1-10-2016

An Adaptive Security Protocol for a Wireless Sensor-based Monitoring Network in Smart Grid Transmission Lines

Xuping Zhang
Nanjing University

Feng Ye
University of Dayton, fye001@udayton.edu

Sucheng Fan
Nanjing University

Jinghong Guo
China Electric Power Research Institute

Guoliang Xu
Nanjing University

See next page for additional authors

SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2016; **9**:60–71
Published online 26 October 2015 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1382

RESEARCH ARTICLE

An adaptive security protocol for a wireless sensor-based monitoring network in smart grid transmission lines

Xuping Zhang[1], Feng Ye[2], Sucheng Fan[1], Jinghong Guo[3], Guoliang Xu[1] and Yi Qian[2]*

[1] Institute of Optical Communication Engineering, Nanjing University, China
[2] Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, NE, USA
[3] China Electric Power Research Institute, China

ABSTRACT

In this paper, we propose a new security protocol for a wireless sensor network, which is designed for monitoring long range power transmission lines in smart grid. Part of the monitoring network is composed of optical fiber composite over head ground wire (OPGW), thus it can be secured with conventional security protocol. However, the wireless sensor network between two neighboring OPGW gateways remains vulnerable. Our proposed security protocol focuses on the wireless sensor network part, it provides mutual authentication, data integrity, and data confidentiality for both uplink and downlink transmissions between the sensor nodes and the OPGW gateway. Besides, our proposed protocol is adaptive to the dynamic node changes of the monitoring sensor network; for example, new sensors are added to the network, or some of the sensors are malfunctioning. We further propose a self-healing process using an "*i*-neighboring nodes" public key structure and an asymmetric algorithm. We also conduct energy consumption analysis for both general and extreme conditions to show that our security protocol improves the availability of the monitoring sensor network. Copyright © 2015 John Wiley & Sons, Ltd.

KEYWORDS
smart grid; security protocol; monitoring sensor network; energy efficiency

***Correspondence**
Yi Qian, Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, NE, USA.
E-mail: yi.qian@unl.edu

1. INTRODUCTION

Smart grid applies communication technology to gather grid operational information by deploying sensors, field automated devices, and smart meters. Such information is used to provide automatic control over the power grid. Therefore, the efficiency, reliability, and sustainability of the power grid will be enhanced [1–6]. Smart grid enables quick and accurate detection of the time and location of a malfunctioning component and informs the operators and utilities so that proper actions can be applied to prevent a power failure or to reduce the damage of such failure [7,8]. Smart grid is capable of providing those functions because of reliable two-way communication networks in parallel with the power grid system.

The two-way communication networks established in the grid monitor and control the status of most parts in the smart grid, for example, power generators, transmission lines, and substations. Therefore, smart grid is more efficient and reliable than traditional power grid [9–11]. In this paper, we study the monitoring network over the transmission line in smart grid. Specifically, the monitoring network consists of numerous sensor nodes, data centers and hierarchical communication links [12]. As the optical fiber composite overhead ground wire (OPGW) technology can provide the great advantages for communications in capacity, effectiveness, reliability, security, and so on [13], such OPGW has been deployed along the transmission lines in many places already [14]. However, because of the attenuation of signal and the cost of equipment, it is impractical to grant access to OPGW for every sensor node along the monitoring network. Therefore, in our studied monitoring network, OPGW is assumed to be accessed by selected nodes, which are referred to as gateway nodes. For other intermediate nodes in between two gateway nodes, they are connected by a lower cost multihop wireless network [15–22]. In fact, this design of smart grid has been considered by some countries already, for

example, the smart grid in China has been allocated a dedicated spectrum (230 MHz [23,24]) for wireless transmission for this purpose.

Our focus in this paper is the cyber security on the concerned monitoring and control network of the transmission lines, because it is one of the most important issues among all requirements of the sensor network for transmission lines. The wireless portion of the monitoring network must meet the demand of smart grid (e.g., latency requirement); it is also important for the sensor nodes to be energy efficient. We assume that the sensor nodes are powered by green energy (e.g., solar power) for two reasons: (i) the transmission line is too powerful to power a sensor; (ii) it would be more flexible to deploy and cheaper to maintain the sensor nodes by using green energy. Therefore, the studied wireless monitoring network cannot afford expensive or complicated security protocols for traditional networks.

In this paper, we propose a security protocol for the wireless portion of the monitoring sensor network, which uploads the monitoring data (e.g., voltage status, humidity of the environment, etc) of the transmission lines. The sensor network delivers the status information from the monitoring point of each sensor node through uplink to the gateway and then to the data collection center through OPGW. The control center delivers control information through the downlink in the similar way. Our proposed protocol meets both security and reliability requirements for the wireless portion of the monitoring network. The proposed protocol consists of several security mechanisms including authentication of both equipment and messages transmitted, as well as data encryption for both uplink and downlink transmissions.

Generally, a protocol designed for a network with complicated topology is more likely to find a new route to avoid malfunctioning nodes. However, the investigated wireless sensor network is simply a chain topology, and the maintenance of the nodes is hard to pursue. Therefore, how to maintain reliable communications is a challenge. We propose a self-healing process to tackle such a challenge based on a new public key structure of "*i*-neighboring nodes" and an asymmetric encryption algorithm.

The rest of the paper is organized as follows. In Section 2, related work is presented. In Section 3, the studied wireless monitoring sensor network is illustrated. In Section 4, a security protocol is proposed. In Section 5, the proposed protocol is analyzed in details. In Section 6, the simulation results are presented to demonstrate the availability of the sensor network for the proposed security protocol. In Section 7, the conclusion and future work are given.

2. RELATED WORK

Many researchers have studied the cyber physical system of smart grid including data transmission, power management, cyber security, and so on [10,15,16,25]. However, not many research works have been focused on the monitoring network of the power line transmission system. Two types of status are monitored by the high-voltage electrical transmission lines monitoring system, electric current and line positions. With real-time monitoring, electricity overload, phase unbalance, fluctuation, and so on can be avoided or reduced. Some situations such as sagging and galloping can be tracked by the control center.

Research works that are conducted on the monitoring network focused on monitoring technologies rather than communications. For example, Ren *et. al* proposed a dynamic line rating system to monitor the online sag under complex climates (e.g., heavy rains, heavy snow, strong wind, etc.). [26]. Huang *et al.* proposed an online scheme to monitor the icing density and type of the transmission line [27]. Sun *et. al* proposed a high-voltage transmission line monitoring system based on magnetoresistive sensors [28], which calculate both the current flow and the line positions from the magnetic field emnated from the phase conductors.

Lin *et. al* proposed a wireless sensor network based on power transmission line monitoring frame [15]. Specifically, the authors proposed to establish a wireless mesh sensor network on each tower. The gateway on a tower is able to relay data to the gateway on its neighboring tower. However, network security was not thoroughly studied. In our work, the focus is on the network security of the long distance data delivery of the monitoring network. The main contributions of our work include:

- A new security protocol for transmission line monitoring network is proposed.
- The flexibility demand of smart grid is considered; for example, a sensor node can be added to the network, or an existing sensor can be ruled out at any time.
- Reliability of the communication is considered.
- Energy efficiency is considered because of limited power supply of sensor nodes.

3. NETWORK MODEL

Figure 1 shows a typical model of the monitoring network for power transmission lines. The server located in an operational center performs the short term data storage and management and also works for the data transmission. The authentication server (AS) used in initialization process and data collection center (DCC) used in both uplink and downlink processes are also included in the server. The data aggregation units (DAUs) located on the transmission tower are utilized to collect the sensing data of the surroundings, for example, humidity, the precipitation, the range of shake, and so on. A dual-link gateway DAU (DGD) and a regular DAU are similar, expect that DGD has access to the optical fiber network, so each DGD serves as the gateway to the OPGW for wireless network consisting of the DAUs. Our focus is on the multi-hop wireless sensor network between two DGDs in the rest of the paper.

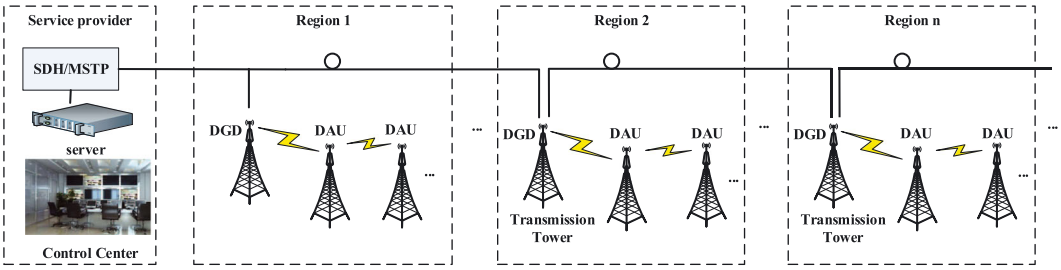

Figure 1. Network model of the monitoring network.

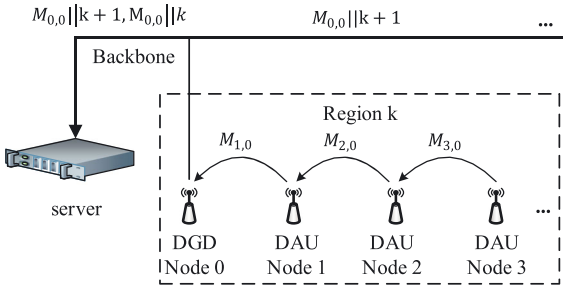

Figure 2. Monitoring data uplink transmission model.

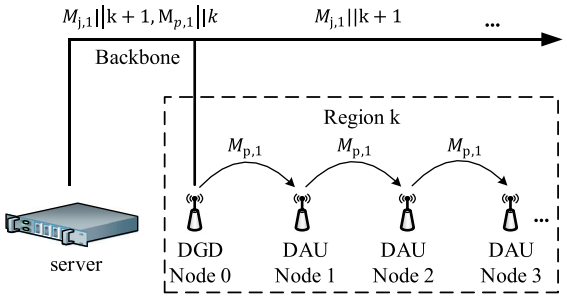

Figure 3. Control command downlink transmission model.

The DAUs in a region (between two DGDs) are tagged from node 1 to node n; the gateway is tagged as node 0 in a region. Every region also has its unique number, so if the server wants to communicate with a node, it should find the DGD of the designated node's region first and then find the target node. As for the communication mode and the protocol, we assume a DGD with the following communication capability.

Figure 2 shows how the monitoring data are uploaded in the network. In the uplink process, we combine all the monitoring data of the nodes in a region together to generate an aggregated message transmitted to DGD (i.e., node 0). Node 0 aggregates its data to the data from other nodes, but it also adds an extra code to state from which region the message comes. The uplink transmission consumes more energy compared with that of the downlink transmission because of different data sizes. Figure 3 shows the process of downlink transmission for control messages. Note that either broadcast/multi-cast or uni-cast, the size of the data is much smaller compared with the aggregated data in uplink transmission. Without loss of generality, we introduce the case of uni-cast. The broadcast/multi-cast case can be simply extended from the uni-cast case in a network with chain topology.

4. PROPOSED SECURITY PROTOCOL

In the conventional security protocol for such a network scenario, the message of node i is encrypted using symmetric encryption algorithm, and the nodes between node i and data center are relay nodes. The great advantage of the conventional protocol is of its simplicity and efficient operation with a certain extent of security, so it is a good fit for the wired portion of the monitoring network because of the high transmission rate and physically secured structures. However, for the wireless sensor monitoring network, it is inappropriate to adopt the conventional protocol or symmetric encryption algorithms because of their low flexibility, scalability, and relevance between every message. Therefore, we propose a new protocol for the wireless sensor monitoring network. The proposed security protocol uses a lightweight asymmetric encryption algorithm that each sensor node only occupies temporarily generated public keys of some neighboring nodes.

In this section, we describe the proposed security protocol, which includes authentication of both equipment and messages, decryption of messages, and solution to the vulnerability of the network structure. The proposed security protocol consists of four parts, namely initialization process, uplink data process, downlink command process, and self-healing process for malfunctioning nodes. The main task of initialization process is to authenticate every newly added node and to establish the network route. Moreover, we need to achieve the key distribution in this process too. The uplink and downlink command process are designed for the secure transmission of message in each direction. The self-healing process for malfunctioning nodes can improve the reliability of the monitoring sensor network.

4.1. Initialization process

The proposed initialization process addresses the two issues: (i) to authenticate a newly added node and (ii) to distribute the corresponding keys securely to the newly added node and to its neighbors within i hops.

Security Comm. Networks 2016; **9**:60–71 © 2015 John Wiley & Sons, Ltd.
DOI: 10.1002/sec

Definition 1. *"i-neighboring nodes" of node k are the nodes within i-hop to node k.*

In our design, we assume that node n stores the public keys of its i-neighboring nodes (e.g., $PU_{n\pm j},\ 0 < j \leq i < n$). Different i defines the level of flexibility, where the network is more robust with larger i. For example, if $i = 1$, the communication will be broken if an intermediate node is malfunctioning, but we can continue communication in the same situation when $i = 2$ because it is capable of hopping over the malfunctioning node. However, increasing i leads to a higher transmission energy consumption. Therefore, i must be appropriate so that it can balance the reliability and the transmission power consumption of the wireless sensor network.

For simplicity, we list the keys used by node n in Table. I. For node n, K_n is the pre-installed key for authentication, and it is known to node n and the AS. PR_n is the private key which is generated and distributed by the AS during the initialization process. The public keys of node n and n's i-neighboring nodes are $PU_{n-i}, \ldots, PU_{n+i}$. Moreover, we specify that $PU_{n-j},\ 0 < j \leq i,\ i < n$ as backward keys, which will be used in downlink transmission, and $PU_{n+j},\ 0 < j \leq i,\ i < n$ as forward keys, which will be used in uplink transmission. The generating algorithms of public/private keys can be arbitrarily chosen by the AS. Note that if node $n–k$ does not exist, we assume $PU_{n-k} = 0$. During normal operation, node n only communicates with its one-hop neighboring nodes (i.e., $n-1$ and $n+1$); therefore, we also define the public keys with one-hop neighboring nodes (i.e., PU_{n-1} and PU_{n+1}) as *default keys*. $K_{n-1,n}$ and $K_{n,n+1}$ as the communication keys, which are generated by node n with PR_n to authenticated message in transmission process between node $n-1 \leftrightarrow$ node n, and node $n \leftrightarrow$ node $n+1$. It means that node n will communicate with node $n-1$, and node $n+1$ when the network is working properly. But if one of them is broken down, for example, node $n+1$, the default forward key will be replaced by PU_{n+2}, and communication key will be updated to $K_{n,n+2}$ too.

After knowing the structure of keys in Figure 4, we describe the authentication process and the distribution process of the private keys. We assume that a secure network from node $n-1$ to node 1 has already been built. Now a new node n wants to add itself to the network after node $n-1$. It has an authentication key, which is only known to the AS and n itself. So node n and node $n–1$ need to achieve mutual authentication through the AS. They perform a two-way handshake first. Node n send $M_0 = \text{Request}||n||C_0$ to node $n-1$ and receive $M_1 = \text{Accept}||(n-1)||C_1$ from node $n-1$ if M_0 is standard. The "Request" and "Accept" are two given messages used in the authentication process, which are only known by nodes and AS. It can protect the communication from forgery to a certain extent before the message being discovered. Note that "n" is the ID embedded in node both n and the AS. "C_i" is a hashed value used as a message authentication code for message i. After this simple handshake, node n will send its authentication message $M_2 = E_{K_n}(T + K_n)||n||C_2$ to node $n-1$. To be secure from replay attack, node n generates a challenge (e.g., a time stamp or a nonce T). Then node $n-1$ forwards the message to the AS through the intermediate nodes from $n-2$ to node 1, which are simply intermediate nodes with secure links between node $n-1$ and the AS in the authentication process. So the security can be provided as only $n-1$, and the AS are directly involved in the authentication process. After the AS receives the M_2, it decrypts the message using K_n to obtain T and sends $M_2' = E_{K_n}(T)||C_2'$ back to node n. Node n authenticates the AS by comparing T decrypted from M_2' and replies T to the AS. Upon receiving T, the AS confirms the initialization process of node n.

Table I. Key structure for node n.

Authentication key	K_n
Private key	PR_n
Forward public key	$PU_n, PU_{n+1} \ldots PU_{n+i}$
Backward public key	$PU_n, PU_{n-1} \ldots PU_{n-i}$
Communication key	$K_{n-1,n}, K_{n,n+1}$

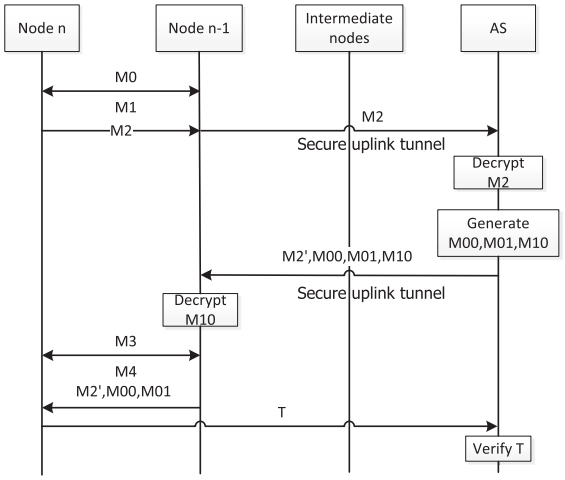

Figure 4. Authentication and private key distribution process.

After the authentication process, node n should be added to the network if it is legitimate. The next step is to distribute corresponding keys. There are two parts of key distribution which are private key distribution and public key distribution. The private key distribution is done after the authentication process. The AS generates three messages in this process, that is, $M_{00} = E_{K_n}(PR_n)||C_{00}$, $M_{01} = E_{K_n}(PU_{n-1})||C_{01}$, and $M_{10} = E_{PU_{n-1}}(PU_n)||C_{10}$. The messages are sent to node $n–1$ first through the security network consisting of all the authenticated nodes. Node $n-1$ can only decrypt the M_{10} to obtain the PU_n, the public key distributed to node n, so that it is informed of which node is allowed to be added to the network. Node $n-1$ relays M_{00} and M_{01} to node n after a two-way handshake. The $M_3 = \text{Request}||(n-1)||C_3$ and $M_4 = \text{Allow}||n||C_4$ are utilized in the handshake similar to the previous process. The M_{00} contains the private key of node n, PR_n, which is

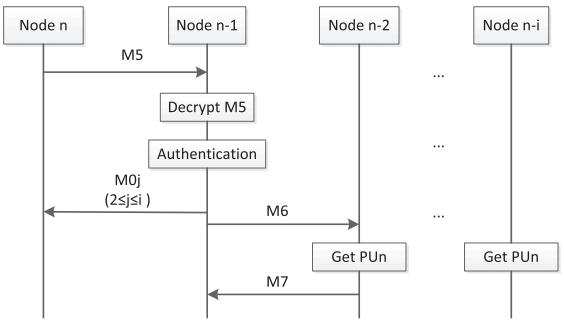

Figure 5. Public key distribution process.

distributed by the AS and the M_{01} contains the public key of node $n-1$, PU_{n-1}, which is utilized to inform node n that node $n-1$ is creditable too.

The public key distribution is shown in Figure 5. As node n and $n-1$ can authenticate each other now, the message $M_5 = E_{PU_{n-1}}(PU_n \| \text{Request}) \| C_5$ is utilized as a "hello" to node $n-1$. Node $n-1$ will authenticate the PU_n with the public key from the AS to ensure the identity of the sender. Then it will reply a series message $M_{0j} = E_{PU_n}(PU_{n-j}) \| C_{0j}$, $2 \le j \le i$, $i < n$, to node n to distribute the public key. Now, the public key distribution of node n has been finished but we have to update the public key of node $n-2$ to node $n-i$ (transmitting PU_n from node $n-1$ to node $n-i$ one by one) using the process between node $n-1$ and node $n-2$. Messages $M_6 = E_{PU_{n-2}}(PU_n \| \text{Request}) \| C_6$ (from node $n-1$ to node $n-2$) and $M_7 = E_{PU_{n-1}}(\text{Accept}) \| C_7$ (from node $n-2$ to node $n-1$) are responsible for the public key update. The proposed initialization process not only adds a new node to the secure network, but also updates all the keys to provide high security.

4.2. Uplink data process

After a secure network from node n to the DCC has been built after the initial process, the network for monitoring data transmission is active. The message sent from node k to node $k-1$ is $M_{k,0} = M_n \| M_{n-1} \| \ldots \| M_k \| M'_k \| C_k$. The '0' behind '$k$' in the $M_{k,0}$ is the indicator of transmission direction, for example, '0' stands for uplink transmission. The $M_{k,0}$ consists three parts. The first part is $M_n \| M_{n-1} \| \ldots \| M_k$, where M_i is the monitoring data of node i, which has been encrypted; it is appended to the encrypted message of node k to the message from the node before it. $M'_k = M_n + M_{n-1} + \ldots + M_k$ ("+" stands for XOR function), which is utilized for generating message authentication code and encryption process in the next node, node $k-1$. The last part C_k is the message authentication code generated by M_k and the communication key between node k and node $k-1$, $K_{k,k-1}$. The message authentication code is for the data integrity.

After explaining the structure of the message, we then present how to transmit a message in the uplink process for a normal situation using node n and $n-1$ as an example shown in Figure 6. Before transmitting the message $M_{n,0}$ to node $n-1$, node n processes a two-way handshake with node $n-1$ to authenticate node $n-1$ and make sure it is operating properly. The "hello" message $M_{h,0} = E_{PU_{n-1}}(E_{PR_n}(\text{hello}) \| n)$ is sent from node n to node $n-1$. The "D&I" stands for decryption and integrity validation for simplicity. Node $n-1$ decrypts the $M_{h,0}$ using its private key PR_{n-1} first to get "n", so it knows the message from node n. Then node $n-1$ decrypts $E_{PR_n}(\text{hello})$ with PU_n to further verify the sender authentication. Then node $n-1$ replies node n with the message $M_{r,0} = E_{PU_n}(E_{PR_{n-1}}(\text{response}) \| (n-1))$. Node n can authenticate the $n-1$ through the same way. After node n authenticating the $n-1$, it runs function FE_n to generate the $M_{n,0}$ and then sends the $M_{n,0}$ to node $n-1$. The node $n-1$ will do a message authentication first after receiving $M_{n,0}$ to check data integrity. It will generate a message authentication code C'_n using the middle part of the message M'_n and $K_{n,n-1}$ stored in itself. If C'_n is equal to C_n, which is generated by node n, then the transmission is successful. Then, the node $n-1$ will repeat the same process to transmit aggregated messages to node $n-2$.

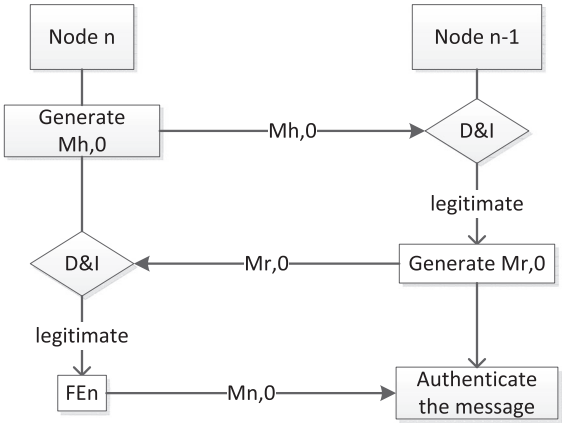

Figure 6. Uplink data process.

For node i, its function FE_i is illustrated in Figure 7. The monitoring data of node i, D_i, is conducted an XOR ($\bigoplus$) operation with the M'_{i+1} first to enhance avalanche effect. Node n will use an initial vector IV, which is known by both node n and DCC indicating that it is the first node in the uplink process. Then node i encrypts the result with the public key of node i, PU_i to generate $M_i = E_{PU_i}(D_i + M'_{i+1})$. In public-key cryptograph, the message encrypted by the public key PU_i can just be decrypted by the corresponding private key PR_i, and PR_i is known by node i and the DCC only. So it can ensure the security of data. Afterwards, we let $M'_i = M'_{i+1} + M_n$ to generate a new intermediate message for node i ($M'_n = 0 + M_n = M_n$ if it is the first node of the network). Node i also generates a hash value C_i based on M'_i and the communication key $K_{i,i-1}$ so that the next node can authenticate the message. Then M_n is XORed with M_i, and the result is compared with M'_i to ensure the data integrity. At last, M_i, M'_i, and C_i are appended to $M_n \| M_{n-1} \| \ldots \| M_{i+1}$ as $M_{i,0}$.

DOI: 10.1002/sec

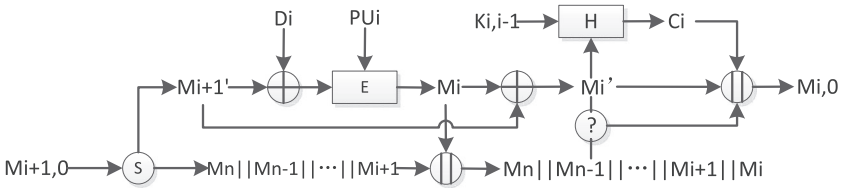

Figure 7. FE_i function for node i.

4.3. Downlink command process

The downlink process is different from the uplink process mainly in three ways. (i) In the uplink process, we need to transmit the monitoring data of all nodes to the DCC, but the control command from DCC can be unicast, multicast, or broadcast. (ii) The monitoring data can be sent in a given schedule, but the control command can be sent sparsely. (iii) The monitoring data are relatively large in data size, but the control command can be very short and the same size or content to different nodes. The different characteristics between uplink and downlink communications requires a different security procedures, which can transmit control command securely and timely to the designated node for the downlink. The proposed security protocol for downlink process is about to be not only simpler but also secure compared with the protocol for uplink process. The first change is the structure of message. We have stated that the message transmitted from node k is $M_{k,0} = M_n||M_{n-1}||\ldots||M_k||M'_k||C_k$, which contains the data and authentication message of all the nodes before it. Now, we examine the control command, which is to be sent to node k as $M_{k,1} = E_{PU_k}(CM_k)||k||C_k$. The first part of $M_{k,1}$ is the encrypted command, and the middle part is the ID of the receiving node. These two parts are fixed after the $M_{k,1}$ is generated. The last part C_k is generated as an authentication code, so it will be changed after the message sent from one node to the other. The transmitting route is also changed as we note in the network model section. The simple structure and distribution way provided by the encryption and authentication can ensure timely and securely transmission to designated nodes in the downlink.

For example, if the DCC wants to send message $M_{k,1}$ to node k using the downlink command process, $M_{k,1}$ is sent hop by hop because of network structure. Similar to the uplink process, the sender and the receiver perform a similar two-way handshake. Then the receiver node i processes the steps shown in Figure 8. The node i will separate the ID part first and compare the ID with its own after authenticating the C_k generated by the sender node $i-1$. If they are the same, that is to say $i = k$, it will decrypt the $E_{PU_k}(CM_k)$ to get the control command CM_k. If it is different, the node i will continue to transmit the message $M_{k,1}$ to node $i + 1$ after it updates the C_k using the $E_{PU_k}(CM_k)||k$ and $K_{i+1,i}$ and generate the new $M_{k,1}$.

For this process, we do message authentication in every node to make sure the validity of transmitted control

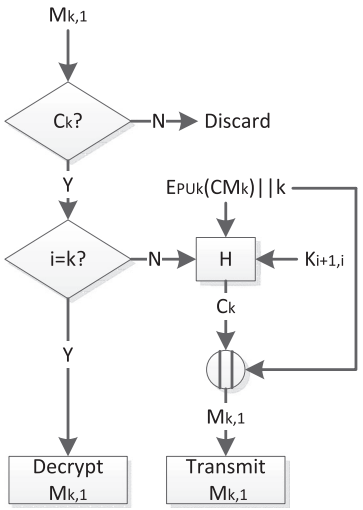

Figure 8. Downlink process of node i.

command message, and we do not need to decrypt if the node is not the designated receiver. This design can make the transmission process more efficient.

4.4. Self-healing process for malfunctioning nodes

The monitoring sensor network could suffer from low reliability because the communications will be interrupted even if there is only one malfunctioning node. To enhance the reliability, we propose the i-neighboring public key structure. If there are some malfunctioning nodes, we first confirm which nodes can work well and build a new link based on them as shown in Figure 9. We assume that the node from $n-1$ to $n-k$ $(1 < k < i)$ do not operate properly for some reasons, for example, being compromised by an attacker, being damaged due to bad weather, and so on. Node n must be informed with the status of those malfunctioning nodes and build a new link with the node $n-k-1$.

In the uplink process, data transmission starts after a two-way handshake. As node $n-1$ has been malfunctioning, it cannot reply the "hello" message $M_{h,0}$ from node n in the given way. Node n knows that node $n-1$ is not operating properly because there is error response or no response. So, it will generate a new "hello" message $M_{h,1} = E_{PU_{n-2}}(E_{PR_n}(hello)||n)$ and then sends it to node

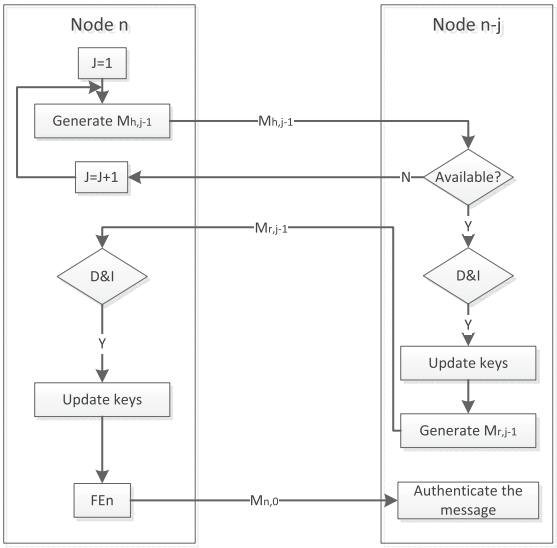

Figure 9. Self-healing process.

$n-2$. The communication can not be built until node $n-k-1$ because all the previous nodes are malfunctioning. Node $n-k-1$ decrypts the $M_{h,k} = E_{PU_{n-k-1}}(E_{PR_n}(\text{hello})\|n)$ and realizes that the "hello" message did not come from its default node $n-k$ because the ID "n" in the $M_{h,k}$. So, it will decrypt $E_{PR_n}(\text{hello})$ using PU_n stored by itself. If it finds the message is impeccable, it will update its default forward key from PU_{n-k} to PU_n and generate a new communication key $K_{n,n-k-1}$ with both PU_n and PR_{n-k-1}. Then it will reply the node n with the message $M_{r,k} = E_{PU_n}(E_{PR_{n-k-1}}(\text{response})\|(n-k-1))$. After receiving and handling $M_{r,k}$, the node n can see that the available node next to itself is node $n-k-1$, so it will update its default backward key from PU_{n-1} to PU_{n-k-1} and generate the communication key $K_{n,n-k-1}$ too, so that it does not need to inquire the malfunctioning node in every time's uplink transmission. After that, the communication continues in the new network route node n, node $n-k-1$, node $n-k-2, \ldots,$ node 1.

The similar process is applied to downlink process. If a malfunctioning node appears, we can recover the original route by doing an initial process after the malfunctioning nodes repaired. In the process, larger i in the i-neighboring public key structure makes it a more reliable system. However, in practice, because of limited transmission rage of the nodes as well as low possibility of multi-node malfunctioning occurrence, we usually apply $i = 2$ or $i = 3$ at most.

5. SECURITY ANALYSIS

The security of the proposed security relies on the actual cryptographic operations (e.g., encryption algorithms, hash functions, etc.) that are applied to the security. Without loss of generality, we assume that cryptographic operations applied are computationally secure unless corresponding keys are compromised. For simplicity, we briefly discuss the security based on the aforementioned assumption without rigorous mathematical proofs.

5.1. Security analysis of initialization process

In authentication process, the main task is to ensure the pre-installed authentication key of the unauthenticated node to be sent to the AS securely. If the newly added node is node n, we just need to establish the secure communications between node n and node $n-1$ because the network between node $n-1$ and AS is secure. We perform a handshake first as a simple sender authentication. As node n has not been authenticated by AS and it cannot ensure whether node $n-1$ has been authenticated, the given message "Request" in M_0 and "Accept" in M_1 can do little contribution for equipment authentication as these messages should be known by every legitimate DAU. We use authentication key K_n and time stamp T encrypted each other and combine them to generate the authentication message of node n, so the message cannot be forged because the K_n is just known by node n and AS. The replay attack does not work because of the time stamp T. Certainly, every message has its message authentication code C_i generated by hash operation to ensure the data integrity.

In the key distribution part, we need to accomplish the key distribution when a new node is added to the network. The conventional symmetric key based protocol does not meet the requirement of the wireless sensor monitoring network very well because each communication link of such wireless sensor monitoring network must be kept independently secure. Therefore, our proposed protocol and key structure are based on an asymmetric encryption algorithm. In order to simplify the process, after node n and node $n-1$ finishing mutual authentication with each other through the AS, then they will process the remaining tasks locally. The private key of node n and public keys of node n and its i-neighboring nodes are sent through a secure tunnel (secured with the authentication key). The entire message used in the process is encrypted with the public key of the receiver for confidentiality. The message authentication code is used in every message to provide data integrity.

5.2. Security analysis of uplink process

The sender initiates a handshake before actual data transmission for mutual authentication. The main part of uplink process is the encryption function FE_i. In this function, we aggregate the raw data with previous incoming data first to decrease the relevance of the message of every node and encrypt it with the public key of node i so that it can only be decrypted only by the DCC, which has the private key of node i (besides node i). Data integrity is protected by two operations. First, m_n is XORed with M_i and compared with M_i' to make sure that $M_n\|M_{n-1}\|...\|M_{i+1}$ is not manipulated.

Second, message authentication code C_i further authenticate the integrity of M_i'. Message authentication code is not generated for all the messages so that the overhead can be reduced for shorter delay.

5.3. Security analysis of downlink process

In the downlink process, the proposed design focuses on the efficiency while the security is guaranteed at the same time. First, message authentication code is generated by every node using its communication key, it provides data integrity and authenticates the sender. Forgery and data manipulation can hardly be achieved without knowing the communication key, which is generated by the private key of the receiver and public key of the sender. When the control command is transmitted to a specific node, confidentiality is provided by encrypting the message with the public key of the receiver.

5.4. Security analysis of self-healing process

Because of the asymmetric encryption algorithm in the proposed protocol, public keys are shared with other nodes. In this way, a node can communicate with others by distributing its public key to others, and the confidentiality is ensured as its private key is just known by the sever and itself. Furthermore, it enables the self-healing function of the network because of malfunctioning nodes. The security measure is the same as the uplink and downlink processes; it processes one more handshake after the default handshake failed and then generates a new communication by updating the key. So the security can be provided with more reliability.

6. AVAILABILITY ANALYSIS

In this section, we analyze the availability of the network with our proposed security protocol considering both energy consumption and end-to-end delay. We also show that it is practical to recover the network with a few malfunctioning nodes in many network scenarios.

6.1. Energy consumption analysis

In Table II, we list the key parameters for the ease of analysis.

Table II. Key parameters.

M	packet length after channel coding
L	data length
R	physical layer transmission data rate
γ_i	SINR of node i
p_i	transmission power of node i
$h_{i,j}$	path gain of node i at node j

SINR, signal-to-interference-plus-noise ratio

Compared with the energy consumption of data-processing such as encryption and authentication, the energy consumption of data transmission is much larger. If we choose to hop over malfunctioning nodes, the computational cost may reduce because of the reduced amount of data. Therefore, we mainly discuss the energy consumption of data transmission. Let each data packet of the proposed protocol contain L bit information. With channel coding, the total size of each packet is $M > L$ bits. The physical transmission rate is R bit/s. Considering node i, the probability of correct reception is $q(\gamma_i)$, where γ_i is the signal-to-interference-plus-noise ratio (SINR) at the receiver. Assuming that all the transmissions are statistically independent, then we have $E[n] = 1/q(\gamma_i)$. Therefore, we can get the total transmission time T_t, required for correct reception as Equation (1).

$$T_t = \frac{M}{Rq(\gamma_i)} \tag{1}$$

With the transmitted power p_i watts and the length of information L, we can find the transmitter efficiency U, which means how much Joule we need when we transmit one bit message correctly. We can also substitute the basic function of $q(\gamma_i)$ in U, and we can get the Equation (2) as [29]

$$U = \frac{Mp}{RL(1 - \mathrm{BER})^M} \tag{2}$$

where BER is the bit error rate and it is calculated from Equation (3) for our simulation with the quadrature phase-shift keying (QPSK)

$$BER = \frac{1}{2} erfc\left(\sqrt{\gamma_i/2}\right) \tag{3}$$

When we calculate γ_i, we first make an assumption that the p are identical for all nodes. Then we can get a general formulation for γ_i as

$$\gamma_i = \frac{ph_{i-1,i}}{\sigma^2 + \frac{p}{N}\sum_{j=1}^{i-1} h_{i,j}} \tag{4}$$

where N is the processing gain. For simplicity, path gain h is calculated according to free space model,

$$h = \frac{G_t G_r \lambda^2}{(4\pi)^2 d^2} \tag{5}$$

where the G_t is the gain of transmitting antenna, and the G_r is the gain of receiving antenna. The λ is wavelength, and $d = S/n$ is the distance between two neighboring nodes. We then relax Equation (4) with the assumption that noise is only from background, the interference is from node $i + 1$ and node $i + 2$ for node i, then we have

$$\gamma_i = \frac{ph_{i-1,i}}{\sigma^2 + \frac{p}{N}\left(h_{i,i+1} + h_{i,i+2}\right)} \tag{6}$$

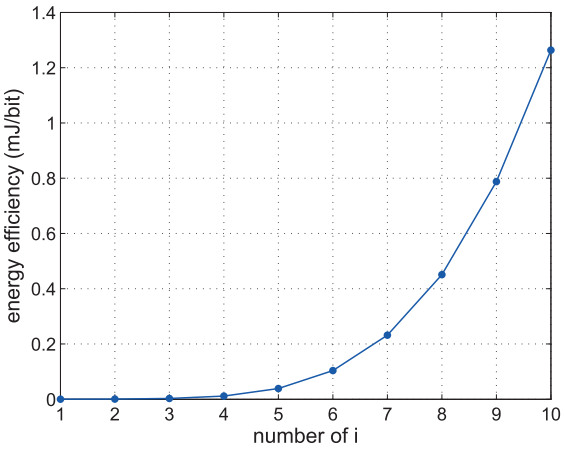

Figure 10. Energy efficiency of different i.

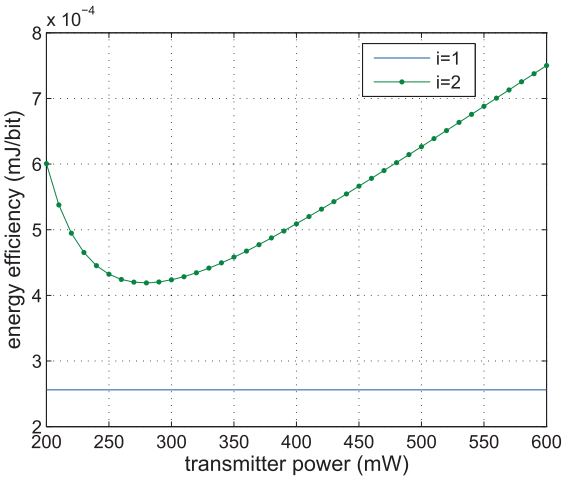

Figure 11. Energy efficiency with different p when i=1 and i=2.

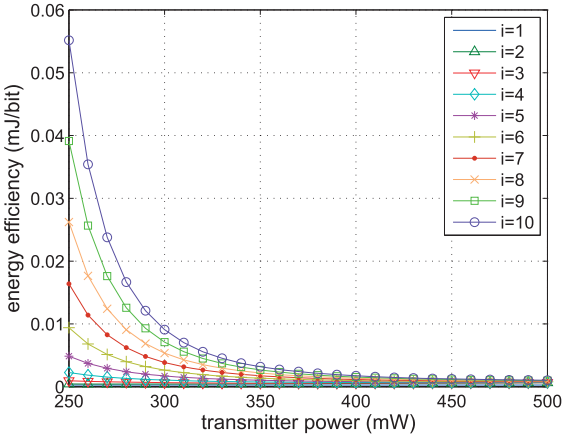

Figure 12. Energy efficiency with different p when i from 1 to 10.

After combining Equation (2) with Equation (3), Equation (5), and Equation (6), we can find the energy cost of every bit. In the original case, we assume that $N = 5$, $L = 192$, $M = 240$, $R = 10^6$ bps and $p = 200$ mW. Receiver noise power spectral density is assumed to be 10^{-21} W/Hz (which produces a noise power of $\sigma^2 = 10^{-15}$ W in a receiver with 1 MHz), transmitting antenna gain $G_t = 1$ dB, receiving antenna gain $G_r = 2$ dB, and total distance of the line $S = 20$ km with 20 nodes deployed in the network. Then we have the energy efficiency for every bit is $U = 2.5602 \times 10^{-4}$ mJ. Because of the chain topology, the node neighboring to the gateway consumes the maximum energy among all the nodes, that is, $E_t = 1.23$ mJ, which can be achieved by renewable energy (e.g., solar power).

One of the contributions of our proposed protocol is the scheme to deal with the failure of intermediate nodes by hopping over the malfunctioning nodes. We prove that the method is feasible to energy consumption. For handling the problem, we propose "*i*-neighboring nodes" public key structure. We first simulate a case for increasing *i*s from 1 to 10 when transmitter power $p = 200$ mW. the results are shown in Figure 10. We can see that the cost of energy increase a lot with i increasing. Compared with the result of the original case before, $E_t = 1.23$ mJ, and i changes to 2 (there is 1 malfunctioning intermediate node); the energy efficiency of every bit will be $U = 6.006 \times 10^{-4}$ mJ, so the maximum energy consumption of transmitting will amplify to $E_t = (20 - 1) \times 240 \times 6.006 \times 10^{-4} = 2.74$ mJ. It seems not so large but when the i is bigger, we can see a surge of energy cost. For example, when i is 7, the maximum energy cost will be more than 672 mJ. That is to say, if we use the fixed transmitter power, i cannot be arbitrarily large.

As a solution to this issue, we propose to increase the transmitter power at the node one-hop away from the malfunctioning node. In Figure 11, we take $i = 1$ and $i = 2$ as examples. The line of $i = 1$ is horizontal because there is no malfunctioning node. The line $i = 2$ is always above $i = 1$, that is to say we should spend more energy to hop over the malfunctioning node. But we can also find when $p = 280$ mW and the energy consumption for every bit can be minimum at the same time. So, the result has confirmed that we can reduce the energy cost by increasing the transmitter power. However, there is still a limit of both transmitter power and energy consumption, so that we should choose an appropriate i. To find the i, we simulate for $i = 1$ to 10 with different p, as shown in Figure 12.

Table III shows the transmitter power with minimum energy consumption and the maximum energy consumption for one node with i from 1 to 10. The maximum energy cost for each node shows that if all the malfunctioning nodes neighboring to the gateway, then we should send entire message of all remaining nodes in the wireless network to the gateway directly. When $i \leq 3$, both the transmitter power with minimum energy consumption and the maximum energy consumption for one node are less than half of the original circumstance, so the DAU can work regularly. If $i = 4$ or $i = 5$, the equipment may work in a high pressure of both transmitter power and energy consumption, which is considered as the extreme cases. When $i \geq 6$, we can see that the maximum energy consumption

Security Comm. Networks 2016; **9**:60–71 © 2015 John Wiley & Sons, Ltd.
DOI: 10.1002/sec

Table III. The minimum transmission power and maximum energy cost for one node with different i.

number of i	p with min energy cost(mW)	ratio	max energy cost for one node (mJ)	ratio
$i = 1$	200	1.00	1.23	1.00
$i = 2$	280	1.40	1.91	1.55
$i = 3$	370	1.85	2.40	1.95
$i = 4$	440	2.20	2.67	2.17
$i = 5$	480	2.40	2.79	2.27
$i = 6$	520	2.60	2.82	2.29
$i = 7$	550	2.75	2.78	2.26
$i = 8$	570	2.85	2.69	2.19
$i = 9$	590	2.95	2.57	2.09
$i = 10$	610	3.05	2.42	1.97

may decrease because of the decreasing of transmission data, but the transmitter power will increase continuously and may exceed the sustainable limit of equipment. In summary, we should utilize $i = 1$ to 3 "i-neighboring nodes" public key structure design in general and $i = 4$ or $i = 5$ in some special situation, for example, there is ample solar energy and in tough environment.

6.2. End-to-end delay analysis

As we use asymmetric encryption algorithm, the data processing delay may be large. So we should consider the delay of data processing and transmission at the same time. In Equation (1), we have calculated the transmission time for one node. Now, we assume that the first q nodes in a total of 20 nodes are functional and others are malfunctioning, we can get the maximum value of the transmission delay for different i. It is easy to find that the first q–1 nodes have the same delay for one packet, T_{t1} and the transmission time for one packet of node q is T_{t2} ($T_{t1} = T_{t2}$ when $i = 1$). The delay of data process T_p is the same for every node, and we can get $q = 21 - i$ easily. So the total delay T can be expressed as

$$T = \frac{(21-i)(20-i)}{2} T_{t1} + (21-i)T_{t2} + (21-i)T_p \qquad (7)$$

$T_{t1} = 0.25$ ms can be found based on the settings. T_{t2} is calculated as a function of i with the parameters and results in 5.1. For T_p, in our proposed security protocol, we select the Rivest-Shamir-Adleman (RSA) algorithm for encryption, which has the key length of 1024 bits and MD5 to generate the message authentication code. From [21] and [30], we see that the processing time of RSA and MD5 is 1.65 ms/Byte and 0.11 μs/Byte respectively. So, $T_p = 192/8 \times (1.65 + 0.11 \times 10^{-3}) \simeq 39.6$ ms is also a fixed value. We can get the total delay T with variable i, as shown in Figure 13. In this figure, we can find that the delay will decrease when the i increases because of the slow traditional RSA algorithm. More malfunctioning nodes also indicate that less encryption is processed.

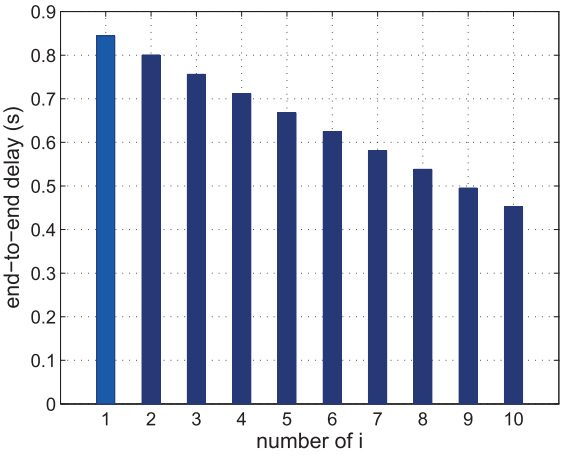

Figure 13. End-to-end delay with different i.

7. CONCLUSIONS

In this paper, we proposed a security protocol for a wireless sensor network that monitors transmission lines in smart grid. The proposed protocol provides authentication for equipment and data, message encryption for uplink transmission, and command encryption for downlink transmission. We also proposed an "i-neighboring nodes" public key structure and using asymmetric algorithm to make the network more adaptive. The new protocol is adaptive to the network change so that a new sensor node can be added at anytime. Moreover, we proposed a self-healing process using "i-neighboring nodes" public key structure for the sensor network to maintain network connectivity when there are some malfunctioning nodes. We further conducted security analysis to show how the proposed protocol protect the wireless sensor network in every step. We also analyzed the energy consumption and end-to-end delay. The results showed that our protocol would enhance the reliability of the wireless sensor monitoring network when choosing appropriate i with "i-neighboring nodes". The end-to-end delay simulation results showed us that we may further decrease the end-to-end delay by hopping over some nodes on purpose.

ACKNOWLEDGEMENTS

This work was supported by 863 Program under Grant No. 2012AA050802 and China Electric Power Research Institute Research Program No.XXN17201300084.

REFERENCES

1. Yan Y, Qian Y, Sharif H, Tipper D. *A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges*, Vol. 15, 2013.
2. Ye F, Qian Y, Hu RQ. Energy efficient self-sustaining wireless neighborhood area network design for smart grid. *IEEE Transactions on Smart Grid* 2015; **6** (1): 220–229.
3. Jokar P, Arianpoo N, Leung VCM. A survey on security issues in smart grids. *Security Comm. Networks*, DOI: 10.1002/sec.559.
4. Ye F, Qian Y, Hu R. A real-time information based demand-side management system in smart grid. *IEEE Transactions on Parallel and Distributed Systems*, DOI: 10.1109/TPDS.2015.2403833.
5. Yan Y, Qian Y, Sharif H, Tipper D. *A Survey on Cyber Security for Smart Grid Communications*, Vol. 14, 2012.
6. Ebrahimi MS, Daraei MH, Behzadan V, Khajooeizadeh A, Behrostaghi SA, Tajvidi M. A novel utilization of cluster-tree wireless sensor networks for situation awareness in smart grids, *Innovative Smart Grid Technologies Asia (ISGT)*, 2011; 1–5.
7. Jia D, Meng X, Song X. Study on technology system of self-healing control in smart distribution grid. *Advanced Power System Automation and Protection* 2011: 26–30.
8. Gungor VC, Bin Lu, Hancke GP. Opportunities and challenges of wireless sensor networks in smart grid. *IEEE Transactions on Industrial Electronics* 2010; **57**(10): 3557–3564.
9. U.S. Department of Energy. (Available: www.oe.energy.gov) [Accessed on 26 April 2015].
10. Ye F, Qian Y, Hu RQ, Das SK. Reliable energy-efficient uplink transmission for neighborhood area networks in smart grid. *Smart Grid, IEEE Transactions on* 2015; **6**(5): 2179–2188.
11. Luan W. Advanced metering infrastructure. *Southern Power System Technology* 2009: 6–10.
12. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, Office of the National Coordinator for Smart Grid Interoperability, January 2010.
13. Nishimura F, Cicarelli LD, Arellano RR, Soares MR. OPGW Installation in Energized Transmission Line, *IEEE TDC '06*, August 15-18, 2006; 1–8.
14. Ali SA, Alvi BA, Asif M. OPGW - our experience in KESC, *IEEE Canda Electric Power Conference*, October 6-7, 2008; 1–6.
15. Kayastha N, Niyato D, Hossain E, Han Z. Smart grid sensor data collection, communication, and networking: a tutorial. *Wireless Communications and Mobile Computing* 2014; **14**(11): 1055–1087.
16. Lin J, Zhu B, Zeng P, Liang W, Yu H, Xiao Y. Monitoring power transmission lines using a wireless sensor network. *Wireless Communications and Mobile Computing* 2015; **15**: 1799–1821, DOI: 10.1002/wcm.2458.
17. Gungor VC, Lu B, Hancke GP. Opportunities and challenges of wireless sensor networks in smart grid. *IEEE Transactions on Industrial Electronics* 2010; **57**(10): 3557–3564.
18. Erol-Kantarci M, Mouftah HT. Wireless sensor networks for cost-efficient residential energy management in the smart grid. *IEEE Transactions on Smart Grid* 2011; **2**(2): 314–325.
19. Gungor VC, Sahin D, Kocak T, Ergut S, Buccella C, Cecati C, Hancke GP. Smart grid technologies: communication technologies and standards. *IEEE Transactions on Industrial Informatics* 2011; **7**(4): 529–539.
20. Guo Z, Ye F, Guo J, Liang Y, Xu G, Zhang X, Qian Y. A wireless sensor network for monitoring smart grid transmission lines, *IEEE International Conference on Computer Communication and Networks (ICCCN)*, Shanghai, China, 2014; 1–6.
21. Fan S, Ye F, Guo J, Liang Y, Xu G, Zhang X, Qian Y. A security protocol for wireless sensor networks designed for monitoring smart grid transmission lines, *IEEE International Conference on Computer Communication and Networks(ICCCN)*, Shanghai, China, 2014; 529–535.
22. Ye F, Qian Y, Hu RQ. A security protocol for advanced metering infrastructure in smart grid, *IEEE GLOBECOM'14*, Austin, December 2014; 649–654.
23. Xiao S. Consideration of technology for constructing chinese smart grid. *Automation of Electric Power Systems* 2009; **8**(1): 18–28.
24. Li J. Analysis on strategic significance of construction and development of smart grid in china. *Journal of Changjiang Engineering Vocational College* 2011; **8**(1): 18–28.
25. Zhou J, Hu RQ, Qian Y. Scalable distributed communication architectures to support advanced metering infrastructure in smart grid. *IEEE Transactions on Parallel and Distributed Systems* 2012; **23**(9): 1632–1642.
26. Lijia R, Hong L, Yan L. On-line monitoring and prediction for transmission line sag. *International*

Conference on Condition Monitoring and Diagnosis (CMD) 2012: 813–817.
27. Huang X, Wei X. A new on-line monitoring technology of transmission line conductor icing. *International Conference on Condition Monitoring and Diagnosis (CMD)* 2012: 581–585.
28. Sun XX, Lui KK, Wong K, Lee W, Hou Y, Huang Q, Pong P. Novel application of magnetoresistive sensors for high-voltage transmission-line monitoring. *IEEE Transactions on Magnetics* 2011; **47**(10): 2608–2611.
29. Goodman D, Mandayam N. Power control for wireless data. *Personal Communications IEEE* 2000; **9**: 48–54.
30. Fan W, Chen X, Li X. Parallelization of RSA algorithm based on compute unified device architecture. *Grid and Cooperative Computing (GCC)* 2010: 174–178.