Exploration of Wireless Sensor Network Based on RSSI Positioning Algorithm

https://doi.org/10.3991/ijoe.v14i11.9519

Shuan Liu
Huanghuai University, Henan, China
shuanliu28193@163.com

Abstract—Based on the security of the receiving signal strength indicator positioning algorithm, the RSSI positioning algorithm in the environment of witch attack, wormhole attack and replication attack has largely failed. Although existing security positioning algorithms can effectively prevent attacks from occurring, the massive consumption of network resources can't be ignored. Therefore, a tolerable security positioning method is proposed for each of the three attacks in order to improve the security of positioning. According to the node's physical information, the attack node is detected. Through simulation experiments, compared with the traditional indoor security positioning method, the proposed algorithm can significantly reduce the intervention of witch attack, wormhole attack and replication attack on positioning error. While achieving the goal of combating attacks, it reduces the computational complexity, decreases node energy consumption, and extends the network life cycle.

Keywords—RSSI positioning algorithm, prevention of attacks, network resources

1 Introduction

Wireless sensor network technology rises on the basis of the rapid development of wireless communication technology, microelectronics technology, and low-power embedded technology. The traditional sensor data acquisition mode shifts from a single mode to an integrated, networked mode. The wireless sensor network monitors the environmental information in the network distribution area in real time through the cooperation of micro-sensors and transmits it to the receiving end in a multi-hop self-organizing network. It has been widely used in fields such as location information navigation, security firefighting, medical security, defense military, and environmental monitoring.

Location technology is an essential technology in the WSN. The sensor node must know its own location information to understand the specific events that occur in the specific coordinates for the next task. In addition to determining the location of the event, the location information of the node can also be used to assist the routing, network management, etc. In outdoor environments, satellite positioning systems such as GPS, GLONASS, Galileo, and Big Dipper can meet most of the military and civilian

positioning requirements. However, in the interior of a building, the accuracy of the satellite positioning system is severely reduced and it is difficult to meet the application requirements. With the improvement of wireless communication technology and information processing technology, indoor positioning technology relies more on parameter measurement and calculation to perform indoor positioning.

The existing localization algorithm defaults that the nodes are deployed in an environment without attacks and doesn't consider the location of the nodes in the presence of malicious attacks. Sensor networks have been widely used in businesses and industries that require data security. The monitoring and tampering of information and the resistance of heterogeneous node intrusions have gradually become an arduous and challenging problem. The focus of positioning technology is mainly on precision and energy consumption, and a very good result has achieved through the unremitting efforts of the predecessors. The security of positioning process data transmission has become a new hot spot in wireless sensor network positioning technology.

2 Literature review

The original TOA positioning algorithm uses the time consumed by the signal transmission to predict the distance between the node and the beacon node and requires a high degree of time synchronization. ActiveBat positioning system uses TOA algorithm, its positioning accuracy is about 9cm. TDOA ranging technology mounts ultrasonic generators and receivers on nodes. Cricket indoor positioning system uses TDOA technology, and its positioning accuracy is within 10cm in the range of 2*2*2.5. Combined with TDOA positioning algorithm and NTP protocol, some researchers proposed a time-synchronized hybrid algorithm based on ranging. An algorithm based on time synchronization requires additional hardware and the ranging distance is short, not for practical applications. Early RSSI positioning methods used RSSI to estimate the distance between nodes. SpotONtags system is an indoor positioning system with RSSI positioning technology. The relative position between nodes is used for positioning calculation. The nodes are arranged in a cube with a length of 3m and the positioning accuracy is within 1m after calculation. At present, many wireless sensor chips have built-in RSSI registers, which provide convenience for RSSI-based positioning systems. Niculescu et al. proposed many distributed point algorithms and DV-Hop positioning algorithms to calculate the minimum hops, average hops, shortest paths, and distances from unknown nodes to each beaconing node. The relative coordinates of unknown nodes are obtained by methods such as least squares. When the beacon node density is 10% of all nodes, the relative positioning error is 33%. He et al. proposed the APIT algorithm. The main idea of the algorithm is the triangle coverage approximation. The unknown node selects three adjacent beacon nodes to determine whether they are located within their triangles, and multiple beacon node combinations are selected multiple times for judgment. Finally, the intersection of all the triangles containing the target node is calculated to obtain the centroid of the intersection. The centroid is the coordinate of the node to be measured.

The algorithm has high requirements on the density of beacon node and the relative positioning accuracy is 40%.

Tomic et al. (2017) proposed a WSN local space constrained problem based on a distributed localization method. It estimates the coordinates of an unknown node by iteratively solving a local space constrained program, and then the neighboring nodes are jointly updated to update the positioning error [1]. Nayak and Devulapalli (2016) proposed a cluster-based WSN localization algorithm that uses cluster structure and a global system to represent network distribution, reduces measurement error through multi-hop probability calculation, and improves node positioning accuracy [2]. Asaei et al. (2017) proposed a localization method based on perceptual sparse matrix, transforming the distribution of nodes into discrete regions of sparse matrices, and using greedy algorithms and deterministic monitoring matrices to reduce the number of measurements [3].

Sicari (2015) used a global single key to encrypt nodes in the TinSec positioning system. However, the key is the key to the security of the entire network. Once the key is stolen, the entire network is exposed to the enemy. The LEAP protocol adopts a complex key method. The heavy key management work increases the energy consumption of the system dramatically [4]. Devanagavi et al. (2016) proposed a secure routing protocol INSEN that can tolerate aggressiveness and solve the attack risk through cooperation between redundant routing and authentication mechanisms [5].

Ferng et al. (2016) proposed the LAD scheme to mark the abnormal beacon node during the positioning process and determine whether the estimated coordinate of the detection node is the same as or similar to its actual position. If the number of inconsistent nodes exceeds a certain value, it is determined that there is an attack. But how to deal with exceptions, no solution is given [6]. Khairi et al. (2018) proposed a scheme to detect anomalies and delete the abnormal beacon node. By cancelling the scheme, the beacon nodes with abnormalities are isolated from the positioning calculation. However, the pressure of the aggregation node and the base station is increased, and the calculation amount of algorithm and energy consumption are large [7].

The safety positioning system proposed by Cui (2017) is based on the gradient descent method and has a low computational complexity. Compared with the classic algorithms such as Newton method, greedy algorithm and particle swarm algorithm, the convergence speed is faster, the positioning accuracy is higher, and it is easy to implement on hardware. It is suitable for scenarios with high real-time requirements [8].

Our country's research on WSN started later than the Western countries. In early 2002, with the support and encouragement of the National Natural Science Foundation of China (NSFC), the domestic wireless sensor research began its climax. Many scholars have invested in this research. There are as many as 36 state-financed research projects and topics related to WSN. Research institutions such as Harbin Institute of Technology, Zhejiang University, Institute of Computing Technology, Chinese Academy of Sciences, Fudan University, Tsinghua University, and Shanghai Jiaotong University have all conducted in-depth studies.

Many scholars have conducted in-depth research on positioning algorithms in sensor networks. Cui et al. (2017) used differential particle swarm algorithm to optimize the coordinates of unknown nodes and proposed to use percentages to correct the average hop distance between beaconing nodes in DV-Hop. Xin et al. (2015) used a quantitative model to represent the positioning error of the node, and then used a weighting factor to correct the relative position coordinates of the node. Teng (2014) proposed the integration of RSSI positioning method and centroid algorithm, and a beacon node weighting method is also proposed. The calculated amount and cost are relatively reduced, but the positioning accuracy is easily affected by RSSI. Chai (2016) proposed a four-side measurement positioning algorithm, which increases the amount of calculation on the basis of trilateration, but the positioning error of the node is reduced to some extent.

In summary, in addition to being able to effectively combat attacks, the security location algorithms for wireless sensor networks under malicious attacks should also fully consider the robustness of the network, traffic, and computation. Since the existing sensor nodes carry the RSSI device by default, the RSSI-based positioning algorithm has become one of the most widely used positioning algorithms. A secure location algorithm based on RSSI positioning is proposed to combat witch attacks, wormhole attacks, and replication attacks during RSSI positioning. Finally, through simulation experiments, in the specific indoor environment, the proposed security location algorithms corresponding three attacks are simulated to verify the effectiveness and low energy consumption of the algorithm.

3 The analysis of wireless sensor network positioning system and security

3.1 The structure of wireless sensor network

The nodes in the WSN are divided into three categories: sensor nodes, sink nodes, and task management nodes. As shown in Figure 1, the sensor node has wireless communication and computing capabilities and can collect related data. The nodes use a wireless multi-hop way to transfer the collected data to the sink node, and then the sink node sends the data to the network link to complete the intelligent network system for the relevant application requirements.

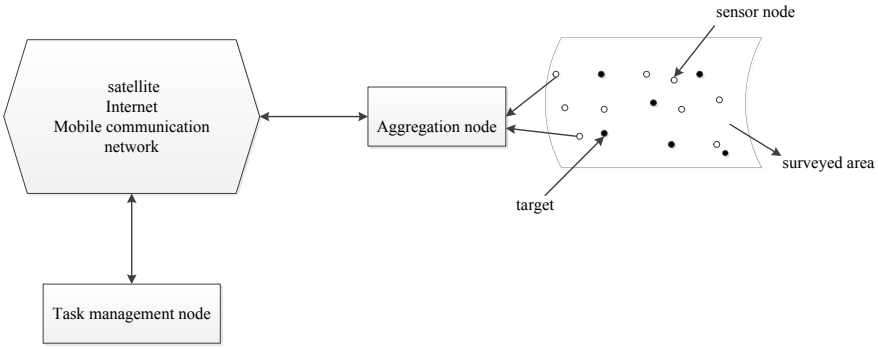

Fig. 1. The architecture of wireless sensor network

In the WSN, there are different sensors in each node to sense and collect data in the monitoring area, and some nodes also have data processing capabilities. The purpose of use for the user is to collect information. Therefore, data-centricity is the main feature that distinguishes WSN from other types of networks.

The sensor node consists of two parts: software system and hardware system. The hardware system mainly includes four parts: energy supply module, communication module, processing module and data acquisition module. As shown in Figure 2, its main functions are as follows:

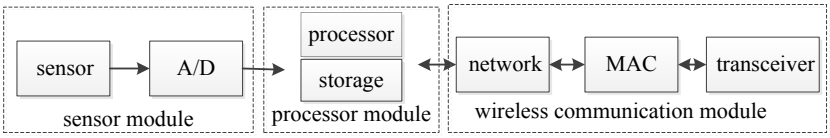

Fig. 2. The module structure of wireless sensor node

This module provides nodes with the energy to maintain the normal operation of the node. Miniature batteries are usually used. Designing an effective energy-saving positioning algorithm can reduce the energy loss and extend the life cycle of the network. It is the main research topic of WSN.

The data acquisition module consists of a sensor device and an A/D conversion module. The sensor collects the relevant data of the monitoring object, and the A/D conversion module converts the analog quantity into a digital signal. The processing module is mainly composed of a memory and a microprocessor and is responsible for executing a communication protocol and processing data. The embedded CPU processor is generally used. The communication unit is mainly responsible for communication between nodes, including the sending, receiving, and exchanging of data between nodes. The energy consumption of the communication unit is proportional to the distance. Different communication modules can be used depending on the distance. Data fusion techniques can also be used to reduce network flow.

3.2 Analysis of node location technology in wireless sensor networks

As shown in the schematic diagram of the trilateration method in Figure 3, O is the node to be measured. There are three nodes in the communication range: OA, OB, and OC. The coordinates are (xA, yA), (xB, yB), and (xC, yC). The distances from O are dA, dB, and dC, respectively. It assumes that the A coordinate is (x,y).

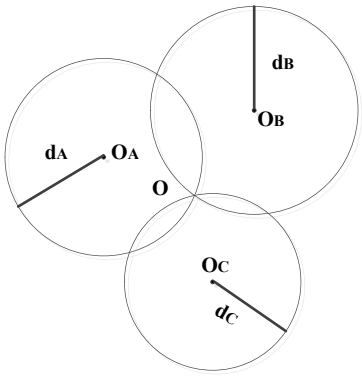

Fig. 3. Trilateration

According to the geometry of the circle there are:

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

The coordinates of O from (1) are:

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

Triangulation calculates unknown node coordinates through the angle between beacon nodes. The principle is shown in Figure 4. D is the node to be measured, and A, B, and C are three beacon nodes in the D communication range, and the coordinates are (xA, yA), (xB, yB), (xC, yC), respectively. The angles of D to A, B, and C are ∠CDA, ∠BDA, and ∠CDB, respectively, and the coordinates of D are assumed to be (x,y).

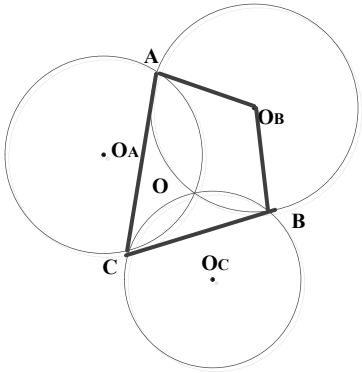

Fig. 4. Triangulation location

For the nodes A, B, and ∠ADB, the center coordinate of the circle is O(xo, yo), and the circle of radius r is α=∠AOB:

$$\begin{cases} \sqrt{(x_o - x_a) + (y_o - y_a)^2} = r \\ \sqrt{(x_o - x_b)^2 + (y_o - y_b)^2} = r \\ (x_a - x_c)^2 + (y_a - y_c)^2 = 2r^2 - 2r^2 \cos\alpha \end{cases} . \quad (3)$$

The coordinates of the circle O are calculated by the equations set. For A, C, ∠ ADC and B, C, and ∠CDB, O1 and O2 can also be calculated, and then the estimated coordinates of the unknown node D can be calculated.

3.3 RSSI-based positioning algorithm

The RSSI-based wireless sensor network positioning algorithm is known for its low energy consumption, low cost and easy implementation, and it has been applied in many fields. The principle of RSSI ranging technology is to record the RSSI signal strength transmitted by the beacon node, calculate the loss of the signal in the medium propagation process according to the RSSI signal strength received by the measurement node, and finally use the appropriate signal propagation model and the loss of the signal in the propagation process to derive the distance. The RSSI value has certain symmetry. When measuring the RSSI value between two nodes, only one message packet can be sent and received to complete the measurement. There is no need to send messages back and forth between the two nodes. The algorithm can be used when pursuing the low complexity of the positioning algorithm when the accuracy requirement of the algorithm is not high.

At present, there is no clear mathematical model for the relationship between path attenuation and distance. It is mainly a model based on a variety of data measurement values and a semi-empirical model. According to the actual work environment, differ-

ent models are used. Whether the selected model can better simulate the wireless system also depends on the match between the environment and the model. The commonly used wireless signal propagation model is:

$$P(d) = P(d_0) - 10n \lg(\frac{d}{d_0}) + X. \tag{4}$$

In the formula, P(d) is the signal strength received by the node under test with a distance d from the beacon node, d represents the distance between the two nodes required, P(d0) represents the signal strength of the reference distance d0, and n is the path consumption index. The path consumption index depends on the environment, and X represents a Gaussian random variable with an average value of 0 added to reduce the influence of obstacles. The RSSI average of a certain distance is mainly obtained by collecting measured data, and then using the mean value to correct the propagation model of the area.

4 The improvement of RSSI positioning algorithm against witch attack

Witch attacks are proposed in point-to-point networks. Attacking nodes claim that they have multiple identities, illegally existing in the network with multiple identities, participating in network communications and destroying redundancy mechanisms in distributed storage systems.

Witch attacks have the following two attack modes:

Direct communication: witch attack nodes communicate directly with legitimate nodes, send fake information to legitimate nodes, and reflect different identities at different times, thereby disrupting network communications.

Forged identity: an attacking node can forge multiple node identities and participate in network communication. It allows legitimate nodes to think that there are multiple nodes around, which disrupts the message communication of legitimate nodes.

In the positioning process, if the unknown node receives multiple position information from the same node, the positioning system will add all the position information to the position calculation, resulting in a great error in the positioning algorithm. The basis for the normal operation of the positioning system is the correspondence between the identity and the actual position. The witch attack is an attack against this correspondence.

It assumes that all nodes in the environment are stationary and all nodes are divided into beacon nodes and unknown nodes. The node uses a simple, idealized radio communication model. In the process of RSSI positioning, the unknown node calculates the distance to the beacon node with the attenuation model according to the degree of attenuation of the signal. It is assumed that only the node within the communication range of the node can receive the position information of the node.

Since the RSSI ranging error is affected by the reflection of the signal in the medium, obstacles, multipath effects, etc., in the process of RSSI positioning, a method of averaging the multiple RSSI measurement values is adopted to eliminate the environmental factors on the positioning, but it also gives the witch attack an opportunity to attack. Witch attack can be divided into two parts: one ranging process and multiple ranging process.

Through the ratio of nodes receiving energy, it is detected that there is a witch attack in the network. All nodes with the same ratio of received energy are considered to be the virtual location information of the attacking node. These nodes are eliminated from the positioning calculation, and the purpose of combating the witch attack is achieved.

Matlab2014a is used to simulate the algorithm and verify the effectiveness and low energy consumption of the algorithm. The simulation environment is designed on a hypothetical manufacturing shop with 100 randomly distributed sensor termination nodes. The workshop is a 100m*100m area, and the area is divided into 20m*20m grids according to the distribution of equipment. Because the indoor sensor beacon nodes can be deployed, the beacon nodes are arranged in the center of the grid in the simulation.

For better simulation experiments, the replication attack nodes are also randomly distributed in the area. The average positioning error formula is:

$$error = \frac{\sum_{i=1}^{N} \sqrt{(x_i - x_i^1)^2 + (y_i - y_i^1)^2}}{N \times R}. \quad (5)$$

In the formula, N is the number of unknown nodes, R is the communication radius of the radio frequency, x is the actual value of the node to be measured, and y is the measurement value of the unknown node. For each case, 100 independent repeat experiments are performed and the average of 100 test results is taken as the final experimental result.

In the above experimental environment, the impact of replication attacks on the average positioning error is analyzed through simulation experiments: simulation experiments are performed on the positioning error under normal environment and the positioning error under the threat of witch attack.

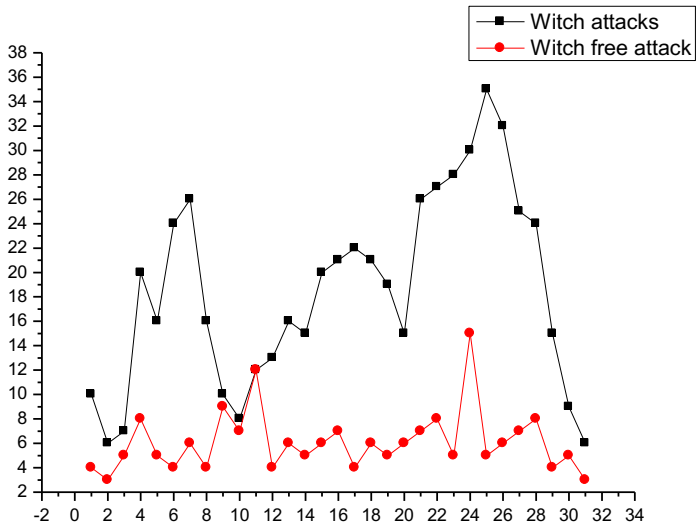

Fig. 5. Effect of witch attack on error

As shown in Figure 5, when there are two Witch attack nodes, after positioning, 31 nodes with larger errors are selected, o is the positioning error of 31 nodes when there is no attack, and □ is the positioning error of 31 nodes when there is a witch attack. It can be concluded from the figure that the witch attack has a great influence on the positioning error. Under normal circumstances, the node positioning error is maintained within 8m, and the positioning error of individual nodes is around 10m. In the attack, the positioning error of most nodes has reached 15m-30m, and even the positioning error of individual nodes has reached more than 35m, and the positioning algorithm has basically failed.

Through learning and researching various security location algorithms, the attack principle of witch attack is analyzed, and a security positioning mechanism that uses the physical characteristics of nodes to defend against witch attacks is proposed: in the one-ranging phase and multiple-ranging phases of the RSSI positioning, ratios are used to filter the witch attack nodes to achieve the purpose of combating witch attacks and reducing RSSI positioning errors. In the following simulation experiments, the meaning of this algorithm is discussed in terms of the impact of witch attack on positioning, the effectiveness of the algorithm in this chapter, and the low energy consumption of the essential algorithm.

5 The improvement of RSSI positioning algorithm under replication attacks

Replication attack is one of the most destructive attacks in wireless sensor networks. It means that the attacker captures the node and copies a large number of attacking nodes with the same legal identity. The replication attack carries the same information as the captured node. The attacker places attack nodes in the network and participates in network communications. Once a replication attack is initiated, the performance of the WSN's location system, routing system, etc. will be drastically reduced due to the wrong location information and routing information. If the attacker replicates the unknown node, the copied node will not carry the position information, or the carried position information will be covered by the next positioning data and will not affect the positioning result. If the attacker replicates the beacon node, the attacking node will directly participate in the positioning, and the surrounding unknown nodes will use the location information as an important basis for positioning. Therefore, only the situation where the attacker replicates the beaconing node is considered in this chapter.

When the distance between two attacking nodes is greater than 2R, no node exists in the communication range of the two attacking nodes at the same time. According to the physical property of RSSI, when the location information carried by a node and the real location correspond to each other, any node can't communicate with a node outside its RSSI communication range.

This brings about the limited characteristics of the communication range.

$$\sqrt{(X - x_i)^2 + (Y - y_i)^2} \succ R. \tag{6}$$

Under normal circumstances, the limited characteristics of the communication range will not be violated, but when the node is subject to a replication attack, if there are no two replication attack nodes in the communication range of the same node, the limited characteristics of the communication range will be violated. As shown in Figure 4.1, C1 and C2 are replication attack nodes. The distance between C1 and C2 is greater than 2R. Assuming that all carry the coordinates of C1, then according to the position information carried by C2 to calculate the distance d between C2 and B, d must be greater than the communication radius R of B, which violates the limited characteristic of the communication range.

When there is a distance between two attacking nodes is less than 2R, the nodes in the network will not receive two or more messages from the same node. If two replication attack nodes exist within the communication range of a certain node at the same time, according to the physical property of RSSI, when the location information carried by the node and the real location correspond to each other, one node can only receive information from the same node once.

Compared with other detection IP algorithms, this algorithm can not only detect the replication attack node, but also detect the legitimate node being copied, thereby reducing the misjudgment rate of the algorithm and better protecting the robustness of

the WSN network. After the WSN node is initialized, it detects the unique characteristics of the received message. If a replication attack node is found, it will be immediately deleted from the positioning calculation; after that, the location information is calculated, it is checked whether or not the limited characteristics of the communication range are violated. If a replication attack node is found, it is immediately deleted from the location calculation. As long as one of the two characteristics is violated, the existence of a replication attack can be determined. Finally, normal RSSI positioning calculations are performed.

Communication radius R of radio frequency is 50m, and the experimental path loss coefficient n is set to 3. For better simulation experiments, replication attack nodes are also randomly distributed within the area. The average positioning error formula is:

$$error = \frac{\sum_{i=1}^{N} \sqrt{(x_i - x_i^1)^2 + (y_i - y_i^1)^2}}{N \times R}. \tag{7}$$

By learning and studying various security location algorithms and analyzing the attack principle of replication attacks, a security location mechanism that uses the physical characteristics of nodes to protect against replication attacks is proposed: the limited characteristics of the communication distance, the unique characteristics of the received message. In the following simulation experiments, the significance of this algorithm is discussed in three aspects: the impact of the replication attack on the positioning, the effectiveness of the algorithm in this chapter, and the low energy consumption of the essential algorithm.

6 Improvement of RSSI positioning algorithm in wormhole attacks

Wormhole attacks are mainly directed to defensive routing protocols in the network. A dedicated channel is established between malicious nodes. The attacker records information sent by eavesdropping nodes and passes the received information to another accomplice node over the private channel. In general, this dedicated channel has low delay and high quality characteristics, making the link easier to participate in network communications. It can be concluded that although the two attacking nodes can't theoretically communicate, in reality, the data can be transmitted and the wrong location information can be sent, thereby affecting the positioning error.

When the distance between the attacking node and the unknown node is greater than 2R, the attacking node and the unknown node can't have a communication relationship in principle and can't transmit position information to each other. According to the physical property of RSSI, when the location information carried by a node and the real location correspond to each other, any node can't communicate with a node outside its RSSI communication range.

$$\sqrt{(x - x_i)^2 + (y - y_i)^2} \succ R. \quad (8)$$

Under normal circumstances, it is impossible for a node in the network to communicate with nodes outside its RSSI communication range. As shown in Figure 5.2, R is the RSSI communication radius of the node. The distance between B2 and B3 is obviously greater than 2R. There is no communication relationship. B3 can't receive the message packet from B2. If there are wormhole attack nodes W1 and W2 in the network, the attack node W1 listens to the message sent by the beacon node B2 and sends it to the attack node W2 through the private link, and W2 immediately broadcasts the message packet from the W1. At this time, B3 received a message from B2. B3 and B2 generated a communication relationship that should not exist, which violated the restricted characteristic of the communication range.

The security location algorithm that resists the wormhole attack is studied, and the attack principle of wormhole attack and several methods to fight wormhole attack are described. An attack method based on RSSI positioning is proposed, and the restricted characteristics, the message restricted characteristics, and the uniqueness of received messages are proposed in the communication range. Through the simulation experiments, the effectiveness and low energy consumption of the algorithm are verified, which can effectively reduce the impact of wormhole attack on positioning while improving the positioning accuracy.

7 Conclusion

Node location technology is a key technology in WSN applications and has been widely applied in various fields of people's daily life. Currently existing localization algorithms have defaulted nodes deployed in an environment without attacks and don't consider the location of nodes in the presence of malicious attacks. In times of peace, large-scale wars have moved away from us. Urban operations such as fighting terrorism and rescuing hostages have become major battlefields. If the sensor network in the building is infringed by terrorists, the implementation of network attacks and disruption of network communications will bring great misdirection to the combatants. The resistance to the eavesdropping and tampering of information and the intrusion of heterogeneous nodes has gradually become a challenging research. Therefore, some improvements are proposed in the traditional positioning algorithm. The improved algorithm can effectively fight witch attack, copy attack and wormhole attack, and achieve the purpose of security on the basis of positioning.

8 References

[1] Tomic S, Beko M, Dinis R. (2017). Distributed algorithm for target localization in wireless sensor networks using RSS and AoA measurements. Pervasive and Mobile Computing, 37: 63-77. https://doi.org/10.1016/j.pmcj.2016.09.013

[2] Nayak P, Devulapalli A. (2016). A fuzzy logic-based clustering algorithm for WSN to extend the network lifetime. IEEE sensors journal, 16(1): 137-144. https://doi.org/10.1109/JSEN.2015.2472970
[3] Asaei A, Bourlard H, Taghizadeh M J. (2016). Computational methods for underdetermined convolutive speech localization and separation via model-based sparse component analysis. Speech Communication, 76: 201-217. https://doi.org/10.1016/j.specom.2015.07.002
[4] Sicari S, Rizzardi A, Grieco L A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer networks, 76: 146-164. https://doi.org/10.1016/j.comnet.2014.11.008
[5] Devanagavi G D, Nalini N, Biradar R C. (2016). Secured routing in wireless sen-sor networks using fault-free and trusted nodes. International Journal of Communi-cation Systems, 29(1): 170-193. https://doi.org/10.1002/dac.2810
[6] Ferng, H. W., & Khoa, N. M. (2016). On security of wireless sensor networks: a data authentication protocol using digital signature. Wireless Networks, 23(4): 1-19.
[7] Khairi M H H, Ariffin S H S, Latiff N M A. (2018). A Review of Anomaly Detec-tion Techniques and Distributed Denial of Service (DDoS) on Software Defined Net-work (SDN). Engineering, Technology & Applied Science Research, 8(2): 2724-2730.
[8] Cui Z, Sun B, Wang G. (2017). A novel oriented cuckoo search algorithm to im-prove DV-Hop performance for cyber–physical systems. Journal of Parallel and Dis-tributed Computing, 103: 42-52 https://doi.org/10.1016/j.jpdc.2016.10.011

9 Authors

Shuan Liu works as associate professor at School of Information Engineering, Huanghuai University, Henan, China

Article submitted 02 September 2018. Resubmitted 19 September 2018. Final acceptance 29 September 2018. Final version published as submitted by the author.