A Hybrid Encryption Scheme for Advanced Metering Infrastructure Networks

Samer Khasawneh and Michel Kadoch
Department of Electrical Engineering, École de Technologie Supérieure, University of Quebec
1100 Rue Notre-Dame O, Montreal, Canada
samer.khasawneh.1@ens.etsmtl.ca, michel.kadoch@etsmtl.ca

Abstract. Smart grid has been recognized as a promising solution to overcome the limitations in functionality and requirements of the legacy power grid. In order to enable positive transition in providing electricity services, two-way communication between different smart grid devices must be activated. Integrating communication will raise many security concerns. Failure in achieving secure communication will annul the smart grid outcomes.
In this research, we exploit hybrid encryption to design a cryptographic scheme for Advanced Metering Infrastructure networks. Elliptic Curve cryptography is known to use shorter key sizes compared to other public key cryptosystems, thereby we utilize Elliptic Curve Encryption for key encapsulation. The proposed scheme is evaluated in terms of computation and communication overhead. Simulation results indicate the validity of the proposed scheme for AMI networks. As of this writing, we are unaware of any efficient hybrid encryption system designed for AMI networks.

Keywords: AMI networks, Hybrid encryption, Elliptic curve, ECIES, Integrity code.

1 Introduction

In spite of providing us with energy for decades, legacy power grid becomes obsolete and no longer able to accommodate the increasing human demand for energy. Therefore, the need for newer and smarter source of energy generation is indispensable. Smart grid is designed to provide reliable, efficient, intelligent and sustainable source of power generation and distribution [1]. The main feature that characterizes the smart grid is the incorporation of two-way energy and information flow between the utility station and the smart meters. The integration of two-way communication into the power grid provides efficient exchange of real-time information and enables near-optimal balance of supply and demand [2]. Demand-response [3], load shedding [4] and peak shaving [5] are examples of smart grid services that highly depend on the incorporation of high-speed and two-way communication technologies.

The legacy power grid is already facing several threats ranging from physical attacks to failures due to the outdated infrastructure. However, as with any new technology, the increased automation has its challenges and threats. Therefore, smart

grid is subject to extra attacks driven from the integration of information communication. Leading among the new smart grid threats are the remote attacks and the compromise that could result from the increasing amount of interconnectivity [6]. Rolling out communication functionality to each customer will definitely change threat dynamic and will pose new challenges and vulnerabilities that have not been faced anywhere else. The nature of the attacks and the attack vectors for smart grid networks are likely to be different from the conventional attacks associated with the enterprise networks. Therefore, as pointed out by Electric Power Research Institute, cyber security is one of the most eminent requirements facing the smart grid development [7].

Advanced Metering Infrastructure (AMI) is an integral part of the smart grid as it comprises smart meters, collectors, controllers and Meter Data Management Systems (MDMSs). AMI relies on different network architectures such as home display, Wide Area Networks (WANs) and utility demilitarized zones (DMZ). According to US Department of Energy, AMI attract the most development and planning attention in the smart grid. The architecture of AMI enables the two way communication between the utility and the smart meters. For this reason, secure communication between the utility and smart meters is considered the key requirement in accomplishing the overall security in smart grid networks. However, the adaption of any security measures in AMI communications requires an efficient, low overhead, scalable, and robust key management system (KMS) that is able to support the very large number of smart meters. The role of KMS in AMI networks is to generate cryptographic keys with suitable length and then use the different communication links available to distribute the keys to the communicating parties.

Due to the unique features of AMI networks, there exist several constraints associated with the development of security measures and key management frameworks for AMI networks. It is important to highlight these issues in order to determine the effectiveness of any proposed solution.

Cope with resource constraints. Smart meters, gateways and concentrators are all equipped with very limited processing and storage capabilities, making it infeasible to adapt cryptographic algorithms that require high computation overhead.

Low bandwidth. Typically, AMI networks have low bandwidth that is able to transfer short messages. Yet, cryptographic algorithms increase the size of every message by adding extra bits. Furthermore, key management system requires continuous exchange of keys-update messages. This will lead to channel contention that will increase data latency.

Delay requirements. Applications in smart grid require real-time communication with minimum delay and latency. Therefore, computation-intensive cryptosystems may result in violating the delay and latency constraints.

Long lifetime. Smart grid infrastructures have long lifespan compared to other system, which might outlast the timeliness of a cryptography algorithm. Thereby, cryptographic techniques must ensure sufficient security level that survive for long time taking into consideration that any upgrade procedures will not maintain power availability.

The limitations aforementioned demonstrate that applying security to smart grid networks is a complex and tangled problem. Fundamental security techniques for enterprise internet and IP networks can hardly been adapted. This is due to the fact

that smart grid communication systems have different nature and objectives regarding what need to be protected in cyber security. Nevertheless, in the past few years, several researches have been proposed in the literature to secure the communication in smart grid networks. The majority of the proposals consider the problem for AMI networks [8-11], yet some of the researches target SCADA systems [12,13]. As we will target securing AMI communication solely, numerous schemes have been already proposed, however few of them can completely satisfy the security goals and requirements for AMI networks. Hence, we propose a security framework that exploits hybrid encryption (HE) with a lightweight key management scheme. In our model, we aim to utilize secret-key and public-key cryptography together, in order to benefit from the strengths of each one of them. In addition, the proposal reduces the overhead of keys distribution, management and update by using randomly generated keys and appending them encrypted to the message.

The rest of the paper is organized as follow. Section 2 provides a brief overview of the related work. Section 3 presents the models and design goals. The proposed hybrid cryptosystem is illustrated in section 4. The performance of the proposed scheme is presented in section 5. Finally, the paper is concluded in Section 6.

2 Related Work

Recently, security in smart grid networks has been an area of considerable research attentions. The three fundamental security goals that the researches have focused on are availability, integrity and confidentiality. Denials of Service (DoS) attacks are mitigated using anti-spoofing and anti-jamming techniques, whereas cryptography is the mechanism used to ensure message integrity and confidentiality. Nian L. et al. [8] presented a centralized key management technique for the different transmission modes in AMI networks. The utility generates symmetric keys, group keys and cryptographic parameters and distributes them to the smart meters through secure channel. The smart meters use the received data to generate session keys. The generated keys are used only once and need to be regenerated before sending or receiving encrypted messages. The proposal provides confidentiality and integrity as the session keys are used to encrypt and digitally sign the messages. Simulation results show that the procedure used in KMS has low computation overhead due to the use of simple bitwise binary operations and hashing functions. KMS has some performance limitations such as the need to perfectly synchronize the network devices and the assumption of fixed key size and meter.

A zero-configuration identity-based signcryption for end-to-end communication in AMI networks is proposed in [9]. The scheme provides encryption and authentication services through asymmetric key cryptography. The scheme has zero-configuration overhead as it generates the public key from information that is derived from sender identity. In the registration phase, a device communicates with a Key Generation Server (KGS) to obtain a private key. The private key is used either to decrypt a received message or to sign a message before transmitting it. In the transmission phase, the sender calculates the public key of the receiver using information derived from receiver identity and encrypt the message using the public key calculated.

An authentication scheme based on Merkle-Tree hashing for Home Area Networks (HANs) is proposed in [10]. The scheme exploits Merkle hashing by constructing a binary tree where the utility is consider the root and smart meters as the leaves. Each smart meter is assigned an ID which is the hash code of a certain cipher. Smart meters are authenticated using their hash codes and the Authentication Path Information (APIs). The smart meter encrypts the information to prevent eavesdropping and transmits it to the gateway. Upon receiving the encrypted electricity report, the gateway checks the report to detect replay attack and to check for any content alternation. The proposal is resilient against analysis attacks, replay attack, message injection attack and message modification attacks. Despite the fact that the scheme is scalable and has low computation overhead, it can sign limited number of messages as it is based on Merkle-Tree hashing.

Authors in [11] proposed a dynamic secret-based encryption scheme for smart grid devices. Sender and receiver synchronously and continuously monitor packets loss and retransmissions in the link layer in order to build a Retransmission Sequence (RS). When the length of the sequence reaches a predefined threshold, it is hashed to obtain Dynamic Encryption Key (DEK). Encryption and decryption is carried out between the utility and the smart meters using DEK. The proposed scheme is lightweight as it uses hashing and binary operations. Although dynamic secret generation is not-scalable, the main limitation of the proposed technique is that it does not provide Integrity and authentication.

3 Models and Design Goals

In this section, we will describe AMI network model, attacks model and the design goals.

3.1 AMI Network Model

We will use the network model shown in Fig 1, where the AMI network has three device types: utility master computer, Neighborhood Area Network (NAN) gateways and Home Area Network (HAN) smart meters. The utility master computer is equipped with very high storage and processing capabilities and could not be compromised. The gateway is responsible for routing the information received from several smart meters to the utility. Smart meters are small devices equipped with limited storage and communication capabilities. These devices are responsible for collecting and reporting information such as energy consumption and energy loss/ restoration to the gateways. As shown in the network model, neighborhood area gateway routes information sourced from multiple smart meters. Encryption and decryption operations could be done at any one of the three devices simultaneously and asynchronously.

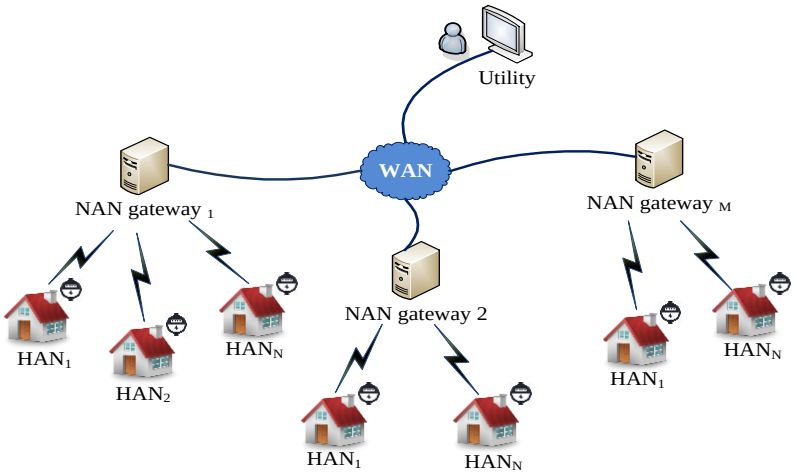

Figure 1: The network model of AMI network

3.2 Threat Model

In this research, we assume that the utility computer could not be compromised in opposite to smart meters and gateways that the adversary may compromise if he has the sufficient power and knowledge. In our threat model, the adversary can issue the following set of attacks:

1. *Passive attacks* (such as eavesdropping, traffic analysis). In such attacks, the adversary captures the traffic generate by the smart meter or gateways with no intention to corrupt the communication. He rather invades the privacy of the power grid users.
2. *Message modification attack*. The attacker alters the data exchange by tampering with or dropping the captured messages.
3. *Message injection attack.* The adversary injects falsified messages in the network to obtain undesirable performance deterioration. .
4. *Reply attack.* The attacker maliciously retransmits previous messages to gateways or smart meters. Obviously, replay attack can occur even if the exchanged messages are encrypted or digitally singed.

3.3 Design Goals

The proposed hybrid encryption scheme has the following objectives:

1. Building a lightweight key management scheme to reduce the overhead of key generation, distribution and renewal to cope with AMI constraints.
2. The proposed scheme is being designed to achieve high efficiency by combining the strength of public key cryptography with the computation speed of private key cryptography.
3. The proposed scheme should be resilient against the attacks discussed in the threat model.

4 The Proposed Hybrid Encryption Scheme

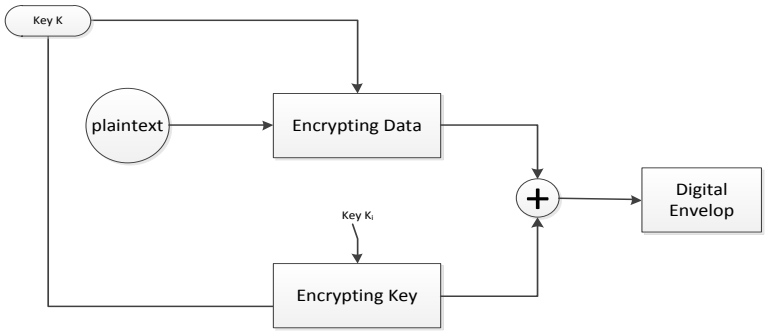

Figure 2: Hybrid cryptosystem structure

Hybrid Cryptosystems (HC) combines the strength of public key cryptography with the efficiency of symmetric encryption. HC is composed of two subsystems namely: data encapsulation and key encapsulation systems as shown in Fig 2. Data encapsulation system is a symmetric key cryptosystem, where the plaintext is encrypted using an arbitrary cryptographic key using one of the symmetric encryption algorithms. On the other hand, key encapsulation system is a public key cryptosystem that is used to encrypt the previously used arbitrary key using one of the secure asymmetric encryption algorithms. The result of both encapsulation systems are merged together to obtain what is called "digital envelop". The resulted cryptosystem will inherit the efficiency of the symmetric algorithms with the security of the public key cryptography.

In our scheme, we will use Advance Encryption standard (AES) for the data encapsulation cryptosystem and Elliptic Curve Encryption (ECE) for the key encapsulation cryptosystem. AES is the algorithm that is used in most of US federal government organization, has different key sizes, secure block size and known to be efficient in hardware and software. Elliptic curve encryption is used instead the well-known RSA cryptosystem because it appears to offer equal security with smaller key size. However, several approaches to encryption/decryption using elliptic curves have been analyzed in the literature. However, we will employ Elliptic Curve Integrated Encryption Scheme (ECIES) cryptosystem that is part of the ANSI X9.63 standard [14]. Compared to another elliptic curve schemes, ECIES has small communication overhead, do not require point mapping and implement authentication code.

4.1 Initialization

Whenever a new smart meter (SM) joins the network, it initiates an initialization procedure with the corresponding gateway (GW) to generate public/private keys that will be used by Key Derivation Function (KDF) to derive ECIES keys. SM and GW generate pair of keys: private and public. The generated keys are used to derive a shared session key based on Diffie-Hellman algorithm. In our model, we assume that the gateway is able to verify the legitimacy of the new smart meter SM by checking its

identification (ID). Therefore, the smart meter sends it's ID ciphered using the shared secret K_{SS} to the gateway, which stores the ID of valid smart meters.

Payload	Synch	Clock Tolerance($\boldsymbol{\theta}$)	key	MIC

Figure 3: The message format of the proposed hybrid cryptosystem

4.2 Message Format

The messages that will be exchanged using proposed protocol must have the format shown in Fig 3. Synch and clock tolerance fields are used to prevent against reply attack. Synch stores the message timestamp corresponding to the message creation time, whereas the clock tolerance indicates for how long (in milliseconds) the message still good. The choice of clock tolerance value depends on many factors such as computation speed, network bandwidth and network congestion status. Hybrid cryptosystems encrypts the key used to encrypt the message and appends it to the message. The encrypted key is stored in key field. The size of this field depends on: the original key size and the public key algorithm used to encrypt the key. Message Integrity Code (MIC) is used to protect message integrity and authenticity. Shaded fields represent encrypted content.

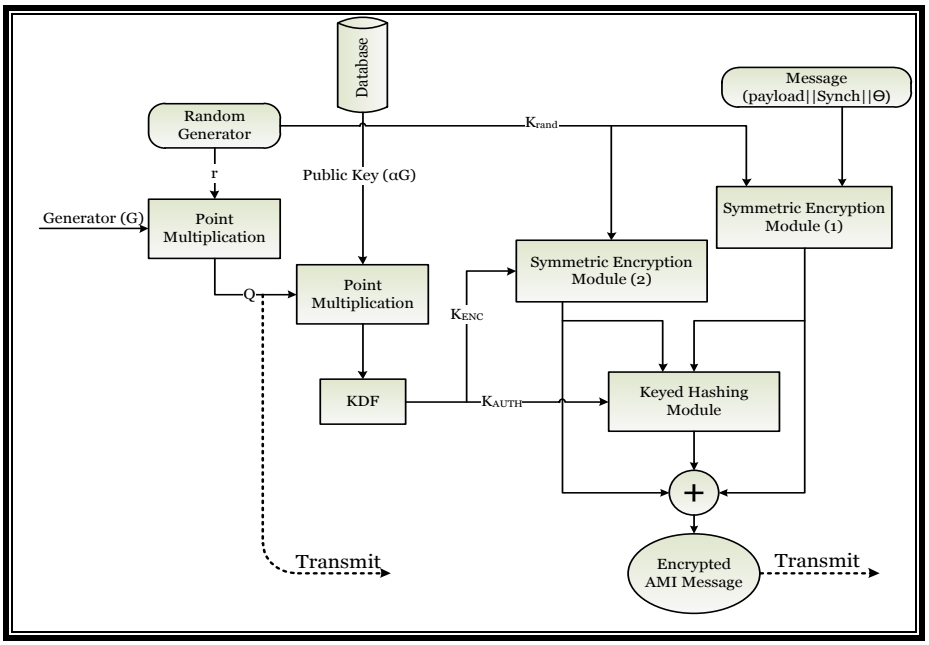

Figure 4: Secure AMI Message Construction

4.3 The Proposed Hybrid Cryptosystem in Details

The process of constructing an encrypted message complying with the format discussed in the previous section is depicted in Fig 4. The smart meter prepares the consumption report (payload) and appends the appropriate timestamp (synch) and clock tolerance (Θ). It encrypts the data using a randomly generated key in symmetric encryption module (1). KDF and two point multiplication units are used to derive keys K_{ENC} and K_{AUTH}. The random key is encrypted in symmetric encryption module (2) using K_{ENC}. Integrity code is generated in hashing module (such as HMAC) keyed by key K_{AUTH}. The smart meter will transmit the composed AMI message along with point Q to the gateway. It is important to include Q in the transmission to enable the receiving gateway to use his private key to compute keys K_{ENC} and K_{AUTH}. Upon receiving AMI message, the gateway will process it as shown in algorithm 1. 5

5 Performance Analysis

Here, we assess the performance of the proposed hybrid cryptosystem (HC) in terms of computation, communication and storage overhead. The performance of HC is compared with RSA algorithm. We implemented the proposed scheme in software with the simulation parameters shown in Table 1.

Table 1: Simulation parameters

Processor Speed	2.4 GHz
Memory Capacity	4 GB
Operating system	Linux Mint 13.0 mate
KDF	SHA-256
MIC	HMAC-128
Symmetric Encryption Module (1,2)	AES128
Message Size	32Kbyte
Number of smart meters	Variable
Number of gateways	1

5.1 Computation Overhead

Computation overhead is the time required to prepare the ciphertext in the format that will be transmitted in the network. The computation overhead of HC is determined by the time required to perform: key generation, AES, point multiplication, KDF and MIC algorithm. In the proposed HC, encryption involves two elliptic curve point multiplications and decryption does not require random key generation, therefore decryption is faster. Fig 5 shows the computation cost of the neighborhood gateway when the proposed scheme is implemented to support different number of smart meters. It's evident that the proposed HC with the two elliptic curve variations

SECP112r1 and SECP224K1 requires much smaller computation time compared to 1024 bits RSA. This is due to the implementation of symmetric key algorithm and lightweight hashing functions.

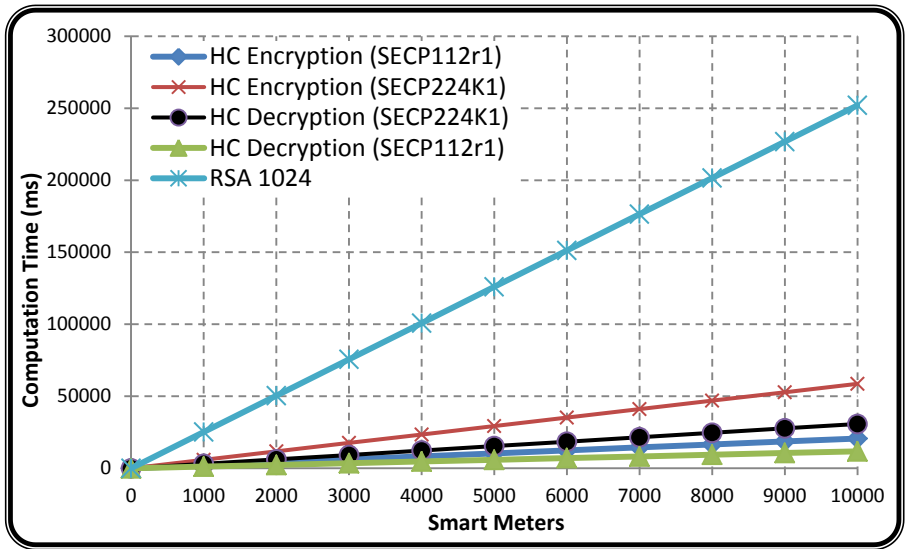

Figure 5: The computation overhead of the proposed hybrid cryptosystem

5.2 Communication Overhead

Communication overhead is measured by the amount of extra bits added to the message in order to secure it. Due to the fact that AMI networks have limited bandwidth, cryptographic schemes should consider minimizing the communication overhead a priority. According to the simulation parameters presented previously, the proposed hybrid cryptosystem adds 256 bits to each message in addition to the elliptic curve point Q. The size of Q depends on the elliptic curve (several variations are found in [15]). Fig 6 shows the communication overhead of the proposed scheme implemented based on SECP112r1 and SECP224K1 for AMI network with variable number of smart meters. HC adds considerably less amount of bits per message compared to RSA that adds a minimum of 1K bit.

5.3 The Hybrid Cryptosystem: Security Analysis

In the proposed HC, the communicated messages are transmitted encrypted, thereby an attacker that manages to collect messages from the network will not be able to read the content of the message or gather any useful information regarding the sender of the message. As a result, *passive attacks* are prevented and customer *privacy* is preserved. The proposal resists *message modification attack* by attaching

message integrity code to every message. The receiver of the message validates the received MIC and detects tampering if the received MIC is found different from the received one.

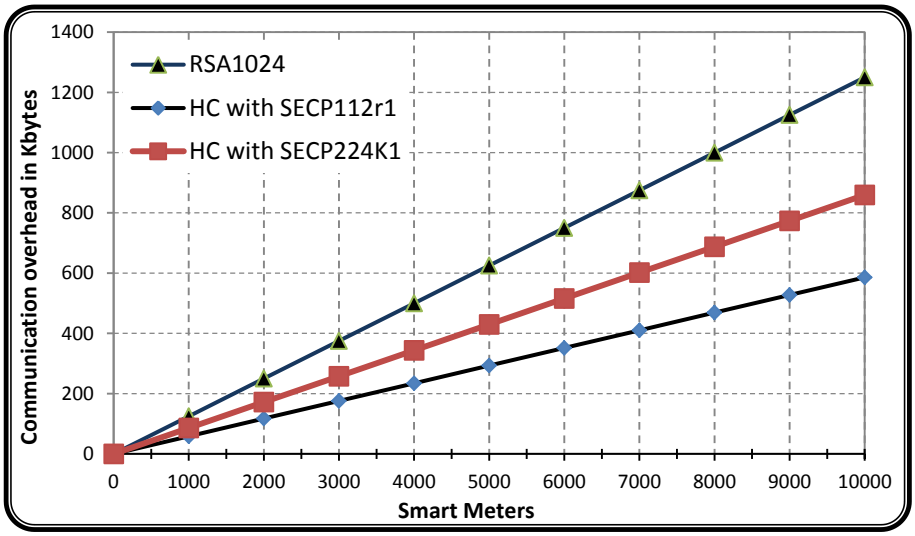

Figure 6: HC communication overhead for different number of smart meters

During the initialization phase, the identity of the smart meter is verified by the gateway. Therefore, smart meters that manage to share the elliptic curve parameters with a gateway are considered authentic. As, MIC is generated using a keyed hashed function that uses K_{SS}; verifying MIC of a message indicates that the message is originated from a legitimate source. Consequently, ensuring message integrity and authenticity can resist *false data injection attack*.

The proposed scheme is designed to prevent *reply attack* by adding timestamp (synch) and clock tolerance. Checking synch and Θ will determine if the message is obsolete (replayed) and should be ignored.

In summary, the proposed protocol can ensure message integrity, confidentiality and authenticity. Furthermore, the proposal can resist false data inject and reply attacks.

6 Conclusion

AMI networks are vulnerable to various threats that may disrupt the operation of the smart grid; therefore secure communication in AMI networks is indispensable. Hybrid encryption can achieve the security of public key cryptography with the convenience of secret key cryptography. In this research, we propose a hybrid encryption system that is designed to secure the communication between the different devices of AMI networks. The proposal combines symmetric key cryptography,

ECIES and authentication codes to generate secure messages. Thoughtful performance analysis proves the validity of the proposed scheme.

References

1. Wang, W., Xu, Y., Khanna, M.: A survey on the communication architectures in smart grid. Computer Networks. 55:3604–3629, 2011.
2. Fangxing, L., Wei, Q., Hongbin, S., Hui, W., Jianhui, W., Yan, X., Zhao, X., Pei, Z.: Smart transmission grid: Vision and framework. IEEE Transactions on Smart Grid , vol. 1, no. 2, pp. 168–177, 2010.
3. Strengers, Y.: Smart metering demand management programs: challenging the comfort and cleanliness habitus of households. Proceedings of the 20th Australasian Conference on Computer-Human Interaction: Designing for Habitus and Habitat, December 08-12, 2008, Cairns, Australia.
4. Kok, K., Karnouskos, S., Nestle, D., Dimeas, A., Weidlich, A., Warmer, C., Strauss, P., Buchholz, B., Drenkard, S., Hatziargyriou, N., Lioliou, V.: Smart Houses for a Smart Grid. CIRED 20th International Conference on Electricity Distribution, June 2009, Prague.
5. Komninos, N., Philippou, E., Pitsillides, A.: Survey in smart grid and smart home security: Issues, challenges and countermeasures. Communications Surveys and Tutorials, IEEE , vol.PP, no.99, pp.1,1
6. Sorebo, G.N., EcholsM.C: Smart Grid Security: An End-to-End View of Security in the New Electrical Grid. Taylor&Francis, New York (2012)
7. Electric Power Research Institute: Report to NIST on smart grid interoperability standards roadmap. 2009.
8. Liu, N., Chen, J., Zhu, L., Zhang, J., He, Y.: A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid. IEEE Transactions on Industrial Electronics, vol. 60, no. 10, pp. 4746-4756, Oct. 2013.
9. So, HKH., So., Kwok, S.H.M., Lam, E.Y., Lui, K-S.: Zero-configuration identity-based signcryption schemefor smart grid. IEEE International Conference on Smart Grid Communications, Oct. 2010.
10. Li, H., Lu, R., Zhou, L., Yang, B., Shen, X.: An efficient merkle-tree-based authentication scheme for smart grid. IEEE Systems Journal 8.2 (2014): 655-663.
11. Liu, T., Liu, Y., Mao, Y., Sun, Y., Guan, X.: A dynamic secret-based encryption scheme for smart grid wireless communication. IEEE Transactions on Smart Grid 5.3 (2014): 1175-1182.
12. Bartman, T., Carson, K.: Securing Communications for SCADA and Critical Industrial Systems. Proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2015.
13. Taylor, C.R., Shue, C.A., Paul, N.R.: A Deployable SCADA Authentication Technique for Modern Power Grids. In Proceedings of the IEEE International Energy Conference, Dubrovnik, Croatia, 13–16 May 2014; pp. 696–702.
14. ANSI Standards Committee X9, Public key cryptography for the financial services industry: Key agreement and key transport using elliptic curve cryptography, ANSI X9.63-2001
15. SEC 2: Recommended Elliptic Curve Domain Parameters, Certicom Research, September 20, 2000.