

**A Mechanism to Increase Quality of Service by Improving Security  
in Mobile Ad-hoc Network**

*Dissertation submitted in fulfilment of the requirements for the Degree of*

**MASTER OF TECHNOLOGY  
in  
COMPUTER SCIENCE AND ENGINEERING**

By  
**Ankit Singh**

**11205627**

Under the guidance of

**Mr.Gurpreet Singh**  
**(Associate Professor)**

(APRIL 2017)



**L** OVELY  
**P** ROFESSIONAL  
**U** NIVERSITY

---

@ Copyright LOVELY PROFESSIONAL UNIVERSITY, PUNJAB (INDIA)

April, 2017

ALL RIGHTS RESERVED

## TOPIC APPROVAL PERFORMA

School of Computer Science and Engineering

**Program:** 1202D: B.Tech -M.Tech (Dual Degree) - CSE

**COURSE CODE:** CSE545

**REGULAR/BACKLOG :** Regular

**GROUP NUMBER :** CSERGD0028

**Supervisor**

**Name:** Mr.Gurpreet Singh

**UID :** 17671

**Designation :** Assistant Professor

**Qualification :** \_\_\_\_\_

**Research Experience :** \_\_\_\_\_

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Ankit Singh	11205627	2012	K1209	8288882835

**SPECIALIZATION AREA:** System Architecture and Design

**Supervisor Signature:** \_\_\_\_\_

**PROPOSED TOPIC:** A Mechanism to Increase Quality of Service by Improving Security in Mobile Ad-hoc Network

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	Parameter	Rating (out of 10)
1	Project Novelty: Potential of the project to create new knowledge	6.33
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	7.00
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	6.67
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	7.33
5	Social Applicability: Project work intends to solve a practical problem.	6.33
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	7.17

PAC Committee Members		
PAC Member 1 Name: Gaurav Pushkarna	UID: 11057	Recommended (Y/N): Yes
PAC Member 2 Name: Mandeep Singh	UID: 13742	Recommended (Y/N): Yes
PAC Member 3 Name: Er.Dalwinder Singh	UID: 11265	Recommended (Y/N): Yes
PAC Member 4 Name: Balraj Singh	UID: 13075	Recommended (Y/N): Yes
PAC Member 5 Name: Harwant Singh Arri	UID: 12975	Recommended (Y/N): Yes
DAA Nominee Name: Kanwar Preet Singh	UID: 15367	Recommended (Y/N): Yes

**Final Topic Approved by PAC:** A mechanism to increase quality of service by improving security in mobile ad-hoc network

**Overall Remarks:** Approved

**PAC CHAIRPERSON Name:** 11011::Rajeev Sobti

**Approval Date:** 26 Oct 2016

## **ABSTRACT**

---

With an instant increase of wire free networks and mobile computing application, Quality of Service (QoS) of mobile ad-hoc network (MANET) has grasps the interest of various researchers. Security is the significant property in QoS, facilitated to the MANETs environment. Not having any safety system from the security mechanism, attacks over QOS can lead to routing failure, intervention of reserve resource or failing of QOS facilities. MANET's properties like limited computation capacity, limited communication and battery power, instant change in topology, the traditional are not sufficient enough to provide security to the network. Therefore a novel security technique is required. In this thesis the security problems are addressed for networks QoS system. This research will design Security mechanism to alleviate the effect of malicious behaviour of Blackhole node in the network.

## DECLARATION

---

I hereby declare that the research work reported in the dissertation entitled “**A Mechanism to Increase Quality of Service by Improving Security in Mobile Ad-hoc Network**” in partial fulfilment of the requirement for the award of Degree for Master of Technology in **Computer Science and Engineering** at **Lovely Professional University, Phagwara, Punjab** is an authentic work carried out under supervision of my research supervisor **Mr. Gurpreet Singh**. I have not submitted this work elsewhere for any degree or diploma.

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

Date:

Investigator  
Name **Ankit Singh**  
RegNo. **11205627**

## **SUPERVISOR'S CERTIFICATE**

---

This is to certify that the work reported in the M.Tech Dissertation entitled “**A Mechanism to Increase Quality of Service by Improving Security in Mobile Ad-hoc Network**”, submitted by **Ankit Singh** at **Lovely Professional University, Phagwara, India** is a bonafide record of her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree

Signature of Advisor

Name: **Mr.Gurpreet Singh**

Date:

**Counter Signed by:**

**1) Concerned HOD:**

HoD's Signature: \_\_\_\_\_

HoD Name: \_\_\_\_\_

Date: \_\_\_\_\_

**2) Neutral Examiners:**

**External Examiner**

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Affiliation: \_\_\_\_\_

Date: \_\_\_\_\_

**Internal Examiner**

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Date: \_\_\_\_\_

## ACKNOWLEDGMENTS

---

The satisfaction that accompanies the successful completion of any task would be incomplete without the mention of people whose ceaseless cooperation made it possible, whose constant guidance and encouragement crown all efforts with success.

I would like to convey my most heartfelt and sincere gratitude to my mentor **Mr. Gurpreet Singh** for his valuable guidance, advice, understanding and supervision throughout the development of this dissertation study. His willingness to motivate me contributed tremendously to achieve the goal successfully. I would like to thank to the **Project Approval Committee members** for their valuable comments and discussions.

I owe my thanks to my family and friends for their consistent moral support. They are ones who have encouraged me at every step of my life.

Name **Ankit Singh**

RegNo. **11205627**

# TABLE OF CONTENTS

---

	<b>Page</b>
ABSTRACT.....	i
DECLARATION.....	ii
CERTIFICATE.....	iii
ACKNOWLEDGMENTS.....	iv
TABLE OF CONTENTS.....	v
LIST OF FIGURES.....	vii
LIST OF TABLES.....	viii
<b>Chapter 1.....</b>	<b>1</b>
<b>INTRODUCTION .....</b>	<b>1</b>
1.1 Wireless Networks.....	1
1.2 Suitability Offered from Wireless Networks.....	1
1.3 Types of Networks.....	2
1.3.1 Personal Area Network (PAN).....	2
1.3.2 Local Area Network (LAN).....	2
1.3.3 Wide Area Network (WAN).....	2
1.3.4 Wireless Local Area Network (WLAN).....	4
1.4 IEEE 802.11 Standards, Specifications and Technologies.....	4
1.5 Wireless Local Area Network Modes.....	6
1.6 Infrastructure Network.....	6
1.7 Mobile Ad-Hoc Networks .....	8
1.8 MANET Application .....	10
1.9 Issues in Mobile Ad-Hoc Networks .....	12
1.10 Quality of Service .....	12
1.11 Quality of Service Metrics .....	13
1.12 MANET Characteristics .....	14
1.13 MANET Security .....	15
1.14 MANETs Vulnerabilities .....	16
1.15 Attacks in MANETs .....	17
1.16 Routing Protocol Techniques for MANET .....	18
<b>Chapter 2 .....</b>	<b>23</b>
<b>LITERATURE REVIEW .....</b>	<b>23</b>



<b>Chapter 3 .....</b>	<b>36</b>
<b>SCOPE OF THE STUDY.....</b>	<b>36</b>
<b>Chapter 4 .....</b>	<b>37</b>
<b>OBJECTIVE OF THE STUDY .....</b>	<b>37</b>
4.1 Problem Definition .....	37
4.2 Objectives .....	37
<b>Chapter 5 .....</b>	<b>38</b>
<b>NETWORK SIMULATOR (NS-2).....</b>	<b>38</b>
5.1 Network Simulator.....	38
<b>Chapter 6 .....</b>	<b>40</b>
<b>RESEARCH METHODOLOGY .....</b>	<b>40</b>
<b>Chapter 7 .....</b>	<b>41</b>
<b>OUTCOMES .....</b>	<b>41</b>
<b>Chapter 8 .....</b>	<b>48</b>
<b>SUMMARY AND CONCLUSION.....</b>	<b>48</b>
<b>LIST OF REFERENCES .....</b>	<b>49</b>

## LIST OF FIGURES

---

	<b>Page</b>
Figure 1 - Wireless technology interconnection in diverse environments.....	3
Figure 2 - graph of Data rates and mobility for different wireless technology.....	3
Figure 3 - IEEE 802 family and relation with the ISO models.....	5
Figure 4 - Wi-Fi certified logos with SII.....	5
Figure 5 - Infrastructure Network.....	6
Figure 6 - Ad-hoc Network.....	6
Figure 7 - demonstration of Extended Service Set (ESS).....	7
Figure 8 - Wireless Distribution System.....	8
Figure 9 - Mobile Ad-Hoc Networks.....	9
Figure 10 - Public Safety System .....	10
Figure 11 - Vehicular Ad-Hoc Networks .....	11
Figure 12 - Military Mobile Communication Networks.....	12
Figure 13 - Structure of Twofish algorithm .....	28
Figure 14 - Flowchart of proposed Black Hole Detection Algorithm .....	32
Figure 15 - Black Hole Detection Algorithm .....	32
Figure 16 - flow chart represent the proposed method.....	33
Figure 17 - Proposed Method.....	35
Figure 18 - NS-2 schema.....	38
Figure 19 - Proposed method for Black Hole Node .....	40
Figure 20 - Simulation of RREQ Packet in NS-2.35.....	44
Figure 21 - Simulation of RREP Packet in NS-2.35.....	44
Figure 22 - Simulation of Packet Transmission in NS-2.35.....	45
Figure 23 - Simulation of Blackhole Attack in NS-2.35.....	45
Figure 24 - Average End to End Delay.....	46
Figure 25 - Packet Delivery Ratio.....	46
Figure 26 - Packet Drop Ratio.....	47
Figure 27 - Throughput.....	47

## LIST OF TABLES

---

	<b>Page</b>
Table 1 - Comparison of 802.11 standards.....	4
Table 2 - Outcomes of Average End to End Delay under Blackhole Attack.....	41
Table 3 - Outcomes of Throughput under Blackhole Attack.....	41
Table 4 - Outcomes of Packet Delivery Ratio under Blackhole Attack.....	42
Table 5 - Outcomes of Packet Drop Ratio under Blackhole Attack .....	43

# Chapter 1

## INTRODUCTION

---

*“It shouldn't surprise you that a system that is designed to be manufactured as cheaply as possible is designed with no security constraints whatsoever”. Peter Neumann*

The Wireless Networks was invented in 1970 under the supervision of Defence Advanced Research Projects Agency (DARPA) in United State of America. The first Wireless Data Network is called “Packet Radio Network” which was designed, built and performed by Bolt, Bernanke and Newman Technologies (BBN) and SRI International. This Packet Radio Network system anticipated the Internet and has played a measure role in motivating for the Internet Protocol suite. In 1980's Survivable Radio Network (SURAN) project was successfully executed by DARPA. Packet Radio networks system did not progress much further until the wireless ad-hoc networks are innovated due to slower data rate, and it was inefficient in maintaining its links in high mobility condition and was bulky elements. Later in mid of 1990's the inexpensive 802.11 radio card came for personal computers. The roots of wireless technology are found in Military advancement. These days wireless ad-hoc network are essentially produced for military utility.

### **1.1 Wireless Networks**

Wireless communication are very useful to share information between devices without using any wired framework. By utilising electromagnetic waves, mobile device can communicate through transmitting and receiving information over the wireless medium. Wireless communication expands from homes network to satellites communication, from Mobile communication to walkie-talkies communication. The wireless communication are becoming more popular because of its mobility, flexibility, simplicity and cost saving installation benefits, specifically from past few decades the mobility requirements of client are rising exponentially and growth in the usage of laptops, personal computer and personal digital appliance are itself the major cause for the acceptance of wire free network.

### **1.2 Suitability Offered from Wireless Networks**

**Mobility:** - The most noticeable advantage of the wireless networks that users are able to roam in the range and remain connected to the wireless network which means now while moving client can join to the current network also enjoy the freedom.

**Simplicity:** - All are able to convert simplicity into fast growth. It is straightforward to set up a Wire free network, in comparison to a network connected through wires.

**Flexibility:** - Wire free communicating network covers a large amount of range which can reach wherever wired infrastructure can't be deployed. This network is extremely helpful to those places where wired links are not practical like traditional block of buildings.

### **1.3 Types of Networks**

Wireless network allows user to share information with each other, use application and access information in a wireless environment. It provide an ability to deliver the service of application to user through wireless medium. According to transmission range, three types of wireless network has been identified.

- Personal Area Network (PAN),
- Local Area Network (LAN),
- Wide Area Network (WAN).

#### **1.3.1 Personal Area Network (PAN)**

Personal Area Network are an interconnection of computing devices which are interested in transmitting information to another computing device (consisting laptop, personal digital appliance, extra.) near to each other in range. Usually Personal Area Networks are connected through Bluetooth, Sensor networks and ZigBees. The Standard Board IEEE granted the standard 802.15, as media access control MAC and physical PHY provision for Wireless PANs (WPANs).

#### **1.3.2 Local Area Network (LAN)**

It is a different kind of network, in which appliances will be interconnected to all appliances in network range which could be office or college. Wireless Local Area Network (WLAN) is a replacements to the traditional LAN linked through wires. Wired medium interconnected device have to communicate through physical medium like metals wire. Whereas in a Wireless Local Area Network nodes utilise air for transmission as a medium. WLANs have been authorized by IEEE.

#### **1.3.3 Wide Area Network (WAN)**

Wide Area Network comparatively covers a large amount of geographical area than above mention network type. For example between neighbouring city or neighbouring town. This type of networks could be applied to interconnect branches of offices of business or as public Internet access service system for public. The wireless

interconnections are established between access points by using microwave parabolic dish on 2.4 GHz band frequency not through Omni directional antennas usually used for smaller networks. Normally a Wide Area Network consist group of one or more LAN. 2<sup>nd</sup> Generation and 3<sup>rd</sup> Generation Cellular ad hoc Network, Paging Networks also Satellite Systems are some few examples of Wireless WANs (WWANs). Figure 1 illustrate interconnection of networks through wireless medium. One can access it personal computer in mobile or any equivalent device through wireless technology. Indeed Figure 1 shows the way wireless technology serve mobility, simplicity and flexibility

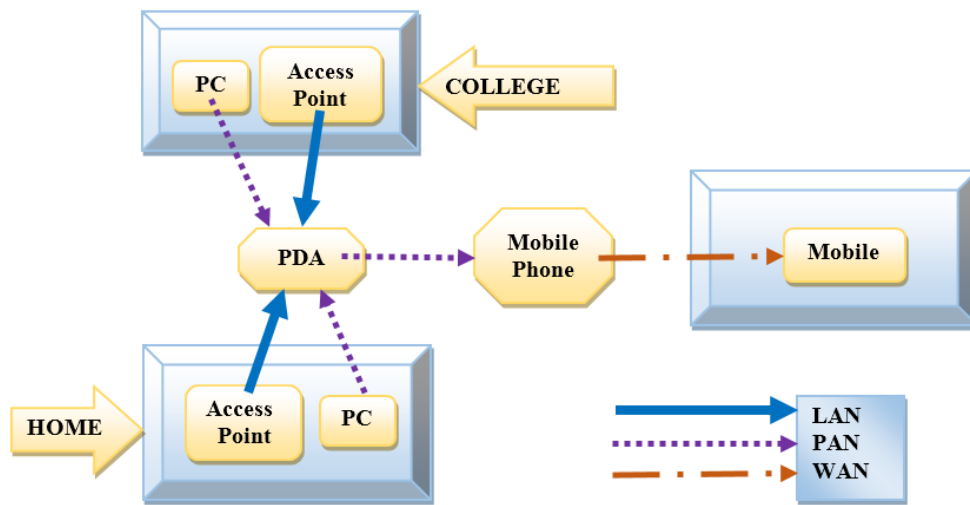


Figure 1: - Wireless technology interconnection in diverse environments

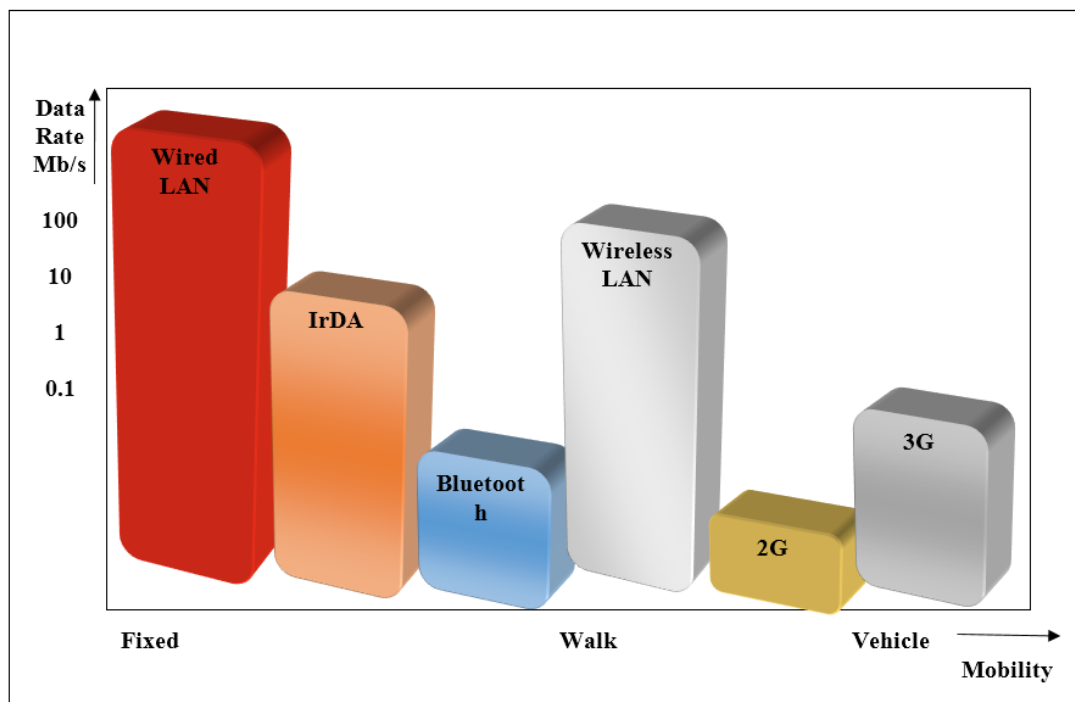


Figure 2: – Graph of Data rates and mobility for different wireless technology.

Figure 2 illustrate different kind of wireless technology communicating together and graph between data rates and mobility.

### 1.3.4 Wireless Local Area Network (WLAN)

Wireless Local Area Network is another possible option to traditional LAN which joins devices with wired nature of network. Wireless Local Area Network communicate message through air as a medium not through wired medium. A Wireless LAN is a shared medium transmission channel which propagate data packet via air as a medium for reach to every devices of network (e.g. personal digital appliance). WLAN is normally utilise interlinking the device to the Internet. Wire free internet access points (AP) are termed as “hot spots” and are in advance are utilise in teahouse and other public location of city for example aviation, railway and in many restaurant. Due to so many advantages, WLAN had acquire considerable recognition between moving clients to retrieve current information. In reality WLAN put into action in mobile devices for example laptops, personal digital appliance etc. for transmitting information among each other without any use of wire Ethernet IEEE 802.3. In a WLAN utilise wireless Ethernet protocol, IEEE 802.11 is utilize rather than wired Ethernet protocol, IEEE 802.3.

## 1.4 IEEE 802.11 Standards, Specifications and Technologies

IEEE 802.11 specifications is associated with the family of IEEE 802 protocol that explains the specifications of fully functional Local Area Network (LAN) technologies. IEEE 802 specifications mainly concentrate on two lowest layers of the OSI model, the Medium Access Control (MAC) also known as Data Link and the physical (PHY) module which combine each other. In the IEEE standard of 802 series, the specifications of individuals are regulated after the point. 802.3, for example design of Carrier Sense Multiple Access network with Collision Detection (CSMA/CD) and Token-Ring specification is determined by 802.5.

Table 1 - Comparison of 802.11 standards

IEEE Standards	Frequency	Interface	Speed
802.11	2.40 GHz	IR FHSS DSSS	till 2 Mbps
802.11/a	05 GHz	OFDM	till 54 Mbps
802.11/b	2.40 GHz	HR-DSSS	till 11 Mbps
802.11/g	2.40 GHz	OFDM	till 54 Mbps

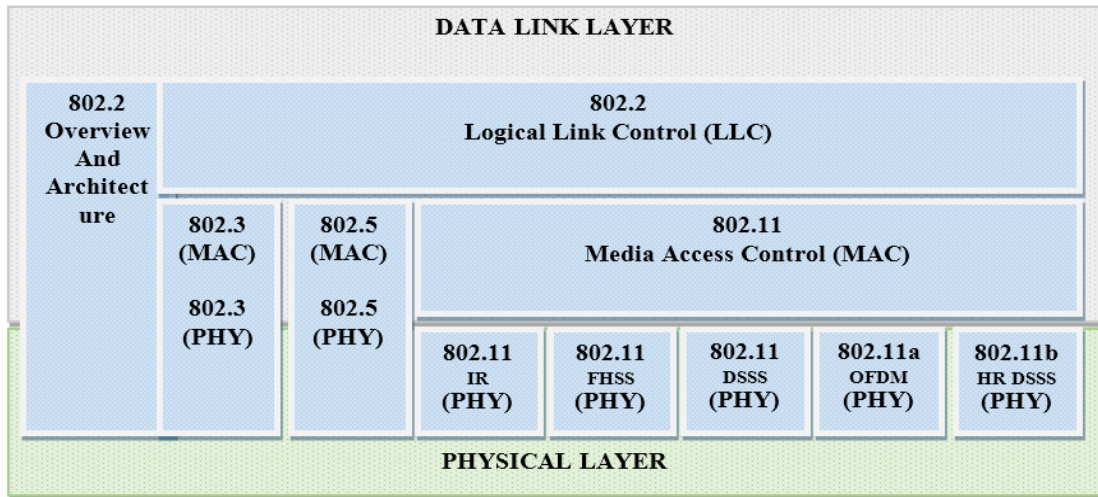


Figure 3: – IEEE 802 family and relation with the ISO models

Figure 3 illustrate different types of component related to 802 family and relationships with the ISO models. In Figure 3, there are four modulation techniques in the physical layer and four specifications in 802.11 family.



Figure 4: - Wi-Fi certified logos with SII

IEEE 802.11 technologies / specifications / standards is defined as Wireless Fidelity Wi-Fi. The Wi-Fi alliance had it as a trademark, WECA (Wireless Ethernet Compatibility Alliance) formed it as a non-profit organization. In 1999, Wi-Fi certification program was published by WECA. The products of any vendor of 802.11 using Wi-Fi certification can test for interoperability. Products which pass test are rewarded by Wi-Fi Certified logo with colour SII (standard Indicator Icon). Figure 4 represents the Wi-Fi certified logo with SII.



## Dictionary of 802.11 Wireless Term

**Station (STA):** any wireless network Ethernet card enabled computing device is an 802.11 compliant device termed as Station.

**Access Point (AP):** The device which act as link between station and wired network while transmission of information also known as bridging function device is AP.

**Wireless Distribution System (WDS):** It is strong base of the device utilize for transmitting frames linked to access point.

**Basic Service Set (BSS):** It led foundation for 802.11 network, in this basically collection of stations shares information among one other.

**Basic Service Area (BSA):** It is a fuzzy space which can be determine through communication feature of wireless environment.

## 1.5 Wireless Local Area Network Modes

Let say only two station are present in a Basic Service Area and communicate within themselves, these are elements of the Basic Service Set. The standard 802.11 has two Basic Service Set mode. These are as shown in Figure 5 and Figure 6 infrastructure and ad-hoc network.

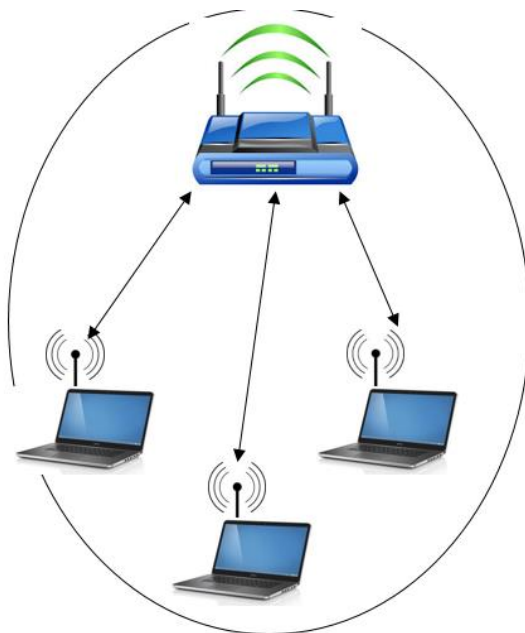


Figure 5: - Infrastructure Network

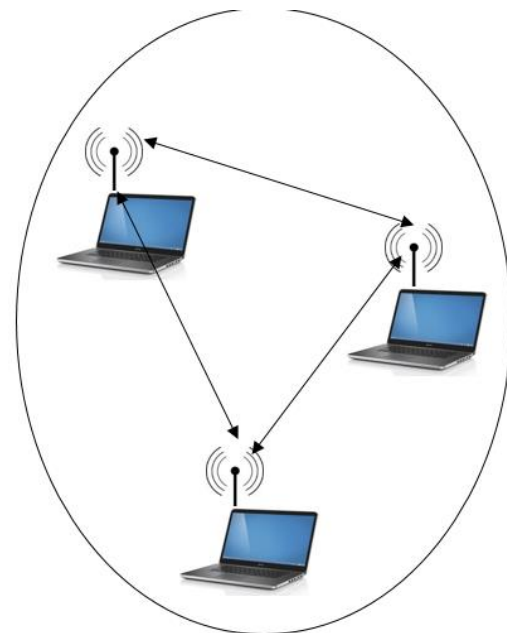


Figure 6: - Ad-hoc Network

## 1.6 Infrastructure Network

These network is referred as Infrastructure Basic Service Set (Basic Service Set (BSS) is never called as Infrastructure Basic Service Set (IBSS)). It is a collection of access point, laptops, PDA and extra. It is more familiar arrangement highlighting that the

WLAN doesn't change the wired LAN but increase the operation of wireless devices. A single access point is able to handle 15 to 200 user according to the configuration and technology. Stations during the same Basic Service Area (BSA) share information among one other through access point. Therefore, a station transfer information to another node at two hops count. First, frames of information packet are sent to the access point, then after reaching access point it process packet and then forwards the information packet to the destination station. Being a unit of a Basic Service Set (BSS), stations have to link themselves with the access point. Association operation of the infrastructure networks is exactly similar to connecting cable to the wired networks. Basic Service Sets (BSSs) normally covers minimum amount of space, for example offices and home. 802.11 standard specification permits the stations to be in motion in a larger space area than Basic Service Sets (BSSs). More number of access points can generate Extended Service Set (ESS) by chaining each other with a backbone of freely roaming ad hoc network. Figure 7 shows an Extended Service Set (ESS) which is made up of three Basic Service Sets (BSSs).

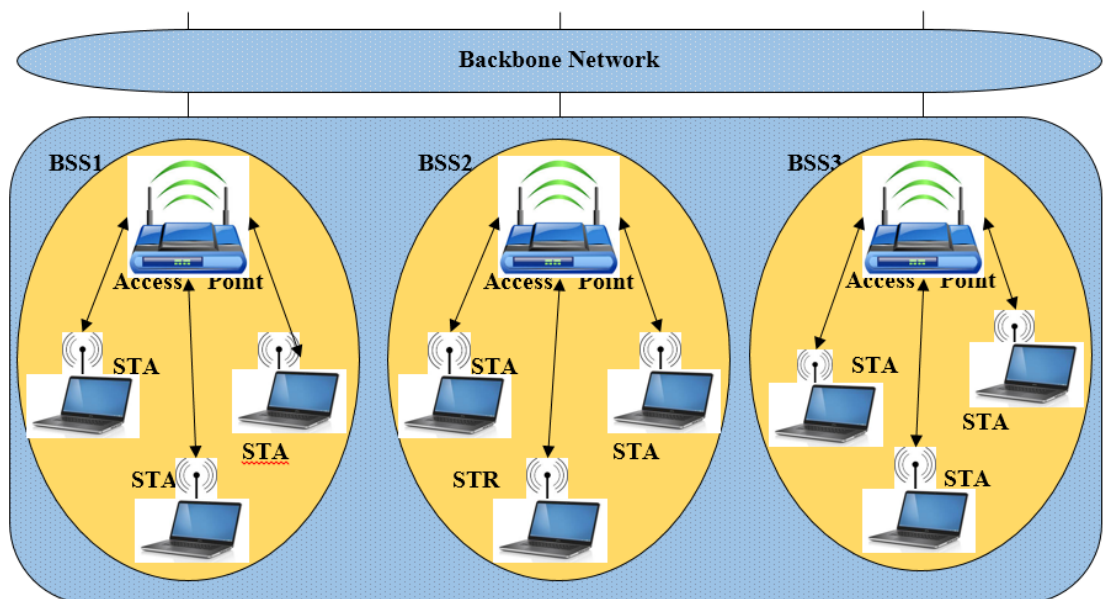


Figure 7: - Demonstration of Extended Service Set (ESS)

The major advantage of the 802.11 standards is the mobility of nodes. Within the current Extended Service Set (ESS), stations are able to move freely irrespective of which Basic Service Sets (BSSs) they are present. Wireless medium behave similar to a single layer two connection. Access point adhere to stations while using association disassociation operations of the Basic Service Sets (BSSs). While a station is moving

in an Extended Service Set (ESS), access points can track where it is. An access point in a Basic Service Sets (BSSs) or an Extended Service Set (ESS) is required to know which station is linked to itself. Station may require to share information to other station that is present in the current or different Basic Service Sets (BSSs). If access points notes the address of the stations, they can bridge the ten information to the precise Basic Service Sets (BSSs). This operation is followed with Wireless Distribution System of 802.11 standard. Another operation of the Wireless Distribution System is to join two link layers, 802.11 and 802.3. Wireless Distribution System containing the bridging operation of access point and Ethernet backbone of network. Figure 8 represents the composition of these two operation in a Wireless Distribution System.

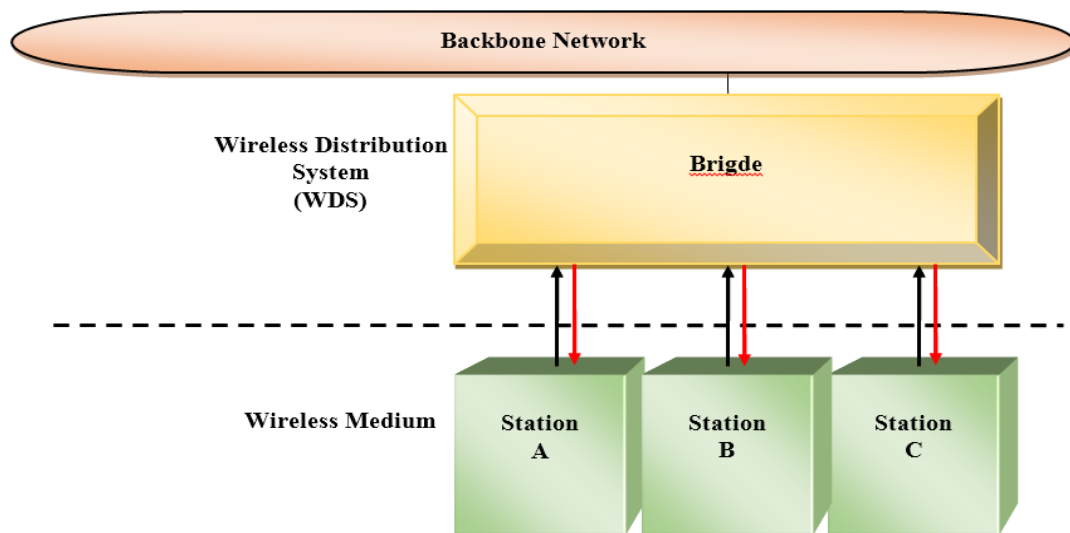


Figure 8: - Wireless Distribution System

## 1.7 Mobile Ad-Hoc Networks

The Wireless Local Area Networks (WLANs) allow to communicate over wireless channel, one device can send and receive data, like one can send voice and video to another device which is connected to same network. A precise class of standard which has controlled the market is Institute of Electrical and Electronics Engineers (*IEEE*) 802.11 wireless LAN, also called as Wireless-Fidelity (Wi-Fi). Wireless LAN networks can be in action two modes:-

- Ad-Hoc mode in which the device itself act as routers and can create self-configuring networks by interconnecting wireless links, it also known as Mobile

Ad-Hoc Networks (MANET) and device can enable there routing functionalities into the mobile nodes.

- Infrastructure mode in which the device are connected using wireless access point.

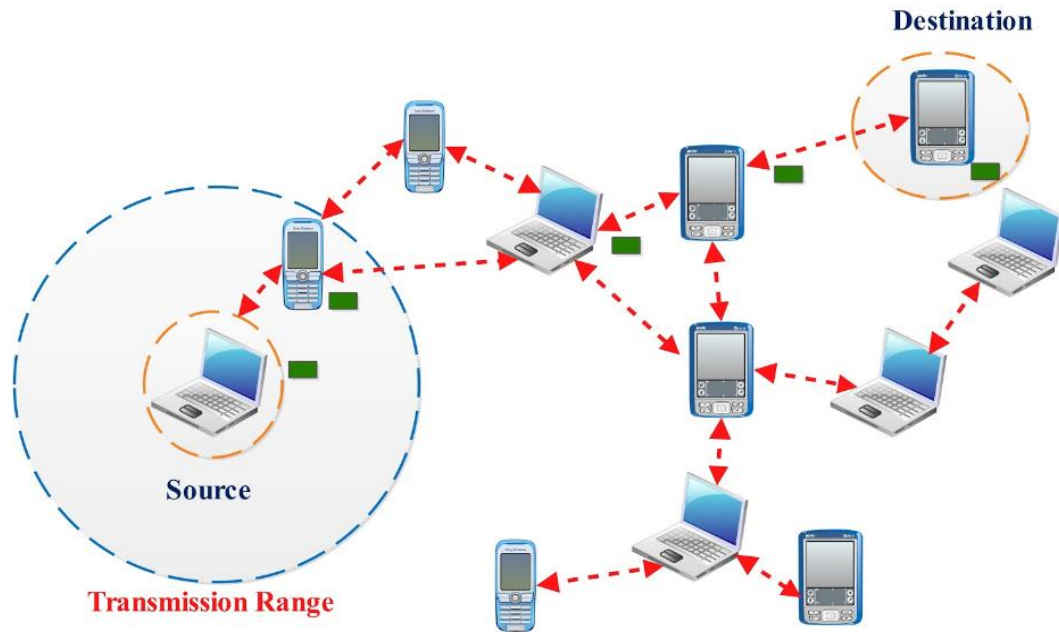


Figure 9: - Mobile Ad-Hoc Networks [21].

[MANET as illustrated by the Internet Engineering Task Force (IETF) MANET Working Group is a permanent or temporary self-governing network in which the nodes can freely move in any direction intending to establish to communication over wireless connection in absence of network infrastructure. [9]

The main function of MANETs is to facilitate wireless and mobile communication service without expensive service provider network and without network infrastructure set up. In this case the network is decentralised and the mobile Nodes should take care of network activities (network discovery) and should deliver the messages with each other by acting as router. In MANET nodes are capable of sensing the presence of other nodes present in the same network, establish connecting links among them and share or communicate information.

MANETs is a set of self-configured communicating node that can act as of data source, router and destination. The information can be directly communicated between source node to a destination node if the both nodes are in the range of each other. The range can vary according to the type of technology used for communication for example Bluetooth, Zigbee and Wi-Fi.

## 1.8 MANET Application

Followings are the major categorise of MANET application:

**Wireless Mesh Networks:** In these networks the broadband wireless connectivity is provided indoor as well as outdoor in rural, suburban and urban environments without any wired network infrastructure.

- **Public Safety System:** Wireless mesh networks can be used for addressing the requirements of law enforcing department and government such that catastrophe can be handle.

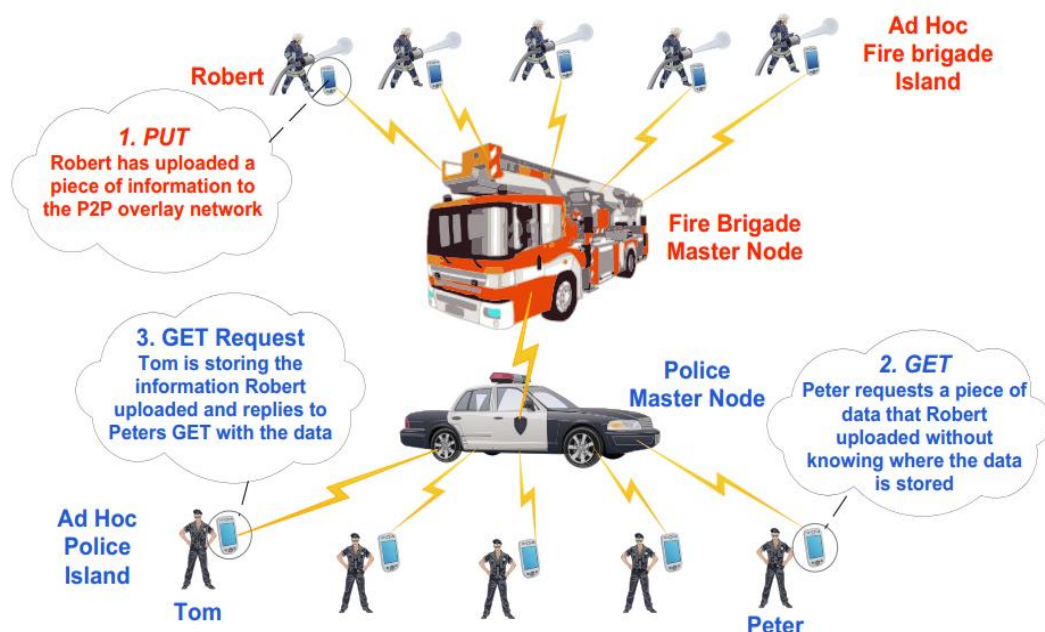


Figure 10: - Public Safety System data sharing [22].

- **Intelligent Transport System:** Wireless mesh networks helps in management of transport service, traffic can be easily manage, as it act as information delivery system.
- **Public Internet Access Networks:** Wireless mess networks are very helpful for providing broadband service in a town.
- **Health Monitoring:** Wireless sensors could be very useful as a part of health monitoring system connected with patient so that doctor and patient can communicate over wireless networks in order to check health status or send notification in case of emergency health condition.

**Wireless Sensor Networks:** In these networks nodes are battery powered with computing and communication abilities. Examples wireless sensor networks which communicate information between sensor nodes or to central entity are as follow:

- **Environmental monitoring:** Wireless sensors can be very useful in keeping up to date about environmental condition for handling it before getting uncontrollable such as forest fire detection, flood detection.
- **Smart homes:** In today's world the modern homes are having wireless sensor which can communicate with surrounding and people, providing smart home service, like smart lighting.
- **Tracking Application:** Wireless sensor service can be used to locate the location of person or object in specific area.

**Vehicular Ad-Hoc Networks:** these networks communicate take place between nodes and roadside device to assist safe driving, to avoid accident and to avoid traffic jams. In case of any accident it can propagate alert message to life saving service and also to divert traffic.

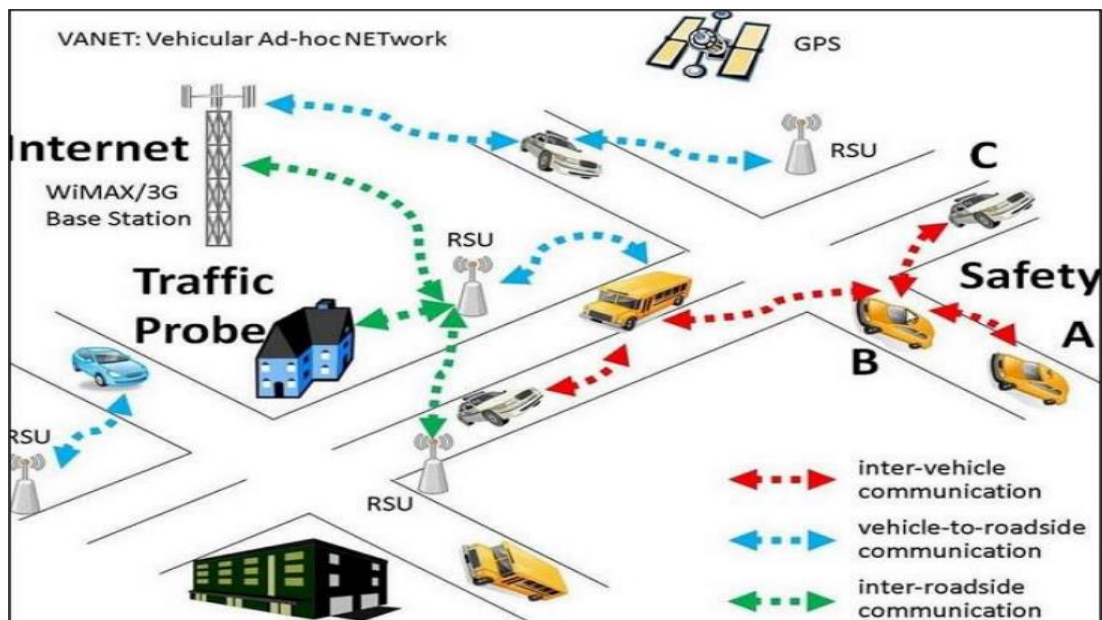


Figure 11: - Vehicular Ad-Hoc Networks [23].

**Military Mobile Communication Networks:** Battlefields does not consist infrastructure oriented networks due to its difficult terrain geography. In such condition wireless ad-hoc networks plays a major role for coordination among the military personnel and are easy to deploy in difficult terrain.[18]

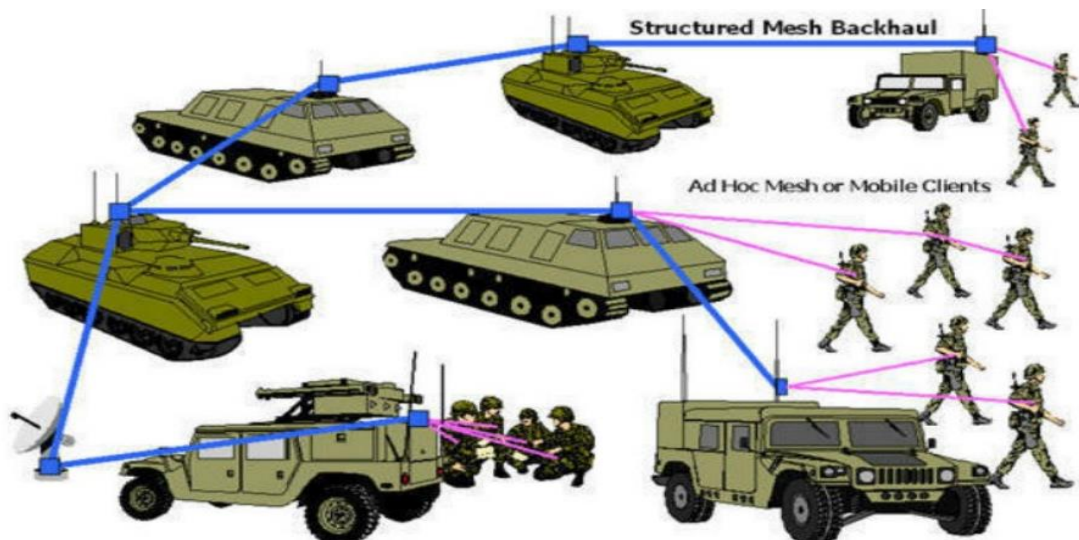


Figure12: - Military Mobile Communication Networks [24].

## 1.9 Issues in Mobile Ad-Hoc Networks

Mobile Ad-Hoc networks are not suitable to integrate with the present global internet. They are more vulnerable due its self-organizing nature of communication. Following are addressing some problems.

- **Quality of Service:** Maintaining Quality of Service in wireless Ad-Hoc network is a difficult task due to its constantly changing topologies, the network condition in hostile environment are very complicated to maintain quality of service due to the limitation of mobile ad-hoc networks.
- **Security:** Mobile ad-hoc network is generally more vulnerable than any other wired networks. The designer have designed without keeping security in their mind, they have assumed all nodes in the network will behave in a friendly manner and there will be not any threat to nodes and data packets.
- **Routing:** In mobile ad-hoc network have one major problem that is routing to have seamless connectivity to other nodes in its surrounding environment. Each node have to behave like a router to forward the data packets to allow information sharing among the moving nodes.

## 1.10 Quality of Service

For successful communication between the nodes in wireless ad-hoc network requires a set to service for packet streaming from source node to destination node. It also means that the ratio of packet delivery to the correct destination. It is expected from the wireless networks to insure a set of computable pre-specified service attribute to the users for evaluating the end-to-end performance, for example delay, and delay variance

(jitter), power consumption, probability of lost packet, bandwidth extra. Initially the Mobile ad-hoc network was developed for military use. Due its flexibility, easy to install and its mobility nature. Later this technology was made available for the public use also. The demand for wireless network has increased exponentially and penetration of wireless service has now made user to expect better quality of service and high performance as compare to available wired network. Some elements of network which has impact on quality of service are as follows:

#### **Data Dropped**

- Data Dropped because of inaccessible to medium.

#### **Channel Access Delay**

- Channel Access Delay because of queuing and assertion delay of data.

#### **Throughput of Network**

- Throughput of Network express the number of bits transmitted from one place to another according to given time span.

#### **Retransmission Attempts**

- Retransmission Attempts express the number of attempts made for successful transmission or reached to limit.

## **1.11 Quality of Service Metrics**

Quality of Service Metrics are the basic parameters of quality for a network. Quality of Service parameter consist security, bandwidth, jitter, availability network availability, delay, packet loss and battery life. For multimedia application the quality of service metrics are end-to-end delay in between arrival of data packet and appropriate delivery to destination, jitter, throughput, loss and bandwidth. Access delay is another metric which is time between packet arriving and packet transmitting by the sender node. In multimedia application jitter is an important metric which means variation in delay. The successful transmitted data and received data in a unit time is the measure of data transmission capacity is called as Bandwidth and it has great impact on throughput of the wireless network. Due to the infrastructure less nature and the limited power of MANET it is very much needed to provide quality of service to network. Although the MANET characteristic make quality of service a very complex process. Quality of Service includes issues in OSI layer such as application layer, transport layer, network layer, and data link layer extra.



## 1.12 MANET Characteristics

A large amount of researchers have examined the aspects, requirements and solutions for MANET security. Providing solutions for maintaining the security standard such as confidentiality, integrity and availability is a challenging task in MANETs due to following characteristics:

### **Exposure to wireless medium:**

- MANETs impose various challenges since the use of wireless links lets a large set of attacks to aim these networks. It is happening due to wireless medium of communication means signals are propagating over open air in all direction from a source node and this leads to prospective attacks from any direction and can be launch by anyone. In spite of this there is a mechanisms which maintains confidentiality and integrity of the content transmitted over a MANETs, but it has no mechanisms which can set up defence against traffic analyses. In addition to it opponent can trigger a Denial of Service (DOS) attack, for example jamming, for interrupting the communication between the nodes of MANETs.

### **Insufficiency of Routing Protocols:**

- In MANETs nodes are required to work together to perform the routing functionalities. Routing can lead off a significant security loopholes in the existence of malicious nodes. Data manipulation, impersonation and DoS attacks are some of the malicious activities which can be easily triggered against MANETs because of its cooperative nature of routing protocol.

### **Lack of fixed or centralised infrastructure:**

- In MANETs there is not any fixed infrastructure which means central nodes to direct packet does not exist. For this reason monitoring traffic in MANETs have become much harder riddle while public key cipher schemes are difficult to implement because it needs a existence of Certificate Authority (CA) which should be a central trustworthy point. Another perspective that uplift the difficulty level for monitoring the network traffic is the network segmentation in MANETs which appear when nodes of MANETs move from one place to another place of the network in such a way that they create communication partitions while some of the nodes loses there communicating links towards some destination nodes. The same conditions appears when MANET nodes die faster by wiping out their battery levels.

**Limited Resource:**

- MANET devices are generally smart gadget such as laptops, tablets, personal digital assistant and mobile phone extra. All these gadgets are having limited battery level, storage space and computational power and does not support higher bandwidth of network. These hampers the processing of the profound security algorithm such as greedy asymmetric cryptographic schemes or data management. This hampering of computation also leads to high consumption of battery due to which device dies faster.

**Dynamic topologies and Mobility:**

- In MANETs , the node are permitted to move arbitrary as they require, therefore topology of the network keeps on changing in a non-stochastic manner leads to change in the routing table of MANETs. Subsequently this can leads to high complexity in terms of network management. Also the prevailing changes in dynamic network topology makes harder to identify the normal from malicious behaviour. In addition to this nodes can be at risk of being compromised due to mobility.

## 1.13 MANET Security

**Confidentiality:**

- Confidentiality ensures that the content of message will never be disclose to MANETs entities that are not permitted to interpret it. Due to MANET wireless mode of communication the links are vulnerable to eavesdropping, confidentiality are very critical for protecting the transmitting private information. Particularly in certain conditions like emergency cases, where life of human is in danger, the leakage of information or routing information could be very harmful. In MANETs the information needs to be transmit from source node to destination node, and maintaining the confidentiality is difficult. In such case any malicious node present in MANET could try to disclose the confidential information as a first step in network attacks.

**Integrity:**

- Information integrity guarantees that transmitted message is not altered in between the transmission by any unauthorised node. In certain conditions the alteration could be due to some error influence by the wireless nature of node rather than a malicious nodes action perform against the MANET links. To

figure out and recover these kind of error protocols like TCP and IP use checksum. Moreover an attacker can manipulate the information by insertion, deletion or substitution. Message origin authentication ensures the identity of another node of MANET with which communication is taking place. Node authentication is concentrating on the verification of a claiming node is through actual communication on MANET. In MANET, if these kind of attribute are not present then an attacker can perform masquerade attack as a legitimate node, therefore attacker could gain unauthorised access to the resource of MANET. The verification of origin of data is related with data authentication. And data integrity is also provided by data authentication.

Non repudiation guarantees that a node of MANETs cannot disagree its action or claim that another node has perform an action.

**Availability:**

- Availability guarantees that if any node of MANET requires any network service that should be available to the node. This characteristics provide strength towards the attack like Denial-of service which restricts the authorised nodes from gaining access to important network services.

## **1.14 MANETs Vulnerabilities**

The usage of wireless nodes and routing functionalities impose by the MANETs routing protocol are the major factor of vulnerabilities in MANETs. These key functionalities depend on believe between each participating nodes.

**Routing Vulnerabilities in MANETs:**

Following are the vulnerabilities of MANET routing;

- In MANET the intermediate nodes are expected to participate in the correct delivery of a packet to a destination node in hop-by-hop manner.
- The accurate delivery and transmission of the packet depends on the information that other nodes (probably untrusted) broadcast.
- A malicious node can insert a fault routing information in MANET by generating incorrect routing table information and thus hampers the end to end MANET transmission.
- The malicious node could hamper the functionalities of the routing protocol of MANET in many different ways and this node can manipulate the

functionalities of incoming and outgoing transmission of a certain part of the MANET.

- A malicious node are also capable in blocking, modifying and dropping any routing or traffic.

### **Usage of wireless nodes**

The usage of wireless nodes can introduce vulnerabilities in MANETs as mention in following:

- Whenever an attacker is present in the transmission range then it is easier for him to intercept the MANET traffic.
- Due to short range transmission, wireless nature of the nodes and collaboration, required for transmission of information to destination.
- From passive eavesdropping to active intrusion all are the vulnerable attacks that can be launched to MANETs
- Malicious nodes has an ability to modify the protocol to launch attacks such as denial-of-service attack due to protocol that follow pre-defined rule of accessing the channel in MANETs

## **1.15 Attacks in MANETs**

The malicious nodes which are not part of the mobile network can launch various attacks against the MANET. In order to prevent the network resource from penetration triggered by malicious node MANET nodes use cryptographic techniques for verification of identity of nodes and secure transmission between the nodes of MANETs. Beside from external attacker, attacks can also be triggered by nodes which are authentic part of MANETs from inside the network or from nodes which are hacked. The malicious nodes are tend to attack on the routing protocol of MANETs. Many of the time, such protocol does not include any security system which make nodes vulnerable to misbehave. Some of the attacks are summarise in following:

### **Packet Dropping:**

- In this attack the malicious node present in the MANET publicise routes through itself to all other nodes of network intending to start dropping the packet instead of transmitting them to next hop towards the correct destination.

### **Black hole Attack:**

- In this attack the malicious nodes within the network advertises according to routing protocol itself as a nodes which is having the smallest path to reach the

destination node. In such a way malicious node acquire the data packets heading towards the destination node and drop them and return acknowledgement for further transmission. Therefore one of the following can be performed by attacker.

- Denial-of -service attack.
- Man-in-middle attack.

**Selfish nodes:**

- In this case the MANET nodes can choose to refrain from routing procedure in order to preserve their battery power. This could lead to segmentation of a MANET and nodes will not be able to sense each other if many of the nodes follows this method.

**Wormhole Attack:**

- In this attack malicious nodes collaboratively work together to transfer control such as routing and transmits the data packet out of band by using some other channels disturbing the operation of routing protocol.

**Spoofing:**

- In this attack a malicious node seeks to advertise a fake identity of another node to in order to get all the packet moving to such node and it also misguide the MANET by advertising false routes.

**Rushing attack:**

- In this attack a malicious node tries to move some packets in the direction of destination in order to position itself in between source and destination. In this case the node who is forwarded route request is unable to find any usable routes other than attacker. The rushing attack is a powerful denial of service attack towards a routing protocol.

**Routing packet modification in transmission:**

- In this attack malicious nodes changes routing message forwarded by other nodes in order to misguide established MANETs nodes by changing vital communicated routing information like sequence number on a routing packet. In such case new advertised route s are not considered.

## **1.16 Routing Protocol Techniques for MANET**

Mobile nodes have finite set of resource such as memory space, battery level and computational power which makes complex protocol design. A set of protocol has been

developed for mobile ad-hoc network. The routing protocol works efficiently under some of the situation for which they are designed, but these design fails completely in some other condition occurred in network [14].

The routing protocol are classified as following:

### **Proactive/Table-Driven Routing Protocol**

- In proactive routing nodes consist one or more routing table which contain the fresh information of the routes of other nodes in the network. Each tuple contain next hop for gaining the node/subnet and the cost of route. [31] Several table-driven protocol vary in a way the information about routing topology is propagated via all the node in the network. There are two types of table updating in proactive protocols they are triggered update and periodic update. Proactive protocol leads to waste energy and bandwidth in the network this is due to need of broadcasting the routing table/update. Following are the proactive protocol:[30]
  - Destination Sequenced Distance Vector (DSDV).
  - Optimized Link State Routing (OLSR).

### **Reactive/On-demand Routing Protocol**

- In reactive protocol node do not update or maintain routing table while the topology of the network remain dynamic. Whenever a node want to transmit any information it sends a query in the network to discover the route to the destination. The discovered route is preserve until the node required for transmission or destination turn inaccessible. This protocol is consider as an efficient as compare to proactive routing protocol. Following are the reactive protocol:
  - Dynamic Source Routing Protocol (DSR)
  - Ad hoc On-Demand Distance Vector routing protocol (AODV).
  - Temporally Ordered Routing Algorithm (TORA).

### **Hybrid Routing Protocol**

- In a network with less number of nodes, proactive and reactive routing protocol performs well. But when the number of nodes increases then both reactive and proactive routing protocol are combined for achieving better performance. Hybrid protocol tries to integrate the advantage of proactive and reactive routing protocols. Following are the hybrid protocol:

- Zone Routing Protocol (ZRP).
- Hybrid Ad hoc Routing Protocol (HARP).

Following are description of functional routing protocols of network:-

### **Destination Sequence Distance Vector (DSDV)**

The Destination Sequence Distance Vector (DSDV) is an effective routing protocol which is formulated using Bellman Ford algorithm to resolve the loop routing in MANET[34]. This is one of the type of proactive routing protocol of freely movable network also called as table driven routing protocols. Every node of mobile ad-hoc network contains table of paths to neighbouring node with distance and sequence number in DSDV routing protocol. The sequence number in table is used for updating routes of the table with latest sequence number to prevent Ad-hoc network from loop routing. Since this routing protocol is table driven, therefore it is required to maintain the routes updated, each node broadcast their routing table to the other nodes of network. [24][28]

### **Optimized Link State Routing Protocol (OLSR)**

The Optimized Link State Routing Protocol is well-known protocol of internet routing protocol which enhanced the working of freely moveable network. This protocol is a one type of proactive routing protocol of network which is also called as table driven routing protocols. And this protocol operate with following control message to locate nodes and broadcast the link state information among the nodes for updating the routes with shortest possible routes of ad-hoc network.

- a.) HELLO control message which is propagated to figure out the node present in one hop or two hop distance from their reply. Multipoint Relay (MPR) are select by the sender depending on one hop node offering shortest route to next hop nodes.
- b.) TOPOLOGY CONTROL (TC) is a control message of OLSR which are transmitted along with Multipoint Relay (MR) for broadcasting the neighbouring node information inside ad-hoc network.

### **Dynamic Source Routing (DSR)**

The Dynamic Source Routing Protocol is such a protocol that utilises concept of Source Routing. This protocol is one of the type of reactive routing protocol which is also named as On-demand routing protocols. Source routing is also known as path addressing in which the route is discovered whenever node need to propagate

information for node of freely movable networks. When path is traced, then header is linked with data packet which contain the list of all node through which it will traverse for successful delivery of data packets to valid destination node. At each node in the route will process the header part of data packets and transmit it to the next listed node of route. And the same header is used for replying acknowledgement to sender in reverse order.

### **Ad-hoc On-demand Distance Vector (AODV)**

Ad-hoc On-demand Distance Vector is fully functional routing protocol uses principle of both Dynamic Source Routing protocol for finding route and Destination Sequence Distance Vector routing protocol for latest information. [12][15] Ad-hoc On-demand Distance Vector (AODV) is functional routing protocol which belongs to reactive routing protocols also called as On-demand routing protocol. This protocol finds way for valid destination when a node requires to pass on the data packets to other node of present movable network. [20][23] AODV routing protocol process two measure function, they are route discovery for destination and their maintenance. [27][29] In AODV routing protocol when a node of ad-hoc network has to send some short of information to other node of same network then sender node broadcast Route Request (RREQ) packet in freely movable network. And this RREQ packet will be retransmitted in same network by the intermediate node until the packet arrives at the target destination node. When Route Request (RREQ) packet via intermediate nodes arrives at correct destination node, node has to unicast a Route Reply (RREP) packet through same path to sender node after that the transmission of actual data packets can start moving from source node of movable network to valid destination node. In between if the transmission of data packet link failure occur then Route Error (RERR) packet is generated from intermediate node and transmitted back to source node for restarting the route discovery process. [30]

### **Zone Routing Protocol (ZRP)**

Zone Routing Protocol is collectively using principle of proactive routing protocol and reactive routing protocol for transmission of information in the ad-hoc network hence Zone Routing Protocol belongs to hybrid routing protocols. It was innovated for reducing the processing overhead and to increase the rate of delivery by proper implementation of most effective type of enhanced routing protocol over freely movable ad-hoc network. [33] Zone Routing Protocol creates zone for each node with some radius in the ad-hoc network. Let the target destination node is present with in the



zone of source node then it will use routing table for data packet delivery to destination node as proactive routing protocol delivers. If the destination node is present out of zone of source node, then source node uses the reactive routing protocol which checks every next zone in the ad-hoc network whether the route of valid destination node. [32] With this process routing protocol is able to trim down overheads at the time of route discovery operation & packet delivery to the destination node. Zone Routing Protocol helps to deliver data packets immediately to valid destination node present within the zone using the routing table. It also helps to reduce the overheads for destination node outside the zone and the time to deliver of data packet. [14]

*“The artist is nothing without the gift, but the gift is nothing without work”, Emile Zola*

[1] Salwa Othmen et al (2016), has proposed a method to enhance the network functionalities and reduce the limitations that are posed by some of the proposed protocol. This proposed method is a better routing protocol which include three parameter, they are bandwidth, traffic load and battery level. The bandwidth for data transmission is considered by selecting only those nodes which satisfy the needed bandwidth. To increase the network endurance it propose to choose the node which have higher energy level. Another parameter is included in this method to save power consumption and increase network lifespan is the traffic load balancing between the nodes within the network. Indeed the nodes with the higher load loses more power in forward or handling all received data packet. Therefore battery decay can turn very fast, which can leads to link failure. Also the involvement of bottlenecked nodes in message transmission increment the end to end delay as their memory are fully loaded. Therefore a best route is the route which include all nodes with less traffic load and higher battery levels. It proposed method that choose multiple routes which fulfil the performance requirements. Therefore if a problem take place in the primary route, it moves to the secondary route without re-initializing any route discovery procedure.

All of these discovered paths fulfil the following prerequisite.

- All the intermediate nodes are stable in terms of remaining battery level.
- Choosing the nodes which are having low traffic load for preserving the power of the nodes and decreasing the end to end delay.
- Fulfil the needed bandwidth by choosing only that nodes which have adequate bandwidth.

This method represents an effective multi-path routing protocol for mobile ad-hoc network. It choose the route that include nodes which are having the needed bandwidth. Moreover the nodes which are bottlenecked and has low battery level are avoided to simply to increment network lifespan and reduce end to end delay.[29] The number of chosen routes are set corresponds to the needed power by the source node to transmit all of its data. This proposed protocol specify an enhancement of network in terms of lifetime, packet delivery ratio and end-to-end delay.

[2] Saswati Mukherjee et al (2016), have design a fresh trust based Ad-Hoc On-Demand Distance vector ( AODV ) routing mechanism known as Average Encounter rate - Ad-Hoc On-Demand Distance vector (AER-AODV) in MANETs. In this trust base model the Average Encounter rate (AER) is considered in evolution of trust in addition to successive cooperation frequency, which is specified according to the behaviour of nodes. All along the while, the refresh Dumpster-Shafer evidence theory is used to accumulate the selected information to obtain the overall trust value. The trusted routing protocol based on a new trust parameter is represented by enhancing the AODV protocol. At last the proposed AER-AODV is compared with AODV by analysing the performance parameters. The simulated result shows that AER-AODV is having an effective ability to eliminate affected nodes during the route formation. In addition to this proposed method attains improvement in packet delivery ratio but the throughput is compromised even though the method is able to eliminate the malicious node and extend the lifespan of the MANETs.

[3] Siddharth Dhama et al (2016), had analyse the proposed algorithm in five different cases, each of these is having Ad-Hoc On-Demand Distance vector (AODV) routing protocol is used with 20 nodes in network and later after getting the result they have analyse the same model in the presence of black hole nodes. This resulted in reducing the effect of black hole node. It resulted that conventional AODV routing protocol has very low packet loss in absence of black hole node but in presence of black hole node packet loss raised up to 88%. And when the same network model is used for propose algorithm then the packet loss reduced to 66%. In this method the first RREP is not considered for transmission.

[4] Houda Moudni et al (2016), has examine the effect of some attacks on the AODV routing protocol in MANETs. Attacks are blackhole, rushing and flooding which are simulated using NS-2 network simulator to analyse their impact on performance parameter like a packet delivery ratio which is the ratio of the number of successful packet delivery to a destination as compare to the total number of packet transmitted by the sender, another parameter is average end to end delay, it is a average time taken by the packet to move within the network from source node to destination node, another parameter is normalized routing load, this is the number routing message transmitted as per the number of received message by the intermediate node of MANETs. The

outcome reflect that blackhole attacks are truly very harmful to mobile network by making average end to end delay to an unreasonable range and has high impact on packet delivery ratio. Flooding attacks has unexpectedly raise the normalized load of the routing protocol. Rushing attack has very low impact on the network performance parameters.

[5] Sagar R. Deshmukhet al (2016), has propose an algorithm for detection and eliminating the malicious nodes at the time of initial phase of Dynamic source routing (DSR) i.e. route discovery and restrict the malicious nodes from damaging the network routing performance. The source node receives RREPs from different link, authenticate the fitness of route, source node obstruct those nodes who reply fake RREPs. It does not include any control packet for detecting the blackhole attack which introduce minimum overheads. Therefore the malicious node can be eliminated from network and no packet loss will improve the packet delivery ratio (PDR) effectively. MANET is growing area but it include very high security issue in wireless as compare to wired networks. The propose method is an efficient and effective routing against this attack. This method include a meagre overhead that is a single bit used to validate the authenticity of route. This method is flexible with other routing protocol and it also do not need any extra storage or processing power. This method detects and eliminate the blackhole node in early stage routing and forbids it from participating in the network.

[6] Zne-Jung Lee et al (2016), discussed that a mobile ad-hoc network is set up by collection of mobile station randomly establish within a specific area without infrastructure. A new technique is of cross layer algorithm is proposed based on the feature of reactive routing protocol and multi-hop jumping. Furthermore, artificial bee colony algorithm is conducted to calculate the contention window of the nodes across the routing path over MAC layer. This methodology can help to avoid packet collision in MAC layer and outcome turns better in transmission of data packet in network layer.

[7] Sweata Dixit et al (2016), has proposed productive approach for detection and prevention from black hole and grey hole attacks within the MANETs. The proposed algorithm is mostly applied to the well-known protocol that is Ad-Hoc On-Demand Distance vector (AODV) routing protocol. Tool used for simulating is NS2 network simulator. The effectiveness of this routing protocol is that it discover the grey hole and black hole attack within the network and ensure the existences in the MANETs. Initially

the working of existing Intrusion Detection System (IDS) is presented and then the procedure of malicious node detection is executed by which we will receive total number of votes. If the votes are found to be positive then Data Transmission Quality (DTQ) of doubted node will be updated else will proceed with routine which has been proposed. This algorithm is mainly grouped in three phases, noticing phase, and conformation of doubted node to be malicious and to enhance the routing protocol.

[8] Apurva Jain et al (2016), has implemented Ad-Hoc On-Demand Distance vector routing protocol along with trust model. The transmission between the nodes of mobile ad-hoc network relies on the collaboration and trust level with neighbours. On the bases of security with neighbour, a useful value of nodes can be classified as follows;

- Unreliable: A node turns unreliable when the value of trustworthiness is less than minimum trust level.
- Reliable: A node is said to be reliable when the value of trustworthiness lies between maximum trust level and minimum trust level.
- Most Reliable: A node is said to be when the value of trustworthiness is more maximum trust level.

The value of trustworthiness depends number of packet receive from neighbour node.

[9] Dhiraj Nitinware et al (2016), has proposed technique to shift the consequence of black hole attack on efficiency of Dynamic MANET On-Demand (DYMO) protocol. This technique is based on black hole detection and prevention system (BDS). Every node of DYMO runs BDS system. That means every node within network has a in-built agent in the form of fragment with DYMO routing protocol. BDS fragment evaluate the suspicious value called Transmission Power and Antenna height of all node to observe the high capability node into network. When a suspected value of nearby nodes raise more than a threshold then that node is eliminates the node from the MANETs as no other node will not transmits any message through the suspected malicious.

Following are the outcomes of simulation:

- Improvement of mobile nodes, also boost the throughput and packet delivery ratio for fixed area pause time and speed.
- Broad network area gives ample amount of space for node mobility and downgrade capabilities of network in response to area improvement.
- The efficiency of network has observe low with greater pause time.

- The efficiency of network has observe low with greater pause time. Efficiency in standard and altered is found similar with respect to speed fluctuation but in presence of black hole node the speed degrade in the network.

[10] Sushama Singh et al (2016), has proposed the Ad-Hoc On-Demand Distance vector (AODV) routing protocol is fixed with trust function. The transmission between nodes of mobile ad-hoc network depends on trust level and neighbour. Nodes can be categorized on the bases of trust level of neighbour and threshold value of nodes.

- Unreliable
- Reliable
- Most Reliable

At the time of route discovery under the AODV routing protocol it also have to calculate the trust value of all its neighbouring nodes. The outcome of trust computation is the trust- status of all the neighbour node as most reliable, reliable or unreliable.

For the detection of malicious nodes in the network each node maintain a trust table. In trust table the node is use to maintain trust status of neighbour of the nodes. Trust table contains two attributes which represent name of all its neighbouring nodes and its correlation with its neighbouring nodes that could be most reliable, reliable or unreliable. When an intermediate node receive a data packet it's refer to trust-status of neighbour node before forwarding to destination node.

Threshold (T) value of calculating the trust-status of neighbouring nodes, trust eliminating function is proposed

$$\mathbf{T = \tanh(R1+R2)}$$

Where tanh is a Hyperbolic tan function

$$\mathbf{\tanh x = \frac{\sinh x}{\cosh x} = \frac{e^x - e^{-x}}{e^x + e^{-x}}}$$

- T = trust value.
- R1= Ratio between the number of packet transmitted to the number of packet receive for transmission.
- R2= Ratio of number of packet received from neighbour nodeoriginated by other node to the total number packet receive from neighbour.

The outcome after simulating the proposed method are as follow:

- The end to end delay in AODV as the number of nodes increase but in trusted model remains stable even if the number of nodes increase in network.

- Throughput is almost similar in both cases.
- Packet Delivery Ratio is better in trusted model with respect to AODV as the number of nodes increases within a network.

[11] N.Venkatdri et al (2016), has proposed a method in which digital signature concept is applied and protocol Temporally Ordered Routing Algorithm (TORA) is used for computing trust index value of a node by doing some changes. To detect black hole attack. The Twofish algorithm is used to apply the digital signature method. The packet QRY is encrypted at the source node and transmitted to all the neighbouring nodes in the network. The node which is having the key to decrypt will be able to decrypt the QRY packet correctly and then produce an UDP packet and transmit it back to the source node based on QRY packet decryption. After receiving packet source node verify whether the UDP packet is transmitted by authentic node and calculate the trust index value for that node which transmitted back. Security between the communicating nodes depends on management system which produce and issue symmetric or asymmetric encryption or decryption keys.

In proposed method to order enhance the security of the network Twofish cryptographic algorithm is used. Twofish cryptographic algorithm uses sixteen rounds structure of feistel cipher with extra whitening input and output.

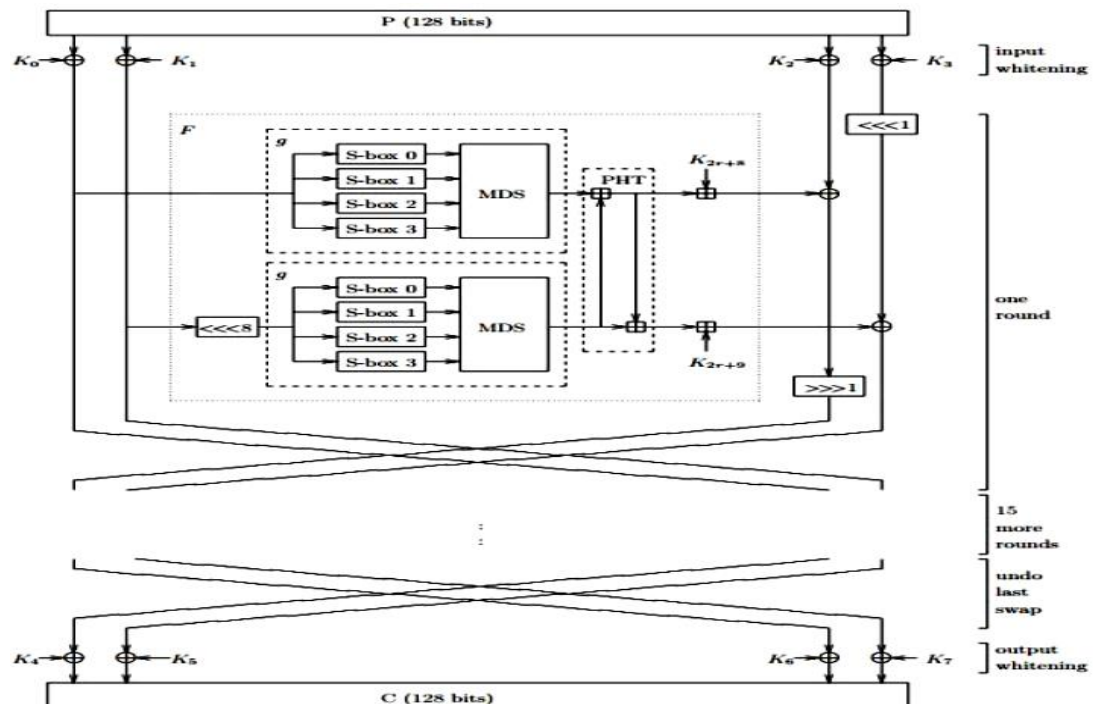


Figure 13: - Structure of Twofish algorithm [11].

Twofish cryptographic algorithm step:

1) Input plaintext of 128 bits

$P_0 \dots P_3$  (32 bits each)

2) Input whitening, in this step XOR operation is performed between plaintext and sub-keys.

3) Sixteen iterations round for function computation

4) XOR operation between Output and sub-keys

5) Cipher text is obtained

$C_0 \dots C_3$

(32 bits each)

This is little-endian convention method

Reverse little endian convention is used to retrieve plaintext.

Outcomes proposed Algorithm performance under attack:

- It takes minimum average time to transmit the data packet whereas the conventional Temporally Ordered Routing Algorithm takes more time to deliver end to end information packet.
- It takes minimum average energy power to transmit the data packet whereas the conventional Temporally Ordered Routing Algorithm takes more energy power to deliver end to end information packet.
- It increases throughput in transmitting the data packet whereas the conventional Temporally Ordered Routing Algorithm has low throughput for delivering end to end information packet.

[12] Priya Sethuraman et al (2016), has proposed a Refined Trust based Energy effective routing algorithm ReTE-AODV and compared with TE-AODV, AODV, and AOTDV in three different cases. From evolution it is analysed that proposed ReTE-AODV works better than all these three existing algorithms. In proposed algorithm, although the ratio packet overhead and energy consumption values are higher because of massive computation of final trust value, the throughput of network is not compromised. This proposed algorithm is found that the routes are more trust worthy for MANETs in response to dynamic topology.

Outcome of the proposed ReTE-AODV algorithm:



- ReTE-AODV algorithm increases packet delivery ratio in transmitting the data packet whereas the conventional TE-AODV, AODV, and AOTDV Algorithm have lower packet delivery ratio for delivering end to end information packet.
- ReTE-AODV algorithm have better average end-to-end latency in transmitting the data packet whereas the conventional TE-AODV, AODV, and AOTDV Algorithm have lower average end-to-end latency for delivering end to end information packet.

[13] S.H. Jaychandra et al (2016), has perform examine the effect of black hole attack in two routing protocol, they are AODV and MAODV. Analysis is performed using NS-2 network simulator by taking following performance parameter.

- Packet-to-Delivery Ratio:

Packet-to-Delivery Ratio is number of packet delivered to destination node in response to total number packet transmitted by the sender.

$$\text{PDR} = \text{number of packet receive} \div \text{number of packet send}$$

- Average Throughput:

Average Throughput is number of packet delivered to destination node in specific time.

$$\text{Throughput} = (\text{Packet size} * 8) / 100.$$

Analysis of Packet-to-Delivery Ratio under AODV and MAODV routing protocol.

- Under AODV routing protocol all packet were able to reach destination in ideal condition that is when there is no attack. And the packet delivery turns to none when attack is performed.
- Under MAODV routing protocol there are multiple routes to destination. So it can deliver data packet better than AODV due to the availabilities of multiple route, even if one of the route fails it deliver through another route.

Analysis of Throughput under AODV and MAODV routing protocol.

- Under AODV routing protocol all packet were deliver to destination therefor throughput is higher in ideal condition that is when there is no attack. And the packet delivery turns to none when attack is performed therefore throughput decreases and effect the network performance.
- Under MAODV routing protocol the throughput is better than AODV because it contain multiple routes to destination. Therefore it can transmit data packet better than AODV routing protocol in the network.

It implies that AODV routing protocol is used to avoid higher overhead. And MAOVD routing protocol is used when we require greater packet delivery ratio and throughput.

[14] Balram Swami et al (2016), has analyse the performance of three different routing protocol, they are AODV, DSDV and MOWL. AODV is one of the most known routing protocol. It is a reactive routing protocol. it generate a RREQ whenever it requires to communicate and broadcast in the network and wait for reply, Destination node receive RREQ and transmit RREP to the source node to start communication. If in case the link failure occur RERR is generated by the leaf node. MOWL is an improved version of OWL routing protocol. MOWL perform hybrid searching algorithm, hybrid searching algorithm is a collaboration of breath first searching and depth first searching. Hybrid searching algorithm contain less network overhead. DSDV is proactive routing protocol also called as table driven routing protocol. It update routing protocol periodically and when a node need to communicate it search route in route table for transmitting data packet.

- In analysis of delay to the number of connected links per node, delay increases as the strength of connected nodes raise in all the routing protocols. DSDV is found to work better in network with small number of nodes.
- In analysis of packet delivery fraction, in AODV and MOWL routing protocol the performance and packet delivery fraction decreases as the number of connection increase but in DSDV the packet delivery fraction increase as the number of connection increases.
- In analysis of drop packet ratio, the AODV and MOWL routing protocol perform similar but DSDV routing protocol perform opposite to AODV and MOWL it have higher drop packet ratio.

[15] Sathish M et al (2016), has introduce a new methodology for reducing the single and collaborative black hole attacks also cutting down computational, storage and routing overhead. This approach include a dummy route request, next hop details and destination sequence number to reduce the limitation of existing system. To avoid black hole attack in network, it is important to identify malicious node in route discovery procedure, while passing fake RREP packet replicating the source. On the bases of next hop detail and sequence number of destination node that is extracted from RREPs, this method can manage single and collaborative black hole attacks slow computation, storage and routing overhead. There are three additional parameters in the algorithm

such as fake RREQ, list of black hole consist single black hole no and list of collaborative black hole. Proposed algorithm is as followed:

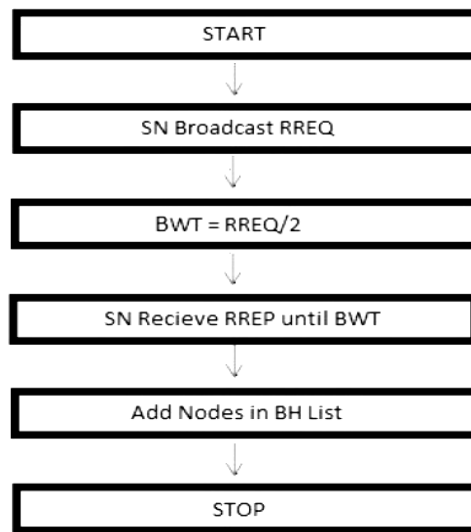


Figure 14: - Flowchart of proposed Black Hole Detection Algorithm [15].

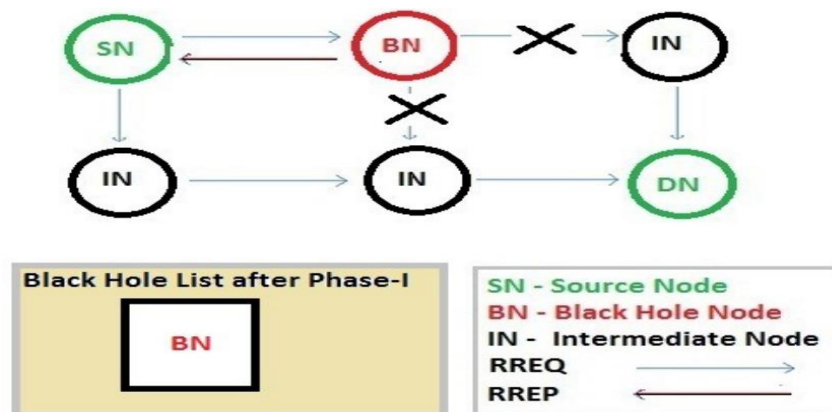


Figure 15: - Black Hole Detection Algorithm [15].

It is observe that this methodology has shown better performance in presence of malicious node in the network. It has resulted 71% reduction in end-to-end delivery delay, 13% improvement in throughput of the network and 46% growth in packet delivery ratio. It is found that this algorithm has better efficiency in MANET.

[16] Bikramjeet Singh et al has proposed a methodology which is mainly grounded for freely moveable ad-hoc network deployed in military operational areas next to the international border. The proposed method utilise the fundamental functionality of flooding a counterfeit Route Request (RREQ) packet in the freely moveable ad-hoc network for recognizing the Blackhole node (BN). When a node is detected then it is verified with the neighbouring nodes whether the detected node characterised as

[17]Blackhole node (BN) is transmitting any packet to the next node towards the destination. Subsequently if neighbouring node provides positive reply to the query therefore the attack is recognized as Cooperative Blackhole attack rather than single Blackhole attack. In either of the case the Blackhole List will be updated. He explained that it is of supreme important for army environment to recognize Blackhole node along with its grid location for eliminating the Blackhole node on ground by utilising the node delimitation process by identifying the nearest effective node. It is essential to notice that the location of the node is presumed to be stationary once the RREQ is transmitted from source node to destination node. This is performed for locating the precise coordinates of Blackhole nodes and then calculating their distance from other nodes after calculating distances messages coming from Blackhole node are not entertained and the message is forwarded to all nodes of network for isolating all of these Blackhole node. The Euclidean distance formula is used for calculating distance between nodes as follows.

$$d(x, y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2}$$

The following flow chart represent the proposed method.

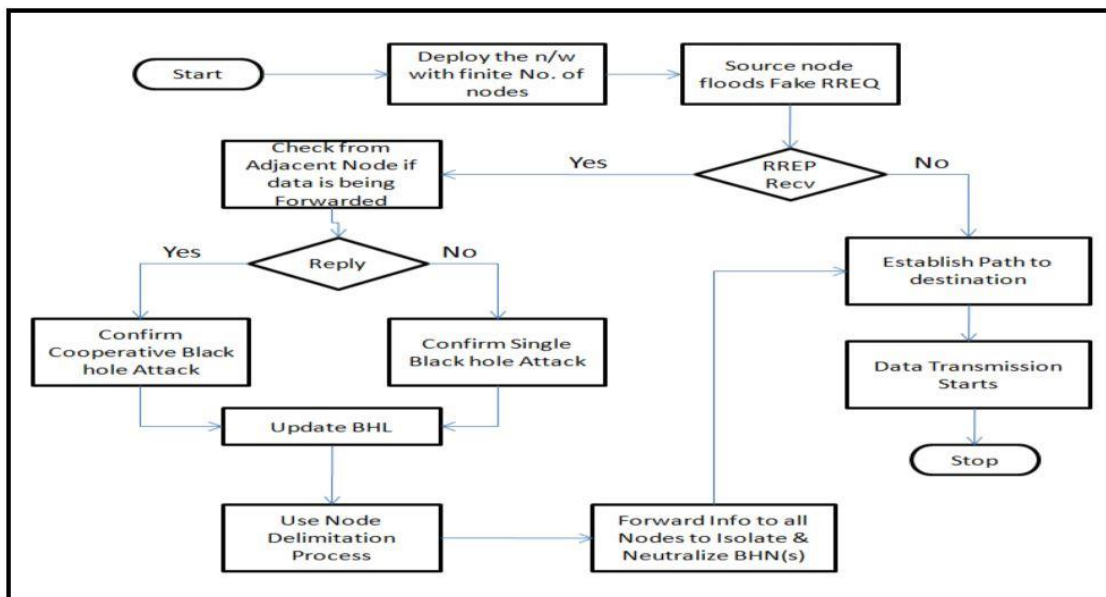


Figure 1

This proposed methodology was performed using network simulator NS-2. The simulation is performed on AODV routing protocol in presence of Blackhole Node. The performance key metrics which considered are delay, packet delivery ratio and throughput. It showed that packet delivery ratio and throughput of the ad hoc network has been improved in the presence of Blackhole node by using the proposed methodology. But the delay of the network has increased due to increase in the time of processing of packet as per the proposed method.

[26] Mohamed A. Abdelshafy et al have proposed a novel method of self-protocol trustiness where the detection of malicious nodes are achieved using the actual functionality of implemented protocol and attract the malicious node to identify through its malicious behaviour. Author have presented a Blackhole repelling method to repel these attacks that can affect the functionality of any routing protocol of freely roaming ad-hoc network. This method does not need any complex cryptography or authentication process for detection of malicious node. This method depends on current applied timer and threshold value for detecting the malicious behaviour of a node. There is no need to do modification in packet for detection so there will be small amount overhead for calculation at node level and extra transmission are also not required. In method is aimed for eliminating the effect of maliciously behaving Blackhole node over AODV routing protocol as soon as possible. It made changes to actual AODV by storing previous three per hop time for a route request reply for destination node. Per hop time is computed as delay in between transmitting a RREQ and getting its related RREP divided by hop count adhere with RREP. Every single node present in the network will have to monitor the operation of its neighbouring node for detecting whether it behaves properly or not. This method has no threshold value which can be used to detect the Blackhole node. In this methodology a node transmits a fake RREQ as non-existing source node to non-existing destination node. Node stores fake addresses of source node and destination node in its trust table for evaluation and it also sets expiry time to avoid table inflation for this table entry and node stores the trust value to normal then it transmits fake RREQ and waits for RREP and sets it as threat. The methodology is performed with the help of Network Simulator. The outcomes of simulation shows that a Blackhole repelling method under AODV routing protocol results in high improvement of freely roaming ad-hoc network performance in each metrics over AODV and SAODV. And it is capable of detecting Blackhole nodes and the period for which participated.

[18] R.Priyanka et al have proposed a methodology which is grounded on trust credibility of the nodes of the freely roaming ad-hoc network. In these Mobile network the non-malicious nodes usually perform some steps of calculating the trust value of neighbouring nodes over an interval of time for detecting the attacker nodes in its neighbourhood. The methodology suggests that when the route for transmission is selected from source node to destination node only then the process of detection of

jellyfish node is processed. It has examined minimum of three jellyfish attacker node in between the transmission of source node and destination node. By utilising the DTD algorithm detection mechanism is applied for detection and simulation of jellyfish attacker node. The trust value of each neighbouring node is being monitored in their routing table. The trust value of nodes lies in between 0 to 1. The nodes are identified as a jelly fish attacker node on the basis of their trust value calculated by the nodes. Each node has to maintain their routing table in the meantime the node also maintain the trust table in routing table itself. The packet transmission of node at the time of communication is used for trust value id. Every node calculate the trust value over an interval of time. At some time t1 node A sends a packet to next node B further node B do not forward it with in an estimated time of interval thus node A will reduce the trust value of B in its trust table. The node below the threshold value will be blacklisted and timer is added.

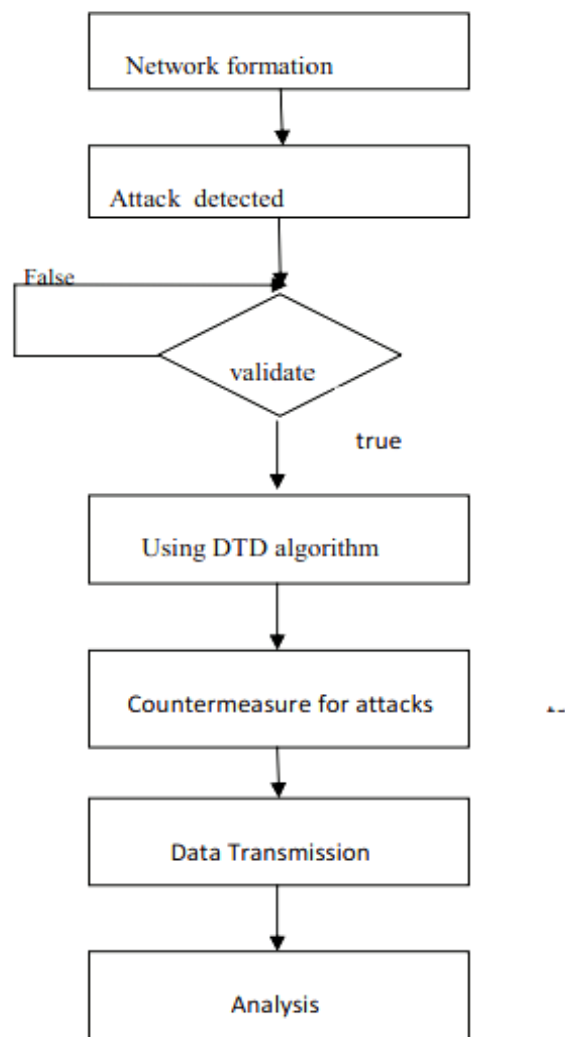


Figure 16: - Proposed Method

- The study will lead to understand the impact of various black hole attacks in mobile ad-hoc (MANET) network using routing protocol such as ad-hoc on-demand distance vector (AODV).
- Assessment of method for avoiding single black hole attack is considered.
- The effect of method for avoiding multiple black hole attacks on efficiency of the network is measured and realising whether the method for single black hole attack is similarly applicable to multiple black hole attacks.
- The simulation will be perform on NS-2.35 version of network simulator tool.
- Simulation will evaluate the performance of MANET without any malicious node and when black hole node present, MANET when one black hole node is present, MANET when two black hole nodes are present, MANET when three black hole nodes are present. Also to check if the MANET performs well in given situation, with 5 nodes, 25 nodes and 50 nodes separately.
- The result will be acquired using following parameter:
  - Packet loss percentage.
  - Packet delivery ratio.
  - Average end-to-end delay.
  - Throughput.

#### 4.1. Problem Definition

Mobile Ad Hoc Network (MANET) has turn out into one of the most significant infrastructure less method, offering transmission facilities to army and another security organisation serving in the traditional combat situation on enemy terrain or Counter Terrorism/ Counter Insurgency operations out of the range of a fixed network support. Though, the networks fundamental structure does not have any defensive mechanism, it is vulnerable to the security threats. Single black hole attack is one of the well-known security compulsions in network where the compromise node mislead the sender node by advertising of having shortest routes through it at the time of path finding procedure and receives all transmitted message aimed towards particular node. Scholars from all over the world have introduce several threat detection method and systems to discover these kind of security attack on network. This study will propose a novel mechanism for eliminating the consequence of black hole attack assuming army in war scenario in our case. Simulation will be perform in NS-2.35 network simulator [25]. Parameters which will be considered to analyse performance are Packet Delivery Ratio, throughput and delay.

#### 4.2. Objectives

- To study and understand various routing protocol in mobile ad-hoc network.
- To analyse the existing mechanism providing security to the mobile ad-hoc network.
- To propose a mechanism to eliminate the effect of black hole node and increases the security in the network.
- To perform the proposed and existing method and compare the outcome with following metrics Packet loss percentage, Packet delivery ratio, Average end-to-end delay, Route request overhead and Throughput



### NETWORK SIMULATOR (NS-2)

In this portion of thesis, our focus was to measure the corresponding consequences of the Blackhole attack in the freely moving self-governed Networks. For this purpose we have performed the freely roaming self-governed network scenarios which consist Blackhole node with the Network Simulator. To perform the working of Blackhole station in a freely roaming self-governed network we have applied a malicious procedure to the node which intentionally drops message packets just after receiving them from neighbouring node. In this portion we represent NS-2.35 and our input for eliminating the effects of Blackhole attack to this software.

#### 5.1 Network Simulator

Network Simulator is an event driven network simulator software, developed by the University of California Berkley, which consist too many network instance for example application, protocol and traffic behaviour. The Network Simulator is a one portion of software of the VINT work which was supported by DARPA.

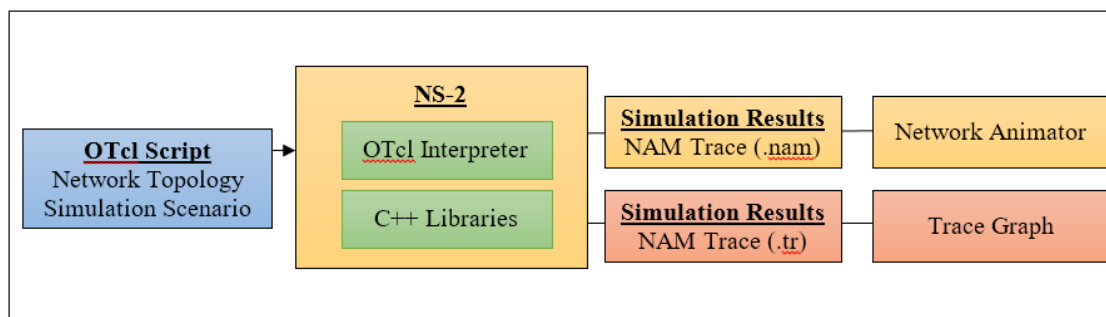


Figure 17: - NS-2 schema

In the simulation layer Network Simulator require an Object oriented Tool Command Language programming language (OTcl) for understanding user scenario through simulation scripts. Object oriented Tool Command Language programming language is actually an object oriented expansion of the Tool Command Language. The Tool Command Language is completely relevant with the C++ programming language. At the upper layer, Network Simulator is a compiler of Tool Command Language scripts provided by the users, they execute concurrently with CC files.

As shown in Figure 13 an Object oriented Tool Command Language script provided by the user is compiled by Network Simulator. Meanwhile Object oriented Tool Command Language script is being compiled, Network Simulator generates two important

analysis reports files concurrently. One of these is Network Animator (NAM) instance which represents the pictorial animation of the simulation. Another one is the trace instance which include of the behaviour of each nodes present in the simulation. Both of these are generated as a file by Network Simulator. Earlier one is .nam file utilised by NAM program which is one of the part of Network Simulator. Second is a “.tr” file that consist every simulation traces in formatted style. Network Simulator software is actually circulated along with numerous of packages for example ns, nam, tcl, otcl etc termed as “all-in-one package”, but these package could be accessed and downloaded individually. In this work we have taken help of version 2.35 of Network Simulator all-in-one bundle and installed the package in the Ubuntu 14.04 environment using VMware in windows 10. After arrival of version 2, Network Simulator is has become very popular as NS-2 and in our wok we have refer to it as NS-2.35. We havev prepare the “.tcl” file in the editor and examined the outcomes through “.tr” file using “awk” commands of linux Operating System.

In mobile ad-hoc network to eliminate the impact of Black hole attack is a challenging task. Therefore a method is proposed in which a malicious node will be restricted to participate communication within the network, even if the malicious node is present within the range of network. In this method cryptography is used to encrypt the parameter of RREP packet here we have used feistel block cipher encryption technique and receiving node will decrypt using same technique. It will help node to verify before transmitting the data packet to alleviate the effect of black hole attack.

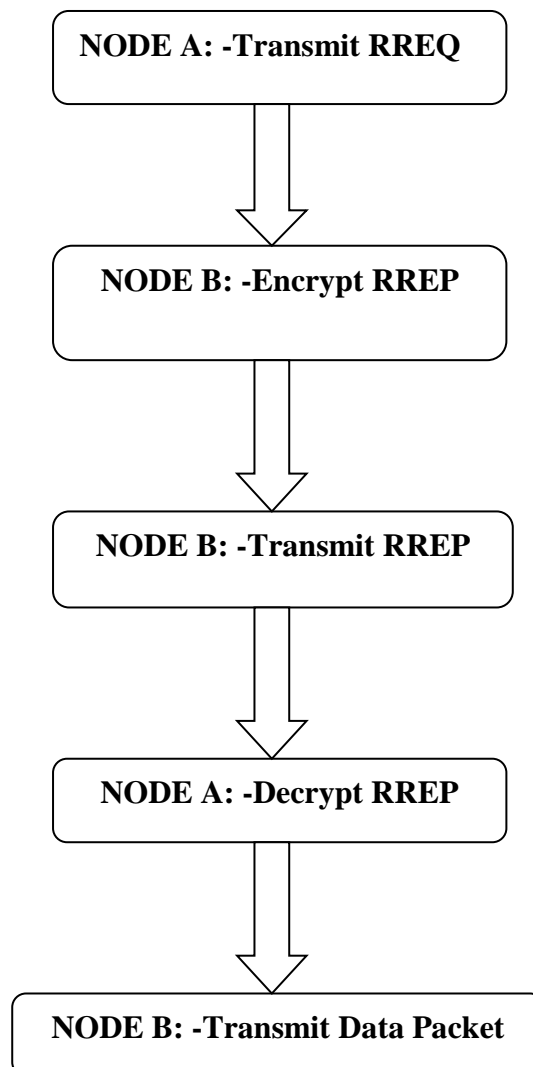


Figure 19: - Proposed Method for Black Hole Node

## Chapter 7

### OUTCOMES

The proposed method has shown better results than the traditional routing protocol of mobile ad-hoc network. The impact of black hole attack on performance of ad-hoc network has been reduce. Throughput of network when malicious node is present has increase. Delay at the time of transmission between nodes in a network has reduce. Packet delivery ratio is better as compare to earlier system. Following table are showing outcome of simulation, Table 2 represents Outcomes of Average End to End Delay under Blackhole Attack, Table 3 Outcomes of Throughput under Blackhole Attack Table 4: - Outcomes of Packet Delivery Ratio under Blackhole Attack, Table 5: - Outcomes of Packet Drop Ratio under Blackhole Attack, these result shows that in normal AODV routing protocol is not able to defend itself from Blackhole Attack. But the proposed method is able to eliminate blackhole attack and also increase efficiency of network. Figure 24, 25, 26, 27 shows graphical representation of output of network.

Table 2: - Outcomes of Average End to End Delay under Blackhole Attack

S.no	No. of Nodes	AODV	Proposed Method
1	10	0	0.05952532
2	20	0	0.05956009
3	30	0	0.05954003
4	40	0	0.09940913
5	50	0	0.11979151
6	60	0	0.05950985
7	70	0	0.08957158
8	80	0	0.16001797
9	90	0	0.19247322
10	100	0	0.10179121
11	110	0	0.09941096
12	120	0	0.09945818
13	130	0	0.12323541
14	140	0	0.13956167
15	150	0	0.09943236

Table 3: - Outcomes of Throughput under Blackhole Attack

S.no	No. of Nodes	AODV	Proposed Method
1	10	0	1000.207
2	20	0	1000.212
3	30	0	1000.208
4	40	0	999.804
5	50	0	999.611
6	60	0	1000.203
7	70	0	999.906
8	80	0	999.201
9	90	0	970.890
10	100	0	997.802
11	110	0	997.382
12	120	0	999.807
13	130	0	993.147
14	140	0	999.400
15	150	0	999.806

Table 4: - Outcomes of Packet Delivery Ratio under Blackhole Attack

S.no	No. of Nodes	AODV	Proposed Method
1	10	0	99.92
2	20	0	99.92
3	30	0	99.92
4	40	0	99.92
5	50	0	99.92
6	60	0	99.92
7	70	0	99.92
8	80	0	99.84
9	90	0	97.01
10	100	0	99.12
11	110	0	99.68

12	120	0	99.92
13	130	0	99.27
14	140	0	99.84
15	150	0	99.92

Table 5: - Outcomes of Packet Drop Ratio under Blackhole Attack

S.no	No. of Nodes	AODV	Proposed Method
1	10	100	0.08077544
2	20	100	0.08077544
3	30	100	0.08077544
4	40	100	0.08077544
5	50	100	0.08077544
6	60	100	0.08077544
7	70	100	0.08077544
8	80	100	0.16155089
9	90	100	2.98869144
10	100	100	0.88495575
11	110	100	0.32310178
12	120	100	0.08077544
13	130	100	0.72697900
14	140	100	0.16155089
15	150	100	0.08077544

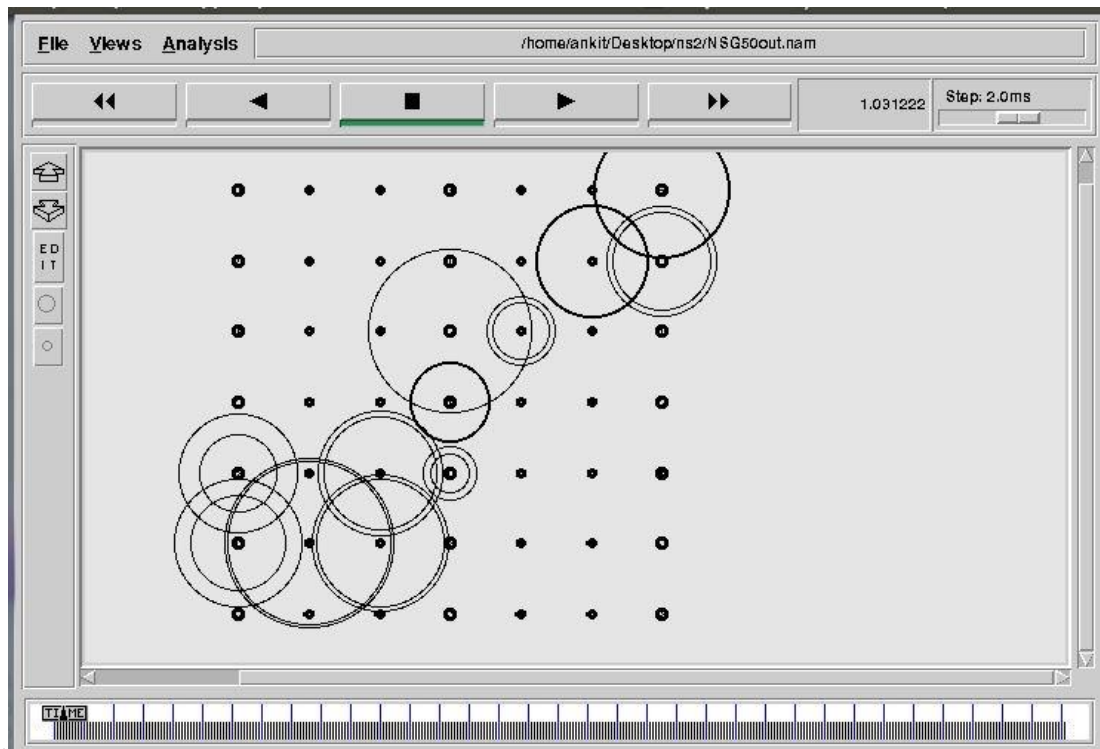


Figure 20: - Simulation of RREQ Packet in NS-2.35

Figure 20 shows Route Request process before transmitting the information in mobile network and in Figure 21 shows Route Reply process which is used to transmit information

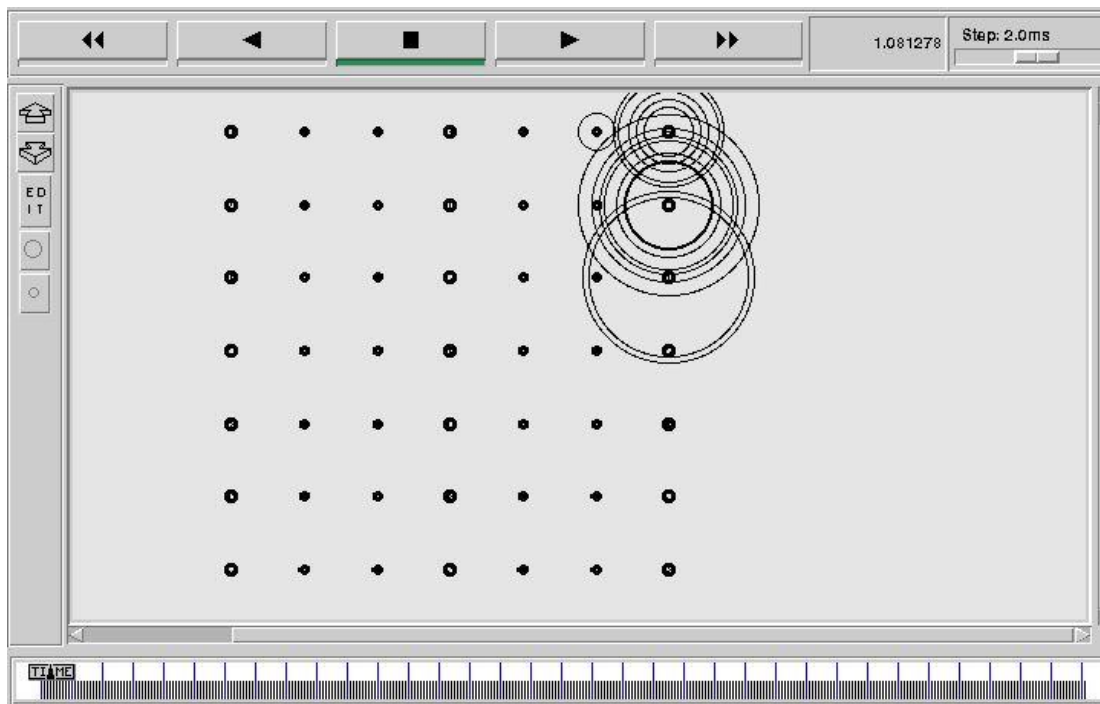


Figure 21: - Simulation of RREP Packet in NS-2.35

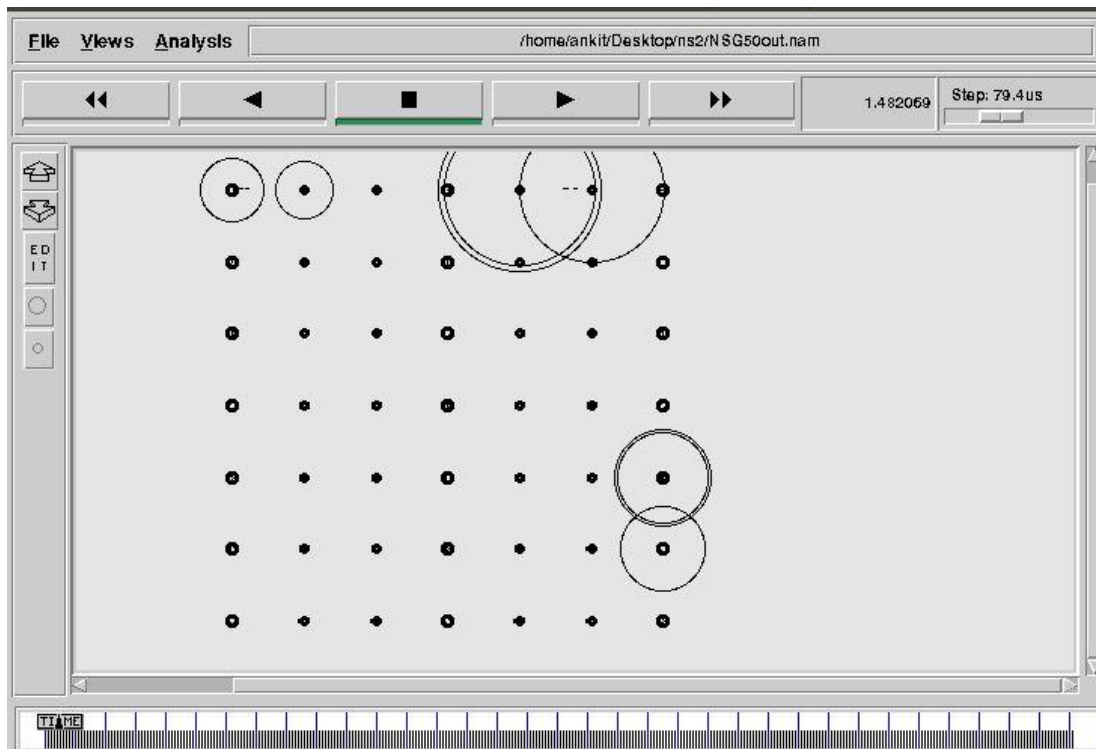


Figure 22: - Simulation of Packet Transmission in NS-2.35

Figure 22 represent the packet transmission after receiving RREP packet whereas figure 23 shows Blackhole attack attracting packet and dropping them for no reason, and this attack can be reduce via proposed method. As result shows increase in efficiency.

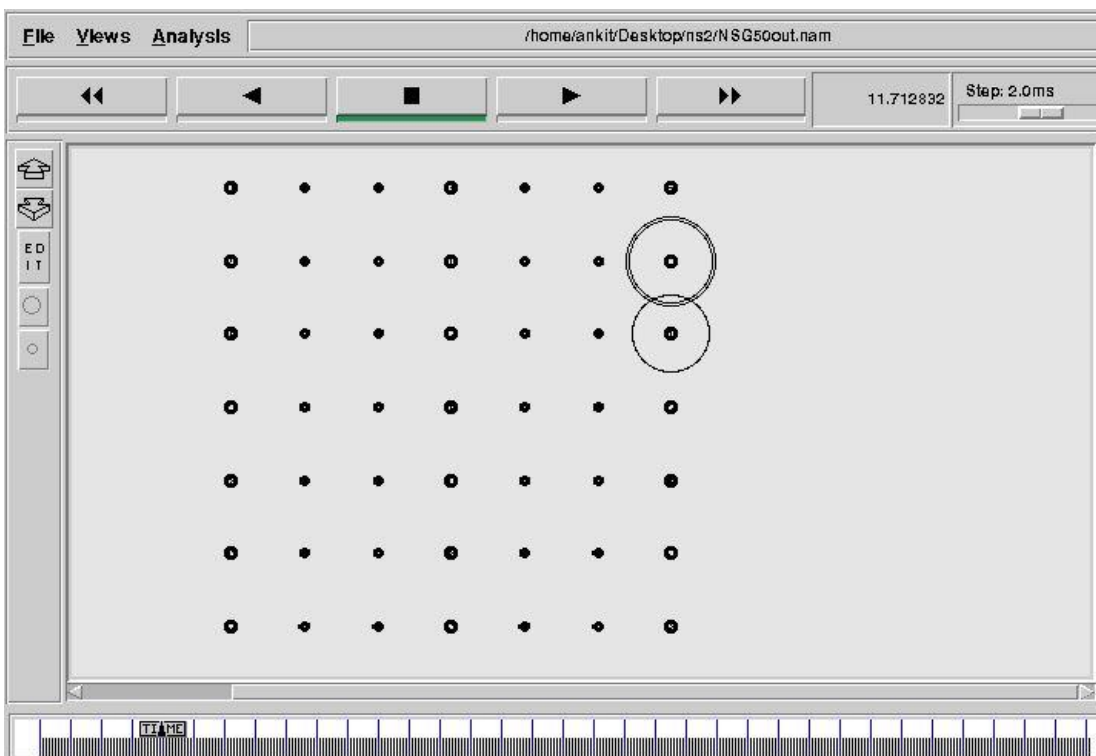


Figure 23: - Simulation of Blackhole Attack in NS-2.35



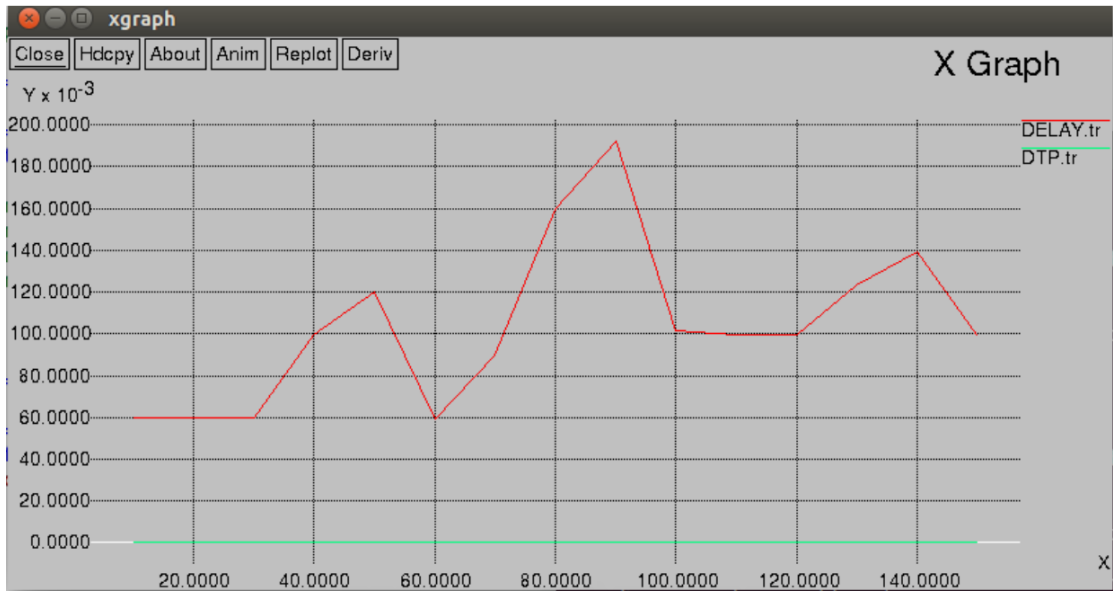


Figure 24: - Average End to End Delay

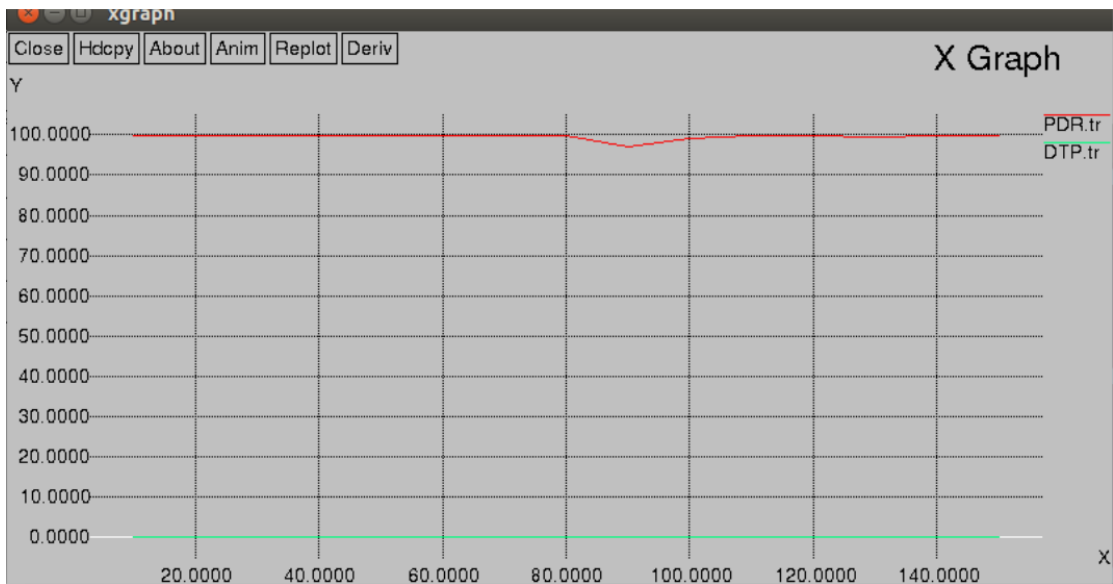


Figure 25: - Packet Delivery Ratio

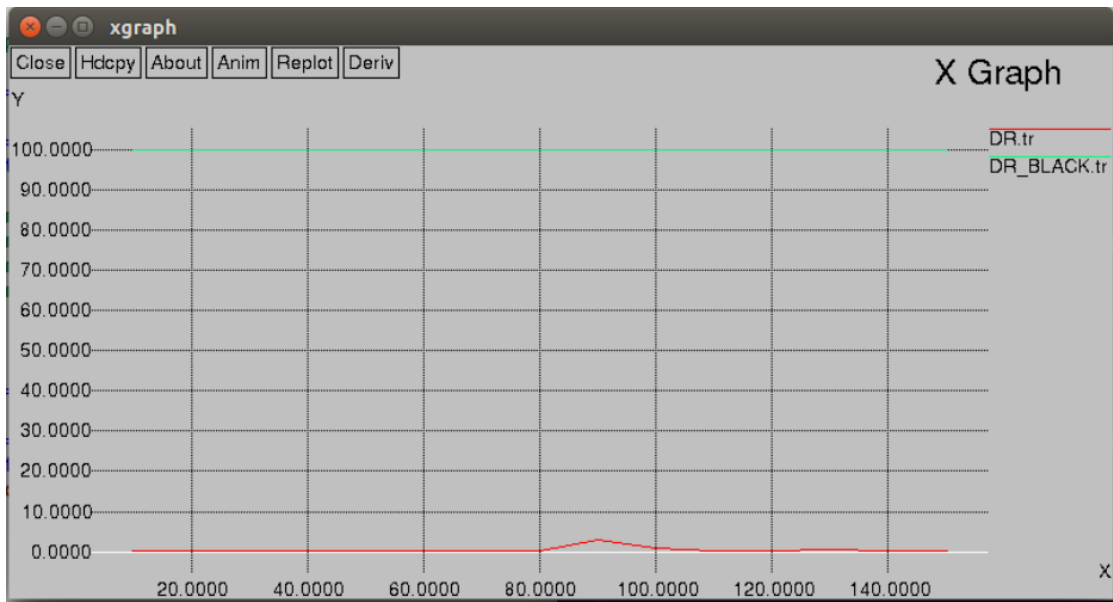


Figure 2: - Packet Drop Ratio

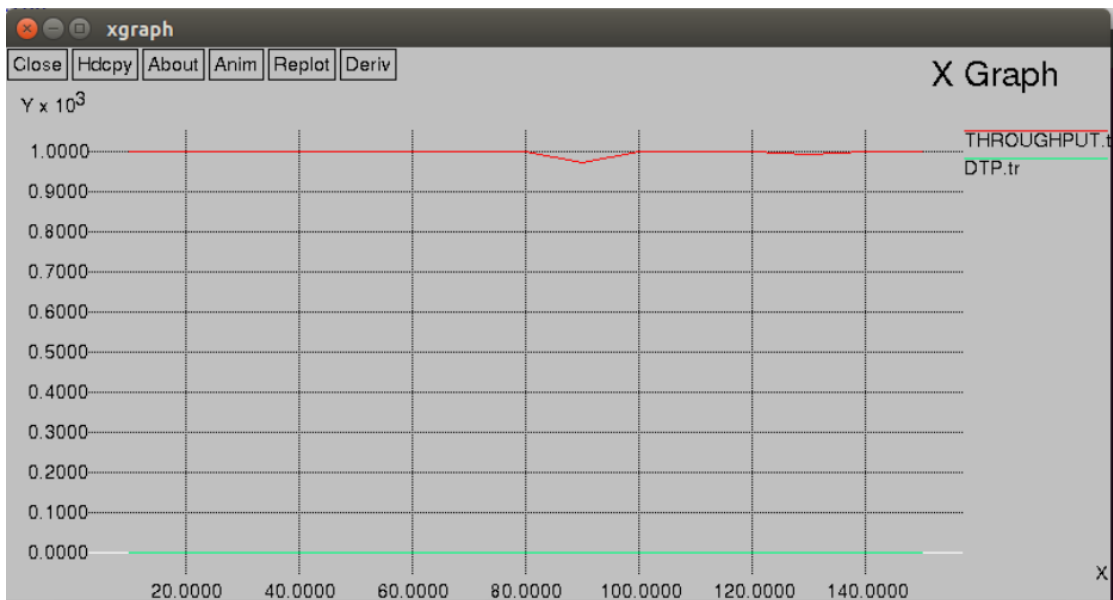


Figure 27: - Throughput

### SUMMARY AND CONCLUSIONS

---

MANETs are capable of offering efficient and effective communication system in those area which are not in the range of permanent network infrastructure. Due to integral design faults, it affects the security mechanism of routing protocol of the network. Several technique were proposed by the scholars of networking discipline from around the world for reducing the effect of a black hole attack. This attack reduce communication efficiency of a network, it broadcast itself as shortest path through it to destination node therefore source node start transmitting data packet aimed to destination through black hole node and it drops all received data packet and send acknowledgement to the source node. The proposed methodology has been simulated in NS-2.35 network simulator in response to the behaviour of black hole attack over AODV routing protocol, and analysed through parameter as follow drop ratio, delay, packet delivery ratio and throughput of a network. The proposed method has shown better results than the traditional AODV routing protocol. It will be helpful for technologies like VANET, IoT and other wireless network.

## LIST OF REFERENCES

---

- [1] Salwa othmen, Faouzi, Aymen Belghith, lotfi kamoun, “Energy , Load and QoS-aware Routing protocol for Ad-Hoc Networks”, IEEE, 978-1-5090-0304-4, 2016.
- [2] Saswati Mukherjee, Matangini Chattopadhyay, Samiran Chattopadhyay, “A Novel encounter based trust evaluation for AODV routing in MANET”, IEEE, 978-1-4799-1848-5, 2016.
- [3] Siddharth Dhama, Sandeep Sharma, Mukul Saini, “Black Hole Attack Detection and Prevention Mechanism for Mobile Ad-Hoc Networks”, IEEE, 978-9-3805-4421-2, 2016.
- [4] Houda Moudni, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi, “Attacks against AODV routing protocol in MANET”,IEEE, 978-15090-0811-7, 2016.
- [5] Sagar R. Deshmukh, Dr. P. N. Chatur, “Secure Routing to Avoid Black Hole Affected Routes in MANET”, IEEE, 978-1-5095-0669-4, 2016.
- [6] Zne-jung lee, So-Tsung Chou,Chou-Yuan lee, “AODV with intelligent priority flow scheme for multi-hop ad-hoc netnork” , Springer, 40595-016-0072-2, 2016.
- [7] Sweta Dixit, Priya Pathak, Sandeep Gupta, “ A Nonel Approch for Gray hole And Black hole Detection And Prevention ”, IEEE, 978-1-5095-0669-4, 2016.
- [8] Apurva Jain, Urmila Prajapati, Piyush Chouhan, “Trust Based Mechanism with AODV Protocol for Prevention of Black-Hole Attack in MANET Scenario”, IEEE, 978-1-5090-0669-4, 2016.
- [9] Dhiraj Nitnaware, Anita Thakur, “Black Hole Attack Detection and Prevention Strategy in DYMO for MANET”, IEEE, 978-1-4673-9197-9, 2016.
- [10] Sushama Singh, Atish Mishra, Upendra Singh, “ Detecting and Avoiding Of collaborative Black hole attack on MANET using Trusted AODV Routing ”, 2016, IEEE, 978-1-5090-0669-4, 2016.
- [11] N.Venkatadri, K.Ramesh Reddy, “Secure TORA: Removal of Black Hole Attack using Twofish Algorithm”, IEEE, 978-1-8286-1, 2016.
- [12] Priya Sethuraman, N. Kannan, “Refined trust energy ad-hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET”, Springer, 2016.

- [13] S.H. Jayachandra, R. Manjunatha, “Analysis of Black hole attack using AODV”, Springer, 2016.
- [14] Balram swami, Ravindra Singh,” Simulation Based compression Between MOWL, AODV and DSDV using NS2”, Springer, 978-3-319-30927-9, 2016.
- [15] Sathish M, Harikrishnan V S, Arumugam K, S.Neelavathy Pari, “Detection of Single and Collaborative Black Hole Attack in MANET ”, IEEE, 978-1-4673-9338-6, 2016.
- [16] R.Priyanka, P.Ramkumar, “Trust based detection algorithm to mitigate the attacker nodes in MANET” , IEEE, 978-1-5090-0669-3, 2016.
- [17] Bikramjeet Singh, Dasari Srikanth , C.R. Suthikshn Kumar “Mitigating effects of Black hole Attack in Mobile Ad-hoc Networks: Military Perspective” ,IEEE, 978-1-4673-9916-6, 2016.
- [18] Houda Moudni, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi “Modified AODV Routing Protocol to Improve Security and Performance against Black Hole Attack” , IEEE, 978-1-4673-7689-1, 2016.
- [19] Kannan Govindan, Prasant Mohapatra, “Trust Computations and Trust Dynamics in Mobile Ad-hoc Networks: A Survey”, Springer, 95616, 2016.
- [20] Lathies Bhasker T,” A Scope for MANET Routing and Security threats”, ICTACT ISSN: 2229-6948, 2013.
- [21] Chaitali Biswas Dutta & Utpal Biswas. An energy aware blackhole attack for multipath AODV. In Business and Information Management (ICBIM), 2014 2nd International Conference. IEEE (2014)
- [22] Emmanouil A. Panaousis, “Security for Mobile Ad-hoc Networks”, book 2012.
- [23] Chaitali Biswas Dutta & Utpal Biswas. A novel blackhole attack for multipath AODV and its mitigation. In Recent Advances and Innovations in Engineering (ICRAIE-2014), International Conference. IEEE (2014)
- [24] <http://www.atacwireless.com/pics/image001.jpg>.
- [25] <https://www.nsnam.org/>.
- [26] Mohamed A. Abdelshafy & Peter J. B. King. Dynamic source routing under attacks. In Reliable Networks Design and Modeling (RNDM), 2015 7th International Workshop. IEEE (2015)

- [27] Sakshi Jain & Ajay Khuteta. Detecting and overcoming blackhole attack in mobile Adhoc Network. In Green Computing and Internet of Things (ICGCIoT), 2015 International Conference. IEEE (2015)
- [28] Hemant Sharma, Koushik Banerjee & Brijesh Kumar Chaurasia. Blackhole Tolerant Protocol for ZigBee Wireless Networks. In Computational Intelligence and Communication Networks, 2014 International Conference. IEEE (2014).
- [29] Kriti Patidar & Vandana Dubey. Modification in routing mechanism of AODV for defending blackhole and wormhole attacks. In IT in Business, Industry and Government (CSIBIG), 2014 Conference. IEEE (2014).
- [30] Abhijeet Salunke & Dayanand Ambawade. Dynamic Sequence Number Thresholding protocol for detection of blackhole attack in Wireless Sensor Network. In Communication, Information & Computing Technology (ICCICT), 2015 International Conference. IEEE (2015).
- [31] Neeraj Arya, Upendra Singh & Sushma Singh. Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm. In Computer, Communication and Control (IC4), 2015 International Conference. IEEE (2015).
- [32] Ankit D. Patel & Kartik Chawda. Blackhole and grayhole attacks in MANET. In Information Communication and Embedded Systems (ICICES2014), 2014 International Conference. IEEE (2014).
- [33] Ram Kishore Singh & Parma Nand. Literature review of routing attacks in MANET. In Computing, Communication and Automation (ICCCA), 2016 International Conference. IEEE (2016)
- [34] Anurag Gupta & Kamlesh Rana. Assessment of various attacks on AODV in malicious environment. In Next Generation Computing Technologies (NGCT) 2015 1st International Conference. IEEE (2015).