ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Secure Location Verification using Localization Algorithms

Parthiban. M
Graduate Student, Dept. of CSE, Roever Engineering College, Perambalur, India

Abstract
The information of sensors' locations is vital data for numerous requisitions in Wireless Sensor Networks (WSNs). The point when sensor hubs are deployed in adversary environments, the localization designs are susceptible to various attacks, e.g., wormhole, pollution, range enlargement attack, and etc. Therefore, sensors' locations are not dependable and need to be verified before they can be used by location-predicated applications. Earlier verification schemes either need group-based deployment knowledge of the sensor field, or rely upon expensive or dedicated hardware, so they cannot be used for low-cost sensor networks. In this paper, we propose a location verification system that performs location verification against malicious attacks. The verification system proposes to verify if the locations asserted by sensors are far from their factual locations beyond a certain distance. We propose probabilistic method to calculate location assurance for each sensor. They are robust in the occurrence of malicious attacks that are commenced throughout the verification method.

Index Terms
Localization, verification, on-field, in-zone, security, wireless sensor networks.

I. Introduction

LOCALIZATION in wireless sensor networks, i.e., understanding the position of sensor nodes, is very significant for many submissions such as natural environment supervising, target tracking, and geographical routing. Since wireless sensor systems may be established in adversary environment, sensors' localization is subjected to numerous malicious attacks. For example, adversaries can bargain sensors and infuse false location data. Hence, the areas assessed in the localization process are not dependably right. In the previous verification system, some algorithms [1-3], were proposed to help improve sensors' imperviousness to attacks, they can't totally dispose of wrong location estimations.

We consider the location verification into two categories, namely, on-field and in-zone. On-field confirmation is to check if a sensor's actual position is the same as its evaluated position. In-zone confirmation is to check if a sensor is inside a geological region given that its assessed position is in that region.

In this paper, we propose the verification system that overcomes the previous problems. The verification system can adequately confirm if sensors' evaluated areas are reliable. First, to provide on-field confirmation, we propose two algorithms namely, Bayesian Matrix algorithm and Memetic algorithm that recognize abnormal locations by investigating the inconsistencies between sensors' claimed positions and their neighborhood perceptions. Second, to perform in-zone confirmation, Probabilistic algorithm is used to calculate the assurance that a sensor is inside a specific region. The verification system can be applied to low-cost networks.

II. Problem Statement

In this paper, we propose to design a verification system in which the control center can effectively work if sensors' approximated positions are reliable. Our verification system should have following features. First, it should not need costly equipment such as directional antennas, and quick processors that presents XOR computation. It should not acquire high communication overhead on sensor edge, which would rapidly consume the scares power retained at sensors. Second, the algorithm should be effective by achieving high detection rate and reduced untrue alert rate. The previous rate is defined as the ratio between the numbers of detected incorrect positions and the number of all incorrect positions, while the second rate is characterized as the ratio between the number of correct positions that are mistakenly identified as incorrect ones, and the number of all correct positions.

III. Verification Determination

The battlefield surveillance application is one of the location-based submissions. In such submissions, sensors are implemented in a battlefield to supervise enemy's behaviors and report doubtful occurrence such as appearance of objects or soldiers. In Fig. 1. S and S' denote a sensor's factual and approximated position. At some time, the sensor detects the object and notifies the control center. Before the control center projects a blasting device to decimate the object, it should consult the verification system if the estimated location of the sensor is reliable, so that it can have some self-assurance about whether the object can be wrecked.

In battlefield surveillance, sensors that detect a doubtful object will inform the control center to decimate the object. There can be many advances to working out the projection position, for ease, we assume it is the mean position of all the approximated positions of the sensors that notice the object. We do not need sensors to be equipped with any exceptional hardware such as antennas or distance-measuring apparatus, however, the determination of the verification region of sensors will be diverse relying upon if the angle and distance information are available.

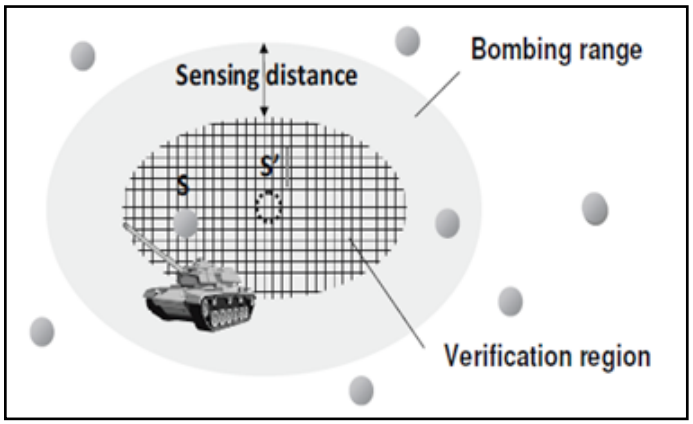

Fig. 1 : Battlefield surveillance application.

A. Bayesian Matrix and Memetic Algoithm:

Just like the adversaries can attack the localization designs to make sensors' positions incorrectly approximated, they can also attack the verification algorithm to make abnormal positions not to be noticed by the control center. To achieve this goal, the adversaries will compromise a sensor and force it to report fake information about their neighbors' node that is reliable with the asserted location. We show such an attack in Fig. 2. In the figure, sensor S4 is compromised and localized at location L' that is far away from its true position L. If sensor S4 submits the factual position O4 = (S1, S2, S3), then the Bayesian algorithm will easily find inconsistencies because the estimated locations of sensors S1, S2 and S3 are far away from position L'. To get away from being noticed, S4 may report a fake observation O4 = (S5, S6, S7), which includes sensors that are localized in the neighborhood of position L'.

We will use the above example to investigate Bayesian algorithm's performance. In Fig. 3, the elements in the 4th row and in the 4th column of matrix Md are shown. For simplicity, matrix Mw is not engaged here. The metric values for sensor S4 are AD4 = 0, PD4 = 6 and AS4 = 6. The standards of PD4 and AS4 are very high, therefore, it is very probable that S4 will be revoked. A more sophisticate attack scenario is that S4 does not announced its ID information, thus none of S1, S2 and S3 can observe sensor S4. Then the elements in Md need to be recalculated appropriately, and the metric values become AD4 = 0, PD4 = 3 and AS4 = 3. Thus, the inconsistency has been mitigated. However, according to the delineation of reliable neighbors, the consistent-neighbor metric becomes CN4 = 0, so that S4 can still be revoked throughout the last ascertain at line (13)-(14) of the Bayesian algorithm. To generalize this attack from this example, we assume sensor Si reports a fake position L' which is far away from its factual position L. Meanwhile, it assertions to observe n sensors in the neighborhood of L and n' sensors in the neighborhood of L'. There are really m and m' sensors in the neighborhood of L and L' respectively, where $m \geq n$ and $m' \geq n'$. Because the n sensors are not in the neighborhood of L', the Active difference metric is Adi = n +m' – n'. Second, since none of the sensors in neighborhood of L' would observe sensor Si, the Passive Difference metric is Pdi = n + m'. Furthermore, the Asymmetry metric is Asi = m – n + m' – n' and the reliable Neighbor metric is Cni = 0. In order to minimize the values for the first three metrics, the attackers would take large worth for n' such as n' = m'. While lesser worth of n would boost metric AS, bigger worth of n would increase metric publicity and PD. More importantly, since there is none reliable close by existing for sensor Si, it will be revoked at the last check by the Bayesian algorithm.

Inconsistency can be absolutely taken if sensors S4, S5, S6 and S7 are all compromised. Sensor S4 does not announced its ID, and reports a false neighborhood fact O4 = (S5, S6, S7); meantime, sensors S5, S6 and S7 all report to observe S4. Thus, we resolve that as long as the adversaries will not compromise the most of sensors in a local locality, inconsistencies always exist and localization anomaly can be detected.

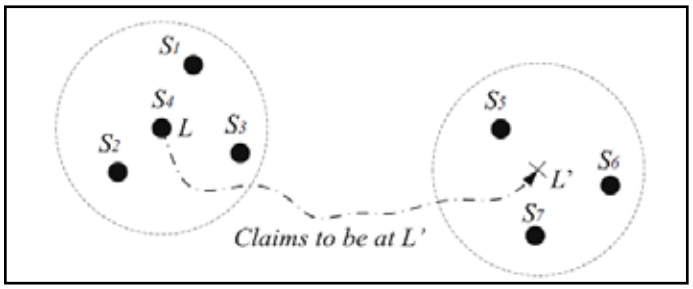

Fig. 2: Attack to Bayesian algorithm.

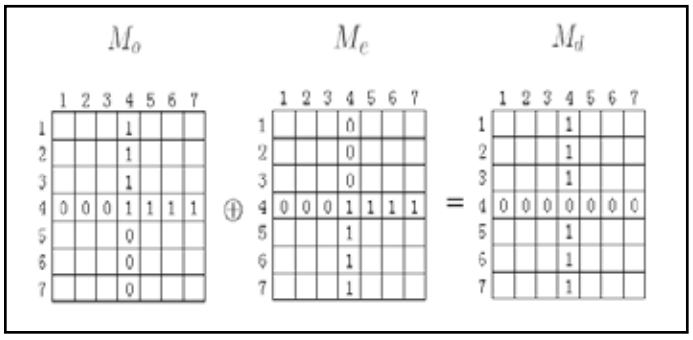

Fig. 3 : Bayesian matrixes under attacks.

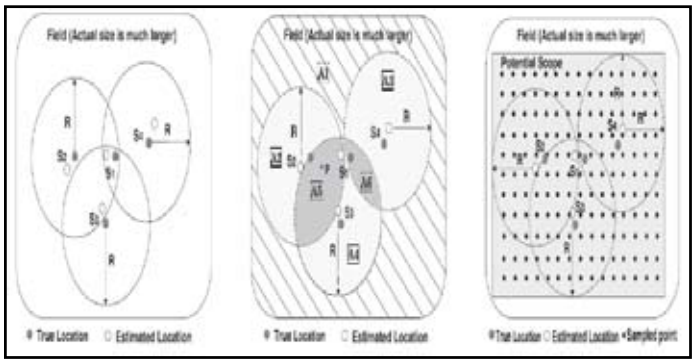

Fig. 4 : Sensor fields

B. Algorithm

1: compute matrix Minc
2: compute metrics AD, PD, AS for all sensors
3: while (sensor Si exists that can be filtered out)
4: if ADi > AD-threshold
5: revoke Sk that ADk is the largest among all sensors
6: else if PDi > PD-threshold
7: revoke Sk that PDk is the largest among all sensors
8: else if ASi > AS-threshold
9: revoke Sk that ASk is the largest among all sensors
10: set zeros to kth row and kth column in Me, Mo, Minc
11: recalculate metrics AD, PD, AS for all sensors
12: while (sensor Si exists that CNi < CN-threshold)
13: revoke sensor Si for not having enough neighbors
14: verify remaining sensors not revoked

IV. Related Work

In recent years, a large number of localization schemes were designed for wireless sensor systems. Because localization designs can be compromised by malicious adversaries, who can launch wormhole attack, range enlargement attacks, many protected localization schemes are designed. Since these algorithms run on sensors which have very restricted resources, some enhancement methods have been evolved for very quick computing of region intersections [4]. These secure localization designs mainly aim

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

to enhance innocent sensors' proficiency to correctly localize themselves, in presence of malicious attacks. Although, since sensors may not be innocent, i.e., they are effortlessly be compromised, they report false positions exactly to the command center. Therefore, position verification is necessary to fight back against such attacks. The location verification difficulty was first addressed in [5], in which Sastry et al. [5] suggested Echo protocol to verify if a device is inside some personal region, such as a room or a football stadium. The Echo protocol is mostly to supply location-based access to command, and will not be exactly applied for position verification in other submissions. Capkun and Hubaux [3] proposed the Verifiable Multilateration (VM) method to verify if a sensor's approximated location is at its factual position using the distance bounding protocol [3]. These algorithms supply on-field verification results, i.e., if a sensor's claimed position is the same as its true position, therefore they need some additional costly hardware to be established through the field. Some verification designs that do not require extra infrastructures have furthermore been proposed.Most of previous algorithms aim on detecting position anomalies, namely, verifying if sensors' claimed positions are far away from their factual positions. They do not take into consideration the application's obligations on the accuracies of sensors' positions. From this sense, ours is the first work that attempts to study an application's location-related functions and propose verification algorithm to facilitate the application's operations.

V. Conclusion

In this paper, we propose a position verification scheme that presents both "on-field" and "in-zone" position verifications. The Bayesian and Memetic algorithms verify whether the positions asserted by sensors are far from their factual locations beyond a certain distance. A probabilistic procedure is designed to supply the self-assurance that a sensor is inside the verification region. Moreover, our proposed verification system is more effective, and robust compared to existing works. It does not need any dedicated or costly infrastructures in the field; it yields satisfactory verification results to a kind of submissions, which is approved by the replication outcomes; furthermore, it is resilient to malicious attacks and can be used in adversary environments.

References

[1] *L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," Proc. 11th Network and Distributed System Security Symp., 2003.*

[2] *L. Lazos and R. Poovendran, "SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks," Proc. ACM Workshop Wireless Security (WiSe), 2004.*

[3] *L. Lazos, R. Poovendran, and S. Capkun, "ROPE: Robust Position Estimation in Wireless Sensor Networks," Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN '05), 2005.*

[4] *Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust Statistical Methods for Securing Wireless Localization in Sensor Networks," Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN '05), 2005.*

[5] *N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, "Position Based Cryptography," Proc. Int'l Cryptology Conf. (CRYPTO '09), pp. 391-407, 2009.*

Parthiban.M, College Graduate, Roever Engineering College, Perambalur,India