International Journal of Education and Science Research Review
E-ISSN 2348-6457
Volume-6, Issue-2, April - 2019
P-ISSN 2349-1817
www.ijesrr.org
Email- editor@ijesrr.org

Detection of Clone Node Detection Attacks in Mobile Sensor Networks

Dr. Sunny Arora
Guru Kashi University, Talwandi Sabo

ABSTRACT

Nowadays, detecting clones is a serious problem in mobile sensor networks. Clone nodes may be easily recognised in a static sensor network using position information. A clone is discovered when a node ID appears in two separate places. However, in a mobile sensor network, due to the nature of sensor node mobility, the same node may be present in many locations after a period of time. As a result, location data alone is insufficient to determine the clone node. Using cryptographic key information and node movement speed, this research provides a method for detecting clone nodes in mobile sensor networks. The simulation results demonstrate that the suggested technique is efficient and offers excellent detection rate and throughput outcomes.

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

I. INTRODUCTION

A wireless sensor network (WSN) with mobile sensor nodes is referred to as a mobile wireless sensor network (MWSN). Because they may be implemented in any environment, MWSNs are far more flexible than static sensor networks. Environment monitoring applications include light, heat, humidity, and temperature detection. The nodes are made up of a radio transceiver and a battery-powered microprocessor. People can have sensors connected to them for health monitoring, such as heart rate, blood pressure, and so on. Sensors can be fitted to animals to track their movements for migratory patterns, eating habits, and other purposes. Unmanned aerial vehicles (UAVs) can also be equipped with sensors for observation and mapping of the area. Sensor nodes in Mobile Sensor Networks may roam about freely and interact with one another without the requirement for a permanent infrastructure [1]. This extends the network lifetime, saves power consumption, and provides higher channel capacity when compared to a static network. Currently, the most significant subject on which researchers are focusing is assaults or intrusion detection in sensor networks. Clone attacks are one of the most dangerous threats in both static wireless sensor networks and mobile sensor networks. A sensor node obtains another node's credentials, including ID and cryptographic information, then instals many nodes with this information in the network, disrupting network

functioning such as data leakage, data modification, and data routing errors, among other things. Sensor nodes in Mobile Sensor Networks may roam about freely and interact with one another without the requirement for a permanent infrastructure [1]. This extends the network lifetime, saves power consumption, and provides higher channel capacity when compared to a static network. Currently, the most significant subject on which researchers are focusing is assaults or intrusion detection in sensor networks. Clone attacks are one of the most dangerous threats in both static wireless sensor networks and mobile sensor networks. A sensor node obtains another node's credentials, including ID and cryptographic information, then instals many nodes with this information in the network, disrupting network functioning such as data leakage, data modification, and data routing errors, among other things. For the suggested technique, there are no false positives and no false negatives. The following is how the rest of the paper is organised: The full known algorithm for mobile sensor networks is described in Section II. The suggested technique is discussed in Section III, which also covers system architecture. Section IV describes the simulation findings, and Section V concludes with recommendations for future improvements.

II. RELATED WORK

In a static wireless sensor network, there are several strategies for finding replica nodes. They are divided into two categories: centralised and scattered. Each has its own set of benefits and drawbacks. Each one demonstrates its effectiveness. To discover the clone node, all of these techniques rely on location information. However, because the nodes in a mobile sensor network are mobile, these methods cannot be used. The preceding techniques are not suited for mobile sensor networks since a node existing in location (x,y) is transferred to a new site (p,q) in a short time interval. Sequential Probability Ratio Test (SPRT), in which a node travels faster than the specified system speed, is one of the centralised techniques for identifying clone nodes in mobile sensor networks[2][3]. Mobile nodes are discovered through hypothesis testing. The nodes are deployed in the node initialization phase of A New Protocol for Detecting Node Replication. Each node reports the quantity of keys established with ID, and a key server produces pair-wise symmetric keys. This report is submitted to BS, and it uses Blooming Filter to count the amount of pair-wise keys. A clone node is one whose key count exceeds a certain threshold. [4] For dispersed cases, there are two ways. When two nodes in communication range meet for the first time, they exchange their allocated random numbers in Xtremely Efficient Detection (XED) [5][6]. If they meet again in a short time and exchange random numbers, and the received and original numbers are not the same, then a clone node has been discovered. The clone

node is discovered in Efficient and Distributed Detection (EDD) when the number of times a node A encounters node B is considerably high than the threshold value [7].

III. SECRET KEY ALGORITHM

3.1 Network Model & Assumptions

The sensor nodes in a mobile sensor network have the ability to move around. A movable sensor node stays in one place for a set amount of time before moving to a random site [8]. Then it advances towards its target at the speed set by the user, which can vary from 0 to Vmax. The specified system speed is Vmax. When a mobile node arrives, it stops for a set amount of time before continuing the procedure. A bi-directional communication link exists between two nodes. Every mobile node is capable of determining its location without the assistance of GPS [9].

3.2 System Architecture

Figure 1 illustrates this. The algorithm's workings are depicted in the system architecture. A Cluster Agent is chosen depending on the degree of trust and energy in the network region. The registration request is sent to all nodes in the cluster by each Agent. All of these nodes transmit the registration message, which includes the ID, Previous Loc, Current Loc, and the secrete key that BS assigned during deployment. CA produces and distributes the secret key for all registered nodes after receiving all messages and records it in the agent database. Calculate the speed by subtracting the previous Loc from the current Loc. If the speed is greater than the system speed, a clone node has been discovered. The agent tables have now been swapped out. If a node relocates, CA will inquire about the secret key. If the specified secret key matches the one in the database, a clone node has been discovered.

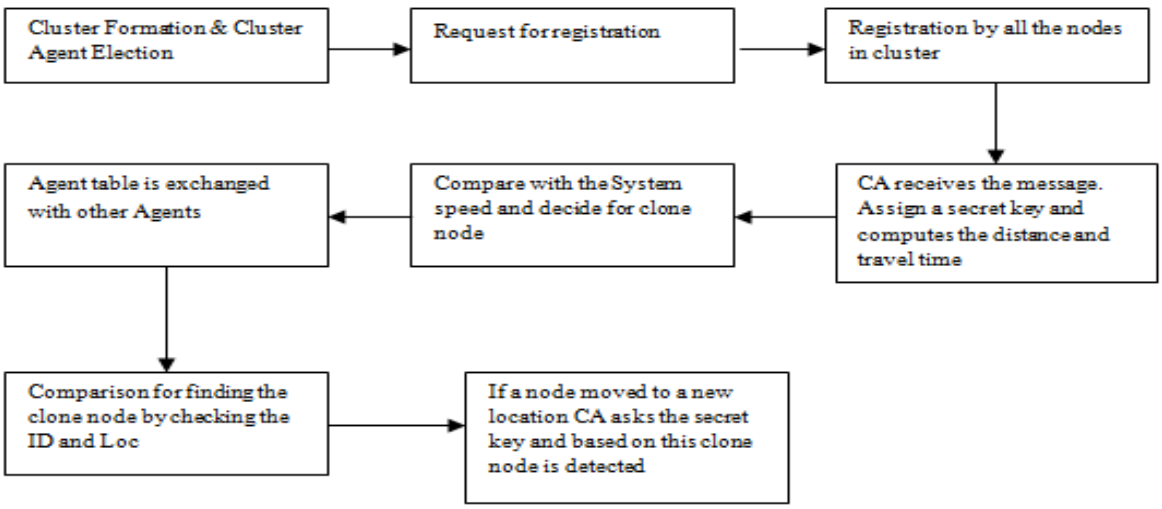


Figure 1. System Architecture

3.3 Proposed Method

1. 1. Based on coverage area, the network is segmented into a number of clusters.
2. 2. A cluster Agent is assigned to each cluster. (CA)
3. 3. When the nodes are first deployed in the network, the Base Station assigns them a secret key (BS).
4. 4. For the registration procedure, CA sends a message to all nodes in the cluster.
5. 5. After receiving the request message, the nodes send ID, Present Loc, Previous Loc, and the secret key to CA.
6. 6. CA evaluates the distance between prior Loc and Present Loc from the received messages and, if it is zero, records all the facts in a table. CA generates a new secret key to replace the old one, which is also communicated to the sensor node.
7. 7. If the distance difference is more than zero, calculate the distance travel time and compare it to the system speed. If the system speed Vmax is exceeded, a clone node is discovered. This is done for the messages that have been received. If this isn't the case, secret keys (which have been received and are listed in the table) are compared. A clone node is discovered if both are distinct.

8. After the table has been created, the CAs exchange the table with one another. The comparison is conducted in all CAs, and practically every clone node is discovered as a result.

9. When a node relocates from one place to another, it is required to register with the new area CA by providing the secret key. We can simply locate the clone while checking the keys.

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)

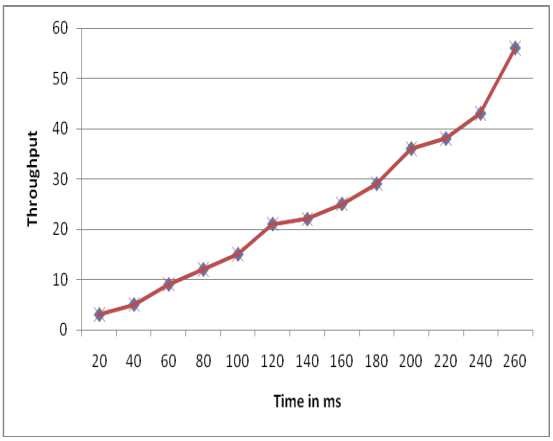
$$\frac{D}{System\ Speed\ Vmax} \quad (2)$$

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

IV. SIMULATION RESULTS

The method is tested with 50 mobile nodes in a 500mx500m region using NS-2. The mobile nodes move at a minimum of 0.1ms every iteration, for a total of 100 iterations. The graph is created by

averaging all of these iterations. Random Waypoint Mobility selects the node to be moved and the pace at which it will move.



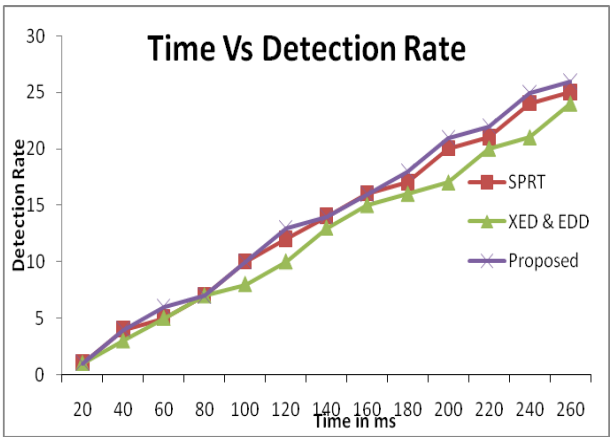


Figure. 2 Time Vs Throughput **Figure. 3. Time Vs Detection Rate**

When compared to other existing algorithms, the suggested technique achieves a very good result. The communication overhead is O(1) per node, which is quite low. Every node sends just the secret key to the CA. When the energy level of CA falls below a certain threshold, a new high-energy node is picked as the CA, and the information from the old one is transferred to the new one. As a result, the algorithm is fault-tolerance. When the suggested algorithm's false positives and false negatives are compared, the result is zero. Only a small percentage of nodes are incorrectly classified as clone nodes or non-malicious nodes. The secret key comparison identifies the remaining clone nodes, whereas the distance and speed comparison identifies the majority of them. The programme quickly discovers the clones since two verifications are conducted.

Figure 2 depicts the throughput, which increases linearly as time passes. The detection rate is shown in Fig. 3 in comparison to other techniques. In the Cluster Agents, the computation will be a little bit higher.

V. CONCLUSION & FUTURE WORK

To locate the clone node, the proposed approach employs a secret key. In static networks, the placement of a clone is crucial. However, because nodes in mobile networks are mobile, we can't rely only on their position. It also makes use of the speed and secretive keys in addition to the location and ID. The proposed approach simply and quickly discovers clone nodes without any communication cost. The algorithm's drawback is the large amount of data transmitted between CAs. After receiving fresh registration, CA must determine the node's distance and speed. This work can be updated in the

future to meet algorithmic features such as faster computing and less storage space than the given approach.

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.*