

**Impersonation based Sybil attack to disrupt the Lowest ID
Clustering algorithm in Mobile Ad Hoc Networks**

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

In

Computer Science and Engineering

By

Rupali Sharma (121292)

Under the supervision of

Mr. Amol Vasudeva

To



Department of Computer Science & Engineering and Information
Technology

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

CERTIFICATE

Candidate's Declaration

I hereby declare that the work presented in this report entitled “ **Impersonation based Sybil attack to disrupt the Lowest ID Clustering algorithm in Mobile Ad Hoc Networks**” in complete 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 work carried out by Rupali Sharma (121292) over a period from August 2015 to May 2016 under the supervision of **Mr. Amol Vasudeva**(Assistant Professor Computer Science And Engineering).

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

Signature of Student:

Rupali Sharma (121292)

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

Signature of Supervisor:

Mr. Amol Vasudeva

Designation: Assistant Professor

Department: Computer Science and Engineering.

Dated:

ACKNOWLEDGEMENT

The project entitled as Impersonation based Sybil attack on mobile Ad hoc Networks using lowest ID clustering is done to better understand the impacts of Sybil attack on system and networks.

I would like to extend my heartiest gratitude to my project guide **Mr. Amol Vasudeva** who is an esteemed lecturer of Department of computer Science and engineering and IT, JUIT. He has guided us to proceed this project in best of his capability. He has given me the push that I need to go further and to do more. So I take this opportunity to express my sincere gratitude and thanks to him for lending his cooperation.

TABLE OF CONTENT

Topics	Page no.
CERTIFICATE	i
ACKNOWLEDGEMENT	ii
LIST OF ABBREVIATIONS	iii
LIST OF FIGURES	vi
ABSTRACT	vii
Chapter 1: INTRODUCTION	1
1.1 Introduction	1
1.1.1 MANET	3
1.1.2 Mesh networks	4
1.1.3 Sybil Attack	5
1.2 Problem Statement	9
1.3 Methodology	10
Chapter 2: LITERATURE SURVEY	12
2.1 Study of MANET	12
2.2 Security threats in MANET	14
2.3 Routing Protocols and Challenges in Ad hoc Wireless Networks	17
2.4 Study of various mobility models	21
Chapter 3: SYSTEM DEVELOPMENT	24
3.1 Software Requirement Specification (SRS)	24
3.2 Data Flow Diagram	28
3.3 Use case Diagram	30
3.4 Functional Requirements	31
3.5 Non Functional Requirements	32
3.6 Design and Development	33

3.7 Feasibility Study	37
3.8 Testing	38
Chapter 4: PERFORMANCE ANALYSIS	39
Chapter 5: CONCLUSIONS	42
5.1 Conclusions	
5.2 Future Scope	
REFERENCES	44

LIST OF ABBREVIATIONS

Qos	Quality of service
Dos	Denial of service
WMN	Wireless mesh network
MANET	Mobile ad hoc network
DSDV	Destination Sequenced Distance Vector
WRP	Wireless Routing Protocols
DFR	Direction Forward Routing
HSR	Hierarchical State Routing Protocols
AWDS	Ad hoc Wireless Distribution Service
CGSP	Cluster Head Gateway Switch Routing Protocols
AODV	Ad hoc On-demand Distance Vector
DSR	Dynamic Source Routing
ZRP	Zone Routing Protocols
OORP	Order One Routing Protocols

LIST OF FIGURES

Figure 1: A Mobile Ad hoc network

Figure 2: A Sybil attacker with multiple identities

Figure 3: Formation of cluster using lowest ID clustering algorithm

Figure 4: Demonstration of Passive Attack

Figure 4: Demonstration of Active Attack

Figure 6: Categorization of ad hoc routing protocols

Figure 7.1: Zero Level DFD

Figure 7.2: First Level DFD

Figure 7.3: Second Level DFD

Figure 8: Use case diagram

ABSTRACT

A **Mobile ad-hoc network** is a self-configuring network that does not depend on any infrastructure for communication. Every node is free to move anywhere in the network and data is exchanged independently across the network.

Network security in an MANET is a very challenging issue. Open nature communication of MANET makes it more vulnerable to security attacks. Our major focus in the project will be impersonation of Sybil Attack, in which a malicious node illegitimately claims multiple identities. This attack can disrupt various operations of the mobile ad hoc networks for Example, voting, fair resource allocation scheme, Detection and routing mechanisms etc. In addition to these the Sybil attack can also disrupt the head selection mechanism of the lowest ID cluster-based routing protocol.

CHAPTER- 1

INTRODUCTION

1.1 Introduction:

Ad hoc Network:-

The word ad hoc is a Latin word and means “for this (only)”. In computer networks, the ad hoc networks mean wireless network without infrastructure, or they can be called spontaneous network. Therefore Ad hoc Network is a network without any base stations, and there is no dependence on infrastructure. The wireless ad hoc networks only consist of nodes equipped with transceiver. There is a collection of wireless nodes that communicate over a common wireless medium. The nodes communicate without an infrastructure, such as a base station or wired access point.

Each node in the wireless network is an end system itself and also acts as a router that sends packets over the network. The nodes must be able to arrange their own networks. a node can now communicate only with other nodes in its transmission range. It is not that the ad hoc networks are not powerful enough. Each node has its own transmission range, if these small transmission areas are combined, they will form a much bigger transmission area [1].

Ad-hoc networking is often used in scenarios where we do not want or where we cannot deploy and manage an infrastructure.

Ad hoc networks are mostly used by military, rescue mission team, taxi driver Special circumstances such as disaster relief, etc.

Importance of Ad hoc networks:-

1. Ease of deployment.
2. Speed of deployment because they can be set anytime anywhere.
3. Decreased dependence on infrastructure.

It supports anytime and anywhere computing

Categories of Ad hoc network:-

1. MANET
2. Mesh Networks

Problems Facing Routing in Ad hoc Networks:-

- Routers are moving.
- Link changes happen quite often.
- Packet losses due to transmission errors.
- Event updates are sent often – a lot of control traffic.

Mobility characteristics of different nodes are: -

- Speed.
- Predictability.
- Direction of movement.
- Pattern of movement.
- Non uniformity

Mobility in Ad hoc Networks:-

- Mobility patterns may be different.
- People sitting at an airport lounge.
- Taxi cabs.
- Military movements.
- Personal area network.

1.1.2 MANET:-

MANET is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Devices in MANET are free to move in any direction, and will therefore links with other device are changed frequently. Each device is a router itself .The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such type networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes.

There is a highly dynamic topology in this network. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming network.

MANETS can be used for helping with the collection of sensor data for data mining for a variety of applications such as air pollution monitoring and different types of architectures can be used for such applications.

In a MANET mobile nodes communicate to each other in the absence of a fixed infrastructure. Therefore, they operate with on battery power. Because of certain these limitations, there must be certain algorithms which are energy-efficient as well as operating with limited processing and memory resources. Sometimes it is also happens that while receiving data from someone, the battery is almost depleted. Therefore repeating the transfer process after recharging is necessary. Hence a MANET is not suitable for a permanent network [2].

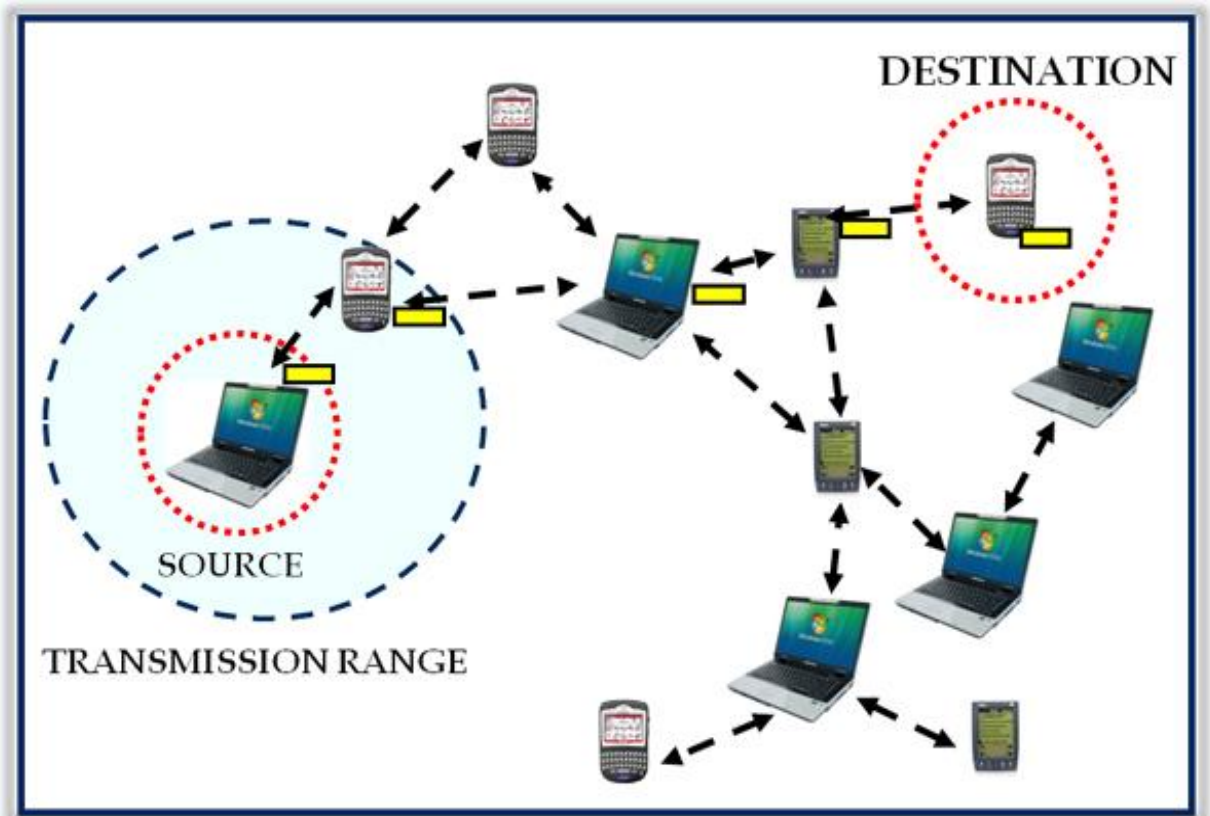


Figure 1: A Mobile adhoc network [18]

1.1.3 Mesh Networks:

It is also a form of wireless ad hoc network. Mesh networks can relay messages using either a flooding technique or a routing technique. With routing, the message is propagated along a path by hopping from node to node until it reaches its destination. A wireless mesh network (WMN) is a communications network made up of radio nodes organized in a mesh topology. Wireless mesh networks consist of mesh clients, mesh routers and gateways. Mesh networking technology powers many of the largest mobile networks in the world. The redundant nature of mesh networks is an essential characteristic for military strategists. High performance and scalable broadband networks can be built at very low cost using a mesh net. The mesh clients can be:-

1. **Laptops**
2. **Cell phones**
3. **Wireless devices**

Mesh routers forward traffic to and from the gateways which may, but need not, connect to the Internet. The coverage area of the radio nodes working as a single network is sometimes called a mesh cloud. A mesh network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes. Wireless mesh networks can self form and self heal. The topology of a mesh network is reliable, as each node is connected to several other nodes. If in any case one node drops out of the network, due to hardware failure or any other reason, its neighbours can quickly find another route using a routing protocol and can communicate [3].

1.1.4 Sybil Attack:

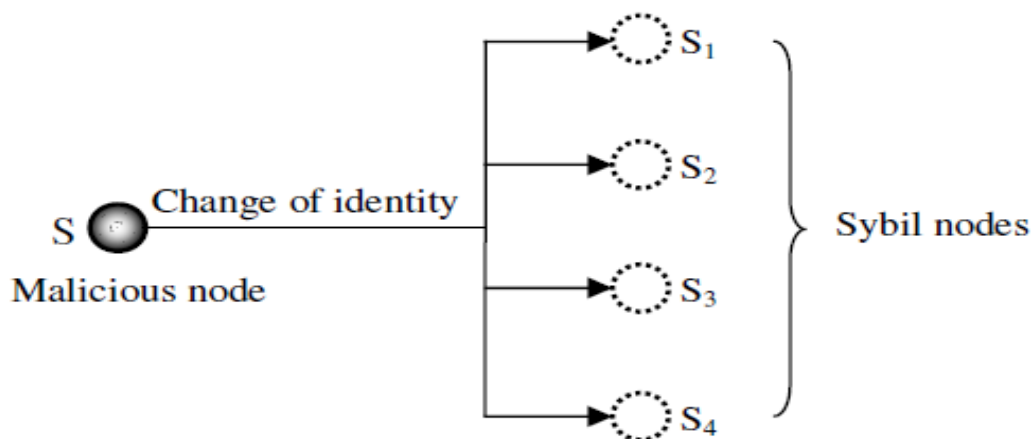


Figure 2: A Sybil attacker with multiple identities [4]

Sybil Attack is Named after the case study of a woman have multiple personality disorder. It is first described by John Douceur in peer to peer network. Sybil attack is an attack in which a single entity can control a substantial fraction of the system by presenting multiple identities. Sybil attack is implemented when a malicious node claim multiple identities in network the node represent multiple fake identity and affect the network operation. Sybil attack in effective in both Distributed and Peer to peer network. It is important to detect and mitigate Sybil attack. Sybil attacks harmful for security and trust of network in peer to peer and distributed network such as torrent or anomaly network such as tor .The proposed problem may happen in MANET [4].

Sybil Attack Dimensions:

- 1. Communication**
- 2. Participation**
- 3. Identity**

1. Communication

There are two ways of communication:

Direct and **Indirect**: In a direct communication, as the name suggests, the malicious node allows its Sybil nodes to communicate directly with the legitimate nodes. Thus, the legitimate nodes will have an illusion of having these Sybil nodes as their neighbours. But in Fact, the messages are being sent and received by the malicious node.

In case of indirect communication, the malicious node does not allow its Sybil nodes to communicate directly with the legitimate nodes; instead it claims to have its Sybil nodes as its neighbours that are not within the reach of the legitimate nodes. Therefore, the legitimate nodes will be using the malicious node as a router to reach these Sybil nodes [4].

2. Participation

This dimension is basically concerned about the participation of Sybil nodes in the communication with legitimate nodes in the network. These nodes can participate simultaneously or non-simultaneously. In a simultaneous participation, the malicious node launches the entire fake Identities i.e. the Sybil nodes at once. in a non-simultaneous way on the other hand, the malicious node presents the Sybil identities, after fixed or variable interval of time one by one [4].

3. Identity

Identity represents the spoofing of identities for the Sybil nodes. There are two methods by which a Sybil node can get the identity: In the first method a Sybil node can steal the identity of a legitimate node by impersonating it. The second method Sybil node can fabricate a fresh fake identity and present it to the neighbours.

1.1 5 Effects of Sybil Attack in Mobile Ad Hoc Networks

If a single malicious node is able to convince its neighbours by presenting multiple identities, it will have control over the substantial portion of the network and can adversely affect the functioning of this network. Once a Sybil attack has been launched in the system, it also opens the doors for different types of other attacks.

Data Aggregation

Even a single Sybil attacker node with multiple fake identities can participate in the data aggregation, many times and can alter the result of the data aggregation.

Fair Resource Allocation

Fair resource allocation scheme is also affected by the Sybil attack because if large numbers of fake identities are present then most of the resources are claimed by those fake nodes and legitimate nodes will not get any resources .For example some network resources may be allocated on a per node basis; in that case a malicious node can have a larger share of any resource by presenting multiple identities.

Voting

A Sybil attacker node is also capable of altering the result of a voting scheme. For example, in a vote based intrusion detection system, a malicious node with multiple Sybil nodes can expel a legitimate node from the network by voting against this node. Also, to win the trust of the legitimate nodes in the network, a Sybil attacker can take advantage of its multiple Sybil nodes that will vote in its favour.

Routing

Sybil attacks can also impact the functioning of certain routing protocols in MANETs such as geographic based routing protocols [5] and multi-path routing protocols [6]. In geographic routings, the nodes exchange their location information with their neighbours, to forward the packets in an efficient manner.

Thus the legitimate nodes will have false routing information in their tables and will lead to disruption in the routing process. In multi path routing protocol, if the Sybil attacker has presented multiple Sybil nodes among the legitimate nodes, then for the legitimate sender nodes it may appear that the route request packets are being forwarded through different paths, whereas they are being actually passed through a single malicious node [4].

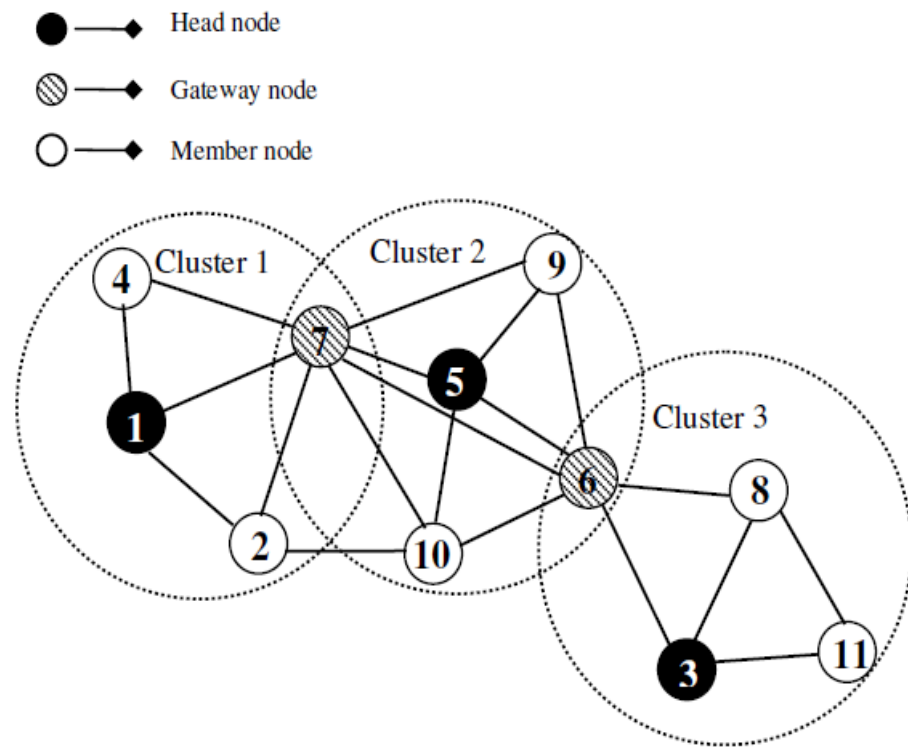


Figure 3: Formation of cluster using lowest ID clustering algorithm [4]

1.2 Problem Statement

In this project we have to attack a network system by impersonating the node with lowest ID. Here the intention is to make a legitimate node with lowest ID, the cluster head again and again to drain its battery. User will give the criteria for building of clusters. We have to show that how the malicious node creates more Sybil nodes and impersonate the system and how Sybil attack affects a system.

1.3 Methodology

Sybil Attack is implemented through the lowest Id clustering algorithm in which a node with Lowest Id is chosen as cluster head again and again.

- A node with the minimum id is chosen as a cluster head. Each node is assigned a distinct id. Periodically, the node broadcasts the list of nodes that it can hear including itself
- A node becomes a cluster head if it hears nodes with the ID's higher than itself. The lowest-id node that a node hears is its cluster head, unless the lowest-id specifically gives up its role as a cluster head

1.4.1 Lowest Id Clustering algorithm:

- Take N number of nodes in a Mobile Ad Hoc Network, at any instant of time, and their IDs are as $x: i 1, 2 \dots N$; where m is a malicious node.
- These nodes will behave normally for some time in the network, and then this malicious node will gain the access to the necessary information about the network including its neighbours and their IDs.
- In the next step the malicious node m generates S number of Sybil nodes that participates in communicate with the legitimate neighbouring nodes $n j S j := 1, 2, \dots, S$, where $S < N$.
- These IDs of the malicious nodes are taken such that $n_j > n_i$ i.e. ID's of malicious nodes are always greater than the legitimate nodes.

- The Sybil attacker node m will also use its Sybil nodes to communicate again and again using its different IDs so as to keep the head node busy all the time, until its battery is drained, completely.

- After the battery of this cluster head node is drained completely, the malicious node can impersonate its ID and assign it to one of its Sybil nodes to make it a cluster head [4].

Effects of Sybil Attack:

- In the presence of Sybil nodes in the network, it may make difficult to identify a misbehaving node.
- Sybil attacks prevent fair resource allocation among the nodes in the network.
- In certain application, sensors can be used to perform voting for decision making.
- Due to presence of duplicate identities the outcome of voting process may vary.
- Sybil nodes affect the normal operation of routing protocols by appearing itself at various locations in network.

CHAPTER-2

LITERATURE SURVEY

2.1 STUDY OF MANET: [5]

ABSTRACT:

In this paper characteristic challenges and problems of Ad hoc network are explained.

Problems in Ad hoc network:-

The wireless communication is very famous nowadays, because very few cables are used.

But with advantages there are some disadvantages also some of these are:-

1. Lower data rate.
2. Security.
3. Medium access control.

Higher error rate: The wireless transmission may deal with problem of the electronic wave. For example if there is a free room which has no obstacles the electronic wave propagates linear independently from its frequency. If the obstacle is present then it causes shadowing, reflection, scattering, fading, refraction, diffraction of the wave. Due to this propagation the received packets may contain error.

Lower data rate: One of biggest Problem of ad hoc networks is reduced data rates. The characteristic of wave, which is used for wireless communication, prevents wireless communication to transmit data better than wired communication. A higher frequency can transmit more data, but then it is more vulnerable to interference but performs well in short range. `

Dynamic topology and scalability: Since the MANET's nodes are mobile, the routing changes as the nodes move. Information regarding the current node must be propagated to the entire nodes in network. Control messages have to send around the network frequently. Because of the large number of control messages there is imposed a burden on the bandwidth. Therefore, the ad hoc protocols are typically designed to reduce the number of control messages, such as by keeping the current information. A good

algorithm for ad hoc networks must be able to evaluate and compare networks' relative scalability in the face of increased number of nodes and nodes mobility. It is very important to know how many control messages is required. So we can control bandwidth's usage.

Security: Due to dynamic distributed infrastructure and lack of centralized access points, the ad hoc networks are vulnerable to various kinds of attacks. The wireless channel is accessible to both legitimate network users and malicious attacker also. Therefore, the ad hoc networks are vulnerable to attacks such as eavesdropping, interfering [2].

For MANET, limited power consumption due to energy limitation causes incapability to execute computation-heavy algorithms like public key algorithms. Passive attack means, that the attacker does not send any message. The attacker just listens the channel; therefore, it is almost impossible to detect this attack. In contrast, the active attack modifies, delete the packets, injects packets to invalid destination. Active attack can be detected. There are numerous security problem issues in the ad hoc networks.

Challenges in Ad hoc Mobile Networks:-

1. Host is no longer an end system it can also act as an intermediate system.
2. Changing the network topology over time because the nodes in the network are not stable and keep on changing.
3. Every node can be mobile.
4. Limited power capacity.
5. Limited wireless bandwidth.
6. Presence of varying channel quality

2.2 SECURITY THREATS IN MANETS: A REVIEW [2]

ABSTRACT:

There are some security constraints that must be implemented for security purposes:-

- 1. Confidentiality:** Confidentiality in the network must be implemented to prevent the disclosure of any part of the information to unauthorized entities during the transmission of data. Ad hoc networks may face harmful consequences if confidentiality is not taken into consideration.
- 2. Integrity:** Integrity is violated when a message is actively modified when it is passing through an area. The network should be able to maintain the integrity so that the unauthorized entities are not able to modify or corrupt any message.
- 3. Availability:** The main purpose of any network is to exchange the information. If the security constraints are maintained then data availability in the network can be ensured. This constraint can be violated by the denial of service attacks (DoS) in the ad hoc networks.
- 4. Authenticity:** Authenticity ensures that a node is a real or trusted node in the network. In absence of authentication any malicious node can falsify a real node and hence can have an access to the confidential information of the trusted network.[ref]

ATTACKS:

There are two types of attacks on ad hoc networks - Passive Attacks and Active Attacks.

- 1. Passive Attacks:** - Passive attacks mainly target the networks just to steal the valuable information. Attackers do not disturb the normal network functioning of the network for example inducing or dropping false packets. They behave as if they are a part of network only.

It becomes very difficult to identify such attacks, because they do not initiate any malicious activity to disrupt the normal functioning of the network.

Examples of such types of attacks are traffic analyses, traffic monitoring and eavesdropping [3].

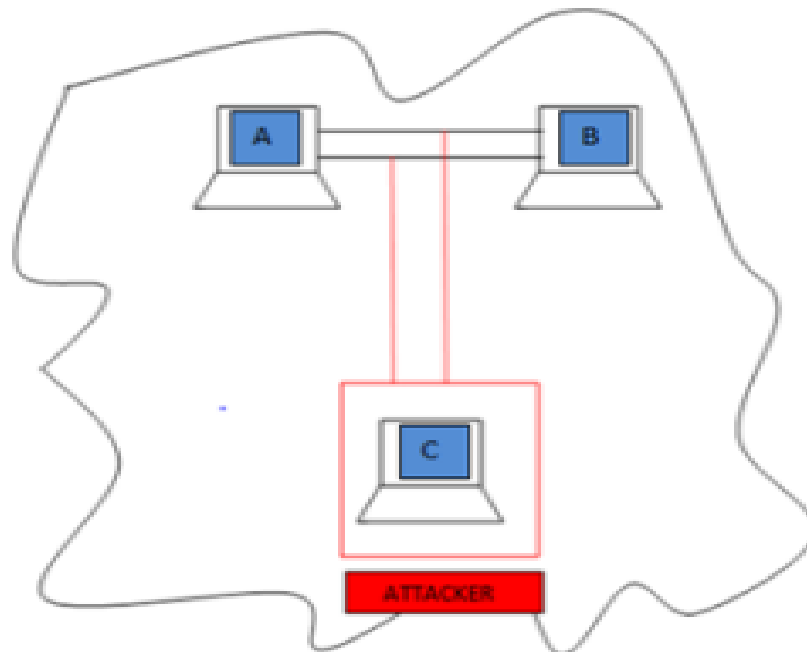


Figure 4: Demonstration of Passive Attack [3]

- 2. Active Attacks:** -Active attacks are type of attacks which actually interfere with the normal functioning of the network and active attackers tamper with the network traffic. Due to their active participation, they can be detected and prevented using suitable prevention algorithms. For example they cause congestion, and might propagate incorrect routing information etc. Examples of passive attacks include impersonation, fabrication, modification attack and message replay.[4]

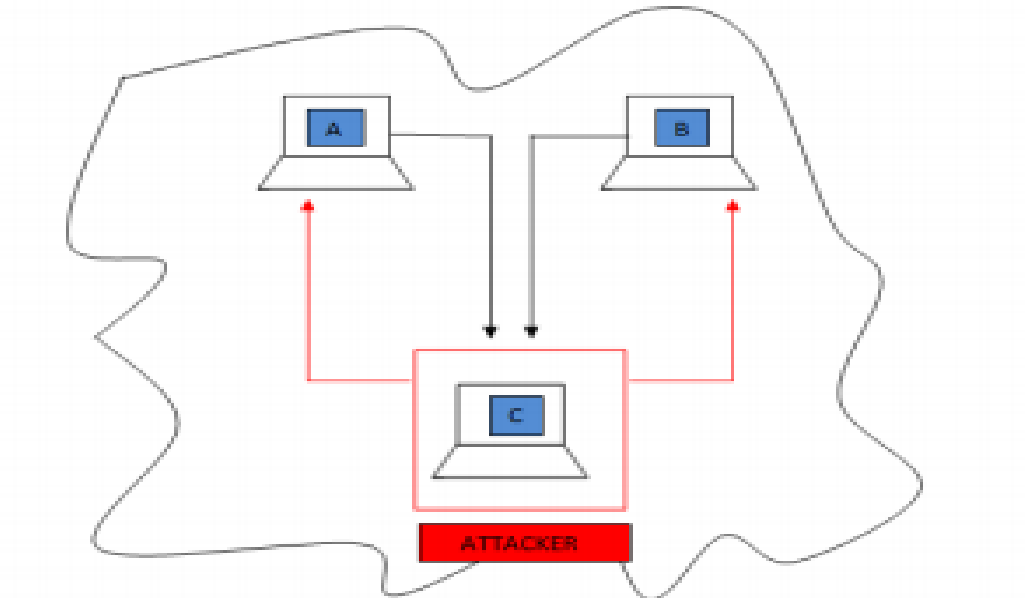


Figure 5: Demonstration of Active Attack [3]

There are attacks which can be classified depending upon the position of the attacker in the network.

1. **External attacks:** - External Attacks are the attacks made by the unauthorized nodes which are not a part of the network. In such kind of attacks attackers can flood false packets into the network, impersonation etc. Their main aim is to cause congestion or to disrupt normal functioning of the network [5].
2. **Internal attacks:** - Internal Attacks are caused by the authorized or legitimate nodes in the network. The reason for their malicious behaviour may be the following:
 - 2.1 Hijacking authorized nodes by some external attacker and then using them for launching internal attacks in the network.
 - 2.2 Internal nodes become selfish to save their limited resources like battery power, processing capabilities, and the communication bandwidth and exploiting other nodes for their benefit.

2.3 Routing Protocols and Challenges in Ad hoc Wireless Networks: [7][8]

ABSTRACT:

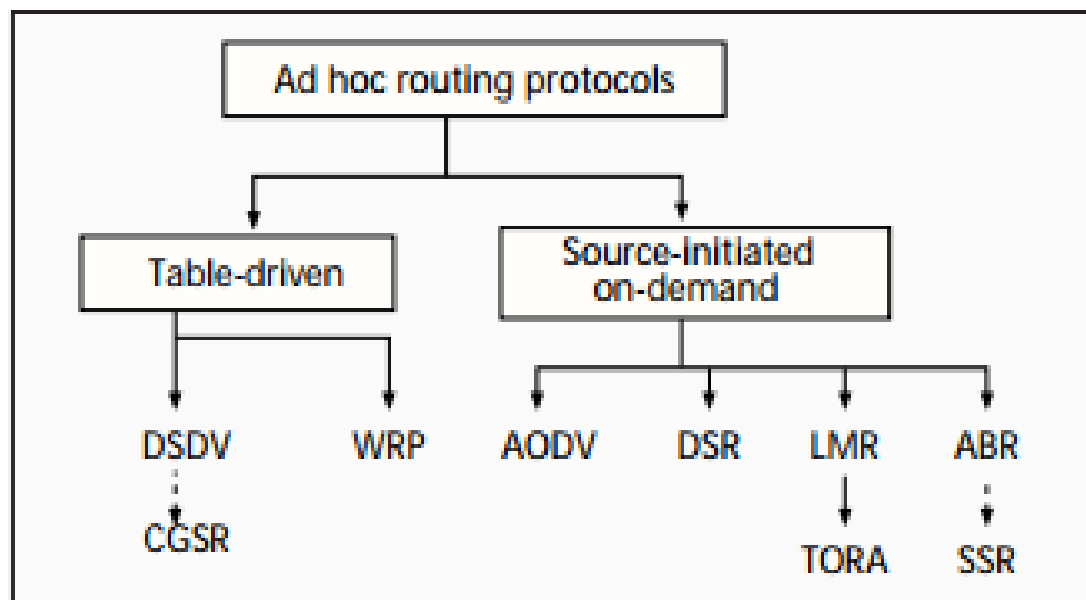


Figure 6: Categorization of ad hoc routing protocols [7]

Routing is the exchange of information or data packets from one station of networks to other. Protocol is the set of standard or rules to exchange data between two nodes. These protocols deal with the limitations of the networks, which include high power consumption of network, a high error rate and low bandwidth.

Some routing protocols are classified as:-

1. **Table driven**
2. **On-demand driven**
3. **Hybrid protocols.**

2.3.1 Table driven or Proactive: In Table-driven routing protocols each node in the network maintains one or more tables containing routing information to every other node in the network. In the table driven routing protocols each node maintains either one or two tables to store routing information and also it updates the table according to if any change of nodes in the network. The disadvantage of table driven, it has to maintain the additional control traffic to continually update route entries [6].

Some of Proactive routing protocols are:-

1. **DSDV** (Destination Sequenced Distance Vector)
2. **WRP** (Wireless Routing Protocols)
3. **DFR** (Direction Forward Routing)
4. **HSR** (Hierarchical State Routing Protocols)
5. **AWDS** (Ad hoc Wireless Distribution Service)
6. **CGSR** (Cluster Head Gateway Switch Routing Protocols)

2.3.2 On-Demand or Reactive: On demand or Reactive protocols produce routing table only when it is actually needed. When a node requires a route to a destination to send data packets, it initiates the route discovery process within the network at that instant only [7].

The main advantage is that reactive protocols are much suitable and perform better for ad hoc networks than any other protocols. The periodic updates are not required in on-demand routing protocols, due to this it uses low bandwidth as compared to table driven protocols. Some of the reactive routing protocols are:-

1. **AODV** (Ad hoc On-demand Distance Vector)
2. **DSR** (Dynamic Source Routing)

2.3 Hybrid Protocols: Hybrid protocol is the combination of both Proactive and Reactive protocols. In this routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes. Some of hybrid routing protocols are:-

1. **ZRP** (Zone Routing Protocols)
2. **OORP** (Order One Routing Protocols)

Comparison between Table driven and On Demand Routing Protocol:

The table-driven ad hoc routing approach is similar to the connectionless approach of forwarding packets, with no emphasis to when and how frequently such routes are desired. It relies on the routing mechanism in which table is updated regularly and involves the constant propagation of routing information.

However, for on-demand routing protocols when a node using an on-demand protocol desires a route to a new destination, it will have to wait until such a route can be discovered.

Because routing information is constantly propagated and maintained in table-driven routing protocols, a route to every other node in the ad hoc network is always available, regardless of whether or not it is needed. This feature, although useful for datagram traffic, incurs substantial signaling traffic and power consumption.

Both bandwidth and battery power are scarce resources in mobile computers, this becomes a serious limitation. All of the protocols, except for CGSR, use a flat addressing scheme. While flat addressing may be less complicated and easier to use, there are doubts as to its scalability.

A different approach from table-driven routing is source-initiated on-demand routing. This type of routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined.

Once a route has been established, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or until the route is no longer desired.[6]

CHALLENGES:

Vulnerability is a weakness in security system [6]. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable to security attacks than wired network.

Some of the vulnerabilities are:

- 1. Lack of centralized management:** MANET doesn't have a centralized monitoring server. Because of the absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc network.
- 2. Resource availability:** Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

3. **Scalability:** Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

4. **Cooperativeness:** Routing algorithms for MANETs usually assume that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications. Vulnerabilities of ad-hoc networks from a security point of view; there are several reasons why wireless ad-hoc networks are more vulnerable than their wired counterparts. Sybil attack is a serious threat for today's wireless ad hoc networks.

2.3 Study of various mobility models: [9] [10]

Mobility models are used to represent the movement of mobile users, and how their velocity, location and acceleration change over time. These kind of models are very frequently used for simulation purposes when new communication or navigation techniques are investigated.

For mobility modeling, the behavior or activity of a user's movement can be described using both analytical and simulation models.

The input given to analytical mobility models are simplifying assumptions regarding the movement behaviors of users. Such models can provide performance parameters for simple cases through mathematical calculations. Whereas simulation models consider more realistic and detailed mobility scenarios. Such models can derive valuable solutions for more complex cases [9].

Types:

1. Random Waypoint Mobility Model
2. Random Walk Mobility Model
3. Random Direction Mobility Model

2.4.1 Random Waypoint Mobility Model

The random waypoint mobility model contains pause time between changes in direction and/or speed. Once a node begins to move, it stays in one location for a specified pause time. After the specified pause time is elapsed, the randomly selects the next destination in the simulation area and chooses a speed uniformly distributed between the minimum speed and maximum speed and travels with a speed v whose value is uniformly chosen in the interval $(0, V_{max})$.

V_{max} is some parameter that can be set to reflect the degree of mobility. Thereafter, it continues its journey toward the newly selected destination at the chosen speed. As soon

as it arrives at the destination, it stays again for the indicated pause time before repeating the process [9] [10].

2.4.2 Random Walk Mobility Model

In this mobility model, a node moves from its current location to a new location by randomly selecting a direction and speed in which to travel. The new speed and direction are both chosen from pre defined ranges. Each movement in the Random Walk Mobility Model occurs in either at constant time interval 't' or a constant distance traveled 'd', at the end of which a new direction and speed are calculated. If any node reaches to the simulation boundary, it bounces off the simulation border with an angle determined by the incoming direction. The node then continues along this new path [10].

2.4.3 Random Direction Mobility Model

In random direction mobility model each node alternates periods of movement (move phase) to periods during which it pauses (pause phase). During the beginning of each move phase, a node independently selects its new direction and speed of movement. Speed and direction are kept constant for the whole duration of the node movement phase [10].

CHAPTER- 3

SYSTEM DEVELOPMENT

SOFTWARE DEVELOPMENT METHODOLOGY:

The establishment and use of sound engineering principles in order to obtain economically developed software that is reliable and works efficiently on real machines is called software engineering.

Software engineering is the discipline whose aim is:

1. Production of quality software
2. Software that is delivered on time
3. Cost within the budget
4. Satisfies all requirements.

A software life cycle is the series of identifiable stages that a software product undergoes during its lifetime .A software lifecycle model is a descriptive and diagrammatic representation of the software life cycle .A life cycle model represents all the activities required to make a software product transit through its lifecycle phases .It also captures the order in which these activities are to be taken.

Life Cycle Models:

There are various life cycle models to improve the software processes.

1. Waterfall Model
2. Prototype Model
3. Incremental Model.
4. Evolutionary Model.
5. Spiral Model.

In the project, Incremental Model of software development is followed.

INCREMENTAL MODEL

The incremental build model is a method of software development where the product is designed, implemented and tested incrementally a little more is added each time until the product is finished

In incremental model the whole requirement is divided into various phases. Multiple development cycles take place making the life cycle a “multi-waterfall” cycle. Cycles are divided up into smaller, more easily managed modules. Each module passes through the requirements, design, implementation and testing phases. A working version of software is produced during the first module, so we get working software early on during the software life cycle. Each subsequent release of the module adds function to the previous release. The process continues till the complete system is achieved.

- This model can be used when the requirements of the complete system are clearly defined and understood.
- Major requirements must be defined whereas; some details can evolve with time.
- There are some high risk features and goals.

In this project in the first phase nodes are given random speed direction according to the Random Waypoint mobility model. In which nodes change their direction when they touch the boundaries of the simulation area.

In second phase clusters using lowest-ID scheme are made and cluster-heads are elected.

In the third phase Sybil nodes are introduced and Sybil attacked is launched in the network of nodes.

Software Requirement Specification (SRS)

This section provides software requirements to a level of detail sufficient to enable designers to design the system and testers to test the system.

1. External Interface Requirements:

- User Interfaces:

Simulation area and number of nodes input screen: Various fields available on this screen will be:

- Simulation area
- Number of nodes

Start, pause and stop button screen: These buttons would be present on the same screen on which the movements of nodes will be shown.

Malicious node and number of Sybil nodes input Screen: Various fields available on this screen will be:

- Information related to malicious node
- Number of Sybil nodes

2. Software and Hardware Requirements

Operating System Requirements

Windows

- Windows 10
- Windows 8.x (Desktop)
- Windows 7
- RAM: 128 MB
- Disk space: 124 MB for JRE; 2 MB for Java Update
- Processor: Minimum Pentium 2 266 MHz processor
- IDE(Net beans)
- Support for printer for printing results

3. Software Product Features

Sequencing Information: All the information regarding simulation area, number of nodes, routing table malicious node and Sybil nodes should be handled sequentially, i.e., data should be stored only in a particular sequence to avoid any inconvenience

Error Handling: If any of the validations or sequencing flows does not hold true then appropriate error messages will be prompted to the user for doing the needful.

4. Software System Attributes:

Security: Only authorized users will be able to access the application by entering the correct login name and corresponding password.

Maintainability: The application can be maintained in present or future. It will be easy to incorporate new requirements in the individual modules.

Portability: As the website is java based so will be easily portable on various systems.

5. DIAGRAMS

5.1 DATA FLOW DIAGRAM:

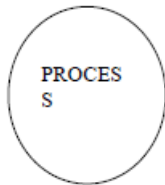
A DFD also known as ‘bubble chart’ has the purpose of clarifying system requirements and identifying major transformations. It shows the flow of data through a system. It is a graphical tool because it presents a picture.

DATA FLOW: The data flow is used to describe the movement of information from one part of the system to another part

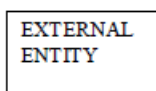
Data flow is represented by an arrow.



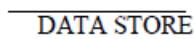
PROCESS: A circle or bubble represents a process that transforms incoming data to outgoing data. Process shows a part of the system that transform inputs to outputs.



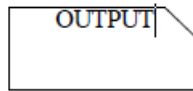
EXTERNAL ENTITY:-A square defines a source or destination of system data. External entities represent any entity that supplies or receive information from the system but is not a part of the system.



DATA STORE:-The data store represents a logical file. A logical file can represent either a data store symbol which can represent either a data structure or a physical file on disk. The data store is used to collect data at rest or a temporary repository of data. It is represented by open rectangle.



OUTPUT:-The output symbol is used when a hard copy is produced and the user of the copies cannot be clearly specified or there are several users of the output.



LEVEL 0 DFD (Context Diagram)

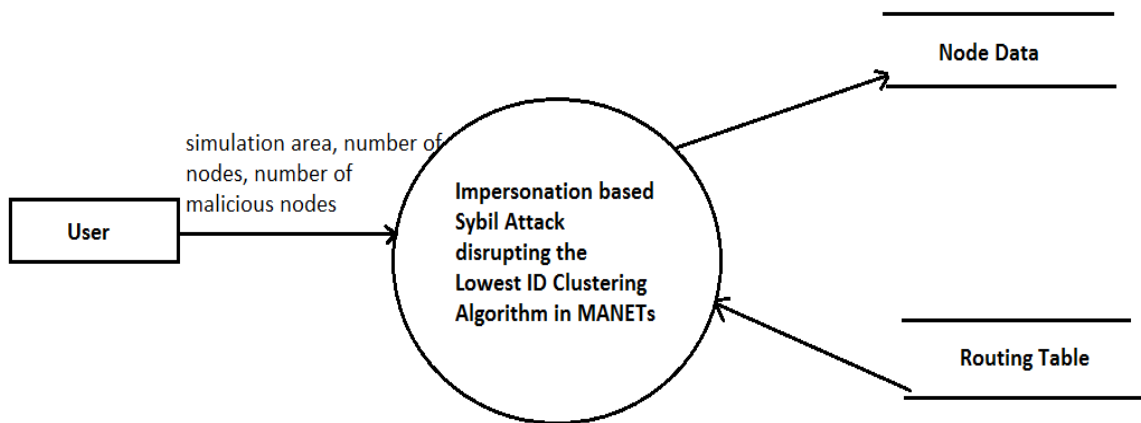


Figure 7.1: Zero Level DFD

LEVEL 1 DFD

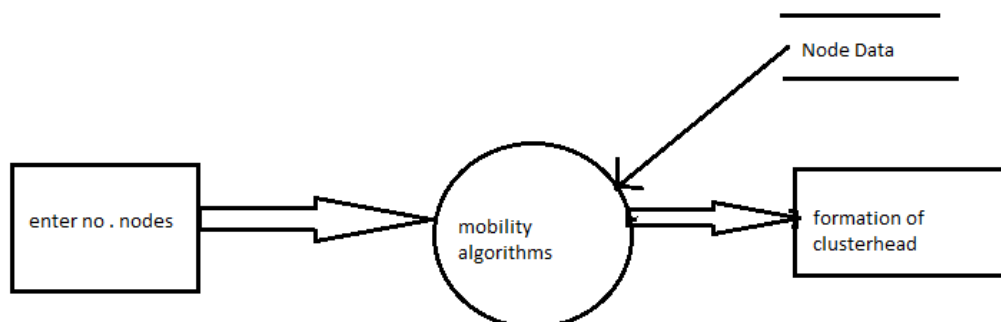


Figure 7.2: First Level DFD

LEVEL 2 DFD

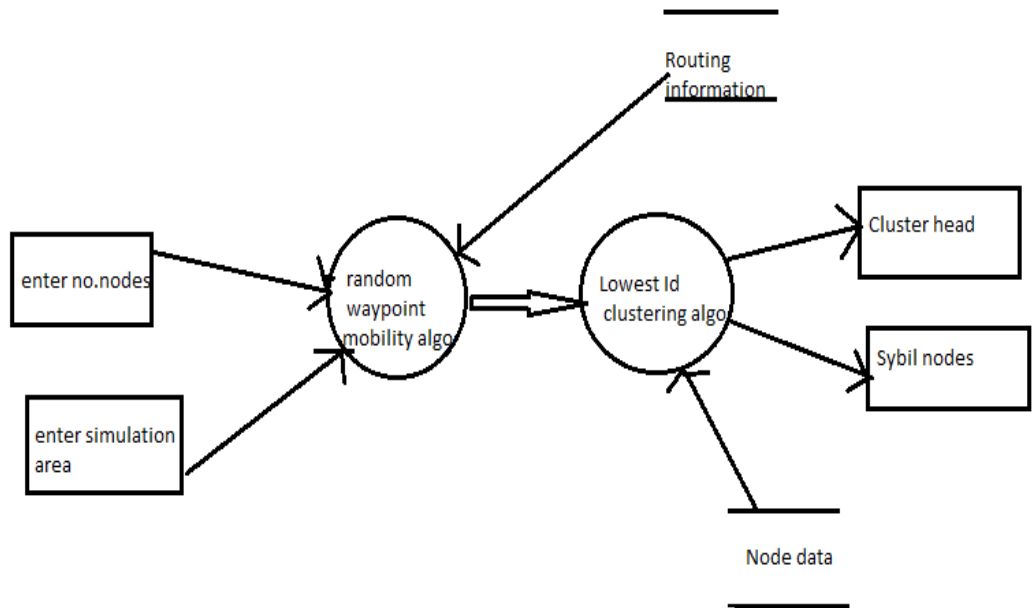


Figure 7.3: Second Level DFD

5.2 Use Case Diagram:

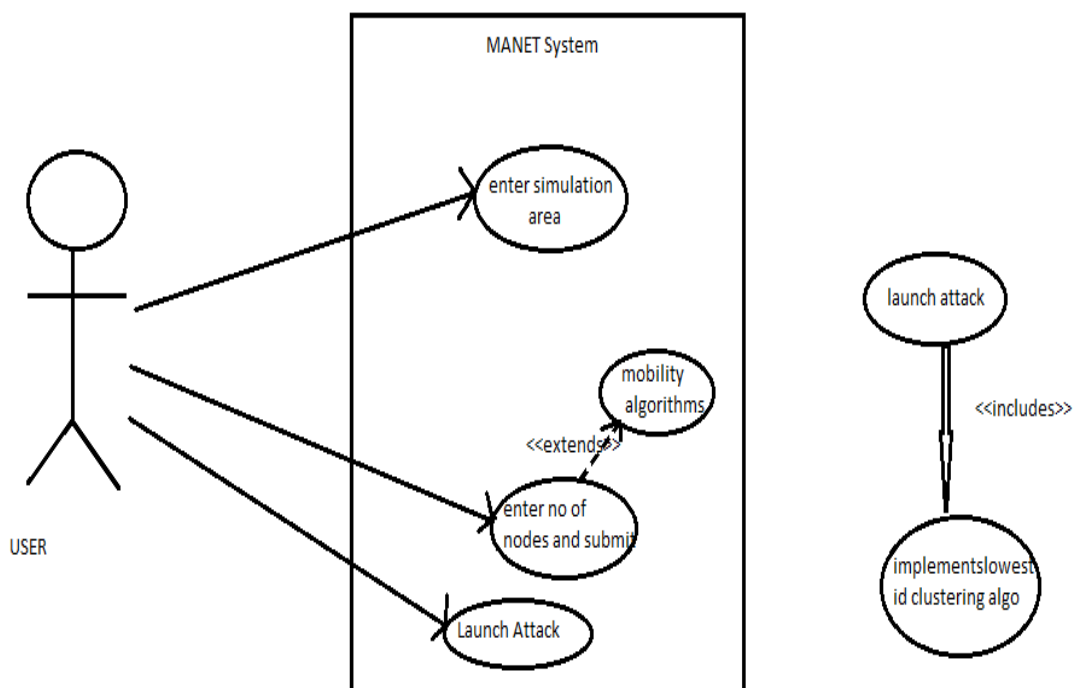


Figure 8: Use case diagram

FUNCTIONAL REQUIREMENTS

It deals with the functionalities required from the system which are as follows:

- The application will help in better understanding of network security attacks in MANETs.
- Only authorized users (attackers) can use the application or make any modification.
- The simulation area and initial number of nodes will be entered on the run time.
- The velocity of each node will be random and different.
- The nodes will change their directions after random time intervals.

The technologies used to develop this application:

FRONTEND (Languages):

Java

Applet

NON FUNCTIONAL REQUIREMENTS

They are the quality requirements that stipulate how well software does what it has to do.

Performance

After taking input from user about the nodes, the adjacency table of each node will be calculated as per the rules in less than a second.

Availability

If in future this application is converted into a web application then it should have 24*7 availability, i.e., it can be accessed for 24 hours a day.

For this UPS support must be on the server site with a backup of at least 8 hours in case of power failure.

Reliability

It means the extent to which program performs with required precision. The application developed should be extremely reliable and secure.

Usability

The application should be user friendly and should require least effort to operate.

Portability

The application is made using JAVA which is platform independent and can be transported to other systems with minimum effort. Therefore java makes the application a portable application.

Flexibility

It is effort required to modify operational program. The whole application should be made using independent modules so that any changes done in 1 module should not affect the other one and new modules can be added easily to increase functionality.

Design and Development

Algorithm:

Assumptions:

1. Lets say we have N number of nodes in a Mobile Ad Hoc Network, at any instant of time with their IDs as $x_i: i= 1,2,\dots,N$.
2. We will introduce one node in the network, say, m_x is a malicious node.
3. The malicious node m_x is capable of introducing its Sybil nodes by varying the transmission power.
4. Malicious node will behave normally for some time and then this malicious node will gain the access to the necessary information about the network including its neighbours and their IDs.
5. In the next step the malicious node m_x generates S number of Sybil nodes that can communicate with the legitimate neighbouring nodes. Here the IDs of Sybil nodes are $N_j: j = 1,2,\dots,S$, where $S < N$.
6. These IDs are chosen such that they are less than the other ID's in the network
 $N_j > N_i$
7. Now, in addition to itself, the malicious node will also include its Sybil nodes for the selection of cluster head. Since the IDs of all the Sybil nodes is greater than the IDs of all other legitimate nodes in the networks, the legitimate node with the lowest ID will become cluster head, repeatedly[4].

In addition, the Sybil attacker node m_x will also use its Sybil nodes to communicate again and again using its different IDs so as to keep the head node busy all the time, until its battery is drained, completely.

8. After the battery of this cluster head node is drained completely, the malicious node can impersonate its ID and assign it to one of its Sybil nodes to make it a cluster head.

Algorithm to calculate clusters:

Make an array $ch[]$ which will store the cluster heads and an array $d[]$ which will initialize all the nodes with a count.

Calculate the distance between two nodes by using:

$$\text{Math.sqrt}(\text{Math.pow}((x[i])-(x[j]), 2)+\text{Math.pow}((y[i])-(y[j]), 2))$$

for every node i

do

If $d[i]$ is not zero

Then

$ch[i]=1$

$g.\text{drawOval}()$

$d[i]=0;$ // set count to zero for that node

end if

for every node j

do

If distance <120

$d[j]=0;$

end for

end for

Through this algorithm if a node has become cluster head once then it will not participate in the cluster head selection and the next node with the lowest ID is made cluster head and so on.

SLEEP DEPRIVATION ATTACK:

The idea of the sleep deprivation attack was proposed by Stajano. [1]The main victim of this attack is a computing device which is battery powered, such as a sensor node, which attempts to remain in a low power sleep mode for as long as would possible without adversely affecting the node's applications.

The attacker launches a sleep deprivation attack by interacting with the victim in a manner that appears to be legitimate; however, the purpose of the interactions is to keep the victim node out of its power conserving sleep mode. Thus this attack can be used to dramatically reduce the lifetime of the victim. Further, this attack is difficult to detect given that it is carried out solely through the use of seemingly innocent interactions.

VAMPIRE ATTACK:

Vampire attack is such kind of attack whose aim is to disrupt the network by draining resource capability. In this attack, Attacker communicates worthless messages which are usually known as false packet to increase network traffic and make target node busy in useless activity. [14]

Vampire attack is energy draining attack where messages send by the malicious node which causes more energy consumption. Complex and large messages are sent by the malicious node. This energy consumption is very high and leading to slow depletion of network node's battery life.

Vampire attacks are not protocol-specific, i.e. They do not rely on design properties or implementation faults of particular routing protocols, but they exploit general properties of protocol classes such as link-state, distance vector, source routing and geographic.

These attacks do not rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain, so it takes large energy to transmit the data and consumes the node energy [15].

FEASIBILITY STUDY

Feasibility study means Can we build software to meet this scope? Is the project feasible? When we are developing the system software, we must know the proposed system will be feasible or i.e. practically implemented or not it may possible the proposed system may not implemented due to many reasons like it may take long time in development than the specified time limit ,cost may increase than proposed one etc. Therefore we must analyse the feasibility of the system.

Feasibility is the analysis of risks, costs & benefits relating to economics, technology& user operation.

There are several types of feasibility depending on the aspect they covers.

Some important feasibility is as follows:-

1. Technical Feasibility
2. Operational Feasibility
3. Economical Feasibility

1. TECHNICAL FEASIBILITY:-

The technically feasibility study basically centres on alternatives for hardware, software and design approach to determine the functional aspects of system.

Here we are using IDE (Net beans). Hardware requirements used are compatible with all O.S. Only authorized person would be able to use the application so it would be secure. The system can also be expanded as per the needs of requirement specification.

OPERATIONAL FEASIBILITY:-

Operational Feasibility is a measure of how people are able to work with system. This type of feasibility demands if the system will work when developed and installed.

Since application is very user friendly so users will find it comfortable to work on this site.

ECONOMICAL FEASIBILITY

Economic analysis is the most frequently used evaluating the effectiveness of proposed system, more commonly known as Benefit analysis. The Benefit analysis is to determine benefits and savings which are expected from candidate system and compare them with cost. If the benefits are more than the cost, then decision is made to design and implement the system. The cost and benefits may be direct or indirect and tangible or intangible.

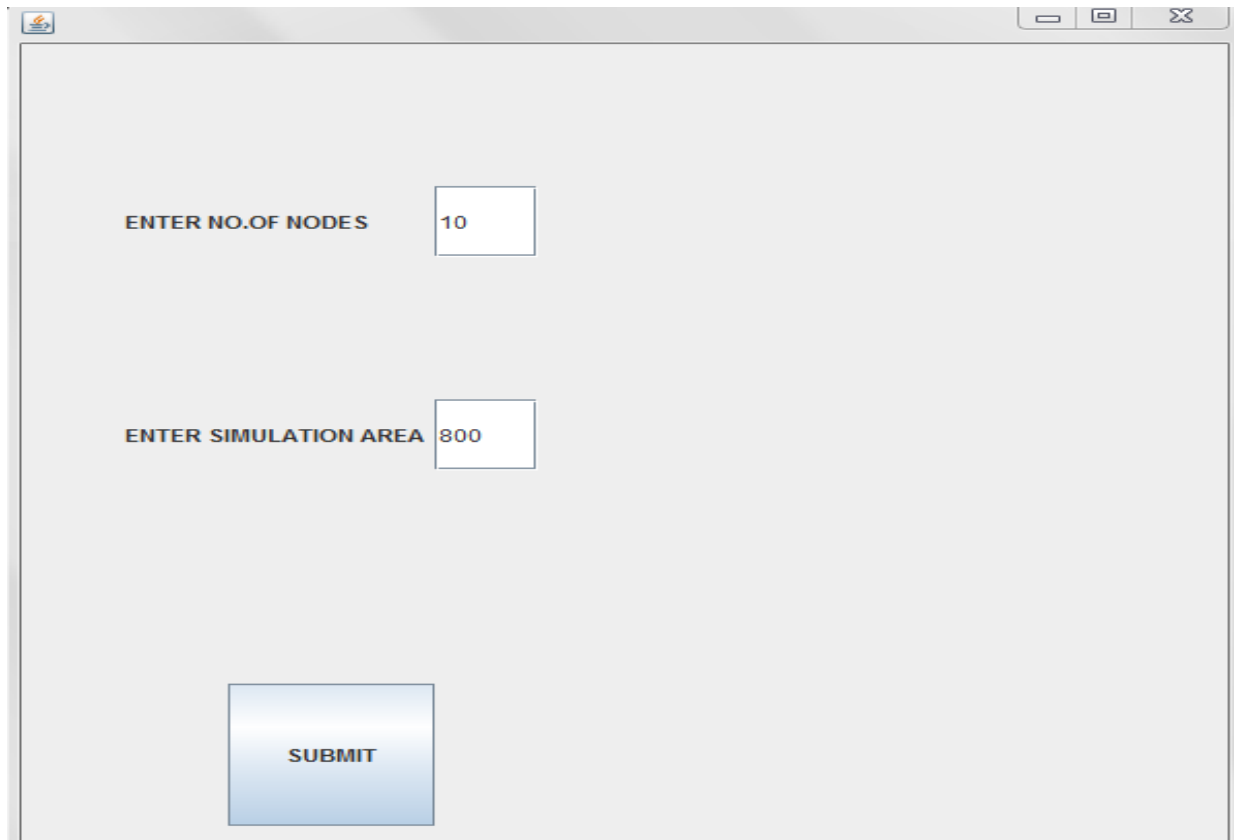
TESTING

- Software testing is the process of executing a program with intension of finding errors in the code. It is a process of evolution of system or its parts by manual or automatic means to verify that it is satisfying specified or requirements or not.
- Generally, no system is perfect due to communication problems between user and developer, time constraints, or conceptual mistakes by developer.
- To purpose of system testing is to check and find out these errors or faults as early as possible so losses due to it can be saved.
- Testing is the fundamental process of software success.
- Testing is not a distinct phase in system development life cycle but should be applicable throughout all phases i.e. design development and maintenance phase.
- Testing is used to show incorrectness and considered to success when an error is detected.

CHAPTER- 4

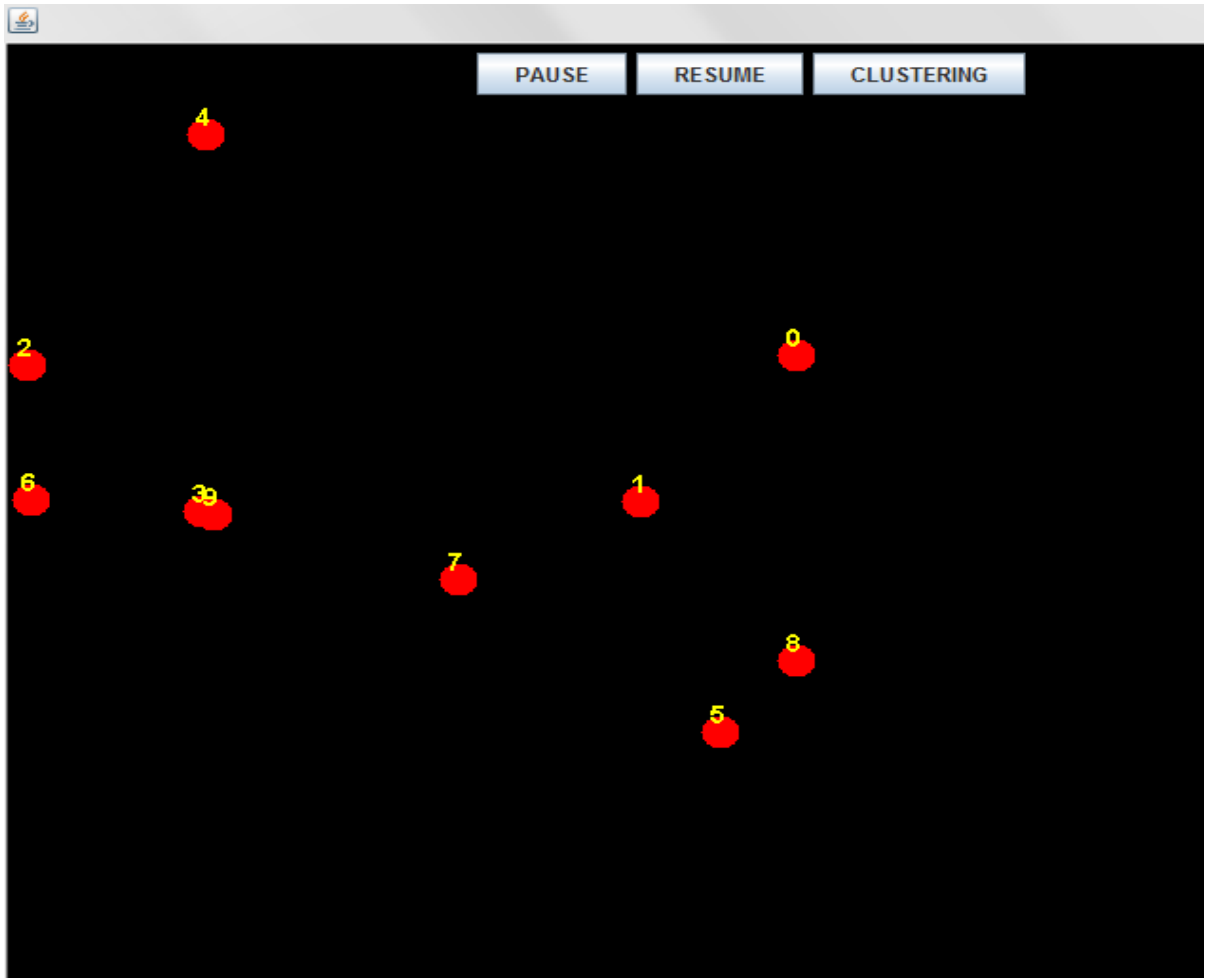
PERFORMANCE ANALYSIS

Screenshots:



The screenshot shows a web application window with a light gray background. At the top left, there is a small icon. At the top right, there are standard window control buttons (minimize, maximize, close). The main content area contains two input fields and a submit button. The first input field is labeled "ENTER NO.OF NODES" and contains the value "10". The second input field is labeled "ENTER SIMULATION AREA" and contains the value "800". Below these fields is a blue button with the text "SUBMIT".

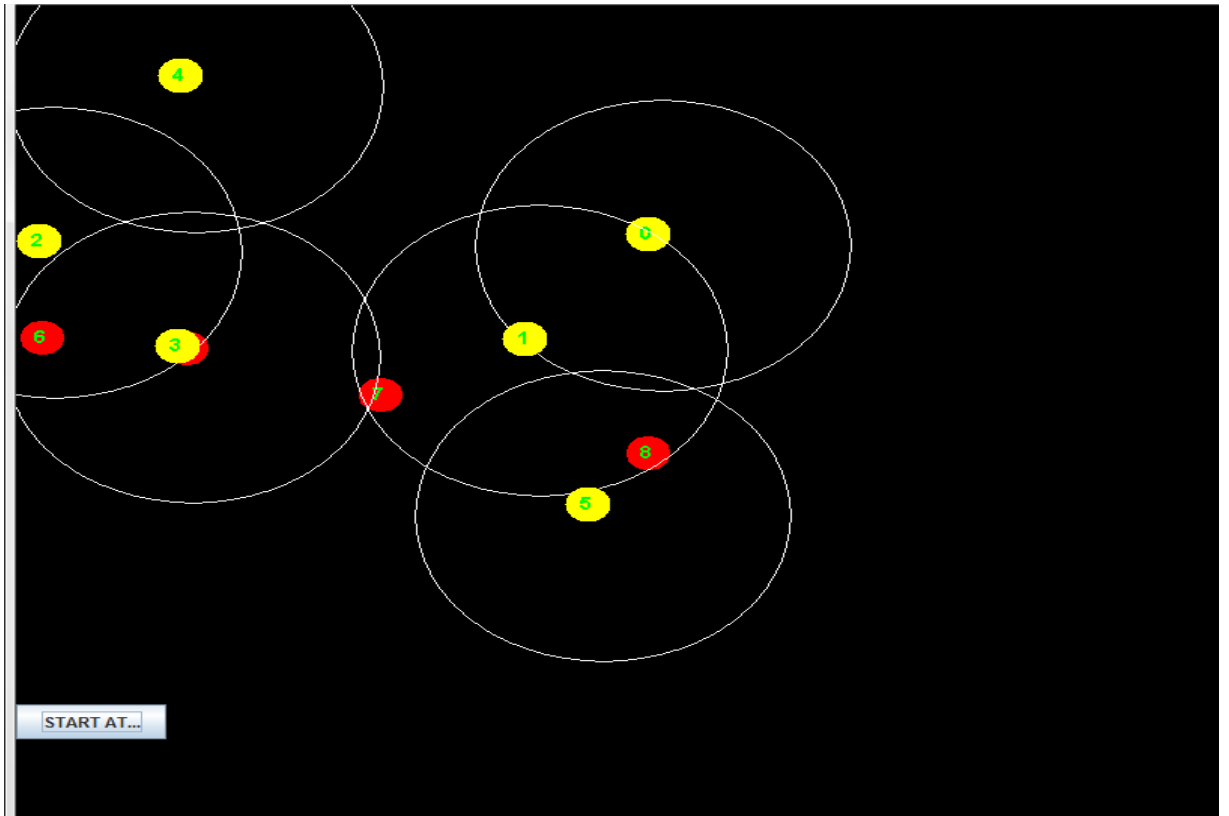
This is the home page of the application. The application will start executing when 'SUBMIT' button will be pressed. User is asked to enter the simulation area and number of nodes he want to enter in the network.



After pressing the submit button nodes will appear on the simulation area and will start moving at random speed and direction.

When nodes reach the boundary of the simulation area they change their direction speed. We can pause and resume the movement of the nodes by pressing the buttons provided in the panel.

Whenever we want to start clustering press the clustering button a new panel will appear.



Clustering is done according to lowest ID clustering algorithm .The node with lowest ID is made cluster head and these are:

```
cluster head is 1
cluster head is 0
cluster head is 3
cluster head is 4
cluster head is 5
```

There are three types of nodes which **are normal nodes** that are member of one cluster only.

Cluster heads which are responsible for resource allocation and the management of cluster.

And **gateway nodes** which are member of more than one clusters .Gateway node can cater to both the cluster heads involved.

For example **node 8** is a gateway node.

Cluster heads only hears nodes with ID's higher than themselves.

CHAPTER-5

CONCLUSIONS

5.1 CONCLUSION:

Clustering sensor nodes and organizing them hierarchically have proven to be an effective method to provide better data aggregation and scalability for the sensor network while conserving limited energy.

In an impersonation based Sybil attack, a malicious can disrupt the lowest ID based cluster algorithm by presenting multiple Sybil nodes with IDs greater than its neighbouring legitimate nodes a legitimate node with lowest ID is targeted to make it cluster head again and again, and finally its battery is drained, also the multiple Sybil nodes are utilized to communicate repeatedly with the cluster head so as to make it busy all the time. After the battery of cluster head is completely drained, the malicious node can impersonate its ID for one of its Sybil node to become the cluster head.

If malicious nodes are greater in number and are spread across all over the network, the impact of the Sybil attack will be more on this clustering scheme, as most of the clusters will now be under the control of these Sybil nodes.

The Lowest-ID scheme concerns only with the lowest node ids which are assigned arbitrarily without considering any other conditions of a node for election as a cluster head. Because the node ids do not change with time, those with lowest ids are more likely to become cluster heads than nodes with larger ids. Thus, drawback of lowest ID algorithm is that some nodes are prone to power drainage because they are serving as cluster heads for longer periods of time.

An ordinary node is allowed to belong to multiple clusters, and if it does, it may be used as a gateway node, which is used for relaying data between clusters. [12]

The attack becomes more destructive and difficult to detect if the malicious node presents its fake identities by varying the transmission power. Malicious node can take advantage of it in following ways:

1. It cannot be detected on the basis of same signal strengths of its Sybil nodes.
2. By decreasing the transmission power for different Sybil nodes, the message will not reach all the neighbours of the malicious node and hence cannot be detected on the basis of the fact that if a set of nodes are seen together for a long period of time by an observer node, then they are suspected to be the identities of Sybil attacker.

So, here we investigated ways by which a Sybil attack can disrupt the head selection mechanism of lowest ID clustering method.

5.2 Future Scope

The main objective of this study is to provide a better understanding of challenges offered by the Sybil attack on this type of routing protocol, and to understand that how Sybil attack can affect the network system and routing protocols so that in future better solutions can be developed to detect and overcome this network security threat.

REFERENCES

- [1] Stefano Basagni Northeastern University, Marco Conti (CNR), Silvia Giordano University of applied sciences Switzerland Ivan Stojmenovic University of Ottawa
MOBILE AD HOC NETWORKING
- [2] Shikha Jain Department of Computer Science, Delhi University, New Delhi, India
SECURITY THREATS IN MANETS: A REVIEW
- [3] Ian F. Akyildiz, Xudong Wang, Weilin Wang Wireless mesh networks: a survey
- [4] Amol Vasudeva¹ and Manu Sood² Department of Computer Science & Engineering and Information Technology, Jaypee University of Information Technology, Wazirpur, Solan, Himachal Pradesh, India
² Department of Computer Science, Himachal Pradesh University, Summer Hill, Shimla, Himachal Pradesh, India SYBIL ATTACK ON LOWEST ID CLUSTERING ALGORITHM IN THE MOBILE AD HOC NETWORK
- [5] Dr. Aarti and Dr. S. S Tyagi. Comparative Analysis of Various Attacks on MANET Pooja Chahal, Gaurav Kumar Tak India Anurag Singh Tomar Department of Computer Science Lovely Professional University Phagwara, India STUDY OF MANET: Characteristics, Challenges, Application and Security Attacks by
- [6] C.K TOH Ad hoc Mobile wireless Networks PROTOCOLS AND SYSTEMS Age of pervasive Mobile networking and computing
- [7] Elizabeth M. Royer, University of California, Santa Barbara Chai-Keong Toh, Georgia Institute of Technology: A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks

[8] D.Baker et al., “Flat vs Hontrol Architecture,” ARO/DARPA Wkso. Mobile Ad-hoc Networking

[9]Christian Bettstetter, Hannes Hartenstein, Xavier Pérez-Costa Stochastic Properties of the Random Waypoint Mobility Model

[10] Fan Bai and Ahmed Helmy University of Southern California,U.S.A
A SURVEY OF MOBILITY MODELS in Wireless Adhoc Networks

[11] Dr. A K Verma Department of Computer Science and Engineering Thapar University Patiala an Introduction MOBILE ADHOC NETWORKS (MANETs)

[12] Hao Wu and Zhangdui Zhong State Key Laboratory of Rail Traffic Control and Safety Beijing Jiaotong University Beijing, China A Cluster-head Selection and Update Algorithm for Ad Hoc Networks.

[13] Herbert Schildt, Complete Reference JAVA, 5th edition, Tata McGraw Hill.

[14] Anamika Garg Department of CSE, RGPV University Mayank K Sharma Asst. Professor, Department of CSE, RGPV University, Detection and Prevention of Vampire Attack in MANET

[15] Eugene Y. Vasserman* and Nicholas Hopper Kansas State University University of Minnesota, Draining life from wireless ad-hoc sensor networks

Web links:

[16] <http://www.isr.umd.edu/courses/workshops/MANET/program.html>, Mar. 1997

[17] <http://www.intechopen.com/books/mobile-ad-hoc-networks-applications>

[18] https://www.google.nl/search?q=a+mobile+adhoc+network&espv=2&biw=1366&bih=643&source=lnms&tbn=isch&sa=X&ved=0ahUKEwiDncry7fnMAhXMmBoKHSnsDF8Q_AUIBigB#imgrc=jm6rtlB04KWUCM%3A

Tool used for Diagrams:

Visual paradigm