DV-based Robust Localization against Wormhole Attacks in Wireless Sensor Networks

ANATHA KUMAR 1, SMT. K. KAVITHA 2, G. NAGESWARARAO 3

1AVANTHI'S ST.THERESSA COLLEGE OF ENGG, DEPT OF INFORMATION TECHNOLOGY, GARIVIDI, GARIVIDI, VIZIANAGARAM

2,3ADITYA INSTITUTE OF TECHNOLOGY AND MANAGEMENT, DEPT OF INFORMATION TECHNOLOGY, TEKKALI.

Abstract

Localization is a basic service and significant technology in wireless sensor networks (WSNs) while in the applications of WSNs, security has become an important issue. Secure localization has thus become a serious issue due to increasing security threats in wireless sensor networks. In this paper, we address the problem of making sensors in WSNs locate their positions in an environment in which there exists the threat of wormhole attacks. We propose a distance vector (DV)-based robust localization (DVRL) scheme which can fight against wormhole attacks in wireless sensors networks without increasing hardware complexity or incurring too much computational cost. In DVRL, sensors estimate the position relationship between each other by the distance vector (DV) and ensure the security of their localization by using an effective detection mechanism, which can enhance the robustness of the localization method. Experiment results show that the proposed scheme is capable of fighting against wormhole attacks while improving accuracy compared to the basic DV-Hop algorithm.

Keywords: Localization; Distance Vector; Wormhole Attack; Wireless Sensor Networks

1. Introduction

With the increasing functionality and decreasing cost of sensor nodes, wireless sensor networks (WSNs) have started to be used in applications. WSNs can be applied in military and industry due to the capability of sensor nodes in indoor and outdoor environments. Since the data collected by the sensors is usually accompanied by the sensor’s positions to make the data more meaningful, localization has become a significant issue in WSNs. Meanwhile, security has also become a critical issue for WSNs. Security is also required in localization. This is because when sensors are under attack, the accuracy of localization results could be reduced. Consequently, any localization algorithm should be capable of fighting against attacks in hostile environments.

Current localization algorithms can be divided into two categories: range-based algorithms and range-free algorithms with the difference being whether the distance between the nodes is determined through physical measurement. Range-based algorithms are able to achieve better accuracy and typical such algorithms include Ad Hoc localization algorithm (AHLos) [1] and RADAR [2]. Although accuracy could
be lower, range-free algorithms usually incur lower cost. Therefore, range-free localization algorithms are widely used and typical such algorithms include centroid algorithm [3] and Approximate Point-In-Triangulation Test (APIT) algorithm [4]. In recent years, some secure localization algorithms have also been proposed such as a series of secure localization algorithms proposed by Lazos [5-7], the SPINE algorithm proposed by Capkun [8] and the SLA algorithm proposed by Li [9]. DV-based Positioning [10] is a serious of distributed localization algorithms based on distance vector routing in which DV-Hop is a basic one. DV-Hop can provide approximate position for all nodes in a network where only a small fraction of nodes have self-positioning capability. However, DV-based algorithms are vulnerable to some attacks such as the wormhole attack. For some localization algorithms based on DV-Hop [11], the trust mechanism has been introduced to improve the security of localization.

In this paper, we propose a robust localization scheme based on distance vector called DV-based robust localization (DVRL) scheme that can achieve secure localization against wormhole attacks. We also perform some experiments to show that DVRL can locate the positions of sensors with improving accuracy in hostile environments.

The rest of this paper is organized as follows. In the next section, we analyze the wormhole attack model in DV-based localization. In Section 3, we present the DVRL scheme and describe some implementation details. In Section 4, we analyze the DVRL scheme to verify its performance. Finally, in Section 5, we conclude this paper in which we also describe our future work.

2. Wormhole Attack Model in DV-based Localization

2.1. Problem Statement

In this paper, we design secure localization to achieve the following goals: robustness against wormhole attacks; improving accuracy; acceptable computational cost and communication overhead.

In the discussion, we assume that the network consists of beacon nodes, sensor nodes and attackers. The beacon nodes are capable of positioning themselves while the sensor nodes need to locate their own positions. The DVRL is developed also with the following assumption:

1) All sensor and beacon nodes become static after deployment;
2) Beacon nodes are credible and would broadcast location information to any requesting sensor nodes;
3) Each node has a unique identifier $ID$ in the network;
4) Any two nodes are able to communicate to each other when they are within each other’s transmission range and signals won’t get lost due to collision or background noise.

2.2. Wormhole Attack Model for DV-Hop

DV-Hop is the most basic scheme in DV-based Positioning which has three non-overlapping stages [8]. In the first stage, each node in the network gets a hop-count to the beacon nodes. In the second stage, beacon nodes calculate the average size for one hop to other beacon nodes. In the third stage, sensor nodes estimate their positions by using trilateration after calculating their distances to the beacon nodes. Wormhole attack is a typical threat for in DV-Hop, which results in the packets being transmitted through longer paths. Hence, we analyze the secure issue of wormhole attacks in DV-Hop localization for WSNs.
Wormhole attack is usually implemented by two nodes in conspiracy to establish a wormhole link between the two attacking nodes. Attackers can reduce the hop counts easily through wormhole link to get the right of message propagation. Wormhole attacks are difficult to detect since they can be launched without compromising any sensor nodes. As shown in Fig. 1, the normal path between the two beacon nodes B1 and B2 is B1-S1-S2-S3-S4-S5-B2. But the two attackers W1 and W2 can make B1-S6-W1-W2-S7-B2 a shorter path through the wormhole link. In DV-Hop localization, the error in estimation of the hop count between two nodes can cause wrong hop count, thus a lower accuracy of localization as the result.

To achieve our goals, in DVRL, we introduce a wormhole detection mechanism into DV-Hop to equip the network with the capability of detecting wormhole attacks and segregating the attackers from the sensor nodes before the stage of position estimation to ensure the accuracy of localization even in the presence of wormhole attackers.

3. The DV-based Robust Localization Scheme

DVRL deals with the problem of wormhole attacks in localization for WSNs, which helps improve the accuracy of localization and make the localization system more secure. Main steps of the algorithm are described as follows.

3.1. Routing Initialization

Beacon nodes broadcast messages that include the positions of themselves and the initial hop-count value of 0. A node that receives such a message would learn the position of a beacon node, write its own ID into the message and send it to its neighbors with an increment of the hop-count value. Each beacon node can thus get the positions of other beacon nodes and the shortest distance in hops between itself and the other beacon nodes with this method. Then, each beacon node calculates the average size of one hop using Equation (1) in which $c_i$ denotes the average hop size of beacon node $i$ to other beacon nodes and $h_i$ denotes the hop-count of beacon node $i$ to other beacon nodes. In the equation, we assume that the two-dimensional coordinates of beacon node $i$ is $(X_i, Y_i)$, and all the beacon nodes around $i$ are denoted by $j$ with their coordinates being denoted as $(X_j, Y_j)$.

$$c_i = \frac{\sum_{j \neq i} \sqrt{(X_i - X_j)^2 + (Y_i - Y_j)^2}}{n-1},$$

(1)
3.2. Detection of Attacks

Wormhole attacks are mainly implemented by packet encapsulation or proprietary channel. In the first approach, the attackers envelop the routing packets to make hop-counter fail to work normally while in the second approach, the attackers transfer routing packets through a proprietary channel with high bandwidth. Based on the different approaches, we classify wormhole attackers into two types: hidden identity and un-hidden identity.

- Hidden identity attacker: The normal sensor node in the routing path adds its own ID and increments the hop-count. However, the attacker doesn’t add itself into the packet, nor does it change the hop-count.
- Un-hidden identity attacker: The attacker receives and sends packet normally, but makes the hop-count smaller by getting the packet going through a proprietary channel.

The goal of our scheme is to detect both types of wormhole attackers. Main steps of the detection are described as follows:

1. Each node in the routing path checks whether the previous node has added its ID into the packet. The previous node will be labeled as an attacker unless it adds its ID into the packet and increments the hop-count. If the node determines that its previous node is an attacker, it will broadcast an alarm message to remove the attacker. Un-hidden identity attackers will be detected in this way.

2. If every node in the routing path detects and thus ensures that its previous node receives and sends routing packet normally, a whole routing path will be constructed between beacon nodes. Beacon nodes will get the minimum hop-count between each other and estimate the average hop size using Equation (1). A beacon node will then compare the average hop size $c$ with transmission radius $R$. If $c > R$, wormhole attackers exist in the path.

3. After the presence of wormhole attackers is detected, the network should detect the attacking nodes and remove them. The network compares the actual distance $d$ between each pair of nodes with transmission radius $R$ using Equation (2) in which $d$ denotes the actual transmission distance of signals, $v$ denotes the propagation velocities of the signals and $l$ denotes the propagation time between the nodes. If $d > R$, the nodes at both ends of this distance are a pair of wormhole attackers. The actual transmission distance between the nodes can also be estimated by other measurement method [12, 13].

\[ d = v \cdot l \]  

3.3. Position Estimation

Sensor nodes estimate their positions through maximum likelihood estimation [14] after getting the positions around beacon nodes and the distance between each other. Suppose the number of beacon nodes around an sensor node is $n$ and their coordinates are $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$, respectively, and the distance between sensor node $U(x, y)$ and the beacon nodes are $d_1, d_2, \ldots, d_n$, respectively. Using Equation (3), the sensor node’s position can be derived.

\[ (x-x_i)^2 +(y-y_i)^2 = d_i^2, i = 1,2,\ldots,n \]  

In addition, $n$ distance equations about $U$ and $n$ beacon nodes are listed with each of the first $n-1$ equations minus the last equation with the results shown in Equation (4).
\[4 \cdot x^2 - 20_1 \cdot x_1 + y_1^2 - y_2^2 - 20_1 \cdot y_2 \cdot y = d_1 \cdot \Delta d \]

\[d_1 - \Delta d \cdot 2(V_1 \cdot x_1) x + y_1^2 \cdot y_1 - 2(y_2 - 1 \cdot y_2) = d_1 \cdot \Delta\%\]

\[U(x, y) \text{ can then be calculated using Equations (5).} \]

\[U = \mathbf{A}^{-1} \mathbf{b} \]

The matrices in the Equations (5) can be described as (6) - (8):

\[
\mathbf{A} = \begin{bmatrix}
1 & y - y_n \\
\sqrt{\mathbf{W} - 1} & y - y_n \\
\mathbf{A} & \mathbf{A}
\end{bmatrix}
\]

\[4 - \mathbf{M} \cdot \mathbf{A} - 4^+ \]

\[
\begin{bmatrix}
\mathbf{A} \\
\mathbf{A} \\
\mathbf{A}
\end{bmatrix}
\]

\[
\begin{bmatrix}
\mathbf{A} \\
\mathbf{A} \\
\mathbf{A}
\end{bmatrix}
\]

And the solution to Equation (5) is Equation (9).

\[U = (\mathbf{A}^T \mathbf{A})^{-1} \mathbf{A}^T \mathbf{b} \]

4. Experiments

We have done some experiments to analyze the performance of DVRL in an environment in which there exists the threat of wormhole attacks as described below.

1. The network configuration of the experiment is set up as follows: 50 sensor nodes, 10 beacon nodes and 6 attacking nodes are deployed randomly in a 40 X 60 m² area. The transmission radius of each beacon and sensor node is 10 m.

We compare the performance of DVRL to that of DV-Hop localization algorithm in the presence of wormhole attacks. We show the improvement on the average location error when DVRL is used. The localization error is calculated using Equation (10) and the average localization error of all the nodes is calculated using Equation (11) in which \((x_t, y_t)\) denotes the measurement coordinates of sensor node \(i\) while \((x'_t, y'_t)\) denotes its actual coordinates, \(A^*\) denotes the number of sensor nodes and \(R\) denotes the transmission radius of sensor nodes. We repeat the two localization algorithms 20 times in the network. The results of the experiments are shown in Fig. 2.

\[e_i \left[ \frac{(x_t - x'_t)^2 + (y_t - y'_t)^2}{R} \right] \]

\[Y e_i / N \]
2. For performance evaluation, we randomly distribute 50 sensor nodes within an area, which generates a topology as shown in Fig. 3 in which we randomly select 6 wormhole attackers. Then, we compute the average location errors for different numbers of beacon nodes. Fig. 4 shows the average localization errors of sensor nodes in the presence of wormhole attackers with varying numbers of beacon nodes.

3. For performance evaluation about resistance against wormhole attackers, we randomly distribute 100 sensor nodes within an area, which generates a topology as shown in Fig. 5 in which we randomly select 10 beacon nodes. Then, we compute the average location errors for different numbers of wormhole attackers.
Fig. 6 shows the average localization errors of sensor nodes in the presence of varying numbers of wormhole attackers.

![Fig. 5 Topology of the Sensor Network](image)

![Fig. 6 Localization Errors for Varying Number of Wormhole Attackers](image)

### 5. Conclusion

In this paper, we described the wormhole attack which is a common attack for localization based on distance vector routing and analyzed the characteristics of wormhole attacks in DV-based localization. We then proposed a secure localization scheme called DVRL to detect and fight against wormhole attacks in WSNs that can improve localization accuracy in the presence of wormhole attacks. We described how DVRL detects the attackers in the network to get more accurate positions of sensor nodes. Our experiments showed that (1) DVRL can decrease the average localization error of sensor nodes in the presence of wormhole attacks, (2) DVRL is not very sensitive to the density of beacon nodes, and (3) DVRL can get satisfactory localization accuracy in the presence of varying numbers of wormhole attackers. Overall, DVRL can achieve higher localization accuracy in the presence of wormhole attacks than the basic DV-based positioning algorithm.

In the future, we will extend our secure localization scheme to improve the security of localization in the case of other kinds of attacks without incurring too much computational overhead and communication cost. Another effort will be to improve the reliability of positioning system through constructing trust.
relationships between the nodes in the network. We will also consider secure localization for WSNs with mobile sensors.

References


Smt. K. Kavitha. Designation: Assistant Professor Qualification: M.Tech Teaching Exp. in Years: 7, Aditya Institute of Technology and Management.

G. Nageswara Rao, M.Tech(CST),MISTE,MCSI, ( Ph.D) - Head of the Department Presently the head of the department of Information Technology. He has worked for more than 12 years in various capacities in reputed colleges. M.Tech and doing Ph.D. participated in International conference on bioinformatics Diabetics mellitus(ICBDM2006) and got best paper award on "Drug development and design". Also has very good command over computer related topics. Aditya Institute of Technology and Management.

ANATHA KUMAR is currently pursuing his M.TECH course as INFORMATION TECHNOLOGY from JNTUK. Aditya Institute of Technology and Management, TEKKALI.