Information Hiding data security based on Wireless Sensor Networks

Zhidan Wang
Zhengzhou university of industrial technology.Henan.China

Keywords: Wireless sensor networks; network secure; information hiding; received signal strength indication (RSSI)

Abstract. Information hiding technology is very important to wireless sensor network security, copyright protection and so on. This paper uses RSSI (Received Signal Strength Indication) as hidden information carrier and designs a Information Hiding Algorithm (RIHA). It does not affect original data or bring additional communication cost. RIHA is a novel information hiding method, which is very suitable for resource constrained wireless sensor networks. The simulation results show that RIHA has high hidden information transmission accuracy without bringing additional communication energy consumption. RIHA provides a new way for information hiding technology in wireless sensor networks.

INTRODUCTION

Wireless sensor networks (WSN) are self-organized distributed multi-hop wireless networks consisted by sensor nodes with limited communication and computation capabilities deployed in the monitoring region [1]. They are widely used in many fields, such as national military defense, environment monitoring and protection, geological disasters forecast, mineral resources exploration, traffic monitoring and management etc.

In the battlefield, sensor networks are often used to perceive equipment deployment, spy enemy's condition and terrain information, locate targets, evaluate battlefield losses, scout dangerous attack, and so on. The information WSN sampled could be used to analysis battlefield situation. These important data be obtained or falsified by enemy will cause serious consequences. However, sensor networks did not consider security issues in the protocol design stage, did not establish a perfect security system, which is a huge security risk [2]. Therefore, research on sensor network security has important theoretical significance and application value.

At present, research on sensor network security has made great progress, many techniques in sensor network security are proposed [3][4], These schemes are mainly concentrated in the field of encryption technology [5], such as data encryption, message authentication, integrity authentication and radio identification. As sensor nodes' computation, storage and communication capabilities are limited, complex encryption and decryption mechanisms are unable to realize in sensor nodes. It's difficult to address security issues in sensor networks.

The birth of information hiding technology brought new opportunities for the study of sensor network security. Information hiding is a new field of information security in recent ten years. Its basic idea is hiding information in public media, the information is hard to found. Others cannot get embedded information without key even when the information is found [6]. The information hiding technology has unique advantages compared with cryptogram technology. Researches on sensor network information hiding technology are numbered, and most of them add hidden information in the transmission data, which increases the computation and communication consumption.

This paper does not use conventional carrier such as image information, video information, text information, database information [7][8], it takes the received signal strength indication (RSSI) as carrier according to the characteristics of sensor networks. The information hidden in RSSI does not change original data, dose not increase data transmission amount, does not bring extra communication overhead, which is a new exploration of information hiding technology in sensor networks.

The main contents of this paper are as follows:

(1) Taking RSSI as hidden information carrier in wireless sensor networks, which is a new way for sensor network information hiding.

(2) Designing a RSSI based information hiding algorithm (RIHA), and using redundancy to improve the accuracy of hidden information transmission.

(3) Theoretical analysis and simulation experiment prove the reliability and validity of RIHA. It transmits hidden information accurately without extra communication consumption, which is suitable for wireless sensor networks.

The structure of the paper is as follows: The second part introduces the research status on sensor network information hiding technology. The third part analyses the feasibility of using RSSI in sensor network information hiding, and designs RSSI based information hiding algorithm. The fourth part proves the performance of RIHA through simulations. The fifth part summarizes the work of this paper.

RESEARCH STATUS

Information hiding technology is widely used in data security, intellectual property right protection, covert communication and other fields, which is an important method to guarantee network data security. The traditional information hiding algorithms in network security domain have high computational complexity and large amount of transmission, which can not be applied in sensor networks directly. The research result for sensor network information hiding is very limited [9].

Due to sensor nodes allow micro-error between actual value and measured value, RWT (Real-time Watermarking Techniques) embeds hidden information in the measured value [10]. It doesn't affect the use of sensory data when the error caused by embedded hidden information does not exceed the limitation. The hidden information can be extracted from the error. ID Modulation embeds sensory data into time series of RFID (Radio Frequency Identification) as node's authentication [11]. The node sends the synchronization code, calculates the transmission delay according to the embedded information, and then cross transmits information using two different radio frequency chips. The receiver extracts embedded hidden information according to the information delay after synchronization.

RFW (Radio Frequency Watermarking) is a radio frequency watermarking technique for OFDM (Orthogonal Frequency Division Multiplexing) sensor networks [12]. It makes use of spread spectrum technology, conducts base band signal waveform modulation on the physical layer, and extends a watermark energy spectrum to a very wide frequency band. The energy assigned to each frequency band is very small, embedded hidden information difficult to be found. Sion et al. propose hidden information in data stream realize copyright protection [13]. The data is regarded as discrete data flow, and transformed to eligible data to hide information based on information acquisition time.

Honggang Wang et al. use a wavelet based adaptive watermarking algorithm for wireless image sensor networks. The image watermarking information can be identified as embedded in the transmission data [14]. CW (Chaining Watermarks) aims at characteristic of streaming data [15]. It first determines the synchronization point according to the collected data, and then groups the data, generates and embeds watermark information with two sets of data.

Sum up, existing information hiding techniques do not consider the constraint of data processing ability, computation ability, and power supply of sensor networks [16]. Some of them require complicated calculation or increase the energy consumption of data communication; some of them cause a long time delay, which are difficult to practical application. RIHA is different from existing techniques, which adopts RSSI as hidden information carrier to guarantee accurate hidden information transmission. It does not change the original data, does not need complex calculation, and does not increase communication overhead. It is suitable for wireless sensor networks.

RSSI BASED INFORMATION HIDING

In this section, we introduce the characteristics of RSSI first, and analyze the feasibility of taking it as hidden information carrier. Then we design the RSSI based information hiding algorithm which is called RIHA, and analyze its performance in theory.

A. Feasibility analysis

In resource constrained sensor networks, gathering RSSI value is "free lunch", because it neither adds communication overhead nor increases network burden. It is widely used in node location, target tracking, protocol design and so on.

Although RSSI changes with environment, a large number of studies show that the variation has certain regularity. Generally log distance path loss model is used to describe wireless signal propagation energy variation in wireless sensor networks [17]:

$$RSSI(d) = P_T - P_L(d_0) - 10\eta \log_{10} \frac{d}{d_0} + X_\sigma \quad (1)$$

In which, P_T is the emission energy, $P_L(d_0)$ is the path loss of propagation unit distance d_0. The unit of energy is *dBm*, the unit of distance is *m*. η is the path attenuation index, its value between 2 and 5. Random Gauss function $X_\sigma = N(0, \sigma^2)$ represent the uncertainty of RSSI, σ between 4 and 10, its value depends on the actual environment.

RSSI relates to initial transmit power and path loss, path loss can be computed out when the environment and distance is known. Thus the initial transmit power is the main factor of RSSI. Existing sensor nodes can set different transmit power to meet different application requirements. Adjusting node's transmit power could obtain corresponding RSSI that provides the feasibility of information hiding. The sending node uses different transmit power to deliver hidden information, and the receiving node restores the hidden information from received RSSI value.

As RSSI varies with spatial and temporal, taking it as hidden information carrier is undetectable. This method does not require complex computation, does not change original data, does not affect communication process, and does not bring additional energy consumption. It is very suitable for source limited wireless sensor networks. It not only can be used in hidden information transfer and extract, but also can be used in network data integrity protection, security transmission check and etc.

B. Algorithm design

In order to improve the discrimination and reduce the fluctuation impact of RSSI, RIHA uses the maximum transmit power behalf of 1, and the minimum transmit power behalf of 0. RIHA sets the upper and lower limit values of RSSI, if sampled RSSI value greater than the upper limit value represents the hidden information is 1, if it less than the lower limit value represents the hidden information is 0.

Before hidden information transmission, coding rules should be determined. Coding rules are set before node deployment, and be used after deployment. In order to improve network security, the base station changes the coding rules by broadcasting periodically. Thus, hidden information cannot be obtained without coding rules, which improves network security greatly.

RIHA can be divided into three steps: establish hidden information transmission link; transmit hidden information; release hidden information transmission link.

The first step: establish hidden information transmission link.

Sensor nodes select transmit power randomly to send routine data when there is no hidden information to be sent. A node with hidden information to be transmitted is called source node. The source node sends a link establish request information according to the decided rule, for example, the sequence of "maximum power - minimum power" repeats *n* times. Then it sends the hidden information receiving node's ID according to the encoding rule.

The node receives the link establish request information, for example, received information's RSSI with the sequence of "larger than the upper limit - less than the lower limit" repeated *n* times. Then it judges whether to receive the hidden information according to the node ID received subsequently. The receiver will work normally when the received node ID neither matches its ID nor

in its routing table. The receiver will become destination node when the received node ID matches its ID or in its routing table. The destination node sends a confirmation message to the source node in accordance with the decided rule. The hidden information transmission link is established. If the hidden information transmits through multi hop routing, repeat above steps until the integral information transmission path is established.

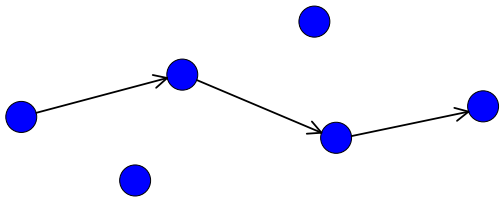

Figure 1. RSSI based information hiding

In order to explain RIHA better, take figure1 for example. The decided rule is 8421 code, nodes are used to collect temperature, humidity information, and transmit suspicious target position with covert. Node 1 (ID code 0001) finds the suspicious target, it has to send the target's position (6, 8) (coordinate code 01101000) to node 6 (ID code 0110).

Node 1 sends *n* times of temperature and humidity information with the sequence of "maximum power - minimum power". Then it sends temperature and humidity information with the sequence of "minimum power - maximum power - maximum power - minimum power" in accordance with node 6's ID code "0110". Node 2 receives this information, "0110" does not match its ID and not in its routing table, it does not do any treatment. Node 3 finds that the ID in its routing table. It sends confirm information to node 1 and establishes transmission link. Then, node 3, node 5 and node 6 establish the transmission link in the same way.

The second step: transmit hidden information.

After the transmission link is established, the source node begins to send hidden information in accordance with the determinate coding rule. The destination node decodes hidden information according to the coding rule. If the hidden information transmits through multi-hops routing, intermediate forwarding nodes do not decode the information. They only determine the information transmit power, and send message with the same transmit power until the information is transferred to the destination node or base station.

However, RSSI is fluctuating due to interference and other reasons, especially in the disrupting situation like battlefield. And packet loss also brings hidden information decode error. Redundant information is used to improve the reliability of hidden information transmission. The source node sends information with the transmit power correspond to the hidden information repeatedly, rather than each hidden information's transmit power used only once. The number of repetition depends on the environment and packet loss rate. The destination node uses filtering algorithm to dispose received RSSI, checks received information integrity and corrects error to get more accurate and effective information.

Still using the example of figure 1, the transmit power of each hidden information is used 3 times. That is to say node 1 sets different transmit power in accordance with the sequence of "000 111 111 000 111 000 000 000" to send temperature and humidity information. Node 3 does not decode the hidden information, it judges the transmit power and sends message to Node 5 with the same transmit power. In the same way, Node 5 forward information to Node 6. Node 6 uses filtering algorithm to handle received RSSI value, such as average filtering and so on, then it could get the position of target.

The third step: release hidden information transmission link.

The source node sends link release request information according to the decided rule when the hidden information transmission complete. For example, it sends *m* regular data with the sequence of "maximum power - minimum power - minimum power". The destination node receives link release

request information, and sends a confirmation according to the determined rule. The information transmission link is released, and the hidden information transmission process complete.

As shown in figure 1, when the data transmission is complete, node 1 sends temperature, humidity information *m* times with the sequence of "maximum power - minimum power - minimum power". Node 3 sends a confirmation message to node 1. It sends temperature, humidity *n* time with the sequence of "maximum power - minimum power - minimum power", and gets the confirmation of node 5. In the same way, Node 5 obtains node 6's confirmation. The transmission process of hidden information is over.

In many applications, networks transmit hidden information all the time which does not need to establish and release the transmission link frequently. In this case, the first step runs only one time after network deployment. Nodes transmit hidden information with routine data until died without running the third step.

C. Performances analysis

Generally, sensor nodes' transmit power can be divided into more than 30 levels, RIHA only makes use of the highest and lowest transmit power, and filters are used at the receiving end, which is sufficient to distinguish RSSI value. Therefore, the rate of packet loss is the greatest impact factor for receive hidden information correctly. Assume the number of continuously received signal in the same strength section is N_{RSSI}, the repetition number of each hidden information code is T_N, the number of encoding message in the same section I_R is:

$$I_R = \left\lceil \frac{N_{RSSI}}{T_N} \right\rceil \quad (2)$$

The number of continuously send hidden information in the same section is I_S, network packet loss rate is $Loss$, to ensure $I_s = I_R$, then

$$I_S * T_N * Loss < T_N$$

$$I_S < 1/Loss \quad (3)$$

Thus, to ensure receiving hidden information correctly, the number of continuous hidden information coding in the same section should less than the reciprocal of packet loss rate.

The hidden information transmission delay relates to the hidden information code number and time of iteration. The hidden information transmission delay is $I_S * T_N$. Visibly, increasing the repetitions of hidden information coding improves reliability, but also increases transmission delay. We should regulate the repetition time according to the environment and data's importance degree.

In addition, the amount of hidden information associates with the coding rules, simple coding rule's information hiding ability is limited, coding rules with large information hiding capacity often more complex in computation. It should consider the requirement of information hiding and design rational encoding rules.As can be seen from the figure, energy consumption of hidden information transmission almost the same as no hidden information transmission in the first half, and increases in the last half slightly. It related to the encoding rule and data to be transmitted. In this simulation, the middle part and the last part of hidden information have several 1 multiply, so that the node has to transmit information with maximum power continuously, which leads the increase of energy consumption. Sending more 0 in hidden information will make its energy consumption lower than no hidden information transmission. That is to say the network energy consumption depends on the original data, whether transmission hidden information has little effect on it.

CONCLUSIONS

This paper researches on the RSSI based information hiding technology in wireless sensor networks. RSSI is used as hidden information carrier, a RSSI based information hiding algorithm is designed. Its calculation process is very easy. The simulation results show that RIHA can realize hidden information transmission and extraction efficiently. It does not change original data, does not affect transmission process, and does not bring additional communication consumption, which is

suitable for resource constrained sensor networks. It is a new research approach for information hiding technology in wireless sensor networks.

REFERENCES

[1] Horneber J., Hergenroder, A., A survey on testbeds and experimentation environments for wireless sensor networks, *IEEE Communications Surveys & Tutorials*, 2014,16(4):1820-1838.

[2] Hailun Tan, John Zic, Sanjay Jha, Diethelm Ostry. Secure multihop network programming with multiple one-way key chains. *IEEE Transactions on Mobile Computing*, 2011, 10(1): 16-31.

[3] Silva F., Industrial Wireless Sensor Networks: Applications, Protocols, and Standards, *IEEE Industrial Electronics Magazine*, 2014, 8(4): 67-68.

[4] Bielefeldt J., Chellappan S., Sensor authentication in collaborating sensor networks, *13th Annual Mediterranean Ad Hoc Networking Workshop*, 2014, 55-62.

[5] K.P. AlSakib, T.D. Tran, S.H. Chong. A key management scheme with encoding and improved security for wireless sensor networks. *ICDCIT 2006*, 102-115.