IM-AODV: An Improved Protocol to Mitigate Blackhole Attack

Anishma Talwar , Dr. Naveen Hemrajani

Abstract : Blackhole attack is one of the most severe networking attack in a Mobile Ad Hoc network in which the blackhole node, impersonates itself as a valid destination for the data packets and then swallows the data traffic just like the blackhole in universe where all the matter disappears. Many studies have been done on detection, prevention and mitigation of blackhole attacks in MANET. Mobile Ad Hoc networks become vulnerable to such type of attacks due to their inherent characteristics such as wireless medium, no boundaries, altering topology, lack of central monitoring, no clear defense mechanism and so on. In this paper we have proposed a more robust and an improved routing protocol which we have named as IM-AODV(Improved Ad Hoc Distance Vector Routing Protocol). As AODV(Ad Hoc On Demand Distance Vector) protocol is the most researched routing protocol in MANET so our proposed protocol is concentrated on solutions dealing with AODV .

Keywords : AODV, Blackhole, IM-AODV, MANET

1 INTRODUCTION

A mobile ad-hoc network (MANET) is a collection of wireless mobile nodes. Ad hoc is a Latin word meaning "no fixed -establishment network" or "self-organize network". Similarly in Mobile Ad hoc network the nodes function as router as well as a host computer and interact dynamically to form a temporary network without the aid of any existing infrastructure. Such type of wireless and dynamic networks are becoming popular day by day due to increasing need of mobile communication MANET has received a great deal of attention due to its inherent special characteristics like dynamic topology, decentralize administration, expandability , minimal configuration and lack of infrastructure. However the same characteristics pose a great deal of threat to the security of mobile networks.

Blackhole attack is one of the most severe attacks in MANET. In blackhole attack , one or more mobile nodes come under the influence of attack and start behaving maliciously[1][2]. The malicious node impersonates itself as a valid destination node and thus disrupts the data communication between source and destination node by attracting data traffic towards itself and swallowing the packets that reach its interface. The blackhole node behaves similar to the blackhole in universe where all the matter disappears.

Security in MANET is a challenging task as the mobile networks are exposed to various kinds of attacks and moreover conventional defense mechanisms against these attacks are not suitable[3][4][5]. Due to its unique infrastructure, it creates a number of consequential challenges to the security design. There is a need to make a decent tradeoff between security and performance.

- *Anishma Talwar is currently pursuing M.Tech. (Computer Science Engineering) from JECRC University,Jaipur., India.PH: 93109020230 Email: talwaranishma@gmail.com*
- *Professor Dr Naveen Hemrajani is currently working as HOD in Computer Science Department in JECRC university, Jaipur India.PH-9829032657 E-mail: hod.cse@jecrcu.edu.in@jecrcu.edu.in*

Many researchers have studied the mobile ad hoc network to make it more secure and robust against attacks[6][7][8][9][10]. In this piece of work we have proposed a new version of AODV protocol which detects blackhole without compromising on data communication between nodes and thus IM-AODV makes MANET a more stable and stronger network.

Many techniques have been proposed to avoid, detect, prevent and mitigate the blackhole attack in Manet. MANET is vulnerable to various attacks. This paper mainly focused on the black hole attack in MANET. Going through various researches done in the field of detection, prevention and mitigation of blackhole attack, it is revealed that most of the work done in the field of securing Ad Hoc Networks deals with securing the routing mechanism and analyzing the changes in various network prameters in presence of an attacking node[10][11][12]. As blackhole attack is a serious problem in MANET, lot of research studies have been dedicatedly focused on detecting blackhole node and analyzing the after effects of such a malicious node through simulation. Many researchers have proposed an advancement in routing protocols to counter the attack by removing the loopholes associated with routing protocols[12][13][14][15]. AODV protocol is the most researched protocol in the field of secure routing in MANET.

2 Proposed Solution

The proposed solution in this paper also deals with AODV. The paper proposes a more efficient and improved version of AODV named as IM-AODV. More than detection , IM-AODV is focused on unhindered data communication between source and destination node. Hence the protocol attempts a tradeoff between security and performance. This paper focuses on recognising the path having blackhole node and selecting a safe path to mitigate the effect of blackhole node. Some improvements have been made in AODV protocol. The enhanced AODV i.e IM-AODV incorporates position and Euclidean distance parameters of source and destination for data communication to take place. Consider two random points X1 and X2 located in a square area of size L × L with coordinates (x1, y1) and (x2, y2), respectively. If d is the euclidean distance between X1 and X2, then d is given by :

$$d = (x1 - x2)2 + (y1 - y2)2$$

The new protocol works on assumption that data communication between two random nodes would only materialize if the Euclidean distance between the two nodes falls within requisite distance range, else data transfer will not be initiated. [15][16]

In conventional AODV if a blackhole node is detected, pakets drop at the malicious node which completely disrupts the data communication in the mobile ad hoc network. On the other hand in case of IM-AODV, data communication continues with very little packet dropping in the presence of blackhole node. These improvements make the protocol robust against black hole attack . The performance of proposed approach has been investigated using NS2 SIMULATOR.[17][18]

3 Validation

In this section, the proposed approach is validated by comparing the theoretical and simulation results. We first validate the theoretical analysis of the IM-AODV by network simulation. For this validation, Ubuntu 11 is used as the operating system because it is user friendly which makes it easy to manage. Network Simulation 2 (NS2.35) is used as simulation software which runs smoothly over Ubuntu 11 to analyze and manage the mobility scenarios for ad hoc networks. We consider a simulation scenario consists of mobile nodes . A set of 50 nodes are arranged in two cluster formations. We assume that nodes communicate either within cluster or from one

cluster to another cluster. The two clusters communicate via head nodes in each cluster. Every node moves towards the destination point with a velocity chosen uniformly from 0 to maximum speed (V max). When it reaches the destination it chooses and moves towards a new destination in a similar manner. The maximum moving speed is set to 20 m/s. A zero pause time was chosen to make the nodes move all the time. All nodes have a radio range of 250m.

For each mobility scenario, the expected distance between any source-destination pair is computed by using Euclidean distance algorithm. A node in the improved AODV protocol is assigned position , distance and velocity parameters. Many different mobility scenarios (with different random seeds) are generated until the expected distance between nodes is within a threshold value . In the new protocol more importance is given in continuance of data transfer from source and destination then on detecting blackhole node and isolating it. The data transfer continues and the packet drop rate is analysed to identify malicious nodes unlike in conventional AODV where data packets abruptly drop on detection of blackhole attack. Figure 6 shows simulation and analysis results for the proposed approach. The comparison between simulation results of AODV and IM-AODV shows the accuracy of the proposed analysis.

The proposed work is implemented for the proposed routing protocol IMAODV. In the proposed work, black hole attack is implemented in AODV and IMAODV. Finally comparison will be made for black hole attack on the basis of various problem formed after the implementation. Moreover, the comparison will be done on the basis of requisite parameters like Throughput and packet delivery ratio.[19]

The simulations were performed using Network Simulator (Ns-2), which is popularly used for ad hoc networking community. The routing protocols were compared based on the following two performance metrics:

Packet Delivery Ratio (PDR): Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. Mathematically, it can be defined as:

$$PDR = S1 \div S2$$

Where, S1 is the sum of data packets received by the each destination and S2 is the sum of data packets generated by the each source.

Throughput: Throughput or network throughput is the rate of successful message delivery over a communication channel. In this context it is defined as the total number of packets delivered over the total simulation time. Mathematically, it can be defined as:

Throughput= N/1000

Where N is the number of bits received successfully by all destinations.

4 Implementation Of Proposed Routing Protocol

For implementing our proposed routing protocol IM-AODV we have made certain changes in the ns2 environment some of them are:

a) Since, the protocol should be improved of AODV so we have to use directory as same as AODV directories and follow certain rules of AODV routing protocol. Furthermore, we also implement position determination and Euclidean distance algorithm in which the broadcasting between nodes will be done for proposed routing protocol only when they are in distinct range otherwise the packet discards.

b) Add a new directory named as IM-AODV

c) Changes should be made in make file to declare and generate object files.

d) We have to define packet format for the requisite name of the proposed routing protocol in the packet.h file.

e) We have to declare agent in agent.tcl file, declare nodes and mobile nodes in mobilenode.tcl and packet for communication, send, receive and drop packets inpacket.tcl

f) For generation trace we have to make changes in cmutrace.cc and cmutrace.h files

g) Some additional changes also done to improve the features of the proposed routing protocol like define position and implement proposed Euclidean distance algorithm.

h) Then compile the ns2 to perform all the requisite function

5 Implementation of Black hole attack

Now, we have our proposed routing protocol IMAODV and as the work is highly based over black hole attack. Then for this, implementation of black hole attack is carried out in both routing protocol which could be clearly seen through our proposed scenario. When the attack keywords introduce the node behave as blackhole and there will be no transmission of data which is further included with packet drops. In Fig 4, the snapshot depicts blackhole attack in AODV protocol and fig 5 depicts continuous data transfer even in presence of blackhole node in IM-AODV protocol.

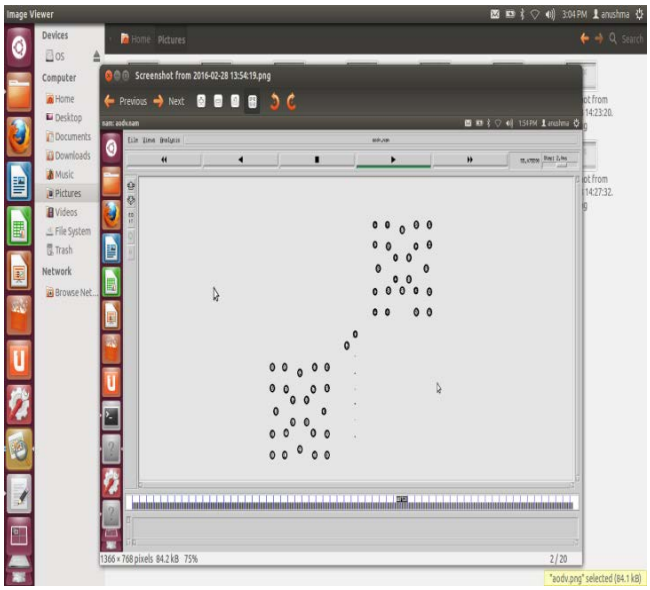

Fig 4: Blackhole in AODV

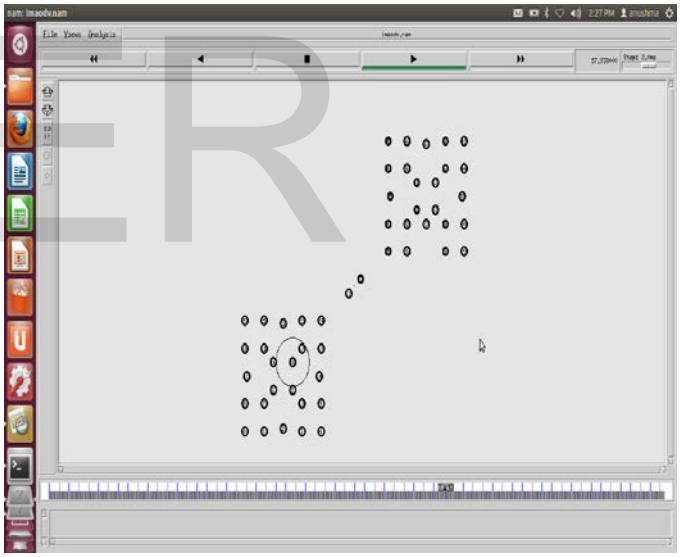

Fig 5: Blackhole in IMAODV

6 Mobile Ad Hoc Network Implementation

The simulation is carried out using the Network simulator(version 2.35),which simulates the events such as sending, receiving, dropping, forwarding, etc. The wireless channel is used as the mobile nodes deployed, communicate wirelessly with each other. The propagation models are used to compute the received power. When a packet is received, the propagation model

determines the attenuation between transmitter and receiver and computes the received signal strength. The two-Ray ground Radio propagation model is used. An omni-directional antenna is employed for carrying out the transmissions which can transmit signal over a 360 degree angle. Omni-directional wireless mobile networks are modeled such that a bidirectional link is established between neighbouring mobile nodes if they are within communication radius.The scenario is simulated for 90 seconds. The participating nodes are not stationary. The routing protocol which monitors and carries out the transmission is Improved Ad-hoc On Demand Distance Vector routing Protocol(IM-AODV).The following table gives an overview of all the simulation parameters used.

Parameter	Values
Simulator	NS-2
Simulation Duration	90 sec
Topology	2500 meter X 2500 meter
No. Of nodes	50
Traffic type	FTP (TCP)
Routing protocol	IMAODV, AODV
Channel Type	Wireless Channel
Mobility Model	Two Ray Ground Propagation Model
Network Interface Type	Wireless Phy IEEE 802.11

Table 1: Used Simulation Parameters

6.1 Algorithm

- Node i broadcast the neighbor discovery packet and collect neighbor node's echo message.
- Introduce the requisite functions and arguments and attach it to sequence number, labels, and IM-AODV proposed routing protocol.
- Implementation of proposed IM-AODV which is further improved by position aware and Euclidean distance algorithm.
- Proposed algorithm clearly identifies that the communication between appropriate nodes will done only when the nodes are between particular range of distance. That's why there is first need to identify the position of nodes and after that a proper analysing of black hole attack.
- Result analysis to distinguish the effect of black hole attack in AODV and IM-AODV.
- Result analysis and comparison for the desired parameters like PDR, throughput etc.

The graphs obtained using simulation further help in analyzing the robustness of IM-AODV.

Fig 6: PDR Vs Simulation Time in AODV Protocol

In fig 6, the xgraph is plotted with packet delivery ratio on Y axis and simulation time(ms) on X axis with AODV routing protocol. At 0th second, when the simulation starts, PDR is 100 % i.e all the packets sent by source reach the destination. In conventional AODV , 99.38% PDR is obtained [11]. In presence of blackhole node, AODV performance drops drastically as packets are dropped at the malicious node. The above graph testifies

the effect on PDR at 15th and 43rd time interval when PDR drops significantly as the malicious node attacks on 15th and 43rd time interval.

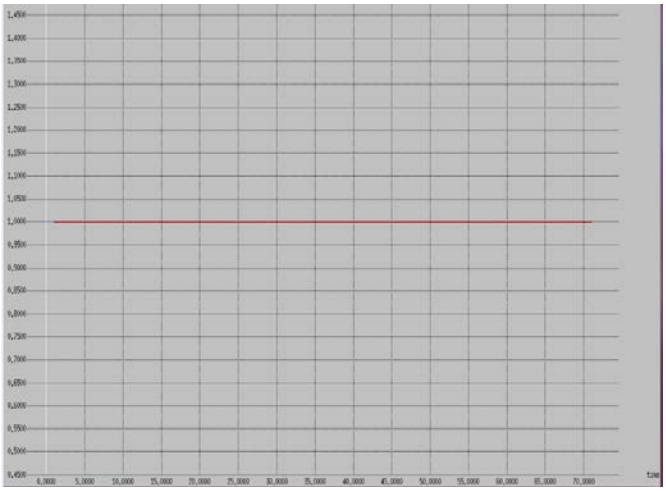

Fig 7: PDR Vs Simulation Time in IM-AODV Protocol

In fig 7, the xgraph is plotted with packet delivery ratio on Y axis and simulation time(ms) on X axis with IM-AODV routing protocol. The proposed protocol is an improved version of AODV protocol. It counters the effect of blackhole node. Hence data communication between source and destination is maintained uninterrupted with minimal loss of packets when blackhole node becomes active at 15th and 43rd time interval. The graph testifies no loss of packets even in presence of attack.

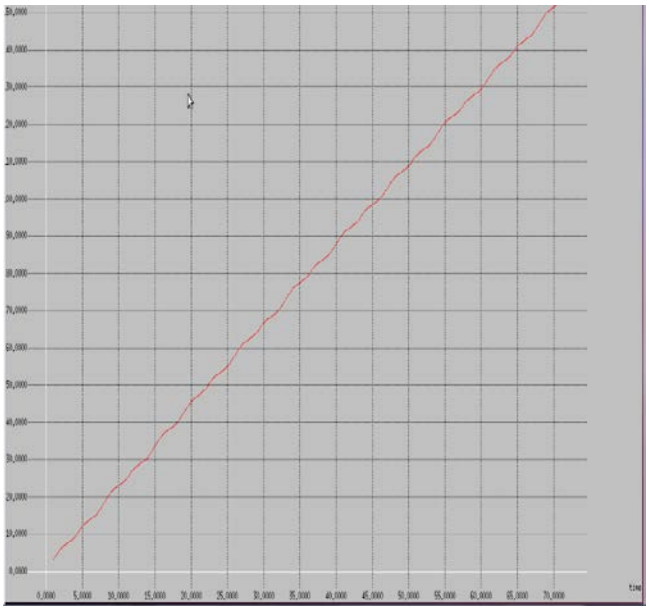

Fig 8: AODV Throughput Vs Time

The fig 8 illustrates a xgraph with simulation time(ms) on x axis and average throughput (kbps) on y axis. Throughput in case of network with no attack increases with time whereas in case of black hole attacked network the throughput become constant when the malicious node comes into action in the network.

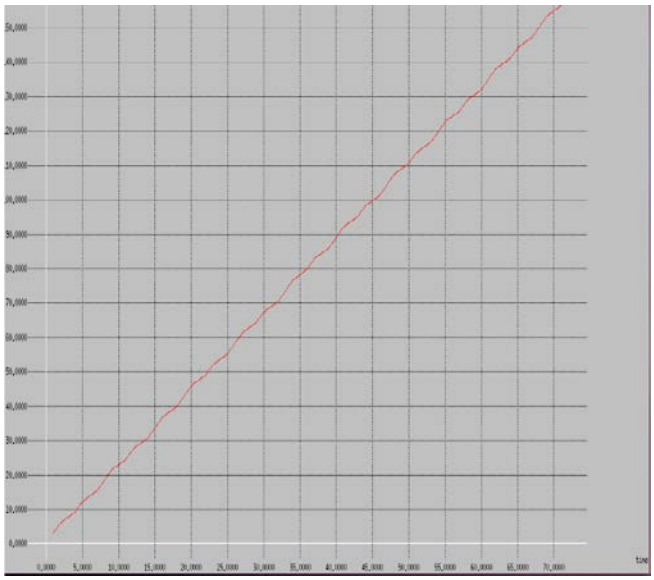

Fig 9: IMAODV Throughput Vs Time

In fig 9, xgraph with simulation time(ms) on x axis and average throughput (kbps) on y axis shows better performance than conventional AODV. The difference is very minute in the above case as we have used small number of nodes. Throughput is is the average rate of successful message delivery over a communication channel which remains unhindered in case of IM-AODV. This signifies the effectiveness of our proposed protocol. Further the charts shown in figures 10 and 11 illustrate the effectiveness of IM-AODV over AODV.

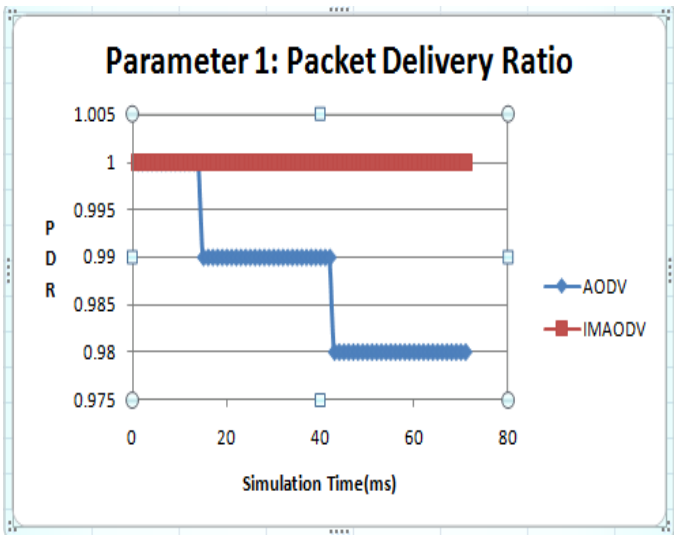

Fig:10 Comparison of AODV & IM-AODV in PDR

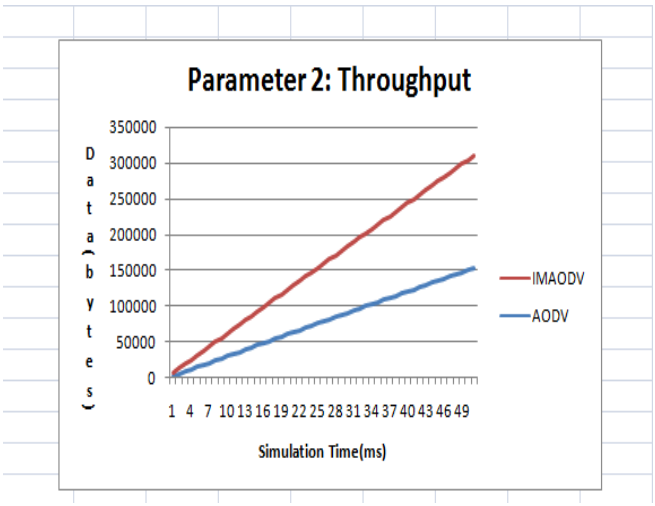

Fig11:Comparison of AODV & IM-AODV in Throughput

7 Conclusion

In mobile ad hoc networks, the attacks always degrade the service of the entire network. Blackhole attack is one of the most vulnerable attacks in MANET. We have proposed an enhancement of the conventional AODV protocol to detect and mitigate the effect of blackhole node. Most of the solutions dealing with securing MANET concentrate on detecting the malicious node and isolating it from the network. But the proposed routing protocol is concerned more on continuous data transmission even in presence of blackhole node. This paper has worked on simulations to justify the effectiveness of the new protocol using two important parameters like packet delivery ratio and throughput. In the future , the work can be extended to cover more parameters . The protocol could be extended for more number of nodes to understand real life robustness.

8 Acknowledgments

A sense of satisfaction overcomes me with the termination of my dissertation, more so I feel a sense of gratitude towards all my mentors, friends and family whom I wish to thank. I express my deepest heartfelt gratitude and humbleness with utmost sincerity to my teacher and my guide, Dr. Naveen Hemrajani ,Professor

and Head, Department of Computer Science & Engineering, JECRC University, Jaipur, for his sagacious guidance and encouragement throughout my course work.

REFERENCES

[1] A Review - Prevention and Detection of Black Hole Attack in AODV based on MANET: Bhoomika Patel & Khushboo Trivedi

[2] Advanced Topics in Wireless Networks : Dr. Baruch Awerbuch & Dr. Amitabh Mishra

[3] Security Challenges In Mobile Ad Hoc Networks: A Survey: Ali Dorri , Seyed Reza Kamel & Esmail kheyrkhah

[4] Security Threats in Mobile Ad Hoc Networks: Sevil Şen, John A. Clark, Juan E. Tapiador

[5] Security Issues in Mobile Ad Hoc Networks - A Survey: Wenjia Li and Anupam Joshi

[6] Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol :Mehdi Medadian & Khossro Fardad

[7] Detection Prevention and Mitigation of Black Hole Attack for MANET : Mehak Kaushal & Mr. Gunjan Gandhi

[8] Mitigating Scheme for Black Hole Attack in AODV Routing Protocol : Ei Ei Khin & Thandar Phyu

[9] Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method: Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto

[10] DPRAODV: A DYANAMIC LEARNING SYSTEM AGAINST BLACKHOLE ATTACK IN AODV BASED MANET : Payal N. Raj, Prashant B. Swadas

[11] Modified AODV Routing Protocol to Detect the Black Hole Attack in MANET: Ali Abdul Rahman Mahmood, Dr. Taha Mohammed Hasan, Dhiyab Salman Ibrahim

[12] An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network: Vimal Kumar a , Rakesh Kumar

[13] Detection and Prevention Of Black Hole Using Clustering In MANET Using Ns2:Gurnam Singh, Gursewak Singh

[14] An enhanced AODV routing protocol for MANETs
Ashraf Abu-Ein, Jihad Nader

[15] A Location Based Approach to Prevent Wormhole Attack in Wireless Sensor Networks : Nishant Sharma Upinderpal Singh

[16] WORMHOLE DETECTION METHODS IN MANET:
Ankita Gupta Sanjay Prakash Ranga

[17] NS Simulators for Beginners: Lecture Notes, University of France

[18] SIMULATION STUDY OF BLACKHOLE ATTACK
IN THE MOBILE AD HOC NETWORKS: Sheenu Sharma, Roopam Gupta

[19] Effects of Traffic Load and Mobility on AODV, DSR and DSDV Routing Protocols in MANET : Viral Parekh & K. H. Wandra.

.