ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Securing and Region Based Algorithms For Wireless Sensor Networks

M.M.Chithra[1], A.Gayathri[2], S. Selva Birunda[3]

PG Students, V.P.M.M.Engineering College For women, Krishnankovil1, Tamilnadu, India[1, 2]

AP/CSE, V.P.M.M.Engineering College For women, Krishnankovil, Virudhunagar Dist, Tamilnadu, India[3]

ABSTRACT –The knowledge of sensors' locations is crucial information for many applications in Wireless Sensor Networks. 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 region based 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. We study how to derive the verification region for different applications and design a probabilistic algorithm to compute in-region confidence for each sensor. They are robust in the presence of malicious attacks that are launched during the verification process. By using the location based pseudorandom authentication protocol we can overcome the problems which all are occurred by this algorithms.

KEYWORDS—Localization, verification, on-spot, in-region, security, wireless sensor, Networks, location pseudorandom authentication protocol.

I. INTRODUCTION

Localization in wireless Sensor Networks is to know about the location of a node. It is very useful in many applications such as environmental monitoring etc., the attackers can compromise sensors and inject false location information and they can also interrupt signal transmission between sensors and contaminate distance measurements. Some secure algorithms are used to help enhance sensor's resistance to attacks but they cannot completely wrong location estimations.

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. 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 region measurements. These special base stations communicate with one another via the wired links and hide their existences from being discovered by sensors. The base stations will 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.

As the first work, Echo successfully utilizes in-region verification to facilitate location-based access, however, it cannot be directly used for other location-based applications, because the verification may not be explicitly given and needs to be determined carefully by analyzing applications' functions. Second, 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

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 Trustability-indicator (GFT) algorithm. Both algorithms exploit the inconsistency between sensors' estimated locations and their neighborhood observations. 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. In this paper we are using the random partition mechanism is used to divide the pseudorandom identifier and pre-shared secret value for bitwise operations to overcome the problems occurred in the verification algorithms.

II. SYSTEM MODEL AND ASSUMPTIONS

In our system, all sensor nodes can estimate their locations in the field using any of the existing localization schemes. These locations are called sensors' estimated or claimed locations, and the distances between sensors' estimated locations and true locations are called localization errors. 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. Notice that environmental interruptions and permutations exist, so that neighborhood observation is not always symmetric. For example, sensor B may not observe sensor A when A observes B. We consider such asymmetry in our design. Our system is consisted of ordinary sensors and a 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 pairwise key with the VC, so they can encrypt the message and authenticate themselves. Such pairwise keys can either be preloaded offline 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, because sensors' locations are not trustworthy and wrong locations will lead to loops or even delivery failures. The only assumption we make about the attackers is that in a local area, the attackers are not the majority compared with benign ones. For example, if a sensor has five neighbors and more than three of them are compromised, then the chance that the VC could still correctly verify the sensor's location is small. We notice such attacks are very expensive to launch because the attackers need to compromise many sensors in order to distort one location estimation. We leave the study of defending against such local dominating attackers to our future research.

III. PROBLEM STATEMENT

In this paper, we intend to design a verification system in which the VC can effectively determine if sensors' estimated locations are trustable. According to the requirements of different applications, the system should provide either on- spot or in-region verification results. On-spot verification is to verify whether a sensor's estimated location is away from its true location less than a certain distance; in-region verification, on the other hand, is to verify whether a sensor is within a geographical region given that its estimated location is in that region. If the verification succeeds, the location will be recognized by the VC as a correct location; otherwise, it will be recognized as a wrong one. On-spot verification is to verify whether a sensor's localization error is less than a certain distance. Let L 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. In this paper, we consider D as an input parameter and assume its value has already been given to our system. In-region verification is to verify whether a sensor is inside a physical region or not. The region may be different for each location-based application. Given an application, we define a physical region in which if a sensor can be verified, then the application goal can be achieved

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Application goal is fulfilled →, Li € Vi, where Li is the location of sensor Si, and Vi is the verification region.

IV. LIGHTWEIGHT ON-SPOT VERIFICATION

In this section, we propose two algorithms for on-spot verification. The first one is named Greedy Filtering using Matrix. The second one is named Greedy Filtering using Trustability indicator. Both algorithms utilize the inconsistency between sensors' estimated locations and neighbor- hood observations.

4.1 Greedy Filtering Using Matrix The first step in the verification process is that each sensor broadcasts its ID within its communication range and meanwhile overhears the IDs broadcast by other sensors. We denote sensor Si's neighborhood observation by Oi.

4.1.1 Constructions of Matrixes

Suppose there are totally n sensor nodes in the field denoted by S1,…,Sn. For convenience, we assume sensor Si's ID is integer i where i€{1,…. N}.In GFM algorithm, five nxn square matrixes are calculated based on the reported information from sensors.

a)Observation matrix. This matrix is computed using sensors' neighborhood observations. Elements in this matrix are either 1 or 0 depending on whether sensors can observe each others.

b)Estimation matrix. This matrix is computed using sensors' estimated locations.

c)Difference matrix. This matrix is calculated by XOR ing the observation matrix and the estimation matrix

d)Weight matrix. In our experiment, we randomly deploy 1,200 sensors in the field. Sensors' communication range is R =20 m and the anomaly degree is given by D = 10 m.

e)Inconsistency matrix. We multiply each element in the difference matrix with the corresponding element in the weight matrix.

4.1.2 Metric for Filtering Abnormal Locations

Active Difference Metric:This metric quantifies the consistency between sensor Si's neighborhood observation and the estimated locations.

Passive Difference Metric:This metric quantifies the inconsistency between other sensors' observation on Si and the estimated locations of sensors.

Asymmetry Metric: In non attack environment, sensors' observations are not symmetric due to environmental disturbance.

Consistent-Neighbor Metric: This metric counts the number of a sensor's consistent neighbors. Here we define that a sensor Sk is a consistent neighbor of sensor Si if it can observe Si and its estimated location is in the communication range of Si's estimated location.

4.1.3 Greedy Filtering Procedure

In this section we describe how GFM algorithm calculates all the above matrixes and utilizes filtering metrics to greedily filter out abnormal locations.

VC computes matrix Minc and metrics ADi, PD i, and ASi for all i €{ 1;2;...n}.If there is any sensor whose metric value exceed that metric's threshold, VC revokes the sensor that has the largest metric value (say node Sk), and sets all zeros to the kth row and the kth column in matrixes Me, Mo, and Minc. This process repeats until no more sensors can be filtered out. Then the metric CNi is considered: sensors that do not have enough number of consistent neighbors are revoked. Finally, the remaining sensors are accepted by the VC as correctly localized sensors.

4.2 Greedy Filtering Using
Trustability-Indicator

In GFT algorithm VC determines a trustability indicator for each sensor and updates the indicator's value in multiple rounds. If the value is higher than the threshold the sensor is accepted as correctly localized sensor. Finally sensors have lower than the threshold are detected and revoked.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

4.2.1. Calculation of Weights

For each sensor that can observe Si,if its estimated location is within communication range of sensor Si's estimated location ,then this sensor is considered neighbor, otherwise, it is considered as an inconsistent neighbor.

Compute the weight using consistent neighbor:

We discuss how to compute Tk ij using a consistent neighbor. The distance between sensor Si's and Sj's estimated locations is dij; R is the radius of the communication range; D is the anomaly degree. Verifying whether sensor Si's localization error is smaller than D equals verifying whether Si's true location is in the circle Cr. Thus, we compute the following probability:

P(Si € Cr)=P(Si €Cr| Si € Cl).P(|Si € Cl)

+P(Si€Cr|Si€Cl).P(Si€Cl)≈P(Si€Cr|Si€ Cl)=(So/S1).f(dij) where the approximation follows because the conditional probability P(Si €Cr|Si€Cl) is very small.

Compute the weight using inconsistent neighbor:

We compute the probability that sensor Si cannot be verified, namely, the probability that sensor Si's true location is outside the circle Cr. To the opposite of consistent neighbors, inconsistent neighbors should reduce the trustability of sensor Si's location, therefore, we decrease Si's previous indicator by the amount.

4.2.2 Greedy Filtering Procedure

In each round VC updates each sensor's trustability indicator, and then verifies that sensor's locator value is higher than the threshold value. If a sensor's indicator changes with negligibly small amount in two consecutive rounds, VC recognizes that the indicator has converged and stops updating its value. Threshold can be obtained through training on experimental data.

V. LIGHTWEIGHT IN-REGION VERIFICATION

In this section we are going to propose that how to determine the region inside which a sensor's location should be verified. Here we are using the following considerations.

5.1 Verification Region Determination

Given a location-based application, we define the verification region as the physical region inside which the sensor should be verified if and only if the application goal can be achieved

Application goal is fulfilled↔ Li€Vi

where Li is the true location of sensor Si, and Vi is the verification region for sensor Si. Notice that the verification region for different sensors may be different. In addition, we define two variants to the above region, and name them sufficient region and necessary region, respectively,

Application goal is fulfilled←Li€Vi where Vi is the sufficient region and Vi is the necessary region. From the geographical point of view, region Vi is fully contained by region Vi.

5.2 In-Region Verification

This algorithm also utilizes sensors' neighborhood observations. 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.

5.2.1 Scored Districts

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Communication range is the region that gives the sensor's true location with radius R. Here we are using Estimated Communication Range which is an circle gives the sensor's estimated location. VC uses the VCR's region divides the field into several region.

We notice that a sensor may not be inside the highest scored district, because the ECRs are estimated communication ranges and may not cover a sensor's true location.

5.2.2 Continuous Distribution

The probability density function value gives the sensor's reside in different location. Let us assume that the probability density within one district is uniform. If the sensor has same number of confirmed neighbors at two points within one district then the two points will not be differentiated statistically. The formula for calculating the pdf fuction for sensor si can be given by following:

Pdfi(l)=Pr(Li€ Dim),

S(Dim) where the dividend Pr(Li€ Dim)is the in-district probability

5.2.3 Discrete Distribution

The weights corresponding to the zero scored district have very small values and the area of zero scored district is very large. Therefore the probability density inside zero scored district will be very small. Based on this observation, our algorithm VC determines a potential scope.

5.2.4 Verification Confidence

The verification confidence is the confidence that a sensor can be verified within the verification region. If the distribution is continuous, the in-region confidence is computed by taking the 2D integral of the probability density function in within the verification region

Pr(Li€ Vi)=∫∫vi pdfi (x ,y) dx dy

If the distribution is discrete, the in-region confidence is the addition of probabilities of all points in the verification region

Pr(Li € Vi)=∑ pmfi(l).I(l€ Vi)

l€Pi

VI. SECURITY ANALYSIS

The nature of the WSN makes them vulnerable to several types of attacks. Such attacks can be perpetrated in a variety of ways, most notably are the denial or service attacks (Dos) but there are also traffic analysis attacks, eavesdropping, physical attacks, and others. If the sensor's locations wrongly estimated, they can also attack the verification algorithms to make they can also attack the verification algorithms to make abnormal locations not detected by the VC. In GFM algorithm attackers can compromise a sensor and produce fake neighborhood observation. In GFT algorithm, since consistent neighbors can increase a sensor's indicator, attackers may sophisticatedly generate consistent neighbors around a victim sensor. In the in-region verification algorithm, since the VC relies on sensors' neighbor- hood observations to derive probability distributions, the attackers can distort neighborhood observations. It is important that our algorithm is robust in presence of malicious attacks. Because of space limitation.

VII. FUTURE WORK

The verification problem was first proposed by Echo protocol to verify if a device is inside some physical region such as a room or football stadium. But this protocol cannot be directly applied for location verification in other applications. Most of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

the solutions utilize distance bounding techniques. The covert base stations which can keep their existence and communications unknown to sensors. These algorithms provide on-spot verification results, 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. The location anomaly detection (LAD) scheme that examines the consistency between sensors' estimated locations and the deployment knowledge of the sensor field. 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 .But these algorithms will determine the location only on the specified region. By applying the random partitions mechanism of the pseudorandom authentication protocol the random partitions provide relative robust security with dynamic update mechanism and double-entity-round mutual authentication mechanism, which can withstand the typical attacks efficiently. Moreover, lightweight bitwise operations are required to realize eximious functions, and it can be applied to low-cost and resource-limited for all the nodes.

VIII. CONCLUSION

In this paper we proposed the region based verification algorithms for wireless sensor networks. These are determine the location only the particular region, not in the entire region. In future to improve the performance,security we will use Location based Pseudorandom Authentication protocol. The random partitions provide relative robust security with dynamic update mechanism and double entity round mutual authentication mechanism, which can withstand the typical attacks efficiently.

REFERENCES

[1]W. Du, J. Deng, Y.S. Han, and P.K. Varshney, "Pairwise Key Pre- Distribution Scheme for Wireless Sensor Networks," ACM Trans. Information and System Security, vol. 8, pp. 42-51, 2003.

[2] W. Du, J. Deng, Y.S. Han, S. Chen, and Y.S. Han, S. Chen, and P.K. Varshney, "Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," Proc. IEEE INFOCOM, 2004.

[3] D. Liu and P. Ning, "Improving Key Pre-Distribution with Deployment Knowledge in Static Sensor Networks," ACM Trans. Sensor Networks, vol. 1, no. 2, pp. 204-239, 2005.

[4] Z. Yu and Y. Guan, "Key Pre-Distribution Scheme Using Deployment Knowledge for Wireless Sensor Networks," Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN '05), pp. 261-268, 2005.

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

[6]A.Kerckhoffs, La cryptographie militaire, Journal des sciences militaires. IX(1):5C38, IX(2):161C191. 1883.

[7] T. He, C. Huang, B. Blum, J. Stankovic, and T. Abdelzaher, "Range-Free Localization Schemes in Large Scale Sensor Net- work," Proc. ACM Mobi Com, 2003.

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

[9]Yawen wei and Yong Guan "Lightweight
Location Verification Algorithms for Wireless Sensor Networks" IEEE Transactions on Parallel and Distributed Systems,VOL.24,NO.5,pp 938-950.,2013.