Node Replication Attack in Mobile Wireless Sensor Networks: A survey

Dr. G. Padmavathi  
Professor and Head  
Department of Computer Science  
Avinashilingam Institute for Home Science and Higher Education for Women  
Coimbatore, India  
Email: ganapathi.padmavathi@gmail.com

Ms. L.S. Sindhuja  
Research Scholar  
Department of Computer Science  
Avinashilingam Institute for Home Science and Higher Education for Women  
Coimbatore, India  
Email: sindhujakarthick2011@gmail.com

Abstract  
The emerging Wireless Sensor Network (WSN) technology has many security issues due to its unattended nature. Node Replication Attack is a kind of application independent attack in which an adversary deploys its own inexpensive sensor nodes in the network as legitimate sensor nodes. Significant Wireless Sensor Network Applications are object tracking and military surveillance are affected by this attack. Existing researches on detection of the node replication attack are discussed in this survey.  

Keywords: Wireless sensor Networks, Active attacks, node replication attacks, security threats

1. Introduction  
A Wireless Sensor Network consists of number of small, inexpensive resource constrained sensor nodes. Since it is deployed in unattended environment, security is a crucial task. The [3]adversary can easily capture the credentials of the node and use them for various malicious
activities like injecting false data in the network, disrupting the network operations and also listening to the communication in the network. The node replication attack is one of the active attacks. The threats caused by active attacks and classification of active attacks are discussed in this survey. The various detection methods used for detecting node replication attack in mobile wireless sensor network is addressed in this survey.

2. Attacks on Wireless Sensor Networks
The Wireless Sensor Networks are vulnerable to many different types of attacks because of the hostile environment in which it is placed and also the broadcast nature of its transmission medium. There are two types of attacks namely active attacks and passive attacks. Specifically active attacks are concentrated in this survey because of the unattended nature of the wireless sensor environment, the attacker can easily gains the physical access and also captures the transmissions that takes place in the network.

2.1 Active Attacks
The active attacks are the one that are used by the attackers to bypass or even break the secured system. This attack [6] generally rises against the backbone of the network, grows when the information is transmitted and they penetrate electronically into the network and attack the users when they connect to the network. Denial of Service, data modification, data dissemination and data disclosure are the few results of this attack.

2.2 Threats due to Active Attack
The active attack causes various threats to the network in which it is deployed because of its unauthorized change in the state. The threats are listed out as follows:

- The origin of the message content and also the destination of the message and also the blocks of the message will be altered by the adversary.
- The adversary replays the message which is already transmitted in order to create a false message and even the message acknowledgement will also be inaccurate.

3. Classification of Active attacks
The active attacks are classified into four different types namely [4] data integrity and confidentiality, service availability and bandwidth consumption, routing and identity attacks and these attacks are further classified as shown in Figure.1.
3.1 Service Availability and Bandwidth Consumption Attacks

In this type of attack, the bandwidth [4] [6] is consumed insufficiently and also the nodes forwarding capability is destroyed. If the service is denied it is then known as variant of denial of service attacks.

3.1.1 Flooding Attack

Flooding attack is a type of Denial of Service attack in which the attacker sends a large number of packets to the target node or to the access point thereby discontinues their communication in the network.

3.1.2 Jamming Attack

In Jamming attack, an electromagnetic interference is caused in the frequency of the network operations and also in the targeted receiver so that the transmitted message is corrupted. To degrade the network performance, the fundamental way used is jamming the wireless networks.
3.1.3 Replay Attack
A replay attack is caused when the transmitted data is maliciously replayed. It is caused either by the originator or by the adversary. The forwarded packets are copied and repeatedly transmitted to the targeted node by the attacker. The poorly designed system gets affected by this attack.

3.1.4 Selective Forwarding Attack
When the packets transmitted in the network are blocked by a node in order to forward or drop the packets in the network leads to selective forwarding attack which is also known as grey hole attack. The message may be forwarded to the wrong path so that the routing information is created unfaithfully.

3.2 Routing Attacks
In routing attacks, the routing information [4] [5] [6] is changed by the attacker.

3.2.1 Unauthorized Routing Update Attack
The adversary updates the routing information which are maintained in the confidential places such as base station, access point thereby taking advantage of the routing protocol and update the information of the routing table. It leads to isolation of nodes from the base station, partitioning of network and so on.

3.2.2 Wormhole Attack
In the wormhole attack, the attacker tunnels the packets received from one point to the other point in the network and replays the packet.

3.2.3 Spoofing Attack
In spoofing attack, the routing loop is created and the routing information are attracted and replayed so as to complicate the network by the adversary.

3.2.4 Sinkhole Attack
In the sinkhole attack, the base station is prevented from getting the information regarding the sensing data. It draws the attention of the network traffic by just advertising them as the trusted node or as the shortest path.
3.3 Identity Attacks
The main target of this attack is the authentication entity. These attacks get the network address [4] [5] and the MAC address thereby cooperating with eavesdropping attack and sniffing attack.

3.3.1 Impersonate Attack
The adversary disguises as another node by its identity to launch attacks in the victim. They access the network illegitimately using the credentials of the targeted nodes.

3.3.2 Sybil Attack
The spoofed identifications such as network address and MAC address are used to present a single node to the other nodes. In the network layer, the attacker just creates the identities of the other node.

3.4 Data Integrity and Confidentiality attacks
In this type of attack, confidentiality and integrity of the data [4] [5] [6] that has transmitted will be captured by the adversary.

3.4.1 Denial of Service Attack
In the Denial of Service, the network will be made unavailable for its legitimate users. The adversary reads the data prior to the sensor nodes thereby leading to false data. This attack mainly affects the physical layer applications.

3.4.2 Eavesdropping Attack
In eavesdropping attack, the adversary overhears the communication between the two nodes in an unauthorized way. It just collects the information of MAC address and cryptographic information.

4. Categories of Active Attacks
The active attacks affect different layers of the network. The classification of different attacks, their effects and the layer in which it attacks and their preventive measures [8] are listed in Table.1.
### Table: 1 Category of Active Attacks

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Classification</th>
<th>Attack Layer</th>
<th>Attack Effects</th>
<th>Preventive Measures</th>
</tr>
</thead>
</table>
| Service Availability and Bandwidth Consumption Attacks | - Flooding Attack  
- Jamming Attack  
- Replay Attack  
- Selective Forwarding Attack | - Transport  
- Physical  
- Network  
- Network | - Exhaustion of Resources  
- Transmission Interference, Exhaustion of resources  
- crash and exploit vulnerable holes in poorly designed system  
- Unfaithful routing information in the network | Client Puzzles  
Spread Spectrum techniques  
Priority messages  
Mapping  
Lower duty cycles  
Mode change  
Egress filtering  
Anti replay protection  
Multiple Disjoint routing paths  
Diversity coding |
| Routing Attacks                              | - Unauthorized Routing Update Attack  
- Wormhole Attack  
- Spoofing Attack  
- Sinkhole Attack | Network | - Exploit Routing protocol  
- Launches different attacks  
- Network is complicated  
- Attracts the traffic by creating false routing  
- Causes Jamming in the network traffic | False routing information detection  
Probing  
Identity protection |
| Identity Attacks                             | - Impersonate Attack  
- Sybil Attack | Network | - Unauthorized access of server using victims credentials  
- Packets traversing by attacked channel is dropped | Radio Resource Testing Random Key Predistribution  
RSSI based detection scheme  
Code and Position verification |
| Data Integrity and Confidentiality Attacks   | - Denial of Service Attack  
- Eavesdropping Attack  
- Node Replication Attack | - Physical  
- Data link  
- Network  
- Transport  
- Application  
- Network | - Prevents the functioning of the network  
- Causes jamming and tampering of the network  
- Reduces data confidentiality  
- Controls the captured node and replicates, launches insider attacks | Hiding Access restriction |

## 5. Node Replication Attack

In the node replication attack, an adversary captures a node physically and reproduces the node using the secret credentials which has been extracted and deploys them in the network and
disables the Wireless Sensor Network applications. It affects a wide variety of applications such as object tracking to battle surveillance because of its application independent nature. It is also known as clone attack which is shown in Figure.2. For both the static and mobile wireless sensor networks, the security issues are the same.

![Node Replication Attack](image.png)

**Figure: 2 Node Replication Attack**

5.1 **Vulnerabilities of Node Replication attack**
The vulnerabilities caused by 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.

6. **Existing Detection Methods for Node Replication Attack in Mobile WSN**
The node replication attack in mobile Wireless Sensor Nodes is detected by various detection methods. The detection methods are classified as centralized and distributed detection and they are further classified as shown in Figure.3.
6.1 Centralized Detection Methods
In mobile wireless sensor networks there is only one centralized detection method namely the Sequential Probability Ratio Test (SPRT).

6.1.1 Sequential Probability Ratio Test (SPRT)
In SPRT, each and every time the node claims its location and time information to their neighbors and they forward it to the base station when they enter into a new location. By taking speed as the sample the base station computes the SPRT and when the limit is exceeded it is detected as replica.

6.2 Distributed Detection Methods
The distributed detection methods used in mobile wireless sensor networks are XED, EDD and mobility assisted distributed detection methods are the existing detection methods.

6.2.1 eXtremely Efficient Detection (XED)
In XED, the sensor nodes communicate with each other through the random numbers which has been generated already. If they are unable to generate the random numbers they are detected as replicas.

6.2.2 Efficient and Distributed Detection (EDD)
In EDD, the two assumptions are
• **Offline Step**- In the network without replicas, the number of times a node meets a specific node should be limited for a given time interval
• **Online Step**- In the network with replicas, the number of times a node meets a particular node should be greater than the threshold.
A node is capable of detecting replicas should be able to differentiate between the above two steps.

6.2.3 Mobility Assisted Distributed Detection
According to this detection method [7], when two nodes meet each other they exchange time-location claim and only when the witness is encountered, the data is encountered. Based on the storage of location claim it is divided as follows:
• **Unary Time Location Storage and Exchange** which stores only one location claim to detect replicas
• **Multi Time Location Storage and Exchange** which stores only multiple location claim to detect replicas

6.3 Comparison of the Existing Detection Methods
The existing methods are compared based on the performance evaluation metrics. The comparison is shown in Table.2.

<table>
<thead>
<tr>
<th>Detection Method</th>
<th>Storage Overhead</th>
<th>Computation Overhead</th>
<th>Communication Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized Detection</td>
<td>O(√N)</td>
<td>O(N)</td>
<td>O(N√N)</td>
</tr>
<tr>
<td>Sequential Probability Ratio Test (SPRT)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed Detection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eXtremely Efficient Detection (XED)</td>
<td>O(n)</td>
<td>O(1)</td>
<td>O(1)</td>
</tr>
<tr>
<td>Efficient and Distributed Detection (EDD)</td>
<td>O(1)</td>
<td>O(1)</td>
<td>O(1)</td>
</tr>
<tr>
<td>Mobility Assisted Distributed Detection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unary Time Location Storage and Exchange</td>
<td>O(√n)</td>
<td>-</td>
<td>O(n)</td>
</tr>
<tr>
<td>Multi Time Location Storage and Exchange</td>
<td>O(√n)</td>
<td>-</td>
<td>O(n)</td>
</tr>
</tbody>
</table>

**Table: 2** Comparisons of Detection Methods
7. Conclusion
In this survey, various types of active attacks has been identified and addressed based on the threats and vulnerabilities of the active attacks in WSN. Also in this paper specifically node replication attack is concentrated and various detection methods in mobile wireless sensor network environment are presented.

References