Detecting Node Replica Attack Mitigation for Static Sensor Network

Vikram.A, Latha.A

***Abstract*—Wireless Sensor Networks (WSN) is tiny independent devices enclosed firmly in surrounding nodes, able to communicate using wireless links. A wireless sensor network holds huge number of nodes they are spread in antagonistic and nodes are unattended. So, they are easily tracked by the adversary with no protection. An opponent can hold and compromise some node to initiate to make duplicate of them. Once a node is capture, adversary can easily insert replica nodes at any location in the wireless sensor network. An adversary can holds a node, replicate it indefinitely and insert duplicated nodes at any location in the network. If no detection mechanism is done, can reprogram it by injecting false data revoke them into legitimate nodes. To defeat this problem in this paper presented a algorithm for fight against node replication attacks in mobile sensor networks and various detection methods used in mobile sensor network for detecting node duplication attack in the distributed approach.In this paper we conclude with future research and challenges.**

***Index Terms*— Distributed, Security, Replication Attacks, Witness Node, Mobile Sensor Networks.**

I. INTRODUCTION

Sensor networks, which are poised of a huge collection of nodes with resources are restricted that collaborate in order to achieving a common goal such as climate sensing and Health care monitoring. To put forward, robotics have made it possible to develop a different of new architectures for independent wireless networks of sensors. Sensor nodes are interconnected to form the sensor network and are deployed in antagonistic environment where they are concern to different attacks are Sybil attack Sinkhole Attack, information attack and False routing, Selective forwarding attack, Wormholes and eaves dropping, [8]. One can also thrust with a node and alter its behavior and counter measures can be identified by different types of attacks. A serious outcome of node compromise is that once an opponent has obtained the secrets of a sensor node, it can insert Duplicated node at pertaining locations within the network or more witness nodes in the wireless sensor network as shown in (Fig. 1) Replicas having the same identity ID from the captured node, and put these replicas back into original positions in the network for extend malicious activities. This is called node replication attack.

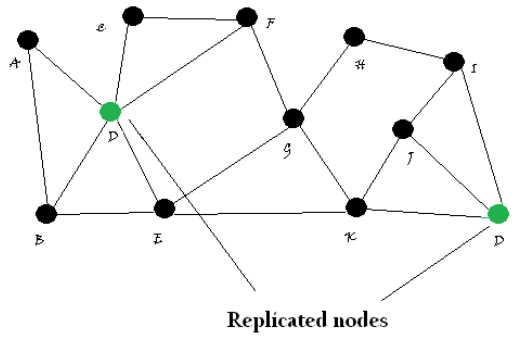

Fig. 1: Node Replication Attack

An adversary can easily holds a single node, replicate it uncertainly, and insert duplicated nodes at any location in the network. If no detection, the hacker could lead many attacks such as corrupt data aggregation protocols by interject false data, and break the connection [4]. In Distributed approaches for detecting node replications is to reduce communication based on location information for a node being collect at one if the replicated nodes are prudent placed at selected locations.

II. LITERATURE SURVEY

The algorithms proposed in [7] it makes effective usage of random numbers and hashing pairs to authenticate users to detect replicated node. But it does not consider the possibilities of Collusion. When attempting to engage the network, must broadcast a quality location claim to its neighbors, most of the existing distributed detection methods [5], vote the witness-finding strategy to detect the replicated node. In Attentive, the general procedure of applying witness-finding to detect the replicated node can be stated as follows. After chosen the signed location Synonyms for each neighbor of the node, denominate the location and the hashing function [2] respectively, sends the collected signed location synonyms to proper subset of nodes which

***Vikram.A**, Department of Computer Science and Engineering, Sapthagiri College of Engineering, Karnataka, India*

***Latha.A**, Department of Computer Science and Engineering, Sapthagiri College of Engineering, Karnataka, India*

is witness node. When replicated nodes in the network, witnesses, according to the received location synonyms, have possibility to search a node ID with two different locations, which indicate that the node ID is being used by replicas. Afterward, the detected replicated node can be eliminated, for example, network-wide revocation. In distributed detection [6] method, information about the every node is used but, all nodes stop working as soon replica node is detected.

III. Detection Of Replicated Node

Protections of sensor networks can be done in distributed approaches are needed for mobile sensor networks by cryptography hashing function.

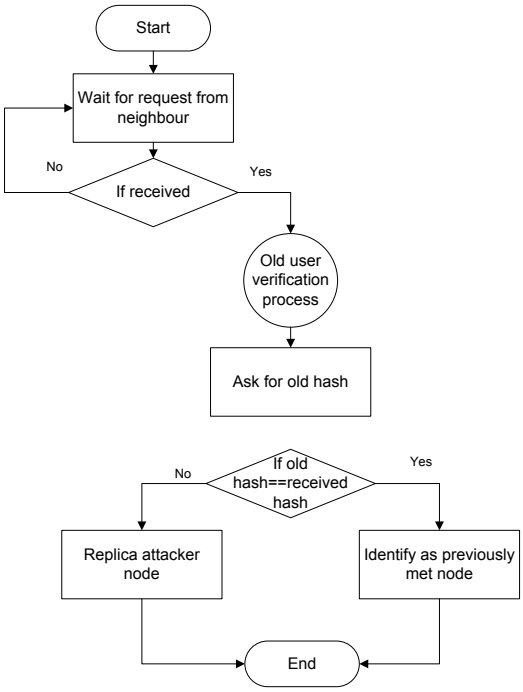

Fig. 2: Detection of replicated node

Newly deployed nodes are able to set up, pair-wise keys with their neighbors, and all sensor nodes in the network know the number of highest deployed generation. Therefore, the nodes will establish pair-wise keys with their neighbors since the nodes belong to and pertain deployed generation. This detection approach utilizes a simple broadcast protocol. As shown in (Fig.2) identifying previous hash value, replicated nodes are detected. According to average time compute the node detection in the network. In our proposed system generality typify of distributed algorithm like XED can oppose without the intervention of the base station [3]. As shown in (Fig.3) each node in decentralize algorithm can communicate with only its one-hop neighbors. This recommendation is helpful in reducing in the communication overhead and concern with the misfortune against node compromise.

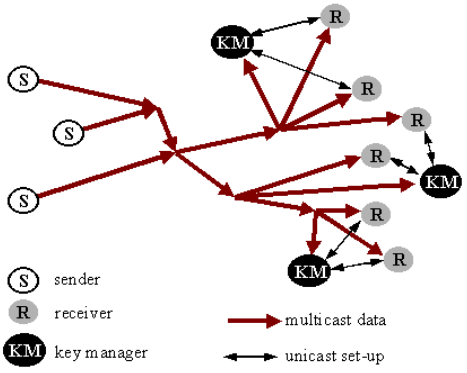

Fig. 3: Uni-cast communication

The revocation of the duplicated node can be performed by each node without flood tide the entire network with the revocation messages.

IV. Protocal Framework

In this section, we introduce to utilize the unshielded nature of the nodes to learn their system, network and adversary models arrogated in our hashing information from memory.

A. System and Network Model

The communication is assumed to be exhibiting symmetry. In addition, every node is assumed to repeatedly broadcast a beacon containing its identities to its neighbors. The nodes have mobility and motility according to the Random Waypoint (RWP) model [8], which is commonly used in representing the mobility of *ad hoc* and sensor networks [3]. This is usually required in different applications, for example, tracking the object. The time is divided into system time intervals, each of which has the same state .The time among sensor nodes does not what to be synchronized. In this model, each node randomly selects a destination point (waypoint) in the sensing field, and change the location toward it with velocity, randomly selected from a Predecease interval [Vmin,Vmax]. After stretch out the destination point, the node remains stationary for a random time and then start moving according to the identical rule. Duplicated node can intercommunicate and conspire together with each other in order to avoid duplicated node detection in Efficient Distributed Detection (EDD). For example, replicas can share their secrets and can chosen silent for a certain time if required after the collusive. Owing to the use of the hashing function [5], [6], the replicas cannot create a new identities or attire themselves as the nodes being not compromised before, because it is too problem for the adversary to have the check security secret. Disdain indefinite security issues on wireless

sensor networks such as key management technique [7], protect query [8].

B. Adversary Model

The adversary can luncheon a node attack by compromises a few sensor nodes and uses the hashing information establish from the compromised nodes to produce replicas and then inserts the replicas into the sensor network. The compromised nodes and replicas are controlled by the adversary and can interchange with each other at any time. We assume sensor nodes controlled by the opponent follow the replica-detection protocol, since the adversary always wants to keep him not obtain to others. They play obscure and seek, the opponent may not participate in the regular detection or gives the false location information [9]. Since, if any replicas are detected, furthermore starting a revoke process to revoke the duplicated node and behave as furthermore node, without forwarding data to required location. This behavior can be discover and evaluated with custody model.

V. PROPOSED METHODS

In this paper, replicated node detection algorithms for sensor networks, are proposed to detect find the duplicated node in the network in the way of dynamic approach

A. XED (eXtremely efficient detection)

Step1: Every sensor node is having a random number generator. When a node encounters another node, they exchange the random numbers [9].

Step2: Nodes encounter again, can determine by requesting the random number previously given and system time are verified. If random number no match in the node.

Step3: The materials used to verify the legitimacy of received random numbers, sequentially, along with a set representing the nodes having been blacklisted.

Step4: Security argument and a hashing function are stored in every node.

Advantages**:**

- Location information is not needed to detect the replicated node.
- Communication cost is persistent.

B. EDD (Efficient Distributed Detection)

The possible number of times, node are encountered, should be confined with high probable during a fixed period of time, while the least number of times. Nodes meets the replicas with the same identity, should be more than a threshold during the same period of time. If each node can distinguish between these two cases, it has the ability to check the replica node [9]. Then calculating threshold is used for discernment between the genuine node and the legitimate node [7]. Each node verifies its own neigh boring nodes for its related threshold. Finally anatomize the number of encounters occur on each node.

EDD advantages**:**

- Each node is considered as witness node
- Reducing the communication overhead and minimize energy by threshold value.

VI. CONCLUSION

The paper concludes detection of replicated node attacks in mobile sensor networks without the intervention of the base station. Various methods replica node detection methods have been proposed in the literature to represent against static sensor network and node need to perform the task with the intervention of base station. Notably, communication overhead is more.

- In distributed approach is more efficient in detecting replica node and reduces the communication in the network.
- Our propose methods are more effective in terms of detection the false data replication attack and data security in traffic level.

REFERENCES

[1] 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 (Secure comm), Nice, France*, 2007, pp.341–350.

[2] J. Ho,M.Wright, and S. K. Das, "Fast detection of replica node attacks in mobile sensor networks using sequential analysis," *in Proc. IEEE Int. Conf. Computer Communications (INFOCOM), Brazil*, 2009, pp.1773–1781

[3] B. Parno, A. Perrig, and V. 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.

[4] 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.

[5] J. Yi, J. Koo, and H. Cha, "A localization technique for mobile sensor networks using archived anchor information*," in Proc. IEEE Conf. Sensor, Mesh, and Ad Hoc Communications and Networks (SECON), California, USA,* 2008, pp. 64–72.

[6] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, "Mobile sensor network resilient against node replication attacks*," in Proc. IEEE Conf. Sensor, Mesh, and Ad Hoc Communications and Networks (SECON), California, USA,* 2008, pp. 597–599, (poster).

[7] 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.

[8] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, "Noninteractive pairwise key establishment for sensor networks," *IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp*. 556–569, Sep. 2010.

[9] Chia-Mu Yu, Yao-Tung Tsou, Chun-Shien Lu, Member, and Sy-Yen Kuo, Fellow," Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks", *ieee transaction on information forensics and security*, VOL. 8, NO. 5, MAY 2013.

Vikram.A received B.E degree in Computer Science Engineering from Sjb institute of technology and currently doing M.Tech degree in Sapthagiri College of Engineering.

.

Latha.A completed M.Tech and currently working as Assistant Professor in Sapthagiri College of Engineering.

