www.sensorsportal.com

Sensors & Transducers

© 2013 by IFSA
http://www.sensorsportal.com

Anti Spoofing Attack Positioning Algorithm for Wireless Sensor Networks Based on Distance Verification

[1,2] Hongbin WANG, [3] Yueqi HAN

[1] Department of Computer Science, Xinzhou Teachers University,
Xinzhou, 034000, China
[2] College of Electric Information Engineering, Tianjin University,
Tianjin, 300072, China
[3] College of Mechanical Engineering, Taiyuan University of Science and Technology,
Taiyuan, 030024, China
[1] E-mail: kinghongbin@yeah.net

Received: 10 September 2013 /Accepted: 25 October 2013 /Published: 30 November 2013

Abstract: The precise location of sensor node is the premise of guaranteeing the effectiveness and validity of WSNS in its application and nodes positioning technology is a key technology of wireless sensor networks. For its inherent characteristics, such as limitation of the resources, insecurity and openness of the deployment environment, mechanism of location for wireless sensor networks has security problems. An effective approach to monitoring and detecting spoofing attacks based on distance verification are proposed. The detecting mechanism is based on the visualization of the consistency between the time of transmission and the loss of the power. Experimental studies are conducted to investigate the effect of the algorithm. *Copyright © 2013 IFSA.*

Keywords: Wireless sensor networks, Secure positioning, Spoofing attack, Distance verification, Algorithm.

1. Introduction

Wireless sensor networks, by its unique merits, has wide application potential in industry, agriculture and military domain. The precise location of sensor node is the premise of guaranteeing the effectiveness and validity of WSNS in its application and nodes positioning technology is a key technology of wireless sensor networks. For its inherent characteristics, such as limitation of the resources, insecurity and openness of the deployment environment, mechanism of location for wireless sensor networks has security problems [1-7].

This paper based on distance validation against deception attack localization algorithm FaltBdv (Forge Attack-resistant Localization Technology Based on distance verification). The secure localization algorithm respectively with the signal power loss and propagation time calculating the distance between nodes, using the distance of the consistency of eliminating positioning reference concentration of abnormal nodes, then the use of LS (Least Squares Estimate) – Newton positioning algorithm for estimating the unknown node coordinate. Because power measurement and the measurement of the propagation time can be done at the same time, so the FaltBdv algorithm can at no additional time cost at the same time, effectively detect the attack nodes.

2. Detection Principle

Analysis of node location process and principle of available node distance consistency principle, which assumes that the nodes in the wireless sensor network is stationary, then the node between the objective distance is constant, is also in the absence of attacks, through the signal transmission time by calculating the distance between the nodes should be equal to the received power calculation the distance (in considering error exists, the difference between the two distance should be less than a smaller value).

If want to achieve the purpose of malicious node attacks, must change with time to transmit signals and power loss of two parameters. Therefore, you can design a special positioning mechanism, the malicious nodes can change two parameters, and then through the surveillance by the time of calculating distance and power loss are consistency of the distance to judge whether the presence of ARP spoofing attack. Undertake surveillance detection tasks and nodes is called the detecting node, may be unknown nodes can also be the beacon node.

a) Distance between two nodes and signal propagation time relationship.

Signal propagation time and the distance between the nodes is proportional, meet

$$d_t = (T_1 - T_0) * V \tag{1}$$

type, based on the signal propagation time between the nodes is calculated distance, is the signal propagation speed, the unknown node transmits a request for location signal moments, this signals arrive at the beacon nodes when the. Beacon node will be written reply unknown node location request packet. If the beacon node capture, an attacker can change the value to change the node between the measured distance value can be increased, which can also be reduced. In order to reduce the possibility of malicious node attacks, this paper uses signal feedback time calculating the distance between the nodes, as shown in formula (2):

$$d_t = \frac{\left[(T_3 - T_0) - (T_2 - T_1)\right] * V}{2} \tag{2}$$

Unknown nodes in sending position request packet, the packet in time to reach beacon node, beacon node in a reply to the request for reply packet, in time to reach the unknown node. As the beacon node processing packet time, processor speed, value is approximately equal to the constant. As can be seen, the return time calculating the distance between nodes can reduce the possibility of malicious attack, where the attacker can extend the propagation time of a signal, is only to increase the distance between the nodes.

b) Distance between two nodes and the power loss of the relationship.

In the same transmission power, node receiving power and inversely proportional to the distance between nodes, content type (3):

$$P_{rcv} = c\frac{P_{tx}}{d_p^{\alpha}} \Leftrightarrow d_p = \sqrt[\alpha]{\frac{cP_{tx}}{P_{rcv}}} \tag{3}$$

Wherein, said by the power loss calculated distance, and constant. As the unknown node receives beacon node power, to write the packet transmit power, when the beacon node is the attacker capture, malicious nodes can be changed through the write data packet to the objective of the attack.

c) d_t and d_p relationship.

From the propagation time and the received power of the calculated distances between nodes in the ideal condition should be equal, i.e.

$$d_t = d_p \tag{4}$$

By the formula (2) and (3) to

$$\frac{\left[(T_3 - T_0) - (T_2 - T_1)\right] * V}{2} = \sqrt[\alpha]{\frac{cP_{tx}}{P_{rcv}}} \tag{5}$$

d) Detection basis.

The attacker in order to achieve the purpose of success, must also change the spread time of the signal and power loss, to make the change of the power of the distance change the volume of the cause Δd_p and the change of the time of the distance change the volume of the cause Δd_t meet

$$\Delta d_p = \Delta d_t \tag{6}$$

To RTOF ranging method, attacker only change the distance between nodes measurement by increasing spread time.

If malicious node intentionally delay Δt reply the positioning of the unknown nodes request, malicious node can change power consumption by the two ways.

Malicious node will make the reply to request packets P_{tx} increase, the actual launch power constant. Power change the volume Δd_p should meet

$$\Delta d_t = \sqrt[\alpha]{\frac{c(P_{tx} + \Delta p)}{P_{rcv}}} \quad \left(\Delta p \geq 0\right) \tag{7}$$

Malicious node don't change written reply packet's P_{tx}, reduce the actual transmission power, then, Δd_p should meet

$$\Delta d_t = \sqrt[\alpha]{\frac{cP_{tx}}{P_{rcv} - \Delta p}} \qquad (\Delta p \geq 0) \qquad (8)$$

We can know from (7) and (8), to malicious node, P_{rcv} and Δp are unknown, can't accurately get's solution. So, we can use the power loss and signal transmission time testing whether there are attacks.

3. FaltBdv Algorithm

FaltBdv algorithm's basic idea is based on such a fact, at WSN node location's process, spread by time and power loss the calculated the distance between the nodes in ideal condition should be equal, cheating on attack happened, malicious node can't change power and time caused the distance change the same amount.

Because wireless transmission of scattering characteristics, there is always some node in a malicious node of the communication area. As shown in Fig. 1, when unknown nodes S neighbor node to send positioning request information, malicious A to its launch deceive attack node. In a node A communication within the scope of the beacon nodes B_1 and B_3 and unknown nodes S and S_i will be listening to the wrong position parameter from A, the nodes can be as the test node to other nodes the authenticity of the test. So, can use these test nodes, through the test of the consistency of the distance to judge whether there are malicious attacks, recognition malicious node.

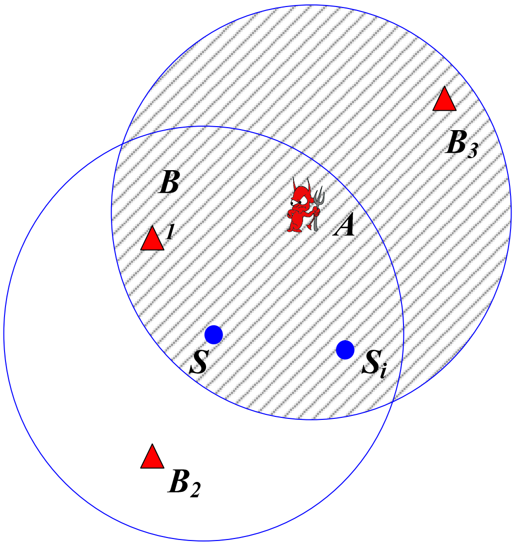

Fig. 1. An Illustration of Detection Nodes.

FaltBdv algorithm provisions of the beacon nodes reply positioning parameters packet format as shown in Fig. 2. Among them, (x, y) is the beacon node of the coordinates id_B, t_{rcv} and P_{rcv} are the beacon nodes to receive unknown nodes ids request information moment and receive power, t_{tx} and P_{tx} are the beacon nodes reply the time and send request power. Based on (2) and (3) can be calculated d_t and d_p respectively.

id_B	id_s	x	y	t_{rcv}	t_{tx}	P_{rcv}	P_{tx}

Fig. 2. Packet format of a Beacon message for FaltBdv.

As shown in Fig. 1 shows, unknown nodes to its neighbors sent S node location information request, node A, B_1, S and S_i are neighbors, the four nodes can write to each other. If A malicious node to S launch deceive attack, beacon nodes B_1 right, unknown nodes S and S_i can afford the testing tasks, called test node.

a) Unknown nodes S as a test node

- Node S received from node of A reply information and record receiving moment, measurement and receive power from A combination of positioning parameters are calculated d_t, d_p;
- If $|d_t - d_p| \leq \varepsilon \ (0 \leq \varepsilon)$, no attack, accept A by the positioning parameter, if $|d_t - d_p| > \varepsilon \ (0 \leq \varepsilon)$, then A for fraud against node;
- If in the B_i S communication within the range, the property 3-5, it is known that the node A and node distance between B_i d_{AB} must be less or equal to 2 R, R for beacon nodes communication radius. Node S validation i $d_{AB} \leq 2R$ is formed, if not set up, then A for fraud against node

b) The unknown node S_i as the detecting node

- Node S_i receives from node A reply information, recording the received data packet time and measuring the received power and calculating d_t and d_p;
- Validation of $|d_t - d_p| \leq \varepsilon \ (0 \leq \varepsilon)$ is established, if not established, then the A spoofing attack node.

c) Beacon node B_1 as the detecting node.

Beacon node coordinate position B_1 is known, its coordinates is (x_i, y_i), and the distance "d" between B_1 and the node A can be calculated by formula (9)

$$d=\sqrt{(x-x_i)^2+(y-y_i)^2}\,, \qquad (9)$$

where (x, y) is the node A location coordinates.

- Beacon node B_1 receives from node A information, recording the received data packet time and measuring the received power and calculating d_t and d_p;
- The data packets in a location parameter calculation of distance "d";
- Validation of $|d_t-d_p|\le\varepsilon\ (0\le\varepsilon)$, $|d-d_p|\le\varepsilon\ (0\le\varepsilon)$ and $|d_t-d|\le\varepsilon\ (0\le\varepsilon)$ is established, if not established, then the A spoofing attack node.

The detecting node once found cheating attack node, node id will store the attack, at the same time to its neighbor nodes releases exist attack warning.

4. Simulation Experiments and Results Analysis

a) Experimental parameters

The simulation experiment, in 100 unknown nodes in 10 randomly set of nodes as the detecting node, set the beacon nodes for sensor node. Maximum credible reference sets the number of elements is set to 4, between the nodes location using RSSI and RTOF combination method. The experiment mainly node average localization error, the success probability of detection as a performance index to evaluate the performance of algorithm. Each test scene runs 100 times and the statistical results of operation.

b) The effect of positioning algorithm.

The first application of FaltBdv security positioning algorithm to node layout scene simulation, the simulation results as shown in Fig. 3. Map (a) for node localization effect diagram, diagram (b) to the nodes of the original layout diagram, diagram (c) for positioning the effect chart and the original layout of the superimposed comparison chart. The experimental setting attack node number is 5. As can be seen from the graph, in the introduction of FaltBdv secure localization algorithm, positioning effect is improved obviously.

In the simulation scene randomly placed 5 spoofing attack nodes, nodes in the communication range and unknown nodes and beacon node is the same as, for 15 m. Fig. 4 shows no attack network node average localization error (curve 1), presence of attack in the case of network node location error (curve 2) and the use of FaltBdv algorithm node positioning error (curve 3). The results showed that: in the use of FaltBdv algorithm, node average position error of approximation in the attack position error, and the beacon node numbers, better approximation degree. This is because of the increasing number of beacon, involved in the detection of the number of nodes increases, thereby detecting the success rate increases, the unknown node by node pollution smaller attack.

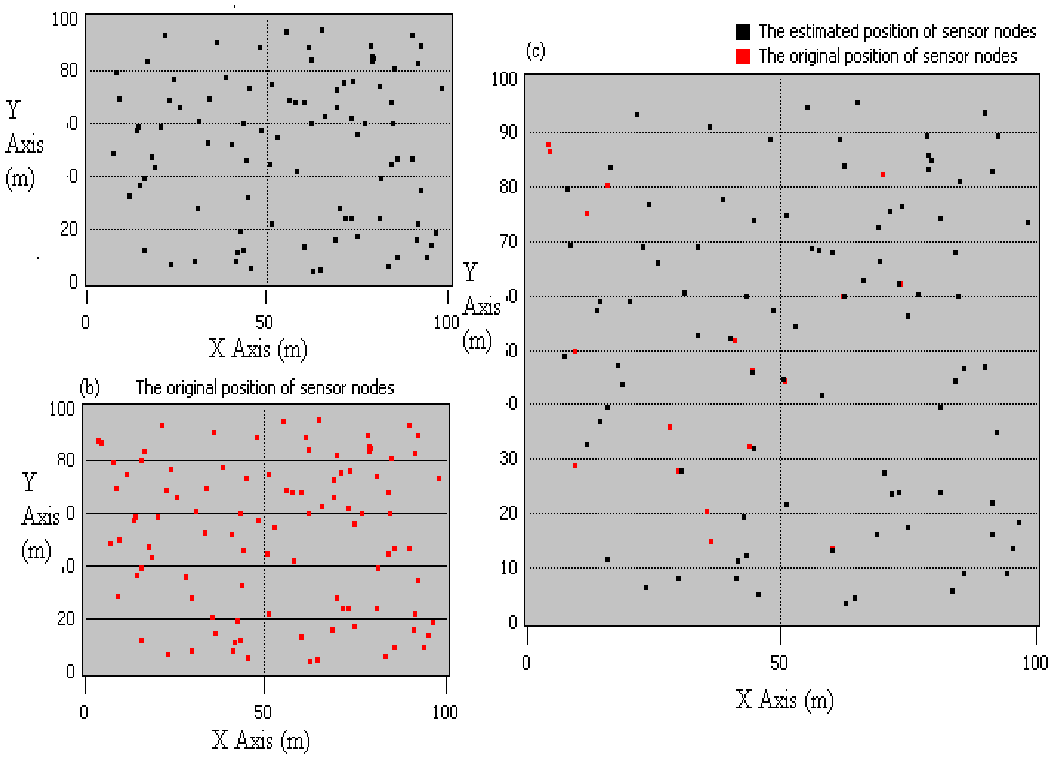

Fig. 3. Estimation Results of the Whole Network.

c) Number of nodes to attack algorithm.

Fig. 5 shows the attack number of nodes on node positioning accuracy, the experimental set-up, beacon node into 23 nodes, detection for 33. Curve 1, 2 and 3 respectively represent attack exists, network node average localization error, using FaltBra algorithm of node location error and using the FaltBdv algorithm node positioning errors with the number of nodes in the changing trend of attack.

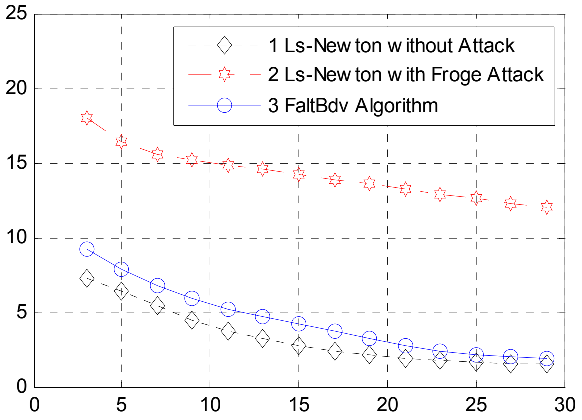

Fig. 4. Average Estimation Location Error varying the Number of Beacon Nodes.

Obviously, the use of FaltBdv algorithm of node localization error almost tends to be stable, i.e. to attack the number of nodes does not significantly affect the node location. And FaltBdv algorithm to attack a number of nodes is small FaltBra, the reason is that FaltBdv algorithm will not accord with standard nodes from the reference collection all removed, and FaltBra algorithm is the reference collection of residuals is different from the other node beacon out, if the reference set against the number of nodes is greater than or equal to good beacon node number, FaltBra algorithm will lose the ability to judge.

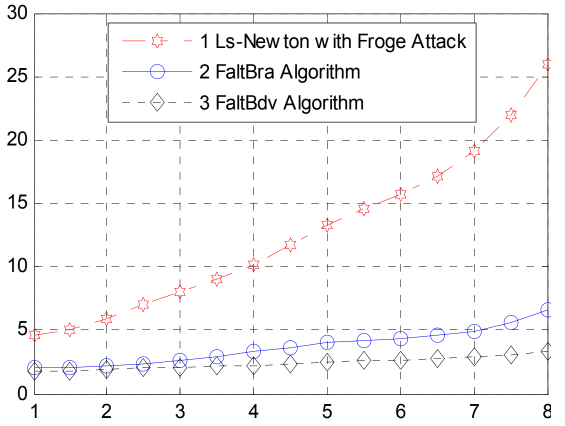

Fig. 5. Average Estimation Location Error varying the Number of Malicious Nodes.

d) The detection rate.

In the FaltBdv algorithm, in attack node communication within the scope of any benign nodes are able to act as the detecting node, and only need a sensor node can complete the detection task. If the beacon nodes and the unknown node deployment density respectively and, node communication radius, node receives beacon node probability obeys the Poisson distribution, all beacon nodes and unknown node can bear the detection task, so the detecting node density, the sensing region of the malicious nodes can receive a detection of the probability of the node type (available 10) says.

$$P\left(L_S=k\right)=\frac{\left(\left(\rho_B+\rho_S\right)\pi R^2\right)^k}{k!}e^{-\left(\rho_B+\rho_S\right)\pi R^2} \quad (10)$$

Type, says the malicious node receives the detection of node number.

By type (10) can be detected nodes to detect malicious node probability value

$$\begin{aligned}P\left(k\geq 1\right)&=1-P\left(k=0\right)\\&=1-e^{-\left(\rho_B+\rho_S\right)\pi R^2}\end{aligned} \quad (11)$$

Obviously, the malicious node communication radius and the detecting node deployment density affect the FaltBdv security positioning algorithm of detection probability of important factors. As a result of malicious nodes in the communication radius can not be changed, so can increase the detection of the density of nodes to improve the detection probability.

5. Conclusions

WSN secure node positioning algorithm to make the sensor node accurately, effectively to obtain the position information. FaltBdv algorithm for the analysis of malicious nodes to achieve spoofing attack way, using deceit attack nature, the signal propagation time and the power loss of consistency as attack detecting standard. Establish the process safety location algorithm based on the testing standards. The simulation results show that, the detection method can detect malicious nodes, thereby reducing the malicious attack effect, the unknown node from spoofing attack threat.

Acknowledgements

This work is supported by Scientific and Technological Innovation Programs of Higher Education Institutions in Shanxi under Grant No. 20121112 and the project of key discipline construction in Xinzhou Teachers University under Grant No. ZDXK201204.

References

[1]. Y. Shang, W. Ruml, Y. Zhang, et al., Localization from mere connectivity, in *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Annapolis, USA: ACM, 2009, pp. 201-212.

[2]. X. Ji, H. Zha, Sensor positioning in wireless ad-hoc sensor networks using multidimensional scaling, in *Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies*, Hong Kong, China: IEEE, 2011, pp. 2652-2661.

[3]. Y. Shang, W. Ruml, Y. Zhang, et al., Localization from connectivity in sensor networks, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 15, Issue 11, 2012, pp. 961-974.

[4]. J. A. Costa, N. Patwari, A. O. Hero, Distributed weighted-multidimensional scaling for node localization in sensor net-works, *ACM Transactions on Sensor Networks*, Vol. 2, Issue 1, 2008, pp. 39-64.

[5]. Hongyang Chen, Kaoru Sezaki, Ping Deng, Hing Cheung So, An improved DV-hop localization algorithm with reduced node location error for wireless sensor networks, *Communications and Computer Sciences*, Vol. E91-A, Issue 8, 2008, pp. 2232-2236.

[6]. Dю Niculescu, B. Nath, DV based positioning in Ad hoc networks, *Journal of Telecommunication Systems*, Vol. 31, Issue 4, 2012, pp. 267-280.

[7]. R. Nagpal, H. Shrobe, J. Bachrach, Organing a global coordinate system from local information on an ad hoc sensor network, in *Proceedings of the 8nd International Workshop on Information Processing in Sensor Networks (IPSN'03)*, California, USA, 2009.