ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

A Robust and Effective Detection of Anomaly Location in Wireless Sensor Networks

Sheela T, Ramkumar N

Dept. of ECE, Dhanalakshmi Srinivasan Engineering College, Perambalur, India.

Dept. of ECE, Dhanalakshmi Srinivasan Engineering College, Perambalur, India.

ABSTRACT--In wireless sensor network localization schemes are used to knowing the location of all sensor nodes. But some localization is subjected to many malicious attacks in the network such as wormhole attack. Since sensors locations are not truthful, there is a need to verify the sensors' locations whether it is trustable or not. To detect the abnormal location in wireless sensor networks, more verification schemes are used previously. This paper proposes a technique that performs "Distributed in-region verification". Distributed In-region verification algorithm intends to verify whether a sensor is inside an application verification region or not. To strengthen the detection accuracy and energy efficiency in the in-region algorithm, distributed verification center is implemented. Since each sensor node communicates with the corresponding verification center, collision is avoided. Through the use of single verification center for each region, energy consumption will be reduced. Therefore the detection accuracy is highly achieved in the network.

KEYWORDS— Wireless sensor network, Localization , in-region, Location verification**.**

I. INTRODUCTION

Wireless sensor network is a huge network. It is a new technology that consists of spatially distributed autonomous sensors mainly for monitoring functions. Military applications and many civilian applications require monitoring that can identify objects in a specific area. Monitored areas that are large relative to objects of interest often require multiple sensors. One of the important factors of wireless sensor network is localization process that knows the location of sensor nodes. This factor is important for many applications such as environment monitoring, geographical routing, target tracking and many others. Wireless sensor networks may be deployed in hostile environment, where sensors' localization is subjected to many malicious attacks such as wormhole. Also attackers can compromise sensors and inject false location information; they can also interrupt signal transmission between sensors and contaminate distance measurements. So the locations estimated in the localization process are not correct always. Although some localization algorithms [4], [5], [6], [7], [8] were proposed to verify the sensor locations, but they cannot performs efficiently. So we consider this problem as necessary one to workout. One of the previous algorithms [1] describes the on-spot verification algorithm and in-region verification algorithm.

On-spot verification is to verify whether a sensor's true location is the same as its estimated location or with very small errors and most existing verification algorithms [8], [9] belong to this category. These algorithms either utilize the deployment knowledge of sensors in the field or make use of some dedicated hardware to verify distance measurements. In sensor network covert base stations-special base station 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. Some cases it is required that sensors are able to measure time in nanoseconds in order to detect range reductions that directly impact the localization results. Though existing verification algorithms either require deployment knowledge or depend on hardware that is expensive. A lightweight verification algorithm designed for effectively performs on-spot verifications [1]. Besides the on-spot verification, some study effort has also been devoted to designing in-region location verification algorithms too.

In this paper, we designed a verification system that overcomes the shortcomings of previously used algorithms. This proposed verification system can effectively verify whether sensors' estimated locations are trustable. This proposed system can provide distributed in-region verification results. For that it uses distributed verification algorithm. This verification algorithm, first calculate the verification region, and then a probabilistic algorithm is used to compute the confidence about the sensor inside the region. This system is robust against malicious attacks that are launched by sophisticated attackers.

II. SYSTEM MODEL

This system is consisted of ordinary sensors and a Verification Center (VC) that verifies the sensor locations which is acceptable or not. The VC resides at the base station and safely protected from malicious attcker. In this system, estimated location of each sensor is reported along with its neighborhood observation to the VC. To encrypt the message and authenticate, each sensor shares a pairwise key with the VC. Pairwise keys can either be preloaded offline or distributed online using some existing key distribution algorithms. Though the sensors' locations are not trustworthy and wrong locations will lead to loops or even delivery failures, routing protocol used to route sensors' reports to the VC except the location-based routings.

In our system, all sensor nodes can estimate their locations in the field using any of the existing localization methods. The communication range of a sensor is a denoted as long circle and has a certain radius for each communication range. Dark circle denotes the range of the sensor s4 and s1, s2, s3, s5, s6, s7, s8, s9, s10 are the neighbours based on the true location of s4. We assume all sensors' communication ranges have the same radius and each sensor broadcasts its ID within its communication range, and passively overhears ID of other sensors[1]. But based on the estimated locations of all the sensors s5 goes out of range of s4 which stops s5 from being the neighbour of s4. Using this contradiction localization error of the sensor can be identified by the verification centre. To deceive the VC into accepting wrong locations, multiple attackers can collude together and the only assumption we make about the attackers is that in a local area. The thing is the attackers are not the majority compared with benign ones.

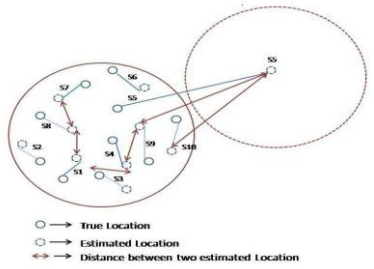


Fig.1 System model

III. PROBLEM STATEMENT

Sensor networks may be deployed in hostile environments, where sensor nodes can be compromised, beacon nodes (Other sensors node discover their locations based on the reference information provided by these beacon nodes. which already know their absolute locations via GPS or manual configuration.) can be compromised, communication can be redirected, etc. Most of the localization schemes are designed to work in environments where all the beacon nodes behave correctly; when those nodes can be compromised and act maliciously, sensors using the existing localization schemes might be mislead to believe that they are in locations far away from their actual locations. This can cause severe consequence. For example, when sensor networks are used for battle field's surveillance, if sensors are mislead by enemies, such that their derived locations are far off, then when sensors report that their regions are safe, this wrong information can cause The estimated sensor of the neighbors is divided into number of regions. Each region has a score value which is the number of the estimated communication range that covers this region. It also contains the same score value with two or more number of region. So these regions are under the same scored value. A sensor may not be inside the highest scored value, because estimated communication ranges may not cover a sensor's true location. So, it is assigned the probability for each sensor nodes. If the probability of sensor node is high, a sensor is inside a higher scored district is higher. Then verification center is assigned

the weights for the appropriate neighbors with scored valuessignificant damage. In a wormhole attack, an attacker records a packet or individual bits of a packet at one location in the network [5]. Then, it tunnels the packet (possibly selectively) to another location and replays it. Therefore, it will be of great importance if sensors can discover whether their derived location is correct or not

IV. IN-REGION VERIFICATION

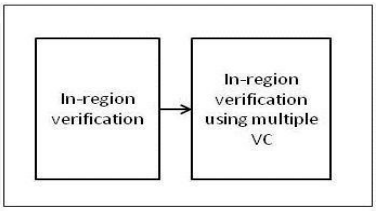
In this section, we propose a lightweight algorithm that the VC can use to perform in-region verification and distributed in-region verification

In-region verification

In-Region Verification is used to determine the region inside which a sensor's location should be verified. In-Region Verification each sensor reports the estimated location and neighborhood to verification center. Fig 2a shows the steps taken in in-region algorithm [1]. Verification center finds the estimated sensor (estimated location) of the neighbors. These neighbors are within the communication range of the estimated sensor.

The estimated sensor of the neighbors is divided into number of regions. Each region has a score value which is the number of the estimated communication range that covers this region. It also contains the same score value with two or more number of region. So these regions are under the same scored value. A sensor may not be inside the highest scored value, because estimated communication ranges may not cover a sensor's true location. So, it is assigned the probability for each sensor nodes. If the probability of sensor node is high, a sensor is inside a higher scored district is higher. Then verification center is assigned the weights for the appropriate neighbors with scored values**.**

Distributed in-region verification

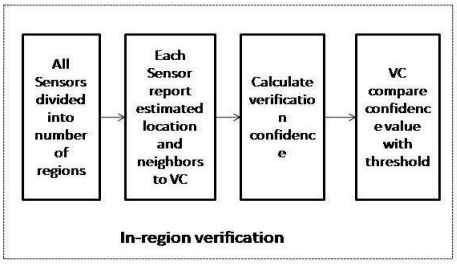


2b distributed in-region verification

A distributed in-region verification algorithm use single verification center for each region. Steps taken in distributed algorithm shown in Fig 2b. For each regions within the verification center calculates the in-region confidence for sensor nodes. After calculates the in-region confidence value for sensor nodes with compared to threshold values. The main advantages of using multiple verification centers in the network are reducing communication overhead, energy savings. Due to the usages of single verification center for each region, communication overhead involved in the network will be reduced. Through the use of multiple verification center number of hops, packet loss in the data transmission will be reduced. Hence the detection accuracy is highly achieved in the network.

V. PERFORMANCE EVOLUTION

By analyzing the verification schemes used , we observe that detection rates of on-spot verification algorithms increases when network density increases. For example, when the number of sensors increases from 400 to 700, GFM 's the detection rate raises from 65 to 85 percent, so the false positive rate is maintained at 5 percent[1].



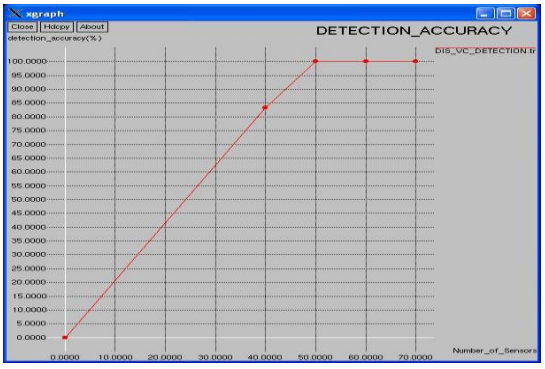


Fig 3a False positive rate ofdistributed in-region

Fig 3a depicts the false positive rate of distributed - region verification algorithm. The graph shows that false positive ratio of wireless sensor network in stable at certain point. Hence the rate is efficeint than exisitng algorithms. Fig 3b shows the energy consumption of in-region verification algorithm which tells about , better energy consumption than on-spot verification algorithms.

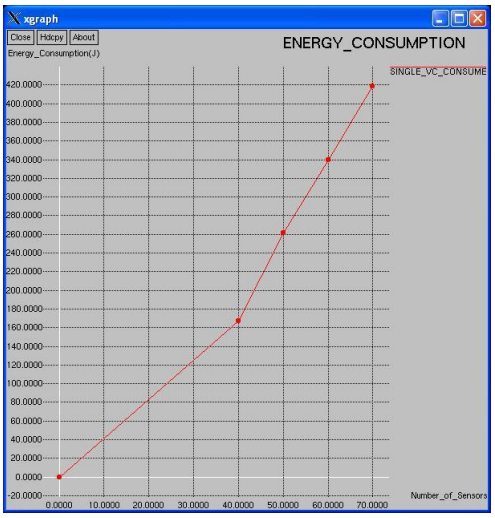


Fig 3b Energy consumption

When think about in-region verification algorithm using of single verification center which results in more communication overhead and packet loss occurrence. Fig 3a depicts the detection accuracy for distributed in-region verification algorithm. Fig 3b shows the false positive rate of distributed in-region verification algorithm. Detection accuracy rate is even better than existing one, as well false positive rate shows the better performance.

VI. COMPARISON TO PREVIOUS WORK

Existing location verification algorithm provides good results althougth our proposed one gives better than existing one. While compare to existing in-region verification algorithm, energy consumption of wireles sensor node is high than proposed algorithm. Fig 4a shows the comparison between the false positive rate of GFM, GFT and on-spot algorithms. that the detection accuracy of distributed VC and single VC is increased with increase of number of sensors.

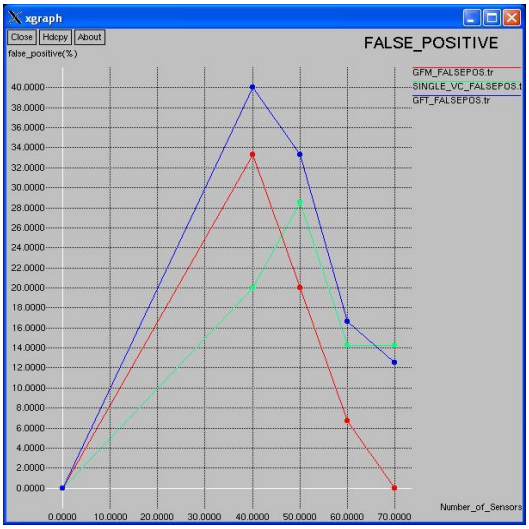


Fig. 4a False positive rate

The false positive rate of GFM, GFT and in-region is decreased as the network density increases. Hence GFM outperforms for both of the GFT and in-region verification algorithms[1]. Fig 4b shows the comparison of Detection accuracy of single VC and DVC. The detection accuracy of GFM, GFT and in-region is increased as the network density increases. The detection accuracy of GFM and GFT is high compared with the detection rate of GFT and In-region. Since GFM and GFT is detected the abnormal locations by consistencies and inconsistencies between sensors' claimed locations and their neighborhood observations.

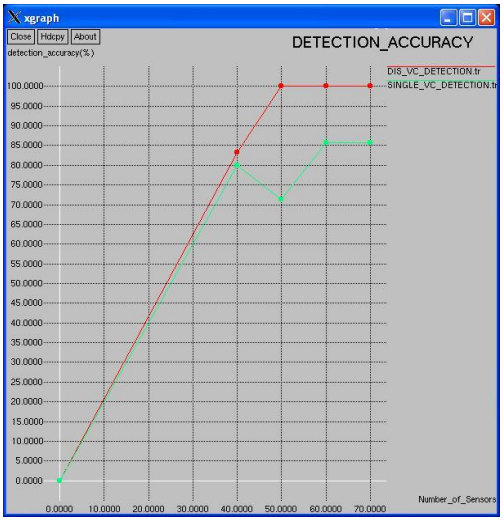


Fig 4b Detection rate of in-region and distributed in-region

The detection accuracy of distributed VC is high. Because each VC only communicate particular region of sensors and detect the sensors are inside the application region or not. Therefore each VC detects the attack only for the particular regions of the sensors.

VII. ANALYSIS ON LOCALIZATION FACTORS

Some factors for localization is important for analysing the performance of localization process [13]. Such parameters are taken into account for analysis.

A. Energy Consumption

Fig 5a shows the energy consumption of distributed verification algorithm. Energy consumption of single VC (verification center) is higher than the Distributed VC. Since each sensor node communicates with the single verification center, so during the data transmission the packet loss will be increased. Therefore energy is highly consumed at the each sensors and VC. And detection accuracy rate for existing algorithm also shows that distributed one is better than in-region algorithm which contains single VC.

B.Communication Overhead

Fig 5b shows that the communication overhead curves for distributed in-region verification algorithm. Communication Overhead of Distributed VC is slower than the single VC. Because Distributed Verification center communicating only for particular regions of the each sensor. So each regions of communication overhead in the network will be reduced. But Single Verification Center communicates all sensor nodes in the network.

C. Collusion Avoidance

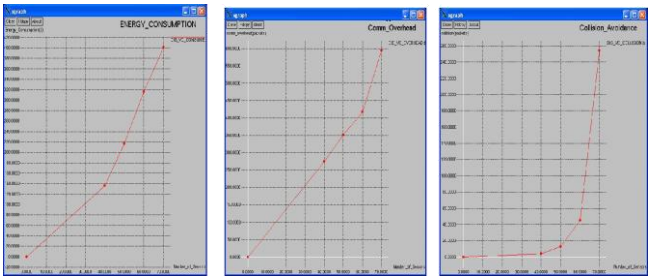


Fig 5c shows that the collision avoidance of single and multiple VC are increased with increase of time. But distributed VC of collision avoidance is slower compare to the single VC of collision avoidance. In Distributed VC sensor nodes only communicate with particular verification center responsible for its region. Since each sensor node communicates with the corresponding verification center, collision is avoided.

VIII. CONCLUSION

In this paper, a distributed location verification system is proposed. The in-region verification verifies whether a sensor is inside an application-specific verification region. Distributed algorithm contains multiple Verification Center which gives better performance than existing. A probabilistic method is designed to provide the confidence that a sensor is inside the verification region. The work takes the first step to integrate the application requirements in determining the trustability of sensors' estimated locations. Moreover, this proposed verification system is more effective and robust compared to existing schemes. It is resilient to malicious attacks and can be used in hostile environments.

REFERENCES

[1] Yanchao Zhang, Wei Liu, Yuguang Fang, and Dapeng Wu, "Secure Localization and Authentication in Ultra-Wideband Sensor Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 4, pp. 829-835, Apr. 2006.

[2] Yanchao Zhang, Wei Liu, Yuguang Fang, and Dapeng Wu, "Secure Localization and Authentication in Ultra-Wideband Sensor Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 4, pp. 829-835, Apr. 2006.

[3] Yanchao Zhang, Wei Liu, Yuguang Fang, and Dapeng Wu, "Secure Localization and Authentication in Ultra-Wideband Sensor Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 4, pp. 829-835, Apr. 2006.

[4] Yanchao Zhang, Wei Liu, Yuguang Fang, and Dapeng Wu, "Secure Localization and Authentication in Ultra-Wideband Sensor Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 4, pp. 829-835, Apr. 2006.

[5] Yanchao Zhang, Wei Liu, Yuguang Fang, and Dapeng Wu, "Secure Localization and Authentication in Ultra-Wideband Sensor Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 4, pp. 829-835, Apr. 2006.

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

[7] 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.

[8] D. Liu, N. Peng, and W.K. Du, "Attack-Resistant Location Estimation in Sensor Networks," Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN '05), 2005.

[9] S. Brands and D. Chaum, "Distance-Bounding Protocols," Proc. Workshop the Theory and Application of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT '93), pp. 344C359, 1994.

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

[11] W. Du, L. Fang, and P. Ning, "LAD: Localization Anomaly Detection for Wireless Sensor Networks," Proc. IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS '05),

[12] S. Capkun, M. Cagalj, and M. Srivastava, "Secure Localization with Hidden and Mobile Base Stations," Proc. IEEE INFOCOM, 2006.

[13] Freddy L_opez Villafuerte, Jochen Schiller, " Evaluating Parameters for Localization in Wireless Sensor Networks: A survey" Freie