AN OPTIMIZED AD HOC ON-DEMAND DISTANCE VECTOR PROTOCOL IN MOBILE AD HOC NETWORKS.

Dissertation submitted in fulfilment of the requirements for the Degree of

MASTER OF TECHNOLOGY

in

INFORMATION TECHNOLOGY

By

Hiren Thakor

11609514

Supervisor

Makul Mahajan

School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

November 2017

ABSTRACT

MANET is the dynamic environment where mobile node dramatically changes their short-life status according the network infrastructure. Every single mobile node has its own wireless hardware i.e. antenna and receiver. It is useful in ad hoc network to communicate each other using wireless link to transfer data to freely moving nodes, in simple every single node will act as router as well as end device. The core feature of the MANET is self-organized, decentralized, and a dynamic change in the topology. Mobile nodes are using this kind of environment to archive multi- hop free network without any backbone support. Dealing with ad hoc environment we faced so much challenges including bandwidth also limited resource like battery, processing power and on-board memory. In the term of QoS we will provide the best practical solution for this technology through routing.

DECLARATION

I hereby declare that the research work reported in the dissertation/dissertation proposal entitled " **AN OPTIMIZED AD HOC ON-DEMAND DISTANCE VECTOR PROTOCOL IN MOBILE AD HOC NETWORKS.**" 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.Makul Mahajan. 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.

Hiren Thakor

11609514

ACKNOWLEDGEMENT

Gratitude cannot be seen or expressed. It can only be felt in heart and is beyond description. Often, words are inadequate to serve as a model of expression of one's feeling, specially the sense of indebtedness and gratitude to all those who help us in our duty. It is of immense pleasure and profound privilege to express our gratitude and indebtedness along with sincere thanks to our mentor Mr. Makul Mahajan, for her invaluable guidance, motivation and encouragement in spite of her busy schedule. I am grateful to our Lovely Professional University for me with an opportunity to undertake this research topic in this university and providing all the facilities. Finally, we would like to thank our parents and our family members for their constant support. We whole heartedly thank them all for their encouragement and support all the way from home from their hearts. We dedicate all our success to each one of them.

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation/dissertation proposal entitled "**AN OPTIMIZED AD HOC ON-DEMAND DISTANCE VECTOR PROTOCOL IN MOBILE AD HOC NETWORKS."**, submitted by **Hiren Thakor** at **Lovely Professional University, Phagwara, India** is a bonafied record of his / her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Signature of Supervisor

Makul Mahajan

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: _____

TABLE OF CONTENTS

first page i

PAC form ii

Abstract iii

Declaration by the Scholar iii

Supervisor's Certificate iv

Acknowledgement vi

Table of Contents vii

List of Figures x

List of Tables xi

CHAPTER 1 1

INTRODUCTION 1

1.1 Introduction 1

1.2 The Proactive protocol 2

1.2.1 Destination-Sequenced distance vector 2

1.2.2 Wireless routing protocol 2

1.2.3 Global State Routing Protocol 3

1.2.4 Fisheye State Routing Protocol 3

1.2.5 Source-Tree Adaptive Routing Protocol 3

1.2.6 Distance Routing Effect Algorithm for Mobility 4

1.2.7 Multimedia support in Mobile Wireless Network 4

1.2.8 Cluster-head Gateway Switch Routing Protocol 4

1.3 The Reactive protocol 5

1.3.1 Ad Hoc On-demand distance Vector (AODV) 6

1.3.2 Dynamic Source Routing(DSR) 6

1.3.3 Routing on demand acyclic Multipath (ROAM) 6

1.3.4 Light-Weight Mobile Routing (LMR*)* 6
1.3.5 Temporally Ordered Routing Algorithm (TORA) 7
1.3.6 Associatively Based Routing (ABR) 7
1.3.7 Signal Stability Adaptive (SSA) 8
1.3.8 Relative Distance Micro-discovery ad-hoc Routing (RDMAR) 8
1.3.9 Location-Aided Routing (LAR) 8
1.3.10 Ant-Colony based Routing Protocol (ARA) 8
1.3.11 Cluster Based Routing Protocol (CBRP) 9
1.4 Security in Mobile Ad-Hoc Network 9
1.4.1 Network Overhead 10
1.4.2 Processing Time 10
1.4.3 Energy Consumption 10
1.5 Security Challenges in MANET 10
1.5.1 Security Services 11
1.5.2 Attacks 12
1.6 The Black Hole Attack 13
CHAPTER 2 14
LITERATURE SURVEY 14
CHAPTER 3 20
SCOPE OF STUDY 20
CHAPTER 4 20
OBJECTIVE OF RESEARCH 20
CHAPTER 5 21
RESEARCH METHODOLOGY 21
CHAPTER 6 24
EXPECTED OUTCOME 24
REFERENCES 24

LIST OF FIGURES

FIGURE NO.	FIGURE DESCRIPTION	PAGE NO.
Figure 1.2	Proactive Protocols.	2
Figure 1.3	Reactive Protocols.	5
Figure 1.4	Relation between Security Parameter and Security aspect	10
Figure 1.6	Black hole attack in AODV	14
Figure 5.1	"Acknowledgement bit" without Malicious node.	22
Figure 5.2	"Acknowledgement bit" without Malicious node	22

CHAPTER 1

INTRODUCTION

1.1 Introduction

MANET is the dynamic environment where mobile node dramatically changes their short-life status according the network infrastructure. Every single mobile node has its own wireless hardware i.e. antenna and receiver. [1] It is useful in ad hoc network to communicate each other using wireless link to transfer data to freely moving nodes, in simple every single node will act as router as well as end device. The core feature of the MANET is self-organized, decentralized, and a dynamic change in the topology. Mobile nodes are using this kind of environment to archive multi- hop free network without any backbone support. Dealing with ad hoc environment we faced so much challenges including bandwidth also limited resource like battery, processing power and on-board memory. In the term of QoS we will provide the best practical solution for this technology through routing.

Routing is the heart of any network topology. The routing algorithm is categorized mainly in the three manner in MANET,

- Proactive Routing
- Reactive Routing
- Hybrid Routing.

Also it categories even based on implementation that is,

- Geographical Routing
- Geo-cast Routing.

The IEEE 802.11 is the name of the MANET. The MANET is built by very dedicated mechanism of the freely moving nodes. Which is interconnected though wireless medium. That's why the routing in MANET are very complex and very interesting part of MANET's node life. Apart from that we can manipulate routing is the art of delivering data form one single node to another node, as we called it sender and a receiver. Although the in the MANETS there are some obstacles that we need to consider seriously, like minimal control overhead, minimal processing overhead, multi hop routing capability, dynamic topology maintenance and loop presentation [2].

1.2 The Proactive protocol

Each node maintains routing every other node in the network. The routing information define by a number or different tables. These tables are updated in specific time interval or when the network topology changes. Apart from that each protocol is divided on the basis of how they update the routing information. The diagram shows the list of proactive protocols and their information,

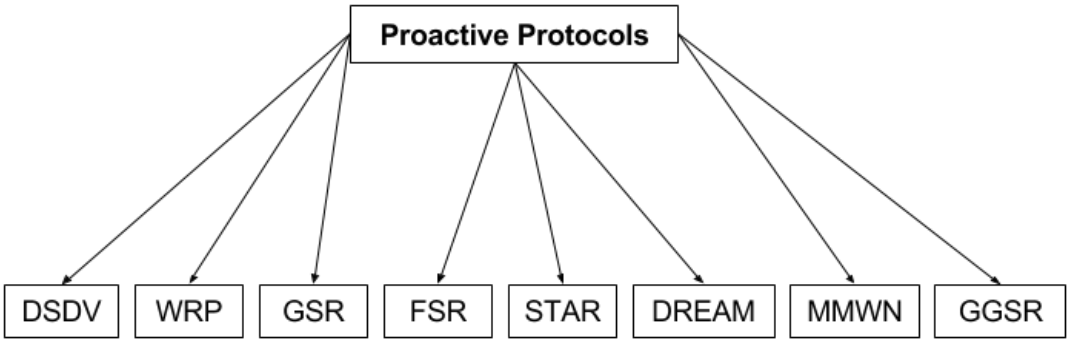


Fig.1.2 Reactive Protocols.

1.2.1 Destination-Sequenced distance vector

The DSDV calculation is development of DBF, which gives circle free courses. It gives single way to goal, which is chosen by remove vector most brief way steering calculation. For lessening measure of overhead transmitted through system, two sort of refresh parcel are utilized, first is "Full Dump", Second is "incremental" [1, 2]. Full dump bundles convey all the accessible steering data and the incremental parcels conveys just the data change in full dump parcels. Still the convention not fit for good the reason is that it creates vast

measure of overhead to the system, because of the necessity of the occasional refresh messages, and the overhead becomes as indicated by O(N2), Therefore the convention does not give QoS in the expansive system.

1.2.2 Wireless routing protocol

WRP also provides loop free information with the help of pre-processor data. WRP requires each node to maintain four routing tables. This introduce significant amount of memory to overhead at each node according to network size. Another drawback of this protocol is that it establishes communication with neighbours with hello messages, so it takes significant amount of time and bandwidth of the network.

1.2.3 Global State Routing Protocol

GSR is acquired from customary connection state convention. This control the data of connection state calculation by limited refresh message between middle of the road hubs. In the GSR all hubs have one connection state table that stores data of courses utilizing neighbouring hubs and refresh by occasionally trade information between neighbouring hub. This assistance in diminishing control messages yet it likewise gives us the bigger refresh message while the system a lot of huge, that is the reason it devours huge measure of data transfer capacity of system to executing this kind of refresh messages.

1.2.4 Fisheye State Routing Protocol

FSR is the elder child of the GSR while it better to make applicable bring up-to-date messages by updating network data using at higher frequency than for the remote node, which relies outside the fisheye scope. This makes FSR more scalable in the large network. Although this makes some impact on the QoS of the network [1, 2].

1.2.5 Source-Tree Adaptive Routing Protocol

It additionally relative of connection state steering convention, where every member switch keeps up its own particular source tree, which is set of connections that contain the data about goal. This convention diminishes real measure of directing overhead in the system utilizing slightest overhead steering approach (LORA) [1, 2], additionally it utilizes the ideal steering approach(ORA) when it required. The convention utilizes both of this ways

to deal with make the conceivable adaptability to the colossal system. That is the reason it lessens the use of data transmission in the system. In any case, this convention expends the noteworthy measure of time to handling independently keep up the tree of all hubs in the system [1].

1.2.6 Distance Routing Effect Algorithm for Mobility

In this protocol all node knows its geographical position by using GPS, this position or coordinates are periodically exchange and stores in the location table or routing table. The advantage of this type of construction is reduce the bandwidth usage instead of delivering the link state routing table to each node just send the location table, and that means this gets more scalability in the network.

1.2.7 Multimedia support in Mobile Wireless Network

This convention in light of grouping approach that contain two kind of hub that is, switch and endpoints, each bunch has additionally a locationmanager (LM), which play out the area administration undertaking of each group. All data of this convention is stores in the dynamic conveyance database. The upside of this convention is that the LM is utilized for area finding and refreshing, that is the reason the system overhead decrease contrast with another table driven conventions. Notwithstanding, the area finding and refreshing is most mind boggling assignment in the group based system. That is the reason it is hard to actualize in the substantial system.

1.2.8 Cluster-head Gateway Switch Routing Protocol

This is also type of cluster based protocol, where all nodes are included in the cluster, within a cluster a single node maintain the communication of all the inner nodes of the cluster. This type of node called cluster head node. And the also there is one gateway node that connects all cluster together in the network. The advantage of this protocol is that it all communication done by the cluster head node so we don't need to send any type of routing information, that's why the routing overhead is too much low.

1.3 The Reactive protocol

On demand routing is kind of dynamic way to update information to reduce overhead in the proactive protocols, that means the rout information only update when the transmission is occurs between sender and receiver. The optimal route discovery held by flooding the packets over the network to find the receiver, If the packets reach to the receiver then the route- reply packet will be sent back to the sender by piggybacking or same flooding.

The reactive routing protocols categorized in two ways,

- Source routing
- Hop-Hop routing

In the Source routing protocols each packets carry complete source to destination information in it. That's why each node need to forward these packets according to information in the header packets. It means that the no need to worry about up-to-date routing information about active route for the intermediate node in order to forward packets to the destination. The unreliability of the source routing protocols is that it not performs well in the large networks.In the Hop-by-Hop or Point-By-Point routing protocol each packets carry only destination information and next hop address. in that way every node need to use the routing table to reach out destination node. The advantage of this way is accepted dynamic change in the network due to that reason it's scalable in the large MANETs network overhead increased as continue increased amount of the network traffic. And therefore highly dynamic and large networks.

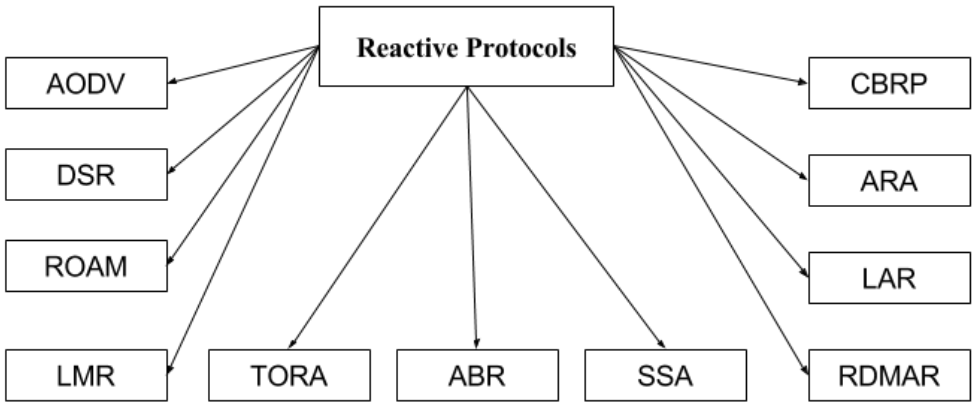


Fig.1.3 Reactive Protocols.

3.1 Ad Hoc On-demand distance Vector (AODV)

The convention's capacity inherent from the based DSDV and DSR Algorithms. It utilizes the interfered with beaconing and sequencing numbering technique of DSDV and comparable course revelation method as in the DSR and furthermore from AODV [1]. The most known contrast amongst AODV and DSR in DSR parcels contain the all the steering data yet AODV bundles contain just goal address. This implies AODV has less steering overhead in the system then DSR. The other contrast is the DSR course answers conveys all the course data alongside each hub address however, in the AODV the course answers contain just conveys goal ip address and grouping numbers [1, 2].

1.3.2 Dynamic Source Routing(DSR)

As specify prior in the DSR every parcel conveys all steering data to all the directing hub. That implies more activity and not appropriate for the vast systems. As the measure of overhead expanded as proceed expanded measure of the system movement. Also, hence profoundly powerful and vast systems overhead expend the most data transfer capacity. Nonetheless, this convention has brilliant side for little systems contrasted with AODV and TORA, this convention can perform extremely powerful little system. Discussing advantage the DSR hub can store the numerous course data in their course reserve, its implies that it can exceptionally successful when its drive course disclosure process, simply check the course store! Also, if substantial course is found there then no need of course revelation process [1, 2].

1.3.3 Routing on demand acyclic Multipath (ROAM)

The Routing convention utilizes Inter-Nodal Coordination with coordinated Subgraphs, which is gotten from Router's separation to the goal. This operation is Referred to as "Dispersion calculation". [02] From that the convention dispense with The pursuit to unendingness Problem Which is available a large portion of On-Demand Routing Protocol. This convention stops the Multiple surge look When no longer goal seek required or not reachable. Another imperative thing is that this convention every switch keeps up passages of the goal, which is stream the information bundle through them. This is exceptionally valuable for decreasing Significant measure of capacity and expend low transfer speed.

This is extremely Improving Network availability in exceptionally mind boggling and vast systems [1, 2].

1.3.4 Light-Weight Mobile Routing (LMR*)*

The LMR also categories in on-demand routing protocols which is used flooding technique that help for determine routes. this protocol is reliable because of by allowing nodes to choose the next available route to a Particular destination without Initiating route discovery procedure [02]. Also LMR maintains multiple route to each require destination. Another advantage of this protocol is only each node is maintained only of its neighbours Routing information. This means very less delay and low use of bandwidth in the route discovery process. although LMR produce fake routes which is held in the delay [1, 2].

1.3.5 Temporally Ordered Routing Algorithm (TORA)

The TORA is acquired from the LMR convention progressively on the off chance that it courses repair technique is same as in the LMR and furthermore the comparative connection inversion process is the same. The principle preferred standpoint of this convention is bolster multicasting from utilizing lightweight versatile multicast calculation. [02] Also another favorable position of the TORA is that its control messages are connect extremely far through its neighbor hub which why it is helpful in where the topology changes every now and again. The disservice of the calculation is that it likewise delivers counterfeit course simply like LMR [1, 2].

1.3.6 Associatively Based Routing (ABR)

The ABR is also source initiative routing protocol which is introduce in the 1993 by Chai Keong Toh. Toh realize that The primary argument behind the protocol is there is no point of choosing route for particular node while it knows that the route is unstable or going to be broke soon. So, he introduces the new routing metric that is associativity tick, also the concept of associativity. The primary route selection based on the stability constraint. however, the protocol consumes too much bandwidth for maintaining stability therefore it uses beaconing in periodic time. this leads to the major power consumption [1, 2].

1.3.7 Signal Stability Adaptive (SSA)

The SSA protocol is inherited from the ABR. The SSA is using temporary wireless link for temporary stability route discovery and connection route establishment. The stable route is selected by using the process of how much longer lived the temporary link. The SSA is also use the ROUTE_REQ like DSR protocol. From the stability route choosing process chose the best strength live link which is always short path, that's why the protocol is potentially creates the delay for the finding the long route [1, 2].

1.3.8 Relative Distance Micro-discovery ad-hoc Routing (RDMAR)

The RDMAR maintain the overhead by calculating minimum distance for source to destination and try to minimize the result and store in the overhead, therefore the in the route request packet has limited number of hop. From that the route discovery procedure only covers the localized region. And this will lead to consume very generous amount of energy and bandwidth. but the major disadvantage of this protocol is to perform discovery process, the source and destination must be communicated previously, if the they are communicating for the first time then the protocol act as old flooding algorithm [1].

1.3.9 Location-Aided Routing (LAR)

LAR is based on flooding algorithm like DSR. But the difference of LSR is it uses route discovery using traditional flooding technique with optimize the overhead adding location information. This protocol is performing the task in two part, first one assume that every node knows its location using GPS, and using that information the protocol for finding the zone using creating boundary where each route request packet reaches the desired destination. another part is the to store the route information in the route request packet that is only considered for the desired destination node. And from this two method will gives protocol reliability and uses the low bandwidth. The disadvantage of the protocol is that each and every node needs GPS, that is very unusual [1].

1.3.10 Ant-Colony based Routing Protocol (ARA)

The ARA is based on the behaviour of the one of the activity of the ant while they search for food. In that activity an ant walks through the food directly from colony to the food but also it leaves the trail of its route in for the others. For the trail it marking of the path from

the colony to food by using its pheromone, which is also not permanent. The others ants are follow that pheromone to reach out the food. As same our protocol works first the route discovery process a Forwarding ANT(FANT) is spread to the network just like RREQ, Here the pheromone is the calculation of numbers of hop count that FANT has taken to reach each node, when the FANT reaches to destination it will generate Backward ANT(BANT) who will return to the source and after it reaches to source then the packet dissemination start. The protocol uses the flooding for the first time that means it may be scalability problem with the protocol [1].

1.3.11 Cluster Based Routing Protocol (CBRP)

The CBRP is generate the clusters of the node, and each cluster has its own cluster head that communicate to other cluster's head node. And the all routing information exchange through this head node. So, the advantage of the protocol is the less overheads are transmitted to the network compared to the traditional flooding protocol. Although the overhead is carrying the large amount of data that is cluster hierarchical information, which causes the bandwidth and delay also the route maintenance is very complex in this structure of nodes [1,2].

1.4 Security in Mobile Ad-Hoc Network

As mention that Mobile Ad-Hoc network is self-organizing and self-maintains network [3]. In MANETS each node responsible for communicating and act as itself routers. Also maintain the perfect synchronized work thorough communicating its neighbours. From lack of central-point control in the network communication we face the most critical situation of malicious activity by the other fake node [3].

In MANET's we use some important matrices known as "Security Parameter" fig 3 shows the importance of relation of the security parameter with MANET.

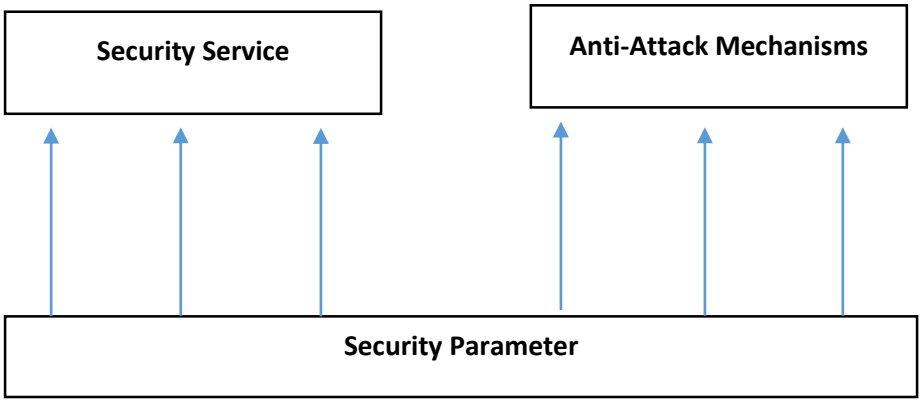


Fig. 1.4. Relation between Security Parameter and Security aspect.

1.4.1 Network Overhead

This parameter is defining by the numbers of control packets generated by security approaches. Due to the nature of the network, numbers of the easily lost or collide. And packet lost is the most responsible for the congestion and collision [17].

1.4.2 Processing Time

This parameter stated that every security approaches need to be work done by in the time manners which is the most effected in the MANET network environment, which relay on the very short time [17].

1.4.3 Energy Consumption

As we all know in MANET, all node has limited energy resources, therefore optimizing energy consumption is highly recommended. High energy consumption reduce life of the node in the node [17].

Each security protocol must be aware of this parameter for better performance and high reliability [17].

1.5 Security Challenges in MANET

In the MANET security is very challenging task to maintain without central administration. So in order to secure the network we use the security services and the attacks [17]. Security

services is the strong polices that protect the network. The attacks are the different methods that are used to defeat the real threat in the network. The next two section describes the two mechanism of the security in the MANET.

1.5.1 Security Services

There are five security services that implemented on the MANET networks by the creators. This five terms are the most respected for preventing the attackers. This are depending to each other so, if any of them fail to perform other will be affected.

1.5.1.1 Availability

According to this service, each and every node which is take part in the communication have access to the corresponding data. Also it has access to that in the specific time manner because time is also a major factor of the network [17].

1.5.1.2 Authentication

According to this service, each and every node must be conformed the identity of participant node. For that they use the certification from both side and verified each other in the network [17].

1.5.1.3 Data confidentially

According to this service, each node has the access for the data that is transfer over the network. By executing this task, we use the encryption for the data to secure the data. The encryption is the main key of the network and performing nodes use the distributed key encryption technique because of the lacked of the central management [17].

1.5.1.4 Integrity

According to integrity security service, the data which is modify by the authorized nodes only. The node can perform modification or delete that packet data which is created. This is very useful in the man in the middle attack for generating the authentication and access limit of the data [17].

1.5.1.5 Non-Repudiation

According to security service, not a single node denies their performing act or role to do. That means if node A send data to node B when the data is reach to the node B, at that node B cannot deny that I don't have that data it should be send conformation packet to the node A [17].

1.5.2 Attacks

MANET has very dashing features like hop-to-hop communication, open border, wireless communication easy to setup [17], so this all features invites the real threats in the network in the in the face of malicious node. All the malicious node work as the attacker of the network. There are many type of attacker nodes but mainly they are in the in two categories first, insider node and second is outsider attacker node. The internal node is very difficult than external attacker node, by detecting and removing it. Also they sometime synchronized and make damage on network, also called collaborative attack [3]. Following table contain the different type of attacks that found in the MANETs.

Attack Type	Attack Behaviour
Selective forwarding attack	Subjective refuse to forward specific packets and discarded packets.
Black hole attack	Neighbouring nodes send all packets to malicious nodes, which are then discarded by these nodes.
Spoofing and tampering attack	Subjective forge and modify message content.

Sinkhole attack	Similar to the black hole attack but with malicious nodes located closer to the sink node.
Denial of Service attack	A malicious node forces the node that provides services to produce an error or exhaust resources via either dishonesty or camouflage.
Wormhole attack	A malicious node has a strong transceiver ability, causing the physical nodes on multi-hop neighbouring nodes to be mistaken for one another.
Flooding attack	Malicious nodes communicate with and query other nodes for replies constantly, exhausting these node's energies.
Sibyl attack	Malicious nodes disguise a node using multiple identities.

Table 1. various MANET's attacks

1.6 The Black Hole Attack

The black hole attack threated only on network layer, in this attack the performing node never pass the data packet to the destination node for the sender. It is either drop that packets or pass to the other malicious node.

In the process of route discovery process, the source node broadcast the route request packets, RREQ to all neighbor to reach out the destination node. From that, the malicious node rapidly response the RREQ to the sender saying that it has perfect route with high sequence numbers and less hop counts, so on behalf of that information the source node marks the route information on the routing table. And after words it makes the communication through the malicious node. Aftermath, the attacker now drops all the packets or send to the other malicious node. The

following illustration is a describes the working image of the black hole attack.

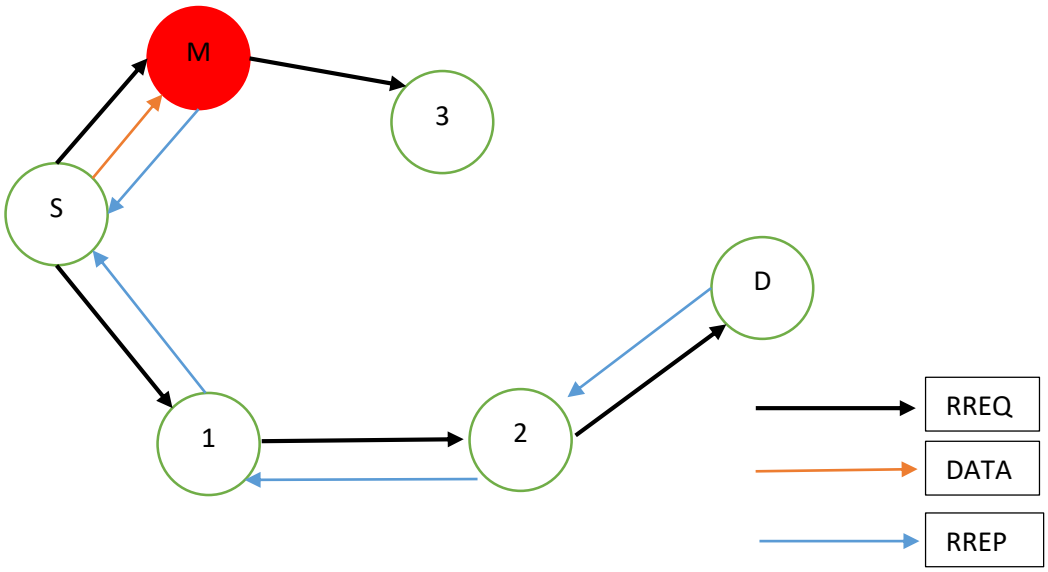


Fig. 1.6. Black hole attack in AODV

CHAPTER 2
LITERATURE SURVEY

Research in MANETs is very vast subject, many researcher is work so hard for the making this technology very reliable and very robust. Some of the research are very helpful in my research work. This are some of the summary is describe below.

Mehran Abolhasan *et. al.* [1] stated reviwed the manets protocol using very authenic manner by providing the ns2 simulatous's data that used to defaine which protocol perform better. Also in this paper the aouther provide the information about working of the all the above protocole. [1].

S. Mohapatra *et. al.* [2] stated to desine any kind of wireless network the primary stratages are path routing and the selaction. The seleceted protocol in Mobile Adhoc Network (MANET), the data delievery and data integrity should be better. Before analysis of any protocol we need to select the performance of a particular protocol. In this paper, it carried out the performance analysis on Dynamic Source Routing(DSR), ADHOC On- demand

vector(AODV), Optimized link, Destination Sequenced Distance Vector(DSDV),Optimized Link Staet Routing(OlSR). [2]

Xianji Jin *et. al.* [3] stated that an intrution detation scheme based on multiagent system and node trust value can archive both hieger detaction rate and lower false positiverate of internal node intrution detaction in the cluster Wireless sensor network. In the paper t establish both culster head and normal sensor node which perform Intrution detaction to detact the threts.

Kapang Lego *et. al.* [4] In this paper, all the famous protocol has been verified and compare over the simulation with the parameter packet delivery ratio and avrage end to end delay. The protocols are AODV, DSR and DSDV.

Md Raqibull Hasan *et. al.* [5] in this paper they found the way to detect and avoid black hole attacks, also propose a new routing protocol, termed Enhanced Ad hoc On-Demand Distance Vector (E-AODV) by modifying the Route Reply (RREP) system based on AODV. The RREP in E-AODV updates the destination sequence number corresponding to a fresh route request. By comparing sequence numbers from multiple replies, it detects the existence of black hole behavior because the attacker usually sends a much higher sequence number, compared to the actual one generated from the destination. After detection, the receiving meter sends a deny reply to the destination. Upon receipt of the deny reply, the destination regenerates RREP with an updated sequence number, which is kept to itself. Since attackers only respond when a new request is initiated, this time the attacker will not act because no request is initiated. Therefore, it is able to avoid the effects of malicious meter.

Kavneet Kauri *et. al.* [6] stated that it enables the communication between ech other as well as unit on the road side by the Vehicular Adhoc Network(VANETS). It is a challengeing job to develop a an efficient routing for the network because of large mobility and regular changes in the network. Ant Colony Optimization based AODV-R protocol for better data aggregation and route selection.

Mohammed Aashkaar *et. al.* [7] propose that in AODV protocol is enhanced by the aouther which is the most proper manner with the new one proposed method. Like they use

the most probably work in the different manner. Also they describe the all AODV functionality over the NS2 siimulation. [7]

Nicklas Beijar et. al. [8] stated that a routing protoocl wichi is known as zone routing based on the cluster routig protocol. In the routing protocol packets are reach to the destination by zone way. The main aim of the protocok is define a poerful anti thret mecahnism by usuing the zone routin. The aouther mainly focused on the zone routing protocol's function work, that is totally depand on the cluster routing protocol. There are seprate node in the zone or cluster which show the working of the zone routing protocol. First zone is depand on the secound one also the chain goes on.

Yumei Liu *et. al.* [9], in this paper multipath routin protocol is desccused by the aouter. The protocol define as MMRE and AOMDV that is Ad Hoc on demand multipath Distance Vector Routing protocol.The enaergy is incresded by the node if the nodoe is used to forward to rest of the nodes wichi is not in the use. That is define the bettery usage of the nodes. Also they define the seprate nodes energy without any further communication.

Kulasekaran *et. al.* [10] stated a routing protool that defines the security by proposing new protocol named as SAODV-2. This protocol works by maintaining the security activity more preciely. Also they utilize the based validation procedure. Also they include the hop count facility by the adding it on another hop to hop methology. In which the data of the hop count is maintain without the information.

Houda Moudni, Mohamed Er-rouidi *et. al.* [11], proposed an answer, which enhances the security of the Ad-hoc On-request Distance Vector (AODV) steering convention to chance the dark gap assaults. The arrangement evacuate the dark gap and the different dark opening assaults. The recreation comes about utilizing the Network Simulator NS2 demonstrates whicu is given the consequence of most famous parameter.In the proposed technique the RREQ is changed by the creator keeping in mind the end goal to give the secutrity component. From that they utilize the new felid called VERIFIED additionally the it contain the one piece that is either 0 or 1, which is checked to other bury intervene hub that the accompanying RREQ parcel is geniune or not. Likewise this calculation works fine in the clarified situations.

Jaisankar, N. *et. al.* [12] the authors were proposed an approach to detect black hole nodes in the MANET. In the proposed method,the watch over node calculate the ratio of the

number of packet drops with forwarded packet numbers. And this ratio is compare with pre defined threshold after that it will be decide that the node is malicious or not.

Jhaveri, R. H., Patel *et. al.* [13] In a plan for the steering convention AODV is proposed to recognize and expel Gray Hole and Black Hole Attacks. In this plan, the moderate hub distinguishes the malevolent hub sending false directing data by computing a PEAK esteem, where the PEAK esteem is the most extreme conceivable estimation of the arrangement number that any RREP can have in the present state. At that point, when this halfway hub gets a RREP having arrangement number higher than the ascertained PEAK esteem; it is set apart as DO_NOT_CONSIDER.

Ghathwan *et. al.* [14] in this paper it defines the method of defancive attacke mechanism for the blcak hole attack that is totally works on the AODV routing protocol. Also thet use the a* algorithm and other one is floyed algoorithm for mitigating the black hole attack. The protocol use the hope count and other two algorithm wich is usesd to deside the shortest routing path.

Ahmad, S. J. *et. al.* [15], in this paper the aouther provide the security mecahanism in MANETs to prevant the black hole attack. It provides the method called security Code Diistion Security Method (CDAM), it represent the nodes code by using the packet header. They consider the packet imformation for mitigaing the vlack hole attack.

Debarati Roy Choudhurya *et. al.[*16] proposed the approach they follow, basically only modifies the working of the source node, using an additional function pre_ Request Receive Reply (Packet P).Apart from this, they also added a new table _RREP _Tab, a timer M_WAIT_TIME that is the total RREP time or half of it and a variable Mali_ node to the data structures in the default AODV protocol. They provide such great solution for the detactting the malicious node.

Ali Dorri *et. al.* [17] in this paper authers are given brif information about the Challenges in the MANET network. From that the security protocool and the security services defines in the very decent manner. The securitty atacks are also very well explain to understand the how they work perfactly. Authors present an elaborate view of issues in MANET security. Based on MANET's special characteristics, also define three security parameters for MANET. In addition they divided MANET security into two different aspects like security services and attacks. A comprehensive analysis in security aspects of MANET and

defeating approaches is presented. In addition, defeating approaches against attacks have been evaluated in some important metrics.

Vimal *et.al.* [18] authors provides the method for the mitigating the black hole attack in the ad hoc network they use the time slot technique for the choosing the right path at the routh descovery prosess. They use the CCRT table for the storing the RREP from all the coresponding intermediate node and also from the source node. By the given time slot they use the hop count and packet delay ratio to find out the better route. Aslo they give the NS2 simulation of that proposed working alsorithm. They also compare the enhanced protocol from the traditional protocol on the bases of the standerd parameter.

Ehsan Amiria *et. al.*[19] stated various intrution detaction system in the friendly manner. IDSis the most reliable security system that detact the threts and then aoutomaticly moitored the network. To detect the attack, the IDS system, crate an analysing a monitor the activities of the network. it also verifies [19].

Yuvraj Singh *et. al.* [20] stated the IDS for the making MANET more reliable. Making the two phases of the IDS wich is, detection during route establishment and detection during data forwarding. They propose an algorithm for the detection of malicious nodes in the wireless ad hoc networks.The malicious node may be defined as a node which does not follow the exact behavior. Most of the attacks are accomplished by modifyinga message or simply not to forward the message which it is supposed to forward.

J.Manoranjini *et. al.* [21] propose a new protocol with hybrid automatic detector and kalman Bucy filters that detect the black holes more accurately regardless of the node movements. Also provide a trust model for the aoutoomatic anylizing and detaction tecnique. By the tiem it will adopt all network communication over the network.

Nadeem *et.al.* [22] stated that Intrusion detection and prevention provides a way to protect mobile ad hoc networks (MANETs) from attacks by external or internal intruders. There are two principal intrusion detection techniques: anomaly based intrusion detection (ABID) and knowledge based intrusion detection (KBID); additionally, specification based intrusion detection techniques (SBID) have also been proposed.

Ahmed M *rt. al.*[23] expressed a technique for detacting vindictive hub in the OLSR convention. Likewise the proposed work relieve the impact of the bad conduct hub in the

system. Likewise Focusing on the Optimized Link State Routing (OLSR) convention, an IDS component to precisely recognize and disconnect misconduct node(s) in OLSR convention in light of End-to-End (E2E) correspondence between the source and the goal is proposed. The cooperation of a gathering of neighbor hubs is utilized to settle on precise choices. Making and broadcasting assailants rundown to neighbor hubs empowers other hub to disconnect trouble making hubs by killing them from the steering table. Dispensing with mischief hub enables the source to choose another confided in way to its goal. The IDS is ropose has a place with determination based discovery with conveyed helpful hubs that are reasonable for MANETs. The approves the correspondence way at that point recognizes and secludes trouble making hubs in the invalid ways.

Muhammad Imran *et. al.* [24] expressed that the reviwe mali of cious hub detaction for the wormhole assault in the MANETs. The detaction procedure depends on the some imperative parameter that is, Location, Time,Hop Count, Neighborhood, Data parcel, Route Reply and Route Request. So the creator give the short data of the considerable number of terms that is utilized for the correspondence in the MANETs. Likewise they defrentiate the a portion of the IDS for the absence of the eperformance based. Likewise they influence a concise informtion to table for the copmparition and simulaion result utilizing the above parameter. The conceivable impediments of Intrusion Detection Systems (IDSs) are likewise talked about. This work gives a premise to fabricate an effective IDS to identify wormhole assaults in MANETs. Concurring creator, the procedures in light of course ask for (RREQ) or bounce tally would be superior to anything different methods to distinguish wormhole assaults [24].

CHAPTER 3

SCOPE OF STUDY

Portable Ad hoc Networks (MANETs) work with no settled foundation and every hub in the system carries on as a switch keeping in mind the end goal to transmit information towards the goal. Because of the absence of essential issue of control, MANETs are more helpless against steering assaults when contrasted with different systems. Wormhole assault is a standout amongst the most extreme steering assaults, which is anything but difficult to execute yet difficult to identify [24]. The extent of the examination is valuable for the alleviating the system assaults and keeping the system dangers. The component of the examination is giving the better and secure correspondence for the MANET systems. In particular, the AODV convention and other receptive conventions. Additionally, the exploration distinguishes the pernicious hubs, so we can simple withdraw it from the correspondence.

CHAPTER 4

OBJECTIVE OF RESEARCH

1. To propose the secure AODV protocol for mitigating the effect of black hole attack in the Mobile Ad-Hoc Network.
2. To propose the reliable method for detecting and removing the malicious nodes from the Mobile Ad-Hoc Network.
3. To implement the above proposed matter using NS2 simulator on the parameters Throughput, Packet-Delay Ratio and Delay.

4. To compare the proposed protocol with traditional AODV protocol using the above parameter.

CHAPTER 5

RESEARCH METHODOLOGY

The black hole attack threated only on network layer, in this attack the performing node never pass the data packet to the destination node for the sender. It is either drop that packets or pass to the other malicious node. In the process of route discovery process, the source node broadcast the route request packets, RREQ to all neighbor to reach out the destination node. From that, the malicious node rapidly response the RREQ to the sender saying that it has perfect route with high sequence numbers and less hop counts, so on behalf of that information the source node marks the route information on the routing table. And after words it makes the communication through the malicious node. Aftermath, the attacker now drops all the packets or send to the other malicious node. The following illustration is a describes the working image of the black hole attack. See the fig.3.

For detecting the malicious nodes, we propose following methodology, which is carry out in the route discovery process. For that first consider an ad hoc network. In to the network a sender S wants to communicate to receiver R, and there are also intermediate nodes A and B also one malicious node M.

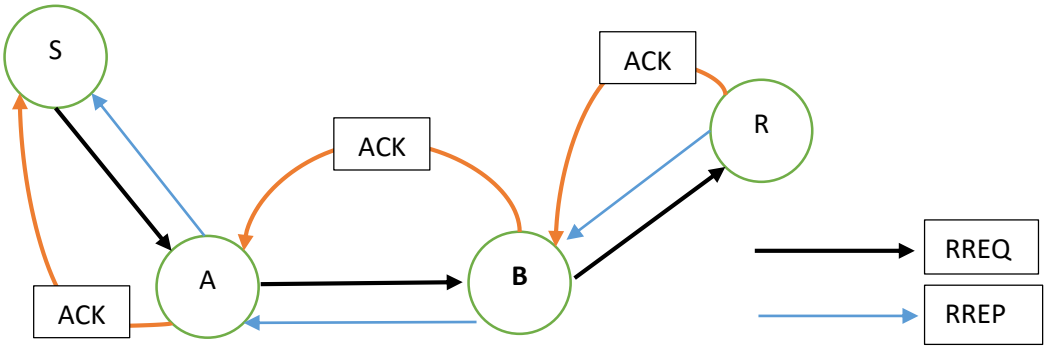


Fig. 5.1 “Acknowledgement bit” without Malicious node.

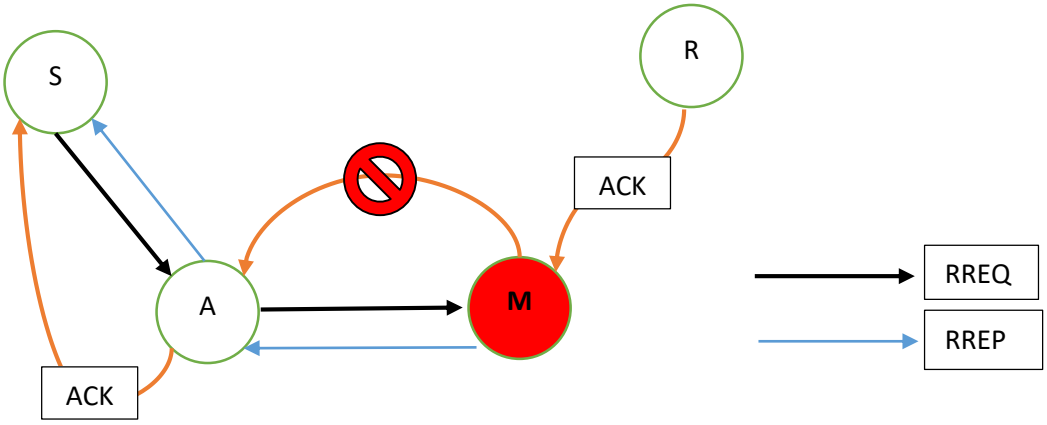
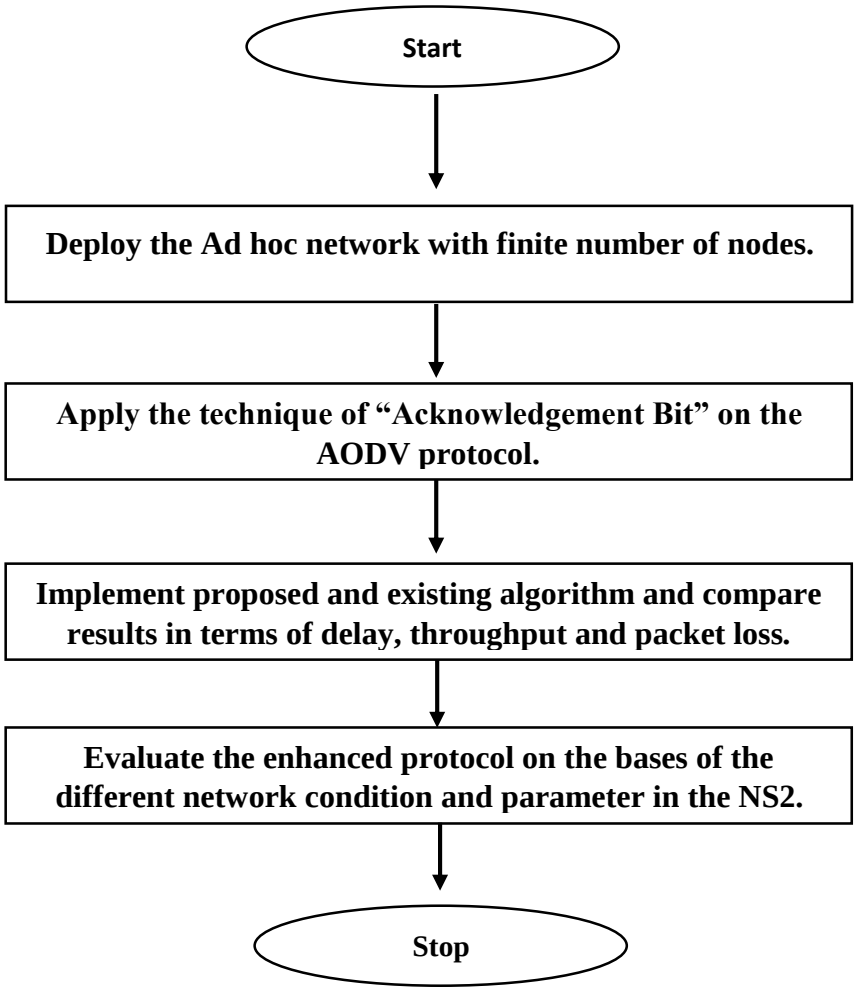


Fig. 5.2 “Acknowledgement bit” with Malicious node.

Step 1: Consider the first scenario, in that node S wants to send the data to the node R. while route discovery process, first node S Broadcast the RREQ to their neighbours node, in our case node A get the RREQ, if it has the route to the R it will reply with RREP otherwise forward the RREQ to the other intermediate nodes. And send one Acknowledgement packet to the origin node. In the ACK packet we will propose the one-bit field named “ACK_Bit” which is contain one bit 0 or 1 where 0 represent malicious node and 1 represent opposite of it.

Step 2: Whenever the intermediate node sends back the ACK to the its previous node it makes the ACK_Bit to 1, if the and the previous node checks the ACK_Bit fist and pass this ACK to the Sender. If that node is in case of malicious node it will be not understand the ACK_Bit and by default it is set to 0. So, the malicious node passes that ACK to the previous node it will be identified as the malicious node.

Step 3: After the detecting the malicious node, put it in the routing table under the malicious node and remove it from all communication from the network.



CHAPTER 6

EXPECTED OUTCOME

It has been concluded that the enhanced protocol will be work in very efficient manner, which will be beneficial for the MANETs communication network. Also we hope to implement this mythology in various protocol for the further research and development also for the better performance.

REFERENCES

[1] Mehran Abolhasan, Tadeusz Wysocki and Eryk Dutkiewicz "*A review of routing protocols for mobile ad hoc networks*" in Ad Hoc Networks, 2 (1), 2004, 1-22.

[2] S. Mohapatra and P.Kanungo "*Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator*," in International Conference on Communication Technology and System Design 2011.

[3] Xianji Jin, Jianquan Liang, Weiming Tong, Lei Lu, Zhongwei Li, "*Multi-agent trust-based intrusion detection scheme for wireless sensor networks*," 2015.

[4] Kapang Lego, Pranav Kumar Singh, Dipankar Sutradhar, "*Comparative Study of Adhoc Routing Protocol AODV, DSR and DSDV in Mobile Adhoc NETwork*," in Indian Journal of Computer Science and Engineering Vol. 1 No. 4 364-371

[5] Md Raqibull Hasan, Yanxiao Zhao, Guodong Wang, Yu Luo and Rob Winter, "*Enhanced AODV: Detection and Avoidance of Black Hole Attack in Smart Meter Network*," IEEE 2017.

[6] Kavneet Kauri and Sandeep Kad, "*Enhanced Clustering based AODV-R Protocol using Ant Colony Optimization in VANETS*" in 1st IEEE International Conference on Power Electronics. Intelligent Control and Energy Systems (ICPEICES-2016)

[7] Mohammed Aashkaar and Purushottam Sharma " *Enhanced Energy Efficient AODV Routing Protocol for MANET*" in International Conference on Research Advances in Integrated Navigation Systems (RAINS - 2016), May 06-07, 2016, R. L. Jalappa Institute of Technology, Doddaballapur, Bangalore, India

[8] Beijar Nicklas "Zone Routing Protocols" *Networking Laboratory. Helsinki University of Technology, Finland.*

[9] Liu, Lili Guo,Huizhu Ma,Tao Jiang, "*Energy Efficient on– demand Multipath Routing Protocol for Multi-hop Ad Hoc Networks*", IEEE 2008.

[10] Kulsekaran A. Sivakumar and Mahalingam Ramkumar, 2007, "*Safeguarding Mutable Fields in AODV Route Discovery Process*," Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th international Conference on, 13-16 Aug, IEEE.

[11] Houda Moudni, Mohamed Er-rouidi and Hicham Mouncif, Benachir El Hadadi, "*Modified AODV Routing Protocol to Improve Security and Performance against Black Hole Attack*," IEEE, 2016.

[12] Jaisankar, N., Saravanan, R., & Swamy, K. D. (2010) "*A novel security approach for detecting black hole attack in MANET*," In Information Processing and Management (pp. 217-223). Springer Berlin Heidelberg

[13] Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012, January). "*A novel approach for grayhole and blackhole attacks in mobile ad hoc networks*," In Advanced Computing

& Communication Technologies (ACCT), 2012 Second International Conference on (pp. 556-560). IEEE.

[14] Ghathwan, K. I., & Yaakub, A. R. B. (2014). "*An Artificial Intelligence Technique for Prevent Black Hole Attacks in MANET*," In Recent Advances on Soft Computing and Data Mining (pp. 121-131). Springer International Publishing.

[15] Ahmad, S. J., Reddy, V. S. K., Damodaram, A., & Krishna, P. R. (2015, January). "*Detection of Black Hole Attack Using Code Division Security Method*," In Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2 (pp. 307-314). Springer International Publishing.

[16] Debarati Roy Choudhurya, Dr. Leena Raghab, Prof. Nilesh Marathe.b, "Implementing and improving the performance of AODV by receive reply method and securing it from Black hole attack," International Conference on Advanced Computing Technologies and Applications (ICACTA2015)

[17] Ali Dorri and Seyed Reza Kamel and Esmail kheyrkhah, "*SECURITY CHALLENGES IN MOBILE AD HOC NETWORKS: A SURVEY,* " International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015

[18] Vimal Kumar and Rakesh Kumar, "*An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network,*" International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014)

[19] Ehsan Amiria, Hassan Keshavarzb, Hossein Heidaric, Esmaeil Mohamadid, Hossein Moradzadehe, "*Intrusion Detection Systems in MANET: A Review*," International Conference on Innovation, Management and Technology Research, Malaysia, 22 – 23 September, 2013

[20] Yuvraj Singh and Sanjay Kumar Jena, "*Intrusion Detection System for Detecting Malicious Nodes in Mobile Ad Hoc Networks*" D. Nagamalai, E. Renault, and M. Dhanushkodi (Eds.): PDCTA 2011, CCIS 203, pp. 410–419, 2011. c Springer-Verlag Berlin Heidelberg 2011

[21] J.Manoranjini, A.Chandrasekar, D.Rajinigirinath " *Hybrid Detector for Detection of Black Holes in Manets*" 2013 International Conference on Electronic Engineering and Computer Science.

[22] Adnan Nadeem and Michael P. Howarth, "An Intrusion detction & adaptive response Mechanism for MANETs" in Ad Hoc Networks 2013

[23] Ahmed M. Abdalla, Imane A. Saroit, Amira Kotb, Ali H. Afsaric, "Misbehavior Nodes Detection and Isolation for MANETs OLSR Protocol," World Conference on Information Technology 2011

[24] Muhammad Imran, Farrukh Aslam Khan, Tauseef Jamal, Muhammad Hanif Durad, "Analysis of Detection Features for Wormhole Attacks in MANETs," International Workshop on Cyber Security and Digital Investigation (CSDI 2015) .