# Detection of Node Replication Attacks in Wireless Sensor Networks

Ramneet Kaur
Department of Computer Science
Lovely Professional University
Jalandhar - Delhi G.T. Road (NH-1), Phagwara
Punjab (India) – 144411
dhaliwal_ramneet@hotmail.com

***ABSTRACT:*** *Because of their exceptional qualities, WSNs are grabbing attention in the research community. WSNs are very less into view. Subsequently it is easily possible for an assaulter to catch a node physically, altering its code and getting private data like cryptographic keys. Wireless medium is inherently broadcast in nature which makes it open to attacks. These attacks can bother the operation of WSN and can even kill the purpose of their deployment [3]. Keeping in mind the end goal to ensure the data in WSN, some approaches are severely required that can make data transmission more secure from the attackers. Node replication attack or clone attack is a standout amongst the most destructive and perilous risk to an unattended wireless sensor network in light of the fact that in this attack, an adversary not only compromises the sensor nodes but can also carry out a large class of internal attacks for instance DoS attack, Sybil attack, and Black hole, and wormhole attack. Numerous strategies have been proposed for the detection of node replication attack and some fairly serious limitations like the base station introduce a single point of failure, and any compromise of the base station makes the solution useless. This leads to the motivation to work in this research area. A solution to avoid the node replication attack has been proposed. The solution will be implemented in NS-2.*

**Keywords:** Wireless Sensor Network, Node Replication Attack Detection, Distributed Protocol, Resilience, Efficiency

**Received:** 7 November 2013, Revised 16 December 2013, Accepted 22 December 2013



## 1. Introduction

Wireless Sensor Networks (WSN) are emerging as both a key new space in the IT environment and a hot research including system design, networking, distributed algorithms, programming models, data management, security and social components. The basic considered sensor system is to dissipate minor sensing gadgets over a particular geographic zone for some specific purposes like target tracking, surveillance, environmental screening and so on. These minor units are prepared for sensing a couple of movements of parameters and communicating with distinctive units. A wireless sensor network (WSN) is a remote framework containing a broad number of geographically scattered sensor nodes. These sensor nodes could be viably passed on at fundamental locale effortlessly easily. Sensor nodes work together with each one in turn to screen physical or biological conditions, for instance, temperature, sound, picture, vibration, weight, movement or contamination with the aid of distinctive

sorts of sensors. While much attention is continually paid to the routing systems and remote sensor system, the security issues are yet to be brought into light [1]. Basically, the utilization of any effective security conspire in wireless sensor systems is encouraged by many factors, for instance, the span of sensors, the processing power, memory and sort of capacities foreseen from the sensors. Sensor systems are not generally accepted registering gadgets; in this manner the existing security models and procedures need to run with them. In sensors, the geographic dispersal of the units permits an attacker to gain control of nodes and study critical information like key material, or to capture messages. The hierarchical nature of sensor networks and their route maintenance protocols permit the attacker to confirm where the root node is placed [2].

Wireless networks might be distinguished as two types: infrastructure network and ad-hoc (infrastructure less) network. Infrastructure network is a sort of a network with fixed and wired gateways. A mobile host interacts with a bridge in the network within its communication radius. The mobile unit can mobile geographically while it is communicating. When it goes out of range of one base station, it connects with new base station and starts communicating through it. This phenomenon is termed as handoff. On the other hand, Mobile ad hoc network is an aggregation of wireless mobile nodes in which nodes team up by sending packets for each other to permit them to communicate outside range of direct wireless transmission. Ad hoc networks require no fixed network infrastructure such as base stations or access points, and could be rapidly and economically set up as required.

## 2. Security in WSN

Security is a completely used term holding the security parts of verification, trustworthiness, protection, non-renouncement, and dangerous to playback. The danger of secure transmission of information over the systems is specifically corresponding to the reliance on the information furnished by the networks. For the protected transmission of diverse sorts of data over systems, a few cryptographic and distinctive methods are used. WSN have various a more excellent amounts of numbers of restrictions than other traditional computer networks. Due to these stipulations, it is unfeasible to use the acknowledged security approaches in these resource-constrained networks.

Security systems are needed in correspondence part of the systems to furnish safe information. The core motive for this is that sensed information of sensor nodes is inclined to diverse sorts of noxious before landing at the base station. The security is moreover fundamental concern to get full beneficial of in-network data processing preparing sensor systems. Undoubtedly, WSNs are prone to different sorts of compromises that explore known and obscure vulnerabilities of protocols, software and hardware, and threaten the security, integrity, authenticity, and availability of data that resides in these networked systems.

## 3. Security Requirements

The crucial component to the success of mission-critical applications working in unattended WSN applications is Communication security. There are significant security prerequisites for WSNs to ensure that the network functions correctly and securely as purposed:

### 3.1 Authenticity

Authenticity empowers a sensor to guarantee the identities of its communicating entities with the goal that no enemy could disguise another entity, and perform forging. Here, the adversary can make receiving node accept that the information originates from an authentic source

.

### 3.2 Confidentiality

Confidentiality ensures that the content of the message being exchanged is never unveiled to unauthorized entities. Network transmission of sensitive information requires confidentiality. On numerous applications, the nodes need to communicate exceptionally confidential data hence, it is very important to fabricate a secure communication channel in WSN.

### 3.3 Integrity

Integrity guarantees that a message being exchanged is never altered by an intruder without being distinguished. Data integrity serves to guarantee that the appropriated information have not been changed in transit.

### 3.4 Data Freshness

Data freshness recommends that the data is latest, and assures that no old message has been resent. This necessity is

particularly imperative when imparted keys systems are continuously utilized. Typically, shared keys need to be renewed over time.

## 4. Attacks in WSN

The nature of the WSN makes them vulnerable to several types of attacks. The various kinds of attacks are explained as:

### 4.1 Denial of Service

Denial of Service (DoS) is processed by the unintentional disappointment of nodes or malicious action. Here, the resources are exhausted by sending additional unnecessary packets and thus prevents legitimate users from gaining access to the services or resources. In wireless sensor networks, several types of DoS attacks in different layers might be performed.

### 4.2 Black hole/Sinkhole Attack

In this attack, a pernicious node acts as a black-hole to lure all the traffic in the sensor network. Particularly in a flooding based convention, the assailant listens to demands for routes then answers to the target nodes that it holds the high caliber to the base station. Once the malicious device has capacity to embed itself between the communicating nodes, it is able to do anything with the packets passing between them. Indeed, this attack can influence even the nodes those are extensively a long way from the base stations.

### 4.3 Warm Hole Attack

In a warm-hole attack, the messages are taken from one part of the network to another through a low latency link via virtual tunnel made by an adversary. The easiest instance of this attack is when one node is found between two other nodes that are forwarding. However, wormhole attacks commonly involve two distant nodes that are conspired to underestimate the distance between them and forward packets through an outside correspondence channel that is only available to the adversary.

### 4.4 Node Replication Attack

To propose and create proficient avoidance systems for attacks on wire-less sensor systems it is principal to know and understand the method for the potential adversaries. The point when an adversary propels node replication attack, most of the security destinations are impacted amazingly. Here, an adversary makes its specific sensor hubs called clone nodes and tricks the system to remember them as legitimate ones. To induce this strike, an enemy just needs to physically get one hub, and in the wake of gathering all mystery qualifications, a foe duplicates the sensor node and conveys one or more clones of the bargained node into the system at vital positions, harming the entire arrange via doing numerous interior strike. Detecting the node replication attack has turned into a basic research point in sensor system security, and outlining detection schemes against node replication attack involves different threatening issues and challenges. Node replication attack is altogether hurtful to the networks in light of the fact that these imitations or clones have authentic keys, and they are distinguished as real parts of the network, since they convey all cryptographic materials extricated from the caught nodes so a foe can utilize them to mount an assortment of insider strike [4].

## 5. Proposed Scheme

Wireless sensor networks have pulled in a ton of consideration throughout the most recent decade in wireless and mobile computing research community. However, due to distributed nature and their deployment in remote areas, systems are helpless to various security dangers that can unfavourably influence their execution. As the current sensor nodes lack hardware support for tamper-resistance and are often deployed in unattended environments where they are susceptible to catch and trade off by a foe, new security tests emerge in sensor systems [4]. Thus, that makes us to accept that existing security instruments are deficient, and new thoughts are required. Luckily, the new issues likewise move new research and speak to a chance to fittingly address sensor organize security from the begin.

### 5.1 Objectives

The objective of confidentiality is required in WSN environment to avoid the disclosure of the data going around the sensor nodes of the system or between the sensors and the base station. Authentication in sensor systems is major for each sensor node and base station to affirm that the data picked up was sincerely sent by a trusted sender or not. While clustering of nodes in WSNs, authentication is needed. Integrity controls must be executed to insurance that information won't be altered in any unexpected way. Secure administration is required at base station, clustered nodes, and protocol layer in WSN since security

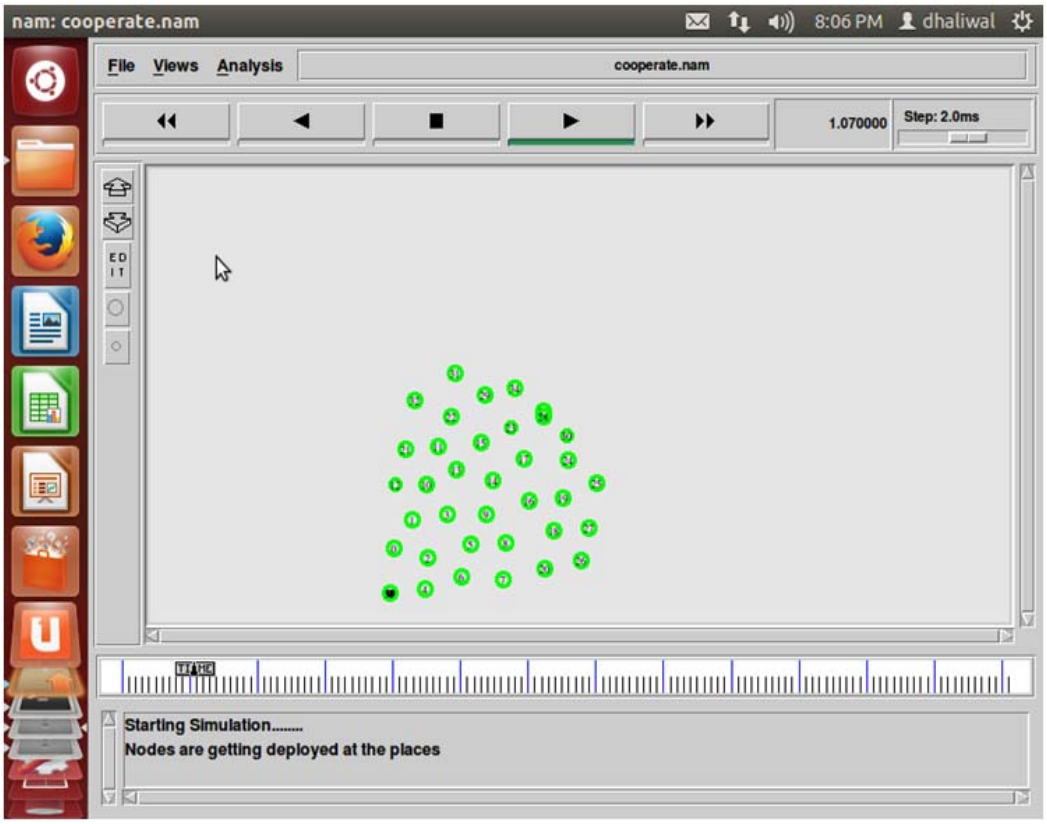


Figure 1. Nodes are getting deployed at different positions

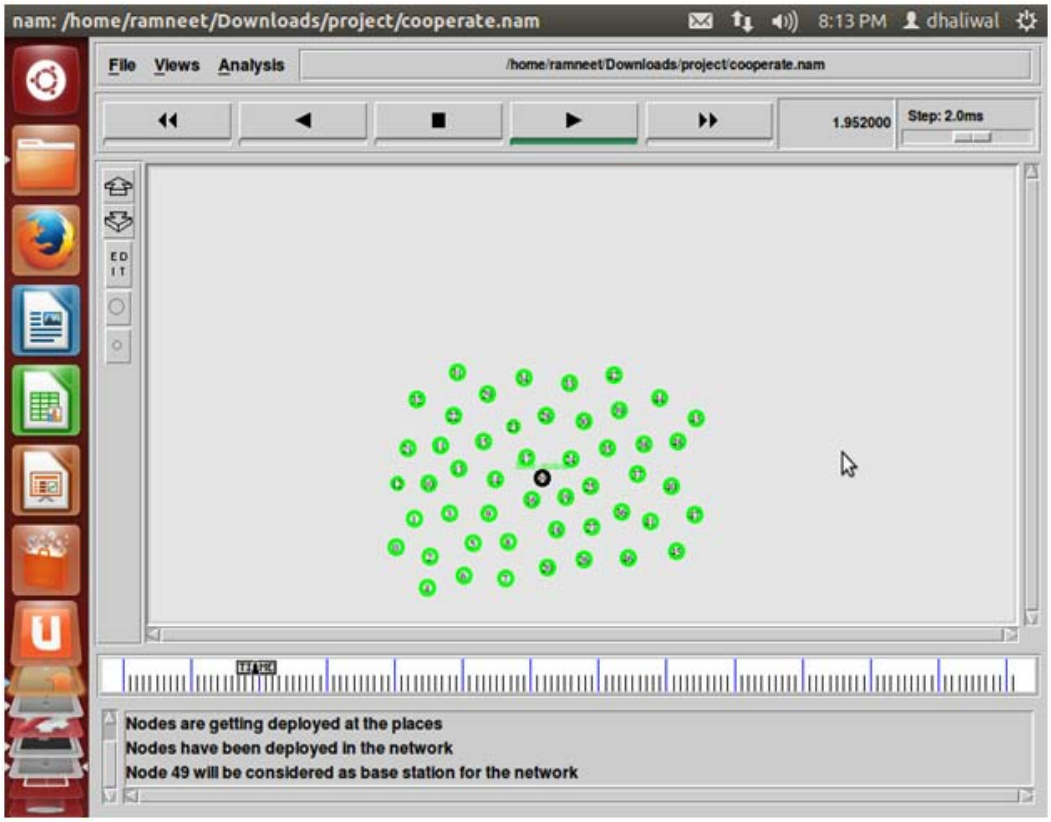


Figure 2. Node 49 is selected as base station

issues like key dissemination to sensor nodes with a particular final objective to make encryption and following information require secure organization.

### 5.2 Proposed Method

In this work, a very severe and important physical attack on WSN which is called node replication attack or clone attack has been taken into consideration. It is also known as identity attack. In this attack, an adversary first physically catches genuine nodes, then replicates them fabricating those replicas having the same identity (ID) with the captured node, and finally deploys a number of clones throughout the network. In WSN, a variety of insider attacks can be launched by an adversary by replicating the captured sensors and deploy them in the network [4]. Relying on the Centralized base station is one of the first solutions for the detection of node replication attacks. In this solution, each node sends a list of its neighbors and the geographic coordinates to a Base Station (BS). The same entrance in two records sent by hubs that are not "*close*" to one another will bring about clone recognition. At that point, the BS repudiates the clones. This result is not exceptionally productive as it has a few hindrances, for example, the base station goes about as a solitary purpose of disappointment and high correspondence takes because of the substantial number of messages. Further, nodes close to the BS will be required to route far more messages than other nodes, hence shortening their operational life. In the event that these duplicated nodes or clones remain undetected or unattended for quite a while, they can further begin the progressions in convention conduct and interruption into the frameworks security [4]. It is simple for an adversary to start such assaults because of the way that the clones have real data and they may be recognized as authentic nodes.

### 5.3 Methodology

RSD protocol (Randomization, Selection, and Detection) is a new protocol for detection of node replication attacks. RSD executes at fixed intervals of time. RSD is stationary centralized technique, where Base Station is responsible for overall functionality of nodes in Wireless Sensor Network (WSN). In stationary centralized technique, nodes are deployed at initial stage by base station will not change their location in future. Only base station can change nodes' location at the time of redeployment. In RSD, we have taken three kinds of nodes.

- Base Station node
- **Sensor Nodes:** Which send and receive messages to each other over the network.
- **Witness Nodes:** Responsible for secure transmission of messages between sensor (sender and receiver) nodes.

#### 5.3.1 Randomization

At the first step, a random value rand is shared among all the nodes by Base Station using centralized broadcasting (for example from a satellite).

#### 5.3.2 Selection

a) In the second step, a sensor node or sender who wants to send message to another sensor node (receiver), asks Base Station to select a witness node, which is close to receiver node, for secure transmission of message.

b) Base Station takes in input the current rand value, sensor node (sender) ID + location and total number of witness node g of location to apply pseudo-random function to select a witness node randomly.

#### 5.3.3 Detection

Base station acknowledges both sensor node (sender) and witness node about each other. Base station also sends a list of all the sensor nodes' ID + Location(the list of the deployment of sensor node at initial stage) to selected witness node. So witness node compares this list with current ID + Location of sender node and sender node's neighbor nodes.

a) If sensor nodes are present with different location having same ID, it means a clone node having ID of the real node has been forwarded by an adversary. So witness node will detect this clone node/replicated node and inform about this to base station and base station will revoke clone node and inform other nodes about revoking through broadcasting.

b) If a sensor node is captured by an adversary, it will be absent at current time and selected witness node will tell about this to base station that a sensor node at the time of deployment is not present currently.

c) In case, if witness node may be get captured by an adversary, base station can ensure about it using the same detection procedure. BS will ask its neighbor witness node to compare captured witness node's current ID+Location with the ID+Location


Figure 3. Base node is assigning random value to each node

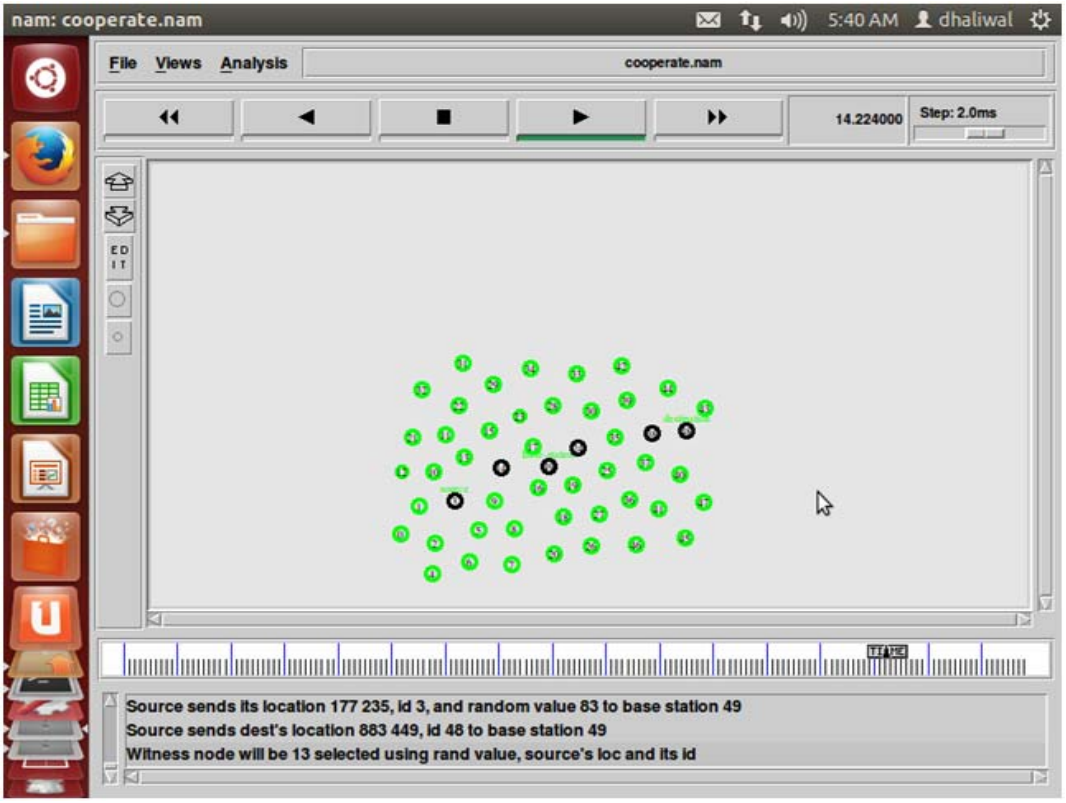


Figure 4. Source node sends its own and receiver node details to base node, so that witness nodes can be selected by base station

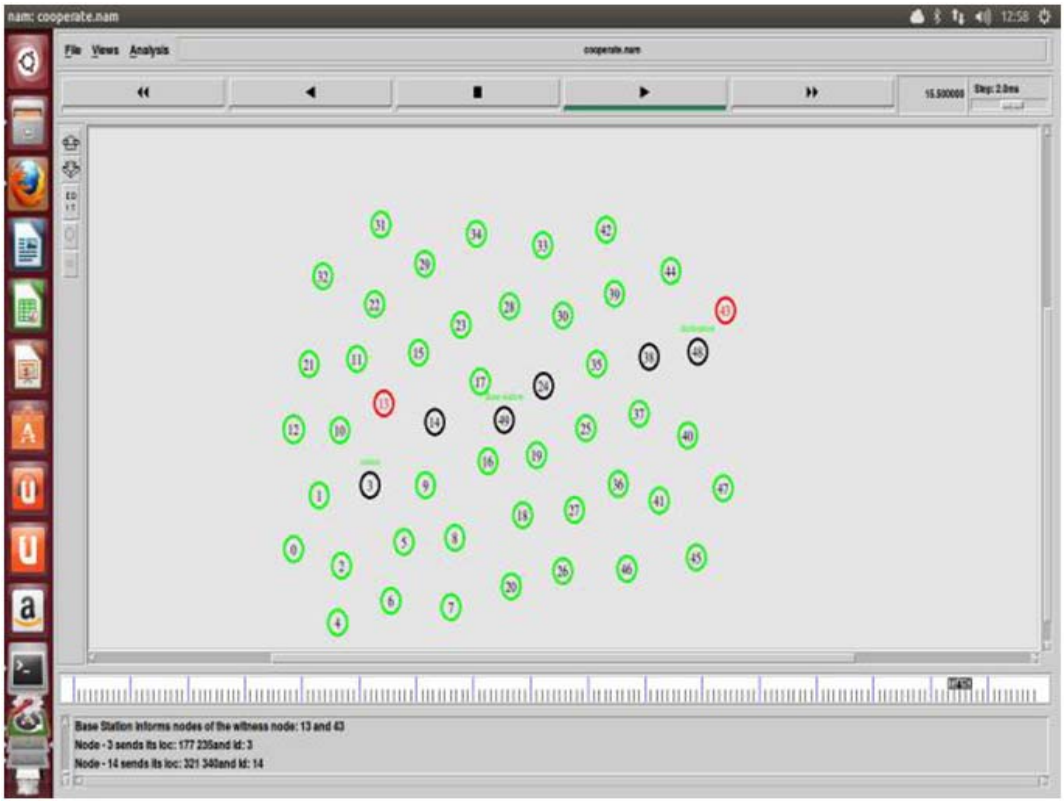


Figure 5. Base station informs nodes about the witness nodes


Figure 6. Witness node inform the base station about the clone ID and other details

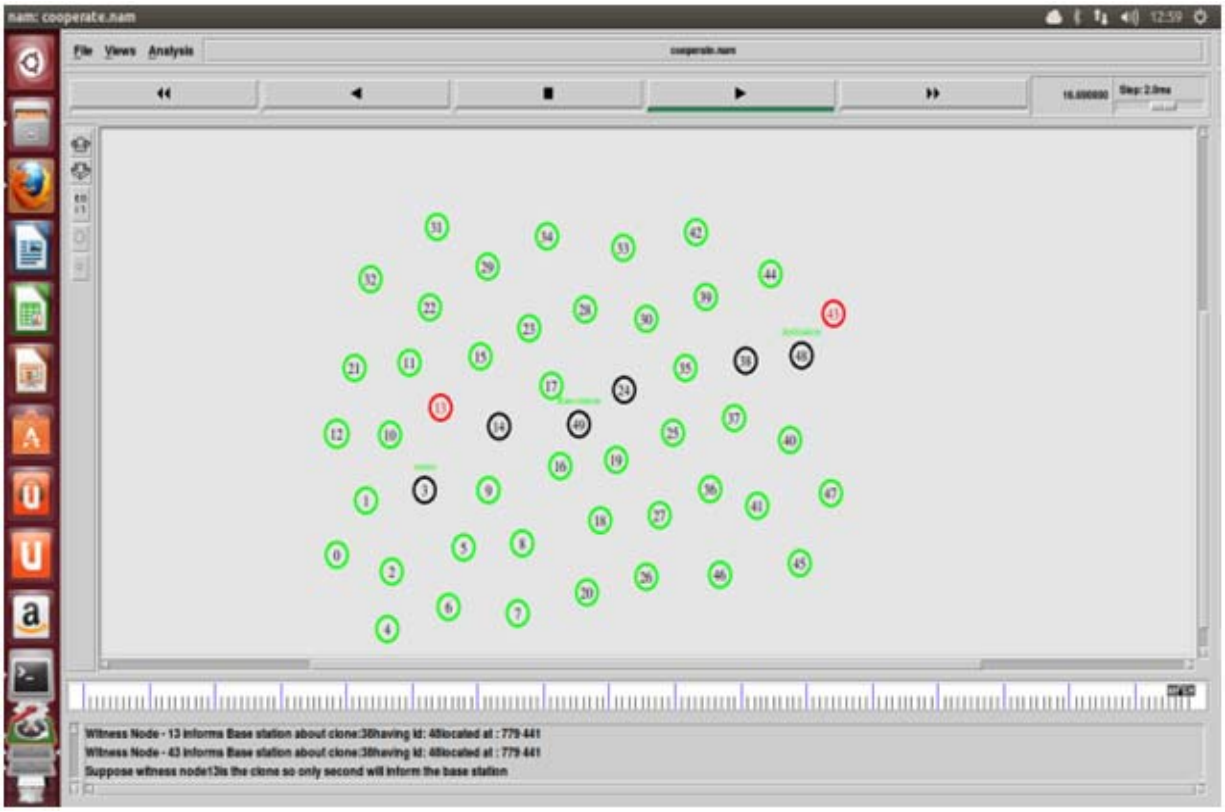


Figure 7. One of the two witness nodes is detected as clone and hence only other sends the clone details to base station

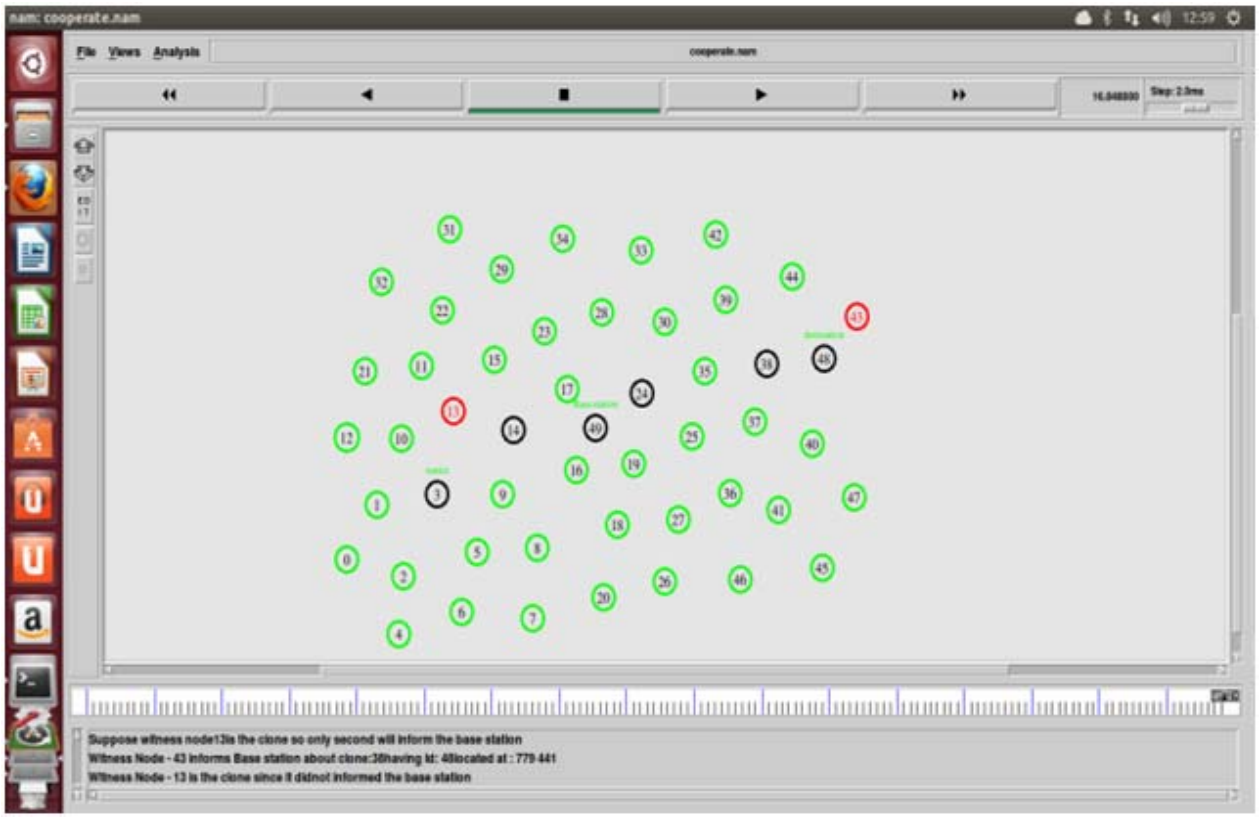


Figure 8. Witness node 13 is considered as the clone. Hence the clone is identified and attack is detected

at the time of deployment. And if witness node is really captured or replicated, neighbor witness node will inform about this to base station and base station will revoke captured witness node.

The proposed methodology is needed to be implemented in a tool. The tool opted for simulation of the proposed work is NS-2.

**6. Experimental Results**

The proposed method has been implemented in NS 2 and the experimental results have been presented.

**7. Conclusion**

Wireless Sensor Networks (WSNs) are frequently sent in dangerous situations where an enemy can physically capture some of the nodes, can reprogram, and, can replicate them in a large number of clones, easily taking control over the network. A couple of appropriated solutions to address this fundamental problem have been recently proposed. However, these solutions are not agreeable. This paper proposes RSD protocol which contributes highly in prevention of node replication attack.

**8. Acknowledgment**

The paper has been written with the kind assistance, guidance and active support of my department who have helped me in this work. I would like to thank all the individuals whose encouragement and support has made the completion of this work possible.

**References**

[1] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong. (2006). Security in Wireless Sensor Networks: Issues and Challenges, p. 20-22, ICACT.

[2] Asmae BLILAT, Anas BOUAYAD, Nour el houda CHAOUI, Mohammed EL GHAZI. (2012). Wireless Sensor Network: Security challenges, IEEE.

[3] Vijay Bhuse, Ajay Gupta, Ala Al-Fuqaha. (2007). Detection of Masquerade Attacks on Wireless Sensor Networks, 4244-0353-7/07/2007 IEEE.

[4] Wazir Zada Khan, Mohammed Y. Aalsalem, Mohammed Naufal Bin Mohammed Saad, Yang Xiang. (2013). Detection and Mitigation of Node Replication Attacks in Wireless Sensor Networks: A Survey, *International Journal of Distributed Sensor Networks*. Article ID 149023, p. 22.

[5] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary. (2006). Wireless Sensor Network Security: A Survey, Security in Distributed, Grid, and Pervasive Computing Yang Xiao, (Eds.) © 2006 Auerbach Publications, CRC Pres.

[6] Mauro Conti, Roberto Di Pietro, Luigi V. Mancini. (2007). A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks, MobiHoc'07, September 9-14, 2, Montréal, Québec, Canada Copyright 2007 ACM 978-1-59593-684-4/07/0009.

[7] Luis E. Palafox, J. Antonio Garcia-Macias. (2008). Security in Wireless Sensor Networks, IGI Global.

[8] Kuthadi Venu Madhav, Rajendra, C., Raja Lakshmi Selvaraj. (2010). A Study Of Security Challenges In Wireless Sensor Networks, *Journal of Theoretical and Applied Information Technology,* © 2005 - 2010 JATIT& LLS.

[9] Hero Modares, Rosli Salleh, Amirhossein Moravejosharieh. (2011). Overview of Security Issues in Wireless Sensor Networks, Third International Conference on Computational Intelligence, Modelling & Simulation.

[10] Eirini Karapistoli, Anastasios A. Economides. (2012). Wireless Sensor Network Security Visualization, 4th International Workshop on Mobile Computing and Networking Technologies.

[11] Sunil Gupta, Harsh K Verma, AL Sangal. (2012). Analysis and Removal of Vulnerabilities in Masquerading Attack in Wireless Sensor Networks, *International Journal of Computer Technology and Electronics Engineerin*g (IJCTEE), 2 (3), June.

[12] Patrick Tague, David Slater, Jason Rogers, Radha Poovendran. (2009). Evaluating the Vulnerability of Network Traffic Using Joint Security and Routing Analysis, 1545-5971/09/2009 IEEE.

[13] Ravi Kumar, Sunil Kumar, Prabhat Singh. (2013). Enhanced Approach for Reliable & Secure Wireless Sensor Network, 3 (7) July, *International Journal of Advanced Research in Computer Science and Software Engineering*.

[14] Md. Safiqul Islam, Syed Ashiqur Rahman. (2011). Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches, *International Journal of Advanced Science and Technology*, 36, November.

[15] Babli Kumari, Jyoti Shukla. (2013). Secure Routing in Wireless Sensor Network, 3 (8) 746, August, *International Journal of Advanced Research in Computer Science and Software Engineering*.

[16] Chakib Bekara, Maryline Laurent-Maknavicius. Defending Against Nodes Replication Attacks on Wireless Sensor Networks.

[17] Ahmad Salehi, S., Razzaque, M. A., Parisa Naraei, Ali Farrokhtala. (2013). Security in Wireless Sensor Networks: Issues and Challenges, *In*: Proceeding of the 2013 IEEE International Conference on Space Science and Communication (IconSpace), p. 1-3 July.

[18] Maneesha V. Ramesh, Aswathy B. Raj, Hemalatha T. (2012). Wireless Sensor Network Security: Real-Time Detection and Prevention of Attacks, Fourth International Conference on Computational Intelligence and Communication Networks, IEEE.

[19] Chia-Mu Yu, Chun-Shien Lu, Sy-Yen Kuo. (2012). CSI: Compressed Sensing-Based Clone Identification in Sensor Networks, 8th IEEE International Workshop on Sensor Networks and Systems for Pervasive Computing, Lugano.

[20] Yan-Xiao Li, Lian-Qin, Qian-Liang. (2010). Research On Wireless Sensor Network Security, International Conference on Computational Intelligence and Security, IEEE.

[21] Yilin Wang, Maosheng Qin. (2010). Security for Wireless Sensor Networks, International Conference on Control, *Automation and Systems*, Oct. p. 27-30.

[22] Heesook Choi, Sencun Zhu, Thomas F. La Porta. SET: Detecting node clones in Sensor Networks.

[23] Wazir Zada Khan, Mohammed Y Aalsalem, Mohamad Naufal Mohamad Saad. Detection of Masked Replication Attack in Wireless Sensor Networks.