International Journal of Computer Network and Security (IJCNS)
Vol 6. No.1 – Jan-March 2014 Pp. 66-68
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0975-8283

SECURE PROBABILISTIC LOCATION VERIFICATION FOR WIRELESS SENSOR NETWORKS

R.Vidhyalakshmi, G.Surya
Mount Zion College of Engineering and Technology
Lena vilakku, Pudukkottai.
vidhyavisudur@gmail.com, surya.ganeshan@gmail.com,

ABSTRACT

Security is one of the important factors for any Wireless Sensor Networks application. Location verification system provides that security for retrieving data from Wireless Sensor Networks application. Previous System requires group deployment knowledge of sensors or depends on highly expensive, dedicated hardware because of these requirement it is very expensive. In this paper location verification system with trusted token analyzer and Attack resistant location estimation scheme in secure manner is proposed. This system provides highly feasible true location estimation of sensor node with low cost and reduces false estimation due to attacks such as malicious attack, wormhole attack, pollution attack etc.

Keywords- wormhole attack, claimed location, true location beacon node.

1. INTRODUCTION

Localization i.e., knowing the location of sensor nodes in wireless sensor networks is important topic in every WSN application.WSN application deployed in hostile environment, location of sensor node information attacks may be highly possible. Existing system's location verification algorithms are categories into two namely on-spot verification and in-region verification [1]. Both verification system requires Expensive hardware i.e., Antenna, etc. On-Spot verifies whether the sensor true and claimed location is same or not. In-Region verification verifies whether sensor is on the application region or not. Verification system uses matrix for estimate inconsistencies between claimed locations. In this paper, secure way location verification system is designed to estimate the true location through monitoring the sensor node within a region. For this token is assigned to each sensor node by token analyzer. With the help of token, sensor's location and speed and packet transfer location are monitored within a region. The Attack resistance location verification is to identify and remove the malicious attack node and action via beacon location references.

2. RELATED WORK

Geographical routing [3], geographic key distribution [4], and location-based authentication [5] require the location of unknown nodes. Basically, there are two categories of sensor nodes: unknown and anchor nodes [2]. SNA and SIV classification discussed in secure localization scheme. A lot of localization scheme are proposed in existing system. Some covert base stations are deployed in application field for estimate the claimed location of sensor. Via covert base station 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 [1]. However, those schemes are cannot work properly whenever the anchor nodes i.e., beacon nodes are compromised.

Because of verification system highly depends on neighbor observation. For example many neighbor nodes are compromised with attackers automatically it provides wrong observation result using those observation the verification system estimate localization wrongly.

3. BACKGROUND

Two approaches trusted token analyzer scheme and Attack Resistant Location Estimation Technique are used to find the location of the Sensor nodes. On-spot Verification is to verify whether a sensor's localization error is less than a certain distance and In-region verification is to verify whether a sensor is inside a physical region or not. By analyzing the

International Journal of Computer Network and Security (IJCNS)
Vol 6. No.1 – Jan-March 2014 Pp. 66-68
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0975-8283

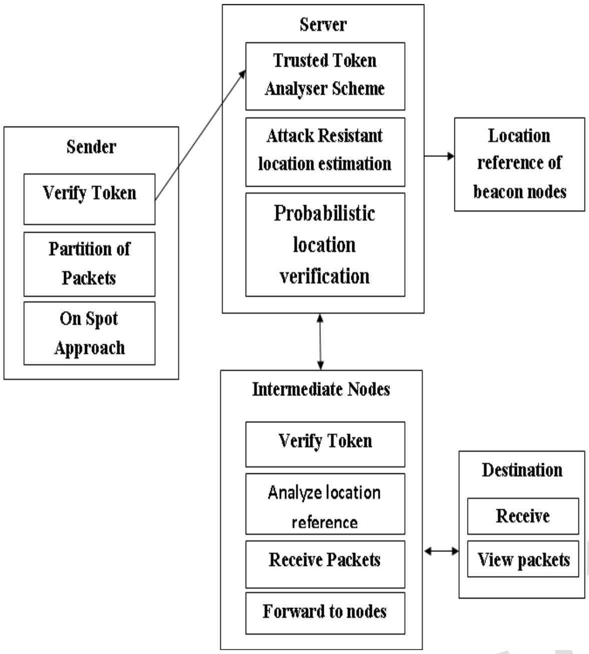

Server
Trusted Token Analyser Scheme
Attack Resistant location estimation
Probabilistic location verification
Location reference of beacon nodes
Sender
Verify Token
Partition of Packets
On Spot Approach
Intermediate Nodes
Verify Token
Analyze location reference
Receive Packets
Forward to nodes
Destination
Receive
View packets

Figure.1 System Architecture

Result of both on spot and in region, the shortest path is generated to provide communication in the wireless sensor network. Token analyzer creates token for each sensor node and monitor the sensor location and speed of packet transfer with the help of token. The Attack Location Estimation Filter the malicious attacks based on location references. Through these schemes we are able to achieve the estimation of true localization by eliminating false detection, reduces computational overhead, secure to communicate, possibilities to identifies the high wormhole attack and revoke it.

Refer Fig.1, server describes verification system actions. Here proposed schemes and techniques are implemented. Trusted token analyzer generate token to Sensor node in deployment fields. Using those token sensor i.e., sensor transmit packets.
Server verifies the sensor as well as packet via token. Token is unique identifier for each sensor node. Location references from beacon node are used to identify malicious attackers in WSN application and filter via Attack Resistant Location Estimation Technique.

4. SCHEME AND TECHNIQUES

In this section describes schemes and techniques for estimating true localization.

Probabilistic Location Verification

The broadcast packets should contain the hop count in addition to the claimed location information. A node receiving a broadcast packet re-broadcasts the packet only if it has the lowest hop count of the same information received. Every packet must contain the hop count as well as the claimed location information. Sensor nodes do not need to be equipped with specialized hardware, only a small number of specialized verifiers are needed.

Trusted Token Analyzer Scheme

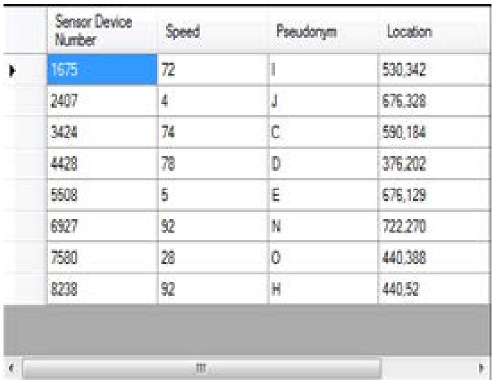
The token analyzer scheme is based on an analogy of a fixed capacity bucket into which tokens, normally representing a unit of bytes or a single packet of predetermined size, are added at a fixed rate. When a packet is to be checked for conformance to the defined limits, the bucket is inspected to see if it contains sufficient tokens at that time.

Attack Resistant Location Estimation Technique

These techniques are purely based on a set of location references. The location references may come from beacon nodes that are either single hop or multiple hops away or from those non-beacon nodes that already estimated their locations .First approach is extended from the minimum mean square estimation (MMSE). It uses the mean square error as an indicator to identify and remove malicious location references. The second one adopts an iteratively refined voting scheme to tolerate malicious location references introduced by attackers.

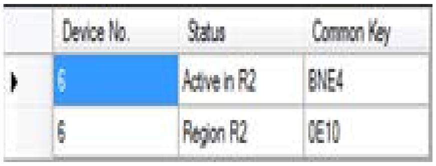
5. EXPERIMENTAL CONSIDERATION

In this section, experimental consideration of our proposing system is going to be discussed. Fig. 2 shows verification center (VC) report of localization information which means sensor device number in column one, speed of packet traverse in column two, Pseudonym otherwise called as sensor id in column three and the location of the sensor node in column four. By using information report easily able to verify the location of sensor node in the field. In our experiment application field is split into four i.e., R1, R2, R3, R4.



Sensor Device Number	Speed	Pseudonym	Location
1675	72	I	530,342
2407	4	J	676,328
3424	74	C	590,184
4428	78	D	376,202
5508	5	E	676,129
6927	92	N	722,270
7580	28	O	440,388
8238	92	H	440,52

Figure. 2 Verification center Report



Device No.	Status	Common Key
6	Active in R2	BNE4
6	Region R2	0E10

Figure. 3 Sensor's activation Region status

Fig. 3 shows the status of sensor's active region. Here the sample activation Region status describes the Sensor which has 6 as a Device No is active in R2.

6. CONCLUSION

Previous verification system require special hardware such as directional antenna or precise time measurement device, which are very expensive and are not reasonably priced for low-cost large-scale wireless sensor systems. Rather depends on hardware to verify the location of a sensor in our verification system uses token and location reference information provide inconsistencies in estimation of claimed location. This paper proposes Location verification system in effective way estimation with probabilistic location verification, Trusted Token Analyzer and Attack Resistant Location Estimation with high performance.

REFERENCES

[1] Yawen Wei, Student Member, IEEE, and Yong Guan, Member, IEEE, "Lightweight Location Verification Algorithms for Wireless Sensor Networks," IEEE Trans.parallel and Distributed systems, vol. 24, no. 5,may 2013

[2] Jinfang Jiang, Guangjie Han1, Chuan Zhu1, Yuhui Dong and Na Zhang , "Secure Localization in Wireless Sensor Networks: A Survey," JOURNAL OF COMMUNICATIONS, VOL. 6, NO. 6, SEPTEMBER 2011

[3] 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.

[4] 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.

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

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

[7] Ting ZHANG, Jingsha HE, Yang ZHANG, Yuqiang ZHANG and Xiaoyu SONG," DV-based Robust Localization against Wormhole Attacks in Wireless Sensor Networks", Journal of Computational Information Systems 7: 13 (2011) 4732-4739

[8] Manoop Talasila, Reza Curtmola, and Cristian Borcea," LINK: Location verification through immediate Neighbors Knowledge," Computer Science Department New Jersey Institute of Technology Newark, NJ, USA

[9] Tingting Sun, Bin Zan, Yanyong Zhang and Marco Gruteser, "The Boomerang Protocol: Tying Data to Geographic Locations in Mobile Disconnected Networks , "IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 11, NO. 7, JULY 2012