A Research of RSSI-AM Localization Algorithm Based on Data Encryption in Wireless Sensor Networks

* Wang Wei, Wang Zhaoba
School of Information and Communication Engineering, North University of China,
Taiyuan, Shanxi, China
* Tel.: 13015348037, fax: 3559521
* E-mail: 41695559@qq.com

Received: 16 July 2014 /Accepted: 28 July 2014 /Published: 31 July 2014

Abstract: In practical application of wireless sensor networks, because of open environment, signal is easy to be attacked and traditional RSSI location technology produces errors. By analyzing the location modal of RSSI, this paper proposes a new encryption modulation algorithm: RSSI-AM, which is unlike most approaches. The location algorithm has the following advantages: simple calculation, strong security, powerful anti-interference ability and no hardware expansion required. Besides, the simulation experiment shows the location precision of ranging method based on RSSI-AM has obvious improvement compared with traditional algorithm. It can be used in the environment of wireless sensor network nodes with low cost and performance of hardware. Copyright © 2014 IFSA Publishing, S. L.

Keywords: Wireless sensor networks, RSSI, Modulation, Encryption, Anti-attack.

1. Introduction

WSN, Wireless Sensor Network, is a hot technology at present. It integrates three fields: calculation, communication and sensor, which becomes a brand-new acquisition and processing information technology. It is generally acknowledged to be current and future research direction and it will generate a prolonged influence on human beings’ lifestyle. WSN is a self-organizing wireless network composed of sensor nodes with data-collecting, data-proceeding and wireless communication ability, whose purpose is to cooperatively perceive, collect and process information which come from perception objects in network coverage intra-region, then transmits to main control center to execute system decision [1-3]. As many technologies, like wireless communication, microprocessor and micro electromechanical system, develop increasingly rapidly, with low cost, self-organization, small size and flexible distribution, wireless sensor network technology gradually becomes matured. Its adaptability is becoming wider and wider and has a broad prospect in military detection, environmental information monitoring, space exploration, agriculture production, medical health monitoring, architecture and intelligent house, industrial production control, traffic control and commercial field [4-6].

In wireless sensor network, location information of sensor nodes is an emphasis to whole network’s information acquisition and processing. Currently, there have been many systems and algorithms committed to researching WSN location technology, but because WSN has many adaptabilities in open environment, location system is liable to be interfered by outer signals, including outer attack [7-9]. Location algorithm of WSN needs a
safety protection in order to provide a safe and effective network. In recent years, many researchers have proposed some relevant algorithms, which have strong pertinent suggestion and mainly emphasize certain specific attack. Once attack type is changed, safety protection will produce failure. What’s more, most of algorithms mainly study how to prevent malicious attacks, however, in the practical and applied environment, there are other unavoidable interference-signals. It is extremely necessary to think about preventive methods [10-13].

2. Related Work

The location in WSN means how a node in network obtains its geographical location information. Most of WSN adopt the distributed localization technology, whose principle is as follows: Network contains a small quantity of anchor nodes, which use self-carrying GPS location component to obtain location information, then send referential information and establish coordinate system. Other unknown-nodes measure or estimate location relation between self nodes and anchor nodes, including distance, angle and relation of region, then adopt these relation and specific algorithm to calculate location of unknown nodes. The methods of location algorithm often used have trilateration, triangulation and maximum likelihood estimation method, etc. [14-16].

According to the location seeking mechanism, the location method of WSN can be divided into two types: range-based and range-free. The former is used to measure distance between nodes or angle information, then it applies mathematics method to calculate nodes location, whose methods often utilized are based on TOA (time of arrival), TDOA (time difference of arrival), AOA (angle of arrival), RSSI (received signal strength indication) and so on. The latter needn’t distance and angle information. It makes use of network connectivity and other information to realize node location, whose methods often used are centroid algorithm, amorphous algorithm, DV-HOP, APIT and so on. These algorithms mentioned above are in ideal environment to locate and don’t consider that outer factors have location influence on the system [17-22].

3. RSSI Algorithm Research

Under the situation of known transmission power, through receiving node measurement to receive power, RSSI uses receiving power loss of receiving node to calculate transmission loss, ultimately, it turns transmission loss into distance by applying theory or practical signal transmission model. After obtaining relevant distance information between anchor nodes and unknown nodes, adopt trilateration or maximum likelihood estimation method to get the location of unknown nodes. In practical environment and adaptability process, especially in the situation of dense-nodes distribution, reflection, multi-path transmission, antenna gain and other factors can generate different effect.

Because the value of RSSI has symmetry, when measuring the value of RSSI between nodes, task can be completed by sending and receiving a message package, but not a roundtrip. Distance value between the value of RSSI and nodes possesses monotonicity, which will decrease with increase of distance. Thus, RSSI can satisfy location algorithm requirement of range-based and range-free simultaneously. When nodes have communication, RSSI is the value of signal strength from receiving signal of opponents. So when wireless sensor nodes have normal communication, signal needn’t any other equipment and can be directly extracted from hardware. In this way, it can decrease network cost and complexity.

Let us analyze the basic principle of RSSI from the angle of mathematics. The mathematical relation between transmission power of wireless signal from sensor nodes and its receiving power can be expressed as follows in Formula (1). The receiving power of wireless signal is \( P_R \); the transmission power is \( P_T \), the distance between transceiver units is \( r \), the transmission factor is \( n \), the transmission environment of wireless signal has great influence on the value of transmission factor.

Signal transmission theory model is generally used to analyze radio wave transmission loss model. The establishment of signals empirical models is the matching between location of each point and database of signal strength. Because loss affects location precision of RSSI value greatly, it is cautious to select suitable loss model. In general, it is reasonable to choose free space transmission loss model and log normal distribution model to execute calculation.

Free space transmission loss model is as follows:

\[
PL(d_0) = 32.44 + 20 \log d_0 \quad \text{(1)}
\]

In the model, when \( d_0 = 1 \) meter, \( PL(d_0) \) is pass loss of wireless transmission distance, \( n \) is the distance loss factor, \( f \) is the signal frequency.

Log normal distribution model is as follows:

\[
PL(d) = PL(d_0) + 10n \log(d/d_0) + \xi \quad \text{(2)}
\]

In the model, \( PL(d) \) is the pass loss of transmission distance, \( d \), \( PL(d_0) \) is the pass loss, when the transmission distance \( d_0 = 1 \) m, \( n \) is the attenuation coefficient of signal, the value is between 2 and 5, \( \xi \) is the zero-mean Gaussian random distribution function.

The signal strength of location nodes receiving referential nodes is:

\[
\text{RSSI} = P_s + P_r - PL(d) \quad \text{(3)}
\]

In (3), SSI is the power of receiving, \( P_s \) is the
power of node transmission, \( P_a \) is the antenna gain, and \( P_L(d) \) is the path loss.

Formula (1) and (2) are introduced into Formula (3), then the result is

\[
\text{RSSI} = P_s + P_a - 32.44 - \frac{\xi}{\lg(10)\lg(\frac{44.32}{P_{RSSI}})}
\]

(4)

Setting a parameter: \( M = P_s + P_a - 32.44 - \xi \),

Formula (4) is:

\[
\text{df} = 10\lg\frac{M - \text{RSSI}}{d_f}
\]

(5)

In WSN, because RSSI signal is transmitted in space, it not only possesses a feature of transmission, but also it will be interfered by other signals. Aiming at the practical problem, we pose a solution to solve the problem by improving algorithm to reinforce anti-interference ability and resistance ability of malicious attack.

In the process of WSN layout, calculation of difference from multi RSSI signals is

\[
\text{RSSI}_i - \text{RSSI}_j = (M_i - 10\lg f_i) - (M_j - 10\lg f_j)
\]

\[
= M_i - M_j + 10\lg \frac{d_i f_j}{d_j f_i}
\]

(6)

When, in WSN nodes, transmission frequency, transmission power, antenna gain and path loss gain are the same, the result is

\[
\text{RSSI}_i - \text{RSSI}_j = 10\lg \frac{d_i}{d_j}
\]

(7)

In the same principle, the relation of RSSI difference value between two nodes is also gotten by using RSSI difference value of relevant nodes to transmit signal location information.

### 4. Encryption RSSI-AM Algorithm Research

Base-band modulation signal and carrier start to modulate at the beginning, then obtain modulated wave (also called modulated signal). Modulated signal is transmitted to receiving terminal by channel after receiving terminal demodulates and restores original base-band signal. Demodulation is reverse transform of modulation, which is a process of extracting modulated signal from modulated wave. Modulation and demodulation signal communication system not only optimizes hardware requirement of receiving and transmitter, but also decrease interference and attack damage during transportation process. In WSN, nodes receive RSSI difference signal to modulate so that it can increase the ability of anti-inference and anti-attack of information transmission system, using Formula (7) to modulate. \( y \) is the carrier signal:

\[
y = 10A\frac{d_i}{d_i} \cos wt
\]

(8)

A is the signal amplitude; \( w \) is the angular frequency.

Adopting RSSI difference value to modulate amplitude on carrier wave can realize long-distance transmission, and the frequency of carried wave is changeable, in open environment, it is not liable to be attacked maliciously. The result of modulation is:

\[
y = 10A\frac{d_i}{d_i} \cos wt
\]

(9)

where \( n \) is the corresponding node number in WSN. In the Formula (9), \( d_i/d_j \) is the discrete value. In the practical application, use a timer to make the signal keep an amplitude value unchanged in a carrier circle.

Because the WSN is often set in open environment, it is easily attacked and interfered from outsiders. According to the basic principle of RSSI, unknown node is needed at least three anchor nodes of known location information to locate. Simulation adopts MATLAB to establish a unified simulation environment in the range of 50 m×50 m×50 m and anchor nodes are distributed in the range. On the basis of three RSSI difference values, \( d_1=1.5 \text{ m}, d_2=1.7 \text{ m}, d_3=1.9 \text{ m}, A=1 \text{ m}, f=250 \text{ Hz} \), the Formula (9) is simulated with MATLAB, and the result is Fig. 1.

![Fig. 1. Modulation of three RSSI difference values.](image-url)
Under the circumstance that a WSN system has been a small application scale, which means the number of anchor nodes is limited. If the system simply depends on the anchor nodes to locate unknown nodes, it is easily destroyed especially when there are attacks from outsiders. Based on the RSSI-AM, which is studied in the paper, system can possess security and anti-interference. Firstly, all sensors are set physically. The layout process can be regular or at random. Then, according to RSSI relation, sensor network locates all nodes by anchor nodes. In this situation, the system can get location information of all nodes, which they are accurate. All nodes can act as the role of anchor nodes and help the system to establish an inter-relative node location relation. If nodes are destroyed or attacked by opponents, or nodes have itself performance fault, the system can realize the accurate location by much more known nodes.

Location information is converted into ciphertext and formed encrypting key, then at receiving terminal, use decryption key to identify location information. Current encryption algorithm mainly adopts the symmetrical key algorithm and the non-symmetry key, because the calculation complexity of two algorithms is much higher and has better security. However, because it is limited for sensor equipments to use available resources in WSN, we consider adopting a substitution algorithm to encrypt.

According to the normal sequence to the arrange data, make them correspond with 3, 4, 5, 6, 7, 8, 9, 0, 1, 2 (encryption key is 3) and substitution encryption is implemented on the 10 RSSI difference value signals mentioned above.

Plaintext: 1.5 m, 1.7 m, 1.9 m, 2.3 m, 2.5 m, 2.9 m, 3.3 m, 3.7 m, 3.8 m, 3.9 m.
First ciphertext: 3.7 m, 3.9 m, 3.1 m, 4.5 m, 4.7 m, 4.1 m, 5.5 m, 5.9 m, 5.0 m, 5.1 m.
Next, add the first ciphertext with 5, 6, 7, 8, 9, 0, 1, 2, 3, 4 (encryption key is 5) correspondently and get the secondary ciphertext.
Secondary ciphertext: 8.7 m, 9.1 m, 10.1 m, 12.5 m, 13.7 m, 4.1 m, 6.5 m, 7.9 m, 8.0 m, 9.1 m.
Then, according to 5-3=2 (2 is encryption key),
The amplitude and location sequence of the original data are all changed after three encryptions, and attacker is difficult to decrypt the data. Algorithm is not complex and it satisfies hardware limit requirement of WSN, furthermore, it doesn’t occupy much too large calculation resources, energy consumption is small and security is strong.

The receiver of the receiving terminal demodulates modulation signals and the modulation of signals terminal has received are executed an analysis of envelope detection. After detection, Fig. 6 is gotten.

![Fig. 6. The result of envelope detection.](image)

Decrypt the demodulation signals and its process is a reverse process of encryption. According to encryption key 3 and 5, we implement three inverse transformations on ciphertext and get RSSI difference value information of sending terminal. It is the plaintext: 1.5 m, 1.7 m, 1.9 m, 2.3 m, 2.5 m, 2.9 m, 3.3 m, 3.7 m, 3.8 m, 3.9 m. RSSI difference signal information, which receiving terminal has received, is processed according to a synchronous clock.

\[ E = \text{RSSI}_1 - \text{RSSI}_2 = 10\ln \frac{d_1}{d_2} \]  
\[ d = \frac{d_n}{10^{0.05}} \]

where \( E \) is the RSSI difference value nodes have received, \( d_n \) is the distance between known nodes and target node. By the Formula (11), we can get the correspondent distance \( d \).

Using the maximum likelihood estimation algorithm, we get location information of target nodes. From 1 to \( N \) node coordinates can be represented as \((x_1, y_1), (x_2, y_2), (x_3, y_3), ..., (x_n, y_n)\), assume knowing: \( d_1, d_2, d_3, ..., d_n \), which are the distance from node \( D \) to \( n \) nodes. Suppose the coordinate of node \( D \) as \((x, y)\) (Fig. 7).

![Fig. 7. Maximum likelihood estimation method.](image)

The formula is:

\[(x_1-x)^2 + (y_1-y)^2 = d_1^2\]
\[\vdots\]
\[(x_n-x)^2 + (y_n-y)^2 = d_n^2\]

First formula deducts the last formula respectively, the result is

\[x_1^2 - x_n^2 - 2(x_1 - x_n)x + (y_1^2 - y_n^2 - 2(y_1 - y_n)y = d_1^2 - d_n^2\]
\[\vdots\]
\[x_{n-1}^2 - x_n^2 - 2(x_{n-1} - x_n)x + (y_{n-1}^2 - y_n^2 - 2(y_{n-1} - y_n)y = d_{n-1}^2 - d_n^2\]

The formula rewrites to linear equations: \(AX = b\),

\[X = \begin{bmatrix} x \\ y \end{bmatrix}\]

\[b = \begin{bmatrix} x_1^2 - x_2^2 + y_1^2 - y_2^2 + d_1^2 - d_2^2 \\ \vdots \\ x_{n-1}^2 - x_n^2 + y_{n-1}^2 - y_n^2 + d_{n-1}^2 - d_n^2 \end{bmatrix}\]

\[b = \begin{bmatrix} x_1^2 - x_2^2 + y_1^2 - y_2^2 + d_1^2 - d_2^2 \\ \vdots \\ x_{n-1}^2 - x_n^2 + y_{n-1}^2 - y_n^2 + d_{n-1}^2 - d_n^2 \end{bmatrix}\]

Using the standard optimal mean the square estimation can get the coordinate of node \( D \): 
\[X = (A^T A)^{-1} A^T b\]. The feature of Maximum likelihood estimation is that it can make full use of location information that nodes have collected and its expression way is brief so that many location algorithms often use it.

5. Comparison of Property

In order to compare the property between the RSSI-AM location node algorithm and the traditional RSSI location algorithm, we adopt MATLAB to establish a simulation environment in the range of...
50 m×50 m×50 m. Anchor nodes are evenly distributed in the range. Anchor nodes can deliver itself information periodically and each unknown node can receive information from all anchor nodes. Simulation adopts 100 results from unknown nodes evenly distributed in the measured range to get arithmetic average as the final result. In Fig. 8, when the ratio of anchor node is less than 16 %, the location precision of RSSI-AM is obviously higher than the RSSI algorithm. As the number of anchor nodes increases, the location precision of two algorithms gets continual improvement. When the ratio of anchor nodes is nearly approaching to 30 %, the precision approaches to the constant value.

**Fig. 8.** The precision of location algorithm.

Fig. 9 shows the communication traffic comparison of RSSI-AM ranging algorithm and RSSI ranging algorithm. Although the RSSI-AM algorithm increases some communication expense, however, the expense is not costly and doesn’t bring huge burden to communication.

**Fig. 9.** Time of location algorithm.

### 6. Conclusion and Future Work

The paper proposes a new location encryption modulation algorithm: RSSI-AM based on the RSSI sensor network. The algorithm adopts the RSSI basic ranging principle, space transmission loss model and lognormal distribution model to deduce the relation of unknown nodes and anchor nodes. In order to adjust to complicated environment for living and malicious attack in WSN, the algorithm encrypts data and uses the RSSI difference value to modulate carried wave amplitude. In the receiving terminal, get the RSSI by the envelope detection and the decryption. Then the maximum likelihood estimation can help get location information of nodes. The algorithm has not higher requirements on hardware and is utilized to ranging requirement of most of WSN location.

In the future research work, we will aim at the technology features of WSN, increase the number of detected nodes and do a large quantity of simulation experiments over different distribution models in order to verify location effect when sensors are applied in large scale. Besides, we will make a lot of simulation analysis and functionalities comparison directing at different modulation methods, master its application functionalities and scope and do a further research of data encryption algorithm which is suitable to WSN.

### Acknowledgements

This work was supported by the national natural science founds of shanxi province of China under grant 2013021015-2 and in part by the national natural science founds of China under grant 60672005.

### References


