Label-Based DV-Hop Localization Against Wormhole Attacks in Wireless Sensor Networks

Junfeng Wu[†,§], Honglong Chen[‡], Wei Lou[‡], Zhibo Wang[†], and Zhi Wang[†]

[†]State Key Lab of Industrial Control Technology, Zhejiang University, China
[‡]Dept. of Computing, The Hong Kong Polytechnic University, Hong Kong
[§]Dept. of Electronic and Computer Engineering, The Hong Kong University of Science and Technology, Hong Kong
jfwu@ust.hk, {cshlchen, csweilou}@comp.polyu.edu.hk, {zbwang, wangzhi}@iipc.zju.edu.cn

Abstract

Node localization becomes an important issue in the wireless sensor network as its broad applications in environment monitoring, emergency rescue and battlefield surveillance, etc. Basically, the DV-Hop localization mechanism can work well with the assistance of beacon nodes that have the capability of self-positioning. However, if the network is invaded by a wormhole attack, the attacker can tunnel the packets via the wormhole link to cause severe impacts on the DV-Hop localization process. The distance-vector propagation phase during the DV-Hop localization even aggravates the positioning result, compared to the localization schemes without wormhole attacks. In this paper, we analyze the impacts of wormhole attack on DV-Hop localization scheme. Based on the basic DV-Hop localization process, we propose a label-based secure localization scheme to defend against the wormhole attack. Simulation results demonstrate that our proposed secure localization scheme is capable of detecting the wormhole attack and resisting its adverse impacts with a high probability.

Keywords: DV-Hop localization; wireless sensor networks; wormhole attack.

I. Introduction

With the advantages of low cost, large scale, densely distributed deployment, self-configuration, etc., wireless sensor networks (WSNs) have been applied in many fields to monitor and control the physical world [1]. In WSNs, sensed data make no sense without the nodes' position information. Hence, nodes are required to locate themselves in many WSN applications, such as environment monitoring, emergency rescue, and battlefield surveillance, to name a few.

Many protocols and algorithms are designed to solve the node's positioning problem, which are categorized into two categories: range-based and range-free [2]. Range-based protocols calculate the location using the point-to-point distance (or angle) estimates. Though range-based schemes are able to obtain relatively accurate results, they can be applied only when nodes are equipped with sophisticated hardware. Range-free solutions do not rely on the availability of range (or angle) estimates, so they need no expensive hardware. Considering that the hardware requirement of range-based solutions is inappropriate for resource-constrained WSNs, researchers are pursuing range-free localization techniques as a cost-effective alternative [2].

The DV-Hop [3] localization, as a range-free positioning algorithm, is applied with the assumption of isotropic networks. First, beacons, as location-known nodes, flood their positions through the network so that all nodes in the network can obtain the hop-counts to each of the beacons. Then each beacon, after receiving the position information from other beacons, calculates the average distance per hop, which is also broadcasted among its neighborhood, by averaging the distances to all other beacons over the hop-counts. Sensors, being location unknown, estimate their locations to corresponding beacons, based on the received beacons' locations, average distance per hop and hop-counts.

As sensor networks usually work in a hostile environ-

978-0-7695-4134-1/10 $26.00 ©2010 IEEE.

ment, they are vulnerable to various malicious attacks. The wormhole attack, as a typical external attack, can be easily launched by two colluding attackers without the system's authorization. When such attack is initiated, one attacker tunnels its received packets to another attacker, thus, packets can be delivered through a shorter path. The wormhole attack can deteriorate the DV-Hop localization dramatically. It not only reduces the hop-counts to all the beacons in the network, but also contaminates the average distance per hop. As a result, the location estimate will be far away from precision.

In this paper, we focus on defending against the wormhole attack in the DV-Hop localization process, i.e., overcoming the impacts of the wormhole attack on the DV-Hop localization. We propose a label-based secure localization scheme which is wormhole attack resistant based on the DV-Hop localization process. The main idea of our scheme is to generate a pseudo neighbor list for each beacon node, use all pseudo neighbor lists received from neighboring beacon nodes to classify all attacked nodes into different groups, and then label all neighboring nodes (including beacons and sensors). According to the labels of neighboring nodes, each node prohibits the communications with its pseudo neighbors, which are attacked by the wormhole attack.

The main contributions of this paper include: (1) We analyze the impact of the wormhole attack on the DV-Hop localization process; (2) We propose a wormhole attack resistant approach that can remove the packets delivered through the wormhole link to achieve secure localization; (3) We conduct the simulation to validate the effectiveness of our proposed secure localization scheme.

The rest of this paper is organized as follows. Section II reviews the related work on the secure localization. In Section III, we describe the network model, the DV-Hop localization approach, and the wormhole attack model and its impacts on the DV-Hop localization process. Section IV describes our proposed label-based secure localization in details. In Section V, we present the performance evaluation. Finally, Section V concludes this paper and outlines our future work.

II. Related Work

The secure localization [4] has been well studied in the recent decade. We first review the range-based secure localization systems and range-free secure localization systems respectively, and then discuss the schemes against wormhole attack.

Liu et al. [5] propose two secure localization schemes against the compromise attack which adopt the concept of consistency. SPINE [6] enables verifiable multilateration and verification of positions of mobile devices for secure computation in the presence of attackers. In [7], a secure localization scheme is presented to make the location estimation of the sensor secure, by transmitting nonces at different power levels from beacon nodes. The secure localization approach in [8] relies on a set of covert base stations, whose positions are unknown to the attacker during the localization. The covert base stations listen to the beacon signals sent by the nodes and compute the nodes' positions, then check the validity of the nodes.

Lazos et al. [9] propose a robust positioning system called ROPE that allows sensors to determine their locations without centralized computation. In addition, ROPE provides a location verification mechanism that verifies the location claims of the sensors before data collection. In [10], a suit of techniques are introduced to detect malicious beacons that supply incorrect information to the sensor nodes. These techniques include a method to detect malicious beacon signals and techniques to detect replayed beacon signals, identify malicious beacons, avoid false detections and revoke malicious beacons. In [11], robust statistical methods are proposed, including triangulation and RF-based fingerprinting, to make localization attack-tolerant.

For the wormhole attack detection, Hu at el. [12] present a general mechanism called packet leashes based on the notions of geographical and temporal leashes. Wang and Bhargava [13] propose to detect the wormhole by visualizing the anomalies introduced by the attack, which needs all the distance messages between each pair of nodes. To make it suitable for large scale network, Wang and Lu [14] propose an interactive wormhole detection which selects some feature points to reduce the overlapping issue and preserve major topology features. Xu at el. [15] propose a wormhole attack detection algorithm using a hop counting technique as a probe procedure, reconstructing a local map for each node and using a "diameter" feature to detect abnormalities caused by wormholes. In [16], the wormhole attack detection scheme adopts the maximum number of independent neighbors of two non-neighbor nodes.

As the localization process will be greatly deteriorated by the wormhole attack, some secure localization approaches have been proposed. SeRLoc [17] uses directional antennas to detect the wormhole attack based on the sector uniqueness property and communication range violation property. The secure localization can be obtained after detecting the attacked locators. HiRLoc [18] further improves SeRLoc by utilizing antenna rotations and multiple transmission power levels to provide richer information for higher localization resolution. Chen et al. [19], [20] propose a secure localization scheme using the distance consistency to defend against the wormhole attack. In [21], inter-node messaging properties are used to detect the abnormality of the network when the wormhole attack

exists. A so-called conflicting set is built to detect the wormhole attack and to further resist against the impact of the attack on the localization. However, all these approaches [19], [20], [21] are proposed to deal with the range-based localization. In this paper, we address the security issue of the wormhole attack upon the range-free DV-Hop-based localization process, which is so far never been discussed in literature.

III. Problem Statement

In this section, we describe the network model, the DV-Hop localization approach, and the wormhole attack model and its impacts on the DV-Hop localization process.

A. Network Model

We assume that there are three types of nodes in a WSN: beacons, sensors, and attackers. Beacons are location-fixed nodes with their positions known in advance (by GPS device or manual configuration). The sensors, either moving around or staying at a place, are position-unknown nodes that need to locate themselves with the assistance of beacons. The attackers exist in a pair and collude with each other to launch a wormhole attack, which can invade the WSN without any system's authorization. We assume that all the nodes have an identical transmission range R and each pair of nodes whose distance is within the range R can communicate with each other with no packet loss.

We also assume that sensors and beacons are deployed independently, following the Poisson distribution with node densities ρ_b and ρ_s, respectively. That is, the probability of k beacons in an area D_b and that of k sensors in an area D_s are given as $P(N_b = k) = \frac{(D_b\rho_b)^k}{k!}e^{-D_b\rho_b}$ and $P(N_s = k) = \frac{(D_s\rho_s)^k}{k!}e^{-D_s\rho_s}$, respectively.

B. DV-Hop Localization Approach

The DV-Hop localization approach has three phases [3]:

- In the first phase, a typical distance vector routing mechanism is employed. Beacons flood their location information throughout the network with the initial hop-count of 0. Each node that relays the message increases the hop-count by one. After the flooding procedure, every node can obtain the minimum hop-count to each beacon.
- In the second phase, each beacon, after obtaining the position and hop-count information to all other beacons, estimates the average distance per hop. Beacon *i* calculates the average distance per hop, called as hop-size HS, using the formula $HS_i = \frac{\sum_{j\neq i}\sqrt{(x_i-x_j)^2+(y_i-y_j)^2}}{\sum h_j}$, where (x_i, y_i) and (x_j, y_j) are the coordinates of beacons *i* and *j* respectively, and h_j is the hop-count value from beacon *i* to beacon *j*. Once calculated, HS_i will also be flooded to the sensors near to beacon *i*.
- In the last phase, before conducting the self-localization, each sensor estimates the distance to each beacon based on its hop-count and the hop-size to this beacon. Sensor *k* can get the distance d_{kj} (distance from sensor *k* to beacon *j*) using $d_{kj} = h_j \times HS_j$. After obtaining all the distance information, each sensor conducts the *triangulation* or *maximum likelihood estimation* [22] to estimate its own location.

Note that the DV-Hop localization does not need any sophisticated hardware for the distance measurement, and thus, it is free from range measurement errors.

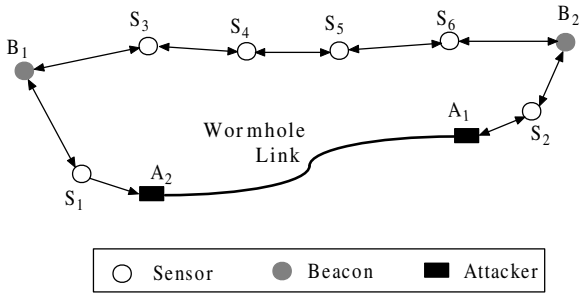

Fig. 1. The impact of wormhole attack on DV-Hop localization.

C. Wormhole Attack Model and Its Impacts on DV-Hop Localization

In this paper, we consider an adversarial environment where the localization procedure of sensors is attacked by a wormhole attack. During the wormhole attack, when one attacker receives packets at one point of the network, it forwards the packets through the wormhole link to the other attacker, which retransmits them at the other point of the network. We assume that the wormhole link is bi-directional and symmetrical so that the packets could be transmitted via either direction. Considering that if the length of the wormhole link is less than R, both attackers are within each other's transmission range such that the packets transmitted by one attacker can be received and retransmitted by the other attacker, resulting in endless packet transmission loop. To exclude this exceptional case, we simply assume that the length of the wormhole link is larger than R.

The wormhole attack can greatly deteriorate the DV-Hop localization procedure. As shown in Fig. 1, two attackers A_1 and A_2 collude to launch a wormhole attack in

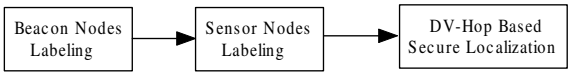

Fig. 2. The flowchart of the label-based DV-Hop localization scheme.

the network. In the first phase of the DV-Hop localization, beacons B_1 and B_2 initiate the flooding in the network so that other nodes can obtain the hop-counts to these beacons. For instance, the original minimum hop-count to beacon B_2 for sensor $S1$ is 6 ($B_2 \rightarrow S_6 \rightarrow S_5 \rightarrow S_4 \rightarrow S_3 \rightarrow B_1 \rightarrow S_1$). However, the flooding message from beacon B_2 would be received by S_2, then relayed by the wormhole link to S_1. Consequently, S_1 will consider the minimum hop-count to B_2 as 2, which is less than the real value 6. The wormhole attack can also affect the second phase of the DV-Hop localization when the beacons calculate the hop-size. As shown in Fig. 1, the original minimum hop-count from B_1 to B_2 is 5, B_1 will calculate the hop-size as $\frac{\sqrt{(x_1-x_2)^2+(y_1-y_2)^2}}{5}$, where (x_1, y_1) and(x_2, y_2) are the coordinates of beacons B_1 and B_2. However, as the existence of the wormhole attack, B_1 will get a minimum hop-count to B_2 as 3, the hop-size calculated by B_1 will be $\frac{\sqrt{(x_1-x_2)^2+(y_1-y_2)^2}}{3}$, which is larger than the real value. Therefore, the wormhole attack can disturb the first two phases of the DV-Hop localization. In the first phase, a sensor may obtain a smaller hop-counts to beacons. In the second phase, a beacon may calculate an incorrect hop-size, which is delivered to its neighboring sensors. Finally, each sensor may use incorrect hop-counts and hop-size to estimate the distances to all the beacons for the self-localization.

IV. Label-Based DV-Hop Localization

In this section, we describe our proposed wormhole attack resistant localization scheme, called label-based DV-Hop localization. The label-based DV-Hop localization scheme includes three phases, beacon nodes labeling, sensor nodes labeling, and DV-Hop-based secure localization. The flowchart of the label-based DV-Hop localization scheme is shown in Fig. 2. Firstly, the beacon nodes are differentiated and labeled according to their geographic relationship under a wormhole attack. The sensor nodes are further differentiated and labeled by using the labeling results of neighboring beacon nodes. After eliminating the illegal connections among the labeled neighboring nodes which are contaminated by the wormhole attack, the DV-Hop localization procedure can be successfully conducted.

To describe the label-based DV-Hop localization scheme more clearly, we provide the following definitions,

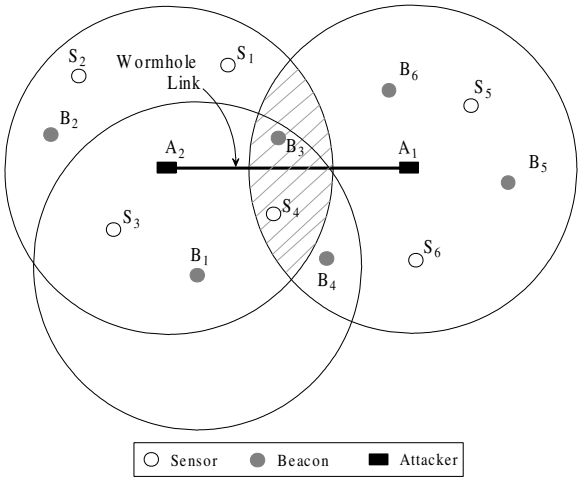

Fig. 3. The wormhole attack in a WSN.

some of which are borrowed from our previous work [21]:

Definition 1. *Duplex Wormhole Attack* : A node is under a duplex wormhole attack if it lies in the common transmission area of the two attackers.

Definition 2. *Simplex Wormhole Attack*: A node is under a simplex wormhole attack if it lies only in the transmission range of either one attacker but not in the common transmission area of the two attackers.

Definition 3. *Pseudo Neighbor*: A node is a pseudo neighbor if it can be communicated with via the wormhole link.

For the network shown in Fig. 3, node S_4 is under the duplex wormhole attack, node S_3 is under the simplex wormhole attack. Node B_6 is a pseudo neighbor of node B_1.

To ease the description of our proposed scheme, we also define $D_R(u)$ as a disk with radius R and center u; $L_N(i)$ and $L_P(i)$ are defined as the neighbor list and pseudo neighbor list of node i, respectively.

A. Beacon Nodes Labeling

Since nodes in the network, including both beacons and sensors, periodically broadcast *Hello* messages to its neighbors, each node can build a neighbor list after receiving the *Hello* messages from its neighbors. The *Hello* message include the node's type (i.e., beacon or sensor), identification, and coordinate if its type is "beacon". When building the neighbor lists, the beacon nodes may observe some abnormalities due to the existence of a wormhole attack. By examining these abnormalities, the beacon nodes can be classified and labeled into three categories: beacon nodes under the duplex wormhole attack, beacon nodes under the simplex wormhole attack, and beacon nodes without the wormhole attack. As shown in Fig. 3,

beacon nodes in the region $D_R(A_1) \cap D_R(A_2)$ are under the duplex wormhole attack, beacon nodes in the regions $D_R(A_1) \backslash D_R(A_2)$ and $D_R(A_2) \backslash D_R(A_1)$ are under the simplex wormhole attack, and beacon nodes outside the region $D_R(A_1) \cup D_R(A_2)$ are without the wormhole attack. The classification of the beacon nodes is according to the following three properties:

- **Self-exclusion property**: A node normally cannot hear a message sent from itself in a loop-free path.
  For each beacon node under the duplex wormhole attack (i.e., the beacon node lies in the region $D_R(A_1) \cap D_R(A_2)$ as shown in Fig. 3), the *Hello* message it sends will be relayed by attacker A_1 through wormhole link to attacker A_2 and then received by itself; similarly, the message will also be transmitted from A_2 to A_1 via wormhole link and then received by itself. Therefore, the beacons under the duplex wormhole attack can be identified using the self-exclusion property.
  Beacon Labeling Scheme BL1: Every beacon node checks whether it violates the self-exclusion property when building its neighbor list. The beacon node which violates the self-exclusion property can determine that it is under the duplex wormhole attack.
- **Packet uniqueness property**: A node normally cannot receive more than one copy of the same packet from any one of its neighbors.
  As shown in Fig. 3, beacon node B_4 lies in the common transmission region of attacker A_1 and beacon B_1, i.e., $D_R(A_1) \cap D_R(B_1)$. B_1 can receive *Hello* message from B_4 twice: one directly from B_2 and the other from A_2 (A_1 relays the message via the wormhole link to A_2 after receiving it from B_4). Therefore, if a beacon node receives the same message more than once from a neighbor node, it is under a wormhole attack.
  Beacon Labeling Scheme BL2: Every beacon node checks whether it violates the packet uniqueness property. If it does, i.e., it receives more than one copy of the same packet from one of its neighbors, it can determine that it is under a wormhole attack (either a duplex or simplex wormhole attack).
- **Transmission constraint property**: A node normally cannot communicate with nodes outside its transmission range.
  As shown in Fig. 3, beacon node B_5 lies outside the transmission region of beacon node B_1. However, the *Hello* message transmitted by B_5 can be received by attacker A_1, after that A_1 will relay it through the wormhole link to A_2 which will further relay it to B_1. When receiving the *Hello* message from B_5, B_1 can calculate the distance between them as the coordinate of B_5 is included in this *Hello* message. B_1 can observe that it receives a message from a node which is outside its transmission range. Thus, it can determine that it is under a wormhole attack.
  Beacon Labeling Scheme BL3: Every beacon node checks whether it violates the transmission constraint property when building its neighbor list. If the transmission constraint property is broken, it determines that it is under a wormhole attack.

The basic beacon labeling algorithm uses the above three schemes to classify the beacons, which is shown in Algorithm 1: Every node periodically broadcasts a *Hello* message. It also receives the *Hello* messages from its neighboring nodes to build its neighbor list. Each beacon node initially labels itself with 'N'. It further classifies itself using the beacon labeling schemes BL1, BL2 and BL3. If the beacon node detects that it violates the self-exclusion property using the scheme BL1, it labels itself with 'D' to indicate that it is under the duplex wormhole attack. Otherwise, if the beacon node detects that it is under the simplex wormhole attack using the schemes BL2 or BL3, it labels itself with 'S' to indicate that it is under the simplex wormhole attack. Note that for those beacon nodes that do not violate any property, their labels will be kept with 'N's to indicate that they are without the wormhole attack.

Algorithm 1 Basic Beacon Node Labeling

1: Each node B_i periodically broadcasts a *Hello* message to its neighbors and receives *Hello* messages to build its neighbor list.
2: Each beacon node is initially labeled with 'N'.
3: **if** B_i detects the duplex wormhole attack using scheme BL1 **then**
4: B_i is labeled with 'D'.
5: **end if**
6: **if** B_i detects the simplex wormhole attack using schemes BL2 and BL3 **then**
7: B_i is labeled with 'S'.
8: **end if**

After all beacon nodes are classified, we have the following theorems:

Theorem 1. Given a network under the wormhole attack, any beacon node under the simplex wormhole attack can detect all its pseudo neighboring beacons.

Proof: For any beacon node under the simplex wormhole attack, it lies in $(D_R(A_1) \setminus D_R(A_2)) \cup (D_R(A_2) \setminus D_R(A_1))$. Without loss of generality, we take beacon node B_1, which lies in $D_R(A_2) \setminus D_R(A_1)$ as shown in Fig. 3, for discussion. All the pseudo neighboring beacons of B_1 are located in $D_R(A_1)$, which can be grouped into two groups:

Group 1: The pseudo neighboring beacons of B_1 lie in $D_R(A_1) \cap D_R(B_1)$ (e.g., B_3 and B_4 in Fig. 3). As the *Hello* messages of these pseudo neighboring beacons can arrive at B_1 twice, one directly received by B_1, the other one relayed by the wormhole attack and then received by B_1, B_1 can identify all these pseudo neighboring beacons using the beacon labeling scheme BL2.

Group 2: The pseudo neighboring beacons of B_1 lie in $D_R(A_1) \setminus D_R(B_1)$ (e.g., B_5 and B_6 in Fig. 3). For these beacons, the *Hello* messages they send can be relayed by the wormhole attack and received by B_1. Therefore, B_1 can also identify all these pseudo neighboring beacons using the beacon labeling scheme BL3.

Therefore, any beacon node under the simplex wormhole attack can detect all its pseudo neighboring beacons. ■

Theorem 2. Given a network under the wormhole attack, two beacon nodes under the simplex wormhole attack lie in the transmission range of the same attacker if and only if their pseudo neighboring beacon lists are identical.

Proof: Necessary condition: For any two beacon nodes under the simplex wormhole attack that are attacked by the same attacker, without loss of generality, we take the beacons that lie in $D_R(A_2)$ (e.g., B_1 and B_2 as shown in Fig. 3) for discussion. From Theorem 1, we can see that each of such beacon nodes can identify all its pseudo neighboring beacons, which lie in $D_R(A_1)$. Therefore, their pseudo neighboring beacon lists, which include all beacons within $D_R(A_1)$, are identical.

Sufficient condition: For any two beacon nodes under the simplex wormhole attack, the possible scenarios are (1) both beacon nodes lie in $D_R(A_1)$, (2) both beacon nodes lie in $D_R(A_2)$, and (3) one beacon node lies in $D_R(A_1)$ and the other one lies in $D_R(A_2)$. We now proof by contradiction that if these two beacon nodes have the identical pseudo neighboring beacon list, scenario 3 is impossible. Assume scenario 3 is possible. Without loss of generality, we assume, for two beacon nodes B_1 and B_2 under the simplex wormhole attack, B_1 lies in $D_R(A_1)$ and B_2 lies in $D_R(A_2)$. From Theorem 1, B_1 will detect B_2 to be a pseudo neighboring beacon. As B_1 and B_2 have the identical pseudo neighboring beacon list, B_2 is also in B_2's pseudo neighboring beacon list, which suggests that B_2 lies in $D_R(A_1)$. As B_2 lies in both $D_R(A_1)$ and $D_R(A_2)$, i.e., B_2 lies in $D_R(A_1) \cap D_R(B_1)$, B_2 is under the duplex wormhole attack, which contradicts to the assumption that B_2 is under the simplex wormhole attack. Therefore, scenario 3 is impossible. For scenarios 1 and 2, both beacon nodes lie in the transmission range of the same attacker. ■

We can see this from the example shown in Fig. 3. B_1 and B_2 are under a simplex wormhole attack, and they both locate in $D_R(A_2)$, thus, they have the identical pseudo neighboring beacon list, i.e., $L_P(B_1) = L_P(B_2) = \{B_3, B_4, B_5, B_6\}$.

We further classify the beacons labeled 'S' into two categories according to their geographic locations, i.e., the beacons lie in the transmission range of the same attacker are grouped into one category. After beacons build their pseudo neighboring beacon lists, two neighboring beacons exchange their pseudo neighboring beacon lists with each other so that they can compare the pseudo neighboring beacon list received from its neighboring beacon with its own pseudo neighboring beacon list. If two pseudo neighboring beacon lists are identical, these two beacons belong to the same category; otherwise, they belong to different categories. These two categories of beacons are called as *attacked beacon set one* (ADS-1) and *attacked beacon set two* (ADS-2). When comparing the nodes in these two sets, the set which has the beacon with the minimum ID among those different beacons is named as ADS-1 and all beacons in this set are labeled with 'S1'; the other set is named as ADS-2 and all beacons in the set are labeled with 'S2'. Take B_1, B_2 and B_5 in Fig. 3 for example, $L_P(B_1) = L_P(B_2) = \{B_3, B_4, B_5, B_6\}$, $L_P(B_5) = \{B_1, B_2, B_3\}$. After exchanging the pseudo neighboring beacon lists with each other, B_1 can observe that $L_P(B_1) = L_P(B_2)$ and $L_P(B_1) \neq L_P(B_5)$, thus, B_1 determines that B_1 and B_2 belong to the same category and B_5 belongs to the other category. Moreover, B_1 and B_2 are labeled with 'S1' and B_4, B_5 and B_6 are labeled with 'S2' as B_1 has the minimum node ID among them. Note that B_3 is labeled with 'D' since it is under the duplex wormhole attack.

The advanced beacon node labeling algorithm is shown in Algorithm 2. Every beacon node B_i which is under the simplex wormhole attack (labeled 'S') broadcasts a *PseudoNeighborBeacon* message including its pseudo neighboring beacon list. It also collects the *PseudoNeighborBeacon* messages from its neighboring beacons. B_i then builds the ADS-1 and ADS-2 based on these pseudo neighboring beacon lists. B_i searches itself in these two sets, if it is found in ADS-1, B_i is labeled with 'S1'; otherwise, B_i is labeled with'S2'.

B. Sensor Nodes Labeling

In the previous subsection, we have just labeled the beacon nodes in the network with 'D', 'S1', 'S2', or 'N'. This is not adequate for the localization procedure to defend against the wormhole attack. Therefore, in this subsection, we will further label the sensor nodes in the network. Similar to the beacon nodes, if sensor nodes lie in region $D_R(A_1) \cup D_R(A_2)$ (as shown in Fig. 3), they are attacked by the wormhole attack; if sensors lie outside the above region, they are not attacked by the wormhole

Algorithm 2 Advanced Beacon Node Labeling

1: Each beacon node B_i labeled with 'S' broadcasts a *PseudoNeighborBeacon* message including its pseudo neighboring beacon list and receives the pseudo neighboring beacon lists from its neighboring beacons' *PseudoNeighborBeacon* messages.
2: B_i builds the ADS-1 and ADS-2 based on these pseudo neighboring beacon lists.
3: B_i searches itself in both sets.
4: **if** B_i is found in the ADS-1 **then**
5: B_i is labeled with 'S1'.
6: **else**
7: B_i is labeled with 'S2'.
8: **end if**

attack.

Each attacked beacon node broadcasts an *Alert* message if it is being labeled with 'S1', 'S2' or 'D'. The *Alert* message includes its label, the attacked beacon set and its members' labels. For each beacon node with a label 'D', its attacked beacon set will include all beacons in region $D_R(A_1) \cup D_R(A_2)$.

Initially, each sensor node will label itself with 'N'. After receiving an *Alert* message from any of its neighboring beacons, the sensor node relabels itself with 'U' to indicate that the sensor node may be affected by the wormhole attack and its final label is still uncertain. For each sensor node labeled with 'U', it will further conduct the following labeling schemes[1].

Similar to the beacon labeling scheme BL1, sensor labeling scheme SL1 is used to detect if a sensor node is under the duplex wormhole attack.

Sensor Labeling Scheme SL1: Each sensor node labeled with 'U' checks whether it violates the self-exclusion property. If yes, it determines that it is under the duplex wormhole attack. The sensor node will mark itself with label 'D'.

Sensor nodes can use the following schemes to label themselves if they are under the simplex wormhole attack.

Sensor Labeling Scheme SL2: For a sensor labeled with 'U' but not 'D', if it receives two copies of the same message from its neighbor node, it can conclude that it is under the simplex wormhole attack and labels itself with 'S'.

Sensor Labeling Scheme SL3: For a sensor labeled with 'U' but not 'D', if it receives messages from two beacon nodes, it can calculate the distance between these two beacon nodes as their coordinates can be obtained from the messages. If the distance is larger than $2R$, the sensor node can conclude that it is under the simplex wormhole attack and labels itself with 'S'.

For the sensor nodes labeled with 'S', they can further use the following extended sensor labeling schemes:

Extended Sensor Labeling Scheme ESL1: For a sensor S_i labeled with 'S', it will check the beacons in both attacked beacon sets after it receives the *Alert* message. If it can find a beacon B_j that is not in the neighbor list of S_i, S_i will will mark itself with the label of B_j.

Extended Sensor Labeling Scheme ESL2: For a sensor labeled with 'S' using scheme SL2, if the received two copies of the same message are from one beacon node, the sensor further checks the label of this beacon node. If the beacon node is labeled with 'S1', the sensor labels itself with 'S2'; otherwise, if the beacon node is labeled with 'S2', the sensor labels itself with 'S1'.

Extended Sensor Labeling Scheme ESL3: For a sensor labeled with 'S' using scheme SL3, if one of these two received beacon nodes is labeled with 'N', the sensor further checks the label of the other beacon node. If the other is labeled with 'S1', the sensor labels itself with 'S2'; otherwise, if the other is labeled with 'S2', the sensor labels itself with 'S1'.

The next sensor labeling scheme can be used to label an uncertain sensor if it is not under the wormhole attack.

Sensor Labeling Scheme SL4: For a sensor S_i labeled with 'U', it will check the beacons in both attacked beacon sets after it receives the *Alert* message. If S_i can find one beacon in each set, i.e., one beacon in the ADS-1 and one beacon in the ADS-2, such that these two beacons are not in the neighbor list of S_i, then S_i can conclude that it is not under the wormhole attack and will mark itself with label 'N'.

The sensor nodes labeling scheme is illustrated in Algorithm 3. Each sensor node is initially labeled with 'N'. If it receives an *Alert* message from a neighboring beacon, it labels itself with 'U'. The sensors labeled with 'U' can build the two attacked beacon sets after receiving all *Alert* messages from their neighboring beacon nodes. After that, the sensor nodes labeled with 'U' conduct the sensor nodes labeling schemes SL1, SL2, SL3 and SL4. The sensor nodes labeled with 'S' further conduct the extended sensor nodes labeling schemes ESL1, ESL2 and ESL3.

C. DV-Hop Based Secure Localization

As the existence of the wormhole attack, a node may receive messages from its pseudo neighbors. The DV-Hop localization is therefore deteriorated. To obtain a successful positioning for the DV-Hop-based localization, each node has to eliminate those pseudo neighbors from its neighbor list. Considering that nodes may be labeled with 'N', 'U',

[1]The proof of correctness of these labeling schemes is omitted due to space limitations.

Algorithm 3 Sensor Nodes Labeling

1: Initially, each sensor node is labeled with 'N'.
2: Each sensor labels itself with 'U' if it receives an *Alert* message from a neighboring beacon.
3: **if** Sensor S_i is labeled with 'U' **then**
4: S_i builds the two attacked beacon sets based on the received *Alert* messages.
5: S_i conducts the sensor nodes labeling schemes SL1, SL2, SL3 and SL4.
6: **if** S_i is labeled with 'S' **then**
7: S_i conducts the extended sensor nodes labeling schemes ESL1, ESL2 and ESL3.
8: **end if**
9: **end if**

'D', 'S', 'S1', 'S2', different labeled nodes will execute the elimination operations according to the following rules[2]:

- For each node (beacon or sensor) with label 'N': no removing operation is needed.
- For each node (beacon or sensor) with label 'D': 1) remove sensors with label 'U'; 2) remove beacons and sensors with labels 'S1', 'S2' or 'S' if only one copy of the message can be received from these beacons and sensors; 3) remove beacons and sensors with label 'D' if exactly two copies of the same message can be received from these beacons and sensors.
- For each node (beacon or sensor) with label 'S1': 1) remove beacons and sensors with labels 'U', 'D' or 'S'; 2) remove beacons and sensors with label 'S2' if only one copy of the message can be received from these beacons and sensors.
- For each node (beacon or sensor) with label 'S2': 1) remove beacons and sensors with labels 'U', 'D' or 'S'; 2) remove beacons and sensors with label 'S1' if only one copy of the message can be received from these beacons and sensors.
- For each sensor with label 'U': remove beacons and sensors with labels 'U', 'D', 'S1', 'S2' or 'S'.
- For each sensor with label 'S': 1) remove beacons and sensors with labels 'U', 'S1' or 'S2'; 2) remove beacons and sensors with labels 'S' or 'D' if only one copy of the message can be received from these beacons and sensors.

After each node eliminates the abnormal nodes from its neighbor list, the DV-Hop localization procedure will be conducted. In the first phase of the DV-Hop localization, every node will not forward the message received from the node out of its neighbor list. With this strategy, the impacts of the wormhole attack on the localization will be avoided. Thus, our proposed scheme can obtain the secure localization against the wormhole attack.

[2]The proof of correctness of these rules is omitted due to space limitations.

V. Performance Evaluation

In this section, we firstly build the theoretical model for determining the probability of detecting the wormhole attack successfully. After that, the simulation results are presented to validate our theoretical model and evaluate our proposed secure localization scheme.

A. Theoretical Probability of Wormhole Attack Detection

According to the beacon nodes labeling schemes, as long as there are beacon nodes in the communication range of the two attackers, these beacon nodes can detect the wormhole attack successfully. Let P_s denote the theoretical probability that beacon nodes successfully detect the wormhole attack, while P_f denotes the probability that the beacon nodes fail to detect the wormhole attack. Hence we have: $P_s = 1 - P_f$. As shown in Fig. 3, the wormhole attack cannot be detected only under the following two scenarios: 1) there is no beacon node in $D_R(A_1)$; and 2) there is no beacon node in $D_R(A_2)$.

As the beacon nodes are randomly deployed in the network with density ρ_b, the probability that there is no beacon node in $D_R(A_1)$ is $P(A) = e^{-\rho_b D_R(A_1)}$. Similarly, the probability that there is no beacon node in $D_R(A_2)$ is $P(B) = e^{-\rho_b D_R(A_2)}$. Thus, we can get:

$$\begin{aligned} P_f &= P(A \cup B) = P(A) + P(B) - P(AB) \\ &= 2e^{-\rho_b \pi R^2} - e^{-\rho_b D_R(A_1) \cap D_R(A_2)} \end{aligned} \quad (1)$$

Therefore, the probability of the wormhole attack detection is:

$$\begin{aligned} P_s &= 1 - P_f \\ &= 1 - 2e^{-\rho_b \pi R^2} + e^{-\rho_b D_R(A_1) \cap D_R(A_2)} \end{aligned} \quad (2)$$

B. Simulation Evaluation

The network configuration of our simulation is set as follows: 100 nodes, including both the beacon nodes and sensor nodes, are deployed randomly in a $50 \times 50m^2$ region. The transmission range of each node equals to $10m$. We evaluate the performance of our proposed scheme when varying the ratio of beacons to sensors as well as the ratio of the length of the wormhole link to the node transmission range (L/R).

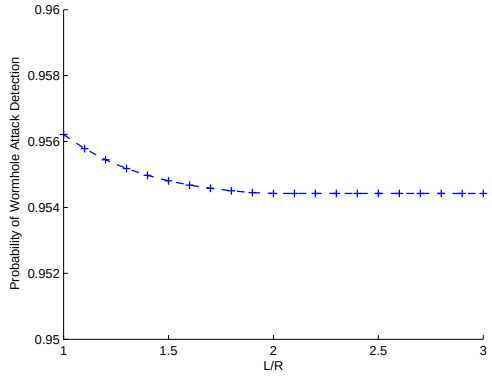

Fig. 4. Probability of wormhole attack detection.

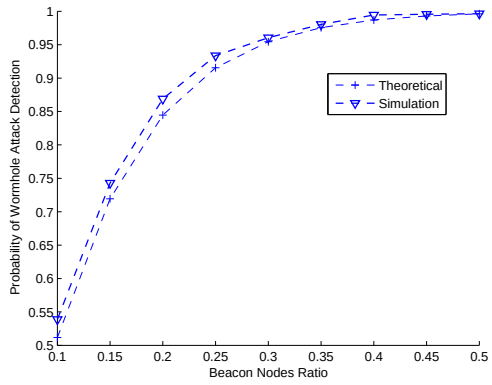

Fig. 5. Probability of wormhole attack detection: Theoretical Model vs Simulation.

Fig. 4 illustrates the probability of the wormhole attack detection when varying the ratio of the length of the wormhole link to the transmission range L/R. In this figure, the ratio of beacon nodes to sensor nodes is set to 30%. We can see that the probability descends slightly with the increase of L/R. However, the probability keeps above 95.4%, implying that our proposed scheme can detect the wormhole attack with a high probability.

Fig. 5 shows the results of determining the probability of the wormhole attack detection through the theoretical model and simulations. To analyze how the ratio of beacons to sensors effects the probability of the wormhole attack detection, we set the L/R to 2 and vary the ratio of beacons to sensors from 10% to 50%. The curves in Fig. 5 illuminate that the theoretical calculation of the probability matches the simulation result quite well (with the maximum difference of 3%). Also, when increasing the ratio of beacons to sensors from 10% to 30%, the probability of the wormhole attack detection raises up drastically to almost 95%. After that the increasing trend becomes slower. Finally, the probability reaches 99.6% when the ratio of beacons to sensors is 50%.

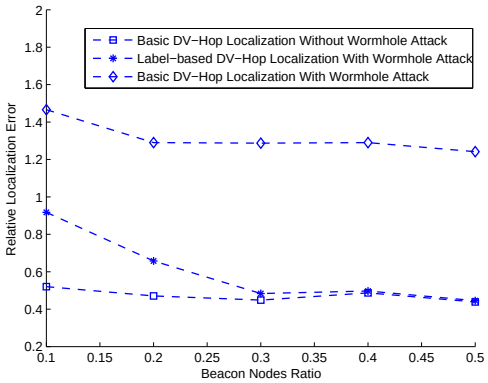

Fig. 6. Comparison of relative localization error.

The impacts of the wormhole attack on the DV-Hop localization process and our proposed wormhole-attack-resistent localization scheme are illustrated in Fig. 6 when the ratio of beacons to sensors varies. In this figure, the relative localization error is used to indicate the impact of the wormhole attack on the localization scheme. The curve with the label "Basic DV-Hop Localization Without Wormhole Attack" indicates the relative localization error for the DV-Hop localization scheme when there is no wormhole attack. We can see that the curve is quite stable when the ratio of beacons to sensors varies, which suggests that the accuracy of the DV-hop localization is insensitive to the number of beacons in the network. Therefore, this curve is used as the reference when the wormhole attack exists. The curve with the label "Basic DV-Hop Localization With Wormhole Attack" indicates the relative localization error for the DV-Hop localization under the wormhole attack. We can see that when the wormhole exists, the relative localization error for the DV-Hop localization scheme increases drastically, which demonstrates the negative impacts of the wormhole attack on the DV-Hop localization. However, for the label-based DV-Hop localization under the wormhole attack, which is the curve with the label"Label-based DV-Hop Localization With Wormhole Attack", the relative localization error is gradually close to that of the basic DV-Hop localization without wormhole attack as the ratio of beacons to sensors increases from 10% to 30%. When the ratio of beacons to sensors is larger than 30%, the label-based DV-Hop can totally conquer the negative impacts of the wormhole attack on the localization process.

VI. Conclusion and Future Work

In this paper, we analyze the severe impacts of the wormhole attack on the DV-Hop based localization in wireless sensor networks. To tackle this secure problem, we propose a label-based secure localization scheme to detect and resist the wormhole attack for the DV-Hop localization process. We also conduct simulations to demonstrate the effectiveness of our proposed scheme under different network parameters.

The proposed scheme works well in the scenario when the network has no packet loss, and the transmission ranges of all nodes are identical. In our future work, we will extend our secure localization scheme to tolerate the packet loss. Also, we will consider the scenario when different types of nodes have different transmission ranges.

VII. Acknowledgment

This work is supported in part by grants NSFC 60873223, NSFC 90818010, International Cooperative Project of Science and Technology Department of Zhejiang Province (2009C34002), PolyU 5236/06E, PolyU 5243/08E, PolyU 5253/09E, 1-ZV5N, and ZJU-SKL ICT0903.

References

[1] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less low cost outdoor localization for very small devices," pp. 28–34, 7 2000.

[2] T. He, C. Huang, B. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-Free Localization Schemes for Large Scale Sensor Networks," in *Proc. of ACM MOBICOM*, 2003, pp. 81–95.

[3] D. Niculescu and B. Nath, "Ad Hoc Positioning System (APS) using AOA," in *Proc. of IEEE INFOCOM*, 2003.

[4] A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Secure Localization Algorithms for Wireless Sensor Networks," *IEEE Communications Magazine*, pp. 96–101, 2008.

[5] D. Liu, P. Ning, and W. Du, "Attack-Resistant Location Estimation in Sensor Networks," in *Proc. of IEEE IPSN*, 2005.

[6] S. Capkun and J. P. Hubaux, "Secure Positioning of Wireless Devices with Application to Sensor Networks," in *Proc. of IEEE INFOCOM*, 2005.

[7] F. Anjum, S. Pandey, and P. Agrawal, "Secure Localization in Sensor Networks using Transmission Range Variation," in *Proc. of IEEE MASS*, 2005.

[8] S. Capkun, M. Cagalj, and M. Srivastava, "Secure Localization With Hidden and Mobile Base Stations," in *Proc. of IEEE INFOCOM*, 2006.

[9] L. Lazos, R. Poovendran, and S. Capkun, "ROPE: Robust Position Estimation in Wireless Sensor Networks," in *Proc. of IEEE IPSN*, 2005.

[10] D. Liu, P. Ning, and W. Du, "Detecting Malicious Beacon Nodes for Secure Localization Discovery in Wireless Sensor Networks," in *Proc. of IEEE ICDCS*, 2005.

[11] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust Statistical Methods for Securing Wireless Localization in Sensor Networks," in *Proc. of IEEE IPSN*, 2005.

[12] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks," in *Proc. of IEEE INFOCOM*, 2003.

[13] W. Wang and B. Bhargava, "Visualization of Wormholes in Sensor Networks," in *Proc. of ACM WiSec*, 2004.

[14] W. Wang and A. Lu, "Interactive wormhole detection and evaluation," *Information Visualization*, vol. 6, no. 1, pp. 3–17, 2007.

[15] Y. Xu, G. Chen, J. Ford, and F. Makedon, "Detecting Wormhole Attacks in Wireless Sensor Networks," in *Proc. of IFIP*, 2008.

[16] R. Maheshwari, J. Gao, and S. R. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," in *Proc. of IEEE Infocom*, 2007.

[17] L. Lazos and R. Poovendran, "SeRLoc: Robust Localization for Wireless Sensor Networks," *ACM Trans. on Sensor Networks*, pp. 73–100, 2005.

[18] ——, "HiRLoc: High-Resolution Robust Localization for Wireless Sensor Networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 233–246, 2006.

[19] H. Chen, W. Lou, and Z. Wang, "A Consistency-based Secure Localization Scheme Against Wormhole Attacks in WSNs," in *Proc. of the International Conference on Wireless Algorithms, Systems and Applications (WASA)*, 2009.

[20] H. Chen, W. Lou, X. Sun, and Z. Wang, "A Secure Localization Approach Against Wormhole Attacks Using Distance Consistency," *Eurasip Journal on Wireless Communications and Networking, Spacial Issue on Wireless Network Algorithms, Systems, and Applications*, 2009.

[21] H. Chen, W. Lou, and Z. Wang, "Conflicting-Set-Based Wormhole Attack Resistant Localization in Wireless Sensor Networks," in *Proc. 6th Int. Conf. on Ubiquitous Intelligence and Computing(UIC)*, 2009.

[22] K. Langendoen and N. Reijers, "Distributed Localization in Wireless Sensor Networks: a Quantitative Comparison," *Computer Networks*, pp. 449–518, 2003.