Hindawi
Discrete Dynamics in Nature and Society
Volume 2020, Article ID 1306084, 9 pages
https://doi.org/10.1155/2020/1306084

Research Article

Research on Wireless Sensor Network Security Location Based on Received Signal Strength Indicator Sybil Attack

Hongbin Wang and Liping Feng

Department of Computer Science, Xinzhou Teachers University, Xinzhou, Shanxi 034000, China

Correspondence should be addressed to Liping Feng; fenglp@yeah.net

Received 28 July 2020; Revised 26 September 2020; Accepted 28 October 2020; Published 12 November 2020

Academic Editor: Qingyi Zhu

This paper studies the security location mechanism of the sensor network node under the attack of Sybil and analyzes the safe attacks which are possibly accepted and safe requirement in the location system. Since RSSI (Received Signal Strength Indicator) possesses the energy transmission function, different transmission energy will cause it to produce different RSSI readings. Furthermore, this kind of method cannot increase the burden on Wireless Sensor Network (WSN). It conducts an analysis between two receiving nodes, compares RSSI ratios to tickle the problem of time inconsistency of RSSI, and sets a threshold to detect Sybil by the emulation results. Research shows that the ratio value of different receiving nodes by using RSSI can resolve time difference because of the RSSI or unreliability which results from the asymmetry of transmission ratio. The thesis makes a comparison that the number of receiving nodes has an influence on attack effect. Utilizing the RSSI ratio values can exactly detect the Sybil attack. Emulation findings demonstrate that the detection method put forward by the thesis owns better security.

1. Introduction

Wireless Sensor Network (WSN) is composed of a great number of sensor nodes by means of wireless communicational technology and self-organization mode. It has a wide applicable prospect in the civilian aspect and the military aspect, but at present, the researches about WSN still have a lot of questions to solve, such as routing protocol, location technology, and network security. Location technology is one of the significant technologies of WSN. WSN establishes spatial relationship depending on the node's position to report the monitored incident. In addition, the node's position, which can help routing and other network functions, is also an essential basis. However, the location of the network node is easy to be attacked by enemies, because WSN is mainly used under the hostile and unguarded environment. The frangibility depends on the importance of the security issue in the process of location.

This paper studies the security location mechanism of sensor network node under the attack of RSSI Sybil; RSSI (Received Signal Strength Indicator) ranging technology is known for its low energy consumption, low cost, and easy to implement and has been widely used. But in the face of complex security environment, to resist attacks has become a key issue of applying the RSSI ranging technology to WSN.

2. Basic Principle of RSSI

RSSI calculates the loss of signal in the propagation process using the known signal strength at the receiving node according to the received signal strength and then transforms the propagation loss into the distance using the theoretical or empirical signal propagation model.

First, the basic principle of RSSI was introduced. The relationship between the transmitted power and the received power of radio signal can be expressed as formula (1), where P_R was the received power of radio signal, P_T was the transmitted power of radio signal, r was the distance between receiving unit and transmitting unit, n was the propagation factor, and its value depended on the environment of radio signal propagation.

$$P_R = \frac{P_T}{r^n}. \tag{1}$$

Formula (2) can be obtained by taking the logarithm on both sides of formula (1):

$$10\, n\lg r = 10\lg \frac{P_T}{P_R}. \tag{2}$$

If the transmitted power of the node was known, formula (3) can be obtained by substituting the transmitted power into formula (2):

$$10\lg P_R = A - 10n\lg r. \tag{3}$$

$10\lg P_R$, the left part of formula (3), was the expression of converting the received signal power to dBm, which can be expressed directly as formula (4), where A can be regarded as the received signal power when the signal was transmitted 1 m:

$$P_R\,(\text{dBm}) = A - 10n\lg r. \tag{4}$$

By formula (4), it can be seen that the value of constants A and n determined the relationship between the received signal strength and signal transmission distance, and the influence of the two constants on the signal transmission distance was analyzed. First, assume that n remained unchanged. When the A changed, then the signal propagation factor n was a constant, and the relationship between the RSSI and propagation distance was obtained under different initial transmitted signal power, showing that the radio signal attenuation was very serious in the near distance propagation process and not serious in the long-distance propagation process. When the transmitted signal power increased, the propagation distance increased was approximated for the ratio of the signal power increase to the slope of the curve in the gentle phase.

When A remained unchanged, the relationship between the RSSI and propagation distance was obtained under different n. The smaller the value of n, the smaller the radio signal attenuation in the propagation process, and the farther the propagation distance of the radio signal. Increasing the transmitted signal power can increase the propagation distance. The propagation factor depended mainly on the attenuation, multipath effect, and interference reflection of the radio signal in the air. The smaller the interference, the smaller the propagation factor n, the farther the propagation distance of radio signal, the closer the propagation curve of the radio signal to the theoretical curve, and the more accurate the RSSI ranging [1].

Due to the limitation of the condition, no field measurement experiment was conducted in this paper. In the literature [2], a wireless sensor node made of CC2420 was used to measure the relationship between the RSSI and propagation distance, and a series of measurement experiments were conducted only in the open area, where the RSSI was received signal strength indication, which was represented by an 8-bit signed complement and stored in the RSSI_VAL memory of CC2420.

According to a large number of experimental measurements, the relationship between the RSSI and propagation distance was very complicated, which was related to the existence of obstacles, the distance between the node and the ground, and the antenna angle. When the transmitting node and the receiving node were not less than 2 m from the ground, the influence of antenna angle on the relationship between the RSSI and propagation distance was very small, and the error caused by the antenna angle was also very small. Therefore, when the transmitting node and the receiving node were placed about 2 m away from the ground, the RSSI mean and distance data were measured as in Table 1 [3].

After fitting, formula (5) of calculating the distance using the RSSI value was obtained:

$$d = 0.0023 \times \text{RSSI}^2 + (-0.4345) \times \text{RSSI} - 4.1458, \tag{5}$$

where the unit of d was m and the unit of RSSI was dBm.

Figure 1 shows that there was a certain error between the fitting curve and the actual distance, which was affected by many factors, such as climate and obstacles. Thus, the traditional and classical attenuation model of radio signal propagation was as

$$\text{RSSI}\,(d) = \text{RSSI}\,(d_0) - 10\lambda\lg\left(\frac{d}{d_0}\right) + \zeta_\sigma, \tag{6}$$

where $\text{RSSI}\,(d)$ was the RSSI intensity value received from the place d meter from the transmitter, unit: dBm; $\text{RSSI}\,(d_0)$ was the RSSI intensity value received from the unknown node d_0 meter from the transmitter, unit: dBm; d was the distance between the transmitter and the receiver; d_0 was the reference distance, unit: m; λ was the path attenuation index, which was closely related to the surrounding environment and obstacles; ζ_σ was the standard deviation, which was the normal random variable of σ depending on the specific multipath environment, unit: dBm.

The RSSI ranging was a ranging method to judge the location of the target node using the appropriate radio propagation model by measuring the intensity of the radio frequency signal received by CC2420. The key to this method was to estimate the distance between the unknown node and multiple beacon nodes with the measured attenuation degree of radio frequency signal. Finally, the location of the unknown node was estimated with the measured distance value.

Formula (7) was obtained by formula (6):

$$d = 10^{\dfrac{\text{RSSI}\,(d_0) - \text{RSSI}\,(d) + \zeta_\sigma}{10\lambda}} \times d_0. \tag{7}$$

Formula (7) was the classical computation relation between the distance d and RSSI, where λ and ξ_σ were closely related to the external environment.

Table 2 showed the range of values of λ and ξ_σ in different environment.

There are many mathematical models for calculating the attenuation of radio waves, but there is no explicit mathematical model between the path attenuation and distance.

Table 1: RSSI average value and distance data.

Distance (m)	20	30	50	80	100
RSSI average value (dBm)	−10.897	−16.771	−19.378	−23.921	−24.509

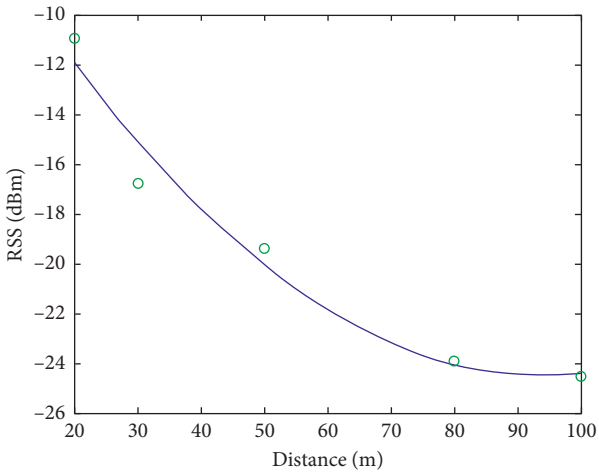

Figure 1: Echoism between RSSI and distance.

Table 2: The values of λ and ξ_σ in different condition.

Environmental conditions	Path attenuation index λ	Deviation ξ_σ
Playground	$2.7 < \lambda < 3.4$	$1.55 < \xi_\sigma < 4.12$
Corridor	$1.9 < \lambda < 2.2$	$1.37 < \xi_\sigma < 3.32$
Laboratory	$1.4 < \lambda < 2.2$	$2.39 < \xi_\sigma < 3.46$
Alley	$2.1 < \lambda < 3.0$	$2.19 < \xi_\sigma < 4.47$
Patio	$2.8 < \lambda < 3.8$	$1.00 < \xi_\sigma < 3.03$
Balcony	$1.4 < \lambda < 2.4$	$2.00 < \xi_\sigma < 4.00$
Road	$3.3 < \lambda < 3.7$	$2.97 < \xi_\sigma < 4.27$
Grassland	$4.6 < \lambda < 5.1$	$1.67 < \xi_\sigma < 2.23$

There are pure empirical models based on various measurements and semiempirical models for theoretical analysis based on physical parameter measurements. The best applicability of a particular model depends on whether it can simulate the actual working environment of a wireless system; thus, the method of mathematical model calibration for propagation attenuation was proposed. When using this method, the RSSI means of specific distances were obtained by collecting the measured data and used to correct the propagation model in the region to obtain the attenuation characteristics of the signal in the region in the propagation process. Therefore, the results predicted by the model were more close to the results in the actual field environment, which thus effectively improve the node localization accuracy.

The RSSI-based localization algorithm calculated the distance between unknown node and beacon node using the received value of the measured signal by formula (7). The acquisition of RSSI intensity value can be implemented either by unknown node or by beacon node. The method was called self-localization if the acquisition of RSSI intensity value was implemented by unknown node, and telemetric localization by beacon nodes. In the self-localization mode, the target node can measure the distance between itself and multiple beacon node in WSN and then calculate the location relative to the beacon node. By contrast, in the telemetric localization mode, the RSSI intensity value of unknown node was measured by the beacon node to determine the location of unknown node. For the self-localization mode, the RF transmitted power of each beacon node was the same. For the telemetric localization mode, the WSN must have both the function of power measurement to determine the RF transmitted power of each unknown node and the ability of data transmission [4].

As shown in Figure 2, suppose (x_i, y_i) was the location coordinate of the ith beacon node in WSN; (x, y) was the location coordinate of the unknown node; RSSI_{i-t} was the RSSI value of the ith beacon node received by the unknown node at t; and the distance between the unknown node and the ith beacon node was obtained by formula (7); thus, formula (8) was established:

$$\Gamma(x, y) = \sum_{i-1}^{n} W_i \left[\sqrt{(x - x_i)^2 + (y - y_i)^2} - d_{i-t} \right]^2, \quad (8)$$

where n was the total number of beacon nodes in WSN.

At this point, the localization problem was transformed into the problem of finding the minimum value of the function of two variables in mathematics, where W_i was the weighting factor. From the geometric point of view, in the coordinate system, the distance between the unknown node (x, y) and the ith beacon node (x_i, y_i) met the following geometric relation:

$$d_{i-t} = \sqrt{(x - x_i)^2 + (y - y_i)^2}. \quad (9)$$

Suppose the RSSI decay was the same in the communication between the unknown node and its adjacent beacon node; then formula (10) can be obtained from formula (9):

$$AX = B, \quad (10)$$

where

$$A = \begin{bmatrix} 2(x_1 - x_n) & 2(y_1 - y_n) \\ \vdots & \vdots \\ 2(x_{n-1} - x_n) & 2(y_{n-1} - y_n) \end{bmatrix},$$
$$B = \begin{bmatrix} x_1^2 - x_n^2 + y_1^2 - y_n^2 + d_n^2 - d_1^2 \\ \vdots \\ x_{n-1}^2 - x_n^2 + y_{n-1}^2 - y_n^2 + d_n^2 - d_{n-1}^2 \end{bmatrix}, \quad (11)$$
$$X = \begin{bmatrix} x \\ y \end{bmatrix}.$$

Thus, the coordinate of unknown node can be expressed by the least square method:

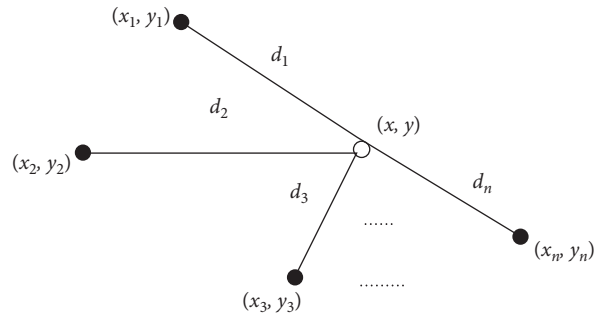

Figure 2: Classic RSSI position location.

$$\widehat{X} = \left(A^T W A\right)^{-1} A^T W B, \tag{12}$$

where W was symmetric positive definite matrix (simple diagonal positive definite matrix), and selecting the appropriate weighting matrix can effectively improve the location accuracy.

When $W = \begin{bmatrix} 1, 0, \ldots, 0 \\ 0, 1, \ldots, 0 \\ \cdots\cdots \\ 0, \ldots, 1, 0 \\ 0, \ldots, 0, 1 \end{bmatrix}$, formula (12) was trilateration method.

3. Application Advantages of RSSI

The RSSI is an important method to solve the problem of node localization. Its main application advantages are as follows:

(1) Convenient application: The RSSI is the received signal strength from the other side in mutual communication and often can be extracted directly from the hardware in normal communication between wireless sensor nodes without requiring additional devices, which is of great significance to reduce the network cost and complexity.

(2) Symmetry: The RSSI value is often symmetric, so the RSSI value between two nodes can be completed only by sending and receiving a message packet, which is of great significance to reduce the complexity of localization algorithm and the application scene which is not very demanding for location accuracy.

(3) Distance monotonicity: The distance value between the RSSI value and node is monotonic and becomes smaller with the increase of distance. Therefore, the RSSI can meet the requirements of ranging and ranging-free localization algorithms.

4. Detection Method of Sybil Attacks

The solution to Sybil attacks based on RSSI will not increase the burden of WSN. When a message was received, the receiver will contact the RSSI with the sender ID. Later, when another message containing the same RSSI but with different sender ID was received, the receiver will assume it as a Sybil attack. However, this method was not feasible due to the difference in receiving time of RSSI [5, 6]. In addition, the energy of WSN transmitter can be easily changed, so one Sybil node can send messages with different IDs and transmission energies in order to deceive the receiving node. With the function of energy transmission, sending messages with different transmission energies will result in different RSSI readings.

In this paper, a method of solving the Sybil attacks in WSN based on RSSI was studied. This method had good robustness and simple structure and can be easily implemented in sensors. According to the existing data, this method is the best way to solve the Sybil attacks in WSN.

It was verified by experiment that although the RSSI was unreliable and had time differences and nonequivalent transmission ratios [5], these problems can be easily solved by using the RSSI ratios of multiple receiving nodes that were introduced in the literature [7]. The problem of time differences in RSSI ratios was studied with a variable RSSI receiver by experiment, and the standard deviation was very small. Then the reliable intervals of these time differences were given by the experiments of different distances. To simplify the problem, there was no need to calculate the location of the sender so as to avoid the calculation of distance attenuation, thus reducing the calculation requirements of the system.

The literature [8–11] studied the localization algorithm based on the distance between nodes obtained by RSSI ranging. In WSN, theoretically, the spatial location of an unknown node can be determined by the trilateration method through the RSSI information of four anchor nodes. Thus, the location of all sensors can be found. Suppose that the ith node received the radio signal from the Oth node; thus, the RSSI was

$$R_i = \frac{P_0 \cdot K}{d_i^{\alpha}}, \tag{13}$$

where R_i was RSSI, P_0 was the transmitted signal energy, K was constant, d_i was the Euclidean distance, and α was the rate of change between distance and energy. Suppose the jth node received the radio signal from the Oth node; thus, R_j had the same calculation conclusion similar to formula (13).

Thus, the RSSI ratios of the ith node and the jth node were obtained:

$$\frac{R_i}{R_j} = \frac{\left(P_o \cdot K/d_i^{\alpha}\right)}{\left(P_o \cdot K/d_j^{\alpha}\right)} = \left(\frac{d_i}{d_j}\right)^{\alpha}. \tag{14}$$

Formula (15) can be obtained by solving the following ith, jth, kth, and lth receiving nodes by the location coordinate (x, y) of node:

$$\begin{aligned}
&(x - x_i)^2 + (y - y_i)^2 \\
&\quad = \left(\frac{R_i}{R_j}\right)^{1/\alpha} \left((x - x_j)^2 + (y - y_j)^2\right) \\
&\quad = \left(\frac{R_i}{R_k}\right)^{1/\alpha} \left((x - x_k)^2 + (y - y_k)^2\right) \\
&\quad = \left(\frac{R_i}{R_l}\right)^{1/\alpha} \left((x - x_l)^2 + (y - y_l)^2\right),
\end{aligned} \tag{15}$$

where (x_i, y_i) was the location coordinate of the ith node and the location coordinate of other nodes was similar.

When a message was received, four detection nodes calculated the location of the sender by formula (15) and contacted the location of the sender with the message containing the sender ID. Later, when another message containing different sender ID was received, the receiver will assume it as a Sybil attack as the calculation structure of location coordinate of the sender was the same as earlier.

However, the amount of calculation of the location of each node by formula (15) was very huge. In fact, it was not necessary to detect the Sybil nodes through this calculation. The location of all x, y and x_i, y_i remained consistent; thus, the Sybil attacks can be detected by comparing the RSSI ratio of the received message. Suppose the IDs of four detection nodes were D_1, D_2, D_3, and D_4, respectively, and the forged IDs of one Sybil node were S_1 and S_2. The topology is shown in Figure 3.

At t_1, the Sybil node broadcast a message and forged its ID as S_1. The four neighbor nodes received the energy ratio and S_1 from the Sybil node, transmitted the message containing their own ID, and received the RSSI from the Sybil node to the normal node. Note that R_i^k was RSSI value (when the transmitting node K received the signal of the ith node). Thus, D_1 calculated the ratio for each node:

$$\begin{gathered}
\frac{R_{D_1}^{S_1}}{R_{D_2}^{S_1}}, \\
\frac{R_{D_1}^{S_1}}{R_{D_3}^{S_1}}, \\
\frac{R_{D_1}^{S_1}}{R_{D_4}^{S_1}}.
\end{gathered} \tag{16}$$

And these ratios were stored.

Similarly, at t_2, the Sybil node broadcast a message again and forged its ID as S_2. The four neighbor nodes received the energy ratio from the Sybil node and reported it to D_1. Thus, D_1 calculated each other's ratio:

$$\begin{gathered}
\frac{R_{D_1}^{S_2}}{R_{D_2}^{S_2}}, \\
\frac{R_{D_1}^{S_2}}{R_{D_3}^{S_2}}, \\
\frac{R_{D_1}^{S_2}}{R_{D_4}^{S_2}}.
\end{gathered} \tag{17}$$

At this point, D_1 can detect the Sybil nodes according to the ratios at t_1 and t_2. D_1 can conclude that if the gap between the values of two messages was close to zero, then there was a Sybil attack in this region. The received energy ratio was the same, so the location was the same. Normally, the messages broadcast by the node came from multiple IDs, but when there was a Sybil attack, the messages broadcast by the node came from the same ID. The following formula was used to calculate:

$$\begin{gathered}
\left(\frac{R_{D_1}^{S_1}}{R_{D_2}^{S_1}} = \frac{R_{D_1}^{S_2}}{R_{D_2}^{S_2}}\right), \\
\left(\frac{R_{D_1}^{S_1}}{R_{D_3}^{S_1}} = \frac{R_{D_1}^{S_2}}{R_{D_3}^{S_2}}\right), \\
\left(\frac{R_{D_1}^{S_1}}{R_{D_4}^{S_2}} = \frac{R_{D_1}^{S_2}}{R_{D_4}^{S_2}}\right).
\end{gathered} \tag{18}$$

If formula (18) was valid, a Sybil attack was detected.

5. Experimental Simulation Analysis

Ideally, if the transmitting node and receiving node are kept in place, the RSSI will remain the same. Even under these conditions, the RSSI still fluctuates in the actual situation. Therefore, in this paper, the amount of the fluctuation was determined by experiment to further study the difference in the RSSI and explore how to solve this problem.

First, a node with constant energy (0 dbm) was used to transmit the message "nihao." Another node was used as a receiving node to automatically capture the RSSI values through the program TOS_Msg- > strength in TinyOS and to transmit them to the PC through the RSC-232 serial port. The transmitting node transmitted this message 2,000 times. The distance between the transmitting node and the receiving node was set as 30 cm and changed to 1 m to repeat the experiment, as shown in Figure 4.

The mean and standard deviation σ of the data in Figure 4(a) were 54.55 and 14.32, respectively, and the mean and standard deviation σ of the data in Figure 4(b) were 133.26 and 12.38, respectively, suggesting RSSI

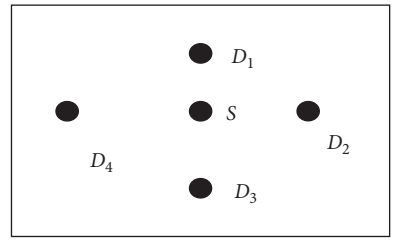

Figure 3: Topology model.

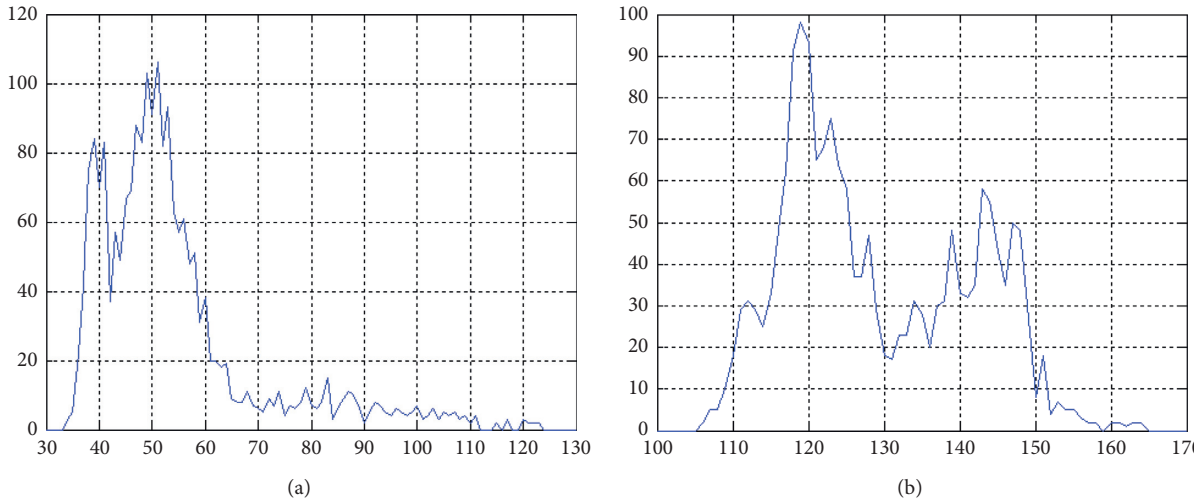

Figure 4: Comparison of RSSI difference. (a) The distance is 30 cm (X: RSSI value; Y: frequency of occurrence). (b) The distance is 1 m (X: RSSI value; Y: frequency of occurrence).

inconsistency. The correlation between the RSSI values was very small, making it unsuitable for detecting the Sybil attacks.

Then, two receiving nodes were used to analyze and compare their RSSI ratios to solve the problem of RSSI time inconsistency. It should be noted that the RSSI ratios also needed to solve the problem that the transmitting nodes had different transmission energies. In this experiment, the transmitting node broadcast a message 2,000 times with random and different transmission energies each time. The two receiving nodes recorded the RSSI values and transmit them to the base station to connect to the PC. The distance between the transmitting node and the receiving node was changed to 1 m to repeat the experiment twice.

The base station calculated the RSSI ratios of the two receiving nodes at t_1 and t_2, respectively, and then calculated and recorded the difference between the two RSSI ratios, as shown in Figure 5.

The mean and standard deviation σ of the data in Figure 5(a) were 0 and 0.068, respectively, and the mean and standard deviation σ of the data in Figure 5(b) were 0 and 0.098, respectively, suggesting RSSI inconsistency. The difference in the RSSI ratio at point 0 controlled other data changes. The −0.2 and 0.2 in Figure 5(a) appeared only once in 2000 times (accounting for 0.5% of the total times), and the same applied to the −0.35 and 0.425 in Figure 5(b).

Therefore, a threshold $k * \sigma$ was set to determine the Sybil node. If $K > 3$, the Sybil attacks can be stably detected by the following formula according to the algorithm given earlier. If s_1 and s_2 were different but had the same location, the Sybil attacks can be inferred by judging whether the difference in the RSSI ratios of two events was within the threshold $k * \sigma$.

$$\left(\frac{R_{D_1}^{S_1}}{R_{D_2}^{S_1}} - \frac{R_{D_1}^{S_2}}{R_{D_2}^{S_1}}\right) < \sigma,$$

$$\left(\frac{R_{D_1}^{S_1}}{R_{D_3}^{S_1}} - \frac{R_{D_1}^{S_2}}{R_{D_3}^{S_2}}\right) < \sigma, \tag{19}$$

$$\left(\frac{R_{D_1}^{S_1}}{R_{D_4}^{S_1}} - \frac{R_{D_1}^{S_2}}{R_{D_4}^{S_2}}\right) < \sigma.$$

If the standard deviation deviated from the Gaussian distribution by about 70%, the threshold σ meant that the detected rate of the Sybil node was 70%. To reach 99.9%, the threshold was set as 5σ.

To estimate the influence of distance on the threshold σ, the second step experiment was repeated by increasing the distance between the transmitter and the receiver. The

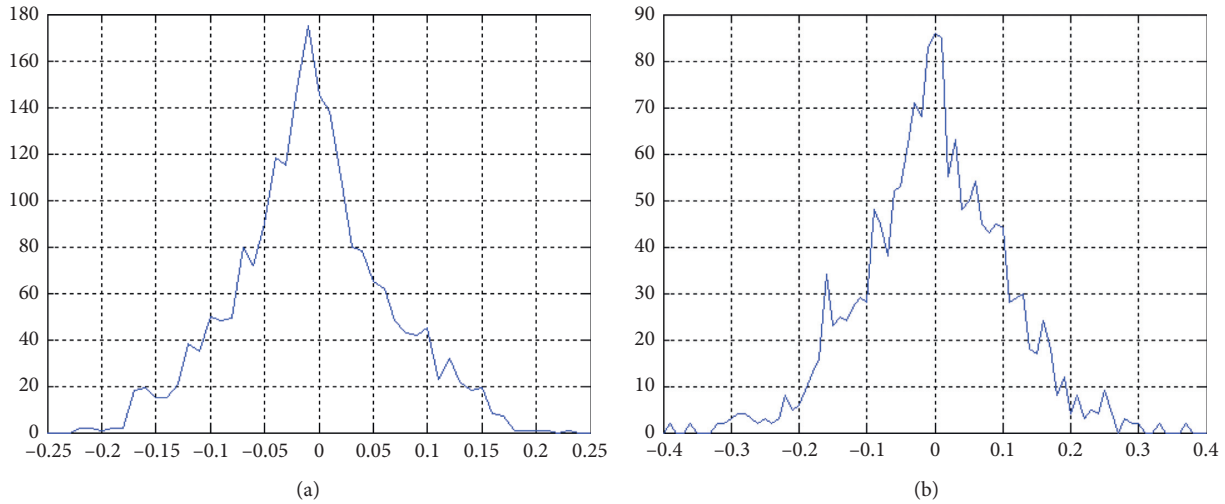

Figure 5: Comparison of RSSI difference. (a) The RSSI ratio at t_1 (X: RSSI value; Y: frequency of occurrence). (b) The RSSI ratio at t_2 (X: RSSI value; Y: frequency of occurrence).

second step experiment was performed 100 times at each distance, and the range of changing the distance was 1 m to 10 m, and the step length was 1 m.

As shown in Figure 6, the data 1 was median value, the data 2 was mean, the data 3 was standard deviation distribution, and the σ deviation will not exceed 0.15. Thus, the conclusion was drawn that if σ was set as 0.15, the Sybil node can be protected from attack when the threshold was set as 0.75.

Based on the Sybil attack protocol, the detection effect of RSSI was detected through different experimental steps. In the first step, four receiving nodes were used. In the second step, two receiving nodes were used. In the last step, as a control experiment, the Sybil nodes were limited by the transmission energy of changing nodes to evaluate the integrity and accuracy of the detection technology.

In the first step, four detection nodes were used to detect the Sybil attacks. First, the integrity of the detection technology was evaluated by experiment. The node distribution topology is shown in Figure 7(a). There was one Sybil node and four receiving nodes in WSN. When the Sybil node broadcast a message, the four detection nodes will record the RSSI value and ID according to the message, and D_2, D_3, and D_4 will transmit the data to D_1. When the Sybil node broadcast a message with different IDs and transmission energies, the four detection nodes will record the RSSI value and ID according to the new message and then transmit the data to D_1 again. D_1 detected the Sybil attacks in WSN by formula (18).

The threshold was set as $5 * \sigma$. According to the previous analysis, the threshold was set as 0.75. To avoid message conflict in the experiment, the transmission time of each message was controlled with a timer. In the experiment, the Sybil node broadcast a message once every 30 seconds, and the receiving nodes transmitted the data to D_1 three seconds after detecting the Sybil node.

The distance between the receiving nodes and the Sybil node was changed to repeat the above experiment 100 times. Transmitting the message at a 30-second interval meant that the topology was changed every one minute. Even in this case, D_1 can detect the Sybil attacks.

To detect the accuracy, the topology was changed, as shown in Figure 7(b). Here, the Sybil nodes in WSN were ignored, and two normal nodes were deployed to use only their own ID to broadcast messages. For the purpose of energy efficiency, some protocols required nodes to transmit messages with different transmission energies. The transmission energy will inevitably change when the energy of battery reduced and the environment changed, so the two normal nodes broadcast messages with different transmission energies. It should be noted that when the receiving nodes analyzed by the RSSI ratio, the change of transmission energy will not affect the correctness of evaluation of the Sybil nodes by the normal nodes. In each operation, the normal nodes' mutual locations were changed.

In the 100 times of experiments, D_1 did not report any Sybil attack. Even when the two normal nodes were only a few centimeters away, D_1 did not detect any Sybil node in WSN. Thus, the conclusion was drawn that four detection nodes can be used to detect the Sybil attacks based on RSSI.

In the second step, two detection nodes were used to detect the Sybil attacks. First, the integrity of the detection technology was evaluated by experiment the same as the first step. The node distribution topology is shown in Figure 8(a). There were two receiving nodes and one Sybil node. The distance between the receiving nodes and the Sybil node was changed to repeat the experiment 100 times the same as above. Because there were only two receiving nodes, only one comparison by formula (18) was required.

A conclusion similar to the first step was drawn that D_1 can detect the Sybil attacks in WSN.

To study whether the detection nodes can identify the Sybil attacks or normal events, the topology shown in Figure 8(b) was adopted. There were two monitors and two normal nodes in the topology, and each normal node had different IDs and transmission energies. The experimental

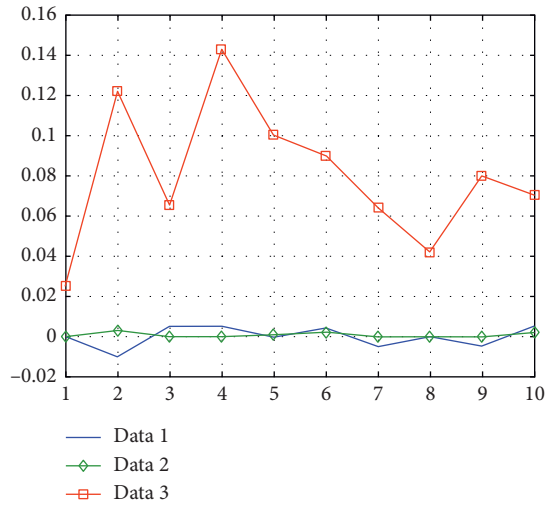

Figure 6: Distribution of median, mean value, and standard deviation (X: distance (m)).

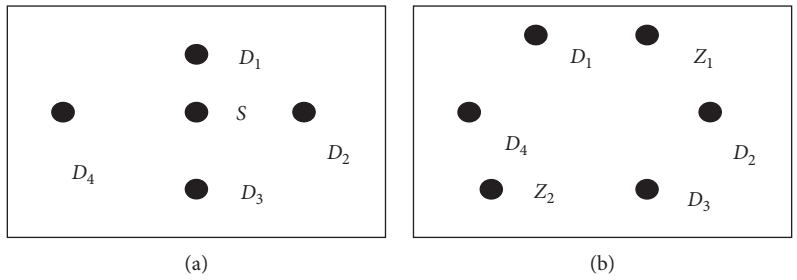

Figure 7: Four nodes detect Sybil attacking topology model. (a) 4 detection nodes and 1 Sybil node topology; (b) 4 detection nodes and 2 normal node topologies.

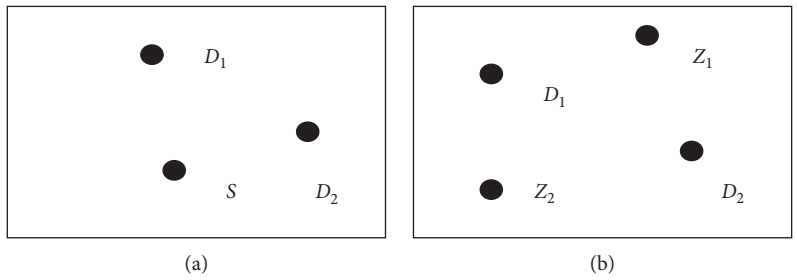

Figure 8: Two nodes detect Sybil attacking topology model. (a) 2 detection nodes and 1 Sybil node topology; (b) 2 detection nodes and 1 normal node topologies.

steps were the same as above, but only one comparison was required. The locations of the normal nodes were changed to repeat the experiment 100 times. During the 100 times of experiments, D_1 did not accurately detect the Sybil attack three times; that is, the error rate was lower than 5% when there were only two receiving nodes.

It should be noted that the Sybil attacks can be detected with only one transmission when there were two receiving nodes. Therefore, the energy consumption will be very small, but the error rate will increase. However, the integrity was more important than accuracy for the Sybil attacks; that is, the consequence of failing to detect the Sybil nodes was much more serious than low accuracy. Based on this evaluation, it was suggested that the detection of Sybil attacks based on RSSI used two detection nodes rather than four detection nodes.

6. Conclusion

In this paper, first, the basic principle and typical algorithm of RSSI were introduced. Then, a detection method of Sybil attacks based on RSSI was proposed, the formulas of the basic principle were derived, and a simulation experiment of the algorithm was conducted. From the experiment results,

the appropriate threshold was found. The simulation results showed that the detection method can effectively resist the Sybil attacks. Finally, the effects of the number of receiving nodes on the detection effect of Sybil attacks were compared, and the Sybil attacks can be accurately detected by using the RSSI ratios of two receiving nodes. The method will be simulated in a larger and more complex environment so as to further study the stability and security of the work in the future.

Data Availability

The values of the initial experimental distance and the coordinate value are set by authors, and the remaining parameters are empirical data.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by Cultivate Scientific Research Excellence Programs of Higher Education Institutions in Shanxi (2020KJ025); Research Project Supported by Shanxi Scholarship Council of China (2020-139); Xinzhou Teachers University Academic Leader Project.

References

[1] W. E. I. Dapeng, *Research on Node Location Algorithm in Wireless Sensor Networks*, Taiyuan University of Technology, Shanxi, China, 2015.

[2] Z. Haoling, S. Shou, and W. Xia, "Dynamic distance estimation algorithm based on RSSI and LQI," *Electronic Measurement Technology*, vol. 30, no. 2, pp. 142–144, 2017.

[3] Y. Sun, "Review of wireless sensor networks," *Journal of Communication*, vol. 25, no. 4, pp. 114–124, 2019.

[4] Y. Liu, *Design and Implementation of Wireless Sensor Network Positioning System*, Northwestern Polytechnical University, Xian, China, 2017.

[5] D. Kotz, C. Newport, R. S. Gray, J. Liu, Y. Yuan, and C. Elliott, "Experimental evaluation of wireless simulation assumptions," in *Proceedings of the 7th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM'04)*, Venice, Italy, 2014.

[6] G. Zhou, T. He, S. Krishnamurthy, and J. A. Stankovic, "Impact of radio irregularity on wireless sensor networks," in *Proceedings of the 2nd International Conference on Mobile Systems, Applications, and services (MobiSys' 04)*, Boston, MA, USA, 2018.

[7] S. Zhong, L. Li, Y. G. Liu, and Y. R. Yang, "Privacy-preserving location based services for mobile users in wireless networks," Technical Report YALEU/DCS/TR-1297, Yale Computer Science, July 2014.

[8] D. Nicolescu and B. Nath, "Ad2Hoc positioning systems (APS)," in *Proceedings of the 2001 IEEE Global Telecommunications Conference (IEEE GLOBECOM 01)*, San Antonio, TX, USA, 2011.

[9] D. Niculescu and B. Nath, "DV based positioning in ad hoc networks," *Journal of Telecommunication Systems*, no. 22, pp. 267–280, 2013.

[10] Y. Feng and S. Haoshan, "An intelligent location algorithm for wireless sensor networks based on ranging," *Chinese Journal of Sensors and Actuators*, vol. 21, no. 1, pp. 135–140, 2018.

[11] M. M. Patil, U. Shaha, U. B. Desai et al., "Localization in wireless sensor networks using three masters," in *Proceedings of the Personal Wireless Communications (ICPWC)*, New Delhi, India, 2015.