A Novel Method of Secured Scheme for Smart Grid Wireless Communication

R. Naveenraj, UG Scholar,
Dept of ECE,
Knowledge Institute of Technology,
Salem, Tamilnadu, India.

S. Ranjithkumar, UG Scholar,
Dept of ECE,
Knowledge Institute of Technology,
Salem, Tamilnadu, India.

G. Vasanthi, UG Scholar,
Dept of ECE,
Knowledge Institute of Technology,
Salem, Tamilnadu, India.

V. Ramya, UG Scholar,
Dept of ECE,
Knowledge Institute of Technology,
Salem, Tamilnadu, India.

K. Rathinakumar,
Assistant professor ECE,
Knowledge Institute of Technology,
Salem, Tamilnadu, India.

***Abstract*— In Future, the smart grid power transmission can be most usable system. This system is very useful for power transmission, but also introduces many security problems. To overcome the above problem, we are using an encryption scheme which is introduced by using an information network in the communication medium. In this project, the information network can be integrated in to the smart grid power transmission. In between the two systems of communication, the previous packets can be taken as retransmission sequences. Where the retransmitted packet is marked as "1" and the non-retransmitted packet can be marked as "0". At the time of communication, the retransmission sequences can be generated at both sides to update the encryption key. In this project, the smart grid is built by using ZigBee protocol for wireless communication to the information network. The encryption system is designed based on this platform. The result shows the retransmission and packet loss can be very low and it is impossible for the attacker to track the updating of encryption key.**

Keywords*— Encryption, retransmission, security, smart grid, wireless communication, ZigBee.

I. INTRODUCTION

According to the latest statistical data rapid increase in electrical power demand and renewable energy mandates are push towards electrification in the transportation sector is expected to increase power system Stresses and disturbances [1].

Federal Energy Regulatory Commission states that 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. In which the built-in information networks support two-way energy and information flow that facilitate penetration of renewable energy sources into the grid and empower consumer with tools for optimized energy consumption [3], [4].

P. Jokar, N. Arianpoo, and V. C. M. Leung[5] described that A survey on security issues in smart grids. which consider the advent of the smart grid concept, security has al-ways been a primary concern. Pricing information and control actions are transmitted via the information network. Various at-tacks 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.

P. McDaniel and S. McLaughlin[7] described that Security and privacy challenges in the smart grid where 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.

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].

W. Xudong and Y. Ping [10] described that Security framework for wireless communications in smart distribution grid 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 of following two main reasons. First one is home area net-work, it is too expensive to build wired networks to monitor various devices with different interfaces and another one is when hundreds of parameters in the grid need to be monitored, wired network can result in a costly and complicated system architecture.

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 primary thing to design any system. In order to be cost effective, the computational power, memory and storage area 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 [5]; 2) third party applications, such as private key generator [14], may visibly increase the cost of whole wireless system.

Low-bandwidth:

Efficiency of the communication is based on the size of 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 app in SG [5]. Distributed IDS 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 mA 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 wire-less techniques. The DSE key is dynamically generated during the normal communication without additional traffic and control command.

II. 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

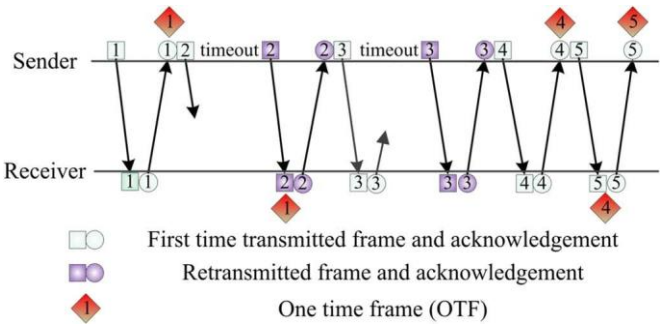

Fig.1. SW protocol and OTF identification (reproduced from [19]).

DSE scheme for smart grid wireless communication. In this session, we firstly introduce the basic algorithms of dynamic secret; and then present the DSE scheme.

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

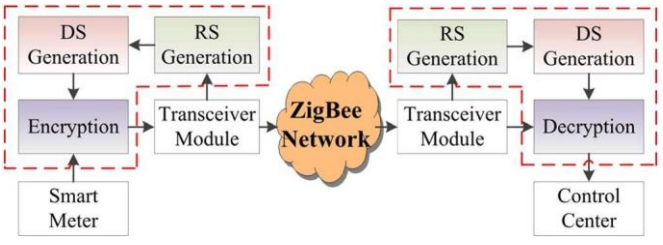

Fig. 2. Framework of DSE scheme.

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 $f_{hh\ as}$ are recommended in DSG module.

$$DS(K)=f\ HASH\ (\psi L\_RS)$$

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

$$DEK(k)=DS(K).DEK(k-1)$$

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.

$$DATA.DEK^*(k)=Cipher$$

$$Cipher.DEK^*(k)=DATA$$

DSE scheme is an appropriate solution for securing SG wire-less 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.

III. 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 wire-less network in the platform. IEEE 802.15.4 standard defines the physical and MAC layers of ZigBee, while the ZigBee Alliance defines the network and application layers. Since it is de-signed as a low cost, low rate, low power and low complexity personal area network,

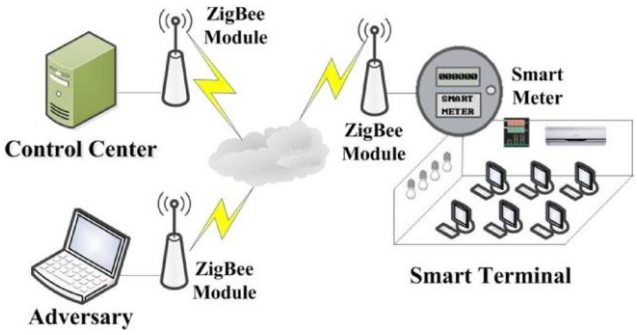

Fig. 3. Experiment platform.

ZigBee is considered as an ideal pro-tocol 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 eaves drop 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.

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.

IV. 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.

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. Ac-cording 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 examples 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%.

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

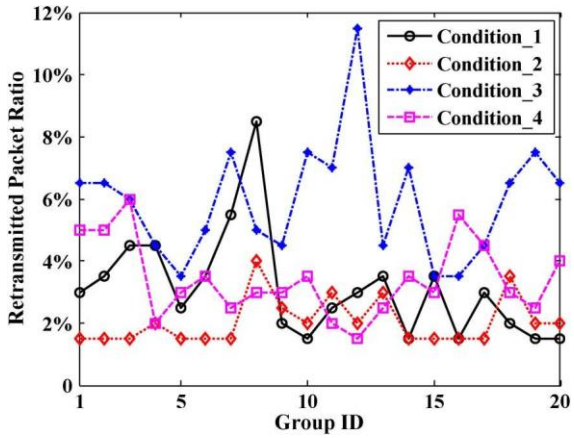

Fig. 6. Retransmitted packet ratio between ST and CC (Condition_1: ST is 3 meters from the CC with a wall between them; Condition _2: 3 meters without obstacle; Condition_3: 8 meters with a wall; Condition_4: 8 meters without ob-stacle)

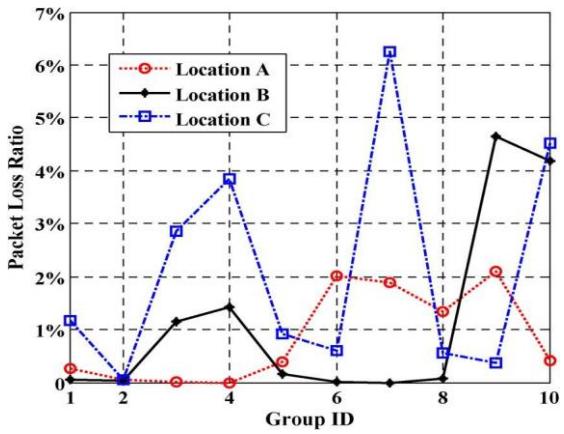

Fig. 7. Packet loss ratio on adversary (The CC, ST and Adversary are placed on a line without obstacle. The ST is 3 meters from the CC without any obstacle. Location_A: 2 meters from ST and 1 meter from CC; Location_B: 1 meter from ST and 2 meters from CC; Location_C: 5 meters from ST and 2 meters from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

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.

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 up-date 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:

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

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

V. CONCLUSIONS

In this concept, an encryption scheme is proposed to secure the smart grid wireless communication. To reduce its complexity, the retransmission sequence can be implemented to update the encryption key. . The example of 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 can be easily implemented on various algorithms; 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 effi-ciency—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 De-livery 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]. Avail-able: http://http://onlinelibrary.wiley.com/doi/10.1002/sec.559/ab-stract
[6] T. Liu, Y. Gu, D. Wang, Y. Gui, and X. Guan, "A novel method to de-tect 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 stan-dards," 2010 [Online]. Available: http://www.nist.gov/smartgrid/
[9] Cisco,, "Security for the smart grid," 2009, White Paper [On-line]. Available: http://www.cisco.com/web/strategy/docs/en-ergy/white_paper _c11_539161.pdf
[10] W. Xudong and Y. Ping, "Security framework for wireless communi-cations in smart distribution grid," *IEEE Trans. Smart Grid*, vol. 2, pp. 809–818, 2011.