Secure and Privacy-Preserving AMI-Utility Communications via LTE-A Networks

Zaher Haddad†‡, Mohamed Mahmoud‡, Sanaa Taha‡, and Imane Aly Saroit †
†Department of Electrical & Computer Engineering, Tennessee Tech University, Cookeville, TN, USA
‡Department of Information Technology, Cairo University, Cairo, Egypt
†Department of Electrical & Computer Engineering, Aqsa University, Gaza, Palestine

Abstract—In smart grid Automatic Metering Infrastructure (AMI) networks, smart meters should send consumption data to the utility company (UC) for grid state estimation. Creating a new infrastructure to support this communication is costly and may take long time which may delay the deployment of the AMI networks. The Long Term Evolution-Advanced (LTE-A) networks can be used to support the communications between the AMI networks and the UC. However, since these networks are owned and operated by private companies, the UC cannot ensure the security and privacy of the communications. Moreover, the data sent by the AMI networks have different characteristics and requirements than most of the existing applications in LTE-A networks. For example, there is a strict data delay requirement, data is short and transmitted every short time, data is sent at known/predefined time slots, and there is no handover. In this paper, we study enabling secure and privacy preserving AMI-UC communications via LTE-A networks. The proposed scheme aims to achieve essential security requirements such as authentication, confidentiality, key agreement and data integrity without trusting the LTE-A networks. Furthermore, an aggregation scheme is used to protect the privacy of the electricity consumers. It can also reduce the amount of required bandwidth which can reduce the communication cost. Our evaluations have demonstrated that our proposals are secure and require low communication/computational overhead.

Index Terms—Smart grid AMI; LTE security and privacy preservation; Data Aggregation; Key Management.

I. INTRODUCTION

The smart grid is a revolutionary upgrade to the existing power grid. It is characterized by two-way communications and power flow between the grid and the consumers [1], [2]. The smart grid aims to improve the grid’s reliability via self-healing and generate and distribute power efficiently, which can reduce electricity prices [3]. An important component of smart grid is called Automatic Metering Infrastructure (AMI) networks which provide two-way communications between smart meters (SMs) and the utility company (UC). The smart meters should send fine-grained data consumption to the UC to monitor the power demands over short periods and estimate the grid state [4]. The readings’ transmission rate can be less than 30 seconds for business premises and less than 15 minutes for residential ones [5].

Creating a new infrastructure to support the AMI-UC communications is costly and may take long time which may delay the deployment of the AMI networks. The Long Term Evolution-Advanced (LTE-A) network is a packet based cellular network specified by the Third Generation Partnership Project (3GPP) towards fourth-generation (4G) mobile. It aims to enhance the capacity of cellular networks by providing higher bit rate in a cost efficient way [6]. Brown et al. [7] investigated the possibility of using the LTE technology in the smart grid, and they concluded the LTE-A network has the following attractive features that can make it a good choice for smart grid applications: (1) Flat architecture: all radio related protocols are defined between the subscriber and the base station, and (2) Flexible spectrum usage: LTE-A supports both sorts of mode of operations; frequency division dupplex that allows subscribers to use different spectrum allocations for uplink/downlink and time division dupplex that allows subscribers to use one spectrum allocation for the uplink/downlink ensuring both of them efficient simultaneously. In this paper, we will use time division dupplex to send the meters’ data.

LTE-A network is a promising way to support the communications between the AMI networks and the UC because of their large coverage area and high availability. However, since these networks are owned and operated by private companies, the UC cannot ensure the security and privacy of the communications. The LTE-A operator may examine the meters’ data to obtain sensitive information about the electricity consumers, e.g., when they sleep, wake up, return home etc. They can also analyze the data to figure out the appliances used by consumers. An aggressive operator may alter the meters’ data to send wrong data to the UC. Moreover, the data sent by the AMI networks has different characteristics and requirements than most of the existing applications in LTE-A networks [4]. For example, there is a strict requirement on data delivery delay and the meters transmit a large number of small-size packets, e.g., the sessions are short and thus it is not efficient to exchange several packets to setup a connection. Unlike phone calls, data is sent at known/predefined time slots, and there is no handover because meters are stationary. The amount of transmitted data is known and expected which can help better design the base stations. A good AMI-UC communication protocol via LTE-A should not trust the LTE-A networks and should consider the characteristics of the AMI communications. Specifically, it should allow the transmission of a large number of small-size packets with low latency and minimum communication overhead to reduce the communication cost.

In this paper, we study enabling secure and privacy preserving AMI-UC communications via LTE-A networks. The proposed scheme aims to achieve essential security require-
ments such as authentication, confidentiality, key agreement and data integrity without trusting the LTE-A networks. First, we discuss a key agreement protocol to enable the SMs, the UC, and the LTE network to share keys. These keys are used for securing the communications and masking the meters’ readings to preserve privacy. Then, we use an aggregation scheme to aggregate the meters’ consumption data to protect the consumers’ privacy. Data aggregation can also reduce the amount of required bandwidth which can reduce the communication cost. In order to eliminate the overhead of sending several packets for connection setup, we use time multiplexing technique where each meter sends its reading in a reserved time slot assigned by the LTE network. This can reduce the communication overhead and the delay. Our evaluations have demonstrated that our schemes are secure and require low communication/computational overhead.

The remainder of this paper is organized as follows. The related works are discussed in section II. Section III presents the system models. Section IV presents the design goals. Section V discusses the proposed scheme. The security and privacy analysis are explained in Section VI. Performance evaluations are given in Section VII, followed by conclusions in Section VIII.

II. RELATED WORK

Gerasimenko et. al. [8] expect that the LTE-A networks will be used to support the SMs’ communications. Eissa et. al. [9] investigate the performance of the wireless communication scheme used for collecting data from phase measuring units (PMUs). The performance of LTE network from the point of view of the communication standard and PMUs data transmission is discussed. Wu et. al. [10] propose an experimental access layer platform for power distribution network based on LTE technology. Cheng et. al. [11] focus on applying LTE technology to build a high-reliable and low-latency Distribution Automation network for the smart grid. Cao et. al. [12] propose an electric power wireless communication network. The system is designed based on LTE technology, and rebuilds its physical layer according to the need of the power system. Chen et. al. [13] analyzed the physical layer and the MAC protocol capability of the LTE-A to perform machine-to-machine communication.

Cao et. al. [14] propose a group-based authentication scheme for a large number of machine-type-communication devices. Ya et. al. [15] proposed a smart grid communication architecture based on home area network, cognitive wide area network, and cognitive neighborhood area network. Therefore, authors conclude that the proposed architecture is able to intelligently allocate spectra to support the communication requirements of the smart grid such as data volume, data traffic, and quality of services. Liu et. al. [16] focused on designing a massive a machine access control protocol for heterogenous M2M network where the devices have different services requirements such as channel utility, packet drop ratio, average transmission delay, and energy consumption. Although extensive attention has been paid to smart grid recently (e.g., [17]), using the LTE networks to support the smart grid communications has received limited attention. Also, although privacy in different wireless networks have received extensive attention recently [18]–[25], these schemes cannot be used in our problem because they address different network and threat models. Costantio et.al. [26] investigated the suitability of LTE for the interconnection of aggregated edge devices in the Internet of Things. In [3], Akula et al propose a scheme to enable energy storage units to communicate with the utility without revealing any private information. Unlike this work, we address AMI networks in this work and aim to preserve the privacy of the power consumption data.

III. SYSTEM MODELS

A. Network Model

As shown in Fig. 1, the considered network has three main entities: the UC, the LTE-A network, and the AMI networks. The AMI networks and the UC communicate via LTE-A network. The LTE-A network has two main parts: the core network and the Radio Access Network. The core network has a set of switches, servers, etc. with mostly wired communications [4]. The core network connects the evolved node B (eNB) with the UC. The radio access network is the wireless part that connects the subscribers (meters) with the eNB [27]. We consider two different topologies to the AMI networks: single and multi-hop. In single-hop AMI networks, the smart meters communicate with the eNB in one hop. Each smart meter has a Subscriber Identity Module (SIM) card with a unique identifier similar to the ones used in cell phones. In multi-hop AMI networks, multi-hop packet relay may be employed to enable the meters to communicate with a lead meter (or a gateway) that connects the meters to the eNB. The eNB sends the data to the LTE core network to send to the UC. The communications between the meters and the UC can be bidirectional, i.e., the meters or the UC can initiate the communication sessions.

B. Adversary Model

The UC and the LTE-A network are interested to know the consumers’ power consumption data. They do not collude because they are owned and operated by two different authorities.

Figure 1: The considered network model.
The meters are interested to know others consumption data. Attackers can also eavesdrop on the network transmission to figure out sensitive information, such as power consumption data. The LTE-A networks can alter or fabricate the meters’ consumption data. The UC is interested in the proper operation of the system and it does not aim to launch active attacks such as altering the consumption data.

Some attackers record valid data transmission packets and retransmit them in the same AMI or a different one to let the eNB and the UC believe that the data is sent by the meters. In Man in the Middle Attack (MitM), a node (may be in the network core) is located between a meter and the UC and tries to communicate with the meters as if it is the UC and communicates with the UC as if it is the meter. When a meter wants to establish a shared key with the UC, the attacker tries to share a key with the meter and another key with the UC so that it can decrypt the exchanges messages. MitM attack is a threat in our network model because the LTE-A network is not trusted. In Impersonation attack, the attacker tries to impersonate one entity that can be a meter, eNB, or the UC, to send data under its name. For instance, if an attacker could impersonate a meter, it can send false consumption data.

IV. DESIGN GOALS

In this paper, we aim to achieve the following objectives:

1) **Mutual authentication**: The UC, the eNB, and the SMs need to mutually authenticate each other in order to protect the system from the attacks that can be launched by external attackers, such as launching denial of service attacks (by sending false packets) and impersonation attacks.

2) **Key agreement**: The UC and the SMs should share secret keys to secure their communications.

3) **Key evolution**: It is a very common practice to periodically refresh the shared secret keys. This can protect against cryptanalysis and lessen the amount of information the attacker can obtain if a key is exposed. Forward secrecy is a very desirable property where the attackers cannot derive the new key if the current one is exposed.

4) **Confidentiality/data integrity and authenticity**: The unintended nodes should not be able to interpret the packets. This is important to preserve the privacy of the consumers from eavesdroppers who sniff the data consumption packets. Moreover, the recipient of a packet should be able to ascertain that the packet has been sent by the intended node and it has not been modified during transition.

5) **SM revocation**: The UC should be able to revoke the SMs (invalidate their credentials), e.g., in case of compromised meters.

6) **Secure and privacy preserving data aggregation**: The consumers need to assure that their consumption data cannot be obtained by the LTE-A network or the UC to preserve their privacy. The UC needs to ensure that the aggregated consumption data is sent from the intended meters and it has not been altered, without accessing the meters’ individual data.

V. PROPOSED SCHEMES

In this section, we explain authentication, key agreement and aggregation schemes.

A. Initialization phase

In this phase, the UC bootstraps the whole system. It chooses a random large prime number $q$, $Z_q$ is a finite field of order $q$ and $G$ is an additive group of order $q$ and generator $P$. $G_T$ is a multiplicative group of order $q$ and $H_1$ and $H_2$ are two one-way hash functions, where $H : \{0, 1\}^* \rightarrow G$ and $H_1 : \{0, 1\}^* \rightarrow Z_q$. $\hat{e}$ is a bilinear pairing function, where $\forall P$ and $Q \in G$, $\hat{e}(P, Q) \rightarrow G_T$. Moreover, $\forall a, b \in Z_q$, $\hat{e}(aP, bQ) = \hat{e}(bP, aQ) = \hat{e}(abP, Q) = \hat{e}(P, abQ) = \hat{e}(P, Q)^{ab}$ [28]. The UC chooses a random element $sk_u \in Z_q$ and computes $PK_u = sk_uP$, where $sk_u$ and $PK_u$ are the private and public keys, respectively. The UC publishes $\{q, P, PK_u, G, H, H_1, \hat{e}\}$ and keeps $sk_u$ secret.

For each $eNB_j$, the UC chooses a random element $sk_j \in Z_q$ and computes $PK_j = sk_jP$ as private and public keys, respectively. Similarly, for each smart meter $i$, the UC chooses a random element $sk_i \in Z_q$ as a private key and computes the public key $PK_i = sk_iP$. The UC issues certificates to the meters and the eNBs to bind the public key with the identifier.

B. Authentication and key agreement

The scheme presented in this section aims to mutually authenticate the smart meters to the UC and eNB. The scheme also aims to establish shared key between the meters and the UC. This key will be used to send the reading data. This scheme is run in one of these cases: a new smart meter is first deployed; a meter loses synchronization with the eNB (will explained later in details); and a meter refreshes the shared keys with the eNB and UC. As illustrated in Fig. 2, our authentication and key agreement scheme is executed as follows:

1) $SM_i$ composes an authentication request packet and sends it to $eNB_j$. The packet has the identifiers of the meter, eNB and UC ($id_i$, $id_j$ and $id_u$, respectively), and

![Figure 2: Authentication and key agreement.](image-url)
Then, it verifies freshness of the packet and drops stale packets. It also has the identifiers of the meters, the eNB and the UC. It also request packet to the UC. As illustrated in Fig. 2, the packet follows:

\[ \pi \]

The same

\[ \hat{e}(\sigma_i, P) = \hat{e}(sk_i, H(id_i||id_j||id_u||r_iP||TS), P) \]

\[ = \hat{e}(H(id_i||id_j||id_u||r_iP||TS), sk_iP) \]

\[ = \hat{e}(H(id_i||id_j||id_u||r_iP||TS), PK_i) \]

If the signature verification is valid, eNB \( j \) composes aggregated signature (\( \sigma_i \)), where \( \sigma_i = \sigma_i + \sigma_j \) and \( \sigma_i = sk_j, H(id_i||id_j||id_u||r_iP||TS) \). Obviously, signature aggregation can reduce the packet overhead because the size of the aggregated signature is less than appending two signatures from eNB \( i \) and SM \( i \). Finally, eNB \( j \) sends authentication request packet to the UC. As illustrated in Fig. 2, the packet has the identifiers of the meters, the eNB and the UC. It also has the aggregated signature and the certificates of the the eNB \( j \) and the SM \( i \).

3) The UC verifies the timestamp to verify the freshness of the packet, and verifies \( \sigma_i \) by checking whether \( \hat{e}(\sigma_i, P) = \hat{e}(H(id_i||id_j||id_u||r_iP||TS), PK_i + PK_j) \). The signature verification can prove that the packet has been sent from SM \( i \) via eNB \( j \). The proof of the signature verification is as follows:

\[ \hat{e}(\sigma_{ij}, P) = \hat{e}(\sigma_i + \sigma_j, P) \]

\[ = \hat{e}(sk_i, H(id_i||id_j||id_u||r_iP||TS)) \]

\[ + sk_j, H(id_i||id_j||id_u||r_iP||TS), sk_iP \]

\[ = \hat{e}(sk_i + sk_j), H(id_i||id_j||id_u||r_iP||TS), P \]

\[ = \hat{e}(H(id_i||id_j||id_u||r_iP||TS), (sk_i + sk_j)P) \]

\[ = \hat{e}(H(id_i||id_j||id_u||r_iP||TS), sk_iP + sk_jP) \]

\[ = \hat{e}(H(id_i||id_j||id_u||r_iP||TS), PK_i + PK_j) \]

Then, the UC chooses a random element \( r_u \in Z_q \) and computes the two secrets \( \pi_i \) and \( k_i \) that are shared with the meter, where \( \pi_i = H_1(\hat{e}(PK_u, sk_u, r_2, r_1P)) \) and \( k_i = H_1(\pi_i || PK_u) || PK_u \). \( k_i \) is a long-term shared that is used to ensure the readings’ integrity and authenticity but \( \pi_i \) is one-time mask value that will be used to preserve the consumers’ privacy by masking the readings. The UC computes a proof for correctly calculating the key \( D_1 = H(\pi_i || K_i || 1) \). Finally, the UC sends the authentication response packet to the SM \( i \). The packet has \( r_u P \) and \( D_1 \) as illustrated in Fig. 2.

4) SM \( i \) computes \( \pi_i \) and \( k_i \) as follows: \( \pi_i = H_1(\hat{e}(PK_u, sk_u, r_2, r_1P)) \) and \( k_i = H_1(\pi_i || PK_u) || PK_u \). Then, it verifies \( D_1 \) to make sure that the UC has computed the same \( \pi_i \) and \( k_i \). SM \( i \) computes a proof for correctly calculating the shared secrets \( D_2 = H(\pi_i || K_i || 2) \) and sends the authentication confirmation packet to the UC. The packet has \( id_i, id_j, id_u, TS, D_2, \) and \( \sigma_{ij} \).

5) The UC verifies \( D_2 \) and sends the authentication completion packet to the eNB \( j \). The the packet has \( id_i, id_j, id_u, TS, \) and \( \sigma_U \).

6) Once the eNB \( j \) receives the packet, it allocates a time slot to the meter to transmit its readings and sends it to the meter. The packet has \( id_i, id_j, time\ slot, \sigma_j \).

C. Key management

**Key Renewal:** It is a very common practice to periodically refresh the shared secret keys. This can protect against cryptoanalysis and lessen the amount of information the attacker can obtain if a key is exposed. Forward secrecy is a very desirable property where the attackers cannot derive the old keys if the current one is exposed. The symmetric key (\( k_i \)) and the initial mask value (\( \pi_i \)) should be updated after some time of use. If a key is compromised, the attacker should not be able to use this to compute the next keys. This property is called forward secrecy. In our scheme, each key has a predefined lifetime and before it expires, the meter should initiate a new authentication/key agreement scheme to update the key. Since \( r_i \) and \( r_u \) are random, the meter and the UC calculate a new key each time they run the scheme. In addition, forward secrecy property can be achieved because \( k_i \) and \( \pi_i \) are not used to compute the new ones, i.e., the knowledge of \( k_i \) and \( \pi_i \) does not help the attacker to calculate the new key.

**Key Revocation:** There are several cases that necessitate revoking the meters’ keys before they expire. Some of these cases are as follow.

- **Key compromise:** The secret keys of a meter is compromised. If the key is not revoked, the attacker who knows the keys can impersonate the meter without any suspicion.
- **End of a meter’s purpose:** The purpose of the meter for which its keys were issued does not exist anymore, e.g., defective meters and meters deployed for a temporary purpose such as makeshift premises.
- **Malicious behavior:** If the system loses trust in a meter, e.g., due to evident malicious behavior, the system must promptly revoke its credentials.
- **Insecure key length:** Key revocation is necessary when the secure key length becomes more than the used one. This might be due to advances in cryptoanalysis and computing capabilities.

All packets sent by revoked keys should be discarded by both the UC and the eNB. The time slot of the revoked SM becomes free and the eNB may need to redefine the time slots of the meters. In our scheme, the meters should use their certificates to share a key with the UC. If a meter’s certificate is revoked, eNB \( j \) does not accept the authentication request message and the meter cannot establish a key. Certificate revocation is out of scope and we refer to references [29]–[33].
D. Data Aggregation

In order to eliminate the overhead of connection establishment, we use a time multiplying technique to collect the meters’ readings. In each time frame, the eNB collects one reading from each meter. As illustrated in Fig. 3, each time frame is divided into slots and a small guard period separates between each two slots. The eNB assigns one time slot for each meter to send its reading. In this subsection, we explain data aggregation scheme and a pairing-based message authentication code that are variations from the ones proposed in [3]. The aggregation scheme can achieve two main objectives: preserving consumer privacy and reducing the required bandwidth to send the data to the UC by reducing the data size. The pairing-based message authentication code can enable the utility to ensure the integrity of the aggregated power data size. The pairing-based message authentication code that are variations from the ones proposed in [3]. The aggregation scheme can achieve two main objectives: preserving consumer privacy and reducing the required bandwidth to send the data to the UC by reducing the data size. The pairing-based message authentication code can enable the utility to ensure the integrity of the aggregated power consumption without accessing the individual measurements to preserve consumer privacy.

From Fig. 4, each smart meter sends a packet having its measurement reading in its assigned time slot. After eNB receives all the meters’ packets, i.e., in one time frame, it composes a packet for the aggregated readings and sends the packet to the UC. The SM_i masks its reading using a one time mask value \( \pi_i^{(j)} \), where \( \pi_i^{(j)} = \pi_i^{(j-1)} \) and \( j \geq 1 \) and \( \pi_i^{(0)} \) is computed in the authentication scheme. Each mask value is used only for one message, \( C_i = (m_i + \pi_i^{(j)})P \), where \( m_i \) is a fine-grained power consumption. The meter also computes a pairing-based message authentication code \( \text{PMAC}_i = \hat{e}(P, (m_i + k_i\pi_i^{(j)})P) \). The meter sends \( C_i, \text{PMAC}_i \), in addition to its signature \( \sigma_i = sk_iH(C_i||\text{PMAC}_i) \).

The eNB verifies the meters’ signatures to ensure the packets’ authenticity and integrity. This can be done by verifying that \( \hat{e}(P, \sigma_i) = \hat{e}(PK_i, H(C_i||\text{PMAC}_i)) \). However, in order to reduce the computation overhead, a batch verification technique can be used instead of individually verifying the signatures [34]. Batch verification requires \( n+1 \) pairing operations while individual signature verification requires \( 2n \) pairing operations, where \( n \) is the number of signatures. The eNB accepts a batch of signatures if \( e(P, \sum_{i=0}^{n} \sigma_i) = \prod_{i=0}^{n} e(P, PK_i, H(C_i||\text{PMAC}_i)) \). The proof of this is as follow:-

\[
e(P, \sum_{i=0}^{n} \sigma_i) = e(P, \sum_{i=0}^{n} k_iH(C_i||\text{PMAC}_i))
= \prod_{i=0}^{n} e(P, k_iH(C_i||\text{PMAC}_i))
= \prod_{i=0}^{n} e(PK_i, H(C_i||\text{PMAC}_i))
\]

The eNB aggregates the meters’ readings and PMACs. The value of the aggregated readings is \( C = \sum_{i=1}^{n} C_i \) and \( \text{PMAC} = \prod_{i=1}^{n} \text{PMAC}_i \). Finally, eNB signs the packet and sends it to the UC, where \( \sigma_j = sk_jH(C||\text{PMAC}) \).

The UC verifies the signature and calculates the total readings as follows. \( \sum_{i=1}^{n} m_iP = C - \sum_{i=1}^{n} \pi_i^{(j)}P \). This is because \( C = \sum_{i=1}^{n} m_iP + \sum_{i=1}^{n} \pi_i^{(j)}P \). Then, using \( \sum_{i=1}^{n} m_iP \), the UC can compute \( \sum_{i=1}^{n} m_i \). To do this computation, the UC can do exhaustive search until it finds \( \sum_{i=1}^{n} m_i \) or it can pre-compute some values for \( \sum_{i=1}^{n} m_i \) with different values of \( \sum_{i=1}^{n} m_i \) and use these values to figure out the value of \( \sum_{i=1}^{n} m_i \). In order to ensure that the readings are sent from the intended meters and they have not been modified in transition, the UC verifies whether \( \text{PMAC} = \hat{e}(P, P)\sum_{i=1}^{n} m_i + \sum_{i=1}^{n} (k_i\pi_i^{(j)}) \). The proof of this is as follows:-

\[
\text{PMAC} = \prod_{i=1}^{n} \text{PMAC}_i \\
= \prod_{i=1}^{n} \hat{e}(P, (m_i + k_i\pi_i^{(j)})P) \\
= \hat{e}(P, (m_1 + k_1\pi_1^{(j)})P)\hat{e}(P, (m_2 + k_2\pi_2^{(j)})P) \\
...\hat{e}(P, (m_n + k_n\pi_n^{(j)})P) \\
= \hat{e}(P, (\sum_{i=1}^{n} m_i + \sum_{i=1}^{n} (k_i\pi_i^{(j)}))P) \\
= \hat{e}(P, P)\sum_{i=1}^{n} m_i + \sum_{i=1}^{n} (k_i\pi_i^{(j)}) 
\]
VI. Security and Privacy Analysis

The security of our scheme is based on the following known mathematical difficulties. Discrete logarithm difficulty: given \( P \) and \( aP \), it is infeasible to calculate \( a \) [28] if \( a \) is a large number. Actually, if \( a \) is a small number, it is easy to compute it. This has been used to compute \( \sum_{i=1}^{n} m_i \) from \( \sum_{i=1}^{n} m_i P \). The second difficulty we used is the unidirectionality of the hash function. If the mask value \( \pi^{(k)} \), is compromised, the attacker cannot figure out the old readings because it is infeasible to compute \( \pi^{(j-1)}_i \) from \( \pi^{(j)}_i \).

Our scheme is resilient to packet replay attack. In this attack, the attacker records valid packets and replay them in a different place or time to pretend as they are fresh. We consider two cases: packets are replayed either by external attacker or LTE-A. If the eNB or the UC cannot detect this attack and accept the stale packets, this can cause chaos to the readings collection technique. The use of timestamp enables the nodes to identify stale packets and drop them. Also, since each mask value \( \pi^{(j)}_i \) is used for only one packet, the verification of the PMAC fails if the attacker replays a packet that uses old mask value. PMAC does not only enable the UC to verify readings integrity and authenticity but also freshness. In impersonation attacks, the attacker tries to impersonate the eNBs, the UC or the meters. These attacks are infeasible in our scheme because of using signatures. The attackers cannot compute valid signatures because they do not know the private keys.

In man-in-the-middle attack, the attacker that resides between a meter and the UC tries to establish two keys: one with the UC and the other with the meter to fool the meter and the UC to believe that they communicate with each other directly. The attacker can sniff on the communications between the meter and the UC or impersonate the meter and the UC. Our scheme is resilient to this attack because the private keys of the meters and UC, that are not known to the attackers, are used to secure the authentication/key agreement scheme. If the attack is successful, the attacker can know \( k_i \) and \( \pi^{(0)}_i \) and use them to sniff the meter’s readings or send false readings under its name. Resilience to this attack is important because the communications have to be transmitted via the LTE-A network that is not trusted. If an attacker tries to use a meter’s credentials at a different eNB, it needs to run the authentication/key management scheme. In this case, the UC denies the authentication request.

In order to preserve the consumers privacy, each meter should mask its readings with a secret mask. Given \( (m_i + \pi^{(j)}_i)P \) and \( P \), it is infeasible to calculate \( m_i \). Eavesdroppers and LTE-A networks cannot figure out the readings \( m_i \) because they do not know the secret mask. The eNB sends the aggregated readings to the UC that uses the masks to obtain the total readings. The UC cannot obtain the meters’ readings because it has no access to the individual readings and there is no way to decompose the aggregated readings. The existing schemes assume that the AMI gateway and the UC do not collude [34] but we assume that the LTE-A network and the UC do not collude. Our assumption is more realistic because the the LTE-A networks and the UC are owned and operated by different authorities but the UC will mostly own the gateways. The use of each mask value for only one reading can boost the privacy preservation and security of the scheme. If the same mask is used in two messages, the attacker can calculate the difference between the two readings but he still cannot know the readings. Specifically, given two readings sent from a meter at two different times \( C_1 = (m_1 + \pi^{(j)}_i)P \) and \( C'_1 = (m'_1 + \pi^{(j)}_i)P \), the attacker can calculate \( C_1 - C'_1 = (m_1 - m'_1)P \). Using this value, the attacker can calculate \( m_1 - m'_1 \).

The proposed scheme can achieve the desirable forward secrecy property. If a meter is compromised and the key \( k_i \) is exposed, it is infeasible to calculate the previously used keys because they were calculated using one-use random numbers (\( r_i \) and \( r_u \)) that are not stored in the meter. Moreover, if the attacker could figure out \( k_i \), he cannot use it to calculate the next keys or the previous. He cannot also use it to calculate \( \pi^{(j)}_i \), where \( j \geq 1 \) because hash functions are one way, i.e., there is no way to obtain \( \pi^{(0)}_i \) from \( k_i = H_1(\pi^{(0)}_i||PK||PK_u) \). Given the key \( k_i \), it is infeasible to calculate the next key when it expires because each time the authentication/key agreement scheme is run, the meters and the UC use new random numbers (\( r_i \) and \( r_u \)). If a device is compromise, the attacker can calculate the old mask values and thus he cannot compute the old readings. The meters should only store the last mask value so that if the meter is compromised the attacker cannot obtain the old mask values and thus he cannot compute the old readings.

In addition, the masked value \( \pi^{(0)}_i \) is used for only one packet. If \( \pi^{(j)}_i \) is exposed, the attacker can calculate the meter’s readings until the meter runs the authentication/key agreement protocol to update \( \pi^{(j)}_i \). That is why it is always a good idea to frequently update the key. However, the attacker cannot calculate the meter’s old readings or the key \( k_i \) because hash functions are one way, i.e., given \( \pi^{(j)}_i \) there is no way to calculate \( \pi^{(x)}_i \), where \( 1 \leq x < j \) and \( \pi^{(j)}_i = H_1(\pi^{(j-1)}_i) \). We can call this property forward privacy preservation. In the key agreement scheme, \( k_i \) and \( \pi_i \) are computed mutually by the UC and the SMs. Neither the meters nor the UC has full control on the computed key because the contributions (random values) are needed for both sides. This is a desirable property because if the key calculation is done by one party, the chance of selecting weak key is higher.

VII. PERFORMANCE EVALUATIONS

In this section, we evaluate the performance of the proposed scheme.

A. Communication Overhead

The communication overhead is measured by the amount of data (in Bytes) that should be transmitted. We assign two byte for each identifier, 160 bits for \( q \), 20 bytes for each elliptic curve point, and 20 bytes for signatures. A standard certificate should have a public key, an identifier, the issuer’s identifier,
the issuing data, the expiry date and a signature. The size of each certificate and the timestamp are 54 and 5 bytes, respectively.

1) Authentication and Key Agreement Scheme: The size of the SM’s authentication request (\(id_i, id_j, id_u, r_iP, TS, \sigma_i, Cert_i\)) is \(2 + 2 + 2 + 20 + 5 + 20 + 54 = 105\) Bytes. The size of the eNB’s authentication request (\(id_i, id_j, id_u, r_iP, TS, \sigma_ij, Cert_i, Cert_j\)) is \(2 + 2 + 2 + 20 + 5 + 20 + 54 + 54 = 159\) Bytes. The size of the UC’s authentication response (\(id_i, id_j, id_u, TS, r_uP, D_1, \sigma_ij, Cert_i\)) is \(2 + 2 + 2 + 2 + 20 + 20 + 20 + 54 = 125\) Byte. The size of the SM’s authentication confirmation (\(id_i, id_j, id_u, TS, D_2, \sigma_ij\)) is \(2 + 2 + 2 + 5 + 20 + 20 = 51\) Bytes. Instead of two signatures \(\sigma_i\) and \(\sigma_j\), they are aggregated to produce a smaller size aggregated signature, where the size of the aggregated signature \(\sigma_ij\) equals to the size of the individual signatures. The size of the UC’s authentication completion message (\(id_i, id_j, id_u, TS, aU\)) is \(2 + 2 + 2 + 5 + 20 = 31\) Bytes. Finally, the BS’ time slot allocation packet (\(id_i, id_j, time\ slot, \sigma_j\)) is \(2 + 2 + 2 + 20 = 26\) byte.

2) Aggregation Scheme: The size of a SM’s power usage packet (\(C_i, PMAC_i, \sigma_i\)) is \(20 + 20 + 20 = 60\) Byte. The size of the eNB’s total power consumption packet of \(n\) meters (\(C_i, PMAC, \sigma_j\)) is 120 Bytes for any number of meters. The size of the data sent from the eNB to the UC does not depend on the number of meters in the AMI. This property is important as it can reduce the required bandwidth to transmit the data from eNBs to the UC. This can support the scalability of the AMI and reduce the cost of using LTE-A networks, which can support the use of LTE-A to connect the UCs with the AMIs.

B. Computation Overhead

The computation overhead is measured by the time required to compose a packet or perform an operation in milliseconds (ms). In our scheme, batch verification has been used to reduce the computation overhead. In the authentication and key agreement scheme, instead of verifying two signatures from SMi and eNBj, one aggregated signature is verified. The verification of the aggregated signature \(\sigma_ij\) takes the same time as verifying the individual signatures. Batch verification has also been used in the readings’ collection phase to reduce the number of pairing operations from \(2n\) to \(n + 1\). It is worth to point out that the computations in our scheme can be sped up by pre-computing some values. For example, \(\phi_{ij}(0)P\) for different values of \(j\) can be computed and stored. When the meter needs to send a reading, it can compute \(m_iP\) which is very efficient because \(m_i\) is small. Then, it adds \(m_iP\) to \(\phi_{ij}(0)P\) to obtain \((m_i + \phi_{ij}(0))P\). This is much faster than computing \((m_i + \phi_{ij}(0))\) first and then multiplying it by \(P\). Moreover, the values of \(m_iP\) at different values for \(m_i\) can be computed once and stored, so that when a meter sends a reading, it just picks up the stored value for \(m_iP\). This should also be memory efficient because the readings are sent every short period and thus the space of \(m_i\) is not large. The required memory space can be reduced by storing only the odd (or even) values of \(m_i\). If the reading is even, the meter can add \(P\) to the nearest odd value.

In our evaluations, we will focus on measuring the time required for performing the cryptographic operations because it is usually the main source of the packet delay. In [35], Scott used a 3-GHz Pentium computer system to measure the computation time of the cryptographic operations. The measurements are given in Table I. The cryptographic computational overhead in our scheme is as follows.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Operation</th>
<th>Computational time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\hat{\epsilon})</td>
<td>paring</td>
<td>4.14</td>
</tr>
<tr>
<td>(r_iP)</td>
<td>Point – Multiplication</td>
<td>0.86</td>
</tr>
<tr>
<td>(P + Q)</td>
<td>Point – Addition</td>
<td>0.58</td>
</tr>
<tr>
<td>(H)</td>
<td>Hash – Function</td>
<td>0.0065 Byte/ms</td>
</tr>
</tbody>
</table>

Table I: Computational time of required cryptographic operations.

1) Authentication and Key Agreement Scheme: The SM should compute \(\sigma_i = sk_iH(id_i \parallel id_j \parallel id_u \parallel r_iP \parallel TS)\) that takes \(0.16 + 51 * 0.0065 = 0.5215\) ms. The verification of a single signature requires two pairing operations like the aggregated signatures for any number of signatures. \(\pi_i(0) = H_1(\hat{\epsilon}(PK_u, sk_i, r_iP, id_u))\) takes \(3 * 1.57 + 4.14 + 20 * 0.0065 = 8.98\) ms, and \(k_i = H_3(\pi_i(0), PK_i, PK_u)\) takes \(60 * 0.0065 = 0.39\) ms. \(D_2 = H(k_i, 2)\) takes \(21 * 0.0065 = 0.1365\) ms. The eNB should compute \(\epsilon(\sigma_i, P) = \hat{\epsilon}(H(id_i \parallel id_j \parallel id_u \parallel r_iP \parallel TS, PK_i)\) that takes \(2 * 4.14 + 24 * 0.0065 + 0.19 = 8.639\) ms. It should also calculates \(\sigma_j = sk_jH(id_i \parallel id_j \parallel id_u \parallel r_iP \parallel TS)\) that takes \(0.16 + 24 * 0.0065 = 0.316\) ms. The UC should compute \(\hat{\epsilon}(\sigma_ij, P) \hat{\epsilon}(H(id_i \parallel id_j \parallel id_u \parallel r_iP \parallel TS), PK_i + PK_u)\) that takes \(2 * 4.14 + 24 * 0.0065 + 0.16 = 8.6065\) ms. It should also compute \(\pi_i(0) = H_1(\hat{\epsilon}(PK_i, sk_u, r_2P))\) that takes \(3 * 1.57 + 4.14 + 20 * 0.0065 = 8.98\) ms and computes \(k_i = H_3(\pi_i(0), PK_i, PK_u)\) that takes \(60 * 0.0065 = 0.39\) ms and \(d_i = H(K_i, 1)\) that takes \(21 * 0.0065 = 0.1365\) ms.

2) Aggregation Scheme: Each SM needs to compute \(C_i, PMAC_i, \sigma_i\), and \(\sigma_i\) that takes \(0.16 + 0.16 + 4.14 + 0.16 = 4.62\). The eNB aggregates all the signatures and verifies them as a batch. The batch verification needs two pairing operations that take \(2 * 4.14 = 8.25\) ms. The eNB computes the aggregated data usage \(\sum_{i=1}^{n} C_i\) that needs \(n - 1\) addition operations. Aggregating the pairing message authentication code for \(n\) meters needs \(n - 1\) point multiplications \(\prod_{i=1}^{n} PMAC_i\) that takes \(0.16 * (n - 1)\). The signature \(\sigma_i\) of the the eNB takes \(0.16\) ms. The UC verifies the signature of the eNB that takes \(2 * 4.14 = 8.25\) ms. Then, it verifies the integrity of the SMs data that takes \(2 * 4.14 + 1.57 = 9.85\) ms.

VIII. CONCLUSIONS

In this paper, we have proposed a scheme to enable the secure and privacy preserving AMI-UC communications via LTE-A networks. The proposed schemes can achieve essential security requirements such as authentication, confidentiality,
key agreement and data integrity without trusting the LTE-A networks. Furthermore, an aggregation scheme is used to aggregate the consumption data to protect the privacy of the electricity consumers. It can also reduce the amount of the required bandwidth which can reduce the communication cost. Our evaluations demonstrate that the proposed scheme can achieve our privacy and security objectives. We have calculated the computation delay and the communication overhead. The results indicate that the proposed scheme requires low computation and communication overhead.

REFERENCES


