Identifying Clone Attack In Mobile Sensor Network Using Localized Algorithm

Divya.S
PG Scholar, Dept.of Cse
Sri SaiRam Engineering College
Chennai-44, India

Mrs.V.Kavitha M.E.,
Associate Professor, Dept.of Cse
Sri SaiRam Engineering College
Chennai-44, India

***Abstract*— As detector networks may be deployed during a hostile region to perform important missions. The adversary can launch clone attacks by replicating the compromised node, distributing the clone throughout the network. Since the credentials of replicas square measure all clones of the captured nodes, the replicas will be thought of as legitimate members of the network, creating detection tough. From the security point of view, the node replication attack is extraordinarily harmful to networks as a result of replicas, having keys, will simply launch corporate executive attacks, while not simply being detected. The static networks have faith in the witness-finding strategy that cannot be applied to mobile networks. The location- exceeding strategy used in mobile networks incurs efficiency and security problem. Localized algorithms are proposed to resist node replication attack in mobile sensor networks. The proposed Algorithm XED (Extremely Efficient Detection) and EDD (Efficient and Distributed Detection) come under localized algorithm. The advantages of our proposed algorithms embody 1) localized detection; 2) potency and effectiveness; 3) network-wide synchronization rejection; and 4) network-wide revocation avoidance. Performance comparisons with proverbial strategies are provided to demonstrate the potency of our planned algorithms.**

Keywords- Clone attack detection, wireless sensor network security, EDD and XED algorithm, resilience.

I.INTRODUCTION

A Wireless Sensor Network (WSN) is a collection of sensors with limited resources that collaborate to achieve a common goal. WSNs can be deployed in harsh environments to fulfill both military and civil applications. Due to their operating nature, they are often unattended, hence prone to different kinds of novel attacks. For instance, an adversary could eavesdrop all network communications; further, an adversary could capture nodes acquiring all the information stored therein—sensors are commonly assumed to be not tamper-proof. Therefore, an adversary may replicate captured sensors and deploy them in the network to launch a variety of malicious activities. This attack is referred to as the clone attack. As sensor networks could be deployed in a hostile region to perform critical missions, the sensor networks are unattended and the sensor nodes normally are not equipped with tamper-resistant hardware. This allows a situation since the credentials of replicas are all clones of the captured nodes, the replicas can be considered as legitimate members of the network, making detection difficult. From the security point of view, the node replication attack is extremely harmful to networks because replicas, having keys, can easily launch insider attacks, without easily being detected. Recently, due to advances in robotics, mobile sensor networks have become feasible and applicable. Nevertheless, although the problem of node replication detection in static networks has been extensively studied, only a few schemes have been proposed for mobile sensor networks. Even worse, as indicated in the techniques used in detecting replicas in static environments are not useful in identifying replicas in mobile environments. With the consideration of nodes' mobility and the distributed nature of sensor networks, it is desirable, but very challenging, to have efficient and effective distributed algorithms for detecting replicas in mobile sensor networks.

II.RELATED WORK

The general procedure of applying witness-finding to detect the replicas can be stated as follows. After collecting the signed location claims for each neighbor of the node and sends the collected signed location claims to a properly selected subset of nodes, which are witnesses. When there are replicas in the network, the witnesses, according to the received location claims, have possibility to find a node ID with two distant locations, which implies that the node ID is being used by replicas. RM and LSM were proposed to determine the witnesses randomly.

The difference between RM and LSM is that the witness nodes that find the conflicting location in the former are primarily affected by the number of witness nodes and the ones in the latter are primarily affected by the forwarding traces of location claims. SDC and P-MPC can be thought of as the cell versions of RM and LSM. In particular, before sensor deployment, the sensing region is divided into cells. Compared to RM and LSM which forward location claims node by SDC and P-MPC forward location claims cell by cell. Based on the double ruling, a suite of memory-efficient detection algorithms is introduced. The idea is to guarantee the intersection of traces in LSM via double ruling and to reduce the memory usage of intermediate nodes in LSM via the Bloom filter. In addition, to better distribute the responsibility of witness node selection, the random walk technique is utilized in LSM. Some algorithms exploit other characteristics like social fingerprint, redistributed keys, and random clustering to detection the replica. Unfortunately, all

of the above methods are only for static sensor network, and are not useful if nodes have mobility.

III.PROPOSED WORK

In this section, our proposed algorithm, extremely efficient detection (XED) and Efficient Distributed Detection (EDD), for clone detection in mobile networks is as follows.

Extremely Efficient Detection (XED):

A sensor node 'B' meets another sensor node 'A' at earlier time and 'B' sends a random number to A at that time. When 'B' and 'A' meet again, 'B' can ascertain whether this is the node 'A' met before by requesting the random number. It has capability to detect replicas based on the response of random key. In XED, we assume that the replicas cannot collude with each other but this assumption will be removed in EDD algorithm.

Efficient and Distribution Detection (EDD):

The maximum number of times, Y1, that node 'B' encounters a specific node 'A' during fixed time. In the minimum number of times, Y2, that node 'B' encounters the replica with the same id A. It has capacity to identify replicas by discriminate between these above two cases. Different from XED, EDD assumes that the replicas can collude with each other.

We combine both proposed algorithm (XED and EDD) together ill increases security level and decreases time complexity. The main Advantages of our proposed localized Algorithm are, it not only detects the replicas but also can revoke the replicas within short time period. It has high detection accuracy. Time Synchronization is not essential. The architecture of identifying clone attack is shown in figure 1.

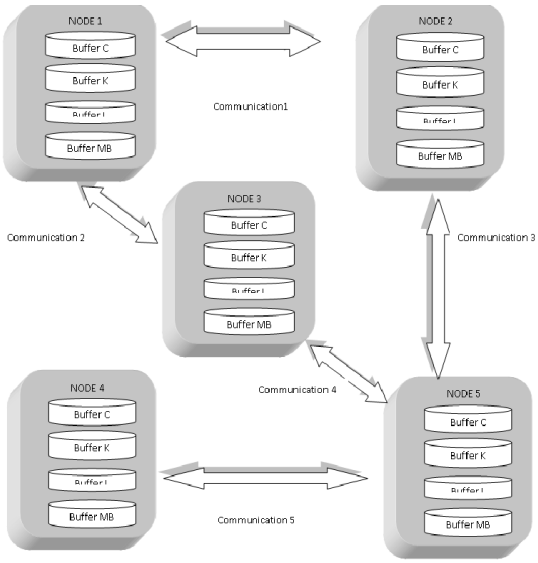

Fig 1 Architecture

IV.IMPLEMENTATION

Each node created by assigning some name and range. Once you moving your node automatically that particular nodes x-axis and y-axis changes accordingly and a random port number is assigned to each node. After establishing the Network with N nodes. These nodes are used to communicating each other with their neighbor nodes. Any node which is going to move from its current region, it must forward to neighbor where it going to move in next 'n' seconds. Then, the node check whether the neighbor node will come under their communication range or not. If it lies in communication range means the sender node will be neighbor, else it will be removed from the neighbor list. During the detection phase, if any node receives a data, first it checks the clone buffer. It checks the communication buffer, if it is already communicated means, first it asks for last location details of both the node and its random number.Then, it check key buffer whether the sender keys matches or not.Then, the malicious behavior of the each and every nodes are added to the malicious buffer. In addition to all the features of previous detection algorithm, detecting clone nodes by means of location is more efficient. Firstly, the node is act as malicious by insisting that it going to change the location but actually it doesn't move, so it acts as clone node. Each and every node is in different location, all nodes have the location details of each and every nodes, so clone nodes are easily detected.

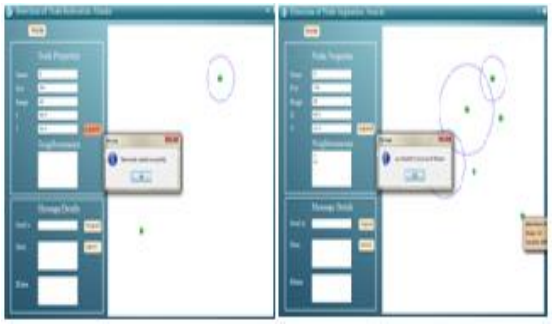

Fig 2 Implementation

V.CONCLUSION

In this paper, two replica detection algorithms for mobile sensor networks, XED and EDD, are proposed. Although XED is not resilient against collusive replicas, its detection framework, *challenge-and-response*, is considered novel as compared with the existing algorithms. Notably, with the novel *encounter-number* detection approach, which is fundamentally different from those used in the existing algorithms, EDD not only achieves balance among storage, computation, and communication overheads, which are all , but also possesses unique characteristics, including network-wide time synchronization avoidance and network-wide revocation avoidance, in the detection of node replication attacks.

VI.REFERENCES

[1] C.-M. Yu, Yao-Tung Tsou and Chun-Schien Lu, "Localized Algorithm for detection of Node Replication Attacks in Mobile Sensor Networks" in IEEE Transaction On Information Forensics And Security" May 2013 pp. 754-766.

[2] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor

networks," IEEE Trans. Depend. Secure Computation, vol. 8, no. 5, pp. 685–698, Sep. /Oct. 2012.
[3] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "Localized multicast: Efficient and distributed replica detection in large-scale sensor networks," IEEE Trans. Mobile Computation., vol. 9, no. 7, pp. 913–926, Jul. 2010.
[4] C.-M. Yu, C.-S. Lu and S.-Y. Kuo, "Efficient and distributed detection of node replication attacks in mobile sensor networks," in Proc. IEEE Vehicular Technology Conf. Fall (VTC-Fall), Anchorage, AK, USA, 2009, pp. 1–5.
[5] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M.T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," IEEE Trans. Syst., Man, Cybern. C, Applicat.Rev, vol. 37, no. 6, pp. 1246–1258, Nov. 2007.

.

