International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

RANDOM-AODV: Efficient Adhoc on Demand Distance Vector Routing Protocol using Fuzzy Logic during Black Hole Attack

Bijender Bansal., Bright Keswani., Pankaj Gupta., Deepak Goyal

Abstract: ***However the black hole attack prevention has been proposed earlier but it is observed that the packet dropping increases constantly as the number of black hole attack are increased. The proposed work is making use of fuzzy logic. This mechanism allows the random node selection so it is supposed to maintain the packet delivery ratio. Results of this research show that the proposed mechanisms do not allow packet dropping on constant rate. Many studies are made that are simulating influence of attack made by .black .hole in the network based on .AODV. It has been observed that there is constant fall in the packet dropping ratio if number of malicious packet increases. This paper has represented the Black Hole attack over AODV routing when random node selection mechanism is applied. Proposed work is allowing selection of nodes on random basis. Such mechanism is supposed to improve the ratio of delivery of packet. Results of Simulation indicates the impact of black hole attack over packet delivery ratio , packet .loss .ratio, .Average .end to .end delivery, and .routing over head. Moreover the comparative analysis of .traditional and .proposed model is made considering packet delivery ratio.***

Keywords: Network simulation, Routing protocol, .AODV, Black hole attack, NS2, Random node selection

I. INTRODUCTION

AODV

AODV has been used to maintain the routing information for the execution of route discovery with the maintenance of the route. Nodes consist of the sequence numbers. These are applied for the checking of out new route as well as the BroadcastID. In the case of the majority of the sequence number related to the requested route packet than the destination node, this route will be a new route. In other case the Intermediate nodes deal with the source node. It is the fact that there are four different data packet message such as R.REQ, RREP, R.ERR, and H.ELLO. RREQ Intermediate nodes are used to send messages to destination nodes. It has been done to transfer the packet to destination using a source .node. .Route Reply (R.REP) packet has been transferred to Destination node. It has been made using the help of reverse path in the form of a reply to R.REQ.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
Mr. Bijender Bansal*, Research Scholar, Department of Computer Engineering, Suresh Gyan Vihar University, Jaipur, India.
Dr.Bright Keswani, Professor, Supervisor, Department of Computer Applications, Suresh Gyan Vihar University, Jaipur, India.
Dr. Pankaj Gupta, Professor, Co-Supervisor, Department of CSE, Vaish College of Engineering, Rohtak, India.
Dr. Deepak Goyal, Profeesor, Department of CSE, Vaish College of Engineering, Rohtak, India.

There is source address, in RREP packet. In addition, it consists of .destination .sequence number along with .destination .address. RERR stands for Route Error Message. It has been
broadcast at the time of path failure. There is destination sequence number which is unreachable. [6] in RE.RR packet consists**.** HELLO has been required for monitoring of the link status. In addition, it is used to broadcast the connectivity information. A node must apply this messages merely in the situation in which it is part of an active route.

BLACK HOLE ATTACK

It can be defined as a mixture of .attack. A malicious uses the sequence number in Black Hole attack. RREQ message from neighboring node has been received by the Attacker node. After that he makes increment in the .value of .destination sequence number. In next step, the .reply has been made source node. After the receiving of RREQ, the .routing table has been changed. This message has been received from source node S by the neighboring node. It is used to rebroadcast data to the nodes which is neighboring. Each RR.EQ message specially categorized the RREQ-Id as well as the Source IP address.

RANDOM NODE SELECTION

The proposed work has made use of random node selection in AODV network. The random selection reduce the probability of continues downfall of packet delivery ratio. It occurs when there is continues increment in malicious nodes. The random node selection has been made in proposed work in .order to decrease the loss ratio of packet as the .number of malicious node increases. Proposed work is allowing selection of nodes on random basis. This technique is supposed to improve pac.ket delivery ra.tio. It would also minimize the packet loss ratio in AODV based network as .compare .to traditional .models. Simulation is showing results that are representing impact of malicious nodes on the .packet delivery. Ratio as well as packet .loss ratio along with .average end to .end delivery and routing over head.

NETWORK SIMULATOR

A sequence of event network simulators is known as Network simulator. Network simulator includes to the n.s-1, n.s-2, n.s-3 and n.s-4. These are able to use in research work as well in teaching. It is the fact that NS2 is a simulation tool. One can run on multiple platforms. It is a discreet event simulator which is capable to use in research and helpful in simulation. It can support the multicast protocols as well as the IP protocols. Such protocols are UDP, TCP, RTP and. These are applied in multiple networks. Nodes are integrated in simplex and duplex inn case of ns2 .

II. RESEARCH GAP

However there has been several researches in field of AODV. Some of research focused on making improvement in Route discovery for AODV in order to avoid the Black hole as well as the Grayhoel attacks in MANETS [1]. On other hand some highlighted the Routing attacks and provide the solution in MANETs[2]. Many author focused on the .Intrusion detection [3] in wireless ad-hoc networks while researchers discussed the Robust Routing in Wireless Adhoc Network [4]. Black hole attack by dynamic learning method [5] is the theme of some researches. Traditional researches also proposed the work on RFC-.3561 Ad. hoc On.-Demand Distance Vector (AODV) routing [6]. Effect of Wormhole Attacks in Wireless .Networks [7] has been discussed in many researches. Many researchers did work to prevent the .Black Hole attack in Mobile Ad-hoc Networks using Anomaly[8] Recognition. While many researchers did analysis and Performance Evaluation of MANET Routing Protocols [9] and Reactive Routing Protocols in Mobile Ad hoc Networks [10][11]. Simulation Study of Malicious Activities [12] has been made under Various Scenarios in Mobile Ad hoc Networks. Traditional researches offered a Performance Evaluation of different Routing mechanism in MANET [13]. Analysis the Black Hole Attack in MANET applying AODV Routing Protocol [14] requires further research. There is need to propose a mechanism that could tackle the issue of constant packet dropping when malicious nodes increases in such network. To achieve this objective the fuzzy based random node selection has been proposed. This mechanism is supposed to maintain the packet delivery ratio even after constant increment in number of malicious nodes.

III. COMPARATIVE. ANALYSIS OF SI.MULATION RE.SULT O.F TRADITIONAL WORK AND PROPO.SED WORK..

It has been observed that in previous research uses AODV as routing protocol in making simulation using NS2. As .compared its .performance .with traditional work.. Only sixteen nodes were used for simulation in tradional work also size of packet was 1000bytes and for routing protocol they used AODV. There were 5 malicious nodes 2,4.,6,11., 13. Table shows the simulation parameters like simulator, number of nodes, simulation times, traffic type, and network structure. packet size., mobility model., Routing p.rotoco.l, channel, application used and malicious nodes.. In proposed work the ns-2 has been used as network simulator In this simulation 225 Nodes are considered and applied the fuzzy logic at the time of node selection.. The size of packet is kept 15.00 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. The proposed work is expected to perform better than traditional work.

Table 3 Simulation Parameter of Proposed Work

Considered Parameters	Values
Simulator used in research	NS-2
Number of Nodes	225
Simulation Times	100 secs
Type of traffic	CBR(Constant bit rate)
Structure of network	Grid Position allocator
Size of packet	1500 bytes
Name of Mobility Model	Constant Position Mobility Model
Protocol used for Routing	AODV Routing
Number of Nodes that are Malicious	1,7,13,10,70,130

After .simulation the packet .delivery .ratio and .packet loss ratio has .been represented in following table. The number of packet .delivery ratio get decreased and packet loss ratio .increased according to the increment of .malicious .nodes.

In proposed work Black Ho.le .Attack effect on .PDR in .different cases

Case. 1

If the number .of malicious node i.s 1

Produced Packets	22355
Captured Packets	19898
Packets that have been dropped	2456
Observed Ratio of Packet Delivery	89.0098
Observed Ratio of packet loss	10.9902
Average delay during End to End Delivery	2.11249ms
Overhead inspected during Routing	0.785528

Case. 2

If there are two malicious node

Produced Packets	20296
Captured Packets	17326
Packets that have been dropped	2970
Observed Ratio of Packet Delivery	85.3666
Observed Ratio of packet loss	14.6334
Average delay during End to End Delivery	0.06829ms
Overhead inspected during Routing	0.771794

C.ase 3

If there are three malicious node

Produced Packets	=22774
Captured Packets	=20089
Packets that have been dropped	=2685
Observed Ratio of Packet Delivery	=88.2102
Observed Ratio of packet loss	=11.7898
Average delay during End to End Delivery	=2.20663ms
Overhead inspected during Routing	=0.781187

Case. 4
If there are four malicious node
Case. 5
If there are five malicious node

Produced Packets	21416
Captured Packets	18158
Packets that have been dropped	3258
Observed Ratio of Packet Delivery	84.7871
Observed Ratio of packet loss	15.2129
Average delay during End to End Delivery	2.15048
Overhead inspected during Routing	0.76629
Produced Packets	=19093
Captured Packets	=16355
Packets that have been dropped	=2738
Observed Ratio of Packet Delivery	=85.6597
Observed Ratio of packet loss	=14.3403
Average delay during End to End Delivery	=2.18814ms
Overhead inspected during Routing	=0.774274

Case. 6
If there are six malicious node

Produced Packets	=23315
Captured Packets	=20601
Packets that have been dropped	=2714
Observed Ratio of Packet Delivery	=88.3594
Observed Ratio of packet loss	=11.6406
Average delay during End to End Delivery	=2.16604ms
Overhead inspected during Routing	=0.781258

Below given table shows the routing overhead and average. end to end delay as per the malicious nodes..

Table. 4 Chart representing packet delivery ratio and received packet along with overhead and average delay

Number of Malicious nodes	Produced Packets	Captured Packets	Packets that have been dropped	Observed Ratio of Packet Delivery	Observed Ratio of packet loss	Average delay during End to End Delivery	Overhead inspected during Routing
1	22356	19899	2457	89.0097	10.9903	2.11249ms	0.785528
2	20296	17326	2970	85.3666	14.6334	2.06829ms	0.771794
3	22774	20089	2685	88.2102	11.7898	2.20663ms	0.781187
4	21416	18158	3258	84.7871	15.2129	2.15048ms	0.76629
5	19093	16355	2738	85.6597	14.3403	2.18814ms	0.774274
6	23315	20601	2714	88.3594	11.6406	2.16604ms	0.781258

Imitation results

Following chart is representing the number of produced packet in different scenarios

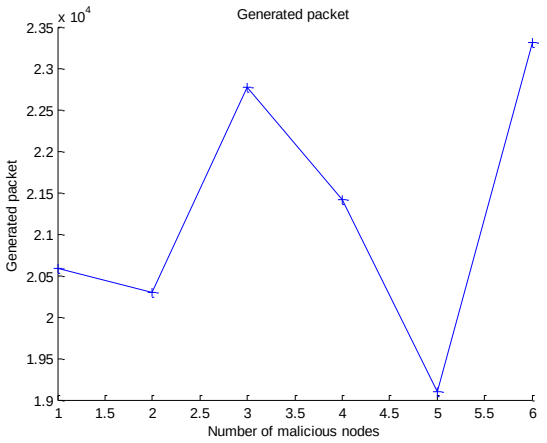

Fig 1 Produced Packet

Following chart is representing the simulation of Received Packet.

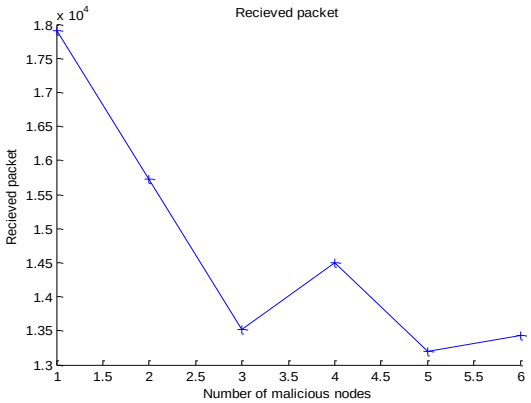

Fig 2 Captured Packet

Following chart is representing the simulation of Dropped Packet.

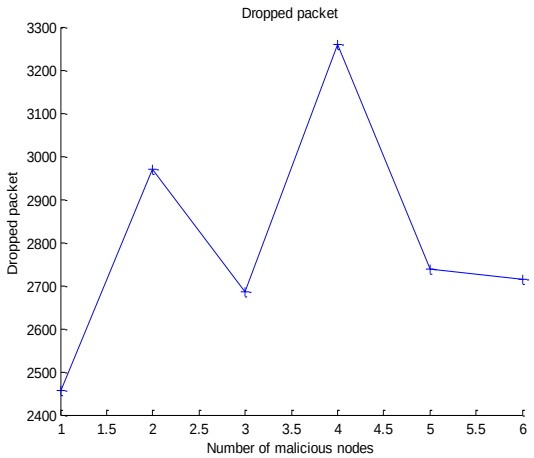

Fig 3 Packets that are dropped

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

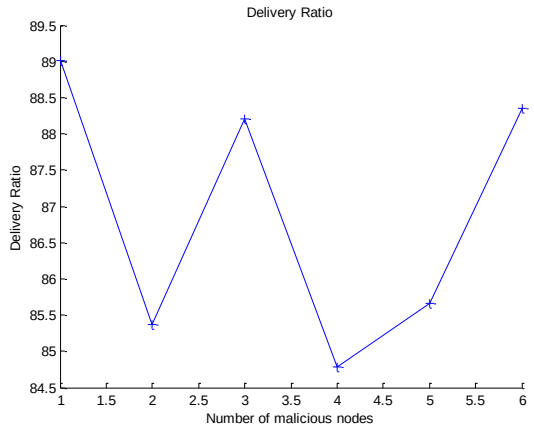

Fig 4 Observed Ratio of Packet Delivery

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

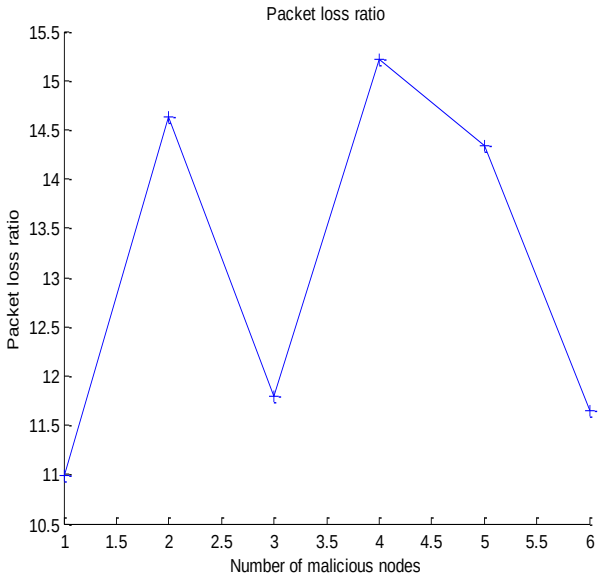

Fig 5 Ratio of Packet Loss

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

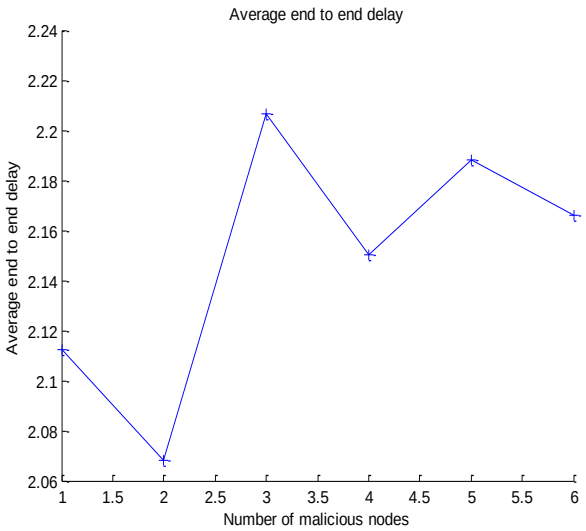

Fig 6 Average delay during End to End Delivery

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

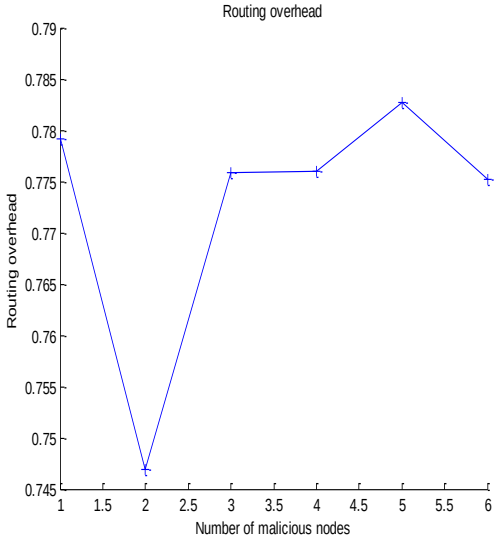

Fig 7 Overhead inspected during Routing

Below table is representing comparative analysis of Traditional and Proposed Model on the base of Packet Delivery Ratio.

Table 5 Comparative analysis of Existing and Proposed Model on the base of Packet Delivery Ratio

Nodes that are Malicious	Ratio of Packet Delivery in traditional (%)	Ratio of Packet Delivery in proposed (%)
1	64.86	89.0097
2	59.35	85.3666
3	39.93	88.2102
4	24.22	84.7871
5	18.12	85.6597

The simulation of above table is plotted in Matlab which is stated below

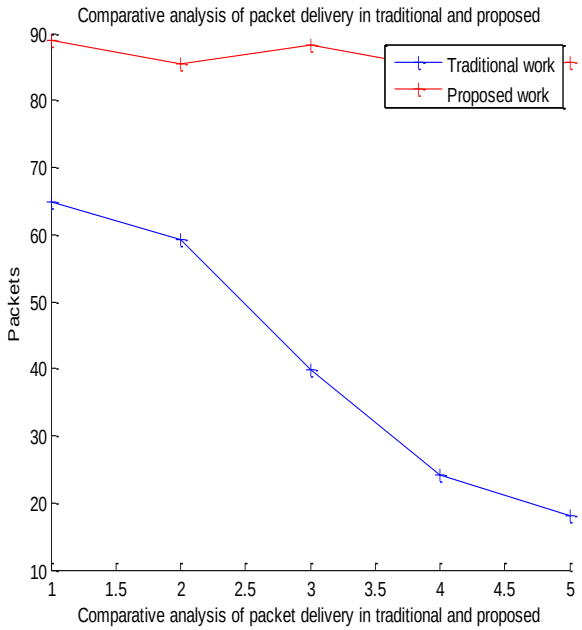

Fig 8 Comparison of Packet Delivery between Existing and Proposed Work

In the below table, the packet loss ratio of traditional and proposed model is presented.

The simulation of above chart has been shown in following figure

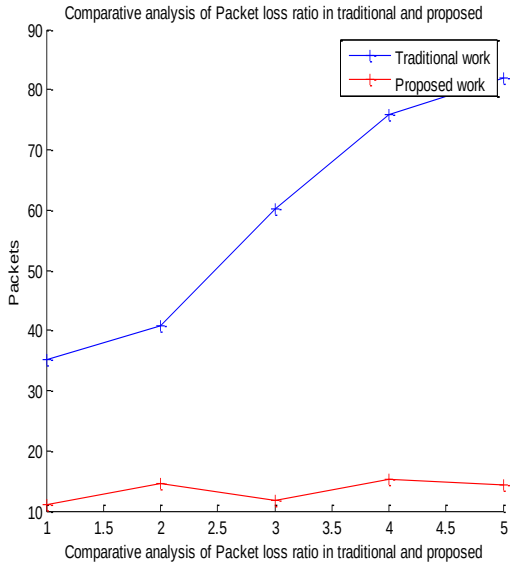

Fig 9 Comparison between packet loss ratio in Existing and Proposed Model

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

Malicious Node	Packet loss ratio in Traditional work (%)	Packet Loss ratio in Proposed work (%)
1	35.1399	10.9903
2	40.6499	14.6334
3	60.06	11.7898
4	75.7799	15.2129
5	81.88	14.3403

IV. CONCLUSTION

The effect of black hole attacks on Produced Packets, Captured Packets, and Dropped Packets is discussed in the research work. Additionally, the effected packet delivery and the ratio of packet loss from black holes attacks are also considered here. In the proposed work, the fuzzy logic mechanism is used which allows the random node selection and enable to maintain the packet delivery ratio. It is concluded by the research work that the increment in malicious nodes reduced the overall performance of a network. Numerous researchers are discussed to analyze the working of routing protocol. Main focus of research work is to avoid the influence of Black Hole attack on random AODV routing applying Fuzzy logic. For this, an NS2 simulator is utilized. In random node selection based network, Nodes would perform transmission on random basis. The comparative analysis of .traditional and .proposed model is made on the base of packet delivery ratio, Captured Packets, Dropped Packets etc. The proposed comparative analysis clearly indicated that the proposed random AODV is an efficient routing protocol to avoid black hole attacks.

REFERENCE

1. Rutvij H. Jhaveri,Sankita J. Patel,Devesh C. Jinwala (2013) "Improving Route Discovery for AODV to Prevent Black hole and Grayhole Attacks in MANETs".
2. Geng Peng, Zou Chaanyun (IEEE 2006)"Routing Attack and Solutions in Mobile ad hoc Network".
3. Y.Zhang and W.Lee,(2000) "Intrusion detection in wireless ad-hoc networks", 6th annual international Mobile computing and networking.
4. Seungjoon Lee, Bohyung Han, Minho Shin (2002) "Robust Routing in Wireless Ad Hoc Networks"
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",
6. C. Perkins, E. Belding-Royer, S. Das(2003) "RFC-3561 Ad hoc On-Demand Distance Vector (AODV) Routing".
7. Y-C. Hu, A. Perrig, and D. Johnson(2006), "Wormhole Attacks in Wireless Networks",
8. Alem & Zhao Hheng Xaun from Tainjin 300222, China (IEEE 2010) "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection by Yibeltal Fantahum"
9. K. Natarajan and Dr. G. Mahadeven, IEEE (ICCCI -2013), "A Succinct Comparative Analysis and Performance Evaluation of MANET Routing Protocol".
10. Akshai Aggarwal, Nirbhay Chaubey and Keyurbhai A Jani from Gujrat, India (IEEE 2013),." A Simulation Study of Malicious Activities under Various Scenarios in Mobile Ad hoc Networks (MANETs) "
11. M. Shobana and Dr. S. Karthik from Coimbatore-641035, (IEEE 2013), "A Performance Analysis and Comparison of various Routing Protocols in MANET"
12. Sarita Badiwal, Aishwary Kulshrestha, (2017)" Analysis of Black Hole Attack in MANET using AODV Routing Protocol"