IOP Conf. Series: Materials Science and Engineering **242** (2017) 012092 doi:10.1088/1757-899X/242/1/012092

Design and Analysis of Secure Routing Protocol for Wireless Sensor Networks

Jiong Wang, Hua Zhang

Fujian Provincial Key Laboratory of Information Processing and Intelligent Control(MinJiang University),Fuzhou 350121 China

Abstract: In recent years, with the development of science and technology and the progress of the times, China's wireless network technology has become increasingly prosperous and it plays an important role in social production and life. In this context, in order to further to enhance the stability of wireless network data transmission and security enhancements, the staff need to focus on routing security and carry out related work. Based on this, this paper analyzes the design of wireless sensor based on secure routing protocol.

1. Introduction

With the development of the times and the progress of science and technology, China's wireless network technology has developed by leaps and bounds. In this context, the role of the wireless sensor network in the social production and life is increasingly prominent. In fact, as a combination of sensors, embedded computing, distributed processing and other high-tech networks systems, in the process of running wireless sensor networks often encounter different levels of security attacks, which led to the user's network security to further reduced. Therefore, the technical staff need to design a secure routing protocol, to promote the acquisition and promotion of the benefits.

2. The overview of wireless sensor network

2.1wireless sensor network connotation

The so-called wireless sensor network, refers to the use of various types of micro-sensor nodes combined network system. In the process of running this type of network collect, analyze, organize information on coverage area, thus driving the smooth development of the operation.

2.2 the characteristics of wireless sensor networks

As one of the three high-tech industries of the future society, in the process of running the wireless sensor network system has many characteristics. The author gives the relevant summary, the specific content is as follows.

2.2.1 large-scale network. In order to improve the accuracy of information acquisition, the wireless sensor network system often needs to set a large number of sensor nodes in the monitoring area, and the number of nodes in this category is often more. At present, the large-scale sensor network system is mainly reflected on two aspects: First, the sensor node distribution area is larger; Second, the sensor is deployed more intensive in the node.

2.2.2 self-organizing network . In the process of building a sensor network, the technician often needs to install it in an area which lacks of infrastructure. Under such background, the neighbor relationship of nodes is often unknown, but the self-organization ability of sensor nodes is strong. So it can realize the

autonomous configuration and management. Based on this, through the topology control mechanism and network protocols the technical staff can promote the construction of network systems. In addition, in the use of domestic production the network system there are often some nodes fail, but some nodes of the monitoring accuracy is improved. In this context, the number of nodes in the sensor network system is in a dynamic change, and this leads to the stability of the network system.

2.2.3 Dynamic network. In addition, the network system also has a dynamic feature. This feature is mainly manifested in two aspects: First, the network node is out of the dynamic change of the situation, thus ensuring the safety of the entire system and stability of the upgrade; Second, the three factor ： the wireless sensor network sensor, the perception of the object and the observer is also in motion. In fact, in such a system, the technician needs to ensure that the sensor network system is reconfigurable.

2.2.4 Reliable network. In general, the wireless sensor networks system in the process of running to adapt to all kinds of natural environment, and can not be designed in the human region to play an important role.

In this context, in order to ensure the stability and improve the security of the sensor network system, the staff need to ensure that the sensor node quality to meet the design requirements, with the characteristics of strong, difficult to damage and adapt to a variety of harsh environmental conditions. Therefore, in the process of running China's common wireless sensor network system has a strong reliability, thus, it able to adapt to various environments, access to a wide range of promotion and use.

3. The design principles of wireless sensor network routing protocol

In the process of design wireless sensor network routing protocol, technical personnel often needs to strengthen the energy efficiency, the accuracy of data transmission and other factors, and follow various principles to carry out design operations. The author made a summary on the wireless sensor network routing protocol designs principles, the specific content is as follows.

3.1 the principle of energy utilization priority

In the process of wireless sensor network system designs, the WSN nodes are used in the use of a class of energy such as batteries. Under such a background, the energy consumption of WSN nodes often has a more direct impact on the efficiency of system operation. Based on this, designers need to follow the energy utilization priorities to ensure that WSN survival time is extended. In general, the technical staff need to use data fusion, localization algorithms and other means to reduce the communication consumption, to ensure that the node battery consumption is fair and average, to promote the improvement of the benefits.

3.2 the principle of data center

At present, in the application process China's wireless sensor network system, need to collect and analyze various types data of the task area, so as to provide users data support with all kinds of work. Based on this, in the relevant network in the process of the system construction and design operations the staff need to strengthen the principle of data center compliance, and thus ensure that the sensor node can be based on the naming mechanism to describe the various types of data, and collect the interest of a named data by sending to all nodes data.

In fact, in the actual operation of the process the data-centric routing protocol is often able to achieve the entire system of node data concerns, thus avoiding a single node failure for system damage, help the promotion of the entire network system security and reliability.

3.3 the principle of data aggregation

Because in the process of running the sensors in the WSN can use different sense of precision to carry out the perception of the target environment, so the technical staff often collect and transmit a large number of duplicates and redundant data in the process of constructing data-centric routing protocol, that leads to further reduction of system operation efficiency, which is not conducive to the acquisition of relevant benefits.

Based on this, in order to further achieve the processing of various types of data, the technical staff need to strengthen the use of data aggregation technology, which as a basis for the realization of various types of duplication of data to eliminate and reduce, and by simplifying the scale of data transmission, achieve the energy conservation purposes.

In fact, the principle and the use of technology can not only simplify the node data, but also can be a number of sensor nodes which can combine the data onto meaningful information according to the characteristics of the data, thereby enhancing the accuracy of the information, while enhancing the robustness of the system.

3.4 node positioning, target tracking principle

The so-called node location, refers to in the process of construction and operation of the sensor nodes the system can be marked on the system location, so the wireless sensor network routing protocol decision-making work can provide a variety of information reference. In addition, through the smooth positioning of the node to carry out the work, the operating staff can be dedicated to the intelligent selection of various types of node tasks. In general, the application of this method not only can reduce the energy consumption of the system, but also can further to improve the system's life expectancy, to ensure that the system in the process of running to obtain higher economic and social benefits.

4. Security threats and coping strategies

4.1 routing attacks

In the transmission and use of the process routing information often encounter a variety of forms of attack damage, the current attack are divided into two categories, namely: passive attack and active attack. Passive attack refers to the attacker through eavesdropping routing information, and the direction of data transmission and content changes, resulting in damage, and active attack is through false routing information, selective forwarding, sinkhole attacks and other means to attack, and thus lead to wireless the sensor network system is faulty and can not run efficiently.

4.2 the connotation of secure routing protocol

In order to ensure the security and stability of the transmission of the network system, designers need to ensure that the routing process can isolate the non-authorized nodes during the process of protocol design and ensure the formal nature of the route discovery and ensure Node topology confidentiality, to avoid all kinds of problems which can caused system failure. In this context, the designers are often able to take measures to solve the above problems of the node authentication, key management, message source certification and other aspects.

4.3 commonly used security technology

4.3.1 secret sharing technology. The so-called secret sharing technology, refers to in the process of running the network system sent the network operation password and other confidential information on many participants, in order to achieve the confidential file shunt, only the participants of the sub-combination of authorized can restore the secret file information. In the process of using the technology for system design and work, the technical staff often need to use the secret distribution, reconstruction algorithm for specific operations. In the process of doing a job of a secret distribution algorithm, the designer needs to divide the secret document data onto several parts and distribute it among the participants to ensure that each participant gets a secret share. The secret reconstruction algorithm is often able to ensure that the participant union with the qualified subset can recover the secret correctly, while the non-qualified subset can not participate in the relevant job.

4.3.2 ID-based authentication and key negotiation. WSN systems are often built on the exchange of broadcasts (unicast messages). Under such a background, the sensor nodes are able to carry out periodic broadcasts and to the neighbor nodes. In this process sensor can use ID authentication and key agreement technology to ensure the safe operation of the system. In this process, when the A node is added to the network system, it will often broadcast to the neighboring nodes Hello message, and the surrounding node will be initiated into A node authentication, key establishment process. Under this background, saving the interaction between nodes, and promote the system to achieve a substantial increase in efficiency. In fact, with the node ID authentication, it can further negotiate the unicast key and obtain the other party's broadcast key.

4.3.3 the design of secure routing protocols. In the process of building a secure routing protocol, there is an offline trusted center of the designer erection protocol, and it can distribute the ID private key to each node during the running process and it can realize the data onto multiple node data by means of secret technology sharing. These shared informations about multiple nodes that cooperate to update the key for the node and distribute the private key to the newly added node. On the routing protocol design flow chart, the author made a summary,the specific content is shown in Figure 1.

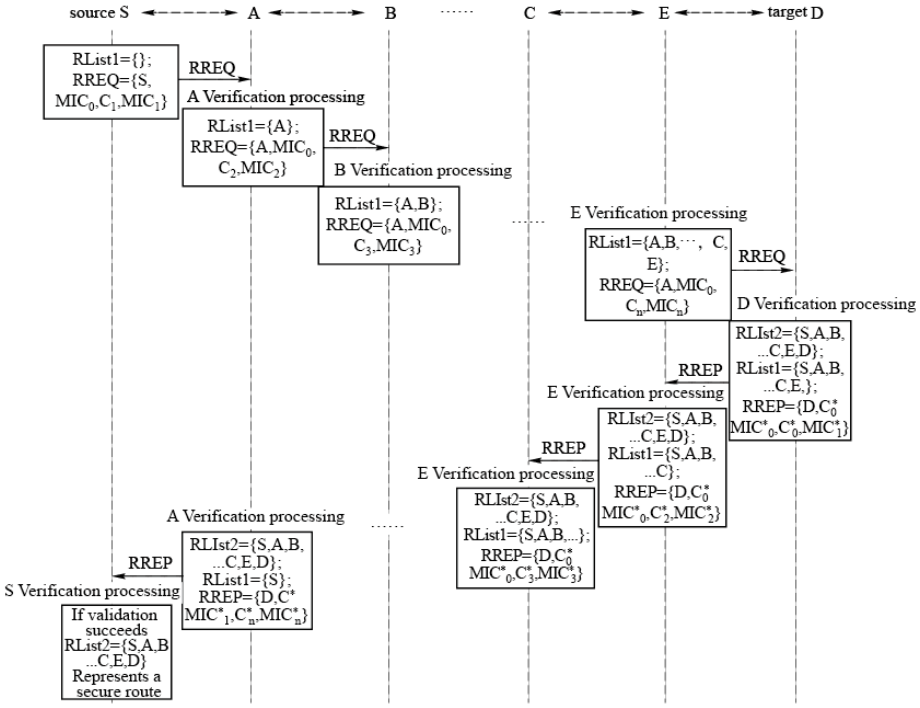

Figure 1 routing protocol flow chart

In this process, the protocol uses the D-identity information to carry out the calculation of the shared key ksD, and the unicast encryption key between the S and D and the unicast integrity key is exoprted, and then the route requests message to construct RREQ. Subsequently, the intermediate node A will accept the request information and use the broadcast integrity key of the RS to calculate the MICi and compare the value with the design value of ensure that the same information is transmitted to the neighboring node for broadcast. And in order to find the target node of the Keei warehouse, to ensure that the source node S receives the routing response messages RREP, and take measures to achieve the entire routing system security and stability of the upgrade. Through the design and development of the protocol, the technical staff also summarizes the processing methods of various types of routing attacks, and draws the relevant forms, the specific contents are as follows.

Table 1 scenario running table

Attack category	Attack processing	effect	case analysis
case analysis	Using identity authentication, message source authentication, news freshness and other technologies	Great	the authentication and key program communication and computing performance which based on IDand bilinear pairs is higher
Unauthorized access	Using identity authentication technology	Great	Can be used to prevent Sybile technology
Retry attack	Using a unique serial number method	Great	The serial number needs to be transmitted, increase the communication burden, but can be used to prevent Hello attacks
Transmission analysis	Encrypt protection of routing information	Great	Able to prevent passive eavesdropping attacks
Black hole attack	Avoid the intermediate point to provide a response message to prevent the intermediate point from attracting the network data stream itself	Great	The routing efficiency is lost, but the reliability will be greatly increased, is conducive to the prevention of Sinkhole attacks attacks and selective forwarding attacks
Tunnel attack	Using the probability of combining the number of hops and the time extension	general	This method can make the probability of tunnel attack greatly reduced, so that the tunnel attack failed. Reasonable use of this method, can effectively prevent Wormholes attacks
Critical point attack	Secret sharing technology	better	Through the secret sharing technology in a number of nodes to share, which makes the key point of failure, but the system performance will be affected
Isolate malicious attacks	Secret sharing and secret update technology	general	When a certain number of broadcasts of a node's malicious attacks reaches a certain number, the network node key can be updated by secret sharing technology to exclude the malicious node from the network but with poor performance.

Through the analysis of the program we can learn: in the process of running the program can be based on various types of routing security risks and take positive measures, and thus achieve the entire system operating efficiency and quality improvement, to ensure that the user network information security, to further enhance the realization of the benefits of the acquisition.

5. Intermodulation Interference Analysis Model

In the process of wireless router network security routing protocol design, the technical staff also need to strengthen the intermodulation interference analysis model for the construction and use. At present, the relationship between the output current ic of the nonlinear device and the input voltage can be written as: ic = a0 + a1u + a2u1 + a3u2 + ... In this formula, ai refers to the characteristic coefficient of the nonlinear device. According to the above analysis, it is assumed that two signals simultaneously act on the

nonlinear device, that is, u = AcosωAI + BsinωBI. In general, the distortion term of this relation can be expressed as

(cosωAI + BsinωBI) n.

Through the expansion of the above formula, the analysis can be learned: 2ωA-ωB, 2ωB-ωA two frequency interference on the receiver of the greater harm, and by the combination of these two frequency interference is often referred to as the third order Intermodulation interference.

Concluding remarks:

Based on these above mentioned information, this paper mainly discusses the connotation and characteristics of wireless sensor networks, and discusses the design principles of routing protocols and the security threats and coping strategies of wireless sensor networks. Finally, the design of secure routing protocol is analyzed. I believe that with the implementation of relevant measures in place, China's wireless sensor network security routing protocol will be developed by leaps and bounds, and thus meet the needs of social needs of the community, to promote the realization of the benefits and enhance the realization of China's network security. As well as the improvement on reliability, and ultimately lead the development of the network.

Acknowledgment

1. Research on Security Access Technology of Mobile Ad hoc Network, JAT160385，2016 Young and Middle-Aged Project Funded by Fujian Provincial Education Bureau
2. Research and Implementation of Campus Network IVI Transition Technology Based on IPv6, JB12159，2012 Class B Project Funded by Fujian Provincial Education Bureau
3. Research on Aodv Routing Protocol Simulation and Multipath Optimization. YKY12006, 2012 Science and Technology Incubator Project of Minjiang University
4. Research on IT Management and Service Model of Library Based on Cloud Computing. YSY12015, 2012 Social Science Project of Minjiang University

References

[1] Ren Xiao-gang.Study on Secure Routing Protocol Technology of Wireless Sensor Networks [J]. Computer Programming Skills & Maintenance, 2013, (24): 111-112 + 114.
[2] Zhao Qi, Wang Ru Chuan. Wireless sensor network routing protocol security problem analysis [J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2016, (3): 83-87.
[3] Tan Bo-ping, Zhou Xian-wei, Yang Jun, LI Xiao-qin.Study on security mechanism based on routing protocol of wireless sensor networks [J] .Technical Journal of Sensors and Actuators, 2016 (4): 1276-1278 + 1283.
[4] Long Zhao-hua, Gong Jun, Wang Bo, Qin Xiao-huan, Liu Da-ming.Study on Energy Efficiency of Clustered Secure Routing Protocol in Wireless Sensor Networks [J] .Journal of Electronics & Information Technology, 2015, (8): 2000-2006.
[5] Song Zhigao, Chen Fei, Chen Kefei, Li Hui. Wireless Sensor Network Routing Protocol Security Analysis and Research [J]. Computer Simulation, 2015, (5): 134-136 + 140.
[6] Yu Xiehua, Zhang Xiaofang, Huang Zexin. Wireless sensor network security routing protocol research [J]. Journal of Yangtze University (Natural Science Edition), 2011, (8): 98-101 + 279.
[7] He Liyuan, Li Yongming, Wang Quandi. Analysis of cluster routing protocols for wireless sensor networks [J]. Journal of Chongqing University (Natural Science Edition), 2017 (1): 50-53.
[8] Jiang Yi, Zhang Ruonan, Shi Haoshan. A geo-based wireless sensor network security routing protocol [J]. Journal of Northwestern Polytechnical University, 2012, (1): 11-16.
[9] Wang Wei, Tang Minghao, Xu Yunmin.Design of multi-path routing protocol for wireless sensor networks [J]. Computer Engineering and Applications, 2014, (12): 136-138