LOCATION BASED DETECTION OF REPLICATION ATTACKS AND COLLUDING ATTACKS

P.S.Nivedita Sai
Sri Sairam Engineering College
Chennai-44, India

T.P.Rani
Sri Sairam Engineering College
Chennai-44, India

Abstract -Wireless sensor networks gains its importance because of the critical applications in which it is involved like industrial automation, healthcare applications, military and surveillance. Among security attacks in wireless sensor networks we consider an active attack, NODE REPLICATION attack and COLLUDING attack. We use localized algorithms, ((ie) replication detection is done at the node level and eliminated without the intervention of the base station) to solve replication attacks and colluding attacks. Replication attacks are detected to using a unique key pair and cryptographic hash function. We propose to use XED and EED algorithm[1] (authenticates the node and tries to reduce the replication) , with this using the Event detected location , non-beacon node is used to find the location of a malicious node and by a simple threshold verification we identify malicious clusters.

Keywords: replication attacks ,collusion attacks, localized detection XED, EED

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are used in various applications. They consist of many autonomous sensor nodes deployed in spatially distributed manner. They are used to sense various parameters like temperature, pressure etc. The network consists of small sensors and a unit which is used to store information also called data center. It consists of an antenna for transmission and a power source. Some typical examples are Industrial monitoring, Environment monitoring, Healthcare monitoring, Area monitoring, Passive Area location detection. These WSN's are more prone to attacks of different types as they are deployed under various conditions. This is because the attackers may intend to learn information from the WSNs or disable the functions of the WSNs. For example, on the battlefield, the enemies would hope to learn the private locations of soldiers by injecting wrong commands into the sensor network. It becomes important to ensure security of data transmitted , this security also will save considerate amount of battery power which will in increase the efficiency of the network. In this paper we have considered replication attack which is considered as a major compromise on the security. When a genuine node is compromised either by brutal force or by software attacks. This compromised node's id and key are copied into another node and randomly deployed in wireless scenario. This is replication attack , when this replicated nodes form a group and launch attacks against the benign nodes , this is collusion attacks. Collusion attacks results in attacks like selective forwarding , selective drop of packets, looping of data. There are many techniques which have been proposed for reducing this collusion attacks, some are deterministic (they use some abnormal pattern for detection) some are non deterministic . Centralized detection results in whole network synchronization and wastage of bandwidth hence here we make use of a localized detection algorthim.

2 .LITERATURE REVIEW

Many mechanisms have been proposed to overcome this replication and collusion attacks. The algorithms proposed in [1] it makes efficient usage of key and hash pairs to authenticate users to detect replica but it doesn’t consider the possibilities of collusion . A random walk model is used in [2], as nodes in a sensor network environment are randomly only deployed. Whereas in Witness collusion technique[3] uses three techniques , DIP,QP, WIP , the major shortcoming of these policies are they cannot detect collusion beforehand. Localized detection [4] uses omni-directional antennas which again emphasizes on the necessity of three beacons minimum .In RED model [5] the mechanism involved uses the mechanism of id obviousness and area obviousness but the major disadvantage is network wide synchronization required. Whereas in distributed detection [6] the topology information about the nodes is used but , all nodes stop working as soon as a replica is detected The detection protocols involving a central control have inherent limits such as a single point of failure.

To detect the node replicas in mobile sensor networks, two localized algorithms, XED and EDD, are proposed. The techniques developed in our solutions, challenge-and-response and with new counter-number with location based information, which are fundamentally different from the others.

3. PROPOSED SYSTEM

The idea behind XED is the basic key exchange mechanism where both the nodes initially during the setup phase will exchange a key , id pair and also a hash function value. These values are stored in a list or a hash table, every time they both encounter each other they will exchange these values and cross verify their authenticity.

For the generation of random numbers we use **[x^2 mod N]** [7] where

Let N {integers N|N } such that P, Q are equal length (|P| |Q|) are distinct primes =3 mod 4} be the set of parameter values.

For N € N, let Xn={x^2 mod N |x€ Zn*}

X=disjoint U_{NEN} Xn be the seed domain.

These random numbers are used in hash function which is generated using anyone of the cryptographic hash function family. These universal hash functions form a group and are stored together.

When a user needs to be authenticated anyone of the hash functions from the family of hash functions (n^2) is chosen and cuckoo hashing [8][9] procedure is used and the hashed values are stored in two tables following the code defined below.

```
procedure insert(x)
if lookup(x) then return
loop MaxLoop times
if T1[h1(x)] = ? then f T1[h1(x)]   x; return g
x $ T1[h1(x)]
if T2[h2(x)] = ? then f T2[h2(x)]   x; return g
x $ T2[h2(x)]
end loop
rehash(); insert(x)
end.
```

During the insertion process if all the positions in tables are filled then rehashing is done.

Time taken for both lookup and delete is O(n).

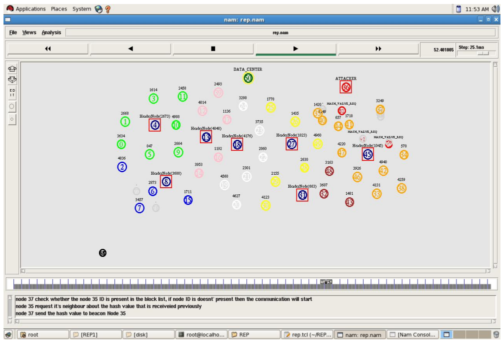
Advantages

Our algorithms possess the following advantages.

- Efficiency and Effectiveness: These algorithms are found to be more efficient then the other localized algorithms
- Network-Wide Revocation Avoidance: Since this is localized detect there is no need for all nodes to stop working as soon as a replica is found
- Time Synchronization Avoidance: There is no need for all nodes to operate in the same time slot for exchange of id’s etc
- Security: Security level increased by a good amount
- Computational time: since we don’t need to go through all the list the computational efficiency becomes O(n)

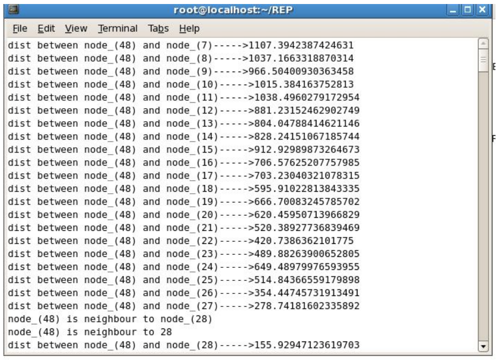
4. SIMULATION RESULTS

The preliminary stages of this work is network configuration and the Hash value is verified. We use random number generation and the cuckoo hashing technique. The network is deployed by using NS 2.34 and cygwin as an interface on Windows system. This process implementation is shown below.



node 37 check whether the node 35 ID is present in the block list, if node ID is doesnt' present then the communication will start
node 35 request it's neighbour about the hash value that is receiveied previously
node 37 send the hash value to beacon Node 35

Figure 1: Node distribution



```
dist between node_(48) and node_(7)----->1107.3942387424631
dist between node_(48) and node_(8)----->1037.1663318870314
dist between node_(48) and node_(9)----->966.50400930363458
dist between node_(48) and node_(10)----->1015.384163752813
dist between node_(48) and node_(11)----->1038.4960279172954
dist between node_(48) and node_(12)----->881.23152462902749
dist between node_(48) and node_(13)----->804.04788414621146
dist between node_(48) and node_(14)----->828.24151067185744
dist between node_(48) and node_(15)----->912.92989873264673
dist between node_(48) and node_(16)----->706.57625207757985
dist between node_(48) and node_(17)----->703.23040321078315
dist between node_(48) and node_(18)----->595.91022813843335
dist between node_(48) and node_(19)----->666.70083245785702
dist between node_(48) and node_(20)----->620.45950713966829
dist between node_(48) and node_(21)----->520.38927736839469
dist between node_(48) and node_(22)----->420.7386362101775
dist between node_(48) and node_(23)----->489.88263900652805
dist between node_(48) and node_(24)----->649.48979976593955
dist between node_(48) and node_(25)----->514.84366559179898
dist between node_(48) and node_(26)----->354.44745731913491
dist between node_(48) and node_(27)----->278.74181602335892
node_(48) is neighbour to node_(28)
node_(48) is neighbour to 28
dist between node_(48) and node_(28)----->155.92947123619703
```

Figure 2: Trace file format

5. CONCLUSION

The first module of proposed system examined the WSNs configurations and clustering the WSN nodes. The sensor nodes clustering is done based their energy level because of entire WSNs mostly depend on power capacity so they can be communicated without communication break. A LEACH routing protocol is used to communicate with corresponding sensor nodes and routes to destination nodes are established. In addition the authenticity of the nodes are verified using XED algorithm

6. REFERENCES

[1] Chia-Mu Yu, Yao-Tung Tsou and Chun-Shien Lu,” Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks ,“IEEE transactions on information forensics and security, vol. 8, NO. 5, MAY 2013.

[2] Yingpei Zeng, Jiannong Cao, Senior Member, IEEE, Shigeng Zhang, Shanqing Guo and Li Xie ,“Random-Walk Based Approach to Detect CloneAttacks in Wireless Sensor Networks”In Proc.IEEE journal on selected areas in communications, vol. 28, NO. 5, JUNE 2010 677

[3] Amirali Salehi-Abari and Tony White ,” On the Impact of Witness-Based Collusion in Agent Societies “,in Proc. Of the International Conference on Principles of Practice in Multi-Agent Systems Pages 80-96.

[4] Zhuhong yOU, Max Q.-H. Meng, Huawei Liang, Shuai Li, Yangming Li, Wanming Chen ,Yajin Zhou, Shifu Miao, Kai Jiang and Qinglei Guo ,” An ocalization Algorithm in Wireless Sensor Network Using a Mobile Beacon Node ,” in Proc. of the 2007 International Conference on Information Acquisition July 9-11, 2007, Jeju City, Korea.

[5] Mauro Conti Di,Roberto Di Pietro,Luigi V. Mancini and Alessandro Mei, ‘’ A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks,’’ in Proc. Of MobiHoc’07, September 9-14, 2007, Montréal, Québec, Canada.

[6] Parno,A.Perrig,andV.Gligor,“Distributed detection of node replication attacks in sensor networks,” in Proc. IEEE Symp. Security and Privacy (S&P), Oakland, CA, USA, 2005, pp. 49–63.

[7] L. Blum, M. Blum AND M. Shub” A simple unpredictable pseudo-random number generator” , in SIAM Journal on Computing ,Vol 15, issue 2, May 1986, page no-364-383.

[8] Rasmus Pagh and Flemming Friche Rodler,“Cuckoo hashing”, Journal of Algorithms 51 (2004) 122–144