Towards a Light-weight Message Authentication Mechanism Tailored for Smart Grid Communications

---

Citation:

Mostafa M. Fouda, Zubair Md. Fadlullah, Nei Kato, Rongxing Lu, and Xuemin (Sherman) Shen, "Towards a Light-weight Message Authentication Mechanism Tailored for Smart Grid Communications," 30th IEEE International Conference on Computer Communications (INFOCOM 2011), Security in Computers, Networking and Communications (SCNC) Workshop, Shanghai, China, pp. 1018-1023, Apr. 2011.

URL:

http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5928776

Towards a Light-weight Message Authentication Mechanism Tailored for Smart Grid Communications

Mostafa M. Fouda[1*], Zubair Md. Fadlullah[1†], Nei Kato[1‡], Rongxing Lu[2§], and Xuemin (Sherman) Shen[2¶]
[1]Graduate School of Information Sciences, Tohoku University, Japan
[2]Department of Electrical and Computer Engineering, University of Waterloo, Canada
*mfouda@it.ecei.tohoku.ac.jp, †zubair@it.ecei.tohoku.ac.jp, ‡kato@it.ecei.tohoku.ac.jp,
§rxlu@bbcr.uwaterloo.ca, ¶xshen@bbcr.uwaterloo.ca

***Abstract*—Smart Grid (SG) technology, which aims at bringing the world's aging electric grids into the 21^{st} century by utilizing intelligent transmission and distributed networks, has been gaining momentum in recent years. Despite its attractive features, the SG technology remains vulnerable to some security threats, such as spoofing and man-in-the-middle attacks. In this paper, to address these potential security issues, we propose a light-weight and secure message authentication mechanism. The proposed mechanism is based on Diffie-Hellman key establishment protocol and hash-based message authentication code, which allows various smart meters at different points of the SG to make mutual authentication and achieve message authentication with low latency and few signal message exchanges. Detailed security analysis shows it can satisfy the desirable security requirements. In addition, extensive computer-based simulation also demonstrates its efficiency.**

I. Introduction

The Smart Grid (SG) concept is synonymous to intelligent grid or future grid [1], and is aimed at providing the end users (i.e., consumers) with more stable and reliable power. The common aspect of the different SG proposals consists in the two-way communication framework between the power source and the consumers. In addition, sensing entities and control systems lie along the path of the power source and the end-users. The sensors are capable of detecting malfunctions or deviations from normal operational ranges, which usually require appropriate response from the SG control center. Furthermore, the responses from the control center need to be converted into control messages and transmitted to different segments of the SG. Therefore, the SG communication framework and functionality should be characterized, particularly in terms of its ability of provisioning consumer participation and resiliancy against malicious threats. In SG, consumers are usually equipped with smart meters, which are able to identify power consumption in a much more elaborate manner in contrast with the conventional energy meters. While the information collected by a smart meter can be obtained by the power company (i.e., the utility provider) for monitoring and billing purposes, the consumer can also access his/her smart meter to check the current usage and accordingly adjust the power usage (e.g., to use less electricity during peak hours to minimize unnecessary use of electric appliances). This may require the users to send periodic request messages to the utility provider. By doing so, they are able to actively participate in the power dissemination within the SG in a dynamic manner. To facilitate the two way communication between the consumers and the utility provider, the smart meters are integrated in the SG by the Advanced Metering Infrastructure (AMI). Furthermore, in order to create an effective SG communication backbone, IP-based networks are considered to be the most suitable choice for home area, buildings, and larger neighborhoods. An IP-based SG implies that each smart meter and each smart appliance (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, IP-based communication networks are likely to be challenged by a huge volume of delay-sensitive data and control information. Furthermore, the attacks against both wired and wireless IP-based networks may be easily carried out against IP-based SG communication networks. Therefore, it is crucial to prevent all possible security threats by properly designing SG communication protocols. In this paper, we propose a light-weight message authentication protocol 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 authentication code, the proposed scheme allows smart meters to make mutual authentication and achieve message authentication in a light-weight 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. Section II surveys related works. Section III presents an SG communications system model. Section IV describes the proposed light-weight message authentication scheme to secure communications amongst various SG entities. Section V provides the security analysis of our proposed mechanism. Simulation results are provided in Section VI to verify the effectiveness of the proposed mechanism followed by the concluding remarks in Section VII.

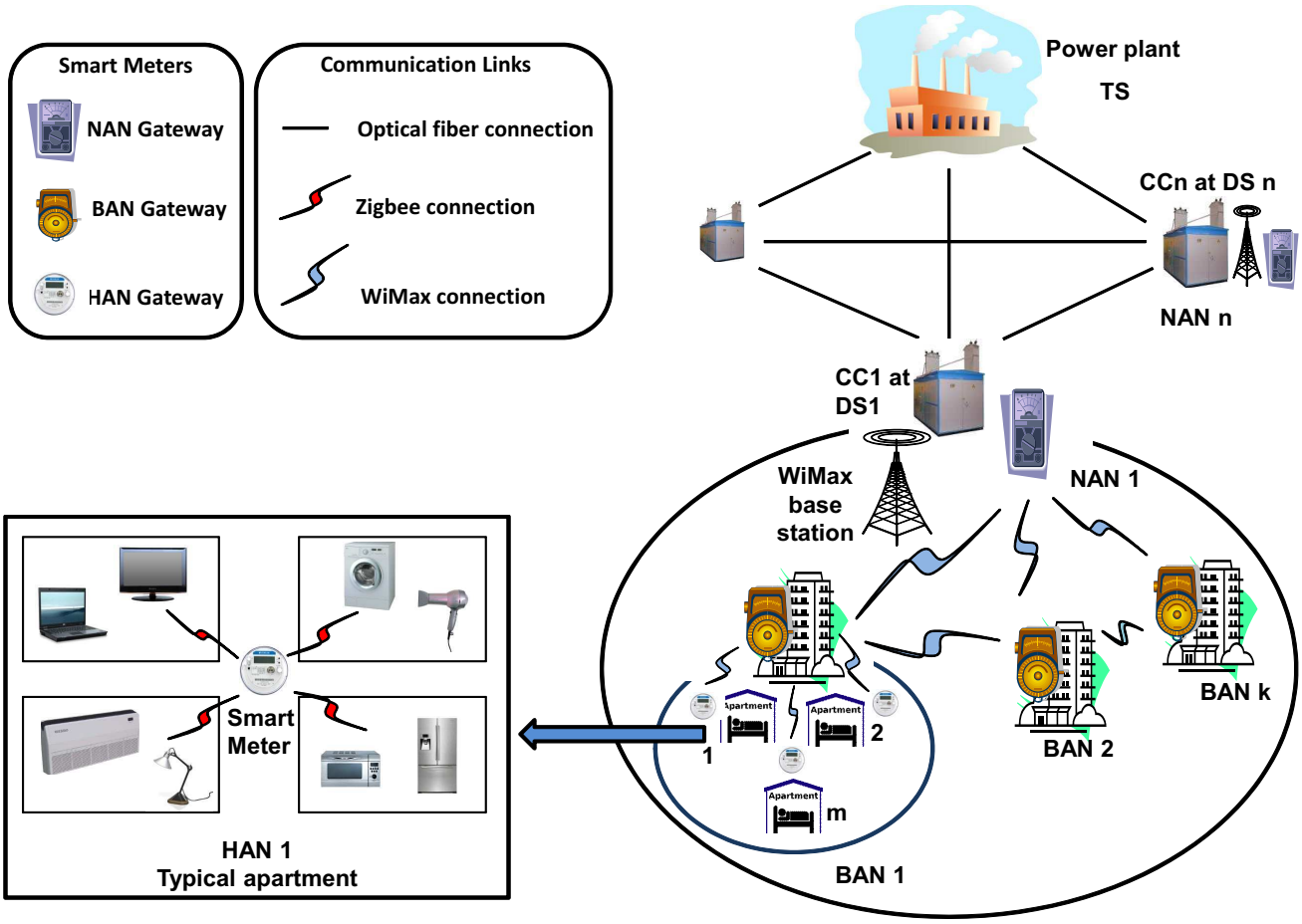

Fig. 1. Considered SG communications architecture.

II. Related Research Work

Three task forces have been created for IEEE P2030 Smart Grid standards to implement SG. One of the task forces is pertaining to cyber security, which describes system and communications protection policies and procedures to combat cyber attacks against SG [2]. However, these policies are broad in nature and should be considered as coarse desgin directives for enforcing security in SG communications.

Hamlyn *et al.* [3] proposed a utility computer network security management and authentication for actions and commands request in SG operations. However, their work focused on securing host area electric power systems and electric circuits.

Power system communication and cyber security issues are considered to be crucial components of SG [4]. It is suggested that numerous cyber security issues are to be addressed. For example, integrated Supervisory Control and Data Acquisition (SCADA)/energy management systems and administrative office Information Technology (IT) environments may lead to evolving security threats. In addition, the broadband capabilities have opened up new ways of introducing new functionality, both at smart meters and the central system collecting metering data. The utilites are interested in transferring data to the households that may include price information and special offers. However, such data may also contain control signals, which may raise delicate issues to deal with.

Metke *et al.* pointed out in [5] that SG deployments must satisfy strict security requirements. For instance, strong authentication is considered to be a requisite for all users and devices of the SG. With the large number of users and devices affected, scalable key and trust management systems, tailored to the particular requirements of the utility provider will be essential. In our work, by providing a broad SG communications framework, we propose a light-weight message authentication protocol, customized to the specific needs of SG.

III. SG Communications System Model

Fig. 1 depicts our considered SG communication framework, where the SG power transmission and distribution system is separated from the communication one. For clarity, we first briefly describe the power Distribution Network (DN). Power is delivered from the power plant to end-users through two components, namely the Transmission Substation (TS) at the power plant and a number of Distribution Substations (DSs). The former delivers power from the power plant over high voltage transmission lines (usually over 230 KV) to DSs. On the other hand, DSs are located at different regions and they are responsible for converting the electric power into

medium voltage levels and distributing the same to the feeders of the buildings. The building feeders convert the medium voltage level into a lower one for consumers' use.

From communications point of view, the considered SG topology is split into a number of networks. The TS, located at the power plant, and the Control Centers (CCs) of the DSs are connected with one another in a meshed network, which is built over optical fiber technology.

The communication framework for the lower distribution network (i.e., from CCs onward) is split into a number of hierarchical networks, namely Neighborhood Area Network (NAN), Building Area Network (BAN), and Home Area Network (HAN). For simplicity, each DS is considered to cover only one neighborhood area. Thus, in Fig. 1, there are n DSs covering n neighborhoods, i.e., the number of NANs is n. Each NAN is composed of a number of BANs. For instance, $NAN1$ consists of k BANs. On the other hand, every BAN contains a number of apartments. In Fig. 1, there are m apartments with their respective local area networks, each of which is referred to as a HAN. In addition, there are advanced meters called smart meters deployed in the SG architecture which comprise AMI for enabling an automated, two-way communication between the utility meter and the utility provider. The smart meters are equipped with two interfaces, namely for reading power and for communication gateway. The smart meters used in NAN, BAN, and HAN are referred to as NAN GW (GateWay), BAN GW, and HAN GW, respectively. For ease of understanding, we adopt a bottom-up approach where we start describing the SG communications framework from the HAN. In addition, it is also worth mentioning that based upon the existing standards of SG, IP-based communications networking is preferred which permits virtually effortless interconnections with HANs, BANs, NANs, CCs, and TS.

A. Home Area Network

The Home Area Network (HAN) is a subsystem within the SG dedicated to efficiently manage the on-demand power requirements of the end-users. $HAN1$ in Fig. 1 connects the equipments (e.g., television, washing machine, oven, and so forth) in the end-user's apartment to a HAN GW, which, in turn, communicates with $BAN1$. We adopt Smart Energy Profile (SEP) Version 1.5 as the communication protocol in HANs that employ ZigBee radio communications. We choose IEEE 802.15.4 ZigBee instead of other wireless solutions (e.g., WiFi and Bluetooth) due to its low power requirements, and simple network configuration and management. Indeed, ZigBee provides a decent communication range of 10 to 100 meters while maintaining significantly low power requirement (1 to 100 mW) and cost.

B. Building Area Network

A Building Area Network (BAN) consists of a number of apartments having HANs. The BAN smart meter/GW is typically set up at the building's power feeder. It can be used to monitor the power need and usage of the residents of the corresponding building. In order to facilitate BAN-HANs communication, WiMAX may be used to cover more areas. It should be noted that 3G, and other modes of communications may also be alternative solutions for this purpose.

C. Neighborhood Area Network

Each Neighborhood Area Network (NAN) consists of a number of BANs. One or more WiMAX base stations can be located in every NAN. It should be mentioned that the WiMAX framework used for SG communications should be separated from the existing ones used for providing other services, e.g., Internet, to prevent network congestion and possible security threats. A NAN, thus, represents a locality or a particular region. The NAN GW can monitor how much power is being distributed to a particular neighborhood by the corresponding CC at the DS.

IV. Secure and light-weight authentication scheme for SG communication

Any secure framework for SG communications needs to be light-weight so that (i) it does not contribute to high latency [6], and (ii) exchanges as few signal messages with other entities as possible [7]. Also, security headers contribute to increased packet size. Therefore, if we are to devise any authenciation algorithm for the HAN/BAN/NAN GWs, we should envision a light-weight authentication mechanism to keep the message size overhead as low as possible. Towards this end, we focus on the first step of securing communication between the SG entities by providing a light-weight, fast authentication scheme, which we present below.

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 [8] 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 light-weight message authentication scheme is shown in Fig. 2, and the detailed steps are as follows.

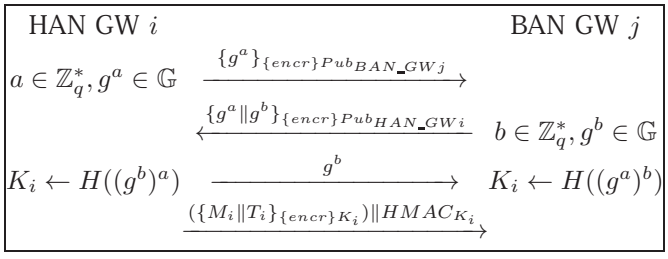

Fig. 2. Proposed message authentication scheme

1. HAN GW i chooses a random number $a \in Z_q^*$, computes g^a, and sends g^a in an encrypted request packet

to BAN GW j.

$$\text{HAN GW}_i \rightarrow \text{BAN GW}_j : \{g^a\}_{\{encr\}Pub_{BAN\_GWj}}$$

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

$$\text{BAN GW}_j \rightarrow \text{HAN GW}_i : \{g^a \| g^b\}_{\{encr\}Pub_{HAN\_GWi}}$$

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 $K_i = H((g^b)^a)$, where $H : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$ is a secure cryptographic hash function, and also 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 also computes the same shared session key $K_i = H((g^a)^b)$.
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.

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

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.

V. Security Analysis

In this section, we will analyze the security of the proposed light-weight 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. Due to these two reasons, the proposed scheme can provide mutual authentication between HAN GW i and BAN GW j.

• *The proposed scheme can also establish a semantic-secure shared key in the mutual authentication environment.* The semantic security of the shared key under the chosen-plaintext attack shows that an adversary $\mathcal{A}$ can't 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 [9]. To cater for these random oracle queries, we maintain an $\mathcal{H}$-list. When a new query $C_i \in \mathbb{G}$ is asked, we choose a fresh random number $Z_i \in \mathbb{G}$, set $\mathcal{H}(C_i) = Z_i$, put (C_i, Z_i) in $\mathcal{H}$-list, and return Z_i to $\mathcal{A}$. At some time, 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 $K_i = H(g^{ab})$, then we have

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

and

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

In addition, since

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

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 challenge with the success probability $1/q_H$ given the event $\mathcal{E}$ occurs. Combining the above probabilities together, we have

$$\mathbf{Succ}^{\text{CDH}} = 1/q_H \cdot \Pr[\mathcal{E}] \geq \frac{\varepsilon}{q_H}$$

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 in the proposed scheme, the mutual authentication environment can't 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 also achieves perfect forward secrecy [8].

• *The proposed scheme can also 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 $(\{M_i \| T_i\}_{\{encr\}K_i}) \| HMAC_{K_i}$ 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 transmission.

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

VI. Evaluation

The proposed message authentication scheme is evaluated by analytical results using MATLAB [10]. For the SG topology, we consider 10 NANs, each having 50 BANs. The number of HANs in each BAN is varied from 10 to 100. The other simulation parameters are listed in Table I. We compare the performance of our proposed authentication mechanism with Elliptic Curve Digital Signature Algorithm (ECDSA). The reason behind this choice is the fact that ECDSA was considered and demonstrated to be a secure authentication protocol for SG demand response communications in [11]. It should be noted that each packet authenticated using our proposed mechanism is encrypted by 128-bit Advanced Encryption Standard (AES). To compare with this, we considered ECDSA-256 in our simulations since its security level is comparable to that of 128-bits cryptography [12].

It is worth noting that only the messages exchanged between HANs and their corresponding BAN are considered for authentication using the proposed scheme and the conventional ECDSA. To make realistic assumptions, we also consider at least 80% of the HANs communicating with their respective BAN at any given time.

Two performance metrics are considered for evaluation, namely communication overhead and message decryption/verification delay. The size of the HAN packet bound for the BAN is assumed to be up to 102 bytes, which is sufficient to contain the users' power requirements and request to the CC. The sizes of the generated MAC in our proposed approach is set to 16 bytes based on RIPEMD-128 algorithm. The reason behind choosing this hash algorithm for creating the MAC is due to its resiliency against collision and preimage attacks. The comparative results are presented in Figs. 3 and 4. Fig. 3 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.

TABLE I
Simulation parameters.

Simulation parameter	Value
BAN GW CPU clock	32MHz
Number of HANs	10-100
HAN message generation interval	10s
TCP header	20 Bytes
Message header	50 Bytes
Raw message	32 Bytes
Hash header	16 bytes
Simulation time	500s

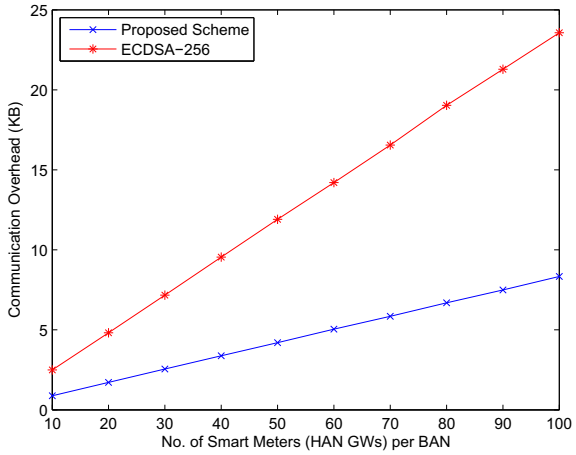

Fig. 3. Average communication overhead experienced by the BAN GW in case of the proposed scheme and the conventional ECDSA protocol for varying number of smart meters (i.e., HAN GWs)

This increase is, however, more significant in case of the conventional ECDSA protocol. For instance, when 100 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 (23 KB) in contrast with a relatively low value (8 KB) 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 method demonstrates higher scalability for larger topologies.

On the other hand, the plot in Fig. 4 shows the 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 protocol. The OpenSSL package was used on a computer running Intel Xeon Processor (E5450) and Linux distribution 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 100 times to fit the 32MHz 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 light-weight authentication process followed by AES encryption, which is faster than the conventional ECDSA protocol which relies on signature verification along with decryption at the BAN for every message coming from each HAN.

Fig. 5 shows the memory usage of the proposed and conventional authentication algorithms over time for varying message volumes received by a given BAN GW. The memory usage consists of two upper bounds, namely the RAM boundary and the RAM plus flash memory boundary that comprise 8Kb and 128Kb, respectively. When the message rate is 15 per second,

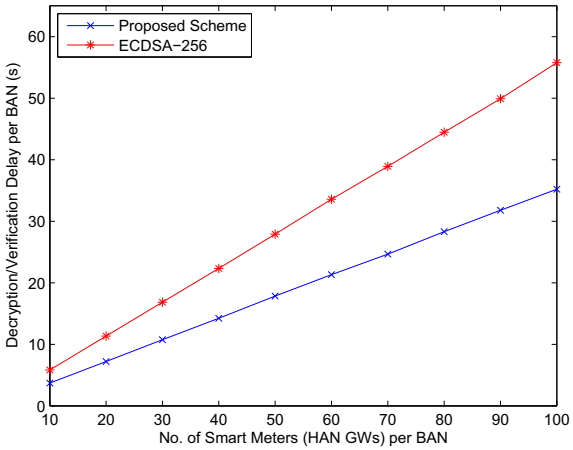

Fig. 4. Average delay at the BAN GW in case of the proposed scheme and the conventional ECDSA scheme for varying number of smart meters (i.e., HAN GWs).

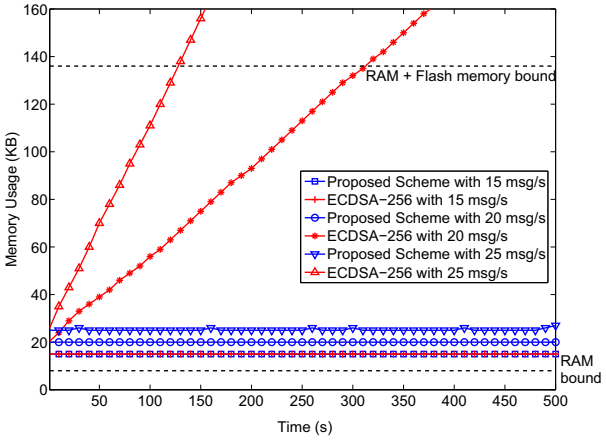

Fig. 5. Memory usage of the proposed and conventional authentication algorithms for different message volumes received by BAN.

the conventional scheme takes about 15KB of memory, which exceeds the allocated RAM in the BAN GW. This means that many messages from the BAN are buffered in the slow flash memory and are accessed later by the RAM. 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. This result indicates that few of the messages are buffered in the slow memory and can be accessed without significant delay in case of both the considered schemes when the BAN GW is receiving 15 messages per second. When the number of messages arriving at the BAN GW increases to 20, 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 300s. In contrast with this, the proposed scheme achieves much lower memory usage (approximately 20KB) and continues to support this throughout the entire course of the simulation (i.e., 500s). However, when the number of apartments in a given building is raised which results in a higher message reception rate of 25 at the BAN GW, the results change even more significantly. Fig. 5 shows that the conventional method, in this case, takes up all the available memory at the BAN GW rather quickly (within 125s of the start of the simulation). On the other hand, the proposed scheme manages to stay below 30Kb of the overall available memory throughout the simulation. This good performance of the proposed scheme can be attributed to the less processing in decrypting and/or verifying the signature of the packets that result in less queueing time in the RAM and the flash memory.

VII. Conclusion

In this paper, we have provided a broad framework of SG communications and designed a light-weight message authentication mechanism tailored for the requirements of SG communications. we have performed security analysis on our proposed mechanism and demonstrated its viability. The performance of the proposed scheme is verified through computer-simulations, which demonstrate that the proposed scheme is feasible to be deployed to the SG.

References

[1] C. W. Gellings, The smart grid: Enabling energy efficiency and demand response. Lilburn, GA: Fairmont Press, 2009.
[2] Available at, "SG drafts", http://sites.google.com/site/ieeep2030tf1sgenergysources/cybersecurity
[3] 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.
[4] G. N. Ericsson, "Cyber Security and Power System Communication-Essential Parts of a Smart Grid Infrastructure", IEEE Trans. Power Delivery, Vol. 25, No. 2, Apr. 2010.
[5] 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.
[6] 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, Maryland, USA, Jan. 2010.
[7] 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, Nos. 1/2, 2008.
[8] D. R. Stingson, Cryptography: Theory and Practice, 3rd ed. Boca Raton, FL: CRC, 2005.
[9] M. Bellare and P. Rogaway, "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols," ACM CCS 1993, pp. 62-73
[10] Mathworks - MATLAB and Simulink for Technical Computing, available at, http://www.mathworks.com/
[11] 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.
[12] 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.