ARTICLE IN PRESS

Pervasive and Mobile Computing ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

journal homepage: www.elsevier.com/locate/pmc

# Securing DV-Hop localization against wormhole attacks in wireless sensor networks

Honglong Chen [a,b], Wei Lou [c,d], Zhi Wang [a,*], Junfeng Wu [e], Zhibo Wang [a], Aihua Xia [a]

[a] State Key Lab of Industrial Control Technology, Zhejiang University, Hangzhou, PR China

[b] College of Information and Control Engineering, China University of Petroleum, Qingdao, PR China

[c] Department of Computing, The Hong Kong Polytechnic University, Hong Kong

[d] The Hong Kong Polytechnic University Shenzhen Research Institute, Shenzhen, PR China

[e] Department of Electronic and Computer Engineering, The Hong Kong University of Science and Technology, Hong Kong

ARTICLE INFO

*Article history:*
Received 8 May 2013
Received in revised form 27 December 2013
Accepted 17 January 2014
Available online xxxx

*Keywords:*
DV-Hop localization
Wireless sensor networks
Wormhole attack

ABSTRACT

Node localization becomes an important issue in the wireless sensor network as its wide applications in environment monitoring, emergency rescue and battlefield surveillance, etc. Basically, the DV-Hop localization scheme 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 severely disrupt the DV-Hop localization process. The distance-vector propagation phase during the DV-Hop localization can even aggravate the positioning error, compared to the localization schemes without wormhole attacks. In this paper, we analyze the impacts of wormhole attack on the DV-Hop localization scheme, based on which we propose a label-based DV-Hop secure localization scheme to defend against the wormhole attack. We further theoretically prove the correctness of the proposed scheme. Simulation results illustrate the effectiveness of the proposed label-based DV-Hop secure localization scheme.

© 2014 Elsevier B.V. All rights reserved.

## 1. Introduction

With the advantages of low cost, large scale, densely distributed deployment and self-configuration, Wireless Sensor Networks (WSNs) have been applied in many fields to monitor and control the physical world [1]. In WSNs, sensed data will 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, etc.

Many protocols and algorithms are proposed to solve the node's localization problem, which can be classified into two categories: range-based and range-free [2] schemes. Range-based schemes 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 for the distance measurement. Range-free schemes do not rely on the availability of range (or angle) estimates, thus they need no expensive hardware. Considering that the hardware requirement of range-based schemes is inappropriate for the 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 localization scheme, is applied with the assumption of isotropic networks. First, beacons (or anchors), as location-known nodes, flood their positions through the network so that all the nodes can

* Corresponding author. Tel.: +86 18658100255.
*E-mail addresses:* wangzhizju@gmail.com, wangzhi@iipc.zju.edu.cn (Z. Wang).

1574-1192/$ – see front matter © 2014 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.pmcj.2014.01.007

Please cite this article in press as: H. Chen, et al., Securing DV-Hop localization against wormhole attacks in wireless sensor networks, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.01.007

obtain their 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 will be broadcasted to its neighbors, by averaging the distances to all the other beacons over the total hop-counts. Sensors, being location unknown, can then estimate their distances to each of the beacons based on the average distance per hop and hop-counts, after which they can easily localize themselves.

As WSNs usually work in a hostile environment, they are vulnerable to various malicious attacks. The attacks, which can threaten the localization of the nodes in a hostile WSN, can generally be classified into two categories, *external* attacks and *internal* attacks [4]. External attacks can distort network behaviors without obtaining the system's authorization, while internal attacks are authenticated ones and thus more devastating to the security of the system. The wormhole attack, as a typical external attack, can be easily launched by two colluding attackers. When such attack is launched, one attacker tunnels its sniffed packets to another attacker via the wormhole link which will broadcast them to its neighbors, thus the packets can be delivered along a shorter path, i.e., with less hops. The wormhole attack can deteriorate the DV-Hop localization dramatically. It not only reduces the hop-counts to all the beacons, but also affects the estimation of average distance per hop. Consequently, 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., eliminating 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 the proposed scheme is to mark the nodes (including beacons and sensors) with different labels according to the communication properties they violate, after which each node can pick up its pseudo neighbors (they are originally not neighbors of each other and become neighbors due to the wormhole attack). Then the communication links between the pseudo neighbors will be forbidden to secure the localization.

The main contributions of this paper are summarized as follows:

- We analyze the impacts of the wormhole attack on the DV-Hop localization process;
- We propose a wormhole attack resistant scheme for each node to determine their pseudo neighbors, the communication links between which will be forbidden to achieve secure localization;
- We theoretically prove the correctness of the proposed secure localization scheme;
- We conduct the simulations to validate the effectiveness of our proposed secure localization scheme.

The rest of this paper is organized as follows. Section 2 reviews the related work on the secure localization. In Section 3, we describe the network model, the DV-Hop localization approach, the wormhole attack model and its impacts on the DV-Hop localization process. Section 4 describes our proposed label-based secure localization in details. In Section 5, we present the performance evaluation. Finally, Section 6 concludes this paper and outlines our future work.

## 2. Related work

The secure localization [5] has been well studied in the past few years. We first review the range-based secure localization scheme and range-free secure localization schemes respectively, and then discuss the wormhole attack detection schemes and the wormhole attack resistant localization schemes.

*Range-based secure localization schemes*: Liu et al. [6] propose two secure localization schemes against the compromise attack which adopt the concept of consistency. SPINE [7] enables verifiable multilateration and verification of positions of mobile devices for secure computation in the presence of attackers. In [8], 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 [4] 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. In [9,10], Chen et al. propose a novel secure localization approach called TSCD to defend against the distance-consistent spoofing attack using the consistency check on the distance measurements.

*Range-free secure localization schemes*: Lazos et al. [11] 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 [12], 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 [13], robust statistical methods are proposed, including triangulation and RF-based fingerprinting, to make localization attack-tolerant.

*Wormhole attack detection schemes*: The "packet leashes" mechanism [14] uses geographical and temporal leashes to detect whether or not the packets are attacked by wormhole attacks. Wang and Bhargava [15] 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 [16] propose an interactive wormhole detection which selects some feature points to reduce the overlapping issue and preserve major topology features. In [17], a wormhole attack detection mechanism is proposed which uses geographic information to detect anomalies in neighbor relations and node movements. Another set of wormhole attack preventing techniques [18–20] use the round-trip time of packets as a measurement to detect the existence of wormhole attacks, which are similar in nature to temporal packet leaches. Xu et al. [21] propose a wormhole attack detection algorithm using a hop counting technique as a probe procedure,

Please cite this article in press as: H. Chen, et al., Securing DV-Hop localization against wormhole attacks in wireless sensor networks, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.01.007

reconstructing a local map for each node and using a "diameter" feature to detect abnormalities caused by wormholes. In [22], the wormhole attack detection scheme adopts the maximum number of independent neighbors of two non-neighbor nodes. Another connectivity-based wormhole detection approach is proposed in [23] which is robust to different communication models and energy efficient. A topological approach is proposed in [24] to detect the wormhole attacks. In [25], a localized algorithm that detects the wormhole attacks directly using the connectivity information implied by the underlying communication graph is designed, and it requires no specialized hardware, which makes it practical in the real-world scenarios. However, all the above wormhole attack detection schemes emphasize the detection without considering the localization procedure.

*Wormhole attack resistant localization schemes*: As the localization process will be greatly deteriorated by the wormhole attack, some secure localization approaches have been proposed. SeRLoc [26] 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 [27] further improves SeRLoc by utilizing antenna rotations and multiple transmission power levels to provide richer information for higher localization resolution. The schemes in [28] can also be applied into the localization against wormhole attacks, but it does not suit for the scenario when a large percentage of locators are attacked. Chen et al. [29,30] propose a secure localization scheme using the distance consistency to defend against the wormhole attack. In [31–33], 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 [26–31] 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 rarely discussed in literature.

## 3. Problem statement

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

### 3.1. Network model

We assume that there are three types of nodes in a WSN: beacons (or anchors), sensors, and attackers. Beacons are location-fixed nodes with their positions known in advance (by GPS device or manual configuration), they will keep stationary after deployment. The sensors, either moving around or staying at a place, are position-unknown nodes that need to locate themselves with assistance of the beacons. The system can conduct the localization procedure periodically for the sensor nodes to update their current locations since they may be mobile. The attackers exist in a pair and collude with each other to launch a wormhole attack, which can invade the WSN without passing any system's authorization. We assume that all the nodes have an identical transmission range $R$. The sensors and beacons are deployed independently, following the Poisson distribution with node densities $\rho_b$ and $\rho_s$, respectively. That is, the probability of $k$ beacons in an area $D_b$ and that of $k$ sensors in an area $D_s$ are $P(N_b = k) = \frac{(D_b\rho_b)^k}{k!}e^{-D_b\rho_b}$ and $P(N_s = k) = \frac{(D_s\rho_s)^k}{k!}e^{-D_s\rho_s}$, respectively. (Note that $D_b$ and $D_s$ are subareas of the deployed wireless sensor networks.)

### 3.2. DV-Hop localization approach

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

- In the first phase, a typical distance vector routing mechanism is employed: each beacon initiates a flooding, which includes its location information, ID and the hop-count of 1, throughout the network; each node that relays the flooding message will increase the hop-count by one and add its own ID onto the flooding message as the sender; after the flooding procedure, every node can obtain the minimum hop-count to each of the beacons.
- In the second phase, each beacon, after obtaining the position and hop-count information to all the other beacons, estimates the average distance per hop in the network. For example, beacon $i$ can calculate 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 between them. Once calculated, $HS_i$ will also be flooded to all the nodes in the network.
- In the last phase, each sensor can estimate its distance to each beacon based on its hop-count to this beacon and the average hop-size. For example, sensor $k$ can estimate the distance $d_{kj}$ (the distance from sensor $k$ to beacon $j$) using $d_{kj} = h_j \times HS_j$. After obtaining the distance information to all the beacons, each sensor can conduct the *triangulation* or *maximum likelihood estimation* [34] scheme to estimate its own location.

### 3.3. Wormhole attack model and its impacts on DV-Hop localization

In this paper, we consider a hostile environment where the DV-Hop localization procedure of sensors may be disrupted by wormhole attack. In the wormhole attack, one attacker sniffs packets at one point of the network, tunnels them via

Please cite this article in press as: H. Chen, et al., Securing DV-Hop localization against wormhole attacks in wireless sensor networks, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.01.007

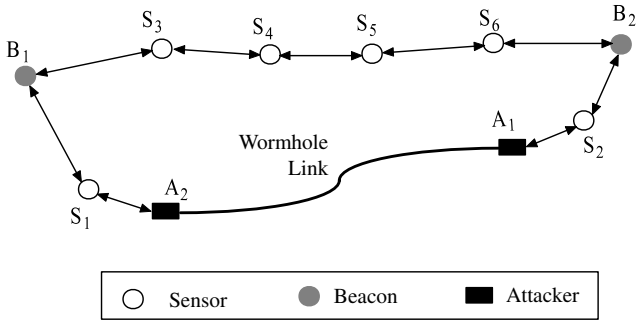


**Fig. 1.** The impact of wormhole attack on DV-Hop localization.

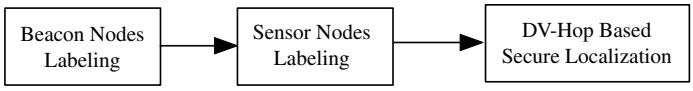


**Fig. 2.** The flowchart of the label-based DV-Hop secure localization scheme.

the wormhole link to the other attacker which locates at the other point of the network, then the attacker broadcasts the received packets to its neighbors. We assume that the wormhole link is bi-directional and symmetrical so that the packets could be transmitted via either direction. The communication between each pair of colluding wormhole attackers is not limited to $R$ since they can communicate with each other using certain communication technique, i.e., the wormhole link, which may be implemented with wired communication. 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 $R$, in which case, two colluding wormhole attackers can still communicate with each other via the wormhole link.

Due to the characteristic of the wormhole attack, it can greatly deteriorate the DV-Hop localization procedure of sensors. As shown in Fig. 1, two attackers $A_1$ and $A_2$ collude to launch a wormhole attack in 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 minimum hop-counts to them. For instance, sensor $S_1$' original minimum hop-count to beacon $B_2$ 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 $S_1$. As the relay behaviors of the attackers are invisible to the beacons and sensors, $S_1$ will consider the minimum hop-count to $B_2$ as 2 ($B_2 \rightarrow S_2 \xrightarrow{\dashrightarrow A_1 \dashrightarrow A_2 \dashrightarrow} S_1$), 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 $\sqrt{(x_1-x_2)^2+(y_1-y_2)^2}/5$, where $(x_1, y_1)$ and $(x_2, y_2)$ are the coordinates of beacons $B_1$ and $B_2$. However, under 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 $\sqrt{(x_1-x_2)^2+(y_1-y_2)^2}/3$, 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 smaller hop-counts to beacons. In the second phase, a beacon may calculate an incorrect hop-size, which will be flooded to other nodes in the network. Finally, each sensor may use incorrect hop-counts and hop-size to estimate the distances to the beacons, based on which the self-localization will be inaccurate.

In this paper, we mainly focus on the security problems caused by the wormhole attackers. We do not consider the complex scenario that the other nodes including the beacon nodes and sensor nodes would be compromised. Thus, during the localization procedure, the beacon nodes and the sensor nodes are friendly to cooperate with each other and will not inject faked information, such as position and hop count, into the network.

## 4. Label-based DV-Hop secure localization scheme

In this section, we will describe our proposed wormhole attack resistant localization scheme, called label-based DV-Hop secure localization, which includes three phases, beacon nodes labeling, sensor nodes labeling, and DV-Hop based secure localization. The flowchart of the secure localization scheme is shown in Fig. 2. Firstly, the beacon nodes are differentiated and labeled according to their geographic relationships under a wormhole attack. Secondly, the sensor nodes are further differentiated and labeled based on the labeling results of neighboring beacon nodes. After forbidding the abnormal communication links, which are via the wormhole link, among the labeled neighboring nodes, the DV-Hop localization procedure can then be conducted to achieve secure localization.

To describe the label-based DV-Hop secure localization scheme more clearly, we provide the following definitions, some of which are borrowed from our previous work [33]:

Please cite this article in press as: H. Chen, et al., Securing DV-Hop localization against wormhole attacks in wireless sensor networks, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.01.007

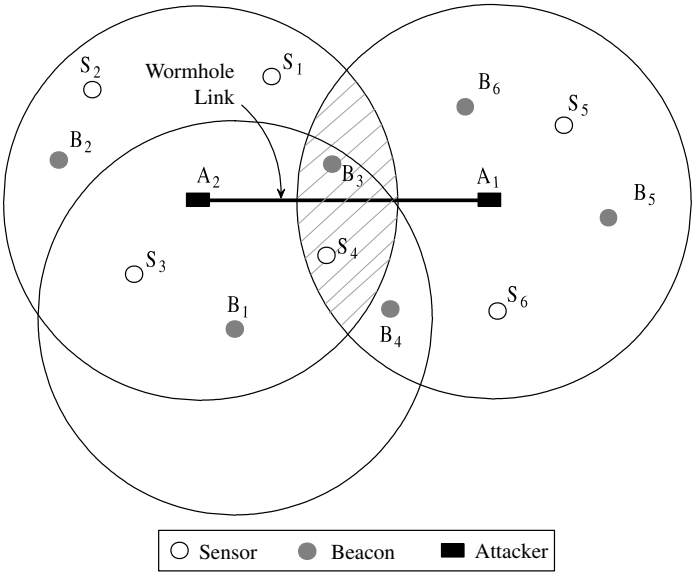


**Fig. 3.** The wormhole attack in a WSN.

**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.** *Dubious neighbor*: A node is a dubious neighbor of the other node if they can communicate with each other via the wormhole link.

**Definition 4.** *Pseudo neighbor*: A node is a pseudo neighbor of the other node if they can only communicate with each other via the wormhole link.

**Definition 5.** *Valid neighbor*: A node is a valid neighbor of the other node if they can communicate with each other via the direct link.

For the network as shown in Fig. 3, node $S_4$ is under the duplex wormhole attack, and node $S_3$ is under the simplex wormhole attack. Nodes $B_4$ and $B_6$ are dubious neighbors of $B_1$, $B_6$ is a pseudo neighbor of $B_1$, and nodes $B_3$ and $B_4$ are valid neighbors of $B_1$. Note that the pseudo neighbor of a node will also be its dubious neighbor. While during the localization procedure, the communication links between the pseudo neighbors should be forbidden (since these links only exist under the wormhole attack) to secure the localization.

To ease the description of our proposed scheme, we define $D_R(u)$ as a disk with radius $R$ and center $u$; $L_D(i)$, $L_P(i)$ and $L_V(i)$ are defined as the dubious neighboring beacon list, pseudo neighboring beacon list and valid neighboring beacon list of node $i$, respectively.

### 4.1. Beacon nodes labeling

Before localization, all nodes in the network, including both beacons and sensors, periodically broadcast *Hello* messages to its neighbors, then each node can build a neighbor list after receiving the *Hello* messages from its neighbors. The *Hello* message includes the node's type (i.e., beacon or sensor), ID, and coordinate if it is a beacon. When building the neighbor lists, the beacon nodes may detect some abnormalities caused by the wormhole attack. By analyzing these abnormalities, the beacon nodes can be classified and labeled into three categories: under the duplex wormhole attack, under the simplex wormhole attack, and without the wormhole attack. As shown in Fig. 3, beacon nodes in $D_R(A_1) \cap D_R(A_2)$, i.e., $B_3$, are under the duplex wormhole attack, beacon nodes in $D_R(A_1) \setminus D_R(A_2)$ and $D_R(A_2) \setminus D_R(A_1)$, i.e., $B_1$, $B_2$, $B_4$, $B_5$ and $B_6$, are under the simplex wormhole attack, and beacon nodes outside $D_R(A_1) \cup D_R(A_2)$ are without the wormhole attack. The classification of the beacon nodes can be based on the following three properties:

- *Self-exclusion property*: A node normally cannot receive a message sent from itself in a loop-free path.
  For each beacon node under the duplex wormhole attack (i.e., $B_3$ as shown in Fig. 3), the *Hello* message it sends will be relayed by attacker $A_1$ via wormhole link to attacker $A_2$ and then received by itself; similarly, the *Hello* message will also

Please cite this article in press as: H. Chen, et al., Securing DV-Hop localization against wormhole attacks in wireless sensor networks, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.01.007

be transmitted from $A_2$ to $A_1$ via wormhole link and then received by itself. However, without the wormhole attack, a node cannot receive a message sent from 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 message from any 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 $A_2$ ($B_4 \rightarrow A_1 \rightarrow A_2 \rightarrow B_1$). Thus, if a beacon node receives the same message more than once from a neighboring 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 message 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 the *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 beacon nodes, which is shown in Algorithm 1: Every node periodically broadcasts a *Hello* message. It also receives the *Hello* messages from its neighbors to build the neighbor list. Each beacon node initially labels itself with $\overline{N}$. It can further classify itself using beacon labeling schemes BL1, BL2 and BL3. If the beacon node detects that it violates the self-exclusion property using scheme BL1, it labels itself with $\overline{D}$ 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 schemes BL2 or BL3, it labels itself with $\overline{S}$. Note that for those beacon nodes which do not violate any of the above properties, their labels will be kept with $\overline{N}$ to indicate that they are not under the wormhole attack.

**Algorithm 1** Basic Beacon Node Labeling Algorithm

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

After all the beacon nodes are labeled, we can get the following theorems:

**Theorem 1.** *Given a network under the wormhole attack, each of the beacon nodes under the simplex wormhole attack can detect all its dubious neighboring beacon nodes.*

**Proof.** For each beacon node under the simplex wormhole attack, it must lie 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 example. All the dubious neighboring beacon nodes of $B_1$ lie in $D_R(A_1)$, which can be divided into two groups:

Group 1: The dubious 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). The *Hello* messages of these dubious 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 $B_1$, which violates the packet uniqueness property. Thus $B_1$ can identify all these dubious neighboring beacons using the beacon labeling scheme BL2.

Group 2: The dubious 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 distance between each of them and $B_1$ is larger than $R$, but the *Hello* messages they send can be relayed by the wormhole attack and then received by $B_1$, which violate the transmission constraint property. Thus $B_1$ can identify these dubious neighboring beacons using the beacon labeling scheme BL3.

Therefore, each of the beacon nodes under the simplex wormhole attack can detect all its dubious neighboring beacon nodes. ■

Please cite this article in press as: H. Chen, et al., Securing DV-Hop localization against wormhole attacks in wireless sensor networks, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.01.007

**Theorem 2.** *Given a network under the wormhole attack, if two beacon nodes are under the simplex wormhole attack, then they lie in the transmission range of the same attacker if and only if they have the same dubious neighboring beacon list.*

**Proof.** *Necessary condition*: For any two beacon nodes under the simplex wormhole attack that are within the transmission range of the same attacker, without loss of generality, we take the beacons in $D_R(A_2)$ (e.g., $B_1$ and $B_2$ as shown in Fig. 3) for example, according to Theorem 1, each of the two beacon nodes can identify all its dubious neighboring beacons, which lie in $D_R(A_1)$. Therefore, they have the same dubious neighboring beacon list, which includes all the beacon nodes in $D_R(A_1)$.

*Sufficient condition*: For any two beacon nodes with the same dubious neighboring beacon list under the simplex wormhole attack, there are three possible scenarios: (1) both the two beacon nodes lie in $D_R(A_1)$, (2) both the two 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 $D_R(A_2)$. As in the first two scenarios, the beacon nodes are within the transmission range of the same attacker, we only need to discuss scenario 3. We now prove by contradiction that if these two beacon nodes have the same dubious 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 $B_5$ with the same dubious neighboring beacon list under the simplex wormhole attack as shown in Fig. 3, $B_1$ lies in $D_R(A_1)$ and $B_5$ lies in $D_R(A_1)$. According to Theorem 1, $B_1$ will detect $B_5$ to be a dubious neighboring beacon. As $B_1$ and $B_5$ have the same dubious neighboring beacon list, $B_5$ is also in $B_5$'s dubious neighboring beacon list, which suggests that $B_5$ lies in $D_R(A_2)$. Thus, $B_5$ lies in both $D_R(A_1)$ and $D_R(A_2)$, i.e., $B_5$ lies in $D_R(A_1) \cap D_R(A_2)$, indicating that $B_5$ is under the duplex wormhole attack, which contradicts to the assumption that $B_5$ is under the simplex wormhole attack. Therefore, scenario 3 is impossible.

Thus we can conclude that given a network under the wormhole attack, if two beacon nodes are under the simplex wormhole attack, then they lie in the transmission range of the same attacker if and only if have the same dubious neighboring beacon list. ■

We can verify Theorem 2 with 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 dubious neighboring beacon list, i.e., $L_D(B_1) = L_D(B_2) = \{B_3, B_4, B_5, B_6\}$.

We can further classify the beacons labeled $\overline{S}$ into two categories according to their geographic locations, i.e., the beacons lie in the transmission range of the same attacker will be grouped into the same category. After beacons build their dubious neighboring beacon lists, two neighboring beacons exchange their dubious neighboring beacon lists with each other so that they can compare the dubious neighboring beacon list received from its neighboring beacon with its own dubious neighboring beacon list. If they 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* (ABS-1) and *attacked beacon set two* (ABS-2). When comparing the nodes in these two sets, the set which includes the beacon with the minimum ID among all the beacons in the two sets will be named as ABS-1 and all beacons in this set will be labeled with $\overline{S1}$; the other set will be named as ABS-2 and all beacons in this set will be labeled with $\overline{S2}$. According to Theorem 2, the beacon nodes under the simplex wormhole attack within the same group (ABS-1 or ABS-2) are within the transmission range of the same attacker. Take $B_1$, $B_2$ and $B_5$ in Fig. 3 for example, $L_D(B_1) = L_D(B_2) = \{B_3, B_4, B_5, B_6\}$, $L_D(B_5) = \{B_1, B_2, B_3\}$. After exchanging the dubious neighboring beacon lists with each other, $B_1$ can observe that $L_D(B_1) = L_D(B_2)$ and $L_D(B_1) \neq L_D(B_5)$, 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 $\overline{S1}$ (within the transmission range of $A_2$) and $B_4$, $B_5$ and $B_6$ are labeled with $\overline{S2}$ (within the transmission range of $A_1$) as $B_1$ has the minimum node ID among them. Note that $B_3$ is labeled with $\overline{D}$ 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 $\overline{S}$) broadcasts a *DubiousNeighborBeacon* message including its dubious neighboring beacon list. It also collects the *DubiousNeighborBeacon* messages from its neighboring beacons. $B_i$ then builds the ABS-1 and ABS-2 based on these dubious neighboring beacon lists. $B_i$ searches itself in these two sets, if it is found in ABS-1, $B_i$ is labeled with $\overline{S1}$; otherwise, $B_i$ is labeled with $\overline{S2}$.

**Algorithm 2** Advanced Beacon Node Labeling Algorithm

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

### 4.2. Sensor nodes labeling

In the previous section, we have just labeled the beacon nodes in the network with $\overline{D}$, $\overline{S1}$, $\overline{S2}$ or $\overline{N}$. This is not adequate for the localization procedure to defend against the wormhole attack. Therefore, we will further label the sensor nodes in

Please cite this article in press as: H. Chen, et al., Securing DV-Hop localization against wormhole attacks in wireless sensor networks, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.01.007

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 attack.

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

Initially, each sensor node will label itself with $\overline{N}$. After receiving an *Alert* message from any of its neighboring beacons, the sensor node can then relabel itself with $\overline{U}$ to indicate that the sensor node's self-localization may be affected by the wormhole attack and its final label is still uncertain. For each sensor node labeled with $\overline{U}$, it will further conduct the following labeling schemes.

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

*Sensor labeling scheme* SL1: Each sensor node labeled with $\overline{U}$ 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 $\overline{D}$.

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 node labeled with $\overline{U}$ but not $\overline{D}$, if it receives two copies of the same message from its neighboring node, it can conclude that it is under the simplex wormhole attack and label itself with $\overline{S}$.

*Sensor labeling scheme* SL3: For a sensor node labeled with $\overline{U}$ but not $\overline{D}$, if it receives messages from two beacon nodes, it can calculate the distance between these two beacon nodes since 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 label itself with $\overline{S}$.

If the sensor is not under the wormhole attack, it can use the next sensor labeling scheme to determine its label.

**Theorem 3.** *If there is at least one beacon node in each of the two attacked beacon sets, which is not neighbor of the sensor, then the sensor is not under the wormhole attack.*

**Proof.** We assume that there are two beacon nodes $B_1$ and $B_2$, $B_1 \in$ ABS-1, $B_2 \in$ ABS-2, and both the two beacon nodes are not neighbors of the sensor. As $B_1$ and $B_2$ are with different attacked beacon sets, they are within the transmission range of different attackers. If the sensor is within the transmission range of the same attacker with $B_1$, then $B_2$ must be neighbor of the sensor since they can communicate with each other via the wormhole link, which contradicts to the condition that $B_2$ is not neighbor of the sensor. Thus the sensor is not within the transmission range of the same attacker with $B_1$. Similarly, the sensor is not within the transmission range of the same attacker with $B_2$. Therefore, the sensor must be out of the transmission range of both the two attackers, indicating that it is not under the wormhole attack. ■

*Sensor labeling scheme* SL4: For a sensor $S_i$ labeled with $\overline{U}$, it can check the beacons in both the two attacked beacon sets after it receives the *Alert* message. If $S_i$ can find one beacon from each set, i.e., one beacon from the ABS-1 and one beacon from the ABS-2, such that the two beacons are not its neighbors, then $S_i$ can conclude that it is not under the wormhole attack and will mark itself with label $\overline{N}$.

For the sensor nodes labeled with $\overline{S}$, they can further use the following extended sensor labeling schemes.

**Theorem 4.** *For a sensor node under the simplex wormhole attack, if it can identify a beacon node in either of the attacked beacon sets which is not its neighbor, then the sensor node and the beacon node are within the transmission range of the same attacker.*

**Proof.** Since this beacon node is in the attacked beacon sets, it must lie in $D_R(A_1) \cup D_R(A_2)$. Suppose that this beacon node is in different attacker's transmission range with the sensor node, then its message can be tunneled to the sensor node via the wormhole link. Thus, the beacon node must be in the senor's neighbor list, which contradicts to the condition that the beacon node is not the sensor's neighbor. Therefore, the sensor can conclude that it is within the transmission range of the same attacker with this beacon node. ■

*Extended sensor labeling scheme* ESL1: For a sensor $S_i$ labeled with $\overline{S}$, it will check the beacons in both the two 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 mark itself with the label of $B_j$.

**Theorem 5.** *For a sensor node under the simplex wormhole attack, if it can receive two copies of the same message from a beacon node which is also under the simplex wormhole attack, then the sensor and this beacon node are within the transmission range of different attackers.*

**Proof.** Suppose that this beacon node is within the transmission range of the same attacker with the sensor. Since the beacon node is under the simplex wormhole attack, it must be out of the transmission range of the other attacker. Thus, the message from this beacon node cannot be tunneled to the sensor via the wormhole link, which contradicts to the condition that the sensor receives two copies the of same message from this beacon node. Therefore, the sensor can conclude that it is not in the transmission range of the same attacker with the beacon node. ■

*Extended sensor labeling scheme* ESL2: For a sensor labeled with $\overline{S}$ using scheme SL2, if the received two copies of the same message are from one beacon node, the sensor can further check the label of this beacon node. If the beacon node is labeled with $\overline{S1}$, the sensor labels itself with $\overline{S2}$; otherwise, if the beacon node is labeled with $\overline{S2}$, the sensor labels itself with $\overline{S1}$.

Please cite this article in press as: H. Chen, et al., Securing DV-Hop localization against wormhole attacks in wireless sensor networks, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.01.007

**Theorem 6.** *For a sensor under the simplex wormhole attack, if it can receive packets from two beacon nodes, the distance between which is larger than* $2R$ *and one of them is not under the wormhole attack, then the sensor and the other beacon node are within the transmission range of different attackers.*

**Proof.** We assume there are two beacon nodes $B_1$ and $B_2$, the distance between which is larger than $2R$, $B_1$ is not under the wormhole attack and the sensor can receive packets from both of them. Suppose that the sensor and $B_2$ are in the transmission range of the same attacker. As $B_2$ is under the simplex wormhole attack and is in the transmission range of the same attacker with the sensor, it can be determined that $B_2$ cannot communicate with the sensor via the wormhole link. Thus $B_2$ must be in the transmission range of the sensor since the sensor can receive message from $B_2$. Also, as the sensor can receive message from $B_1$ and $B_1$ is not under the wormhole attack, $B_1$ must also be in the transmission range of the sensor. Thus, both $B_1$ and $B_2$ are in the transmission range of the sensor, which contradicts to the condition that the distance between the two beacon nodes is larger than $2R$. Therefore, the sensor and the other beacon node (i.e., $B_2$) are within the transmission range of different attackers. ■

*Extended sensor labeling scheme* ESL3: For a sensor labeled with $\overline{S}$ using scheme SL3, if one of these two beacon nodes is labeled with $\overline{N}$, the sensor can further check the label of the other beacon node. If it is labeled with $\overline{S1}$, the sensor will label itself with $\overline{S2}$; otherwise, if it is labeled with $\overline{S2}$, the sensor will label itself with $\overline{S1}$.

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

**Algorithm 3** Sensor Nodes Labeling Algorithm

```
1: Initially, each sensor node is labeled with N̄.
2: Each sensor labels itself with Ū if it receives an Alert message from a neighboring beacon.
3: if Sensor S_i is labeled with Ū 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 S̄ then
7:       S_i conducts the extended sensor nodes labeling schemes ESL1, ESL2 and ESL3.
8:    end if
9: end if
```

### 4.3. DV-Hop based secure localization

Due to the wormhole attack, a node may receive messages from its pseudo neighbors, leading to incorrect distance estimation to the beacons, which can deteriorate the DV-Hop localization procedure. To secure the DV-Hop based localization, each node has to determine the type of each node in its neighbor list, i.e., pseudo neighbor or valid neighbor, after which the communication links between the pseudo neighbors will be forbidden to secure the localization procedure. Considering that nodes may be labeled with $\overline{N}$, $\overline{U}$, $\overline{D}$, $\overline{S}$, $\overline{S1}$, $\overline{S2}$, in this section we will propose the rules for the nodes to determine its pseudo neighbors and eliminate them before the localization.

**Theorem 7.** *For a node (beacon or sensor) with label* $\overline{N}$*, it has no dubious neighbor and also it is not the dubious neighbor of any other node.*

**Proof.** Suppose node $A$ is labeled with $\overline{N}$, thus $A \notin D_R(A_1) \cup D_R(A_2)$. Consequently, node $A$ cannot communicate with other nodes via the wormhole link, indicating that node $A$ will have no dubious neighbor and it will not be the dubious neighbor of any other node. ■

*Rule* 1. For a node (beacon or sensor) with label $\overline{N}$, it does not need to remove any node from its neighbor list.

According to Theorem 7, a node with label $\overline{N}$ is not a dubious neighbor of any other node, indicating that it is not a pseudo neighbor of any other node. Thus, each node can consider all the nodes with label $\overline{N}$ in its neighbor list as the valid neighbors.

**Theorem 8.** *For any two nodes (beacon or sensor) with label* $\overline{D}$*, they are the pseudo neighbor of each other if and only if each of them can receive exactly two copies of the same message from the other; they are the valid neighbor of each other if and only if each of them can receive exactly* 3 *copies of the same message from the other.*

**Proof.** Suppose node $A$ and node $B$ are two nodes (beacon or sensor) with label $\overline{D}$, thus $A, B \in D_R(A_1) \cap D_R(A_2)$. Via the wormhole link, i.e., $A \leftrightarrow A_1 \leftrightarrow A_2 \leftrightarrow B$ and $A \leftrightarrow A_2 \leftrightarrow A_1 \leftrightarrow B$, each of them can receive two copies of the same message from the other. If the distance between $A$ and $B$ is larger than $R$, only two copies of the same message can be received by each other since they have no direct communication link, indicating that they are pseudo neighbor of each other. Otherwise, if

Please cite this article in press as: H. Chen, et al., Securing DV-Hop localization against wormhole attacks in wireless sensor networks, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.01.007

the distance between $A$ and $B$ is less than $R$, i.e., they have a direct communication link and they are the valid neighbor of each other, then each of them can receive a third copy of the same message from the other. ■

*Rule* 2. For a node (beacon or sensor) with label $\overline{D}$, it will remove nodes with label $\overline{D}$ from its neighbor list if it can receive exactly two copies of the same message from each of them.

**Theorem 9.** *For a node (beacon or sensor) with label $\overline{D}$ and the other node (beacon or sensor) which is under the simplex wormhole attack with label $\overline{S1}$, $\overline{S2}$ or $\overline{S}$, they are pseudo neighbor of each other if and only if each of them can receive exactly one copy of the same message from the other; they are valid neighbor of each other if and only if each of them can receive exactly two copies of the same message from the other.*

**Proof.** Suppose node $A$ is a node with label $\overline{D}$ lying in $D_R(A_1) \cap D_R(A_2)$; node $B$ is a node under the simplex wormhole attack, whose label is $\overline{S1}$, $\overline{S2}$ or $\overline{S}$. If node $B$ lies in $D_R(A_1) \setminus D_R(A_2)$, node $A$ and node $B$ can receive one copy of the message from each other via the wormhole link $B \leftrightarrow A_1 \leftrightarrow A_2 \leftrightarrow A$; otherwise, if $B$ lies in $D_R(A_2) \setminus D_R(A_1)$, node $A$ and node $B$ can also receive one copy of the message from each other via the wormhole link $B \leftrightarrow A_2 \leftrightarrow A_1 \leftrightarrow A$. Then, if the distance between $A$ and $B$ is larger than $R$, only one copy of the same message can be received from each other since they cannot communicate with each other directly, indicating that they are pseudo neighbor of each other. Otherwise, if the distance between $A$ and $B$ is less than $R$, i.e., each of them can receive a second copy of the same message directly from the other, indicating that they are valid neighbor of each other. ■

*Rule* 3. For a node (beacon or sensor) with label $\overline{D}$, it will remove nodes (beacon or sensor) with label $\overline{S1}$, $\overline{S2}$ or $\overline{S}$ from its neighbor list if it can only receive one copy of the same message from each of them; for a node (beacon or sensor) with label $\overline{S1}$, $\overline{S2}$ or $\overline{S}$, it will remove nodes with label $\overline{D}$ if it can receive only one copy of the same message from each of them.

**Theorem 10.** *For two nodes (beacon or sensor) under the simplex wormhole attack, if one of them is labeled with $\overline{S1}$ and the other is labeled with $\overline{S2}$, then they are pseudo neighbor of each other if and only if each of them can receive only one copy of the message from the other; they are valid neighbor of each other if and only if each of them can receive two copies of the same message from the other.*

**Proof.** Without loss of generality, suppose node $A$ (beacon or sensor) is labeled with $\overline{S1}$, which lies in $D_R(A_1) \setminus D_R(A_2)$ and node $B$ (beacon or sensor) is labeled with $\overline{S2}$, which lies in $D_R(A_2) \setminus D_R(A_1)$. Thus, node $A$ and node $B$ can receive one copy of the message from each other via the wormhole link $A \leftrightarrow A_1 \leftrightarrow A_2 \leftrightarrow B$. If the distance between $A$ and $B$ is larger than $R$, then each of them can only receive one copy of the same message from the other since they have no direct communication link. Thus, they are pseudo neighbor of each other. Otherwise, if the distance between $A$ and $B$ is less than $R$, then each of them can receive a second copy of the same message from the other since they can communicate with each other directly, indicating that they are valid neighbor of each other. ■

*Rule* 4. For a node (beacon or sensor) with label $\overline{S1}$ ($\overline{S2}$), it will remove nodes with label $\overline{S2}$ ($\overline{S1}$) from its neighbor list if it can only receive one copy of the same message from each of them.

**Theorem 11.** *For two sensor nodes with label $\overline{S}$, they are valid neighbor of each other if and only if each of them can receive two copies of the same message from the other.*

**Proof.** Obviously, only sensor nodes can be labeled with $\overline{S}$, which cannot be further labeled into $\overline{S1}$ or $\overline{S2}$. Without loss of generality, suppose $A$ and $B$ are two sensor nodes with label $\overline{S}$ and they are the neighbor of each other. According to the geographical relationships between them and the attackers, there are four cases for the two sensor nodes:

Case 1: They are within the transmission range of different attackers and the distance between them is larger than $R$. In this case, each of them can receive only one copy of the message from the other, i.e., they can communicate with each other only via the wormhole link, indicating that they are pseudo neighbor of each other.

Case 2: They are within the transmission range of different attackers and the distance between them is less than $R$. In this case, each of them can receive two copies of the same message from the other, one via the wormhole link and the other via the direct communication. Since the two sensor nodes have a direct communication link, they are valid neighbor of each other.

Case 3: They are within the transmission range of the same attacker and the distance between them is larger than $R$. In this case, it is obvious that each of them cannot communicate with each other, either via the wormhole link or direct communication. Thus, they are not neighbor of each other.

Case 4: They are within the transmission range of the same attacker and the distance between them is less than $R$. In this case, each of them can receive only one copy of the message from the other since they can communicate with each other only via the direct communication link. Thus, they are valid neighbor of each other.

Thus, for two sensor nodes with label $\overline{S}$, if each of them can receive two copies of the same message from the other, then it must be case 2, indicating that they are valid neighbor of each other. ■

According to Theorem 11, for two sensor nodes with label $\overline{S}$, if each of them can receive only one copy of the message from the other, then it can be case 1 or 4. Since the two sensor nodes cannot determine whether they are within the transmission

Please cite this article in press as: H. Chen, et al., Securing DV-Hop localization against wormhole attacks in wireless sensor networks, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.01.007

range of the same attacker, they cannot determine whether or not they are pseudo neighbor of each other. However, to make sure that each node can eliminate all the pseudo neighbors from its neighbor list before localization procedure, we propose Rule 5.

*Rule* 5. For a sensor node with label $\overline{S}$, it will remove the sensor nodes with label $\overline{S}$ from its neighbor list if it can receive only one copy of the same message from each of them.

**Corollary 1.** *For a sensor node with label $\overline{S}$, $\overline{S1}$ or $\overline{S2}$ and a node (sensor or beacon) with label $\overline{D}$, they are pseudo neighbor of each other if and only if each of them can receive only one copy of the same message from the other.*

**Proof.** For a sensor node with label $\overline{S}$, $\overline{S1}$ or $\overline{S2}$ and a node (sensor or beacon) with label $\overline{D}$, they can communicate with each other via the wormhole link. Thus, if each of them can receive only one copy of the message from the other, then we can determine that they cannot communicate with each other directly, indicating that they are pseudo neighbor of each other. ■

*Rule* 6. For a sensor node with label $\overline{S}$, $\overline{S1}$ or $\overline{S2}$ and a node (sensor or beacon) with label $\overline{D}$, they will remove each other from their neighbor lists if each of them can receive only one copy of the same message from the other.

For a sensor node with label $\overline{U}$ which cannot be further labeled into $\overline{N}$, $\overline{D}$, $\overline{S1}$, $\overline{S2}$ or $\overline{S}$, it may be pseudo neighbor of other nodes. To guarantee that each node can eliminate all the pseudo neighbors from its neighbor list before localization procedure, we propose Rule 7.

*Rule* 7. For a sensor node with label $\overline{U}$, it will remove nodes with label $\overline{D}$, $\overline{S1}$, $\overline{S2}$, $\overline{S}$ or $\overline{U}$ from its neighbor list; for a node with label $\overline{D}$, $\overline{S1}$, $\overline{S2}$, $\overline{S}$ or $\overline{U}$, it will remove nodes with label $\overline{U}$ from its neighbor list.

For a sensor node with label $\overline{S}$ which cannot be further labeled into $\overline{S1}$ or $\overline{S2}$, it may be pseudo neighbor of other nodes with label $\overline{S}$, $\overline{S1}$ or $\overline{S2}$. Thus we propose Rule 8.

*Rule* 8. For a sensor node with label $\overline{S}$, it will remove nodes with label $\overline{S}$, $\overline{S1}$ or $\overline{S2}$ from its neighbor list; for the nodes with $\overline{S1}$ or $\overline{S2}$, it will remove nodes with $\overline{S}$ from its neighbor list.

After each node eliminates the pseudo neighbors from its neighbor list, the DV-Hop localization procedure can then be conducted, in which the communication links between each node and the nodes out of its neighbor list will be forbidden. Under this strategy, the impact of the wormhole attack on the DV-Hop localization procedure can be counteracted and the secure localization can be achieved.

## 5. Performance evaluation

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

### 5.1. 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 $\rho_b$, 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:

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

Therefore, the probability of the wormhole attack detection is:

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

Since $D_R(A_1) \cap D_R(A_2) = 2R^2 \arccos \frac{L}{2R} - L\sqrt{R^2 - \frac{L^2}{4}}$, we can get:

$$P_s = 1 - 2e^{-\rho_b \pi R^2} + e^{-\rho_b 2R^2 \arccos \frac{L}{2R} - L\sqrt{R^2 - \frac{L^2}{4}}} \tag{3}$$

where $L$ is the length of the wormhole link.

Please cite this article in press as: H. Chen, et al., Securing DV-Hop localization against wormhole attacks in wireless sensor networks, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.01.007

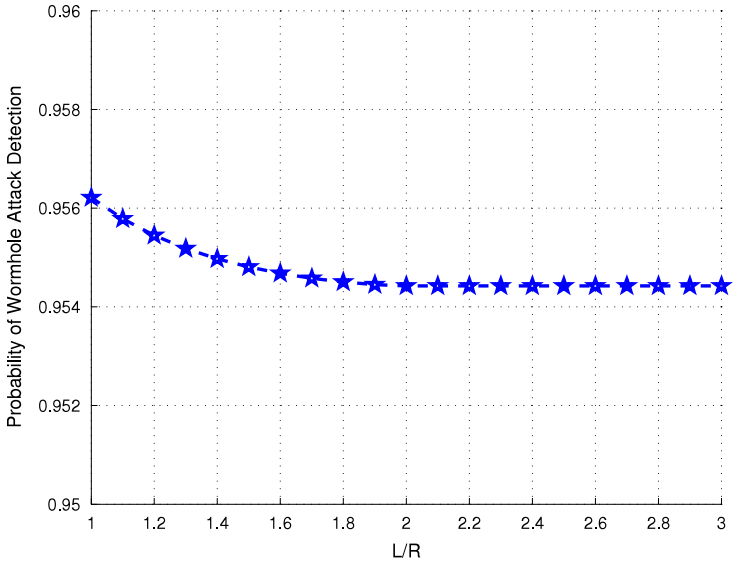


**Fig. 4.** Probability of wormhole attack detection.

### 5.2. Simulation evaluation

We conduct the simulations to illustrate the effectiveness of our proposed secure localization scheme. The network configuration of the simulation is set as follows: 100 nodes, including both the beacon nodes and sensor nodes, are deployed randomly in a $50 \times 50$ m$^2$ region. The transmission range of each node equals to 10 m. 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 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%.

The impacts of the wormhole attack on the DV-Hop localization process and our proposed wormhole attack resistant localization scheme are illustrated in Fig. 6 when the ratio of beacons to sensors varies. In this figure, the ratio of the length of the wormhole link to the transmission range $L/R$ equals is set as 2 and 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.

## 6. 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 defend against

Please cite this article in press as: H. Chen, et al., Securing DV-Hop localization against wormhole attacks in wireless sensor networks, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.01.007

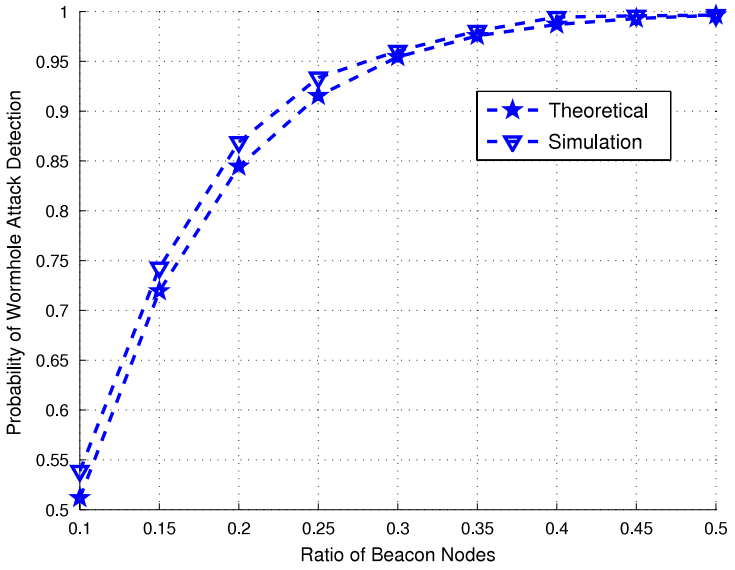


**Fig. 5.** Probability of wormhole attack detection: theoretical model vs. simulation.

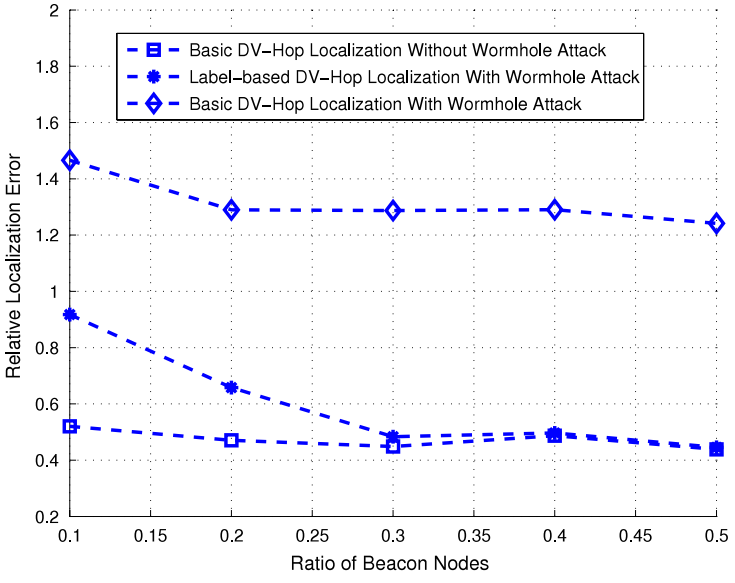


**Fig. 6.** Comparison of the relative localization error.

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 radii 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 radii.

## Acknowledgments

This work was supported in part by NSFC grants (Nos. 61309023, 61272463, and 61273079), Shandong Provincial Natural Science Foundation, China (No. ZR2013FQ032), the Fundamental Research Funds for the Central Universities (No. 13CX02100A), Open Project in Zhejiang Provincial Key Lab of Intelligent Processing Research of Visual Media (No. 2012008), Hong Kong GRF grants (PolyU-524308, and PolyU-521312), HKPU grants (A-PL16, and A-PL84), and State Key Laboratory of Industrial Control Technology (Nos. ICT1206 and ICT1207).

Please cite this article in press as: H. Chen, et al., Securing DV-Hop localization against wormhole attacks in wireless sensor networks, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.01.007

## References

[1] N. Bulusu, J. Heidemann, D. Estrin, GPS-less low cost outdoor localization for very small devices, vol. 7, 2000, pp. 28–34.
[2] T. He, C. Huang, B. Blum, J.A. Stankovic, T. Abdelzaher, Range-free localization schemes for large scale sensor networks, in: Proc. of ACM MOBICOM, 2003, pp. 81–95.
[3] D. Niculescu, B. Nath, Ad hoc positioning system (APS) using AOA, in: Proc. of IEEE INFOCOM, 2003.
[4] S. Capkun, M. Cagalj, M. Srivastava, Secure localization with hidden and mobile base stations, in: Proc. of IEEE INFOCOM, 2006.
[5] A. Boukerche, H.A.B.F. Oliveira, E.F. Nakamura, A.A.F. Loureiro, Secure localization algorithms for wireless sensor networks, IEEE Commun. Mag. (2008) 96–101.
[6] D. Liu, P. Ning, W. Du, Attack-resistant location estimation in sensor networks, in: Proc. of IEEE IPSN, 2005.
[7] S. Capkun, J.P. Hubaux, Secure positioning of wireless devices with application to sensor networks, in: Proc. of IEEE INFOCOM, 2005.
[8] F. Anjum, S. Pandey, P. Agrawal, Secure localization in sensor networks using transmission range variation, in: Proc. of IEEE MASS, 2005.
[9] H. Chen, W. Lou, J. Ma, Z. Wang, TSCD: a novel secure localization approach for wireless sensor networks, in: Proc. of the International Conference on Sensor Technologies and Applications, SensorComm, 2008.
[10] H. Chen, W. Lou, Z. Wang, A novel secure localization approach in wireless sensor networks, EURASIP J. Wirel. Comm. Netw. 2010 (2010) 12. http://dx.doi.org/10.1155/2010/981280. Article ID 981280.
[11] L. Lazos, R. Poovendran, S. Capkun, ROPE: robust position estimation in wireless sensor networks, in: Proc. of IEEE IPSN, 2005.
[12] D. Liu, P. Ning, W. Du, Detecting malicious beacon nodes for secure localization discovery in wireless sensor networks, in: Proc. of IEEE ICDCS, 2005.
[13] Z. Li, W. Trappe, Y. Zhang, B. Nath, Robust statistical methods for securing wireless localization in sensor networks, in: Proc. of IEEE IPSN, 2005.
[14] Y.C. Hu, A. Perrig, D.B. Johnson, Wormhole attacks in wireless networks, IEEE J. Sel. Areas Commun. 24 (2) (2006) 370–380.
[15] W. Wang, B. Bhargava, Visualization of wormholes in sensor networks, in: Proc. of ACM WiSec, 2004.
[16] W. Wang, A. Lu, Interactive wormhole detection and evaluation, Inf. Vis. 6 (1) (2007) 3–17.
[17] W. Wang, B. Bhargava, Y. Lu, X. Wu, Defending against wormhole attacks in mobile ad hoc networks, Wireless Commun. Mobile Comput. 6 (4) (2006) 483–503.
[18] S. Capkun, L. Buttyan, J.-P. Hubaux, SECTOR: secure tracking of node encounters in multi-hop wireless networks, in: Proc. of ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003.
[19] Y.C. Hu, A. Perrig, D.B. Johnson, Rushing attacks and defense in wireless ad hoc network routing protocols, in: Proc. of ACM workshop on Wireless Security, 2003.
[20] J. Eriksson, S. Krishnamurthy, M. Faloutsos, TrueLink: a practical countermeasure to the wormhole attack in wireless networks, in: Proc. of IEEE Internation Conference on Network Protocols, ICNP, 2006.
[21] Y. Xu, G. Chen, J. Ford, F. Makedon, Detecting wormhole attacks in wireless sensor networks, in: Proc. of IFIP, 2008.
[22] R. Maheshwari, J. Gao, S.R. Das, Detecting wormhole attacks in wireless networks using connectivity information, in: Proc. of IEEE Infocom, 2007.
[23] X. Ban, R. Sarkar, J. Gao, Local connectivity tests to identify wormholes in wireless networks, in: Proc. of ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc, 2011.
[24] D. Dong, M. Li, Y. Liu, X.Y. Li, X. Liao, Topological detection on wormholes in wireless ad hoc and sensor networks, IEEE/ACM Trans. Netw. 19 (6) (2009) 1787–1796.
[25] T. Dimitriou, A. Giannetsos, Wormholes no more? Localized wormhole detection and prevention in wireless networks, in: Proc. of the International Conference on Distributed Computing in Sensor Systems, DCOSS, 2010.
[26] L. Lazos, R. Poovendran, SeRLoc: robust localization for wireless sensor networks, ACM Trans. Sensor Netw. (2005) 73–100.
[27] L. Lazos, R. Poovendran, HiRLoc: high-resolution robust localization for wireless sensor networks, IEEE J. Sel. Areas Commun. 24 (2) (2006) 233–246.
[28] D. Liu, P. Ning, A. Liu, C. Wang, W. Du, Attack-resistant location estimation in wireless sensor networks, ACM Trans. Inf. Syst. Secur. 11 (4) (2008) 1–36.
[29] H. Chen, W. Lou, 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.
[30] H. Chen, W. Lou, X. Sun, Z. Wang, A secure localization approach against wormhole attacks using distance consistency, EURASIP J. Wirel. Comm. Netw. (2010). Special Issue on Wireless Network Algorithms, Systems, and Applications.
[31] H. Chen, W. Lou, 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.
[32] H. Chen, W. Lou, Z. Wang, Secure localization against wormhole attacks using conflicting sets, in: Proc. of IEEE International Performance Computing and Communications Conference, IPCCC, 2010.
[33] H. Chen, W. Lou, Z. Wang, On providing wormhole attack resistant localization using conflicting sets, Wireless Commun. Mobile Comput. (2014) http://dx.doi.org/10.1002/wcm.2462.
[34] K. Langendoen, N. Reijers, Distributed localization in wireless sensor networks: a quantitative comparison, Comput. Netw. (2003) 449–518.

Please cite this article in press as: H. Chen, et al., Securing DV-Hop localization against wormhole attacks in wireless sensor networks, Pervasive and Mobile Computing (2014), http://dx.doi.org/10.1016/j.pmcj.2014.01.007