A Dynamic Secret-Based Encryption Scheme for Smart Grid Wireless Communication

Ting Liu, *Member, IEEE*, Yang Liu, Yashan Mao, Yao Sun, Xiaohong Guan, *Fellow, IEEE*, Weibo Gong, *Fellow, IEEE*, and Sheng Xiao

***Abstract*—Integrating information network into power system is the key for realizing the vision of smart grid, but also introduces many security problems. Wireless communication offers the benefits of low cost, rapid deployment, shared communication medium, and mobility; at the same time, it causes many security and privacy challenges. In this paper, the concept of dynamic secret is applied to design an encryption scheme for smart grid wireless communication. Between two parties of communication, the previous packets are coded as retransmission sequence, where retransmitted packet is marked as "1" and the other is marked as "0." During the communication, the retransmission sequence is generated at both sides to update the dynamic encryption key. Any missing or misjudging in retransmission sequence would prevent the adversary from achieving the keys. In our experiments, a smart grid platform is built, employing the ZigBee protocol for wireless communication. And a dynamic secret-based encryption demo system is designed based on this platform. The experiment results show that the retransmission and packet loss in ZigBee communication are inevitable and unpredictable, and it is impossible for the adversary to track the updating of the dynamic encryption key.**

***Index Terms*—Dynamic secret-based encryption, retransmission, security, smart grid, wireless communication, ZigBee.**

I. Introduction

RAPID increase in electric power demand, renewable energy mandates, and a push towards electrification in the transportation sector is expected to increase power system stresses and disturbances [1]. In the United States, 31 states have established the Energy Efficiency Resource Standards and Goals which target 30% energy savings by 2020; 30 states have launched the Renewable Portfolio Standards and Goals which require the renewable energy occupy 15% by 2020 in CA, 50% by 2025 in AK [2]. The smart grid (SG) is considered as a desirable infrastructure for energy efficient consumption and transmission, where the built-in information networks support two-way energy and information flow, facilitate significant penetration of renewable energy sources into the grid, and empower consumer with tools for optimized energy consumption [3], [4].

Since the advent of the smart grid concept, security has always been a primary concern. Pricing information and control actions are transmitted via the information network. Various attacks such as eavesdropping, information tampering, and malicious control command injection that have almost ruined the Internet, would impose serious threat on secure and stable smart grids operation. Moreover, SG is an attractive target for various hackers with diversified motivations, e.g. unethical customers may want to modify their meter readings to evade the electric charge; malicious users are able to extract the behaviors of household by eavesdropping the communications of smart meters (called non-intrusive appliance load monitoring); vicious terrorists want to inject the false data or command to disrupt the grid [5]–[7]. The U.S. National Institute of Standards and Technology lays out the guidelines for developers and policy makers, covering cyber security requirements of the smart grids that should be included from the beginning of the development process [8]. In Cisco Smart Grid Framework, security concern plays the role across all functional components [9].

Various communication technologies are applied to meet the specific requirements for power system generation, transmission, distribution, and consumption. In the power grids, dedicated wired networks such as optical cables are usually built to ensure the robustness and security. Wireless technology is the indispensable part of SG communication for distribution grids that connect directly to customers because: 1) in home area network, it is too expensive to build wired networks to monitor various devices with different interfaces; 2) when hundreds of parameters in the grid need to be monitored, wired network can result in a costly and complicated system architecture [10]. However, wireless network is regarded as the Achilles' heel of SG security, which is inherently vulnerable to several attacks, such as eavesdropping and identity forging since various users communicate through the shared medium of air.

Manuscript received September 22, 2012; revised February 14, 2013; accepted May 07, 2013. This project is supported in parts by a gift fund from the Cisco University Research Program, National Natural Science Foundation of China (91118005, 91218301, 61221063, 61203174), U.S. Army Research Office (20110201120010), U.S. Army Research Office, the United States National Science Foundation grants EFRI-0735974, CNS-1065133 and CNS-1239102, the U.S. Army Research Office contract W911NF-08-1-0233, and the University of Massachusetts CVIP Technology Award Fund. Paper no. TSG-00618-2012.

T. Liu, Y. Liu, and Y. Mao are with the Ministry of Education Key Lab for Intelligent Networks and Network Security (MOE KLINNS), School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: tliu@sei.xjtu.edu.cn; yliu@sei.xjtu.edu.cn; ysmao@sei.xjtu.edu.cn).

Y. Sun is with the Department of Electrical and Computer Engineering, University of Toronto, ON M1S 7UB, Canada (e-mail: sunyao.sun@mail.utoronto.ca).

X. Guan is with Ministry of Education Key Lab for Intelligent Networks and Network Security (MOE KLINNS), School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China, and also with Center for Intelligent and Networked Systems, TNLIST, Tsinghua University, Beijing 100084, China (e-mail: xhguan@sei.xjtu.edu.cn).

W. Gong is with the Department of Electrical and Computer Engineering, University of Massachusetts, Amherst, MA 01003 USA, and also with Center for Intelligent and Networked Systems, TNLIST, Tsinghua University, Beijing 100084, China (e-mail: gong@ecs.umass.edu).

S. Xiao is with the Department of Electrical and Computer Engineering, University of Massachusetts, Amherst, MA 01003 USA (e-mail: shengxiao2006@gmail.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2013.2264537

The standard security techniques in information networks, such as dedicated network or channel, intrusion detection systems (IDS) [11], [12], third-party authentication and cryptography [13], [14], etc., may not be applicable for SG wireless communication because of the following limitations.

- *Low-cost*: The cost is the first priority of the users and suppliers. In order to be cost effective, the computational power, memory and storage of the smart devices are limited. It leads to severe restriction on modern security techniques, such as: 1) complicated cryptographic algorithms may exhaust all computation and storage resource of units; 2) third party applications, such as private key generator [14], may visibly increase the cost of whole wireless system.
- *Low-bandwidth*: The communication channels in lower distribution and consumption grids are designed to transmit short message, and require only low bandwidth. Integrity protection mechanisms such as cipher-based message authentication code (CMAC) add typically 64 to 96 bits to every message. This leads to a high overhead in such a channel and might cause latency which is not affordable in many applications in SG [5]. Distributed IDS [15] can detect and classify malicious data and possible attacks by monitoring the communication traffics on many modules with doubled traffic flows, but might exhaust the bandwidth on these modules.
- *Easy-maintenance*: The wireless networks in SG should be flexible and easy to manage. It would be unrealistic to hire hundreds of engineers to manage users' encryption keys and change battery. Xia and Wang present that applying public key infrastructure (PKI) to SG requires significant work and maintenance of the public key management. A utility with 5.5 million smart meters, it requires 500 staff members who can manage approximately 1000 X.509 certificates [16], [17]. A sensor with 600 mAh battery will not last for more than 180 days, if its power requirement is 25 mA on active mode and 100 μA on sleep mode, and it stays in the active mode for 1 s and operates after every 10 min [1].

Under these constraints, we believe the ideal security method for SG wireless communication should satisfy: 1) applying simple algorithms that can be implemented with limited computational power, memory and storage, 2) few or none additional communication burden, 3) self-organizing, self-management and being independent of any third-party. Moreover, it is desirable to integrate with the common protocols with few modifications, and support existing applications seamlessly.

In this paper, based on the dynamic secrets proposed in [18], [19], we design an encryption scheme for SG wireless communication, named as dynamic secret-based encryption (DSE). The basic idea of dynamic secrets is to generate a series of secrets from inevitable transmission errors and other random factors in wireless communications [19]. In DSE, the previous packets are coded as "1" or "0" according to whether they are retransmitted due to channel error. This 0/1 sequence is called as retransmission sequence (RS) which is applied to generate dynamic secret (DS). Dynamic encryption key (DEK) is updated by XOR the previous DEK with current DS.

A SG platform is built to demonstrate and analyze various attacks on SG wireless communication. In this platform, the SIEMENS Smart Meter (PAC 4200) is applied to monitor the power grid, and several Windows workstations simulate the control center and attackers, and the ZigBee module (CC2430-F128 demo board) is applied to build the wireless communication network. An attack is simulated to reveal the risk on information leaking and forging.

A DSE demo system is developed on the SG platform. As shown in the experiments, it is inevitable for the adversary to miss few packets when he monitors the communication between the smart meter and control center. These inevitable and unpredictable errors will prevent the hacker from tracking the secrets. In addition, the DSE is a light encryption method, which only requires several simple operations, such as Hash and XOR, and can support various applications and integrate with most wireless techniques. The DSE key is dynamically generated during the normal communication without additional traffic and control command.

The remainder of this paper is organized as follows. In Section II, many cryptography methods for SG are reviewed. In Section III, the dynamic secrets method and the DSE scheme are introduced. The attack cases in smart grids are demonstrated in Section IV. The experiments and analysis of DSE scheme are analyzed in Section V. Section VI concludes this paper

II. Related Work

Cryptography plays a significant role in improving the integrity and confidentiality of the data in SG. Many existing standard encryption algorithms and authentication schemes are adopted in SG.

Symmetric cryptographies, such as DES (Data Encryption Standard), Triple DES, AES (Advanced Encryption Standard), are widely employed in SG to efficiently defend against possible threats. For example, ZigBee employs 128-bit AES encryption for security. Compared with the asymmetric cipher, symmetric cipher handles large amounts of data more efficiently, but often has a shorter lifespan [20]. It is recommended to change the symmetric cipher periodically. However, it becomes an importance challenge in SG, because there are millions of wide-spread entities [21].

The asymmetric encryption is also applied to meet their specific requirements. Nguyen and Rong employ the identity-based cryptography to secure ZigBee communication. The sender uses the receiver's identification as the public key to encrypt the message; the receiver obtains the corresponding private key from the private key generator to decrypt the message [14]. Li *et al.* present a secure information aggregation approach for smart grids. When the smart meters submit their own data and forward other's data, the homomorphic encryption is employed to ensure that intermediate results are not revealed to any device en route [22]. As they mentioned "asymmetric encryption is more computationally expensive than symmetric encryption," the cost of device and power consumption should be considered in cryptography design.

The management of the encryption key is a challenging and necessary issue in utilizing cryptographic algorithms for the

smart grid. PKI is considered as the basis of most effective key management solution in smart grid [23]. Wu and Zhou propose a new key management scheme for smart grid, combining the public key and symmetric key. The elliptic curve cryptography is applied as public key to securely establish the symmetric keys for the agents to communicate; the Needham-Schroeder authentication protocol is employed as symmetric key [24]. Xia and Wang propose a secure key distribution protocol for smart grid. A trust anchor which is set up in the third party environment, can work as a Lightweight Directory Access Protocol (LDAP) server. They show their method is secure against impersonation attack, replay attack, man-in-the-middle attack and so forth [16]. Kim and Choi introduce an efficient and scalable key management protocol for secure unicast, multicast, and broadcast communications in smart grids, based on a binary tree to manage secret keys shared among entities [21]. All of these methods rely on a third party for identity authentication or key generation. It might cause additional equipment cost and communication traffic.

Many researchers focus on the special characteristics of the smart grid systems and propose lots of novel methods. Focus on the privacy aspect of smart metering data, Efthymiou and Kalogridis propose a solution for anonymizing high-frequency metering data which need to be transmitted to the control center often enough but doesn't need to be attributable, by employing a pseudonymous ID without compromising the operations of the utility and/or distribution network [6]. To protect the home area network (HAN), Yan *et al.* propose a secure data aggregation and dispatch scheme. The orthogonal chip code is employed to keep the confidentiality and anonymity for collecting the reading-data of smart home devices to the household smart meter and for distributing the control message [25]. To improve the efficiency and security of advanced metering infrastructure (AMI), Li *et al.* propose a new wireless communication scheme. The measurements are transmitted only when there is a significant change in the power consumption to improve the spectrum efficiency. And the artificial spoofing packets are sent to prevent the attackers from analyzing user behaviors by monitoring communication traffic [26]. A lightweight message authentication scheme is proposed by Fouda *et al.*. The Diffie-Hellman exchange protocol is applied to achieve mutual authentication and establish the shared session key between the smart meters; the hash-based authentication is used to authenticate the subsequent messages [13]. To secure the information aggregation in SG, Lu *et al.* proposed an efficient and privacy-preserving aggregation scheme, using a super-increasing sequence to structure multi-dimensional data and encrypt the structured data by the homomorphic Paillier cryptosystem technique [27].

III. Methodology

Dynamic secret was firstly proposed by Xiao and Gong for securing wireless communication. The basic idea of dynamic secret is that the legitimate users dynamically generate a shared symmetric secret key utilizing the inevitable transmission errors and other random factors in wireless communication [18], [19]. In present work, the dynamic secret is employed to design the DSE scheme for smart grids wireless communication. In this session, we firstly introduce the basic algorithms of dynamic secret; and then present the DSE scheme.

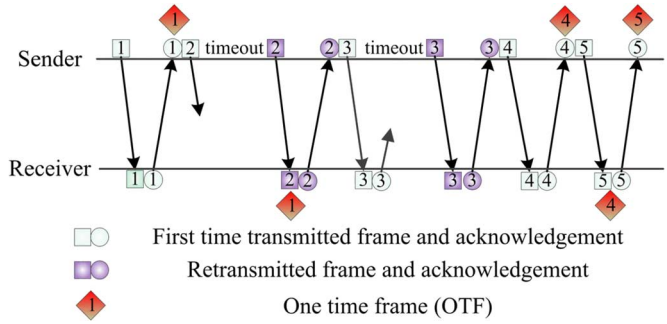

Fig. 1. SW protocol and OTF identification (reproduced from [19]).

A. Dynamic Secret

The sender and receiver monitor the error retransmission in link layer to synchronously select a group of frames. These frames are hashed into dynamic secret to encrypt the data. This part is a brief introduction of dynamic secret from [19].

1) Retransmission Analysis/OTF Set Generation: On the link layer's communication, error retransmission happens unavoidable and randomly at both side of the sender and the receiver. According to Stop-and-Wait (SW) protocol, the sender transmits a frame and waits for the corresponding acknowledgement before sending a new frame. If a frame is only transmitted once and its acknowledgement frame is received in time, this frame is named as one time frame (OTF). As shown in Fig. 1, the packet 1 is confirmed as an OTF on the sender until the acknowledgement of packet 1 is received; it is confirmed on the receiver until the second packet is received. It will be added into OTF set Ψ. Both the transmitted frame (packet 2) and acknowledgement (packet 3) are retransmitted, thus they are not added into OTF set.

2) Dynamic Secret Generation: Once the number of OTF set Ψ reaches the threshold, the sender and receiver agree on a uniformly random choice of universal-2 hash functions to compress Ψ into the dynamic secret $DS(k)$. Then, the Ψ is reset to empty. It is proved that $DS(k)$ will fully retain the adversary's information loss.

3) Encryption/Decryption: When a new dynamic secret is generated, it will be applied to update the encryption key at both sides of communication. This symmetric encryption key is used to encrypt the data at sender and decrypt the cipher at receiver. To reduce the computation consumption, the XOR function is used for encryption and decryption.

B. DSE Scheme for SG Wireless Communication

Dynamic secret-based encryption (DSE) scheme is designed to secure the wireless communication between the smart devices and control center. The framework of DSE scheme is shown in Fig. 2, consisting of retransmission sequence generation (RSG), DS generation (DSG), and encrypt/decrypt.

1) RSG: This module is applied to monitor the link layer error retransmission. The communication packets which have been retransmitted are marked as "1" and the non-retransmitted

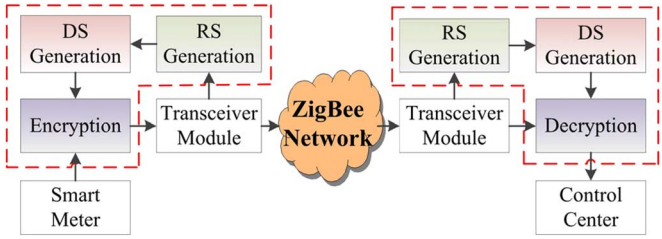

Fig. 2. Framework of DSE scheme.

packets are marked as "0." The pervious packets are coded as 0/1 sequence φ, named as retransmission sequence (RS).

In DSE, RS is applied to replace the OTF set for dynamic secret generation due to the limitation of computation capability and storage resources. The comparisons between the RS and OTF set are shown in Section V.

2) DSG: Once φ reaches the threshold L_RS (length of RS), it would be compressed to a DS in DSG module. Considering the limitation on computation power, the hash functions f_{hash} are recommended in DSG module.

$$DS(k) = f_{HASH}(\varphi_{L\_RS}) \tag{1}$$

3) Encrypt/Decrypt: The new dynamic secret $DS(k)$ is applied to update the dynamic encryption key (DEK) by

$$DEK(k) = DS(k) \oplus DEK(k-1) \tag{2}$$

$DEK(k)$ is generated at both sides of communication synchronously. The sender applies it to encrypt the $Data$, and the receiver applies it to decrypt the $Cipher$. XOR function, as one of the most light-weight and easy-implementation algorithm, is applied to update the DEK and encrypt/decrypt the data on both sides. If DEK is shorter than the data, $DEK(k)$ is replicated and padded circularly to generate $DEK^*(k)$ whose length is equal to the raw data or cipher text.

$$\begin{aligned} Data \oplus DEK^*(k) &= Cipher \\ Cipher \oplus DEK^*(k) &= Data \end{aligned} \tag{3}$$

DSE scheme is an appropriate solution for securing SG wireless communication. It can prevent eavesdropping and forging by utilizing the inevitable errors in wireless communication; can reduce the cost on computation and storage by applying the simple algorithms; can self-organize and self-manage.

IV. Attack Case in Smart Grids

A micro smart grid platform is constructed in our lab to investigate how the attacker intercepts the communication of smart meter and injects bad data into smart meter.

A. Micro Smart Grid Platform

As shown in Fig. 3, a micro smart grid platform is established, consisting of three sides: Smart Terminal (ST), Control Center (CC), and Adversary. ZigBee is applied to build wireless network in the platform. IEEE 802.15.4 standard defines

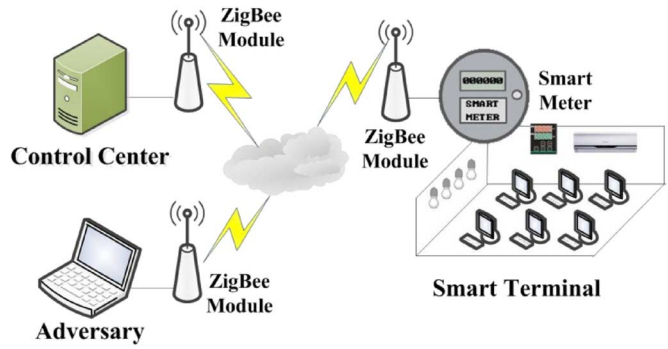

Fig. 3. Experiment platform.

the physical and MAC layers of ZigBee, while the ZigBee Alliance defines the network and application layers. Since it is designed as a low cost, low rate, low power and low complexity personal area network, ZigBee is considered as an ideal protocol for smart grid applications, such as real-time system monitoring, load control, and building management [28], [29]. In this platform, CC2430-F128 demo board is applied to design the ZigBee Module for wireless communication. CC2430-F128 chip is a system-on-chip solution specifically tailored for IEEE 802.15.4 and ZigBee applications.

On the ST, several smart meters (SIEMENS SERTRON PAC4200) are applied to monitor a micro power grid including various electronic devices. SIEMENS SERTRON PAC4200 is a power monitoring device for displaying, storing, and monitoring all relevant system parameters, such as voltages, currents *et al.*. In present experiments, 12 parameters: voltage, current, active power, and apparent power on three-phase, are selected to monitor and report.

Several computers are deployed as the CC and Adversary. On the CC, the ZigBee module is set as normal mode to communicate with ST. On the Adversary, it is set as promiscuous mode to eavesdrop the communication between the ST and CC.

B. Smart Grid Attack Cases

Most terminal devices in smart grid are connected into intranet, such as smart sensors and intelligent applications. It is believed that the malicious users could not access them without the intranet and mac address of these devices. In our experiments, the Adversary obtains the address of the smart meter by monitoring their communication and then injects the false data into the meter.

As shown in Fig. 4, the Adversary can capture the packet sent from ST. The application protocol is Modbus which is widely used to connect the supervisory computer with the remote terminal unit in industrial network, such as supervisory control and data acquisition (SCADA) systems. The header of the packet shows that: the address of ZigBee module on Smart Meter is "12 FF FF FF FF FF FF FF" (64-bit extended IEEE address [29]), and the short address of coordinator on control center is "00 00" (16-bit short address [29]). Moreover, the measurement can be decoded from the data part of the packet, e.g. the current voltage on phase A is 231.9385 V.

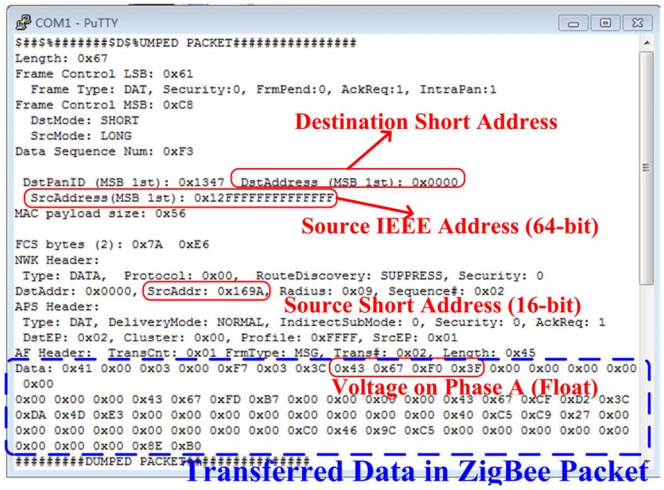

Fig. 4. Information leaking.

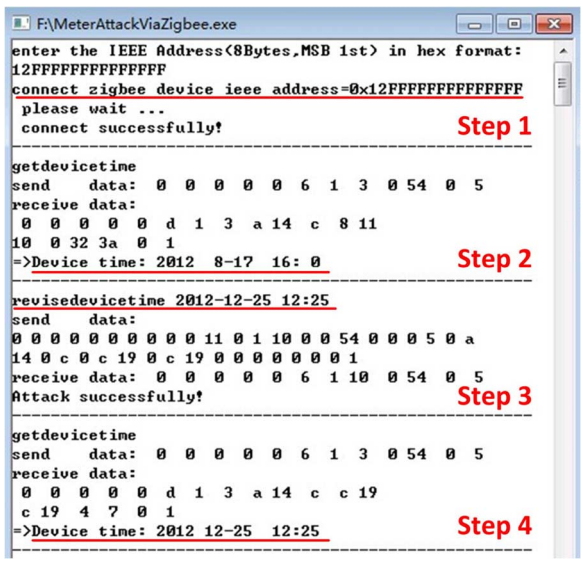

Fig. 5. False data injection.

Using the captured address, attacker can access the smart meter and inject false data. As shown in Fig. 5, an attack application is developed to modify the data of smart meter.

Step 1: Access the smart meter with the address of ZigBee module on smart meter.

Step 2: Read the current time on device. The current time on device is 2012-08-17 16:00.

Step 3: Manipulate the device time to 2012-12-25 12:25.

Step 4: Read the current time on device again. The readings show that our attack is successful.

V. Experiments and Analysis

In this section, numerous experiments are conducted to analyze the security of DSE. Firstly, RS on the CC and Adversary are listed to show the difference between them. Then, retransmitted packet ratio (*RPR*), packet loss ratio (*PLR*) and length of RS (L_RS) are investigated to guide the design of DSE. Finally, a DSE demo system is developed to demonstrate the detailed process of DSE scheme.

TABLE I
Sequence Number of Retransmitted Packets

CC & ST *Received: 5000 Retransmitted: 89*	**18,80,142,204,267**,329,392,454,516,578,640,702,765,827,889,951,1014,1076,1078,1139,1201,1263,1326,1388,1451,1513,1576,1638,1660,1701,1763,1806,1825,1837,1887,1950,2012,2070,2074,2137,2199,2262,2324,2387,2449,2512,2574,2637,2699,2761,2823,2865,2884,2947,3009,3072,3134,3141,3197,3259,3322,3384,3447,3509,3572,3589,**3634,3697,3759**,3821,3884,3945,4008,4050,4069,4132,4194,4257,4319,4382,4444,4507,4569,4632,4695,4757,4820,4881,4944
Adversary *Received: 4987 Retransmitted: 88*	**18,80,142,204,266**,327,388,449,511,573,635,697,760,822,884,946,1009,1071,1073,1134,1195,1257,1320,1382,1444,1506,1569,1631,1653,1694,1756,1799,1818,1830,1880,1943,2004,2062,2066,2129,2191,2254,2316,2379,2441,2504,2566,2629,2691,2753,2815,2857,2876,2939,3001,3064,3126,3133,3189,3251,3314,3376,3439,3501,3564,3581,**3626,3750**,3812,3875,3936,3998,4040,4059,4122,4184,4247,4309,4372,4434,4497,4559,4622,4684,4746,4808,4869,4932

A. Retransmission Sequence

A three-party experiment is conducted to show the RS generated on the CC and Adversary. 5000 packets are sent from the ST with 1 packet per second. The sequence numbers of all retransmitted packets are listed in Table I. According to the SW protocol, the Control Center and Smart Terminal obtain the same RS in which there are 89 retransmitted packets in 5000 packets. The Adversary captures 4987 packets in which there are 88 retransmitted packets. Before No. 204 packet, the Adversary captures all packets and can track the dynamic secret. The fifth retransmission packet is No. 267 on the CC, but No. 266 on the Adversary. It indicates that the Adversary loses one packet between No. 204 to No. 267. Between No. 3634 and No. 3759, there is one retransmission packet (No. 2697) that is not captured by the Adversary.

The Adversary obtains different RS from the CC and ST. According to (1) and (2), the Adversary would generate the wrong DS and fail to track the DEK. If the Adversary tries to crack the RS, the complexity is related to three key factors: the number of retransmitted packets, the lost packets of the Adversary and the length of the RS.

B. Retransmitted Packet Ratio

The complexity of RS is determined by the number of the retransmitted packet. For example, if there is no retransmitted or non-retransmitted packet, the RS is all-zeroes or all-ones; if there is only 1 retransmitted packet, the Adversary can easily crack the RS using brute force. Thus, we need enough retransmitted and non-retransmitted packets to prevent against the brute force cracking. The number of retransmitted packet is determined by two factors: the *RPR* and the L_RS.

In the subsection, *RPR* in Zigbee communication is investigated. The ST and CC are deployed to communicate in four various conditions; in each condition, 20 groups of experiments are conducted and 200 packets are sent in each group. The *RPR* in all experiments are displayed in Fig. 6. It shows that: 1) It is difficult to predict how many packets would be retransmitted. In Condition_3, there are 7 retransmitted packets in group 5 and 23 retransmitted packets in group 12. The variance of the number of retransmitted packet is 11.7, 2.3, 14.7, and 6.1 in condition 1 to 4 respectively. 2) The *RPR* is high enough to protect the RS from cracking. The average *RPR* of all experiments is 3.8%.

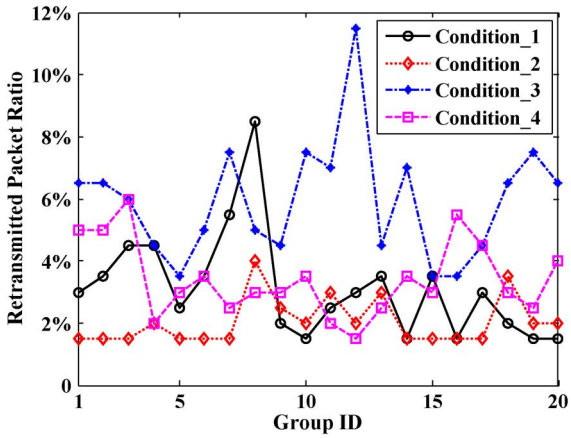

Fig. 6. Retransmitted packet ratio between ST and CC (Condition_1: ST is 3 meters from the CC with a wall between them; Condition_2: 3 meters without obstacle; Condition_3: 8 meters with a wall; Condition_4: 8 meters without obstacle).

Assuming L_RS is 110, the number of retransmitted packet is 4, and the combination of RS is $C_{110}^{4} \approx 5.77$ million.

C. Packet Loss Ratio

As shown in previous experiments, it is difficult for the Adversary to brute force crack the RS. But it is not proven whether the Adversary can obtain the RS by eavesdropping. In this subsection, three Adversaries are deployed at 3 different locations to eavesdrop the communication between ST and CC. Ten groups of experiments are carried out; in each group, 5000 packets are sent.

On all Adversaries and CC, the received packets are recorded to calculate the *PLR*, as shown in Fig. 7. The experiment results show that: 1) The packet loss is inevitable in Zigbee communication. Although three Adversaries are deployed around the CC within 2 meters, the average *PLR* is 0.85%, 1.17%, 2.11% on Location A, B, and C respectively; and the lowest *PLR* is 0.04% (2 lost packets) in all experiments. 2) There are enough lost packets to prevent the attacker's tracking on the dynamic secret. The maximum *PLR* is applied to measure the difficulty for the adversary to eavesdrop and generate the RS, because it is difficult for the Adversary to track the dynamic secret again once he lost one RS. In present experiments, the maximum *PLR* is as high as 2.1%, 4.64%, and 6.26% on Location A, B, and C respectively.

D. Length of RS

L_RS is restricted mainly by two factors: the resource of hardware and security.

RS and OTF set with various L_RS are implemented on the ZigBee chip CC2430 to investigate the consumption on time and memory. RS and OTF set need to be random access in ultra-low-power mode. On CC2430, there are only 4 KB SRAM that satisfy the requiems of RS and OTF set, which is expensive and needs lots of space on chip. In RS method, a packet is coded as one bit; the size of RS is $L\_RS/8$ bytes. In OTF set method, the whole packet is stored; and CC2430 can store 32 OTFs (assuming the packet is 128 bytes on average). The same as CC2430, most Zigbee chips integrate few SRAM. Thus, the OFT set is too large to store on Zigbee chips.

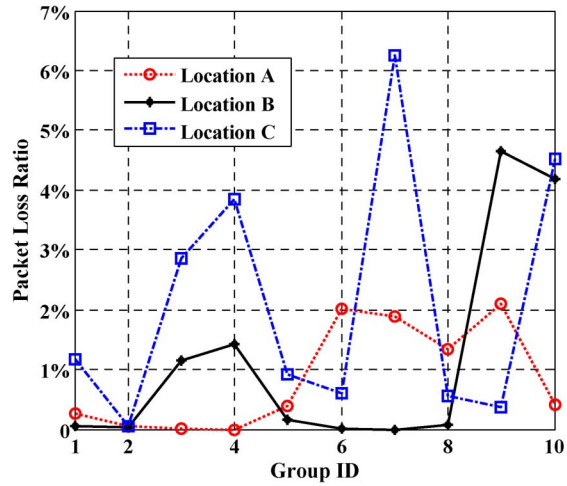

Fig. 7. Packet loss ratio on adversary (The CC, ST and Adversary are placed on a line without obstacle. The ST is 3 meters from the CC without any obstacle. Location_A: 2 meters from ST and 1 meter from CC; Location_B: 1 meter from ST and 2 meters from CC; Location_C: 5 meters from ST and 2 meters from CC).

TABLE II
COMPARISON BETWEEN RS AND OTF SET

Length of RS	*0/1 RS*		*OTF set*	
	Memory (bytes)	*Time (microsecond)*	*Memory (bytes)*	*Time (microsecond)*
16	*2*	*9696*	*2k*	*558144*
32	*4*	*9700*	*4k*	*1106472*
64	*8*	*9703*	*NULL*	
128	*16*	*14017*	*NULL*	
256	*32*	*18306*	*NULL*	
512	*64*	*26875*	*NULL*	

The MD2 message-digest algorithm is applied to translate RS to DS. In MD2, the message is divided into parts size of 16 bytes; these parts are processed one by one. Thus, the time consumption increases with the size of the message. As shown in Table II, the CC2430 needs about 9.7 milliseconds to process the RS that is less than 16 bytes. With the increasing of the length, the time consumption grows linearly. The CC2430 needs about 1.1 seconds to process a 32-packet OTF set, which is 40 times longer than a 512-packet RS. It is shown that the OTF set is too complicated to implement on Zigbee chip.

The L_RS is related to three security factors: the retransmitted packets in RS, the lost information of Adversary and the update frequency of DEK. The complexity for the Adversary to guess the RS and recover the incomplete RS are usually measured according to the combination of retransmitted packets and lost packets in the RS that increase linearly with the growth of L_RS. It is believed that the larger the L_RS is, the more secure the RS is. However, L_RS is inversely proportional to the update frequency of DEK, and equal to the validity period of key. The longer the validity period is, the higher the risk of encryption key cracking is.

Therefore, the L_RS is a tradeoff between the complexity of RS and the validity period of DEK. Since the RS is used to update the DEK, the L_RS is set as the least power of 2 which can ensure the user's request on the complexity of RS. For example, if the combination of RS is set to be no less than one million, the problem could be described as:

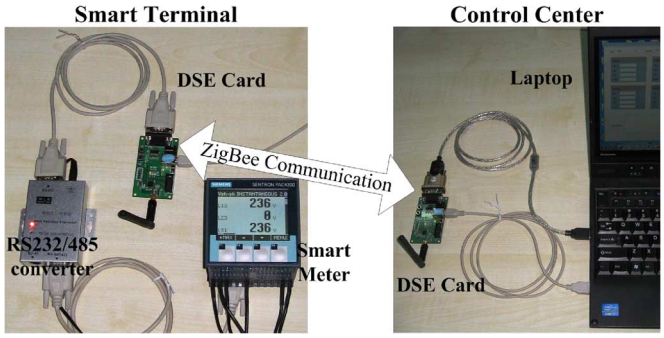

Fig. 8. DSE demo system.

$$\min_{L\_RS} \{C_{L\_RS}^{L\_RS \times RPR} > 1000000, L\_RS = 2^m, m \in N\} \quad (4)$$

Assuming the *RPR* is 3.8% (the average in our experiments), the L_RS is 128.

E. DSE Demo System

A DSE demo system is designed to encrypt the communication in smart grids, including DSE card and DSE monitor, as shown in Fig. 8.

The DSE card is developed on the CC2430-F128 demo board to generate RS, update the encryption key encrypt and encrypt/decrypt the data. In this demo, the MD2 message-digest algorithm is chosen as the hash function due to its high efficiency (it is specially designed for 8-bit processor); the L_RS is set as 128; and the interval of data uploading is 3 seconds. On the ST, a SIEMENS SENTRON PAC4200 is employed to measure the states of micro power grid; a DSE card is applied to obtain the measurements from smart meter, encrypt the data, and send the cipher text to the CC; and a RS232/485 converter is used to connect the smart meter and DSE card. On the CC, a DSE card is applied to receive and decrypt the cipher text; and the DSE monitor is installed on laptop to display the decrypt data and recode the whole process of decryption.

The DSE monitor is designed to show the process of dynamic secret generation and cipher text decryption, as shown in Fig. 9. The history information of received packets and last RS (in hex) is displayed in Block 1; current received cipher text, RS and DEK are presented in Block 2–4; the decrypted data is shown in Block 5; and 12 measurements are listed in Block 6.

In the three-party experiment, we assume the Adversary has the same DSE demo system as the CC and knows the initial secret of the smart meter. He tries to monitor the communication between ST and CC to track the dynamic secret, and decrypt them. In the following, we describe the details of decryption process on the Control Center [Fig. 9(a)] and Adversary [Fig. 9(b)] to show how to prevent the eavesdropping with DSE scheme.

1) Received Cipher Text (Encrypted Data): The CC and Adversary receive the same ZigBee packets in most cases. As shown in Block 2, they obtain same cipher text as follow (in hex)

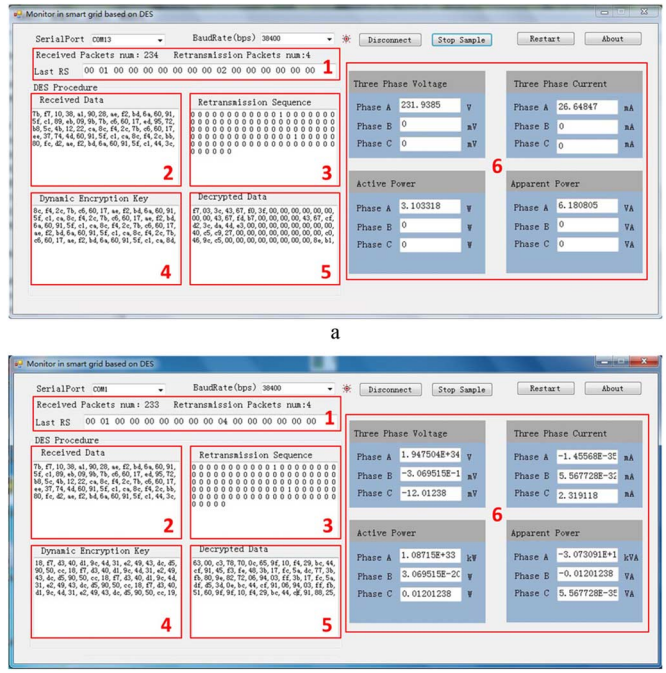

Fig. 9. DSE demo system interface. (a) Control center; (b) Adversary.

$$Cipher = \{7b, f7, 10, 38, a1, 90, 28, ae, f2, bd, 6a, 60, 91, 5f, c1, 89, eb, 09, 9b, 7b, c6, 60, 17, ed, 95, 72, b8, 5c, 4b, 12, 22, ca, 8c, f4, 2c, 7b, c6, 60, 17, ee, 37, 74, 4d, 60, 91, 5f, c1, ca, 8c, f4, 2c, bb, 80, fc, d2, ae, f2, bd, 6a, 60, 91, 5f, c1, 44, 3c\}$$

2) Retransmission Sequence and DEK: As shown in Block 1, the Last RS on the CC is "00 01 00 00 00 00 00 00 00 02 00 00 00 00 00 00," which indicates the sequence number of two retransmitted packets are 16th and 79th; the Last RS on the Adversary is "00 01 00 00 00 00 00 00 00 04 00 00 00 00 00 00," which indicates the retransmitted packets are the 16th and 78th packets. It reveals that the Adversary has lost one packet between the 17th and 79th packets. Moreover, the lost packet results in the Current RS on the Adversary are different from that on CC as shown Block 3.

According to the formula (1) and (2), the current DEK on the CC and the Adversary could be calculated as follows.

$$\begin{aligned} DEK_{CC}(1) &= DEK_{CC}(0) \oplus f_{MD2}(RS_{CC}) \\ &= 8c, f4, 2c, 7b, c6, 60, 17, ae, f2, bd, 6a, 60, \\ &\quad 91, 5f, c1, ca \end{aligned} \quad (5)$$

$$\begin{aligned} DEK_{Ad}(1) &= DEK_{CC}(0) \oplus f_{MD2}(RS_{Ad}) \\ &= 18, f7, d3, 40, d1, 9c, 4d, 31, e2, 49, 43, dc, \\ &\quad d5, 90, 50, cc \end{aligned} \quad (6)$$

Obviously, the Adversary generates the different DEK even he has the same device and knows the initial key.

3) Decryption and Measurement: According to the formula (3), $DEK^*(1)$ is generated by replicating $DEK(1)$ to decrypt

the received cipher text, as shown in Block 4 and 5. With the wrong decryption key, the Adversary could not obtain the real measurements, e.g. the voltage on Phase A is $1.9475^{*}10^{34}$ V as shown in Block 6.

VI. Conclusions

In this paper, a dynamic secret-based encryption scheme is designed to secure the wireless communication of SG. To reduce its complexity, the retransmission sequence is proposed to update dynamic encryption key, replacing the OTF set; and MD2 is selected as the hash algorithm. By implementing RS and OTF set with various lengths on the Zigbee chip, we find RS outperforms OTF set at time and memory consumption.

A demo system is developed to investigate the performance of DSE scheme. The numerous experiments reveal that: 1) the DSE scheme can protect the users against eavesdropping by updating the dynamic encryption key with retransmission sequence in communication, even the attackers know the details of DSE scheme and obtain the encryption key at some time; 2) it is a light-weight encryption method with only simple operations, such as MD2 and XOR; 3) it is self-contained, that is, it is dynamically generated during the normal communication without additional traffic and control command; 4) it is easy to implement on various SoC, such as CC2430; 5) it has good compatibility, which could be integrated with many wireless techniques and applications, such as ZigBee and Modbus.

References

[1] R. Moghe, F. C. Lambert, and D. Divan, "Smart "Stick-on" sensors for the smart grid," *IEEE Trans. Smart Grid*, vol. 3, pp. 241–252, 2012.

[2] Federal Energy Regulatory Commission, "Renewables & energy efficiency—Generation & efficiency standards" 2011 [Online]. Available: http://www.ferc.gov/market-oversight/othr-mkts/renew.asp

[3] K. Ren, Z. Li, and R. C. Qiu, "Guest editorial cyber, physical, and system security for smart grid," *IEEE Trans. Smart Grid*, vol. 2, pp. 643–644, 2011.

[4] "The smart grid: An introduction," in DOE's Office of Electricity Delivery and Energy Reliability 2008.

[5] P. Jokar, N. Arianpoo, and V. C. M. Leung, "A survey on security issues in smart grids," *Security Commun. Netw.*, 2012 [Online]. Available: http://http://onlinelibrary.wiley.com/doi/10.1002/sec.559/abstract

[6] T. Liu, Y. Gu, D. Wang, Y. Gui, and X. Guan, "A novel method to detect bad data injection attack in smart grid," in *Proc. IEEE INFOCOM Workshop Commun. Control Smart Energy Syst.*.

[7] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, pp. 75–77, 2009.

[8] Office of the National Cordination for Smart Grid Interoperability, "NIST framework and roadmap for smart grid interoperability standards," 2010 [Online]. Available: http://www.nist.gov/smartgrid/

[9] Cisco,, "Security for the smart grid," 2009, White Paper [Online]. Available: http://www.cisco.com/web/strategy/docs/energy/white_paper _c11_539161.pdf

[10] W. Xudong and Y. Ping, "Security framework for wireless communications in smart distribution grid," *IEEE Trans. Smart Grid*, vol. 2, pp. 809–818, 2011.

[11] P. Jokar, H. Nicanfar, and V. C. M. Leung, "Specification-based intrusion detection for home area networks in smart grids," in *Proc. 2011 IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, pp. 208–213.

[12] Z. Yichi, W. Lingfeng, S. Weiqing, R. C. Green, and M. Alam, "Artificial immune system based intrusion detection in a distributed hierarchical network architecture of smart grid," in *Proc. 2011 IEEE Power Energy Soc. Gen. Meet.*, pp. 1–8.

[13] M. M. Fouda, Z. M. Fadlullah, N. Kato, L. Rongxing, and S. Xuemin, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, pp. 675–685, 2011.

[14] S. Nguyen and C. Rong, "ZigBee security using identity-based cryptography autonomic and trusted computing," in *Proc. 4th Int. Conf. Autonomic Trusted Comput. (ATC'07)*, 2007, vol. 4610, Lecture Notes in Computer Science, pp. 3–12.

[15] Z. Yichi, W. Lingfeng, S. Weiqing, R. C. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Trans. Smart Grid*, vol. 2, pp. 796–808, 2011.

[16] J. Xia and Y. Wang, "Secure key distribution for the smart grid," *IEEE Trans. Smart Grid*, vol. 3, pp. 1437–1443, 2012.

[17] H. Khurana, M. Hadley, L. Ning, and D. A. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, pp. 81–85, 2010.

[18] S. Xiao and W. Gong, "Wireless network security using randomness," U.S. Patent 8 204 224 B2, Jun. 19, 2012.

[19] X. Sheng, G. Weibo, and D. Towsley, "Secure wireless communication with dynamic secrets," in *Proc. 2010 IEEE INFOCOM*, pp. 1–9.

[20] The Smart Grid Interoperability Panel Cyber Security Working Group, "Introduction to NISTIR 7628 guidelines for smart grid cyber security," 2010 [Online]. Available: http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf

[21] J. Kim and H. Choi, "An efficient and versatile key management protocol for secure smart grid communications," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 1–4, 2012, pp. 1823–1828.

[22] L. Fengjun, L. Bo, and L. Peng, "Secure information aggregation for smart grids using homomorphic encryption," in *Proc. 2010 1st IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, pp. 327–332.

[23] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Trans. Smart Grid*, vol. 1, pp. 99–107, 2010.

[24] W. Dapeng and Z. Chi, "Fault-tolerant and scalable key management for smart grid," *IEEE Trans. Smart Grid*, vol. 2, pp. 375–381, 2011.

[25] Y. Ye, Q. Yi, and H. Sharif, "A secure data aggregation and dispatch scheme for home area networks in smart grid," in *Proc. 2011 IEEE Global Telecommun. Conf.*, pp. 1–6.

[26] H. Li, S. Gong, L. Lai, Z. Han, R. Q. Qiu, and D. Yang, "Efficient and secure wireless communications for advanced metering infrastructure in smart grids," *IEEE Trans. Smart Grid*, vol. 3, pp. 1540–1551, 2012.

[27] L. Rongxing, L. Xiaohui, L. Xu, L. Xiaodong, and S. Xuemin, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, pp. 1621–1631, 2012.

[28] Y. Peizhong, A. Iwayemi, and Z. Chi, "Developing ZigBee deployment guideline under WiFi interference for smart grid applications," *IEEE Trans. Smart Grid*, vol. 2, pp. 110–120, 2011.

[29] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards," *Comput. Commun.*, vol. 30, pp. 1655–1695, 2007.