DOI: 10.3969/j.issn.1673-5188.2015.03.003
http://www.cnki.net/kcms/detail/34.1294.TN.20150909.0929.002.html, published online September 9, 2015

Secure Communication Networks in the Advanced Metering Infrastructure of Smart Grid

Feng Ye and Yi Qian
(Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, Lincoln, NE 68124, USA)

Abstract

In this paper, a security protocol for the advanced metering infrastructure (AMI) in smart grid is proposed. Through the AMI, customers and the service provider achieve two-way communication. Real-time monitoring and demand response can be applied because of the information exchanged. Since the information contains much privacy of the customer, and the control messages need to be authenticated, security needs to be ensured for the communication in the AMI. Due to the complicated network structure of the AMI, the asymmetric communications, and various security requirements, existing security protocols for other networks can hardly be applied into the AMI directly. Therefore, a security protocol specifically for the AMI to meet the security requirements is proposed. Our proposed security protocol includes initial authentication, secure uplink data aggregation, secure downlink data transmission, and domain secrets update. Compared with existing researches in related areas, our proposed security protocol takes the asymmetric communications of the AMI and various security requirements in smart grid into consideration.

Keywords

smart grid; advanced metering infrastructure; network security; privacy

1 Introduction

In smart grid, the communication networks have been updated to more complicated and bidirectional ones. Data transmitted more frequently over the networks in much larger quantity. Therefore, compared with the communication in traditional power grid, network security issues are more important [1]–[3]. The advanced metering infrastructure (AMI) is a system that collects and analyzes data from smart meters, and giving intelligent management of various power-related applications and services based on that data. An AMI has a hierarchical network structure. It consists of home area networks (HANs), neighborhood area networks (NANs), and a wide area network (WAN). In each HAN, there is a smart meter which monitors the energy consumption of the appliances and other power line status in that household. Metering data (data that is generated by smart meters) is uploaded to the metering data management system (MDMS) at the service provider side. Based on the metering data and other monitoring data from sensors, the service provider is able to have precise real-time monitor over the power grid. Moreover, demand response [4]–[7] can be applied with timely information exchange between the customers and the service provider. As a result of the modern control system, smart grid is more efficient and eco-friendly compared with the traditional power grid. However, in order to achieve optimal control and demand response through the AMI, the data in uplink transmissions from smart meters to the MDMS includes secret information. For example, power usage of a household is included in metering data. Those data will be collected by the MDMS and be further applied to determine the power generation and the usage of renewable energy. Nonetheless, power usage pattern may reveal lifestyle of the corresponding customers. The controlling data in downlink transmissions involve the price/tariff information. Forgery or manipulation of such information may let the demand response be astray from being efficient.

In this paper, we propose a network security protocol for the AMI. The WAN in AMI is a high speed backhaul network, which has robust security mechanisms from fiber optic networks or ethernet. Therefore, the security issues in AMI. Thus, our focus is on the wireless portion of the AMI, including smart meters from HANs and data aggregate points (DAPs) from NANs. Specifically, the proposed network security protocol includes four parts: initial authentication, secure uplink data aggregation, secure downlink data transmission, and domain secrets update. Initial authentication is for the nodes such as smart meters and DAPs to join the AMI. Security schemes for

The work was supported by the National Science Fourdation under Grant No. CNS-1423408.

uplink and downlink transmissions are independently designed because of the asymmetric communications. Data in the uplink is more in quantity and higher in frequency. It features a many to-one communication. Moreover, aggregated data is enough, for instance, the aggregated power consumption for the service provider. Nonetheless, confidentiality of the controlling data in downlink may not be an issue. For instance, pricing/tariff is supposed to be public for the customers. Data integrity and sender authentication are more important for such controlling data. In addition, domain secrets such as session keys, public/private keys, and other secrets need to get refreshed once in a while. In the proposed domain secret update process, the communications remain uninterrupted.

The rest of the paper is organized as follows. In Section 2, related work is discussed. In Section 3, the studied AMI is illustrated. In Section 4, the security schemes for the AMI are proposed. In Section 5, the conclusion and the future work are given.

2 Related Work

Although HANs and NANs in the AMI have structures of wireless mesh networks (WMNs) [8], [9], difference can be addressed in three holds. First, each smart meter must be available and be treated equally in the network since fairness must be applied to each of the customers while traditional WMN does not emphasize availability for each wireless node let alone fairness. Second, the deployment of smart meters are fixed and in specific orders since they are deployed in each household and the houses are in fixed position in most cases, while the wireless nodes in traditional WMN are usually deployed randomly and redundantly. Third, the uplink transmission and downlink transmission in AMI are asymmetric where the uplink transmission consists of different data from each smart meter to the MDMS and the most of the downlink transmissions are in broadcast mode, while in traditional WMN, the uplink or downlink can even barely be distinguished. Our proposed network security protocol is designed to match the uniqueness of AMI.

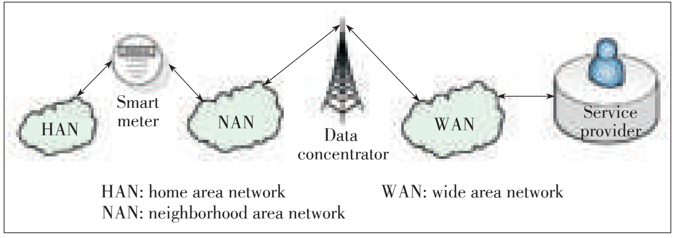
There are several researches for the security issues in AMI [10]–[13], however, there are very few comprehensive security protocols for AMI. In [12], the authors proposed a protocol called integrated authentication and confidentiality (IAC) which involves the initial authentication of a smart meter, and the security in both uplink and downlink transmissions. However, IAC has several problems to be addressed. 1) The smart meters are not treated equally where some of them are chosen to be the backbone nodes and proceed with security protocol, while the others must go through the backbone nodes, however the backbone nodes selection does not have any security concern. 2) The initial authentication process cannot prevent replay attack or even forgery if the initial request is overheard by the attacker. 3) The security protocol in uplink transmission cannot handle multiple incoming data at an intermediate node. 4) Compromise of a node will at least endangers another node since they share the same secret key for message encryption. 5) The security protocol for downlink transmission is too complicated since IAC did not consider broadcast scenario as the main transmission mode for downlink. 6) Once a node malfunctions in the network, IAC cannot function any longer. An improved security protocol for the AMI was proposed in [13]. However, it applied many digital signatures for uplink transmissions which may not be practical. As a preliminary work, the protocol was not comprehensive enough. For instance, some of the messages may suffer from replay attack, and domain secret update mechanism was not mentioned. In this paper, an enhanced security protocol which addresses those shortages is proposed.

3 Advanced Metering Infrastructure

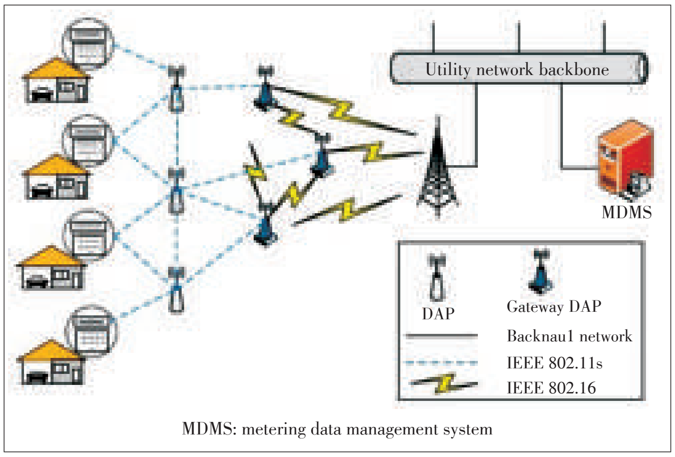
The communication networks of the AMI have a hierarchical structure, including HANs, NANs, and WAN. This structure is shown in **Fig. 1**. A HAN consists of several smart appliances and a smart meter (Some may suggest that a gas meter is also involved. However, for simplicity, we restrict the discussion to electricity power grid and rule out gas meters.) . The sensing/measuring of the power grid status inside households and apartments (e.g., energy-consumption, damage to power equipment, voltage-fluctuation, etc.) is gathered by smart meters. A NAN consists of many DAPs. Each DAP covers a few smart meters. The gathered data from smart meters is uploaded to the MDMS through DAPs. The gateway of a NAN is the data concentrator, which has fast and reliable network connection to the MDMS. Such fast and reliable network is the WAN. It covers a much larger area compared with a NAN.

Because the AMI has a complicated structure, there is no single communication technology that can perfectly fulfill all the needs in the AMI. For example, the optical fiber used in backhaul networks is reliable (0:99999 reliability) and fast (in the order of Gbps). However, it will be too expensive to use it in HAN where data is usually in the order of KB. Therefore, researchers have proposed to use different types of technologies so that communication requirements can be met while the deployment cost and the maintenance cost can be reasonably low.

In the studied AMI as shown in **Fig. 2**, various communication technologies are applied. A HAN is connected by local ar-



▲**Figure 1. Two-way communication networks in smart grid.**



MDMS: metering data management system

▲Figure 2. Studied advanced metering infrastructure.

ea networks, e.g., IEEE 802.11 (Wi-Fi) and/or IEEE 802.15.4 (Zigbee). In a NAN, the DAPs form a wireless mesh network based on IEEE 802.11s (Wi-Fi based). Compared with Zigbee applied in HANs, Wi-Fi can achieve much higher transmission data rate. It is necessary because local NAN transmissions among DAPs introduce multi-hop wireless mesh networking and it requires higher data rate for the transmissions. Some of the DAPs are chosen as gateway DAPs which have direct communication with the concentrator. It is not necessary for the gateway DAPs to be close to the concentrator. In fact, multiple gateways need to be deployed sparsely in a NAN for its wide ranged latency requirement (3 ms to 5 min) [14], [15]. If a customer has too many hops to reach a gateway, it may not be able to successfully deliver the data with most critical latency requirements. Therefore, gateway DAPs are equipped with IEEE 802.16 (WiMAX) interface for longer distance transmission. Adopting WiMAX has a bonus compared with similar technology (e.g., LTE) that it can be deployed using unlicensed band (e.g., 5:8 GHz) in order to lower the service cost by not paying license band accessing fee. However, using unlicensed bandwidth must follow certain restrictions by the FCC [16]. Without loss of generality, the concentrator can be deployed in the center of the neighborhood. It is the gateway of the NAN to the wired backhaul network which connects to the MDMS (or the service provider) in a fast and reliable way.

In the uplink of AMI, information such as energy consumption and monitoring data is transmitted from the customer side to the service provider. In the downlink of AMI, information such as control message and pricing/tariff is transmitted from the service provider to the customer.

The data from customers (metering data) contains much privacy. For example, from the pattern of the energy consumption, it is possible to have a sketch of the lifestyle of that customer. Therefore, it is a must to provide confidentiality to metering data. In addition, integrity is also important to metering data. Manipulation of energy consumption (e.g., energy theft) may cause loss to the service provider. More importantly, manipulated energy consumption will deviate the service provider from optimal control of the power grid, in turn will lead to unnecessary fuel waste and pollution. However, non-repudiation may not be as critical as the other two security requirements for two reasons. 1) Providing non-repudiation which usually is achieved by digital signature may compromise the identity of the customer, and thus jeopardize the privacy. 2) Data in the uplink is frequently transmitted by simple devices such as smart meters, DAPs, sensor nodes. They are equipped with limited computational capability. Therefore, applying public key cryptograph frequently is not practical. The monitoring data of power grid status is gathered by low profile sensors (e.g., phasor measurement unit). Obviously, data integrity needs to be provided so that the service provider can monitor the grid correctly. However, with limited computational power and real-time transmission requirement, it is not necessary to provide confidentiality and non-repudiation to monitoring data.

In the downlink transmission of the AMI, the service provider sends control messages to customers or some components in the power grid. Since control messages usually have real-time transmission requirement and the privacy of control message may not be very important, confidentiality is not required for control messages. Nonetheless, data integrity is critical. Non-repudiation is supposed to be important since the control messages need to be verified from a legitimate sender (i.e., the service provider). However, due to the low-latency requirement and limited computational power at the receiver side, it varies from case to case. Pricing/tariff is also sent from the service provider to customers in downlink transmissions. Confidentiality of such information is not needed because it is for the public. Data integrity and non-repudiation is nonetheless critical.

4 Proposed Security Protocol for AMI

The proposed security protocol consists of four schemes, initial authentication scheme, secure uplink transmission scheme, secure downlink transmission scheme, and domain secret update scheme.

For simplicity, the notations of the keys used in the proposed security protocol are listed in **Table 1**.

4.1 Initial Authentication

An uninitialized node that does not function in the AMI

▼Table 1. Notations of the keys

K_i	Pre-shared secret key of n_i
k_i	Active secret key of n_i
Pu_i	Public key of n_i
Pr_i	Private key of n_i
$k_{i,j}$	Session key between n_i and n_j
Pu_{AS}	Public key of the AS
Pr_{AS}	Private key of the AS

properly must be authenticated through the initialization process. Generally speaking, if a node is closer to the AS, it will be authenticated before the others that are further away. Therefore, before smart meters join the AMI, gateway DAPs and normal DAPs are initialized. Note that gateway DAPs are initialized before normal DAPs since they have direct communication to the concentrator. For simplicity, gateway DAPs are not specified in the rest of the discussion.

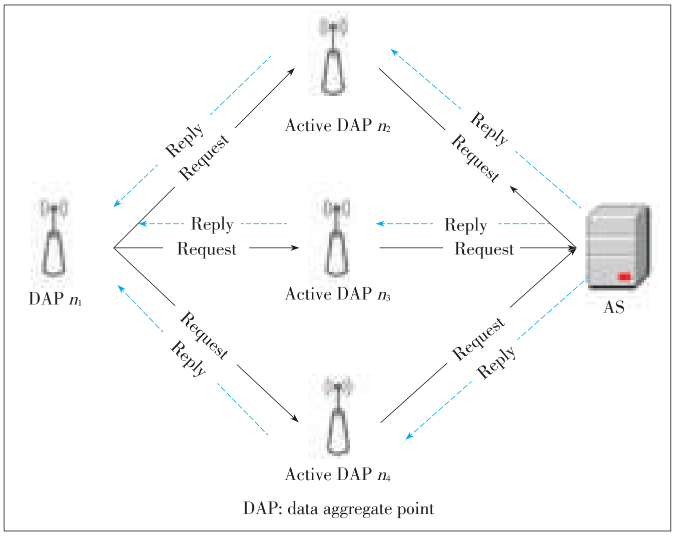
Let the DAPs be divided into two groups, one is active and the other is uninitialized. An active node has been authenticated by the AS to join the AMI communication and is functioning in a healthy status. An uninitialized node can be one of the four types shown in the following:

1) A newly installed node
2) A node which is recovered from malfunctioning status
3) A node which is updated with new pre-shared keys
4) A node which is reinstalled to another location.

For example, if DAP n_1 wants to join the AMI, the initialization process goes through all of its active neighbors (e.g., n_2, n_3 and n_4). As illustrated in **Fig. 3**, n_1 sends requests to all of its active neighbors, which will relay the request to the AS through established secure links. After being authenticated by the AS, n_1 will receive different reply messages from the AS through its active neighbors. Through this initial authentication process, there are mainly three tasks accomplished,

- n_1 is authenticated to be an active node and join the AMI
- n_2 establishes secure connection to the AS through one of its active neighbors which has the shortest distance to the AS
- n_1 establishes backup secure connections to the AS through the rest of its active neighbors.

Without loss of generality, n_2 is chosen to illustrate the detailed initialization process. The processes through n_3 and n_4 are similar. n_1, a secure link between n_2 and the AS, and the AS are involved. Note that the nodes in the secure link do not get useful information from the process. Therefore, we focus on n_1, n_2, and the AS. The initialization process has three mutual authentications. One is between n_1 and the AS, one is between n_2 and the AS, and the other one is between n_1 and n_2. The mutual authentication between n_1 and the AS is obvious since the legitimate nodes are allowed to join the AMI by AS and the nodes also only trust the AS. The mutual authentication between n_2 and the AS is to ensure n_2 is active and is trusted to relay the request from n_1. The mutual authentication between n_1 and n_2 is to help further establish secure communications from n_1 to n_2. Assuming that each node has a pre-shared secret key (i.e., K_i for node n_i) with the AS before initialization. Each active node has been assigned with an active secret key (i.e., K_i for n_i) mainly for uplink data encryption. This active secret key is also used to verify if this node is active or not. Similar to K_2, k_2 is only known to n_2 and the AS. In order to establish a secure connection from n_1 to the AS, an active secret key k_1 must be generated by the AS and assigned to n_1 during the initialization process. Note that n_1 does not bare k_1 before initialization process, only K_1 is known to n_1.

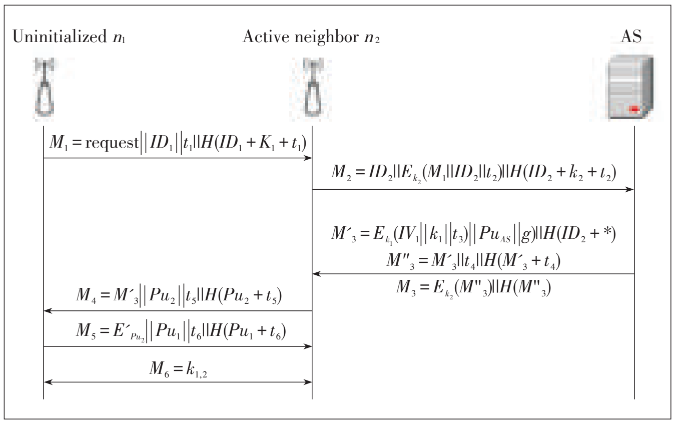


▲**Figure 3. Initial authentication process for DAP n_1.**

As shown in **Fig. 4**, the whole initialization process involves 6 messages.

1) $M_1 = request\|ID_1\|t_1\|H(ID_1 + K_1 + t_1)$: n_1 sends M_1 to the AS through n_2, where $H(\cdot)$ is a hash function, ‘ + ’ is *XOR* function, and t_1 is a time stamp. The authentication is achieved by K_1 since with given ID_1 and t_1, the AS is the only entity other than n_1 to be able to compute $H(ID_1 + K_1 + t_1)$.

2) $M_2 = ID_2\|E_{k_1}\left(M_1\|ID_2\|t_2\right)\|H(ID_2 + k_2 + t_2)$: n_2 sends M_2 to the AS, where $E_k(\cdot)$ is a symmetric encryption function with key k. Once n_2 receives M_1, it generates another time stamp t_2 and appends $H(ID_2 + k_2 + t_2)$ to M_1. The extra information is used for the AS to authenticate n_2 as a genuine node and validates the integrity of time stamp. n_2 then encrypts the entire message and appended its own identification with k_2. This is used to protect its identity verification code $H\left(ID_2 + k_2 + t_2\right)$ and also let the AS authenticate its a-


Uninitialized n_1
Active neighbor n_2
AS
$M_1 = \text{request}\|ID_1\|t_1\|H(ID_1 + K_1 + t_1)$
$M_2 = ID_2\|E_{k_2}(M_1\|ID_2\|t_2)\|H(ID_2 + k_2 + t_2)$
$M'_3 = E_{k_1}(IV_1\|k_1\|t_3)\|Pu_{AS}\|g)\|H(ID_2 + *)$
$M''_3 = M'_3\|t_4\|H(M'_3 + t_4)$
$M_3 = E_{k_2}(M''_3)\|H(M''_3)$
$M_4 = M'_3\|Pu_2\|t_5\|H(Pu_2 + t_5)$
$M_5 = E'_{Pu_2}\|Pu_1\|t_6\|H(Pu_1 + t_6)$
$M_6 = k_{1,2}$

▲**Figure 4. Detailed initial authentication process through one active neighbor.**

ctive status.

3) $M_3 = E_{k_2}(M_3^{\prime\prime} \| H(M_3^{\prime\prime}))$: Once the AS receives M_2 , it authenticates n_2 by decrypting M_2 using k_2 . Time stamp t_2 is validated by computing $H(ID_2 + k_2 + t_2)$. The AS then authenticate n_1 by computing $H(ID_1 + K_1)$. Once n_1 is authenticated, the AS generates a message $M_3^{\prime} = E_{K_1}(IV_1 \| k_1 \| t_3 \| PU_{AS} \| g) H(ID_2 + *)$ for n_1 . In $M_3^{\prime}$, IV_1 is the initial vector for further uplink transmission. k_1 is the active key for uplink transmission. Pu_{AS} is the public key of the AS for downlink transmission protocols. Moreover, g is the generating parameter for public key cryptography in the communication domain. It can be a set of parameters depending on chosen public key cryptography schemes. For instance, g stands for two primes numbers if RSA is applied [17], and for more parameters if identity-based cryptography [18]-[20] is applied. Nonetheless, g remains the same in the communication domain. Although the AS generates g , it does not generate public/private keys for each node. It is safer to keep the nodes as independent as possible to other nodes and the AS. Those data for n_1 is encrypted with the pre - shared secret key K_1 . Moreover, in $M_3^{\prime}$, $H(ID_2 + *) = H(ID_2 + IV_s + k_1 + t_3 + PU_{AS} + g)$ is the integrity checksum. Note that ID_2 is also part of the input and thus n_1 is able to authenticate n_2 through the AS. Then, the AS generates another time stamp t_4 (it is possible that $t_4 = t_3$) and $M_3^{\prime\prime} = M_3^{\prime} \| t_4 \| H(M_3^{\prime} + t_4)$. Finally, the message sent back to n_2 is $M_3 = E_{k_2}(M_3^{\prime\prime} \| H(M_3^{\prime\prime}))$.

4) $M_4 = M_3^{\prime} \| Pu_2 \| t_5 \| H(Pu_2 + t_5)$: After n_2 receiving M_3 , it verifies the message and recovers $M_3^{\prime}$. So far, n_2 has authenticated n_1 from the AS, then n_2 relay $M_3^{\prime}$ to n_1 along with its public key Pu_2 . A time stamp t_5 is generated for message freshness. Hash function is applied to $Pu_2 + t_5$ for data integrity.

5) $M_5 = E^*_{Pu_2}(Pu_1) \| t_6 \| H(Pu_1 + t_6)$: Once n_1 receives M_4, it reveals IV_1, k_1, Pu_{AS} and g. After verifying the integrity of the received information, n_1 computes a pair of public/private keys based on given g. The public key Pu_1 is encrypted with the public key of n_2 s.t. $E^*_{Pu_2}(Pu_1)$, where $E*$ is the encryption function of the adopted public key cryptograph. A time stamp t_6 is generated and $M_5 = E*_{Pu2}(Pu_1 \| t_6 \| H(Pu_1 + t_6)$: is computed to keep the integrity of the message.

6) $M_6 = k_{1,2}$: After exchange public keys, n_1 and n_2 can work out a way to generate a session key $k_{1,2}$ for communication. Session key $k_{1,2}$ is only shared between n_1 and n_2 . It is subject to get refreshed frequently.

After exchanging these 6 messages, n_1 is fully initialized and it is able to join uplink communications through n_2 . The initial authentication processes through other active neighbors are similar. The AS sends back the same IV_1, k_1, Pu_{AS} , and g . In the final hand-shake, n_1 will send the same Pu_1 to its active neighboring node n_x encrypted with Pu_x . By doing so, n_1 shares the same public key to all of its active neighbors. Therefore, n_1 is able to join the uplink transmission through any of the active neighbors, in other words, both operating and backup secure communication channels are established through the initial authentication process.

When the DAPs are initialized by the AS, the NAN is formed. Smart meters will then be initialized through active DAPs. Unlike DAPs, smart meters do not have many neighbor nodes because of two reasons. First, smart meters have limited transmission range. They are unlikely to have direct connection with more than one DAPs. Second, it is not a good idea to let smart meters communicate with each other since the data contains much privacy and smart meters are easier to get access to than DAPs. A smart meter sends an initialization request to an active DAP, and the DAP will relay the request to the AS through a secure communication link. The detailed process is similar to that shown in Fig. 4 and thus is not repeated.

Security Analysis:

- Confidentiality: Confidentiality of the authentication request is unnecessary, therefore it is not provided. Much information is transmitted in plain text.
- Data integrity: All the messages (except for M_6) are provided a hash value for integrity check. Moreover, the input is not the original message which can be captured easily by an eavesdropper. The input is the XORed messages of the useful information, which cannot be captured or forged. Therefore, the messages in this protocol is unforgettable. Moreover, with time stamps being applied in each message, replay attack is unlikely to succeed in the process. The detailed process of M_6 is not given in this protocol, because the real application may vary based on different public key schemes. With a given public key scheme, data integrity can be provided in a similar way for session key $k_{i,j}$.
- Non-repudiation: The idolization process does not use a digital signature for sender authentication except for M_5 . However, secret pre-shared keys are applied for message encryption. With the sender and the receiver being the only ones that can encrypt and decrypt the message, nonrepudiation is achieved for all messages (except for M_5). Non-repudiation of M_5 is indeed provided by a digital signature.

4.2 Security Protocol in Uplink Transmission

In the uplink transmission, data from each node is aggregated in a chain topology and is finally delivered to the service provider (assuming that the AS and the service provider share the same entity). As discussed before, data confidentiality and data integrity are important security requirements for metering data since the wrong data may cause unnecessary loss of the power generation. Sender authentication or non - repudiation may be considered in certain situation if there is enough computational resources. To achieve all those requirements mentioned above, we propose the security protocol for data aggregation in uplink transmission as shown in **Fig. 5**. Suppose in one path there are N nodes with an order of $(n_1, n_2, \cdots, n_N)$. As the

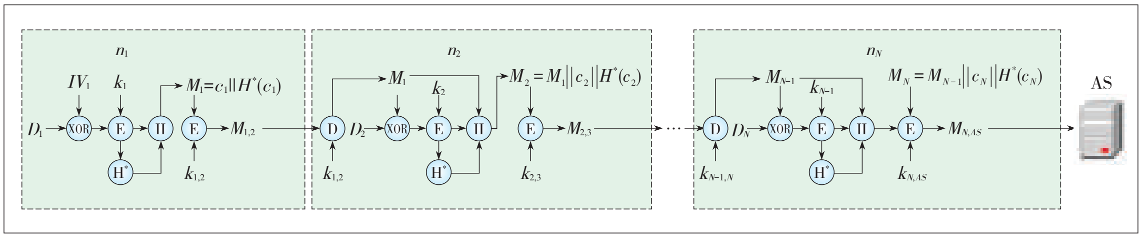


Figure 5. Data aggregation process in uplink transmission.

first one of the aggregation, n_1 mixes its raw data D_1 with IV_1 and encrypts it with k_1 so that confidentiality can be achieved. $H^*(\cdot)$ is a hashed message authentication code function which provides data integrity. Different hash functions can be used for initialization process and uplink transmission, therefore we use $H^*(\cdot)$ for clearer illustration. Finally, n_1 encrypts the entire message with $k_{1,2}$ so that n_2 can verify that the data is from n_1 which is an active node. The intermediate nodes first decrypt the incoming data with the session key of the previous node. Then, they mix their raw data with the previous data. After that, they follow the same steps as the first node.

If an intermediate node has multiple incoming nodes, it treats each of them as a separate chain and aggregates its own data to one of the incoming data while simply padding the data from the other incoming nodes to it with flags. The details are shown in **Fig. 6**. Assume n_p has two incoming nodes n_i and n_j, and n_p chooses to aggregate incoming data from n_i. Then n_p follows the usual steps dealing with D_p and $M_{i,p}$. For $M_{j,p}$, n_p authenticates the sender by getting M_j, and simply flags M_j such that $f_0||M_j||f_1$ to the original M_p, thus $M_p=f_0||M_j||f_1||C_p||H^*(C_p)$.

Once the AS receives the aggregated data, it starts the recovery process of the data. The AS first authenticates the incoming node by decrypting the receiving data with the pre-shared public key $Pu_{N,AS}$. Before recovering the raw data, the AS needs to verify the data integrity by checking the hashed value. Since the data of each node are not further processed by nodes after it, if some of the data corrupt, the AS will simply discard them instead of wasting the whole message from that transmission path. The detailed raw data recovery process (without integrity check) is shown in **Fig. 7**. Message $M_i=M_{i-1}||C_i||H^*(C_i)$, after verifying the data integrity, the AS decrypts C_i and XOR the result with M_{i-1} to recover D_N. Note that D_1 is recovered by XORing IV_1. If the message includes data from multiple chains, the AS extracts the message between f_0 and f_1 first and recovers the data following the same process as shown in Fig. 7 without verifying the sender authentication (the decryption process with $Pu_{N,AS}$).

Security Analysis:

- Confidentiality: The confidentiality is achieved by two steps in this protocol. For each node n_i, its raw data is mixed with the incoming data from the previous node.
- The first node achieves this step by mixing its data with the initial vector given by the AS. Moreover, mixed data is encrypted with the active key k_i.
- Data integrity: The message cannot be manipulated since message integrity is verified using a hash value. The message of n_i is unforgeable unless an active key k_i is compromised.
- Non-repudiation: On one hand, since each message is encrypted by an active key from the corresponding node, sender authentication is provided. On the other hand, no digital signature is used in the proposed protocol for non-repudia-

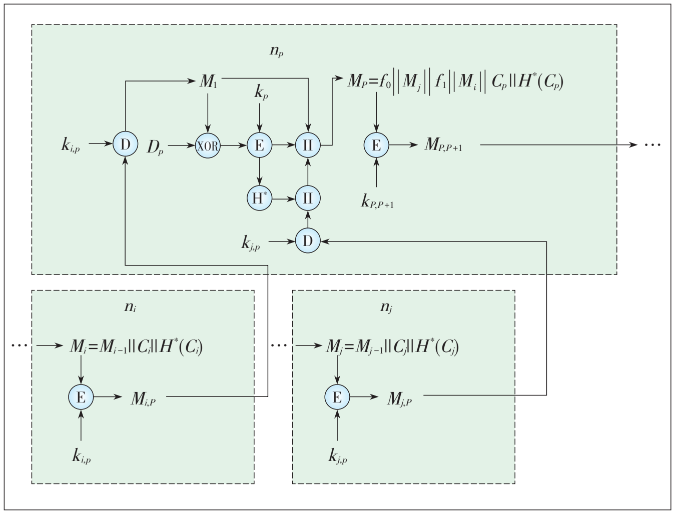


Figure 6. Multi-flow data aggregation process.

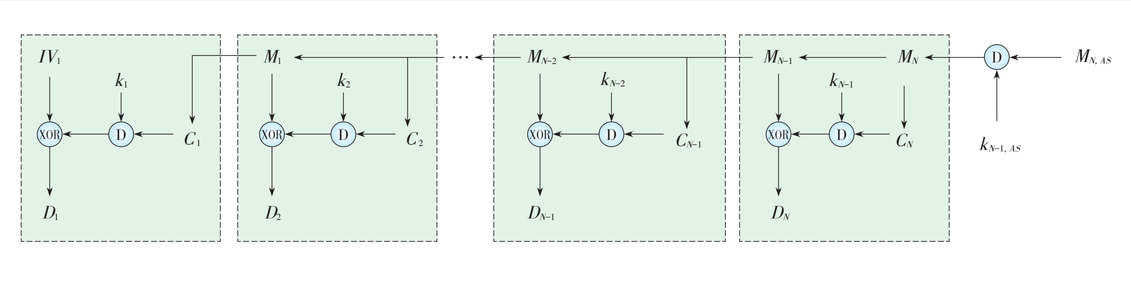


Figure 7. Data recovery process in uplink transmission.

tion. In fact, if a message is susceptible or invalid, the service provider will simply discard it without wasting resources on it.

4.3 Security Protocol in Downlink Transmission

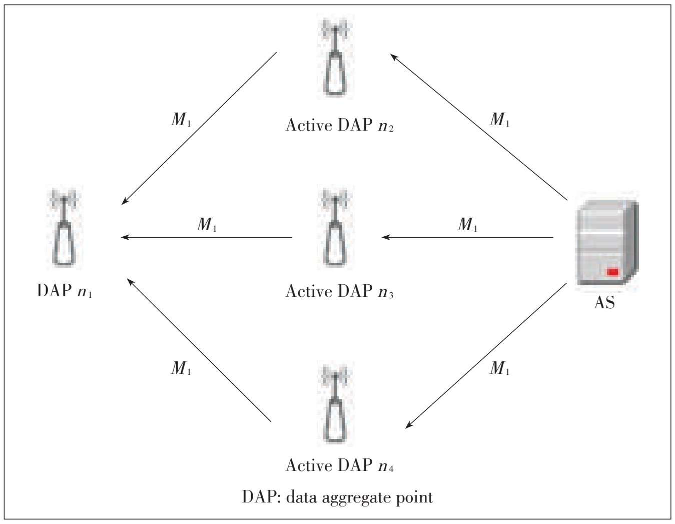
The downlink transmission involves control messages from the service provider to the nodes. Most of the control messages (e.g., price and tariff information) are for all the smart meters in the neighborhood, where the confidentiality is not as important as that of the uplink data. Nonetheless, as discussed before, data integrity is important. Message manipulation will cause further responding in power usage and will finally result in unnecessary fuel waste due to excess power generation. Moreover, non-repudiation is critical for such control messages so that the customers can trust the sender.

Let C_B be the control message to be broadcast. To provide message integrity, a hash value (achieved by hash function $H^*(\cdot)$) is appended to the original message, the entire message is then signed with Pu_{AS} as a digital signature to provide non-repudiation and sender authentication. $E^*_{\mathrm{Pr}_{AS}}(\cdot)$ is an encryption function using public key cryptography, the encryption key is Pr_{AS}. In all, $M_B = E^*_{\mathrm{Pr}_{AS}}\left(C_B \| t \| H^*(C_B + t)\right)$, where t is a time stamp for data freshness. At the receiver side, the original information (i.e., C_B and t) is revealed by performing $D^*_{Pu_{AS}}(M_B)$, where $D^*_{Pu_{AS}}(\cdot)$ is a decryption function using public key cryptography with decryption key Pu_{AS}. An integrity check will be performed to verify both the hash value and the time stamp. If the integrity check is not passed, the receiver will request a retransmission from the AS through its secure uplink transmission tunnel. This rarely happens unless the message is not legitimate. Because each node will receive multiple copies of the control message from all of its active neighbors. If one of the message is valid, then a retransmission will not be necessary.

Some of the control messages (e.g., request for update) are for a specific node (e.g., n_i). Let such control message be C_i. Apparently, message integrity, nonrepudiation and sender authentication shall still be provided, moreover, confidentiality of the message is also important, therefore the message is encrypted with k_i such that $M_i = E^*_{\mathrm{Pr}_{As}}\left(E_{k_i}\left(C_i \| t \| H^*(C_i + t)\right)\right)$. Unlike M_B, broadcasting M_i is a waste of resource and is unnecessary. However, sending M_i through the corresponding uplink path may reduce the availability of the message. Therefore, we propose to send such specific control message to n_i through all of its active neighbors, as illustrated in **Fig. 8**.

Security Analysis:

- Confidentiality: For downlink broadcasting messages, confidentiality is not provided. For downlink messages to a specific node (e.g., n_i), confidentiality is provided by encrypting the message with the active key k_i.
- Integrity: First of all, both the broadcasting and unicasting control messages are unforgeable since they signed by the AS using its private key. Secondly, any manipulated control messages will be recovered since their hash values cannot pass the data integrity check.
- Non-repudiation: Since each control message is signed by the AS, the control message is non-repudiable.



▲**Figure 8. Example of Control message M_1 to n_1.**

4.4 Domain Secrets Update

In order to keep the AMI secure in the long run, domain secrets need to be refreshed once in a while (e.g., daily or even hourly). For the AS, its public and private key needs to be refreshed. After the AS generates a new pair of public/private keys (i.e., $Pu'_{AS}/\mathrm{Pr}'_{AS}$), it transmits the public key to all the active nodes in a broadcasting way (signed by current private key of the AS), s.t., $M_B = E^*_{\mathrm{Pr}_{AS}}\left(Pu'_{AS} \| t \| H^*\left(Pu'_{AS} + t\right)\right)$, where t is a time stamp which keeps the freshness of the message. The update of Pu'_{AS} is for all the active nodes in the same time slot. In the meantime, separate control messages signed by Pr_{AS} and Pr'_{AS} will be sent so that the downlink transmission is not interrupted.

For an active node (e.g., n_i), its active secret key k_i needs to be refreshed. To do so, the AS picks a new active secret key k'_i for n_i, and sends $M_i = E^*_{\mathrm{Pr}_{AS}}\left(E_{k_i}\left(k'_i \| t \| H^*\left(k'_i + t\right)\right)\right)$ to n_i, where t is a time stamp which keeps the freshness of the message. However, it is not necessary to refresh the active secret keys for all the nodes at the same time. The AS can do a batch at a time when the network is not heavily loaded, for example, after mid night. Moreover, as mentioned before, the session key (e.g., $k_{i,j}$) between two active nodes (i.e., n_i and n_j) needs to be refreshed more frequently. To do so, n_i and n_j simply run the 6-th step from the initialization process again.

The pre-shared key of a node is not refreshed as frequently as the other keys since it is used much less frequently. Therefore, the pre-shared key can last longer before it wears out. However, it is reasonable to refresh the pre-shared key in some cases. For example, if a DAP is compromised and recovered, or if a DAP is redeployed to another NAN, or if a house has been sold and thus its smart meter has a new owner. An on-site firmware update will be recommended in this case. A customer can also request a firmware update and then load it to his/her smart meter. Automatic update can also be achieved. For example, if DAP n_i needs a pre-shared key update, the AS picks a new $K_i^{'}$, and sends $M_i = E^*_{\mathrm{Pr}_{AS}}\left(E_{k_i}\left(K_i^{'}\|t\|H^*\left(K_i^{'}+t\right)\right)\right)$. It is also reasonable to encrypt this message with K_i if k_i has been compromised. However, if both K_i and k_i are compromised, then a physical update will be inevitable.

5 Conclusions

In this paper, we propose a security protocol for the AMI in smart grid. In order to meet various security requirements for the asymmetric communication of the AMI, the proposed security protocol consists of initial authentication scheme, independent security schemes for uplink and downlink transmissions, and a domain secrete update scheme. The security scheme in uplink scheme provides confidentiality, data integrity to metering data and other monitoring data. The security scheme in downlink provides data integrity and non-repudiation to controlling data and pricing/tariff information. In the future work, we will extend the network security protocol so that cloud computing and various external information sources can be involved in the modern control of smart grid.

References

[1] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communications Surveys Tutorials*, vol. 14, no. 4, pp. 998–1010, 2012. doi: 10.1109/surv.2012.010912.00035.

[2] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Communications Surveys Tutorials*, vol. 15, no. 1, pp. 5– 20, 2013. doi: 10.1109/SURV.2012.021312.00034.

[3] F. Ye, Y. Qian, and R. Hu, "Energy efficient self-sustaining wireless neighborhood area network design for smart grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 220–229, 2015. doi: 10.1109/TSG.2014.2344659.

[4] J. Ma, J. Deng, L. Song, and Z. Han, "Incentive mechanism for demand side management in smart grid using auction," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1379–1388, 2014. doi: 10.1109/TSG.2014.2302915.

[5] H. Soliman and A. Leon-Garcia, "Game-theoretic demand-side management with storage devices for the future smart grid," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1475–1485, 2014.

[6] Z. Fadlullah, D. M. Quan, N. Kato, and I. Stojmenovic, "Gtes: An optimized game-theoretic demand-side management scheme for smart grid," *IEEE Systems Journal*, vol. 8, no. 2, pp. 588–597, 2014. doi: 10.1109/JSYST.2013.2260934.

[7] F. Ye, Y. Qian, and R. Hu, "A real-time information based demand-side management system in smart grid," *IEEE Transactions on Parallel and Distributed Systems*, no. 99, pp. 1, 2015.

[8] K. Ren, S. Yu, W. Lou, and Y. Zhang, "Peace: A novel privacy enhanced yet accountable security framework for metropolitan wireless mesh networks," *IEEE Transactions on* Parallel and Distributed Systems, vol. 21, no. 2, pp. 203–215, 2010.

[9] E. Witzke, J. Brenkosh, K. Green, L. Riblett, and J. Wiseman, "Encryption in mobile wireless mesh networks," in *2012 IEEE International Carnahan Conference on* Security Technology (ICCST), Boston, Massachusetts, USA, 2012, pp. 251–256.

[10] M. Thomas, I. Ali, and N. Gupta, "A secure way of exchanging the secret keys in advanced metering infrastructure," in *2012 IEEE International Conference on Power System Technology (POWERCON)*, Auckland, New Zealand, Oct 2012, pp. 1–7.

[11] B. Vaidya, D. Makrakis, and H. Mouftah, "Secure multipath routing for ami network in smart grid," in *2012 IEEE 31st International Performance Computing and Communications Conference (IPCCC)*, Austin, USA, Dec 2012, pp. 408–415.

[12] Y. Yan, R. Hu, S. Das, H. Sharif, and Y. Qian, "An efficient security protocol for advanced metering infrastructure in smart grid," *IEEE Network*, vol. 27, no. 4, pp. 64–71, 2013. doi: 10.1109/MNET.2013.6574667.

[13] F. Ye, Y. Qian, and R. Hu, "A security protocol for advanced metering infrastructure in smart grid," in *2014 IEEE Global Communications Conference (GLOBECOM)*, Austin, USA, Dec 2014, pp. 649–654.

[14] G. Rajalingham, Q.-D. Ho, and T. Le-Ngoc, "Attainable throughput, delay and scalability for geographic routing on smart grid neighbor area networks," in *Wireless Communications and Networking Conference (WCNC 2013)*, Shanghai, China, 2013, pp. 1121–1126.

[15] *Communication Networks and Systems in Substations–Part 5: Communication Requirements for Functions and Device Models*, P-IEC 61850-5ed1.0, 2003.

[16] *FCC Rules for Unlicensed Wireless Equipment operating in the ISM Bands* [Online]. Available: http://www.afar.net/tutorials/fcc-rules

[17] S. Burnett and S. Paine, *The RSA Security's Official Guide to Cryptography*, McGraw-Hill, Inc., 2001.

[18] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[19] B. Libert and J. -J. Quisquater, "The exact security of an identity based signature and its applications," *IACR Cryptology ePrint Archive*, vol. 2004, pp. 102–104, 2004.

[20] F. Ye, Y. Qian, and R. Q. Hu. *Hibass: hierarchical identity-based signature scheme for ami downlink transmission* [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1002/sec.1217/abstract

Manuscript received: 2015-04-21

Biographies

Feng Ye received his BS degree from the Department of Electronics Engineering, Shanghai Jiaotong University, Shanghai, China, in 2011. Currently he is pursuing his PhD degree at the Department of Electrical and Computer Engineering in University of Nebraska-Lincoln, NE, USA. His current research interests include smart grid communications and energy optimization, big data analytics and applications, cyber security and communication network security, wireless communications and networks.

Yi Qian (yi.qian@unl.edu) received his PhD degree in electrical engineering from Clemson University. He is an associate professor in the Department of Electrical and Computer Engineering, University of Nebraska-Lincoln (UNL). Before joining UNL, he worked in the telecommunications industry, academia, and the government. His research interests include information assurance and network security, computer networks, mobile wireless ad-hoc and sensor networks, wireless and multimedia communications and networks, and smart grid communications. Several of his recent journal articles on wireless network design and wireless network security are among the most accessed papers in the IEEE Digital Library.