ISSN:0975-9646

An Approach in Detection of Replication Node in Wireless Sensor Networks: A Survey

Raju M, Selvan M

Department of CSE,
CMS College of Engineering,
Namakkal, Tamilnadu, India

***Abstract*— This paper presents a complete study on the detection of replication node in wireless sensor networks. Consider a very severe and important physical attack on WSN which is called node replication attack or clone attack. It is also known as identity attack. Several algorithms are developed to detect clone attacks, in static WSNs and mobile WSNs. Each one has its own advantages and disadvantages. This paper surveys these algorithms and compares their performance based on parameters like communication cost and memory.**

***Keywords*— Clone Attack, Sensor Network, Witness Node.**

I. INTRODUCTION

A wireless sensor network (WSN) in its simplest form can be defined as a network of (possibly low-size and low-complex) devices denoted as nodes that can sense the environment and communicate the information gathered from the monitored field through wireless links; the data is forwarded, possibly via multiple hops relaying, to a sink that can use it locally, or is connected to other networks (e.g., the Internet) through a gateway.

- The nodes can be stationary or moving.
- They can be aware of their location or not.
- They can be homogeneous or not.

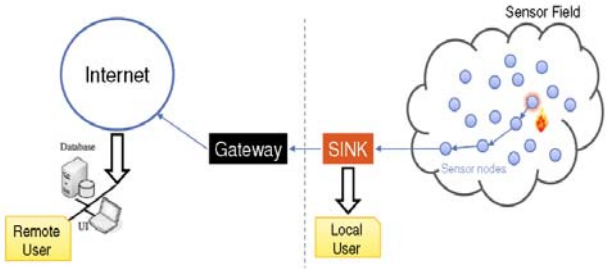

Fig.1 wireless sensor network

WSNs are composed of individual embedded systems that are capable of:

- Interacting with their environment through various sensors.
- Processing information locally.
- Communicating this information wirelessly with their neighbours.

Several software platforms have also been developed specifically for WSNs. Among these, the most accepted platform is the TinyOS.

- Open-source operating system designed for wireless embedded sensor networks.
- Incorporates a component-based architecture (wide available library).
- TinyOS is based on an event-driven execution model that enables fine-grained power management strategies.

Most of the existing software code for communication protocols today is written for the TinyOS platform.

II. NODE REPLICATION ATTACK

Wireless sensor network, an adversary first physically captures only one or few of legitimate nodes, then clones or replicates them fabricating those replicas having the same identity (ID) with the captured node, and finally deploys a capricious number of clones throughout the network.

Causes of node replication attack are as follows:

- It creates an extensive harm to the network because the replicated node also has the same identity as the legitimate member.
- It creates various attacks by extracting all the secret credentials of the captured node.
- It corrupts the monitoring operations by injecting false data.
- It can cause jamming in the network, disrupts the operations in the network and also initiates the Denial of Service (DoS) attacks too.
- It is difficult to detect replicated node and hence authentication is difficult.

A WSN can be either stationary or mobile. In static wireless sensor networks (SWSNs), the sensor nodes are stationary or static; that is, the sensor nodes are deployed randomly, and after deployment their positions do not change. On the other hand, in mobile wireless sensor networks (MWSNs), the sensor nodes can move on their own, and after deployment, appearing at different locations at different times. The advantages of our proposed include 1) localized detection; 2) efficiency and effectiveness; 3) network-wide synchronization avoidance; and 4) network-wide revocation avoidance.

Fig.2 Steps of node replication attack

III. DETECTION TECHNIQUES

Based on the detection methodologies, classify the clone attack detection.

- Detection Techniques for Stationary WSNs
- Detection Techniques for Mobile WSNs

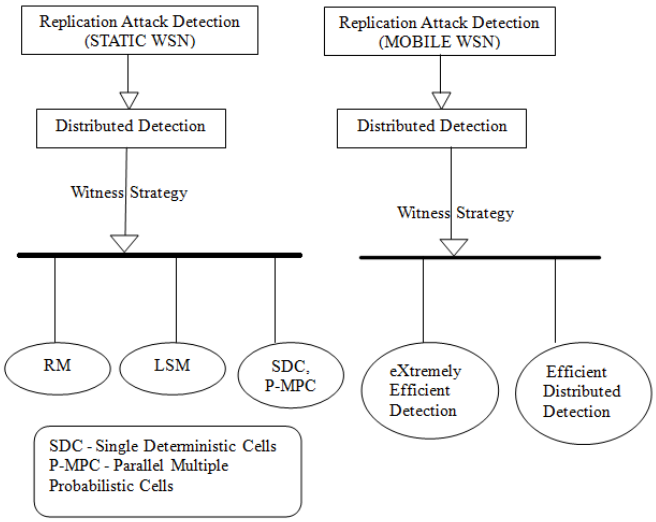

Fig.3 Steps of replication attack detection

❖ *Witness-Finding Strategy*

Node broadcast its location claim to its neighbors, shares a nodes location claims with a limited subset of chosen witness nodes. Checking whether there are the same ID's used at different location to detect the replicas. Static networks trust on the witness-finding strategy, which cannot be applied to mobile networks.

IV. DETECTION TECHNIQUES FOR STATIONARY WNSS

The detection of node replication attack in static WSNs which are categorized mainly into two types as centralized and distributed techniques.

➢ *Centralized Techniques:* In centralized techniques base station is considered to be a powerful central which is responsible for information convergence and decision making. During the detection process every node in the network sends its location claim (ID, Location Info) to base station (sink node) through its neighboring nodes. Upon receiving the entire location claims, the base station checks the node Ids along their location, and if it finds two different locations with the same ID, it raises a clone node.

1. *Random Key Predistribution:* [1] The basic idea is that the keys employed according to the random key predistribution scheme should follow a certain pattern and those keys whose usage exceeds a threshold can be judged to be cloned. In the protocol, counting Bloom filters is used to collect key usage statistics. Each node makes a counting Bloom filter of the keys it uses to communicate with neighboring nodes. It appends a random number (nonce) to the Bloom filter and encrypts the result using base station public key; this encrypted data structure is forwarded to base station. Base station decrypts the Bloom filters it receives, discards duplicates, and counts the number of time each key used in the network. Keys used above a threshold value are considered cloned. Base station makes a bloom filter from the cloned keys, encrypts the list using its secret key and broadcasts this filter to the sensor network using a gossip protocol. Each node decrypts base stations bloom filter removes cloned keys from its keying, and terminates connections using cloned keys.

2. *SET:* [3] The network is randomly divided into exclusive subsets. Each of the subsets has a subset leader, and members are one hop away from their subset leader. Multiple roots are randomly decided to construct multiple subtrees, and each subset is a node of the subtree. Each subset leader collects member information and forwards it to the root of the subtree. The intersection operation is performed on each root of the subtree to detect replicated nodes. If the intersection of all subsets of a subtree is empty, there are no clone nodes in this subtree. In the final stage, each root forwards its report to the base station (BS). The BS detects the clone nodes by computing the intersection of any two received subtrees. SET detects clone nodes by sending node information to the BS from subset leader to the root node of a randomly constructed subtree and then to the BS.

➢ *Distributed Techniques:* In distributed techniques, no central authority exists, and special detection mechanism called claimer-reporter-witness is provided in which the detection is performed by locally distributed node sending the location claim not to the base station (sink) but to a randomly selected node called witness node.

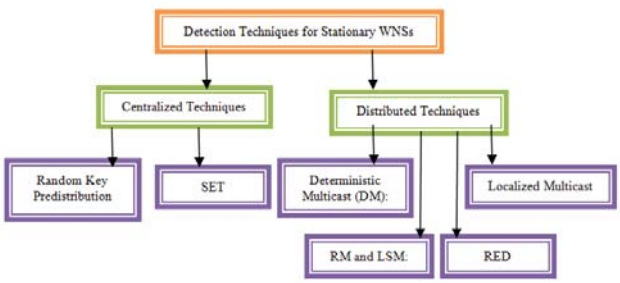

Fig.4 Detection techniques for stationary WNSs

1. *Deterministic Multicast (DM):* [2] DM protocol is a claimer-reporter-witness framework. The claimer is a node which locally broadcasts its location claim to its neighbors, each neighbor serving as a reporter, and employs a function to map the claimer ID to a witness. Then the neighbor forwards the claim to the witness, which will receive two different location claims for the same node ID if the adversary has replicated a node. One problem can occur that the adversary can also employ the function to know about the witness for a given claimer ID, and may locate and compromise the witness node before the adversary inserts the replicas into the WSN so as to evade the detection.

2. *RM and LSM:* [4] The first protocol is called Randomized Multicast (RM) which distributes location claims to a randomly selected set of witness nodes. The second protocol, Line-Selected Multicast (LSM), exploits the routing topology of the network to select witnesses for a node location and utilizes geometric probability to detect replicated nodes. In RM, each node broadcasts a location claim to its one-hop neighbors. Then, each neighbor selects randomly witness nodes within its communication range and forwards the location claim with a probability to the nodes closest to chosen locations by using geographic routing. At least one witness node is likely to receive conflicting location claims according to birthday paradox when replicated nodes exist in the network. In LSM, the main objective is to reduce the communication costs and increase the probability of detection. Besides storing location claims in randomly selected witness nodes, the intermediate nodes for forwarding location claims can also be witness nodes. This seems like randomly drawing a line across the network and the intersection of two lines becomes the evidence node of receiving conflicting location claims.

3. *RED:* [5] Randomized, Efficient, and Distributed protocol called RED, for the detection of node replication attack. It is executed at fixed intervals of time and consists in two steps. In first step, a random value, $rand$, is shared between all the nodes through base station. The second step is called detection phase. In the detection phase, each node broadcasts its claim (ID and location) to its neighboring nodes. Each neighbor node that hears a claim sends (with probability p) this claim to a set of g pseudo randomly selected network locations. The pseudo random function takes as an input ID, random number, and g. Every node in the path (from claiming node to the witness destination) forwards the message to its neighbor nearest to the destination. Hence, the replicated nodes will be detected in each detection phase. When next time the RED executes, the witness nodes will be different since the random value which is broadcasted by the BS is changed.

4. *Localized Multicast:* [8] Two distributed protocols for detecting node replication attacks called Single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cells (P-MPC). In both protocols, the whole sensor network is divided into cells to form a geographic grid. In SDC, each node ID is uniquely mapped to one of the cells in the grid. When executing detection procedure, each node broadcasts a location claim to its neighbors. Then, each neighbor forwards the location claim with a probability to a unique cell by executing a geographic hash function with the input of node ID. Once any node in the destination cell receives the location claim, it floods the location claim to the entire cell. Each node in the destination cell stores the location claim with a probability. Therefore, the clone nodes will be detected with a certain probability since the location claims of clone nodes will be forwarded to the same cell. Like SDC, in the P-MPC scheme, a geographic hash function is employed to map node identity to the destination cells. However, instead of mapping to single deterministic cell, in P-MPC the location claim is mapped and forwarded to multiple deterministic cells with various probabilities. The rest of the procedure is similar to SDC.

V. CHALLENGE IN DETECTING REPLICAS IN MOBILE ENVIRONMENT

A. 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.

B. 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.

C. Time synchronization is needed by almost all detection algorithms. Nevertheless, it is still a challenging task to synchronize the time of nodes in the network, even though loose time synchronization is sufficient for the detection purpose. Hence, as we know that time synchronization algorithms currently need to be performed periodically to synchronize the time of each node in the network, thereby incurring extreme overhead.

D. After identifying the replicas, a message used to revoke the replicas, possibly issued by the base station or the witness that detects the replicas, is usually flooded throughout the network. Nevertheless, network-wide broadcast is highly energy-consuming.

E. The effectiveness in detecting replicas, all of the schemes adopting witness-finding have the common drawback that the detection period cannot be determined. In other words, the replica detection algorithm can be triggered to identify the replicas only after the network anomaly has been noticed by the network planner. Therefore, a detection algorithm that can always automatically detect the replica is desirable.

VI. DETECTION TECHNIQUES FOR MOBILE WSNS

The node replica detection techniques developed for static WSNs, do not work when the nodes are expected to move as in mobile WSNs, and thus they have turned out to be ineffective for mobile WSNs. As a result some techniques (still not mature enough) have also been

developed for mobile WSNs to detect the replica or clone nodes. These techniques are classified into two main classes as centralized and distributed techniques.

➢ *Centralized Techniques:*

1. *Sequential Probability Ratio Test (SPRT):* [9] Based on the fact that an uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed. As a result, an uncompromised (original) mobile sensor node measured speed will appear to be at most the system-configured maximum speed as long as speed measurement system with low error rate is employed. On the other hand, replica nodes will appear to move much faster than original nodes, and thus their measured speeds will likely be over the system-configured maximum speed because they need to be at two (or more) different places at once. Accordingly, if it is observed that a mobile node measured speed is over the system-configured maximum speed, it is then highly likely that at least two nodes with the same identity are present in the network. By leveraging this intuition, the SPRT is performed on every mobile node using a null hypothesis that the mobile node has not been replicated and an alternate hypothesis that it has been replicated. In using the SPRT, the occurrence of a speed that either lessens or exceeds the system-configured maximum speed will lead to acceptance of the null and alternate hypotheses, respectively. Once the alternate hypothesis is accepted, the replica nodes will be revoked from the network.

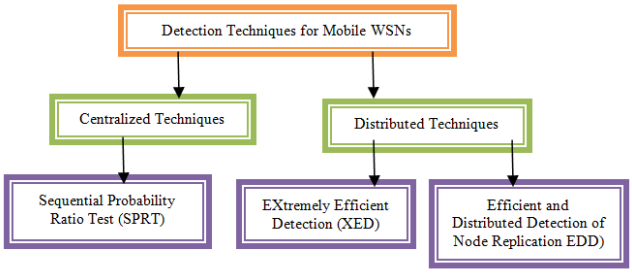

Fig.5 Detection techniques for mobile WNSs

➢ *Distributed Techniques:*

1. *eXtremely Efficient Detection (XED):* [11] eXtremely efficient detection (XED), against node replication attack in mobile sensor networks. The idea behind XED is motivated from the observation that for the networks without replicas, if a sensor node si meets the other sensor node sj at earlier time and si sends a random number r to sjat that time, then when si and sj meet again, si can ascertain whether this is the node sj met before by requesting the random number r. Based on this observation, a "remember and challenge strategy" is proposed. Once two sensor nodes, si and sj, are within the communication ranges of each other, they first, respectively, generate random numbers $rsi\rightarrow sj$ and $rsj\rightarrow si$ of$b$ bits, and then they exchange their generated random numbers. They also use a table to record the node ID, the generated random number, and the received random number in their respective memory. In case the pair of two nodes met before, the above procedure is also performed such that the random number stored in the memory is replaced by the newly received random number. The sensor node si meets another sensor node sj. If si never meets sj before, they exchange random numbers. Otherwise, the sensor node si requests the sensor node sj for the random number $rsi\rightarrow sj$ exchanged at easier time. For the sensor node si, if the sensor node sjcannot replies or reply a number which does not match the number in si memory, si announces the detection of a replica. When the replicas meet the genuine nodes, the replicas can always pretend that they meet for the first time. However, if the genuine nodes have a record showing that they ever met at earlier time, the replicas are also detected.

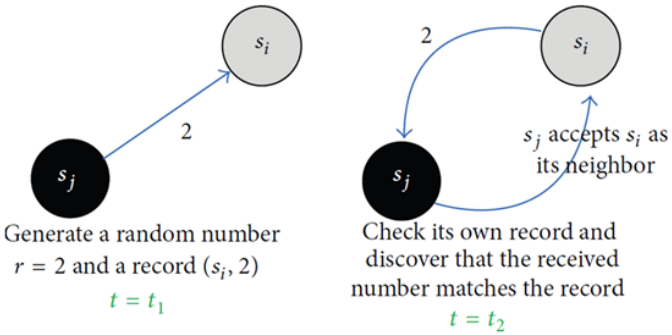

Fig.6 Operations between two genuine nodes in XED at time $t1$ and $t2$

2. Efficient and Distributed Detection of Node Replication EDD): [11] For a network without replicas, the number of times, $\mu 1$, in which the node U encounters a specific node V, should be limited in a given time interval of length T with high probability. For a network with two replicas V, the number of times, $\mu 2$, in which U encounters the replicas with the same ID V, should be larger than a threshold within the time interval of length T. According to these observations, if each node can discriminate between these two cases, each node has the ability to identify the replicas. The EDD scheme is composed of two steps: offline step and online step. The offline step is performed by the network planner before the sensor deployment. The goal is to calculate the parameters, including the length T of the time interval and the threshold ψ used for discrimination between the genuine nodes and the replicas. On the other hand, the online step will be performed by each node per move. Each node checks whether the encountered nodes are replicas by comparing ψ with the number of encounters at the end of a time interval. It can be observed from EDD that each node should maintain a list L, leading to $O(n)$ storage overhead.

VII. DISCUSSION

1) *Localized Detection:* XED and EDD can resist node replication attacks in a localized fashion. Compared to the distributed algorithm, which only requires that nodes perform the task without the intervention of the base station, the localized algorithm is a particular type of distributed algorithm. Each node in the localized algorithm can communicate with only its one-hop neighbors. This characteristic is helpful in reducing the communication overhead significantly and enhancing the resilience against node compromise.

2) *Efficiency and Effectiveness:* The XED and EDD algorithms can identify replicas with high detection

accuracy. Notably, the storage, communication, and computation overheads of EDD are all only.

3) *Network-Wide Revocation Avoidance:* The revocation of the replicas can be performed by each node without flooding the entire network with the revocation messages.

4) *Time Synchronization Avoidance:* The time of nodes in the network does not need to be synchronized.

TABLE I
COMPARISON

Schemes	Communication Cost	Memory
SET	$O(n)$	$O(d)$
SPRT	O(n)	O(d)
Deterministic Multicast	$O(g \ln g\sqrt{n/d})$	$O(g)$
Randomized Multicast	$O(n^2)$	$O(\sqrt{n})$
LSM	$O(n\sqrt{n})$	$O(\sqrt{n})$
RED	$O(r\sqrt{n})$	$O(r)$
SDC	$O(\text{if}\sqrt{n}) + O(s)$	G
P-MPC	$O(\text{if}\sqrt{n}) + O(s)$	G
XED	O(1)	
EDD	O(1)	O(n)

VIII. CONCLUSION

This paper reviewed the state-of-the-art schemes for detection of node replication attack also called clone attack. The existing techniques are broadly categorized into two classes distributed and centralized. Both classes of schemes are proficient in detecting and preventing clone attacks, but both schemes also have some noteworthy drawbacks. However, the current study highlights the fact that there are still a lot of challenges and issues in clone detection schemes that need to be resolved to become more applicable to real life situations and also to become accepted by the resource constrained sensor node.

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 Transactions on Systems, Man and Cybernetics C, vol. 37, no. 6, pp. 1246–1258, 2007.

[2] L. Eschenauer and V. D. Gligor, *"A key-management scheme for distributed sensor networks,"* in Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 41–47,Washington, DC, USA, November 2002.

[3] H. Choi, S. Zhu, and T. F. L. Porta, "*SET: detecting node clones in sensor networks*," in Proceedings of the 3rd International on Security and Privacy in Communication Networks (SecureComm '07), pp. 341–350, September 2007.

[4] Parno, A. Perrig, and V. Gligor, "*Distributed detection of node replication attacks in sensor networks*," in Proceedings of the IEEE Symposiumon Security and Privacy (IEEE S and P '05), pp. 49–63, May 2005.

[5] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "*A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks,*" in Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '07), pp. 80–89, September 2007.

[6] M. Conti, R. Di Pietro, L. Mancini, and A. Mei, "*Distributed detection of clone attacks in wireless sensor networks*," IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 5, pp. 685–698, 2011.

[7] B. Zhu,V. G. K.Addada, S. Setia, S. Jajodia, and S. Roy, "*Efficient distributed detection of node replication attacks in sensor networks*," in Proceedings of the 23rd Annual Computer Security Applications Conference (ACSAC '07), pp. 257–266, Miami Beach, Fla, USA, December 2007.

[8] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L.Wang, "*Localized multicast: efficient and distributed replica detection in large-scale sensor networks*," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 913–926, 2010.

[9] A.Wald, *Sequential Analysis*, Dover, NewYork, NY,USA, 2004.

[10] M. Yu, C. S. Lu, and S. Y. Kuo, "*Mobile sensor network resilient against node replication attacks,*" in Proceedings of the 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '08), pp. 597–599, June 2008.

[11] C. M. Yu, C. S. Lu, and S. Y. Kuo, "*Efficient and Distributed Detection of Node Replication Attacks in Mobile Sensor Networks*," in Proceedings of the 70th IEEE Vehicular Technology Conference (VTC Fall '09), pp. 20–23, Anchorage, Alaska, USA, September 2009.