Secure Localization in Wireless Sensor Networks: A Survey

(Invited Paper)

Jinfang Jiang[1,2], Guangjie Han[1,2], Chuan Zhu[1,2], Yuhui Dong[1,2], Na Zhang[1,2]
[1]Department of Information & Communication Systems, Hohai University, Changzhou, China
[2]Changzhou Key Laboratory of Sensor Networks and Environmental Sensing, Changzhou, China
Email: {jiangjinfang1989, hanguangjie, dr.river.zhu, titiyaya09, zhangna.hehai}@gmail.com

***Abstract*— Secure localization of unknown nodes in a Wireless Sensor Network (WSN) is an important research subject. When WSNs are deployed in hostile environments, many attacks happen, e.g., wormhole, sinkhole and sybil attacks. Two issues about unknown nodes' secure localization need to be considered. First, the attackers may disguise as or attack the unknown and anchor nodes to interfere with localization process. Second, the attackers may forge, modify or replay localization information to make the estimated positions incorrect. Currently, researchers have proposed many techniques, e.g., SeRLoc, HiRLoc and ROPE, to solve the two issues. In this paper we describe the common attacks against localization, and survey research state of secure localization.**

***Index Terms*— wireless sensor network, security, localization**

I. Introduction

Localization is one of the most important topics in Wireless Sensor Networks (WSNs) since many fundamental techniques in WSNs, e.g., geographical routing [1], geographic key distribution [2], and location-based authentication [3] require the positions of unknown nodes. Also, the positions of unknown nodes play a critical role in many WSNs applications, such as monitoring applications include environmental monitoring, health monitoring, and tracking applications include tracking objects, animals, humans, and vehicles [4].

When a WSN is deployed in hostile environments, it is vulnerable to threats and risks. Many attacks exist, e.g., wormhole, sinkhole and sybil attacks, to make the estimated positions incorrect. Specifically for some applications, e.g., military applications like battlefield surveillance or environmental applications like forest fire detection [5], incorrect positions may lead to severe consequences, e.g., wrong military decisions on the battlefield and false alarms to people [6]. Hence, the issues of secure localization must be addressed in WSNs.

Secure localization can be considered from two aspects. First, we discuss the attacks on nodes, since an attacker can compromise or pretend to be an unknown or an anchor node to interfere with localization process. Therefore, we need secure node authentication (SNA). Second, we discuss the attacks on information, since an attacker can forge, modify or replay localization information to make the estimated positions incorrect. Thus we need to detect the correctness of localization information, which we call secure information verification (SIV) in the paper.

The remainder of paper is organized as follows: Section II states problem statement. Section III describes attack model. Section IV and V present the schemes of SNA and SIV. Section VI gives the conclusions and open research problems.

II. Problem Statement

Before discussing secure localization problems, it is essential to take a look at some general concepts used in the localization process. Basically, there are two categories of sensor nodes: unknown and anchor nodes. Unknown nodes in the network have no knowledge of their positions and no special hardware to acquire the positions. Anchor nodes, also called beacon nodes, in fact, their positions are obtained by manual placement or additional equipments such as GPS (Global Positioning System). Therefore, unknown nodes can use localization information of anchor nodes to localize themselves. Usually, the localization process can be divided into two steps: 1) information acquisition and 2) position determination.

A. Information acquisition

Roughly speaking, existing localization schemes of WSNs are classified into two categories: range-based schemes [7], [8] and range-free schemes [9], [10]. For range-based localization schemes, the distance or angle information is measured by RSSI (Received Signal Strength Indicator) [11], TOA (Time of Arrival) [12], Time Difference on Arrival (TDOA) [13] and AOA (Angle of Arrival) [14]. For range-free localization schemes, the localization is realized based on network connectivity or other information, which can be obtained by DV-Hop [15], Convex Optimization [16] and MDS-MAP [17].

B. Position determination

Location determination schemes have two categories: 1) terminal-based schemes and 2) infrastructure-based schemes [18]. In terminal-based schemes, the unknown node localizes itself. After connecting available information about distances/angles and positions of anchor nodes,

Manuscript received February 15, 2011; revised May 15, 2011; accepted June 15, 2011.
Corresponding author: Guangjie Han.

doi:10.4304/jcm.6.6.460-470

the position of an unknown node can simply be computed by trilateration [15], multilateration [19], and triangulation [14]. In infrastructure-based schemes, reference nodes including trusted neighbor nodes, mainly anchor nodes to localize the unknown node.

Adversaries can attack localization in both two steps. The goal of the adversary is to make the unknown nodes obtain false positions, by compromising normal nodes to send false localization information, or pretend to be a legitimate node to forge, modify or replay signals. Thus, security measures are needed to make the estimated positions still correct under attacks.

III. Attack Model

Localization process can be attacked in a number of different ways. Researchers have addressed a set of known attacks [18]. The known attacks can be divided into two categories: external and internal attacks. The adversary is external if it is outside the WSN and implements malicious behaviors without right cryptographic key. Otherwise, the adversary is internal, in which case the adversary controls one or more fraudulent nodes. In this paper, the attacks are classified into two categories: 1) attacks on nodes and 2) attacks on information.

A. Attacks on Nodes

In this paper, malicious nodes contain attackers and compromised nodes. An attacker is an external node which intrudes into the WSN. A compromised node is an normal node (an unknown or an anchor node) in the WSN compromised by the attacker. Attacks on nodes are listed as follows:

Compromise: Node compromise is the most fundamental attack in WSN that leads to other kinds of attacks. It occurs when an attacker gains control of a node in the WSN. Normally, compromised nodes can be obtained by the following methods: 1) attackers capture normal nodes and reprogram them; 2) attackers deploy nodes with larger computing resources such as laptops to attack normal nodes [20]. With compromised node, an attacker can alter the node to listen information in the WSN, revoke legitimate nodes, input malicious data, and cause internal attacks, e.g., DoS attack.

Replication: If an adversary manages to capture a node and extract the authentication/encryption keys, it can produce a large number of replicas having the same identity (ID) from the captured node and integrate them into the WSN at chosen locations, which is called the node replication attack. Since the credentials of replicas are all the clones from the captured nodes, the replicas can be considered as legitimate members of the network [21]. It is always assumed that the adversary cannot create new IDs for replicated nodes, since otherwise the attackers will have to create the corresponding security information (keys, codes, etc.), which is very difficult and even infeasible in most cases [22]. Once the adversary replicates one or more sensor nodes, it can execute the malicious operations. For instance, the replicas may inject false localization information into the WSN.

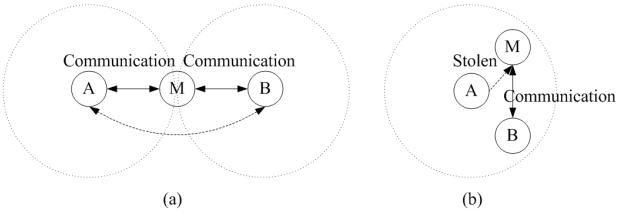


Figure 1. Node impersonation attack: (a) the Invisible Node attack. The malicious node M simply stands between two nodes A and B that are not in direct range. The invisible node M silently repeats the communication between nodes A and B, which misleadingly assume that nodes A and B communicate directly. In this way, the malicious node succeeds in impersonating node A to node B and vice versa. (b) the Stolen Identity attack. The malicious node M succeeds in stealing all the authentication credentials from a legitimate node A, such as the certified signature keys. If the malicious node outraces the legitimate node in updating the stolen credentials, then the credentials of the legitimate node will not be valid anymore. Thus, only the malicious node will be able to communicate with node B. This kind of attack is not just a matter of stealing a nodes identity, but also a matter of abusing the trust relationships that other parties may have had established with the legitimate node.

Impersonation: One form of node impersonation attack is the Invisible Node attack, and the other one is the Stolen Identity attack [23], as shown in Figure 1.

Sybil attack: Sybil attack is launched by a malicious node which has virtually multiple identities (IDs). We refer to a malicious node's additional identities as Sybil nodes. A Sybil node can get an identity in one of two ways. It can fabricate a new identity, or steal an identity from a legitimate node [24]. A sybil node can send messages with different IDs. For example, in localization process, one malicious node may masquerade as several anchor nodes to send false information at the same time.

Wormhole attack: In a wormhole attack, an attacker records a packet or individual bits of a packet at one location in the network. Then, it tunnels the packet (possibly selectively) to another location and replays it. The tunnel can be established in many different ways, for example, through an out-of-band channel, packet encapsulation, high-powered transmission, packet relay and protocol deviations [25]. In localization process, the attack may tunnel totally different and erroneous localization information.

B. Attacks on Information

In the localization systems, unknown nodes always use the localization information of anchor nodes to localize themselves. The target of malicious nodes is usually to make localization information incorrect. Attacks on information are listed as follows:

Forgery: Forgery attack is the malicious node sends misleading information in the localization systems. For example, in the active system [26], the malicious node pretends to be an anchor node to voluntarily send localization information. In the passive system [26], the malicious node pretends to be an unknown node to be localized.

Alteration: Alteration attack is the most direct attack. This attack targets the information exchanged between an unknown and an anchor node. Adversaries may directly alter the coordinates, time or the number of hops and increase the localization error of unknown nodes. For example, in Collaborative Collusion [27], all malicious node can collaborate with each other to alter the information they receives or replays.

Interference: Interference attack is the malicious node interferes with the signal measurements. For example, in range-based localization systems, malicious nodes may place obstacles between signal sender and receiver to prolong transmission time, change angle of arrival or weaken received signal strength [28].

Replay: Replay attack is the most common or simple attack, especially when the capability and resources of the adversary are limited. In this attack, the malicious node congests the information transmission between sender and receiver, then replays the outdated information. Using the outdated information, the unknown nodes calculate inaccurate positions. Unlike other attacks, replay attack can destroy the whole network with one node.

Flooding: Similar to data flooding attack on routing protocol [29], flooding attack on localization is the malicious node broadcasts large quantities of useless data packets to all nodes in its communication range. The common characteristic of flooding attack is to exhaust the available network communication bandwidth so that the other nodes can not communicate with each other. Moreover, the sender and receiver are busy to send or receive the excessive packets from the attacker and consume a lot of network resources.

Selective forwarding: In selective forwarding attack [30], the malicious node behaves like black hole and refuses to forward sensitive messages and simply drops them, ensuring that they are not propagated any further. The selective forwarding attack is difficult to detect. First, to avoid raising suspicions, an adversary selectively drops packets instead of dropping every packet. In addition, there are many reasons result in packet dropout, e.g., unreliable wireless communications. And in some cases, sensor nodes go into sleep state to save power. They cannot send and receive data in this period. Therefore, it is essential to identify the packet dropout is caused by selective forwarding or any other reasons.

IV. Secure Node Authentication

Many secure localization schemes have been proposed [27]. They can be classified into two categories: SNA and SIV. For SNA, in most cases, unknown nodes are localized based on the reference nodes, e.g., trusted anchor nodes. A number of schemes have been proposed to secure the positions of unknown nodes, which are called secure localization for unknown nodes [31], [32]. However, none of these schemes can work properly when the anchor nodes are compromised. Thus, secure localization for anchor nodes is needed.

A. Secure Localization for Unknown Nodes

In general, the main localization algorithms are classified into two categories: range-based and range-free. In this paper, we also classify secure localization for unknown nodes into this two categories.

1) Range-based Secure Localization: Based on the distance-bounding protocols [33], Capkun et al. propose the verifiable multilateration (VM) technique [31], [34]. With a central authority and several anchor nodes which are also named verifiers, VM enables a secure computation and verification of the unknown nodes' positions in the presence of attackers. In VM, verifiers $(v_1, ..., v_n)$ which are in the communication range of the unknown node u perform distance bounding to the node u and obtain distance bounds $db_1, ..., db_n$. These distance bounds, as well as the positions of the verifiers are then reported to the central authority. The authority computes an estimate position $(\hat{x}_u, \hat{y}_u)$ of the unknown node using distance bounds. Then, the authority runs two tests: 1) σ- test: for all v_i, does the distance between $(\hat{x}_u, \hat{y}_u)$ and v_i differ from the measured distance bound db_i by less than the expected distance measurement error σ? 2) point in the triangle test: does $(\hat{x}_u, \hat{y}_u)$ fall within at least one physical triangle formed by a triplet of verifiers? If both the σ and the point in the triangle tests are positive, the authority accepts $(\hat{x}_u, \hat{y}_u)$ as correct; else, the position is rejected.

Based on VM, the authors propose a secure cooperative positioning mechanism called SPINE [31], [34]. SPINE is executed in three phases: 1) the unknown nodes measure distance bounds to their neighbors; 2) the distance bounds are verified through VM; and 3) the positions of the unknown nodes are computed by a distributed algorithm, or by the central authority using a centralized positioning algorithm. Therefore, nodes in SPINE cannot produce erroneous distance measurements. However, SPINE has some drawbacks, e.g., in order to perform verifiable multilateration, a high number of verifiers are required.

Capkun et al. use the Covert Base Station (CBS) and Mobile Base Station (MBS) to verify the positions of unknown nodes [32], [35]. In the CBS case, for infrastructure-centric localization, the public base station (PBS) sends a nonce firstly. When a node replies to the nonce, all the CBSs compute its position together based on TDOA and check if this position is consistent with the time differences. If not, an attack is detected and the estimated position is rejected. For node-centric localization, the unknown node broadcasts a radio signal and an ultrasound signal at the same time, then each CBS obtains the estimated distance based on the arrival time differences of two signals. Also, the CBS obtains calculated distance using nodes reported location and CBS' location. Finally, the CBS compares estimated and calculated distances and rejects inconsistent ones. In the MBS case, it first requires unknown nodes to broadcast a radio signal. After a given period of time, it moves to a different location to broadcast a ultrasound signal. Then the MBS implements the same operations as a CBS does.

In [36], Anjum et al. present a secure localization algo-

rithm called SLA. It is considered that each anchor node has a capability to vary power level. Each power level is assumed to correspond to a different communication range. When an unknown node is localized, the sink node requests anchor nodes to send localization nonce to the node at different power levels. As a result, each unknown node receives a set of unique nonce and retransmits them back to the sink. The sink then determines the position of the unknown node. Compared with VM, SLA do not need fine-grained time synchronization. But the model of power level and transmission range is just suitable for out-door environment not in-door ones [37]. In addition, SLA has a few drawbacks: 1) anchor and sink nodes are all assumed to be trusted; 2) only considering a single sensor node being compromised and ruling out collaborative attacks between sensor nodes; 3) SLA is a centralized approach which creates bottle-neck at the base station.

Zhang et al. [38] propose SLS for ultra-wideband (UWB) sensor networks. To localize a node, anchor nodes first measure their respective distance to the node with a modified two-way ToA approach, called K-distance. The anchor leader then collects all the distance estimates whereby to derive a MMSE location estimate. Subsequently, SLS employs a location validity test by checking whether the location is inside the polygon formed by all the anchor nodes to detect possible attacks. Compared with VM, SLS is more robust and gernal, e.g., using mobile anchor nodes to replace static ones and making each anchor node take turns to act as the leader to balance their resource usage. However, the process of SLS is more complex than that of VM and consumes higher energy.

In [39], based on an attack-driven model specified with the Petri net, an enhanced secure localization scheme (ESLS) is proposed, which extends the idea in [38] and defends against not only distance reduction attacks but also distance enlargement attacks. The major contribution is the first time to use the Petri net to validate a security scheme for WSNs.

In [40], Arisar et al. present a two-way "Greet, Meet and Locate" (GML) mechanism for secure location estimation based on geographical sectorization. GML comprises of three phases: Greet, Meet and Locate. 1) Greet: a light-weight authentication scheme, the HB^+ Protocol, is used to perform two-way authentication, individually by unknown and anchor nodes. 2) Meet: the Diffie Hellman key exchange algorithm is used that allows exchange of secret shared keys between two users in an adversarial environment over an insecure communication medium. 3) Locate: the location is estimated via ToA based technique. Moreover, a double-averaging mechanism is also presented to minimize the localization error.

In [41], Alfaro et al. provide three algorithms that enable the unknown nodes to determine their positions in presence of neighbor sensors that may lie about their locations. The first algorithm is called the Majority-Three Neighbor Signals. When an unknown node is localized, all the neighbor anchor nodes send their locations to it. For every three anchor nodes, the unknown node uses trilateration to calculate a position. Then, a majority decision rule is used to correct the final position of the unknown node. The second algorithm is the Majority-Two Neighbor Signals. The unknown node uses only two neighbor anchor nodes, therefore the correct location is one of the two points of intersection of the two circles centered at two neighbors. The third algorithm is called the Tabulated-Two Neighbor Signals. It is assumed the unknown node may trust one of the neighbor anchor nodes. Then, the unknown node implements the second algorithm for every neighbor anchor nodes except the trusted one. Finally, the unknown node calculates the occurrence frequency of each position and accepts the most frequently occurring one as the correct position. The three algorithms have been extended to localize unknown nodes in [42].

Comparison of the above mentioned schemes is shown in table I.

TABLE I.
COMPARISON OF RANGE-BASED SECURE LOCALIZATION

Algorithm	Technique	Observation
VM	Distance-bounding	Nanosecond clock
SPINE	Distance-bounding	Nanosecond clock High number of anchor nodes
Capkun et al. [32], [35]	CBS and MBS	Centralized approach Rely on locations of CBS
SLA	Distance-bounding Vary power level	Centralized approach Resist only one compromised sensor node
SLS	K-distance approach, MMSE, validity test	Complex Higher energy consumption
ESLS	Petri net	Higher energy consumption
GML	HB^+ Protocol Diffie Hellman ToA	Complex
Alfaro et al. [41]	Trilateration Majority decision	Dense network

2) Range-free Secure Localization: In [43], the authors propose a distributed range-free localization algorithm called SeRLoc, which does not require any communication among unknown nodes. The SeRLoc uses trusted locators equipped with a set of higher-power sectored antennas to replace anchor nodes. The locators have longer transmission range than unknown nodes. They send anchor beacons to unknown nodes, in which contains their positions and the sectors of the antenna. When a node hears multiple locators, it computes the center of gravity of the sectors corresponding to locators as its position. The SeRLoc is robust against severe WSN attacks, such as the wormhole attack, the sybil attack and compromised sensor nodes. However, SeRLoc is based on the assumption that no jamming of the wireless medium is feasible. And it does not protect against attacks on locator's information, which are avoided by checking network properties such as sector uniqueness and communication range. Moreover, in order to minimize the region of sector intersection to improve localization, we need to increase the number of locators and sectored antennas.

In order to reduce the influence on localization ac-

curacy in the SeRLoc caused by different attacks, e.g., misleading anchor beacons. Later, a robust positioning system (ROPE) is proposed [44]. Combining the techniques in SeRLoc and VM [31], ROPE provides both the location determination and location verification function. In location determination, each unknown node obtains its exact location by VM when it is inside at least one triangle formed by locators, and still estimates its location by center of gravity when it is not inside any triangle. The location verification mechanism verifies the location claims of the unknown nodes. Since every unknown node can communicate with at least one locator, when an unknown node reports data to a locator, the locator can verify the unknown node's position by the execution of the distance bounding protocol. Compared with SeRLoc, ROPE is resistant to jamming of the communication medium, limits the maximum spoofing impact and prevents location spoofing due to the Sybil attack, with relatively low density deployment of locators. However, ROPE has higher hardware requirements, e.g., nanosecond time synchronization and instantaneous processing capacity, which is not suitable for low cost WSN.

Based on SeRLoc, in order to minimize the region of sector intersection without increasing the number of locators and sectored antennas, the same authors propose an improved method called high-resolution range-independent localization (HiRLoc) [45], which achieves greater localization accuracy through rotatable antennas and variable transmission power, while increases computational and communication complexity.

In [46], Zeng et al. present a Secure HOp-Count based LOCalization scheme (SHOLOC), which is resistant to different attacks, e.g., hop-count reduction attack and forging packets. In SHOLOC, a protocol combining modified TESLA [47] and hash mechanisms is proposed to authenticate anchor nodes' location information and protect hop-count information. In order to detect wormhole attacks, anchor nodes are responsible to check the distance-impossibility between nodes. Finally, the least median squares (LMS) [48] is used to deal with bad location references.

In [49], [50], Probabilistic Location Verification (PLV) algorithm is proposed. The main idea is to leverage the statistical relationships between the number of hops in a sensor network and the Euclidean distance that is covered. First, an unknown node broadcasts message in the network using flooding, which contains its location as well as the hop count. Each verifier receiving the message can compute the relative distance between it and the unknown node. Then, each verifier computes its probability slack and maximum probability values. Finally, a central node collects the two probability values from all verifiers and a common plausibility for the location advertisement is computed. The central node uses the plausibility to accept or reject the location.

Based on the basic DV-Hop localization process, Wu et al. propose a label-based secure localization scheme to defend against the wormhole attack by removing the packets delivered through the wormhole link [51]. Firstly, the anchor nodes are differentiated and labeled according to their geographic relationship. Then, unknown nodes are further differentiated and labeled by using the labeling results of neighbor anchor nodes. After eliminating the abnormal connections among the labeled neighbor nodes which are contaminated by the wormhole attack, the DV-Hop localization procedure can be conducted. The Label-Based DV-Hop Localization scheme is capable of detecting the wormhole attack and resisting its adverse impacts with a high probability.

In [52], Labraoui et al. similarly propose a Wormhole-free DV-hop Localization scheme (WFDV), to thwart wormhole attacks in DV-Hop algorithm. The main idea of WFDV is to plug-in proactive countermeasure named infection prevention to the basic DV-Hop scheme. Infection prevention consists of two phases: Neighbor List Construction (NLC) and Neighbor List Repair (NLR). NLC applies RSSI and RTT (round trip delay of a link), and utilizes local information to construct neighbor lists. NLR is applied only when a wormhole attack is suspected to remove the packets delivery through the wormhole link. In this phase, frequency hopping and RTS/CTS mechanism are used to confirm the existence of a wormhole and repair the neighbor lists. After eliminating the illegal connections, the DV-Hop localization procedure can be successfully conducted.

Comparison of the above mentioned schemes is shown in table II.

TABLE II.
COMPARISON OF RANGE-FREE SECURE LOCALIZATION

Algorithm	Technique	Observation
SeRLoc	Encryption Sectored antennas	Extra hardware Totally trusted beacons
ROPE	Encryption Sectored antennas	Extra hardware
HiRLoc	Encryption Sectored antennas	Extra hardware Complex
SHOLOC	TESLA Hash mechanisms	Resist simple attacks
PLV	Plausibility Test	Centralized approach
Wu et al. [51]	Label-Based Scheme	Resist only wormhole attack
WFDV	NLC, NLR	Resist only wormhole attack

B. Secure Localization for Anchor Nodes

1) Secure Localization schemes: Du et al. [53] propose LAD (Localization Anomaly Detection) to detect abnormal anchor nodes in the localization process. When sensor nodes are deployed in groups, each node follows two-dimensional Gaussian distribution, which is centered at the deployment point of the node's group. It is assumed that the localization phase has already been ended, and each unknown node has already obtained a position. LAD uses the known deployment information and the group relationship between neighbor sensor nodes to check whether the computed positions of the unknown nodes are consistent with the known deployment knowledge, according to three metrics: the Difference metric, Add-All

metric and Probability metric. LAD has a high detection rate and low false alarm rate, but does not deal with abnormal anchor nodes after detecting them.

Liu et al. [54] introduce a suite of techniques to detect and remove compromised anchor nodes. The anchor node performing the detection is called the detecting node and the anchor node being detected is called the target node. First, the detecting node using a different node ID, called detecting ID, pretends to be an common node and sends request message to each other. Once the target node receives the message, it sends back a beacon signal that includes its own location. Since the detecting node knows its own location, it can calculate the distance between them based on its own location and the target node's location. If the difference between them is larger than the maximum distance error, the detecting node can infer that the received beacon signal is malicious. Then, the wormhole detector and RTT (round trip time) are used to filter replayed beacon signals from Wormholes and locally replayed beacon signals respectively. Finally, the base station checks if the alert counter of the target node exceeds the fixed threshold. If yes, the target node is considered as a malicious one and revoked from the network.

In DRBTS [55], [56], Srinivasan et al. propose a novel reputation based scheme called Distributed Reputation-based Beacon Trust System (DRBTS) for excluding malicious anchor nodes. DRBTS is a distributed security protocol as an extension of the scheme in [54]. In DRBTS, every anchor node monitors its 1-hop neighborhood for misbehaving nodes and accordingly updates the reputation of its neighbor anchor node in the Neighbor-Reputation-Table (NRT). So that unknown nodes can choose some trusted anchor nodes, based on a quorum voting approach. The unknown nodes will only use the anchor node trusted by its neighbor anchor nodes to compute its position.

Since most of secure localization techniques cannot survive malicious attacks in hostile environments where a majority of anchor nodes launch colluding attacks, Wang et al. [57] propose a novel localization algorithm called TMCA. The TMCA is a distributed algorithm based on the cooperation of non-beacon neighbor nodes. It is robust against some known attacks such as the wormhole attack, sybil attack and replay attack. Even when there are more colluding malicious anchor nodes than benign anchor nodes in WSN, TMCA can still work well to generate precise localization results.

Comparison of the above mentioned schemes is shown in table III.

TABLE III.
COMPARISON OF SECURE LOCALIZATION FOR ANCHOR NODES

Algorithm	Technique	Observation
LAD	Three metrics	Requires deployment knowledge No action dealing with anomaly
Liu et al. [54]	RSSI,RTT Wormhole detector	High number of anchor nodes
DRBTS	Encryption	Dense network
TMCA	MMSE	More time consumed

V. SECURE INFORMATION VERIFICATION

SIV schemes can be divided into two categories: filtering and verifying location information.

A. Filtering location information

Many works have been done for filtering the impact of erroneous location information of anchor nodes. In [58] Li et al. introduce the idea of being tolerant to attacks rather than eliminating them. Two classes of localization: triangulation and RF-based fingerprinting, are examined. For the triangulation-based localization, LMS [48] is used to filter the bad localization information. Different from traditional methods that minimize the mean square error, LMS method minimizes the median of square errors. For the fingerprinting-based method, the traditional Euclidean distance metric is not secure enough. Hence, they propose a median-based nearest neighbor scheme.

Liu et al. [59], [60] propose two range-based robust methods to tolerate malicious attacks. The first method is a attack-resistant location estimation called ARMMSE. First, ARMMSE uses MMSE-based methods to estimate unknown nodes' position. Then ARMMSE assesses if the estimated position can be derived from a set of consistent location information of anchor nodes. If yes, the estimation position is accepted; otherwise, the inconsistent location information will be identified and removed. This process may continue until a set of consistent location information is found or it is not possible to find such a set.

The second method is the voting-based location estimation. The ARMMSE obtains a set of location information, which satisfies that the mean square error of the location computed by the subset is below a threshold. In the voting-based algorithm, the deployment field is quantized into a grid of cells. Each anchor node votes to the divided cells, and the centroid of the cells with the highest vote is the estimated position of the unknown node.

In [61], Zhong et al. prove that there are algorithms providing a guaranteed degree of localization accuracy, if the number of malicious anchor nodes k is less than or equal to $\frac{n-3}{2}$ ($k_{\max} = \frac{n-3}{2}$), where n is the number of anchor nodes. Also, two algorithms are proposed to localize the unknown node based on finding a region inside $k_{\max} + 3$ rings. However, such result is obtained under the condition that the measurement error ε is ideally small. In Pollution Attack [62], the adversary can still seriously distort the estimated position when $k_{\max} = \frac{n-3}{2}$ holds.

In [63], Misra et al. propose a critical threshold B for the number of malicious anchor nodes that can be tolerated in the localization process without undermining accuracy. If there are n anchor nodes in the communication range of an malicious node, the maximum number of malicious anchor nodes that can be tolerated is $\lfloor \frac{n}{2} \rfloor - 2$. Then, an enhanced mutually authenticated distance bounding technique (E-MAD) is presented to filter compromised anchor nodes The E-MAD protocol prevents distance reduction attacks. Therefore, the malicious anchor nodes

collude to confuse the localization process by causing an enlargement of the estimated distance.

Comparison of the above mentioned schemes is shown in table IV.

TABLE IV.
COMPARISON OF FILTERING METHODS

Algorithm	Technique	Observation
Li et al. [58]	Triangulation RF-based fingerprinting	High number of anchor nodes
Liu et al. [54]	Pairwise keys Voting scheme	High number of anchor nodes
Zhong et al. [61]	-	Require small measurement error
Misra et al. [63]	E-MAD	Resist only distance reducing attack

B. Verifying location information

Several Verification schemes are proposed based on the distance bounding protocol [33]. Brands and Chaum propose distance bounding protocol to make the prover (P, the claimant waiting to be verified as normal or not) unable to reduce its distance to the verifier (V). The bounding process is: V sends bit α_i to P, and P sends bit $\beta_i = \alpha_i \oplus m_i$ to V immediately after P receives α_i from V. Then, V computes an upper-bound on its distance to P based on the maximum of time delay between sending out α_i and receiving β_i back. Such schemes rely on fine-grained time synchronization, because V needs to measure RF (radio frequency) signal and the transmit time of the signal with nanosecond precision.

In order to reduce the requirement for precise nanosecond clock and sophisticate hardware, Sastry et al. [3] propose the Echo protocol to check whether a prover P is really inside the particular region. In Echo, the verifier V sends a nonce to P using RF and starts the timer, then the prover P immediately echoes the nonce back using ultrasound. V can use the elapsed time to compute the distance between them. Since the ultrasound signal transmits slower than RF, compared with distance bounding protocol, Echo does not require absolutely precise clock and immediately process capability. However, without any kind of authentication, it is possible for an attacker to usurp an honest prover's response and attach its own identity.

In [64] Meadows et al. present a new protocol for distance bounding that requires less message and cryptographic overhead than similar protocol in [33]. First, a full-scale formal analysis of a distance bounding protocol is given to reduce message and cryptographic complexity without reducing security. Then, the collusion attack is addressed. It is showed that the conventional distance bounding protocols are inadequate to collusion attacks.

In [65], Vora et al. propose a new location information verification protocol based on the broadcast nature of radio communication. There are two kinds of verifiers: an acceptor and a rejector. According to the verifier's ability to locate the prover, the network is divided into three zones: the acceptance zone, the ambiguity zone and the rejection zone. A particular protection zone is secure if every point outside the protection zone is also in the rejection zone. The acceptors and rejectors are deployed inside and at the boundary of protected region respectively. The verification process is 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.

In [66], Hwang et al. propose an algorithm to detect the phantom nodes, by getting each node's largest consistent subset which contains all the normal nodes. The algorithm is divided into two main phases: distance measurement phase and filtering phase. In the first phase, each node measures the distances to its neighbors. In the second phase, each node first randomly picks up two neighbors to create a local map. Then in each such map, we try to find the largest consistent subset by checking each node that whether its measured ranges are consistent with its ranges in the map. The above processes are repeated for given times and the largest subset in all the runs is selected, which contains all the normal nodes. In this method, all nodes play the role of verifier. Even the number of phantom nodes is greater than that of honest nodes, we can still filter out most phantom nodes.

In [67], Wei et al. propose two lightweight location verification algorithms, namely, Greedy Filtering by Matrix (GFM) and Trustability Indicator (TI). In GFM algorithm, the Verification Center(VC) calculates several matrices, e.g., Observation Matrix, Difference Matrix and Weight Matrix, based on unknown nodes' estimated positions and their neighborhood observations. These matrixes are used to identify and revoke inconsistent location information. In TI algorithm, VC calculates trustability indicators for each unknown node and accepts those whose final indicators are greater than a threshold.

In [68], Delaet et al. propose the first deterministic distributed protocol, FindMap, for accurate identification of faking sensor nodes based on a distance ranging technique. It is showed that when RSSI is used, FindMap handles at most $\lfloor \frac{n}{2} \rfloor - 2$ faking sensor nodes. When the time of flight (ToF) technique is used, FindMap manages at most $\lfloor \frac{n}{2} \rfloor - 3$ misbehaving sensor nodes. However, it is proved that no deterministic protocol can identify faking sensors if their number is $\lfloor \frac{n}{2} \rfloor - 1$.

In [69], Li et al. focus on an in-region verification problem and propose a secure location verification (SVLE) algorithm. A client (any node needs to be verified) first broadcasts a random challenge nonce. The anchor nodes receiving the nonce calculate the signal strength based on the signal attenuation model. Then, the signal strength, the ID of the client and anchor nodes' location information are sent to base station. Finally, the base station continues to execute the algorithm called VerSec to verify the validity of the signal strength. A node will be considered as an adversary if its signal strength is incompatible with that of other nodes in region.

Comparison of the above mentioned schemes is shown in table V.

TABLE V.
COMPARISON OF VERIFYING METHODS

Algorithm	Technique	Observation
Distance bounding	-	Trusted verifiers
	-	Nanosecond clock
Echo	-	Trusted verifiers
Meadows et al. [64]	-	Just giving analysis
Vora et al. [65]	RSSI	Trusted verifiers
Hwang et al. [66]	-	More time consumed
Wei et al. [67]	GFM, TI	Centralized approach
FindMap	RSSI,ToF	Rely on distance bounding
SVLE	VerSec	Centralized approach

VI. CONCLUSION

In order to address security problem in WSN, a number of methods have been proposed, e.g., secure routing [70], [71], key management [72] and sensor selection scheme [73]. This paper focuses on the secure localization survey. We reclassify the known attacks on localization systems and the proposed secure localization schemes.

The future research directions of secure localization algorithms possibly are: 1) Build up more realistic and destructive attack models against secure localization. 2) Improve security schemes to enhance detection rate for anomaly without nanosecond clocks, additional hardware and any deployment information. 3) Research new localization determination or verification proposals to reduce the localization time and energy consumption. 4) Evaluate the performance of secure localization algorithms with a series of standards. 5) Use other research domains' technology, e.g., the Petri net [39]. 6) Extend to new challenges in special WSNs, e.g., Mobile Multimedia Sensor Networks (MMSNs) [74].

ACKNOWLEDGMENT

The work is supported by "the Fundamental Research Funds for the Central Universities, No.2010B22814, 2010B22914, 2010B24414" and "the research fund of Jiangsu Key Laboratory of Power Transmission & Distribution Equipment Technology, No.2010JSSPD04".

REFERENCES

[1] B. Karp and H. T. Kung, "GPSR: Greedy Perimeter Stateless Routing for wireless networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Network*, 2000, pp. 243–354.

[2] D. Liu and P. Ning, "Location-based pairwise key establishments for static sensor networks," in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, 2003, pp. 72–82.

[3] S. U. Sastry, N. and D. Wagner, "Secure verification of location claims," in *Proceedings of the 2nd ACM workshop on Wireless security*, September 2003.

[4] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor networks: a survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, August 2008.

[5] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, March 2002.

[6] Y. Zeng, J. Cao, J. Hong, and L. Xie, "Secure localization and location verification in wireless sensor networks," in *IEEE 6th International Conference on Mobile Adhoc and Sensor Systems*, October 2009, pp. 864–869.

[7] S. Zhu and Z. Ding, "A simple approach of range-based positioning with low computational complexity," *IEEE Transactions on Wireless Communications*, vol. 8, no. 12, December 2009.

[8] M. Heidari, N. Alsindi, and K. Pahlavan, "Udp identification and error mitigation in toa-based indoor localization systems using neural network architecture," *IEEE Transactions on Wireless Communications*, vol. 8, no. 7, July 2009.

[9] S. Lee, E. Kim, C. Kim, and K. Kim, "Localization with a mobile beacon based on geometric constraints in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 7, pp. 5801–5805, December 2009.

[10] H. Chen, Q. Shi, H. Vincent Poor, and K. Sezaki, "Mobile element assisted cooperative localization for wireless sensor networks with obstacles," *IEEE Transactions on Wireless Communications*, vol. 9, no. 3, March 2010.

[11] P. Bahl and V. Padmanabhan, "RADAR: An In-Building RF-Based User Location and Tracking System," in *Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 21, 2000, pp. 755–784.

[12] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, "The anatomy of a context-aware application," in *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, 1999, pp. 59–68.

[13] L. Girod and D. Estrin, "Robust range estimation using acoustic and multimodal sensing," in *Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems*, 2001, pp. 1312–1320.

[14] D. Niculescu and B. Nath, "Ad hoc positioning system (APS) using AoA," in *Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 3, April 2003, pp. 1734–1743.

[15] ——, "Ad hoc positioning system (APS)," in *Proceedings of the 2001 IEEE Global Telecommunications Conference of the IEEE Communications Society*, vol. 5, 2001, pp. 2926–2931.

[16] L. Doherty, K. Pister, and L. Ghaoui, "Convex position estimation in wireless sensor networks," in *Proceedings of the 20th Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 3, 2001, pp. 1655–1663.

[17] Y. Shang, W. Ruml, Y. Zhang, and M. Fromherz, "Localization from mere connectivity," in *Proceedings of the 4th International ACM Symposium on Mobile Ad Hoc Networking & Computing*, 2003, pp. 201–212.

[18] A. Ferreres, B. Alvarez, and A. Garnacho, "Guaranteeing the authenticity of location information," *IEEE Pervasive Computing*, vol. 7, no. 3, pp. 72–80, July 2008.

[19] A. Savvides, C.-C. Han, and M. Srivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," in *Proceedings of the 7th annual international conference on Mobile computing and networking*, 2001, pp. 166–179.

[20] X. Chen, *Defense Against Node Compromise in Sensor Network Security*. FIU Electronic Theses and Dissertations, http://digitalcommons.fiu.edu/etd/7, 2007.

[21] C. Yu, C. Lu, and S. Kuo, "Efficient and distributed detection of node replication attacks in mobile sensor networks," in *Proceedings of Vehicular Technology Conference Fall (VTC Fall)*, September 2009, pp. 1–5.

[22] K. Xing, F. Liu, C. Cheng, and D. Du, "Real-time detection of clone attacks in wireless sensor networks," in *Proceedings of the 28th International Conference on Distributed Computing Systems*, June 2008, pp. 3–10.

[23] K. Glynos, P. Kotzanikolaou, and C. Douligeris, "Preventing impersonation attacks in manet with multi-factor authentication," in *Proceedings of the Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, April 2005, pp. 59–64.

[24] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis & defenses," in *Proceedings of the Third International Symposium on Information Processing in Sensor Networks*, April 2004, pp. 259–268.

[25] M. Jain and H. Kandwal, "A survey on complex wormhole attack in wireless ad hoc networks," in *Proceedings of the 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies*, December 2009, pp. 555–558.

[26] A. Quazi, "An overview on the time delay estimate in active and passive systems for target localization," *IEEE Transactions on Acoustics Speech and Signal Processing*, vol. 29, no. 3, pp. 527–533, June 1981.

[27] J. Jiang, G. Han, S. L., H. Chao, and S. Nishio, "A novel secure localization scheme against collaborative collusion in wireless sensor networks," in *the 7th International Wireless Communications & Mobile Computing Conference*, July 2011.

[28] X. Cao, B. Yu, G. Chen, and F. Ren, "Security analysis on node localization systems of wireless sensor networks," *China Journal Of Software*, vol. 19, no. 4, pp. 879–887, April 2008.

[29] P. Yi, Z. Dai, Z. Y., and S. Zhang, "Resisting flooding attacks in ad hoc networks," in *Proceedings of the International Conference on Information Technology: Coding and Computing*, no. 2, April 2005, pp. 657–662.

[30] L. Bysani and A. Turuk, "A survey on selective forwarding attack in wireless sensor networks," in *Proceedings of the International Conference on Devices and Communications (ICDeCom)*, February 2011, pp. 1–5.

[31] S. Capkun and J. Hubaux, "Secure positioning of wireless devices with application to sensor networks," in *Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, no. 3, 2005, pp. 1917–1928.

[32] S. Capkun, K. Rasmussen, M. Cagalj, and M. Srivastava, "Secure location verification with hidden and mobile base stations," in *IEEE Transactions on Mobile Computing*, vol. 7, no. 4, 2008, pp. 470–483.

[33] S. Brands and D. Chaum, "Distance-bounding protocols," in *Proceedings of the the EUROCRYPT 93 Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology*, 1994, pp. 344–359.

[34] S. Capkun and J. Hubaux, "Secure positioning in wireless network," in *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, 2006, pp. 221–232.

[35] S. Capkun, M. Cagalj, and M. Srivastava, "Secure localization with hidden and mobile base stations," in *Proceedings of the 25th IEEE International Conference on Computer Communications*, 2006, pp. 1–10.

[36] F. Anjum, S. Pandey, and P. Agrawal, "Secure localization in sensor networks using transmission range variation," in *Proceedings of the 2nd IEEE International Conference on Mobile Adhoc and Sensor Systems Conference*, November 2005, pp. 203–211.

[37] S. Ganu, A. Krishnakumar, and P. Krishnan, "Infrastructure-based location estimation in wlan networks," in *IEEE Wireless Communications and Networking Conference*, March 2004, pp. 465–470.

[38] Y. Zhang, W. Liu, Y. Fang, and D. Wu, "Secure localization and authentication in ultra-wideband sensor networks," in *IEEE Journal on Selected Areas in Communication*, vol. 24, no. 4, 2006, pp. 829–835.

[39] D. He, L. Cui, and H. Huang, "Design and verification of enhanced secure localization scheme in wireless sensor networks," in *IEEE transactions on Parallel and Distributed Systems*, vol. 20, no. 7, July 2009.

[40] S. Arisar and A. Kemp, "Secure location estimation in large scale wireless sensor networks," in *Proceedings of the 3rd International Conference on Next Generation Mobile Applications, Services and Technologies*, 2009, pp. 472–476.

[41] J. Alfaro, M. Barbeau, and E. Kranakis, "Secure localization of nodes in wireless sensor networks with limited number of truth tellers," in *Proceedings of the 7th Annual Communications Networks and Services Research Conference*, 2009, pp. 86–93.

[42] ——, "Secure geolocalization of wireless sensor nodes in the presence of misbehaving anchor nodes," in *Annals of Telecommunications*, November 2010, pp. 1–18.

[43] L. Lazos and R. Poovendran, "SeRLoc: Secure range-independent localization for wireless sensor networks," in *Proceedings of the 3rd ACM Workshop on Wireless Security*, 2004, pp. 21–30.

[44] ——, "ROPE: robust position estimation in wireless sensor networks," in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks*, April 2005, pp. 324–331.

[45] ——, "HiRLoc: High-resolution robust localization for wireless sensor networks," in *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, 2006, pp. 233–246.

[46] Y. Zeng, S. Zhang, S. Guo, and L. Xie, "Secure hop-count based localization in wireless sensor networks," in *2007 International Conference on Computational Intelligence and Security*, December 2007, pp. 907–911.

[47] A. Perrig, R. Canetti, D. Tygar, and D. Song, "Efficient authentication and signature of multicast streams over lossy channels," in *Proceedings of Oakland*, May 2000, pp. 56–73.

[48] P. Rousseeuw and A. Leroy, "Robust regression and outlier detection," in *WileyInterscience*, 2003.

[49] E. Ekici, J. Mcnair, and D. Al-Abri, "A probabilistic approach to location verification in wireless sensor networks," in *IEEE International Conference on Communications*, vol. 8, June 2006, pp. 3485–3490.

[50] E. Ekici, S. Vural, J. Mcnair, and D. Al-Abri, "Secure probabilistic location verification in randomly deployed wireless sensor networks," in *Ad Hoc Networks*, vol. 6, no. 2, 2008, pp. 195–209.

[51] J. Wu, H. Chen, W. Lou, Z. Wang, and Z. Wang, "Label-based dv-hop localization againstwormhole attacks in wireless sensor networks," in *Proceedings of the 5th IEEE International Conference on Networking, Architecture, and Storage*, September 2010, pp. 79–88.

[52] N. Labraoui and M. Gueroui, "Secure range-free localization scheme in wireless sensor networks," in *Proceedings of the 10th International Symposium on Programming and Systems (ISPS)*, April 2011, pp. 1–8.

[53] W. Du, L. Fang, and P. Ning, "LAD: Localization anomaly detection forwireless sensor networks," in *The Journal of Parallel and Distributed Computing*, vol. 66, no. 7, 2006, pp. 874–886.

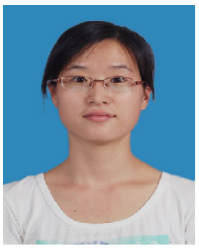
[54] D. Liu, P. Ning, and W. Du, "Detecting malicious beacon nodes for secure location discovery in wireless sensor networks," in *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems*, 2005, pp. 609–691.

[55] A. Srinivasan, J. Teitelbaum, and J. Wu, "DRBTS: Distributed reputation-based beacon trust system," in *Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing*, 2006, pp. 277–283.
[56] A. Srinivasan, J. Wu, and J. Teitelbaum, "Distributed reputation-based secure localization in sensor networks," in *Journal of Autonomic and Trusted Computing*, 2007.
[57] X. Wang, L. Qian, and H. Jiang, "Tolerant majority-colluding attacks for secure localization in wireless sensor networks," in *Proceedings of 5th International Conference on Wireless Communications, Networking and Mobile Computing*, 2009, pp. 1–5.
[58] Z. Li, W. Trappe, and B. Nath, "Robust statistical methods for securing wireless localization in sensor networks," in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN)*, 2005, pp. 91–98.
[59] D. Liu, P. Ning, and W. Du, "Attack-resistant location estimation in sensor networks," in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN)*, April 2005, pp. 99–106.
[60] D. Liu, P. Ning, A. Liu, W. Wang, and W. Du, "Attack-resistant location estimation in sensor networks," in *ACM Transactions on Information and System Security (TISSEC)*, vol. 11, no. 4, 2005, pp. 1–39.
[61] S. Zhong, M. Jadliwala, S. Upadhyaya, and C. Qiao, "Towards a theory of robust localization against malicious beacon nodes," in *Proceedings of the 27th IEEE International Conference on Computer Communication*, 2008, pp. 1391–1399.
[62] Y. Zeng, J. Cao, Z. S., S. Guo, and L. Xie, "Pollution attack: A new attack against localization in wireless sensor networks," in *Proceedings of Wireless Communications and Networking Conference*, April 2009, pp. 2038–2043.
[63] S. Misra, G. Xue, and S. Bhardwaj, "Secure and robust localization in a wireless ad hoc environment," in *IEEE Transactions on Vehicular Technology*, vol. 58, no. 3, 2009, pp. 1480–1489.
[64] C. Meadows, R. Poovendran, D. Pavlovic, L. Chang, and P. Syverson, "Distance bounding protocols: Authentication logic analysis and collusion attacks," in *Secure Localization and Time Synchronization in Wireless Ad Hoc and Sensor Networks*, 2007, pp. 279–298.
[65] A. Vora and M. Nesterenko, "Secure location verification using radio broadcast," in *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 4, December 2006, pp. 377–385.
[66] J. Hwang, T. He, and Y. Kim, "Detecting phantom nodes in wireless sensor networks," in *Proceedings of the 26th IEEE International Conference on Computer Communications*, May 2007, pp. 2391 – 2395.
[67] Y. Wei, Z. Yu, and Y. Guan, "Location verification algorithms for wireless sensor networks," in *Proceedings of the 27th International Conference on Distributed Computing Systems*, June 2007, p. 70.
[68] S. Delaet, P. Mandal, M. Rokicki, and T. S., "Deterministic secure positioning in wireless sensor networks," in *IEEE International Conference on Distributed Computing in Sensor Networks (DCOSS)*, June 2008, pp. 469–477.
[69] C. Li, F. Chen, Y. Zhan, and L. Wang, "Security verification of location estimate in wireless sensor networks," in *Proceedings of the 2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, 2010, pp. 1–4.
[70] T. Mulugeta, L. Shu, M. Hauswirth, C. M., T. Hara, and S. Nishio, "Secure two phase geographic forwarding routing protocol in wireless multimedia sensor networks," in *the IEEE Global Communication Conference*, December 2010, pp. 1–6.
[71] T. Mulugeta, L. Shu, M. Hauswirth, Z. Zhou, and S. Nishio, "Secured geographic forwarding in wireless multimedia sensor networks," in *Journal of Information Processing*, 2010 (to appear).
[72] L. He, Y. Zhang, L. Shu, A. Vasilakos, and M. Park, "Energy efficient location-dependent key management scheme for wireless sensor networks," in *the IEEE Global Communication Conference*, 2010, pp. 1–5.
[73] G. Han, L. Shu, J. Ma, J. Park, and J. Ni, "Power-aware and reliable sensor selection based on trust for wireless sensor networks," in *Journal of Communications*, vol. 5, no. 1, January 2010, pp. 23–30.
[74] L. Shu, Y. Chen, T. Hara, M. Hauswirth, and S. Nishio, "The new challenge: Mobile multimedia sensor networks," in *In Indersicence, International Journal of Multimedia Intelligence and Security*, vol. 2, no. 2, 2011, pp. 107–119.

Jinfang Jiang is currently pursuing Master degree from Department of Information & Communication Engineering at Hohai University, China. She received her B.S. degree in Information & Communication Engineering from Hohai University, China, in 2009. Her current research interests are security and localization for Wireless Sensor Networks.

Guangjie Han is currently an Associate Professor of Department of Information & Communication System at Hohai University, China. He is also a visiting research scholar of Osaka University from Oct. 2010 to Oct. 2011. He finished the work as a Post doctor of Department of Computer Science at Chonnam National University, Korea, in February 2008. He received his Ph.D. degree in Department of Computer Science from Northeastern University, Shenyang, China, in 2004. He has published over 90 papers in related international conferences and journals. He has served as an editor of ANC and IJIDCS. He has served as a Co-chair for more than 10 international conferences/workshops; a TPC member of more than 30 conferences. He has served as a reviewer of more than 20 journals. His current research interests are security and trust management, localization and tracking, cooperative computing for Wireless Sensor Networks. He is a member of IEEE.

Chuan Zhu was born in Liaoning, China. He received his Ph.D. degree in Department of Computer Science from Northeastern University, Shenyang, China, in 2009. He is currently a lecturer of Department of Computer at the Hohai University, China. His current research interests are coverage and connectivity for wireless sensor networks, smart home, Internet of things.



Yuhui Dong is currently persuing her Masters degree from Department of Information & Communication Engineering at the Hohai University, China. She received her B.S. degree in Information & Communication Engineering from Hohai University, China, in 2009. Her current research interests is routing security for Wireless Sensor Networks.

Na Zhang is currently persuing her Masters degree from Department of Communication & Information Engineering at Hohai University, China. She received her B.S. degree in Electronics & Information Engineering from Hohai University, China, in 2009. Her current research interests is sensor localization algorithms in underwater wireless sensor networks .