DETECTION & PREVENTION OF SINKHOLE ATTACK IN MANET

Dissertation submitted in fulfilment of the requirements for the Degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

By

JEEWAN JYOTI

Registration Number

41400024

Supervisor

KIRAN KUMAR KAKI

School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

Month June Year 2017

PAC FORM…….

ABSTRACT

MANET is a kind of Ad Hoc network with mobile, wireless nodes. Because of its special characteristics like changeable topology, hop-by-hop communications and easy and fast setup, MANET faced lots of challenges in routing, security and clustering. The security challenge comes due to MANET's self-configuration and self-maintenance capabilities. So in (MANETs), security is one of the most important concerns. This paper, we present an view of issues in MANET security.

Mobile Ad-hoc Network doesn't require pre-existing infrastructure, thus every node is active in data transmission and reception. In MANET various attacks are created by unauthorized transmitter in the network, which may effects on the performance of the network. "Sinkhole attack" is one of the important attacks in this type of network; this makes trustable nodes to malicious nodes that result in loss of secure information. in this paper we mainly focuses on sinkhole attacks on routing protocols such as DSR, AODV. To overcome the problems due to sinkhole we discuss about Security-aware routing (SAR) which helps to less the impact of such attack.

The main purpose of this research paper is to study about MANET (Mobile ad hoc Networks) and security attacks present in MANET. MANETs are very Powerless against different types of attacks that are present at different layers. Sinkhole attack is one of the important attacks in wireless ad hoc network. In sinkhole attack, a malicious node broadcast wrong routing information to produce itself as a specific node and receives whole network traffic itself. After receiving whole network traffic it change the secret information, such as changes made to data packet them to make the network complicated.

A malicious node tries to change the secure data or information from all neighbouring nodes. Sinkhole attacks affects the performance of ad hoc networks protocols such as AODV, DSR etc. by using flaws as maximizing the sequence number.

KEYWORDS:

Mobile Ad Hoc Network (MANET), protocol, Attacks on MANET, Sinkhole Attack, Security in MANET, Services.

DECLARATION STATEMENT

I hereby declare that the research work reported in the dissertation entitled "DETECTION & PREVENTION OF SINKHOLE ATTACK IN MANET" in partial fulfillment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor Mr. KIRAN KUMAR KAKI. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University's Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

Signature of Candidate

Jeewan Jyoti

41400024

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation entitled **"DETECTION & PREVENTION OF SINKHOLE ATTACK IN MANET"**, submitted by **Jeewan Jyoti** at **Lovely Professional University, Phagwara, India** is a bonafide record of his / her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Signature of Supervisor

KIRAN KUMAR KAKI

Date:

Counter Signed by:

1) **Concerned HOD:**
   HoD's Signature: _____

   HoD Name: _____

   Date: _____
2) **Neutral Examiners:**

   External Examiner

   Signature: _____

   Name: _____

   Affiliation: _____

   Date: _____

   Internal Examiner

   Signature: _____

   Name: _____

   Date: _____

ACKNOWLEDGEMENT

First and foremost, I would like to thank my dissertation advisor Mr. Kiran Kumar Kaki. Your passion for your work encouraged me to pursue my own goals, while your attention to details instilled in me a unique perspective on which to approach problems. I am deeply grateful for your taking me on as a student. Our academic work together has been a truly rewarding and enriching experience, while the lessons learned will help guide me throughout the course of my life in whatever avenue I pursue. I would also like to thank the Head of Deptt. Mr. Dalwinder Singh supporting my degree goals and the valuable time spent in the classroom.

Lastly I would like to thank my parents, you have provided everything that a Daughter could every ask for, and so much more.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Introduction to MANET

In MANET nodes within each other's wireless transmission range can impart easily; nonetheless, nodes out of each other's range need to depend on some different nodes to send messages. Therefore, a multi-hop situation takes place, where intermediate hosts move the packets sent by the source host to make them achieve the goal node. MANET is of the kind that meets up all requirements, without any support from the current foundation or some other kind of stations. This announcement can be formalized by characterizing adhoc network as an independent arrangement of mobile hosts (MHs) associated by wireless connections, the collaboration of which structures a correspondence network demonstrated as a discretionary communication graph. This is opposite to the outstanding single hop cell network demonstrate that the requirements of wireless correspondence by introducing base stations (BSs) as access points. In these cell networks, correspondences between two mobile nodes totally depend on the wired backbone and the fixed (BSs). In a MANET, no such foundation exists and the network topology may dynamically change in a flighty way since nodes are allowed to move. Concerning the method of operation, adhoc networks are essentially distributed multi-hop mobile wireless networks where data packets are transmitted in a "store-and-forward" way from a source to a arbitrary goal, through moderate nodes. As the MHs move, the subsequent change in network topology must be made known to alternate nodes so that obsolete topology data can be either refreshed or removed. The dynamic way of MANETs makes network open to attacks. Routing is dependably the most critical part for any networks. Every node ought work for itself, as well as be agreeable with different nodes [31]. MANETs are defenseless against different security attacks. Henceforth, finding a protected and dependable end-to-end way in MANETs is a real challenge.

1.2 APPLICATIONS OF MANET

The organization of a MANETs is simple because of the absence of setting up any network for correspondence. For the most part such sorts of networks are required in military application and emergency save operations. Be that as it may, gradually MANETs have entered with the regions of gaming, sensing, conferencing, collective and distributive registering. The dynamic has not yet

attained the greater part of the business applications. Research is going on so that MANET can be conveyed in any region with avery fast speed and with less cost and can be set up within seconds.

Figure 2.1 MANET network

1. **Military services:** In this environment communication is provided by MANET in very less time. Soldiers are taken as the mobile nodes here. So the network is supposed to remain connected even though when the soldiers move freely here and there. This support is given by the MANET. Another application in this area can be the coordination or union of the military objects/persons and the personnel in the battlefield. For example, the leader of a group of soldiers may want to pass a message to all the soldiers or a group of soldiers involved in the operation.
2. **Emergency Services:** These arise whenever there is natural disaster and when whole communication system has failed for e.g. tsunami, hurricanes where restoration of communication is very much required. By using ad hoc networks, the system could be set up in hours but not in of days/weeks which is required for wire-line communications.
3. **Education:** Universities and college require communication setting for visual classroom during meetings or lectures.
4. **Sensing and Gaming:** Sensor network is a particular case of ad hoc networks in which no mobility is considered. However the battery power has an important factor. Each sensor is made with a transceiver, a small microcontroller and an energy source. The sensors send information from other devices to transfer data to a central monitor. The sensor environmental condition such as temperature and humidity are sensed by the sensor.

5. **Personal Area Networking:** the network is created for personal communication devices like laptop, PDA, mobile to share data among one other. This is called as PAN (Personal Area Network). It covers very short range of communication.

1.3 Characteristics of MANET

- **Wireless medium:** The wireless medium used by the nodes to communicate with each other has time-varying coverage and asymmetric propagation properties. It is less reliable and more prone to interference compared to a wired medium.
- **Dynamic Topologies:** Nodes are independent to move with different speeds; thus, the network topology can change randomly and at any time.
- **Infrastructure less Network:** Network is not depending on any fix infrastructure for its operation.
- **Power Management:** As the nodes are not fixed, they rely on batteries as their power source. Thus mechanisms and protocols devised for such networks need to keep the energy constraint in mind.
- **Peer-to-Peernature:** These are not fixed nodes with pre-defined roles. All protocols have to be planned for dispersed environments composed of "peers" and have to be strong enough to hold these distributed dynamic topologies. These different characteristics of wireless ad hoc networks require different techniques than the wired networks, especially at the three lower-most layers, to effectively perform the network functions. The widely adopted standard for wireless networks, at the physical and data-link layer is IEEE 802.11(for wireless local area networks).
- **Limited computing and energy resources**: They have limited battery capacity as well as limitation on device size, weight and cost.

1.4 Routing in MANETs

Routing is the act of moving or transferring information from one source to other source or destination in a network. Various metrics decide the efficiency of the route in terms of number of hops, traffic, security etc**.** The main purpose of routing protocols is to lessen delay, increasing the efficiency of the network, increasing network lifetime and improving its energy efficiency. Finding optimal routing. MANET routing protocols are categorized into three main categories Table driven/ Proactive

- Demand driven / Reactive

- Hybrid

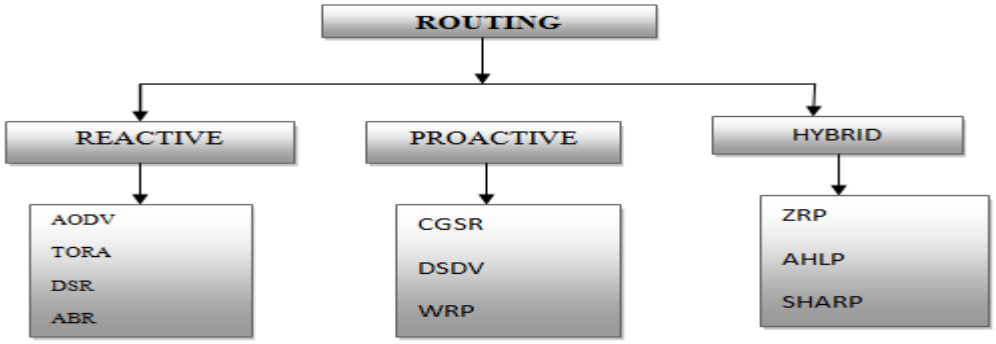


Figure 1.2 Hierarchy of routing protocol

1.4.1 Proactive Protocols

Proactive routing protocols propagate network, updates routes at fixed time intervals and tried to control dependable, progressive routing information within every pair of nodes in the network. These protocols are at times cancelled to as protocols driven by tables because the information of routing is supported in tables. The proactive routing techniques proposed for ad hoc networks are indirect from the usual routing protocols. The proactive techniques acquire a very important feature that every node maintains a route to every other node in the network constantly. The benefit of proactive techniques is that routes are available the instant they are requested. To start packet broadcasting and to transmit data packets to some destination or location, a source has to make sure the routing table because every node again and again maintains an updated route to every other node in the network. However, the key failure of these protocols is that the manage overhead can be dangerous in many networks or in networks with quickly moving nodes. It includes various protocols such as Destination-Sequenced Distance-Vector (DSDV) protocol, Wireless Routing Protocol (WRP), Optimized Link State Routing Protocol (OLSR) and Fisheye State Routing (FSR).

1.4.2 Reactive Protocols

Reactive routing techniques additionally referred to a son-demand routing, take a very unique way to deal with routing than proactive protocols. The need of constant upkeep of route for each node to each other node represents an overhead of the proactive protocols. In a wired network, where connectivity designs change moderately less frequently and assets are plenteous, keeping up full connectivity diagrams is a beneficial cost. The moment accessibility of route is the greatest advantage. In network of an ad hoc, notwithstanding, interface connectivity can change every now

and then and control of overhead is costly. The routing approaches have took a take off from conventional Internet routing approaches as here, the routes are found only when they are really require as opposed to keeping up a constant route between all sets of network nodes. At whatever point a source node needs to send information packets to some destination, it checks its route table to make sense of whether it has a route [25]. On the off chance that no route exists, a route discovery system is performed to discover a way to the destination. Consequently, route discovery moves toward becoming on-demand. The route discovery system commonly involves the all inclusive flooding of a demand message. To lessen overhead, the inquiry region might be diminished by different advancements.

The advantage of this approach is that declining overhead is at risk to be lessened contrasted with the proactive methodologies, mainly in networks with low to direct activity loads. At the point when the quantity of information sessions in the network turns out to be high, then the route disclosures approaches which is made by overhead, and may even outperform, that of the proactive methodologies [29]. The downside of reactive methodologies is that when source node needed a route, there is some limited latency in finding the route.as compare , with a proactive approach, routes are commonly accessible within minute they are required.

1.4.3 Hybrid Routing Protocols

Hybrid protocols represents of combination of the proactive and reactive methodologies. The network is partitioned in zones, and unmistakable protocols are utilized as a part of two particular. Zone Routing Protocol (ZRP) is the case of Hybrid Routing Protocol which utilizes proactive system for route foundation inside neighborhood nodes, and reactive protocols for communication. These nearby neighborhoods are called as zones. Every zone have different size and nodes can be cover in many zones. The extent of zone is measured by radius of length P, where P is number of hops to the border of the zone [26].

1.5 Security Issues in MANETs

Security is more challengeful to maintain in MANETs due to their vulnerability as compare to the wired networks. The use of wireless links makes attacks ranging from passive eavesdropping to further active impersonation, message replay and distortion [27].

Dynamic network topology: Mobile nodes continuously link and depart the network randomly, coming about to change the network topology vigorously. This allows a malicious or harmful node to link the network without earlier detection or checking. [29].

Lack of centralized monitoring: The centralized infrastructure is not present which disallows any monitoring mechanism in the network. This makes certification authorities of security solutions and on-line servers faithful and dependable to traditional security solution. The trust relationships changes particularly among the nodes when some nodes are to be compromised. Hence, security mechanisms must be dynamic and not static.

Cooperative algorithms: These routing algorithms require trust between adjacent nodes.

The limited physical protection of each of the nodes: Network nodes most of the times do not exist in in actually protected places, such as protected rooms. Hence, they are very easily vulnerable and fall under the power of an attacker.

The vulnerability of the links: messages can be eavesdropped or heard and fake messages can be injected / inserted into the network without any obstacle of having physical access to the network components. Eavesdropping may give allowance to an attacker access to secret information and violate confidentiality.

Adversary inside the Network: The nodes of mobile within the MANET can freely join and leave the networks per need. The nodes can also behave maliciously or harmfully. Detection of nodes such that the behavior of the node is malicious is difficult. So in this way the external attack is less powerful than this attack. These nodes are called compromised nodes.

1.6 Overview of AODV

AODV (Ad hoc On-demand Distance Vector) is a reactive routing protocol, in spite of on a very basic level. It starts discovery of route only when there is any need to find node. AODV can handle low, direct, and moderately high versatile rates, together with an assortment of information movement loadings.in all the cases, it makes no facility for security [28]. In Route Discovery Process of AODV there are some of messages: Route Request (RREQ), Route Reply (RREP),and Route Error (RERR) messages.

RREQ-at whatever point a node asserts a route the task, it transmits the route ask for message. A time to live (TTL) value is given by each route ask which expresses the quantity of hops it must be forwarded for. This esteem is introduced first at a predefined value at first transmission and a short time later it continues augmenting at retransmissions. Retransmission occurs when the answer is not available. Each node should keep up two counters: node sequence number and broadcast id [30].

RREP-a route answer message is transmitted to the originator of the RREQ, if the recipient is one of the node utilizing the asked for address or is having a substantial route to the asked for address.

RRER-nodes continue to monitor the connection status of the following hop in the dynamic routes. At whatever point a connection is braked, it is identified in the dynamic route, a RERR message is transmitted to alternate nodes to convey about the loss of the connection.

Advantages:

- Route on demand foundation with little postponement
- Link breakages in dynamic routes can be productively handled
- Destination arrangement numbers are utilized to locate the latest route to the destination.
- Connection set up postponement is not high.

Disadvantages:

- Inconsistency routes can be reached by intermediate routes if the source arrangement number is old. Multiple RERR packets in response to single RREQ packet may lead to overwhelming overhead of control.
- Bandwidth consumption happens with periodic beaconing.

1.7 Overview of DSR protocol

DSR is a reactive routing protocol. It confirms the most ideal route only on one condition when packet should be forwarded. The procedure to discover a way is recently run when a way is required by a node, which leads to On-Demand Routing. The DSR protocol is made out of two fundamental components that coordinate to allow discovery and support of source routes in MANET.

Route Discovery: When a source node S needs to send packet to the destination node D, it acquires a route to D. This is called Route Discovery. Route Discovery is utilized only when Source needs to send a packet to Destination and got no information of the route which it has to adopt.

Route Maintenance: The current routes are no longer usable when there is an adjustment in the network topology. In such a situation, the source S can utilize an option route to the destination D, or conjure Route Discovery. This is called Route Maintenance.

1.8 Classification of Attacks

Developing a good security solution is to understand possible form of attacks. Security of communication in MANET is critical for secure sending of information. When any central co-ordination mechanism is absent and the presence of shared wireless medium, MANET becomes more vulnerable or acceptable to digital/cyber-attacks than wired network. The attacks can be internal or external, and according to the behavior of the attack it can be Passive or Active attack.

1.8.1 **Internal/ External Attack**

External attackers are mainly outside the networks who tries to get access to the network and once they get access to the network they start sending false packets, denial of service in order to disrupt the whole network performance. The nature of the attack is very similar to the wired network attacks. These attacks can be started by executing efforts to establish security such as firewall, which mitigates the access of unauthorized person to the network.

External black hole attack can be summarized in following points:

1. Harmful node first identified the active route then notes the destination address.
2. Harmful node sends a route reply packet (RREP) which contains the destination address field spoofed to an unidentified destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
3. New route for selecting data by source code. The malicious node now drop the entire data which belongs to its route.

As the name suggest, internal attack is present in the network internally. Here, the attacker needs to have ordinary permission to the network as well as participate in the typical exercises of the network. The attacker picks up access in the network as a new node by any method i.e. by trading off a current node in the network or by harmful impersonation and starts its harmful behaviour. In internal attack, node itself belongs to the network internally. Internal attack is more dangerous because here harmful node is present inside the network actively all the time.

1.8.2 Active/ Passive Attack

In active attack, performance is made upset of the network ; important information is taken and the information is removed during the exchange in the network. Active attacks can be any an internal or an external attack. The active attacks are basically to destroy the performance or presentation of network and in these situations the active attack act as internal node in the network. This attack accumulates strong position to the attacker, where attacker can change, fabricate and replays the massages.

Unlike active attacks, in passive attacks, the normal or basic operations of the network are not disrupted. In Passive attack, the attacker listens to network in order to achieve information about the current transmissions. In order to know and understand how the nodes are communicating with each other it listens to the network, how they are located in the network. Prior to the attacker start an attack against the network, the attacker has lots of information information regarding the network that it can without difficulty hijack and infuse attack in the network.

1.9 Attacks possible on various layers

- **Physical layer:**
  - **Jamming :** Jamming is a mainstream Denial of Service (DoS) attack. The attacker in this attack tries to stop the frequencies or efficiency of the radio utilized for correspondence between the nodes in the system... This may make an attacker more powerful to trade off nodes of sensor all together to view the cryptographic keying material, recreate the node and find a few of his own nodes in the system or basically simply crush the sensor nodes in a DoS like way.
  - **Sybil attack:** The Sybil attack is an especially dreadful attack. This attack can traverse a few layers in the convention stack. The pith of the Sybil attack is that one single traded off node can imitate a few nodes. A node is embedded into the system and accepts characters of nodes from various units of the system. The attack base is at the physical layer [23].
- **Data Link Layer:**
  - **Collision:** This is a DoS attack, where affect is in little part only of a transmitted bundle. The packets will then come up short the checksum check, due to the progressions formed on by the crash, and the recipient node will then request a re transmission of the packet Weariness .the attack is taken somewhat further. A noxious node may lead a crash attack over and over focusing on goal to deplete the force supply of the imparting nodes.
  - **Exhaustion:** When the physical layer utilizes Request To Send (RTS)/Clear To Send (CTS) messages in request to have medium access control, a noxious node can over and over send messages of RSS to an objective node and disregard the CTS messages. Thusly, the pernicious node can surge the system connection of the objective node.
  - **Sybil attack:** The Sybil attack turns out to be more conspicuous in the information join layer. Two sorts of the attack of Sybil on the data link layer are:
  - **Data aggregation:** In a data aggregation plot, the information of sensor is collected all through units of the system so as to demonstrate an aggregate perspective of the checked marvel. On the off chance when attacker controls a couple of nodes, it can have some impact on the conglomeration result. In the event that those nodes are Sybil

nodes with numerous personalities, an attacker will be having a more noticeable impact on the collection result.

- **Voting:** In voting plans, nodes of Sybil can be utilized to "apparatus the race". The effect on the voting result relies on upon the measure of personalities the Sybil nodes are in control of.

➢ **Network layer:**

- **Neglect and greed:** In this attack, a malicious that is a piece of a system course can drop the packet yet at the same time transmit ACK to the sender. An attacker can drop only certain parcels, or essentially simply all packets are dropped which are descending the routing way.
- **Misdirection:** In this attack a malicious node can be opposed to dropping packets, entirely just transmit them on an alternate way where course to the destination does not exist.. The noxious node can perform this for specific packet, or all packets.
- **Internet attack:** This attack is one of DoS attack, where the location of a normal node is spoofed by attacker, telecast response and courses the answers to the normal node. Along these lines the malicious node can surge the normal system join.
- **Black hole attack:** This is also known as DoS attack, where a malicious or harmful node promotes a zero cost course within itself. On the off chance that the routing convention in the system is an "ease course first" convention, similar to separation vector, different nodes will picked this node as a transitional node in directing ways. The neighbours of this node will in the same way picked this node in courses, and vie for the transfer speed. Along these lines the malevolent node makes a dark opening inside the system [24].

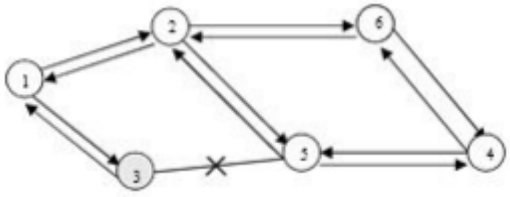


Figure 1.3 Black hole attack [19]

- **Sybil attack :**In multipath directing conventions, a trick can be made by Sybil node that the convention into imagining that numerous ways exist, while all actuality all ways experiences the same Sybil node.

- **Spoofing and altering routing information:** a harmful node might have the capacity to make routing circles in this attack, wormholes, dark openings, packet the system, and so forth, by mocking, adjusting or replaying routing data.
- **Worm hole attack:** Much like same as the hypothetical wormholes in space, this attack can send packet, routing data, ACK and so forth, by a connection out of the system to different node elsewhere in the same system. Along these lines an attacker can trick nodes into supposing that they are neighbors, when they are really in various parts of the system. A wormhole attack can be utilized as a base for roof dropping, not sending packets in a DoS like way, modify data in bundles some time recently sending them and so on.

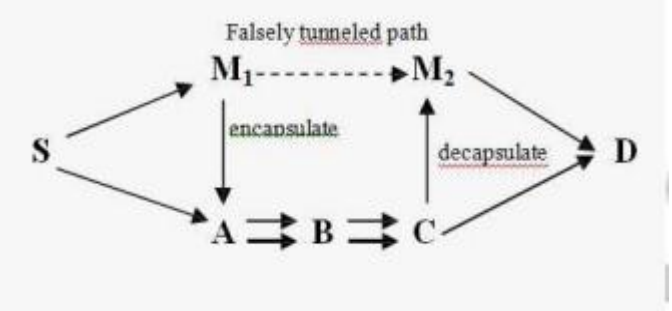


Figure 1.4 wormhole attack [19]

- **Selective Forwarding attack:** In this attack, attacker node can choose not to forward packets of specific sorts or to or from some nodes.

➢ **Transport layer:**

- **Flooding attack:** In this attack, a malicious or harmful node may send constant association solicitations to a normal node adequately flooding the normal system join.
- **SYN Flooding Attack:** The SYN flooding attack is also DoS attack performed by creation of large number of half-opened TCP connections with a target node, the connection of TCP between two communicating parties is made through completing three way handshakes.

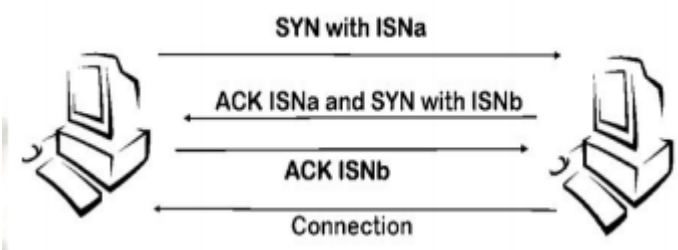


Figure 1.5 synchronous flooding attack

- **Session hijacking attack** victims IP address is spoofed by the attacker, correct sequence number is determined that is expected by the target and then performs a DoS attack on the victim.

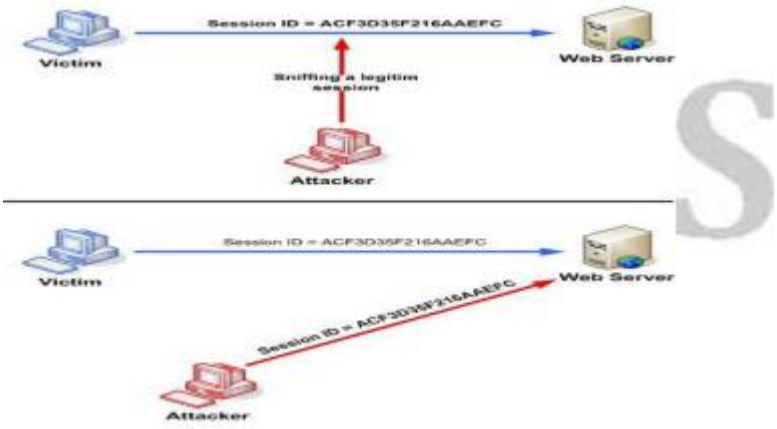


Figure 1.6 session hijacking attack

1.10Introduction to Sinkhole Attack

Since Sinkhole attack is one of the dangerous and biggest attacks in wireless ad hoc network. a malicious node is given in sinkhole attack, it gives a wrong routing information so that it can become a specific node and receives traffic of whole network itself. After getting whole network traffic, the secret information is modified, such that the data packet is changed to make it more complicated. A harmful node tries to attract the secure data or information from all neighbouring nodes. the performance of ad hoc networks protocols such as AODV, DSR etc is affected by sinkhole . In this process the path presented through the harmful node appears to be the better route for the nodes to communicate.

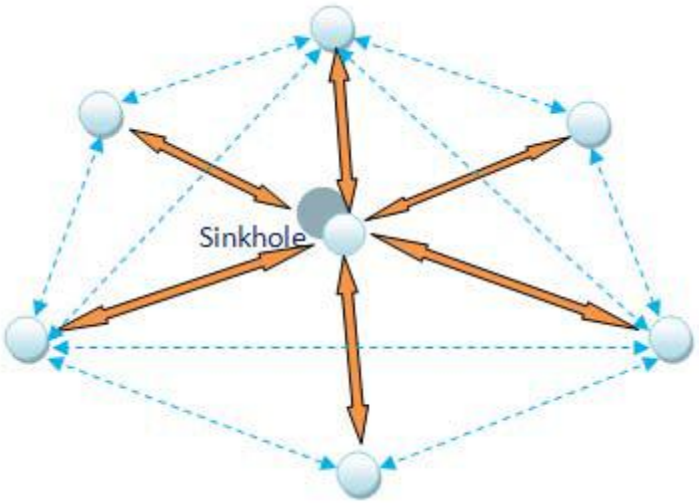


Figure 1.7: Sinkhole Attack in Manet

A Sinkhole attack is a type of attack. A sinkhole node tries to attract the data from all the neighboring nodes, and then it generates wrong information. So the node can now move to local network and can move to specific nodes. Now the sinkhole tries to attract the traffic itself. That is why it informs the data packet or drops the packet without any previous information.

CHAPTER 2

REVIEW OF LITERATURE

Kisung Kim et. aldeveloped the sinkhole detection algorithm using 3 indicators as sequence number duplication. This sinkhole detection algorithm is based all incremental learning proposed to reflect the networking topology changes. It works very well for sequence number below the threshold value. Subsequently a node broad casts alarm message to other node to exclude the sinkhole node in their route.

Gisung Kimet. al, proposed co-operative sinkhole detection algorithm consist of 3 packets named as SAP, SDP & SNP. He proposed a sinkhole indicator which detects the assessment of the RREQ. If a node accepts an RREQ where id of receiving node and source id are equal, it observes the squatness number. If the sequences number of RREQ is larger than the current sequence number of the node then the node know the presence of sinkhole and it recognize this RREQ is from the pseudo node. When the sinkhole indicator is observed, the sinkhole detection procedure is started by distributing a sinkhole detection alarm packet (SAP).

M. S. Sonalet. alproposed that discontinuity in sequence number and advantages of cooperative technique can be approached together. It uses four messages while doing detection. In first one, biggest value will be selected. The biggest value is collection of discontinuity in sequence number. Whenever any RREQ receive biggest value, it will calculate by compare with recent RREQ.

D. Sheelaet. al, algorithm based on mobile agent based on routing algorithm to attack against sinkhole attack in WSN. Mobile agent is software program which is controlled by self that visits every node in the network randomly or periodically. By using the gathered information , every node gets alert of while network so that a right or accurate node will not listen to wrong information which can cause sinkhole at tack .

Maliheh Magellanet. al briefed about the new algorithm for finding sinkhole attacks . The given algorithm works by discussing the controlled fields of the received data packet with the original control packers, when there is need to send data to BS, it initially send a control packet to main BS. After it reaches BS, it compare control field in the data packet.

Ahmad Salahi, gave a very simple algorithm to check the sinkhole attack in the WSN .The algorithm contains two step , The first step is affected node is found in that area by going through the data and the second step is to identity and then introduce in the list effectively .

Murad Aet. al Proposed a confusing and unique rules based detection mechanism of Sinkhole in the mint route WSNS, the detection system is first installed in each & every node to keep checking the whole network And action of detecting the attack in done by the sink by the cooperative mechanism after getting id of the pointed (expected) sinkhole from each node which causes breakdown of communication with all sensor nodes by highlighting the pointed nodes ID.

K. Tunwalet. alhere sinkhole prevention method is based on individual trust management. The entire node have trusted weight, each node further send the packets to next node until it reached the destination. When sinkhole node assume that the node is malicious at that time it decrements the local trust of that node. At last when route is created the node with the lowest trust values are avoided. So, the efficiency and reduce false alarming the time is dynamically modified as per the packet received per seconds. The simulation conforms that method is well suited for robust to network environment.

Nisarg Get. aldiscusses the sinkhole difficulty; its importance & exiting a mechanism of identify and overcome of it in AODV protocol. The technique is based on sequence numbers for prevention and detection. After applying detection & prevention mechanism, it show that performance of AODV is make better which is get worse due to attack. The paper does not consider the problem of duplicate sequence number.

T. Mishraet. alused digital signature concept to secure the data. Here key is used for all nodes, this key generated by digital signature and verify it when decrypt the data. This algorithm provides security to its private nodes. To find the ease of use and corroboration of route on basis of hop count and time interval, a route validation scheme is also used. To changes conservative digital signature in secure routing data chunk, at the same instance, upholding the same level authentication, its advantages of first of all signature, which is more effectively in signing and

validation. Every node in the network verified the digital signature for security purpose, if the signature is not verified or any of the packets has no valid signature than drop that packet.

Harshilet. al This Paper focused on identification of attack of black hole in MANET. In network of mobile (MANET) security requirement is more as compared to wired network. In wireless network attacks are of many kinds like black hole, Sybil attack, worm hole attack etc. are possible. So a successful attack or intrusion detection system (IDS) is needed to detect malicious nodes to identify & separate the problem caused by such nodes and notify the information of malicious node to the other node [22].

Chinky Jain et. al In this paper, Author provide method based on algorithm to concentrate on studying and improving the protection of AODV and it is one of the accepted routing protocols for MANET. Main purpose of this paper is to make sure the protection against Black hole attack. The planned resolution is proficient of identifying & removing Black hole node(s) in the MANET in the starting. In addition the aim of this paper is to give a simulation study which explains the effects of Black hole attack on network performance. Earlier the works done on MANETs paying attention mainly on different protection threats and attacks like Impersonation, Wormhole, Jellyfish, and Intrusion detection. Attack of black hole is essential on routing protocols AODV and OLSR. And also ensure which protocol performs improved aligned with black hole attack. The requirement to tackle all these types of protocols under the attack, and the effects of attacks on MANETs. [32].

Mohammed et. al. Statistics proves that remote innovation is picking up popularity day by day. Today, individuals can speak with each other in any nation with the assistance of wireless technology. This paper proposes an advancement in a AODV protocol which is the modern feature in the current AODV protocol. Calculation of protocol which is received by Energy Efficient Ad Hoc Distance Vector convention (EE-AODV) has advanced the RREQ and RREP taking care of procedure to spare the vitality in cell phones. In this paper AODV protocol is checked or used by using 30 nodes. The main purpose of this paper is to measure the efficiency of protocol at 30 nodes. The execution measurements are delivery ratio for utilization of assessment, throughput, system lifetime and normal energy consumed. using NS2 simulation can be done.[30].

W.K. Kuoet. al. In this paper, They explore EE optimization as measured in bits per Joule for MANETs based on the cross-layer design paradigm. They model this problem as a nonconvex mixed integer nonlinear programming (MINLP) formulation by jointly considering routing, traffic scheduling, and power control. Because the nonconvex MINLP problem is NP-hard most of the time, it is exceedingly difficult to globally optimize this problem. To efficiently solve this globally optimal problem we customized branch and bound algorithm. The newness of our proposed BB algorithm include designs using upper and lower bounding schemes and branching rule using the characteristics of the nonconvex MINLP problem. We demonstrate the efficiency of our proposed BB algorithm by offering numerical comparisons with a reference algorithm that uses the relaxation manners proposed in some papers. Numerical results show that our proposed BB algorithm scheme, respectively, decreases the optimality gap 81.98% and increases the best feasible solution 32.79% compared with the reference algorithm. Furthermore, our results not only provide insights into the design of EE maximization algorithms for MANETs by employing cooperation's between different layers but also serve as performance benchmarks for distributed protocols developed for real-world applications [31].

Faizan Khanet.al In this paper author will concentrate on recognizing the Sybil attack in MANET. It utilizes air medium for correspondence so it is more inclined to the attack .Mobility cause a fundamental issue in discussion of security in Mobile Ad-hoc network. It doesn't rely on upon fixed design, the nodes are constantly moving in an arbitrary form. Sybil attack is one in which single node display various fake characters to different nodes, which cause destruction. Through simulation it is shown that this discovery can be finished by basically utilizing the device NS2.35 [20].

T. Saranya et.al. In this paper, author propose a simple plan to identify the new characters of Sybil attackers without using any trusted third party or any additional equipment, for example, directional receiving wires or a topographical situating system. Completely self-organized mobile adhoc network systems (MANETs) communicate to distributed systems which are complex that may also be a piece of a complex system which is enormous, for example, a typical system-of-systems utilized for emergency administration operations. Because MANETs has complex nature and its asset imperative nodes, there has been a need to create simple security arrangements. Since MANETs require a one of a kind, particular, and diligent identity per node all together to support their security protocol to be practical, Sybil attacks represent a genuine risk to such systems. A

Sybil attacker can make more than one identity on a single physical gadget keeping in mind the end goal to dispatch a facilitated attack on the system or can switch characters keeping in mind the end goal to debilitate the identification procedure, subsequently advancing absence of responsibility in the arrange. Through the simulation author can show that their proposed conspire distinguishes Sybil characters with great exactness even within the sight of mobility [21].

P. Raghu Vamsi and Krishna Kantproposed a technique for identifying Sybil attack utilizing successive investigation. This technique works in two phases. To start with, it gathers the confirmations by watching neighbouring node exercises. Further, the gathered confirmations are united to give contribution to the second stage. In the second stage, gathered confirmations are approved utilizing the successive likelihood proportion test to choose whether the neighbour node is Sybil or kind-hearted. The proposed technique has been assessed utilizing the system test system ns-2. Results demonstrate that the proposed technique is powerful in identifying Sybil attacks with low false positive and false negative rates [33].

Prabhjotkauret al. in this paper an work in which they have a tendency to adjust the brought together IDS plan is proposed which is based on the abuse detection to recognize the malicious cluster head which has the expectation of bringing about the Sybil attack in the remote sensor system. Work affirms the adequacy of our adjusted IDS regarding the right detection of every single existing attack [34].

Vanitha et al. a probabilistic trouble making detection planes proposed and is exceptionally desirable to guarantee the protected DTN routing and also the foundation of the trust, among DTN nodes. A node is utilized to gather the node information inside the range. In a protocol like this it can't accomplish ratio of packet delivery, execution and information loss rate. The explanation with black hole attack is given in the paper which is based on fuzzy rule. Fuzzy control is utilized to determine the tainted node and additionally convey the solution to lessen information misfortune over network. Fuzzy rule lies between the incentive as {0, 1}. One of the most reasonable routing systems in wireless mobile Ad hoc network is geographical routing predominantly because of its adaptability. Multi Input Multi Output strategy used to send information much of the time in routing

protocol. Examination and simulation comes about check the adequacy and productivity of the drop node investigation, high packet delivery ratio, throughput and delay [23].

Kaur et al. a technique to outline a system detection of black hole based on artificial neural networks (ANNs) is proposed. Utilizing a simulated MANET environment, ANNs demonstrating for recognizing attack, the black hole attack is examined and it is demonstrated that model can recognize nodes under black hole attack adequately [24].

P.Kavitha et al. proposed a location method which depends on NDD calculation for distinguishing Sybil attacks. The calculation is utilized to exchange the information from source to goal with no harm or misfortune and additionally every node to have the neighbor's node address. Relies on the address the information will be sending into right goal [7].

Roopali et al. strategy in which when node enters a system is proposed , then checking of parameters are done i.e. speed, energy and frequency and if estimation of all these parameters are not as much as limit esteem then node is taken as genuine node generally as Sybil node [2]

Nidhi et al the RSS based discovery is proposed, alongside the verification of node which will accurately distinguish the Sybil information with Higher True Positive. For the verification of node, utilization of message authentication is used. Verification of node permits as it were true blue node to come into the system. And in addition lower bound recognition limit is utilized, and look at the Received Signal Strength (RSS) value, it's a Sybil identity if comparison value is greater than or equivalent to Sybil identity. Generally it's legal in the system [3].

Danish Shehzad et al. a recognition method in light of Hash Function is proposed, just messages alongside their hash function are acknowledged every particular node distinguishes Sybil attackers by approving the Hash got alongside message by the other member, in the wake of getting message node gets Hash of sender and contrasts it and the past Hash gotten in Hello message for the approval of its identity. In the event that Hash varies to that of Hash got along with hi message than node is selected as both Sybil and node is hindered out of correspondence [4].

Karupiah et al. proposed a vitality productive Sybil attack detection strategy called Sybil Secure. In this strategy, nodes are gathered into clusters and a cluster head (CH)in the system and then further it is chosen from the cluster individuals to start the Sybil attack detection process. CH intermittently conveys an inquiry message requesting that the cluster individuals react. Thus, every cluster part reacts to the CH ask. At that point, CH gathers the data, for example, the personalities of nodes that are not answered inside a reaction period, node personalities whose points of interest are like past records, and nodes that sent diverse location facilitates. At last, Sybil Secure technique breaks down this accumulation to distinguish Sybil personalities [17].

M. Bhaskaret. al. The movement to wireless system from wired system has been a worldwide pattern while previous years. The mobility and efficiency brought by wireless system made it possible in numerous applications. Among all the wireless systems, Mobile Ad hoc network (MANET) is a popular amongst the most critical and one of kind applications. As opposed to old system design, MANET does not need a fixed system framework; each and every node acts as both a transmitter and a recipient. Nodes discuss straightforwardly with each other when both of them are inside a similar relation run., Otherwise they depend on their neighbors to send messages. The self-designing capacity of nodes in MANET made it famous among in mission applications like military utilize. Be that as it may, the open medium and wide transmission of nodes make MANET powerless against pernicious attackers. For a situation like this, it is significant to make productive resistant identification components to shield MANET from attacks. With the upgrades of the technology and reduction in equipment costs, we are seeing a present pattern of extending MANETs into mechanical applications. To make such pattern, we firmly trust that it is fundamental to address its potential security issues.

Shan et al. presented location-based attack with various fake personalities on WSN limitation process. Creators broke down the effect of false personalities and location on the limitation process. In this manner, a pernicious node is said to be Sybil on the off chance that it reports false identity what's more, or location data to twist the system operations. The accompanying segment in continuation presents the related work on Sybil attack detection strategies considering false identity and false location information. Customary cryptography techniques come into power when there is a requirement for security in appropriated systems [36].

Manjunatha T. N et al. security issues, security threats, Sybil attack are focused and various methods to prevent Sybil attack. In this paper, they exhibited the general idea of remote sensor system and security in remote sensor system. The different existing techniques for the detection of Sybil attack have been talked about and for detection of Sybil attack, a calculation is proposed in remote sensor system. By utilizing that calculation they discover the Sybil node or not. They have moreover depicted such a variety of attacks that happen in sensor system furthermore apply to sensor node [35].

Rupinder et al. Mobile Agent Based clone Attack Detection Algorithm (MACAD) is proposed. In MACAD calculation, the framework is intended to fulfill each node mindful of area and character of numerous nodes (let's Say n) so that every neighbor of node A confirms the mark and checks the credibility of Location of A. when a node finds a crash distinctive area at a point , it claims with the same ID. It shows the two clashing cases as confirmation to repudiate the copies [12].

Sohail Abbas el at. Proposed a discovery based on RSS instrument to shield the system against Sybil attacks. The plan took a shot at the MAC layer utilizing the 802.11 protocol without the requirement for any additional equipment. We are shown through different examinations that an identification limit presents for the qualification of true blue new nodes also, new malicious nodes [5].

Bin et al. proposed Sybil attack detection strategies based on correspondence extending in WSNs. These techniques work with the assistance of grapple nodes. These techniques expect that vindictive nodes play out the Sybil attack from a settled location in the system. At the point when a node gets the signal message from its neighbours, it computes the polar separation by measuring the polar point. A Sybil attack is identified when the polar separation of various nodes is not exactly a edge esteem. Be that as it may, this technique requires extra equipment setup, for example, stay nodes. From the previously stated writing, it is watched that every strategy its own particular qualities and confinements. A large portion of the strategies are based on ordinary cryptography, utilization of extra equipment setup, for example, stay nodes, and having overwhelming correspondence process. All in all, nodes need to execute the attack detection

techniques in conjunction with the application conventions. To this end, a node-driven methodology is required to identify the Sybil attacks productively without extra overheads [16].

CHAPTER 3
PRESENT WORK

3.1 PROBLEM FORMULATION

Mobile ad hoc networks are popular networks used broadly due to their dynamic nature. These types of networks are suffered from the sinkhole attack as there is no centralized security management. We will discuss the problems in on-going communication by sinkhole attack in this paper. Sinkhole attack is in MANET is important security problem.

A Sinkhole attack is one type of attack in network layer. The data is attracted by sinkhole from the neighboring nodes and then it fake the routing information which make the node which make the local area network know its way on specific node. So, sinkhole tries to attact all the network traffic to it sel.. Therefore, it alerts the data packet or drops the packet mutely. The main objective of the study is determining one of the most severe routing attacks in adhoc network namely the sinkhole attack.

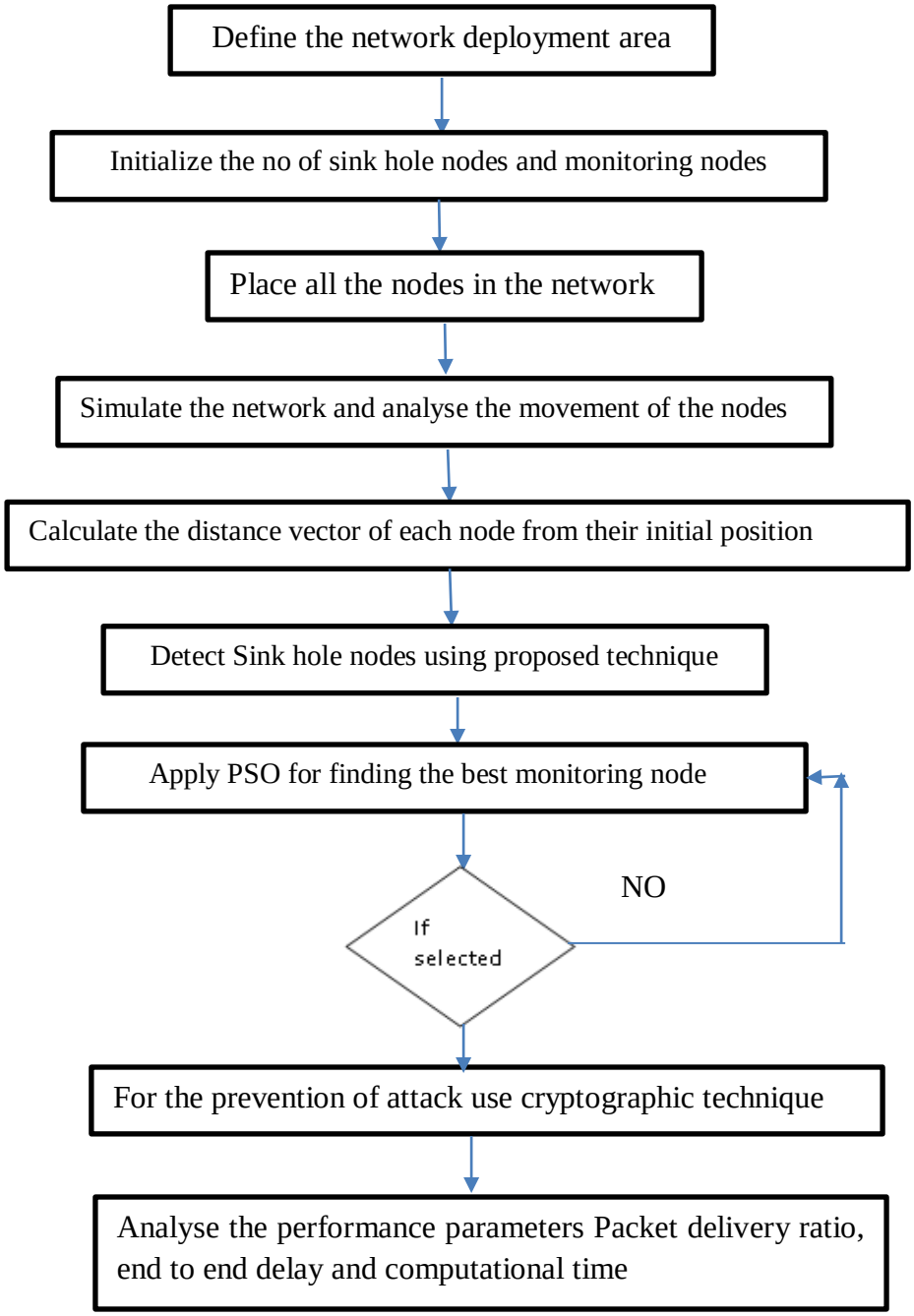
3.2 OBJECTIVES

Sinkhole attack is one of the most important security problems in Manet. The main aim is to detect and isolate the sinkhole node in mobile ad hoc networks and its security is critical challenge because its nature is independent network creation with frequently topology changes. That's why MANET is survival from physical to application layer unsecure. But security is measure issue for the communication so we study number of prevention mechanism and protect thread-hoc network through different attack. In this thesis, our basic objective to protect the ad-hoc network through sinkhole attacks. Sinkhole attack is a type of attack where network traffic is attracted by the comprised nodes by advertising the fake routing update. Other affect of sinkhole attack is that it allows other attacks like selective forwarding attack, drop roying attack.

1 Detect misbehaving node in network
2 To observe the effect of sinkhole attack on network performance
3 Isolate the sinkhole node from network
4 Analysis of sinkhole attack behavior

3.3 RESEARCH METHODOLOGY

1. Define the deployment area of network.
2. Initializes the number of nodes for sink hole attack in the network
3. Initialize the no of monitoring nodes
4. Define the network parameters like node placement, mobility maintenance and distance vector calculation.
5. To create the area for the deployment of the Manet and place the network nodes , monitoring nodes and sink hole nodes and destination node in the network
6. Apply movement to all the nodes from its initial position
7. Calculate the distance vector of all the nodes from their initial position
8. Detect the sink hole nodes using proposed technique.
9. Apply PSO to select the monitoring nodes based on the probability.
10. Provide authentication and integrity to data packets between the source and destination by using cryptographic techniques.
11. Calculating the difference in the parameters like Packet delivery ratio, end to end delay and computational time


Define the network deployment area
Initialize the no of sink hole nodes and monitoring nodes
Place all the nodes in the network
Simulate the network and analyse the movement of the nodes
Calculate the distance vector of each node from their initial position
Detect Sink hole nodes using proposed technique
Apply PSO for finding the best monitoring node
If selected
NO
For the prevention of attack use cryptographic technique
Analyse the performance parameters Packet delivery ratio, end to end delay and computational time

CHAPTER 4

RESULTS AND DISCUSSION

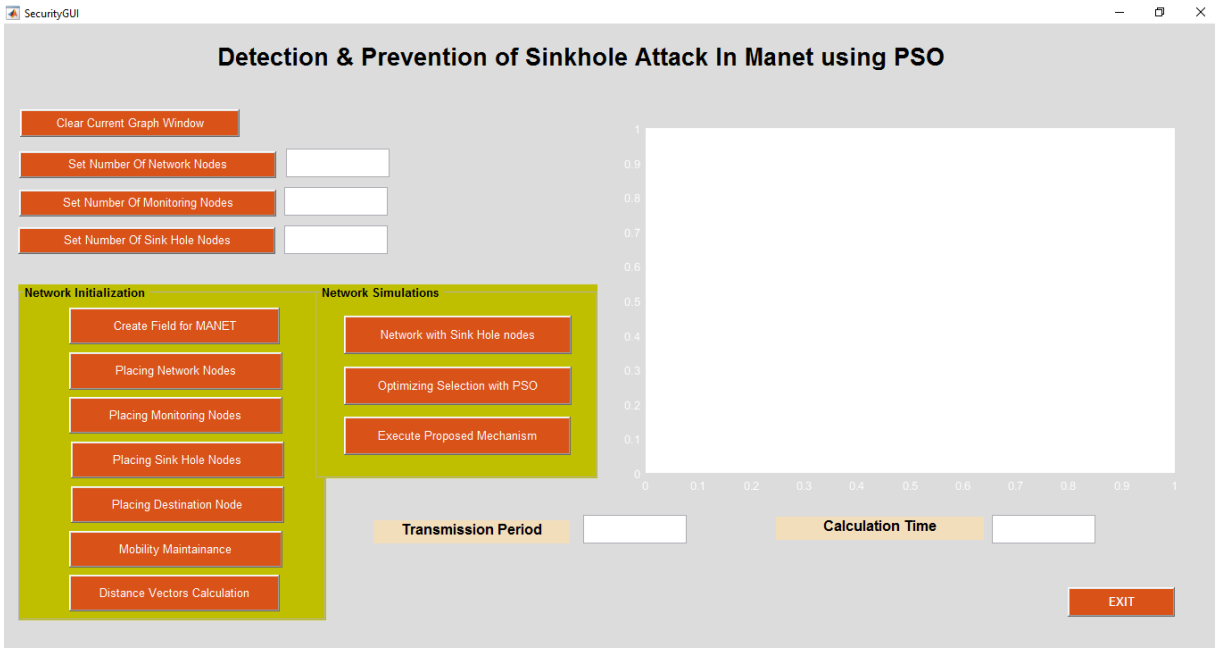


Figure 4.1: GUI Interface

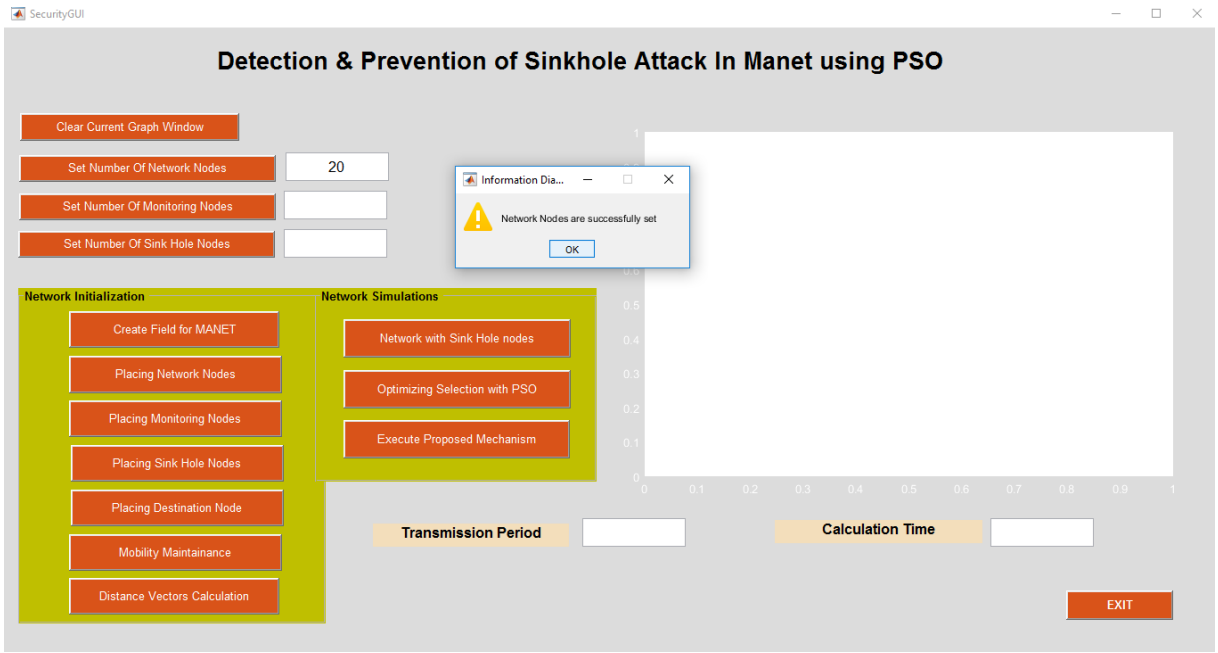


Figure 4.2: Set Number of Network Nodes.

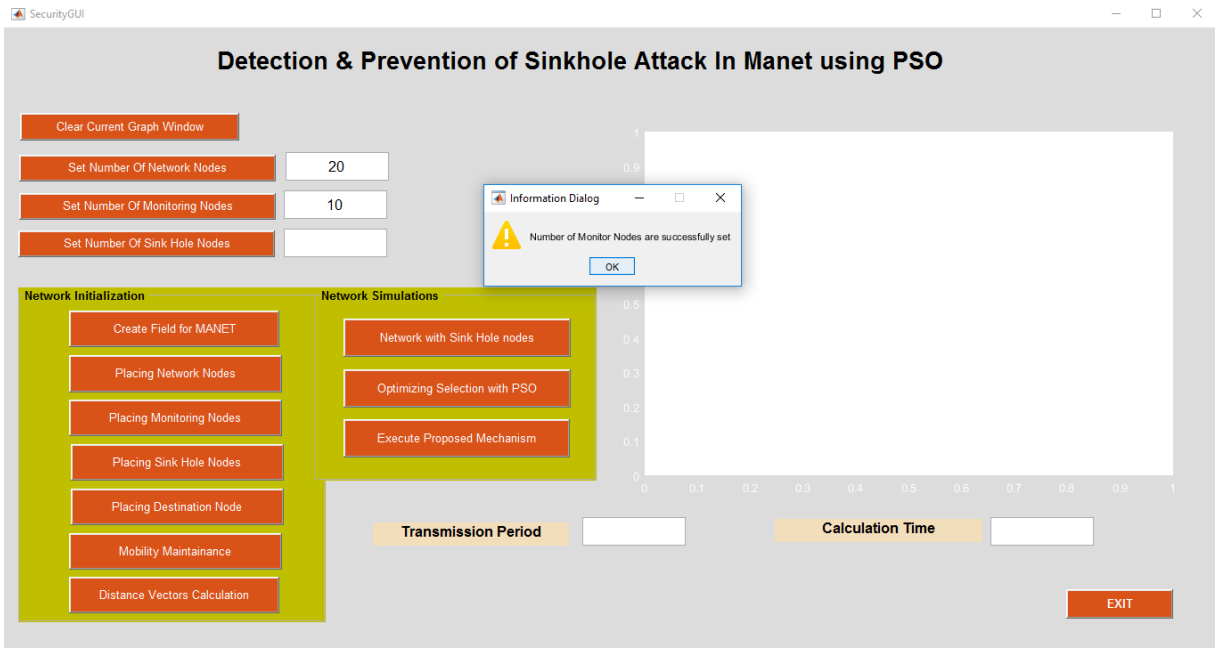


Figure 4.3: Set Number of Monitoring Nodes

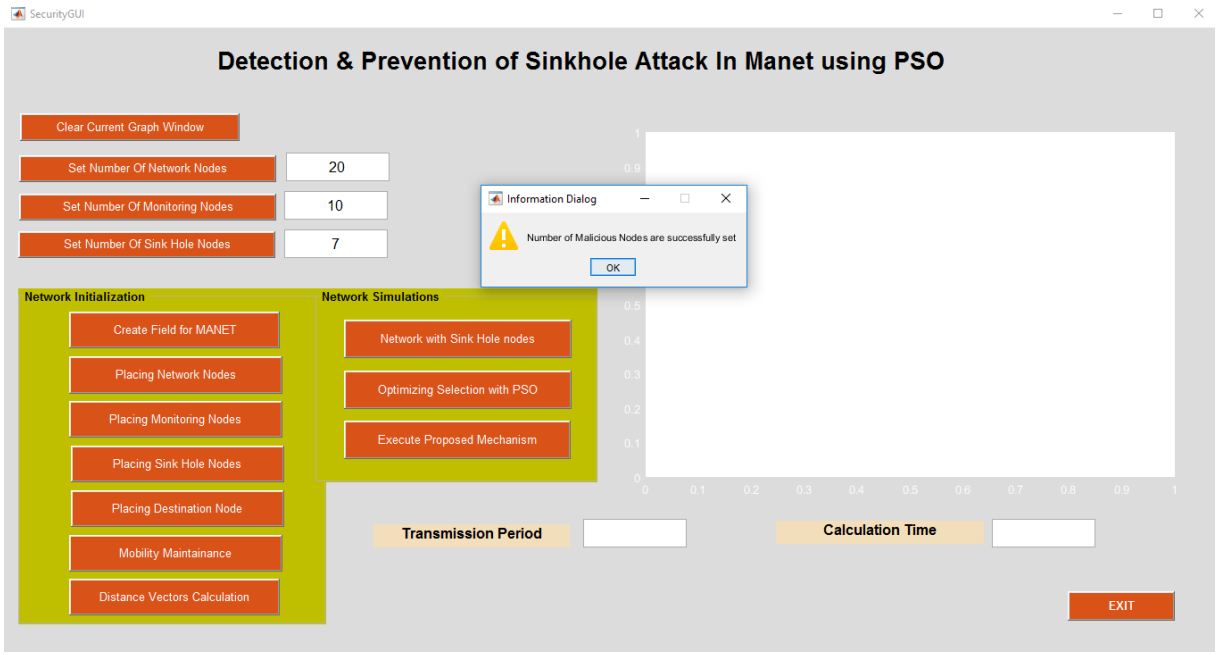


Figure 4.4: Set Number of Sink Holes Nodes

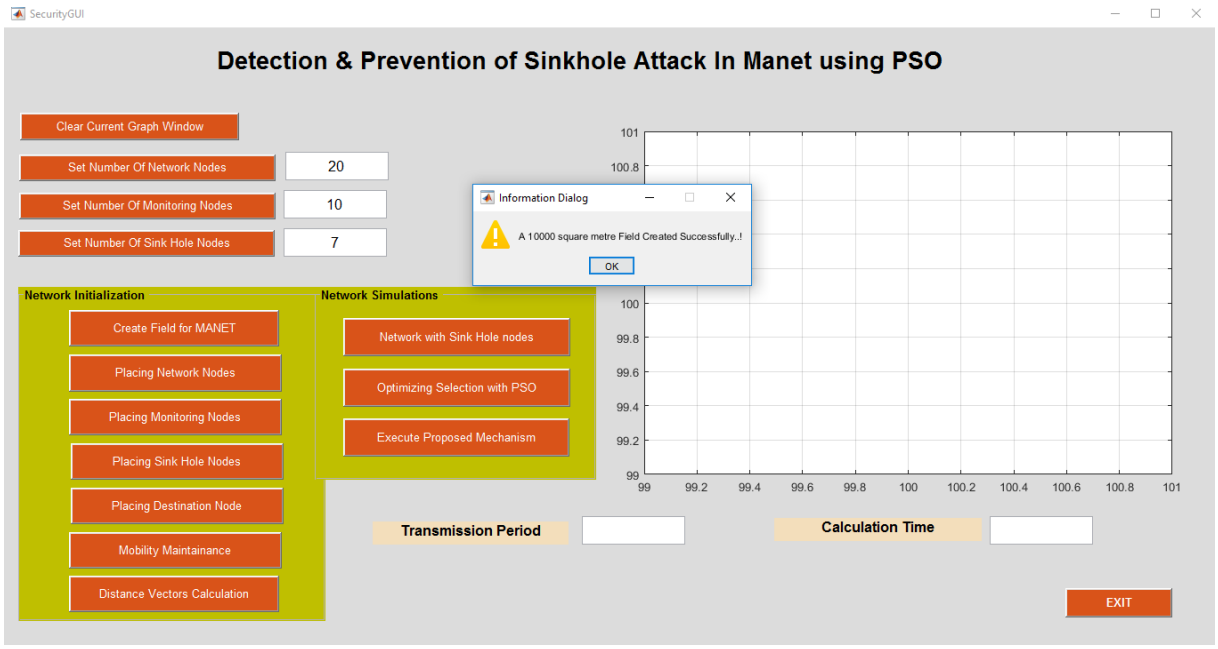


Figure 4.5: Create field for Manet

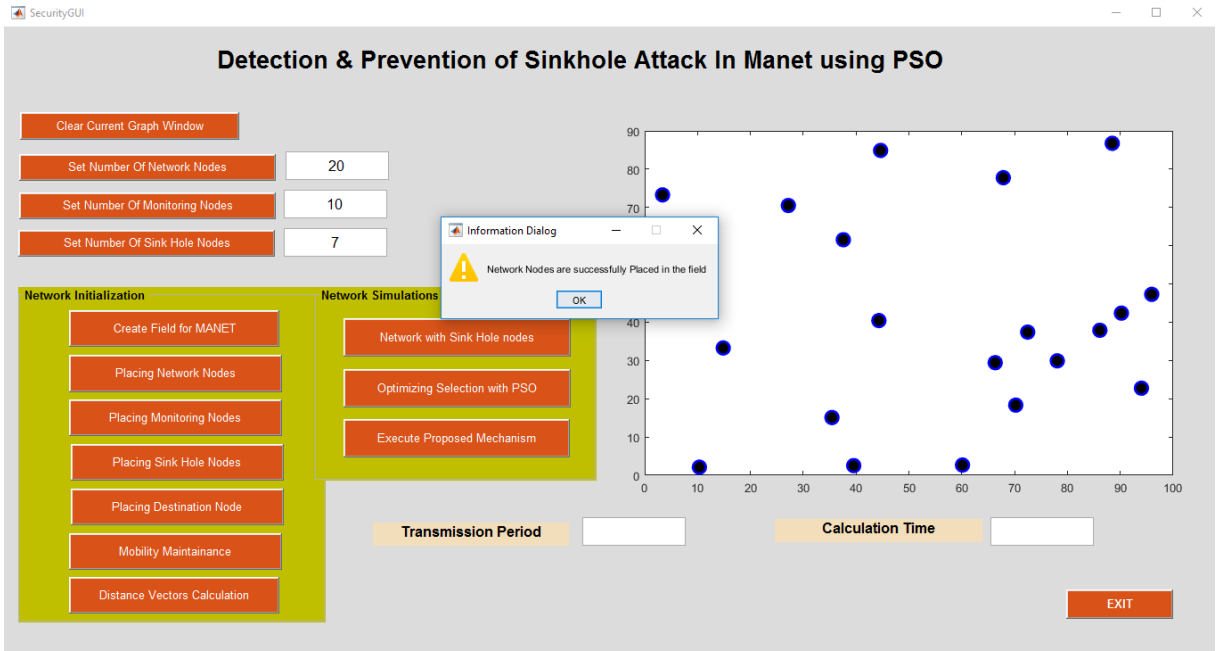


Figure 4.6: Placing Network Nodes

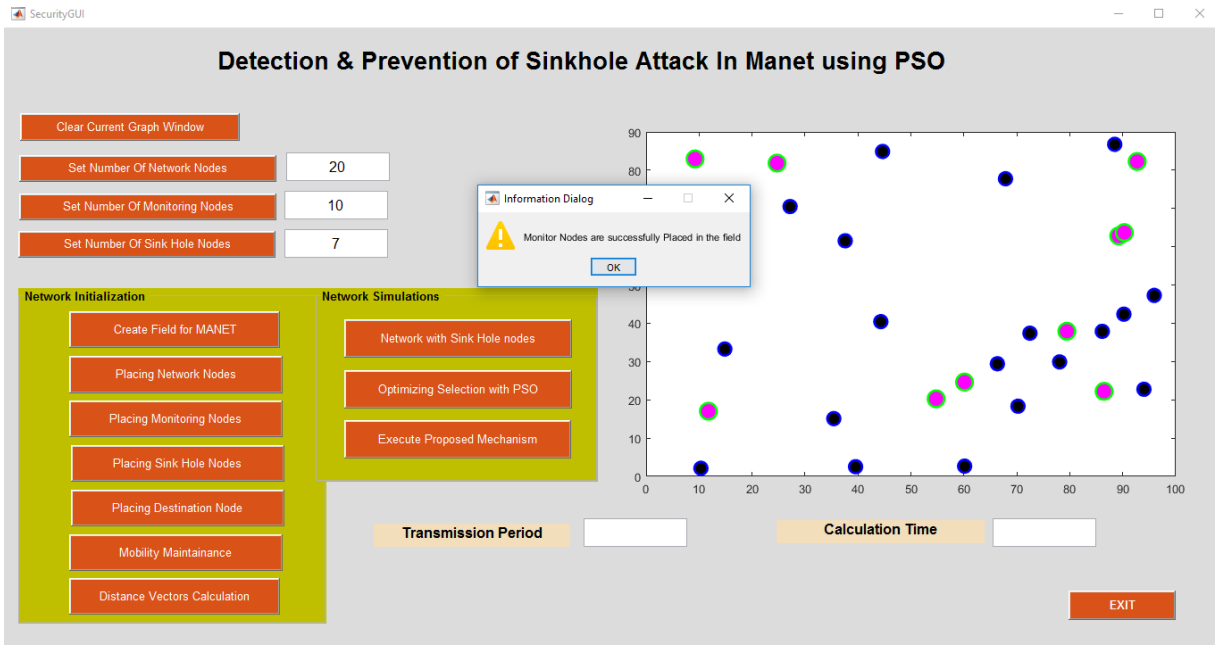


Figure 4.7: Placing Monitoring Nodes

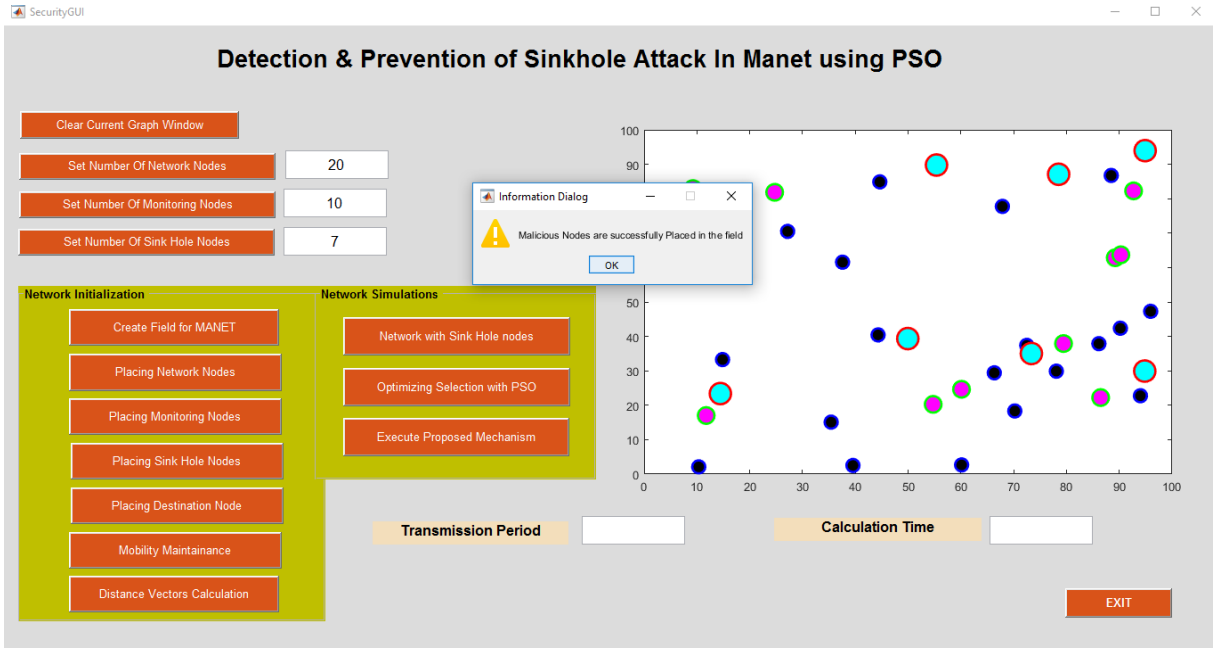


Figure 4.8: Placing Sinkhole Nodes

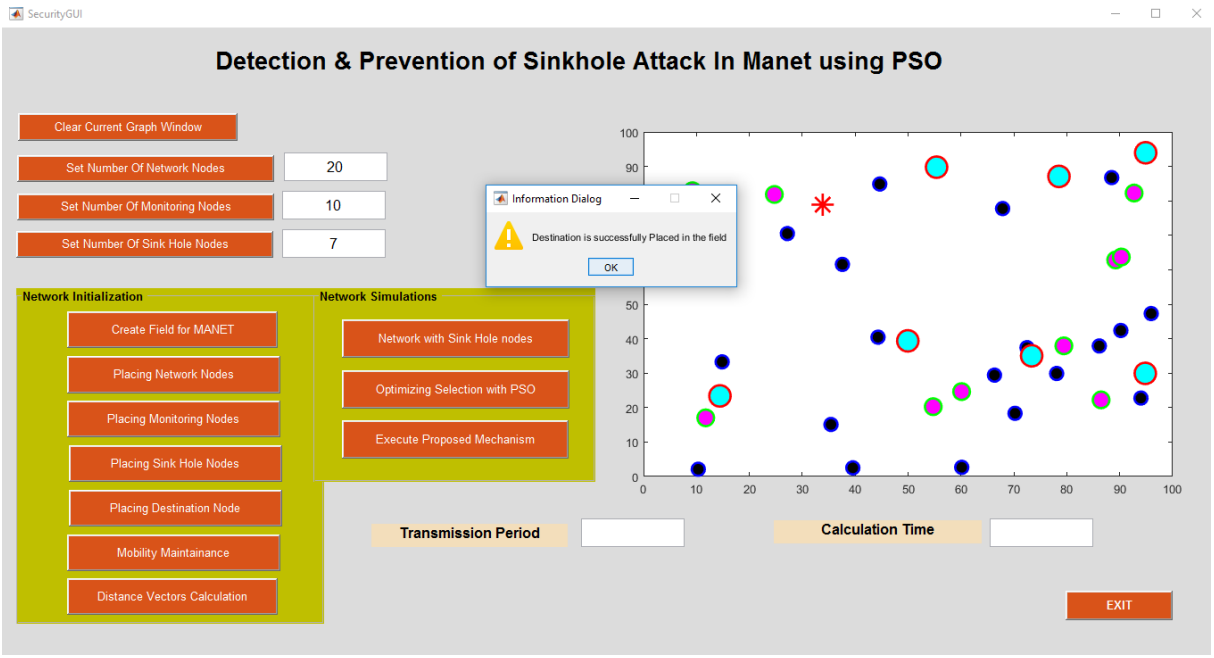


Figure 4.9: Placing Destination Node

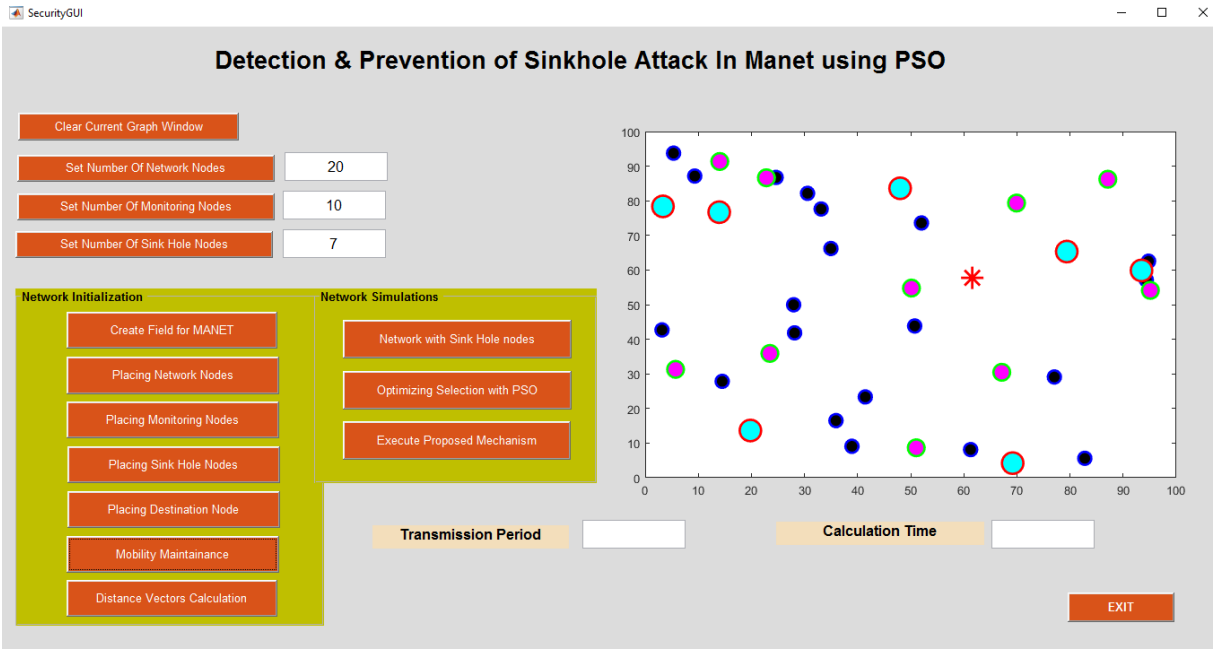


Figure 4.10: Apply Mobility to Nodes

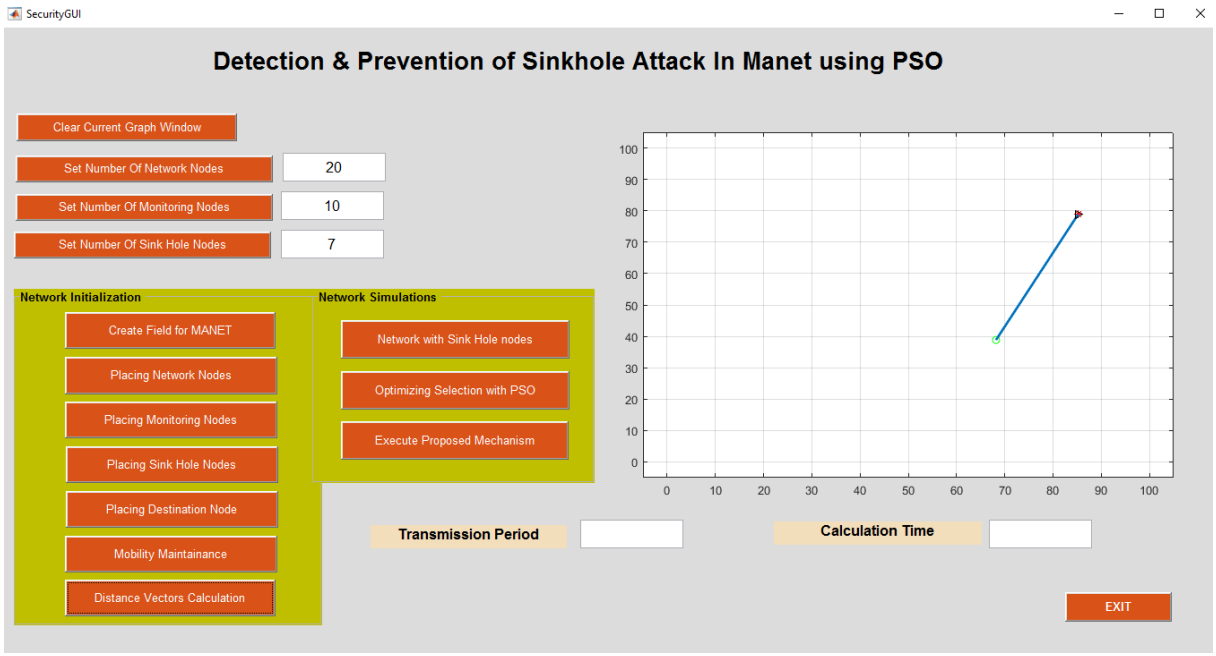


Figure 4.11: Apply Distance Vector Calculation

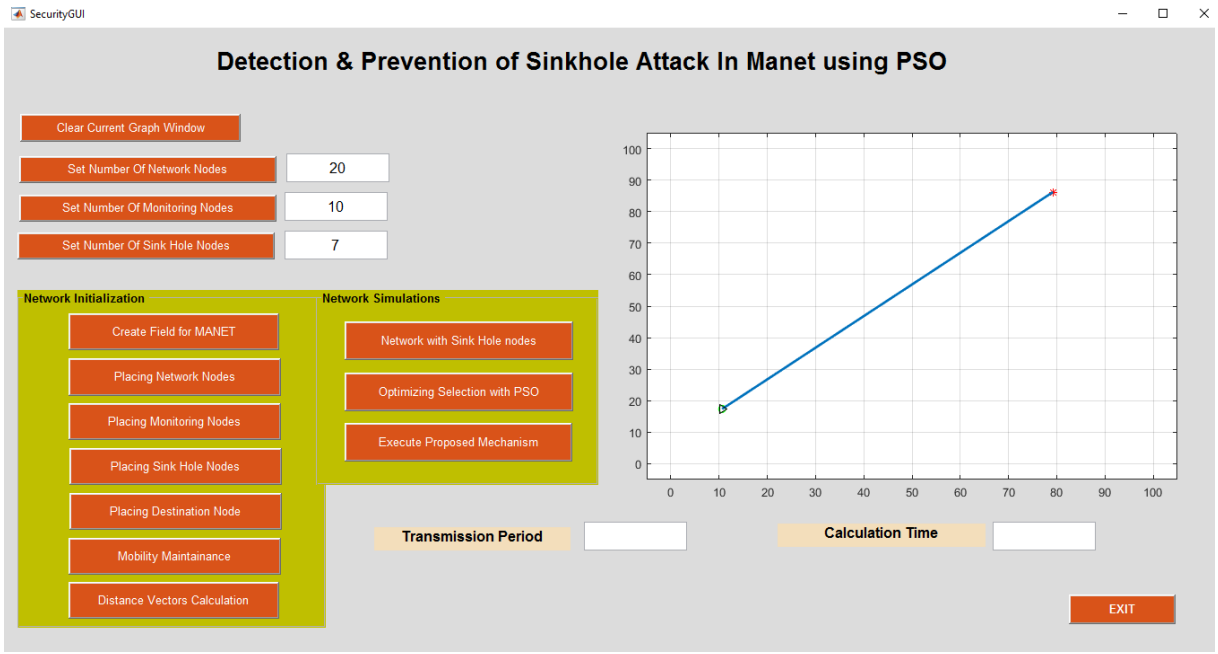


Figure 4.12: Apply Distance Vector Calculation

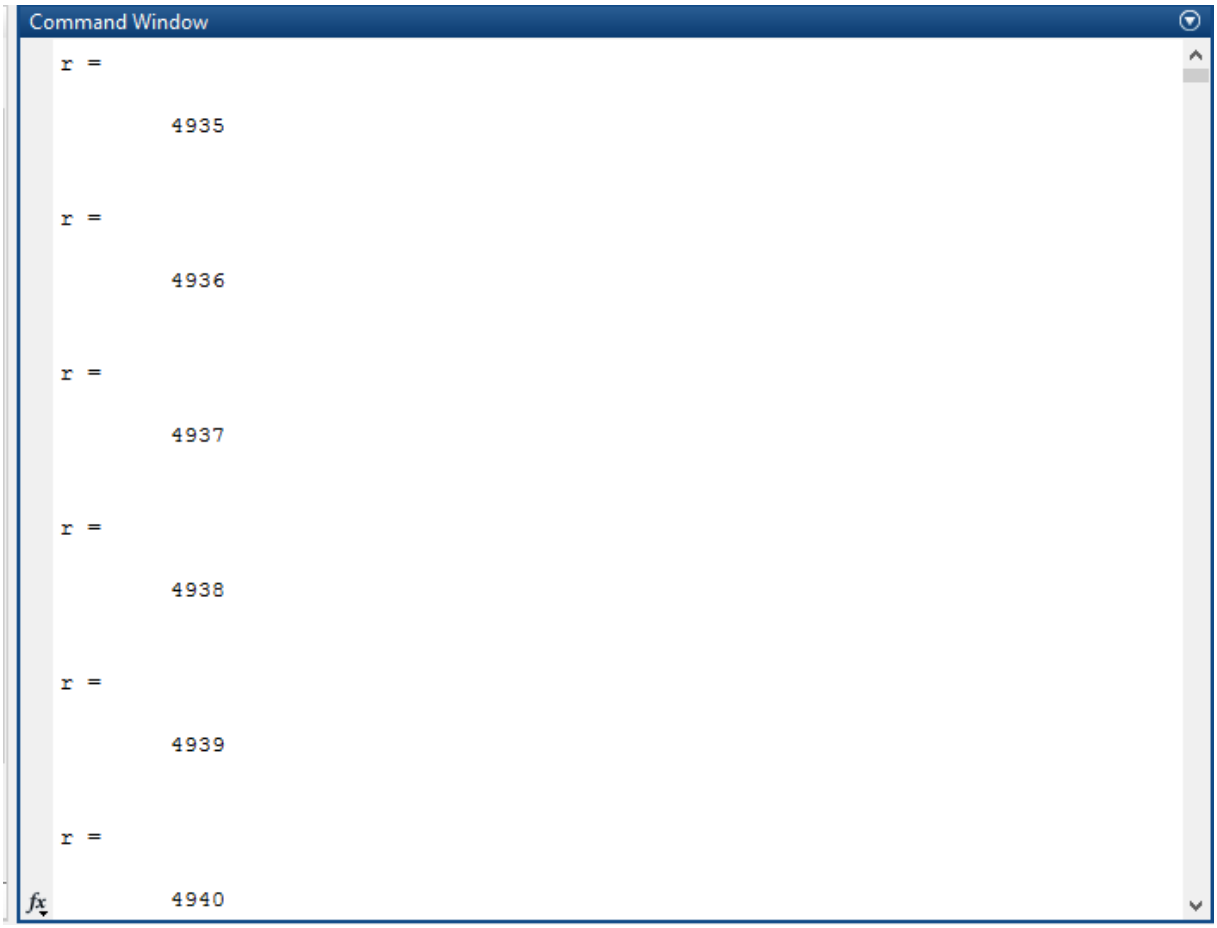


Figure 4.13: Perform Network Simulation with Sink Hole Nodes

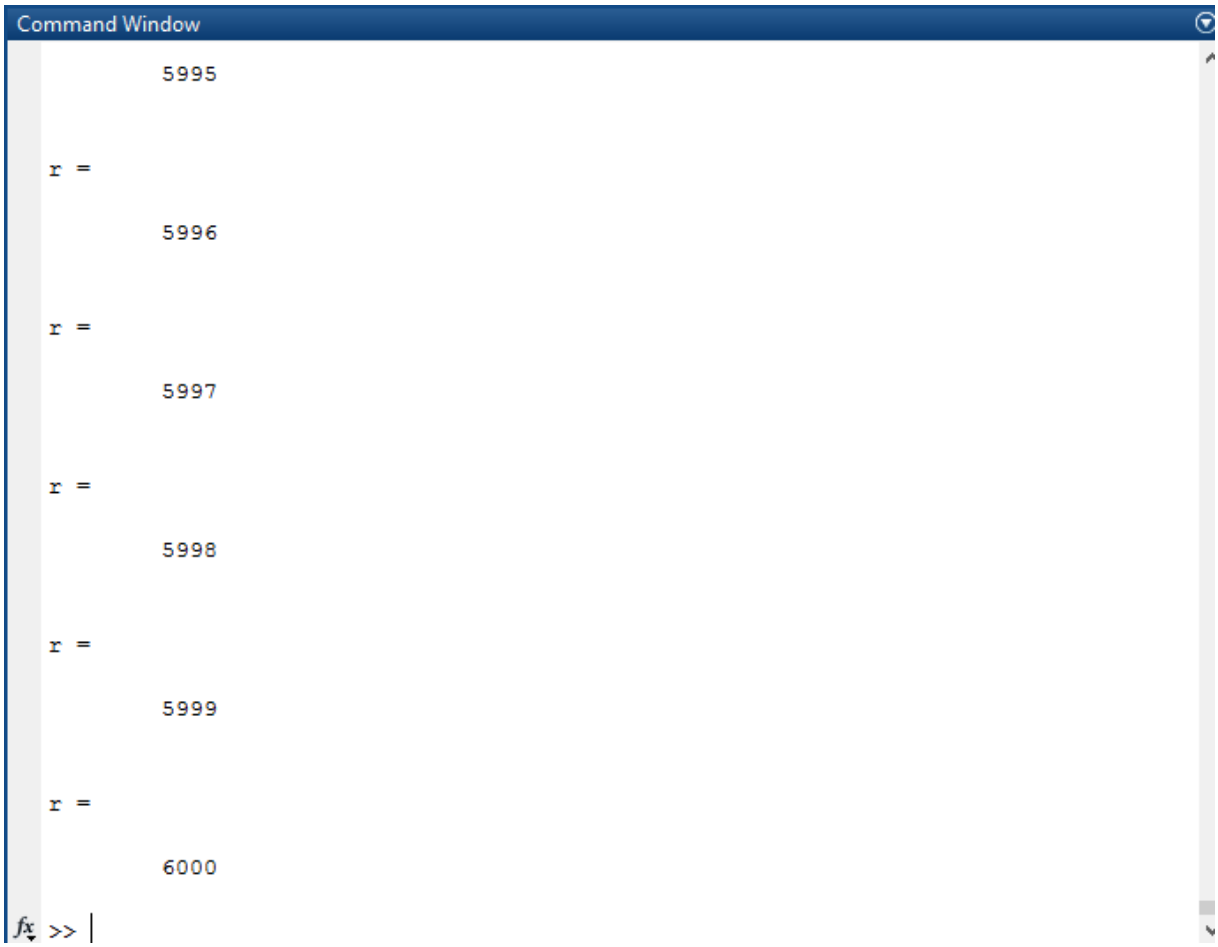


Figure 4.14: Perform Network Simulation with Sink Hole Nodes

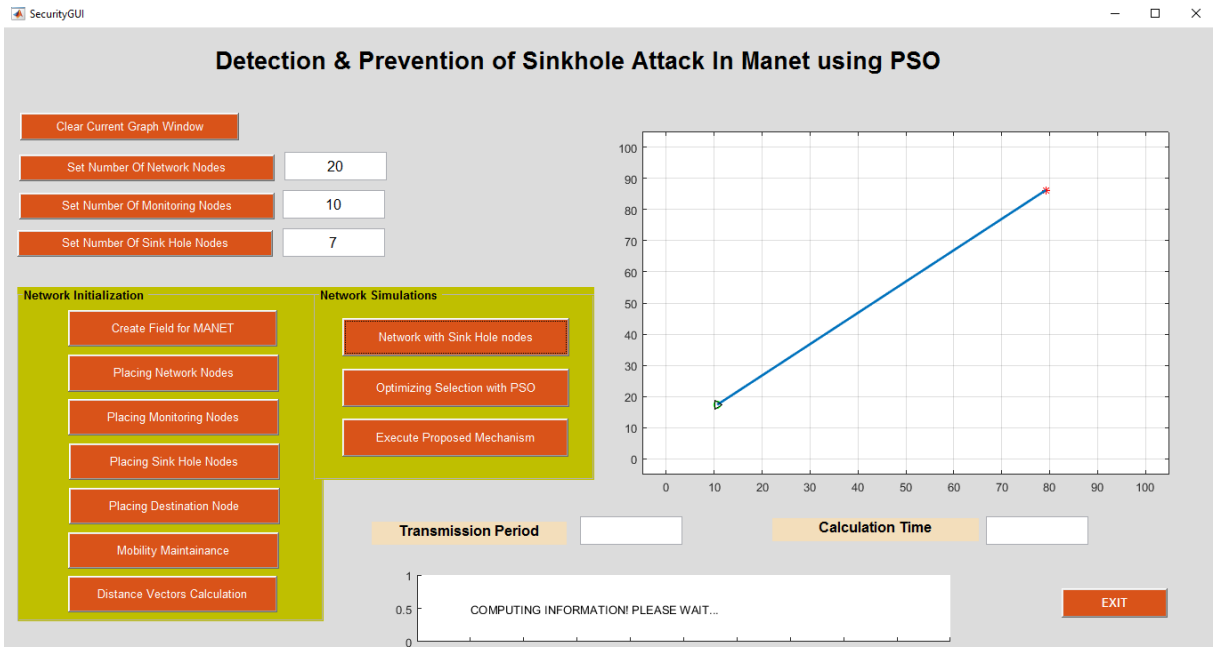


Figure 4.15: **Network Simulation with Sink Hole with PSO**

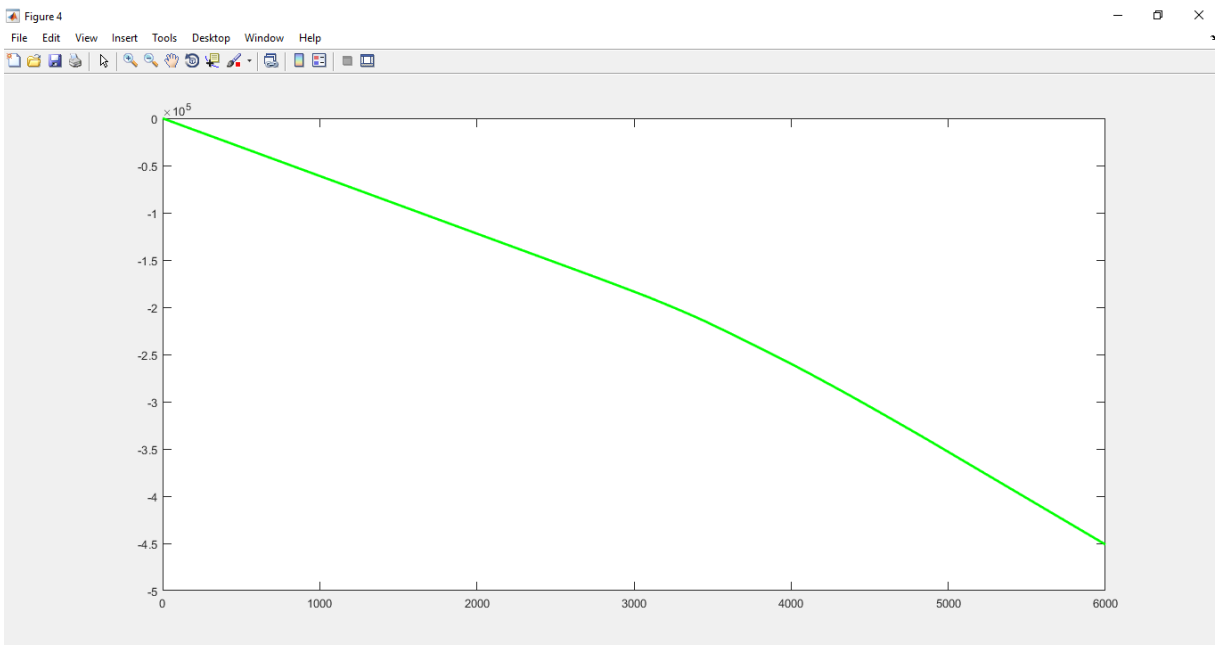


Figure 4.16: Number of Packets to BS, x -label-> number of round

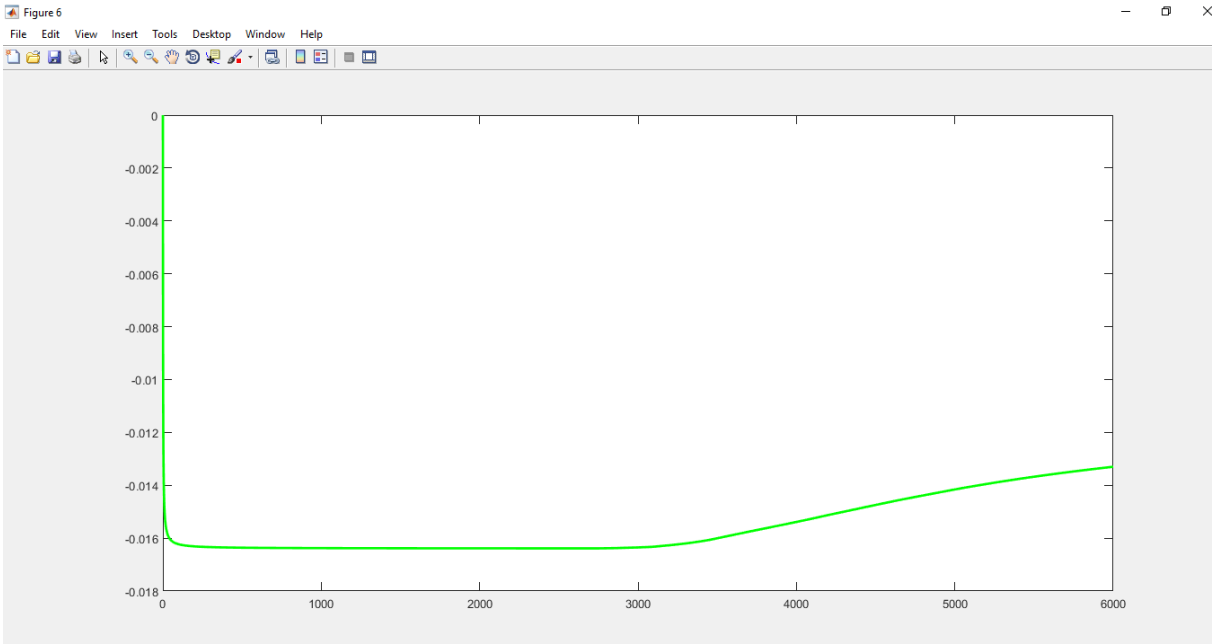


Figure 4.17: Number of Packets to Main = round/number of packet to BS, x -label-> number of round

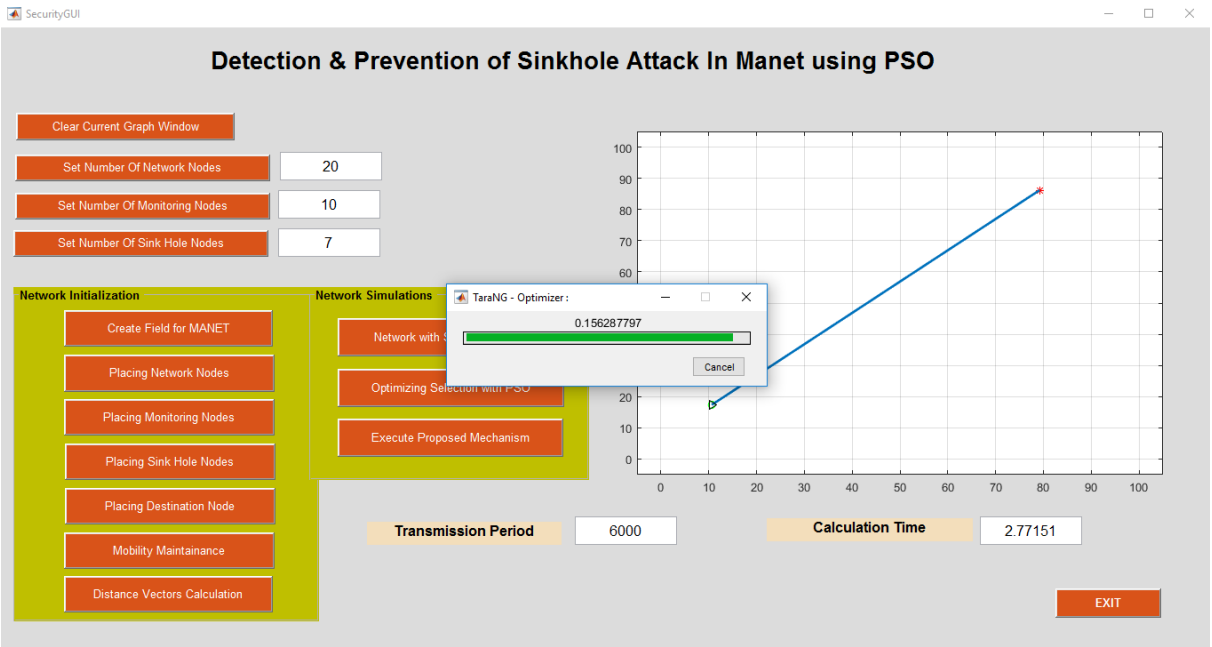


Figure 4.18: Optimization selection using PSO

```
x =

    0.7392    0.5492    0.9756


fvalue =

    0.1505

    0.1505

fx >>
```

Figure 4.19: Fitness Value for Particle Swarm Optimisation

```
Command Window

    313

r =

    314

r =

    315

r =

    316

r =

    317

r =

    318

fx >>
```

Figure 4.20: Proposed Algorithm Round Iterations

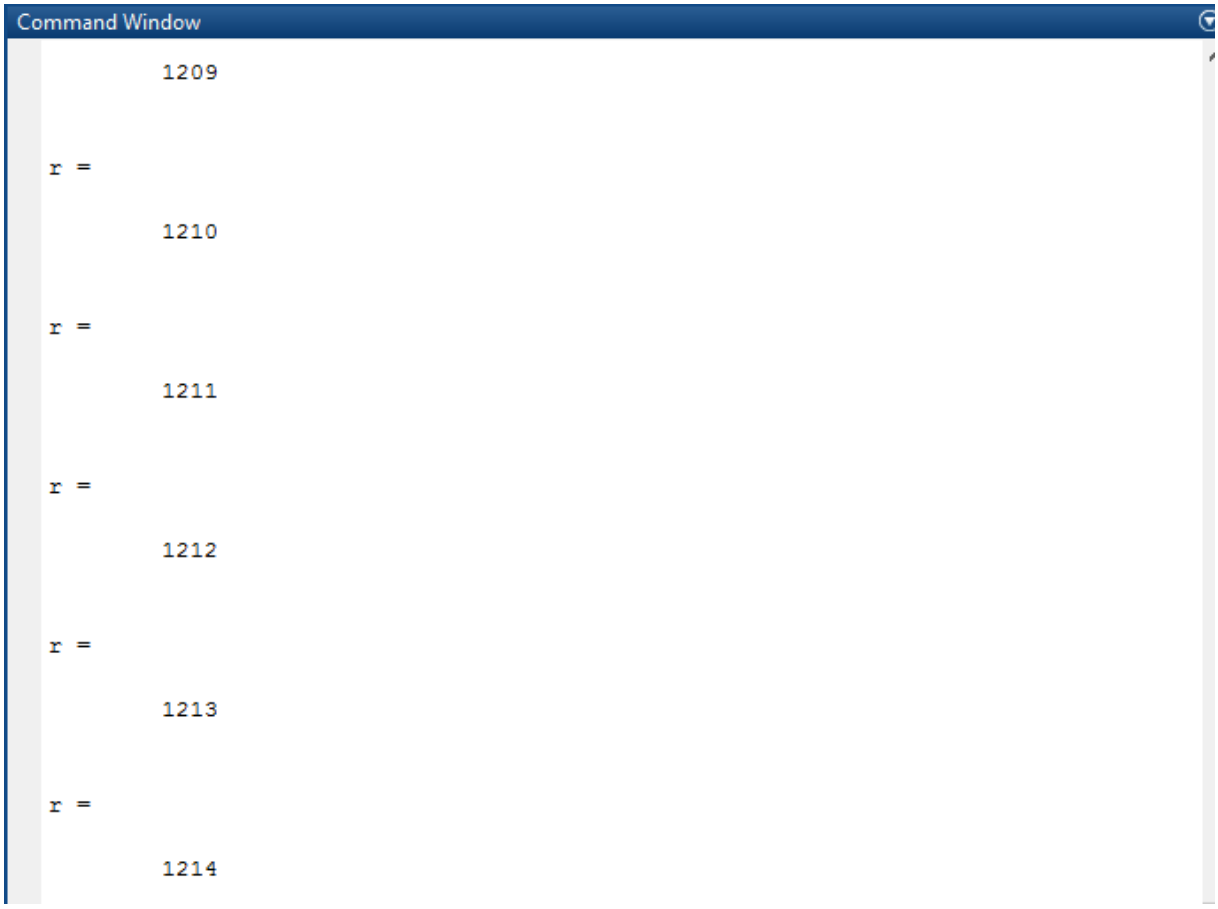


Figure 21: Proposed Algorithm Round Iterations

Figure 4.22: Proposed Algorithm Round Iterations

Figure 4.23: Proposed Algorithm Round Iterations

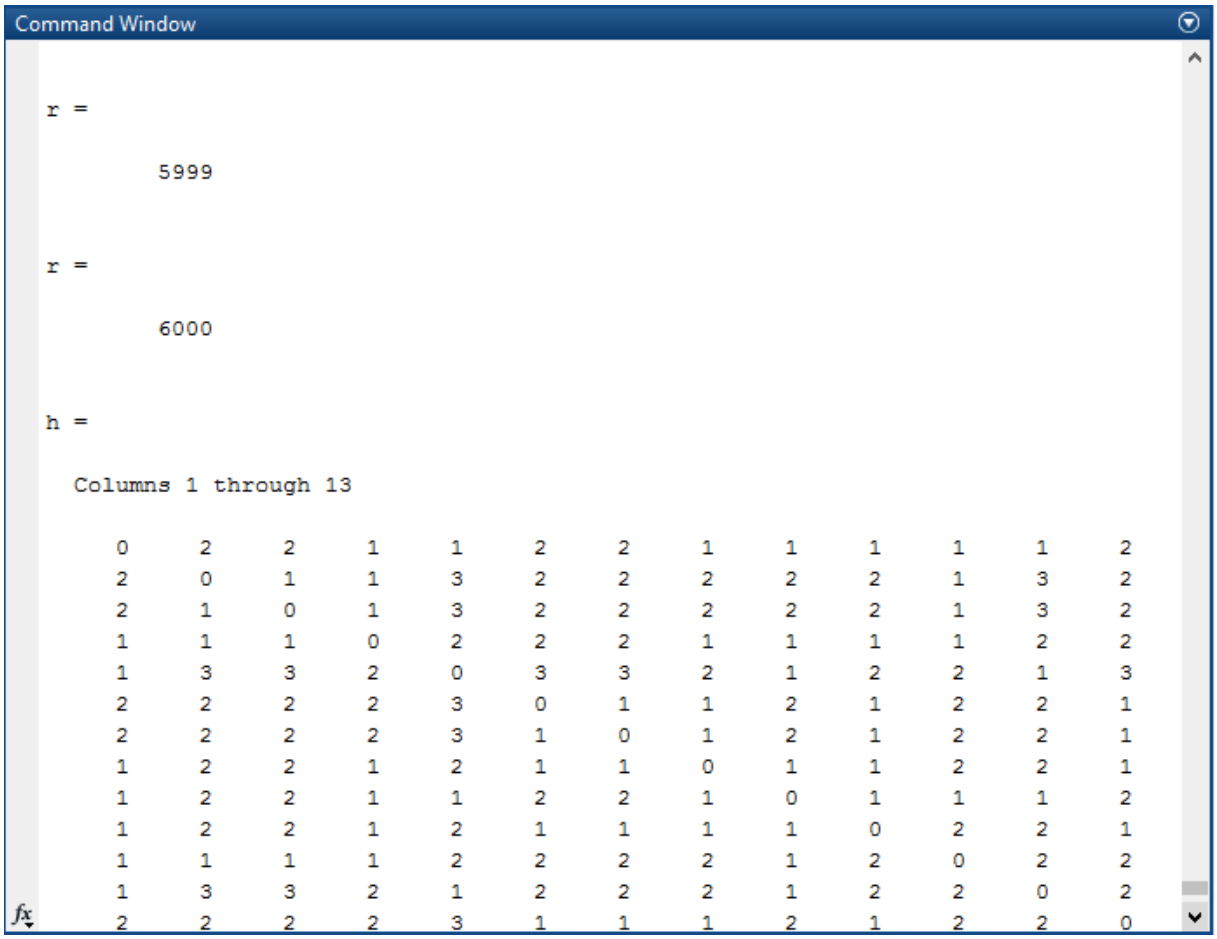


Figure 4.24: Proposed Algorithm Round Iterations

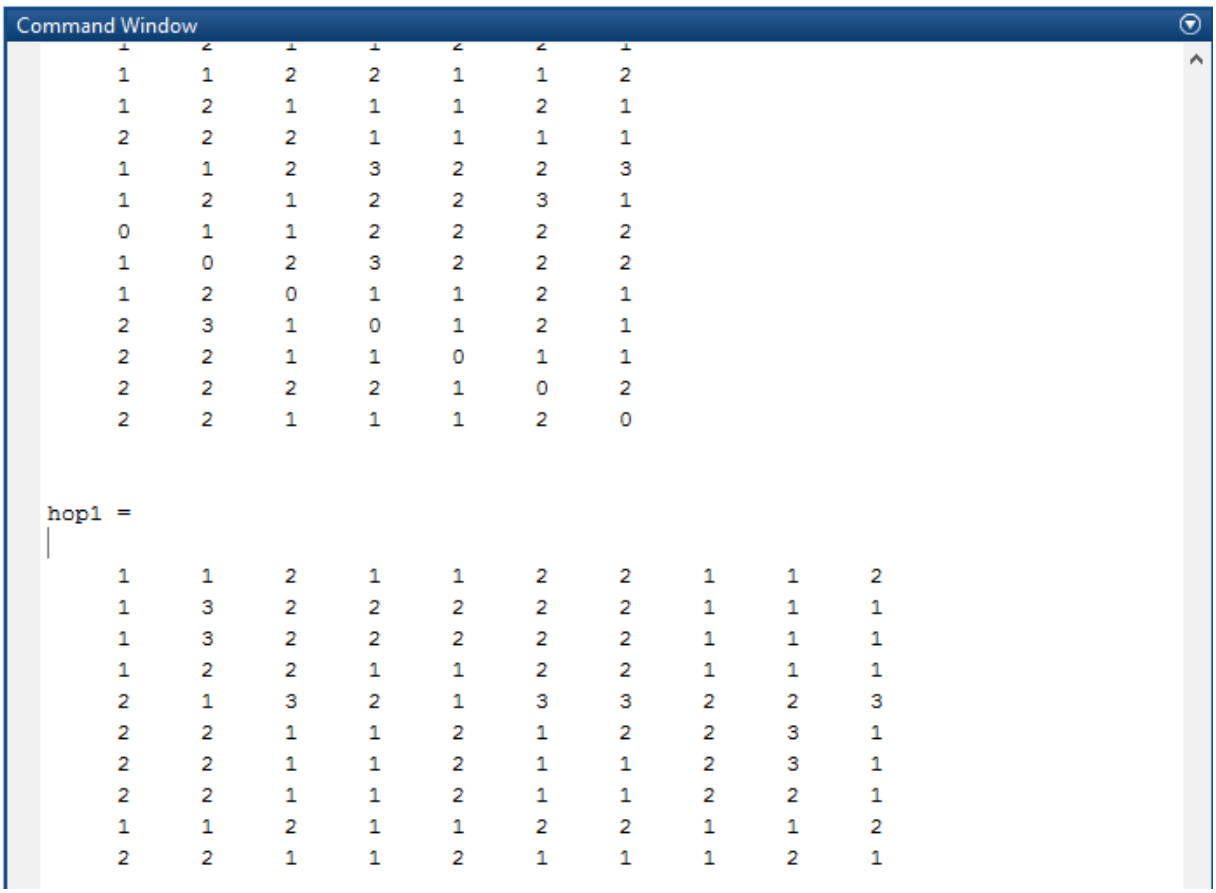


Figure 4.25: Proposed Algorithm Round Iterations

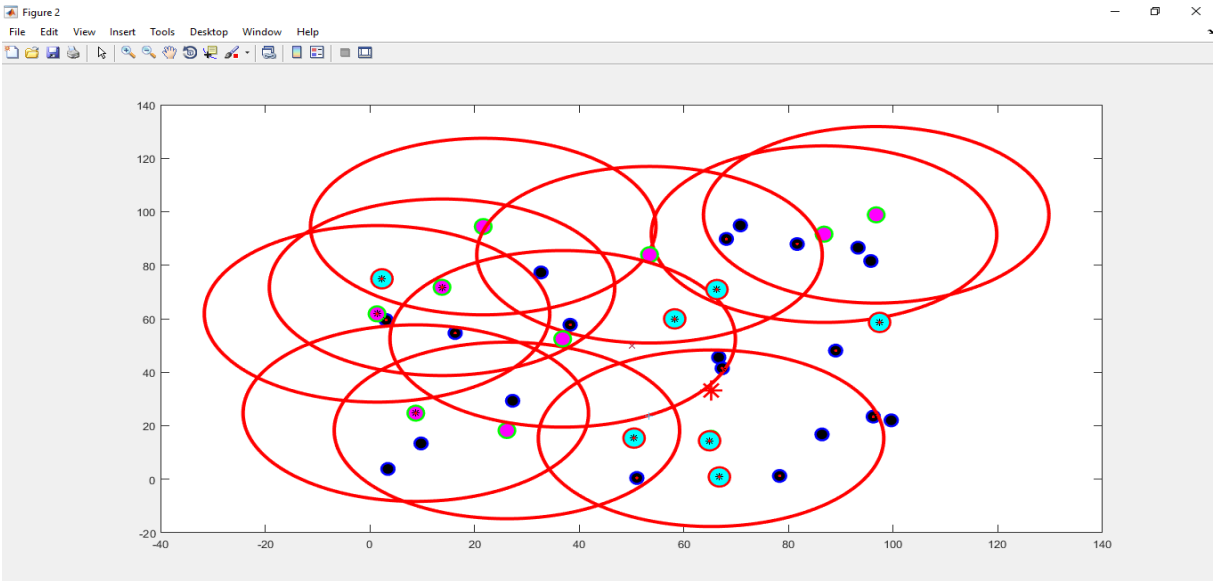


Figure 4.26: Network Visualization

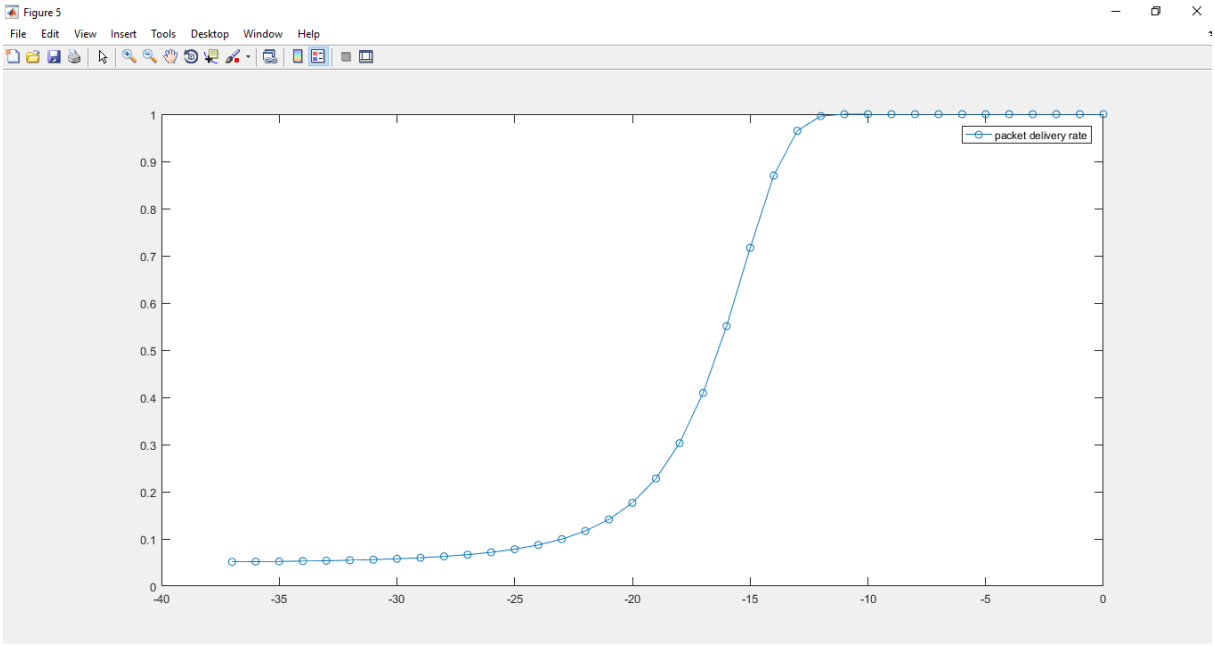


Figure 4.27: Packet Delivery Ratio

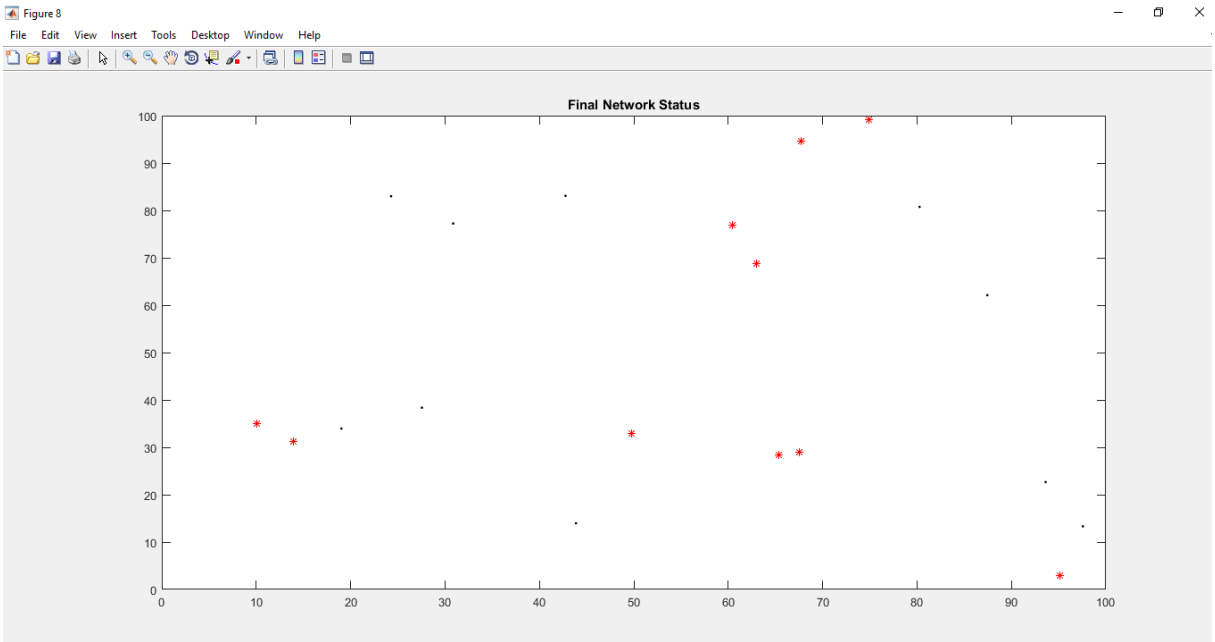


Figure 4.28: Network status after iterations

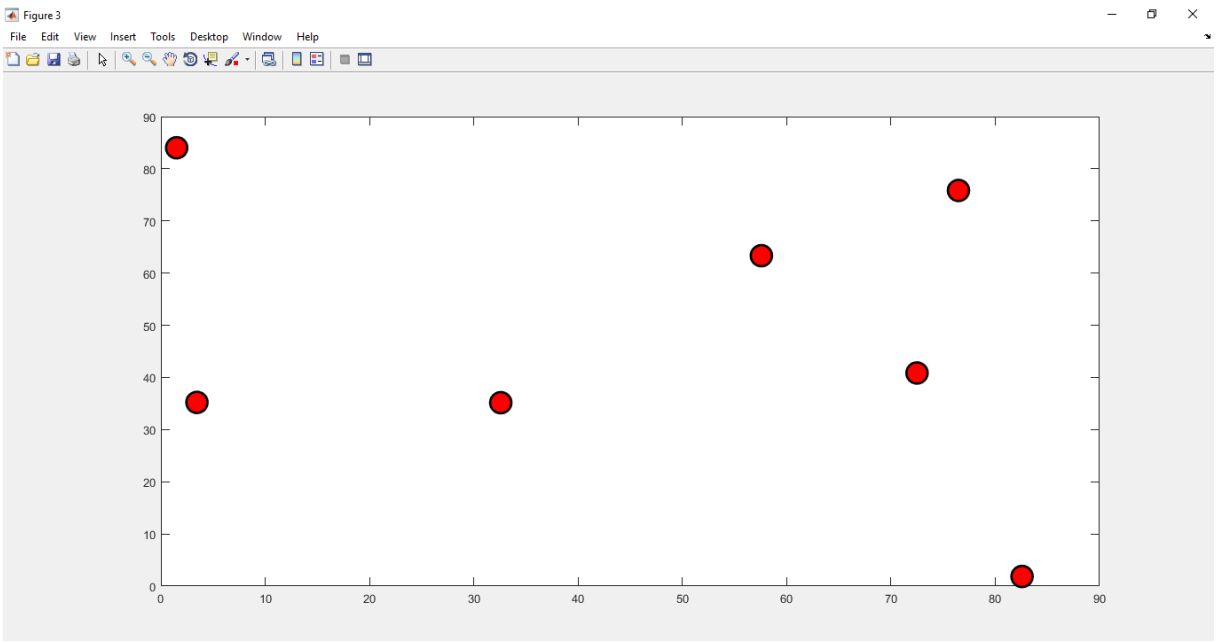


Figure 4.29: Detected Sink Hole Attacker Nodes

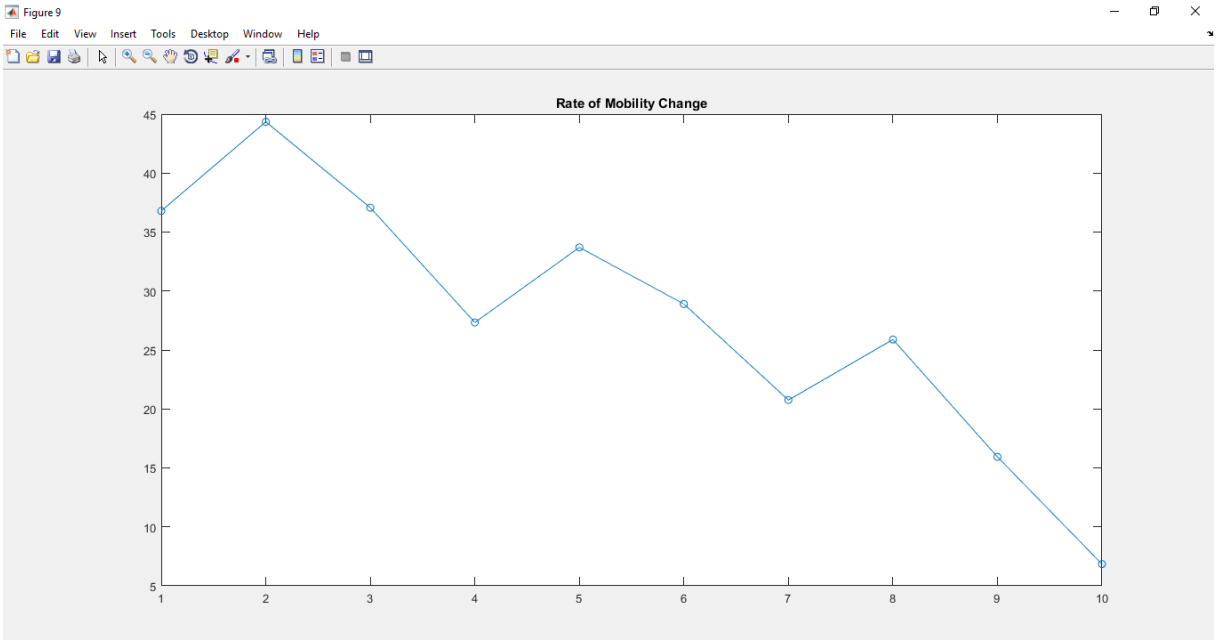


Figure 4.30: Rate of mobility Change

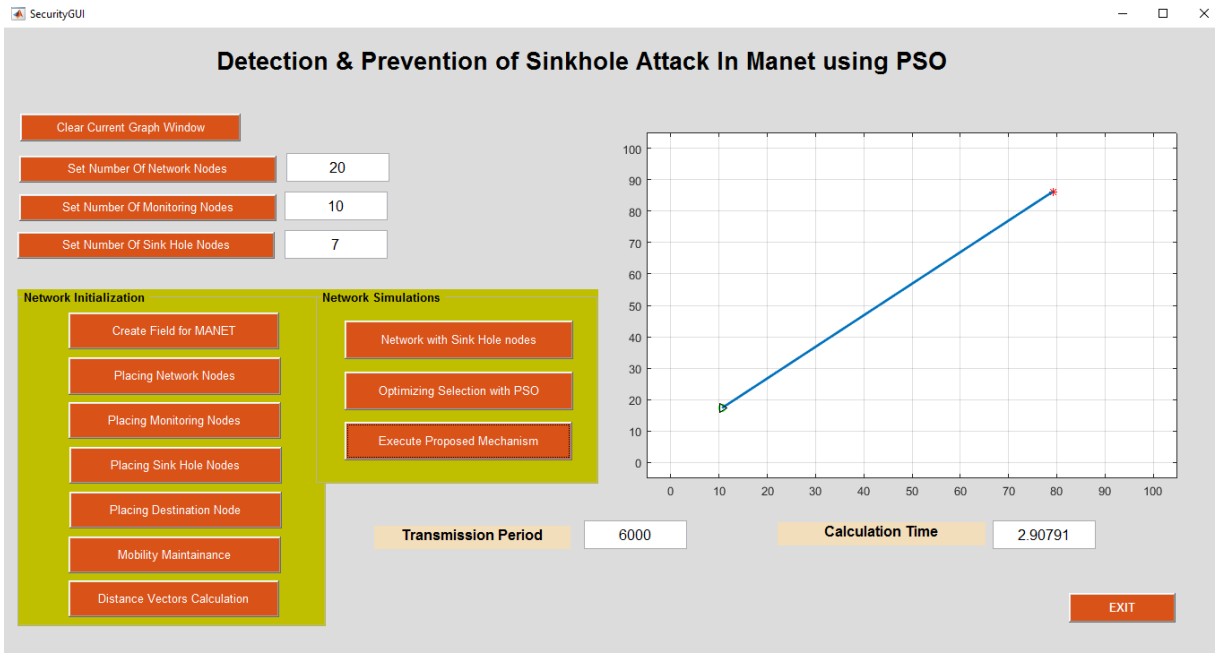


Figure 4.31: Transmission Period and Calculation Time

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

5.1 CONCLUSION

The Mobile Ad hoc Network (MANET) is a dynamic cost-effective network and provides communication with random movement of mobile nodes. The security is the major problem in this kind of decentralized network. The centralized administrator control absence is venerable to network from different attacks. In this research we study the sinkhole attack, security and normal routing in networks and find its affects.

MANETs are popular networks used broadly due to their dynamic nature. These types of networks are suffered from the sinkhole attack as there is no centralized security management. Here in this paper, we focus on to analyse and report sinkhole attack violation in Manet.

5.2 FUTURE SCOPE

In future there is possibility that more and more efficient routing protocols may come which will consider the security as important concern. Till now, routing protocol has mainly focused on the methods of the routing but in future a secured routing protocol could be made. To ensure both parameters will be a difficult task. So an intermediate of these two parameters could be searched in future.

REFERENCES

1. **Jeba veer singh jebadurai, Alfred raja melvin A, Immanuel john raja jebadurai**, "Sinkhole detection in mobile ad hoc network using mutual understanding among nodes". India. IEEE-2011.
2. **Kisung Kim and Sehun Kim**, "A Sinkhole Detection Method based on Incremental Learning in Wireless Ad Hoc Networks"
3. **C. Piro, C. Shields, and B. N. Levine,** "Detecting the Sybil attack in mobile ad hoc networks," in Proc. Securecomm Workshops, 2006, pp. 1–11
4. **Roopali Garg, Himika harma** "Proposed Lightweight Sybil Attack Detection Technique in MANET" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 3, Issue 5, May 2014
5. **Satyendra Singh, Vinod Kumar Yadav, Ganesh Chandra, & Rahul Kumar Gangwar,** " An Efficient and Improving the Security of AODV Routing Protocol" IJCST Vol. 3, Issue 1, Jan. - March 2012.
6. **Nidhi Joshi,Prof Manoj Challa,"**Secure Authentication Protocol to Detect Sybil Attacks in MANETs" International Journal of Computer Science & Engineering Technology (IJCSET), ISSN : 2229- 3345 Vol. 5 No. 06 Jun 2014
7. **Sohail Abbas, Madjid Merabti, David Llewellyn Jones, and Kashif Kifayat**," Lightweight Sybil Attack Detection in MANETs", IEEE systems journal, vol. 7, no. 2, June 2013.
8. **Yamini D Malkhede,Purnima Selokar** "ANALYSIS OF SYBIL ATTACK DETECTION IN MOBILE ADHOC NETWORK" Proceedings of 19 th IRF International Conference , 1st February 2015, Pune, India, ISBN: 978-93-84209-85-8.
9. **P.Kavitha, C.Keerthana, V.Niroja, V.Vivekanandhan,"** Mobile-id Based Sybil Attack detection on the Mobile ADHOC Network", International Journal of Communication and Computer Technologies Volume 02–No.02 Issue: 02 March 2014.
10. **Saurabh, ShekharTandanandPraneet**. "A PDRR based detection technique for blackhole attack in MANET.",2011.
11. **Nath, Ira, and DrRituparnaChaki.** "BHAPSC: A New SYBIL Attack Prevention System in Clustered MANET." International Journal of Advanced Research in Computer Science and Software Engineering 2012.

12. **Bhosle, Amol, TusharThosar and SnehalMehatre**. "Black-hole and wormhole attack in routing protocol AODV in MANET." International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol 2 (2012).
13. **Gagandeep, Aashima, Pawan Kumar**, "Study on Sinkhole Attacks in Wireless Ad hoc Networks", International Journal on Computer Science and Engineering (IJCSE), Volume-4, Issue-5, June 2012
14. **Rupinder Singh Brar and Harneet Arora,"** Mobile Agent Security issue in Wireless Sensor Networks ", Issue 1, January 2013(IJARCSSE).
15. **H. Shen and X.-G. Ye,** "Research on the location attack based on multiple counterfeit identities tech-nology in sensor networks," in 2014 International Conference on Wireless Communication and Sensor Network (WCSN), pp. 193-197, IEEE, 2014.
16. **J. Newsome, E. Shi, D. Song, and A. Perrig,** "The sybil attack in sensor networks: analysis & defenses," in Proceedings of the 3rd international symposium on Information processing in sensor networks, pp. 259- 268, ACM, 2004
17. **K.-F. Ssu, W.-T. Wang, and W.-C. Chang,** "Detecting sybil attacks in wireless sensor networks using neighboring information," Computer Networks, vol. 53, no. 18, pp. 3042- 3056, 2009.
18. **B. Tian, Y. Yao, L. Shi, S. Shao, Z. Liu, and C. Xu,** "A novel sybil attack detection scheme for wire-less sensor network," in 2013 5th IEEE International Conference on Broadband Network & Multimedia Technology (IC-BNMT), pp. 294-297, IEEE, 2013.
19. **M. A. B. Karuppiah and A. R. Prakash,** "Sybilsecure: An energy efficient sybil attack detection technique in wireless sensor network," International Journal of Information, vol. 4, no. 3, 2014.
20. **A. Vasudeva and M. Sood,** "Sybil attack on lowest id clustering algorithm in the mobile ad hoc network," International Journal of Network Security & Its Applications (IJNSA), vol. 4, no. 5, 2012.
21. **Sangeeta Bhatti,Prof Meenakshi Sharma,** "A Review of Sybil Attack in Mobile Ad-hoc Network" in International Journal of Advance Foundation And Research In Science & Engineering (IJAFRSE) Volume 1, Special Issue , ICCICT 2015.

22. **Faizan Khan ,Mayuri Sonar ,Mosmi Tiwari Vyas, "** A Survey Paper on Detection of Sybil Attack in MANET" in International Journal of Computer Networks and Wireless Communications (IJCNWC),Vol.6, No 1, Jan-Feb 2016.
23. **T. Saranya, A.Kumarave,** "Sybil attack detection in MANETS" in International Journal of Electronics and Communication Engineering Volume 3 November 2016.
24. **D. Sheela, Nirmala. S, Sangita Nath and Dr. G Mahadevan,** "A Recent Technique to Detect Sinkhole Attacks in WSN".
25. **Supriya Tayal, Vinti Gupta,"**A Survey of Attacks on Manet Routing Protocols,**"** in International Journal of Innovative Research in Science, Engineering and Technology Volume 2, Issue 6, June 2013.
26. **AA Gurjar, AA Dande,"**Black Hole Attack in Manet's: A Review Study", in International Journal of IT, Engineering and Applied Sciences Research (IJIEASR)Volume 2, Issue 3, March 2013,
27. **Tanu Preet Singh, Neha, Vikrant Das, "**Multicast Routing Protocols in Manets**",** in International Journal of Advanced Research in Computer Science and Software EngineeringVolume 2, Issue 1, January 2012.
28. **Ajay Sharma, Nithesh K. Nandha, Kailash Parik, Prof. K.P. Yadav,"**Survey of Secure Routing Protocols for MANETs", in International Journal of Research Review in Engineering Science and Technology (IJRREST)Volume 1, Issue2, September 2012.
29. **Ashwani Garg and Vikas Beniwal, "**A Review on Security Issues of Routing Protocols in Mobile Ad-Hoc Networks", in International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)Volume 2, Issue 9, September 2012.
30. **Rajneesh Narula and SumeerKhullar, "**Security Issues of Routing Protocols in MANETs", in International Journal of Computers & TechnologyVolume 3, Issue 2, 2012.
31. **Priyanka Goyal, Rahul Rishi, "**MANET: Vulnerabilities, Challenges, Attacks, Application", in International Journal of Computational Engineering & Management (IJCEM)Vol. 11, January 2011.
32. **Nital Mistry, Devesh C Jinwala, Mukesh Zaveri, "**Improving AODV Protocol against Blackhole Attacks**",** Proceeding of the International MultiConference of Engineers and Computer Scientists Volume 2, March 2010.

33. **Adnan Nadeem and Michael P. Howarth**, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE Communication Surveys & Tutorials, accepted for publication, 2013.
34. **K.Vaijayanthi , M.Baskar,** " Detecting and resolving the sybil attack in MANET using RSS algorithm " in International Journal of Computer Science and Mobile Computing november 2014.
35. **P. Raghu Vamsi and Krishna Kant,** " Detecting sybil attacks in wireless sensor networks using sequential analysis" in international journal on smart sensing and intelligent systems vol. 9, no. 2, june 2016
36. **Benjamin J. Culpepper, H.Chris Tseng,**" Sinkhole Intrusion Indicators in DSR MANET"
37. **Prabhjotkaur, Aayushi Chada , Sandeep Singh,** " Review Paper of Detection and Prevention of Sybil Attack in WSN Using Centralizedids" in International Journal of Engineering Science and Computing, July 2016.
38. **Manjunatha T. N, Sushma M. D, Shivakumar K. M,** "Security Concepts and Sybil Attack Detection in Wireless Sensor Networks" in international journal of emerging trends and technology in computer science April 2013.
39. **H. Shen and X.-G. Ye,** "Research on the location attack based on multiple counterfeit identities tech-nology in sensor networks," in 2014 International Conference on Wireless Communication and Sensor Network (WCSN), pp. 193-197, IEEE, 2014