MAODV: To Identify a Secure Route Selection in MANET under Blackhole

Sumer Singh
M-Tech Scholar, S.B.S State Technical Campus, Ferozepur, Punjab

Chakshu Goel
Asst. Professor, S.B.S State technical CampusFerozepur, Punjab

Gurjeevan Singh
HOD-ECE Poly-wing, S.B.S State Technical CampusFerozepur, Punjab

ABSTRACT
Mobile Ad-hoc Network (MANET) is an open loop infrastructure, having independent movement of each node without any decentralized control. Due to dynamic nature. MANET has a many security issues than conventional networks. In this paper Ad- Hoc on Demand Distance Vector (AODV) is used as a routing protocol in MANET. Many types of attack are introduced in MANET such as blackhole attack, wormhole attack,routing table overflow attack, routing cache poisoning attack etc.,which occur due to the malicious node and degrade the achievement of AODV. In this paper, blackhole attack is taken into consideration which is more dangerous than other attacks. To maintain a secure route selection under blackhole attack, it is necessary to make a strong security proposal, which maintain the performance of network. This paper introduces a new security scheme which deals with MAODV (Modified Ad- Hoc on Demand Distance Vector) which enlarges the performance of network and eliminates the risk of blackhole attack in the presence of malicious node.

Keywords
MANET, AODV, MAODV, Malicious node, Security, Blackhole attack.

1. INTRODUCTION
At present, wireless technology has become the most exciting in everybody life. To make mobility of users wireless networks play an important role. There are many way to communicate wirelessly which provide communication means over large areas such as MANET, MESH network, WWAN, Bluetooth, etc, which provide communication for short distance but if we want to communicate short as well as long distance we use a network called MANET [1] [5]. MANET is a collection of self-governing nodes that communicate with each other by forming a multi-hop network and maintaining connectivity in a decentralized manner So, MANET is decentralized, self organizing networks which make a point to point communication in between source and destination from a suitable route in the presence of any one routing protocol like AODV, GRP(Gathering based routing protocol), DSR (Dynamic Source Routing), OLSR (Optimized Link State Routing), TORA etc . At present trend the MANET become one of the most important wireless communication mechanisms among all other [1] [2] [5] [7] [12] [14] [19] [24]. Unlike traditional network, MANET does not have any fixed infrastructure. Each individual node behaves receiver as well as transmitter in network without any access point, as shown in fig1[9] [11] [13].

1.1 Applications of Mobile Ad Hoc Networks

The following are some well-known applications of MANE [8] [17] [6].

- **Military:** Automated battlefield, Special operations, Homeland defence.
- **Civilian:** Disaster Recovery (flood, fire, earthquakes etc), Law enforcement (crowd control), Search and rescue in remote areas, Environment monitoring(sensors), Space/planet exploration.
- **Commercial:** Sport events, festivals, conventions, Patient monitoring, Ad hoc collaborative computing, Bluetooth, Sensors on cars (car navigation safety).

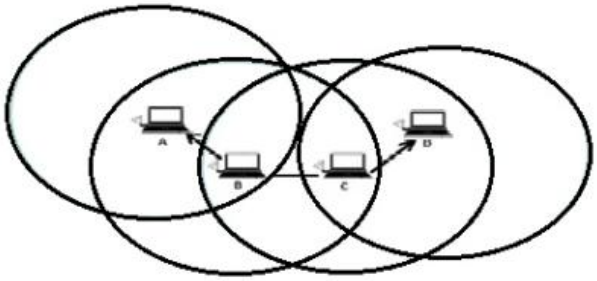

Figure 1: Mobile Ad-hoc Network

Whenever a communication is established between source and destination then destination node should be lie in between the radio range of the source node which wants to initiate the communication, the autonomous and intermediate nodes within the network act like a router as well as host at the same time, which serves the packets from source node to destination node, with the help of routing protocol. These networks are fully self organized, decentralized having smart antennasand capability to work anywhere without any infrastructure.Due to the distributed nature, openness in network topology and absence of centralized administration in the management, MANETs often suffer from many attacks by malicious nodes, these attacks occur due to internal and external attacker in network. Routing protocols, data, battery power and bandwidth are the common targets of these attacks [3] [25] [7] [11].

External attackers arise in network from the outside boundaries of network and attempt to interrupt the network by injecting invalid routing information. They create routing loops or other non-functional routes and try to partition the

network by creating a wormhole. External attackers may also replay old routing information or modify route information being transmitted between nodes.
Internal attackers arise due to internal activities of network, where node power is eventually down then they do not work properly that means the node have been act as amalicious nodes. They advertise false routing information in order to disturb the flow of information in the network that generate gray-hole or blackhole attacks is bring out in network. So, these attacks can degrade the performance of network[9] [7] [3].
In this paper proposal scheme is used to eliminate these attacks from MANET. Section 2 describe the routing protocol, in section 3 various type of security attack is explained, section 4 deals with proposal algorithm, in section 5 simulation setup is described, in section 6 and section 7 shows the result and conclusion.

2. ROUTING PROTOCOL

When a sender node needs to send data to a receiver node, it must first acquire a route to the receiver node[19]. So, data transfer among nodes is realized by means of multiple hops, and rather than just serving as a single terminal, every mobile node acts as a router to establish a route. When a source node intends to transfer data to a destination node, packets are transferred through the intermediate nodes, thus, searching for and quickly establishing a route from a source to a destination node is an important issue for MANETs. Routing protocol is a standard which controls how nodes decide which way to route packets between computing devices in MANET. The different protocols are proposed to deal with routing in the MANET[19] [12] [8] [14] . These routing protocols can be classified into two classes that are Reactive and Proactive. Reactive protocols are characterized by node acquire and maintain routes on demand, example is AODV. Proactive protocols are characterized by all nodes maintain routes to all destination in the network at all times example is OLSR. This paper deals with the AODV routing protocol.

- **Ad- Hoc on Demand Distance Vector**

AODV [3] is basically an improvement of the Dynamic Destination-Sequenced Distance-Vector (DSDV) routing protocol. However, AODV is a reactive routing protocol instead of being proactive. It minimizes the number of broadcasts by creating routes based on demand, which is not the case for DSDV. When any source node wants to send a packet to a destination, it broadcasts a route request (RREQ) packet. The neighbouring nodes in turn broadcast the packet to their neighbours and the process continues until the packet reaches the destination. During the process of forwarding the route request, intermediate nodes record the address of the neighbour from which the first copy of the broadcast packet is received. This record is stored in their route tables, which helps in establishing a reverse path. If additional copies of the same RREQ are later received, these packets are discarded. The reply is sent using the reverse path. For route maintenance, when a source node moves, it can reinitiate a route discovery process. If any intermediate node moves within a particular route, the neighbour of the drifted node can detect the link failure and send a link failure notification to its upstream neighbour. This process continues until the failure notification reaches the source node. Based on the received information, the source might decide to reinitiate the route discovery phase. The AODV algorithm enables dynamic, self-starting, multihop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations and does not require nodes to maintain routes to destinations that are not in active communication. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner. When links break, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link. One distinguishing feature of AODV is its use of a destination sequence number for each routing table entry. The destination sequence number is created by the destination and is included along with any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom and is simple to program. Given the choice between two routes to a destination, a requesting node is required to select the one with the greatest sequence number [14] [13] [17] [21] [18] [23] [24] [19] [1].

3. SECURITY ATTACK ON MANET

There are malicious routing attacks that that target the routing discovery phase, So MANET often suffer from many security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring management, cooperative algorithms and no clear defence mechanism. Security threats in an ad hoc network can be classified into passive and active attacks [4] [5] [14] [2]. A passive attack does not disrupt operation of a routing protocol, but only attempts to retrieve valuable information by listening to routing traffic, which makes it very difficult to detect. An active attack is an attempt to improperly modify data, gain authentication, or procure authentication by inserting false packet transition through the network. Active attacks can be further divided into two category: internal and external attacks. An external attack is caused by nodes that do not belong to the network. An internal attack is initiated from a compromised node that belongs to the network [6] [2] [16].Internal attacks are more dangerous since the misbehaviour node is a part of the selected route.

3.1 Various Type of Attacks

Below some attacks are clarified which degrade the performance of MANET [3] [2] [5] [24] [15] [17] [12] [19].

Routing table overflow attack: A malicious node advertises routes that go to non-existent node to the authorized nodes present in the network. An attacker can simply send excessive route advertisement to overflow the victim's routing table.

Routing cache poisoning attack: In route cache poisoning attacks, attackers take advantages of the promiscuous mode of routing table updating, where a node overhearing any packert may add the routing information contained in that packet header to its own route cache, even if that node is not on the path.

Blackhole attack: A black hole attack can be achieved by a single-node or by several nodes in collusion. The blackhole attack has two type first, a malicious node advertises the route with les hope count for a given destination. Once route is established via malicious node then it will drop all the data packets. Second, Once route is established via malicious node then it will drop the data packets selectively.
Wormhole attack: Routing can be disturbed when routing control messages are tunnelled. This tunnel between two colluding attackers is referred as a wormhole. proposal

4. PROPOSAL ALGORITHM

In above section 2,it has clarified the entire working of AODV. In this algorithm a new approach is illuminate which maintain a secure route under blackhole attack to fulfill the condition, i.e., MAODV routing protocol. As mention in previous section the blackhole attack occurred due to some malicious node present in network. In this paper, new scheme is used to detect and remove malicious nodes from network. This scheme initially introduces some Backbone Node (BBN) in network, just like the human backbone which carries signal to many smaller nerves in the body. Similarly, in MANET, BBN plays important role and these nodes are trustful nodes. The behavior of these nodes is special from another node, power levels and range of these nodes is excellent as compare to another. This backbone nodes contains all information related to route assign between source and destination node, i.e., Route Request message (RREQ), Route Response (RREP), destination adders, destination sequence number and hope counter, information about neighboring nodes.

BBN also deals with restricted IP address. It assigns a separate IP for each and every node in network. Whenever any new node joins the network it sends a broadcast message as a request for IP address, after receiving this message BBN assign a Restricted Internet Protocol (RIP) for each and every node in network, after this node send a acknowledgement to BBN and over all control of nodes are in the hand of BBN.

Whenever a source node communicates with destination node, it firstly determined by BBN after this route is established. Due to the blackhole attack the established route is not a secure which effect the performance of MANET.

To eliminate the effect of blackhole, in this paper, MAODV routing protocol is introduced that deals with BBN which contain the overall information about network nodes, i.e., routing table, destination IP address distinction, hope count, next hope etc.

When source node send a RREQ message in network then many nodes send a acknowledgement of RREP then BBN just check the shortest path for communication and make a route from source to destination. In this case, some time malicious node also be a part of communication route which introduce the blackhole attack, it means the entire valuable data packet will be dropped. To avoid the effect of malicious nodes, assign a specific threshold or sufficient time to send a acknowledgement to source node for RREP. If more delay is generated from specific threshold level it means here some doubt occur therefore to satisfaction for secure route BBN send some dummy data packet to that node if the given packet is discard or dropped more than normal packet drop it means that node behave like a malicious node, the all information regarding this node is store in BBN routing table, BBN mark this node as a fake node and neglected the overall communication from this node.

So, in MAODV this malicious node is not a part of MANET which helps to illuminate the effect of blackhoke attack and maintain a secure route in between the source and destination.

The communication is done in between three main phase i.e.

- RREQ(Route Request) Message

Whenever source node wants to communicate with destination node then it needs a sufficient route in between the source and destination for this purpose it broadcast the RREQ message. As shown in table 1:

Table 1 Formats of RREQ

Type	**Flag**	**Reserved**	**Hop Count**
RREQ (Broadcast)IP			
Destination IP address			
Destination Sequence Number			
Source Sequence Number			

- RREP(Route Response) Message

Table 2 shows the RREQ format

Table 2Formats of RREP

Type	**A**	**Reserved**	**Hop Count**
Destination IP address			
Destination Sequence Number			
Source IP Address			
Source Sequence Number			

- BBN (Back Bone Node) or Routing table

Table 3 Shows the BBN and information about routing table

Table 3Formats of Back Bone Node or Routing Table

Destination IP address
Destination Sequence Number
Source IP Address
Source Sequence Number
Hope Counter
Threshold Time
High Power Levels
High Communication Range

4.1 Performance of MAODV

Steps for source and destination node in between the routing path:

- When a Source Node wants to communication it sends a RRIP (Request to Restricted Internet Protocol) to BBN.
- After receiving the RRIP it sends a RREQ for destination and wait for RREP.
- Before transmitting of data packet entry is build into routing table for the node that forward the RREQ.
- If destination node or intermediate node has a enough route to communication, it replies to RREP.
- After receiving a RREP it again build a information on routing table and send acknowledgement to send data packets
- But if any instant RREP from any node exceed the limit of Threshold Level then BBN send a dummy packet to that node, if the packet dropped rate is above the normal data drop it means that node is malicious node and BBN assign this node as a fake node.
- After assigning the fake node the effect of blackhole is discard and secure route is maintain in between the source and destination node.

5. Simulation Setup

In simulation model, NS 2.35 Network Simulator is used. NS is an event driven network simulator program, developed at the University of California Berkley, which includes many network objects such as protocols, applications and traffic source behavior. The NS is a part of software of the VINT project that is supported by DARPA since1995. In our work, we have evaluated the effects of Blackhole attacks in MANET at scenario 1 With Blackhole AODV and then make another scenario which clarify our algorithm called Modified AODV (MAODV). To achieve this we use a NS Network Simulator program.

Table 4 Parameters defined for simulation

Parameters	Values
Simulation Area	800m x 80m
Simulation Time	10 sec
Application	UDP
Packet Size	512 bytes
Network density	6 nodes
Routing Protocol	AODV
Number of Malicious Nodes	1
Mobility Model	Random Waypoint
Node Transmission Power	0.1
Operation Mode	802.11g
Total No of Scenario	2
Data rate	1 Mb/s
Speed of nodes in network	11 m/s
Network scale	Office
Addressing Mode	IPV4

In simulation results, six numbers of nodes are considered in evaluation process. Firstly in the starting of simulation every node is working in cooperation with each other to keep the network in communication as with further proceed, there are situations in between where emergence of malicious node that produce the effect of blackhole attack. Therefore network results shows degrade the packet delivery ratio later on in the simulation process. In second simulation scenario, the given malicious node is assign as a fake node by BBN which help us to eliminate the effect of blackhole attack and maintain the packet delivery ratio.
Given Screen shots shows the performance of MAODV which shows the communication in between source node 0 and destination node 4.

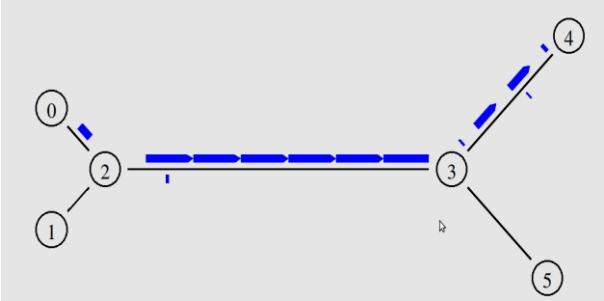

Figure 2: Secure Route in between the soured node 0 to destination node 4

Figure 3 shows the creation of dummy packet (in red line) with the help of BBN and send this dummy packet to node which wants to RRIP for communication.

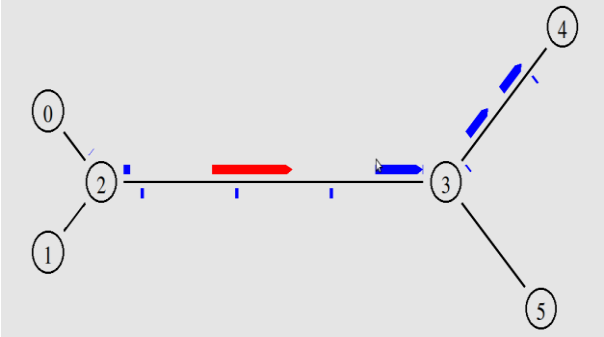

Figure3: Concept of dummy packet

Figure 4 shows the malicious node (node 5) because this node exceed the threshold level and drop all the data packet therefore BBN assign this node as a fake or Malicious node, further no useful data is send to this node.

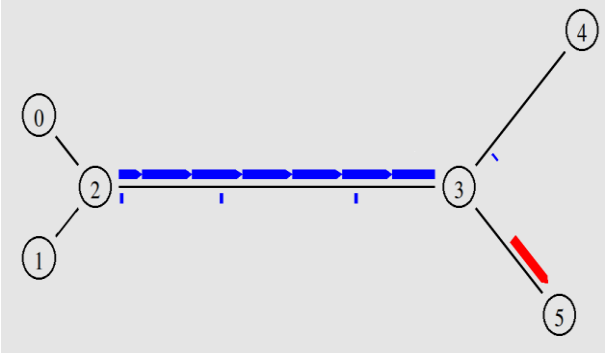

Figure 4: Concept of Malicious node

6. RESULTS

Simulation results has obtained in the presence of two scenario, first scenario deals with presence of malicious node in MANET which generate the effect of blackhole attack at output.

In second scenario, implement algorithm in which MAODV is used that neglect the blackhole attack from MANET and maintain the output.

To show the result of above two scenarios the following system metrics were chosen to evaluate the impact on MANET performance:

- **Total Packet Received**

These metrics shows the total number of Packet Received at output in the case of blackhole attack with AODV and without blackhole attack or MAODV. If malicious node is occurred in network then packet received is decreased in the case of MAODV and output maintain as input.

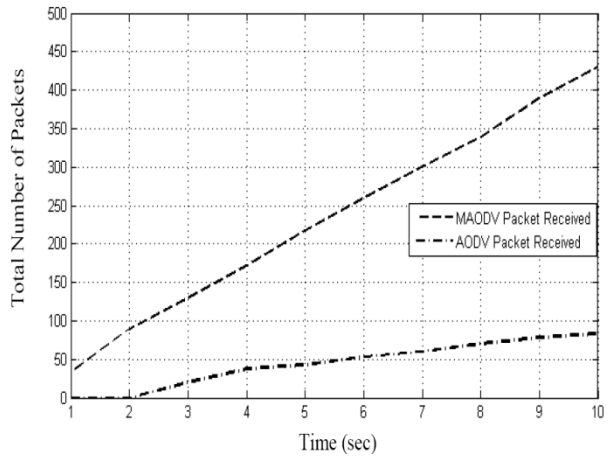

Figure 5: Total Number of Packet Received

In figure 5 the total number of packet received is shown at destination point, here the output of two scenarios is shown in MAODV the number of packet received is excellent as compare to AODV with blackhole scenario. The numeric value is evaluated in Table 4.

- **Total Packet Dropped**

The metrics shows that the total number of packet dropped in the network. Data dropped is increases by increasing the malicious nodes in network, as a result of consistently failing of data packets. Result shows the output of both with and without (MAODV) blakhole attack.

Figure 6 shows the packet drop in MANET, it clarify that there is less number of packet drope is occure in MAODV as compare ti AODV with blackhole attack. the numeric value is further evaluated in Table 5.

Table 4: Packet Received in MAODV and AODV with Blackhole attack

Time	Total No. of Packet Received	
	MAODV	AODV with Blackhole Attack
.5	0	0
1	33	0
2	90	0
3	130	20
4	172	38
5	218	43
6	259	53
7	300	60
8	340	70
9	390	78
10	430	83

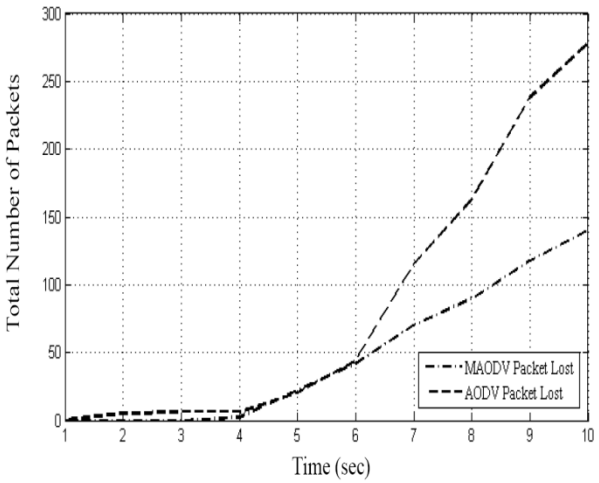

Figure 6: Total Number of Packet Dropped

- **Packet Delivery Ratio**

Packet delivery ratio shows the ratio of packet received and packet sent in between the source and destination point. If malicious node is introduce in network then PDR will be decreased, according to our algorithm the effect of blackhole attack is neglected.

PDR shown in figure 7 here MAODV perform very well as compare to AODV with blackhole attack the numeric value is introduce in Table 6

Table 5: Packet Dropped in MAODV and AODV with Blackhole attack

Time	Total No. of Packet Dropped	
	MAODV	AODV with Blackhole Attack
0	0	0
1	0	0
2	0	5
3	0	6
4	2	6
5	22	20
6	42	44
7	70	115
8	90	163
9	118	238
10	140	278

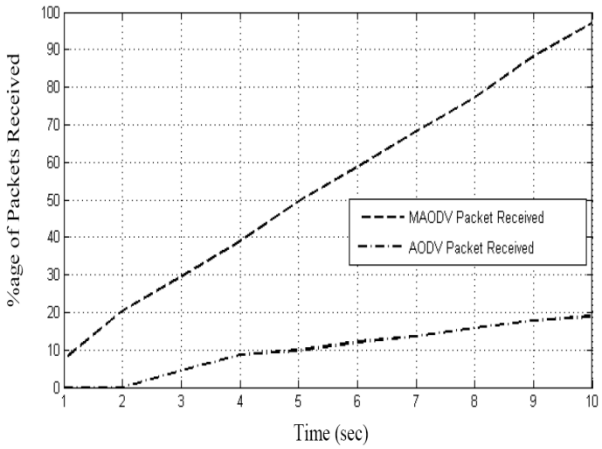

Figure 7: Packet Delivery Ratio

7. CONCLUSION

The paper introduce the effect of blackhole attack in MANET in the present of AODV routing protocol, which indicate that in the occurrence of blackhole attack useful data packet is dropped which shows the negative response to overall performance of MANET. To neglect this blackhole attack new algorithm is introduced which deals with MAODV. MAODV sort out the malicious node very carefully from network and maintain a secure route for communication or preserve the performance of MANET.

Table 6: Packet Delivery Ratio in MAODV and AODV with Blackhole attack

Time	Packet Delivery Ratio	
	MAODV	AODV with Blackhole Attack
0	0	0
1	7.5	0
2	20.45	0
3	29.54	4.54
4	39.09	8.63
5	49.54	9.77
6	58.86	12.04
7	68.18	13.63
8	77.27	15.90
9	88.25	17.72
10	97.15	18.86

8. REFERENCES

[1] A. Babakhouya, Y. Challal, and A. Bouabdallah, \A simulation analysis of routingmisbehaviour in mobile ad hoc networks," pp. 592{597, 2008.Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[2] S. Khan, N. Alrajeh, and K. Loo, \Secure route selection in wireless meshnetworks," Computer Networks: The International Journal of Computer andTelecommunications Networking, vol. 56, no. 2, pp. 491{503, 2012.

[3] I. Raza and S. Hussain, \Identi_cation of malicious nodes in an aodv pure ad hocnetwork through guard nodes," Computer Communications, vol. 31, no. 9, pp. 1796{1802, 2008.

[4] K. Vats, M. Sachdeva, K. Saluja, and A. Rathee, \Simulation and performanceanalysis of olsr routing protocol using opnet," International Journal, vol. 2, no. 2, 2012.

[5] S. Abbas, M. Merabti, and D. Llewellyn-Jones, \The e_ect of direct interactionson reputation based schemes in mobile ad hoc networks," pp. 297{302, 2011.

[6] H. Sun, C. Chen, L. Hsu, Y. Chen, and Y. Chen, \Reliable data transmissiongainst packet dropping misbehavior in wireless ad hoc networks," pp. 419{424, 2011.

[7] N. Kang, E. Shakshuki, and T. Sheltami, \Detecting forged acknowledgements inmanets," pp. 488{494, 2011.

[8] A. Abdalla, I. Saroit, A. Kotb, and A. Afsari, \An ids for detecting misbehaviour nodes in optimized link state routing protocol," pp. 1{5, 2010.

[9] P. John and P. Vivekanandan, \A framework for secure routing in mobile ad hocnetworks," pp. 453{458, 2012.

[10] G. Karri and P. Khilar, \Routing misbehavior detection and reaction in manets,"1, vol. 1, pp. 80{85, 2010.

[11] M. Tamilarasi and T. Sundararajan, \Secure enhancement scheme for detectingsel_sh nodes in manet," pp. 1{5, 2012

[12] S. Singh, P. Jain, P. Bindra, and C. Goel, \Opnet based simulation and perfor-mance analysis of aodv and grp by varying number of misbehavior nodes."

[13] T. Lacey, R. Mills, B. Mullins, R. Raines, M. Oxley, and S. Rogers, \Ripsec{usingreputation-based multilayer security to protect manets," Computers & Security,2011.

[14] A. Ajina, G.R. shaktidhrma,\study of energy efficient, power aware routingalgorithm and their applications.2010 second international conference on machine learning and computing.

[15] S.Usha, S.Radha\ a collective network arbitration protocol to detect mac misbehavior inmanets2010

[16] Md.Sharma, M.Inamullah\ Misbehavior detection in mobile ad hoc networksusing Artificial Immune System approach 2011

[17] F.Xing, W.Wang\ on the survivability of wireless ad hoc Networks with node misbehaviors and failuresieee transactions on dependable and secure computing, vol. 7, no. 3, july-september 2010.

[18] K.Vats, M. Sachdeva, K.Saluja,\Simulation and performance analysis of olsr routing protocol using opnet volume 2, issue 2 feb 2012.

[19] Q Li, G.Cao\ mitigating routing misbehavior in disruption tolerant networks ieee transactions on information forensics and security, vol. 7, no. 2, april 2012

[20] S.agrwal, S.Jain, S.Sharma\ Mobility based performance analysis of aodv and dymo under varying degree of node misbehaviour. Volume 30-No.7,Sep2012

[21] N.Saquid, Md,SabbirViSim: A user-friendly graphical simulation tool for performanceanalysis of MANET routing protocols 2010 elsevier.

[22] A. Baadache, A.Belmunri\ Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networksJournal of Network and Computer Applications 35 (2012) 1130–1139

[23] M.Yang Su\Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems Computer Communications 34 (2011) 107–117

[24] J. Muleret, I. Welech\security threats and solutions in manets: a case study using aodv and saodv Journal of Network and Computer Applications 35 (2012) 1249–1259

[25] P.Joshi\ Security issues in routing protocols in MANETs at network layer Procedia Computer Science 3 (2011) 954–960