A SECRET KEY BASED DETECTION OF CLONE ATTACKS IN MOBILE WSNs

Geetha C[1], Ramakrishnan M[2]

[1]*Research Scholar, Manonmaniam Sundaranar University, Tirunelveli, TN, (India)*

[2]*Director, School of IT, Madurai Kamaraj University, TN, (India)*

ABSTRACT

Clone attack detection is a major issue in mobile sensor network nowadays. In static sensor network by using location information clone nodes are easily identified. If a node ID is present in two different locations then clone is identified. But in mobile sensor network is different, due to the nature of mobility of sensor nodes, the same node can be present in different location after some time. So location information is not sufficient to detect the clone node. This paper proposes a method to detect the clone node in mobile sensor network using cryptographic key information and also node moving speed. The simulation results shows that proposed method is an efficient one which produces very good results in terms of detection rate and throughput.

Keywords: Clone Attack, Cluster Agent, Mobile Sensor Network, Secrete Key, System Speed.

I. INTRODUCTION

Mobile wireless sensor networks (MWSNs) is simply defined as a wireless sensor network (WSN) in which the sensor nodes are mobile. MWSNs are much more versatile than static sensor networks as they can be deployed in any scenario. The applications are environment monitoring such as detecting light, heat, humidity, and temperature. The nodes consist of a radio transceiver and a microcontroller powered by a battery. Sensors can be attached to people for health monitoring, which may include heart rate, blood pressure etc. Animals can have sensors attached to them in order to track their movements for migration patterns, feeding habits etc. Sensors may also be attached to unmanned aerial vehicles (UAVs) for surveillance or environment mapping. Mobile Sensor Networks allows the sensor nodes to move freely and they are able to communicate with each other without the need for a fixed infrastructure [1]. Compared with static network this increases the network lifetime, reduces the power consumption and provide more channel capacity. Nowadays in sensor network the very important issue, the researchers are concentrating much is attacks or intrusion detection. One of the most serious attacks is clone attack in both static wireless sensor network and mobile sensor network. A sensor node captures the credentials of another node which includes ID and cryptographic information and deploys multiple nodes with this information in the network so that the network functionality is disturbed like leaking the data, modifying the data, routing wrong data etc. This attack is called as clone attack or replica node attack. In this paper we propose a method based on secrete key. Several approaches existing are to find the clone attack in static WSNs. All theses use the location information. But those algorithms are not suitable for mobile WSNs. Since location claim cannot be used as major information for detecting the clone attack. The algorithm should be distributed, efficient in terms of

detection rate and throughput. We propose an algorithm which uses node movement speed and the unique secrete key for the detection of clone nodes. The simulation results shows that proposed algorithm works well, efficiently and shows very good results in terms of detection rate and throughput. There is number of false positives and false negatives are zero for the proposed method. The remaining part of this paper is organized as follows: Section II describes the entire existing algorithm for mobile sensor network. Section III deals the proposed method with system architecture. Section IV discusses the simulation results and finally section V gives the conclusion and future enhancements.

II. RELATED WORK

Several algorithms are available to find replica nodes in static wireless sensor network. They are classified into centralized and distributed. Each one is having the advantages and disadvantages. Each one shows its efficiency. All these algorithms mostly use the location information to find the clone node. But these algorithms can't be applied for mobile sensor network because the nodes are mobile nodes. A node present in location (x,y) is moved to a new location (p,q) in short time interval and so above said algorithms are not suitable for mobile sensor network. One of the centralized algorithms for detecting clone node in mobile sensor network is Sequential Probability Ratio Test (SPRT) in which a node moves in a speed exceeding the configured system speed then clone node is found[2][3]. Based on hypothesis testing mobile nodes are identified. A New Protocol for the Detection of Node Replication, the nodes is deployed in the node initialization phase. A key server generates pair-wise symmetric keys and each node reports about the number of keys established with ID. This report is sent to BS and it counts the number of pair-wise keys with the help of Blooming Filter. The node whose key count is above a threshold is considered as clone node.[4] There are two approaches for distributed case. In Xtremely Efficient Detection (XED) [5][6], when two nodes in communication range meet each other for the first time they exchange their assigned random numbers. Again in a short interval if they met, and exchange the random numbers, both received and original are not same then clone node found. In Efficient and Distributed Detection (EDD), when number of times a node A encounters the node B is comparatively high than the threshold value the clone node is identified[7].

III. SECRET KEY ALGORITHM

3.1 Network Model & Assumptions

In the mobile sensor network, sensor nodes are having the characteristic of mobility. A mobile sensor node stays in one location for a certain period of time then selects a random destination [8]. Then it moves towards destination at the selected speed ranges from 0 to Vmax. Vmax is the configured system speed. Upon arrival, mobile node pauses for a specified time period before starting the process again. The communication link between two nodes is bi-directional. Every mobile node is having the capability of obtaining its location without the help of GPS [9].

3.2 System Architecture

In Fig. 1. The system architecture shows how the algorithm works. The network area is clustered with a Cluster Agent elected based on the trust and energy level. Each Agent sends the registration request to all the nodes in the cluster. All these nodes send the registration message with ID, Previous Loc, and Current Loc and secrete key assigned by BS during deployment. After receiving all the messages, CA generates and gives the secret key

for all the registered nodes and records it in the agent table. Find the difference between previous Loc and Current Loc and then the speed. If the speed exceeds the system speed, then clone node found. Now the agent table is exchanged with each other. If a node moves to a new location then CA asks the secrete key. If the given secrete key is same as the one recorded in the table then clone node found.

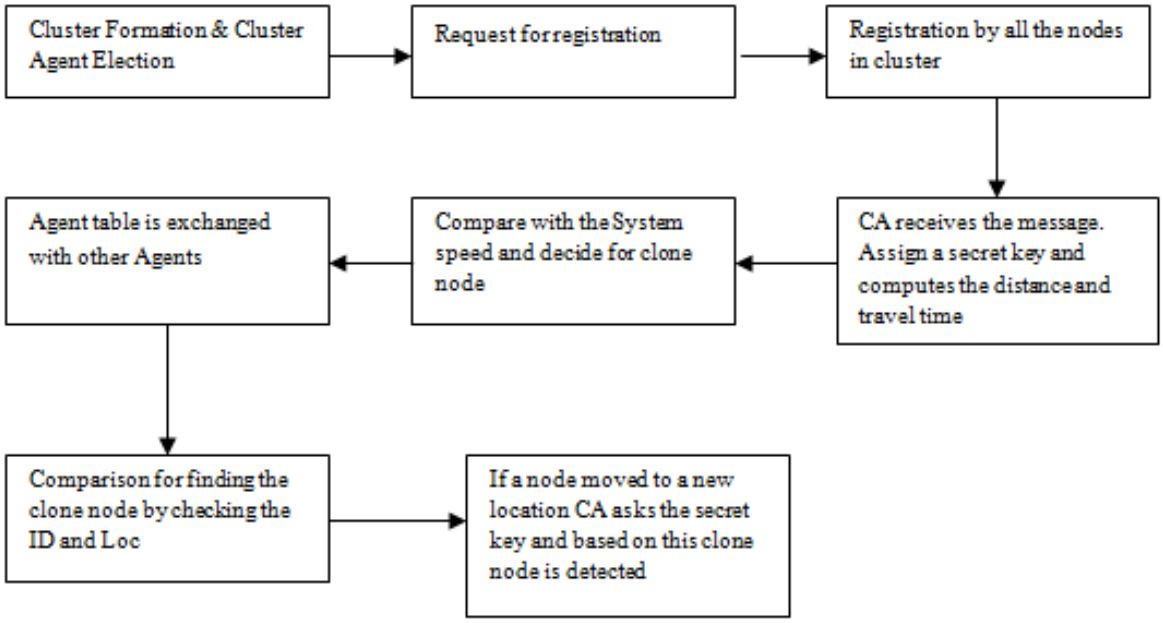

Figure 1. System Architecture

3.3 Proposed Method

1. The network is divided into number of clusters based on coverage area.
2. Each cluster is having a cluster Agent. (CA)
3. When the nodes are deployed in the network initially, a secret key is assigned to it by the Base Station (BS).
4. CA sends a message to all the nodes in the cluster for a registration process.
5. When the nodes received this request message, they send ID, Present Loc, Previous Loc and its secret key to CA.
6. From the received messages CA calculates the distance between previous Loc and Present Loc and if it is 0, stores all the details in a table. A new secret key is generated by CA, and replaces the old one; same is informed to sensor node also.
7. If the distance difference is > 0, find the travel time for the distance and compare this with the system speed. If it exceeds system speed Vmax then clone node found. This is performed for the received messages. If not, secret keys (received and available in the table) are compared. If both are different, clone node is detected.
8. Once table is formed, CAs exchanges the table with one another. In all CAs the comparison is performed and almost the clone node is identified with this.
9. If a node moves from old location to new location then, is asked to register with the new area CA, by giving the secret key. While verifying the keys, we can easily find the clone.

The distance is calculated using Eq.(1)

$$D=\sqrt{(x1-x2)^2+(y1-y2)^2} \quad (1)$$

where (x1,y1) is the previous location and (x2,y2) is the new location.

Speed of the node is calculated using Eq. (2)

$$\frac{D}{System\ Speed\ Vmax} \quad (2)$$

where V_{max} is configured system speed. D is the distance moved by the particular sensor node.

IV. SIMULATION RESULTS

The algorithm is simulated using NS-2 with 50 mobile nodes in the area 500mx500m. The movement speed of the mobile nodes is minimally 0.1ms and the number of iterations performed is 100. The graph is plotted by taking the average of all these iterations. The node to be moved and speed of movement is selected randomly based on Random Waypoint Mobility.

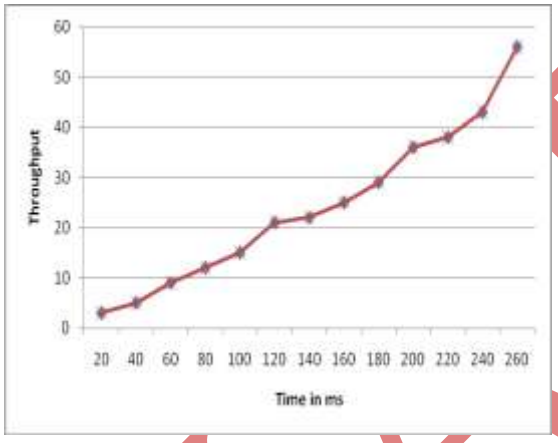

Figure. 2 Time Vs Throughput

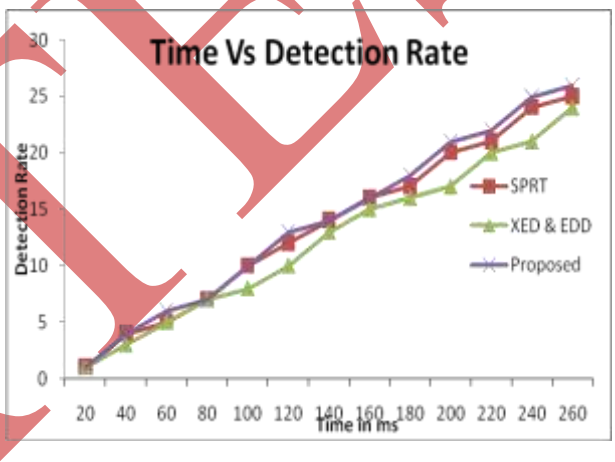

Figure. 3. Time Vs Detection Rate

The graph shows a very good result for the proposed algorithm compared with other existing algorithms. The communication overhead is very less which is O(1) per node. Only secrete key is send to the CA by every node. Every time when the energy level of CA is reduced below a threshold value immediately another high energy node is selected as the CA and the information available with old one is transferred to new CA. So the algorithm is fault tolerant. Comparing the false positives and false negatives of the proposed algorithm it is zero. Very less number of nodes are falsely identified as clone nodes and also falsely identified as non-malicious nodes. With the distance and speed comparison itself most of the clone nodes are identified and the remaining is identified by the secret key comparison. Since two verifications are performed, the algorithm easily detects the replicas.
The Fig. 2 shows the throughput, which is linearly increasing when time goes. The Fig. 3 shows the detection rate compared with other algorithms. Here the computation will be little bit high in the Cluster Agents.

V. CONCLUSION & FUTURE WORK

The proposed algorithm uses a secrete key to find the clone node. In static networks, location is main information to find clone. But in mobile networks, since the nodes are having the mobility nature we can't use

the location alone. In addition to this location and ID, it uses the speed and secrete key. The proposed algorithm detects the clone nodes easily and in a fast manner without any communication overhead. The limitation of the algorithm is the information exchanged between CAs is very lot. And after receiving new registration, CA has to find the distance and speed of the node. In future, this work can be modified so as to satisfy the characteristics of algorithm like less computation time and less storage space than the proposed algorithm.

REFERENCES

[1] Getsy S Sara, D. Sridharan, Routing in Mobile wireless sensor network: A Survey, Springer Science + Business Media NewYork 2013.

[2] Jun-Won Ho, Matthew Wright, Member, IEEE, and Sajal K. Das, Senior Member, IEEE, Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing, IEEE TRANSACTIONS on Mobile Computing, vol. 10,no. 6,June 2011.

[3] Jun-Won Ho, Matthew Wright, Member, IEEE, and Sajal K. Das, Fast Detection of Replica Node Attacks in Mobile Sensor Networks Using Sequential Analysis, INFOCOM 2009, IEEE pg.1773 - 1781

[4] X. M. Deng and Y. Xiong, "A new protocol for the detection of node replication attacks in mobile wireless sensor networks,"*Journal of Computer Science and Technology*, vol. 26, no. 4, pp.732–743, 2011.

[5] B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient Distributed Detection of Node Replication Attacks in Sensor Networks,"*ACSAC*, 2007.

[6] C. M. Yu, C. S. Lu, and S. Y. Kuo, "Mobile sensor network resilient against node replication attacks," in Proceedings of the 5th Annual IEEE Communications Society Conference on Sensor,Mesh and Ad Hoc Communications and Networks (SECON '08),pp. 597–599, June 2008.,

[7] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, "Efficient and Distributed Detection of Node Replication Attacks in Mobile Sensor Networks,"Proc. IEEE Vehicular Technology Conf. Fall (VTC Fall), Sept.2009.

[8] Javad Rezazadeh, Marjan Moradi, Abdul Samad Ismail, Mobile Wireless Sensor Networks Overview, IJCCN International Journal of Computer Communications and Networks, Volume 2, Issue 1, February 2012 pg. 17-22.

[9] D.Vinoth Kannan, S.Bala Murugan, Energy Efficient Detection of Replica Node in Mobile Sensor Networks, *Special Issue of International Journal of Computer Application, on International Conference on Electronics, Communication and Information Systems (ICECI 12) pg. 34-37.*