www.ijiarec.com

NOV 2013

International Journal of Intellectual Advancements and Research in Engineering Computations

CONTRADICTION COMMUNICATION RANGE OF SENSOR NETWORKS

*[1]Mr. G.Parthasarathy, [2]Mr. P.Vijayan,M.E.,

ABSTRACT

The knowledge of sensors' locations is crucial information for many applications in Wireless Sensor Networks (WSNs). When sensor nodes are deployed in hostile environments, the localization schemes are vulnerable to various attacks, e.g., wormhole attack, pollution attack, range enlargement/reduction attack, and etc. Therefore, sensors' locations are not trustworthy and need to be verified before they can be used by location-based applications. Previous verification schemes either require group-based deployment knowledge of the sensor field, or depend on expensive or dedicated hardware, thus they cannot be used for low-cost sensor networks. In this paper, we propose a lightweight location verification system that performs both "on-spot" and "in-region" location verifications. The on-spot verification intends to verify whether the locations claimed by sensors are far from their true spots beyond a certain distance. We propose two algorithms that detect abnormal locations by exploring the inconsistencies between sensors' claimed locations and their neighborhood observations. The in-region verification verifies whether a sensor is inside an application-specific verification region. Compared to on-spot verification, the in-region verification is tolerable to large errors as long as the locations of sensors don't cause the application to malfunction. To study how to derive the verification region for different applications and design a probabilistic algorithm to compute in-region confidence for each sensor. Experiment results show that our on-spot and in-region algorithms can verify sensors' locations with high detection rate and low false positive rate. They are robust in the presence of malicious attacks that are launched during the verification process. Moreover, compared with previous verification schemes, our algorithms are effective and lightweight because they do not rely on the knowledge of deployment of sensors, and they don't require expensive or dedicated hardware, so our algorithms can be used in any low-cost sensor networks.

Index terms: WSN, Lightweight, On-spot, In-region, Sensors.

I INTRODUCTION

Localization in wireless sensor networks, i.e., knowing the location of sensor nodes, is very important for many applications such as environment monitoring, target tracking, and geographical routing. Since wireless sensor networks may be deployed in hostile environment, sensors' localization is subjected to many malicious attacks. For example, attackers can compromise sensors and inject false location information. They can also interrupt signal transmission between sensors and contaminate distance measurements. Hence, the locations estimated in the localization process are not always correct. Although some secure localization algorithms L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks", Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", L. Lazos, and R. Poovendran, "SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks", Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust Statistical Methods for Securing Wireless Localization in Sensor Networks", D. Liu, N. Peng, and W.K. Du, "Attack-Resistant Location Estimation in Sensor Networks", were proposed to help enhance sensors' resistance to attacks, they cannot completely eliminate wrong location estimations. Therefore, we consider location

Author for Correspondence:
*[1]Mr.G.Parthasarathy, PG Scholar, Department of CSE, Sri Krishna Engineering College Panapakam, Chennai-301, India.
E-mail: sarathyp65@gmail.com
[2]Mr.P.Vijayan, M.E., Asst.Professor Department of CSE, Sri Krishna Engineering College, Panapakam, Chennai-301, India.

verification as a necessary second line-of-defense against malicious attacks, which becomes the focus of this paper. We classify previous location verification algorithms into two categories, namely, *on-spot* verification and *in-region* verification. On-spot verification is to verify whether a sensor's true location is the same as its estimated location (or with very small errors). Most existing verification algorithms, belong to this category. To obtain the desired on-spot verification results, these algorithms either utilize the deployment knowledge of sensors in the field or make use of some dedicated hardware to verify distance measurements. For example, in, it is assumed that some *covert base stations* are deployed throughout the field. These special base stations communicate with one another through wired links and purposely hide their existences from being discovered by sensors. Then these base stations can verify sensors' locations by checking whether the distances calculated using sensors' estimated locations are the same as the distances they directly measure using RF signals. In, it is required that sensors are able to measure time in nanoseconds in order to detect range reductions that directly impact the localization results. Since existing verification algorithms either require deployment knowledge or depend on hardware that are expensive and generally unavailable in low-cost wireless sensor systems, a lightweight verification algorithm should be designed that can effectively perform on-spot verifications. Besides the on-spot verification, some research effort has also been devoted to designing in-region location verification algorithms. Shankar and Wagner first defined the concept of in-region verification N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims", in ACM Workshop on Wireless Security *(WiSe)*,2003. They also proposed a protocol named *Echo* to verify if a sensor is inside a physical region such as a room, a building or even a sport stadium. Based on the verification result, it can be decided whether to assign sensors (i.e., people who take the sensors) the accessing right to some resources in that physical region. As the first work, *Echo* successfully utilizes in-region verification to facilitate location-based access, however, it cannot be directly used Digital Object Indentifier for other location-based applications, because the verification region may not be explicitly given and needs to be determined carefully by analyzing applications' functions. Secondly, when performing in-region verification, *Echo* requires the use of multiple *verifiers* that can transmit radio signal and receive ultrasound signal, and bound their XOR operations within the magnitude of nanoseconds. Such verifiers increase the expense and require extra deployment efforts. In this paper, we designed a verification system that overcomes the shortcomings of previous research. The verification system can effectively verify whether sensors' estimated locations are trustable. According to the specific requirements, the system can provide either *on-spot* or *in-region* verification results. First, to provide on-spot verification service, two algorithms can be used by our system, namely, the Greedy Filtering by Matrix (GFM) algorithm and the Greedy Filtering by Trust ability-indicator (GFT) algorithm. Both algorithms exploit the inconsistency between sensors' estimated locations and their "neighborhood observations" (the messages that each sensor can receive from other sensors in its neighborhood). Second, to perform in-region verification, a *verification region* is first calculated according to the applications' functions, then a probabilistic algorithm is used to compute the confidence that a sensor is inside the verification region. All algorithms proposed in this paper are lightweight because they do not require any dedicated hardware or infrastructures, and they do not incur high computation overhead at the sensor side, so that the verification system can be applied to low-cost wireless sensor networks. Moreover, they are robust against malicious attacks that are launched by sophisticated attackers who try to exploit the system's weakness. Simulation results prove the effectiveness of our verification system.

II PROBLEM AND ANALYSIS

In recent years, a large number of localization schemes T. He, C. Huang, B. Blum, J. Stankovic, and T. Abdelzaher, "Range- Free Localization Schemes in Large Scale Sensor Network", in *ACM MobiCom*, 2003. D. Moore, J. Leonard, D. Rus, and S. Teller, "Robust distributed network localization with noisy range measurements", in Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems (*ACM SenSys*), 2004. D. Nicolescu, and B. Nath, "Ad-Hoc Positioning Systems (APS)", in *IEEE GLOBECOM*, 2001. D. Niculescu, and B. Nath, "Dv based positioning in ad hoc networks", in Journal of Telecommunication Systems, 2003. A. Youssef and M.

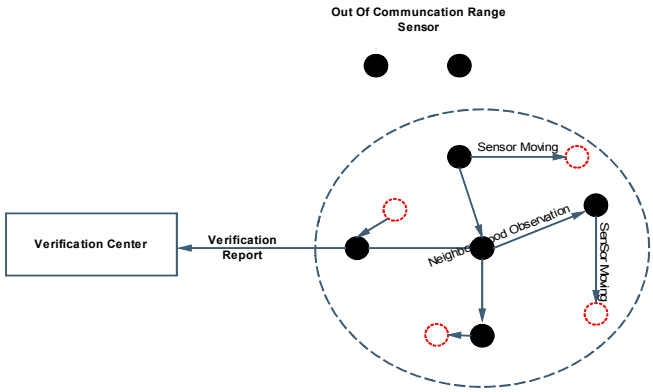
Youssef, “A Taxonomy of Localization Schemes for Wireless Sensor Networks”, In ICWN, pages 444-450, 2007. Y. Zeng, J. Cao, J. Hong, S. Zhang, and L. Xie, “Secure localization and location verification in wireless sensor networks: A survey”, the Journal of Supercomputing, pages 1-17, 2010. Because localization schemes can be compromised by malicious attackers, who can launch wormhole attack, range enlargement/reduction attacks, many secure localization schemes are designed. For instance, Lazos et al. proposed SeRLoc , SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks”, which utilizes directional antennas equipped on anchors to detect wormholes. As an improvement to the SeRLoc, they later introduced High-resolution Robust Localization for WSNs (HiRLoc). This algorithm also makes use of directional antennas but the communication range of locations is variable. Other approaches use stochastic methods to filter out bad location references. Since these algorithms run on sensors which have very limited resources, some improvement methods have been developed for fast computing of region intersections. These secure localization schemes mainly aim to enhance innocent sensors’ ability to correctly localize themselves, in presence of malicious attacks. However, since sensors may not be innocent, i.e., they are easily be compromised, they report false locations directly to the command center. Therefore, location verification is necessary to defend against such attacks. The location verification problem was first addressed, in which Sastry, et al proposed Echo protocol to verify if a device is inside some physical region, such as a room or a football stadium. The Echo protocol is mainly to provide location-based access control, and cannot be directly applied for location verification in other applications. Capkun and Hubaux proposed the Verifiable Multilateration (VM) technique to verify whether a sensor’s estimated location is at its true location using the distance-bounding protocol. Some other solutions K. Rasmussen and S. Capkun, “Location privacy of distance bounding protocols”, in Proc. of the 15th ACM Conference on Computer and Communications Security (CCS’08), pp. 149-160, Oct 2008. J. T. Chiang, J. Haas, and Y.-C. Hu, “Secure and precise location verification using distance bounding and simultaneous multilateration”, in Proceeding of the 2nd ACM Conference on Wireless Network Security (*WiSec*’09), pp. 181-192, 2009. . Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, “Position based cryptography,” in Proceeding of *CRYPTO* ’09, pp. 391-407, 2009. were also proposed to perform location verifications by exploring the trusted network infrastructure. Most of these solutions utilize distance bounding techniques, in which the verifier challenges sensors and measures the elapsed time before they receive sensors’ responses. Recently, Capkun et al. proposed *covert base stations* (CBS) which can keep their existence and communications unknown to sensors. These algorithms provide on-spot verification results, i.e., if a sensor’s claimed location is the same as its true location, thus they require some extra expensive hardware to be deployed through the field. Some lightweight verification schemes that do not require extra infrastructures have also been proposed. Du, et al. presented the location anomaly detection (LAD) scheme that examines the consistency between sensors’ estimated locations and the deployment knowledge of the sensor field. Ekici, et al. proposed the probabilistic location verification (PLV) algorithm that explores the probabilistic relation between hop-counts and Euclidean distance between source and destination. In our earlier version of this paper which was published in ICDCS’07, we introduced Greedy Filtering by Matrix (GFM) algorithm and Trustability Indicator (TI) algorithm , to explore the consistency between sensors’locations and their neighborhood observations to detect location anomalies. Recently, Talasila, et al. proposed a location authentication protocol , which is named LINK (Location verification through Immediate Neighbors Knowledge). In their algorithm, a centralized Location Certification Authority (LCA) receives a number of messages from sensors and their neighbors, then decides whether the claim is authentic based on spatio-temporal correlation between the users, trust scores,However, most of previous lightweight algorithms focus on detecting location anomalies, namely, verifying if sensors’ claimed locations are far away from their true locations. They do not take into consideration the application’s requirements on the accuracies of sensors’ locations. From this sense, ours is the first work that attempts to study an application’s location-related functions and propose lightweight verification algorithm to facilitate the application’s operations.

III SOLUTION AND MECHANISM

The proposed greedy filtering algorithms GFM

and GFT rely on the inconsistencies between sensors' geographical relationships according to their claimed locations and those implied by their neighborhood observations. First, GFM explores the inconsistency directly by comparing the elements in two matrixes, the Estimation Matrix and the Observation Matrix.GFT detects the location anomalies indirectly based on the indicators which indicate the inconsistencies. Second, the GFM algorithm filters out bad locations as soon as one of the metric values is not accepted according to the threshold. Sensors not revoked will be verified in the final round. In GFT algorithm, instead, the good location claims are accepted first, and after multiple rounds when indicators of remaining sensors become stable, the sensors with indicators below the threshold will be revoked. The probabilistic location verification (PLV) algorithm that explores the probabilistic relation between hop-counts and Euclidean distance between source and destination. The location authentication protocol which is named LINK (Location verification through Immediate Neighbors Knowledge). In their algorithm, a centralized Location Certification Authority (LCA) receives a number of messages from sensors and their neighbors, then decides whether the claim is authentic based on spatio-temporal correlation between the users, trust scores

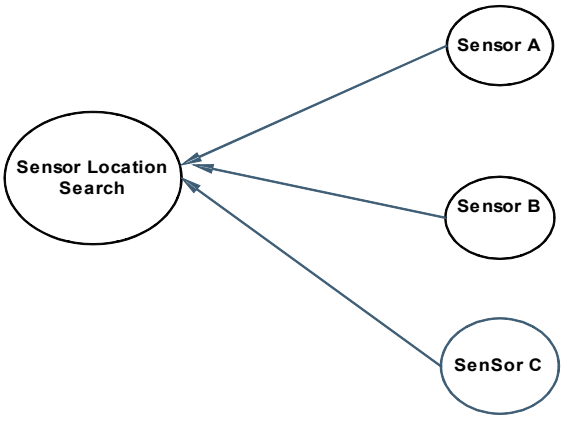
SYSTEM ARCHITECTURE



Modules

Sensor Location Search:

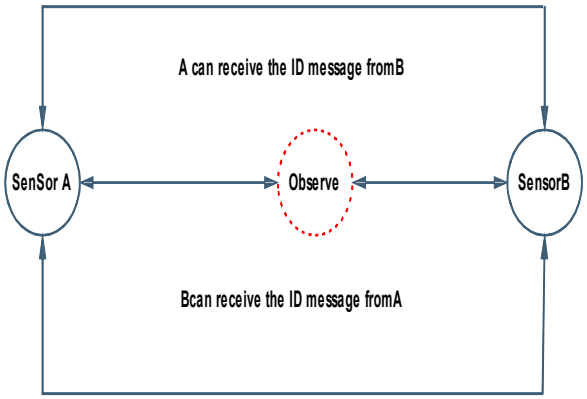
Sensor Location Search Module is the main module of this application to find out the how many sensor are connected in local area network. As the first work, successfully utilizes in-region verification to facilitate location-based access, however, it cannot be directly used. For other location-based applications, because the verification region may not be explicitly given and needs to be determined carefully by analyzing applications' functions.



Neighborhood observation:

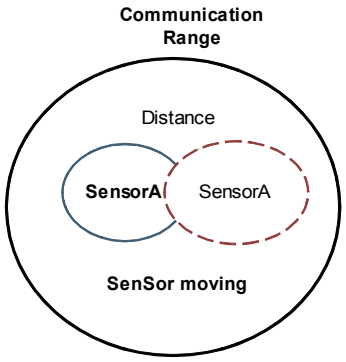
The communication range of a sensor is a circle centered at the sensor's true location and has a certain radius. We assume all sensors' communication ranges have the same radius. Each sensor broadcasts its ID within its communication range, and passively overhears IDs broadcast by other sensors. We say

sensor A can observe sensor B, if A can receive the ID message from B. And we name the list of IDs that a sensor observes the sensor's neighborhood observation.



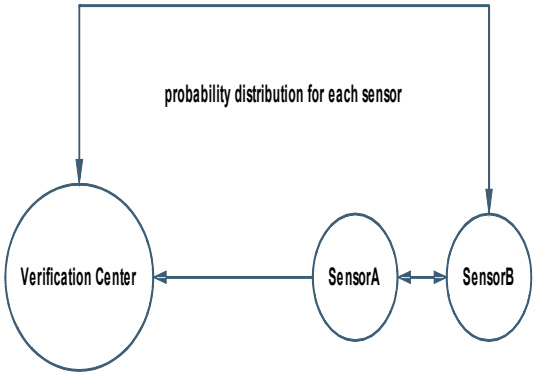
On Spot Verification:

A sensor's localization error is less than a certain distance. Let *True* and *Lest* denote the true location and the estimated location of a sensor, then the verification fails if the following condition holds true: $|Ltrue - Lest| > D$, where D is named the *Anomaly Degree*. The value of D should be set properly with the considerations of the application requirements and the value of "normal" localization errors that are present in no-attack environment. It considers D as an input parameter and assumes its value has already been given to our system.



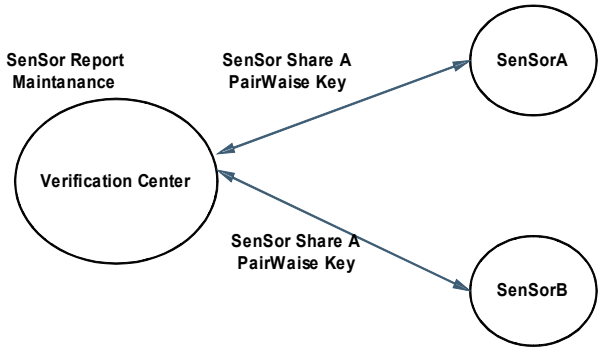
In-region Verification:

Basically, if two sensors observe each other, then the VC considers them to be a pair of "confirmed" neighbors. Then, VC derives a probability distribution for each sensor, which indicates how probably the sensor is at each point in the field. The distribution function can be either continuous or discrete. In the continuous version, the in-region confidence is computed by taking the integral of the distribution function within the verification region; In the discrete version, the in region confidence is the sum of the probabilities of all points within the verification region.



Verification Center

Verification Center (VC) that verifies if sensors' estimated locations are acceptable. The VC resides at the base station or control center, and can be safely protected from the attackers. Each sensor reports its estimated location and its neighborhood observation to the VC. We assume each sensor shares a pair wise key with the VC, so they can encrypt the message and authenticate themselves. Such pair wise keys can either be preloaded off-line into sensors' memories, or distributed online using some existing key distribution algorithms finally; any routing protocol may be potentially used to route sensors' reports to the VC except the location-based routings, and because sensors' locations are not trustworthy and wrong locations will lead to loops or even delivery failures.



IV CONCLUSION

In this paper, we propose a lightweight location verification system that performs both "on-spot" and "in-region" location verifications. The GFM and GFT algorithms verify whether the locations claimed by sensors are far from their true spots beyond a certain distance. Sensors' neighborhood observations are explored for the information inconsistencies. The in-region verification verifies whether a sensor is inside an application specific verification region. A probabilistic method is designed to provide the confidence that a sensor is inside the verification region. Our work takes the first step to integrate the application requirements in determining the trust ability of sensors' estimated locations. Moreover, our proposed verification system is more lightweight, effective and robust compared to previous works. It does not require any dedicated or expensive infrastructures in the field; it yields satisfactory verification results to a variety of applications, which is approved by the simulation results; furthermore, it is resilient to malicious attacks and can be used in hostile environments.

REFERENCE

[1]. W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "pairwise key predistribution scheme for wireless sensor networks", in Proc. ACM CCS, pp. 42-51, 2003.

[2]. W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "key management scheme for wireless sensor networks using deployment knowledge", in Proc. IEEE INFOCOM, 2004.

[3]. D. Liu, N. Peng, and W.K. Du, "Attack-Resistant Location Estimation in Sensor Networks", in *ACM/IEEE IPSN*, 2005.

[4]. Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust Statistical Methods for Securing Wireless Localization in Sensor Networks", in *ACM/IEEE IPSN*, 2005.

[5]. S. Brands and D. Chaum, "Distance-bounding protocols", in Workshop on the theory and application of cryptographic techniques on Advances in cryptology. Springer-Verlag New York, Inc., 1994, pp. 344C359.

[6]. S. Capkun and J. P. Hubaux, "Secure Positioning of Wireless Devices with Application to Sensor Networks", in *IEEE INFOCOM*, 2005.

[7]. N. Tippenhauer and S. Capkun, "Id-based secure distance bounding and localization", in Proceeding of *ESORICS* '09, pp. 621-636, 2009.

[8]. S. Capkun, M. Cagalj, and M. Srivastava, "Secure Localization With Hidden and Mobile Base Statioins", in *IEEE INFOCOM*, 2006.

[9]. W. Du, L. Fang, and P. Ning, "LAD: Localization anomaly detection for wireless sensor networks", in Proceedings of IEEE International Parallel and Distributed Processing Symposium (*IPDPS*), 2005.

[10]. E. Ekici, J. McNair, and D. Al-Abri, "A Probabilistic Approach to Location Verification in Wireless Sensor Networks", in Proceedings of IEEE International Conference on Communications (*ICC*), 2006.

[11]. L. Lazos and R. Poovendran, "Hirloc: high-resolution robust localization for wireless sensor networks", in IEEE Journal on Selected Areas in Communications, 24(2):233-246, 2006.