www.sensorsportal.com

Sensors & Transducers

© 2013 by IFSA
http://www.sensorsportal.com

Research of Security Routing Technology in Wireless Sensor Network

Jixiang Wu
Chongqing Technology and Business Institute, No. 3-5, Cuiyuan Community, No. 1, Hualong Avenue, Jiulong Science and Technology Park, Jiulongpo District, Chongqing City, 400052, China
Tel.: 86+18523073848, fax: 86+18523073848
E-mail: qydbzzw@sina.com

Received: 15 April 2013 /Accepted: 20 July 2013 /Published: 30 July 2013

Abstract: Wireless Sensor Networks WSN (Wireless Sensor Network) as a new access to information technology and network technology, it has a wide range of applications in many important areas for the performances with low-energy, little-cost, distribution and self-organization, such as military, environmental science, health care, etc., is currently study abroad hot spot. In this paper, along with the extensive application of wireless sensor networks, ZigBee wireless sensor network as a typical protocol, widely used in the actual system design. The importance and current situation of the development of security routing technology were especially introduced in this paper. And we have given the design scheme for the wireless router system based on ZigBee protocol and verified the feasibility of the system in order to provide some useful information for the related techniques. *Copyright © 2013 IFSA.*

Keywords: ZigBee, WSN, Security, Routing, Technology.

1. Introduction

Wireless sensor network WSN (Wireless Sensor Network) as a new access to information technology and network technology, in many important areas have a wide range of applications, such as military, environmental science, health care, etc., is the research focus at home and abroad. Wireless sensor network systems typically include sensor nodes, sink node and the management node. A large number of sensor nodes are randomly deployed within or near the detection area can be constituted by self-organized networks. Sensor nodes monitoring data hop along to other sensor nodes for transmission of data during transmission may be more than one node, after a multi-hop route to the sink node, and finally managed to reach via the Internet or satellite nodes. User through the management node of the sensor network configuration and management, release detection task and to collect test data.

At present, both at home and abroad, there are a lot of research on WSN routing protocol, mainly by Wu Di proposed a similar AODV protocol of BRIT (BounceRouting Tunnels) in the new road by the algorithm [3]; Li Hao put forward based on cluster unit topology of wireless routing protocol RGAF (Reliable Geographical Adaptive Fidelity) [4]; The Hong Kong university of science and technology Li Mao put forward the structure of the perception of the adaptive routing algorithm [5]; Tong Min Ming *et al.* proposed a gradient based on location information and network of greedy routing algorithm [6]; Chen Zujue put forward based on the distance of the effectiveness of the hierarchical routing protocol [7]; Zhou Ning of opportunistic routing algorithm based on RSSI and so on [8].

2. Definition and Characteristics of Wireless Sensor Networks

2.1. Nodes and Network Structure of Wireless Sensor Network

The basic unit of the wireless sensor network sensor nodes. Wireless sensor network node component units are shown in Fig. 1.

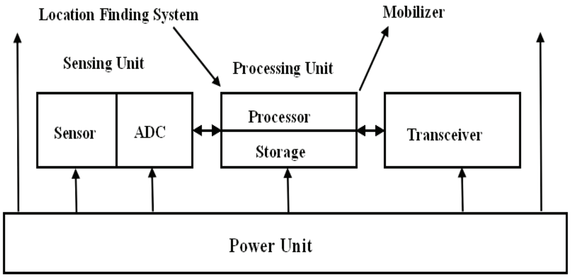

Fig. 1. Structure of nodes in WSN.

The sensor node is composed of a power supply, sensor, processor CPU, memory, communication components and software that several components. Power for the sensor to provide the energy necessary for the correct functioning. Sensors for sensing, to obtain information on the outside, and through the AD converter converts it to a digital signal. Processor is responsible for coordinating the work of the various parts of the node. If the sensing member to obtain the necessary information processing, storage, control and power supply of the sensor components working mode. Communication with other sensors or components responsible for the communication observer. The communication component is responsible for communication with other sensor or the observer. The software is to provide the necessary software support sensors, such as embedded operating system, network protocol stack because sensor networks require sensor nodes is small in volume and low cost, so the sensor node has many resource constraints, the most serious one is energy limited.

Wireless sensor network is composed of a large number of these tiny sensor nodes. They are scattered in the monitoring region, the regional events through the sensor's piece. Each sensor node can share data through wireless communication means, to obtain more accurate monitoring accuracy. The network structure is usually a sensor network as shown in Fig. 2.

The small points in the figure indicate sensor nodes, black square dot indicates the sink. Sensor nodes through wireless networking self-organized manner, node data collected along the way through a multi-hop network path to the sink node. Sensor network aggregation node is a node resource limitations smaller, ordinary nodes to collect the data sent to it, which is responsible for the data sent over the Internet or directly to the user, the node can also send commands to the entire network.

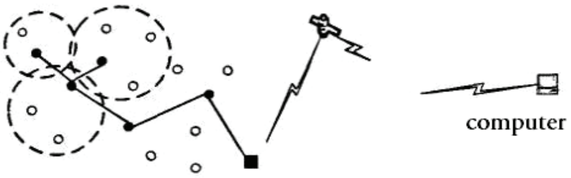

Fig. 2. Structure of wireless sensor network.

2.2. Characteristics of Wireless Sensor Networks

The characteristics of wireless sensor network in general, the following aspects:

2.2.1. Limited Energy

Small size sensor nodes are generally battery powered, energy is limited. And because the wireless sensor network is relatively poor working conditions, the number of nodes, generally impossible supplemental power. The wireless signal attenuation generally transmitted power is proportional to the distance d (d is generally greater than 2), so the wireless sensor networks generally use multi-hop transmission of data in order to save energy. But the use of multi-hop intermediate node will be introduced with the transmitter receiver overhead. Further, in general, the wireless communication module on the node will be able to sleep, so when there is no data to be transmitted, should be allowed to sleep in order to save energy.

2.2.2. Huge Network

In order to obtain accurate information in the monitoring area is usually deployed a large number of wireless sensor nodes. This has two meanings: First, a large range of the node, the second node density is high. Large-scale deployment nodes can observe the same event from a different space, and thus get more resolution. And a large number of redundant nodes exist, making the network has a higher fault tolerance.

2.2.3. Self-Organizing Network

In wireless sensor networks, usually no infrastructure. The location of the sensor nodes is not pre-determined. Require wireless sensor network node has the ability to self-organization, to conduct its own configuration and management, through topology control mechanisms and network control protocol monitoring data automatically form a multi-hop wireless network system.

2.2.4. Dynamic Network

In wireless sensor networks, node failure due to environmental factors or run out of energy, wireless link bandwidth change, a new node joining, etc., will cause the entire network is a dynamic network.

2.2.5. Related to the Application

Wireless sensor network is an application-related network. Different applications in sensor network hardware and software may be completely different.

2.2.6. Data-centric

Different from traditional networks, wireless sensor network is a data-centric network, users do not care who to send data, but only care about what specific data.

3. Routing Protocol for Wireless Sensor Networks

Since there are a lot of standard classification of WSN routing protocol, so the classification method of routing protocol is variety. According to the working principle of different routing protocols of the routing protocol is divided into two types, and analysis of typical routing protocols of each type.

3.1. Plane Route

Flat routing believes that all the sensor nodes in the network have the same function and equal roles, nodes or their event detection results to report to the other node, or any other node sends a query message to the node detection events, data forwarding through multi-hop routing cooperative multi node. Information Negotiation sensor SPIN (Sensor Protocols for Information via Negotiation) is the first plane routing data-centric algorithms, a consultative mechanism through node asked to reduce data redundancy and energy loss. SPIN is a kind of based on negotiation mechanism of data-centric routing algorithm, the first SPIN on the characteristics of node data received by the high level of abstraction, metadata description node receives data characteristics (meta - data). Before forwarding the data received, node A first use metadata to negotiate with neighboring Node B, Node B sends ADV signal to determine whether the data, as shown in the 'a' part of Fig. 3. If the data node B to metadata represents a demand, sends out the feedback signal to REO, as shown in 'b' part of Fig. 3. Otherwise it is discarded the ADV signal, and then the node A will be forwarded to the node B DATA data, as shown in 'c' part of Fig. 3. Node B received from node A to transmit data, adopt the same approach with the node A. First with metadata negotiate all nodes connected to it do not need the data, send ADV signal, as shown in 'd' part of Fig. 3. If there is a demand node reverted REQ signal, no demand is directly ADV signal discard, as shown in 'e' part of Fig. 3, then the node B will reply REQ signal all nodes transmit data DATA, as shown in 'f' part of Fig. 3.

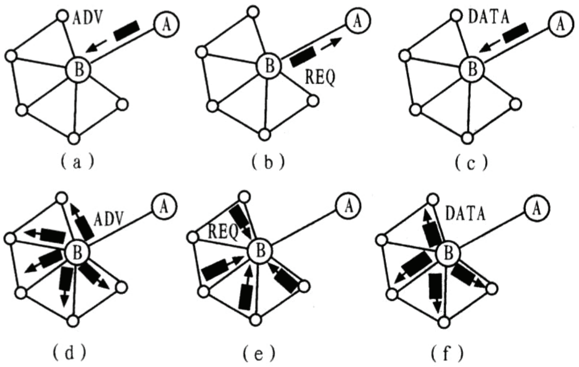

Fig. 3. SPIN algorithm implementation process.

SPIN algorithm does not clearly define metadata format. The specific format and application-related, such as ADV and REQ formats depending on the application requirements in detail. In addition, when the topology changes, each node only needs to maintain its neighboring nodes in the local scope, without the whole network broadcast, both to save energy and reduce the node processing capacity requirements, this kind of SPIN is called SPIN-1. But SPIN-1 does not guarantee the correct delivery of remote data, such as remote node need data and proximal adjacent nodes and the source node is not required, the forwarding to represent metadata for the data is discarded, don't do REQ reply, resulting in data delivery failure. In order to solve this problem, the SPIN-2 joined the energy threshold mechanism based on SPIN-1. Testing the adjacent node energy before the delivery of data, if the energy value is below a certain threshold, it is considered that the remote node does not have sufficient capacity to complete the delivery mission, the data is forwarded to other neighboring nodes with sufficient energy. In addition, for different applications, SPIN the other extended protocol, such as SPIN-BC and SPIN-RL for sensor networks that multicast network, SPIN-PP and SPIN-EC for the traditional ad hoc network have made special optimized.

3.2. Hierarchical Routing

Hierarchical routing (known as the cluster based routing) is first produced and applied to wire networks, efficient communication to meet the large-scale network. Therefore, the concept of hierarchical routing is introduced into the WSN, sensor nodes to meet low power consumption and efficient communication. In hierarchical routing, the high-energy nodes can be used for data forwarding, data query, data fusion, remote communications, and global routing maintenance of high energy-consuming applications; low energy nodes for event detection, targeting and local routing maintenance low energy applications [9]. Thus, the different applications in accordance with the reasonable distribution of nodes of different capabilities, so that nodes can give full play to their respective advantages, to cope with large-scale network conditions, and effectively improve overall network lifetime. Hierarchical routing consists of two levels of routing: one used to select the cluster head node, the second is used for routing. LEACH (low-energy adaptive clustering hierarchy) is a proposed earlier cluster-based hierarchical routing algorithm for WSN thinking. With the traditional fixed network gateway node compared with ample energy, WSN nodes energy is limited, it can not use the same set of cluster head node as gateway. LEACH randomly selected from a small number of WSN nodes as cluster head, taking into account the energy consumption of each node in the network balance, so that other nodes in the cluster head has not done as cluster head rotation so that the network will not run out of energy caused by the first few nodes network paralysis.

LEACH algorithm clustering head up and steady-state two stages, the former is the key to LEACH algorithm, the latter is the guarantee of data transmission. T(n) is as in

$$T(n) = \begin{cases} \dfrac{p}{1 - p.[r.\mathrm{mod}(1/p)]}, n \in G \\ 0, \end{cases} , \qquad (1)$$

where the establishment phase cluster head node randomly selects a number r (O<r<1), if the random number r is less than the threshold T(n), then the node becomes a cluster head in this one. G represents the last 1/p rounds have not been selected as cluster head node set, p represents the concentration of cluster head node (e.g. 5 %),

The structure of LEACH is as shown in Fig. 4.

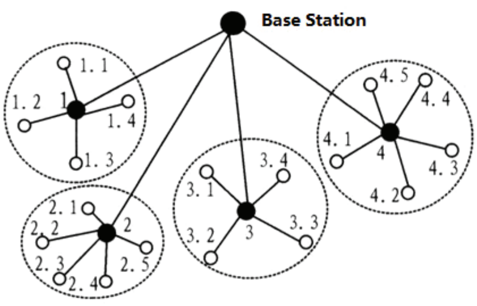

Fig. 4. LEACH network structure.

LEACH clustering mechanism can reduce the overall network energy consumption and prolong the network lifetime; between the nodes in the cluster using TDMA coding, cluster head and base station uses CDMA coding to ensure effective information transfer; data collection and cluster head nodes are periodic, continuous monitoring of the network change event is suitable.

4. Wireless Sensor Network Attacks

Wireless sensor networks from the military field, and its used in commercial and military security issues in the field is particularly prominent. From the network itself, as a result of an open, cooperative and highly arbitrary environment, with fragile links between nodes, dynamic topology, authentication lacking, there is no centralized monitoring or management point and other characteristics, the network itself, there are many security vulnerabilities all these will be exploited by an attacker; applied from commercial, military environment, in an environment of hostility, aggressive behavior more rampant and complex and diverse, attackers do their best to use all means to attack the network from all avenues. Active attack makes the sensor networks faced with data and routing information has been tampered with, the node identity forgery, network energy is depleted, and many other threats. The passive attack to steal information through the network analysis, resulting in leakage of sensitive information network, the key nodes identity, location exposed targets highlights, allowing an attacker to further active attacks launched in one fell swoop [10]. The existence of many attacks decided the WSN is huge, be disastrous consequences which caused by the attack even will cause severe paralysis of the entire sensor network. Therefore, for commercial and military sensor networks, security is a very serious problem, security problem is the precondition of its put into application implementation.

4.1. Common Attacks of Routing Protocol of Wireless Sensor Network

1) Spoofing, change or reproducing route Attack: Attack locking routing information exchanged between nodes, by tampering, forgery or replay attack routing information.

2) Selective forwarding attacks: a malicious node receives a packet, some forward or not forward received packets, resulting in data packets can not reach their destinations smoothly.

3) Witch Attack: Witch Attack (Sybil) way is malicious node pretending to multiple nodes, it can claim to have multiple identities, and even can freely produce multiple false identities, to take advantage of these identities to illegally obtain information and carry out an attack.

4) Sinkhole attack: the sinkhole attack (Sinkhole), the attacker's goal is through has been controlled by the attacker captured nodes, or to attract a particular area of almost all of the data flow through has been

invaded by the node, generating a Sinkhole to the node as the center.

5) Wormhole Attack: wormhole attack (Wormhole) usually takes two malicious nodes collusion, conspiracy to attack. A malicious node is located near the base station, while another malicious nodes far from the base station. Distant malicious nodes near the base station radio nodes themselves and can create high-bandwidth, low-latency links, and thus attract the surrounding nodes send data packets, thus cutting off the route to the base station.

6) HELLO flood attack: malicious nodes via high-power broadcast routing or other information, so that the other nodes in the network for their own malicious neighbor nodes, which sends the information to a malicious node.

4.2. Analysis of LEACH Protocol

Since LEACH protocol uses a single-hop path selection method, that all sensor nodes and aggregation nodes are likely to have direct communication, so the Sinkhole attack, Wormhole attacks, Sybil attacks and fake routing information attacks are defensive capabilities. But in the process of cluster formation, members of the cluster head node based on the signal strength to select the cluster you want to join, so a malicious node can be used HELLO Flood Attack with a large transmission power broadcast messages to the entire network, in order to attract a large number of member nodes to join the cluster, and then the malicious node can choose, change the data forwarding bag, to achieve the goal of attacking. After the above analysis shows that, LEACH protocol is the most vulnerable to attack HELLO Flood attack.

The attack on the HELLO Flood mode, the LEACH-H protocol has been presented, and adopted the following security solutions: authentication relies on a node can be trusted by link bidirectional authentication and node for each cluster head candidate node to a neighbor base station and its jump node confirmed its neighbors, thus successfully against HELLO Flood attack.

Specific operating mechanism: In the broadcast phase, the candidate cluster head node to the base station and hop neighbor nodes transmit their own data, this data includes the candidate cluster head node and the base station shared key, the base station according to the decryption key to confirm the candidate cluster head node is normal, if not normal is to drop packets; clustering stage, node send the information he will join in which cluster to the base station, the base station generates a key from the sensor nodes and cluster head node to node and candidate, and decrypt decrypted successfully matching, accept this candidate cluster head node, otherwise automatic packet loss. Several candidates receiving node from the cluster head node, select the strongest signal candidate cluster head node to its cluster.

5. Conclusions

With the wide application of wireless sensor networks, ZigBee wireless sensor network as a typical protocol, more widely used in the actual system design. This article describes the importance of secure routing technology development status and given based on ZigBee protocol for wireless routing system design studies to verify the feasibility of the system.

References

[1]. Zixiao Cheng, Yun Liu, Efficient data collection methods involved in mobile nodes of wireless sensor network (WSN), *Journal of Beijing Jiaotong University,* Vol. 37, Issue 2, 2011, pp. 48-54.

[2]. Yimei Kang, Tao Wang, Jiang Hu and etc., WSN communication data semantic security algorithm based on changes the mapping table, *Journal of Beijing University of Aeronautics and Astronautics*, Vol. 55, Issue 9, 2010, pp. 1043-1047.

[3]. Xiaoliang Qin, Qinfang Wei and Shuangjie Zhang, Data fusion protocol for WSN with optimization and security features based on a pattern-based code comparing, *Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition)*, Vol. 24, Issue 06, 2011, pp.752-756,+779.

[4]. Yongchao Wang, Wei Wei and Dongming Lu, Overview of wireless sensor network security, *Computer Age*, Vol. 26, Issue 12, 2008, pp. 15-19.

[5]. Zhijuan Peng, Shuchuan Wang and Haiyan Wang, Research on security mechanism for wireless sensor network based on digital watermarking technique, *Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition),* Vol. 47, Issue 04, 2006, pp. 69-72,+78.

[6]. Minming Tong, Lixian Yang, Xiaowen Liu, Study on improved routing algorithm of mine monitoring wireless sensor network, *Journal of Sensor Technology*, Vol. 21, Issue 11, 2008, pp. 1892-1895.

[7]. Ning Zhou, Research of opportunistic routing of WSN based on RSSI, *Journal of Xinxiang College (Natural Science Edition)*, Vol. 25, Issue 12, 2008, pp. 3747-3749.

[9]. Yongchao Wang, Wei Wei, Dongming Lu, Summary of WSN security, *Computer Age*, Vol. 26, Issue 12, 2008, pp. *15*-19.

[10]. Zhijuan Peng, Shuchuan Wang, Haiyan Wang, Study on security mechanism of WSN based on digital watermarking, *Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition),* Vol. 46, Issue 4, 2006, pp. 69-72.