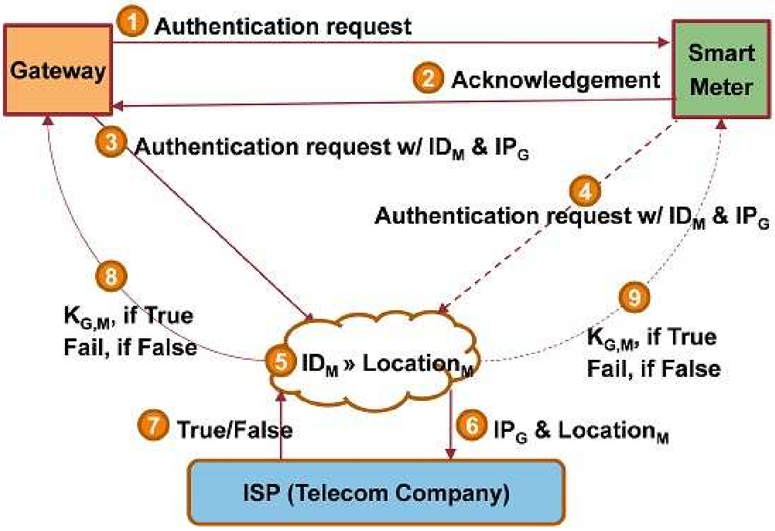

Fig. 2. Authentication mechanism between the gateway and the SM.

Once SM receives (1), it responds with the following acknowledgement (ACK) message.

$$\{\mathrm{ACK}, \mathrm{IP_G}, \mathrm{ID_M}\}. \tag{2}$$

After this message exchange, gateway sends the following message to the trust center (Utility) via the Internet, land line or through a cell phone.

$$\left\{\mathrm{E}_{\mathrm{K_{G,U}}}(\mathrm{AuthReq}, \mathrm{ID_M}), \mathrm{MAC}\left(\mathrm{K_{G,U}}, \mathrm{E}_{\mathrm{K_{G,U}}}(\mathrm{AuthReq}, \mathrm{ID_M})\right), \mathrm{IP_G}\right\}. \tag{3}$$

Similarly, the SM also sends the following message to the Utility.

$$\left\{\mathrm{E}_{\mathrm{K_{M,U}}}(\mathrm{AuthReq}, \mathrm{IP_G}), \mathrm{MAC}\left(\mathrm{K_{M,U}}, \mathrm{E}_{\mathrm{K_{M,U}}}(\mathrm{AuthReq}, \mathrm{IP_G})\right), \mathrm{ID_M}\right\}. \tag{4}$$

Once, the Utility authenticates (3) and (4) using the MACs attached to them, it maps the ID of the SM ($\mathrm{ID_M}$) to its location from its database[2]. As we discussed before, the Utility should make sure that it authenticates the correct gateway to the correct SM. We propose to collaborate with 3rd party service providers (such as the internet service providers, ISPs, or telecommunication companies) depending on the type of gateway-Utility connection to pair the gateway and the SM based on their locations. If the gateway is connected to the Utility via the Internet, the ISP will be able to identify its location from its unique IP. Otherwise, if the gateway is connected to the Utility via the land line or a cell phone[3], the telecommunication company will be able to identify its location from the calling number. Assuming the gateway-Utility connection is via the Internet, the Utility forwards the IP of the gateway ($\mathrm{IP_G}$) along with the location of the SM to the ISP. The ISP processes these two inputs and sends a "True" message back to the Utility if the location of the gateway matches the SM's location as illustrated in Fig. 2. Otherwise, a "False" message is sent back to the Utility.

[2] Utility companies can easily map the unique ID of a SM to its actual location due to the billing support requirement.

[3] The user can use his personal cell phone during the authentication process, similar to activating a credit card via the cell phone.

If the Utility receives a "False" message from the ISP, it sends a "Fail" message to both the gateway and SM, and hence, terminates the authentication process. Otherwise, the Utility pairs the gateway with the SM, creates a pair-wise key between the gateway and the SM for them to establish a secure channel between each other, and sends the following message to the gateway.

$$\left\{\mathrm{E}_{\mathrm{K}_{\mathrm{G,U}}}(\mathrm{K}_{\mathrm{G,M}}, \mathrm{ID}_{\mathrm{M}}), \mathrm{MAC}\left(\mathrm{K}_{\mathrm{G,U}}, \mathrm{E}_{\mathrm{K}_{\mathrm{G,U}}}(\mathrm{K}_{\mathrm{G,M}}, \mathrm{ID}_{\mathrm{M}})\right), \mathrm{IP}_{\mathrm{G}}\right\}. \tag{5}$$

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

$$\left\{\mathrm{E}_{\mathrm{K}_{\mathrm{M,U}}}(\mathrm{K}_{\mathrm{G,M}}, \mathrm{IP}_{\mathrm{G}}), \mathrm{MAC}\left(\mathrm{K}_{\mathrm{M,U}}, \mathrm{E}_{\mathrm{K}_{\mathrm{M,U}}}(\mathrm{K}_{\mathrm{G,M}}, \mathrm{IP}_{\mathrm{G}})\right), \mathrm{ID}_{\mathrm{M}}\right\}. \tag{6}$$

After gateway and the SM authenticate (5) and (6), they both decrypt the encrypted parts using the keys they share with the Utility 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.

2.3 Authentication between the Smart Appliances and the HAN

We assume that the SM is already installed by the Utility, the gateway is set up by the user, and the SM and the gateway are authenticated to each other (and to the Utility) by using the mechanism described in Section 2.2. We note that we do not consider an insider attacker with a legitimate smart meter-gateway pair (as it is not a practical attack scenario due to the limitations of the smart meters). We believe that taking out a smart meter (which is monitored by the Utility) and using it as a mobile device for attack is not practical in reality.

Since the SA has no direct connection to the Utility, it has to communicate with the gateway or the SM during the authentication process[4]. If the SA is authenticated to the HAN via the gateway, the MITM attack is a potential threat against the HAN. 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. We note that the attacker can only take control of the appliances that actually exist in the home and affect their operating schedules. That is, he cannot introduce a non-existing appliance to the home as all the appliances are listed on the UI. Hence, introducing a non-existing appliance will be eventually detected by the user.

We propose to use a collaborative authentication model by using the collaboration of the SM and the gateway to combat the attacker. We describe the details of this authentication process below. The steps of the authentication process are also illustrated in Fig. 3.

The SA initiates the process by sending the following authentication request message to both the gateway and the SM.

$$\{\mathrm{AuthReq}, \mathrm{ID}_{\mathrm{A}}\}. \tag{7}$$

Once the gateway receives (7), it responds with the following acknowledgement (ACK) message.

$$\{\mathrm{ACK}, \mathrm{ID}_{\mathrm{A}}, \mathrm{IP}_{\mathrm{G}}\}. \tag{8}$$

[4] Communication between the SA and the SM can be either direct or via the gateway.

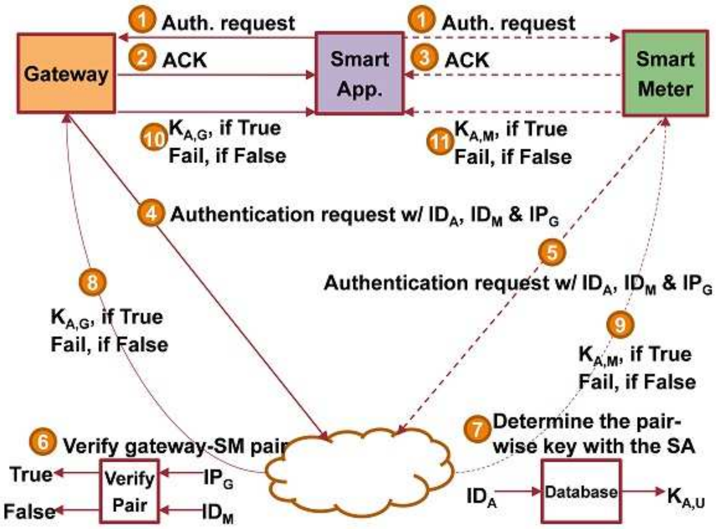

Fig. 3. Authentication mechanism between the SA and the HAN.

Similarly, the SM responds to (7) with the following ACK message.

$$\{\mathrm{ACK}, \mathrm{ID_A}, \mathrm{ID_M}\}. \tag{9}$$

After this message exchange, gateway sends the following message to the trust center (Utility) via the Internet, land line or through a cell phone.

$$\left\{\mathrm{E}_{\mathrm{K_{G,U}}}(\mathrm{AuthReq}, \mathrm{ID_A}, \mathrm{ID_M}, \mathrm{IP_G}), \mathrm{MAC}\left(\mathrm{K_{G,U}}, \mathrm{E}_{\mathrm{K_{G,U}}}(\mathrm{AuthReq}, \mathrm{ID_A}, \mathrm{ID_M}, \mathrm{IP_G})\right), \mathrm{IP_G}\right\}. \tag{10}$$

Similarly, the SM also sends the following message to the Utility.

$$\left\{\mathrm{E}_{\mathrm{K_{M,U}}}(\mathrm{AuthReq}, \mathrm{ID_A}, \mathrm{ID_M}, \mathrm{IP_G}), \mathrm{MAC}\left(\mathrm{K_{M,U}}, \mathrm{E}_{\mathrm{K_{M,U}}}(\mathrm{AuthReq}, \mathrm{ID_A}, \mathrm{ID_M}, \mathrm{IP_G})\right), \mathrm{ID_M}\right\}. \tag{11}$$

Once the Utility authenticates (10) and (11), it performs the following two operations:

1) The Utility verifies that the messages in (10) and (11) are coming from a paired gateway and SM (the Utility pairs the gateway with the SM during the authentication of the gateway as discussed in Section 2.2). If the messages are coming from a valid gateway-SM pair, Utility follows the regular procedure; otherwise, it sends a "Fail" message to both the gateway and the SM to terminate the authentication process.
2) Once the Utility verifies the gateway-SM pair, it maps the ID of the SA ($\mathrm{ID_A}$) to the pair-wise key ($\mathrm{K_{A,U}}$) between the SA and the Utility. Further, it creates two pair-wise keys between the gateway and the SA ($\mathrm{K_{A,G}}$), and between the SM and the SA ($\mathrm{K_{A,M}}$) for them to establish a secure channel between each other.

We note that the Utility can also keep track of the appliances (which appliance is located at which location) as a result of this mechanism. Once the Utility verifies the gateway-SM pair and generates the pair-wise keys, it sends the following message to the gateway.

$$\Big\{\mathrm{E}_{\mathrm{K}_{\mathrm{G,U}}}\left(\mathrm{E}_{\mathrm{K}_{\mathrm{A,U}}}(\mathrm{K}_{\mathrm{A,G}},\mathrm{IP}_{\mathrm{G}}),\mathrm{MAC}\left(\mathrm{K}_{\mathrm{A,U}},\mathrm{E}_{\mathrm{K}_{\mathrm{A,U}}}(\mathrm{K}_{\mathrm{A,G}},\mathrm{IP}_{\mathrm{G}})\right),\mathrm{K}_{\mathrm{A,G}}\right),$$

$$\mathrm{MAC}\left(\mathrm{K}_{\mathrm{G,U}},\mathrm{E}_{\mathrm{K}_{\mathrm{G,U}}}\left(\mathrm{E}_{\mathrm{K}_{\mathrm{A,U}}}(\mathrm{K}_{\mathrm{A,G}},\mathrm{IP}_{\mathrm{G}}),\mathrm{MAC}\left(\mathrm{K}_{\mathrm{A,U}},\mathrm{E}_{\mathrm{K}_{\mathrm{A,U}}}(\mathrm{K}_{\mathrm{A,G}},\mathrm{IP}_{\mathrm{G}})\right),\mathrm{K}_{\mathrm{A,G}}\right)\right),\mathrm{IP}_{\mathrm{G}}\Big\}. \quad (12)$$

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

$$\Big\{\mathrm{E}_{\mathrm{K}_{\mathrm{M,U}}}\left(\mathrm{E}_{\mathrm{K}_{\mathrm{A,U}}}(\mathrm{K}_{\mathrm{A,M}},\mathrm{ID}_{\mathrm{M}}),\mathrm{MAC}\left(\mathrm{K}_{\mathrm{A,U}},\mathrm{E}_{\mathrm{K}_{\mathrm{A,U}}}(\mathrm{K}_{\mathrm{A,M}},\mathrm{ID}_{\mathrm{M}})\right),\mathrm{K}_{\mathrm{A,M}}\right),$$

$$\mathrm{MAC}\left(\mathrm{K}_{\mathrm{M,U}},\mathrm{E}_{\mathrm{K}_{\mathrm{M,U}}}\left(\mathrm{E}_{\mathrm{K}_{\mathrm{A,U}}}(\mathrm{K}_{\mathrm{A,M}},\mathrm{ID}_{\mathrm{M}}),\mathrm{MAC}\left(\mathrm{K}_{\mathrm{A,U}},\mathrm{E}_{\mathrm{K}_{\mathrm{A,U}}}(\mathrm{K}_{\mathrm{A,M}},\mathrm{ID}_{\mathrm{M}})\right),\mathrm{K}_{\mathrm{A,M}}\right)\right),\mathrm{ID}_{\mathrm{M}}\Big\}. \quad (13)$$

After the gateway and the SM authenticate (12) and (13), they both decrypt the encrypted parts using the keys they share with the Utility to obtain the pair-wise keys that they will use to create a secure channel with the SA. We note that neither the gateway nor the SM can decrypt the parts of (12) and (13) which are encrypted by the pair-wise key between the Utility and the SA ($\mathrm{K}_{\mathrm{A,U}}$). Further, they cannot modify these encrypted parts without being detected due to the attached MACs (which are created using $\mathrm{K}_{\mathrm{A,U}}$). Therefore, the gateway sends the following message to the SA.

$$\left\{\mathrm{E}_{\mathrm{K}_{\mathrm{A,U}}}(\mathrm{K}_{\mathrm{A,G}},\mathrm{IP}_{\mathrm{G}}),\mathrm{MAC}\left(\mathrm{K}_{\mathrm{A,U}},\mathrm{E}_{\mathrm{K}_{\mathrm{A,U}}}(\mathrm{K}_{\mathrm{A,G}},\mathrm{IP}_{\mathrm{G}})\right),\mathrm{ID}_{\mathrm{A}},\mathrm{IP}_{\mathrm{G}}\right\}. \quad (14)$$

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

$$\left\{\mathrm{E}_{\mathrm{K}_{\mathrm{A,U}}}(\mathrm{K}_{\mathrm{A,M}},\mathrm{ID}_{\mathrm{M}}),\mathrm{MAC}\left(\mathrm{K}_{\mathrm{A,U}},\mathrm{E}_{\mathrm{K}_{\mathrm{A,U}}}(\mathrm{K}_{\mathrm{A,M}},\mathrm{ID}_{\mathrm{M}})\right),\mathrm{ID}_{\mathrm{A}},\mathrm{ID}_{\mathrm{M}}\right\}. \quad (15)$$

SA initially verifies the integrity of (14) and (15). Then, it decrypts the encrypted parts using the pair-wise key it shares with the Utility. Therefore, the SA authenticates the gateway and the SM, and it also obtains the pair-wise keys generated by the Utility. This finishes the mutual authentication process between the SA and the HAN. Once the SA establishes a secure channel with the gateway and the SM (using $\mathrm{K}_{\mathrm{A,G}}$ and $\mathrm{K}_{\mathrm{A,M}}$), it can securely negotiate on a key exchange protocol with them.

2.4 Authentication between the Transient Devices and the HAN

We denote the transient device (TD) as a portable (or mobile) device that can be used both in its own HAN and other HANs. The best example for a TD is a plug-in hybrid electric vehicle (PHEV) which can be charged either at user's own HAN (referred to as the home HAN including home gateway and home SM) 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 may be billed to their actual owner. As a result of this, 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 Utility 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 is already authenticated to its home HAN by following the procedure described in Section 2.3. Further, the TD (if it is a mobile device such as PHEV) can communicate with its home gateway anytime (even when it is mobile)[5]. We note that this assumption is only required to provide extra security; we will also mention the case in which the TD does not have a stable connection with its home gateway in Section 3.3. The steps of the authentication process are illustrated in Fig. 4.

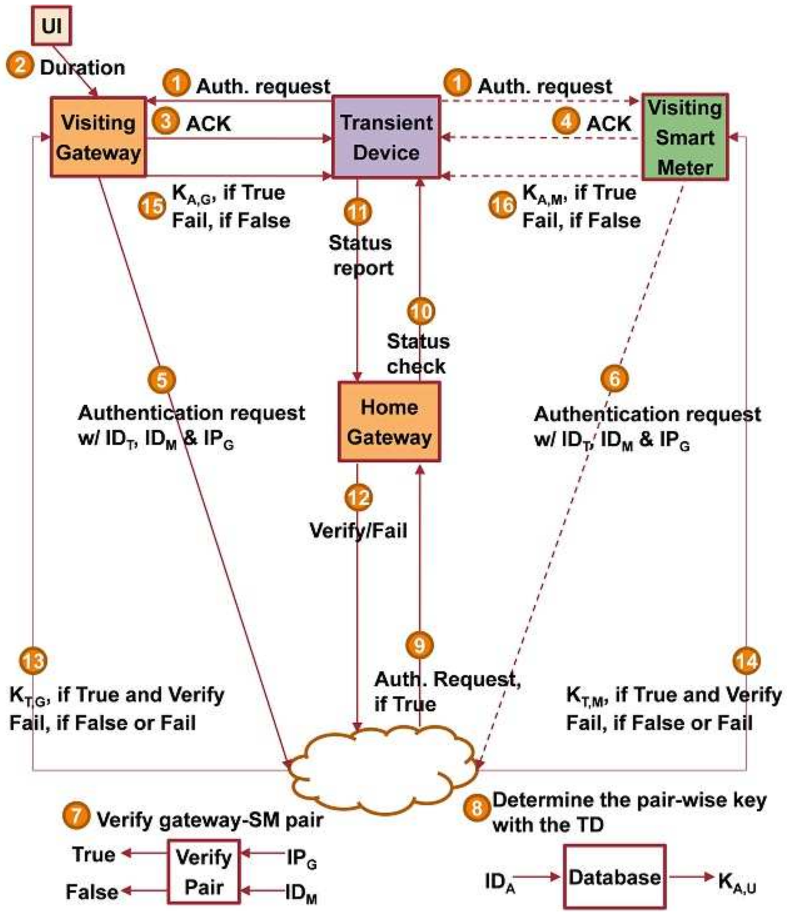
UI
2 Duration
1 Auth. request
3 ACK
Visiting Gateway
Transient Device
1 Auth. request
4 ACK
Visiting Smart Meter
15 $K_{A,G}$, if True Fail, if False
11 Status report
16 $K_{A,M}$, if True Fail, if False
10 Status check
5 Authentication request w/ ID_T, ID_M & IP_G
Home Gateway
6 Authentication request w/ ID_T, ID_M & IP_G
12 Verify/Fail
9 Auth. Request, if True
13 $K_{T,G}$, if True and Verify Fail, if False or Fail
14 $K_{T,M}$, if True and Verify Fail, if False or Fail
7 Verify gateway-SM pair
True
False
Verify Pair
IP_G
ID_M
8 Determine the pair-wise key with the TD
ID_A
Database
$K_{A,U}$

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

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

$$\left\{\mathrm{AuthReq}, \mathrm{ID_T}, \mathrm{ID_M^T}, \mathrm{M}\right\}, \tag{16}$$

where

$$\mathrm{M} = \left\{\mathrm{E}_{\mathrm{K_{T,G}}}(\mathrm{ID_T}, \mathrm{SeqNo}), \mathrm{MAC}\left(\mathrm{K_{T,G}}, \mathrm{E}_{\mathrm{K_{T,G}}}(\mathrm{ID_T}, \mathrm{SeqNo})\right)\right\}, \tag{17}$$

SeqNo is the sequence number of the message between the TD and its home gateway, and $\mathrm{ID_M^T}$ is the ID of TD's home SM. The TD notifies the visiting HAN that it is already

[5] If the TD is not a mobile device, then at any instant, it is either a part of its home HAN or a visiting HAN. Hence, it can communicate with its home gateway any time.

authenticated to a HAN by including the ID of its home SM ($\mathrm{ID}_{\mathrm{M}}^{\mathrm{T}}$) in the authentication request message. Moreover, the authentication request message of the TD also includes a part, M in (17), which is encrypted by the pair-wise key between the TD and its home gateway ($\mathrm{K}_{\mathrm{T,G}}$). This encrypted part is forwarded from the visiting HAN to the Utility and from the Utility 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 (it can be manually removed any time before its authentication period expires by using the UI).

Next, the visiting gateway responds the TD with the following ACK message.

$$\left\{\mathrm{ACK}, \mathrm{ID}_{\mathrm{T}}, \mathrm{IP}_{\mathrm{G}}, \mathrm{T}\right\}, \tag{18}$$

Similarly, the visiting SM responds to (16) with the following ACK message.

$$\left\{\mathrm{ACK}, \mathrm{ID}_{\mathrm{T}}, \mathrm{ID}_{\mathrm{M}}\right\}, \tag{19}$$

After this message exchange among the TD, the visiting gateway and the visiting SM, the visiting gateway sends the following message to the Utility.

$$\Bigg\{\mathrm{E}_{\mathrm{K}_{\mathrm{G,U}}}(\mathrm{AuthReq}, \mathrm{ID}_{\mathrm{T}}, \mathrm{ID}_{\mathrm{M}}, \mathrm{IP}_{\mathrm{G}}, \mathrm{ID}_{\mathrm{M}}^{\mathrm{T}}, \mathrm{T}, \mathrm{M}), \\ \mathrm{MAC}\left(\mathrm{K}_{\mathrm{G,U}}, \mathrm{E}_{\mathrm{K}_{\mathrm{G,U}}}(\mathrm{AuthReq}, \mathrm{ID}_{\mathrm{T}}, \mathrm{ID}_{\mathrm{M}}, \mathrm{IP}_{\mathrm{G}}, \mathrm{ID}_{\mathrm{M}}^{\mathrm{T}}, \mathrm{T}, \mathrm{M})\right), \mathrm{IP}_{\mathrm{G}}\Bigg\}. \tag{20}$$

The visiting gateway includes $\mathrm{ID}_{\mathrm{M}}^{\mathrm{T}}$ and T to the message so that the Utility can contact with the home HAN of the TD and also know how long the TD will be a part of the visiting HAN. Similarly, the visiting SM sends the following message to the Utility.

$$\Bigg\{\mathrm{E}_{\mathrm{K}_{\mathrm{M,U}}}(\mathrm{AuthReq}, \mathrm{ID}_{\mathrm{T}}, \mathrm{ID}_{\mathrm{M}}, \mathrm{IP}_{\mathrm{G}}, \mathrm{ID}_{\mathrm{M}}^{\mathrm{T}}, \mathrm{M}), \\ \mathrm{MAC}\left(\mathrm{K}_{\mathrm{M,U}}, \mathrm{E}_{\mathrm{K}_{\mathrm{M,U}}}(\mathrm{AuthReq}, \mathrm{ID}_{\mathrm{T}}, \mathrm{ID}_{\mathrm{M}}, \mathrm{IP}_{\mathrm{G}}, \mathrm{ID}_{\mathrm{M}}^{\mathrm{T}}, \mathrm{M})\right), \mathrm{ID}_{\mathrm{M}}\Bigg\}. \tag{21}$$

After checking the integrities of (20) and (21), the Utility verifies that the messages in (20) and (21) are coming from a paired gateway and SM (as discussed in Section 2.2). If this verification fails, the Utility immediately sends a "Fail" message to the visiting HAN and terminates the process. Otherwise (if the verification succeeds), the Utility maps the ID of the TD (ID_{T}) to the pair-wise key ($\mathrm{K}_{\mathrm{T,U}}$) between the TD and the Utility 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.

$$\left\{\mathrm{E}_{\mathrm{K}_{\mathrm{HG,U}}}(\mathrm{M}), \mathrm{MAC}\left(\mathrm{K}_{\mathrm{HG,U}}, \mathrm{E}_{\mathrm{K}_{\mathrm{HG,U}}}(\mathrm{M})\right)\right\}, \tag{22}$$

where $\mathrm{K}_{\mathrm{HG,U}}$ is the pair-wise key between the home gateway of the TD and the Utility.

We also propose to use 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. Furthermore, the TD uses sequence numbered messages when it communicates with its home gateway as in (17). 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 (22), it initially verifies that the message M (encrypted via the pair-wise key between the TD and the home gateway) 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 Utility as a feedback which will 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 in order to figure out if it is actually trying to authenticate with any particular visiting HAN[6]. 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 Utility. Otherwise, if the TD does not verify its authentication attempt, a "Fail" message is sent from the home gateway to the Utility. 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 Utility 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 ($\mathrm{K_{T,G}}$), and between the visiting SM and the TD ($\mathrm{K_{T,M}}$) for them to establish a secure channel between each other. Next, the Utility sends the following message to the visiting gateway.

$$\Big\{\mathrm{E_{K_{G,U}}}\left(\mathrm{E_{K_{T,U}}}(\mathrm{K_{T,G}},\mathrm{IP_G}),\mathrm{MAC}\left(\mathrm{K_{T,U}},\mathrm{E_{K_{T,U}}}(\mathrm{K_{T,G}},\mathrm{IP_G})\right),\mathrm{K_{T,G}}\right),$$

$$\mathrm{MAC}\left(\mathrm{K_{G,U}},\mathrm{E_{K_{G,U}}}\left(\mathrm{E_{K_{T,U}}}(\mathrm{K_{T,G}},\mathrm{IP_G}),\mathrm{MAC}\left(\mathrm{K_{T,U}},\mathrm{E_{K_{T,U}}}(\mathrm{K_{T,G}},\mathrm{IP_G})\right),\mathrm{K_{T,G}}\right)\right),\mathrm{IP_G}\Big\}. \quad (23)$$

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

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

$$\Big\{ \mathrm{E}_{\mathrm{K}_{\mathrm{M,U}}} \left(\mathrm{E}_{\mathrm{K}_{\mathrm{T,U}}}(\mathrm{K}_{\mathrm{T,M}}, \mathrm{ID}_{\mathrm{M}}), \mathrm{MAC}\left(\mathrm{K}_{\mathrm{T,U}}, \mathrm{E}_{\mathrm{K}_{\mathrm{T,U}}}(\mathrm{K}_{\mathrm{T,M}}, \mathrm{ID}_{\mathrm{M}})\right), \mathrm{K}_{\mathrm{T,M}} \right),$$
$$\mathrm{MAC}\left(\mathrm{K}_{\mathrm{M,U}}, \mathrm{E}_{\mathrm{K}_{\mathrm{M,U}}}\left(\mathrm{E}_{\mathrm{K}_{\mathrm{T,U}}}(\mathrm{K}_{\mathrm{T,M}}, \mathrm{ID}_{\mathrm{M}}), \mathrm{MAC}\left(\mathrm{K}_{\mathrm{T,U}}, \mathrm{E}_{\mathrm{K}_{\mathrm{T,U}}}(\mathrm{K}_{\mathrm{T,M}}, \mathrm{ID}_{\mathrm{M}})\right), \mathrm{K}_{\mathrm{T,M}}\right)\right), \mathrm{ID}_{\mathrm{M}} \Big\}. \tag{24}$$

After checking the integrities of (23) and (24), the visiting gateway and the visiting SM both decrypt the encrypted parts of the messages using the keys they share with the Utility 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.

$$\left\{\mathrm{E}_{\mathrm{K}_{\mathrm{T,U}}}(\mathrm{K}_{\mathrm{T,G}}, \mathrm{IP}_{\mathrm{G}}), \mathrm{MAC}\left(\mathrm{K}_{\mathrm{T,U}}, \mathrm{E}_{\mathrm{K}_{\mathrm{T,U}}}(\mathrm{K}_{\mathrm{T,G}}, \mathrm{IP}_{\mathrm{G}})\right), \mathrm{ID}_{\mathrm{T}}, \mathrm{IP}_{\mathrm{G}}\right\}. \tag{25}$$

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

$$\left\{\mathrm{E}_{\mathrm{K}_{\mathrm{T,U}}}(\mathrm{K}_{\mathrm{T,M}}, \mathrm{ID}_{\mathrm{M}}), \mathrm{MAC}\left(\mathrm{K}_{\mathrm{T,U}}, \mathrm{E}_{\mathrm{K}_{\mathrm{T,U}}}(\mathrm{K}_{\mathrm{T,M}}, \mathrm{ID}_{\mathrm{M}})\right), \mathrm{ID}_{\mathrm{T}}, \mathrm{ID}_{\mathrm{M}}\right\}. \tag{26}$$

After checking the integrities of (25) and (26), the TD decrypts the encrypted parts using the pair-wise key it shares with the Utility. Therefore, the TD authenticates the visiting gateway and the visiting SM, and it also obtains the pair-wise keys generated by the Utility. This finishes the mutual authentication process between the TD and the visiting HAN. Once the TD establishes a secure channel with the visiting gateway and the visiting SM (using $\mathrm{K}_{\mathrm{T,G}}$ and $\mathrm{K}_{\mathrm{T,M}}$), it can securely negotiate on a key exchange protocol with them.

3 Security Analysis

3.1 Authentication between the Gateway and the Smart Meter

The proposed authentication mechanism between the gateway and the SM 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 as discussed in Section 2.2. To initiate this attack, the attacker sends (1) with its own ID and sends (2) to the actual gateway. Then, the attacker tries to pair itself with the actual gateway (as a SM) and with the actual SM (as a gateway) by following the procedure described in Section 2.2. However, this attack will fail during the verification at the 3rd party service provider (ISP or the telecommunications company). Assuming the 3rd party service provider is the ISP, when the Utility sends the IP of the (attacker's) gateway and the location of the SM to the ISP, the ISP will determine the location of the (attacker's) gateway from its unique IP and see that it does not match with the location of the SM. Therefore, the ISP will send a "False" message back to the Utility, and hence, the authentication process will be failed (i.e., the MITM attack will be prevented).

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 Utility are encrypted by the pair-wise key between them ($\mathrm{K}_{\mathrm{G,U}}$). 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.

Device impersonation is also a threat during the authentication of the gateway to the SM. The attacker can impersonate a legitimate gateway (i.e., capture its IP and keys) and try to pair his bogus gateway with the smart meter. We consider two different scenarios for this attack: 1) a SM can be paired with only a single gateway, and 2) a SM can be paired with multiple gateways. We note that alternatively, the impersonation attack can be avoided by using tamper-proof hardware for the SMs and the gateways.

In the first case, after the original gateway and the SM are paired, the attacker cannot pair his bogus gateway with the SM since the SM can be paired with only a single gateway. This attempt of the attacker will be detected at the Utility when the Utility receives (3) and (4) from the bogus gateway and the SM. After receiving (3) and (4), the Utility realizes that the SM has already been paired with another gateway and detects the attack. In this case, the Utility may solve this problem by requesting minimum user effort (via the UI) during the authentication as described in Appendix A. If the attacker pairs his bogus gateway to the SM before the original gateway, the attack will be detected during the authentication of the original gateway as described above. In this attack scenario, the attacker will not have any impact until the attack is detected at the Utility if either of the following assumptions holds:

- The communication between the SM and the gateway is initiated by user request after the user purchases a gateway.
- A user does not acquire SAs before he acquires a gateway. Therefore, even if the bogus gateway pairs itself to the SM, it will not have an impact on the SAs before the user has his actual gateway, and hence, before the attack is detected at the Utility.

In the second case (if the SM can be paired with multiple gateways), the attacker can spoof the IP of the location and attack by using a legitimate gateway. In this scenario, the SM and the Utility will allow the attacker's bogus gateway to be paired with the SM since the bogus gateway has a valid pair-wise key (with the Utility) and uses the IP of the location where the SM is located. Therefore, in this particular case (when the SM can be paired with multiple gateways) we require that the user manually confirms the authentication of every gateway via the UI as the final step of the authentication process described in Section 2.2.

Even though it is not very likely, the attacker may also try to communicate with the SM and SAs by impersonating the original gateway. However, the communication of the bogus gateway will be overheard by the original gateway and this impersonation attack will be detected at the Utility as a result of the warning messages from the original gateway.

3.2 Authentication between the Smart Appliances and the HAN

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 between the SAs and the HAN is resilient to MITM attacks since the Utility does not verify the process that is not initiated by a paired gateway-SM pair.

The attacker might initiate a MITM attack (as discussed in Section 2.3) by utilizing a compromised gateway-SA pair. Initially, the attacker intercepts the authentication request message, (7), from the actual SA. Then, the attacker sends its own authentication request message with its own ID (behaving as a SA) to the actual gateway and the SM. In the meantime, he also sends (8) and (9) to the actual SA (pretending as a gateway and a SM). Next, it follows the procedure described in Section 2.3 to authenticate itself as a SA to the HAN and authenticate itself as a SM-gateway pair to the SA. However, this authentication attempt will fail at the Utility. Since it is not practical to use a legitimate SM-gateway pair for this attack, the attacker will be detected during the verification of the SM-gateway pair at the Utility and the authentication attempt will be terminated by the Utility.

3.3 Authentication between the Transient Devices and the HAN

The proposed authentication mechanism between the TDs and the HAN is resilient to both MITM and impersonation attacks. The resiliency of the mechanism to the MITM attacks can be shown similar to the discussion in Section 3.2; the attacker will be detected during the verification of the SM-gateway pair at the Utility.

The attacker may also initiate an impersonation attack on a victim TD by capturing its ID and secret keys as discussed in Section 2.4. The attacker initiates the attack by attempting to authenticate its own TD (which impersonates a victim TD) to a visiting HAN so that the power consumption of the attacker will be billed to the victim user. The attacker sends (16) to the visiting gateway and the visiting SM to initiate the authentication process and then follows the procedure described in Section 2.4. Since the victim TD generates and uses a different pair-wise key whenever it communicates with its home gateway and it uses sequence numbered messages at each communication session, it is not likely for the attacker to have the most recent pair-wise key and sequence number when he initiates the attack. Further, it is hard for the attacker to predict the future pair-wise keys from the captured one since each generated key depends on the time of the communication between the TD and its home gateway. Therefore, if the attacker uses an expired pair-wise key or a wrong sequence number, the attack will be detected during the verification of (22) at the home gateway. Otherwise, if the attacker captures the current pair-wise key between the victim TD and its home gateway and guesses the sequence number of the next message correctly, the attack will be detected due to the status messages between the TD and its home gateway. Once the home gateway sends the “status check” message to the victim TD, the victim TD does not verify the authentication attempt to the particular visiting HAN. Hence, the attack will be detected at the home gateway of the victim TD and the authentication process will be failed and terminated by the Utility.

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 (even when it is mobile). 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 the one described in Section 2.4, only with the exception of the status messages (status check and status report) between the TD and its home gateway.

4 Conclusion

In this paper we propose multiple secure, intuitive and low cost authentication mechanisms for the Smart Grid enabled HANs. We show that the proposed authentication mechanisms are resilient to adversarial behavior including MITM and impersonation attacks which cause serious damages to the grid. By using the proposed device authentication mechanisms, the devices in the HAN can be easily and securely added to or removed from the network. Further, transient devices such as PHEVs (Plug-in Hybrid Electric Vehicles) can be securely used at remote HANs, and the billing issues can be securely handled by the Utility. Furthermore, the proposed mechanisms have low computation and communication overheads. Hence, they can be easily implemented to all devices in the HAN which will allow a widespread deployment of smart appliances, gateways and smart meters in HANs.

Appendix

In this particular architecture, gateway has no direct contact other than the SM. Therefore, it is not possible for the Utility to know whether the SM is being authenticated by the correct gateway (i.e., any gateway may authenticate itself to the SM in order to mislead the SM). Thus, we require a minimum user effort during the authentication process for this particular case.

Authentication process for this case is similar to the mutual authentication used in VPN [20] (Virtual Private Network) technologies such as IPSec [21]. The user needs to manually enter a pass-code to the gateway to initiate the authentication process. We describe the details of this authentication process below. The steps of this authentication process are also illustrated in Fig. 5.

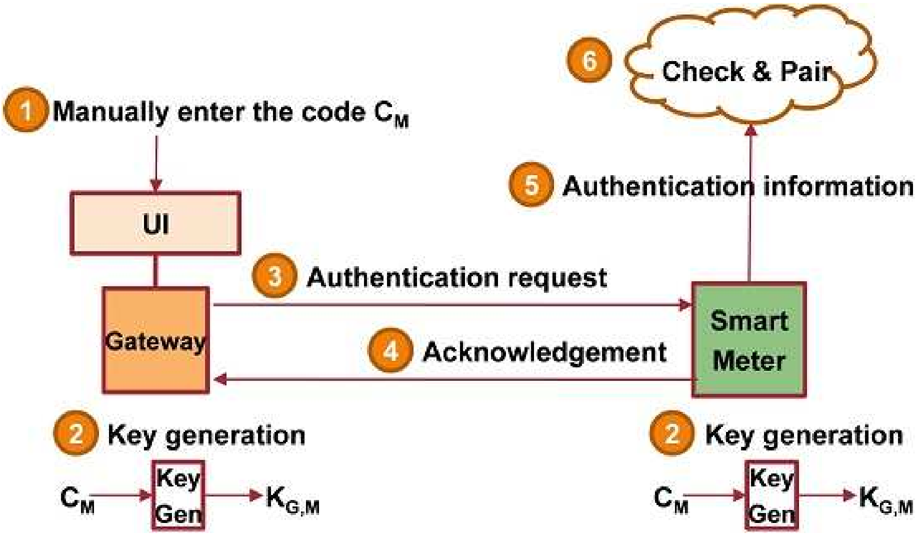

Fig. 5. Authentication mechanism between the gateway and the SM when the gateway has no Utility connection.

We assume that every SM has a unique code (C_M) associated to its unique ID. This code can be either written on the meter or provided to the user by the Utility. We further assume that both the SM and the gateway can generate a pair-wise key, $\mathrm{K_{G,M}}$ (which is at least 128-bits long) from this unique code via a key generator [1], [20].

User initiates the authentication process by manually entering $\mathrm{C_M}$ to the gateway via the UI and the gateway generates $\mathrm{K_{G,M}}$ via its key generator. Next, the gateway sends the following message to the SM.

$$\left\{\mathrm{E_{K_{G,U}}(C_M), MAC\left(K_{G,U}, E_{K_{G,U}}(C_M)\right), MAC\left(K_{G,M}, ID_G\right), ID_G}\right\}. \tag{27}$$

The first part of (A.1) is for the Utility and is encrypted with the pair-wise key between the gateway and the Utility, $\mathrm{K_{G,U}}$. Further, by verifying the MAC (which is generated by $\mathrm{K_{G,M}}$) in the second part of (A.1), the SM confirms that the message is coming from the correct gateway, and hence, authenticates the gateway. If the MAC is verified by the SM, it forwards the following message to the gateway.

$$\left\{\mathrm{MAC\left(K_{G,M}, ID_M\right), ID_M}\right\}. \tag{28}$$

Once the gateway receives (A.2), it also authenticates the SM by verifying the MAC attached to (A.2). Finally, the SM sends the following message to the Utility for the final verification.

$$\Bigg\{\mathrm{E_{K_{M,U}}(ID_G), MAC\left(K_{M,U}, E_{K_{M,U}}(ID_G)\right)},$$
$$\mathrm{E_{K_{G,U}}(C_M), MAC\left(K_{G,U}, E_{K_{G,U}}(C_M)\right), ID_M, ID_G}\Bigg\}. \tag{29}$$

The Utility verifies the MACs in (A.3) to make sure that both the SM and the gateway authenticated the correct devices. Further, once the authentication is verified, the Utility pairs the SM and gateway together and stores this in its database. We note that this authentication process prevents the MITM attack as we assume that the attacker does not have access to $\mathrm{C_M}$.

REFERENCES

[1] Zigbee alliance, zigbee smart energy profile 2.0 technical requirements document .

[2] Cisco, Securing the smart grid http://www.ciscosystemsnetwork.net/web/strategy/docs/energy/SmartGridSecurity_wp.pdf 2009.

[3] M. Davis, Smart grid device security - adventures in a new medium, Proceedings of Black Hat Conference 2009.

[4] N. Sastry, D. Wagner, Security considerations for IEEE 802.15.4 networks, Proceedings of the 3rd ACM workshop on Wireless security (WiSe '04) 2004.

[5] Wi-Fi Alliance, Introducing Wi-Fi protected setup http://www.wi-fi.org/wifi-protected-setup 2007.

[6] INSTEON, Developer's guide http://www.insteon.net.

[7] Z-wave http://www.z-wave.com.

[8] H. Khurana, R. Bobba, T. Yardley, P. Agarwal, E. Heine, Design principles for power grid cyber-infrastructure authentication protocols, Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS '10) 2010.

[9] 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 2008.

[10] F. Cohen, The smarter grid, IEEE Security and Privacy, vol. 8, no. 1, pp. 60-63, 2010.

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

[12] M. Fabro, T. Roxey, M. Assante, No grid left behind, IEEE Security and Privacy, vol. 8, no. 1, pp. 72-76, 2010.

[13] A. R. Metke, R. L. Ekl, Security technology for smart grid networks, IEEE Transactions on Smart Grid, vol. 1, no. 1, pp. 99-107, 2010.

[14] C.Valli, The not so smart, smart grid - potential security risks associated with the deployment of smart grid technologies, Proceedings of the 7th Australian Digital Forensics Conference 2009.

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

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

[17] D. Wei, Y. Lu, M. Jafari, P. Skare, K. Rohde, An integrated security system of protecting smart grid against cyber attacks, Proceedings of the 1st IEEE PES Conference on Innovative Smart Grid Technologies 2010.

[18] A. Hamlyn, H. Cheung, T. Mander, L. Wang, C. Yang, 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 2008.

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

[20] R. Yuan, W. T. Strayer, Virtual private networks: technologies and solutions 2001.

[21] N. Doraswamy, D. Harkins, IPSec: the new security standard for the internet, intranets, and virtual private networks 1999.

Erman Ayday is a Post-Doctoral Researcher at Ecole Polytechnique Federale de Lausanne (EPFL), Switzerland, in the Laboratory for Communications and Applications 1 (LCA1). He received his M.S. and Ph.D. degrees from the School of Electrical and Computer Engineering (ECE), Georgia Institute of Technology, Atlanta, GA, in 2007 and 2011, respectively. He received his B.S. degree in Electrical and Electronics Engineering from the Middle East Technical University, Ankara, Turkey, in 2005. His research interests include wireless network security, privacy, game theory for wireless networks, trust and reputation management, and recommender systems. Erman Ayday is the recipient of 2010 Outstanding Research Award from the Center of Signal and Image Processing (CSIP) at Georgia Tech and 2011 ECE Graduate Research Assistant (GRA) Excellence Award from Georgia Tech. He is a member of the IEEE and the ACM.

Sridhar Rajagopal is a staff engineer at Samsung Telecommunications America, Dallas. His research interests include wireless communication systems, computer architecture, computer arithmetic, and parallel computing. Sridhar has PhD and MS degrees in electrical and computer engineering from Rice University, and a BE in electronics engineering from VJTI, Mumbai University, India. He is a senior member of the IEEE.