Detection of Replication Attacks Using Randomized Unique Identifier

R.Anand[1], C.Bharanivasan[2], M.L.AlphinEzhil Manuel[3], S.Arunmozhivarman[4]

U.G Scholar[12], Assistant Professor[34],
Department of Computer Science and Engineering,
Alpha College of Engineering, Chennai, India.
anand11.rocky@gmail.com[1]

ABSTRACT

In this the problem is node replication detection. Although defending against node replication attacks demands immediate attention, compared to the extensive exploration on the defense against node replication attacks in static networks, only a few solutions in mobile networks have been presented Defending against Node Replication is not achieved in the Present System. Localization Algorithm is used to identify the exact place of the original node. This is verified and compared with the requested node to detect whether it is Replica or original node. This Randomized unique identifier will be generated and will be changed on Random basis with Time Stamp &as attack occurs. Source node will specify Time to live for every data Transmission. Based on the TTL value Priority of the Packet is identified and transmitted accordingly...The advantages of our proposed algorithms include localized detection; efficiency and effectiveness.

Index Terms: Attack, security, wireless sensor networks.

1. INTRODUCTION

Sensor networks, which are composed of a number of sensor nodes with limited resources, been demonstrated to be useful in applications, such as environment monitoring and object tracking. 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 where the adversary can compromise one sensor node, fabricate many replicas having the same identity (ID) from the captured node, and place these replicas back into strategic positions in the network for further malicious activities. This is a so-called node replication attack. 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.

2. PROBLEM STATEMENT

Most of the existing distributed detection protocols adopt the witness-finding strategy to detect the replicas. In particular, the general procedure of applying witness- finding to detect the replicas. There is no Distributed Replica Detection is achieved. LSM, RED Protocols are used to identify the Replica Nodes in one single Network only. All the Methods are Witness based Verification, Highly Complex, Very difficult to identify, Costlier. The witness-finding strategy exploits the fact that one sensor node cannot appear at different locations, but, unfortunately, the sensor nodes in mobile sensor networks have the possibility of appearing at different locations at different times, so the above schemes cannot be directly applied to mobile sensor networks.

Slight modification of these schemes can be helpful for applicability to mobile sensor networks. For instance, the witness-finding strategy can adapt to mobile environments if a timestamp is associated with each location claim. In addition, setting a fixed time window in advance and performing the witness- finding strategy for every units of time can also keep witness- finding feasible in mobile sensor networks. Nevertheless, accurate time synchronization among all the nodes in the network is necessary. Moreover, when witness-finding is applied to mobile sensor networks, routing the message to the witnesses incurs even higher communication cost.

3. RELATED WORK

3.1Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing

An adversary can capture and compromise sensor nodes, make replicas of them and then mount a variety of attacks with these replicas. These replica-node attacks are dangerous because they allow the attacker to leverage the compromise of a few nodes to exert control over much of the network. Several replica node detection schemes have been proposed to defend against such attacks and these schemes does not work on mobile sensor network. Sequential probability ratio test. Performing (sprt) on every mobile node the occurrence of speed is less or more than systems maximum speed leads to alternate hypothesis

3.2 From Time Domain to Space Domain: Detecting Replica Attacks in Mobile Ad Hoc Networks

Detecting replication attacks is a nontrivial problem in MANETs due to the challenges resulted from node mobility. Existing approaches either fail in mobile environments due to the limitations caused by local views. Their dependence on invariant claims such as location and neighbor list are constrained by the number, distribution, and colluding activities of the replicas. Replication detection schemes (TDD and SDD) to tackle all the challenges from both the time domain and the space domain. Providing high detection accuracy and excellent resilience against smart and colluding replicas. Have no restriction on the number and distribution of replicas.

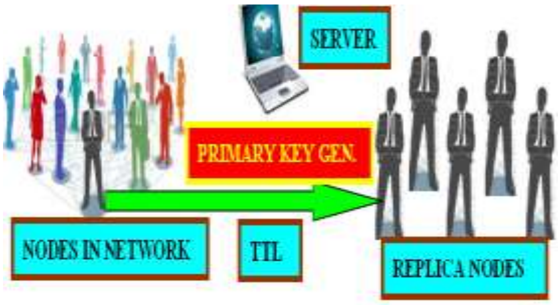
3.3 Supporting Secure Communication and Data Collection in Mobile Sensor Networks

Mobile nodes are often more privileged, their compromise can give the adversary a significant advantage, Security mechanisms for such networks must tolerate mobile node compromises Static sensors, which communicate mostly with their neighbors, mobile nodes may communicate with nodes all over the network. Hence, key establishment is a much harder challenge with mobile nodes. Make, a key redistribution scheme for very general group-based sensor deployments. mGKE allows any pair of neighboring sensors to establish a unique pair wise key, regardless of sensor density or distribution.

4. PROJECT DESCRIPTION

4.1 Network Construction

We have to construct a network which consists of ‘n’ number of Nodes. So that nodes can request data from other nodes in the network. All nodes share their information with each other. The communication is assumed to be symmetric. The Server is used to communicate with other mobile nodes. The server application monitors the mobile’s client accessing information and respond to the client’s requested information. Server will communicate the routes of the places of the client node in graph format. Assigning Time to live to each query.



4.2 Randomized Unique Identifier

To avoid cloning verify the Randomized unique identifier for each node. This Randomized Unique key can be generated using Secure Random Number Generation Algorithm. If it matches then it is considered as genuine. Changing the Randomized unique identifier every time in order to increase the security and to escape from intelligent hackers. After that mailing that key to the user. Only if that user gives the primary key, he can see that value. So, he cannot use the old primary key to see the value.

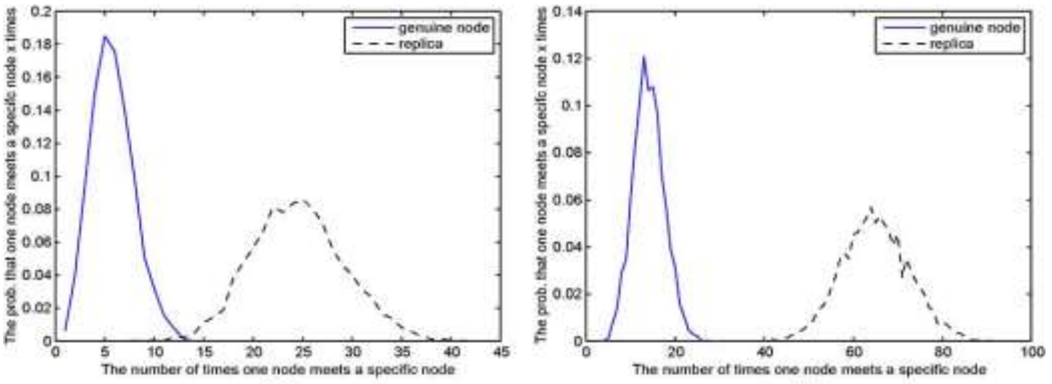
```
importjava.util.Random
Public final class RandonInteger
{
Public static final void main(string aArgs)
{
log('generating 10 random integers in range 0.99');
Randomrandomgenerator=new Random();
for(intidx=1;idx<=10;++idx)
{
intrandomInt=randomgenerator.nextInt(100);
log('Generated:'+randomInt);
}
log('Done.')'
}
Private static void log(String aMessage)
{
System.out.println(aMessage);
}
}
```

4.3. TTL Based Priority Assignment

Assign Time To Live (lifetime of particular query) to each query. Based on that TTL value assign priorities to each query. If it is minimum TTL, it is given low priority. If it is high TTL, it is given high priority. If the lifetime expires, that query is removed from the network.

4.4Detection Time and Detection Accuracy

It can be easily observed that when the number of movements in an interval grows larger, it becomes easier to distinguish between the genuine node and replicas. Here, the term “easier” means higher detection accuracy. This phenomenon can be explained because, from the law of large numbers point of view, the number of encounters with the replicas will get closer to its expected value, which is actually twice as many as the number of encounters with the genuine node. This also means that, although increasing the time interval size can be useful in enhancing the detection accuracy, however, the improvement of detection accuracy cannot be unlimited. As the foundational truth is that there are two replicas in the simulation , the mean value of the distribution of the number of encounters with the replicas must concentrate on the value double that of the number of encounters with the genuine node even if is set to be quite large. Our experience shows at least the detection accuracy of both false positive and false negative ratios lower than 3% is achievable if there are only two replicas in the network.



(a) (b)

5. FUTURE WORK

The future plans are we are using Localization Algorithm to identify the exact place of the original node which is verified and compared with the requested node to detect whether it is Replica or original node. This Process is achieved using two Algorithms. Extremely Efficient Detection (XED) The idea behind XED is motivated by the observation that, if a sensor node meets another sensor node at an earlier time and sends a random number to at that time, then, when and meet again, can ascertain whether this is the node met before by requesting the random number. Algorithmic Description of EDD: The idea behind EDD is motivated by the following observations. The maximum number of times, that node encounters a specific node, should be limited with high probability during a fixed period of time, and while the minimum number of times, Primary Key based Verification is also achieved in this System in order to identify the Replica Nodes.

6. CONCLUSION

In this paper, Localization Algorithm is introduced to identify the exact place of the original node. It is Verified and compared with the requested node to detect whether it is Replica or original node. We introduced a key called Randomized unique identifier to avoid cloning and we are Assigning Time To Live (lifetime of particular query) to each query. Based on that TTL value assign priorities to each query. If it is minimum TTL, it is given low priority. If it is high TTL, it is given high priority. If the lifetime expires, that query is removed from the network.

7. REFERENCES

[1] 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.
[2] C. Bettstetter, H. Hartenstein, and X. P. Costa, “Stochastic properties of the random waypoint mobility model,” *Wireless Netw.*, vol. 10, no. 5, pp. 555–567, 2004.
[3] G. Cormode and S. Muthukrishnan, “An improved data stream summary the count-min sketch and its applications,” *J. Algorithms*, vol. 55, no. 1, pp. 56–75, 2005.
[4] M. Conti, R.Di Pietro, L. V. Mancini, andA.Mei, “Arandomized, efficient, and distributed protocol for the detection of node replication attacksin wireless sensor networks,” in *Proc. ACMInt.Symp. Mobile AdHoc Networking and Computing (MobiHoc)*, Montreal, Canada, 2007, pp. 80–89.
[5] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, “Distributed detection of clone attacks in wireless sensor networks,” *IEEE Trans. Depend. Secure Computing.*, vol. 8, no. 5, pp. 685–698, Sep./Oct. 2012.
[6] M. Conti, R. D. Pietro, and A. Spognardi, “Wireless sensor replica detection in mobile environment,” in *Proc. Int. Conf. Distributed Computing and Networking (ICDCN)*, Hong Kong, China, 2012, pp.249–264.
[7] H. Choi, S. Zhu, and T. F. La Porta, “SET: Detecting node clones in sensor networks,” in *Proc. Int. ICST Conf. Security and Privacy In Communication Networks (Securecomm)*, Nice, France, 2007, pp. 341–350.