Security of Intelligent Building Network Based on Wireless Sensor Network

https://doi.org/10.3991/ijoe.v14i06.8705

Shuang Xu(✉), Tong Zhou
Zhengzhou Institute of Technology, Zhengzhou, China
xushuangcardi@126.com

Abstract—In order to study the intelligent buildings, the intelligent building network security of wireless sensor was explored. Because of its advantages of low cost, easy installation, low maintenance and update cost, wireless sensor network system was applied to intelligent building. In view of the characteristics of various influencing factors on the wireless sensor network working environment, node hardware cost and location accuracy, a secure localization algorithm based on DV-Hop was put forward. The security analysis results showed that the algorithm resisted external attacks and guaranteed the accuracy of location results. Based on the above findings, it is concluded that the algorithm can be used to protect the safety of wireless sensor network in building.

Keywords—Intelligent building, wireless sensor network, security positioning, DV-Hop

1 Introduction

The concept of intelligent building has been widely promoted and developed worldwide since its emergence in the early 1980s. With the progress and development of the times, the scope of "intelligent building" is also developed and enriched. For intelligent building, the faster the technology development and update is, the richer the connotation is, the more difficult the construction of its engineering is, and the higher the requirements for its related technology are. Usually, a large number of sensor nodes are required to monitor the surrounding environment in intelligent buildings. The control system adjusts the surrounding environment according to the monitored data to make them in the best working condition. The monitoring network composed of wired sensors not only has large wiring capacity, high installation and maintenance cost, and poor reliability, but also can't carry out wiring in some buildings in some places. In addition, with the adjustment of the function of the building area, it may be necessary to rearrange the position of the sensor, which takes a lot of manpower and material resources. Wireless sensor networks overcome the disadvantages of large amount of wiring, high cost, and difficult maintenance of wired sensor network. As a result, it can conduct real-time monitoring, sensing and collecting all kinds of environmental or monitoring objects information. In addition, it has great application value and potential application prospect in military, industry, medi-

cal, intelligent building, environmental monitoring, traffic management, disaster relief and other fields. Because wireless sensor network technology has the advantages of convenient and rapid deployment, as well as low cost of wiring and network maintenance, wireless sensor network is especially suitable for application in intelligent building control system. Especially in recent years, with the development of wireless communication technology ZigBee, the BACnet protocol widely used in intelligent building control system can also be transmitted on the ZigBee wireless link, and the sensor nodes supporting BACnet protocol also start to appear. At present, wireless sensor network technology has begun to penetrate into the monitoring of intelligent building and become a hot topic in this field.

2 State of the art

First of all, on the basis of analyzing topology of wireless wireless sensor network, a topology of wireless sensor network suitable for intelligent building is given. And then, the characteristics of wireless sensor networks safety in intelligent buildings are analyzed. At last, some reasonable assumptions are made according to the actual situation of wireless sensor network in intelligent building.

2.1 Topology structure of wireless sensor network in intelligent building

Because of the large number of sensor nodes and the larger scale of the sensor network in the intelligent building, it is not suitable to adopt a planar topology. But using the hierarchical topology directly in the wireless sensor network of intelligent building, there are the following problems:

In order to communicate between the cluster head nodes, the cluster head nodes need to communicate with high power. Although it is easier to select some resource sufficient nodes as cluster head nodes in intelligent buildings, it will exacerbate the interference between nodes, reduce communication efficiency, cause the waste of node energy and reduce the life cycle of nodes. More importantly, there are many factors affecting the spread of indoor wireless signal, and the wireless signal long distance transmission not only has great consumption, but also causes signal loss.

Nowadays, the area of intelligent building is large, while the communication ability of cluster head nodes is limited. There is no direct communication between cluster head nodes and Sink nodes, which needs to transfer through other cluster head nodes. Thus, when the sensor node transfers the collected signal to the Sink node through cluster head node, it needs to transfer through multiple cluster head nodes. It not only increases the possibility of transmitted data packet loss, but also increases the time delay of data packet transmission. In intelligent buildings, many data collected by sensor nodes are very timeliness. In intelligent building wireless sensor networks, it is unnecessary to have many hops from sensor nodes to Sink nodes.

According to the above analysis, the characteristics of the intelligent building make it impossible to use the planar topology and the hierarchical topology of the sensor network directly. Because the data transfer in the buildings of wired networks is little

affected by environment and data transmission has higher reliability, in the control system of intelligent building, the wireless network cannot completely replace the wired network. Suryadevara, N. K. et al. [1] studied intelligent sensors and actuators based on wireless sensor networks in smart power management buildings. When deploying wireless sensor networks in the intelligent building, we can use the network system with wired and wireless combination. Chen, M. et al. [2] studied cloud based wireless networks: virtualization, reconfiguration, intelligent wireless networks, and 5G technology. Li, J. Q. et al. [3] put forward an intelligent wireless sensor network system for multi-server communication. The sensor nodes are grouped according to the geographic location of sensor nodes, such as floors, rooms and so on. Each group sensor node consists of a sensor sub network, and the sub network is communicated through the wired network. Batalla, J. M. et al. [4] proposed a low-cost and highly scalable wireless sensor network solution, which can provide intelligent LED lighting control for green buildings.

Because the BACnet control network has begun to occupy a dominant position in the intelligent building, and gateway products interconnecting wireless sensor networks and wired BACnet network has also emerged, here we take wired control network based on BACnet in intelligent building as the backbone network. BACnet gateway is regarded as the sub Sink node of each sensor network, to show the topology of wireless sensor network in intelligent building, as shown in figure 1. In the whole network, the main Sink node does communicate directly with sensor nodes, just controlling the operation of sub Sink node. Magno, M. et al. [5] pointed out that between the main Sink node and sub Sink node, the network communication is controlled through the wired BACnet. The sub Sink nodes directly control the wireless sensor network operation and process the data sent by the sensor nodes. The sensor node uses the transfer of sub Sink node to send the collected to the main Sink node.

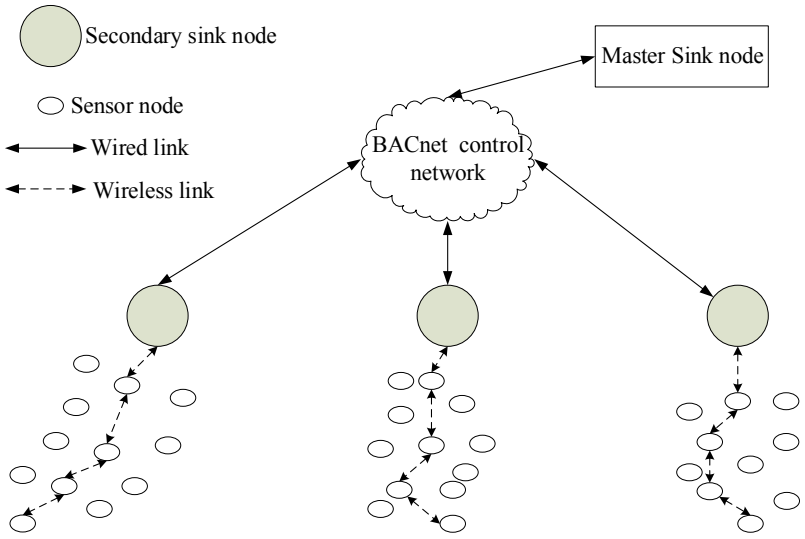

Fig. 1. Wireless Sensor Network Topology in Intelligent Buildings

The topology structure of wireless sensor network in intelligent building in figure 1 is actually a two-layer network structure. It includes a main Sink node and multiple sub networks (equivalent to "cluster" in the hierarchical structure), where each sub network comprises a sub Sink node (equivalent to "cluster head" in the hierarchical structure, which is shouldered by the BACnet gateway) and some sensor nodes. Between the upper nodes and between the upper node and the Sink node, we use the wired network communication; between the lower nodes, and between the lower nodes and the upper nodes, we use wireless communication. Al-Sakran, H. O. [6] studied the intelligent traffic information system based on the integration of the Internet of things and Agent technology. The sensor node transfers the collected data to the sub Sink node through the wireless channel firstly. Then, the sub Sink node converts the data into the BACnet protocol format, and transmits to the main Sink node through the wired BACnet network. Similarly, when the main Sink node issues queries and so on commands to the sensor nodes, the command and other information are transmitted to the sub Sink nodes through the wired BACnet network. Then, each sub Sink node transfers the command information to the sensor nodes in each sub network through the wireless channel. This network topology makes full use of the advantages of the reliable transmission of the wired network and the convenient deployment of the wireless network.

2.2 Security analysis of wireless sensor network in intelligent building

Based on wireless sensor networks and power line communications, Li, M. and Lin, H. J. [7] designed a smart home control system. The security problem of wireless sensor network in the application of intelligent building is a necessity in the first consideration. Peng, C. et al. [8] studied the design and application of the VOC monitoring system based on ZigBee wireless sensor network. If the security system of the network is destroyed, it will not only bring economic losses and sometimes threatens the safety of people's life. Based on wireless sensor networks, Zhou, P. et al. [9] studied large indoor space monitoring systems, including data processing and gas distribution optimization. For example, in the event of a fire, if the sensor network is damaged, then the detected data may not be transferred to the fire control center.

Rawat, P. et al. [10] investigated the recent development and potential synergy of wireless sensor networks. In intelligent building, security problems in wireless sensor networks and those in other sensor networks are similar. Rashid, B. and Rehmani, M. H. [11] pointed out that the wireless sensor network in intelligent building has its own characteristics, making the security problems and solutions of sensor network in intelligent buildings different. Because intelligent building is an open environment, the deployed sensor nodes are easy to be physically captured by attackers. Therefore, when dealing with the safety of wireless sensor network (WSN) in intelligent buildings, we need to pay special attention to attacks from inside. In addition, the lifetime of sensor networks in intelligent building is very long. In the design of security scheme, it is necessary to guarantee a long time to provide security.

To sum up, the existing research does not solve the security problem of wireless sensor network in intelligent building. In view of the characteristics of various influ-

encing factors on the wireless sensor network working environment, node hardware cost and location accuracy, a secure localization algorithm based on DV-Hop was put forward. The security analysis results showed that the algorithm resisted external attacks and guaranteed the accuracy of location results. Therefore, the algorithm proposed in this paper can be used to protect the safety of wireless sensor network in building.

3 Security of wireless sensor network in intelligent building

Many applications of wireless sensor networks in intelligent buildings depend on location information of sensor nodes. For example, when fire occurs, we need to know the location of fire, and when someone invades, we need to know where the intruders are. Though nodes are deployed manually in intelligent building wireless sensor networks, due to the large number of sensor nodes, it is not practical to set positions for each node manually. It is not possible for each node to configure a global positioning system GPS because of the limitations of cost and the use of environment. Because of the effects of building environment complexity and the resource constraints of sensor nodes, many traditional wireless location algorithms cannot be directly applied to sensor node localization in buildings. In addition, the wireless sensor network in the building is working in an open environment, so the location of sensor nodes in the building is vulnerable to attack. This chapter first of all analyzes the location mechanism and location security problem in wireless sensor network. And then, it designs a secure localization algorithm suitable for wireless sensor networks in intelligent buildings according to the characteristics of wireless sensor networks in intelligent buildings.

3.1 Node location of wireless sensor network

In the localization technology of wireless sensor network, according to whether the node knows its location, sensor nodes can be divided into beacon nodes and unknown nodes. Beacon nodes occupy very small proportion in the network, and can get their exact location by carrying GPS devices or other means. In the process of sensor node localization, when unknown nodes get the distance from adjacent beacon nodes or get the relative angle between adjacent beacon nodes and unknown nodes, their positions can be calculated according to the following methods.

The algorithm of triangulation is as follows: it is known that the coordinates of the three nodes A, B and C are (x_a, y_a), (x_b, y_b), and (x_c, y_c), respectively, the distance from them to the unknown node D is d_a, d_b, and d_c, respectively, and it is assumed that the coordinate of node D is (x, y), then there is the following formulas (1) and (2):

$$\begin{cases} \sqrt{(x-x_a)^2+(y-y_a)^2} = d_a \\ \sqrt{(x-x_b)^2+(y-y_b)^2} = d_b \\ \sqrt{(x-x_c)^2+(y-y_c)^2} = d_c \end{cases} \quad (1)$$

The coordinate of the node D can be obtained by (1).

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2(x_a - x_c) & 2(y_a - y_c) \\ 2(x_b - x_c) & 2(y_b - y_c) \end{bmatrix}^{-1} \begin{bmatrix} x_a^2 - x_c^2 + y_a^2 - y_c^2 + d_c^2 - d_a^2 \\ x_b^2 - x_b^2 + y_a^2 - y_c^2 + d_b^2 - d_a^2 \end{bmatrix} \tag{2}$$

Triangulation as shown in Figure 2, it is known that the coordinates of the three nodes A, B and C are A (x_a, y_a), B (x_b, y_b), and C(x_c, y_c), respectively, the angles of the unknown node D relative to the nodes A, B, and C are □ADB, □ADC, and □BDC, and it is assumed that the coordinate of node D is (x, y). For nodes A and C and the angle □ADC, if the arc AC is in □ABC, it can only determine a circle. The center of circle is set to O_1 (x_{O1}, y_{O1}) and the radius is r_1, then α=□AO_1C=(2π-2□ADC), and expressed by (3):

$$\begin{cases} \sqrt{(x_{o_1} - x_a)^2 + (y_{o_1} - y_a)^2} = r_1 \\ \sqrt{(x_{o_1} - x_c)^2 + (y_{o_1} - y_c)^2} = r_1 \\ (x_a - x_c)^2 + (y_a - y_c)^2 = 2r_1^2 - 2r_1^2 \cos\alpha \end{cases} \tag{3}$$

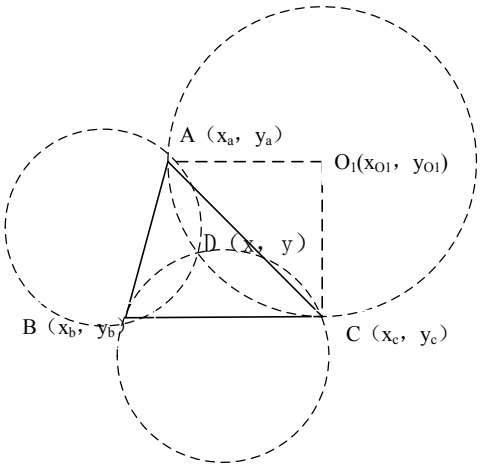

Fig. 2. Triangulation icon

The algorithm of Maximum Likelihood Estimation is: it is known that the coordinates of n node are (x_1, y_1), (x_2, y_2),…, (x_n, y_n), the distances from the unknown node D to them are d_1, d_2,…,d_n, and assuming that the coordinate of node D is (x,y), then, there is the following formula:

$$\begin{cases} (x - x_1)^2 + (y - y_1)^2 = d_1^2 \\ \vdots \\ (x - x_n)^2 + (y - y_n)^2 = d_n^2 \end{cases} \tag{4}$$

The last equation is subtracted from the first equation, and (5) is obtained.

$$\begin{cases} x_1^2 - x_n^2 - 2x(x_1 - x_n) + y_1^2 - y_n^2 - 2y(y_1 - y_n) = d_1^2 \\ \vdots \\ x_{n-1}^2 - x_n^2 - 2x(x_{n-1} - x_n) + y_{n-1}^2 - y_n^2 - 2y(y_{n-1} - y_n) = d_{n-1}^2 \end{cases} \tag{5}$$

The linear equation of (5) can be expressed by (6): AX=b

$$X = \begin{bmatrix} x \\ y \end{bmatrix}, \mathrm{A} = \begin{bmatrix} 2(x_1 - x_n) & 2(y_1 - y_n) \\ \vdots & \\ 2(x_{n-1} - x_n) & 2(y_{n-1} - y_n) \end{bmatrix},$$

$$\mathrm{b} = \begin{bmatrix} x_1^2 - x_n^2 + y_1^2 - y_n^2 + d_n^2 - d_1^2 \\ \vdots \\ x_{n-1}^2 - x_n^2 + y_{n-1}^2 - y_n^2 + d_n^2 - d_{n-1}^2 \end{bmatrix} \tag{6}$$

The coordinates of the node D can be obtained by using the standard minimum mean square method as $\hat{X} = (A^T \mathrm{A})^{-1} A^T b$.

3.2 Security analysis of node location in wireless sensor network

The attack on node location can be divided into external attack and internal attack. External attack refers to that the attacker does not get the system authentication and authorization, unable to access the network. But the internal attack refers to that the attacker becomes the attack issued by the system recognized "legitimate nodes" to the network. An attacker can be captured sensor nodes, or sensor nodes forged according to the legitimate nodes information obtained (including the key information, code, data and so on). Obviously, the internal attack is more difficult to detect and prevent than the external attack, and it is more dangerous. Now, in most of the location algorithms design, the security problems are not fully considered. Therefore, there are many kinds of attack methods for these algorithms, and the common attacks are as follows:

False positioning information: By cheating and tampering the location information, the attacker can deceive the location node to generate the wrong location information.

Replay the attack. This is the easiest and most common way of attack. Attackers can delay the intercepted location information for a period of time, replay it, or relocate information from this location to other locations to replay. As a result, the location node can calculate the wrong location based on the replay information. In hops-based location algorithms, the attacker can use replaying message to make the location node get the error value of the minimum hops from the beacon node.

Sinkhole attack: The attacker's goal is to seduce all the nearby nodes, causing a similar "collapse" attack in the center of the area. An attacker makes all of the surrounding nodes think that it is close to the beacon node with a low number of hops.

Sybil attack: A malicious node forges it to be a false image of multiple nodes, allowing the location node to receive the location information of multiple reference nodes from one node.

Wormhole attack: In Wormhole attack, two malicious nodes collude together to receive messages in partial network through a very small delay link, transmit by tunnel, and replay these messages in different parts of the network. Because the localization algorithm based on ranging positions according to the physical information of measurement reference node signal, and the localization algorithm free from range positions by referring to node signal content, compared with the localization algorithm based on ranging, range free localization algorithm is more vulnerable to Wormhole attack.

An attack on a false beacon node: This is the most serious attack mode of attack. The attackers disguise as beacon node to send false location information to the positioning node. Most location algorithms locate and calculate based on the information of all beacon nodes. In these algorithms, the attacker can make false localization information by impersonating a beacon node so that all the location nodes can locate errors.

3.3 Safety positioning method of sensor nodes in intelligent building

The basic idea of this algorithm is to use the key chain for the certification of beacon node identity. The mean value is replaced by median in the DV-Hop algorithm, and each beacon node is assigned a weight value. In this algorithm, the communication between all beacon nodes and Sink nodes is authenticated by the key shared between the beacon node and the Sink node. The broadcast message mechanism of the Sink node is based on the broadcast authentication mechanism proposed. The localization process of the algorithm is divided into four stages:

The first phase is authentication key preposition: Each beacon node selects a random number R_0 as the initial key of its identity authentication, and conducts multiple Hash operations for R_0. It generates an authentication key: R_0, R_1,...,R_N, where $R_i=H^i(R_0)$, N is the maximum hops between nodes in the network, and H () is a Hash function. The last authentication key RN generated by each beacon node is prepositioned or stored in each node through a secure channel. Each node sets the number of hops from all the beacon nodes to N.

The second phase calculates the minimum hop number of the unknown node and each beacon node. Initiated by each beacon node, each node i broadcasts a location request information to its neighbor node: S_i—>*:{ID(A), P(A), h_i(A), Id_i, R_i(A)}. ID(A) is an identifier of beacon node A, P(A) refers to location information of beacon node A, hi(A) means the hop of node i to beacon node A, and R_i(A) indicates the authentication key of beacon node A stored on the node i. When the node itself is the beacon node A, h_i(A)=0. R_i(A) suggests the initial key R_0(A) authenticated by beacon node A.

In the third stage, the average distance of each hop and the weight of the beacon node are calculated. In order to reduce the effect of abnormal data, the average distance of each jump is calculated by a method different from the DV-Hop. Suppose

that there are n beacon nodes in the system. First of all, the beacon node i calculates the corresponding hop distance based on (7) according to the location information and the hop count of each beacon node.

$$HopL_{ij} = \frac{\sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}}{h_{ij}} \tag{7}$$

In (7), (x_i, y_i) and (x_j, y_j) are the coordinates of the beacon nodes i and j, respectively. h_{ij} suggests the hop number between the beacon node i and j($j \neq i$).

In this way, the beacon node i calculates a series of each hop distance as $HopL_{i,1}$, $HopL_{i,2}$,…,$HopL_{i,j}$,…,$HopL_{i,n-1}$, ($j \neq i$). The beacon node i takes the median of these values as each hop distance $HopL_i$ calculated by the beacon node i. Then, the beacon node i calculates the weight value of the beacon node j according to (8).

$$W_j = 1 - \left(HopL_{ij} - HopL_i\right)^2 / r^2 \tag{8}$$

Here, the minimum of W_j is zero, namely when $W_j<0$, $W_j=0$; r refers to the communication distance of sensor nodes.

The fourth stage is the calculation of the unknown node location: When the unknown node receives the location information sent by the Sink node, the weight-based likelihood estimation method can be used to calculate the coordinates according to the following formula.

$$\begin{cases} w_1[(x - x_1)^2 + (y - y_1)^2] = w_1 d_1^2 \\ \vdots \\ w_n[(x - x_n)^2 + (y - y_n)^2] = w_n d_n^2 \end{cases} \tag{9}$$

4 Simulation results of security positioning algorithm for sensor nodes in intelligent building

We simulate and analyze the calculation performance and security performance of the proposed algorithm, respectively. In simulation operation, 200 sensor nodes are randomly deployed in the square area of 100m * 100m. The communication distance of each sensor node is 15m, and the proportion of beacon nodes is 20% when conducting security analysis and simulation experiments.

From the description of the algorithm, it can be seen that, in computation, the scheme, compared with the DV-Hop algorithm, only conducts several Hash calculation to judge the validity of the received message in the calculation of the unknown nodes and each beacon node minimum hop count. In communication amount, in the calculation of the unknown nodes and minimum hops of each beacon node, each node broadcast message has an authentication key length than the broadcast message of the DV-Hop. As a whole, the amount of computation and communication required for this scheme is not very large, and it can run on the wireless sensor network.

The sensor nodes of wireless sensor network in intelligent building are made of artificial deployment, and it can guarantee that all the sensor nodes are connected. Therefore, in this paper, in the positioning algorithm and DV-Hop localization algorithm, all the unknown nodes can position. That is to say, the positioning coverage of the two localization algorithms is 100% in the intelligent building of sensor network, so the positioning accuracy of the algorithm is only analyzed. Here, the location accuracy is represented by the ratio of the value of node location calculation to the communication range between the node true value distance.

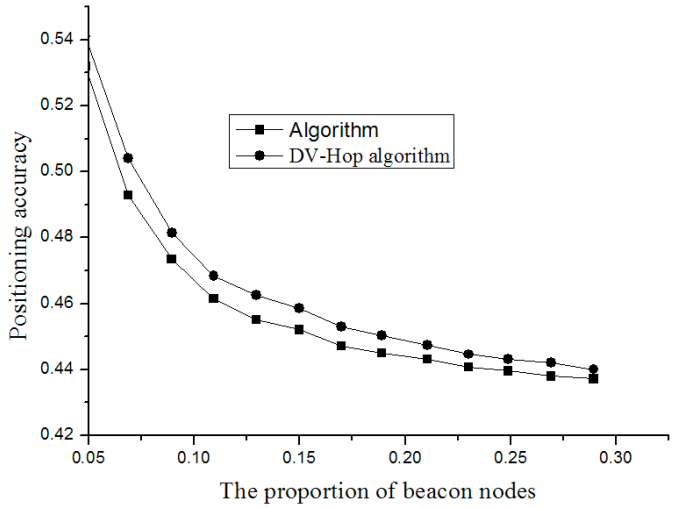

Fig. 3. The proportion and location accuracy of beacon nodes

Figure 3 shows the positioning accuracy of two location algorithms in the case of different proportions of the beacon nodes. It is obvious from the diagram that the positioning accuracy of this algorithm is better than that of the DV-Hop algorithm. This is mainly because in this algorithm, the median is calculated instead of the average method in DV-Hop when calculating the average hop distance of each hop. The median is not sensitive to the abnormal data compared with the mean value. The error of every hop distance has little influence on the algorithm. In addition, according to the error between each hop distance of beacon node and each hop distance of other nodes, each beacon node is assigned with different weights. In the calculation of node location, the beacon nodes with large weights contribute more, which can also improve the accuracy to a certain extent.

Figure 4~7 is the change curves of the proportion of the captured beacon nodes and the location accuracy of the node in the case of different attack intensities. Here, it is assumed that the way and degree for an attacker uses all the captured beacon nodes to attack are the same. We can see from figure 4~7 that, the proportion of the captured beacon nodes and the change of the attack intensity under various attacks have different effects on the location results. In figure 4, figure 5, and figure 6, with the increase of proportion of captured beacon nodes, location accuracy will continue to deteriorate.

But in Figure 5, the positioning accuracy begins to become bad as the proportion of captured beacon nodes increases. When the number of captured nodes is 40% or so, the destroy degree of changing the beacon node hop number is stronger. When the number of the captured nodes increases, the destroy degree of attack is weakened, and then it is strengthened with the further increase of captured beacon node number. Figure 4~7 also shows that, no matter what kind of attack is, the effect of the attack is enhanced with the increase of the attack intensity.

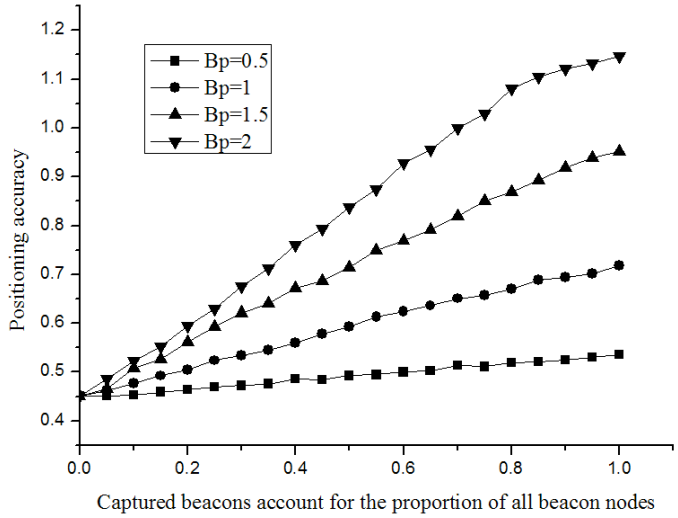

Fig. 4. Attack based on beacon node location

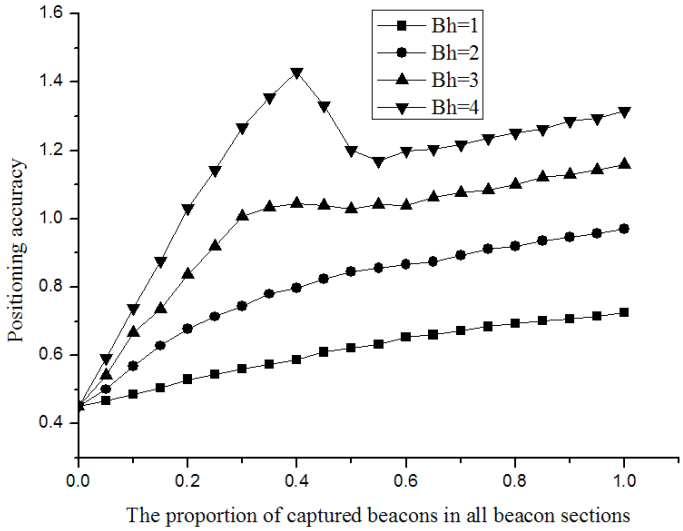

Fig. 5. Hops-based attacks

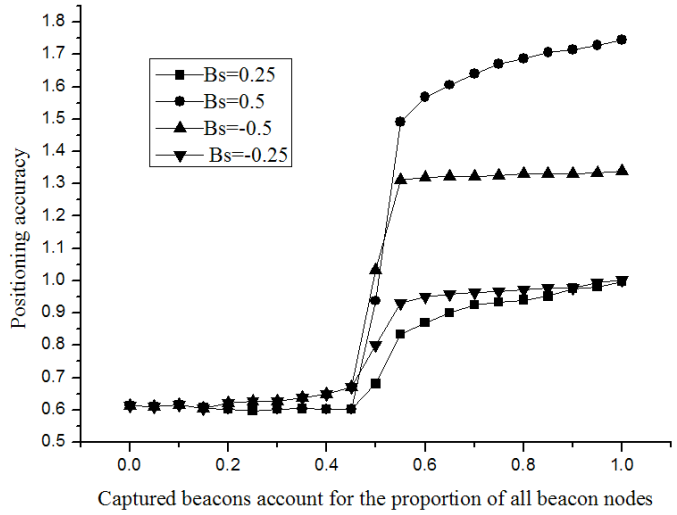

Fig. 6. Attack based on distance per hop

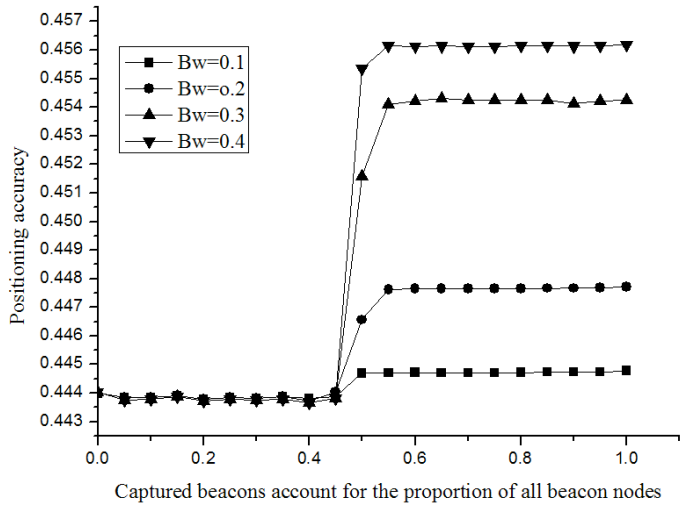

Fig. 7. Attack based on beacon node weight value

5 Conclusion

Based on the analysis of the characteristics of wireless sensor network in intelligent building, a wireless sensor network topology suitable for intelligent building is given. Specifically, the main contents and contributions of this paper are as follows:

(1) The network topology is grouped according to the geographic location of sensor nodes in intelligent buildings, such as floors, rooms and so on. Each sensor node consists of a sensor sub network, and the sub network is communicated through wired

network. This network topology makes full use of the advantages of the reliable transmission of the wired network and the convenient deployment of the wireless network.

(2) A secure location algorithm for wireless sensor network nodes in intelligent building is proposed. The algorithm is based on the DV-Hop algorithm, using the key chain for the certification of beacon node identity. The mean value is replaced by median in DV-Hop location algorithm, and each beacon node is assigned a weight value. The insensitivity of median to abnormal data and weights of beacon nodes are used to reduce the effects of malicious nodes on the positioning accuracy. The performance analysis shows that the computation and communication amount of the algorithm are not large, and it is suitable for application in wireless sensor networks.

6 References

[1] Suryadevara, N. K., Mukhopadhyay, S. C., Kelly, S. D. T., & Gill, S. P. S. WSN-based smart sensors and actuator for power management in intelligent buildings. IEEE/ASME transactions on mechatronics, 2015, vol. 20, pp. 564-571. https://doi.org/10.1109/TMECH.2014.2301716

[2] Chen, M., Zhang, Y., Hu, L., Taleb, T., & Sheng, Z. Cloud-based wireless network: Virtualized, reconfigurable, smart wireless network to enable 5G technologies. Mobile Networks and Applications, 2015, vol. 20.(6), pp. 704-712. https://doi.org/10.1007/s11036-015-0590-7

[3] Li, J. Q., He, S. Q., Ming, Z., & Cai, S. An intelligent wireless sensor networks system with multiple servers communication. International Journal of Distributed Sensor Networks, 2015, vol. 11(8), pp. 960173. https://doi.org/10.1155/2015/960173

[4] Batalla, J. M., Mastorakis, G., Mavromoustakis, C. X., & Zurek, J. On cohabitating networking technologies with common wireless access for home automation system purposes. IEEE Wireless Communications, 2016, vol. 23(5), pp. 76-83. https://doi.org/10.1109/MWC.2016.7721745

[5] Magno, M., Polonelli, T., Benini, L., & Popovici, E. A low cost, highly scalable wireless sensor network solution to achieve smart LED light control for green buildings. IEEE Sensors Journal, 2015, vol. 15(5), pp. 2963-2973. https://doi.org/10.1109/JSEN.2014.2383996

[6] Al-Sakran, H. O. Intelligent traffic information system based on integration of Internet of Things and Agent technology. International Journal of Advanced Computer Science and Applications (IJACSA), 2015, vol. 6, pp. 37-43.

[7] Li, M., & Lin, H. J. Design and implementation of smart home control systems based on wireless sensor networks and power line communications. IEEE Transactions on Industrial Electronics, 2015, vol. 62(7), pp. 4430-4442. https://doi.org/10.1109/TIE.2014.2379586

[8] Peng, C., Qian, K., & Wang, C. Design and application of a VOC-monitoring system based on a ZigBee wireless sensor network. IEEE Sensors Journal, 2015, vol. 15(4), pp. 2255-2268. https://doi.org/10.1109/JSEN.2014.2374156

[9] Zhou, P., Huang, G., Zhang, L., & Tsang, K. F. Wireless sensor network based monitoring system for a large-scale indoor space: data process and supply air allocation optimization. Energy and Buildings, 2015, vol. 103, pp. 365-374. https://doi.org/10.1016/j.enbuild.2015.06.042

[10] Rawat, P., Singh, K. D., Chaouchi, H., & Bonnin, J. M. Wireless sensor networks: a survey on recent developments and potential synergies. The Journal of supercomputing, 2014, vol. 68(1), pp. 1-48. https://doi.org/10.1007/s11227-013-1021-9

[11] Rashid, B., & Rehmani, M. H. Applications of wireless sensor networks for urban areas: A survey. Journal of Network and Computer Applications, 2016, vol. 60, pp. 192-219. https://doi.org/10.1016/j.jnca.2015.09.008

7 Authors

Shuang Xu and **Tong Zhou** are with Zhengzhou Institute of Technology, Zhengzhou, China.

Article submitted 23 February 2018. Resubmitted 09 March 2018. Final acceptance 07 April 2018. Final version published as submitted by the authors.