**NODE REPLICATION ATTACK DETECTION TECHNIQUES IN WIRELESS SENSOR NETWORK – A SURVEY**

**1MEGHA SHARMA, 2RAJSHREE PUROHIT**

1M.Tech. Scholar, Banasthali Vidhayapeeth, Banasthali, Rajasthan  
2M.Tech. Scholar, Central University of Punjab, Bathinda  
E-mail: 1sharma64megha@gmail.com, 2rajshee.purohit13@gmail.com

---

**Abstract**—Node replication attack is one of the most dreadful security attack exist in Wireless Sensor Networks, as a result researchers are paying attention towards developing security schemes against node capture attack. This Survey provides deep insights of Wireless Sensor Networks and security challenges. Also this paper includes review of various vulnerabilities and layer-wise classification of security attacks with counter measure for the same is also presented. Further, a review on one of the most dangerous attack i.e. node replication attack and its detection technique is also discussed. At the end, we put up a comparative study on the detection technique of node replication attack.

**Keywords**—Wireless Sensor Networks (WSN), Mobile Adhoc Networks (MANETs), Node Replication attack, RM, LSM, SET, DM, RED etc.

---

**I. INTRODUCTION**

Wireless sensor network is a wireless network of tiny sensor devices that are scattered throughout an area under investigation. The sensors have the capability to acquire various types of assigned information from their surrounding environment (such as temperature, air pressure, humidity, etc.) and communicate them to some central location within the Wireless Sensor Network so that some central processing can be performed on the sensor data to achieve certain desired functionality. The wireless sensor is networked and elastic, need very little power WSNs are vulnerable to different kinds of attacks. An adversary can attack for different purposes. Attacks are classified based on attacking goals and different OSI layers [11] [15].

The most hazardous attack in this scenario is a Node Replication Attack, in which the nodes are replicated manually based on their id and key values. A cloned node or an adversary promotes the node key or id of the original node, creating more replicas of the particular node in the current network with the same id and also this node may cripple the entire network.

The rest of this paper is structured as follows. In Section II includes the basic concept of WSN and Figure-1 represents the overview of the scenario of the Wireless Sensor Network. Section III and IV includes the description of the characteristics and need of security in WSN respectively. Section V and VI includes description regarding various attacks and layering approach in WSN attack and countermeasures. Section VII describes the node replication attack. Section VIII and IX includes a survey of different techniques used for network resilience against node replication attacks and comparison between them. Section X includes conclusion of this survey paper.

---

**II. BASIC CONCEPTS**

Wireless Sensor Network is large collection of nodes. As sensor nodes communicate through wireless communication link, the network can be hacked and can be invaded. WSN can be formed with the help of three or more sensor nodes and can communicate on-air. Sensor nodes have limited energy, processing and storage capacity. Sometimes if the bandwidth is low then this arises challenge for the security in Wireless Sensor Network [15] [9]. The WSN are self-organizing and self-configuring in nature. In WSN the data flows from one sensor node to another by the applied routing algorithm.

WSN have some special features that make them different from other networks such as wired network [2] [5]. These features are given below-

- WSN are self-organizing and self-configuring in nature.
- WSN topology is un-fixed because number of sensor nodes may vary time to time.
- Sensor nodes have very restricted resources, like battery life, memory space and processor's capability.
- Wireless sensor nodes are centrally controlled. In WSN data flows from one sensor node to another sensor node by the applied routing algorithm.

The general structure of Wireless Sensor Network consists of a base station or “gateway” which can communicate with a number of wireless sensors via a radio link.

As shown in figure 1, information is snatch the Wireless Sensor hub, then condenses, and exchange to the passage specifically or, if obliged, utilizes different remote sensor hubs to forward information to the entryway [9]. The transmitted information is then gone to the framework through the door association. Sensor hubs are like as little PCs, to a
great degree fundamental as far as their interfaces and their segments. They for the most part comprise of a transforming unit with restricted computational power and constrained memory, sensors, a specialized gadget, and a force source normally as a battery. The base stations go about as a passage between sensor hubs and the end client and they typically forward information from the WSN on to a server.

![Outline of Wireless Sensor Network](image)

**Figure 1: Outline of Wireless Sensor Network [4]**

### III. CHARACTERISTICS OF SENSOR NETWORK

On the basis of functionality of sensor nodes and other element, the major features and characteristics of WSN are as following [9] [13]:

- Ability to deal with node failures
- Mobility of nodes
- Potential to withstand harsh environmental conditions
- Communication failures
- Dynamic network topology
- Ease of use
- Heterogeneity of nodes
- Power consumption limitation for nodes
- Scalability to large scale of implementation
- Unattended operation
- using batteries or energy harvesting

### IV. NEED OF SECURITY IN WSN

Wireless mobile ad hoc networks (MANETs) and sensor network have numerous applications in military, country security, and other different territories. In that, many sensor networks have mission-basic assignments [13], [15]. Security is critical for such networks deployed in hostile environments, and security concerns remain a serious impediment to widespread adoption of these wireless networks. The security issues in MANETs are more challenging than those in traditional wired computer networks and the Internet. Providing security in sensor networks is much more troublesome than in MANETs because of the asset confinements of sensor node. Most sensor network effectively screen their surroundings, and it is frequently simple to derive data other than the information observed. This unwanted data spillage regularly brings about protection breaks of the individuals in the environment. Moreover, the wireless communication engaged by sensor networks facilitates eavesdropping and packet injection by an adversary. The composition of these factors demands security for sensor networks at design time to ensure operation safety, secrecy of sensitive data and privacy in sensor environments [10].

### V. SECURITY ATTACKS IN SENSOR NETWORK

Wireless Sensor Networks have the main factor which makes the network vulnerable is its broadcast nature of transmission. WSNs are open to broad range of security attacks due to wireless nature of communication. Because of broadcast nature of communication always there is threat of attacks. Furthermore, as sensor nodes are often placed in open environment so there is bonus threat of physical or natural attacks, because they are not physically protected. Attacks in WSN are follows [3] [6] [16]:

- **Sinkhole Attack**: Sinkhole attack is basically the attack in which opponents try to attract the whole traffic of a particular network. It takes place when a compromised node creates center of attraction for other nodes and attracts whole traffic. This occurs only with the help of a compromised node [11].
- **Selective forwarding**: In selective forwarding attack the compromised node forward only selected data packets not all to the receiver.
- **Wormhole Attack**: In wormhole attack, attacker records data packets in one location and then stores those data packets in another location in order to retransmit them later in the network.
- **Hello flood attack**: Hi surge assault: In hi surge assault an aggressor sends a welcome parcel to the recipient hubs, which is an endeavor to make idiot to the sensor hubs that this welcome message is send by the base station. This welcome parcel functions as a weapon to persuade other sensor node.
- **Sybil Attack**: In Sybil attack a node itself presents in many duplicate identities. This attack basically goals to fault tolerant schemes such as multi-path routing and topology maintenance and distributed storage [2].
- **Jamming**: This is one of the Denial of Service Attacks in which the adversary attempts to disrupt the operation of the network by broadcasting a high-energy
signal. Jamming attacks in WSNs, organizing them as constant, deceptive, random, and reactive [16].

- **Tampering or destruction:** Given physical access to a node, an assailant can separate delicate data, for example, cryptographic keys or other data on the node.

- **Node Replication Attack:** In node replication attack as name implies a replicated copy of a node is added to the network. An attacker adds a replicated node in a sensor network by copying node ID and other details related to their identity. This malicious node may be dangerous for the sensor network because by inserting this node attacker can manipulate a specific network segment or even it can destroy the network.

- **Continuous Channel Access (Exhaustion):** A malicious node upsets the Media Access Control convention, by ceaselessly asking for or transmitting over the channel. This in the end drives a starvation for different nodes in the network as for channel access. Impact: This is all that much like the persistent channel assault. An impact happens when two nodes endeavor to transmit on the same recurrence all the while. At the point when parcels impact, a change will probably happen in the data segment, bringing about a checksum confound at the less than desirable end. The bundle will then be tossed as invalid. A common guard against impacts is the utilization of error-correcting codes [7][14].

- **Route Information Manipulating Confusion:** This is a more dynamic assault in which a malicious node exhibit in the steering way can send the packets in wrong heading through which the destination is inaccessible. Set up of sending the packets in right heading the assailant mislead those and that too towards one node and subsequently this node may be exploited. In the event that it gets watched that a node’s network connection is getting overwhelmed with no helpful data then the victimized person node can be planned into slumber mode for quite a while to beat this [3][14].

- **Monitoring & Eavesdropping:** This is the most common attack to privacy. Snooping is the process by which, the opponent can easily get the message contents. Some times when nodes are communicating information about controls then eavesdropping is very harmful [5].

- **Deluge (reprogram) attack:** Network-reprogramming system let you remotely reinvent nodes in conveyed networks If the reprogramming process isn't secure, a gatecrasher can commandeering this process and take control of vast parts of a network. It can utilize confirmation streams to secure the reprogramming process.

- **Overwhelm attack:** An attacker may endeavor to overpower network nodes with sensor boosts, bringing on the network to forward substantial volumes of movement to a base station. This assault expends network data transmission and channels node vitality. We can moderate this assault via precisely tuning sensors so that just the particularly coveted jolt, for example, vehicular development, rather than any development, triggers them. Rate-restricting and productive data-collection calculations can likewise diminish these assaults' effects.

### VI. LAYERING APPROACH IN SENSOR NETWORK ATTACKS AND COUNTERMEASURES

The table II summarizes the attacks and countermeasures in a layering model in wireless sensor networks [2]-[5][11][14]:

<table>
<thead>
<tr>
<th>Layer</th>
<th>Threat</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Layer</td>
<td>Deluge (reprogram) attack</td>
<td>Integrity Protection</td>
</tr>
<tr>
<td>Transport Layer</td>
<td>Overwhelm attack</td>
<td>Confidentiality Protection</td>
</tr>
<tr>
<td>Network Layer</td>
<td>Flooding</td>
<td>Limiting Connection Numbers, client</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Puzzles</td>
</tr>
<tr>
<td></td>
<td>Route Information Manipulating</td>
<td>Authentication, Encryption</td>
</tr>
<tr>
<td></td>
<td>Redundancy, Probing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sybil Attack</td>
<td>Authentication</td>
</tr>
<tr>
<td></td>
<td>Sinkhole Attack</td>
<td>Authentication, Monitoring</td>
</tr>
<tr>
<td></td>
<td>Wormhole Attack</td>
<td>Flexible Routing</td>
</tr>
<tr>
<td></td>
<td>Hello Flood</td>
<td>Two-way Authentication,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Three-way Authentication,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Handshake</td>
</tr>
<tr>
<td>Data Link Layer</td>
<td>Node Replication Attack</td>
<td>Unique Pair Wise Keys</td>
</tr>
<tr>
<td>Physical Layer</td>
<td>Exhausting</td>
<td>Rate Limitation</td>
</tr>
<tr>
<td></td>
<td>Collision</td>
<td>Error Correction Code</td>
</tr>
<tr>
<td></td>
<td>Tampering</td>
<td>Tamper Proofing, effective Key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Management Schemes</td>
</tr>
<tr>
<td></td>
<td>Jamming</td>
<td>Speed Spectrum</td>
</tr>
<tr>
<td></td>
<td>Eavesdropping</td>
<td>Access Restriction</td>
</tr>
</tbody>
</table>
VII. NODE REPLICATION ATTACK

The Wireless Sensor Networks are inclined to assaults. The most noticeable assault in Wireless Sensor Network is node replication assault were the nodes are repeated for all intents and purposes. The repeated node catches the key or id of the node, makes duplicates of the node in the network with the same id and may handicap the whole network [1].

A. Causation of Node Replication Attack

The Main causation of Node Replication Attack are as follows [8] [9]:

- 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.

B. Steps to perform Node Replication Attack

Following are the steps of Node Replication Attack [4] [9]:

Step1: In this step, the sensor nodes are deployed in the harsh environment to perform specific task.

Step2: In this step, an attacker captures a sensor node physically and that captured node is known as compromised node.

Step3: In this step, an attacker collect all secrete credentials information like node ID, location of the compromised node etc. from the captured compromised node.

Step4: In this step, an attacker replicates or makes clones of captured nodes.

Step5: In this step, an attacker deploys the replicated nodes as strategic positions in the wireless network.

VIII. DETECTION TECHNIQUES OF NODE REPLICATION ATTACK

The detection of node replication attack in static Wireless Sensor Networks is categorized mainly into two types as centralized and distributed techniques [4] [9].

Figure 7: Classification of Node Replication attack detection Techniques
Centralized Techniques: In centralized procedures base station is thought to be an effective central which is in charge of data union and choice making. Amid the discovery process each node in the network sends its area claim (ID, Location Info) to base station (sink node) through its neighboring nodes [4] [9]. After getting the whole area asserts, the base station checks the node Ids along their area, and in the event that it discovers two separate areas with the same ID, it raises a clone node. Centralized Technique again ordered into two types:

1. Random Key Predistribution: The essential thought is that the keys utilized by irregular key predistribution plan ought to take after a certain example and those keys whose use surpasses a limit can be judged to be cloned. In the convention, numbering Bloom channels is utilized to gather key use measurements. Every node makes a numbering Bloom channel of the keys it uses to correspond with neighboring nodes [4] [9]. It attaches an irregular number (nonce) to the Bloom channel and encodes the outcome utilizing base station open key; this encoded data structure is sent to base station. Base station unscrambles the Bloom channels it gets, disposes of copies, and tallies the quantity of time every key utilized as a part of the network. Keys utilized over an edge worth are viewed as cloned. Base station makes a blossom channel from the cloned keys, encodes the rundown utilizing its mystery key and telecasts this channel to the sensor network utilizing a tattle convention. Every node decodes base stations sprout channel expels cloned keys from its keying, and ends associations utilizing cloned keys.

2. SET: 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 [9]. 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 [4]. 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 strategies, no central power exists, and exceptional identification system called claimer-correspondent witness is given in which the location is performed by regional standards distributed node sending the area assert not to the base station (sink) but rather to an arbitrarily chose node called witness node. Distributed Techniques again sorted into four types [4] [9]:

1. Deterministic Multicast (DM): DM protocol is a claimer-journalist witness framework [9]. The claimer is a node which generally shows its area case to its neighbors, every neighbor serving as a journalist, and utilizes a capacity to guide the claimer ID to a witness. At that point the neighbor advances the case to the witness, which will get two distinctive area claims for the same node ID if the enemy has imitated a node [8]. One issue can happen that the foe can likewise utilize the capacity to think about the witness for a given claimer ID, and may find and bargain the witness node before the foe embeds the copies into the WSN in order to avoid the detection.

2. RM and LSM: The main protocol is called Randomized Multicast (RM) which appropriates location cases to an arbitrarily chose set of witness nodes. The second protocol, Line-Selected Multicast (LSM), abuses the directing topology of the network to choose witnesses for a node location and uses geometric likelihood to recognize duplicated nodes. In RM, every node telecasts a location case to its one-bounce neighbors [8]. At that point, every neighbor choses haphazardly witness nodes inside its correspondence range and advances the location claim with a likelihood to the nodes nearest to picked locations by utilizing geographic steering. No less than one witness node is prone to get clashing location cases as per birthday conundrum when recreated nodes exist in the network. In LSM, the primary target is to decrease the correspondence expenses and expand the likelihood of detection. Other than putting away location asserts in arbitrarily chose witness nodes, the intermediate nodes for sending location cases can likewise be witness nodes.

3. RED: Randomized, Efficient, and Distributed protocol called RED [9], for the detection of node replication assault. It is executed at altered intervals of time and comprises in two stages. In first step, an arbitrary worth is imparted between all the nodes through base station. The second step is called detection stage. In the detection stage, every node shows its claim to its neighboring nodes. Every neighbor node that hears a case sends this case to an arrangement of pseudo arbitrarily chose network locations [8]. The pseudo irregular capacity takes as an info ID, arbitrary number. Each node in the way advances the message to its neighbor closest to
the destination. Henceforth, the recreated nodes will be distinguished in every detection stage. At the point when next time the RED executes, the witness nodes will be diverse since the arbitrary quality which is broadcasted by the BS is changed.

4. Localized Multicast: Two distributed protocols for distinguishing node replication assaults called Single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cells (P-MPC). In both protocols, the entire sensor network is separated into cells to frame a geographic network [8]. In SDC, each node ID is remarkably mapped to one of the cells in the framework. At the point when executing detection method, every node telecasts a location case to its neighbors. At that point, every neighbor advances the location claim with a likelihood to an interesting cell by executing a geographic hash cap ability with the data of node ID [8]. Once any node in the destination cell gets the location claim, it surges the location case to the whole cell. Every node in the destination cell stores the location claim with a likelihood. Thusly, the clone nodes will be recognized with a certain likelihood since the location cases of clone nodes will be sent to the same cell. Like SDC, in the P-MPC scheme, a geographic hash capacity is utilized to guide node character to the destination cells. Then again, as opposed to mapping to single deterministic cell, in P-MPC the location case is mapped and sent to numerous deterministic cells with different probabilities [9].

IX. COMPARISON OF CENTRALIZED AND DISTRIBUTED TECHNIQUE

Key advantages and disadvantages of Centralized and Distributed Technique are shown in table II.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Centralized Technique</th>
<th>Distributed Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor cost</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Number of Anchors</td>
<td>Small</td>
<td>Large</td>
</tr>
<tr>
<td>Accuracy</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>scalability</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Computational Overhead</td>
<td>Sensor: Low Server: High</td>
<td>Low</td>
</tr>
<tr>
<td>Communication Overhead</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>

CONCLUSION

This paper gives overview of wireless sensor networks, applications, various security attacks expected at different layer of WSN and countermeasures. In this paper, we have also discussed an important attack of WSN, Node Replication Attack and also summarized detection technique of Node Replication Attack. Both techniques are proficient in detecting and preventing Node Replication Attack, but both techniques also have some noteworthy drawbacks and boon points.

REFERENCES