

**Launching of a Sleep Deprivation Torture Attack on Mobility
based Clustering in Mobile Ad Hoc Networks**

Project Report submitted in fulfillment of the requirement for the
degree of Bachelor of Technology

In
Computer Science & Engineering

By

Vishal Verma (131309)

Under the supervision of
Mr. Amol Vasudeva

to



Department of Computer Science & Engineering and Information
Technology

**Jaypee University of Information Technology Waknaghat, Solan-
173234, Himachal Pradesh**

Candidate's Declaration

I hereby declare that the work presented in this report entitled “**Launching of a Sleep Deprivation Torture Attack on Mobility based Clustering in Mobile Ad Hoc Networks**” in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology in Computer Science and Engineering/Information Technology** submitted in the department of Computer Science & Engineering and Information Technology, Jaypee University of Information Technology Wagnaghat is an authentic record of my own work carried out over a period from August 2016 to December 2016 under the supervision of (**Amol Vasudeva**) (Assistant Professor (Grade-I), Computer Science & Engineering).

The matter embodied in the report has not been submitted for the award of any other degree or diploma.

Vishal Verma 131309

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

Amol Vasudeva

Assistant Professor (Grade-I),

Computer Science & Engineering

Dated:

Acknowledgement

I would like to express my deepest appreciation to all those who provided me the possibility to work on this B. Tech project. I am thankful for their aspiring guidance, invaluable constructive criticism and friendly advice during the project work. I am sincerely grateful to them for sharing their truthful and inspiring views on a number of issues related to the project.

I am especially grateful to **Mr. Amol Vasudeva**, Project Supervisor, for his valuable suggestions, support, and constant encouragement during the course of the project. The constant guidance and encouragement received from him have been of great help in carrying out the project work is acknowledged with reverential thanks. His perpetual energy, motivation, enthusiasm and immense knowledge inspired me to discipline myself in efficiently executing my multiple responsibilities simultaneously. He has given us the push that we need to go further and to do more. Therefore, we take this opportunity to express our sincere gratitude and thanks to him for lending his cooperation.

Date:

Vishal Verma(131309)

Table of Contents

Certificate		ii
Acknowledgment		iii
List of Abbreviations		vi
List of figures		v
List of Graphs		vi
List of Tables		vii
Abstract		ix
Chapter No.	Title	PageNo.
Chapter 1	Introduction	1
	<ul style="list-style-type: none">• Mobile Ad hoc Network (MANET)• Example scenario of MANETs• Application in battlefield• Limitation of MANETs• Routing in MANETs• Problem Statement• Objective• Methodology• Organization of report	

Chapter 2	Literature Review	11
	<ul style="list-style-type: none"> • Study of MANET: Characteristics, Challenges, Application and Security Attacks. • A Mobility Based Metric for Clustering in Mobile Ad Hoc Networks. • Sybil attack on lowest ID clustering algorithm in the mobile ad hoc networks. 	
Chapter 3	System Development	20
	<ul style="list-style-type: none"> • Algorithm to implement mobility clustering algorithm • Algorithm to Implement Sleep Deprivation torture attack in Mobility Based Clustering Algorithm • Design and development of the simulation environment. • Screen sort of the proposed work • Simulation environment parameters • Hardware requirement. • Software requirement. 	
Chapter 4	Simulation and Result Analysis	33
	<ul style="list-style-type: none"> • Complexity • Observation and result 	
Chapter 5	Conclusion and Future Work	43
	5.1. Conclusion	
	5.2. Future Work	
	References	45

List of Abbreviations

MANET	Mobile Ad hoc network
QoS	Quality of service
AODV	Ad hoc On –Demand Distance Vector Routing
UGV	Unmanned Grounded Vehicles
UAV	Unmanned aerial vehicle
DSR	Dynamic Source Routing Protocol
DSDV	Destination sequenced distance vector protocol

List of Figures

Figure No.	Figure Name	Page No.
1	MANETs Dynamic topology	1
2	Routing protocols for MANETs	4
3	Clustering based routing protocols.	6
4	Project life cycle	8
5	The home page of the simulator.	25
6	Simulation Area.	26
7	Nodes coordinates.	27
8	Adjacency Matrix.	28
9	Battery Status.	29
10	Cluster heads formation before the attack.	30
11	Cluster heads formation cluster after the attack.	31

List of Tables

Table No.	Table Name	Page No.
1	Proactive vs Reactive Routing Protocol.	5
2	Simulation parameters.	32
3	Cluster formation before Sybil attack.	36
4	Cluster formation after Sybil attack.	38
5	Percentage calculation of cluster head count	39
6	Percentage calculation of cluster head count with different transmission power	40
7	Percentage calculation of cluster head count with different Nodes speed	42

List of Graphs

Graph No	Graph Name	Page No
1.	Cluster head Count before and after Sybil attack	39
2.	Cluster head Count with different transmission Range	40
3.	Cluster head Count with different nodes speed	41

Abstract

A MANET consists of mobile nodes that can organize themselves dynamically in an arbitrary manner, without the need of a centralized administration. The nodes in a MANET are free to move while communicating with each other using either a single or multi-hop wireless links. As a result, the topology of the MANETs is dynamic in nature. Since the topology of this network is dynamically changing and there is no central management so it becomes difficult to implement security and this gives an opportunity to intrude into the network and exploit the weaknesses of the same.

Because of the fact that each node in the wireless ad-hoc network is aware of others nodes through messages over a broadcast communication channel, hence ad hoc networks are vulnerable to the various kinds of attacks.

Sleep deprivation attack is one such attack which takes the advantage of characteristics of MANET and disrupts the network. It is a kind of Sybil attack where malicious node illegitimately claims multiple identities and is able to repeatedly make the same node as the cluster head. Sleep deprivation attacks are a form of denial of service attack whereby an attacker renders a pervasive computing device inoperable by draining the battery more quickly than it would be drained under normal usage. If an attacker can drain a device's battery, for example, by having it repeatedly execute an energy-hungry program, called a sleep deprivation torture attack, or battery exhaustion. An attacker can quit attacking a battery-powered device once he/she has fully discharged the battery, and can then move on to attack another device. In addition to launching a Sleep deprivation attacks in this project we also aim to disrupt the head selection algorithm of the highest degree clustering protocol. We aim to introduce a malicious node into the network known as Sybil node, which would slowly take over as the head of the cluster by impersonating itself. Once the Sybil node becomes the head of the cluster, it can disrupt will disrupt the normal function of the network included routing. In this project, we visualize how a MANET works and the way clusters are formed. In addition, we see how the communication between the mobile devices occur and how the head of a cluster is selected. Once a MANET is established, we introduce a Sybil node which would impersonate itself and unsettle the system

CHAPTER 1

INTRODUCTION

1.1 Introduction

1.1.1 Mobile Ad hoc Networks

Mobile Ad hoc Networks is a network without any fixed and centralized infrastructure. In such type of network, nodes are mobile in nature. Therefore, the topology of the network is also dynamic in nature. In such type of network, it is expensive or very difficult to use dedicated routers for routing and packet forwarding purpose. Therefore, each node is capable of acting as a router as well as a host node.

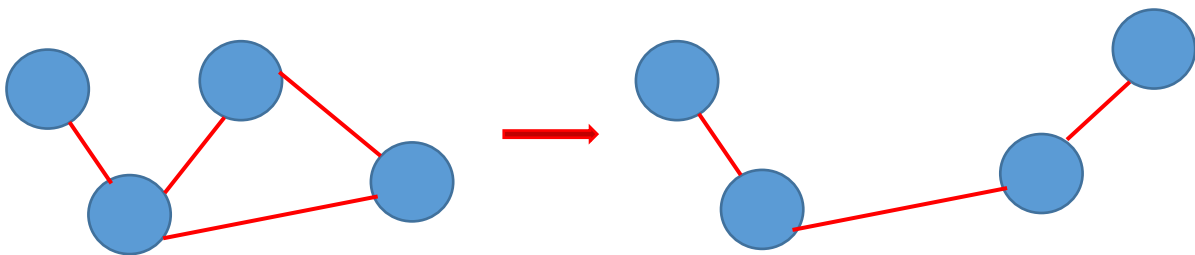


Figure 1: MANETs Dynamic Topology

1.1.2 Example Scenario for MANETs

- Military or Battlefield Purpose
Unmanned Grounded Vehicles (UGV)
Unmanned aerial and underwater vehicle
Communication purpose
- Disaster-affected areas
Communication purpose
Search and rescue

- Other Purposes
 - Personal area network (PAN)
 - Taxi network in a city
 - Wireless sensor network

1.1.3 MANETs in Battlefield as Unmanned Grounded Vehicles(UGV)

Unmanned Ground Vehicles (UGV) is one of the trending topics of Research and Development in Military. Today Unmanned Ground Vehicles (UGV) really became a game changer in a battlefield. Unmanned aerial vehicle (UAV) and unmanned underwater vehicle (UUV) are the counterparts of UGV for air and water respectively. However UGV cannot able to replace human and traditionally weapon from battlefield completely, but the presence of UGV in military operations can do a great deal to help out soldiers like taking images of an enemy held-area , tracking and sensing enemy's activity or tracking and detonating a mine etc. The main application of UGV is to provide safety to military and security personnel from all possible threat and minimize the causality.UGVs provide enhanced information of the hostile environment like fire, harsh weather, biological, chemical and radiological contaminated area which allow army to make effective strategy. Secondly, UGVs will be employed to transport ammunition, food and medical supplies in military combat mission. Thirdly, UGVs can be built smaller so that they can go to such places where manned vehicles with some crew members not able to go.

Teleoperation technology is the most mature method to control UGV remotely by human operator from a safe location via some radio link. However, this technology alone do very little to fulfill the actual objective of UGVs. Teleoperation required large no of operators to control all UGVs used in military combat mission. Secondly, UGVs can be used for longer operations and teleoperations of UGVs for such operation is difficult. Autonomous technology does a much better job in such scenario. Autonomous UGVs operate without the need for a human controller. Such vehicles contain sensors to understand the environment and some controlling algorithm to take essential steps to complete the task. Autonomous UGVs usually work for longer periods as compare to teleoperations UGVs.

Therefore for such Autonomous UGVs MANETs is the perfect networking model for operating.

1.1.4 Limitations of MANETs

Despite of having so many applications of MANETs in Battlefield or disaster affected area etc. There are a lot of challenges and limitations of MANETs. Some of the limitations are:

- Loss of packets during transmission due to variable communication bandwidth and frequently disconnections of the communication link.
- Since the topology of the network dynamic in nature, hence there is a lack of awareness of the topology among the nodes of network.
- Mobile nodes usually have limited resource like small battery life and limited computation capabilities and small memory.
- Routing is one the main challenge of MANETs

1.1.4 Routing in MANETs

As we already discussed in the previous section that due to mobile nature of the nodes and the absence of the fixed infrastructure routing is one of the main challenges in MANETs. Routing is the process of selecting the route for packet delivery from source node to destination node in a network. Today routing is one of a topic of great interest among researcher and until today many routing protocols for MANETs has suggested. Routing protocols broadly differentiated into three categories. These are:

- Proactive Protocols
- Reactive Protocols
- Hybrid Protocols

1.1.5 Routing Protocols for MANETs

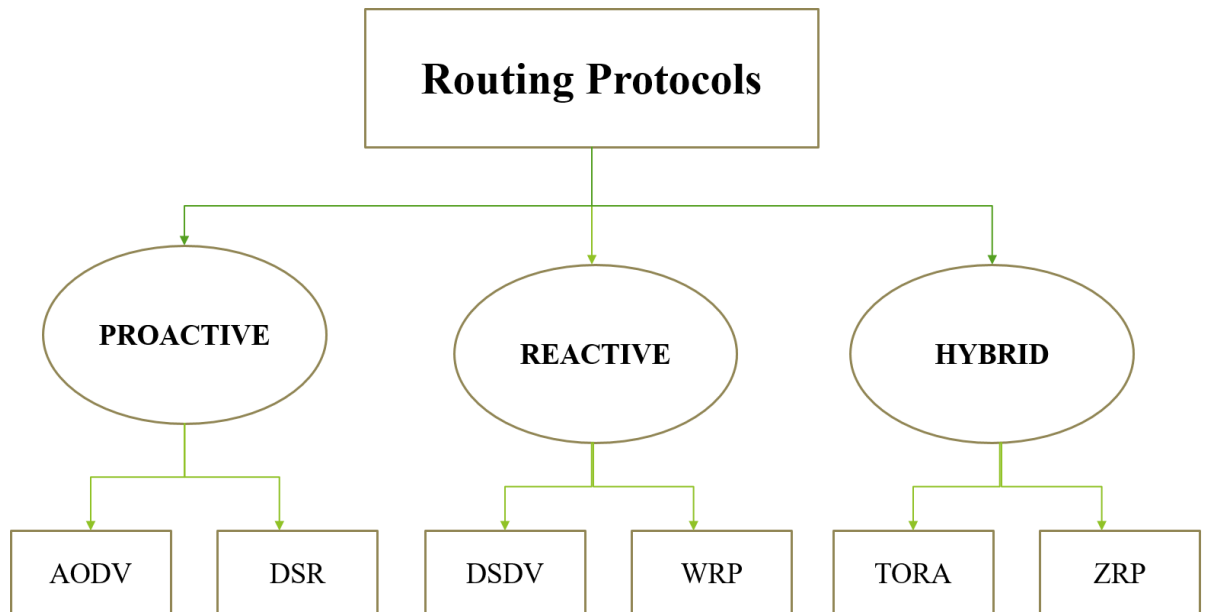


Figure 2: Routing Protocols for MANETs

1.1.5.1 Proactive Routing Protocol

In Proactive Routing Protocol, each node maintains a routing table containing the information of the optimal path from that node to every possible node in that network. Periodically each node shares its routing table with its neighboring node to update its routing table. In this type of routing protocol, source node defines the complete route of the data packet to its destination. The intermediate nodes do not affect the route of the data packet. As we already discussed in the previous section that the mobile nodes in MANETs usually have limited memory and computational power. Therefore, to maintaining the routing table is really an overhead for nodes in MANETs. This type of routing protocols effected only in small network. However, for bigger networks, we need some more advanced routing protocols.

Some of the Proactive Routing Protocols are:

- Ad hoc On-Demand Distance Vector Routing Protocol
- Dynamic Source Routing Protocol

1.1.5.2 Reactive Routing Protocol

In Reactive Routing Protocol, instead of storing and maintaining the routing table for every node in the network each node maintain the information of the path to its neighboring nodes only. When source node wants to send data packet to destination node, it broadcast the packet to its neighboring node and neighboring node further forward packet to its neighboring. This process continues until the packet does not reach its destination. The main advantage of this routing protocol is that there is no overhead to maintaining the routing table and hence this routing protocol can be applicable in big networks. In addition, this routing protocol also affected is case of node failure. One of the biggest disadvantages of this routing protocol is excess traffic in network, which leads to network congestion.

Some of the Reactive Routing Protocol are:

- Destination sequenced distance vector protocol
- Wireless Routing Protocol

Comparison between Proactive and Reactive Routing Protocol

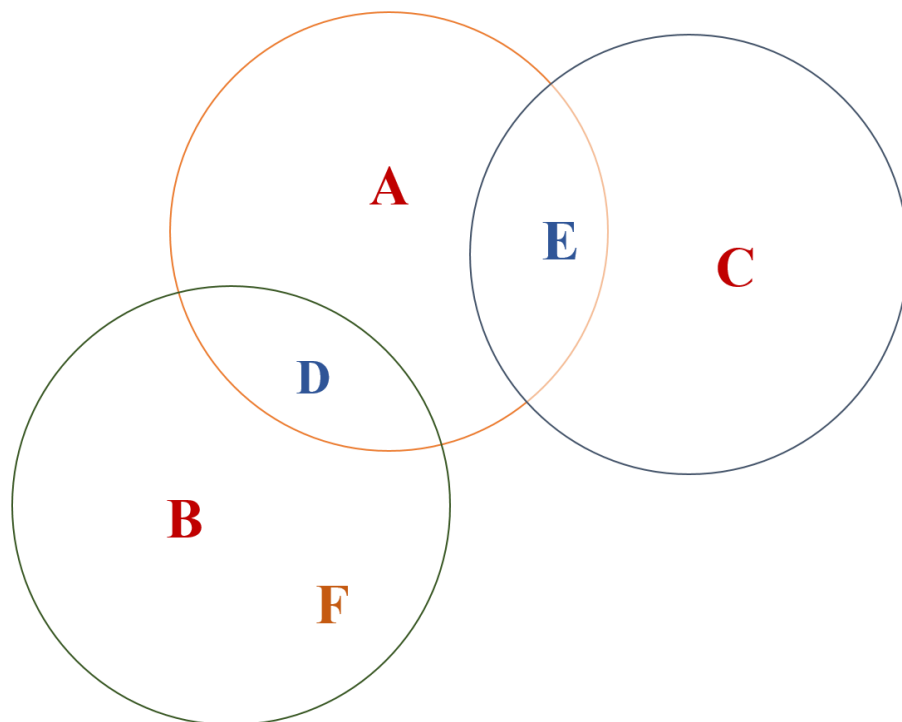
	PROACTIVE	REACTIVE
Routing Overhead	High	Low
Storage	High	Low
Advertisement	Periodic	When needed
Network Size	Small	Moderate
Network congestion	Low	High

Table 1: Proactive vs Reactive Routing Protocol

1.1.5.3 Hybrid Routing Protocol

Hybrid Routing Protocol is a combination of Reactive and Proactive routing protocol. Since the proactive and reactive routing protocol does not perform well in large networks therefore to handle such networks, some type of hierarchical organization structure is required. Clustering based routing protocol is one of such protocols to handle such large MANETs. In Clustering based routing protocol, the whole network is divided into small clusters on the basis of some clustering algorithm. In this type of routing protocol, each node is classified into four categories:

- Cluster head
- Normal node
- Intermediate node or Gateway node
- Isolated node



{A,B,C} - Clusterhead

{D,E} - Intermediate Node or Gateway Node

{F} - Normal Node

Figure 3: Clustering Based Routing Protocol

1.2 Problem Statement

As we already discussed some of the characteristic and limitation of the MANETs are:

- Its Broadcast channel for communication
- Lack of central control
- Limited computational, battery and memory resource

All these limitations and characteristic of MANETs make it vulnerable to various type of attack. **Sleep deprivation torture attack** is one of such attack on MANETs. Sleep deprivation torture attack is a type of Sybil attack where one Sybil node with multiple logical identities tried to affect the network topology or the normal functioning of the network.

This project is to implement the **Launching of a Sleep deprivation torture attack on Mobility based Clustering in Mobile Ad Hoc Networks**. This project needs to develop a simulator where we can simulate the MANETs, implement Mobility based clustering algorithm and then implement the attack.

Mobility based clustering algorithm take relative mobility of nodes with respect to its neighboring node as a measure for the formation of cluster. Then each node calculates the variance of relative mobility values of all its neighboring nodes. A node with lowest variance value selected as cluster head. The aim of this project is to disrupt the cluster formation using sleep deprivation torture attack.

Sleep deprivation torture is a form of denial of service Attack (DoS), where the aim of attacker is to drain the battery of any target node more quickly than normal usage. In this attack, we tried to disrupt the mobility based clustering algorithm by inserting the malicious node. The objective of malicious node is to make the same node as cluster head repeatedly. In mobility based clustering algorithm, node with lowest variance value M_V is chosen as cluster head. The idea of this attack is to decrease the variance of legitimate node and hence increase the chance of that node to become a cluster head. The cluster head works as a router for its cluster and routes the packets from its cluster member (source) to another node (destination). The cluster head also plays an important role in managing the cluster and its resources. Because cluster head performs more complex task than other cluster members do hence consume more power

1.3 Objective

- To analyze the performance of Mobile ad Hoc Network on simulated environment
- To implement a clustering algorithm in MANET.
Eg highest degree clustering algorithm
- To study the effects and consequences of a Sleep Deprivation Torture Attack on Mobile Ad-hoc Network
- Implementation of a Sleep Deprivation Torture Attack on Mobile Ad-hoc Network in Python-based modules like Pygame, Tkinter, Tk, Ttk etc.

1.4 Methodology

The following describes the Project Implementation Methodology employed in the implementation of projects. This will cover the detailed explanation of methodology that is used to make this project complete and working well.

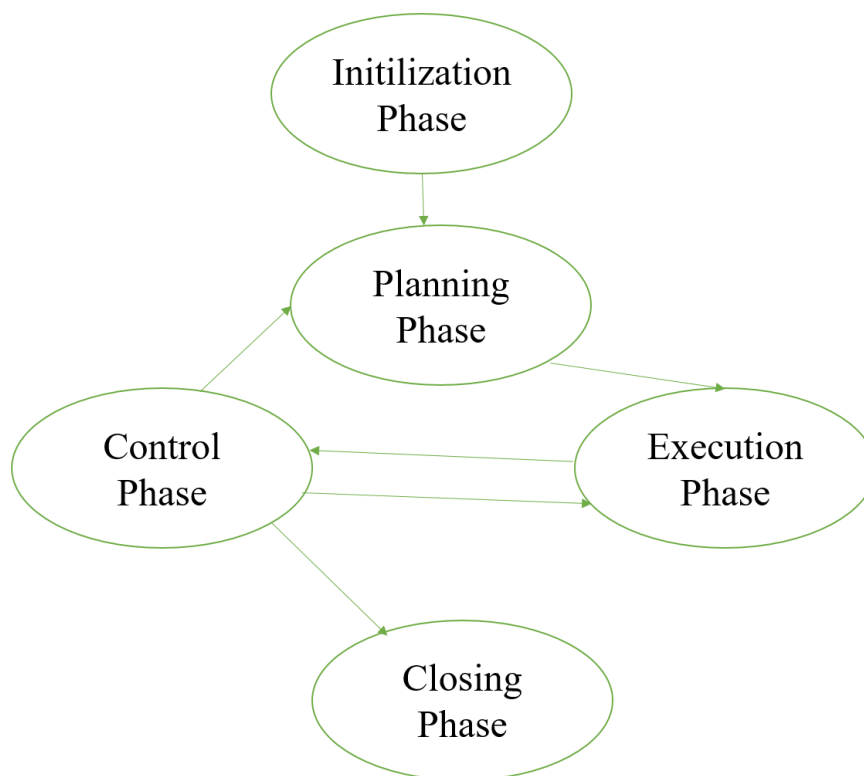


Figure 4: Project Life Cycle

Project Life Cycle

1. Initialization Phase

- Initial meetings with project Supervisor
- Discussing the issue, background and related work to project

2. Planning Phase

- Studying and investigated the research papers, journals, and other related work
- Planning of the requirement (software and hardware)
- Project scheduling

3. Execution Phase

- Design the project
- Implement the Project

4. Control and Analysis Phase

- Analysis the performance
- Test the project with given test cases

5. Closing Phase

- Complete the project
- Submission of report

1.5 Organization

Chapter1 highlights and underlines the MANET, its characteristics, advantages, limitations and challenges. This chapter also discussed various security issues with MANET and then the various routing protocol along with clustering are discussed.

Chapter 2. The detailed literature review from the research paper, books, journals and conferences done in this chapter. The research papers on MANETs, Mobility based Clustering algorithm and Sybil Attacks considered in this chapter.

Chapter 3 covers the system development, which is the key aspect of this work. This chapter emphasized on the design, algorithm used and the implementation of our application. Screenshots used to depict and defend the proposed work.

Chapter 4. In this chapter, the simulation results, observations and relative performance analysis shown.

Chapter 5 ends with the detailed conclusion of our work and scope for the future work, which guides the upcoming students and research scholars to enhance the current work with higher efficiency and effectiveness.

Chapter 2

LITERATURE SURVEY

For the completion of this project, a number of research papers, books, and online websites studied and investigated thoroughly. In this chapter, the extract of all those research paper and journals defined in detail. This chapter includes the content, formula used and the result of the research papers and journals in detail.

2.1 Study of MANET: Characteristics, Challenges, Application and Security Attacks by Aarti, Dr. S.S. Tyagi [2]

MANETs

MANETs is a Collection of independent mobile nodes, works without any fixed infrastructure, having dynamic network topology and no centralized control.

Some of the Characteristics of MANETs are:

- Distributed in nature
No centralized control
Task distributed among nodes
- Multi-hop Routing
The data packet may me travel through many intermediate nodes before reaching its destination.
- Dynamic topology
Since nodes are mobile in nature, therefore, topology of the network is dynamic in nature
- Lightweight terminals
Mobile nodes having low resources like computational power, battery and storage memory
- Share Same Physical Medium

Use broadcast channel as the medium of communication, which is shared by all the nodes.

Advantage of MANETs

- Applicable at any geographical location
- Independent from central control
- Scalable and Flexible in nature
- Robust

Challenges of MANETs

- **Limited bandwidth**
Due to infrastructure less network and nodes having limited resources, MANETs having lower capacity
- **Dynamic Topology**
Dynamic topology effect the routing of the data packets
- **Resources constraints**
Mobile nodes having limited resources like battery, CPU, memory

Application of MANETs

- Used in military
- Used as Personal Area Network
- Used in commercial Sector

Vulnerabilities of MANETs

Some of the Vulnerabilities of the MANETs are

- **Lack of centralized management**
MANETs does not have centralized control. All operations are distributed in nature in MANETs
- **No predefined Boundary**
There are no fixed boundaries for ad hoc network. Any node is free to join and leave the network
- **Cooperativeness**
Each node is cooperative in nature.Cooperation is required for routing and other tasks, because MANETs are distributed is nature.

- Limited power supply

MANETs nodes having limited resources included power supply

2.2 A Mobility Based Clustering in MANETs by P.Basu, N.Khan, and T.D.C. Little [1]

Clustering is an important technique to provide some kind of hierarchical and organization structure to MANETs. Some kind of clustering algorithm is required for the formation of cluster. Some of the already been proposed algorithm in the past are Lowest-ID based clustering where cluster head is selected on the basis on lowest Id.

The author of this paper found that mobility of nodes is the main cause of cluster head selection and cluster formation. Therefore author suggests considering relative mobility of nodes as the measure of cluster formation. A node with least mobile among its neighboring nodes selected as cluster head. This clustering algorithm forms more stable cluster compare to Lowest ID based clustering algorithm. This mobility based clustering algorithm reduces the cluster head change up to 33% over the Lowest ID based clustering algorithm.

2.2.1 Mobility Based Clustering Algorithm

In mobility based clustering algorithm, each node finds its relative mobility with respect to its neighbors and then maintains relative mobility metrics M^{rel} . A node with n neighbors having n such values for M^{rel} . Then, we calculate the aggregate local mobility value M_Y i.e. the variance (with respect to zero) of the entire set of relative mobility values M^{rel} . A node with a low value of M_Y means that node is relative less mobile with respect to its neighbor. Hence, node with low M_Y value among its neighbors is chosen as cluster head.

Steps to calculate the aggregate local mobility value M_Y :

1. Each node broadcast and receive two successive *Hello* messages to/from its neighbors.
2. Receiving power of *Hello* messages received at every node is inversely proportional to square of distance between them and directly proportional to transmission power of hello message

$$\frac{Pr}{Pt} \propto \frac{1}{R^2}$$

Where Pr is receiving power of *hello* message.

Pt is the transmission power of hello message.

R is the distance between two nodes.

3. Then the relative mobility matrix $M_Y^{rel}(X)$,at a node Y with respect to X is calculated as

$$M_Y^{rel}(X) = 10 \log_{10} \left(\frac{RxPr^{new}}{RxPr^{old}} \right)$$

Where $RxPr$ is the receiving power.

4. If $RxPr^{new} < RxPr^{old}$ then $M_Y^{rel} < 0$ and this means that two nodes are moving away from each other

If $RxPr^{new} > RxPr^{old}$ then $M_Y^{rel} > 0$ and this means that two nodes come close to each other.

Else if $RxPr^{new} = RxPr^{old}$ then $M_Y^{rel} = 0$ and this means that two nodes are stable to each other or relative mobility between two nodes is zero.

5. Finally, the aggregate local mobility value M_Y is calculated as

$$M_Y = var(M_Y^{rel}(X_1), M_Y^{rel}(X_2), M_Y^{rel}(X_3) \dots \dots M_Y^{rel}(X_n))$$

2.2.2 Implementation of MOBIC - A Lowest Relative Mobility Clustering Algorithm.

MOBIC is similar to Lowest ID based clustering algorithm except that it choose relative mobility of the nodes as the measure of clustering.

Steps involved in MOBIC

1. Each node broadcast and receive two successive *Hello* messages to/from its neighbors.
2. Each node calculate the receiving power of *Hello* messages using this equation

$$\frac{Pr}{Pt} \propto \frac{1}{R^2}$$

Where Pr is receiving power of *hello* message.

Pt is the transmission power of hello message.

R is the distance between two nodes.

3. Each node finds its relative mobility with respect to its neighbors and then maintains relative mobility metrics M^{rel} . A node with n neighbors having n such values for M^{rel} . Then, we calculate the aggregate local mobility value M_Y i.e. the variance (with respect to zero) of the entire set of relative mobility values M^{rel}
4. Now each node broadcast its aggregate local mobility value M_Y to its neighboring nodes. If the node has the lowest M_Y value among its neighboring nodes than it is selected as cluster head otherwise as cluster member.
5. Any node that became a cluster member of two clusters considers as intermediate node or gateway node.
6. If the M_Y value of two nodes is same than the cluster head is done on the basis of lowest ID based clustering algorithm
7. Any node that not able to become a part of any cluster also consider as cluster head.

2.3 SYBIL ATTACK ON LOWEST ID CLUSTERING ALGORITHM IN THE MOBILE ADHOC NETWORK by Amol Vasudeva and Manu Sood [3]

Security is one of the main issues with MANETs. Some of the characteristics of MANETs like:

- No centralized control
- Broadcast nature of communication
- Limited resources

that make it difficult to achieve security goal in MANETs

In this paper, the author takes advantage of these MANETs limitations and implement the Sybil attack, on Lowest Id based clustering algorithm.

In this attack, one malicious node with multiple identities disrupts the cluster formation and cluster head selection in Lowest Id based clustering algorithm.

2.3.1 Sybil Attack

Sybil attack is the type of attack where single physical device with multiple identities tried to control the network performance and functioning. Sybil attack is effective in distributed network because there is no central control to verify the Ids generated by malicious node.

2.3.2 Dimension of Sybil Attack

There are three dimensions of Sybil Attack

1. Communication

- Direct Communication
Sybil nodes communicate with the legitimate nodes directly.
- Indirect Communication
Sybil nodes communicate with the legitimate Node via malicious node.

2. Participation

- Simultaneous Participation
Attacker participates with all his identities at once.
- Non-Simultaneous
Attacker participates with a large number of identities over a period of time.

3. Identity

- Fabricated Identity
The attacker creates arbitrary new identities for Sybil nodes.
- Stolen Identity
Attacker assigns legitimate identities to Sybil nodes.

2.3.2 Effect Sybil Attack in Mobile Ad Hoc Networks

- Data Aggregation
- Fair Resource Allocation
- Voting
- Routing

2.3.3 Lowest –ID Based Clustering Algorithm

In Lowest Id based clustering algorithm, Ids of the nodes is the measure for the formation of cluster and selecting cluster head. Periodically each node broadcast its Id to its neighboring nodes. If the node has the lowest Id among its neighboring that it is selected as cluster head otherwise node became a cluster member node.

Advantage of Lowest ID based clustering Algorithm

- Simple to implement
- Fast in terms of cluster formation
- System performance is high because rate of change of cluster head is low.

Disadvantages of Lowest ID based clustering Algorithm

- A node with Lowest Id always became the cluster head with result to drainage of battery faster than other nodes.

2.3.4 Sybil Attack on Lowest –ID Based Clustering Algorithm

The cluster head is the most import part of cluster in clustering algorithm. The cluster head is responsible for routing, resource management, storage and maintaining cluster information. Because cluster head performs much more complex task than other member nodes hence drained battery faster than other nodes. The aim of this Sybil attack is to disrupt the cluster head selection and cluster formation and the implement of this Sybil attack in done in two ways.

Firstly malicious node uses lowest id in the network to became the cluster head so that it can gain the information of the cluster.

Secondly, malicious node tried to make the same target node as cluster head again and again so that it can drain battery faster than other nodes.

2.3.4.1 Step to implement Sybil attack on lowest Id based clustering algorithm by becoming cluster head.

1. Malicious node introduces a Sybil node such that its ID is minimum in the network.

2. Malicious node broadcast hello message to its neighboring nodes with its lowest ID
3. Since the Id of malicious node is always less than its neighboring nodes, therefore each time malicious node selected as cluster head.
4. After selected as cluster head, the malicious node stole all the information of the cluster so that it can use that against them.

2.3.4.2 Step to implement Impersonation based Sybil Attack on lowest id based clustering algorithm.

1. After gaining the information of the cluster, the malicious node introduced n Sybil nodes with different Ids such that Ids of Sybil nodes always remain larger than legitimate nodes Ids.
2. To remain undetected each Sybil node broadcast hello messages with different transmission power. Let the malicious node generates n Sybil nodes ($n < N$) with different IDs represented as $s_1, s_2, s_3, s_4, \dots, s_n$. Then the transmission power of such nodes are $TxPr(s_1) > TxPr(s_2) > TxPr(s_3) \dots \dots > TxPr(s_n)$
3. Now, the malicious node selects the target node and follow the direction of target node.
4. During cluster formation, the Id of target node always remains less than Sybil nodes. Hence, target node always selected as cluster head.
5. Since the cluster head performs much more complex task than other member nodes hence the battery of target node drained faster than other nodes.

2.3.5 Detection technique of Sybil Attack on Lowest –ID Based Clustering Algorithm

- Resource testing

Cluster head tests the computational power of member nodes by assigning them some task. Since the Sybil nodes having only one physical device hence there, computational power is divided equally among them. Therefore, computational power of Sybil nodes is less than other legitimate nodes.

- Fixed radio channel allocated

Cluster head Allocate fixed channel to every member nodes to communicate. If the member node uses same channel to sending and receiving packets than it is legitimate node otherwise it is a Sybil node.

CHAPTER 3

SYSTEM DEVELOPMENT

3.1 Algorithm to Implement Mobility Based Clustering Algorithm

1. Each node broadcast and receive two successive *Hello* messages to/from its neighbors.
2. Each node calculate the receiving power of *Hello* messages using Friis transmission equation

$$\frac{Pr}{Pt} = GtGr\left(\frac{\lambda}{4\pi R}\right)$$

Where Pr is receiving power of *hello* message.

Pt is the transmission power of hello message.

Gt and Gr are the gain of transmission and receiver antenna respectively.

λ is the transmission wavelength.

R is the transmission range.

3. Then the relative mobility matrix $M_Y^{rel}(X)$, at a node Y with respect to X is calculated as

$$M_Y^{rel}(X) = 10\log_{10}\left(\frac{RxPr^{new}}{RxPr^{old}}\right)$$

Where $RxPr$ is the receiving power.

4. Finally, the aggregate local mobility value M_Y is calculated as

$$M_Y = var(M_Y^{rel}(X_1), M_Y^{rel}(X_2), M_Y^{rel}(X_3) \dots \dots \dots M_Y^{rel}(X_n))$$

5. Now each node broadcast and receive the aggregate local mobility value M_Y to /from its neighboring nodes.
6. A node with lowest aggregate local mobility value M_Y value among its neighboring nodes selected as cluster head of a cluster.
7. All the neighboring nodes of the cluster head became the member of that cluster.
8. Any node that is not able to become a part of any cluster also became a cluster head and all the neighboring nodes became the member nodes.
9. Nodes that became a part of more than two clusters consider as intermediate node or Gateway node.
10. The whole process repeats itself after fixed interval of time.

3.2 Algorithm to Implement Sleep Deprivation torture attack in Mobility Based Clustering Algorithm

We are going to implement Sleep Deprivation torture attack in Mobility based clustering algorithm in two different ways.

- In the first method, the aim of malicious node is to decrease the aggregate local mobility value M_Y of target node that increases the chance of target node to become the cluster head.
- In the Second method, the aim of malicious node is to increase the aggregate local mobility value M_Y of all neighboring nodes and decrease its aggregate local mobility value M_Y that increase the chance of malicious node to become the cluster head.

Assumption

1. Nodes are very mobile in nature.
2. Malicious node is able to transmit Hello message with different transmission power.
3. Malicious node is able to generate many logical IDs to implement Sybil Attack.

4. A malicious node having very large battery life, large computation capabilities and large memory storage compare to other nodes in the network.

3.2.1 Algorithm to Implement Impersonation based Sleep Deprivation torture attack in Mobility Based Clustering Algorithm.

1. Let there are N number of nodes in an ad hoc network at any instance of time moving randomly with cluster IDs as:

$$x_i: i = 1, 2, 3, 4 \dots \dots n$$

2. Now we insert our malicious node into the network that is able to generate Sybil nodes with different IDs such as:

$$x_i: i = n + 1, n + 2, n + 3, \dots \dots m$$

3. In the next step, the malicious node selects its target node among N nodes and follow the direction of the target node.
4. In cluster formation process, malicious node broadcast many hello messages with different IDs and different transmission power.

Let the malicious node generates n Sybil nodes ($n < N$) with different IDs represented as $s_1, s_2, s_3, s_4 \dots s_n$. Then the transmission power of such nodes are $TxPr(s_1) > TxPr(s_2) > TxPr(s_3) \dots \dots > TxPr(s_n)$

5. The variation in transmission power helps malicious node to remain undetected because the receiving power of hello message is calculated as

$$\frac{Pr}{Pt} = GtGr\left(\frac{\lambda}{4\pi R}\right)$$

And to convince the target node that all Sybil nodes are different, we need to vary the receiving power of every hello message from malicious node. Since the distance between target node and malicious node always remain same as they always move together. Hence, to vary the receiving power we need to vary the transmission power.

6. Since the receiving power $RxPr$ of successive hello message from each Sybil node at target node always remain same (or small variation). Hence, the M^{rel} of target node with respect to Sybil nodes always remain zero(or very small).
7. For the cluster head formation the last step is to calculate the aggregate local mobility value M_Y :

$$M_Y = var(M_Y^{rel}(X_1), M_Y^{rel}(X_2), M_Y^{rel}(X_3) \dots \dots M_Y^{rel}(X_n))$$

Since M^{rel} for target node with respect to Sybil nodes is zero, hence the variance of target node decreases which increase the chance of target node to become the cluster head.

3.2.2 Algorithm to Implement Sleep Deprivation torture attack for disruption of Mobility Based Clustering Algorithm.

1. Let there are N number of nodes in an ad hoc network at any instance of time moving randomly with cluster IDs as:

$$x_i: i = 1, 2, 3, 4 \dots \dots n$$

2. Now we insert our malicious node into the network that is able to generate Sybil nodes with different IDs such as:

$$x_i: i = n + 1, n + 2, n + 3, \dots \dots m$$

3. In cluster formation process, malicious node broadcast hello messages with different IDs and with different transmission power.

Let the malicious node generates n Sybil nodes ($n < N$) with different IDs represented as $s_1, s_2, s_3, s_4 \dots s_n$. Then the transmission power of such nodes are $TxPr(s_1) > TxPr(s_2) > TxPr(s_3) \dots \dots > TxPr(s_n)$

4. The variation in transmission power helps malicious node to remain undetected because the receiving power of hello message is calculated as

$$\frac{Pr}{Pt} = GtGr\left(\frac{\lambda}{4\pi R}\right)$$

And to convince the target node that all Sybil nodes are different, we need to vary the receiving power of every hello message from malicious node. Since the distance between target node and malicious node always remain same as they always move together. Hence, to vary the receiving power we need to vary the transmission power.

5. Unlike the impersonation-based attack, in this attack transmission power, $TxPr$ of two successive hello message from each Sybil node also vary. Therefore, the receiving power $RxPr$ of successive hello messages at all neighboring nodes also varies. Hence, the relative Mobility M^{rel} of all neighboring nodes with respect to Sybil nodes also varies.

6. For the cluster head formation the last step is to calculate the aggregate local mobility value M_Y :

$$M_Y = var(M_Y^{rel}(X_1), M_Y^{rel}(X_2), M_Y^{rel}(X_3) \dots \dots M_Y^{rel}(X_n))$$

Since M^{rel} of all neighboring nodes with respect to Sybil nodes increases, hence the variance of all neighboring nodes of malicious node also increases.

However, the relative mobility of the Sybil nodes with respect to each other always remain zero (as they all are same physical node). Hence, the variance or aggregate local mobility value M_Y of malicious node decreases which increase the chance of malicious node to become the cluster head.

3.3 Design and development of Simulation Environment for the implementation of clustering algorithm and attacks.

Python used as the Programming Language for the development of the application to simulate the complete ad hoc network. Mainly two python based modules used for the development of this simulator.

- Tkinter

Used for development of Graphical User Interface (GUI)

E.g. Button, Menu Bar, Display Window

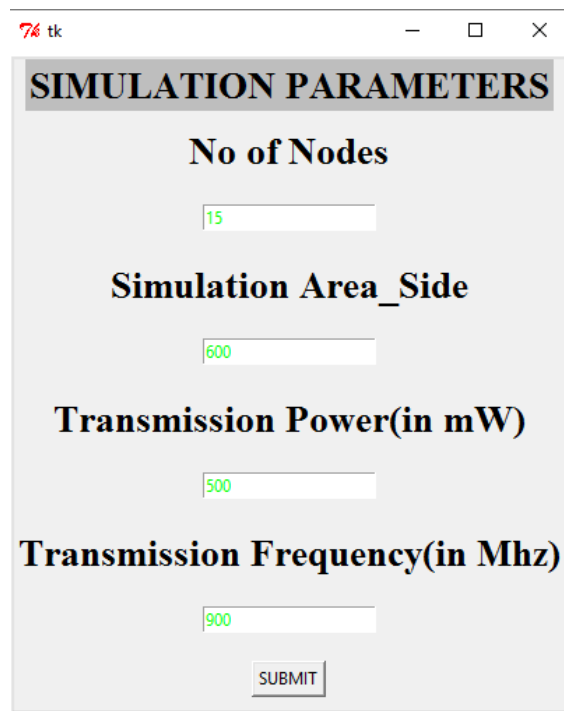
- Pygame
Used to design the rest of the simulation environment
E.g. Nodes

3.4 Screen sort of the proposed work

3.4.1 Home Screen:

The home screen will be shown to the user whenever he runs the python code.

The home screen asks for simulation parameters for the simulation environment. The input parameter includes no of nodes, side length of simulation area, transmission power of node and the transmission frequency of the nodes.



The image shows a screenshot of a Tkinter window titled "7% tk". The window contains a form titled "SIMULATION PARAMETERS" with the following fields and values:

Parameter	Value
No of Nodes	15
Simulation Area_Side	600
Transmission Power(in mW)	500
Transmission Frequency(in Mhz)	900

A "SUBMIT" button is located at the bottom of the form.

Figure 5: Home Page of the simulator

3.4.2 Simulation Area:

After the successful submission of the simulation parameters, the simulation area will be shown to user. Numbers shown in the simulation area are the legitimate node moving randomly and with random speed. Initially, all nodes are legitimate nodes.

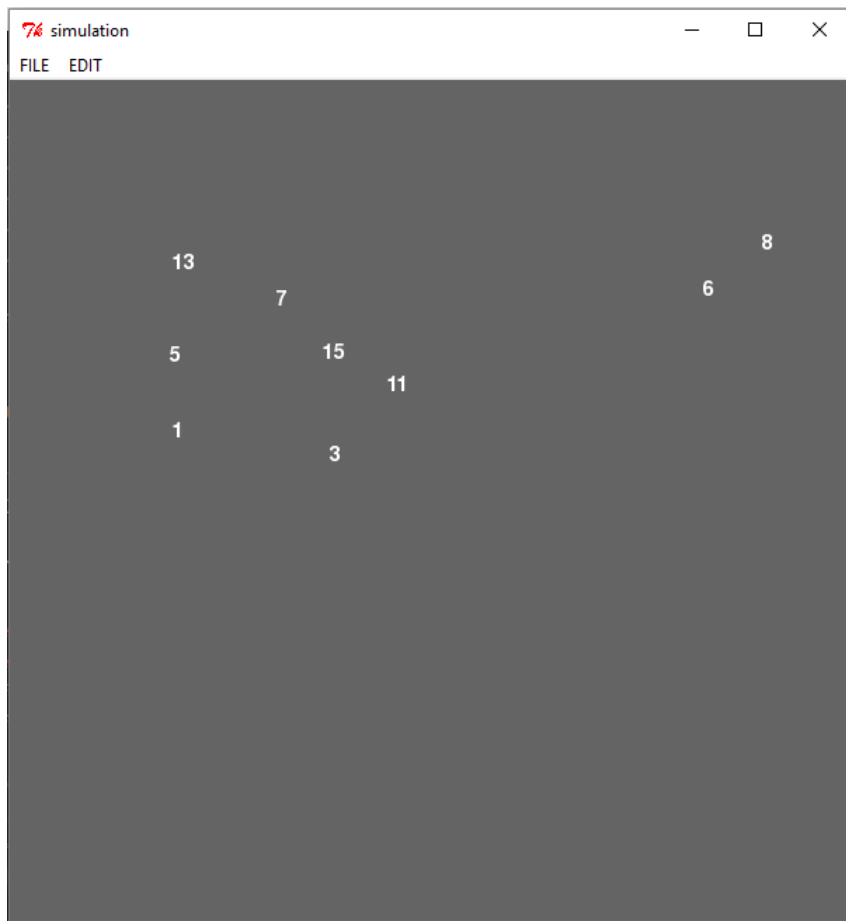


Figure 6: Simulation Area

3.4.3 Nodes Coordinates:

This application allows user to find the coordinates of all the nodes in simulator.

The coordinate of all the nodes in this window continuously updated with the change in the position of nodes in simulation area.

To find the coordinates of the nodes, user needs to go to File→Coordinates.

NODES COORDINATES		
NODES	X AXIS	Y AXIS
1	426	564
2	228	497
3	47	6
4	114	331
5	264	348
6	470	444
7	30	415
8	508	179
9	392	513
10	352	139
11	382	3
12	480	377
13	12	562
14	309	57
15	333	264

Figure 7: Nodes Coordinates

3.4.4 Adjacency Matrix:

The user will be able to see the neighboring nodes of each node using the adjacency matrix.

If the value of slot in adjacency matrix is 1, it means that the nodes are neighbor.

To find the Adjacency Matrix, user needs to go to File → Adjacency Matrix.

		ADJACENT MATRIX															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
1	1	0	0	1	1	0	1	0	0	0	0	1	0	0	0	0	
2	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	
3	0	0	1	0	1	1	0	1	0	0	1	0	0	0	0	0	
4	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	
5	1	0	1	0	1	1	0	1	0	1	1	1	0	0	1	1	
6	0	0	1	0	1	1	0	0	1	0	1	0	0	0	1	0	
7	1	0	0	0	0	0	1	0	0	1	0	1	1	0	0	1	
8	0	1	1	0	1	0	0	1	0	0	0	0	0	0	0	0	
9	0	0	0	0	0	1	0	0	1	1	1	0	0	0	1	1	
10	0	0	0	0	1	0	1	0	1	1	0	1	1	0	0	1	
11	0	0	1	0	1	1	0	0	1	0	1	0	0	0	1	0	
12	1	0	0	0	1	0	1	0	0	1	0	1	0	0	0	1	
13	0	0	0	0	0	0	1	0	0	1	0	0	1	0	0	1	
14	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	
15	0	0	0	0	1	1	0	0	1	0	1	0	0	0	1	0	

Figure 8: Adjacency Matrix

3.4.4 Battery Status:

This application also allows user to find the battery Status of all the nodes in simulator.

To find the Battery Status of the nodes, user needs to go to File → Battery Status.

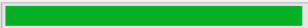
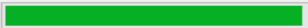
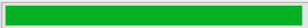






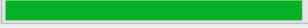
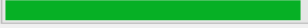
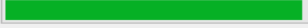




BATTERY STATUS		
NODES	BATTERY	In mAh
0		981.6999999999981
1		981.6999999999981
2		984.1999999999987
3		981.7999999999981
4		980.0999999999977
5		979.9999999999977
6		980.1999999999978
7		981.6999999999981
8		989.3999999999999
9		982.0999999999982
10		975.4999999999967
11		982.7999999999984
12		981.0999999999998
13		983.9999999999986
14		984.0999999999987
15		989.7250000000001

Figure 9: Battery Status

3.4.5 Cluster Formation Details

During Cluster, formation user will be able to see the cluster details includes cluster head and cluster members.

In the simulated area nodes with green color is cluster head and other nodes are member nodes

For initiating cluster formation user need to go to File→Start Clustering

Formation of Cluster before Sybil Attack

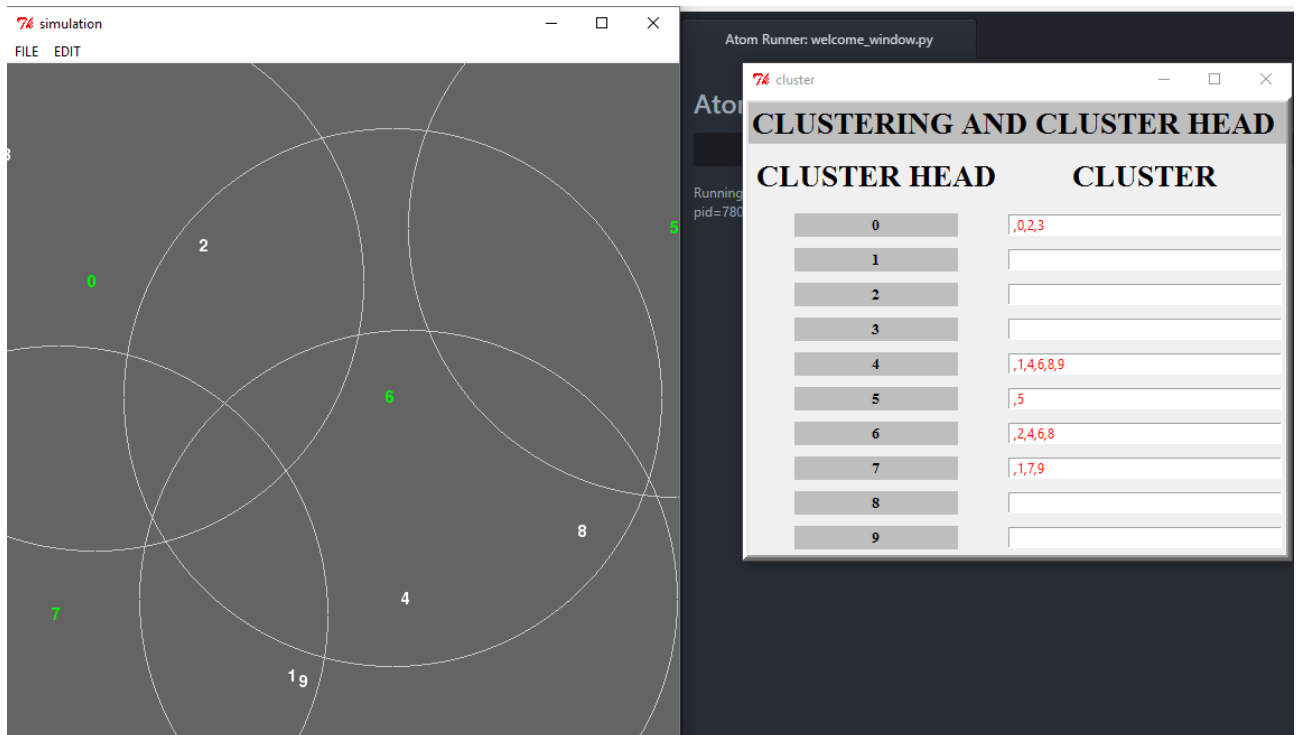


Figure 10: Cluster head formation before Sybil attack

Formation of Cluster after Sybil Attack

In the given Simulated area nodes with green color are Sybil nodes and node with black color (ID=10) is malicious node which targets the node with ID=5 and rest of the nodes are member nodes.

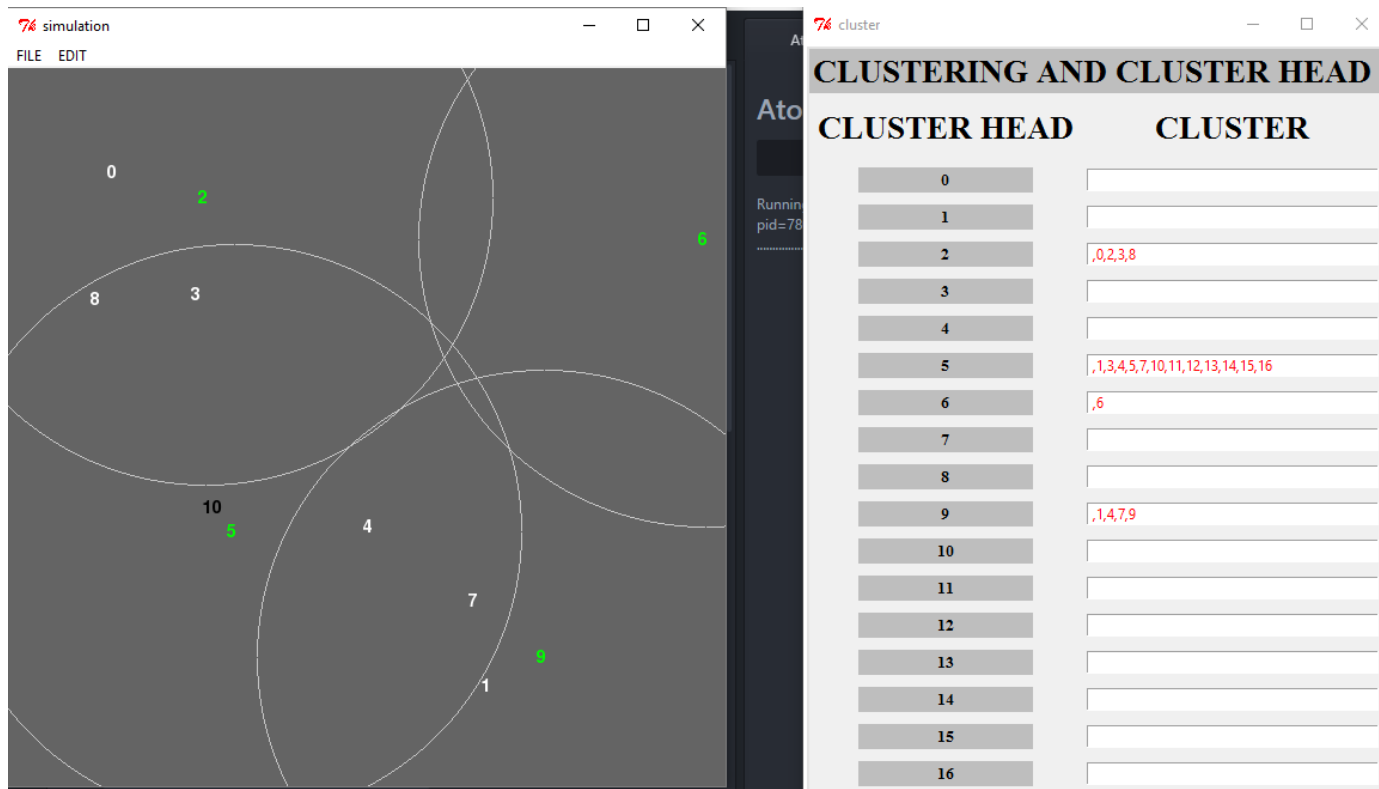


Figure 11: Cluster head formation after Sybil attack

3.5 Simulation environment Parameters

Simulation Environment Parameters	
Parameter	Value
Simulator	Python
Simulation area	600 pixel x 600 pixel
Transmission range of legitimate node	200 pixels
Number of legitimate nodes	10-15
Number of Sybil nodes	5-7
Mobility model	Random Waypoint Model
Speed of nodes	0 to 20 pixels/second
Movement direction	$0-2\pi$

Table 2: Simulation Parameters

3.6 HARDWARE REQUIREMENTS

The minimum requirements needed to perform operations are

- Intel Pentium Processor at 2 GHz or Higher
- RAM 256MB or more
- Hard disk capacity 10GB or more

3.7 SOFTWARE REQUIREMENTS

The software required to perform the implementation are

- Any Operating System (Windows, Linux etc)
- Python and python based modules Pygame ,Tkinter
- Editor e.g. Atom ,Sublime

Chapter 4

PERFORMANCE ANALYSIS

4.1 Complexity of the code

4.1.1 Complexity of the code to find the coordinates and maintain them in a list

- Time complexity $\rightarrow O(n)$
- Space complexity $\rightarrow O(n)$

4.1.2 Complexity of the code to find the adjacency matrix

- Time complexity $\rightarrow O(n^2)$
- Space complexity $\rightarrow O(n^2)$

4.1.3 Complexity of the code to find the battery Status of the nodes

- Time complexity $\rightarrow O(n)$
- Space complexity $\rightarrow O(n)$

4.1.4 Complexity of the code to implement the mobility based clustering algorithm

- Time complexity $\rightarrow O(3n^2)$

For the implementation of mobility based clustering algorithm, we need to run three n^2 loops.

As every node is looking for the two successive receiving message from another node, therefore it has to check for every node two times and for

that, the time complexity is $O(2n^2)$;

The last n^2 loop used for the computation of the relative mobility matrix along with the computation of aggregate local mobility value M_Y (variance).

- **Space complexity** $\rightarrow O(3n^2+n)$

First n^2 space used for the storage of the power of first receiving message from every node to every node.

Second n^2 space used for the storage of the power of second receiving message from every node to every node.

Third n^2 space used for the storage of relative mobility matrix.

Finally, n space used for the storage of aggregate local mobility value M_Y (variance).

4.2 Observations and Result

4.2.1 Cluster formation details before the Sybil attack

Parameters:

Transmission Range \rightarrow 200 pixels

Speed of nodes \rightarrow 0-20pixels

No of legitimate nodes \rightarrow 10

Total No of Observation \rightarrow 50

Observation No	Cluster Head along with Cluster
1	0 {0,5}, 5 {0,5}, 6 {1,6} , 8 {2,3,4,7,8,9}
2	0 {0,2,4,5,6,7}, 3 {1,3,9}, 5 {0,2,4,5,6,7} , 8 {8}
3	0 {0,4,5,7,8}, 2 {2}, 3 {3,5,7,8,9}, 6 {1,4,5,6,9}
4	0 {1,3}, 3 {1,4,8,9}, 6 {0,5,6,7}, 9 {2,4,8,9}
5	2 {0,2,3}, 4 {4}, 6 {1,5,6,7,8}, 9 {0,1,3,9}
6	1 {0,6,8}, 3 {2,3,4}, 5 {5,8}, 7 {0,4,7,9}
7	2 {2,3}, 7 {4,6,7,8}, 9 {0,1,3,5,9}

8	$3\{0,1,3\}, 5\{1,2,5\}, 7\{0,4,6,7,8\}, 9\{8,9\}$
9	$2\{0,2,9\}, 3\{0,1,3,4\}, 5\{1,5,7,8,9\}, 6\{0,6\}$
10	$5\{4,5,9\}, 7\{0,1,6,7\}, 8\{2,3,8\}$
11	$1\{1\}, 2\{2,8\}, 5\{3,5\}, 7\{0,3,4,7\}, 8\{0,2,4,8\}, 9\{6,9\}$
12	$0\{0,6\}, 2\{1,2,3,7,8,9\}, 4\{4,7\}, 5\{5\}, 8\{1,2,8\}$
13	$1\{0,1,5\}, 2\{0,2,4,7\}, 6\{0,5,6\}, 8\{3,8,9\}$
14	$2\{1,2,6,8\}, 4\{0,3,4,5,6,7\}, 7\{0,3,4,5,7,9\}$
15	$0\{0,3,5,6\}, 2\{2,4\}, 7\{5,6,7\}, 9\{1,3,8,9\}$
16	$0\{0,4\}, 5\{1,3,5\}, 7\{1,2,5,6,7,9\}, 8\{8\}$
17	$1\{1\}, 2\{2\}, 5\{4,5,7\}, 9\{0,3,6,8,9\}$
18	$2\{0,1,2,3,5,7\}, 4\{1,4,6\}, 8\{0,8\}, 9\{6,9\}$
19	$1\{1,5,6\}, 2\{0,2,4,8\}, 3\{3,5,6,9\}, 7\{4,6,8,9\}$
20	$2\{0,2,4,6\}, 3\{1,3,7\}, 6\{2,4,6\}, 5\{5\}, 8\{1,6,7,8\}, 9\{9\}$
21	$0\{0,3,8,9\}, 7\{1,2,3,4,5,6,7,8\}$
22	$1\{1\}, 5\{5\}, 7\{0,2,3,4,6,7,8,9\}$
23	$2\{0,2,4\}, 3\{0,1,3,5\}, 5\{0,1,3,5\}, 6\{6,8\}, 7\{1,7\}, 9\{8,9\}$
24	$4\{1,3,4\}, 5\{0,5,6,8,9\}, 7\{2,7\}$
25	$3\{0,1,2,3,7,9\}, 6\{0,1,4,5,6,8\}$
26	$1\{0,1,4,7\}, 3\{3,4\}, 6\{2,5,6,8\}, 9\{5,7,8,9\}$
27	$1\{1,5,6,7,8\}, 2\{0,2,9\}, 4\{0,3,4,8\}, 8\{0,2,9\}$
28	$1\{0,1,3,4,6,7,8,9\}, 2\{2,6,8,9\}, 5\{0,4,5,6,7\}$
29	$0\{0,4\}, 5\{1,3,5,8\}, 6\{2,3,6,7,9\}$
30	$0\{0,1\}, 4\{4,7\}, 6\{1,2,5,6,8\}, 9\{2,3,5,8,9\}$
31	$2\{0,1,2,6\}, 4\{0,1,4,6,7,8\}, 5\{5\}, 7\{4,7,8\}, 9\{3,9\}$
32	$4\{2,4,9\}, 5\{1,3,5\}, 6\{0,6,7\}, 8\{1,8\}$
33	$1\{0,1,2,3,6,7,8,9\}, 4\{4,7\}, 5\{5,6,8\}$
34	$1\{1,5,6,7,9\}, 2\{0,2,3\}, 8\{4,8\}$
35	$1\{1,4,5,7\}, 3\{3\}, 6\{0,2,6\}, 9\{0,2,7,8,9\}$
36	$1\{1,3,6\}, 2\{2,5,7\}, 8\{4,8\}, 9\{0,4,6,9\}$
37	$0\{0,5\}, 3\{3,4,8,9\}, 6\{1,2,6,7\}$
38	$0\{0,2,4,5,6,7,9\}, 1\{1\}, 8\{2,3,4,7,8\}$
39	$0\{0\}, 7\{3,4,7\}, 8\{2,8\}, 9\{1,5,6,9\}$

40	1 {1,3,8}, 6 {0,2,3,4,5,6,7} , 9 {5,8,9}
41	0 {0,2,8}, 1 {1,3,8}, 4 {4,7} , 5 {5,6,9}
42	0 {0,6,8,9}, 1 {1}, 2 {2,3,4,5,6,7} , 8 {0,6,7,8,9}
43	0 {0,4,5,8}, 2 {2,9}, 6 {4,6} , 8 {0,1,3,4,5,7,8}
44	1 {0,1,2,3,4,6,7}, 5 {2,4,5}, 8 {8} , 9 {0,9}
45	5 {3,5,8}, 6 {4,6}, 7 {0,1,3,7,8} , 9 {2,9}
46	0 {0}, 3 {2,3,4,5,6}, 7 {1,7,8,9}
47	1 {1,2,3,4}, 6 {0,6} , 8 {0,3,5,7,8,9}
48	3 {3,6}, 4 {1,2,4,8}, 6 {3,6} , 8 {0,5,7,9}
49	4 {4,8}, 6 {0,2,6} , 9 {1,3,5,7,8,9}
50	5 {2,3,4,5,6,7,9}, 6 {0,1,2,3,4,5,6} , 8 {8}

Table 3: Cluster formation before Sybil attack

4.2.2 Cluster formation details after the Sybil attack

Parameters:

Transmission Range → 200 pixels

Speed of nodes → 0-20pixels

No of legitimate nodes →10

No of Sybil nodes →7

Total No of Observation →50

Observation No	Cluster Head along with Cluster
1	1 {0,1,3}, 2 {2,8}, 3 {4,5,10,11,12,13,14,15,16}, 6 {6} , 7 {7,8}, 9 {9}
2	1 {0,1,3}, 2 {2}, 5 {0,3,4,5,10,11,12,13,14,15,16}, 7 {6,7,8}, 8 {6,7,8}, 9 {9}
3	0 {0,1,2,3,8}, 5 {1,4,5,10,11,12,13,14,15,16}, 6 {6}, 7 {7,9}, 9 {7,9}
4	0 {0,1,2,4,7,9}, 3 {3}, 5 {4,5,6,10,11,12,13,14,15,16}, 8 {4,7,8}
5	2 {1,2,9}, 3 {0,3,6,7}, 4 {4,5,6}, 8 {0,8}

6	$1\{0,1,4\}, 2\{2,3,6,7,9\}, 5\{3,5,9,10,11,12,13,14,15,16\}, 8\{0,4,8\}$
7	$2\{2,3,7,8\}, 5\{1,4,5,6,10,11,12,13,14,15,16\}, 9\{0,6,9\}$
8	$0\{0,4\}, 5\{2,3,4,5,7,10,11,12,13,14,15,16\}, 6\{1,2,6\}, 8\{1,8\}, 9\{9\}$
9	$1\{0,1,2,7\}, 4\{4\}, 5\{2,3,5,10,11,12,13,14,15,16\}, 6\{0,6,7,9\}, 8\{8\}$
10	$1\{0,1,2\}, 4\{4,8,9\}, 5\{3,5,10,11,12,13,14,15,16\}, 6\{3,6\}, 7\{7,8\}$
11	$0\{0,1,3,6\}, 4\{3,4,9\}, 5\{2,5,10,11,12,13,14,15,16\}, 8\{6,7,8\}$
12	$3\{2,3\}, 4\{1,2,4\}, 5\{3,5,10,11,12,13,14,15,16\}, 6\{0,6,7,8\}, 9\{8,9\}$
13	$0\{0,4\}, 1\{1\}, 3\{3,4,8\}, 5\{3,5,10,11,12,13,14,15,16\}, 7\{7\}, 9\{4,6,9\}$
14	$0\{0,3,4,8\}, 5\{1,2,5,6,7,10,11,12,13,14,15,16\}, 9\{9\}$
15	$0\{0,1,2,5,6,7,8\}, 3\{0,3,9\}, 4\{4,5\}$
16	$0\{0\}, 2\{2\}, 3\{3,6\}, 5\{1,5,7,10,11,12,13,14,15,16\}, 8\{8\}, 9\{1,4,9\}$
17	$0\{0,6,8\}, 1\{1,8\}, 2\{2\}, 3\{3,9\}, 4\{4,7\}, 5\{5,10,11,12,13,14,15,16\}, 7\{7\}, 6\{0,6,8\}, 7\{4,7\}, 9\{3,9\}$
18	$0\{0,1\}, 3\{1,3\}, 5\{2,4,5,6,10,11,12,13,14,15,16\}, 7\{4,7,9\}, 8\{2,8\}, 9\{7,9\}$
19	$0\{0,3,9\}, 4\{3,4\}, 5\{5,10,11,12,13,14,15,16\}, 6\{6\}, 7\{1,2,7,8\}, 9\{0,3,9\}$
20	$0\{0,3,4\}, 1\{1\}, 5\{2,5,6,10,11,12,13,14,15,16\}, 7\{7\}$
21	$0\{0,1,2,3,4,8\}, 5\{5,10,11,12,13,14,15,16\}, 7\{6,7\}, 9\{2,8,9\}$
22	$1\{1,9\}, 3\{2,3,6,7\}, 5\{5,10,11,12,13,14,15,16\}, 8\{0,4,8\}$
23	$0\{0,7\}, 5\{1,3,5,6,10,11,12,13,14,15,16\}, 9\{2,3,4,8,9\}$
24	$0\{0,8\}, 2\{2,4,6\}, 3\{3\}, 5\{1,4,5,6,10,11,12,13,14,15,16\}, 7\{6,7\}, 8\{0,8\}$
25	$1\{1,7\}, 2\{2,6\}, 4\{0,3,4,8\}, 5\{5,6,10,11,12,13,14,15,16\}, 9\{9\}$
26	$0\{0,1,3,8\}, 2\{2,9\}, 4\{4,7\}, 5\{5,10,11,12,13,14,15,16\}, 6\{6\}$
27	$0\{0,1,4,6\}, 3\{1,2,3,6,9\}, 5\{4,5,10,11,12,13,14,15,16\}, 7\{7\}, 8\{8\}$
28	$0\{0,1\}, 3\{2,3,4,9\}, 5\{4,5,10,11,12,13,14,15,16\}, 6\{6,8\}, 7\{4,7\}$

29	$0\{0,2\}, 3\{3\}, 4\{1,4,6\}, 5\{1,5,6,8,9,10,11,12,13,14,15,16\}, 7\{7,8,9\}$
30	$0\{0,9\}, 1\{1,9\}, 5\{2,3,5,7,10,11,12,13,14,15,16\}, 6\{2,3,4,6\}, 8\{8\}$
31	$5\{0,2,5,7,8,10,11,12,13,14,15,16\}, 7\{1,4,6\}, 9\{0,3,9\}$
32	$1\{1,3\}, 5\{5,8,10,11,12,13,14,15,16\}, 9\{0,4,6,9\}$
33	$1\{1,4\}, 5\{5,8,10,11,12,13,14,15,16\}, 7\{0,2,3,7\}, 9\{6,9\}$
34	$0\{0,3\}, 2\{2,8\}, 4\{3,4\}, 6\{1,5,6,8,10\}, 9\{1,7,9\}$
35	$1\{1\}, 2\{2,7,9\}, 3\{0,3\}, 4\{0,4,7,9\}, 5\{0,5,8,10,11,12,13,14,15,16\}, 6\{6\}$
36	$0\{0,1\}, 3\{2,3\}, 4\{4,5,6,7,10\}, 7\{1,4,7\}, 9\{8,9\}$
37	$0\{0\}, 1\{1,4,6\}, 2\{2,6\}, 5\{3,5,10,11,12,13,14,15,16\}, 7\{7,8,9\}, 8\{4,7,8,9\}, 9\{7,8,9\}$
38	$2\{2,7,8\}, 3\{3,6\}, 4\{1,4,9\}, 5\{0,1,5,7,10,11,12,13,14,15,16\}, 6\{3,6\}, 8\{2,7,8\}$
39	$0\{0,5,7,10\}, 1\{1,6\}, 3\{3,6,8\}, 4\{2,4\}, 9\{2,9\}$
40	$1\{1\}, 2\{2,3\}, 5\{0,4,5,6,9,10,11,12,13,14,15,16\}, 8\{7,8\}$
41	$3\{2,3,8\}, 4\{4\}, 5\{0,1,2,5,6,8,10,11,12,13,14,15,16\}, 7\{1,7\}, 9\{9\}$
42	$0\{0,1,7,8\}, 2\{1,2,6\}, 4\{3,4\}, 5\{5,9,10,11,12,13,14,15,16\}$
43	$0\{0,1,2,8,9\}, 3\{3\}, 4\{4\}, 5\{1,2,5,8,9,10,11,12,13,14,15,16\}, 6\{6,7\}$
44	$1\{1,6\}, 2\{0,2\}, 5\{3,4,5,7,10,11,12,13,14,15,16\}, 9\{0,8,9\}$
45	$2\{2,6\}, 3\{3\}, 4\{4,7\}, 5\{5,9,10,11,12,13,14,15,16\}, 8\{0,1,6,8\}$
46	$5\{0,1,2,3,4,5,6,7,8,10,11,12,13,14,15,16\}, 9\{9\}$
47	$5\{1,2,4,5,10,11,12,13,14,15,16\}, 6\{6\}, 7\{7\}, 8\{0,3,8,9\}$
48	$0\{0,1,4,7,8,9\}, 3\{3,4\}, 5\{2,5,10,11,12,13,14,15,16\}, 6\{6\}, 8\{0,1,8\}$
49	$0\{0,1,7,8\}, 2\{2,4,6,9\}, 3\{3,4,6,9\}, 5\{5,6,10,11,12,13,14,15,16\}, 8\{0,8\}$
50	$2\{2\}, 5\{1,3,4,5,6,9,10,11,12,13,14,15,16\}, 7\{7,8\}, 8\{0,7,8\},$

Table 4: Cluster formation after Sybil attack

4.2.3 Cluster head count before and after the Sybil attack

Parameters:

Target Node →5

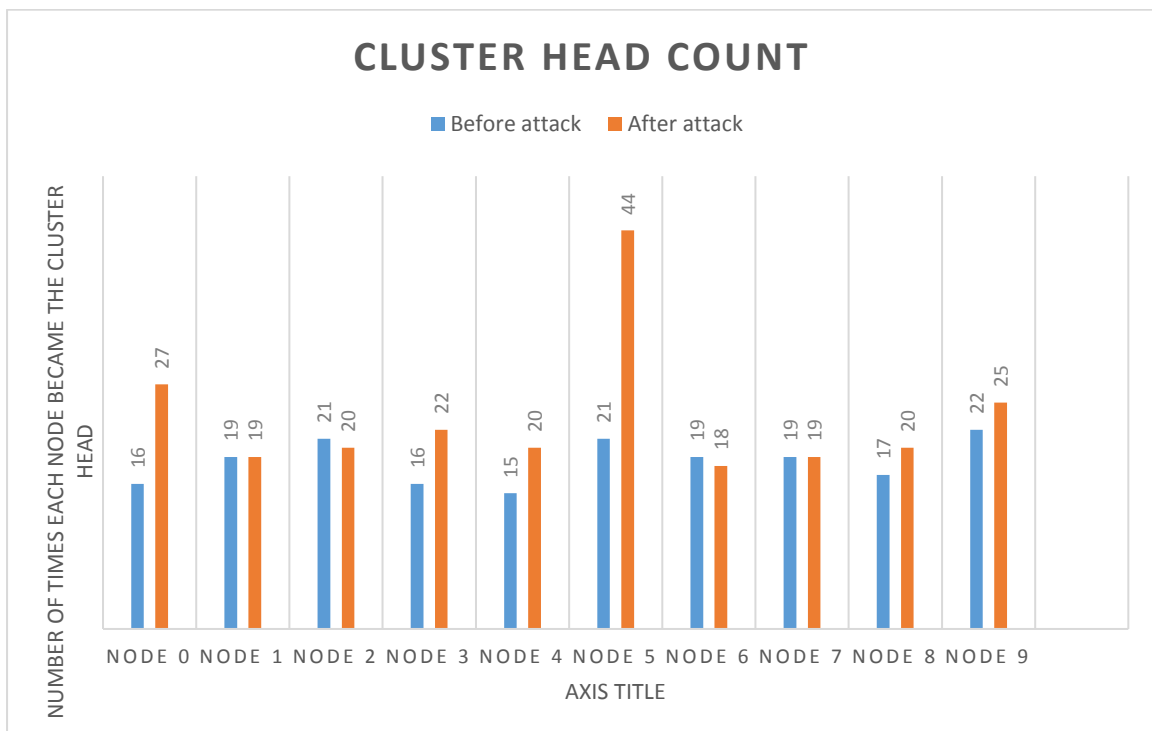
Legitimate node →10

Sybil nodes →7

Speed of nodes →0-20 pixel

Transmission range →200 pixel

Total no of Observation →50



Graph 1: Cluster head Count before and after Sybil attack

	No of times target node(node 5) became cluster head	Percentage
Before attack	21	44%
After attack	44	88%

Table 5: Percentage calculation of cluster head count

4.2.4 Effect of Sybil attack on Cluster head formation with different transmission range

Parameters:

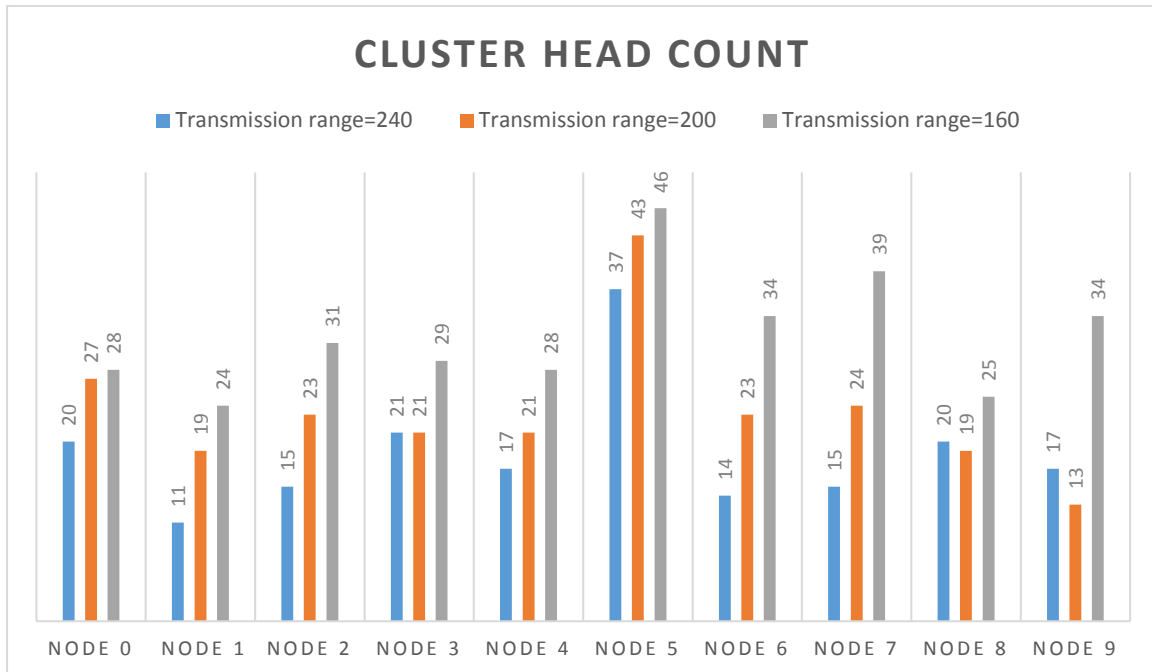
Target Node →5

Legitimate node →10

Sybil nodes →7

Speed of nodes →0-20 pixel

Total no of Observation →50



Graph 2: Cluster head Count with different transmission Range

Transmission Range	No of times target node(node 5) became cluster head	Percentage
240	37	74%
200	43	86%
160	46	92%

Table 6: Percentage calculation of cluster head count with different transmission power

4.2.5 Effect of Sybil attack on Cluster head formation with different nodes speed.

Parameters:

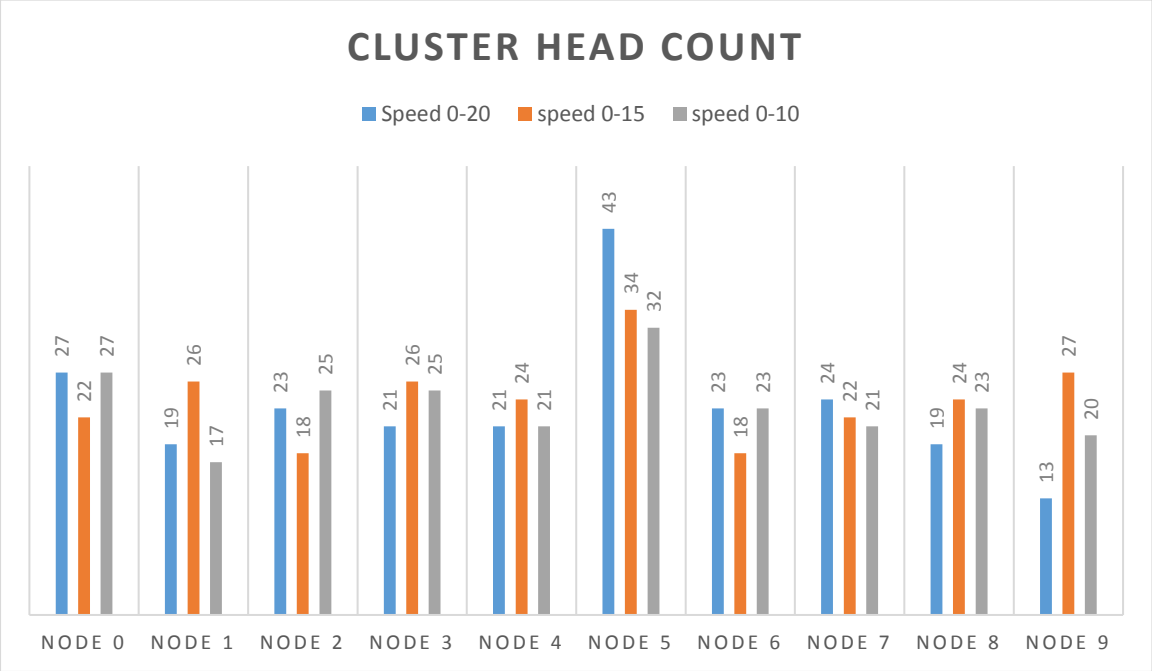
Target Node →5

Legitimate node →10

Sybil nodes →7

Transmission Range →200

Total no of Observation →50



Graph 3: Cluster head Count with different nodes speed

Nodes Speed	No of times target node(node 5) became cluster head	Percentage
0-20	43	86%
0-15	34	68%
0-10	32	64%

Table 7: Percentage calculation of cluster head count with different Nodes speed

4.2.5 The result of Sybil attack with different transmission power and different nodes speed.

- Effect of nodes speed on Sybil attack
This attack is much effective on highly mobile nodes to compare to less mobile nodes.
- Effect of transmission power on Sybil attack
It is shown in our observation that Sybil attack is much effective on MANETs having nodes with low transmission range.

CHAPTER 5

CONCLUSIONS

5.1 Conclusions

Mobile Ad hoc network is the best choice for communication where set up of fixed communication infrastructure is not possible or very expensive. But to handle such ad hoc networks some kind of hierarchical and organizational structure is helpful. Clustering is one of such technique to imposing hierarchical and organizational structure on MANETs. Mobility based clustering algorithm is one of such clustering algorithm. However, the broadcast nature of the communication in MANETs and limited resources of nodes in MANETs make clustering susceptible to many securities attack. Sybil attack is one of such attack where one physical device with multiple identities tried to harm the ad hoc network in one of the various ways.

Sleep deprivation torture attack is one of such attack where the malicious node with the help of all its Sybil nodes interrupts the cluster formation in mobility based clustering algorithm. Mobility based clustering algorithm choose variance of relative mobility between two neighboring nodes as the measure to form cluster. But the malicious node can increase or decrease the relative mobility of other nodes and hence manage the cluster formation.

In our observations, we find that this attack is much effective if nodes are highly mobile in nature. Therefore, this attack has large effective on MANETs of Unmanned Ground Vehicles (UGV) of Unmanned Vehicles (UV).

5.2 Future Scope

To find another type of attacks which could disrupt the Mobile Ad Hoc Network (MANET).

To find and develop defense system against the **Sleep Deprivation Torture Attack** and another type of attacks. Some of the existing methods to defend a Sybil attack are Trusted Certification, Resource Testing, Gate Keeper etc. We can implement these techniques to guard against these attack and even devise a better method to do the same.

Since there are much work remain to do in the field of MANET to improve the QoS and security of the network. Hence we can work on other clustering algorithms to overcome the limitations and drawbacks of the existing algorithms to improve QoS as well as security of the network.

REFERENCES

- [1] Basu P, Khan N, Little T (2001) A mobility based metric for clustering in mobile ad hoc networks. In: Proceedings of the 21st international conference on distributed computing systems workshops (ICDCSW '01), pp 413–418.
- [2] Aarti and Dr. S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2010
- [3]Amol Vasudeva and Manu 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, September 2012
- [4] C. -K. Toh, (2002), "Ad Hoc Mobile Wireless Networks: Protocols and Systems", *Prentice Hall, PTR.*