ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 5, Issue 2, pp: (234-237), Month: April - June 2017, Available at: www.researchpublish.com

# Detecting the Node Replication Attacks in Wireless Sensor Networks

K. Anitha[1], A. Senthil Kumar[2]

Research Scholar, Asst. Professor, Dept. of Computer Science, Tamil university, Thanjavur, Tamilnadu, India

***Abstract:*** **Wireless Sensor Networks are often deployed in unfavourable situations where an assailant can physically capture some of the nodes, first for reprogram the node and then, it occurs replicate them in a large number of clones, easily taking control over the network. This replication node is also called the Clone node. The clone node behaves as a legitimate node or original node. In node replication attack detecting the clone node important issue in Wireless Sensor Networks. A few distributed solutions have been recently proposed, but they are not satisfactory .First, they are energy and memory demanding: A serous drawback for any protocol to be used in the WSN-resource compactness environment. In this project first investigate the selection criteria of clone detection schemes with regard to device type, detection methodologies, deployment strategies, and detection ranges. Further, they are vulnerable to the specific assailant models introduced in this paper. The contributions of this work are threefold. First analyze the desirable properties of a distributed mechanism for the detection of node replication attacks. Second show that the known solutions for this problem do not completely meet our requirements. Third it may consist of sequential probability ratio test protocol using for this algorithm to identify the detection of node replication attacks, and show that it satisfies the introduced requirements. Our implementation specifies, user will specify its ID that means client id, secret key will be create, and then include the port number. The witness node will verify the internally bounded user id and secret key. The witness node means original node. If the verification is success, the information collecting to the packets that packets are send to the destination.**

***Keywords:*** **Static WSNs, Distributed mechanism, Node replication Attacks, Sequential probability ratio test.**

## 1. INTRODUCTION

Wireless Sensor Networks, and particularly their security issues, have received great attention recently in both academia and industry. Since tiny sensor nodes in WSNs have meagre resources for computation, communication, power, and storage, it is challenging to provide efficient security functions and mechanisms for WSNs. Above all, since WSNs are frequently deployed in unfavourable situations, sensor nodes can be captured and compromised easily by an assailant who may extract secret information from the captured nodes. After such a compromise, a clone attack can be launched by replicating the captured nodes and injecting them sporadically over the networks such that the assailant can enlarge the compromised areas by employing the clones. The secret information, such as access keys, extracted from the captured nodes and still contained in clones, may allow the assailant to gain access to communication systems throughout WSNs. For instance, clones would be authenticated as genuine nodes in a key establishment scheme of WSNs in different locations, eventually taking over a local segment or an entire network to launch various attacks, such as corrupting data aggregation, injecting false data, and dropping packets selectively. Thus it is essential to detect clone nodes promptly for minimizing their damages to WSNs.

In wireless sensor networks, sensor nodes are deployed in unattended environment and there is no security. An attacker can easily capture and compromise sensor node and make replicas of them. The replicas nodes are duplicate nodes which are created by an assailant make many replica nodes all having sane ID and these replica nodes are controlled by an assailant. Then these fake data are injected into a network which may cause eaves dropping in network communication. The fake data disrupt the network operations in network communication. Several replica node detection schemes have been proposed to defend against in static sensor network and they do not work well in mobile sensor networks where sensors are expected to move.

However, the hardware-based defensive measures are too expensive to be practical for resource-restricted sensor nodes. Various kinds of software-based clone detection schemes [1]-have recently been proposed for WSNs, considering many different types of network configuration, such as device types and deployment strategies. The limitation of software based clone detection scheme is undoubtedly that they are not generic, meaning that their performance and effectiveness may depend upon their preconfigured network settings. For example, a clone detection scheme designed for mobile WSNs is useless in static WSNs. In order to choose an effective detection scheme for a certain sensor network, it is desirable to have a set of well-designed selection criteria.

In this project first investigate the selection criteria of clone detection schemes with regard to device types, detection methodologies, deployment strategies and detection ranges, then classify the existing schemes according to the proposed criteria. First, divide static and mobile sensors according to their mobility. A static sensor node cannot move, while the location of a mobile sensor changes depending on operational scenarios. Clone detection strategies can be classified in this sense as well. Second, classify the detection schemes to centralized and distributed schemes, i.e., in terms of the ways to collect and verify evidence of clones. One is that a central node, such as a base station, acts solely on detecting clones, and the other is that a group of sensor nodes conduct the clone detection cooperatively. Third, according to the ways how to deploy sensor nodes divide them into random uniform deployment and grid deployment strategies. Finally, according to clone detection locations, divide the schemes into whole area and local area detection scheme. In the former schemes, all sensor nodes work jointly in detecting clones, but in the latter schemes only a subset of them will conduct it locally.

To summarize, classify the existing clone detection schemes based on the following criteria:

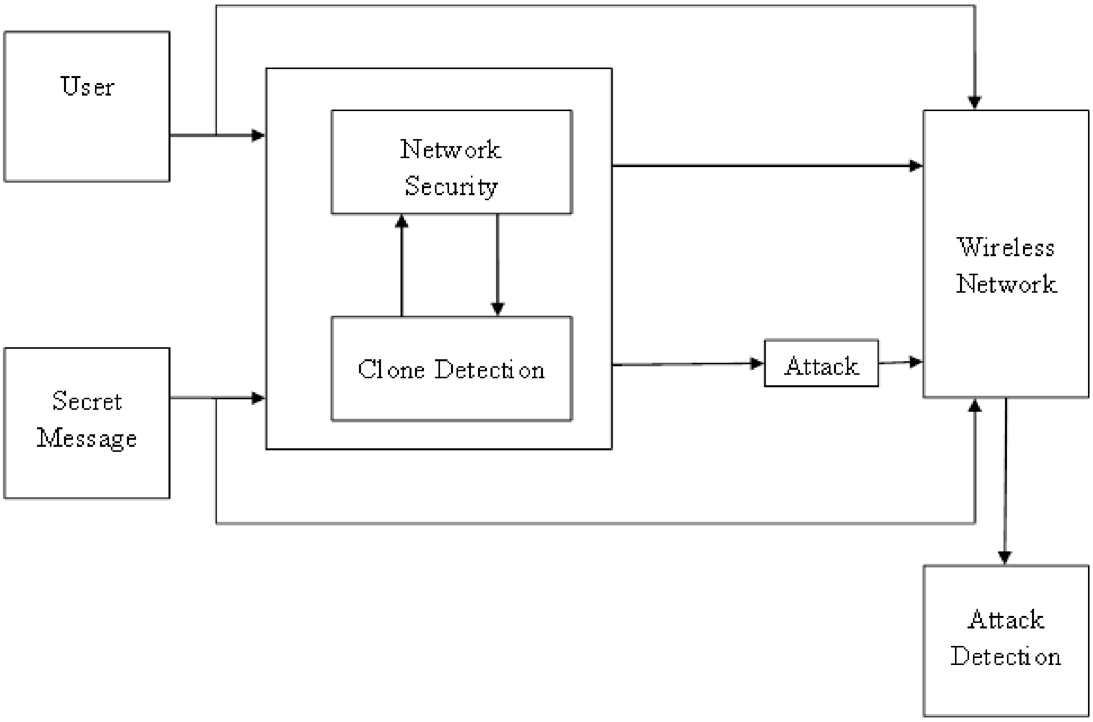
1) Device type: static (sensor) versus mobile (sensor);

2) Detection method: centralized (detection) versus distributed (detection);

3) Deployment strategy: random uniform (deployment) versus grid (deployment);

4) Detection range: whole (area detection) versus local (area detection);

### 1.1 SYSTEM ARCHITECTURE:



## 2. METHODOLOGY

### 2.1. CLONE ATTACK:

A clone attack means that an assailant injects one or more replicated nodes into a network by using same ID as another node, i.e., a captured node; compromise a large fraction of a network successfully. With standpoint to this attack, it is undertake that assailant captures only a tiny fraction of nodes in the network because capturing a large fraction may not even require clones at all and must more costly and easier to detect.

### 2.2. CLONE DETECTION:

In this module starting the clone attack, an assailant captures one or more nodes deployed in the network where the assailant wants to obtain information for achieving goals. After that, the assailant makes clone using the secret information extracted from the captured nodes and then deploys the clones into the targeted areas. To get some useful information from the clone's neighbouring nodes control them in the target areas, the clone should establish a secret key with them for a secure channel. However, before the key establishment procedure, all newly inserted nodes including the clone must pass the clone detection protocol.

### 2.3 NETWORK SECURITY:

Every node in WNSs collects the IDs and locations of its neighbours along with their communication times, 3 and every node then transmits the collected data to the Base Station (BS) in an authentic way. If a node moving over the maximum speed is found, then the BS determines that the node is replicated.

### 2.4. REPLICA ATTACK:

A compromise, an assailant could replica them for clone attacks. In the case that clones are left undetected, the assailant will compromise an entire network very easily, resulting in various kinds of malicious attacks. For example, using clones, an assailant can overhear communications widely inside networks, and assailant can corrupt data aggregation and routing by injecting false data.

### 2.5. WIRELESS SENSOR NETWORKS (WSN):

To test the detection schemes under the same simulation environments as used and focused on detecting single node replications(two clone reproduced from a single genuine node) and then calculated the average of simulation results through more than simulation experiments, which were collected and analyzed based on our performance metrics.

## 3. CONCLUSION

This paper accomplishes recognition of anomaly node attacks in static WSNs using speed measurement testing. Several anomaly node detection schemes have been proposed in the literature to defend against such attacks in static sensor networks. SPRT is a planned method to solve the problem of anomaly node occurrences in WSNs.

The major assistances of this research work are the tender of network architectural background for in effect intrusion detection, the discovery techniques for network and/or host interruption detection systems that use organization and collecting algorithms to augment the presentation of the intrusion discovery system.

## 4. FUTURE ENCHANCEMENT

The problems can be addressed by using a more sophisticated approach. The advancement of sensor hardware is continuously extending the scope of applications of static WSNs, as well as mobile WSNs, further strengthening the power of an assailant, which can launch more powerful attacks using the improved devices. In this project study various strategies taken by assailant to find more effective counter measures against them. This can be explored in our future work.

## REFERENCES

[1] B. Parno, A. Perrig, and V. Gligor, “Distributed detection of node replication attacks in sensor networks,” in Proc. IEEE Symp. Security Privacy, May 2005, pp. 49–63.

[2] 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., vol. 37, no. 6, pp. 1246–1258, Nov. 2007.

[3] M. Conti, R. Pietro, L. V., and A. Mei, “A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks,” in Proc. ACM Int. Symp. Mobile Ad Hoc Netw. Comput. 2007, pp. 80–89.

[4] 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 Comput., vol. 9, no. 7, pp. 913–926, Jul. 2010.