INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

NODE REPLICATION ATTACK DETECTION FOR STATIC SENSOR NETWORKS (NORAD-SSN) : A SURVEY

J. Freeda Heaven Nithya[1], T.R.P. Monisha[2]

M.E Student [1],freedajeyaraj@gmail.com[1]
Assistant Professor[2],monisha.trp@gmail.com[2]
Author Correspondence: K.L.N College of Engineering [1,2], Sivagangai, TamilNadu, India.
7708374205[1] , 9894590542[2], freedajeyaraj@gmail.com[1], monisha.trp@gmail.com[2]

Abstract: - Wireless sensor networks often consist of a large number of low-cost sensor nodes that have strictly limited coverage and communication capabilities. As wireless sensor networks are typically deployed in remote and hostile backgrounds to transmit sensitive information, sensor nodes are likely to node replication attack. In node replication attack an adversary captures only a few of nodes, replicates them and then deploys an arbitrary number of replicas throughout the network. If this attack is not detected, then these replicas will consume network resources and can make the network vulnerable to a large class of internal attacks. Detecting the node replication attack has turn into a crucial research topic in sensor network security. In this survey, we have deliberated the existing detection schemes for detection of clone attacks that comes under the centralized and distributed techniques.

Keywords: SWSNs, MWSNs, Security Attacks, Security Goals, Centralized Techniques, Distributed Techniques

---

1. Introduction

The advances in the field of wireless communication and microelectronics in the last few decades, has made it possible to have cheaply available wireless sensors with which it is possible to modernize and change the way various services are deployed and delivered. With time these technologies of wireless sensor networks have grown in size and are the preferred choice for most commercial and governmental applications. However, due to these resource-constrained unshielded sensor nodes that collect, process, and transmit data in a distributed and collaborative way is often an easy target of the attackers. This unshielded nature of sensor-network nodes combined with their ease of deployment, makes them vulnerable because an adversary can capture these nodes, copy the security information to make replicas and deploy the replicas in the network to render malicious attacks. This paper reviewed the various detection techniques for clone node attack in the static sensor network.

1.1 Wireless Sensor Network

A wireless sensor network (WSN) is a heterogeneous network composed of a large number of small, low-cost devices, denoted as nodes (or motes), and one or few general-purpose computing devices referred to as base stations (or sinks). 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, they can interact with the physical environment by controlling their own movement. The objective of this paper is:

- To understand the issues associated with the node replication attack in static sensor networks
- To study and analyze various node replication detection schemes

Section 2 gives the literature survey this brief about the taxonomy of security concerns in WSNs and also discusses about the security attacks in sensor networks. Section 3 is on clone attack and various detection techniques proposed to detect and prevent clone attack. This work concludes in Section 4.

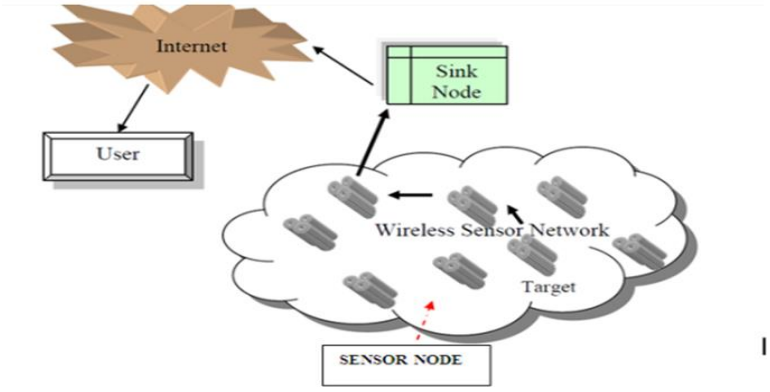

Figure 1: Wireless Sensor Network

2. Literature Survey

2.1 Security in Wireless Sensor Networks

Security is sometimes viewed as a standalone component of a system's architecture, where a separate module provides security. This separation is, however, usually a flawed approach to network security. To achieve a secure system, security must be integrated into every component, since components designed without security can become a point of attack. Consequently, security must pervade every aspect of system design.

2.2 Security Goals For Sensor Networks

To protect the information and resources from security attacks is the main goal of the security services. The basic security goals are:

- **Data Confidentiality:**
  Confidentiality is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. This is the most important issue in network security. A sensor node should not reveal its data to its neighbours.
- **Data Authentication:**
  It empowers a node to guarantee the identity of neighbour to which it is communicating.
- **Data Integrity:**
  It measures that received data has not been modified by an adversary.
- **Data Availability:**
  It ensures that services should be available by WSN whenever it is required.

2.3. Security Attacks in Sensor Networks

Security Attacks can be categorized into two broad classes:

- Active Attacks
- Passive Attacks

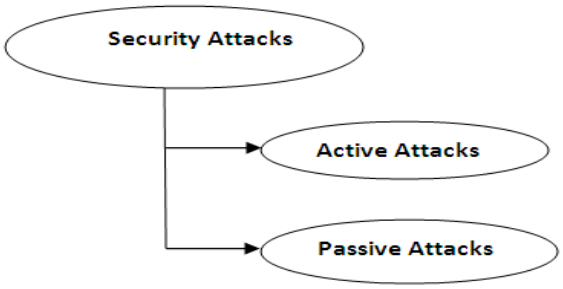

Figure 2:Types of Security Attacks

2.3.1 Active Attacks:

When unauthorized user listens the transmission and modify the information during the transmission is known as active attacks.

Active attacks are of following types- Routing Attacks, Node Replication Attack, Message corruption, Denial of Service Attack, Physical Attack, Node outage, Node Malfunction, Node subversion, False Node, Passive information Gathering.

2.3.2 Passive Attacks:

When an unauthorized user listens or monitor the transmission is known as passive attacks.

Passive Attacks are of following Types:

Monitor & Eavesdropping, Camouflages Adversaries and Traffic analysis.

3. Node Replication Attack

When deployed unattended in hostile environments, static and mobile Wireless Sensor Networks (WSNs) are vulnerable to node capture and cloning attacks, where an adversary physically compromises network nodes and extracts all information known to them, including the assigned cryptographic material and the internal states of network protocols. The obtained knowledge is used to disrupt the network by deploying and controlling copies of captured nodes (clones).

Figure 3:Steps of node replication attack

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.

Thus far, most protocols for detecting node replication have relied on a trusted base station to provide global detection. Also, some of the existing authentication techniques cannot detect such attacks, because all the replicas hold legitimate keys. The existing approaches fall into following two categories:

- **Centralized Techniques**
- **Distributed Techniques**

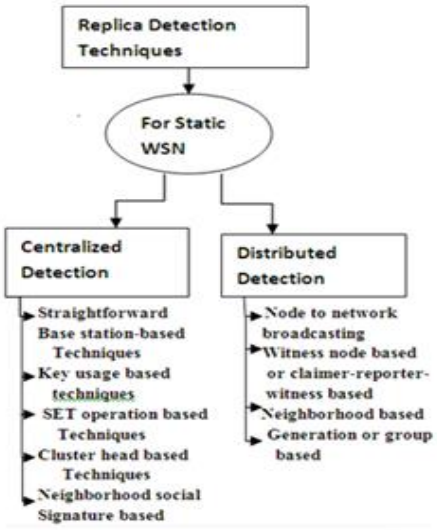

Figure 4: Taxonomy of Replica Detection Schemes for Static WSN

3.1 Centralized Detection Techniques

In centralized techniques, every node in the network sends its location id and location info to the central powerful base station via its neighbouring nodes. On receiving this information, if base station finds two different locations of same ID then it generates a clone node alarm. Some techniques come under this category are explained below:

3.1.1 On the Detection of Clones in Sensor Networks Using Random Key Predistribution

R. Brooks et al [7] have proposed a cloned key detection protocol and the basic idea behind that the keys engaged, according to the random key pre distribution scheme must follow a certain configuration, and those keys whose norm exceeds a threshold can be arbitrated to be replicated. In the protocol, counting Bloom filters is used to assemble key usage numbers and each node attaches a random number to the Bloom filter and encodes the result of base station's public key then forwarded it to the base station. Base station decodes the Bloom filters it collects and counts the numeral of time each key used in the network and if keys used beyond a threshold value are deliberated as cloned.

3.1.2 SET: Detecting clone nodes in sensor networks

H. Choi, et al [6] has proposed a clone detection approach in sensor networks, called SET in which network is arbitrarily divided into limited subsets. Every subset has a subset leader and each subset is a node of the subtree. Members are placed one hop away from their subset leader and every subset leader gathers member information and sends it to the root of the subtree. Each root performed an intersection operation and if intersection of all

subsets of a subtree is empty, then there are no clone nodes in this subtree and this report is forwarded to the base station (BS). The BS detects the clone nodes by calculating the intersection of any two received subtrees.

3.1.3 CSI: Compressed Sensing-Based Clone Identification in Sensor Networks

C. M. Yu et al [3] have proposed a centralized technique called compressed sensing-based clone identification (CSI). In CSI every node transmits a stable sensed data (α) to its one step neighbours, then sensor nodes forward and combined the received statistics from successor nodes along the aggregation tree by means of compressed sensing-based data gathering techniques. Since Base station (BS) is the root of the aggregation tree will receive the aggregated result and improves the sensed data of the system. After reconstructing the result authors defines the node as a clone node whose sense reading is greater than α.

3.1.4 Hierarchical Node Replication Attacks Detection in Wireless Sensor Networks*:*

W. Znaidi, M. Minier and S. Ubeda [9] have proposed a cluster head selection-based hierarchical distributed algorithm in which Bloom filter mechanism is used. This algorithm is based on local negotiated clustering algorithm (LNCA) protocol. This algorithm works in three steps. In the first step, an entirely material essential for Bloom filter calculations and for cryptographic procedures will be pre distributed in each sensor node. The second step accomplishes the cluster head voting. In the third step, Bloom filter creation is performed by all cluster head and Bloom filter authentication is performed by the other cluster heads. By following these three steps, node replication attacks can be determined.

3.1.5 Real-Time Detection of Clone Attacks in Wireless Sensor Networks:

K.Xing, X. Cheng, F. Liu and D.H.C.Du [10] have proposed real-time detection of clone attacks in WSN in which each sensor calculates a fingerprint by integrating the neighborhood information through an overlaid s-disjunct code and stores the fingerprint of all neighbors. When the communication starts between nodes, one node sends its fingerprint along with the message and neighbors will verify the fingerprint. If there is a clone node which is deployed in another place, it will send its own fingerprint which does not belong to the same community as other nodes, then this clone node will be detected because a clone node can have the same ID, keys but cannot have same community neighborhood.

3.2 Distributed Detection Techniques

In distributed techniques a special mechanism is used to call as claimer-reporter-witness in which the detection is accomplished by the nearby distributed node which sends the location claim to a selected node called witness node not to the base station (sink).Some techniques under this category are explained below:

3.2.1 A Randomized, Efficient, and Distributed protocol for the detection of Node Replication Attack in Wireless sensor networks

M. Conti, et al. have proposed a randomized, efficient, and distributed protocol called RED [4] for the detection of node replication attack which consists two steps. In the first step, an arbitrary value rand is shared among all the nodes over base station. The second step is detection phase in which each node transmits its ID and location to its neighbouring nodes. Each neighbour node that perceives a claim send it to a set of g pseudo randomly selected network locations and every node in the pathway from claiming node to the witness node onwards the message to its neighbour nearest to the destination and thus replicated nodes will be discovered in every detection phase.

3.2.2 Randomly Directed Exploration: An Efficient Node Clone Detection Protocol in Wireless Sensor Networks: (RDE)

Z. Li and G. Gong [5] have presented a novel clone node detection protocol called randomly directed exploration. In this protocol each node has to know its neighbour nodes. When the detection phase starts, nodes issue claiming messages to randomly selected neighbours which consist of neighbour list with an extreme hop limit. The intermediate node tries to forward the message. During promoting messages, the intermediate nodes discover the claiming messages for node clone detection. As a simple technique, the proposed protocol can expertly detect clone nodes in the dense sensor networks by consuming minimum memory.

3.2.3 Random-Walk-Based Approach to Detect Clone Attacks in Wireless Sensor Networks

Y. Zeng, J. Cao, S. Zhang, S. Guo and L. Xie [2] have proposed two protocols RAndom WaLk (RAWL) and Table assisted RAndom WaLk (TRAWL) for the detection of clone attack in wireless sensor networks. In RAWL protocol, every node broadcast a location claim and each of node neighbour forwards the claim to some randomly selected nodes and these selected nodes sends message which consists of location claim. These selected nodes starts random walk and the passing nodes are considered as a witness node which stores the location claim. If this witness node find different location claims for same ID it will declared it as a clone node. RAWL has lowest overheads in witness selection and basically TRAWL protocol is used to reduce the memory overhead of RAWL by adding trace table at each node.

3.2.4 Active Detection of Node Replication Attacks

Melchor et al. [11] have proposed a distributed protocol for the detection of replication attack for wireless sensor networks, in which each node verifies at random a few other nodes inthe network.The proposed protocol does not build a distributed database of location claims that will contain local conflicting claims when replicas exist. The idea is that each node will actively test if 1 k other randomnodes are replicated or not; they call them the scrutinized nodes. In order to test whether a scrutinized node α is replicated or not, 2 k nodes are randomly chosen in the network and asked to forward to α a request for a signed location claim. If two replicas exist, each will probably receive a request, and if both answer, two conflicting claims will be obtained by the queerer.

3.2.5 A Neighbor-based Detection Scheme for Wireless Sensor Network against Node Replication Attack

Ko et al. [12] have proposed a real time neighbor-based detection scheme (NBDS) for node replication attack in wireless sensor networks. The main idea of their scheme is that when a person moves to another community, he will meet new neighbors and tell his new neighbors where he comes from through chatting. But new neighbors will not check if he lies or not. However, if some of his new neighbors ask his previous neighbors whether this newcomer really comes from the community that he claims, the identity of the newcomer can be implicitly verified. If previous neighbors say that this person still lives in the original neighborhood, the newcomer can be detected as a replica. This observation motivates their research on node replication attacks, and replicas are detected in the same way.

4. Evaluation Metrics for Replication Detection Techniques

For the performance analysis and evaluation of replica detection protocols, four vital evaluation metrics are mostly used by the detection schemes. These are communication cost, Memory cost, Detection Probability and Detection Time.

- **Communication cost**
  Communication cost is defined as the average number of messages sent by a sensor node while propagating the location claims.
- **Memory cost**
  Memory cost defines the average number of the location claims stored in a sensor node.
- **Detection Probability**
  Detection probability is an important evaluation metric which shows how accurately a protocol can identify and detect the clones or replicas.
- **Detection Time**
  The Detection time is simply the delay between actual replica node deployment and detection.

The Comparison of various Techniques for the detection of node replication attack that are reviewed in the paper is given in table 1 and the notations used are described in table 2.

Table 1: Comparison of various detection Techniques

Technique	**Category**	**Communication cost**	**Memory cost**
Random key Predistribution	Centralized	$O(n \log n)$	—
SET	Centralized	$O(n)$	$O(d)$
CSI	Centralized	$O(n \log n)$	—
Hierarchical Detection	Centralized	$C \cdot (1 + ratio)$	$O(d) + \min(M, \omega \cdot \log 2 M)$
Real-Time Detection	Centralized	$O(t2)$	$O(t)$
RED	Distributed	$O(g \cdot p \cdot dn\sqrt{n})$	$O(g \cdot p \cdot d)$
RDE	Distributed	$O(d \cdot n \cdot \sqrt{n})$	$O(d)$
RAWL	Distributed	$O(\sqrt{n} \log n)$	$O(\sqrt{n} \log n)$
TRAWL	Distributed	$O(\sqrt{n} \log n)$	$O(1)2$
Active Detection	Distributed	$O(\sqrt{n})$	$O(d)$
Neighbour-based Detection Scheme	Distributed	$O(r \cdot \sqrt{n})$	$O(r)$

Table 2:Notations

n	number of nodes in the network
ω	the column weight in the superimposed s-disjunct code
C	Message generated by sensor node
d	degree of sensor nodes
m	The number of rows in the superimposed s-disjunct code
ratio	$\log 2M/L$packet × 100%, and Lpacket: the bit-length of a regular message
g	number of witness nodes
r	Communication radius
p	Probability that neighbouring node will forward the location claim
—	Not Available

4. Conclusion

WSNs are used in many applications like military, health and commercial applications, but due to some limitations in WSNs like minimal energy and storage and due to deployment of sensor nodes in an unattended environment makes very attractive to attacker so it is necessary to secure the network from attacks. This paper explains the classification of Security attacks arise in the network and also explains the Security goals. In this paper there is a survey on various detection centralized and distributed schemes for detecting the clone attack in static sensor networks and this paper will confidently prompt future researchers to come up with more security mechanisms for detection of clone attack in both SWSNs and MWSNs.

REFERENCES

[1] Wazir Zada Khan, Mohammed Y. Aalsalem, Mohammed Naufel Bin Mohammed Saad, and Yang Xiang, Vol 2013 "Detection and Mitigation of Node Replication Attacks in Wireless Sensor Networks: A Survey" *International Journal of Distributed Sensor Networks*,Article ID 149023, 22 pages.

[2] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie,2010 "Random walk based approach to detect clone attacks in wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 5, pp. 677–691.

[3] C. M. Yu, C. S. Lu, and S. Y. Kuo, 2012, "CSI: compressed sensing based clone identification in sensor networks," in *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops '12)*, pp. 290–295, Lugano, Switzerland, .

[4] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, 2007, "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.

[5] Z. Li and G. Gong, 2009, "Randomly directed exploration: an efficient node clone detection protocol in wireless sensor networks," in *Proceedings of the 6th IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS '09)*, pp. 1030–1035, Macau, China.

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

[7] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, 2007,"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.

[8] Zhijun Li, *Member, IEEE*, and Guang Gong, *Senior Member, IEEE 2013,"*On the Clone Node Detection in Wireless Sensor Networks" IEEE/ACM Transactions on Networking, Vol. 21,No. 6.

[9] W. Znaidi, M. Minier, and S. Ubeda, "Hierarchical node replication attacks detection in wireless sensors networks," in *Proceedings of the 20th IEEE Personal, Indoor and Mobile Radio Communications Symposium (PIMRC '09)*, pp. 82–86, Tokyo, Japan.

[10] K.Xing, X. Cheng, F. Liu, and D.H.C.Du,2009, "Real-time detection of clone attacks in wireless sensor networks," in *Proceedings of the 28th International Conference on Distributed Computing Systems (ICDCS '08)*, pp. 3–10, Beijing, China, July 2008

[11] C. A. Melchor, B. Ait-Salem, P. Gaborit, and k. Tamine, 2009, "Active detection of node replication attacks," *International Journal of Computer Science and Network Security*, vol. 9, no. 2, pp. 13–21.

[12] L. C. Ko,H. Y. Chen, andG. R. Lin, 2009,"A neighbor-based detection scheme for wireless sensor networks against node replication attacks," in *Proceedings of the International Conference on Ultra Modern Telecommunications and Workshops (ICUMT '09)*, pp. 1–6, St. Petersburg, Russia.

A Brief Author Biography

J.Freeda Heaven Nithya received the B.Tech degree in Information Technology from the Karunya University, Coimbatore in 2012. She is working toward the M.E degree in Department of Information Technology at K.L.N College of Engineering under Anna University, Chennai. Her Research interests include Wireless sensor Networks and Network Security.

T.R.P. Monisha is currently working as Assistant Professor at K.L.N.College of Engineering, Pottapalayam.She is B.E with Hons, M.E and have experience of 2 years in teaching.Her research interest includes Computer networks,Wireless sensor Networks.She has presented in two international conferences.