PAPER

Robust Node Positioning in Wireless Sensor Networks

Ayong YE[†a)], **Jianfeng MA**[†], **Xiaohong JIANG**[††], *Nonmembers*, *and* **Susumu HORIGUCHI**[††], *Member*

SUMMARY Secure sensor localization is a prerequisite for many sensor networks to retrieve trustworthy data. However, most of existing node positioning systems were studied in trust environment and are therefore vulnerable to malicious attacks. In this work, we develop a robust node positioning mechanism(ROPM) to protect localization techniques from position attacks. Instead of introducing countermeasures for every possible internal or external attack, our approach aims at making node positioning system attack-tolerant by removing malicious beacons. We defeat internal attackers and external attackers by applying different strategies, which not only achieves robustness to attacks but also dramatically reduces the computation overhead. Finally, we provide detailed theoretical analysis and simulations to evaluate the proposed technique.

key words: *wireless sensor networks, node localization, security*

1. Introduction

Wireless sensor networks (WSNs) have critical applications in both military and civilian operations where accurate node position information is vital [1]. Not only location-related applications such as event monitoring and target tracking require sensors' location to identify the location of an event of interest, but many network modules, such as geographical routing [2],coverage checking [3] and topology self-configuring [4], also require location information. Thus, a number of node positioning mechanisms have been proposed for WSNs in the last decade [5]–[11]. In these schemes, the reference points of localization are some special nodes, called beacon node, which are assumed to know their own locations. By observing signals between beacon nodes and sensor nodes, positioning system then can determine the location of sensor nodes using various mathematical solutions.

However, the possible node compromises and the fact that localization relies on certain physical features make most of the existing ranging and positioning techniques vulnerable to attacks. Recently, a number of schemes have been proposed to protect node positioning in WSNs [12]–[19]. A secure range-independent localization scheme (SeRLoc) proposed in [12] uses communication range constraint to determine sensors' location even in presence of attacks. Capkun et al. [13] proposed a technique named verifiable multilateration (VM) to verify positions of the nodes, which relies on distance-bounding protocol. Lazos et al. [14] proposed a hybrid algorithm named ROPE for robust sensor localization and verification of sensor location claims, which is an extension of SeRLoc and VM. Farooq Anjum et al. [15] presented a secure localization algorithm which based on the transmission of nonce at different power levels. However, all above mentioned schemes are vulnerable to compromised attacks. Also, the SeRLoc, VM and ROPE schemes all rely on special hardware to work (like the directional antennas or nanosecond processing hardware). In [16], Liu et al. proposed two methods, which respectively bases on robust statistical method and vote method, to compute the position of sensors using a consistent set of beacon. Li et al. [17] introduced the least median squares (LMS) technique to filter out the outliers in the sample set. However, these two schemes all rely on robust algorithm, which requires higher computational cost. An approach proposed in [18] uses hidden or mobile base stations for secure localization. In [19], the authors introduced a suite of techniques based on intrusion detection method to detect compromised beacon nodes. However, the source node will be identified as villain and revoked from networks, if its beacon is modified by external attacks.

In this work, we focus on robust against internal and external attacks. Rather than introducing countermeasures for every possible attack, our approach is to provide node positioning system more resilience to attacks by removing malicious beacons. To mislead a sensor node about its location, both internal attacks and external attacks must induce inconsistency between claimed position and computed position of a beacon, or between the malicious beacons and the benign ones. To exploit this observation, we first develop a distributed watchdog method to detect malicious beacons by examining the inconsistency within a beacon, which can effectively defense external attacks with a lower computational cost. To defense internal attacks, this paper also proposes a region-vote algorithm to revoke malicious beacons by examining the inconsistency among beacons. We defeat internal attackers and external attackers by applying different strategy, which not only achieves robustness to attacks but dramatically reduces the computation overhead of sensor nodes.

The rest of the paper is organized as follows. The next section discusses the preliminaries work. Section 3 describes our technique in detailed, and show how our propos-

Manuscript received June 16, 2008.
Manuscript revised November 10, 2008.

[†]The authors are with the Key Lab. of the Ministry of Education for Computer Networks and Information Security, Xidian University, Xi'an, P.R. China. A. Ye is also with the Fujian Normal University, Fuzhou, P.R. China.

[††]The authors are with the Graduate School of Information Sciences, Tohoku University, Sendai-shi, 980-8579 Japan.

a) E-mail: yay@fjnu.edu.cn

DOI: 10.1587/transcom.E92.B.2023

als can be used to secure node-centric localization systems. We respectively evaluate the performance of our scheme by theoretical analysis in Sect. 4 and by simulations in Sect. 5. Finally, we conclude the paper in Sect. 6

2. Preliminaries

2.1 System Model and Assumptions

Our system consists of a set of sensor nodes with unknown location and a set of beacon nodes with known location. If two nodes reside within the power range of each other, they are considered neighbors. We assume the sensor nodes can measure the distance to the beacon nodes by observing some basic properties of beacon signals transmission, and determine their positions using multilateration algorithm. We also assume that all communications between legitimate nodes are encrypted with a network-wide group key, in order to allow promiscuous observation in the networks, while preventing outsiders from overhearing. We further assume all network nodes are deployed randomly within a target area.

2.2 Attacker Model

We observe two types of attackers: internal attackers and external attackers. Internal attackers can authenticate themselves to other nodes. We assume when a node is compromised, its secret keys that share with other nodes are known to the attacker.

An internal attacker may report false beacon, including false position or false distance, in order to mislead the location estimation at sensor nodes. Moreover, multiple internal attackers may collude together to make the malicious beacons appear to be consistent. By consistent we mean all these beacons are referring to a false position. However, we assume innocent nodes are always the majority in a local area.

An external attacker can modify the measured positions and distances of benign nodes by applying node displacing or signal interfering. Obviously, physical displacement of node is a direct threat to WSNs. Moreover, since different positioning and ranging techniques are built upon measurement of some basic properties of beacon signals, such as time of flight, signal strength, angle of arrival, hop counts and region inclusion, an external attacker can change those measurements by appropriately modifying their ranging communication. These external threats we identify are directed against the measurement process and primarily non-cryptographic attacks. Consequently, traditional security services such as encryption and authentication are not sufficient to defend against external attackers. As illustrated in Fig. 1, an attacker may speedup the signals by exploiting difference in propagation speeds (Fig. 1(a)), or delay the signals by jamming and replaying (Fig. 1(b)), or enlarge radio region by wormhole (Fig. 1(c)).

2.3 Security Mechanisms

Our scheme is enforced with an authentication mechanism enables node to authenticate the source of the beacons from neighbors. Initially, the key setup server generates a unique password pw_b and a one way key chain $< k_b^0, k_b^1, \ldots, k_b^n >=< pw_b, h(pw_b), \ldots, h^n(pw_b) >$ for each beacon node b. The key chain is computed by iteratively applying the one-way function h, such as SHA-1. The value of n is determined by the number of packets each beacon node transmits. Before node deployment, the key setup server preloads a table containing the ID and corresponding k_b^n of each beacon node b to each node. Since the number of beacon nodes in WSNs is far smaller than that of sensor nodes, so the memory of the sensor node is usually sufficient to store the ID and k_b^n of each beacon node b. For example, for a WSN with 100 beacon nodes and 1000 sensor nodes, we need 16 bits to represent node ID and 128 bits to represent a hash value. Hence the storage requirement of the hash table at each node is only 1.8 Kbytes, while the MICA2 motes have 128 Kbytes of programmable flash memory. Thus, the above key preload is practical. In the positioning phase, each beacon node b appends k_b^{n-j} and the index j into its *j-th* beacon. To authenticate a beacon, every receiver hashes the received key to verify that $h(k_b^{n-j}) = k_b^{n-j+1}$, where k_b^{n-j+1} is the current key of node b in receiver and k_b^{n-j} is the authentication code in received beacon. If the verification is correct, the receiver accepts the beacon, replaces k_b^{n-j+1} with k_b^{n-j} in its memory, and increases the hash counter by one. In case of losing of some intermediate packets, the hash counter facilitates the synchronization with the latest published key. For

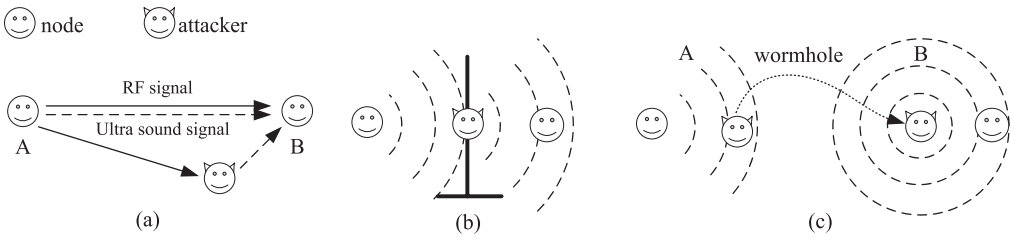

Fig. 1 External attacks: (a) Since US (Ultrasound) signal is slower than RF signal, an attacker located near the target may hear the RF signal and then transmit an US signal that would arrive before the original. (b) The attacker jams the original communication and replays them later. (c) An attacker records beacons in area A, and rebroadcasts them in area B through the wormhole link.

example, if the latest received beacon contains (k_b^i, i) and the current key of node b in receiver is (k_b^j, j). If some intermediate beacons are lost, the receiver can authenticate the lastest received beacon by verifying $\overbrace{h \ldots h}^{i-j}(k_b^j) = k_b^i$ and replaces (k_b^j, j) with (k_b^i, i) in its memory.

3. A Robust Node Positioning Mechanism

Both internal attackers and external attackers mislead the node localization by introducing malicious beacons. In this section, we describe a hybrid approach to detect and remove malicious beacons in node-centric positioning systems. Unlike the existing algorithms [16], [19], this approach detects malicious beacons by checking both internal inconsistency and external inconsistency, without centralized management, heavyweight protocol and vulnerability to false accusation attack.

3.1 A Watchdog for Malicious Beacon

In WSNs, due to the promiscuity of broadcast transmissions and the group key technique, a beacon node can overhear the responses of neighbor. With known location, a beacon node can check whether the measurements derived from a heard beacon satisfy with its claimed location or not. Unlike the developed algorithm [19], our watchdog detects false beacon without centralized management, wormhole detector and locally replaying detector. Figure 2 illustrates the basic idea of the watchdog. The detecting node, a beacon node in WSNs, is positioned at (x_c, y_c), the claimed position in its beacon is (x_b, y_b) and the measured distance from detecting node to source node is $D_{measure}$. Then, a benign beacon must satisfy the following relation:

$$|\sqrt{(x_c - x_b)^2 + (y_c - y_b)^2} - D_{measure}| \le e_{max} \quad (1)$$

Here, e_{max} is the maximum measurement error. Supposed the measurement error obeys $N(0, \sigma^2)$, we can let $e_{max} = 3\sigma$, then, the probability of false positive is small as 0.0026, following to the 3-σ principle.

In our watchdog protocol, whenever a beacon is detected to be malicious, the detecting node may report an alert against it to sensor node of concern. Every sensor node maintains an alert counter for each received beacon, which records the suspiciousness of this beacon. Those beacon, whose alert count are less a threshold τ, will be considered as a secure one. The threshold τ will be discussed in Sect. 4.

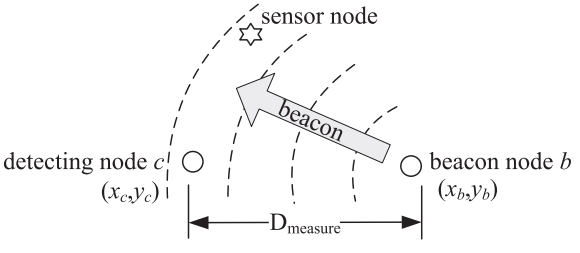

Fig. 2 Detection malicious beacon.

3.2 A Region-Vote Algorithm

The watchdog method can effectively detect the external attacks with a low computation cost, but is vulnerable to internal attacks. The compromised nodes may report false alerts against benign beacons. To copy with these internal threads, we develop a region-vote algorithm for sensor nodes to detect and remove malicious beacons by examining the external inconsistency. In this algorithm, we have each beacon "vote" on the locations at which the sensor node of concern may reside, then select the location with the highest ballot to verify whether each suspicional beacon is malicious or not. To facilitate the voting process, we quantize the target field into a grid of cells $G_{k\times k}$. Our voting algorithm reduces storage and computation overhead by exploiting the observation of the watchdog, compared to the only previously known voting solution [16]. The algorithm is executed by sensor nodes as follows:

region-vote algorithm
BS = {all beacons that sensor node received}
BS^* = {all secure beacons in BS}
$G = \{g_{mn} | m, n = 1, \ldots, k\}$; a grid of cells
$CG = \{\emptyset\}$; set of candidate cells

1. if $BS^* \neq \emptyset$ then
   $\forall\, beacon_i \in BS^*, (x_{min}, y_{min}) \times (x_{max}, y_{max})$
   $= (x_i - d_i, y_i - d_i) \times (x_i + d_i, y_i + d_i)$
   else
   $x_{min} = \min_{beacon_i \in BS} (x_i - d_i)$, $x_{max} = \max_{beacon_i \in BS} (x_i + d_i)$
   $y_{min} = \min_{beacon_i \in BS} (y_i - d_i)$, $y_{max} = \max_{beacon_i \in BS} (y_i + d_i)$
2. quantize $(x_{min}, y_{min}) \times (x_{max}, y_{max})$ into $G_{k\times k}$
   if $BS^* = \emptyset$ then $CG = G$
   else for all $g_{mn} \in G$,
   if for all $beacon_i \in BS^*, |g_{mn} - (x_i, y_i)|_{max} \geq d_i \geq |g_{mn} - (x_i, y_i)|_{min}$ then $CG = CG \cup g_{mn}$
3. for all $cg_j \in CG$, for all $beacon_i \in BS - BS^*$,
   if $|cg_j - (x_i, y_i)|_{max} \geq d_i \geq |cg_j - (x_i, y_i)|_{min}$
   then $vote(cg_j)$++
   select cg with the largest number of votes
   for all $beacon_i \in BS - BS^*$,
   if $|cg - (x_i, y_i)|_{max} \geq d_i \geq |cg - (x_i, y_i)|_{min}$
   then $BS^* = BS^* \cup beacon_i$

Here, $vote(x)$ denotes the number of votes cell x received. Secure beacons studied here are those whose alert count, the observation result of watchdogs, are less a threshold τ. The algorithm is executed in three phases: (1) To reduce storage and computation overhead, sensor node first determines an approximate search area $(x_{min}, y_{min}) \times (x_{max}, y_{max})$ it located, basing on the coordinates of the beacons heard. Here, (x_i, y_i) is the claimed coordinate of $beacon_i$, and d_i is the measured distance. (2) Sensor node quantizes the search area into a grid of cells, and chooses those cells, which are overlapped with all secure beacons, as candidate cells. The beacon $beacon_i$ does not overlap with a cell g_{mn} only when $|g_{mn} - (x_i, y_i)|_{max} \geq d_i \geq |g_{mn} - (x_i, y_i)|_{min}$,

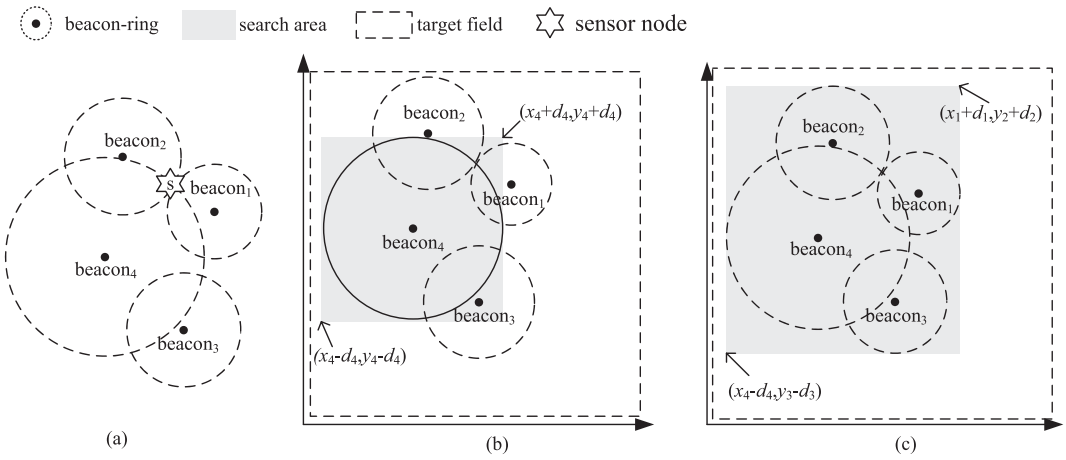

Fig. 3 (a) Sensor node s receives $beacon_1 \sim beacon_4$. (b) Step 1: Determination of the search area, assuming $beacon_4$ is detected to be secure. (c) Assuming no beacon is secure.

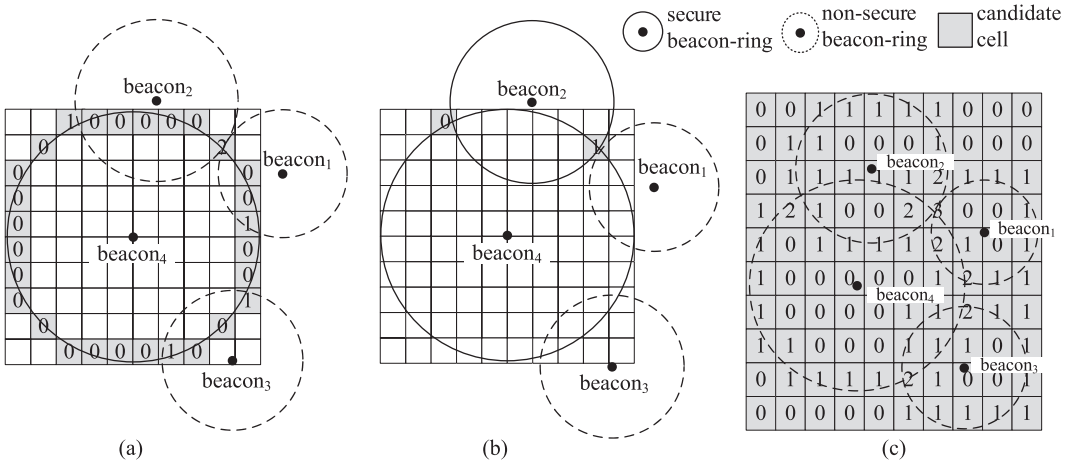

Fig. 4 Illustration for Step 2 and Step 3. (a) Case 1: only $beacon_4$ is secure. (b) Case 2: both $beacon_4$ and $beacon_2$ are secure. (c) Case 3: no beacon is secure.

where $|g_{mn} - (x_i, y_i)|_{min}$ and $|g_{mn} - (x_i, y_i)|_{max}$ are minimum and maximum distance from the cell to point (x_i, y_i), respectively. The value of k determines the dimension of the search area. In order to distinguish between malicious beacon and benign one, the size of cell may match up to e_{max}. Hence, we simply let $k = max(x_{max} - x_{min}, y_{max} - y_{min})/e_{max}$. (3) Sensor node determines the verifiable cell cg using a majority vote scheme, and add those beacons, which are overlapped with cg, to BS^*. The region-vote algorithm is illustrated in Figs. 3 and 4.

In Fig. 3(a), sensor s receives $beacon_1 \sim beacon_4$. For a benign location reference$<x, y, d>$ derived from beacon, the node of concern must be in a ring centered at (x, y) with the radius d. For the sake of presentation, we refer to such a beacon as a ring. Observe in Fig. 3(b) that if $beacon_4$ is detected to be secure by watchdog, s must be located at the ring of $beacon_4$. Hence, search area=$(x_4 - d_4, y_4 - d_4) \times (x_4+d_4, y_4+d_4)$. In Figure 3(c), $BS^*=\phi$, thus, search area=$(x_4 - d_4, y_3 - d_3) \times (x_1+d_1, y_2+d_2)$. Figure 4 illustrates the idea of vote scheme by three examples. In Fig. 4(a), being $BS^*=\{beacon_4\}$, CG={all cells which are overlapped with $beacon_4$}. Since $g_{(2,9)}$ is overlapped with both $beacon_2$ and $beacon_1$ and received a majority of 2 votes, $cg=g_{(2,9)}$. In Figure 4(b), $BS^*=\{beacon_2, beacon_4\}$, hence, CG=$\{g_{(1,3)}, g_{(2,9)}\}$ and $cg=g_{(2,9)}$. In Fig. 4(c), $BS^*=\phi$, hence, CG={all cells} and $cg=g_{(4,7)}$.

3.3 Robust Localization in Node-Centric System

In this subsection, we show how the watchdog and region-vote algorithm can be together used to secure positioning in node-centric positioning system in WSNs. Our protocol is executed as follows:

1. s→ ∗: positioning requisition
2. $\{b|b \in N(s)\} \rightarrow s : beacon_b^j = \{b, p_b, h^{n-j}(pw_b), j\}$
3. $\{w|w \in N(s) \cap N(b)\}$: overhear $beacon_b^j$
   measures D_m with ranging techniques
   if $|\sqrt{(x_w - x_b)^2 + (y_w - y_b)^2} - D_m| > e_{max}$
   then $w \rightarrow s : alert_w^i = \{w, beacon_b^j, h^{n-i}(pw_w), i\}$
4. s: receive all beacons and alerts
   define BS ={$beacon_i$: authentication code is valid}
   define AS = {$alert_i$: authentication code is valid}
   for all $alert_i \in AS$, alarm($alert_i.beacon$)++
   $BS^* = \emptyset$
   for all $beacon_j \in BS$, if alarm($beacon_j$) $\leq \tau$ then
   $BS^* = BS^* \cup beacon_j$
   if $|BS^*|$ <3 then perform region-voting algorithm
   compute p_s by MMSE with BS^*

Here, $h^{n-j}(pw_b)$ is the authentication code of the *j-th* beacon sent by node b, $N(x)$ denotes the neighbor set of node x, D_m denotes the distance from w to b, and alarm(x) denotes the alert count of beacon x. In this protocol, communications between neighbors are protected by authentication mechanism mentioned in Sect. 2. In the initial phase of the protocol, sensor node s sends a broadcast asking for localization references. Each neighbor beacon node b responses a beacon, containing its own position p_b. Another beacon node w overhearing this beacon will report an alert to s, whenever this beacon is detected to be malicious and itself is located near s. If the number of secure beacon heard is less than 3, then s further performs the region-vote algorithm to search for more secure beacons. This case happens only when the sensor node is attacked by internal attackers with false accusation. Finally, s computes its own position p_s by MMSE with BS^*.

4. Analysis

4.1 Security Analysis

Our technique detects the malicious beacons by examining the inconsistency within a beacon and the inconsistency among beacons, respectively. Although sophisticated attacker can even convince a detecting node that the malicious beacon is "internal consistent" by carefully manipulating the beacon packet. In addition, multiple attackers may collude together to make the malicious beacons appear to be "external consistent." However, in fact, the attacker can hardly conceal inconsistency within a malicious beacon from multiple detecting nodes. On the other hand, as long as the majority of beacons are benign, the external inconsistency does exist and the malicious beacons can still be detected by applying majority principle. In addition, we need to specially discuss the locally replying attack. An attacker may replay a beacon received from a neighbor beacon node b, in order to induce other detecting nodes to report alerts against this regular beacon. However, the direct beacon will reach receiver earlier than any replay, and the receiver will acquire the latest published key of b. Hence, any replayed beacon containing an outdated published key will not be authenticated.

False accusation attack is directly against our defense scheme. A compromised beacon node may directly report false alerts against benign beacons, or perform false accusation attack by tampering a previously captured alert whose published key is fresh to the sensor node of concern. These threads, however, can not disturb our scheme to a great extent. To successfully persuade a sensor node to mistreat a benign beacon, the attacker need to compromise τ+1 beacon nodes, or capture τ+1 alerts whose published key is fresh. Even if all innocent beacons are mistreated, the sensor node also can acquire regular beacons using the region-vote algorithm, provided that the benign beacons constitute the majority of received beacons.

4.2 Sensitivity Analysis

To evaluate the efficiency of our proposal, we analyze the detection rate that a malicious beacon being detected by the target sensor node, through using the watchdog mechanism or the region-vote algorithm. For simplicity, we denote the sensor node as SN, and the beacon node as BN. We assume that there are n benign BNs and m compromised BNs in the vicinity of an SN.

A malicious beacon will certainly be detected by the SN with the help of the watchdog mechanism only if its alert-counts is greater than τ. Therefore, the detection rate[†] p_w of the watchdog mechanism equals the probability that there are more than τ benign BNs reside within the SN's vicinity and overhear the malicious beacon. We assume that the BNs are deployed randomly within a target field. The random deployment of the nodes with a density p_b can be modeled as a spatial homogeneous Poisson point process of rate p_b [20]. The probability that there are at least k nodes deployed within an area of size A, is given by the Poisson distribution:

$$P(N \geq k) = 1 - \sum_{i=0}^{i<k} \frac{(p_b \times A)^i}{i!} e^{-(p_b \times A)} \tag{2}$$

Consider any BN b reports a malicious beacon to a particular SN s. Following to Eq. (2), then the detection rate p_w of this malicious beacon is given by:

$$p_w = P(|N| > \tau) = 1 - \sum_{i=0}^{\tau} \frac{(p_b \times A)^i}{i!} e^{-(p_b \times A)} \tag{3}$$

$$A = 2\left[r^2 \arccos\left(\frac{d}{r}\right) - d\sqrt{(r^2 - d^2)}\right], d = \frac{|s-b|}{2} \tag{4}$$

Where, r is the transmission range of BN, p_b is the BNs' density and A is size of the intersection area of SN's vicinity and source BN's vicinity. Figure 5 shows the p_w as a

[†]The detection rate studied here is the probability that a malicious beacon can be detected by the SN when applying a detection mechanism.

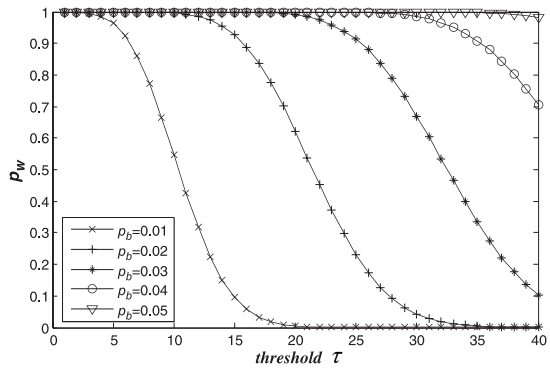

Fig. 5 Probability of a malicious beacon being identified as a non-secure one by the watchdog mechanism, assuming $|BN - SN| = r = 30\,m$.

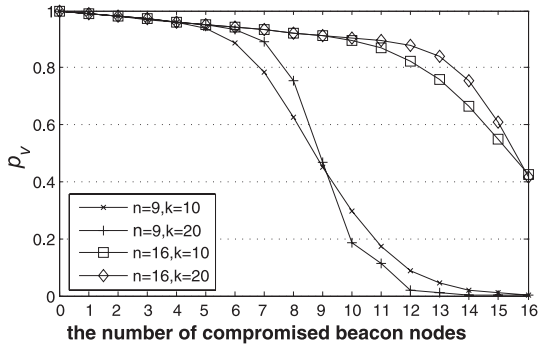

Fig. 6 Probability of a malicious beacon being detected by the region-vote algorithm.

function of τ and p_b when $|s-b| = r$. We observe that the p_w increases with the increase of densities p_b and the decrease of τ. This figure gives a way to set threshold τ to meet the security requirement of different application. For example, for $p_w = 0.99$, we can choose $\tau = 5$ when $p_b = 0.01$, and choose $\tau = 11$ when $p_b = 0.02$.

The malicious beacon will certainly be detected by the SN using region-vote algorithm, only if it can correctly select the verifiable cell cg. Therefore, the detection rate p_v of the region-vote algorithm equals the probability that the number of votes the correct cell received is more than any certain error cell received. A beacon may vote for multiple cells since it can overlap with multiple cells. Without any loss of generality, we assume that the beacon votes uniformly on the cell, except that the benign beacons must vote on the correct cell and the malicious beacons in collusion must vote on a certain error cell. Hence, the detection rate of the region-vote algorithm is given by:

$$\begin{aligned} p_v &= \sum_{i=n}^{m+n}\left(prob(\xi{=}\mathrm{i})\sum_{j=m}^{i-1} prob(\xi = j)\right) \\ &= \sum_{i=0}^{m}\left(prob(\xi{=}\mathrm{i})\sum_{j=0}^{n+i-m-1} prob(\xi = j)\right) \\ &= \sum_{i=0}^{m}\binom{m}{i}p_c^i(1-p_c)^{m-i}\sum_{j=0}^{n+i-m-1}\binom{n}{j}p_c^i(1-p_c)^{n-j} \quad (5) \end{aligned}$$

Here, $prob(\xi = x)$ is the probability that the number of votes a certain cell received is exactly equal to x. The random vote process can be modeled as a binomial distribution of p_c. Here, p_c is the probability that a random beacon exactly overlaps with a particular cell. Since the number of cells is k^2 and the total number of votes cast by a given beacon ranged from 1 to $2k$, then $\frac{1}{k^2} \le p_c \le \frac{2}{k}$.

Figure 6 shows the p_v as a function of n, m and k. To test the resistance of our scheme to attacks in the worst-case scenario, we assume $p_c = 2/k$. We can see that p_v under different choice of n and k decrease with the increase of m. We note that p_v can remain at high level when there are only small numbers of compromised BNs. However, when compromised beacons constitute the majority of beacon, p_v begins to drop dramatically decrease. This is because after malicious beacons carry the majority, the region-vote algorithm based on majority principle is failed.

The sensor node can correctly determine its location only if there is no false information in its localization reference. Thus, it is necessary to study the likeliness $p_{success}$ that an SN succeeds in removing all malicious beacons in the presence of attacks. We assume that the SN receives m malicious beacons. Thus, the probability that all the m malicious beacons can be detected by the watchdog mechanism equals $(p_w)^m$. After the above analysis, we can theoretically compute the $p_{success}$ as follows:

$$p_{success} = \begin{cases} (p_w)^m & \{\text{without voting process}\} \\ (p_w)^m \times p_v & \{\text{otherwise}\} \end{cases} \quad (6)$$

5. Simulation Evaluation

This section presents the simulation results for ROPM. The evaluation focuses on the detection rate and the overhead. The detection rate we concern is the ratio of the number of trials which succeed in removing all malicious beacons, to total trial counts. The overhead we concern is the average number of grid-beacon tests the SN operates in each trial. We evaluate the effect of the number of compromised beacon nodes on the performance, and the effect of the grid resolution.

5.1 Description of Simulation Method

We use the simulation programs run in matlab to evaluate the performance of ROPM in an idealized network environment. In all simulations, a set of benign BNs and a few malicious BNs are uniformly deployed in a 40 m × 40 m target field. The SN is located at the center of the target field. We assume the maximum communication range of node is 30 m, so that the SN can hear all BNs. We also assume the ranging error is Gaussian *error* $N(0, \sigma^2)$. Two attack scenarios are considered: internal attacks and external attacks. In internal attacks mode, the malicious BNs reports alert against all benign beacons and collude together to report false beacons which refer to a same error location. In external attacks

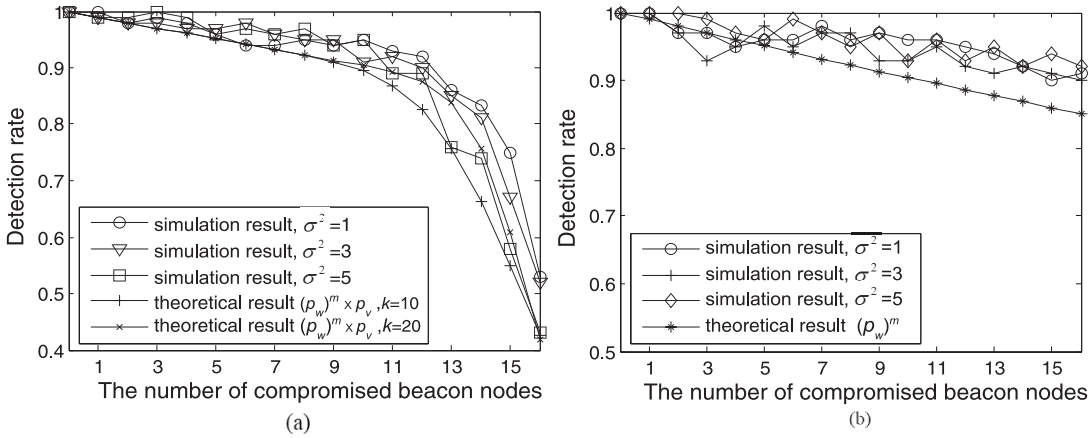

Fig. 7 Detection rate, assuming $n = 16$, $\tau = 5$. (a) Internal attack model; (b) External attack model.

mode, the malicious BNs randomly declare wrong beacons, since external attackers unable to report alert against other beacon and precisely tamper the measurements of SNs.

5.2 Detection Rate

Figure 7 shows the detection rate when $\tau = 5$ and the number n of benign BNs is 16 (thus, $p_b = \frac{16}{40\times40} = 0.01$). The results conform to the theoretical analysis. We can see the decrease in the detection rate when m increases in different attack scenarios. We note that the simulation results are close to the theoretical results of p_w in external attack scenario. In this case, $p_w = 0.99$ given $\tau = 5$ and $P_b = 0.01$. We also note that the simulation results are better than theoretical results of p_v in the internal attack scenario. This is because our theoretical analysis always takes the worst-case scenario into account. In practice, the region-vote process isn't necessary and p_c may less than 2/k. We further note that the detection rate decreases with the increase of σ^2 in external attack scenario. This is because the resolution of grid is higher with a smaller σ^2, and correct cell in the grid then has a higher chance of being selected as the verifiable cell when $n > m$.

5.3 Computation Overhead

Figure 8 shows the effect of m and σ^2 on the computation overhead. We can see that the overheads in external attack model are equal to zero. This is because our scheme detects external attack only by examining the internal inconsistency. We also can see that the overheads under different choice of σ^2 are close to zero at the beginning in internal attack model. However, with m increasing further, the overheads begin to increase dramatically. When m reaches a certain large point (close to 16), the overheads finally remain at a certain level. This is because when there are only small number of compromised BNs in networks, the SN always can acquire enough secure beacons to localization itself without performing the region-vote process, and after the number of compromised BNs reaches a certain point, the probability of the SN performing the vote process finally remains at the highest level (100%). We also can see that the more the σ^2 is, the less the overhead will be. Obviously, this is because the overhead is larger with more cells.

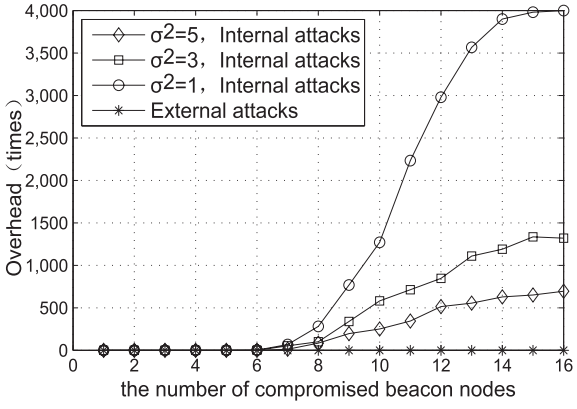

Fig. 8 The overhead.

6. Conclusion

In this work, we propose a robust node positioning mechanism (ROPM) to protect localization techniques from attacks by removing malicious beacon. The proposed technique can be applied to most of the existing range-dependent node localization system. The detail contributions of this paper are as follows. We proposed a viewpoint that instead of revoking malicious beacon nodes from networks, it is reasonable to enable sensor nodes to filter out false beacons induced by malicious attacks, without introducing countermeasure for every possible attack. We also exploit the observation, which both internal attacks and external attacks usually introduce internal inconsistency (between claimed position and computed position within a beacon) and external inconsistency (between the malicious beacons and the benign ones), to identify the malicious beacon. Furthermore, we defeat internal attacker and external attacker by applying different strategy, which not only achieves robustness to attacks but dramatically reduces the computation overhead.

Acknowledgement

These authors would like to thank the anonymous reviewers for their valuable and constructive comments. This work was supported by grants from NSF of China under Grant (No. 60633020, 60874085, 60874085), the Aviation Science Foundation of China (2007ZD31003), the Science Foundation of Fujian High University (2008F5020), and also the the State Key Lab. on Integrated Service Networks, Xidian University, China.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," Comput. Netw., vol.38, no.4, pp.393–422, 2002.
[2] J.C. Navas and T. Imielinski, "Geographic addressing and routing," Proc. MOBICOM'97, pp.66–76, Budapest, ACM, 1997.
[3] S. Meguerdichian, F. Koushanfar, M. Potkonjak, and M.B. Srivastava, "Coverage problems in wireless ad-hoc sensor networks," Proc. IEEE INFOCOM 2001, pp.1380–1387, Anchorage, IEEE Computer and Communications Societies, 2001.
[4] A. Cerpa and D. Estrin, "Ascent adaptive self-configuring sensor network topologies," ACM SIGCOMM Computer Communication Review, vol.32, no.1, p.62, 2002.
[5] N.B. Priyantha, A. Chakraborty, and H. Balakrishnan, "The cricket location-support system," Proc. 6th Annual Int'l Conf, on Mobile Computing and Networking, pp.32–43, Boston, ACM, 2000.
[6] P. Bahl and V. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," Proc. IEEE INFOCOM, pp.775–784, Tel-Aviv, IEEE, 2000.
[7] D. Nicolescu and B. Nath, "Ad-hoc positioning systems (APS)," Proc. 2001 IEEE Global Telecommunications Conf., vol.5, pp.2926–2931, San Antonio, IEEE Communications Society, 2001.
[8] D. Niculescu and B. Nath, "DV based positioning in ad hoc networks," Journal of Telecommunication Systems, vol.22, no.1/4, pp.267–280, 2003.
[9] N. Bulusu, J. Heidemann, and D. Estrin, "Gps-less low cost outdoor localization for very small devices," IEEE Pers. Commun. Mag., vol.7, no.5, pp.28–34, 2000.
[10] T. He, C.D. Huang, B.M. Blum, and T. Stankovic, "Abdelzaher. range-free localization schemes in large scale sensor networks," Proc. 9th Annual Int'l Conf. on Mobile Computing and Networking, pp.81–95, San Diego, ACM Press, 2003.
[11] L. Doherty, K.S.J. Pister, and L.E. Ghaoui, "Convex position estimation in wireless sensor networks," Proc. IEEE INFOCOM 2001, pp.1655–1663, Anchorage, IEEE Computer and Communications Societies, 2001.
[12] L. Lazos and R. Poovendran, "SeRLoc: Secure range-independent localization for wireless sensor networks," Proc. 2004 ACM Workshop on Wireless Security, pp.21–30, Philadelphia, ACM, 2004.
[13] S. Capkun and J.P. Hubaux, "Secure positioning in wireless networks," IEEE J. Sel. Areas Commun., vol.24, no.2, pp.221–232, 2006.
[14] L. Lazos, P. Radha, and S. Capkun, "ROPE: Robust position estimation in wireless sensor networks," Proc. IPSN 2005, pp.324–331, Los Angeles, IEEE Computer Society, 2005.
[15] F. Anjum, S. Pandey, and P. Agrawal, "Secure localization in sensor networks using transmission range variation," Proc. 2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems, pp.195–203, Washington, IEEE Computer Society, 2005.
[16] D. Liu, P. Ning, and W.K. Du, "Attack-resistant location estimation in sensor networks," Proc. IPSN 2005, pp.99–106, Los Angeles, IEEE Computer Society, 2005.
[17] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust statistical methods for securing wireless localization in sensor networks," Proc. IPSN 2005, pp.91–98, Los Angeles, IEEE Computer Society, 2005.
[18] S. Capkun, M. Cagalj, and M. Srivastava, "Secure localization with hidden and mobile base stations," Proc. 25th IEEE Conf. on Computer Communications, ed. J.D. Pascual and M. Smirnow, pp.23–29, Washington, IEEE Computer Society Press, 2006.
[19] D. Liu, P. Ning, and W. Du, "Detecting malicious beacon nodes for secure location discovery in wireless sensor networks," Proc. International Conference on Distributed Computing Systems, pp.609–619, Columbus, IEEE, 2005.
[20] N.A.C. Cressie, Statistics for Spatial Data, John Wiley & Sons, New York, NY, 1993.

Ayong Ye received the M.E. degree in mathematics from FuJian Normal University (Fuzhou) in 2005. Since 1998 he has been with FuJian Normal University as a lecturer. Currently, he is Ph.D. candidate in the school of computer & Technology, Xidian University (Xi'an). His current research interests include wireless networks security, mobile Ad Hoc networks and wireless sensor networks.

Jianfeng Ma received the B.E. degree in mathematics from Shaaxi Normal University (Xi'an) in 1985, and obtained his M.E. and Ph.D. degrees in computer software and communications engineering from Xidian University (Xi'an) in 1988 and 1995 respectively. Since 1995 he has been with Xidian University as a lecturer, associate professor and professor. From 1999 to 2001, he was with Nanyang Technological University of Singapore as a research fellow. Currently, Prof. Ma is the director of the Ministry of Education Key Laboratory of Computer Networks and Information Security, and he is the dean of the school of computer of Xidian University. His research interests include information security, coding theory and cryptography.

Xiaohong Jiang received his B.S., M.S. and Ph.D. degrees in 1989, 1992, and 1999 respectively, all from Xidian University, Xi'an, China. He is currently an Associate Professor in the Department of Computer Science, Graduate School of Information Science, TOHOKU University, Japan. Before joining TOHOKU University, Dr. Jiang was an assistant professor in the Graduate School of Information Science, Japan Advanced Institute of Science and Technology (JAIST), from Oct. 2001 to Jan. 2005. Dr. Jiang was a JSPS (Japan Society for the Promotion of Science) postdoctoral research fellow at JAIST from Oct. 1999–Oct. 2001. He was a research associate in the Department of Electronics and Electrical Engineering, the University of Edinburgh from March 1999–Oct. 1999. Dr. Jiang's research interests include optical switching networks, routers, network coding, WDM networks, VoIP, interconnection networks, IC yield modeling, timing analysis of digital circuits, clock distribution and fault-tolerant technologies for VLSI/WSI. He has published over 120 referred technical papers in these areas. He is a member of IEEE.

Susumu Horiguchi received the B.Eng. the M.Eng. and Ph.D. degrees from Tohoku University in 1976, 1978 and 1981 respectively. He is currently a Full Professor in the Graduate School of Information Sciences, Tohoku University. He was a visiting scientist at the IBM Thomas J. Watson Research Center from 1986 to 1987. He was also a professor in the Graduate School of Information Science, JAIST (Japan Advanced Institute of Science and Technology). He has been involved in organizing international workshops, symposia and conferences sponsored by the IEEE, IEICE, IASTED and IPS. He has published over 150 papers technical papers on optical networks, interconnection networks, parallel algorithms, high performance computer architectures and VLSI/WSI architectures. Prof. Horiguchi is members of IPS and IASTED.