Detecting Node Masquerade Attack Using RLE Method

DISSERTATION-II

Submitted in partial fulfillment of the

Requirement for the award of the

Degree of

MASTER OF TECHNOLOGY

In

Electronics and Communication Engineering

By

Gurminder Saini
(Reg. No. 11301498)

Under the Guidance of

Mr. Gopal Krishan

Assistant Professor

School of Electronics and Communication Engineering

Lovely Professional University, Jalandhar-Delhi G.T. Road (NH-1),

Phagwara, Punjab, India-144411

(May 2015)

CERTIFICATE

This is to certify that the Dissertation-II titlesd "**Detecting Node Masqerade Attack Using RLE Method** " that is being submitted by "**Gurminder Saini**" in fulfillment of the requirements for the award of MASTER OF TECHNOLOGY, is a record of bonafide work done under my guidance. The contents of this Dissertation-II, in full or in parts, have neither been taken from any other source nor have been submitted to any other Institute or University for award of any degree or diploma and the same is certified.

Mr.Gopal Krishan
(Assistant Professor)
LPU, Punjab

Objective of the Dissertation-II is satisfactory / unsatisfactory

Examiner I

Examiner II

ACKNOWLEDGEMENT

I express my sincere gratitude to my Supervisor **Mr. Gopal Krishan, Assistant Professor at LPU, Punjab** for his cooperation and guidance for preparing and presenting this report.

I also extend my sincere thanks to all other faculty members of Electronics and Communication Department and my friends for their support and encouragement.

Gurminder Saini

Reg. No. 11301498

CANDIDATE'S DECLARATION

I hereby certify that the work, which is being presented in the report, entitled "**Detecting Node Masqerade Attack Using RLE Method"**, in partial fulfilment of the requirement for the award of the Degree of **Master of Technology** and submitted to the Department of Electronics and communication Engineering of Lovely Professional University, Punjab, institution is an authentic record of my own work carried out during the period *january-2015* to *May-2015* under the supervision of **Mr. Gopal Krishan**. I also cited the reference about the text(s)/figure(s)/table(s) from where they have been taken.

The matter presented in this thesis has not been submitted elsewhere for the award of any other degree of diploma from any Institutions.

Date: Signature of the Candidate

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Date: Signature of the Research Supervisor

ABSTRACT

Among security challenges raised by mobile Wireless Sensor Networks, clone attack is particularly dreadful since it makes an adversary able to subvert the behavior of a network just leveraging a few replicas of some previously compromised sensors. In this work, we propose a method named as Detecting Node Masquerade Attack Using RLE Method which is used for detecting a clone in the network using RLE method. The main goal of our proposed protocol is to detect the replica of the nodes i.e. clones in the network on the basis of RLE method. RLE method is abbreviated as RSSI and List Exchange method i.e. R represents RSSI means received signal strength indicator. After that we also compare our proposed protocol with the known method i.e. Hip-Hop protocols which are also used to find a clone in mobile wsn and our simulation shows that our proposed protocol outperforms the existing approach in terms of detection rate and time taken to detect a clone. In future work, we can also use a clustering protocol to make this work more efficient.

Table of Contents

LIST OF FIGURES

Fig. No. **Title** **Page No.**

LIST OF ABBREVIATIONS

WSN	Wireless sensor networks
BS	Base Station
CH	Cluster Head
HIP	History information exchange Protocol
HOP	History Information-exchange Optimized Protocol
RLE	RSSI and List Exchange method
RSSI	Received signal strength indicator
DM	Deterministic multicast
RM	Random multicast
LMS	Line selected multicast
SPRT	Sequential Probability Ratio Test
XED	Extremely Efficient Detection Protocol
EDD	Efficient and Distributed Detection

CHAPTER 1
INTRODUCTION

1.1 WSN Introduction

A sensor system is a framework contained detecting (measuring), registering, and correspondence components that gives a manager the capacity to instrument, watch, and respond to occasions and phenomena in a predetermined domain. The chairman ordinarily is a common, framework, or a data innovation (IT) system.. The more present day systems are bi-directional, likewise empowering control of sensor action [1]. The advancement of remote sensor systems was roused by military applications, for example, war zone observation; today such systems are utilized as a part of numerous mechanical and customer applications, for example, modern procedure observing and control, machine wellbeing checking, and so on. The WSN is constructed of "nodes" – from a couple to a few hundreds or even thousands, where every node is joined with one (or now and then a few) sensor.

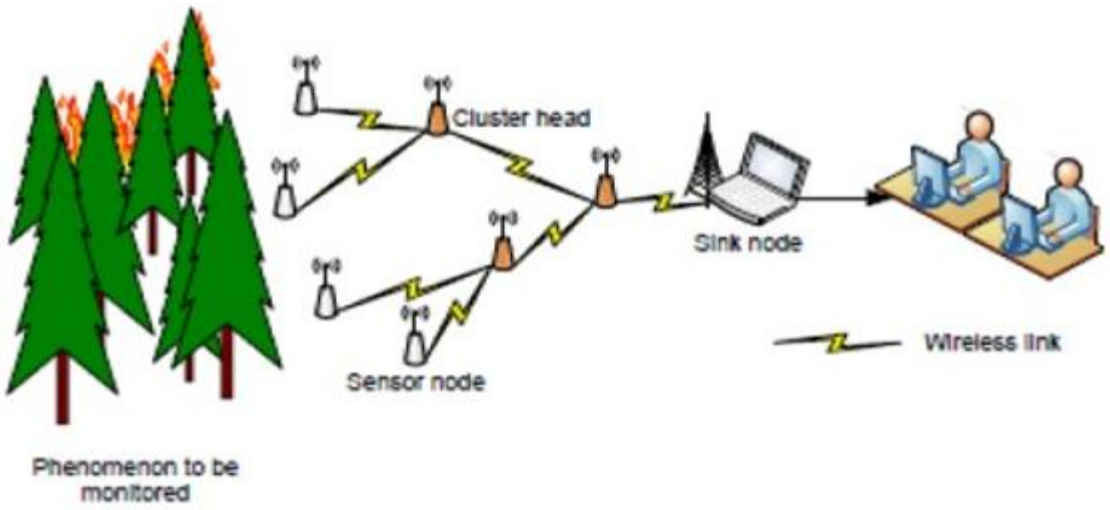

Figure 1. Typical wireless sensor network architecture [1]

The WSN is constructed of "nodes" – from a couple to a few hundreds or even thousands, where every hub is associated with one (or at times a few) sensors. Every such sensor system node has regularly a few sections: a radio handset with an interior receiving wire or association with an outside reception apparatus, a microcontroller, an electronic circuit for interfacing with the sensors and a vitality source, generally a battery. The proliferation strategy between the bounces of the system can be directing. These systems comprise of individual nodes that have the capacity to cooperate with their surroundings by detecting or controlling physical parameters; these nodes need to team up to satisfy their assignments as, as a rule, a solitary node is unequipped for doing as such; and they utilize remote correspondence to empower this joint effort. In the nodes without such a system contain in any event some processing, remote correspondence and detecting or control functionalities. In spite of the way that these systems likewise frequently incorporate actuators, the term remote sensor system has turned into the regularly acknowledged name [2]. Now and then, different names like "remote sensor and actuator systems" are additionally found. These WSNs are intense in that they are manageable to bolster a considerable measure of very different true applications; they are likewise a testing research and designing issue as a result of this very flexibility.

1.2 Applications of WSN

A sensor network performs a set of high-level information farm duties such as exposure, following or categorization. Together with finding of false alarms, errors and track feature, procedures of presentation for these farm duties are well-defined[3]. The applications of sensor networks differ extensively in application necessities and are large ranging, manner of exploitation, sensing modality. A few applications are given below:

- Ecological/environmental Control (e.g. Traffic, security)
- Manufacturing Monitoring (e.g. factory, supply chains)
- Water/wastewater Monitoring (e.g. Landfill ground well level monitoring and pump counter, Agriculture)
- Infrastructure security (e.g. power grid)
- Battleground awareness (e.g. multi-target tracking)
- Health Monitoring
- Context sensitive computing (e.g. intelligent home, responsive environment)

1.3 Characteristics of WSN

First characteristic is that the sensor nodes are little devices and minute in volume. Second is that the sensor nodes have restricted storage ability that does not sustain accessible conventional wireless network's security mechanisms in WSN. Third characteristic is that the sensor networks have restricted resources, so computational power in WSN is very less as compared to conventional networks. The accessible conventional protection has actions like key establishment, encryption and decryption. Fourth characteristic is that the sensor nodes in WSN are battery based, so life time of node depends on the battery [4]. The nodes in the WSN are joined in wireless manner so clash and jamming can occur which gives extra scale to trapping the sensed data in the network.

1.4 Challenges of WSN

- Bandwidth
- Ad-hoc deployment
- Energy
- Medium Access Control (MAC)
- Routing
- Localization
- Operating Systems
- Security

1.5Attacks in WSN

There are numerous types of attacks: eavesdropping, disruption, hijacking and rushing [5].

1.5.1 Eavesdropping: In this an intruder determines the aggregate data i.e. outcome by either the node or the sensor network. The message being transmitted by the nodes may captured by the attacker from the network traffic by listening for sometime or openly compromising the nodes. Types of eavesdropping are:

- **Passive:** The attacker uses only transmitting section to eavesdrop on all messages and stay unidentified to the sensor nodes.

- **Active:** By attacking sensor nodes, the attacker efforts to distinguish information by transmitting queries to sensors.
- **Disruption:** Here the attacker disrupts the sensor's working which is done in two ways:
- **Semantically:** To render aggregated data corrupt or useless, the intruder inserts messages, alters data or change values. Examples are given below:
- **Routing Loop:** In routing loop, an intruder inserts wrong data due to which all packets go round in circles and the nodes forma routing loop and resulting in wasting valuable communication and battery assets.
- **Denial of service:** In DOS, an intruder inserts the wrong data or changes the message and end up averting the routing protocol from functioning properly. DOS can occur due to node failure also. By transmitting additional needless packets, DOS tries to exhaust assets presented to the sufferer node and thus prevents it from accessing the services entitled to it. DOS attack not only disrupt, destroy the network but network's capability to provide services is also diminishes. DOS attack at physical layer could be congestion and tempering. At data link layer could be clash, collapse [5]. At network layer could be neglect and greed, black holes. At transport layer could be flooding and resynchronization. To stop DOS, tough authentication and identification of traffic must be integrated.
- **Sybil Attack:** In Sybil attack, an intruder generates numerous false identities of a malicious node to execute preferred attack on the network. This malicious node will transmit wrong information to all the other nodes in the network. This wrong information can be location of nodes, signal power. To prevent Sybil attack from an outsider, authentication and encryption techniques can be used and the identities of the nodes can be used to prevent Sybil attack inside the network[5]. To prevent inside attack. Public key cryptography can be used. Every sensor node is allocated with some exclusive information before deployment and then the server generates identity certificate required this node's individuality to allocated exclusive information and downloads this information to the node. A node first shows its identity certificate to securely demonstrate its identity and shows that it matches the linked exclusive information.

- **Wormhole Attack:** In this, to forward traffic between each other, two nodes are reasons to use an out-of-band channel and enabling them to mount several other attacks along the way. Sender sends a message to the receiver node and that node will send message to its neighbours. The neighbouring nodes send the message to originating node as they think that the message was sent from sender node, but it in no way appears since it is too distant away.
- **Black hole /Sink hole Attack:** In this nasty node promotes a small distance to all objectives. A nasty node acts as a black hole, especially in flooding based protocol, it listens to the requests and responds to the end nodes that it holds the shortest path or high link value to base station. If an attacker injects in communicating nodes, it is capable to do everything with the packets transient between them. To prevent this, geographic routing protocols can be used.
- **HELLO flood Attack:** In this attack a node transmits a Hello packet with peak power, so that, huge amount of nodes yet extreme away in the network select it as parent node. The sensors are thus convinced that the opponent is their neighbour. Thus during transmission nodes will transmit through this adversary node and ultimately spoofed by the attacker. This attack can be neglected by inspection bidirectional of connection, so that the nodes guarantee that they can attain their parent inside one hop.
- **False or Malicious Node Attack:** Most attacks in WSN are due to insertion of false node in network. This should be checked in Routing layer itself.

- **Physically:** In this an intruder tries to upset the sensor analysis by influencing the environment. For example, by producing heat in the locality of sensors will consequence in mistaken values being reported.

1.5.3 Hijacking: In this an intruder alters the collective outcome of a function on numerous network sensor nodes. This attack will take the power over sensor node in network. This method gives extra power to the eavesdropping and disruption by hijacking major sensor nodes[5].

1.5.4 Rushing Attack: A node requiring a path to sink will transmit ROUTE REQUEST packet. To limit this flood of ROUTE REQUEST packet, every node promotes only one ROUTE REQUEST created from any Route Discovery. The on-demand routing protocols like AODV,

DSR will forward only REQUEST that appears first from every Route Discovery. This is a powerful attack which results on DOS and simple to execute by an intruder.

Motivation

WSN is trend of past few years and in WSN huge numbers of small nodes are deployed. These nodes after sensing the environmental changes, will give the report to the other nodes. Because of deployment of the nodes in the environment, security becomes the key factor in the network. Any attacker can attack the sensor node and get the information about the sensed data before reaching to the base station. In WSN it is essential to upload the novel code image to all the nodes which is also called as reprogramming. There are two types of approaches in WSN: central approach and distributed approach. In central approach base station is involved which have right to reprogram sensor nodes but if the base station fails or any node drop connection to the base station the whole process is gone. So distributed approach is employed for reprogramming in which base station is not considered. In this dispersed approach many certified users can simultaneously communicate and update the code images. So, security becomes the main issue in this approach. The motivation to do work in distributed environment is derived from various research works.

Chapter 2
LITERATURE SURVEY

Edwin Prem Kumar Gilbert, Baskaran Kaliaperumal, and Elijah Blessing Rajsingh ,(2012)
In this survey report, the whole wireless sensor network is discussed about working and applications. Like there are numerous applications of WSN due to its scalability, low cost and flexability.Though wireless sensor networks are constraint by its challenges like energy consumption, security is also the major issue where malicious intruders are there and there is great scope of research in this challenge to secure the information [6].

J.Anthoniraj ,Trichy and T.Abdul Razak(2014) In this paper analysis on the various centralized and distributed protocols in the static and mobile environments. To detect the clone in mobile sensor network. There are some protocols which are developing by researcher such as RED ,BC-MEM and P-MPC. [7]

D Sheela , G. Mahadevan, (2012) The propose of this is lightweight and fast mobile agent technology based security solution against cloning attack, sinkhole attack and black hole attack for wireless sensor networks (WSNs)and also increase the security of the sink. Comparison of communication overhead and cost were made between the proposed attack detection system using mobile agent against the security system in the absence of mobile agents with several base stations. [8]

Jennifer Yick, Biswanath Mukherjee and Dipak Ghosal(2008), This paper gives a detailed description about wireless sensor networks applications like target tracking and remote environment monitoring. Basically the requirement of each applications are different and because of which different protocols and algorithms are needed to support these applications and this paper deals with such issues like internal platform and operating system ,communication protocols and network services.[9]

M.Contia, R.DiPietrob and A.Spognardic, 2013
This paper basically tells that how we can detect clone in the mobile wireless sensor network.
They have firstly proposed two distributed, efficient and cooperative protocols to detect replicas:-HIP and HOP protocols. History information-exchange protocol and its optimised

version i.e. HOP ()History information-exchange optimum protocol) and studied their behaviour against the introduced types of attacker, considering two different mobility models and compare theirs solutions with state of art.[10]

Bryan Parno, Adrian Perrig and Virgil Gligor, 2005

In this paper, they have told about previous technique of clone detection that if clone is distributed in the whole network it cannot be easily detected.So,they give the methodology of detecting clone i.e. Randomized Multicast distributes node location information to randomly-selected witnesses, exploiting the birthday paradox to detect replicated nodes, While Line-Selected Multicast uses the topology of the network to detect replication. Both algorithms provide globally-aware, distributed node-replica detection, and Line-Selected Multicast displays particularly strong performance characteristics. Finally, the result shows that Line-selected Multicast shows better performance.[11]

Heesook Choi, Sencun Zhu and Thomas F. La Porta

This paper describes that if an opponent may obtain all information from these sensors, clone and intelligently deploy them in the network it is called as clone attack and then all such attacks are not just few they also have selective interruption and detection and high overhead. So, in this paper they gave such scheme SET to detect such clone attacks by computing set operations. SET is composed of four components: formation of exclusive subsets, authentication of subset covering, distributed set computation on subset trees, and preservation of reliable set operations on the tree. The results show that this method has less transmission overhead.[12]

Mauro Conti, Member, IEEE, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei (2011)

They have proposed self-healing, Randomized, Efficient, and Distributed (RED) protocol for the detection of node replication attacks. They have introduced the preliminary notion of ID-obliviousness and area-obliviousness that convey a measure of the quality of the node replicas detection protocol; that is, its resilience to a smart opponent. At the end, they compare the RED

protocol with the state-of-art (LSM) and proved that overhead by RED are low as compare to others.[13]

Yih-Chun Hu,Adrian Perrig,Member,IEEE,and David B. Johnson

This paper have description about the wormhole attack is possible even if the attacker has not Compromised any hosts, and even if all communication provides security and confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location in the network, Tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based ireless security systems. They present the general mechanism, called packet leashes, for detecting and thus defending against wormhole attacks, and we present a specific protocol, called TIK, that implement leashes.[14]

Richard Brooks, P. Y. Govindaraju, Matthew Pirretti, N. Vijaykrishnan, and Mahmut T. Kandemir (2007)

This paper gives description of Random key predistribution security schemes as these schemes are suited for use in sensor networks due to their low overhead. However, the security of a network using predistributed keys can be compromised by cloning attacks. In this attack, an opponent breaks into a sensor node, reprograms it, and inserts several copies of the node back into the sensor network. Cloning gives the opponent the simple way to build an army of malicious nodes. In this paper, they have given an algorithm that a sensor network can use to detect the presence of clones. Keys that are present on the cloned nodes are detected by looking at how often they are used to authenticate nodes in the network. The results show that the proposed method accurately detects the presence of clones in the system and supports their removal.[15]

Mohammad Hasan Ansari ,Vahid Tabataba Vakili(2013)

This paper deals with the method of detection of replica of nodes with mobile nodes in wireless sensor networks are analysed and also by using mobility criteria, a new classification for node replica detection procedures and attacker model are proposed. To compare and evaluate different procedures, different metrics are introduced and used for theoretical analysis and classification procedures.[16]

Rajesh yadav, Shirshu varma and N.Malviya,2009

In this paper, they describe current challenges in the design of energy efficient medium access control protocols for wireless sensor networks. They describe several protocols for WSNs emphasizing their strength and weakness whenever possible. In the end, they have compared schedule based TDMA; contention based CDMA, FDMA and CDMA techniques and describe their pros and cons respectively.[17]

Vikash Kumar, Anshu Jain and P N Barwal,2014

This paper only tells about the major challenges in wsn like security and some security mechanism to improve the safety of the network. Basically, they describe about all the security attacks in the wireless sensor networks and with their threats and also security in wsn is an important factor to get acceptance and use of sensor networks. [18]

Chris Karlof , David Wagner,2010

In this paper, they have proposed a routing algorithm but as its not simple routing algorithm although they have proposed a secure routing algorithm in wsn and they introduces two categories of novel attacks against senor networks that is sinkholes and hello floods and examine the security of all sensor networks.[19]

Sepide moradi,Mina zolfy lighvan,2014

Basically, they described the clone attacks in the mobile wsn and there are many ways to tackle a clone attack but they usually suffer from high overhead. In this paper, they proposed a new method i.e. MACDC method which is used to detect replica using mobile technology and results prove that this method is better than the other known solutions in terms of the energy consumption and overhead of the network. [20]

CHAPTER 3
SECURITY IN WSN

3.1 Introduction to Security:

Network application and environmental situations are measured for alternative of good safety/security mechanism and the factors that are measured are: sensor node workstation performance, memory capability and energy. Various typical security necessities are like availability, confidentiality, integrity, authentication, non-repudiation are essential for security . Some unique security necessities that are essential are message novelty, intrusion detection, intrusion tolerance. Several of the security solutions for IP networks are not appropriate for WSN security due to resource, space and cost constraints. Security in WSN is a very dynamic research area where novel and innovative solutions to the security issues are recommended on a normal basis [1].

Security offers five services, out of which four are associated to message replaced using the network: message confidentiality, integrity, authentication and non-repudiation .Fifth service offers entity authentication or identification.

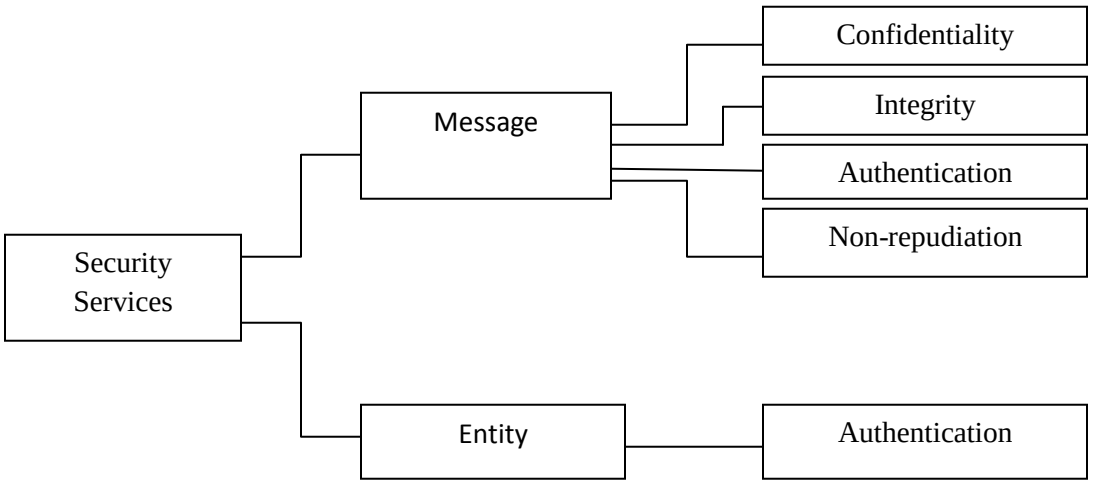

Figure 2. Security services related to message or entity

- **Message Confidentiality:** It is privacy in which sender and receiver expect confidentiality i.e. only the intended receiver must know about the message and message must not leak out of the network. For this purpose encryption is used in which secret key is used by the intended user.
- **Message Integrity:** In this, data is received by the receiver as it was transmitted i.e. the message must be genuine. The message must not be altered by the adversary.
- **Message Authentication:** In this the receiver must be confident about the sender's identity, that the message is transmitted by the authorized transmitter otherwise an intruder can effortlessly contact the network and can insert hazardous message.
- **Message Non-repudiation:** It means that the sender must not reject sending a message otherwise the load of confirmation cascade on receiver.
- **Entity Authentication:** In this the user or entity is confirmed proceeding to contact to the system assets.

3.2 PROTOCOLS FOR THE DETECTION OF CLONE-ATTACKS.

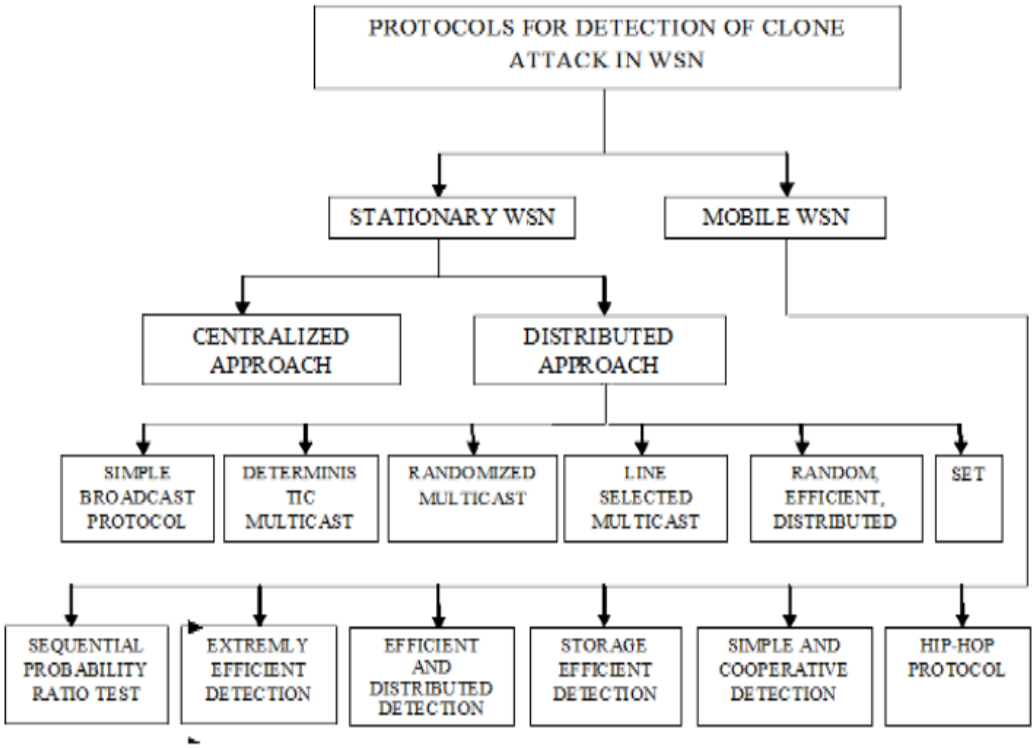

Figure 3: overview of clone detecting techniques

3.2.1 DETECTION APPROCHES FOR STATIONARY WSN

Clone attacks in wireless sensor networks will initiate many insiders attack like wormhole or black hole attack by changing the code of the compromised node and replicating it in various part of network. The detection of clone is based on the location claims and it is discussed below. There are two different approaches in detecting a clone in detection of clone in Stationary WSN. They are

1. Centralized approach
2. Distributed approach

1) Centralized approach:

In this approach [9][10], we have a base station (BS) or a remote sink and this initiates the protocol for detection of clone. All the sensor nodes of the network will report the BS about their location information. And the BS will compare the location claims it has received

For finding conflicts. If there exist, two nodes with different location claims then BS will broadcast the revoke message for the entire network. The drawbacks of this approach are

- If the BS is drained out of energy, then detection can't be preceded. This will make detection protocol to fail. This is referred as single point failure.
- If the adversary compromises the BS, then the clones will not be detected.
- The nodes closest to the BS will have a high routing load. Based on this, if the adversary targets these highly loaded nodes then the detection will fail.
- The BS waits for all sensors to report and then analyse them to find the conflicting claims. Then floods the network which increases the storage and computation overhead at BS.

2) Distributed Approach:

This approach doesn't depend on Base station. The detection of clone is distributed among the sensor nodes in network. The drawbacks of the previous approach are overcome by this distributed approach. There are different protocols that are discussed below under this category:- node-to-network broadcasting, deterministic multicast(dm),random multicast(rm), line selected multicast (lsm), SET protocol and real time detection.

A) Node-to network broadcasting

In this protocol [5], every node in network will broadcast a verified message to surge the network with its area claim. Expect that each node gets the broadcast. Each node stores the area assert in the nearby storage. If it receives a conflicting claim, revokes the offending node. Considering the effectiveness, sensor node needs to store the area claim of d neighbours. Every node needs to send its area claim to all n nodes in system. Thus the total communication cost is O (n2). Despite the fact that, the protocol is straightforward it will legitimate just in small network. If scalability increases, the communication cost will be too costly.

B) Deterministic Multicast (DM)

To reduce the communication overhead incurred in the previous detection strategy, we share the location claim only to a pre determined subset of nodes referred as witness nodes. When a node broadcast its claim to its neighbours it will forward it to witness node alone. If the adversary replicates a node [5], the witness will receive to conflicting location claims for same node ID. This conflicting claim acts as an evidence to trigger the revocation procedure. This method reduces the number of messages broadcasted than the previous technique. The Drawback is, the adversary can find out the witness node easily and compromise it. This will reduce the detection probability.

C) Random Multicast (RM)

This technique [5] defeats the cons in past system by selecting the witness randomly utilizing probability model. Every node signs and broadcast the area claim to its neighbours. This claim thus sent to the random chose witness node. The enemy doesn't know the witness node in earlier. Thus, detection probability is not influenced. Each neighbour sends the claim area to O ($\sqrt{n}$) randomly picked witness, then misusing birthday paradox, no less than one node will get the area claim to detect the Clones. This method increases the communication cost. Every node is sending the claim to O ($\sqrt{n}$) Destinations and this increase the aggregate correspondence expense to O (n). On the off chance that enemy finds the probability model for discovering witness node, then it will compromise those witnesses and clones remains undetected.

D) Line Selected Multicast (LSM)

Detecting the LSM convention [5] makes utilization of routing topology for the recognition of clones in network. Here, every node signs the area claim and advances it to the neighbours. On getting the claim, it is sent to the destination as witness. The sending nodes additionally save the claim area and checks for the same ID in its nearby storage. If the conflict present, then it is shown to the whole network. Thus, the forwarding node likewise goes about as the witness node. This expands the detection probability compared to the RM. It needs just O ($\sqrt{n}$) hop for each node. This will expand the computational overhead by getting signs and confirmed by every rely node

E) SET protocol

SET protocol [4] is proposed to detect clones in network. It has five components for detection Process and they are listed below. First step is to form an exclusive subset maximal independent set (ESMIS) which forms the exclusive subsets in distributed environment. Second, is to ensure security in the subsets construction with compromised nodes. Third, is to form multiple tree based subset computation for the detection of clone and number of trees constructed in network is represented as T. In this approach, each leaf node in tree will check and verify the conflicts. If conflicting location claim arises, it will be informed to the parent node and that node will in turn check, verify and inform to its parent node and this goes on till it reach the root node. But if a clone node is present nearby the root, it may allow the clone to go undetected .This drawback is handled by forming multiple roots on every exclusive subset. It reduces the computational overhead because it uses only basic computations like union and intersection. Total message sent in entire network is O (n).

F) Real time detection

Detecting the clone in real time [14] is done by forming fingerprints based on the neighbours Through superimposed s-disjunct code. It has two steps. First, generate fingerprint of length log2M where M I the number of neighbouring nodes to form fingerprint. Second, detect clones in network. Each node store it own and neighbours fingerprint. For each message sent, add the fingerprints and this can be verified by legitimate neighbours (w). Along, with this normal message transfer also happens and this is denoted as num. If a clone is deployed in other networks this can be identified by the fingerprint which will be different from the original node. In this protocol, it collects the preloaded codeword's from d neighbours and computes the social fingerprints. It also increases the memory overhead by sending the fingerprint along with regular messages.

G) SET protocol

SET protocol [4] is proposed to recognize clones in system. It has five segments for detection Methodology and they are listed below. Initially step is to frame a restrictive subset maximal autonomous set (ESMIS) which shapes the selective subsets in appropriated environment. Second, is to guarantee security in the subsets development with traded off nodes. Third, is to

shape various tree based subset calculation for the location of clone and number of trees developed in system is spoken to as T. In this approach, every leaf node in tree will check and confirm the conflict. On the off chance that clashing area case emerges, it will be educated to the guardian node that node will thus check, confirm and illuminate to its parent node and this goes ahead till it achieve the root node. However, in the event that a clone node is show adjacent the root, it may permit the clone to go undetected. This downside is taken care of by shaping different roots on every elite subset. It lessens the computational overhead on the grounds that it utilizes just fundamental reckonings like union and convergence. Aggregate message sent in whole system is O (n).

H) Real time detection

Recognizing the clone continuously is finished by framing fingerprints taking into account the neighbours through superimposed s-disjunct code. It has two stages. To start with, create finger impression of length log2M where M is the quantity of neighbouring hubs to frame unique mark. Second, identify clones in system. Every hub store its own and neighbours unique mark. For every message sent, include the fingerprints and this can be confirmed by authentic neighbours (w). Along, with this ordinary message exchange likewise happens and this is signified as num. In the event that a clone is conveyed in different systems this can be recognized by the finger impression which will be not the same as the Original hub. In this convention, it gathers the preloaded codeword's from d neighbours and figures the social fingerprints. It likewise builds the memory overhead by sending the unique finger impression alongside regular messages.

I) Hybrid detection

Hybrid detection is the merging of both centralized and distributed protocol. Large systems are partitioned into areas. Every part has a central node, where every node in segment needs to send ID and check it. Central node goes about as server to distinguish the clones. Server node asks for the node to send the ID to any node in its part. That node will give back its secretive data. Server node will cross check the answer by requesting that the neighbour nodes confirm its accuracy. In this discovery convention, division into segments expand the trouble in handling. This thus expands the computational overhead for recognition of node replication.

3.2.2 DETECTION OF CLONES IN MOBILE WSN

Detecting the clones in mobile wireless sensor network increase the trouble to a higher degree. All the Detection strategies examined above are not suitable for this environment. This is on account of; the fundamental idea for all the recognition procedures is in view of the geographic area of sensor nodes. But the nodes that are equipped with mobility, move anyplace in the network. Nodes have the possibility of being in too distinct areas inside the same protocol run. This will be taken as clone in all the stationary WSN. Along these lines, numerous analysts have proposed protocol for MWSN with different detection probability, energy consumption and memory usage. The proposed techniques are discussed and analysed in detail.

1) Sequential Probability Ratio Test (SPRT)

In SPRT [7], each time the sensor moves to the new area it signs the and sends it to its neighbours and to the Base station (BS). BS computes the speed based on the probability ratio test and compares it with the observed speed. In the event that the watched rate is beyond the computed maximum speed then the node is thought to be clone. In this method, every sensor by and large gets b claims. In this way, every node checks b signature. The probability claims that is sent to BS is p. The BS confirms b*p*N signature where N is aggregate number of sensor nodes. The most pessimistic scenario of this method is of False negatives and false positives. False negatives expresses that, if max speed is considered to me small then an ordinary node can be considered as clone. False positives is the other way around of the past one. The detection of clone is in view of base station and the maximum Speed conveyed. If the BS fails, detection of clone fails.(single point failure).

2) Extremely Efficient Detection Protocol (XED)

XED [7] is based on the concept of Remember and Challenge. It argues that, it doesn't need to be aware of location information. If two nodes meet each other for the first time they exchange a random number and store it in table. E(x) is the expected number of moves in network by a sensor. On the occasion of meeting for the second time or more, it request for the previous exchange number saved in table. If both have the same number then we decide as no clone otherwise clone is detected.

Two important factors in this technique are

1. Detection is possible only if the nodes have already met each other.
2. Probability that the genuine node is fooled.

3) Efficient and Distributed Detection (EDD)

EDD [7] suggests that it decides the threshold for number of meeting between the two nodes in a given time T with higher probability. Replica of node is detected if the node experience the other node with higher number than the threshold. This setting up of threshold could be possible in two ways. One is through logged off (Planning before deployment) or in online (In every single step). This builds the capacity overhead to higher degree. This network is suitable in sensors if and if a different memory module is embedded. Computational overhead is expanded in online mode, because of the former planning before deployment. This technique emerges to false positives if edge is situated to low.

3.3 CLONE ATTACKS

Mobile Wireless sensor network consist of sensor nodes that are movable in a network. Mobility is achieved in sensor nodes by equipping it with mobilize for changing their location or sensor is made to move via wheel, robots or vehicles. In several military and civil applications, WSNs are often unattended and deployed in harsh environments. Due to their operating nature, WSNs subject to several threats. For instance, an opponent can easily eaves drop (capture) all network communications, as well as physically capture nodes and misuse them. In this attack there are two type of node deploying node which are actually information nodes and others are replicating nodes which is replica of the deploying nodes. The replicating nodes or clones node has node id's and same information contain in the deploying nodes. Once the clones nodes are deploying in the network by opponent can use them in the harmful manner. for instance, clone node could create a black hole, initiate a wormhole attack. Opponent can inject false information or data can be aggregate in such a manner it may bias the data so that result should be wrong or simply data can be leaked. Moreover, detecting such attack is very challenging, since a clone cannot be easily detected.

In the base paper they described about to detect the presence of cloned nodes in a mobile WSN. In particular, we studied a distributed, efficient, cooperative protocol that has ability to change only one-hop communication and node mobility to enforce the emergent property of node replica

detection. Informally, each sensor records ID and location of met neighbours and compares its own records with the ones of met neighbours. Due to nodes movements, inconsistent location information related to two clones will spread in the network. In this way the clones can be detected only using single-hop communications and they propose two protocols: HIP (History Information-exchange Protocol) and HOP (History Information-exchange Optimized Protocol).

3.3.1 Hip-Hop Protocols.

Basic functioning of the node: There is basic network which consists of the nodes in which has four deployment nodes(a,b,c,d) and one clone node ie replica of node is present in network .At particular instant of time deployment node(a)met with clone node(c) at particular location and exchange information with each other and in the same manner deployment node(b)met with deployment node(c)which is original information source.

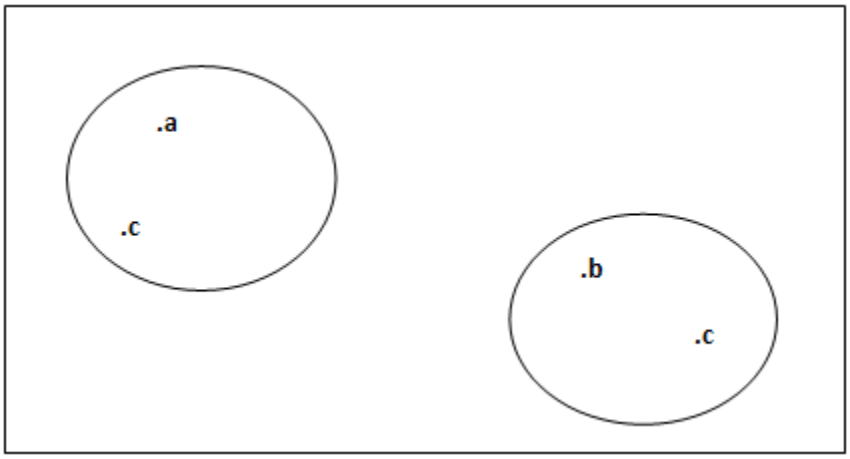

Figure 4.Basic functioning of node

HIP Protocol: After sometime these nodes change their location and met with other nodes but the clone node is not detected yet. By using HIP(history information exchange protocol)clone node will detected when node(a),node(b)met together and exchange the information regarding neighbour nodes with they earlier met.

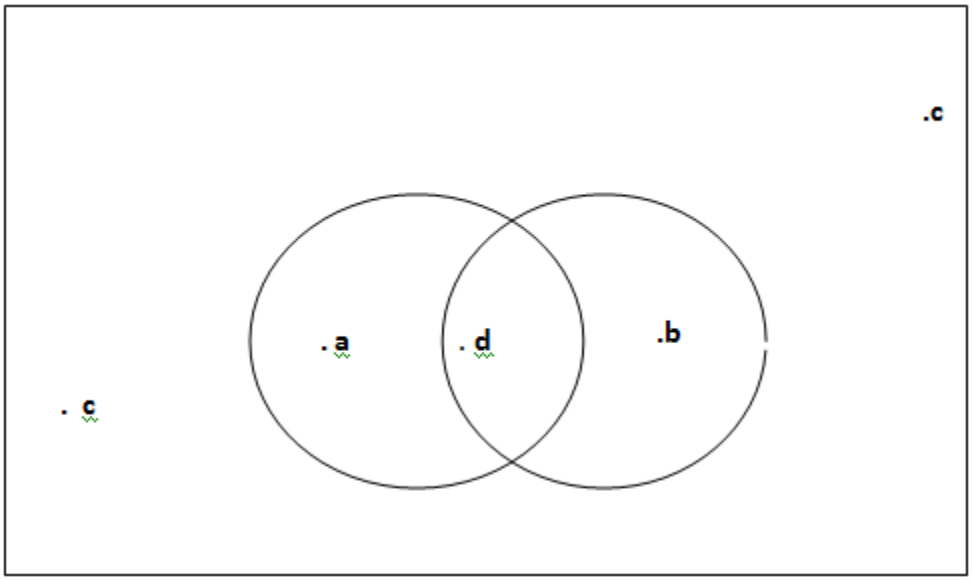

Figure 5: Explanation of clone detection using HIP

HOP PROTOCOL: In the hop protocol clone will detected by common node(d)when at the same instant of time node(a)and node(b) exchange the member list with node(d).Node(d) will campare the member list of node(a)and node(b).if there is some common node between node(a)andnode(b)itimpliesforclonenode.

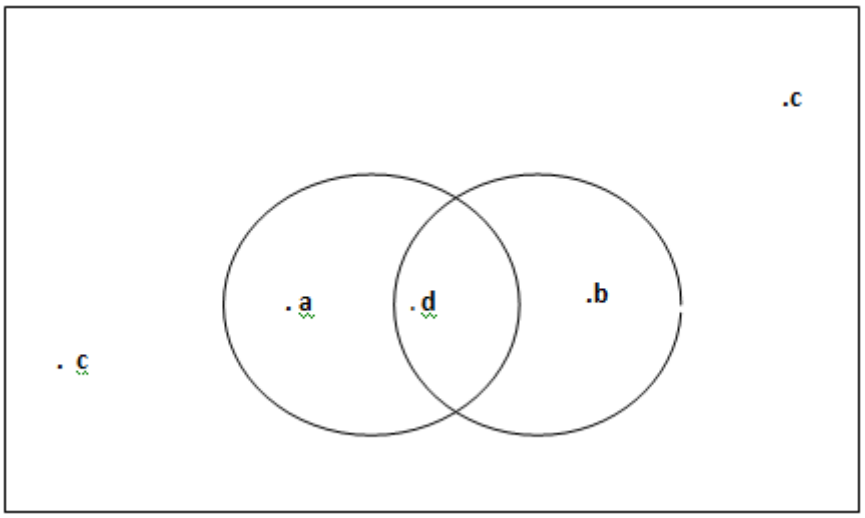

Figure 6: Explanation of clone detection using HOP Protocol

Chapter 4

PROBLEM FORMULATION AND RESEARCH METHODLOGY

4.1 PROBLEM FORMULATION

Wireless Sensor Network is a network of sensor nodes without having any central controller. Its growth is increasing day y day and that's why there is a wide field for research in this area. In the base paper, they described about the detection of the presence of cloned nodes in a mobile WSN and they have proposed two protocols using Hip-Hop protocols. But there are many loopholes in those protocols i.e. if the clone nodes are distributed in whole network. It cannot detected by either hip or hop protocol. For the detection of clone in the hop protocol it necessary to have common node for the detection of clone .So in the both case if the clone cannot detected at the initial stage. The opponent can do any with network (network jamming, steal secure information).

Our proposed algorithm, this protocol works in two parts and the main goal of our proposed protocol is to detect the replica of the nodes i.e. clones in the network on the basis of RLE method. RLE method is abbreviated as R represents RSSI (received signal strength indicator), L represents location of the nodes in the network and E is for energy of the nodes in the network. In the part 1, the nodes in the following network make clusters or groups and in the other part, detection of the replica nodes is being done by using RLE method. This protocol improves the limitations of the base paper and our simulations shows that proposed work outperforms the base protocols in terms of parameters like detection rate and time taken to detect the clone.

4.2 RESEACRH METHODLOGY: - Detection of clone in network using RLE method.

1) Deployment of the nodes
   Size of the network it may be of any size 100*100.
2) Division of network into nine equal clusters.
3) Deployment of base station in the centre of the network through which the detection of clone been done
4) Election of Cluster Head for each cluster.

Process: The node which is nearer to base station will be chosen as cluster head and also have unique id

5) If there are two clones within same cluster, then presence of the clone will be indicated by mismatch of RSSI value sent to cluster head

   Process:

   a) Each Node calculates RSSI value of its entire neighbour with their unique id's

   b) Each node will send two smallest RSSI value of its neighbour list to respective cluster head along with idea of neighbours and unique ID.

6) If there are two clones but in different clusters, then presence of the clone will be Indicated the base station from their id's and detection of clone node by comparing activation time.

7) If any clone node is cluster head then will be detected by the Base Station.

   Process:

   a) Cluster head exchange the member list with base station with its id and base station also have id's of the whole network

   b) Base station checks the cluster head id and whole network id if cluster id matches with node id clone will be detected.

CHAPTER 5
PROPOSED WORK

4.1 Detecting Node Masquerade Attach using RLE method.

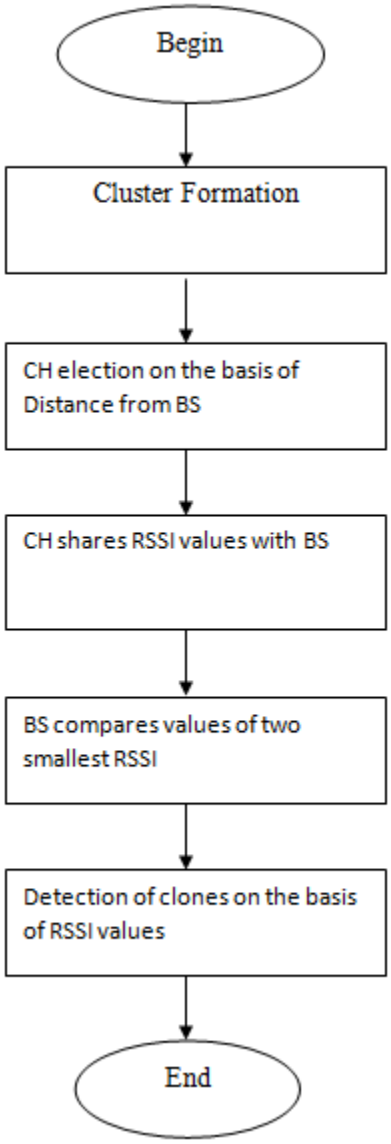

Figure 7.Flowchart of Proposed Work

The main goal of our proposed Detecting Node Masquerade Attack Using RLE Method which is used to detect the replica of the nodes i.e. clones in the network on the basis of RLE method. RLE method is abbreviated as R represents RSSI (received signal strength indicator), LE represents list exchange in the network. This protocol works in two parts. In the part 1, the nodes in the following network make clusters or groups and in the other part, detection of the replica nodes is being done by using RLE method.

Part 1: cluster formation and CH election

Whenever there is deployment of the nodes in the network, firstly the whole network is divided into the clusters and after that each cluster in the network will go for CH election process in which the nodes which are near to the Base station will became leader or CH (cluster head) that means CH election is based upon the distance because the less distanced node will stay for more lifespan in the network and after this part detection process started.

Part 2: Detection of Clones using RLE method

In this part, firstly CH gathered all the information from each node within their cluster and this information includes RSSI value and exchange the member list with their unique ID. Now, each CH within their respective cluster chooses the two nodes with their smallest RSSI values and unique ID and send these gathered information to the BS.The work of comparison of all these values is being done by BS as it have all the information of ID and smallest RSSI values of nodes from CH.Now,on the basis of comparison of unique ID of nodes,BS will find the Clone node because two nodes cannot have the same unique id and after this BS will compare the RSSI values of the same suspected nodes.

CHAPTER 6

EXPECTED RESULTS

The simulation is being done in Mat lab MATLAB is a programming language developed by Math Works. It started out as a matrix programming language where linear algebra programming was simple.

6.1 Deployment of Network. Mainly, in this figure, deployment of all the sensor nodes is done in 100 X 100. Here the number of sensor nodes is 500.

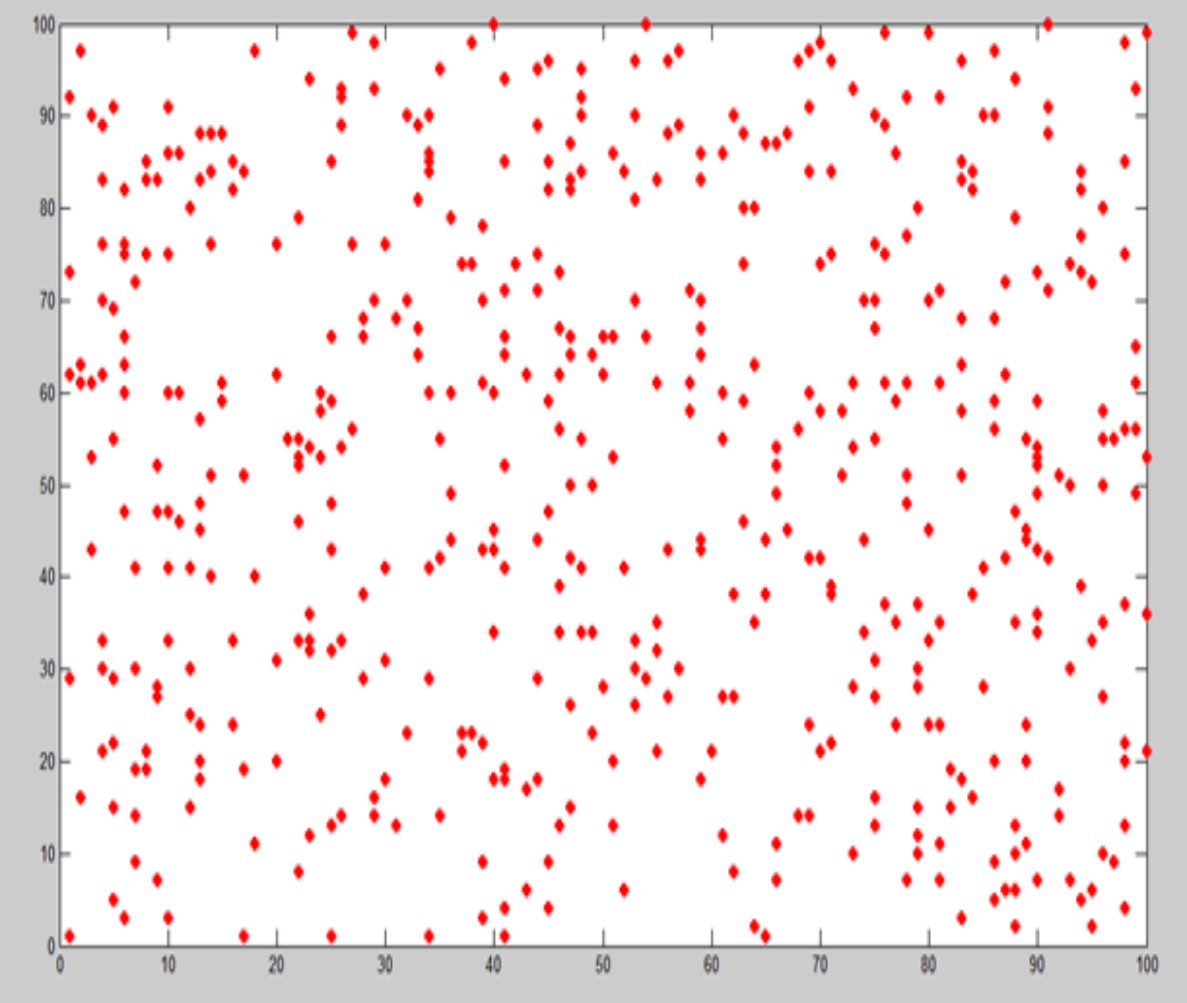

Figure 8.Deployment of network

6.2 Division of Network into clusters.

In this figure, the whole network are divided into nine clusters .

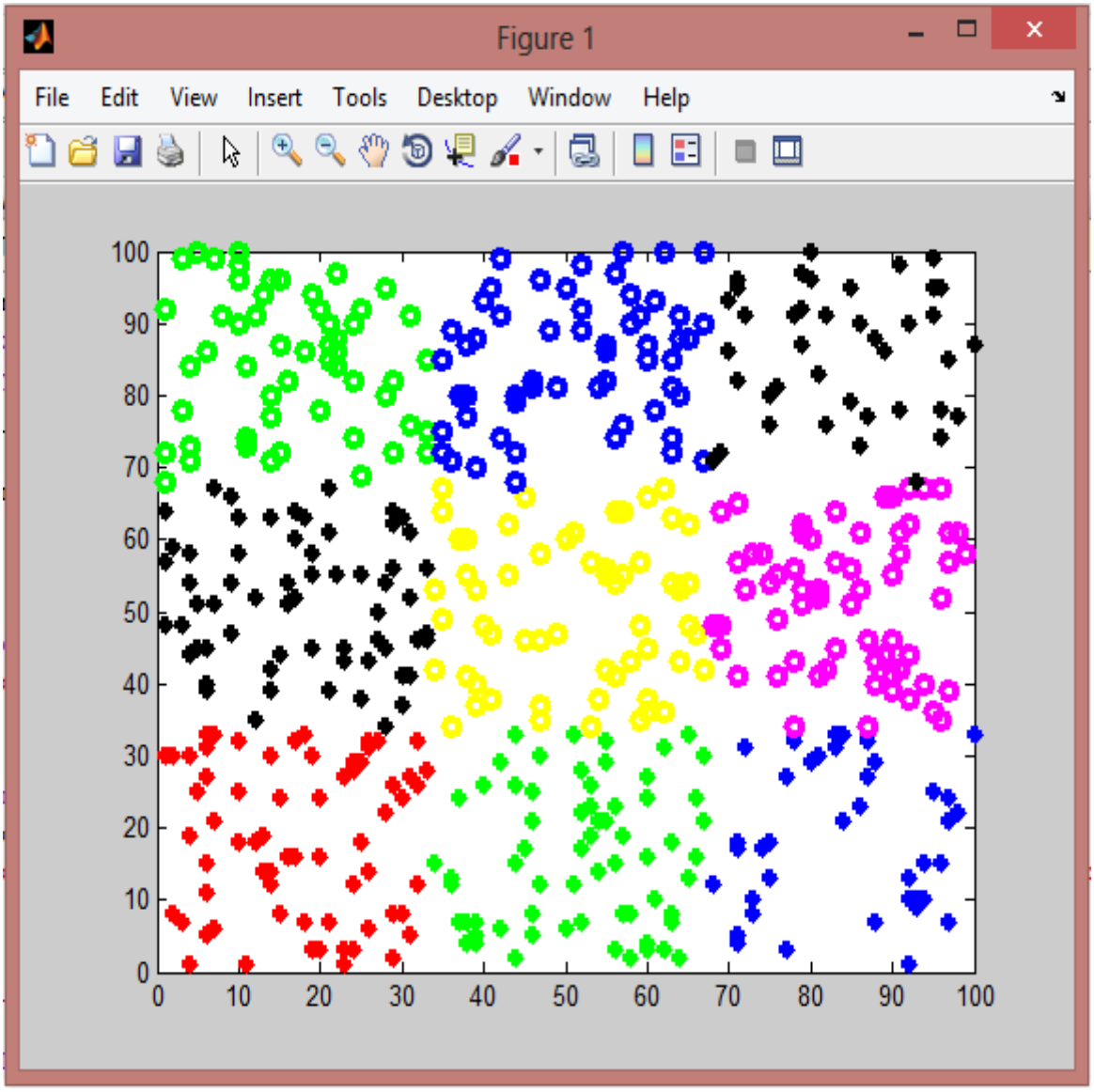

Figure 9. Division of Network into clusters

6.3 Deployment of BS in the centre of the network.

Here, the deployment of the base station occurs in the centre of the network. The BS deployment done at centre here because all the clusters get equal energy from that position.

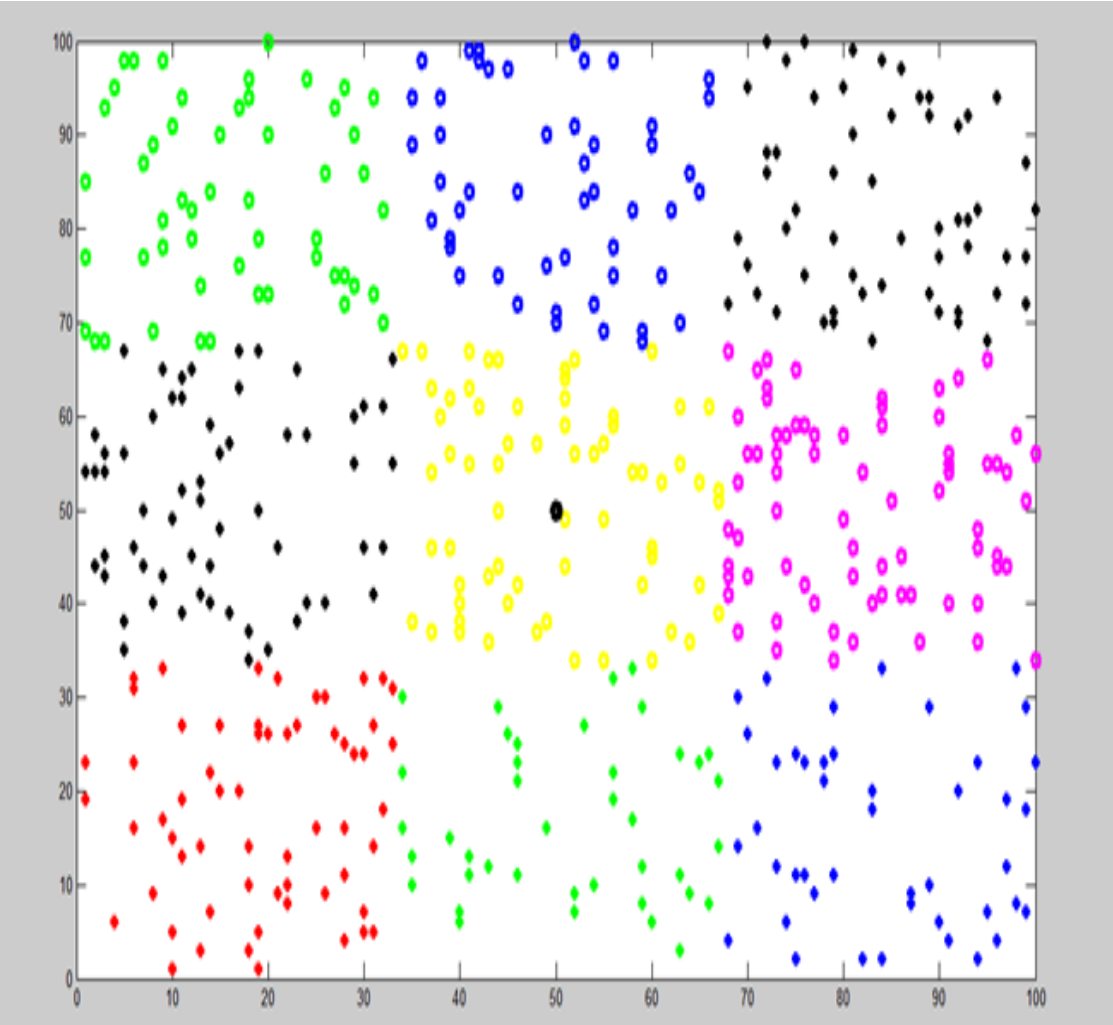

Figure 10.Deployment of BS in the centre of the network

6.4 Formation of clone in the Network

In this figure, the nodes are shown having same id in the network and here we have taken the 5 number of clone nodes in the network.

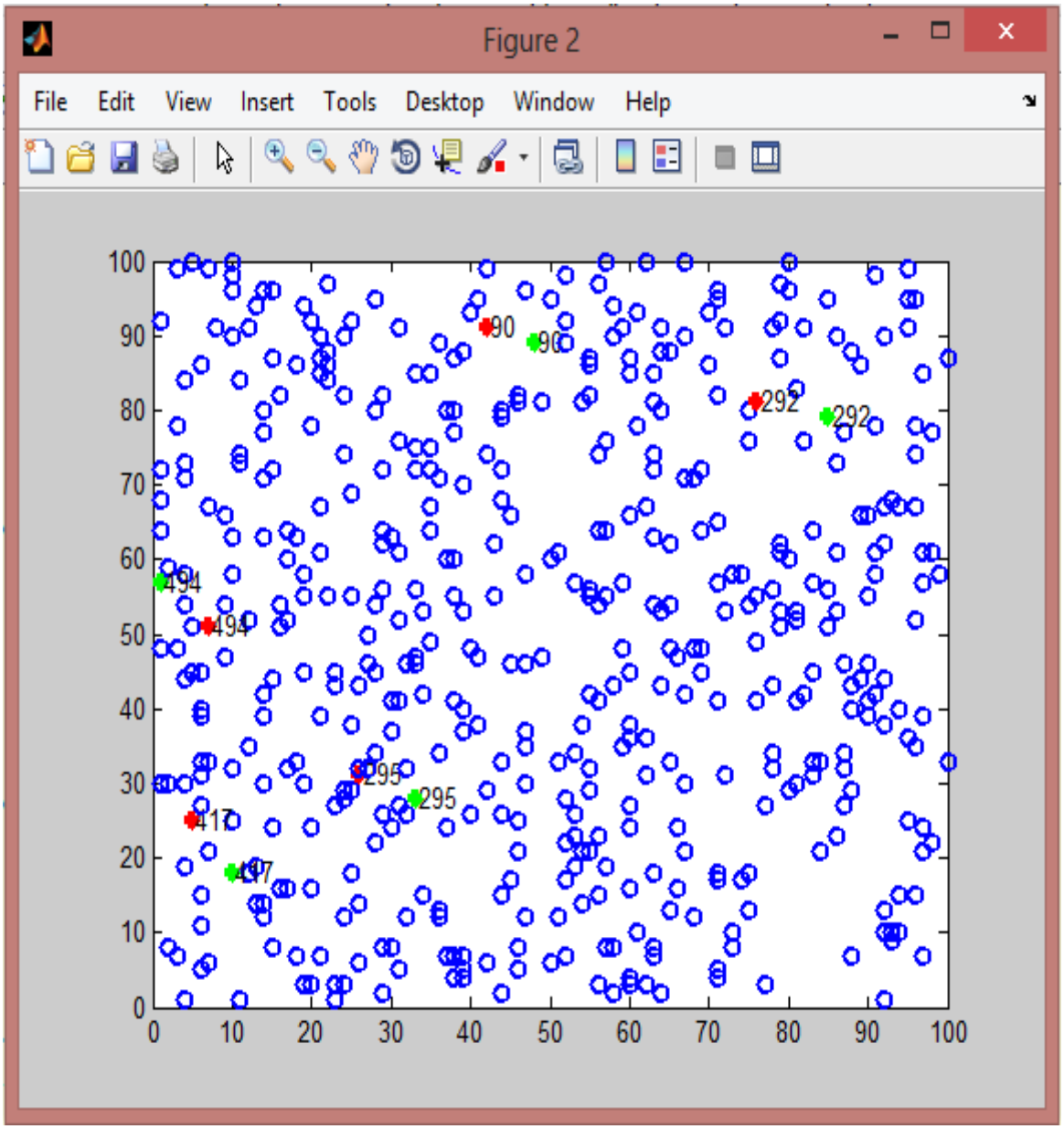

Figure 11Formation of clone in the network

6.5 Scenario of Information sharing of each node to CH

Each node in the cluster needs to inform all the other members in the cluster about its location.

This figure represents one such node. Same happens in the whole network.

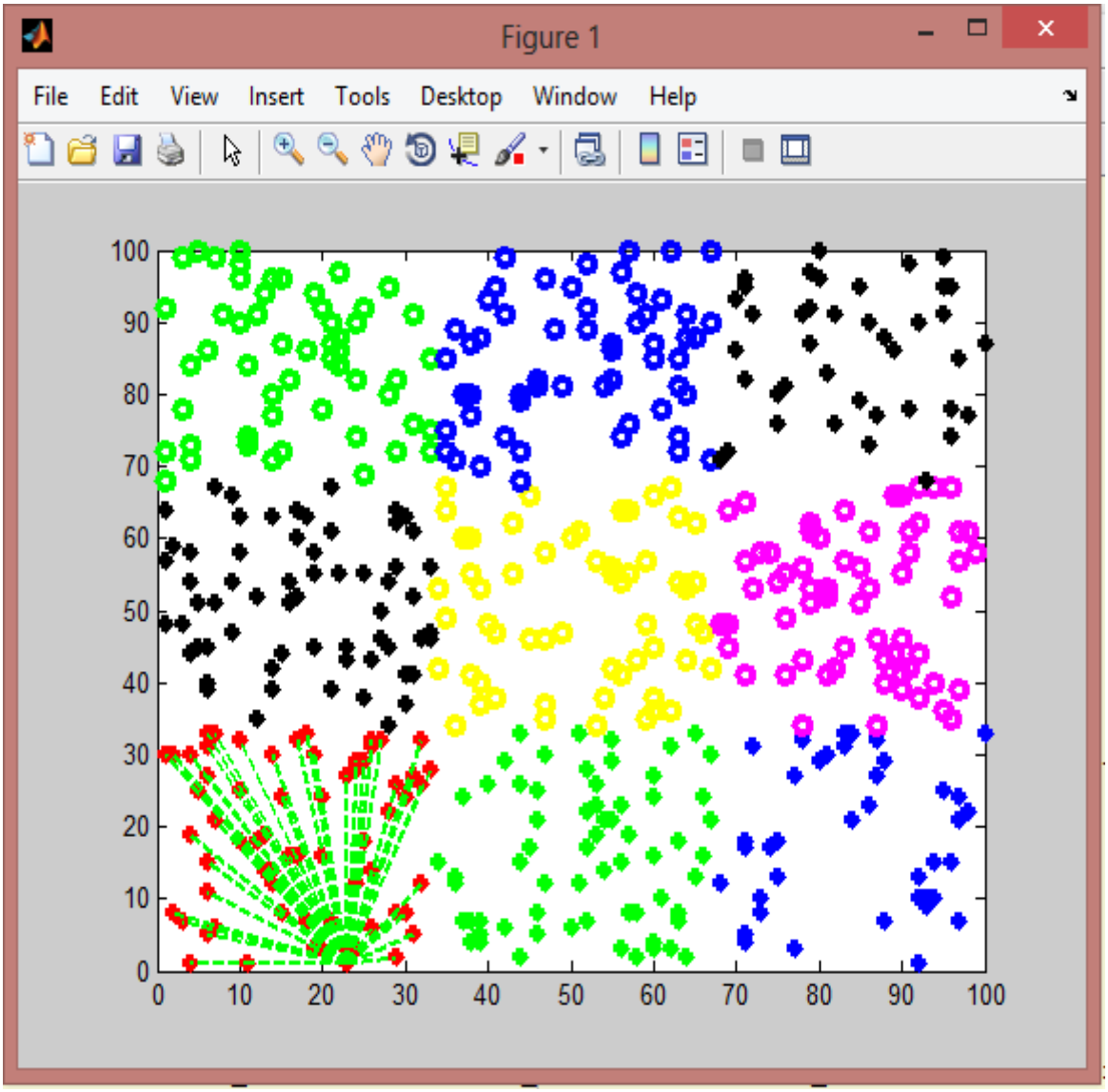

Figure 12.Scenario of Information sharing of each node to CH

6.6 Selection of the CH in the network.

In the previous step the nodes inform each member of the cluster about their location, so here the node which is closest to base station is selected as cluster head and these nodes represents the cluster heads.

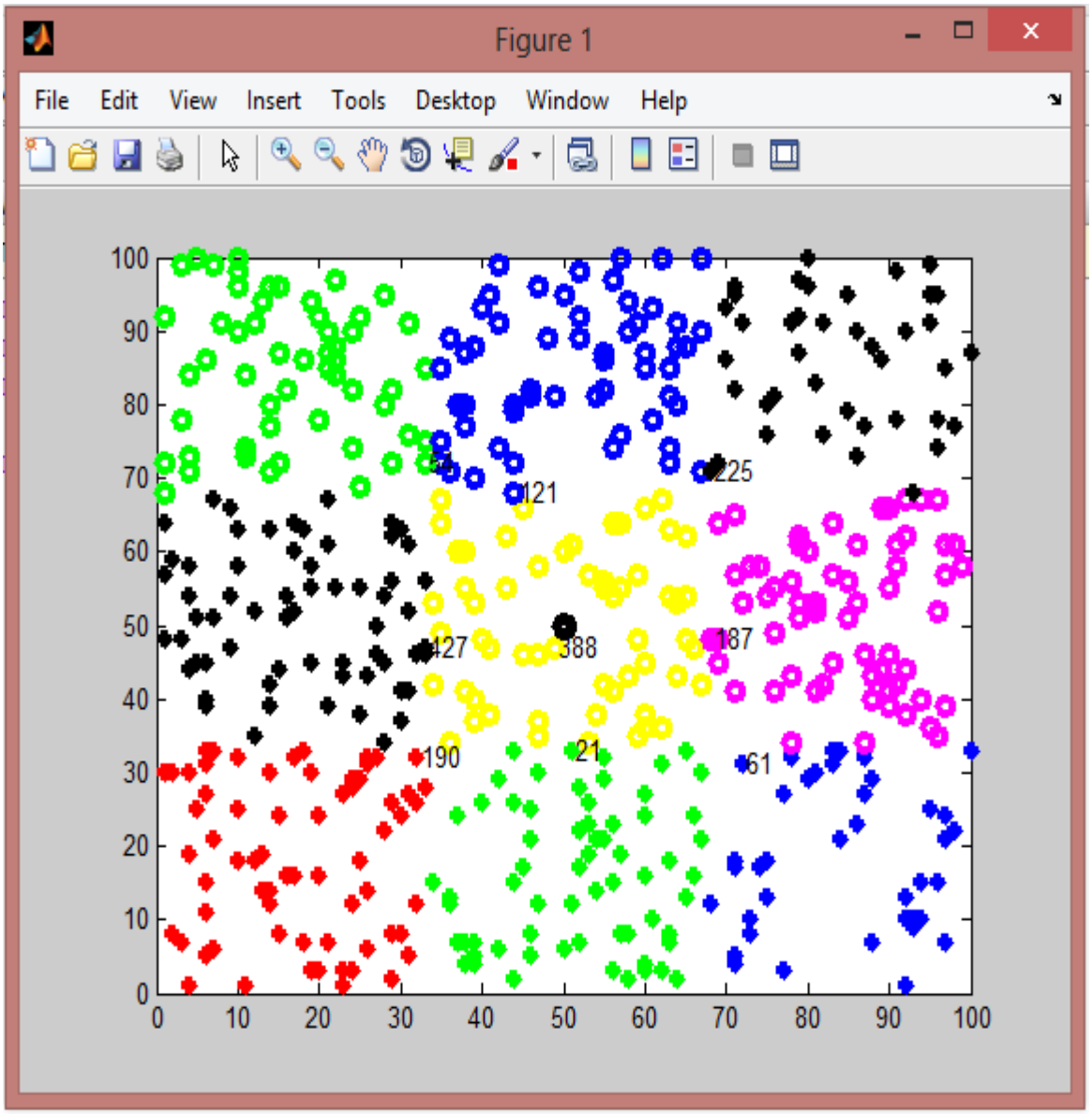

Figure 13.Selection of the CH in the network.

6.7 Scenario of Information sharing to CH

Here in the following figure, the nodes send their smallest neighbours' location and id is to the respective cluster head and also this represents such scenario in the first cluster, same happens in the every cluster.

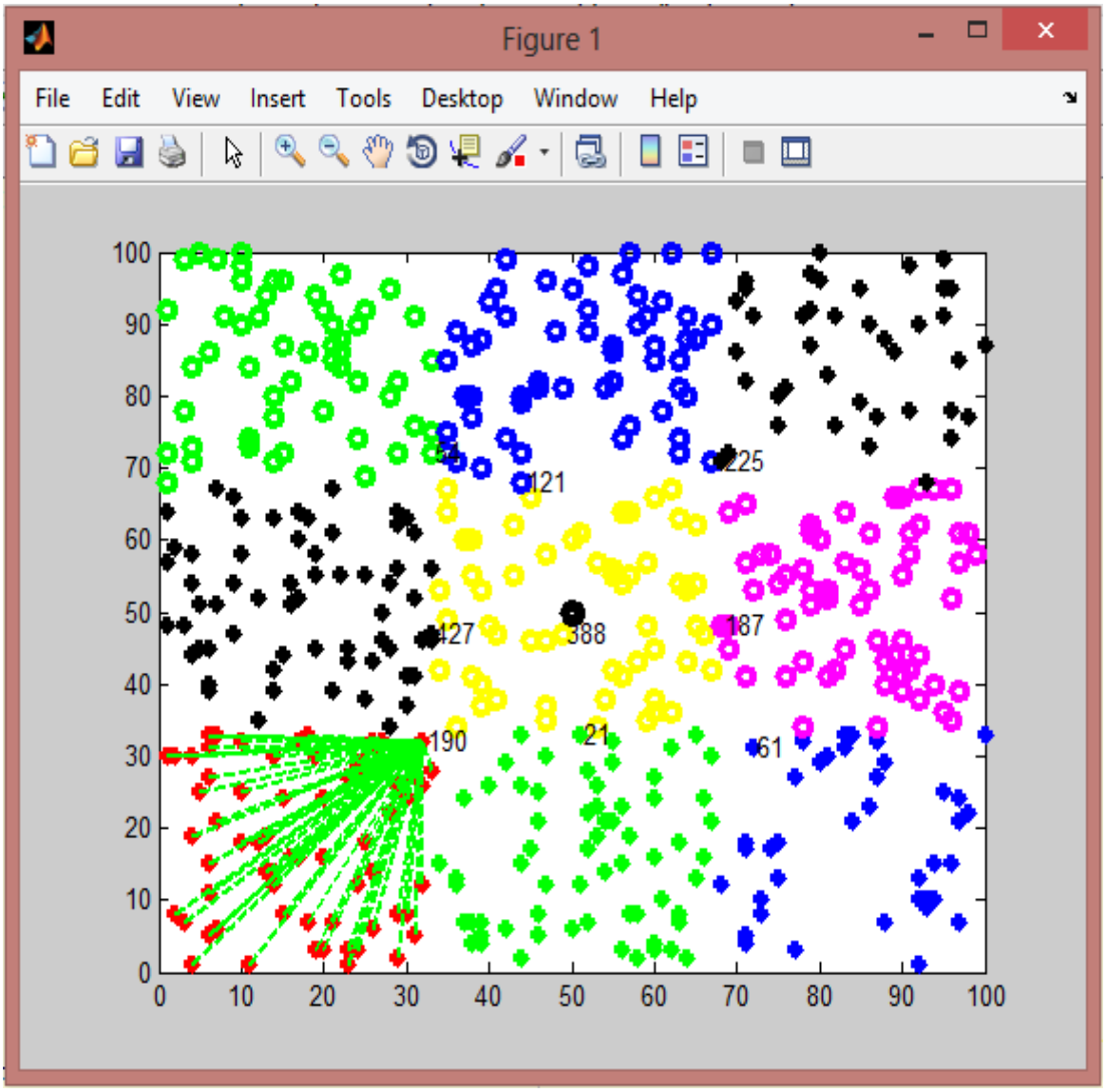

Figure 14. Scenario of Information sharing

6.8 Sharing of Information between CH to BS

In this Figure, the entire cluster heads forward their member list to the base station where the base station compares the lists.

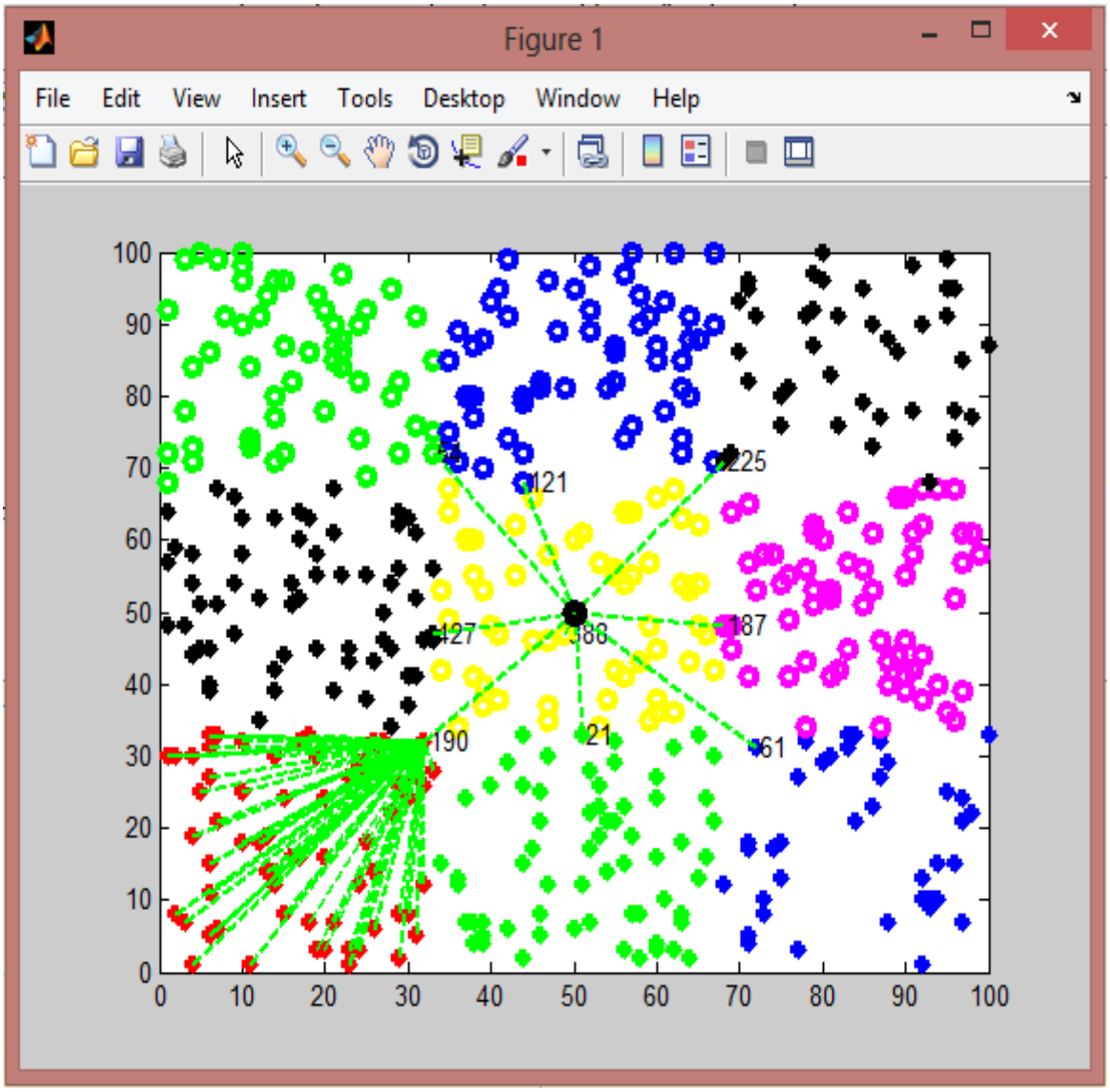

Figure 15. Sharing of Information between CH to BS

6.9 Detection of Clone in the network

Finally, the detection of the clones i.e. replica of the node is being done and here there are 4 clones at report in the network which is shown in green colour

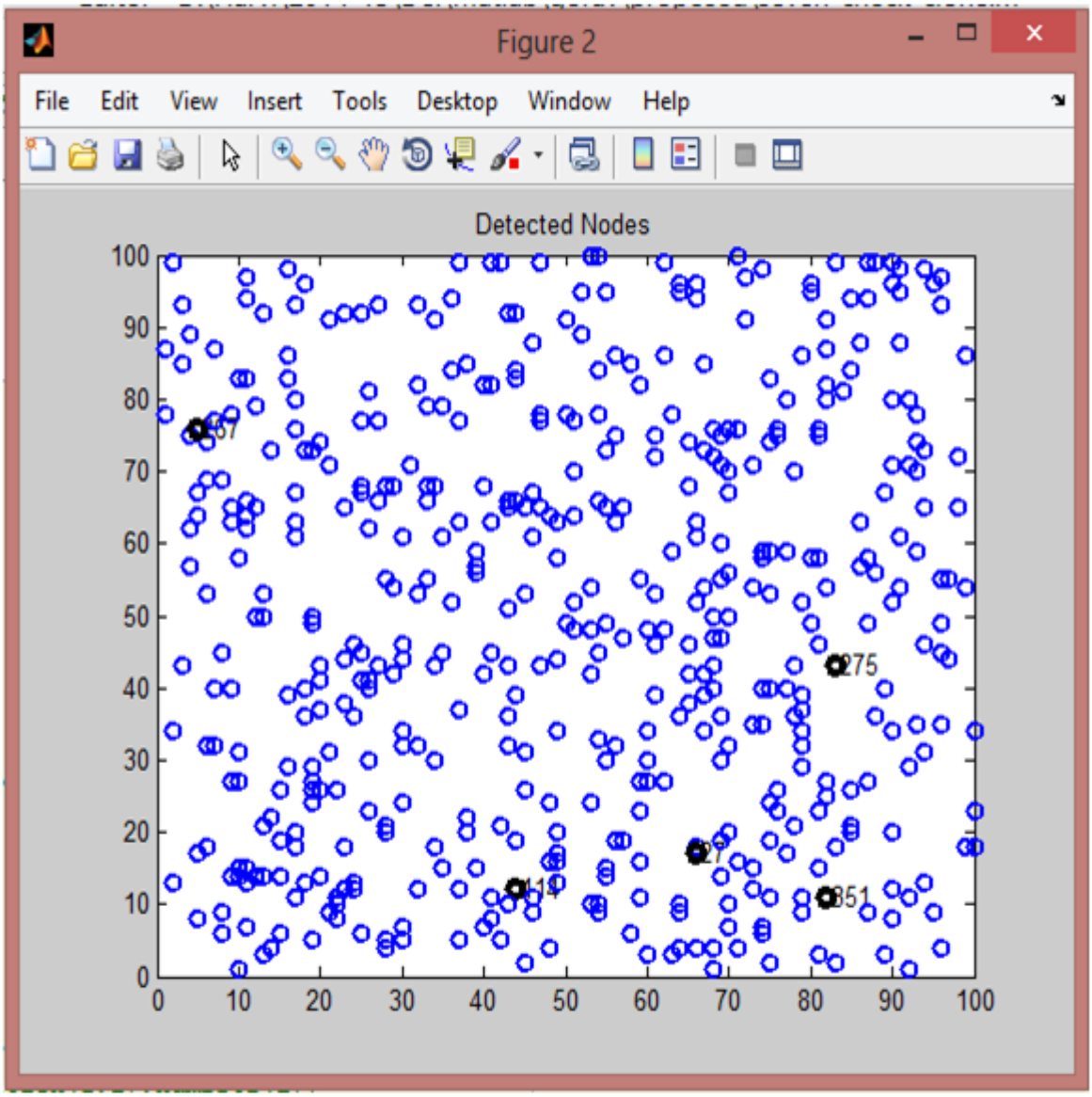

Figure 16. Detection of Clone in the network

6.10 Comparison of Detection Rate.

There are two parameters to check the performance of the network i.e. Detection rate and time.

Detection Rate : Here, the detection rate of hop protocol approx.0.6 and using RLE method it becomes equals to 1

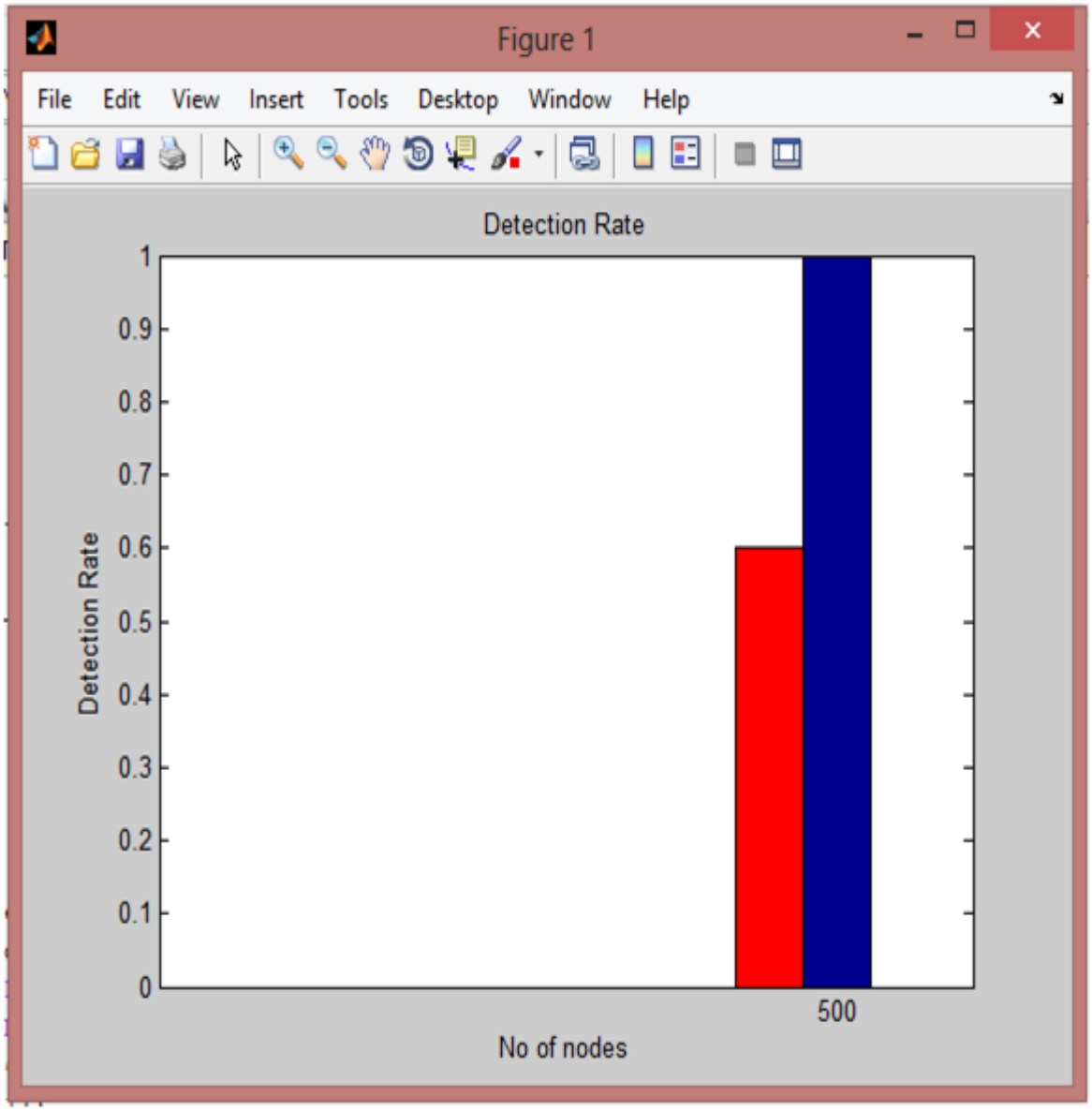

Figure 17. Detection Rate

6.11 Comparison of time to detect clone

Detection time: Here, the detection time of hop protocol approx.3.4 and using RLE method it becomes equals to 2

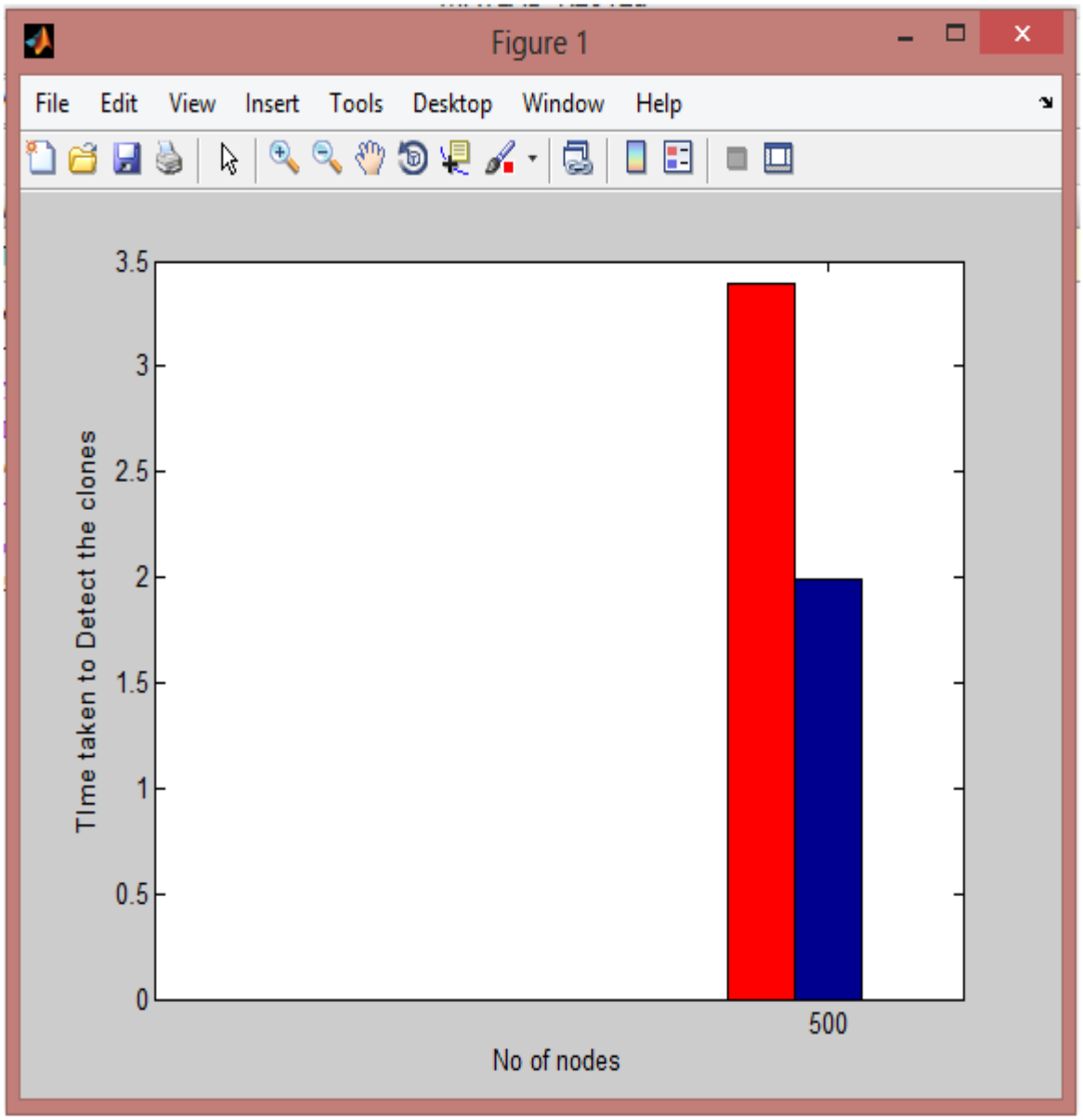

Figure 18. Time to detect clone

REFERENCES.

[1] Hoglar karl Andreas willing, “PROTOCOLS AND ARCHITECTURES FOR WIRELESS SENSOR NETWORKS”, Book, .pp 1-481.

[2]I.F.Akyildiz,W.Su,Y.Sankarasubramaniam,E.Cayirci,”Wirelesssensornetworks:a survey”,Int.J.Comput.Telecommun.Netw.38(4)(2002)

[3]L.Buttyán,D.Gessner,A.Hessler,P.Langendoerfer,”Application of wireless sensor networks in critical infrastructure protection: challenges and design options,WirelessCommun.17(2010)

[4]Al-Sakib Khan Pathan et.al, "Security in Wireless sensor networks: Issues and challenges," ICACT, pp. 1043-1048, 2006

[5]T Newe and E Lewis M Healy, "Efficiently securing data on wireless sensor networks," Journal of Physics: Conference Series, vol. 76, p. 012063, 2007

[6] Edwin Prem Kumar Gilbert, Baskaran Kaliaperumal, and Elijah Blessing Rajsingh , “Research Issues in Wireless Sensor Network Applications: A Survey” International Journal of Information and Electronics Engineering, Vol. 2, No. 5, September 2012

[7] J.Anthoniraj ,Trichy,T.Abdul Razak” Clone Attack Detection Protocols in Wireless Sensor Networks” International Journal of Computer Applications Volume 98– No.5, July 2014

[8] D Sheela , G. Mahadevan” Mollifying the Effect of Cloning, Sink Hole and Black Hole Attacks in Wireless Sensor Networks using Mobile Agents with Several Base Stations” International Journal of Computer Applications Volume 55– No.9, October 2012

[9]Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, “Wireless sensor network survey”, Elsevier,20008

[10]M.Contia,∗,R.DiPietrob,A.Spognardic,“Clonewars:Distributed detection of clone attacks in mobile WSNs”,elsvier,2013

[11]Bryan Parno, Adrian Perrig and Virgil Gligor, “Distributed Detection of Node Replication Attacks in Sensor Networks”,IEEE, 2005.

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

[13]Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei, M, “Distributed Detection of Clone Attacks in Wireless Sensor Networks”, IEEE Transactions on dependable amd secure computing, VOL. 8, NO. 5, SEPTEMBER/OCTOBER 2011

[14]Yih-Chun Hu,Adrian Perrig, David B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks",IEEE,2003

[15]Richard Brooks, P. Y. Govindaraju, Matthew Pirretti, N. Vijaykrishnan, and Mahmut T. Kandemir,"On the Detection of Clones in Sensor Networks Using Random Key Predistribution",IEEE Transcations on System, Vol. 37, no. 6, 2007

[16]Mohammad Hasan Ansari,Vahid Tabataba Vakili,"Performance analysis and classification of Clone attack detection procedures in mobile wireless sensor networks" IJCA Volume 71 - No. 21, June 2013

[17] Rajest yadav,Shirshu Varma and N.malaviya, "A survey of MAC protocols for wireless sensor networks,"volume 4,August 2009

[18] Vikash Kumar, Anshu Jain and P N Barwal, "Wireless Sensor Networks: Security Issues, Challenges and Solutions", International Journal of Information & Computation Technology. Volume 4, (2014)

[19] Chris Karlof ,David Wagner,"Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures" ,DARPA NEST,2010

[20] Sepide moradi,Mina zolfy lighvan, "MadCD: A Mobile Agent Based Distributed Clone Detection Method in Mobile WSNs",IJCNCS,Volume 2,2014