Analysing Influence of Fuzzy Logic in AODV Routing Protocol During Black Hole Attack

Bright Keswani[+], Bijendra Bansal[#], Poonam Keswani[*], Ambarish G. Mohapatra[&]

[+]*Professor, Department of Computer Applications, Suresh Gyan Vihar University, Jaipur, India*

[#]*Research Scholar, Suresh Gyan Vihar University, Jaipur, India*

[*]*Assistant Professor, Akashdeep PG College, Jaipur, India*

[&]*Assistant Professor, Electronics and Instrumentation Engineering, Silicon Institute of Technology, Bhubaneswar, Odisha, India*

Abstract- However there have been several researches that are simulating the influence of black hole attack in AODV based network. This research is addressing influence of using fuzzy logic in AODV routing protocol. Paper has represented the impact of Black Hole attack over AODV routing when fuzzy logic has been applied. Simulation of black hole attacks and determination of effect of such attack on network performance in proposed fuzzy based model and traditional model has been discussed. Fuzzy logic would allow random selection of nodes and this mechanism is suppose to improve the performance AODV based network as compare to traditional models. Simulation has represented results that are showing impact of malicious nodes over packet delivery ratio, packet loss ratio, Average end to end delivery, routing over head. Moreover the comparative analysis of traditional and proposed model has been made considering packet delivery ratio.

Keywords- Network simulation, Routing protocol, AODV, Black hole attack, NS2

I. INTRODUCTION

AODV is capable to maintain routing information to perform route discovery and route maintenance. Nodes are having sequence numbers that are used to check out new route and Broadcast ID. If sequence number of requested route packet is more that of destination node then this route is considered as new route. Intermediate nodes would reply to source node in other case. It has been observed that there have been four types of data packet message that are RREQ, RREP, RERR,HELLO. RREQ Message is broadcasted to destination node by intermediate node when a packet need to be transferred to destination by a source node.Destination node sends Route Reply (RREP) packet to destination with the help of reverse path as a reply to RREQ. RREP packet contains source address, destination sequence number, and destination address. Route Error Message (RERR) is transferred when there is a path failure if RREQ is not capable to reach its destination. RERR packet consists of unreachable destination sequence number along with unreachable destination address and source address [6]**. HELLO is** needed for link status monitoring and for broadcasting connectivity information. A node should use this messages only if it is part of an active route.

As source node need to send data to destination than AODV uses HELLO messages to discover path to destination through intermediate nodes. Each active mobile node transmits this messages in particular time interval to check if there is a path or not. If intermediate node does not receives multiple HELLO messages at regular interval from its neighbors than there is a no path. After path confirmation, source node floods RREQ packet towards destination. When an intermediate node receives RREQ packet, it checks its duplicity. If this RREQ packet is duplicate than it ignores it otherwise forward it towards destination. When reached to destination node, destination node will create a route reply packet and send it back to source node using reverse path. When source node receives RREP packet, it stores path to destination and will start communication. When source node receives multiple RREP packet, it selects shortest path. In case of a link break towards destination, intermediate node will generate Route Error packet and sends it to source node. Source node will delete that route and restart route discovery process [9].

Black Hole Attack has been considered as a category of Denial-of-services attack. In Black Hole attack a malicious are taking benefits of sequence number. Attacker node receive RREQ message fromneighboring node and increase value of destination sequence number. Then reply is made to source node. Greater value of sequence number represents fresh information over network. Thus source node accepts route reply message frommalicious node. It ignores less destination sequence number route reply message. Network traffic getredirected throughmalicious node. As source node S need to transfer data packet to destination node D, route discovery process is made with the help of RREQ message. It has destination sequence number. As neighboring node get RREQ message from source node S it modifies the routing table. It rebroadcast information to neighboring nodes. Every RREQ message has been uniquely identified using RREQ-Id and Source IP address. They support the elimination of duplicates. Route reply message is produced any intermediate node that have fresh route information todestination. Such reply may be produced by destination node too.

Fuzzy logic has been considered as approach to calculate according to degrees of truth instead of true or false (1 or 0). Usually modern computer are based on Boolean logic. Concept of fuzzy logic has been coined by Dr. LotfiZadeh of the University of California at Berkeley in the 1960s. In this logic the value lies between 0 and 1. Fuzzy sets generalize classical sets. As indicator functions of classical sets are special cases of membership functions of fuzzy sets if latter only take value between 0 or 1. Classical bivalent sets are usually called crisp sets in fuzzy set theory.

Network simulator has been considered as sequence of event network simulators. It consists of ns-1, ns-2, ns-3 and ns-4 that are used in research and teaching. NS2 has been considered as a simulation tool which is running over different platforms. NS2 has been considered as a discreet event simulator that is targeted to networking research. It is capable to provide help in simulation. It is supporting multicast protocols and IP protocols. These protocols may be UDP, TCP, RTP and SRM used in different type of networks.In case of ns2 nodes may be connected simplex as well as duplex.

II. LITERATURE REVIEW

In [1] Rutvij H. Jhaveri route detection process of default AODV in occurrence of an attacker. Some researches [2]presented Routing Attack and Solutions in case of Mobile ad hoc Network. Security routing mechanismsdependingon common neighbor listening have been discussed in such researches. In [3] and [4],authors have introducedroute confirmation request and route confirmation reply to avoidblack hole attack. In [5], authors Satoshi Kurosawa et.al. introduced an anomaly detection scheme to detect black hole attack using dynamic training method. Heretraining data is updated at regular time intervals to expressstate ofnetwork. Some researches [6] introduced Ad hoc On-Demand Distance Vector Routing and in [7] authorsdid research on Wormhole Attacks in Wireless Networks.

Mechanism to preventBlack Hole Attack [8] in Mobile Ad-hoc Networks with the help of anomaly Detection has been proposed by some researchers. On other side some have[9] presented Succinct Comparative Analysis and Performance Evaluation of MANET Routing Protocols. Authors [10] made performance analysis of reactive routing protocols in case of Mobile Ad hoc Networks.Many of researchers did[11] performance measurement in network environment. Authors have also[12] performed simulation Study of Malicious Activities under Various Scenarios Networks while some author [13] performed comparative analysis of different Routing Protocols.

III. COMPARATIVE ANALYSIS OF SIMULATION RESULT OF TRADITIONAL WORK AND PROPOSED WORK

In this research the simulation has been made on NS2 that is using AODV as routing protocol. The proposed work has compared its the performance with traditional work. In traditional work [14] there were just 16 nodes for simulation and the packet size was 1000bytes and AODV has been used as routing protocol. There were 5 malicious nodes 2,4,6,11, 13. Following chart is representing configuration of traditional model. This table is representing the simulation parameters such as simulator, number of nodes, simulation times, traffic type, network structure, packet size, mobility model, Routing protocol, channel, application used and malicious nodes.

Table 1 Table representing simulation parameters of traditional work [14]

Simulation Parameters	**Value**
Simulator	NS-2
Number of Nodes	16
Simulation Times	100 secs
Traffic Type	CBR (Constant bit rate)
Network Structure	GridPositionAllocator
Packet Size	1000 bytes
Mobility Model	ConstantPositionMobility Model
Routing Protocol	AODV Routing
Channel	Wifi Helper
Application used	OnOff Helper
Malicious Nodes	2, 4, 6, 11, 13

After simulation in traditional work the packet delivery ratio and packet loss ratio has been represented in following table. As the number malicious nodes increase the number packet delivery ratio get decreased and packet loss ratio increased.

Table 2 Effect of Black Hole Attack on PDR

Number of Malicious nodes	**Packet Delivery ratio (%)**	**Packet Loss ratio (%)**
1	64.86	35.14
2	59.35	40.65
3	39.93	60.07
4	24.22	75.78
5	18.12	81.88

IV. SIMULATION OF PROPOSED WORK

In proposed work the ns-2 has been used as network simulator that has been configured on UBuntu Linux platform. In this simulation the 200 nodes have been considered and the fuzzy logic has been applied while node selection. The size of packet is 1500 bytes in this model. The objective of research is to simulate the performance of proposed work by finding the delivery ratio and packet loss ratio. As from traditional simulation it is clear that as the number of malicious nodes increases then the packet delivery ratio get reduced. The proposed work is supposed to perform better than traditional work. In other words the packet delivery ratio of proposed work is suppose to be more as compare to tradition work.

Table 3 Simulation parameters of proposed work

Simulation Parameters	**Value**
Simulator	NS-2
Number of Nodes	200
Simulation Times	100 secs
Traffic Type	CBR (Constant bit rate)
Network Structure	GridPositionAllocator
Packet Size	1500 bytes
Mobility Model	ConstantPositionMobility Model
Routing Protocol	AODV Routing
Malicious Nodes	1,7,13,10,17,130

After simulation in proposed work the packet delivery ratio and packet loss ratio has been represented in following table. As the number malicious nodes increase the number packet delivery ratio get decreased and packet loss ratio increased.

Effect of Black Hole Attack on PDR in proposed work in different cases

Case 1

If the number of malicious node is 1
Generated packets=19852
Received packets=17366
Dropped packets=14727
Packet Delivery Ratio=87.4773
Loss Ratio=12.5227
Average end to end delay=2.16295ms
Routing overlead=0.784585

Case 2

If the number of malicious node is 2
Generated packets=16080
Received packets=13487
Dropped packets=16324
Packet Delivery Ratio=83.8744
Loss Ratio=16.1256
Average end to end delay=2.13425ms
Routing overlead=0.778856

Case 3

If the number of malicious node is 3
Generated packets=16095
Received packets=13524
Dropped packets=16572
Packet Delivery Ratio=84.0261
Loss Ratio=15.9739
Average end to end delay=2.18679ms
Routing overlead=0.779347

Case 4

If the number of malicious node is 4
Generated packets=14718
Received packets=12361
Dropped packets=14169
Packet Delivery Ratio=83.9856
Loss Ratio=16.0144
Average end to end delay=2.12588ms
Routing overlead=0.784925

Case 5

If the number of malicious node is 5
Generated packets=15563
Received packets=13186
Dropped packets=15299
Packet Delivery Ratio=84.7266
Loss Ratio=15.2734
Average end to end delay=2.19348ms
Routing overlead=0.785723

Case 6

If the number of malicious node is 6
Generated packets= 14927
Received packets= 12504
Dropped packets=15258
Packet Delivery Ratio= 83.7677
Loss Ratio=16.2323
Average end to end delay= 2.16599 ms
Routing overlead=0.78336

Following table is representing the status of generated, received, dropped packet along with packet deliver and packet loss ratio. The table has also represented the average end to end delay and routing overhead in case of different number of malicious nodes.

Table 4 Result of simulation in six cases

Number of Malicious nodes	Generated packet	Received packet	Dropped packets	Packet Delivery ratio (%)	Packet Loss ratio (%)	Average end to end delay	Routing overhead
1	19852	17366	14727	87.4773	12.5227	2.16295ms	0.784585
2	16080	13487	16324	83.8744	16.1256	2.13425ms	0.778856

3	16095	13524	16572	84.0261	15.9739	2.18679ms	0.779347
4	14718	12361	14169	83.9856	16.0144	2.12588ms	0.784925
5	15563	13186	15299	84.7266	15.2734	2.19348ms	0.785723
6	14927	12504	15258	83.7677	16.2323	2.16599 ms	0.78336

Simulation results

Following figure is representing the graph of generated packets.

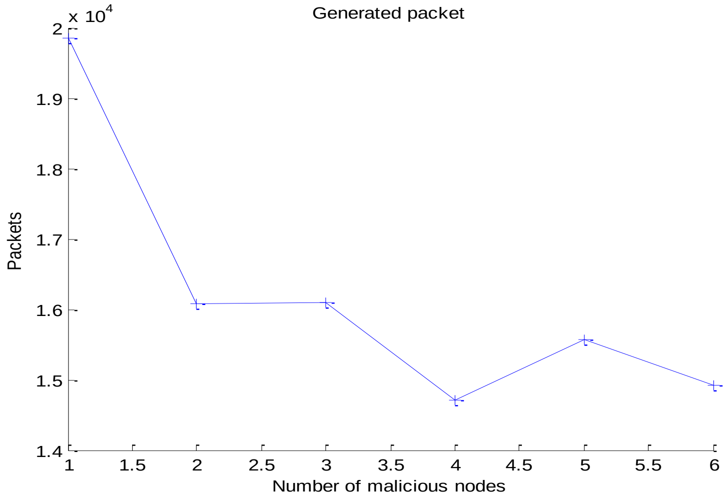

Fig.1: Generated Packet

Following chart is representing the simulation of received packet

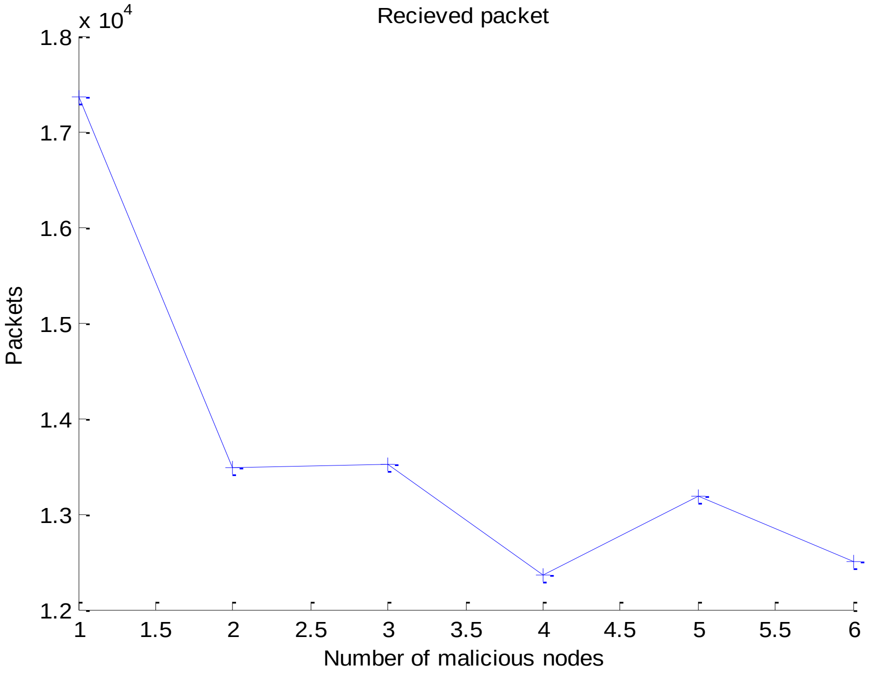

Fig.2: Received Packets

Following chart is representing the simulation of dropped packet

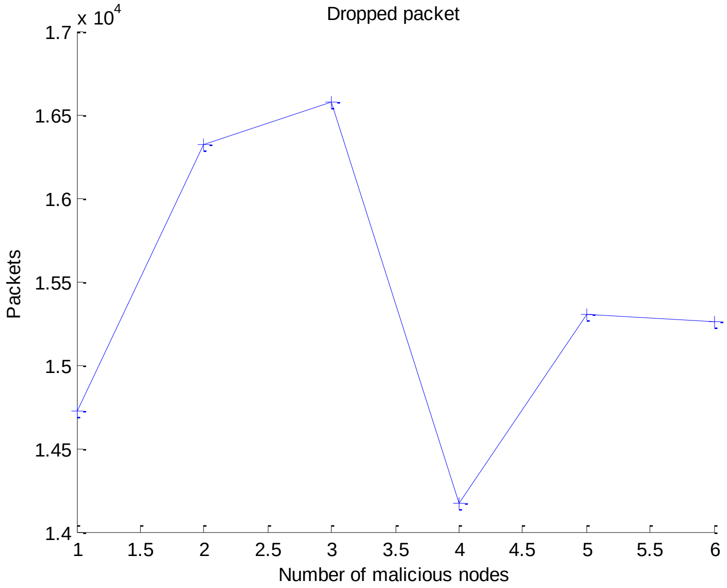

Fig.3: Dropped Packets

Following graph is representing packet delivery ratio with respect to number of malicious nodes

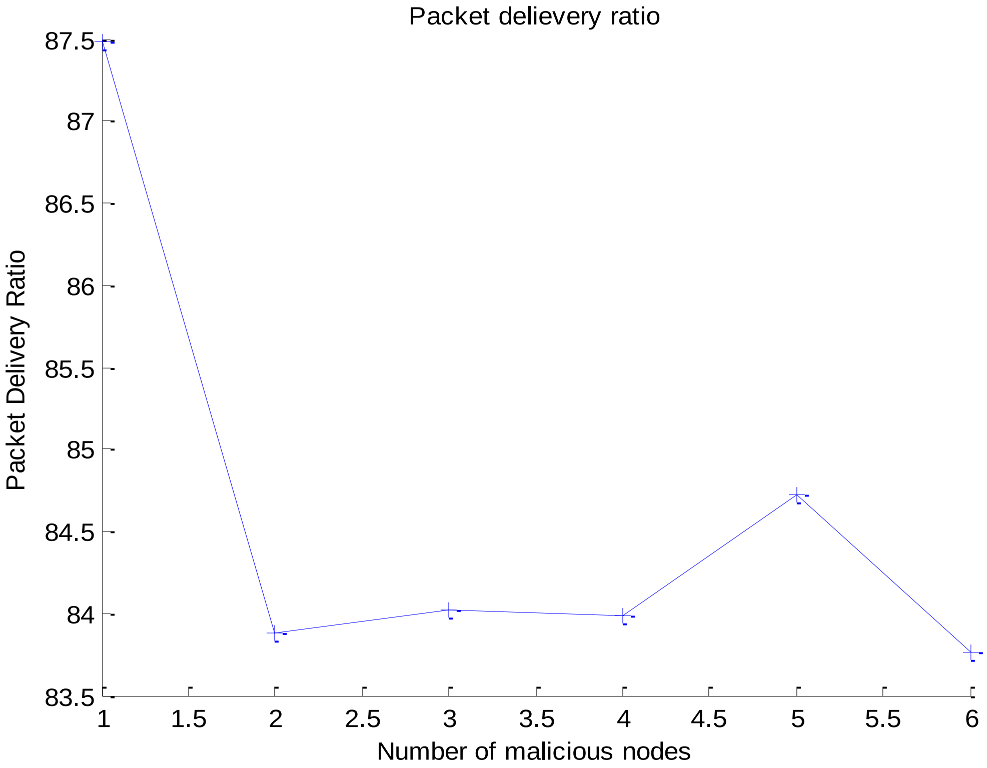

Fig.4: Packet Delivery ratio

Following graph is representing packet loss ratio with respect to number of malicious nodes

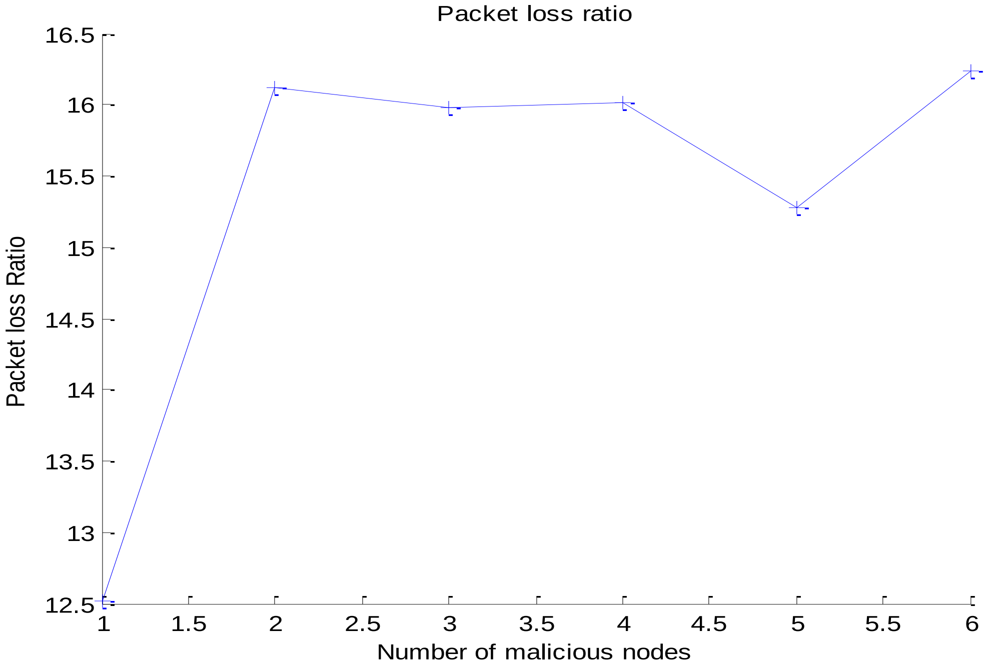

Fig.5: Packet Loss Ratio

Following graph is representing Average end to end delivery delay with respect to number of malicious nodes

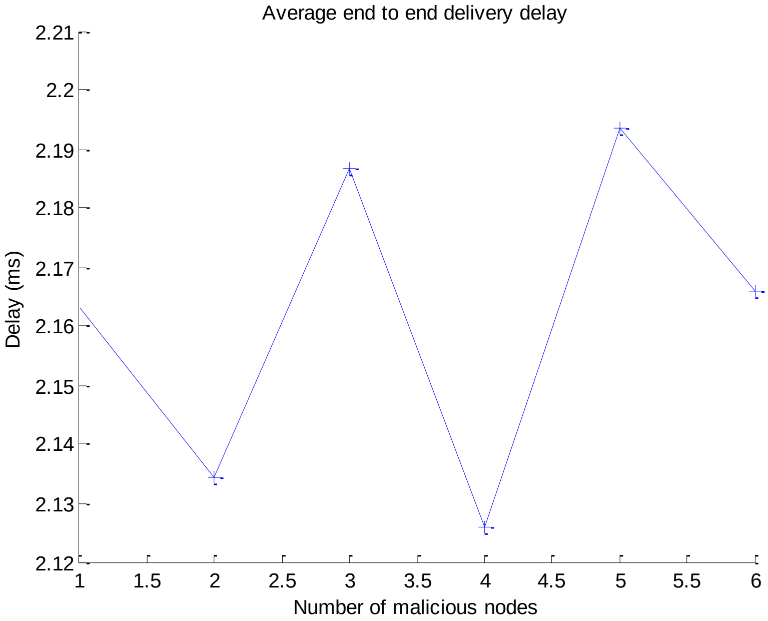

Fig.6: Average end to end delivery delay

Following graph is representing routing over head with respect to number of malicious nodes

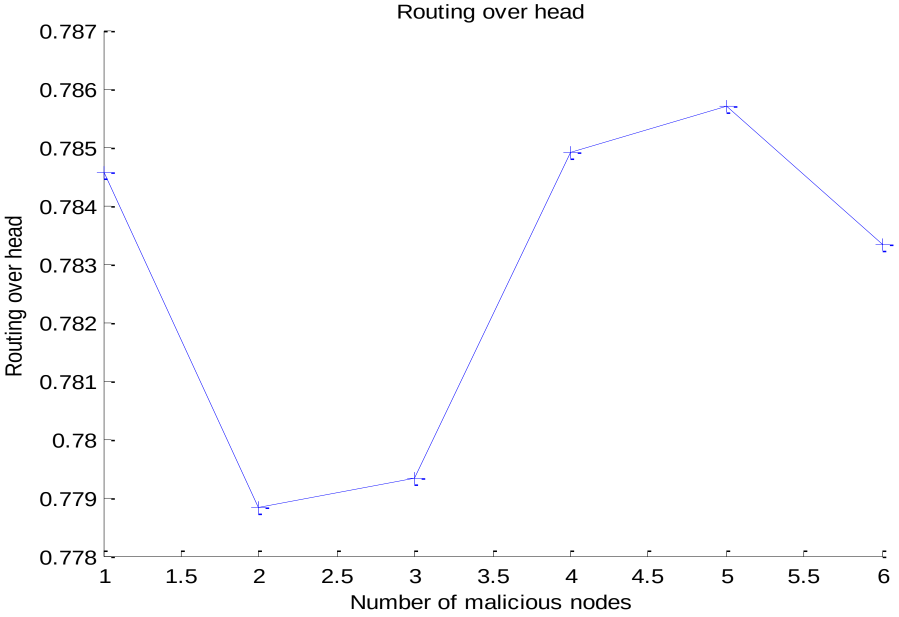

Fig.7: Routing over head

Given table is representing comparative analysis of performance of traditional and proposed considering packet delivery ratio.

Table 5 Comparison of packet delivery ratio in traditional and proposed work

Number of Malicious nodes	Packet Delivery ratio in traditional (%)	Packet Delivery ratio in proposed (%)
1	64.86	87.4773
2	59.35	83.8744
3	39.93	84.0261
4	24.22	83.9856
5	18.12	84.7266

Following figure is representing the simulation of above table in form of matlab chart

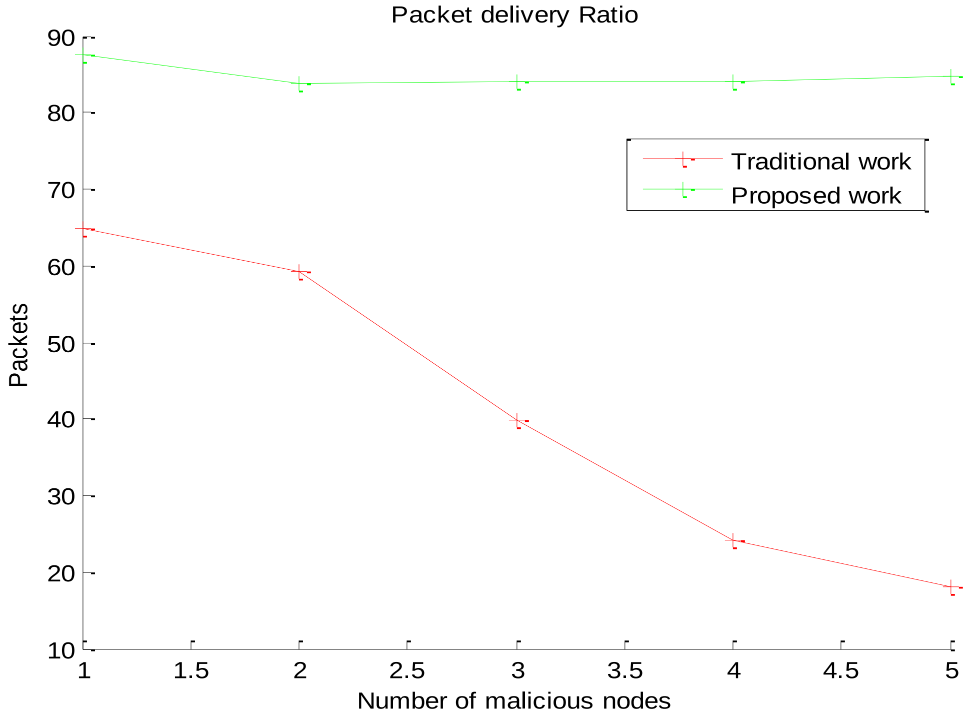

Fig.8: Comparative analysis of packet delivery in traditional and proposed

Following table is representing packet loss ratio in case of traditional and proposed.

Table 6 Comparison of packet loss ratio in case of traditional and proposed work

Number of Malicious nodes	Traditional Packet loss ratio (%)	Proposed Packet Loss ratio (%)
1	35.14	12.5227
2	40.65	16.1256
3	60.07	15.9739
4	75.78	16.0144
5	81.88	15.2734

The simulation of above chart has been shown in following figure

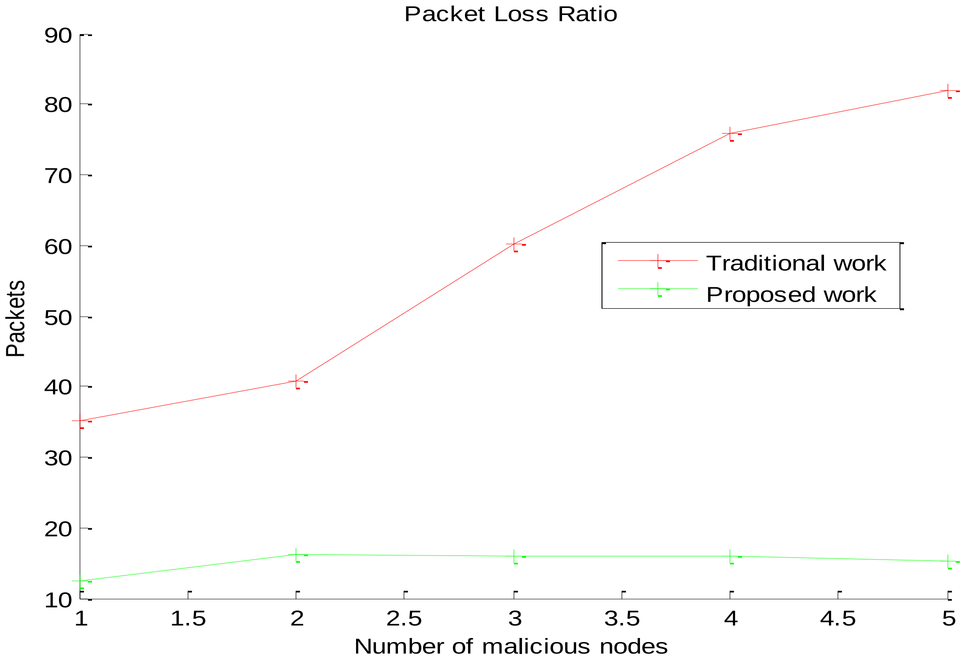

Fig.9: Comparative analysis of packet loss ratio in traditional and proposed

V. CONCLUSTION

Simulation hasrepresented the status of generated, received, dropped packet along with packet deliver and packet loss ratio. The has also considered average end to end delay and routing overhead in case of different number of malicious nodes.A malicious node reducesnetwork performance whennumber of malicious nodes innetwork increased. It has been observed that packet delivery ratio is decreased in such cases. Several researchers analyzed behavior of routing protocol and determinedeffect of Black Hole attack on AODV routing and its detection mechanism using NS2 simulators. The results represent how malicious nodes are influencing the packet delivery ratio, packet loss ratio, Average end to end delivery, routing over head. Results and comparative analysis has concluded that the proposed work is providing better delivery ratio as compare to traditional work. Moreover the number of nodes managed and packet size is more in case of proposed work as compared to traditional work.

In future it has been determinedeffect of Black Hole attack over AODV protocol would be observed in Fuzzy logic based network. In such network, nodes would perform transmission onbasis of fuzzy logic. The fuzzy logic would considervalue between 0 and 1 and selectnodes on random basis instead of sequential selection.

VI. REFERENCES

[1]. Rutvij H. Jhaveri,Sankita J. Patel,Devesh C. Jinwala "Improving Route Discovery for AODV to Prevent Black hole and Grayhole Attacks in MANETs", INFOCOMP 2013.

[2]. GengPeng, ZouChaanyun "Routing Attack and Solutions in Mobile ad hoc Network" IEEE-2006.

[3]. Y.Zhang and W.Lee,"Intrusion detection in wireless ad-hoc networks", 6th annual international Mobile computing and networking conference proceedings, 2000.

[4]. Seungjoon Lee, Bohyung Han, Minho Shin; "Robust Routing in Wireless Ad Hoc Networks" 2002, international Conference.

[5]. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto; "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007, PP:338-346.

[6]. C. Perkins, E. Belding-Royer, S. Das, "RFC-3561 Ad hoc On-Demand Distance Vector (AODV) Routing", pp. 1-32, July 2003.

[7]. Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks", IEEE JSAC, vol. 24, no. 2, Feb. 2006.

[8]. Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection by YibeltalFantahumAlem& Zhao HhengXaun from Tainjin 300222, China 2010, IEEE.

[9]. K. Natarajan and Dr. G. Mahadeven, "A Succinct Comparative Analysis and Performance Evaluation of MANET Routing Protocols", IEEE (ICCCI -2013), Jan. 04 – 06, 2013, Coimbatore, INDIA.

[10]. Michalis Papadopoulos, Constandinos X. Mavromoustakis and GeorgiosSkourletopoulos", Performance Analysis of Reactive Routing Protocols in Mobile Ad hoc Networks", 2014 International Conference on Telecommunications and Multimedia (TEMU),IEEE.

[11]. Performance Measurement in MANET BY Sandeep Kumar Arora, MubashirYaqoobMantooMahnazChishti and NehaChaudhary, 2014 5th International Conference-IEEE.

[12]. A Simulation Study of Malicious Activities under Various Scenarios in Mobile Ad hoc Networks (MANETs) by AkshaiAggarwal, NirbhayChaubey and Keyurbhai A Jani from Gujrat, India 2013, IEEE.

[13]. A Performance Analysis and Comparison of various Routing Protocols in MANET by M. Shobana and Dr. S. Karthik from Coimbatore-641035, 2013, IEEE.

[14]. SaritaBadiwal, AishwaryKulshrestha, " Analysis of Black Hole Attack in MANET using AODV Routing Protocol", International Journal of Computer Applications (0975 – 8887) Volume 168 – No.8, June 2017