Content of smart wireless sensor network security and its network security policy

Xiehua Yu*

Minnan Science and Technology Institute, Fujian Normal University, Fujian, 362332, China

Received 1 October 2014, www.cmnt.lv

Abstract

Wireless sensor network is generally composed by plenty of micro-sensors that arranged on designated area. The supervision of these sensor nodes is used to finish the collecting, disposing and uploading of vast information. However, the security of wireless sensor network has many problems, since the sensor node itself exists plenty of limitation. Aiming at the problems of smart wireless sensor network security as well as the analysis of wireless sensor network node easy been attacked, wiretapped and forged without safeguard, this paper put forward a security policy of smart wireless sensor network. Simple and useful intrusion detection policy was realized from a series of improvement of LEACH protocol of low-energy self-adaptation cluster routing protocol.

Keywords: Smart wireless sensor network security, secure routing, key management, intrusion detection

1 Introduction

According to characteristics of limited self resource, poor computing power and small storage space of wireless sensor network, this paper put forward a security policy of smart wireless sensor network. Through the improvement of LEACH protocol of low-energy self-adaptation cluster routing protocol, and the requirement of low-energy and real-time needed for intrusion detection of wireless sensor network, it also put forward whole network cooperated intrusion detection policy. Low–energy and real-time intrusion detection policy is realized by effectively using base station energy and setting up dynamic parameter.

2 Introduction of Wireless Sensor Network

Wireless sensor network technology is an inter-discipline, which involves in many fields, like computer, micro-electronics, sensor, network, communication, signal processing, etc. With the development of many relevant new technologies, this technology is also rapidly booming [1]. Sensor node is made up of data acquisition module, data processing module, data communication module and energy supply module [2], as shown in Figure 1. Data acquisition module is used for monitoring the collection of information within formulation range and the transformation of information data. Data processing module is used for controlling the disposal operation, routing protocol, synchronization, location, energy management, task management and data infusion of all nodes. Data communication module is used for node to collect data and transmit data. Energy supply module provides the needed energy for the above three modules.

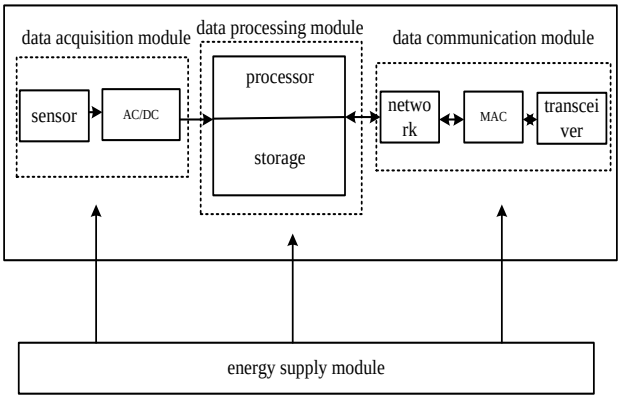

FIGURE 1 Architecture of sensor node

Structure of wireless sensor network is shown in Figure 2 [3]. Wireless sensor network is the newly developing network, which consists of many sensors, reactors and base stations. It finishes the corresponding reaction task and distribution induction with the cooperation of infinite medium. Such kind of wireless sensing actor network must be extensively used in society [4].

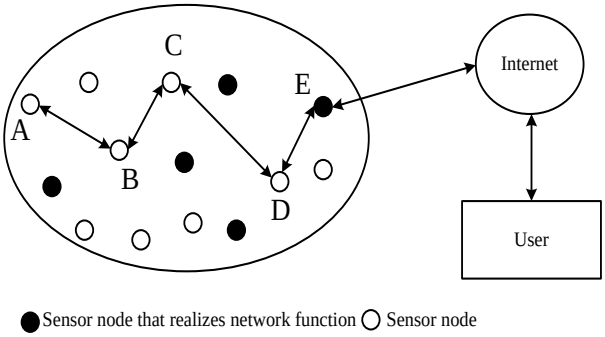

FIGURE 2 Architecture of wireless sensor network system

* ***Corresponding author*** e-mail: yxhxieh@163.com

3 Contents of wireless sensor network security and its technologies

3.1 SECURE ROUTING

The routing algorithms of wireless sensor network are mainly put forward based on characteristics of network itself and energy problems. However, these routing algorithms are not taking security issue into consideration. In order to solve problems like network failure caused by misuse of routing protocol, insecure information transmission, etc, this paper will put forward a safe and reliable routing protocol. Generally, routing security protocol is designed from two large aspects: aspects of message encryption, intrusion detection, identity authentication, etc; the application of multiple path transmissions for providing reliable transmission path.

3.2 KEY MANAGEMENT

Based on wireless sensor key management, the authentication mechanism, confidentiality mechanism, integrity, usability, secure routing, secure localization, etc of wireless sensor network are guaranteed. Key managements based on deployment knowledge, multipath reinforce key, random key and non-symmetric cryptography algorithm are all currently common key management plans [5].

3.3 CRYPTOLOGY

The characteristic of limited energy of wireless sensor network itself will be the main problem of cryptology of wireless sensor network. Low-energy and light weight key algorithm is the characteristic of self-organizing network. More security mechanisms of wireless sensor network are designed based on the key algorithm of wireless sensor network. Many scholars are trying to effectively use public key algorithm on wireless sensor node. With the improvement of technology and the development of wireless sensor technology, the previously not utilized key algorithms begin to be widely accepted and used in wireless sensor network.

3.4 AUTHENTICATION TECHNOLOGY

The authentication technology of wireless sensor network is made up of entity authentication and message authentication. Entity authentication refers to identify user status through method of key management. E-G algorithm and LeaP algorithm are the main representatives of authentication protocol of symmetric key, which are based on the authentication of symmetric cryptography and authentication of identity key mechanism. TinyPk authentication plan is the main representative of the authentication of identity key mechanism. μTESLA protocol is the main protocol of message authentication, of which the function is the guarantee that message is not been forged or falsified [6].

3.5 INTRUSION DETECTION TECHNOLOGY

Intrusion detection includes two kinds of detection models: anomaly detection and misuse detection. The process of intrusion detection is divided into three parts: information collection, information analysis and result processing. Wireless sensor network is subject to be larger intruded, since wireless sensor is generally located in the easily intrusive environment and resource is limited. Intrusion detection is also just emerging. The current intrusion detection technology based on active defense cannot be realized because of the characteristics of wireless sensor itself. Currently, traditional intrusion detection technology cannot apply to wireless sensor network [7].

4 Security Policy of Smart Wireless Sensor Network

4.1 SECURITY POLICY MODEL OF SMART WIRELESS SENSOR NETWORK

Based on the relay node routing protocol of smart energy detection, this model put forward efficient group secrete protocol encryption communication of smart identity authentication matched with it based on cluster structure. In addition, it also added the intrusion detection plan based on smart intrusion detection recognition. This security policy model of wireless sensor network integrated the network security technology of these three aspects together, thus to make this network security policy model more comprehensive, safe and reliable. The model structure is shown in Figure 3.

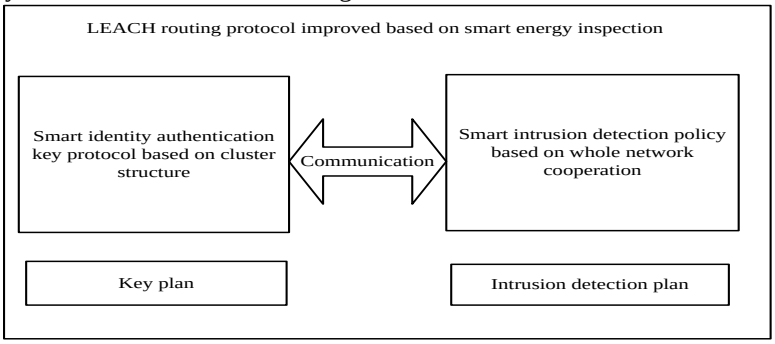

FIGURE 3 Security policy model of smart wireless sensor network

4.2 LEACH ROUTING PROTOCOL IMPROVED BASED ON SMART ENERGY INSPECTION

Routing protocol of wireless sensor network is the carrier of whole network communication, which determines the energy consumption of wireless sensor network and security of network. The current common sensor network routing protocols are all wireless routing protocol. The characteristics of wireless sensor network are greatly different from those of wireless network, thus a more appropriate routing protocol is needed.

The application of this protocol to wireless sensor network may cause the network paralysis with exhausted energy, since LEACH routing protocol consumes large energy on cluster head node. The primarily solved problem is energy consumption that the application of this protocol is needed. This paper put forward the improvement plan based on the routing protocol of smart energy inspection transmission relay mode. Its main content is to set up a relay node and sensor node, which locate on designated detection area. This relay node serves as transit of communication between cluster head node that far away from base station and base station, and it also reveal itself independently in the whole network. This protocol has a kind of smart detection mechanism, and all nodes are equipped with voltage and current detection ability (including relay node). As shown in Figure 4.

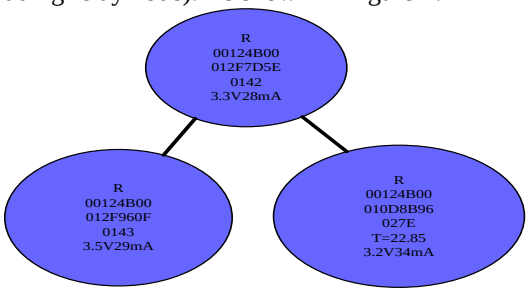

FIGURE 4 Communication mode of wireless sensor

Relay node will detect and record data of cluster head at fixed time. When it detects that cluster head node has little energy, then it will select another node with more energy as cluster head, which will effectively solve problem of energy exhaust of cluster head node. In addition, an independent relay node is established to decrease the intrusion degree of node after been intruded.

4.3 SMART IDENTITY AUTHENTICATION EFFICIENT GROUP KEY AGREEMENT PROTOCOL MODEL BASED ON CLUSTER STRUCTURE

Key management protocol plays an important role in secure communication of sensor. It is responsible for the management task of key, for the development of wireless sensor network also needs larger guarantee for network security. In addition, the application of group key protocol in wireless sensor network has strong reliability. The calculated amount, communication traffic and security of group key agreement protocol also meet the characteristics of wireless sensor network. However, the group key agreement protocol proposed by Burmester and Desmedt (or BD protocol) needs only two round of communication, and its calculated amount is small. BD protocol can resist passive attack brought by the wiretap of external node, but it cannot resist attack from internal node. Based on the above analysis, the application of BD protocol in wireless sensor network is feasible. As for the characteristics of not able to resist internal node attack, this paper put forward a kind of group key agreement protocol of logical key hierarchy in hierarchical structure through the improvement of BD protocol [8].

4.4 SMART INTRUSION DETECTION POLICY MODEL BASED ON WHOLE NETWORK COOPERATION

General intrusion detection model cannot adapt to wireless sensor network, since wireless sensor network have the characteristics of small calculated amount. A da Silva, et al put forward distributed wireless sensor network intrusion detection system, which has synthesized anomaly detection and misuse detection. These two models conducted feature library contrast on attack in network and analysed abnormal data through cooperative work, then found new intrusion feature [9]. These models provided integrated intrusion detection plan, but the plan consumed more energy. Based on the improvement of distributed wireless sensor network intrusion detection model, this paper put forward the intrusion detection plan that suit to cluster wireless sensor network model. Base station implemented complex analysis and detection algorithm through each cluster head node and terminal node. The communication method among nodes was provided through the secure routing protocol of wireless sensor network. At the same time, a simple and lo-energy algorithm was also set up based on intrusion feature comparison for cluster head node as small-scale communication network rendezvous point.

4.5 OVERALL WORKING MODE OF POLICY MODEL

The security policy of wireless sensor network is integrated security architecture. Taking the improved LEACH routing protocol as carrier, an information transmission path is provided for data that need to be send through the networking and information transmission protocol provided for routing protocol, thus to transmit information. In the process of information transmission for routing protocol, key agreement protocol of smart identity authentication and smart intrusion detection policy of whole network cooperation were added to guarantee the security of information transmission, which provided a low-energy security plan of secure transmission for whole information transmission based on smart identity authentication, encryption and decryption of information and smart intrusion detection policy of nodes. The main procedure is shown in Figure 5.

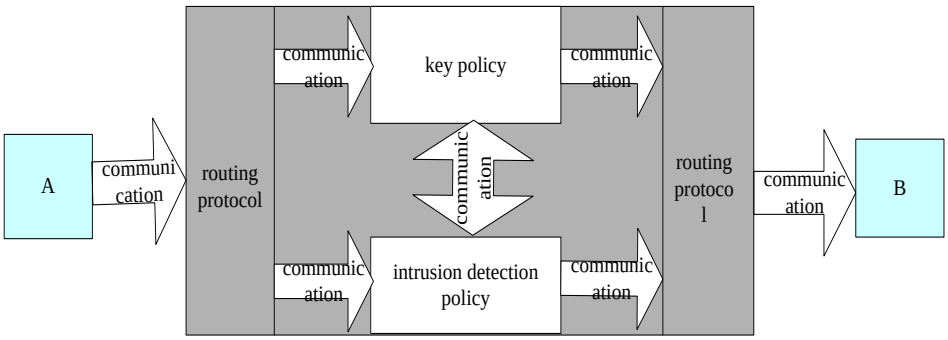

FIGURE 5 Diagrammatic figure of the overall working mode of policy model

5 Implementation of smart wireless sensor network security policy

5.1 IMPLEMENTATION OF LEACH ROUTING PROTOCOL IMPROVED BASED ON SMART ENERGY INSPECTION

According to the analysis and thought of routing protocol based on the relay mode of smart energy inspection, the idea in this paper was realized and verified through experiment and design. Therefore, node was considered based on routing protocol of smart detection relay node. In order to realize the protocol, we also need to provide feasible hardware and interface design plan. The component of wireless sensor are mostly made up of hardware, thus the most of application protocols also need the support of bottom hardware. The analysis was on the need of application layer of network, other communication network layer and physical layer and data link layer that supply hardware support. In addition, communication requirement was also analysed, since communication of protocol has many modules. The primary programming mode of design aid software based on Zigbee protocol was C procedure. Each communication module defines the corresponding function.

5.2 SMART IDENTITY AUTHENTICATION GROUP KEY AGREEMENT PROTOCOL BASED ON CLUSTER STRUCTURE

Burmester and Desmedt put forward the efficient key agreement protocol that only needs two wheel communication processes (BD protocol) [10]. However, this protocol is a non-authenticated group key agreement protocol, which cannot provide authentication function. Zheng Minghui [8] put forward the improved function that added message authentication, which proved the security of protocol under ROM. The identity authentication group key agreement protocol based on cluster structure applied BD protocol that has authentication function to wireless sensor network, which has improved the existing problem of protocol itself. At the same time, it also met the low-energy requirement of wireless sensor network. The requirement of small calculated amount and storage space has met the requirement of wireless sensor network security on data security and node security.

5.3 IMPLEMENTATION OF SMART INTRUSION DETECTION POLICY BASED ON WHOLE NETWORK COOPERATION

Based on smart intrusion detection model, the provided methods for model was analysed and solved according to the detection requirement of wireless sensor network, which verified the idea proposed by the model. According to the characteristics of wireless sensor network, the wireless sensor network security policy that integrated active intrusion detection policy and passive intrusion prevention key policy together was realized with secure routing policy as carrier. It put forward the corresponding implementation method and process of secure routing, key policy and intrusion detection plan.

6 Conclusions

Wireless sensor network is extensively used in modern society. However, such kind of network has many security problems because of the characteristics of wireless sensor network. In order to solve these problems, this paper put forward a security policy of wireless sensor network that integrated three aspects together. Each policy of this module cooperates mutually, and through a set of smart analysis, recognition, authentication and detection mechanism to form a comprehensive security defense and problem solving model for the overall wireless sensor network.

7 Acknowledgements

Supported by Foundation of Fujian Educational Committee (Grant No: JB12280); Supported by Training the Key Members of the Outstanding Young Teacher of Minnan Science and Technology Institute, FuJian Normal University (Grant No: mkq201008)

References

[1] Shao J 2010 Technology and Applications of Wireless Sensor Networks *China Electric Power Press* 3-4 (*in Chinese*)
[2] Akyildiz I F, Su W, Sankarasubramaniam Y, Cayirci E 2002 *IEEE Communications Magazine* **40**(8) 102-14
[3] Yao J, Yang X, Yi J, Han J 2012 Principle and Application of Wireless Sensor Network *Higher Education Press* 51-5
[4] Li J, Gao H 2008 Survey on Sensor Network Research *Journal of Computer Research and Development* **45**(1) 1-15
[5] Levis P, Lee N, Welsh M, Culler D 2005 TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications *The 1st International Conference on Embedded Networked Sensor Systems Los Angeles CA USA New York ACM* **30**(1) 122-73
[6] Enge A 2007 Elliptic Curve and Its Application and Guidance in Cryptology *Beijing Science Press* (*in Chinese*)
[7] Li X 2009 Intrusion Detection Method of Wireless Sensor Network. *Beijing University of Technology* (*in Chinese*)
[8] Zheng M 2008 Key Agreement Protocol of Provable Security *Wuhan Huazhong University of Science and Technology* (*in Chinese*)
[9] DaSilva A, Martins M, Rocha B, Loureiro A, Ruiz L, Wong H 2005 Decentralized Intrusion Detection in Wireless Sensor Networks *Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks Montreal Quebec Canada*
[10] Chen J, Cheng L, Si T, et al 2007 Intranet Security Strategy Based on a Monitor System *Journal of Tsinghua University (Science and Technology)* **47**(4) 606-9 (*in Chinese*)

Author

Xiehua Yu, born in 1982, Hunan Province of China

Current position, grades: associate professor.
University studies: Master's degree of computer science and technology, Central South University in 2004.
Scientific interest: wireless sensor network, artificial intelligence, information and network security.