Analysis of Security Routing Protocol for Wireless Sensor Networks

Yi Wang
Department of Information Engineer
Guangdong Polytechnic
Foshan, China
wangyifsfz@163.com

Zhenjie Cao
International School
Beijing University of Posts and Telecommunications
Beijing, China
470413717@qq.com

Xue Bai *
Department of Economic management
Guangdong Polytechnic
Foshan, China
chenxiaoyunld@163.com
* Corresponding Author

Abstract—Wireless sensor network routing protocol security objective is to ensure data integrity, authentication and availability. In this paper, the characteristics and applications of routing protocols for wireless sensor networks are analyzed. This paper presents the analysis of security routing protocol for Wireless Sensor Networks. Experimental data show that the proposed secure routing protocol has the advantages of short delay time and low energy consumption.

Keywords- Wireless Sensor Network; Routing Protocol; Security Analysis; Topology; Security

I. INTRODUCTION

Sensor module is responsible for the collection and transformation of the information in the monitoring area, the information processing module is responsible for the management of the sensor nodes, storage and processing the data collected by itself or other nodes to transmit data, the wireless communication module is responsible for communication with other sensor nodes, energy supply module is responsible for the operation of the entire sensor network energy supply.

WSNs network is a kind of specific hoc Ad network. The nodes in the network do not need any infrastructure. WSNs network is the most similar to Ad hoc networks MANET (Mobile), although the two are wireless self-organized multi hop network, which has a lot of similarities, but the difference is very big.

Network data transmission can not be separated from the routing protocol, routing protocol is the basis of its network. Routing technology is the core technology of WSN communication layer [1]. Routing problem is the construction of WSN network to focus on a problem, from the point of view of routing, WSN has its own characteristics, so it is different from the traditional network, but they are different in wireless ad hoc networks. Traditional wireless hoc Ad network routing protocol is not suitable for WSN, so it has to be a new, suitable for WSN routing protocol.

802.15.4 and CC2420 are introduced. The analysis and research of the self organization protocol in wireless sensor networks are presented. According to the organizational structure of the wireless sensor network, wireless sensor network self-organizing protocols are classified, divided into two categories: a class is pure global structure (global only, go), another kind is global structure and local structure (Global & local, G & L). According to the classification, the implementation method of some self organization protocols in each category is studied.

Wireless sensor networks are usually deployed in open and friendly to the environment, such as field and battlefield, due to low cost and resource constraints, sensor nodes lack the necessary hardware tamper proof measures, the attacker can more easily captured nodes, the network to decipher the key and the protocol stack information; on the other hand, sensor nodes monitoring information tend to have sensitivity and privacy, nodes with a high degree of autonomy and use wireless communication way of multi hop forwarding.

At the same time, deployment of WSN nodes are often a large number, densely distributed, each node of the collection of information redundancy is big, in the transmission process if the data fusion will greatly reduce the amount of data transferred [2]. These new features make the MANET working group proposed many routing protocol standards and the draft can not be directly applied to WSN. WSN routing protocols must be based on the characteristics and tasks of the application occasions, and to extend the network survival time and improve the network throughput, reduce communication delay between the compromises.

Directed diffusion routing mechanism is divided into the interest of flood, the establishment of two-way gradient, the detection packet flooding, the choice of the path and the strong, and data sending five stages. In the data communication phase, the nodes send the data to the cluster head, and the cluster head is fused and the results are sent to the sink node. Because the cluster head needs to

complete the data fusion and the base station communication and so on. This paper presents analysis of security routing protocol for Wireless Sensor Networks.

II. TYPICAL WIRELESS SENSOR NETWORK ROUTING PROTOCOL

Wireless sensor network is a group of sensors constructed in an ad hoc way wireless network, each node can cooperative sensing, collecting and processing the information of the covered area of geographic information, and transmits the information to the monitor. Fig. 1 shows the architecture of a wireless sensor network. Wireless sensor network consists of a large number of sensor nodes, the use of wireless communication technology, nodes in the network each other as a router to its neighbors (nodes within the communication range), through the node forwarding to realize the communication between the nodes.

In the initial state, the sensor node S is in an isolated state T S will continue to wait until the next Adv message is not received [3]. In this case set, then S2 added to their parent node in the collection, and update their distance parameter value (is equal to the distance parameter adv message value plus 1), the routing process, when a node s will perceive the data information is sent to the gateway node, it is the first to see his father node collection using round robin scheduling algorithm to select a parent node f ', then the data information is sent to a selected parent node f', parent node f using round robin scheduling algorithm from the parent node in the collection selection a parent node f 'data information is sent to its parent node f'.

SPIN uses 3 types of information for communication, namely ADV, REQ and DATA, in the process of operation. ADV - for new data broadcast. When a node has data to be shared, it sends out the metadata in the DATA data packet in a broadcast manner. REQ - used to request sending data. When a node is willing to accept the DATA packet, the REQ packet is sent. DATA -- contains metadata of head (meta-header) of the actual packet.

$$W_j = \overline{span\{\psi_{j,i} : i \in Z\}} \tag{1}$$

At present, based on distance location algorithm using static geometric relationship to determine the location of the nodes, and high on the beacon nodes arrangement and density of the requirements, such as the trilateral, multilateral measurement location, angle measurement positioning algorithm based on, need mobile nodes to obtain at least three or more than three beacon nodes coordinate and distance. Another thought is the beacon or beacon movement, with the known location of the GPS mobile beacon to a planned path or motion model traversal of the unknown node location, and transmits the location signal; the other node gets the signal to compute the location.

The sink node is directly connected with the external network, responsible for the detection task of the management node, and forwards the collected data to the external network. Sensor nodes generally consist of data acquisition module, processor module, wireless communication module and power supply module, which are composed of four parts. Data acquisition module is responsible for data acquisition and conversion, the processor module is responsible for data processing and wireless communication module is responsible for data transmission and other nodes, the energy supply module is responsible for the energy needed to run, usually adopts a miniature battery. Sensor node processors typically are using an embedded CPU, such as Intel 8086. In addition, the system also need to block to a miniature operating system in order to carry out tasks scheduling and management, UC Berkeley TinyOS, such as in Linyx etc.

According to the two different types of networks, the many protocols are divided into two categories -- flat routing protocols, hierarchical routing protocol. This part will mainly introduce flat routing protocols. Fig. 1 when a broadcast information of the nodes, the node B and node C receives information and broadcasting, so that node D receives Fig. 1 two copies of the same message flooding algorithm and gossiping algorithm.

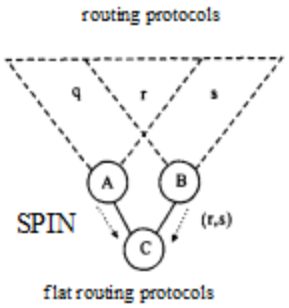

Figure 1. Mainly introduce flat routing protocols.

In addition, the time delay, scalability, sensing accuracy and data fusion are important indicators of metric routing protocol. Compared with the traditional wireless communication network, the traditional wireless communication network research focuses on the quality of service (QoS) for wireless communication, wireless sensor nodes is randomly distributed, battery powered, so the current wireless sensor network routing protocol research focus is on how to improve the energy efficiency, here are a couple of current wireless sensor network routing protocol [4].

The MAC layer protocol for wireless sensor networks is concerned with minimizing the energy consumption, which determines that it should be moderately reduced throughput and delay. Because the nodes of the wireless sensor network always work together to accomplish a task, it is usually not the main problem. Some typical applications of wireless sensor networks (such as battlefield target tracking) are also proposed for the design of MAC layer protocols, which are different from the traditional wireless networks.

Self organization is a very common phenomenon in the life, and it has been studied. In traditional data communication networks and infrastructure is fixed, the network structure is based on router, switches and other network equipment, some functions such as address allocation and name resolution are the central server. However, in a distributed wireless network, there is no pre - set infrastructure, and the network is organized by default. This means that all the functions are run in a self organization. Or rely on such a network without

infrastructure to achieve different functions (routing, broadcasting, address allocation, etc.), or have to do some work. Therefore, researchers want to provide a self organization structure that can support all the functions of the organization. This global structure is obtained by the interaction of local nodes. Because all the protocols, services, and applications use this common structure, the efficiency can be improved.

Reduce the communication between nodes and improve the efficiency of network communication. Wireless sensor network nodes are densely distributed, if each node to high power communication, aggravate the interference between nodes, and reduce the communication efficiency, and waste the energy of the node. On the other hand, if the transmission power is too small, it will affect the connectivity of the network.

III. SECURITY ANALYSIS OF NETWORK NODES AND ROUTING PROTOCOLS

Agent is actually produced and grouping of object consumption, they belong to the transport layer entity, running at the end host, each agent node automatically be endowed with a unique port number (analog udp/tcp port), agents know nodes connected with it, so that the packet is forwarded to the node, it knows the packet size, type of business, the destination address. Agent class is the base class for all kinds of UDP/TCP classes, and the proxy is saved in a linked list called demux.

Internal attacks, by being captured in the internal network nodes send malicious routing information to other nodes, leaked network password, tampering with inside information. External attacks and internal attacks have destroyed the security and availability of the network, which has become an important factor to restrict the application of wireless sensor networks [5]. Therefore, how to resist external attack, guarantee the safety of network nodes and the routing protocol is the need of practice, but also improve the network security theory, has important scientific research value and significance.

At time until the Adv message is received. The initialization process of the routing backbone network is shown in Fig. 1. In Fig. 1, for sensor nodes in a solitary state s at time t received three adv messages, it selects distance parameter minimum sensor nodes 1 and 2 as its parent node, and add it to a parent node in the collection.

$$C(k) = \sigma^2_{s(k)} \beta(k)\beta(k)^T + \Sigma_{\varepsilon(k)} \tag{2}$$

Under normal circumstances, the base station node and sensor nodes use centralized control structure, but between each sensor node is a kind of distributed control network, network terminal generally has a dual function of routers and hosts, among a host of equal status, the network protocol is implemented in a distributed manner, and so it has very strong robustness and survivability.

Wireless sensor networks in communication between the general multi hop wireless path. The limitations of the node function, for wireless sensor networks, and it is the limitations of mobile terminal function are very prominent. A general assumption is that, because of the limitation of the node's computing power, memory and network bandwidth, the key technology can only be used for the sensor nodes.

When a node receives a message of interest, set up to sink proxy message and a query message is spread in a unicast; rumor routing only maintained a source to destination path, do not like directed diffusion routing maintain many paths. Simulation results show that the routing overhead can be significantly reduced and the energy consumption is saved. The rumor route is only suitable for the event number is relatively small. For the event number, the maintenance of the event table and the cost of the handling agent will increase dramatically. At the same time, due to the use of a random way to generate a path, the path of the data transmission is not the optimal path, and there may be a routing loop problem.

A certain strategy is adopted to wrap around the multi path, which allows the redundant path to intersect the optimal path P, thus reducing the number of redundant paths and saving energy consumption. Winding path after the establishment of the main path P, P, apart from the source end and near the end of the source node, each node to send backup path enhanced message to suboptimal node A and node searching optimal node B communication the alternate path enhanced messages, if B is not on the main path P, continue to the optimal node until the transfer and the main path P intersect.

$$MSE(I_k, I_t) = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} \left[I_k(x,y) - I_t(x,y) \right]^2 \tag{3}$$

According to the model, the mobile node is designed and made [6]. Nodes with low-power MCU MSP430, integrated chip SPI, IIC, 12 bit a / D standard interface can be connected via the SPI interface and RF module CC2420, nodes are designed standard sensor interfaces, can connect to the commonly used sensor module through the interface. In order to facilitate the experiment, the nodes are integrated with the DS18B20 temperature sensor and TSL2561 light intensity sensor. At the same time, the node on the vehicle platform and it is the realization of the mobile node.

Here, the network routing attack methods are summed up as the following: hacking, fraud, tampering or replay (relay) routing information, selective forwarding attacks, "collapse" (sink hole) attack, "witch" Sybil attack, bore hole "wormhole attack hit, hello flood attack strike, a cheat (acknowledgement spoofing). 1 the most direct attack target of the routing protocol which is the most direct attack target is the routing information of the nodes. The attacker by eavesdropping, spoofing, altered or replayed routing information, generating a routing loop, inducement or reject traffic, extend or shorten source routing, produce false error message, separate the network, increase the end to end delay (latency). 2 selective forwarding attack multi hop (hop - Multi) networks are typically assumed to be involved in the transmission of a node that transparently forwards the messages it receives. In selective forwarding attacks, malicious nodes may refuse to forward certain messages and discard them. A simple form of this attack is that a malicious node, like a black hole (Hole Black), refuses to forward the packet it receives. However, the weakness of the attack is that the adjacent node can

recognize the invalid of the malicious node and then select the other route.

When an attacker is in the path of data flow, the selective forwarding attack is the most effective. 3. The sinkhole attack in the sinkhole attack, the attackers is through "mutiny" node lure within a specific area of all traffic. In the center of the region caused similar to "collapse" to the same attack. For example, some protocols are based on the link reliability, delay and other information to verify the routing quality. In this case, an attacker can provide a high quality route with a sufficiently large transmit power. Through the "mutiny" node of a real or virtual high quality routing, the attacker to neighboring nodes is likely to by the attacker to the base station, and packet forwarding, can also to its adjacent nodes to propagate the route. In fact, an attacker to build a big hole, so that all the nodes can be attracted to the base station communication, as is shown by Equation (4) [7].

$$\sigma_i = (\sigma_{i1}, \sigma_{i2}, ..., \sigma_{in}) \tag{4}$$

Automatic extraction of index terms, filtering, retrieval of natural language text, automatic extraction of important information, automatic abstract etc. At the same time, because of the emphasis on "mass", stressed the "real text", the two fundamental work below has been paid attention to and strengthen the. Large scale through different depth of processing real text corpus, the research is based on natural language statistical properties. Without them, the statistical method can only be passive water.

Sybil attacks in Sybil attack, the attacker on the network of other nodes in a number of identities. Sybil attack can be enough to the location based routing protocol has a significant threat. Location aware routing protocol usually requires the node and its neighboring nodes to exchange coordinate information, thus effectively sending data packets marked with the specified address. In general, the nodes receive only a set of coordinate values from its adjacent nodes, but the attackers using the Sybil attack can be "at the same time with multiple locations".

Spin algorithm does not apply to such as meteorological information collection, applications that require periodic reliable transmission of data packet. On the other hand, because of the agreement in a per node only to its one hop nodes to send information, so spin arithmetic for in large wireless network routing tables naming scheme to control those nodes do not need to work, thereby saving energy. Directed diffusion algorithm, set the properties of the data to complete the inquiry of sensor nodes [8]. The establishment of the property and need to properties of a series of value, such as the name for the target, the distance.

IV. ANALYSIS OF SECURITY ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORKS

The specific application environment of wireless sensor network and its inherent characteristics, and the design of the sensor network topology have been proposed. In wireless sensor networks, the nodes need to be fully self organized in the form of autonomous networks, and can work in an unattended environment. Based on local interaction is a basic requirement of self organization. Since the organization's goal is to form a global structure from these local interactions. Based on each node determines the global structure as a framework for other network functions (routing, address allocation, broadcast) services. This structure should be able to adapt to the environment, and to make a correct response to the network changes. Since the organization of a significant feature is that any local changes will only affect the local self organization structure, and will not affect the overall structure. In addition to the structure of this structure is in a limited time to respond.

An attacker only needs to capture a node or a small part of the node, to decipher its local storage network key and routing protocol, you can transform the captured nodes into a malicious node, launched internal attacks. The attacker only needs a very small price; it can be paralyzed local or the entire network, a serious threat to the normal work of the network and data security transmission. Therefore, based on password system security mechanism can only resist external attack, the design idea and realization mechanism are unable to solve the private information has been lost, malicious nodes have access to attack inside the network authentication. Trust evaluation mechanism through mutual cooperation between nodes to effectively identify the malicious nodes, selfish nodes and not as a node, provides a new solution to solve the routing protocol internal attacks and to establish safe and reliable data transmission mechanism.

P is the percentage of the total number of nodes in each round (about 4%-5% of the total number of nodes), R is the current number of nodes, G is not a node set of the cluster head in the past [9]. This type makes each node in a certain number of rounds only become a cluster head node. When r=0, the is T=P, that is, the probability for each node to be the cluster head is P. If a node is a cluster head node, then in the subsequent (1/P-1) wheel, the node will not become a cluster head node. If a node is not the probability of a cluster head node, as is shown by Equation (5).

$$\omega_k^i \propto \frac{p(x_{0:k}^i \mid z_{1:k})}{q(x_{0:k}^i \mid z_{1:k})} \tag{5}$$

MAC protocol of wireless sensor networks is based on spanning tree ST-MAC. This protocol is based on the sink node as the root node, and creates a spanning tree of all nodes in the network. ST-MAC adopts the TDMA access mode, and its inherent low working cycle improves the network performance. Performance analysis and experimental results show that: relative to ST-MAC, S-MAC has better effect on energy saving and time delay.

NS simulation is divided into two levels: one is the otcl programming based hierarchical, using NS existing network elements to achieve the simulation, without making any changes to the NS skill, just write the otcl script. Another level is based on C + + and otcl programming level, if it were not for the required network elements in NS, you need to first of NS is extended to add the required network elements.

But in the trilateration method exists great defects, such as shown in Fig. 2, actually measured by the three distance RP1, RP2, RP3 error exists, leading to RP1, RP2, RP3 is the radius of the establishment of three round and not

intersect in a point, but intersect in a region. The Equation set up is not solved, and the position of the nodes can not be realized at all [10]. In some papers, the location of the particles in the region is proposed. The method is not good, and the error of the node location can be greatly improved with the increase of the intersection area.

According to the actual needs of the goal of routing protocol design routing; then in actual communication process, due to the node energy or security attacks, regularly or irregularly team existing routing were maintenance (delete). As can be seen, in the whole process is not involved in any identification of the problem, as well as can not solve the problem of malicious node tampering request information, or posing as the target node problem. Secondly, there is no monitoring of the security of intermediate nodes. How to ensure the security of the request information to establish the correct path between the source node and the target node is a problem worthy of reference.

Experiments will also enable some sensor nodes to test the failure of the middle. Three gateway nodes are set up in the experiment, they are connected with the wireless network and the wired network, and the communication between the gateway nodes is used. Experimental results are shown in Fig. 2. In the experimental initialization state, the gateway node starts the route backbone network.

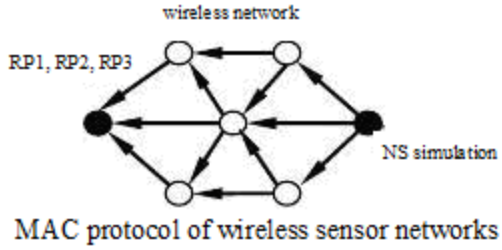

Figure 2. Analysis of security routing protocol for Wireless Sensor Networks.

Experimental data show that this protocol has the advantages of short delay time and low energy consumption compared with the present routing protocol. Another advantage of this protocol is that it has good scalability, and is very suitable for large scale sensor networks. SPIN is the earliest adaptive routing protocol based on data. It can solve the problem of "internal explosion" and "overlap" in the flooding algorithm, and save energy consumption. The protocol is: the more advanced descriptors (also known as metadata) to describe the data, nodes receive data, descriptions of the data broadcast, a sense of interest nodes after receipt of the descriptive information of the data and return the requested information, only after receiving a request to the corresponding node to send the data to the target.

Main goal is to strengthen the security of routing protocol. Therefore, simulation of the main work is inspection of the nodes coordinate calculation is correct, the data transmission and the correct rate and the packet loss rate do not spend too much time talking about. In addition, the experimental results are also analyzed to increase the security verification of the impact on the network load. The simulation program simulates the operation of the 20 nodes, in the layout Tinyviz option, the use of random mode, the coordinates of the unit by the simulator. The test program function is to let the nodes transmit the lightweight packet to the sink node in multi hop mode.

V. SUMMARY

The security objective of the routing protocol is to ensure data integrity, authentication and availability. The recipient only receives the information that the sender wants to send to it, and is capable of verifying the integrity of the message and the identity of the sender. In practical application, it is not the target of security routing to prevent eavesdropping. The security objectives of the routing protocol typically do not include the confidentiality of the data, which should be ensured by other protocols.

The compromised nodes is inevitable, if the damaged node excluded from outside the network, first of all to dynamic update or withdraw damaged key, but at present most plan or agreement is less considered dynamic key management. Existing dynamic key management scheme is more centralized, resulting in excessive computation and communication overhead, key updating and withdrawal should be to collaboration between nodes of the implementation, in order to make the plan or agreement with good distribution characteristics.

REFERENCES

[1] Wei Li, "A Routing Protocol of Combining EADA with AODV Applying in The Wireless Sensor Networks", JCIT, Vol. 8, No. 2, pp. 262 ~ 270, 2013

[2] Sardjoeni Moedjiono, Aries Kusdaryono, Teddy Mantoro, "Energy Efficient Base Station Assisted Cluster Routing Protocol in Wireless Sensor Networks (BCRP)", IJACT, Vol. 6, No. 4, pp. 01 ~ 13, 2014.

[3] Sardjoeni Moedjiono, Aries Kusdaryono, Teddy Mantoro, "Wireless Sensor Network Energy Efficient Layer based on Hierarchical Routing Protocol (LHRP) Optimization", JCIT, Vol. 9, No. 4, pp. 12 ~ 22, 2014.

[4] Yusheng JIANG, Fang GUAN, Chao MA, Hui WANG, "Distributed and Steady Unequal Clustering Routing Protocol for Heterogeneous Wireless Sensor Networks", JDCTA, Vol. 7, No. 9, pp. 352 ~ 360, 2013.

[5] Zifu Fan, Mei Yang, Xiaoyu Wan, "Research on QoS-Based AOMDV Routing Protocol in Wireless Sensor Network", JCIT, Vol. 8, No. 3, pp. 568 ~ 575, 2013.

[6] Muhammad Haneef, Deng zhongliang, "Design Challenges and Comparative Analysis of Cluster Based Routing Protocols Used in Wireless Sensor Networks for Improving Network Life Time", AISS, Vol. 4, No. 1, pp. 450 ~ 459, 2012.

[7] Xu Bao, "Energy Efficient Cluster-Based Routing Protocol for Wireless Sensor Network", JCIT, Vol. 7, No. 22, pp. 101 ~ 109, 2012.

[8] Wang Hai-Bo, "Study on the Energy Consumption Balance WSN Routing Protocol Based on Improved Genetic Algorithm", IJACT, Vol. 4, No. 22, pp. 460 ~ 467, 2012.

[9] Ouyang Xi, Zhang Jianyi, Gong Zhe, Li Qi, "A Reputation-based Ant secure routing Protocol of Wireless Sensor Networks", IJACT, Vol. 4, No. 9, pp. 10 ~ 18, 2012.

[10] Zhang Hanjun, "Dynamic Clustering Routing Protocol for the Grid-based Wireless Sensor Networks", JDCTA, Vol. 6, No. 12, pp. 342 ~ 349, 2012.