*Sensors & Transducers, Vol. 23, Special Issue, July 2013, pp. 15-20*

www.sensorsportal.com

**Sensors & Transducers**



*http://www.sensorsportal.com*

# Analysis on Network Security Protocol of Passive Wireless Sensor in Power System

**[1] Chao Zhao, [2] Ying Han**

[1] School of Computer Science of Henan Business College, Beinong Rd., Huilongguan, Changping District, Beijing, 102206, China

[2] School of Economics and Management of North China Electric Power University, Beinong Rd., Huilongguan, Changping District, Beijing, 102206, China

[1] Tel.: +8613910885685, fax: +8613910885685

[1] E-mail: hanying19900915@163.com

*Received: 20 May 2013 /Accepted: 19 July 2013 /Published: 30 July 2013*

**Abstract:** As a new technology for information gathering and processing, the role that wireless sensor network played in the field of current computer cannot be replaced. It integrates the advantages of sensor technology, communication technology and computer technology into an organic whole and it has great potential and development space. Accordingly, its security problem also becomes the primary consideration objects. It is the key to solve the problem of wireless sensor network in the power system security that if people can design the security protocols suitable for power system. In this paper, we designed the system consistent with the security agreement according to related standard of security requirements, meanwhile we also made a detailed analysis in multiple aspects. *Copyright © 2013 IFSA*

**Keywords:** Power system, Wireless sensor networks, Security protocol.

## 1. Introduction

Wireless sensor networks as a new network technology, with its low cost, low power consumption and flexible networking and easy to deploy advantages are widely used in military, medical, industrial, agriculture and other fields. It is the basic composition unit of a node in the power system applications in the field, according to different ability of nodes, wireless sensor network can be divided into active and passive network two kinds of networks. The former is mainly used in smart home, smart metering and other important electrical equipment condition monitoring and other fields, the latter is mainly used for fault location grid and electrical equipment monitoring and disaster monitoring, etc [1]. Compared with the active network, passive network has the following characteristics: resource-constrained nodes, deployment environment without regulation, limited battery power, the smaller the amount of data transmission, equipment maintenance difficulties, low frequency acquisition. These characteristics are also disadvantages, resulting in passive wireless sensors can easily be malicious control, channel interference, physical capture attacks, in order to prevent these attacks, if the safety protection of operation table is complex, there may be two problems:

- First, electricity and resources are a large consumption of nodes and network life is reduced;
- Second, network deployment costs and complexity increase, and even some application scenarios can not be used for security deployment.

So, the design of an effective, feasible and scientifically sound passive wireless sensor network security protocol quite challenging.

## 2. Passive Wireless Sensor Network Security Needs

Taking into account the limited capacity of the wireless sensor network communications, computing capacity is limited, finite supply of energy, perception data volume, etc, it should have the following security requirements [2].

### 2.1. Data Confidentiality

Sensor networks can not perceive information leakage to neighboring network, especially highly confidential data, in order to protect the confidentiality of data, the standard method is generally used to encrypt the data using the key, and the recipient can decrypt the data, in order to achieve confidentiality sex - the need to establish a secure channel between each nodes.

### 2.2. Data Authentication

Message Authentication multi-sensor networks have become crucial for most applications in the process of building a network, authentication is an essential management tasks. Whereas some insecurity easily insert information, the receiver needs to ensure the accuracy of the data sources, data authentication allows the receivers to send data for validation.

If two entities communicate, can achieve data using symmetric mechanisms for authentication purposes: communication data message authentication code, the sender and receiver share a secret key is evaluated. When the data with the correct authentication code is sent, the recipient can quickly and easily reception.

### 2.3. Data Integrity

Data integrity can protect data during transmission will not be changed, data authentication can be achieved using the data integrity.

### 2.4. Data in Real Time

Sensor network measured data are closely related to time, confidentiality and authentication may be difficult to guarantee, but time must be determined in real time. There are two types of real-time: the strong real-time and the weak real-time, the former provide for the complete order, you can delay prediction, commonly used in network time synchronization; the latter provides only partial information order, but does not carry any delay information, used for sensing measurements.

### 2.5. Key Management

To meet above requirements, the encryption key should be managed. As the wireless sensor network energy and computing power has limits, need to maintain the relationship between the security level and limits.

## 3. Security Protocol Design

### 3.1. Security Services

#### 3.1.1. Key Management

The current key management mechanisms are four types, the first is key pre-distribution, the second is key management which is based on trusted key distribution center, the third is dynamic key management mechanism, the forth is key management which is based on public key physical. Among them, the key pre-distribution mechanism is not only an ideal choice, more suitable for application in the passive wireless sensor network. Present key pre distribution mechanism mainly include sharing key distribution, key distribution based on location information, polynomial key distribution, key distribution and so on, Table 2 refers to the storage, computing, security, scalability and communication overhead and other performance indicators for more than a few key distribution protocol were compared. Table 1 is a description of the relevant symbol.

From the table that, in the power system of passive wireless sensor networks, the shared key distribution is the best choice for the following reasons: the Shared secret key distribution of low power consumption, long life can be maintained network; shared key distribution with good connectivity and scalability to meet the network topology and stability characteristics, to meet the needs of its information collection; shared key assignment in program maintenance and replacement of nodes is relatively simplified; shared key distribution to facilitate saving equipment manufacturers large-scale production.

Shared key distribution protocol Notwithstanding the above advantages, but it is less secure, if the initial shared key is stolen by an attacker, the others can be achieved by any means of attack, its consequences and losses are not envisaged. On this basis, this paper designed a highly secure key management mechanism, set up a new management mechanism are three types of 128 bit key lengths, respectively is: the initial key, global key and session key.

**Table 1.** Symbol description.

| Key | Value |
|---|---|
| K | Global key |
| $K_i$ | Initial key |
| $K_n$ | Session key |
| S | Sponsor identification |
| R | Responsor identification |
| E | Encryption Algorithm |
| Token | Token |
| MAC | Message Authentication Code |
| MIC | Message Integrity Code |
| Random | Random |

**Table 2.** Comparison of key pre-distribution scheme.

| | Conne-ctivity | Mem-ory Cost | Proces-sing Cost | Commu-nication Cost | Secu-rity |
|---|---|---|---|---|---|
| Key sharing | ↑ | ↓ | ↓ | ↓ | ↓ |
| Poly-nomial | ↑ | - | - | ↓ | ↓ |
| Key pool | ↓ | ↑ | ↑ | ↑ | - |
| Polynom-ial pool | ↓ | ↑ | ↑ | ↑ | - |
| Location-based info | - | ↑ | ↑ | - | ↑ |

One. Initial key Ki: all played key nodes for network connectivity as well as the early deployment of new network node device authentication; when the end of the initial deployment, it will save only the initial key Gathering node, the backbone node or sensor node the key will be deleted.

Two. Global key K: this is a whole network shared key generated by the Gathering node, mainly used to identify the network periodically entity in the process of running. At the beginning of network deployment, the global key and initial key agreement.

Three. Session key $K_n$: This equipment is mainly used for network communications security and protection of the equipment at the end of the entity arising after identification [3].

### 3.1.2. Entity Authentication and Session Key Generation

To ensure safe and correct manner node can access the network, reducing the number of the sender and the receiver information interaction, in this paper, the entity is in a double identification mechanism (Fig. 1) on the basis of, the specific steps are as follows:

Step 1. R sending a Random number of Random.

Step 2. S generates a random number of Randoms, then generates Token SR, and sent to R.

Step 3. R to receive the information, decrypts the Token SR, and identifies the correctness of the response side, inspection Random g and the decrypted random number are the same, at the same time get a random number Random.

Step 4. R generates and sends to S.

Step 5. S receives the information transmitted sent by R, decrypting inspection steps are as Step 3.


**Fig. 1.** Diagram of two-way differential mechanism.

Identification of the physical end of the process, the initiator and the responder will combine global key and processes the random number, and 64-bit long address, the session key generated by key generation algorithm, the process shown in Fig. 2.

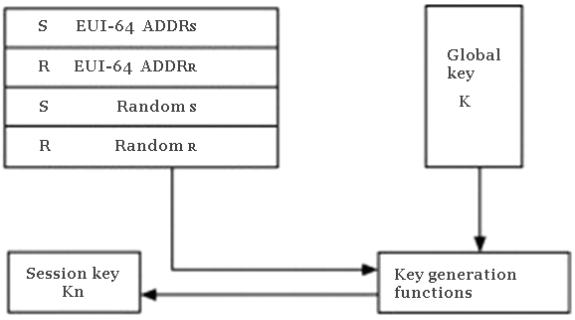


**Fig. 2.** Generating processing of session key.

### 3.1.3. Access Control

Because the ability of sensor nodes and limited battery life, network security services should be archived by strong ability Gathering nodes and backbone nodes, access control services, too, should be set up by the gathering node and backbone nodes and detect maintain dynamic access control list, access control to accomplish the communication between the nodes, the steps are as follows:

The first step: The node do a good job with the adjacent node network access authentication and network certification cycle entity identification;

The second step: The node save the address of the secure connection, and on this basis to create access control lists;

The third step: In the list of update cycle, the node records the number of times which have been successfully received for same message sent by a secure connection;

If more than 3 times, and the node is removed from the list, return to the second step; If not more

than or just 3 times, will continue to maintain the original list.

### 3.1.4. Message Authentication and Integrity Protection

Existing protocol, message authentication and integrity protection often through the message integrity code or a hash function calculates message authentication code two modes, to identify sources of information and protect information is not destroyed by malicious tampering or deletion. To reduce the storage space, WIA - PA, 6 6LowPAN and ZigBee using AES encryption algorithm in CBC mode for calculation for the MIC so as to better protect and promote the integrity of the message authentication. In addition, in order to resist replay attacks, 6LowPAN and ZigBee using the counter value added calculation method to achieve MIC, and WIA-PA is accomplished through the application layer time stamp MIC calculations.

This protocol also uses counter value to Calculate MIC, to achieve message authentication, integrity, and anti-replay protection [4].

### 3.1.5. Confidentiality Protection

Confidentiality protection is the most basic security protocol security mechanisms. In general, it can be encryption algorithm to encrypt data directly, in order to prevent an attacker after listening to the same message repeatedly can guess its contents, wireless sensor networks have semantic security needs, to meet this demand, this agreement with SPINS protocol mechanism, i.e. in the process of data encryption combined with calculator values encrypted file.

## 3.2. Security Processes

### 3.2.1. Network Certification

Network access authentication is to implement security access networks between nodes of a security process, Fig. 3 is the basic flow, start the process has the following three types.

The first type: the initial network deployment, Gathering nodes and backbone nodes, sensor nodes and adjacent backbone nodes, the backbone nodes and backbone nodes execute point-to-point communications between access authentication process, to create the establishment of a secure network connection.

The second type: a new node joins the network in the network operation phase.

Since only gathering node contains the initial key, if the new node is the sensing node, then carries on the convergence between the node and sensor node authentication, backbone nodes in this process mainly responsible for the forwarding of authentication information.

If the new node is the backbone nodes, perform backbone nodes and the adjacent backbone nodes or point to point communication between the sink node authentication, and then carry out the adjacent sensor nodes and backbone nodes in the network access authentication.

If the new node is a gathering node, then re-run the network's initial deployment network certification process.

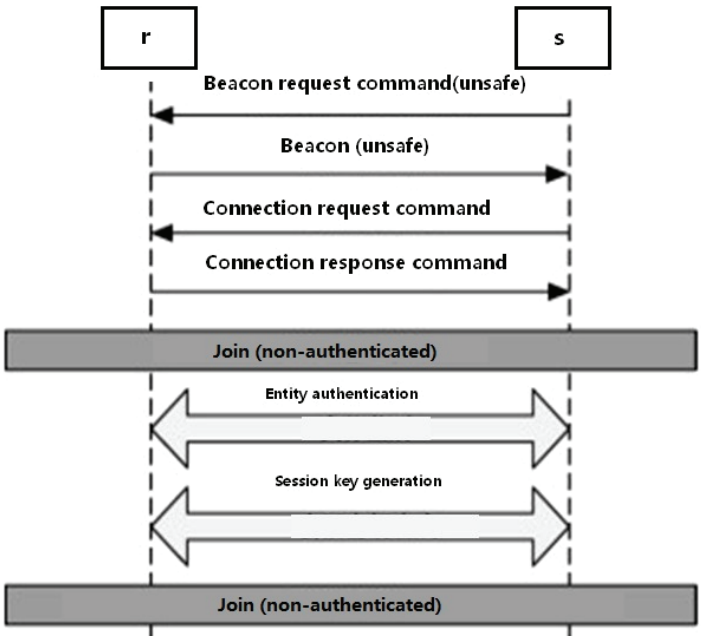


**Fig. 3.** Processing diagram of Restarting the authentication.

The last type: Backbone nodes in the network operation phase failure.

Establish communication with failure of the backbone nodes there are two possible, one sensor node, the second is the backbone nodes, when either send access request to gather around one of the adjacent node or backbone nodes, you need to restart the network authentication process.

### 3.2.2. The Key to Update

Key update process is mainly responsible for the session key and global key update cancellation protection, session key can use entity identification or session key generated complete update services directly, but a global key link must be on the high security of key distribution process can be achieved in the update, the steps are as follows:

Step 1: Gathering node synchronization time information through the system, or by virtue of the locally generated random number to generate a new global key;

Step 2: The distribution of the process, the nodes on the basis of the original session key update data in the process of implementation of message authentication and integrity protection to ensure the three cases (the sink node and the backbone, the backbone nodes and sensor node, the backbone nodes) the safety of point-to-point communication link, and session key between nodes on the basis of existing good key update process confidential data frame static load protection, to prevent leakage global key information.

Step 3: Sensor nodes or backbone node to receive the updated data frames, and verify that the MAC value of the data frame. If validation passes, the new global key will be saved, and continue to follow the second step backbone nodes to the adjacent sensor nodes or backbone nodes forward global key information. If the validation synchronization is not pass. Directly discards the data frame.

Step 4: Success for a new global key nodes, restart authentication process (as shown in Fig. 3), so as to realize the update of the session key between nodes [5].

### 3.2.3. Unicast Safe Handling

Unicast security processing is based on the node type and topology characteristics, select data encryption, message authentication and integrity protection process of security services such as security.

In view of the topology of the wireless sensor, this paper divided unicast communication into uplink and downlink communication two kinds [6]. The former mainly refers to the sensor nodes send backbone nodes to gather information and backbone node sends information, responsible for collecting information. In contrast with the former, the latter is responsible for network control signaling. Control information and device configuration.

The importance according to the status information acquisition, the sensor can be divided into two categories: one is ordinary nodes, is mainly responsible for the low sensitivity of the information, low change frequency information collection work, making no significant impact on the main battle. The second is an important node in the special features, mainly be responsible for the information as well as changes in the sensitivity and accuracy of the higher frequency of information collection work.

### 3.2.4. Broadcast Authentication

Broadcast authentication process is to ensure that a node to another node initiates the authentication process when the broadcast communication. Currently, most wireless sensor network broadcast authentication protocol design is based on μTESLA protocol [7]. μTESLA requires t the hash function, relaxation time synchronization and single-phase key chain combination, to ensure efficient broadcast authentication, and therefore requires a lot of power and storage space for single-phase key chain store or hash function calculation operation. For passive wireless sensor, μTESLA has a great affect on those nodes that resources and energy are limited, and even reduce network lifetime.

Given that only backbone nodes and aggregation nodes can send broadcast messages, wireless sensor network can be divided into passive two points: First, the backbone nodes to the gathering node broadcasts, the second is the backbone of sensor nodes to the cluster nodes broadcasts.

## 4. Conclusion

Wireless sensor networks are more and more widely used, but due to its inherent characteristics, security is also more and more important [8]. In this paper we designed four processes (network access authentication, key management, secure data processing, broadcast authentication), five security services (key principle, entity identification and session key generated, access control, message authentication and integrity protection, confidentiality protection), through the analysis, this article protocol conforms to the standard, to achieve confidentiality, integrity, availability, non-repudiation, and at the same time also can reduce cost, reduce the network deployment, it could be lay the foundation for further research in the future.

## References

[1]. S. Yangzhuo Jing, Sun Hongzhi, Renchen Hong, Wireless sensor network application technology

overview, *China Science and Technology Information*, Vol. 27, Issue 13, 2010, pp. 109-111.
[2]. S. Jianjun Zhu, Zhixi Wang, Wireless sensor network security protocol analysis, *Yulin Normal University*, Vol. 38, Issue 3, 2006, pp. 207-208.
[3]. S. Wenji Hu, Mingwei Xu, Secure routing protocol for wireless sensor analysis, *Beijing University of Posts and Telecommunications*, Vol. 34, Issue S1, 2006, pp. 189-190.
[4]. S. Junmo Xiao, Wireless sensor network security research, *Military Communications Technology,* Vol. 56, Issue 1, 2008, pp. 101-103.
[5]. S. Zhangzhi Tian, MIWI wireless network protocol implemented and applied research, *Journal of Changsha University*, Vol. 36, Issue 5, 2008, pp. 154-155.
[6]. S. Andong Wang, Fangdan Zhang, etc., Wireless sensor network security protocol research, *Computer Engineering*, Vol. 43, Issue 25, 2005, pp. 176-177.
[7]. S. Wenliang Zhang, Zhuangzhi Liu, Mingjun Wang, Smart grid research progress and development trend, *Power System Technology*, Vol. 33, Issue 13, 2009, pp. 210-211.