International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-6, April 2020

Impact of Black Hole Attack over Random Aodv Routing Protocol

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

ABSTRACT: ***There are many researches in which the impact of black hole attacks at AODV networks is highlighted. In the research work, the impact of Black Hole attack over AODV routing is calculated and random node selection technique is used. In addition, the simulation of black hole attacks' impact on network performance is proposed in case of proposed model and traditional model. The selection of nodes is made randomly. The simulation of proposed selection based model is able to enhance the ratio of packet delivery. It is efficient to decrease the ratio of packet loss than traditional models. Comparative evaluation of the performance of existing and proposed model is made on the base of Packet Delivery ratio, Packet loss ratio, Packet Delivery ratio, Packet Loss ratio in case of 200 Node and 225 Node. This research paper also determined Average End to End Delivery and Routing over head during comparative analysis. The proposed work can minimize the downfall in delivery ratio as the amount of malicious node increases.***

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

I. INTRODUCTION

AODV

AODV Routing stands for Ad hoc On-Demand Distance Vector Routing. This Routing protocol is efficient to be used in MANETs as well as in wireless ad hoc networks. AODV maintains the routing information to execute the route discovery. There are sequence numbers in Nodes which are able to check new route. This sequence is used to decide Broadcast ID[1]. There may be different sequence number of requested route packet. In that case, a new route will be used. But on the other hand, Intermediate nodes perform execution along with source node. In RREP packet, source address is applied. Additionally, there are destination sequence number as well as destination address that are make in use. RERR refers to Route Error Message [2,3]. These are broadcasted when there are any failures of path. RERR packet consists of destination sequence numbers that are not reachable.

Revised Manuscript Received on April 30, 2020.
***** Correspondence Author
Mr. Bijender Bansal*, Research Scholar, Department of Computer Engineering, Suresh Gyan Vihar University, Jaipur, India. bijender.vce@gmail.com.
Dr.Bright Keswani, Professor, Supervisor, Department of Computer Applications, Suresh Gyan Vihar University, Jaipur, India. bright.keswani@mygyanvihar.com.
Dr. Pankaj Gupta, Professor, Co-Supervisor, Department of CSE, Vaish College of Engineering, Rohtak, India. pankajgupta.vce@gmail.com.
Ms.Monika Goyal, Assistant Professor, Department of Computer Science, Vaish Mahilla Maha Vidyala, Rohtak, India **monikagoyal.vmm@gmail.com.**
Dr. Deepak Goyal, Profeesor, Department of CSE, Vaish College of Engineering, Rohtak, India. deepakgoyal.vce@gmail.com.

Additional to this, it includes destination address as well as source address. To monitor the link status, HELLO is needed. Furthermore, this has been used for broadcasting the information. A node applies this message in some specific situation.

If a node is part of an active route, this message is obtained. Four separate data packet message are there for example RREQ, RREP, RERR, and HELLO. Intermediate node sends RREQ Message to destination node. [4].

BLACK HOLE ATTACK

In computer networking, packet drop attacks are black hole attacks. These denial-of-service attackers relay the packets that to destroy the information of packets. The black hole attacks are made using router in several causes. The packets can be dropped out to lossy network easily. It is very hard to detect and avoid the packet drop attacks [5,6].

Black Hole Attack has been known as collection of multiple attacks. In Black Hole attack, the sequence numbers are used by malicious. The Attacker node received the RREQ message to node which is neighboring. Afterward, he increases the value related to destination sequence number. After getting the RREQ, there are changes in routing table. This message is obtained to the source node S by node which is neighboring. It is able to be use in rebroadcast data to neighboring nodes. Each RREQ message basically separated the RREQ-Id and Source Internet Protocol address [7,8].

II. RANDOM NODE SELECTION

In proposed research, the selection of random node is made in AODV network. The technique of random selection is used because it is able to decrease the chances of regular downfall of packet delivery ratio if the malicious node increases [9]. Random node selection has been made here in order to make decrement in packet loss ratio that varies as per changes in amount of malicious node. This work makes nodes selection randomly. In order to improve packet delivery ratio, this technique has been used. The proposed random node selection model is able to minimize the packet loss ratio in AODV network. But in traditional models, it was not feasible. The Simulation of proposed work is also made. The results of represents the impact of malicious nodes. Its effect is calculated on the packet delivery ratio as well as packet loss ratio along with average end to end delivery and routing over head [10,11].

III. NETWORK SIMULATOR

Network simulator is a sequence of event network simulators. There are different Network simulator such as ns-1, ns-2, ns-3 and ns-4.

These simulators have efficiency to be used for research purpose as well as teaching purpose also. This support to multicast protocols and IP protocols also [12]. UDP, TCP, and RTP can be used in several networks. In ns2 simulator, the integration of Nodes is made in simplex and duplex. NS2 is a tool, used for simulation of models.

It is the fact that it can perform on different platforms. It has been known as a discreet event simulator. It has features to be used for research purpose. It has been found helpful to complete the simulation phase.[13,14].

IV. RESEARCH GAP

There are several research related to AODV which are discussed here such as.

In 2013, Rutvij H. Jhaveri,et al [1] provide the research work to improve the Route Discovery for AODV to Prevent Black hole and Grayhole Attacks in MANETs. Their aim was to enhance the Route Discovery for AODV and avoid the Black hole and Grayhole Attacks. But the research has ignored black hole attack.

In 2006, Geng Peng, et al [2] wrote on Routing Attack and Solutions in Mobile ad hoc Network. Their aim was to provide the solutions in Mobile ad hoc Network and consider the Routing Attack. But Research was not considered the performance of network.

In 2000, Y.Zhang et al [3] discussed the Intrusion detection in wireless ad-hoc networks. They highlighted the detection of Intrusion in ad-hoc networks which are wireless. But there is Limited scope of research as work is limited to IDS.

In 2002, Seungjoon Lee et al [4] wrote on automatic Routing in Wireless Ad Hoc Networks. In the research work, they considered the Robust Routing in Wireless Ad Hoc Networks. But Research is not providing solution of attacks.

In 2007, Satoshi Kurosawa, et al [5] discussed the Blackhole Attack on AODV -based Mobile Ad Hoc Networks. For this purpose, Dynamic Learning Method has been used by them. Their objective was to highlight the Black hole Attack on AODV -based Mobile Ad Hoc Networks. But there is consistent fall is delivery ratio according to amount of attack increases.

In2003, C. Perkins, et al [6] analyzed on RFC-3561 AODV Routing. This research work considered RFC-3561 AODV Routing. But the Research ignored the several types of attacks to AODV routing.

In 2006, Y-C. Hu, et al [7] stated Wormhole Attacks in Wireless Networks in their research work. Their aim was to discuss the effect Wormhole Attacks in Wireless Networks. But the research is limited to wormhole attack and ignored the performance parameters.

In 2010, Yibeltal Fantahum Alem et al [8] considered the Black Hole Attack in Mobile Ad-hoc Networks. In their research work, they used the Anomaly Detection to avoid the black hole attack. Aim of this research is to avoid Black Hole Attack in Mobile Ad-hoc Networks. For this, Anomaly Detection is made. But this research has worked on limited performance parameters.

In 2013, K. Natarajan et al [9] proposed comparison of Performance on MANET Routing Protocols. They provided the analysis and Performance Evaluation of MANET Routing Protocols. But it did not consider the security.

In 2014 , Michalis Papadopoulos et al [10]analyzed the performance of Reactive Routing Protocols in Mobile Ad hoc Networks. They have performed the analysis of Reactive Routing Protocols in Mobile Ad hoc Networks. But Research is limited to performance and ignored the security.

In 2014, Sandeep Kumar Arora, et al [11] measured the efficiency of MANET. The aim of research work was to provide the performance analysis of Reactive Routing Protocols in Mobile Ad hoc Networks. This Research worked for performance and did not consider the security.

In 2013, Akshai Aggarwal, et al [12] studied the Malicious Activities. These activities are considered under different Scenarios in MANETs.

They proposed simulation of spiteful executions. This work ignored the performance.

In 2013, M. Shobana et al [13] compared various Routing Protocols in MANET. They offered an analysis of Performance. They also compared different Routing Protocols in MANET. Research works for performance and not providing any security from external attack.

In 2017, Sarita Badiwal, et al [14] analyzed the Black Hole Attack in MANET. In this research work, they used AODV that is Routing Protocol. It has been analyzed that increment of malicious packet decreases the packet dropping ratio.

V. [3] COMPARATIVE ANALYSIS OF SIMULATION RESULT OF EXISTING WORK AND PROPOSED WORK

It is analyzed that in existing work, for the simulation, NS2 is used on AODV as routing protocol. In the research work, comparative analysis of performance of proposed work is made with traditional work.

In traditional work [14] there were sixteen nodes which were used in simulation process and the packet size was 1000bytes.

In existing work, AODV is taken as routing protocol and 5 malicious nodes 2, 4,6,11, 13 are taken.

Following chart is representing configuration of traditional model. The simulation parameters are represented by following table such as simulator, number of nodes, simulation times, traffic type, network structure, packet size, mobility model, Routing protocol, channel, application used and malicious nodes.

Here ns-2 has been used as network simulator which is configured on UBuntu Linux platform. In this simulation, the 225 nodes have been considered and the fuzzy logic has been applied while selection of node. In this model, Packet size is 1500 bytes. To simulate the performance of proposed work is the main objective of this research.

Here packet delivery ratio and packet loss ratio are considered [15]. It is clear with proposed work that as the number of malicious nodes increases then the packet delivery ratio gets reduced.

After simulation in proposed work the packet delivery ratio and packet loss ratio are shown in below given table. Packet delivery ratio decreases as the number malicious nodes increase and packet loss ratio increased.

Table 1 Simulation parameters of proposed work

Simulation Parameters	Value
Simulator	NS-2
Number of Nodes	225
Simulation Times	100 secs
Traffic Type	CBR (Constant bit rate)
Network Structure	Grid Position Allocator
Packet Size	1500 bytes
Mobility Model	Constant Position Mobility Model
Routing Protocol	AODV Routing
Malicious Nodes	1, 7, 13, 10, 70, 130

Influence of Black Hole Attack on PDR in six cases

Case 1

If Malicious node = 1

Generated Packets = 22356

Received Packets = 19899

Dropped Packets = 2457

Packet Delivery Ratio = 89.0097

Loss Ratio = 10.9903

Average End-to-End Delay = 2.11249ms

Routing overhead = 0.785528

Case 2

If the number of malicious node is 2

Generated Packets = 20296

Received Packets = 17326

Dropped Packets = 2970

Packet Delivery Ratio = 85.3666

Loss Ratio = 14.6334

Average End-to-End Delay = 2.06829ms

Routing overhead = 0.771794

Case 3

If the number of malicious node is 3

Generated Packets = 22774

Received Packets = 20089

Dropped Packets = 2685

Packet Delivery Ratio = 88.2102

Loss Ratio = 11.7898

Average End-to-End Delay = 2.20663ms

Routing overhead = 0.781187

Case 4

If the number of malicious node is 4

Generated Packets = 21416

Received Packets = 18158

Dropped Packets = 3258

Packet Delivery Ratio = 84.7871

Loss Ratio = 15.2129

Average End-to-End Delay = 2.15048ms

Routing overhead = 0.76629

Case 5

If the number of malicious node is 5

Generated Packets = 19093

Received Packets = 16355

Dropped Packets = 2738

Packet Delivery Ratio = 85.6597

Loss Ratio = 14.3403

Average End-to-End Delay = 2.18814ms

Routing overhead = 0.774274

Case 6

If the number of malicious node is 6

Generated Packets = 23315

Received Packets = 20601

Dropped Packets = 2714

Packet Delivery Ratio = 88.3594

Loss Ratio = 11.6406

Average End-to-End Delay = 2.16604ms

Routing overhead = 0.781258

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 2 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	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

VI. SIMULATION RESULTS

The simulation of proposed model is proposed here such as

Table 3 Comparative Analysis of Packet Delivery

Number of Malicious nodes	Packet Delivery ratio in traditional (%)	Packet Delivery ratio 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

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

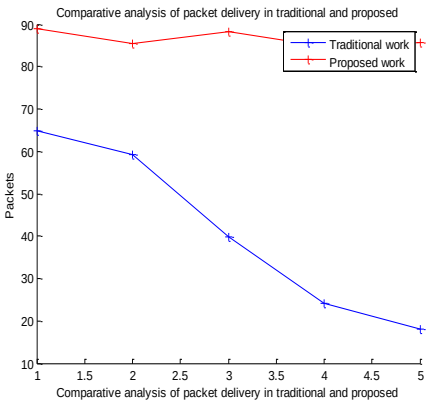

Fig 1 Comparative analysis of packet delivery in traditional and proposed

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

Table 4 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	10.9903
2	40.65	14.6334
3	60.07	11.7898
4	75.78	15.2129
5	81.88	14.3403

Following figure is showing the simulation of above chart.

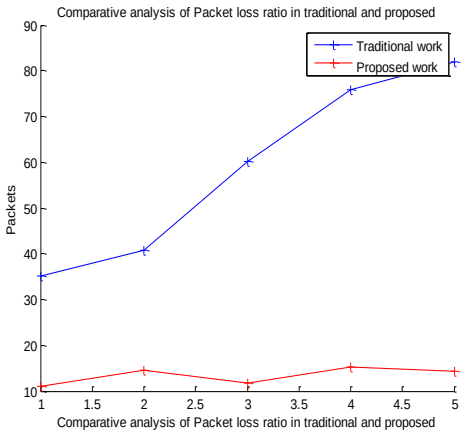

Fig 2 Comparative analysis of packet loss ratio in traditional and proposed

Table 5 Packet delivery ratio with 200 Node and 225 Node

Malicious node	Nodes 200	Nodes 225
1	87.4773	91.1278
2	83.8744	87.4455

3	84.0261	91.3349
4	83.9856	82.9392
5	84.7266	87.5089
6	83.7677	88.3594

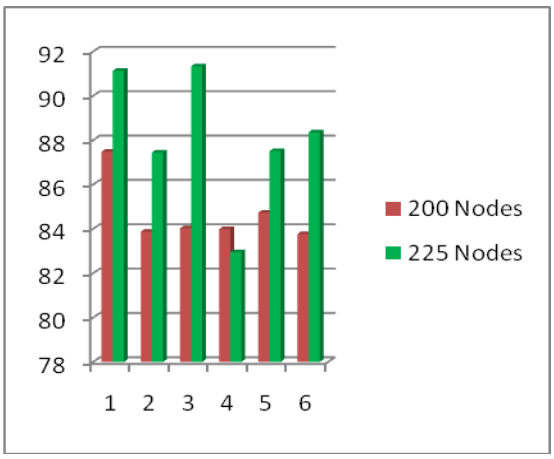

Fig 3 Packet delivery ratio with 200 Node and 225 Node

Table 6 Packet Loss Ratio in case of 200 Node and 225 Node

Malicious node	Nodes 200	Nodes 225
1	12.5227	8.87222
2	16.1256	12.5545
3	15.9739	8.66507
4	16.0144	17.0608
5	15.2734	12.4911
6	16.2323	11.6406

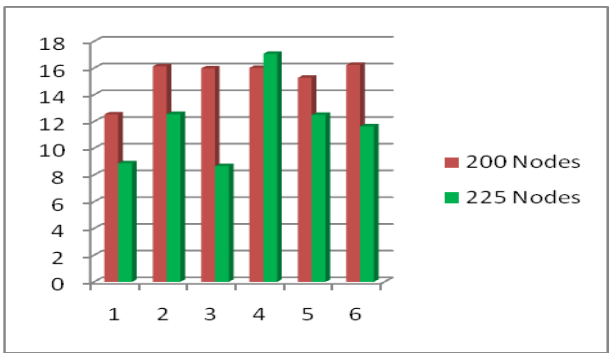

Fig 4 Packet Loss Ratio in case of 200 Node and 225 Node

VII. CONCLUSTION

In this research work, different researchers related to routing protocols are reviewed here. These researches are reviewed in order to analyze how routing protocols perform. This research work is proposed in order to prevent Black Hole attack on random AODV routing. For this purpose, Fuzzy logic technique is used. In this work, an NS2 simulator is used to simulate the result of this research work. Transmission between Nodes is performed randomly in random node selection based network. Black hole attacks affect Generated Packets, Received Packets, and Dropped Packets in case of 200 Node and 225 Node which is also considered here. In addition, the effected packet delivery and the ratio of packet loss in case of 200 Node and 225 Node are calculated in this work. Fuzzy logic mechanism has been applied as it enables to make node selection randomly. Packet delivery ratio can be maintained using this mechanism. This research work concludes that a malicious node can easily reduce the network's performance. Packet deivery ratio, Generated Packets, Received Packets, and Dropped Packets etc are considered to provide comparative analysis of proposed Fuzzy logic based model and existing techniques. It has become clear by the comparative analysis that random AODV routing protocol can be used efficiently to prevent black hole attacks.

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. Geng Peng, Zou Chaanyun "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 Yibeltal Fantahum Alem & Zhao Hheng Xaun 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 Georgios Skourletopoulos", 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, Mubashir Yaqoob Mantoo Mahnaz Chishti and Neha Chaudhary, 2014 5th International Conference-IEEE.
12. A Simulation Study of Malicious Activities under Various Scenarios in Mobile Ad hoc Networks (MANETs) by Akshai Aggarwal, Nirbhay Chaubey 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. Sarita Badiwal, Aishwary Kulshrestha, " Analysis of Black Hole Attack in MANET using AODV Routing Protocol", International Journal of Computer Applications (0975 – 8887) Volume 168 – No.8, June 2017.
15. Bijender Bansal, Bright Keswani, Dr. Pankaj Gupta and Dr. Deepak Goyal "RANDOM-AODV: Efficient Adhoc On Demand Distance Vector Routing Protocol Using Fuzzy Logic During Black Hole Attack", International Journal of Innovative Technology and Exploring Engineering, IJITEE (ISSN: 2278-3075), Volume- 9, Issue -2, December 2019, pp 2730-2734.