A Lightweight Message Authentication Scheme for Smart Grid Communications

---

Citation:

Mostafa M. Fouda, Zubair Md. Fadlullah, Nei Kato, Rongxing Lu, and Xuemin (Sherman) Shen, "A Lightweight Message Authentication Scheme for Smart Grid Communications," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 675-685, Dec. 2011.

URL:

http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5983424

A Lightweight Message Authentication Scheme for Smart Grid Communications

Mostafa M. Fouda, *Member, IEEE,* Zubair Md. Fadlullah, *Member, IEEE,*
Nei Kato, *Senior Member, IEEE,* Rongxing Lu, *Member, IEEE,* and Xuemin (Sherman) Shen, *Fellow, IEEE*

***Abstract*—Smart Grid (SG) communication has recently received significant attentions to facilitate intelligent and distributed electric power transmission systems. However, communication trust and security issues still present practical concerns to the deployment of SG. In this paper, to cope with these challenging concerns, we propose a lightweight message authentication scheme features as a basic yet crucial component for secure SG communication framework. Specifically, in the proposed scheme, the smart meters which are distributed at different hierarchical networks of the SG can first achieve mutual authentication and establish the shared session key with Diffie-Hellman exchange protocol. Then, with the shared session key between smart meters and hash-based authentication code technique, the subsequent messages can be authenticated in a lightweight way. Detailed security analysis shows that the proposed scheme can satisfy the desirable security requirements of SG communications. In addition, extensive simulations have also been conducted to demonstrate the effectiveness of the proposed scheme in terms of low latency and few signal message exchanges.**

***Index Terms*—Smart Grid, Message authentication, Security.**

I. Introduction

Recently, Smart Grid (SG) is the buzz word, which has attracted attentions from engineers and researchers in both electric power and communication sectors [1]–[5]. The concept of SG has appeared in recent literature in different flavors. Some referred to it as intelligent grid whereas some called it the grid of the future. The objective of the SG concept remains more or less the same, namely to provide end-users or consumers with power in a more stable and reliable manner that the aging power-grids of today may not be able to provide in the near future. In this vein, SG incorporates a two-way communication between the provider and consumers of electric power. The two way communication indicates the ability of SG to enable the end-users to express their power requirement demands to the utility provider. In SG, the users are no longer passive players. Instead, they can undertake active roles to effectively minimize energy consumption by communicating back and forth with the provider. Numerous machines including sensing devices, smart meters, and control systems are expected to be between the provider and end-users to facilitate this two-way communication system in SG. To facilitate this, Internet Protocol (IP)-based communication technologies are considered to be the top-most choice for setting up smart grid's networks covering homes, buildings, and even larger neighborhoods. The choice of IP-based SG communication means that every smart meter and each of the smart appliances (e.g., air-conditioners, heaters, dish-washers, television sets, and so forth) will have its own IP address and will support standard Internet Engineering Task Force (IETF) protocols for remote management. However, existing IP-based communication networks, e.g., Internet, are likely to be challenged by a huge volume of delay-sensitive data and control information, and also a wide variety of malicious attacks, such as replay, traffic analysis, and denial of service (DOS) attacks. Therefore, IP-based SG communications will also be vulnerable to security threats. As a consequence, it is essential to properly design SG communication protocols for dealing with all possible security threats. In addition, not all the entities in SG are trusted. As in conventional IP-based communication networks, SG communication framework needs to verify whether the parties involved in communication are the exact entities they appear to be. As a result, the SG communication framework should consider an adequate authentication mechanism [6]–[16] so that malicious users may not be able to compromise the secrecy or privacy of the information exchanged between the provider and consumers.

Current smart metering technologies (e.g., Advanced Metering Infrastructure or AMI) lead to privacy concerns because they depend upon centralizing personal consumption information of the consumers at their smart meters. Since 2009, a legal ruling in Netherlands has made it mandatory to consider privacy issues in case of using smart meters [17]. Similarly, in the USA, NIST dictated that there should be "privacy for design" approach for SG communications [18]. These privacy concerns may be addressed by adequately authenticating the smart meters. However, such a solution should take into account the rather limited resources (i.e., low memory and computational capacity) on the smart meters. As a consequence, any authentication mechanism for smart grid communication should be designed so that it does not put too much burden on the already constrained smart metering resources. In other words, the SG communication requires that a secure authentication framework should minimally increase the messages exchanged amongst the smart meters. In this paper, we propose a lightweight message authentication scheme for securing communication amongst various smart meters at different points of the SG. Specifically, based on the Diffie-Hellman key establishment protocol and hash-based message

Part of the work has been presented in INFOCOM'11 Workshop SCNC [1].

M. M. Fouda, Z. M. Fadlullah, and N. Kato are with the Graduate School of Information Sciences, Tohoku University, Sendai, Japan e-mails: {mfouda, zubair, kato}@it.ecei.tohoku.ac.jp

R. Lu and X. Shen are with Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada e-mails: {rxlu, xshen}@bbcr.uwaterloo.ca

authentication code, the proposed scheme allows smart meters to make mutual authentication and achieve message authentication in a lightweight way, i.e., it does not contribute to high latency and exchange few signal messages during the message authentication phase.

The remainder of this paper is organized as follows. Some relevant research works are presented in Section II. Section III gives our considered SG communications system model. In Section IV, the unique security requirements of SG communication are delineated. We then present our security framework and describe a lightweight message authentication scheme to secure communications amongst various SG entities in Section V. A detailed security analysis of the proposed authentication scheme is provided in Section VI. Comparative evaluation of our proposed scheme with an existing authentication mechanism for SG communication are presented in Section VII, followed by concluding remarks in Section VIII.

II. Related Research Work

From the IEEE P2030 SG standards, three task forces are formulated to carry out the smart grid agenda, namely power engineering techology (task force 1), information technology (task force 2), and communication technology (task force 3), where information technology (task force 2) is related to digital security of SG communications. In other words, this task force is responsible for designing system and communications protection policies and procedures to fend off malicious attacks against SG [9]. However, the main shortcoming of these policies consists in the broad and coarse design directions that they provide. A utility computer network security management and authentication system for SG is proposed by Hamlyn *et al.* [10]. However, it is limited to the authentication between host area electric power systems and electric circuits.

In [11], power system communication and digital security issues are taken into account as critical components of SG. It suggests that a number of digital security issues need to be addressed for SG communication. For example, it was pointed out that combining SCADA/EMS (Supervisory Control and Data Acquisition/Energy Management System) with information technology networks leads to significant security threats. In addition, this work indicated that broadband Internet technologies may enable intruders to access smart meters and even the central system by which they may collect metering data. Indeed, the metering data, along with price information, special offers, and so forth, may contain sensitive data of the client which may lead to breach of privacy.

Metke *et al.* indicated in [12] that SG deployments must meet stringent security requirements. For example, they consider that strong authentication techniques is a requisite for all users and devices within the SG. This may, however, raise to scalability issue. In other words, as the users and devices in SG are expected to be quite large, the strongest authentication schemes may not necessarily be the fastest ones. As a consequence, scalable key and trust management systems, tailored to the particular requirements of the utility provider and users, will be essential as far as SG communication is concerned.

Kursawe *et al.* present the need for secure aggregation of data collected from different smart meters [13]. They present four concrete protocols for securely aggregating smart meters data readings, namely interactive protocols, Diffie-Hellman Key-exchange based protocol, Diffie-Hellman and Bilienar-map based protocol, and low-overhead protocol. Interestingly, the last three protocols rely upon the original Diffie-Hellman key exchange protocol in its securest form or its more relaxed variants. The computation and communication overheads with the relaxed variants of Diffie-Hellman based security aggregation schemes on smart meters are verified to be lower. However, this work does not consider smart meters authentication, for which, we also can extend Diffie-Hellman based approaches.

Three methods are compared in [14] for authenticating demand response messages in SG, namely Bins and Balls (BiBa), Hash to Obtain Random Subsets Extension (HORSE), and Elliptic Curve Digital Signature Algorithm (ECDSA). It is demonstrated that ECDSA offers higher security in contrast with BiBa and HORSE, at the expense of increased computational complexity, particularly at the receiver-end. In this paper, by first providing a broad SG communications framework, we envision a secure and reliable framework comprising a lightweight message authentication scheme, which is customized to the specific needs of SG.

III. SG Communications System Model

Fig. 1 shows our considered SG communication framework. The SG power transmission and distribution system is considered to be separated from the communication system. For the sake of clarity, the power Distribution Network (DN) is described briefly at first. The power, which is generated at the power plant(s), is supplied to the consumers via two components. The first component is the transmission substation at/near the power plant. The second component comprises a number of distribution substations. The transmission substation delivers power from the power plant over high voltage transmission lines (usually over 230 kilo volts) to the distribution substations, which are located at different regions. The distribution substations transform the electric power into medium voltage level and then distribute it to the building-feeders. The medium voltage level is converted by the building-feeders into a lower level, usable by consumer-appliances.

To explore the SG topology from communication point of view, the SG topology is divided into a number of hierarchical networks. The transmission substation located at/near the power plant, and the Control Centers (CCs) of the distribution substations are connected with one another in a meshed network. This mesh network is considered to be implemented over optical fiber technology. Optical fiber technology is chosen because (i) it is feasible for setting up this type of core meshed network, and (ii) it is the most capable broadband technology for sustaining high volume of SG traffic with the least possible communication latency.

The communication framework for the lower distribution network (i.e., from CCs onward) is divided into a number of hierarchical networks comprising Neighborhood Area

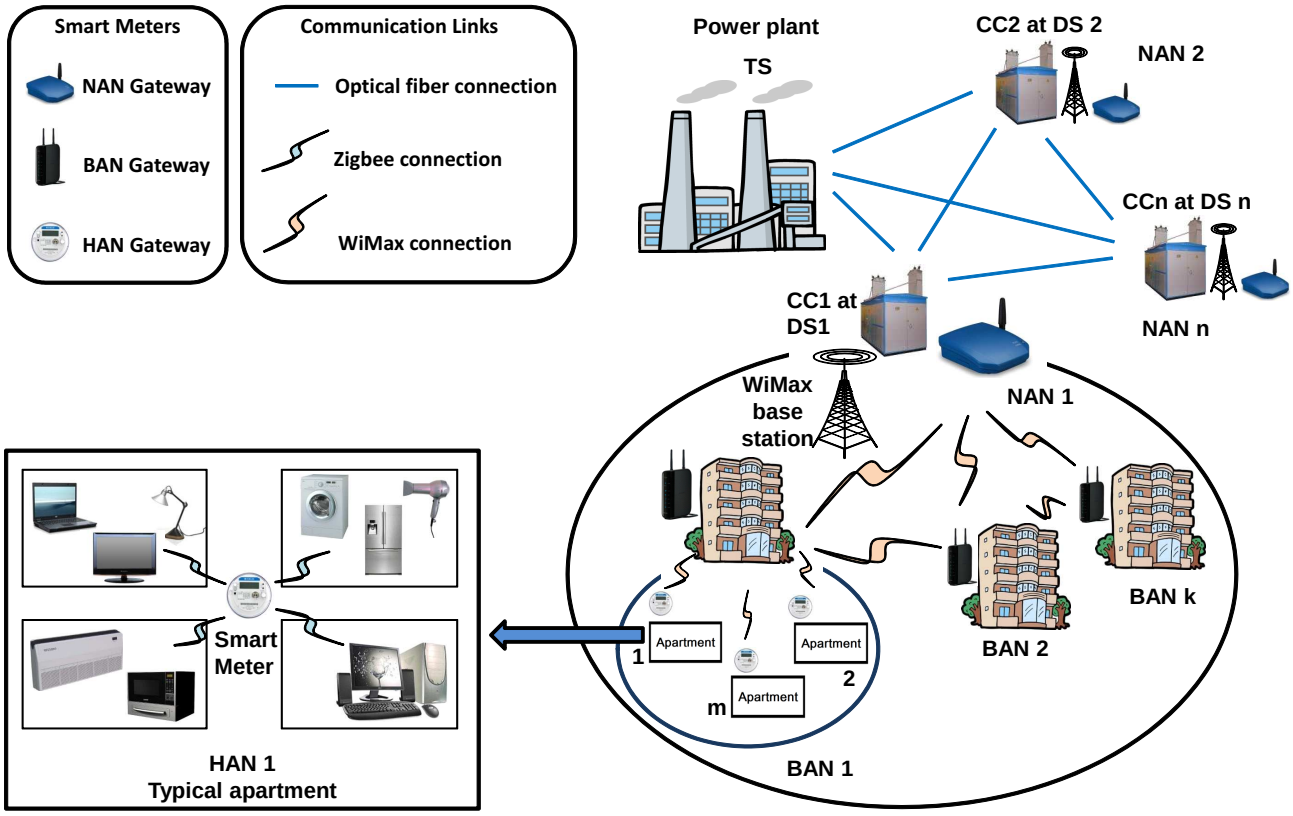


Fig. 1. Considered SG communications framework.

Network (NAN), Building Area Network (BAN), and Home Area Network (HAN). For the sake of simplicity, let every distribution substation cover only one neighborhood area. There are n DSs covering n neighborhoods or NANs. Each of these NANs comprises a number of BANs. For example, the $NAN1$ in Fig. 1 consists of k BANs, each of which is assigned a number of HANs, i.e., several apartment-based networks. Also, there are smart meters deployed in the SG architecture enabling an automated, two-way communication between the utility provider and consumers. Each smart meter has two interfaces - one interface is for reading power and the other one acts as a communication gateway. Throughout this paper, we refer to the smart meters used in NAN, BAN, and HAN as NAN GW (GateWay), BAN GW, and HAN GW, respectively. Through these smart meters/GWs, the consumers are able to determine their currently consumed electric power and decide to change their consumption level by running/shutting down certain appliances. A smart meter comprising MSP430F471xx microcontroller should be able to operate as a typical HAN GW [19]. The memory size of the HAN GW is up to 8KB Random Access Memory (RAM) and 120KB flash memory. The key integrated peripherals of the HAN GW include a 16MHz CPU, 3/6/7 16-bit Analog to Digital Converters (ADCs) and Programmable Gain Amplifiers (PGAs), 160-segment Liquid Crystal Display (LCD), Real Time Clock (RTC), and 32x32 hardware multiplier for easy energy measurement computations. For the BAN GWs, smart metering equipments having ten times more capability than the HAN GWs are considered because industrial standards have not yet released fully functional BAN GWs. In other words, for each BAN GW, a smart meter with 160MHz CPU, 128KB RAM, and 1MB flash memory is considered. Similar lack of industrial specimen for NAN GWs led us to assume NAN GW configuration through a PC with the Intel Core i7 CPU and RAM of 6GB. It is worth mentioning that the difference in these smart metering specifications are attributed to the fact that the consumers on the lower spectrum of the SG hierarchical networks are expected to encounter significantly lower traffic and have budget constraints (i.e., how much the ordinary consumers are willing to pay for their smart meters) while the NAN GW at the CC can easily accommodate one or more high-spec PC(s) for dealing with significantly huge amount of data originating from a substantial number of users in the neighborhood.

Next, we describe the SG communications framework followed by the SG communications packet structure. For clarity, SG communication at HANs is delineated at first. Also, it is worth noting that based upon the existing standards of SG, IP-based communications networking is preferred which permits virtually effortless inter-connections with HANs, BANs, NANs, CCs, and the transmission substation.

A. SG Communication Networks

1) Home Area Network - HAN at the consumer-end: Within the considered SG, a HAN portrays the subsystem in the lowest end of the hierarchical spectrum, i.e., at the consumer-end. The HAN enables consumers to efficiently

manage their on-demand power requirements and consumption levels. Let us refer to $HAN1$ in Fig. 1. $HAN1$ connects the smart appliances (e.g., television, washing machine, oven, and so forth having their unique IP addresses within that smart apartment) to a $HANGW1$. $HANGW1$, the smart meter assigned to the HAN, is responsible for communicating with BANGW1. Smart Energy Profile (SEP) Version 1.5 over IEEE 802.15.4 ZigBee radio communications is considered to be HAN communication protocol. The reason behind opting for ZigBee instead of other wireless solutions (e.g., IEEE 802.11 (WiFi) and Bluetooth) is due to its low power requirements as well as simple network configuration and management provisions citeFFKTI11. The fact that ZigBee provides a reasonable communication range of 10 to 100 meters while maintaining significantly low power requirement (1 to 100 mW) and cost presents itself as a feasible communication technology in the HAN level.

2) Building Area Network - BAN at the building-feeder: To be consistent with practical observation whereby a typical building consists of a number of apartments/homes, in our considered SG topology, a typical BAN comprises a number of HANs. The smart metering equipment installed at the building-feeder, referred to as the BAN GW, can be used to monitor the power need and usage of the residents of that building. For facilitating BAN-HANs communication, conventional WiFi may appear to be an attractive choice at a first glance due to its popularity amongst in-home users in recent time. However, let us consider the scenario of a BAN covering a large number of households (e.g., a hundred or more). In such a scenario, the longest distance from a particular apartment to the BAN node may be hundreds of meters. Because WiFi technology may cover up to a hundred meters, it may not be adequate for this type of scenario. Therefore, WiMAX may be employed to cover more areas to facilitate the communication between a BAN and its covered HANs. [1]

3) Neighborhood Area Network - NAN at the Control Center: NAN exists on the upper end of the SG communications network hierarchy. A NAN represents a locality or a particular region (e.g., a ward within a city). Through a NAN GW, the utility provider is able to monitor how much power is being distributed to a particular neighborhood by the corresponding distribution substation. For facilitating NAN-BANs communication, WiMax or other relevant broadband wireless technologies may be adopted. To this end, one or more WiMAX base stations are located in every NAN. Note that the WiMAX framework used for SG communications should be separate from the existing ones used for providing other services, e.g., Internet. This provision is necessary for preventing network congestion and avoiding possible security threats, which are already present in the existing Internet.

B. Adopted Packet Structure for SG Communications

Fig. 2 shows an overview of SG communication packet structure from industry-oriented smart meter specifications in [20]. In addition to the raw message, each packet also includes three headers, namely the message header, TCP/IP header, and security header. The message header contains meter ID MAC address, equipment status, and the Type of Message (ToM). As shown in Fig. 2, there are nine ToMs that the HAN GW can send to the BAN GW, and the function and size of each ToM are also described.

[1]It is worth noting that 3G, and other modes of wireless broadband communications may be alternative solutions to WiMax.

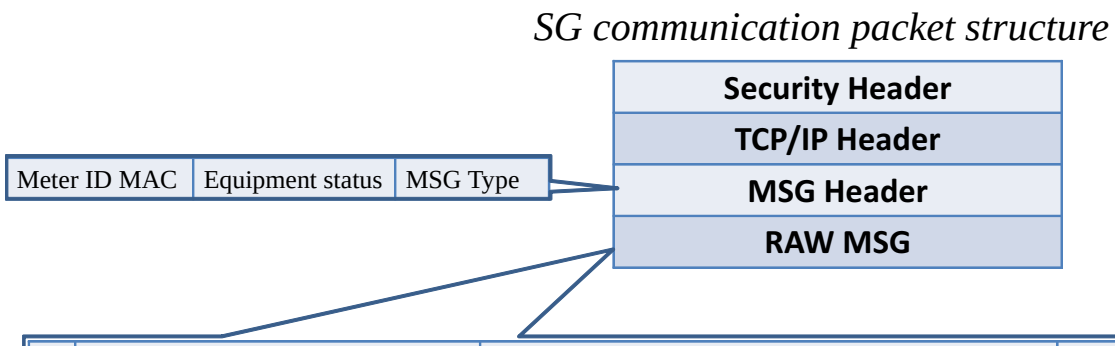
IV. Problem Statement

Securing SG communication depends on two important requirements [21], namely communication latency and large volume of messages in SG. If the CC misses any input from a HAN smart meter, this may affect the decision taken by the CC that may be important. Table I provides the power requirements of different equipments in a typical HAN. In order to avoid any potential emergency situation, which may occur at any time, the SG communication system needs to be able to handle the message delivery to the CC via the BAN and NAN GWs with the minimum delay possible. The power requirements of the HAN devices given in Table I are sent to the respective BAN by meter periodic data read (i.e., ToM#2). The size of each raw periodic request message is 32 bytes. With the mandatory headers, the packet size can be roughly (50+32=) 82 bytes. In addition, there are TCP/IP headers and optional security headers if any security protocol is used. If congestion occurs at the BAN GW, the packet may be delayed to be sent to the NAN GW and CC. Furthermore, it may also be dropped if the RAM and the on-chip flash of the BAN GW are full due to (i) multiple messages arriving from different HANs at the same time, and (ii) limited processing capability of the BAN GWs. If this is the case, the BAN GW may request the HAN GW to retransmit the required packets. This also contributes to the increased communication latency. In practice, the SG communication latency should be in the order of a few milliseconds [21], [22], yet it is hard to achieve in large scale SGs. As a result, how to minimize the communication latency becomes one of research focuses.

TABLE I
Power requirements of different appliances in a typical HAN.

Electrical appliance	Power requirement (KW/hr)
Air conditioner	1
Refrigerator	0.2
Microwave oven	0.1
Light bulbs	0.05
Personal computer	0.2

Hauser *et al.* [21] further suggest that the SG communication network should be able to accommodate more messages simultaneously without any major impact on communication latency. The large volume of messages in SG communication will affect the bandwidth required. Let us consider a model where a CC, connected with 10,000 feeders (and BAN GWs), serves 100,000 customers. Assuming that each HAN GW generates a message every second to the BAN GW [23] in a typically power-intensive period (e.g., during a hot summer day when many consumers want to simultaneously switch on their air-conditioners), the total number of generated messages per second is 100,000. The BAN GWs also generate messages to each other and also to the CC through the NAN GW. If the



	Type of Message (ToM)	Description					Size
1	Command / Request	To update meter, to control load, to change tariff, etc.					25 Bytes
2	Meter Periodic Data read	Real Power (kW)	Reactive Power (kVAr)	Micro-generation (kW)	Voltage	Power Factor	32 Bytes
3	Confirmation / Notification message	Failure notifications, messages, etc.					25 Bytes
4	Meter sends Error Report	This report is automatically produced when failure occurs within the system					18 Bytes
5	Meter sends Performance Report	This report is produced on occurrence of the failure or as scheduled to determine meter performance					150 Bytes
6	Meter sends Outage Report	Outage report is sent after the supply has been restored					14 Bytes
7	Weekly read submission	Output data after one week					28 Bytes
8	One month of data	Meter sends one month of data					40320 Bytes
9	Last day import data	Summary of usage on the last day					192 Bytes

Fig. 2. Considered packet structure for SG communications.

average packet size is 100Bytes, the required transmission line bandwidth is estimated to be 800 Mbps.

As evident from the above illustrative example, any secure SG communication framework requires to have lightweight operations. The reasons behind this are two-fold: (i) to avoid possibly high communication delay, and (ii) to reduce communication overhead by cutting down unnecessary signal messages. In addition, note that the security headers contribute to the increased packet size as well (as shown in Fig. 2). Therefore, we may infer that a lightweight authentication mechanism is essential for designing effective authentication algorithms for HAN/BAN/NAN GWs.

However, the currently available proposals for SG security lack the detailed documentation, including the choice of adequate cryptosystems. Also, to the best of our knowledge, there is no secure framework to reliably authenticate the smart meters in SG. For instance, the BAN GW should authenticate the requesting HAN GWs while the NAN GW should be able to authenticate its BAN GWs. The cryptographic overheads may take up a significant portion of the total packet size. In addition, cryptographic operations also contribute to significant computation cost, especially in the receiver-end, which verifies the message. In a SG, a smart meter may send each message within a time interval of one second. In the afore-mentioned model consisting of 100,000 consumers, the number of messages that requires to be verified per second by the NAN GW may be significantly high. Also, there is processing delay at the respective smart meters for decrypting incoming encrypted messages. This increases the communication latency. Because the conventional Public Key Infrastructure (PKI) schemes are not adequate for the stringent time requirement of SG communications, a lightweight verification algorithm tailored for SG communications is required so that the incoming messages may be processed faster.

In addition, the smart meters are vulnerable to various attacks found in literature. The use of IP enabled technologies make SG more vulnerable to cyber-attacks listed in Table II. To solve this problem, a security framework is required, which can take into account various design objectives in order to thwart these security threats.

V. Secure and Reliable Framework for SG Communication

In order to address the afore-mentioned threats, we propose a framework with security and reliability guarantees. The secure and reliable framework for SG communications should achieve the following objectives.

TABLE II
SECURITY THREATS AGAINST SG COMMUNICATIONS AND SECURITY REQUIREMENTS TO SOLVE THESE PROBLEMS.

Attack	Impact on SG	Security requirement
Sniffing on smart meters	Same problem as conventional network	Encrypted packets: tougher for decoding traffic
Traffic Analysis	Difficult to detect	Change encryption keys periodically
Denial of Service (DoS) Wireless jamming & interference	Can extract keys from second generation Zigbee chips [24]	Authenticated sharing of resources and/or channels
DoS Buffer overflow attack	May delete the content of smart meters	Debug programs and protocol thoroughly
Reconfigure attack	Install unstable firmware on smart meter(s) and electronic appliances	Only permit secure firmware upgrade from authenticated CCs
Spoofing	- Impersonate smart meters - Increase victim's bill - lower attacker's own bill	Authenticate smart meter over Internet Protocol Security (IPSec)
Man-in-the-Middle (MitM)	May impersonate smart meters [25]	Secure communication over IPSec
Replay attack	- Store current data (during low power usage) of smart meter - Then send the stored data to the utility company at a later time (during high power usage) [26]	- Use time-stamp and time-synchronization at smart meters and CC - Use time-variant nonce

1. Source authentication and message integrity: The smart meters should be able to verify the origin and integrity of a received packet. For example, if a BAN GW receives a packet from one of its HAN GWs, the BAN GW needs to authenticate the HAN GW. After successful authentication, it needs to check whether the packet is unmodified.
2. Low communication overhead and fast verification: The security scheme should be efficient in terms of small communication overhead and acceptable processing latency. In other words, a large number of message signatures from many smart meters should be verified in a short interval.
3. Conditional privacy preservation: The actual identity of a smart meter (e.g., the name of the owner, the apartment number, and so forth) should be concealed by adequate encryption technology.
4. Prevention of internal attack: A HAN GW owner, holding its own keying material, should not be able to obtain neighboring HAN GWs' keying materials. In this way, even if a smart meter is compromised, an adversary cannot use the compromised smart meter to access other smart meters' important information.
5. Maintaining forward secrecy: It should be ensured that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in the future.

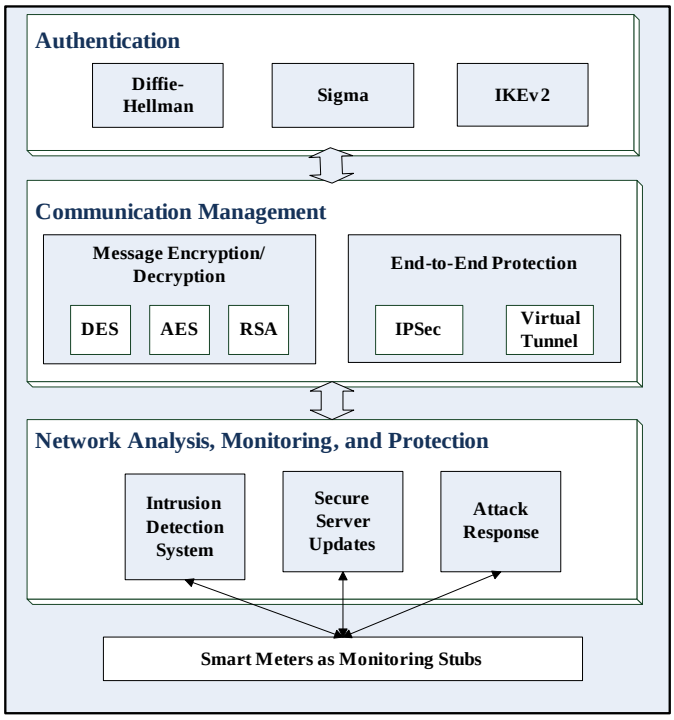


Fig. 3. Envisioned security framework for SG communications.

Fig. 3 presents a security framework for establishing a secure communication environment in SG. The framework is divided into three parts, namely authentication, communication management, and network analysis, monitoring and protection. The smart meters are required to be authenticated prior to their participation in the communication with other smart meters or SG gateways. The authentication scheme may be based on protocols such as Diffie-Hellman, SIGn-and-MAc (SIGMA), or Internet Key Exchange (IKEv2). The communication management module comprises two parts, namely message encryption/decryption and end-to-end protection. Existing cryptographic algorithms, e.g., Data Encryption Standard (DES), Advanced Encryption Standard (AES), or Rivest, Shamir, and Adleman (RSA) public key encryption, may be employed to encrypt the communication. On the other hand, for end-to-end protection, Internet Protocol Security (IPSec) or virtual tunnel may be used to enhance SG communications security. In the network analysis, monitoring, and protection module, smart meters act as monitoring stubs. The monitoring stubs are equipped with anomaly and/or signature-based intrusion detection algorithms in order to detect malicious threats listed in Table II. If the system detects any attack and deems a secure update, it contacts a secure server to download appropriate patches or firmware updates. The monitoring stubs may also provide appropriate responses to the detected attacks. It should be noted that all the features of this SG security framework are not elaborated in this paper. We focus on the first step of the framework, i.e., designing an appropriate authentication scheme, which is lightweight and suited for delay-sensitive

and bandwidth-intensive SG communications. We present our authentication scheme in the rest of this section.

Assume that HAN GW i and BAN GW j have their private and public key pairs. The public and private keys of HAN GW i are denoted by $PubHAN\_GWi$ and $PrivHAN\_GWi$, respectively. The public and private keys of BAN GW j are referred to as $PubBAN\_GWj$ and $PrivBAN\_GWj$. For the initial handshake between the HAN and BAN GWs, the Diffie-Hellman key establishment protocol [27] is adopted.

Let $\mathbb{G} = \langle g \rangle$ be a group of large prime order q such that the Computational Diffie-Hellman (CDH) assumption holds, i.e., given g^a, g^b, for unknown $a, b \in \mathbb{Z}_q^*$, it is hard to compute $g^{ab} \in \mathbb{G}$. Based on the CDH assumption, our envisioned lightweight message authentication scheme is shown in Fig. 4, and the detailed steps are as follows.

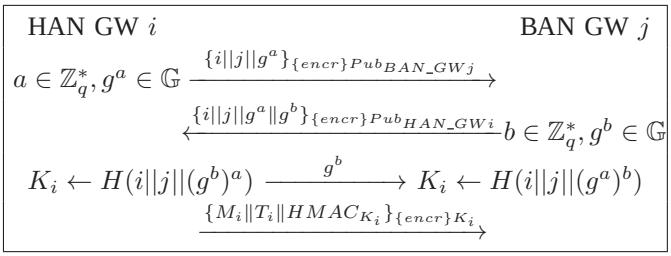


Fig. 4. Proposed lightweight message authentication scheme

1. HAN GW i chooses a random number $a \in \mathbb{Z}_q^*$, computes g^a, and sends g^a in an encrypted request packet to BAN GW j.

   HAN GW$_i \rightarrow$ BAN GW$_j : \{i||j||g^a\}_{\{encr\}Pub_{BAN_GWj}}$

2. BAN GW j decrypts it and sends an encrypted response consisting of g^b, where b is a random number.

   BAN GW$_j \rightarrow$ HAN GW$_i : \{i||j||g^a\|g^b\}_{\{encr\}Pub_{HAN_GWi}}$

3. After receiving BAN GW j's response packet, HAN GW i recovers g^a, g^b with its private key. If the recovered g^a is correct, BAN GW j is authenticated by HAN GW i. Then, with g^b and a, HAN GW i can compute the shared session key $K_i = H(i||j||(g^b)^a)$, where $H : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$ is a secure cryptographic hash function, and sends g^b to BAN GW j in the plaintext form.
4. Once the correct g^b is received by the BAN GW j, BAN GW j authenticates HAN GW i, and computes the same shared session key $K_i = H(i||j||(g^a)^b)$.
5. In our approach, to ensure data integrity in the late transmission, we employ a Hash-based Message Authentication Code (MAC) generation algorithm by using the shared session key K_i. The generated MAC, $HMAC_{K_i}$, is based on the message M_i and recorded time instance of sending the message T_i, where T_i is used to thwart possible replay attacks. Then, HAN GW i transmits the following to the BAN GW j.

   HAN GW$_i \rightarrow$ BAN GW$_j : \{M_i\|T_i\|HMAC_{K_i}\}_{\{encr\}K_i}$

   Because K_i is shared between BAN GW j and HAN GW i itself, BAN GW j can verify the authenticity of the sender and integrity of M_i. Thus, it can provide the NAN GW with the authenticated messages.

VI. Security Analysis

In this section, we analyze the security of the proposed lightweight message authentication scheme to check whether the required security properties can be satisfied.

• *The proposed scheme can provide mutual authentication.* In the proposed scheme, since g^a is encrypted with BAN GW j's public key, only if the adopted public key encryption technique is secure, then BAN GW j is the only one who can recover g^a with the corresponding private key. Therefore, when HAN GW i receives the correct g^a in Step 3, HAN GW i can ensure its counterpart is BAN GW j. With the same reason, because g^b is encrypted with HAN GW i's public key, BAN GW j can also authenticate HAN GW i if it can receive the correct g^b in Step 4. Therefore, the proposed scheme can provide mutual authentication between HAN GW i and BAN GW j.

• *The proposed scheme can establish a semantic-secure shared key in the mutual authentication environment.* The semantic security of the shared key under the chosen-plaintext attack indicates that an adversary $\mathcal{A}$ cannot distinguish the actual shared key K_i from ones randomly drawn from the session key space, when $\mathcal{A}$ is given g^a, g^b and $Z \in \mathbb{G}$, where Z is either the actual shared key K_i or a random value R drawn from the session key space, according to a random bit $\beta \in \{0,1\}$, i.e., $Z = K_i$ when $\beta = 0$, and $Z = R$ is returned when $\beta = 1$. Let $\beta' \in \{0,1\}$ be $\mathcal{A}$'s guess on β. Then, the semantic security indicates $\Pr[\beta = \beta'] = \frac{1}{2}$. Now, suppose there exists an adversary $\mathcal{A}$ who can break the semantic security of the shared key with a non-negligible advantage $\varepsilon = 2\Pr[\beta = \beta'] - 1$ within the polynomial time, we can use the adversary $\mathcal{A}$'s capability to solve the CDH problem, i.e., give (g, g^a, g^b) for unknown $a, b \in \mathbb{Z}_q^*$, to compute $g^{ab} \in \mathbb{G}$.

First, the adversary $\mathcal{A}$ is given the tuple (g, g^a, g^b), and also allowed to make q_H distinct queries on the random oracle $\mathcal{H}$ in the random oracle model [28]. To cater for these random oracle queries, we maintain an $\mathcal{H}$-list. When a new query $C_i \in \mathbb{G}$ is asked for the session key shared between HAN GW i and BAN GW j, we choose a fresh random number $Z_i \in \mathbb{G}$, set $\mathcal{H}(i||j||C_i) = Z_i$, put $(i||j||C_i, Z_i)$ in $\mathcal{H}$-list, and return Z_i to $\mathcal{A}$. When the adversary $\mathcal{A}$ makes a query on the session key, we flip a coin $\beta \in \{0,1\}$, and return a random value $Z^\star \in \mathbb{G}$.

Let $\mathcal{E}$ denote the event that $C = g^{ab}$ has been queried by $\mathcal{A}$ to the random oracle $\mathcal{H}$. If the event $\mathcal{E}$ does not occur, $\mathcal{A}$ has no idea on the session key $K_i = H(i||j||g^{ab})$, then we have

$$\Pr[\beta = \beta' | \bar{\mathcal{E}}] = \frac{1}{2} \tag{1}$$

and

$$\begin{aligned} \Pr[\beta = \beta'] &= \Pr[\beta = \beta' | \mathcal{E}] \cdot \Pr[\mathcal{E}] + \Pr[\beta = \beta' | \bar{\mathcal{E}}] \cdot \Pr[\bar{\mathcal{E}}] \\ &= \Pr[\beta = \beta' | \mathcal{E}] \cdot \Pr[\mathcal{E}] + \frac{1}{2} \cdot \Pr[\bar{\mathcal{E}}] \\ &\leq \Pr[\mathcal{E}] + \frac{1}{2} \cdot (1 - \Pr[\mathcal{E}]) = \frac{1}{2} + \frac{\Pr[\mathcal{E}]}{2} \end{aligned} \tag{2}$$

In addition, since

$$\varepsilon = 2\Pr[\beta = \beta'] - 1 \Rightarrow \Pr[\beta = \beta'] = \frac{1}{2} + \frac{\varepsilon}{2} \quad (3)$$

we have $\Pr[\mathcal{E}] \geq \varepsilon$. Because $\mathcal{H}$-list contains q_H entries, we can pick up the correct $C_i = g^{ab}$ and solve the CDH problem with the success probability $1/q_H$ given the event $\mathcal{E}$ occurs. Combining the above probabilities together, we have

$$\mathbf{Succ}^{\mathrm{CDH}} = 1/q_H \cdot \Pr[\mathcal{E}] \geq \frac{\varepsilon}{q_H} \quad (4)$$

However, this result contradicts with the CDH assumption. Therefore, the proposed scheme can also establish a semantic-secure shared key. Note that, if either HAN GW i or BAN GW j is compromised, the mutual authentication environment cannot be achieved. However, the compromise of either HAN GW i or BAN GW j's private key does not affect the security of the previous session keys. As a result, the proposed scheme can also achieve perfect forward secrecy [27].

- *The proposed scheme can provide an authenticated and encrypted channel for the late successive transmission.* Because both HAN GW i and BAN GW j hold their shared session key K_i, the late transmission $\{M_i \| T_i \| HMAC_{K_i}\}_{\{encr\}K_i}$ can achieve not only the confidentiality but also the integrity. Meanwhile, the embedded timestamp T_i can also thwart the possible replay attacks. Therefore, the proposed scheme can provide an authenticated and encrypted channel for the late successive transmissions.

In summary, the proposed scheme is secure and suitable for the two-party communication in SG environment.

VII. Comparative Evaluation

The proposed message authentication scheme is evaluated by analytical results using MATLAB [29]. For the SG topology, we consider 10 NANs, each having 50 BANs. The number of HANs in each BAN is varied from 10 to 140. The other simulation parameters are listed in Table III. We compare the performance of our proposed authentication scheme with ECDSA. The reason for considering ECDSA is that it is demonstrated to be a secure authentication protocol for SG demand response communications in [14]. In our simulations, we employed AES-128 algorithm to encrypt the packets to be transmitted using the shared session key, K_i, generated during the proposed authentication mechanism. To compare with this, we considered ECDSA-256 authentication and encryption in our simulations since its security level is comparable to that of 128-bits cryptography [30]. It is worth noting that only the messages exchanged between HANs and their corresponding BAN are considered for authentication. In addition, the session key is considered being generated at the commencement of each new session.

The size of the HAN packet bound for the BAN is 102 bytes, which is sufficient to contain the users' power requirements and request to the CC. The sizes of the generated MAC is set to 16 bytes based on RACE Integrity Primitives Evaluation Message Digest (RIPEMD-128) algorithm. The reason to choose this hash algorithm for creating the MAC is due to its resiliency against collision and preimage

TABLE III
Simulation parameters.

Simulation parameter	Value
BAN GW CPU clock	160 MHz
Number of HANs	10-140
HAN message generation interval (Δ)	10s
TCP header	20 Bytes
Message header	50 Bytes
Raw message	32 Bytes
Hash header in proposed authentication scheme	16 bytes
ECDSA certificate size	125 bytes
ECDSA signature size	64 bytes
Simulation time	800s

attacks. The HAN message generation interval, denoted by Δ, is set to 10s, to correspond with highly frequent need for demand-response communications in SG. At first, two performance metrics are considered for evaluation, namely communication overhead and message decryption/verification delay. The comparative results are shown in Figs. 5 and 6. Fig. 5 plots the communication overhead (in KB) at a given BAN GW for varying number of smart meters. It should be noted that only one session per HAN GW with the BAN GW is considered. When the number of smart meters is low, both the proposed and conventional schemes contribute to small overheads (below 5Kb). The communication overheads gradually increase with the increasing number of smart meters. This increase is, however, more significant in case of the conventional ECDSA protocol. For instance, when 140 smart meters (i.e., HAN GWs) are considered for a given BAN GW, the ECDSA communication overhead incurred at the BAN GW is significantly high (36KB) in contrast with a relatively low value (13KB) for the proposed message authentication. The conventional scheme experiences higher communication overheads mainly due to the certificate and signature included in each packet. Thus, the proposed scheme demonstrates higher scalability for larger topologies. Fig. 6 shows the

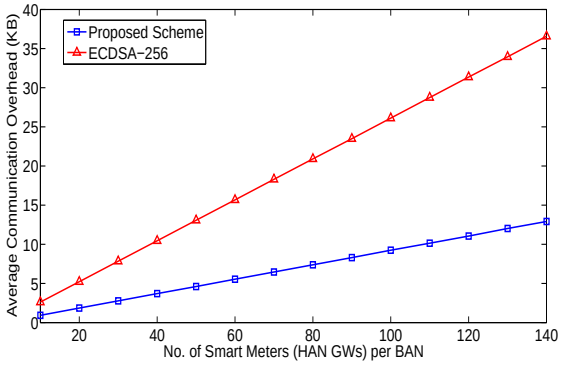


Fig. 5. Average communication overhead experienced by the BAN GW for varying number of smart meters (i.e., HAN GWs).

comparison between the proposed and conventional schemes in terms of decryption/verification delay per BAN GW. It is worth noting that OpenSSL package is used to measure the delays for the proposed scheme and the conventional ECDSA scheme [31]. The OpenSSL package was used on a computer running Intel Xeon Processor (E5450) and Linux distribution

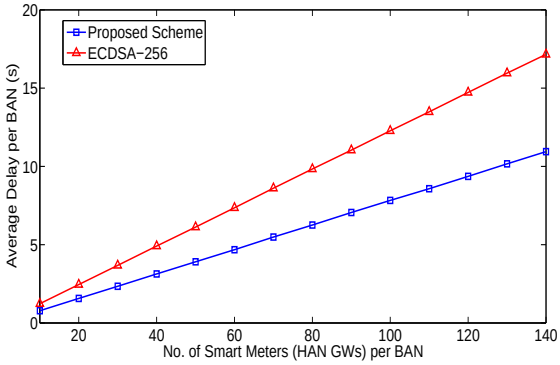


Fig. 6. Average delay at the BAN GW for varying number of smart meters (i.e., HAN GWs).

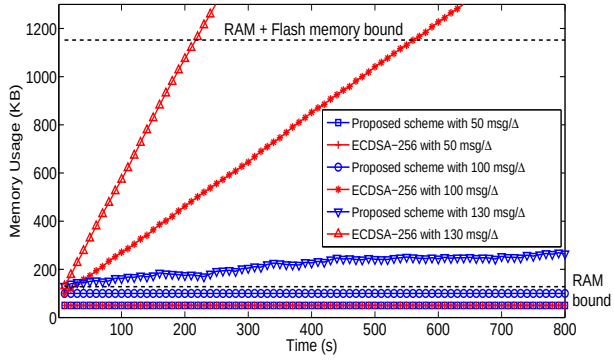


Fig. 7. Memory usage of the proposed and conventional ECDSA authentication algorithms for different message volumes received by BAN.

of Debian 4.0. The processing speed of the experimental PC was 3.0GHz. In order to simulate the BAN GW, we scaled the experimental values (e.g., decryption time) by 19.2 times to fit the 160MHz of the BAN GW. As evident from the results, the decryption delay increases linearly for both these schemes. However, the conventional ECDSA scheme exhibits higher decryption delay compared to that demonstrated by the proposed one. The reason is that the proposed scheme provides a secure authentication process followed by AES encryption, which is faster than the conventional ECDSA scheme which relies on signature verification along with decryption at the BAN for every message coming from each HAN.

Next, the memory usage of the proposed and conventional authentication algorithms over time for varying message volumes received by a given BAN GW is shown in Fig. 7. The memory usage consists of two upper bounds, namely the RAM boundary and the RAM plus flash memory boundary that comprise 128KB and 1MB, respectively. When the message rate is 50 per Δ, the conventional ECDSA scheme takes about 50KB of memory, which is not exceeding the allocated RAM in the BAN GW. In case of the proposed authentication scheme with the same rate of message arrival at the BAN GW, the memory usage is similar to that required by the conventional protocol. When the number of messages per Δ arriving at the BAN GW increases to 100, the conventional ECDSA scheme becomes overwhelmed with the high number of messages coming from the high number of HANs and it exceeds the RAM and flash memory bound after 570s. In contrast with this, the proposed scheme achieves much lower memory usage (approximately 100KB) and continues to support this throughout the entire course of the simulation (i.e., 800s). However, when the number of apartments in a given building is raised which results in a higher message reception rate of 130 messages per Δ at the BAN GW, the results change even more significantly. Fig. 7 shows that the conventional ECDSA method, in this case, takes up all the available memory at the BAN GW rather quickly (within 220s of the start of the simulation). On the other hand, the proposed scheme manages to stay below 270KB of the overall available memory throughout the simulation. This good performance of the proposed scheme can be attributed to the less processing in decrypting the packets that result in less queuing time in the RAM and the flash memory.

Fig. 8 shows the number of HANs supported by the conventional and proposed schemes in terms of usage of the available RAM and flash memory at the BAN GW over time. As for the ECDSA scheme, we can see from Fig. 8(a) that if the number of HANs per one BAN exceeds 81, the memory usage starts to increase with time. This implies that after a while the memory usage will overflow the memory space of the BAN GW (i.e., 1152KB consisting of 1MB of flash memory and 128KB of RAM). At that point, the messages coming from the HANs will be dropped and not served within the BAN GW queue. For instance, for 95 HANs supported by a particular BAN, the conventional ECDSA scheme requires around 1260KB of memory space in order to avoid any drop of messages in the 800^{th} second of the simulation. On the other hand, Fig. 8(b) shows a clear improvement of our proposed scheme in terms of the number of HANs supported by a given BAN. In fact, the proposed scheme can accommodate 127 HANs within the BAN. This is due to the fact that the proposed scheme is able to process the messages coming from the HANs in the BAN memory space much quicker than the conventional scheme.

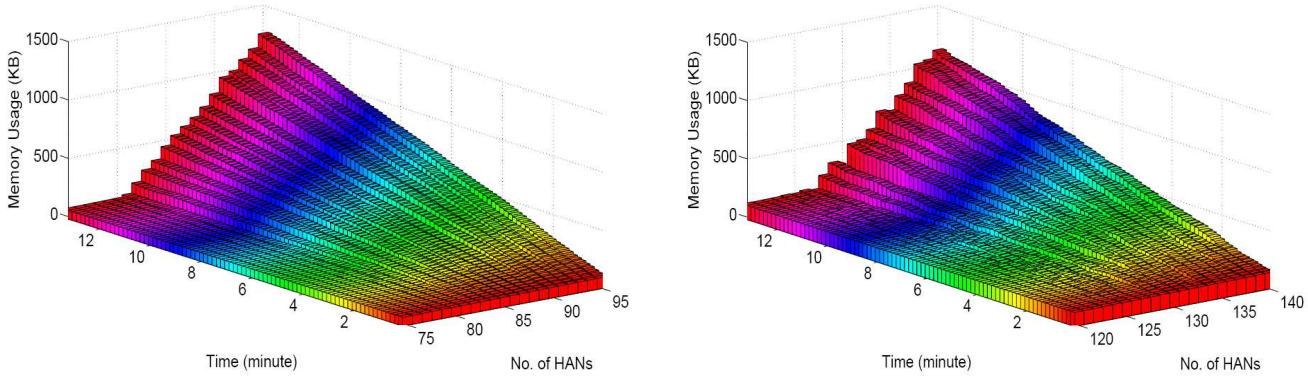
VIII. Conclusion

In this paper, we have proposed a lightweight message authentication scheme tailored for the requirements of SG communications based on Diffie-Hellman key establishment protocol and hash-based authentication code. Detailed security analysis verifies that our proposed scheme is able to satisfy the desirable security requirements within a secure and reliable SG communications framework. In addition, extensive computer-simulations are conducted to demonstrate the high efficiency of the proposed scheme. In our future work, we will further explore other challenging security issues, such as denial of service attacks, in SG environment.

References

[1] M. Fouda, Z. Md. Fadlullah, N. Kato, R. Lu, and X. Shen, “Towards a Light-weight Message Authentication Mechanism Tailored for Smart Grid Communications”, Proc. IEEE INFOCOM’11-SCNC, Shanghai, China, Apr. 2011.

[2] C. W. Gellings, The smart grid: Enabling energy efficiency and demand response, Lilburn, GA: Fairmont Press, 2009.



(a) Number of HANs supported by the conventional ECDSA-256 scheme.

(b) Number of HANs supported by the proposed scheme.

Fig. 8. Number of HANs supported by the proposed and conventional authentication schemes for SG communications.

[3] Y. Yuan, Z. Li, and K. Ren, "Modeling Load Redistribution Attacks in Power System", IEEE Trans. on Smart Grid, vol. 2, no. 2, pp. 382-390, Jun. 2011.

[4] Z. Yang, S. Yu, W. Lou and C. Liu, "P2: Privacy-preserving communication and precise reward architecture for V2G networks in Smart Grid," IEEE Trans. on Smart Grid, to be published.

[5] Z. M. Fadlullah, M. M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, "Toward Intelligent Machine-to-Machine Communications in Smart Grid", IEEE Communications Magazine, vol. 49, no. 4, pp. 60-65, Apr. 2011.

[6] H. Zhu, X. Lin, R. Lu, P.H. Ho, and X. Shen, "SLAB: Secure Localized Authentication and Billing Scheme for Wireless Mesh Networks", IEEE Trans. on Wireless Communications, vol. 7, no. 10, pp. 3858-3868, Oct. 2008.

[7] X. Lin, R. Lu, P.H. Ho, X. Shen and Z. Cao, "TUA: A Novel Compromise-Resilient Authentication Architecture for Wireless Mesh Networks", IEEE Trans. on Wireless Communications, vol. 7, no. 4, pp. 1389-1399, Apr. 2008.

[8] R. Lu, X. Li, X. Liang, X. Lin, and X. Shen, "GRS: The Green, Reliability, and Security of Emerging Machine to Machine Communications", IEEE Communications Magazine, vol. 49, issue 4, pp. 28-35, Apr. 2011.

[9] Available at, "IEEE P2030 Draft Guide", http://grouper.ieee.org/groups/scc21/2030/2030_index.html

[10] A. Hamlyn, H. Cheung, T. Mander, L. Wang, C. Yang, and R. Cheung, "Network Security Management and Authentication of Actions for Smart Grids Operations", in Proc. IEEE Electrical Power Conference, Montreal, Que, Canada, Oct. 2007.

[11] G. N. Ericsson, "Cyber Security and Power System Communication-Essential Parts of a Smart Grid Infrastructure", IEEE Trans. Power Delivery, vol. 25, no. 3, pp. 1501-1507, Jul. 2010.

[12] A. R. Metke and R. L. Ekl, "Smart Grid Security Technology", in Proc. IEEE PES on Innovative Smart Grid Technologies (ISGT'10), Washington D. C., USA, Jan. 2010.

[13] K. Kursawe, G. Danezis, and M. Kohlweiss, "Privacy-friendly Aggregation for the Smart-grid", available online at http://research.microsoft.com/apps/pubs/?id=146092.

[14] M. Kgwadi and T. Kunz, "Securing RDS Broadcast Messages for Smart Grid Applications", in Proc. 6^{th} Int. Wireless Commun. and Mobile Computing Conference, Caen, France, Jun. 2010.

[15] X. Lin, X. Sun, P.H. Ho, and X. Shen, "GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communications", IEEE Trans. on Vehicular Technology, vol. 56, no. 6, pp. 3442-3456, Nov. 2007.

[16] R. Lu, X. Lin, H. Zhu, P.H. Ho and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications", Proc. IEEE INFOCOM'08, Phoenix, AZ, USA, Apr. 2008.

[17] C. Cuijpers and B. J. Koops, Het wetsvoorstel 'slimme meters': een privacytoets op basis van art. 8 evrm., Technical report (in Dutch), Tilburg University, Oct. 2008.

[18] The Smart Grid Interoperability Panel Cyber Security Working Group: Smart Grid Cybersecurity Strategy and Requirements, US National Institute for Standards and Technology (NIST), available at: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

[19] MSP430 for Utility Metering Applications, available at Texas Instruments, http://focus.ti.com/mcu/docs/mcuorphan.tsp?contentId=31498

[20] High-level smart meter data traffic analysis, Engage Consulting Ltd. for the Energy Networks Association (ENA), UK, May 2010.

[21] C. H. Hauser, D. E. Bakken, I. Dionysiou, K. H. Gjermundrod, V. S. Irava, J. Halkey, and A. Bose, "Security, Trust, and QoS in Next Generation Control and Communication for Large Power Systems", Int. J. Critical Infrastructures, vol.4, no. 1/2, pp. 3-16, 2008.

[22] R. Vaswani and E. Dresselhuys, "Implementing the Right Network for the Smart Grid: Critical Infrastructure Determines Long-Term Strategy", White Paper, available at, http://www.silverspringnet.com/pdfs/SSN_whitepaper_UtilityProject.pdf

[23] A. Aggarwal, S. Kunta, and P. K. Verma,"A Proposed Communications Infrastructure for the Smart Grid", in Proc. IEEE PES Innovative Smart Grid Technologies Conf., Gaithersburg, MD, Jan. 2010.

[24] T. Goodspeed, "Extracting Keys from Second Generation Zigbee Chips", Proc. Black Hat USA'09, Las Vegas, NV, Jul. 2009.

[25] S. Blake-Wilson, Authentec white paper, "Embedded Security Solutions", available at, http://www.authentec.com/

[26] M. Carpenter, T. Goodspeed, B. Singletary, E. Skoudis, and J. Wright, "Advanced Metering Infrastructure Attack Methodology", InGuardians white paper, Jan. 2009.

[27] D. R. Stingson, Cryptography: Theory and Practice, 3rd ed. Boca Raton, FL: CRC, 2005.

[28] M. Bellare and P. Rogaway, "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols," Proc. 1st ACM Conference on Computer and Communications Security (CCS), Fairfax, VA, pp. 6273, Nov. 1993.

[29] Mathworks - MATLAB and Simulink for Technical Computing, available at, http://www.mathworks.com/

[30] G. Calandrielloy, P. Papadimitratosz, J-P. Hubauxz, and A. Lioyy, "Efficient and Robust Pseudonymous Authentication in VANET", Proc. VANET'07, Montreal, Quebec, Canada, Sep. 2007.

[31] OpenSSL, available at, http://www.openssl.org/

Mostafa M. Fouda (S09-M11) received the B.Sc. degree with honors in electronics and telecommunications and the M.Sc. degree in electrical communications from the Faculty of Engineering at Shoubra, Benha University, Egypt, in 2002 and 2007, respectively, and the Ph.D. degree from the Graduate School of Information Sciences (GSIS), Tohoku University, Japan, in 2011. He received the prestigious First Place Award from the Faculty of Engineering at Shoubra in 2002.

He is currently serving as a Global COE Postdoctoral Fellow at GSIS, Tohoku University, Japan. He also holds the position of an Assistant Professor in the Faculty of Engineering at Shoubra, Benha University, Egypt. His research interests include smart grid communications, network security, peer to peer applications, and multimedia streaming.

Zubair Md. Fadlullah (S'06-M'11) received B.Sc. degree in Computer Science from the Islamic University of Technology (IUT), Bangladesh, in 2003, and M.S. and Ph.D. degrees from the Graduate School of Information Sciences (GSIS), Tohoku University, Japan, in 2008 and 2011, respectively.

Currently, he is serving as an Assistant Professor at GSIS. His research interests are in the areas of smart grid, network security, intrusion detection, and quality of security service provisioning mechanisms.

Dr. Fadlullah was a recipient of the prestigious Deans and Presidents awards from Tohoku University in March 2011.

Nei Kato (M'03, A'04, SM'05) received his M.S. and Ph.D. Degrees in information engineering from Tohoku University, Japan, in 1988 and 1991, respectively. He joined Computer Center of Tohoku University at 1991, and has been a full professor with the Graduate School of Information Sciences since 2003. He has been engaged in research on satellite communications, computer networking, wireless mobile communications, image processing and neural networks. He has published more than 200 papers in journals and peer-reviewed conference proceedings. He currently serves as the Chair of IEEE Satellite and Space Communications Technical Committee, the Chair of Technical Committee of Satellite Communications, IEICE, a technical editor of IEEE Wireless Communications(2006-), an editor of IEEE Transactions on Wireless Communications(2008-), a co-guest-editor for IEEE Wireless Communications Magazine SI on "Wireless Communications for E-healthcare". He has served as a symposium co-chair for GLOBECOM'07 and ChinaCom'08, ChinaCom'09, the Vice Chair of IEEE WCNC2010 TPC, the ICC 2010 Ad Hoc, Sensor and Mesh Networking Symposium. He is serving as a workshop co-chair of VTC2010 and a symposium co-chair of ICC2011. His awards include Minoru Ishida Foundation Research Encouragement Prize(2003), Distinguished Contributions to Satellite Communications Award from the IEEE Communications Society, Satellite and Space Communications Technical Committee(2005), the FUNAI information Science Award(2007), the TELCOM System Technology Award from Foundation for Electrical Communications Diffusion(2008), and the IEICE Network System Research Award(2009). Besides his academic activities, he also serves on the expert committee of Telecommunications Council, Ministry of Internal Affairs and Communications, and as the chairperson of ITU-R SG4, Japan. Nei Kato is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and a senior member of IEEE.

Rongxing Lu (S'09, M'11) is currently working toward a Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is currently a research assistant with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and trusted computing.

Xuemin (Sherman) Shen (M'97-SM'02-F'09) received the B.Sc.(1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a Professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo, Canada. Dr. Shen's research focuses on resource management in interconnected wireless/wired networks, UWB wireless communications networks, wireless network security, wireless body area networks and vehicular ad hoc and sensor networks. He is a co-author of three books, and has published more than 400 papers and book chapters in wireless communications and networks, control and filtering. Dr. Shen has served as the Technical Program Committee Chair for IEEE VTC'10, the Tutorial Chair for IEEE ICC'08, the Technical Program Committee Chair for IEEE Globecom'07, the General Co-Chair for Chinacom'07 and QShine'06, the Founding Chair for IEEE Communications Society Technical Committee on P2P Communications and Networking. He has also served as a Founding Area Editor for IEEE Transactions on Wireless Communications; Editor-in-Chief for Peer-to-Peer Networking and Application; Associate Editor for IEEE Transactions on Vehicular Technology; Computer Networks; and ACM/Wireless Networks, Guest Editor for IEEE JSAC, IEEE Wireless Communications, IEEE Communications Magazine, and ACM Mobile Networks and Applications, etc. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004 and 2008 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered Professional Engineer of Ontario, Canada, and a Distinguished Lecturer of IEEE Communications Society.