Noname manuscript No.
(will be inserted by the editor)

Secure Localization and Location Verification in Wireless Sensor Networks: A Survey

**Yingpei Zeng · Jiannong Cao ·
Jue Hong · Shigeng Zhang · Li Xie**

Received: date / Accepted: date

Abstract The locations of sensor nodes are very important to many wireless sensor networks (WSNs). When WSNs are deployed in hostile environments, two issues about sensors' locations need to be considered. First, attackers may attack the localization process to make estimated locations incorrect. Second, since sensor nodes may be compromised, the base station (BS) may not trust the locations reported by sensor nodes. Researchers have proposed two techniques, secure localization and location verification, to solve these two issues respectively. In this paper, we present a survey of current work on both secure localization and location verification. We first describe the attacks against localization and location verification, and then we classify and describe existing solutions. We also implement typical secure localization algorithms of one popular category and study their performance by simulations.

Keywords Secure localization · Location verification · Wireless sensor networks · Computer network security

Y. Zeng · J. Hong · L. Xie
State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, P.R. China
E-mail: zyp@dislab.nju.edu.cn

J. Cao
Department of Computing, Hong Kong Polytechnic University, Hong Kong
E-mail: csjcao@comp.polyu.edu.hk

J. Hong
E-mail: jhong@dislab.nju.edu.cn

S. Zhang
Department of Computer Science, Central South University, Changsha 410083, P.R. China
E-mail: sgzhang@mail.csu.edu.cn

L. Xie
E-mail: xieli@nju.edu.cn

1 Introduction

Wireless sensor networks (WSNs) are composed of small, low cost, and low power sensor nodes [1]. WSNs are expected to be widely used in different applications, e.g., environmental applications like volcano monitoring, and military applications like battlefield surveillance [1]. In most of the applications, WSNs are deployed in unattended (even hostile) environments, where we must consider security issues to ensure the operations of WSNs.

The locations of sensor nodes are very important to many WSNs. This is because first the events detected by sensor nodes usually should be bound with locations, e.g., a moving tank detected at location *loc*. Second, many network operations also depend on the locations of sensor nodes, e.g., geographic routing [23], geographic key distribution [32], and location-based authentication [44]. Now many localization algorithms for WSNs have been proposed [37, 54].

When WSNs are deployed in hostile environments, the attackers may attack the localization process to make estimated locations incorrect. They can achieve this by jamming and replaying signals [56, 20], as well as compromising some nodes [4]. Incorrect locations may lead to severe consequences, e.g., wrong military decisions on the battlefield and mistakenly granting access rights to people. Thus, it is important to ensure the correctness of sensors' locations.

We should consider the correctness of sensors' locations from two aspects. On one hand, since sensors themselves need to get their correct locations (e.g., to correctly track an object), we need secure location determination, which is called secure localization in the paper. On the other hand, the base station (BS) also needs to ensure that the sensors' locations it learns are correct (e.g., to make sure an event really happened somewhere). However, when the BS needs to learn sensors' locations from sensors (i.e., in node-centric localization as we will explain later), the sensor nodes may be compromised and they may intentionally report false locations to the BS. Thus, we need to verify the locations learnt from sensors. We call this location verification.

In this paper we survey the current work on the above two issues, secure localization and location verification. This paper is extended from a preliminary version [58]. There are several related review articles in the literature (e.g., [49, 5, 15]); however, they survey one field only (i.e., secure localization only or location verification only) and do not present any quantitative comparison. In this paper, we survey the two related fields, secure localization and location verification, with up-to-date references at the same time, to provide a more comprehensive review on the security of sensor's location. Furthermore, we provide quantitative performance comparison of typical secure localization algorithms of one popular category (i.e., the filtering method introduced later) by simulations. The results suggest that there is still room for improvement.

The rest of this paper is organized as follows. We first describe the problems that secure localization and location verification try to solve in Section 2, and review the known attacks in Section 3. Then we describe current research articles on secure localization and location verification in Section 4 and Section

5 respectively. Finally we present the conclusions and point out several open research problems in Section 6.

2 Problem statement

In this section we define the problems that secure localization and location verification try to solve.

2.1 Secure localization

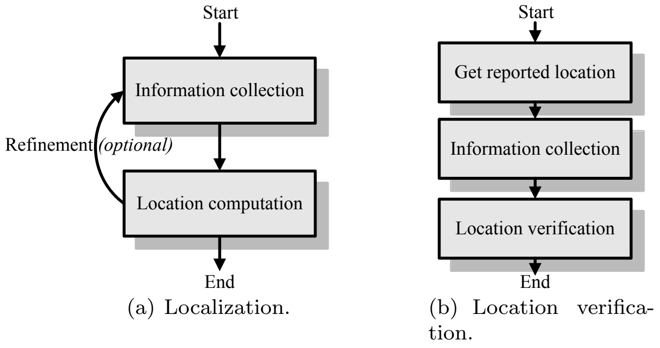
We describe localization before describing secure localization. A sensor network usually contains two kinds of nodes: common nodes and beacon nodes. Common nodes do not know their locations, and beacon nodes know their locations (e.g., by GPS). Then, the localization process is to estimate the locations of the common nodes. Such process can be divided into two steps (with an optional refinement step), as shown in Fig.1(a):

- Information collection: The information for localization is collected, which may include connectivities, distances, and angles between nodes, as well as locations of beacons and preliminary estimated locations (e.g., in [45]) of common nodes. The distances between neighbor nodes can be measured by received signal strength indicator (RSSI), time of arrival (ToA), or time difference of arrival (TDoA) [46]; the distances between multihop-away nodes can be measured by DV-hop [41] or DV-distance [41]. The angles can be measured by angle of arrival (AoA) [42].
- Location computation: Locations are computed with the collected information. Simple computation algorithms include trilateration [41], multilateration [46], and triangulation [42]. More complicated computation algorithms include MDS-MAP [48] (localizing the network as a whole), and RobustQuad [40] (coping with noisy measurements).

The optional refinement step is for iteratively computing locations. In this step the localization algorithm may collect new information (for example, in [46] localized nodes become new beacons and broadcast their locations) and may use new computation algorithms (for example, in [45, 47, 36], new algorithms are executed after obtaining nodes' coarse locations). There are several survey articles for WSN localization [26, 37, 54].

Localization systems can be classified by different methods. They can be classified into *node-centric* and *infrastructure-centric* [9, 10]. In the former sensor nodes compute their locations by themselves. In the latter the infrastructure[1] computes the locations of sensor nodes. They can also be classified into *one-hop localization* and *multi-hop localization* [37]. In the former common nodes are localized only based on one-hop neighbor beacons, whereas

[1] We refer to the infrastructure as the BS and any other nodes the BS trusts, e.g., special mobile stations [61].



(a) Localization. (b) Location verification.

Fig. 1 Localization and location verification process.

in the latter distant beacons are also used. The localization systems can also be classified into *range-based* and *range-free* [19]. In range-based systems, the distances or angles between nodes need to be measured in the information-collection step, while they do not need to be measured in range-free systems.

Secure localization (sometimes also called secure positioning [9]) is proposed to solve the vulnerabilities of current insecure localization systems [7, 27]. Most of current localization systems explicitly or implicitly assume trusted environments, in which information like distances between nodes can be obtained correctly [37]. However, in reality, the adversaries in the environments may intend to disturb the localization. The adversaries may compromise some nodes (common nodes and beacon nodes) [4], as well as intercept, jam, modify, and replay packets [56, 20]. Then the estimated locations will be seriously distorted [7, 27, 57]. Secure localization tries to solve such vulnerabilities and makes the localization process still function properly under attacks. Secure localization systems can be similarly classified (as in the above paragraph).

2.2 Location verification

The infrastructure may not trust the claimed (reported) locations of sensors in node-centric localization systems[2]. First, indeed, if a localization system is infrastructure-centric, the infrastructure will trust the estimation locations and no verification is needed, because the locations are computed by the infrastructure itself (the locations may still be incorrect due to attacks, but securing the localization process is the only thing it can do). Second, however, if a localization system is node-centric, the nodes may be compromised and may intentionally report false locations (even if their locations are obtained through secure localization). So the infrastructure may not simply trust the reported locations. An approach is to add tamper-resistant hardware at each

[2] Sensors using other sensors' locations may not trust these locations either. However, they usually trust the infrastructure. So if locations are verified by the infrastructure as later introduced, they will trust these locations.

node to make node honestly report its location; however such an approach will increase the cost of node and was also shown to be problematic in practice [2].

Thus, when localization system is node-centric, location verification is a sound method for the infrastructure to check the correctness of sensors' reported locations. In this paper such verification is called (secure) location verification[3]. In location verification, a sensor node to be verified usually is called the *prover* and the infrastructure executing the verification is called the *verifier* [6]. The verification process can be divided into three steps as shown in Fig.1(b): 1) get reported location from the prover, 2) information collection (for example, the information may be distance measurement between the verifier and the prover), and 3) location verification.

3 Attacks against localization and location verification systems

In this section we discuss the possible attacks to localization and location verification systems. We note that adversaries can only attack the "information collection" step of localization system, and the "get reported location" and "information collection" steps of location verification system. This is because only in these steps the systems obtain information from the outside, and in other steps the systems only run computation at trusted places (e.g., at node itself in node-centric localization).

Then we can enumerate all the *elementary attacks* (or *meta attacks*) according to their effects. For example, if a localization system collects *range* measurements between nodes in the "information collection" step, an adversary can launch *range-change* attacks to make the system collect wrong range measurements. However, we will only list typical elementary attacks below since others are similar to deduce.

We also list some well-known *combinational attacks*, which are composed of several elementary attacks. For example, in localization, a wormhole attack [20] can make victim nodes receive non-existent beacon locations (beacon locations that they should not receive) and corresponding false range measurements. So, in effect wormhole attack can be consider as the combination of false beacon location attack and range-change attack. Combinational attacks generally are more destructive than elementary attacks since they result in more erroneous information at the same time.

3.1 Elementary attacks

We list typical elementary attacks here.

Range-change attack: In this attack an attacker changes the range or AoA measurements between nodes [12]. For example, if a measurement is

[3] We think here the word "secure" is optional, because "location verification" already implies there are adversaries, and the solutions for location verification should be secure otherwise they will be useless.

RSSI-based, the attacker can increase or decrease the compromised node's transmission power. This attack has effects on both localization and location verification systems. For example, reducing the range measurement between node A and B may distort the estimated location of B when A is a beacon, and may also make A wrongly believe that B is nearer when A is a verifier.

False beacon location attack: In this attack an attacker makes the victim node receive false beacon locations or beacon locations that should not be received by it. For example, an attacker has compromised a beacon and then he can make the beacon broadcast false location. This attack only applies to localization systems.

False reported location attack: This attack is straightforward; a malicious node reports false location, when it is asked for its location in location verification system.

3.2 Combinational attacks

We list typical combinational attacks here.

Impersonation: In this attack an attacker impersonates other nodes in the network. For example, in localization systems, an attacker may impersonate beacon nodes to broadcast false locations and induce false range measurements (e.g., by increasing transmission power), and in location verification systems, an attacker may impersonate a victim node to make verifiers believe that the node is at the attacker's location. This attack can be defeated by authentication.

Wormhole attack: In this attack an attacker records packets at one location in the network, tunnels them to another location, and replays them [20]. The replay attack described in [33] can be considered as a zero-length-wormhole attack. In localization systems, wormhole attack will make the beacons on one side appear on another side and make the collected information erroneous. In location verification systems, an attacker may tunnel the packets of a prover to another location and make verifiers believe that the prover is at the false location.

Sybil attack: In this attack an attacker has obtained several node identities, and then he can make one compromised node masquerade as several nodes at the same time. For example, in localization systems, one compromised node may masquerade as several beacons (their identities are compromised by the attacker), and sends false locations as well as induces false range measurements. We only consider this attack in localization systems.

Location-reference attack: This attack is against some localization systems, in which each common node gets a location-reference set[4] for localization (e.g., in [46, 41, 45]), and the attack is to change a subset of location references [34]. According to the smart level, the attack can be classified into three

[4] The set can be denoted as $\{<loc_i, d_i> \mid 1 \leq i \leq n\}$, where loc_i, d_i, and n are the location of the i beacon, the distance between the beacon and the common node, and the total number of heard beacons respectively. Location reference $<loc_i, d_i>$ corresponds to beacon i.

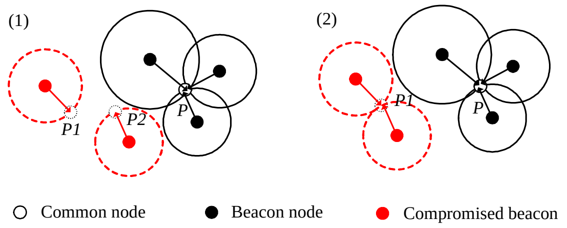


Fig. 2 Three types of location-reference attacks: (1) uncoordinated, (2) collusion, and (3) pollution attacks. In the figure only P is the real location of the common node.

types: *uncoordinated attack*, *collusion attack*, and *pollution attack*. Exemplary scenarios are shown in Fig.2. *In uncoordinated attack*, different bad location references are to mislead the common node to different false locations, e.g., $P1$ and $P2$ in the figure. *In collusion attack*, all bad location references are to mislead the common node to the same randomly chosen false location. This attack is more powerful, but it is still can be defeated when normal location references are in the majority [31]. *In pollution attack*, all bad location references are to mislead the common node, to a specially chosen false location which still conforms to some normal location references. This attack may succeed even when normal location references are in the majority [60]. We will study the localization errors of several secure localization algorithms under the three attacks later in Section 4.3.

4 Solutions for secure localization

Many secure localization systems have been proposed. As we mentioned they can be classified into two types, node-centric and infrastructure-centric.

Based on their design goals, existing solutions can be further classified into three methods: 1) *the prevention method*, to prevent the adversaries from producing erroneous information, 2) *the detection method*, to detect and revoke the nodes producing erroneous information, and 3) *the filtering method*, to filter the received erroneous information in the location computation step.

4.1 Node-centric secure localization

The prevention method: Researchers proposed several solutions belonging to the prevention method [27, 28, 7, 8, 29]. In SeRLoc [27], Lazos et al. used trusted nodes called locators to replace beacons. The locators are equipped with sectored antennas and have longer transmission range. When a node hears multiple locators, it computes the center of gravity of sectors corresponding to the locators as its location. They later proposed an improved method, HiRLoc [28], which achieves higher accuracy by rotating locator's antenna and varying locator's transmission power in localization.

In [7, 8], Capkun et al. proposed SPINE based on the verifiable multilateration (VM) technique introduced by them. In VM, if a node is inside a triangle formed by any three nodes with known locations, through RF-based DB (radio frequency based distance bounding) [6] the location of the node can be uniquely determined. In SPINE, all the distance measurements are verified by VM triangles formed by surrounding sensor nodes, so nodes cannot produce erroneous distance measurements.

In [29], combining the techniques in SeRLoc [27] and VM [7, 8], Lazos et al. proposed ROPE. In ROPE each node obtains its exact location by VM when it is inside at least one triangle formed by locators, or still estimates its location by center of gravity when it is not inside any triangle. In [57], Zeng et al. proposed SHOLOC to prevent the compromised nodes from reducing the hop counts in hop-count based localization algorithms. Their method is to represent the value of hop count by the number of hash operations on a nonce.

The detection method: Two solutions have been proposed in this category [33, 51, 50], and they both focus on detecting malicious beacons. In [33], Liu et al. proposed to use detecting beacons to detect malicious beacons broadcasting false locations. The detecting beacons first pretend to be common nodes and send requests to other beacons. Then they compare the distances computed by using their locations and the replied locations, with the measured distances. If the distances are inconsistent, the beacons being checked are malicious and will be revoked.

In DRBTS [51, 50], Srinivasan et al. generalized the solution of Liu et al. [33] by employing beacons to maintain reputations for their neighbor beacons. Each beacon computes reputations of its neighbor beacons based on the overheard location replies as well as the reputation values heard from other beacons. Common sensor nodes will only use beacons trusted by other beacons (i.e., such beacons' reputations are above a threshold) to compute their locations.

The filtering method: There are many algorithms belonging to this method [34, 35, 31, 53, 38, 39, 25, 62]. They all focus on filtering the bad location references in a location-reference set. In [34, 35] Liu et al. proposed ARMMSE and a voting-based algorithm (Vote). The ARMMSE is to obtain a subset of location references, which satisfies that the mean square error of the location computed by the subset is below a threshold. In Vote, the minimum rectangle covering all the location references is divided into cells, and each location reference votes to the divided cells according to its observation. Then a new rectangle is selected to cover the cells with the highest vote. If the new rectangle is smaller than the previous one, it will be further divided into cells to vote. Otherwise, the algorithm outputs the centroid of current cells with the highest vote as the estimated location.

In [31] Li et al. proposed to use LMS [43] to filter bad location references. Different from traditional methods that minimize the mean square error [46], LMS method is to minimize the median of square errors:

$$loc_0 = \arg\min_{loc_0} med_i \left[|loc_i - loc_0| - d_i \right]^2, \tag{1}$$

where loc_i and d_i are the location and distance in the i location reference respectively, and $|loc_a - loc_b|$ is the Euclidean distance between two locations loc_a and loc_b, and loc_0 is the estimated location.

In [53] Wang et al. proposed i-Multihop algorithm, which aims to filter distance measurements that are larger than or smaller than their real values. The optimization computation of i-Multihop is described as below:

$$\begin{aligned} loc_0 \; = \; & \arg\min_{loc_0} \Big(-\sum(|loc_0 - loc_i|)^2 + k\sum \varepsilon_i \Big) \\ & \text{subject to } |loc_0 - loc_i| \leq d_i + \varepsilon_i, \end{aligned} \tag{2}$$

where k is a large weight coefficient (e.g., 10^6) and ε_is are slack variables.

In [38, 39], Misra et al. proposed a method to filter compromised beacons, where distance bounding [6] is used and then attackers can only enlarge distance measurements. Their method is to compute the geometric center of the intersection of circles corresponding to location references.

In [62] Zhong et al. proved that when there are no more than $\frac{n-3}{2}$ compromised beacons (i.e., $k \leq \frac{n-3}{2}$)[5], we can definitely compute the location of node with an error bound, where n and k are the number of total and compromised beacons respectively. However, such result is proved under the condition that ϵ (i.e., the maximum measurement error) is *ideally small*; in [60] Zeng et al. showed that an adversary can still seriously distort the estimated location with pollution attack, when $k \leq \frac{n-3}{2}$ holds and ϵ is *practically small*. In [62] Zhong et al. also proposed two localization algorithms, based on finding a location inside $k + 3$ rings.

4.2 Infrastructure-centric secure localization

Infrastructure-centric localization systems usually belong to the prevention method, since they have reliable infrastructure (and without vulnerable beacon nodes). Capkun et al. [9, 10] proposed a method to localize nodes based on covert base stations (CBS). The public base station (PBS) first sends a nonce to a node. When the node replies to the nonce, all the CBS will compute its location together based on the TDoA method. Then if the actual time differences deviate from the supposed values over a threshold, an attack is detected and the estimated location is rejected.

Zhang et al. [61] proposed SLS for UWB (ultra-wideband) sensor networks. The authors assume that there is a set of trusted anchors which can perform group movement in the deployment field. In SLS, first, each anchor performs an algorithm called K-Distance to measure the distance between the anchor and the node to be localized. Second, anchors send the measured distances to the anchor leader to compute node's location. Third, SLS employs a location validity test by checking whether the computed location is inside the polygon

[5] It is equal to say that the condition $g \geq k + 3$ should hold, where g is the number of normal beacons. In [38] a similar result is proved.

formed by all the anchors. This test is similar to but more general than VM [7, 8] since polygon is not limited to triangle. He at al. [18] later proposed ESLS to improve the SLS [61] scheme in defeating distance enlargement attacks, and used Petri net to formally verify the security of ESLS.

Anjum et al. [3] proposed SLA to securely localize nodes based on transmission range (TR) variation. Here the anchors are assumed to be reliable and can vary their TRs to several values. In the localization process the BS let anchors transmit different nonces with different TRs. Each sensor then sends its received nonces to the BS. The BS computes sensors' locations based on the unique sets of nonces corresponding to different locations.

4.3 Comparison of secure localization solutions

We compare existing solutions in Table 1, showing their types, resistance to attacks, and requirements on special hardware. We can see that compared with node-centric secure localization systems, infrastructure-centric systems always need to deploy new and reliable infrastructure; however, they also have advantages, e.g., no need for location verification. Secure localization systems belonging to the prevention method usually provide higher resistance to attacks, but they usually need additional hardware as well. In contrast, secure localization systems purely following the filtering method usually do not need any additional hardware, and provide relatively lower resistance.

The three methods, prevention, detection, and filtering, are from radical to conservative, and they may operate in defend-in-depth manner. For example, a system can use prevention, detection, and filtering methods as the first, second, and last lines of defense respectively. Then, if preventing the adversaries from penetration fails, the compromised entities may still be detected and revoked in the detection defense, or the erroneous information caused by the compromised entities is filtered in the last filtering defense. Some existing systems already combine more than one method in their design [29, 28, 57].

Since there are many algorithms [34, 31, 53, 38, 25, 62] belonging to the filtering method, next we simulate to make a quantitative comparison between them. We implement six different localization algorithms: MMSE[6] [46], LMS [31], ARMMSE [34], Vote [34], i-Multihop [53], and FastHeuristic [62]. In all simulations, we randomly deploy 15 normal beacon nodes and k (k from 0 to 14 in steps of 1) malicious beacon nodes in a circular region (radius=250m). The common node to be localized is at the center of the circle. We assume the transmission range is 250m so the common node can hear all the beacons. We assume the distance measurement error follows a Normal distribution with mean 0 and variance $\frac{\epsilon}{2} = 15$m (ϵ is the maximum measurement error), similar

[6] The mean square error of the MMSE method is directly minimized by the *fminsearch* function of Matlab (this function uses the simplex search method [16]) but not the linearized MMSE method [46], because the location computed by the *fminsearch* function is more accurate [31]. To have a fair comparison, the MMSE subroutines employed by other algorithms like LMS and ARMMSE all employ the *fminsearch* function.

Table 1 Secure localization systems comparison. The fourth column represents whether a given system can defeat the known attacks against localization, where RC, FB, Im. Wo., Sy., and LR are abbreviations for range-change, false beacon location, impersonation, wormhole, sybil, and location-reference attacks respectively. "Y", "N", and "P" mean that the given system "can", "cannot" and "partially can" defeat the attacks respectively, and "-" means an attack is not applicable to the given system.

System	**Type**	**Method**	**Can defeat**						**Additional hardware**
			RC	**FB**	**Im.**	**Wo.**	**Sy.**	**LR**	
SeRLoc [27]	node-centric	prevention	-	N	Y	Y	Y	-	locators with sectored anten.
HiRLoc [28]	node-centric	prevention filtering	-	Y	Y	Y	Y	-	locators with sectored anten.
ROPE [29]	node-centric	prevention filtering	Y	Y	Y	Y	Y	-	locators with sectored anten., DB devices
SPINE [7]	node-centric	prevention	Y	-	Y	Y	Y	-	RF-based DB devices
Liu *et al.* [33]	node-centric	detection	Y	Y	Y	Y	N	N	none
DRBTS [51]	node-centric	detection	Y	Y	Y	N	N	N	none
Filtering methods [34, 31, 38, 53, 25, 62]	node-centric	filtering	P	P	Y	N	N	P	usually none, only ROSETTA [38] needs DB devices
Capkun *et al.* [9]	infra.-centric	prevention	-	-	Y	Y	-	-	PBS and CBSs
SLS [61], ESLS [18]	infra.-centric	prevention	Y	-	Y	Y	-	-	mobile anchors
SLA [3]	infra.-centric	prevention	Y	-	Y	N	-	-	reliable anchors

to the setting in [62]. We measure the localization errors of different algorithms under three kinds of location-reference attacks: uncoordinated, collusion, and pollution. All the results are the averages of 200 runs. Our simulation code is available at `http://zyingp.110mb.com/s_loc.html`.

Fig.3(a) shows the localization error under uncoordinated location-reference attack. In this simulation, the false locations of the common node (locations that the malicious beacon nodes try to mislead the common node to) are randomly selected in the circular area but are more than 150m away from the real location. We can find that MMSE, ARMMSE, and Vote have very similar localization errors when there is no bad beacon; their localization errors are also smaller than all other algorithms then. When the number of malicious beacons (k) is increased, although the localization errors of most algorithms (except FastHeuristic) are increasing, the insecure localization algorithm MMSE is the severest one (its localization error increases by nearly three times in the worst case). The increment of localization error of Vote is a bit larger than other secure localization algorithms. Among all the algorithms, FastHeuristic always has the greatest localization error. Also, its localization error decreases when k is increased. This is because it just outputs a location in the intersection of $\lfloor \frac{n-3}{2} \rfloor + 3 = \lfloor \frac{15+k-3}{2} \rfloor + 3 = \lfloor \frac{k}{2} \rfloor + 9$ rings [62], and the intersection becomes smaller and smaller when k is increased.

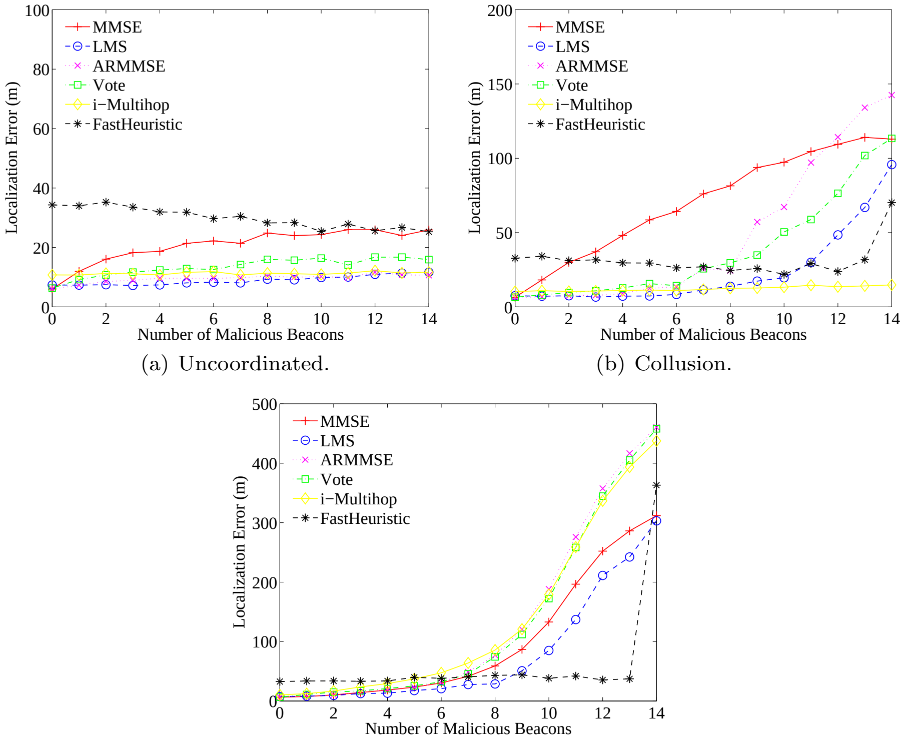
Fig.3(b) shows the localization error under collusion location-reference attack. This simulation is similar to the uncoordinated one except that all the malicious beacons choose the same false location to mislead the common node. We can see that all the algorithms perform worse now. When k is increased, the localization errors of i-Multihop and FastHeuristic are very stable, which show that they are highly resistant to the collusion attack. In contrast, the localization errors of other algorithms, especially ARMMSE, become very large when k is more than 8. This is because the collusion attack makes the false location more and more look like the real location of the common node (e.g., the mean square error at the false location is lower).

We draw the localization errors of different algorithms under pollution location-reference attack in Fig.3(c). Our current pollution strategy is designed against resilient localization algorithms (defined in [60]) such as Vote, but it also has effects on other algorithms. We can see that the localization errors of all the algorithms are larger than the corresponding errors in the case of collusion attack, because pollution attack can catch such chances that collusion attack may miss: finding out the *right* location that it can *successfully* mislead the victim node to. The localization error of FastHeuristic is still stable here, because FastHeuristic considers rings intersecting with more other rings first, which makes it not a pure resilient localization algorithm and become more resistant to current pollution strategy.

We may have two observations from the above simulations. First, we can find that from uncoordinated to pollution the three attacks are successively more powerful. However, fortunately, the adversaries must also launch them with successively higher costs. In collusion attack, compared with the case in uncoordinated attack, malicious beacons need communications to reach a consensus on the false location to mislead. To launch a pollution attack, an adversary should further know the locations of both the normal beacons and the victim common node [60]. Second, we can also find that currently the solutions that have the lowest localization error under the normal condition (i.e., MMSE, ARMMSE, and Vote), are not necessary the solutions that have the lowest localization error under attacks. It seems that current solutions still have room for improvement.

5 Solutions for location verification

Based on the goal of verification, we classify existing location-verification solutions into two types: *in-region* [6, 24, 44, 52, 29] and *single-position* [12, 9, 10,



(a) Uncoordinated.

(b) Collusion.

(c) Pollution.

Fig. 3 Localization under different location-reference attacks.

30, 13, 14, 21, 55, 11] solutions. In-region solutions try to verify that whether nodes (i.e., provers) are inside given regions (e.g., inside a cafe), and single-position solutions try to verify that whether nodes are at given positions (e.g., at loc_a =$<x_a, y_a>$).

Base on the number of nodes verified at a time, we can further classify the verification algorithms into two types: *batch verification* [21, 55] and *one-by-one verification* [6, 44, 52, 12, 9, 10, 30, 13, 14, 11]. The former verifies a batch of nodes at a time, and the latter verifies nodes one by one.

5.1 In-region verification

Currently all the solutions we know for in-region verification belong to the one-by-one verification type. Among them, two solutions are proposed based on the distance-bounding technique [6]. Brands and Chaum [6] first proposed distance bounding (DB) to make the prover (P) unable to reduce its distance to the verifier (V). The bounding process is a rapid bit-exchange process: V sends bit α_i to P, and P sends bit $\beta_i = \alpha_i \oplus m_i$ to V immediately after it receives α_i, where $\mathbf{m}$ is a bit string previously committed to V by P. After that, V can compute an upper bound on its distance to P based on the maximum of delay times between sending out a bit and receiving a bit back. The bounding using RF (radio frequency) signal requires dedicated hardware [7] (because V needs to measure the times with nanosecond precision).

In [44] Sastry et al. proposed the Echo protocol, in which each verifier is in charge of the verification of a small circular region. To verify a prover P that is inside verifier V's circular region, V sends a nonce to P *using RF* and starts the timer, and the prover P immediately echoes the nonce back *using ultrasound*. Then V can use the elapsed time to compute the distance between them. The Echo protocol is similar to the distance bounding protocol [6] but it does not require sophisticate hardware (needs no precise clock).

In [52] Vora et al. proposed a new method not based on distance bounding. They divided the verifiers into acceptors and rejectors. The acceptors are deployed inside the protected region and the rejectors are deployed at the boundary of protected region. The verification process is that the prover step by step increases its signal strength and broadcasts a signal, until a verifier hears the signal and responds. The verifiers accept the prover if none of the rejectors hears the prover during the process.

5.2 Single-position verification

Batch verification: In [55] Wei et al. proposed two algorithms, GFM and TI, to detect abnormal sensor locations. GFM first computes four matrices which represent the neighborhood observed and the neighborhood computed by estimated locations. Then it uses four metrics to measure whether the location of a node is abnormal. In TI, each node observing a node i continues giving an indicator value in respect of i (indicating whether it believes that the node i has abnormal location). TI accepts a node's location when the node's final indicator value is greater than a threshold.

In [21] Hwang et al. proposed an algorithm for detecting phantom nodes (nodes claiming false locations) in the network. Each node first creates a local map using two randomly selected neighbors. Then in such a map, the algorithm tries to find the largest consistent subset, by checking each node whether its measured ranges are consistent with its ranges in the map. The above process is repeated for given times and the largest subset in all runs is selected, which should contain all the normal nodes.

One-by-one verification: In [12] Du et al. proposed LAD, which uses deployment information to detect localization anomaly. When sensors are deployed in groups, each node is assumed to follow a two-dimensional Gaussian distribution, which is centered at the deployment point of the node's group. Then the authors proposed three metrics to detect anomaly. Take the Diff metric for example, it represents the difference between node's actual observation and expected observation (an observation is a vector $\boldsymbol{\mu}$, where μ_i represents the number of neighbors in the i group).

Table 2 Location verification systems comparison. The fourth column represents whether a given system can defeat the known attacks against location verification, where RC, FR, Im., and Wo. are abbreviations for range-change, false reported location, impersonation, and wormhole attacks respectively. "Y" and "N" mean that the given system "can", and "cannot" defeat the attacks respectively, and "-" means an attack is not applicable to the given system.

System	**Type**	**Method**	**Can defeat**				**Additional hardware**
			RC	**FR**	**Im.**	**Wo.**	
DB [6]	in-region	one-by- one	Y	Y	Y	Y	verifiers, RF-based DB devices
Echo [44]	in-region	one-by- one	Y	Y	Y	N	verifiers
Vora *et al.* [52]	in-region	one-by- one	-	Y	Y	N	verifiers (acceptors, rejectors)
GMF, TI [55]	single-pos.	batch	Y	Y	Y	N	none
Hwang *et al.* [21]	single-pos.	batch	Y	Y	Y	N	none
LAD [12]	single-pos.	one-by- one	Y	Y	Y	N	none
Capkun *et al.* [9]	single-pos.	one-by- one	Y	Y	Y	N	(PBS and CBSs) *or* (MBS)

In [9, 10] Capkun et al. proposed to use covert base stations (CBS) and mobile base station (MBS) to verify nodes' locations. In CBS case, the public base station (PBS) first sends a nonce to a node and the node replies by a RF signal and a sound signal. Then each CBS can calculate the distance between the CBS and the node. Each CBS compares the calculated distance with distance computed using node's reported location and CBS' location, and rejects the reported location if the difference is beyond a threshold. In MBS case, the MBS first requires the node to broadcast RF and sound signals after given time. After that time, MBS has moved to a different location not known by the node, and can check the reported location similarly like a CBS.

In [13, 14] Ekici et al. proposed to verify a node's location with trusted verifiers in the WSN. The node to be verified first floods its location in the network, with a hop count field. Each verifier can get both the distance and hop count between the node and verifier (a value pair). Then each verifier computes two probabilities: one represents the probability such value pair occurs with, and another represents the verifier's confidence. Finally a central node (e.g., a designated verifier) collects the information from all verifiers and decides to accept or reject the location.

5.3 Comparison of location verification solutions

We show the comparison of existing solutions in Table 2 in respect of type, resistance to attacks, and additional hardware. We can find that all the solutions can defeat the range-change, false reported location, and impersonation attacks. However, only DB [6] can defeat the wormhole attack, because it relies on the traveling time of RF signal, which cannot be reduced even by a wormhole link. Some single-position verification algorithms do not need any additional hardware [12, 21, 55]; however, in-region verification algorithms usually need additional hardware to represent the region to be protected or verified.

Which verification strategy is better (one-by-one verification or batch verification) depends on the application scenario. One-by-one verification systems usually are more energy efficient than batch verification systems when we only want to verify some critical nodes, e.g., a node which just detected and reported an important event. However batch-verification systems are more appropriate when we want to verify all the nodes at one time.

6 Conclusions and open research problems

In this paper we review secure localization and location verification for WSNs at the same time. First, we described the problems that secure localization and location verification try to solve. Then we discussed the attacks that the secure localization and location verification systems must confronted, and we classified them into two kinds of attacks, elementary attacks and combinational attacks. Finally, we described and compared typical secure localization and location verification systems. Specially, we compared the localization results of typical secure localization algorithms of one popular category by simulations, and found that currently no algorithm has the best performance both under normal condition and under attacks; existing algorithms of this category can probably be improved.

A number of research problems remain in the fields of secure localization and location verification. First, very few secure solutions exist for multihop and range-based localization systems (e.g., RobustQuad [40] and Sweep [17]). A recent work [22] is an attempt to solve the problem. Collecting information through multipath may be also a plausible way to solve it. Second, only a few research articles exist for secure localization in special WSNs, e.g., sparse WSNs [17] and mobile WSNs [59]. Third, to the best of our knowledge, no solution exists for location verification for one node at a time (i.e., one-by-one verification), without any additional infrastructure and deployment information. Possible solutions may utilize within-n-hop neighbors of a node.

Acknowledgements This work is supported in part by Hong Kong Research Grant Council under CERG grant PolyU 5102/07E, the Hong Kong Polytechnic University under the ICRG grant G-YF61, and Natural Science Foundation of China under Grant No.60673154, and Natural Science Foundation of Jiangsu Province under Grant No.BK2009465.

References

1. Akyildiz I, Su W, Sankarasubramaniam Y, Cayirci E (2002) Wireless sensor networks: a survey. Computer Networks 38(4):393–422
2. Anderson R, Kuhn M (1996) Tamper resistance - a cautionary note. In: Proceedings of the Second Usenix Workshop on Electronic Commerce
3. Anjum F, Pandey S, Agrawal P (2005) Secure localization in sensor networks using transmission range variation. In: Proceedings of MASS
4. Becher A, Benenson Z, Dornseif M (2006) Tampering with motes: Real-world physical attacks on wireless sensor networks. In: Proceedings of Third International Conference on Security in Pervasive Computing (SPC '06)
5. Boukerche A, Oliveira H, Nakamura E, Loureiro A (2008) Secure localization algorithms for wireless sensor networks. IEEE Communications Magazine 46(4):96–101
6. Brands S, Chaum D (1993) Distance-bounding protocols. In: Proceedings of EUROCRYPT
7. Capkun S, Hubaux JP (2005) Secure positioning of wireless devices with application to sensor networks. In: Proceedings of INFOCOM
8. Capkun S, Hubaux JP (2006) Secure positioning in wireless networks. IEEE J Sel Areas Commun
9. Capkun S, Cagalj M, Srivastava M (2006) Securing localization with hidden and mobile base stations. In: Proceedings of INFOCOM
10. Capkun S, Rasmussen K, Cagalj M, Srivastava M (2008) Secure location verification with hidden and mobile base stations. IEEE Trans Mobile Comput 7(4):470–483
11. Chandran N, Goyal V, Moriarty R, Ostrovsky R (2009) Position based cryptography. In: Proceedings of CRYPTO
12. Du W, Fang L, Ning P (2005) LAD: Localization anomaly detection forwireless sensor networks. In: Proceedings of IPDPS
13. Ekici E, Mcnair J, Al-Abri D (2006) A probabilistic approach to location verification in wireless sensor networks. In: Proceedings of ICC
14. Ekici E, Vural S, McNair J, Al-Abri D (2008) Secure probabilistic location verification in randomly deployed wireless sensor networks. Ad Hoc Networks 6(2):195 – 209
15. Ferreres AT, Alvarez B, Garnacho A (2008) Guaranteeing the authenticity of location information. IEEE Personal Commun Mag 7(3):72–80
16. Fletcher R (2000) Practical Methods of Optimization, 2nd edn. John Wiley & Sons
17. Goldenberg DK, Bihler P, Cao M, Fang J, Anderson BDO, Morse AS, Yang YR (2006) Localization in sparse networks using sweeps. In: Proceedings of MobiCom
18. He D, Cui L, Huang H, , Ma M (2009) Design and verification of enhanced secure localization scheme in wireless sensor networks. IEEE Trans Parallel Distrib Syst 20(7):1050–1058

19. He T, Huang C, Blum BM, Stankovic JA, Abdelzaher T (2003) Range-free localization schemes for large scale sensor networks. In: Proceedings of MobiCom
20. Hu Y, Perrig A, Johnson D (2003) Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In: Proceedings of INFOCOM
21. Hwang J, He T, Kim Y (2007) Detecting phantom nodes in wireless sensor networks. In: Proceedings of INFOCOM
22. Jian L, Yang Z, Liu Y (2010) Beyond triangle inequality: Sifting noisy and outlier distance measurements for localization. In: Proceedings of INFOCOM
23. Karp B, Kung HT (2000) GPSR: greedy perimeter stateless routing for wireless networks. In: Proceedings of MobiCom
24. Kindberg T, Zhang K, Shankar N (2002) Context authentication using constrained channels. In: Proceedings of WMCSA
25. Kiyavash N, Koushanfar F (2007) Anti-collusion position estimation in-wireless sensor networks. In: Proceedings of MASS
26. Langendoen K, Reijers N (2003) Distributed localization in wireless sensor networks: a quantitative comparison. Computer Networks 43(4):499–518
27. Lazos L, Poovendran R (2004) SeRLoc: Secure range-independent localization for wireless sensor networks. In: Proceedings of ACM WiSe
28. Lazos L, Poovendran R (2006) HiRLoc: high-resolution robust localization for wireless sensor networks. IEEE J Sel Areas Commun 24(2):233–246
29. Lazos L, Poovendran R, Capkun S (2005) ROPE: robust position estimation in wireless sensor networks. In: Proceedings of IPSN
30. Leinmuller T, Schoch E, Kargl F (2006) Position verification approaches for vehicular ad hoc networks. IEEE Wireless Communications 13(5):16–21
31. Li Z, Trappe W, Zhang Y, Nath B (2005) Robust statistical methods for securing wireless localization in sensor networks. In: Proceedings of IPSN
32. Liu D, Ning P (2003) Location-based pairwise key establishments for static sensor networks. In: Proceedings of ACM SASN
33. Liu D, Ning P, Du W (2005) Detecting malicious beacon nodes for secure location discovery in wireless sensor networks. In: Proceedings of ICDCS
34. Liu D, Ning P, Du WK (2005) Attack-resistant location estimation in sensor networks. In: Proceedings of IPSN
35. Liu D, Ning P, Liu A, Wang C, Du WK (2008) Attack-resistant location estimation in wireless sensor networks. ACM Trans Inf and Syst Security 11(4):1–39
36. Liu J, Zhang Y, Zhao F (2006) Robust distributed node localization with error management. In: Proceedings of MobiHoc
37. Mao G, Fidan B, Anderson BDO (2007) Wireless sensor network localization techniques. Comput Netw 51(10):2529–2553
38. Misra S, Bhardwaj S, Xue G (2006) ROSETTA: Robust and secure mobile target tracking in a wireless ad hoc environment. In: Proceedings of MILCOM

39. Misra S, Xue G, Bhardwaj S (2009) Secure and robust localization in a wireless ad hoc environment. IEEE Trans Veh Technol 58(3):1480–1489
40. Moore D, Leonard J, Rus D, Teller S (2004) Robust distributed network localization with noisy range measurements. In: Proceedings of SenSys
41. Niculescu D, Nath B (2001) Ad hoc positioning system (APS). In: Proceedings of IEEE GLOBECOM
42. Niculescu D, Nath B (2003) Ad hoc positioning system (aps) using aoa. In: Proceedings of INFOCOM
43. Rousseeuw P, Leroy A (2003) Robust regression and outlier detection. Wiley-Interscience
44. Sastry N, Shankar U, Wagner D (2003) Secure verification of location claims. In: Proceedings of WiSe
45. Savarese C, Rabay J (2002) Robust positioning algorithms for distributed ad-hoc wireless sensor networks. In: Proceedings of USENIX
46. Savvides A, Han CC, Srivastava M (2001) Dynamic fine-grained localization in ad-hoc networks of sensors. In: Proceedings of MobiCom
47. Savvides A, Park H, Srivastava MB (2002) The bits and flops of the n-hop multilateration primitive for node localization problems. In: Proceedings of WSNA
48. Shang Y, Ruml W, Zhang Y (2003) Localization from mere connectivity. In: Proceedings of MobiHoc
49. Srinivasan A, Wu J (2008) A Survey on Secure Localization in Wireless Sensor Networks, In: B. Furht (ed) Encyclopedia of Wireless and Mobile Communications. CRC Press
50. Srinivasan A, Teitelbaum J, Wu J (2006) Drbts: Distributed reputation-based beacon trust system. In: Proceedings of DASC
51. Srinivasan A, Wu J, Teitelbaum J (2007) Distributed reputation-based secure localization in sensor networks. Journal of Autonomic and Trusted Computing
52. Vora A, Nesterenko M (2006) Secure location verification using radio broadcast. IEEE Trans Dependable Secure Comput 3(4):377–385
53. Wang C, Xiao L (2006) Locating sensors in concave areas. In: Proceedings of INFOCOM
54. Wang C, Xiao L (2007) Sensor localization under limited measurement capabilities. IEEE Netw 21(3):16–23
55. Wei Y, Yu Z, Guan Y (2007) Location verification algorithms for wireless sensor networks. In: Proceedings of ICDCS
56. Xu W, Trappe W, Zhang Y, Wood T (2005) The feasibility of launching and detecting jamming attacks in wireless networks. In: Proceedings of MobiHoc
57. Zeng Y, Zhang S, Guo S, Li X (2007) Secure hop-count based localization in wireless sensor networks. In: Proceedings of CIS
58. Zeng Y, Cao J, Hong J, Xie L (2009) Secure localization and location verification in wireless sensor networks. In: Proceedings of TSP
59. Zeng Y, Cao J, Hong J, Zhang S, Xie L (2009) SecMCL: A secure monte carlo localization algorithm for mobile sensor networks. In: Proceedings of

WSNS

60. Zeng Y, Cao J, Zhang S, Guo S, Xie L (2009) Pollution attack: A new attack against localization in wireless sensor networks. In: Proceedings of WCNC
61. Zhang Y, Liu W, Fang Y, Wu D (2006) Secure localization and authentication in ultra-wideband sensor networks. IEEE J Sel Areas Commun 24(4):829–835
62. Zhong S, Jadliwala M, Upadhyaya S, Qiao C (2008) Towards a theory of robust localization against malicious beacon nodes. In: Proceedings of INFOCOM