Power System Technology
ISSN:1000-3673

Received: 06-06-2024 Revised: 15-07-2024 Accepted: 28-08-2024

Denial-of-service attack (BH and PDA) effect analysis on AODV Routing Protocol with Random Mobility

[1]Dr. Margam Suthar, [2]Dr. Ajay Kumar Vyas, [3]Dr.Jigar A. Soni, [4]Dr.Himanshu Amritlal Patel, [5]Dr. Viral H. Borisagar

[1]Assistant Professor, School of Engineering and Technology, Gujarat Technological University, Ahmedabad, Gujarat, India, margam.19ec@gmail.com

[2]Assistant Professor, Adani Institute of Infrastructure Engg, Gujarat Technological University, Ahmedabad, Gujarat, India, Ajay.Vyas@aiim.ac.in

[3]Assistant Professor, Department of Information and Communication Technology, Sankalchand Patel College of Engineering Visnagar, North Gujarat, India. jasoniict_spce@spu.ac.in

[4]Associate Professor, Department of Information and Communication Technology, Sankalchand Patel College of Engineering Visnagar, North Gujarat, India. hapict_spce@spu.ac.in

[5]Assistant Professor, Computer Engineering Department, Vishwakarma Government Engineering College, Chandkheda, Ahmedabad, Gujarat, India, viralborisagar@yahoo.com

** E-Mail Id: ap1_mcwt@gtu.edu.in.*

Abstract: **-** Mobile ad hoc networks (MANETs) has received significant attention in the research domain of routing protocol as they provide security to transmit the data at the destination node. Mobile ad hoc networks do not have a fixed infrastructure, and nodes have random mobility due to this network topology changing dynamically and it vulnerable to external threats. Block hole and packet dropping are well-known network layer Denial of service attacks. during the route, discovery phase malicious nodes work normally and it became the shortest path to route the data and after that, it will drop all the data instead of transferring the data to the destination and in case of the packet dropping attack node drop the packet due to the elfishness of a node, Lack of energy resources, Bandwidth consumed by the attacker node, Overflow of the transmission queue, Misbehavior of a malicious node, it will drop the packet in the network. In this paper, we analyze the impact of both attacks on the AODV routing protocol in the random mobility environments with the different simulation parameters.

Keywords*: Ad-hoc network, Packet dropping attack (PDA), Blackhole attack (BHA), MANET (Mobile ad hoc network*

1. Introduction

In mobile ad hoc network nodes in the absence of any fixed infrastructure are randomly moved in the network with random mobility. Data is transmitted in the network through the intermediate node if the destination is not indirect transmission range. If any node would like to send the data, it broadcast the request to the neighbored node. Node checks destination address in its routing table. If the destination addresses are available in the neighbor node, then it transmits data directly. but if the receiver node is not in direct transmission range, then a similar request is propagated in the network to find the destination address then the source route

Power System Technology
ISSN:1000-3673
Received: 06-06-2024 Revised: 15-07-2024 Accepted: 28-08-2024

the data through the intermediate node or it transmits the data through multiple hops [1]. A node in the ad hoc network work as a host as well as the router to forward the data. Wireless ad hoc networks are classified into two categories: infrastructure-based and infrastructure-less [1].

Network centralized control in the infrastructure-based wireless network but in this case, the infrastructure-less network does not centralize controlled by the access point, all the node is randomly moved in the network. Ad hoc wireless is an example of the infrastructure-less network, it has the property of self-organizing, self-configuring & Self-Healing the network. Node moves randomly in the network with the random speed and direction due to this topology changing dynamically in the ad hoc network. Random mobility of the node and lack of the infrastructure, ad hoc network has challenges like scalability, quality of service, energy efficiency, and security [1]. Also due to the wireless medium, it has constrained links: dynamically changing Network topology, link bandwidth limitation, no centralized network management, and physical layer limitation.

Traditional routing protocol does not work efficiently in ad hoc networks because of the mobility of the node and infrastructure-less wireless medium. So, it is a challenging task to develop a routing protocol that overcomes such challenges and constrain. MANET has open access, due to this, it has vulnerable to external and internal attacks [2].

In this paper, we are going to discuss the Blackhole and packet dropping network layer attack in mobile ad hoc network and to analyze the effect on a wireless network using the AODV routing protocol through the different simulation parameters like the throughput, Packet Delivery Ratio, Packet Dropping Ratio, Routing overhead and End-to-End Delay.

The rest of the paper is organized as follows. Section 2 and Section 3 discuss the AODV routing protocol routing mechanism and attack in the network layer respectively. In Sect. 4, we discuss the simulation parameter setup. Section 5 provides a detailed analysis of our simulation results. Section 6 concludes the paper.

2. Manets Routing Protocol

To route the data in the mobile ad hoc network many researchers proposed routing protocol, and it is classified into three categories: Proactive, reactive, and hybrid routing protocol. In making the comparative analysis using the AODV routing protocol.

Ad hoc On-demand Distance Vector Routing Protocol:

AODV is the reactive improved form of the DSDV and DSR protocol. It merges the element of the DSDV and DSR routing algorithm. It transmits route requests when the sender node needs to broadcast the data, so it is called the on-demand protocol but in the case of the DSDV, it stored the network information at the node [3].

In the AODV protocol, to find the path it transmits the RREQ packet to all the neighbor nodes. Route request packet has the knowledge regarding the source and destination node. The routing node received the packet, it initially checks the address of the received node in the

Power System Technology
ISSN:1000-3673
Received: 06-06-2024 Revised: 15-07-2024 Accepted: 28-08-2024

routing table. If the destination node address is not available in the routing table, then it broadcast the packet to the neighbor node to find the destination node address [4].

Each node checks the table and if the destination node address is not available in the table, then it follows the same process until it finds the destination address and from the routing table receiver node sends the reply packet to the sender node [5].

3. Attack In Manets

In ad-hoc networks, nodes have dynamic mobility, and they transfer data through the wireless medium. The attacker or unauthorized user will be assessing data, modifying data, or destroying data in the network. Broadly categorized into two categories: Active attack, passive attack [5].

Passive attack: Passive attacker is honest; it does not modify the data in the network. It analyzes the network traffic, and it does not disturb the network operation. The passive attacker will access the data from the network [5]. Using the cryptographic or data encryption techniques, if data is converted to another format that understands only by the authorized user and it prevents the network from the passive attack [6].

Active attack: it modified the data in the network and to prevent the network from this attack, many attack detection, and mitigation techniques were proposed by the researcher. According to academic research databases like ACM Library, Xplore Digital Library, Science Direct, Wiley Online Library, and Springer Library layer-wise main attack summarized in Table 1:

Table 1: LayerWise Attack in MANET

Layers	Main Attacks
Physical layer	Jamming attack
Network layer	Wormhole attack, rushing attack, Blackhole attack, gray hole attack, Packet dropping attack, Sleep deprivation attack, and Sybil attack
Transport layer	SYN flooding attack, Man-in-the-middle attack
Application layer	Worm attack

In this paper, we analyze the network layer blackhole and packet dropping attack on the MANET AODV routing protocol.

Blockhole Attack

"By the falsification of sequence number or hop count, attacker become part of the route and then it will drop all the received packet"

If the source node wants to send the information, then it broad route request packet to the neighbored node. During the route detection process, the attacker replies to the source node with the shorted path and fakes a larger sequence number, So the source selects this path, and the attacker becomes part of the route. After that, it will drop all the received packets [6].

AODV routing protocol assumes that all the node in the network is trusted. Any normal node

Power System Technology
ISSN:1000-3673
Received: 06-06-2024 Revised: 15-07-2024 Accepted: 28-08-2024

checks routing before sending a route reply but the malicious node does not verify the routing table, so its response is faster compared to the normal node [6]. Also, it sends with less hop count. Source nodes select malicious node route reply with less hop count. It starts to transmit the data through the malicious node and completes the route discovery process. Malicious node drops all the received packets.

Packet Dropping Attack

"An attacker drops packets without an attempt to capture any route. This attack can be caused by low battery, overload condition, selfishness, or deliberately dropping packets"

Packet dropping attack is very challenging to identify because it happens in the network because of the node compromise for various reasons. There are various reasons behind stopping packets these are as follows [7]:

- Selfishness of a node
- Broken link.
- Lack of energy resources
- Bandwidth consumed by the attacker node.
- Overflow of the transmission queue.
- Misbehavior of a malicious node.

4. Simulation Parameters

Simulation-based Comparative analysis of the packet dropping and black hole attack using the Network Simulator 2 (NS2). Network Simulator 2 is used to develop the wireless network. We have considered the simulation parameters as given in table 1.

Table 2: Simulation Parameter

Simulation Parameter	Value
Simulator	NS-2.35
Routing Protocols	AODV
Network Area	800m x 800m
No. of nodes	10, 20, 30, 40, 50, 60, 70, 80, 90,100
Mobility Model	Random Mobility
Blackhole attack and Packet Dropping attack	1 Node
Speed	Min 1m/s to Max 30m/s
Pause Time	1s
Traffic Type	UDP
MAC Protocol	IEEE 802.11

Power System Technology
ISSN:1000-3673
Received: 06-06-2024 Revised: 15-07-2024 Accepted: 28-08-2024

Simulation Time	1800s

We compare the performance of different routing protocol AODV routing protocol with the black hole and packet dropping attack using the simulation parameter as mentioned in table 1.

As mentioned in table 1, We increase the number of mobile nodes in our simulation. In the first simulation setup, we crease ad hoc network with 10 nodes, and two nodes continuously communicate to each other with all the nodes having random mobility and one black hole & packet dropping attack present in the network [7].

5. Results Analysis

For the analysis of AODV routing protocol performance under the black hole and packet dropping attack, four performance parameters as discussed below:

Throughput: It characterizes the percentage of the number of packets reaching the reserve from the sender to the time is taken by the receiver to receive all the data.

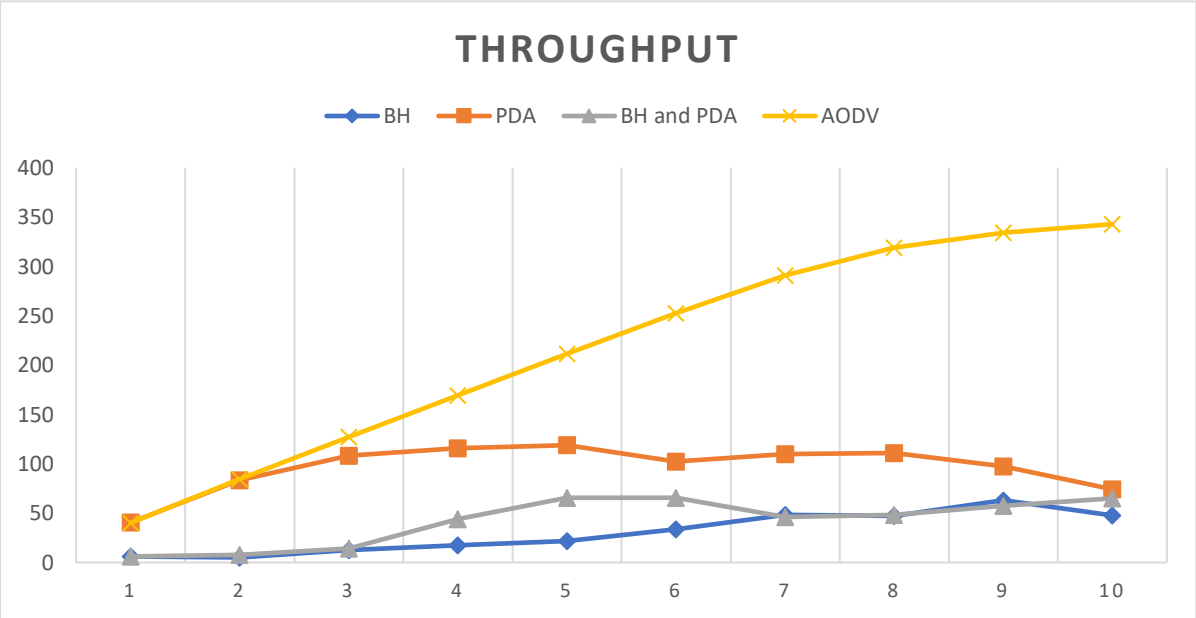

Figure 1:Throughput

Table 3: Throughput

No of Node	Throughput			
	AODV with BH	AODV with PDA	AODV with BH and PDA	AODV without Attack
10	68.423	40.57944	6.192	40.189
20	41.168	83.20917	7.594	84.607

Power System Technology
ISSN:1000-3673
Received: 06-06-2024 Revised: 15-07-2024 Accepted: 28-08-2024

30	63.227	108.1306	14.143	127.168
40	50.285	115.7272	44.002	169.568
50	59.409	118.8786	65.648	211.558
60	68.877	102.4303	65.648	252.542
70	62.74	109.7564	45.882	290.717
80	84.27	111.0114	48.241	318.901
90	71.201	97.29139	57.494	334.089
100	62.542	74.18306	64.788	342.873

Figure 1 and Table 1 show that the AODV routing protocol behaviors analysis under the presence of the black hole and packet dropping attack and if both attacks are present in the network at the time of protocol analyses.

As shown in the analysis blackhole attack will dop all the packets. Packet-dropping attacks will drop the smaller number of the packet compared to the blackhole attack because it will drop the packet due to the battery, overload condition, selfishness of the node. As shown in the table when 100 nodes are present in the network at the time throughput of the BH: 62.542, PDA: 72.18, BH & PDA: 64.78, and Without attack AODV: 342.873.

Packet Delivery Ratio

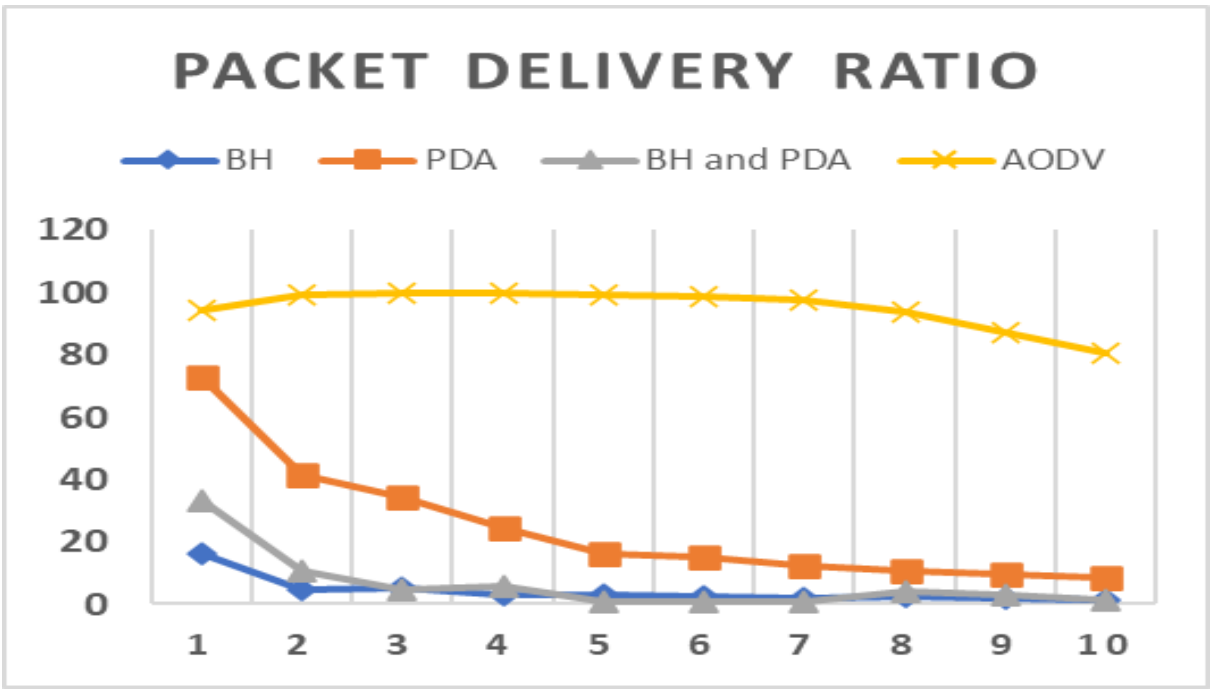

Figure 2: Packet Delivery Ratio

Table :4: Packet Delivery Ratio

	Packet Delivery Ratio

Power System Technology
ISSN:1000-3673
Received: 06-06-2024 Revised: 15-07-2024 Accepted: 28-08-2024

No of Node	AODV with BH	AODV with PDA	AODV with BH and PDA	AODV without Attack
10	16.086	72.952	33.015	94.462
20	4.837	41.651	10.729	99.412
30	4.952	34.247	4.717	99.663
40	2.954	24.211	5.722	99.633
50	2.792	16.19	0.928	99.413
60	2.697	15.005	0.982	98.906
70	2.107	12.387	1.025	97.586
80	2.475	10.86	4.156	93.633
90	1.859	9.561	2.908	87.194
100	1.47	8.323	1.522	80.567

Figure 2 and Table 2 show the packet delivery ratio of the AODV routing protocol under the presence of the black hole and packet dropping attack and both attacks are present in the network.

As shown in the figure the black hole attack will drop all the packets in the network. At the 10 number of the at the time it will deliver up to the 16.086 and at the 100 number of the node at the time it will deliver the packet up to the 1.47

Similarly, in the case of the packet dropping attack and if both the attack present in the network, it will deliver less number of the packet deliver (8.23 % at 100 nodes) compared the without the attack (80.56 % at 100 nodes) present in the network. When the PDA attack is present then it will not drop all the packets because it drops the packet due to the node selfishness and it is lesser than the BH but higher than the network without the attack.

Packet Dropping Ratio:

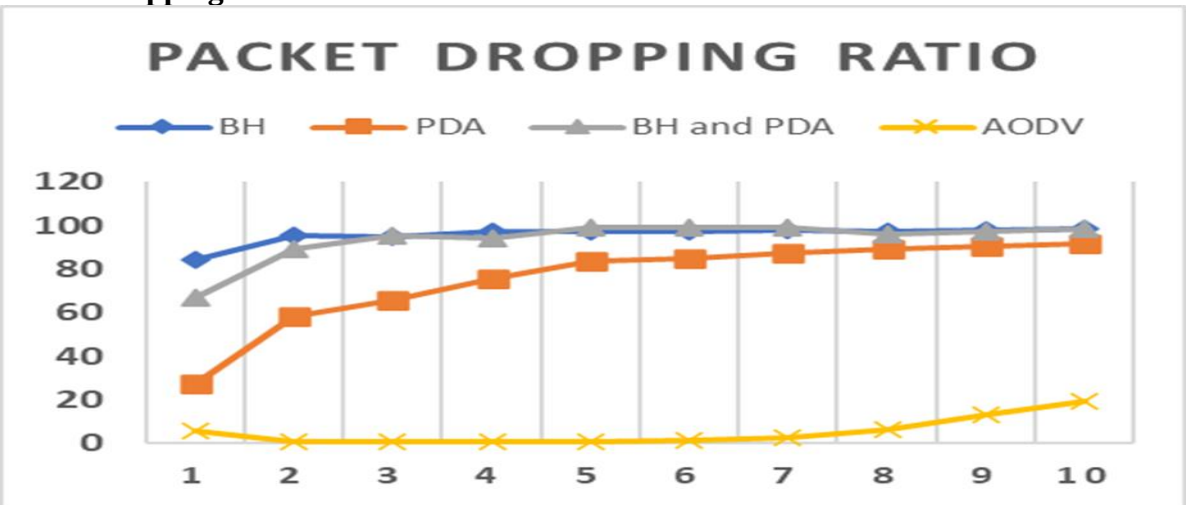

Figure 3: Packet Dropping Ratio

Power System Technology
ISSN:1000-3673
Received: 06-06-2024 Revised: 15-07-2024 Accepted: 28-08-2024

Table:5: Packet Dropping Ratio

No of Node	Packet Dropping Ratio			
	AODV with BH	AODV with PDA	AODV with BH and PDA	AODV without Attack
10	83.914	27.048	66.985	5.538
20	95.163	58.349	89.271	0.588
30	95.048	65.753	95.283	0.337
40	97.046	75.789	94.278	0.367
50	97.208	83.81	99.072	0.587
60	97.303	84.995	99.018	1.094
70	97.893	87.613	98.975	2.414
80	97.525	89.14	95.844	6.367
90	98.141	90.439	97.092	12.806
100	98.53	91.677	98.478	19.433

Figure 3 and Table 3 show the packet dropping ratio of the AODV routing protocol under the BH, PDA, BH & PDA and without the attack in the network.

Packet dropping ratio shows the vice-versa effect of the packet-delivery ratio of the network. Blackhole attack drops up to 98.141% at the No of nodes: 100) of the received packet but in the case of the packet dropping attack it will drop the less number of the packet 91.67 (No of node 100) as the attack characteristics and the same effect observed when both the attack present in the network.

Normalized routing overhead:

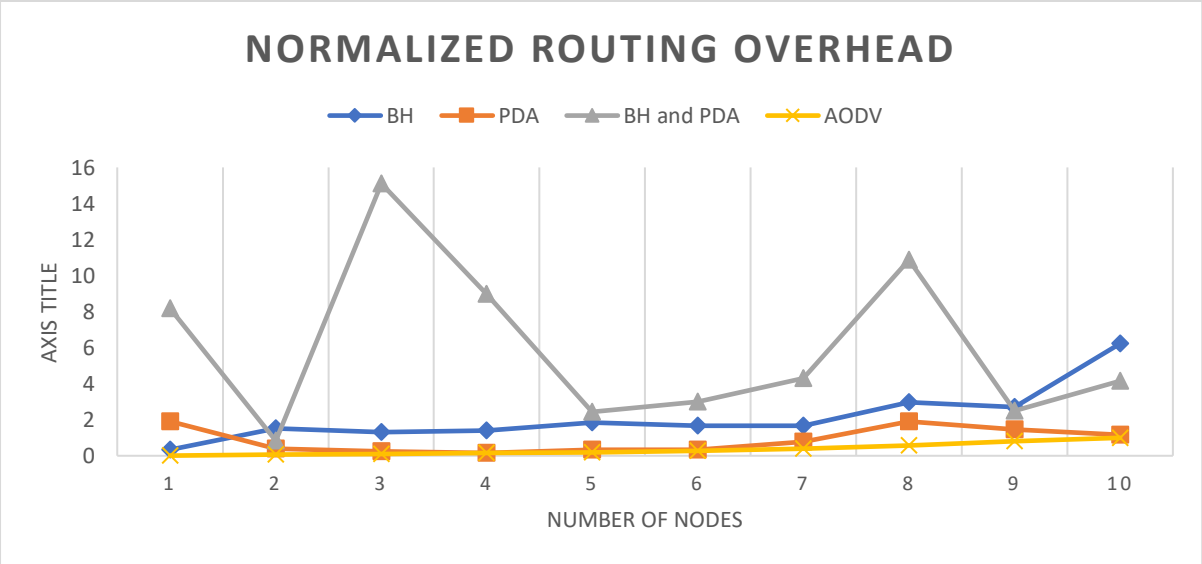

Figure 4: Normalized Routing Overhead

Power System Technology
ISSN:1000-3673
Received: 06-06-2024 Revised: 15-07-2024 Accepted: 28-08-2024

Table-6: Normalized Routing Overhead

No of Node	Normalized Routing Overhead			
	AODV with BH	AODV with PDA	AODV with BH and PDA	AODV without Attack
10	0.3334	1.9069	8.1888	0.0064
20	1.528	0.3768	0.8324	0.071
30	1.3078	0.2512	15.0994	0.1
40	1.3859	0.1545	8.9651	0.152
50	1.8404	0.3444	2.4335	0.197
60	1.6715	0.3392	2.9893	0.284
70	1.673	0.7694	4.2925	0.384
80	2.9544	1.8991	10.8681	0.558
90	2.687	1.4672	2.4973	0.808
100	6.2229	1.1752	4.1592	0.995

Figure 3 and Table 4 show the Normalize Routing Overhead of the AODV routing protocol under the BH, PDA, BH & PDA and without the attack in the network.

As shown in the table the routing overhead in the network increase due to the black hole attack and packet dropping attack behavior. At the 100 nodes in the network BH and PDA has the NRO= 6.22 and 1.17 respectively but at the same time, the AODV protocol has NRO= 0.995. also, a similar effect has been seen when the attacks are present in the network. Routing overhead very highly increases and decrease in the case of both the attack because of the large number of packets are dropped by the effect of both the attack and due to the mobility of the node, it also possible that sometimes any single attack present in the routing of the data and it decrease the overhead.

Conclusions

In this study, analyses the effect of the Blackhole (BH), Packet dropping attack, and if both the attack present in the large (i.e 100 nodes) mobile ad hoc network with the node having the random mobility. BH and PDA have been analyzed with the performance metrics such as throughput, packet delivery ratio, packet dropping ratio, end to end delay, and normalized routing overhead. As traffic increase with 100 mobile nodes the AODV protocol throughput 62.54, 74.18, and 64.78 for the network having the BH, PDA and BH & PDA respectively but without any attack network having the throughput at 100 nodes is 382.87. Blackhole attack will drop a maximum number of the packet and packet dropping attack will drop the less number compared to the BH because it drops the packet due to the node selfishness, Lack of energy resources, Bandwidth consumed by the attacker node, Overflow of the transmission queue and

Power System Technology
ISSN:1000-3673
Received: 06-06-2024 Revised: 15-07-2024 Accepted: 28-08-2024

Misbehavior of a malicious node, etc. but the packet dropping ration higher compared to the network without any attack.

Acknowledgement:

The authors are thankful to Dr Pranav B. Lapsiwala Sarvajanik College of Engg. & Tech. Surat, Gujarat and Prof. Hitesh Shah GCET, Vallabh Vidyanagar (Gujarat) valuable discussion for research work.

Funding: No funding is received for the research work.

Conflicts of interest: None

Reference

[1]. M. Imran, F.A. Khan, H. Abbas, et al., "Detection and prevention of black hole attacks in mobile ad hoc networks," in 2014 International Conference on Ad-Hoc and Wireless Networks (AdHocNets), pp. 111-122, Springer, 2014.
[2]. S. Biswas, T. Nag, and S. Neogy, "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET," in 2014 IEEE International Conference on Applications and Innovations in Mobile Computing (AIMoC), pp. 157-164, IEEE, 2014.
[3]. D. Djenouri and N. Badache, "Struggling against selfishness and black hole attacks in MANETs," Wireless Communications and Mobile Computing, vol. 8, no. 6, pp. 689-704, 2008.
[4]. E. Gerhards-Padilla, N. Aschenbruck, P. Martini, et al., "Detecting black hole attacks in tactical MANETs using topology graphs," in 2007 IEEE 32nd Conference on Local Computer Networks (LCN), pp. 1043-1052, IEEE, 2007.
[5]. M.Y. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," Computer Communications, vol. 34, no. 1, pp. 107-117, 2011.
[6]. H. Kim, R. Oliveira, B. Bhargava, et al., "A novel robust routing scheme against rushing attacks in wireless ad hoc networks," Wireless Personal Communications, vol. 70, no. 4, pp. 1-13, 2013.
[7]. AL. Shahrani and A. Saad, "Rushing attack in mobile ad hoc networks," in 2011 IEEE 3rd International Conference on Intelligent Networking and Collaborative Systems (INCoS), pp. 752-758, IEEE, 2011.
[8]. L. Tamilselvan and V. Sankaranarayanan, "Solution to prevent rushing attack in wireless mobile ad hoc networks," in 2006 IEEE International Symposium on Ad Hoc and Ubiquitous Computing (ISAUHC), pp. 42-47, IEEE, 2006.
[9]. G. Usha, M.R. Babu, and S.S. Kumar, "Dynamic anomaly detection using cross layer security in MANET," Computers and Electrical Engineering, vol. 59, pp. 231-241, 2017.

Power System Technology
ISSN:1000-3673
Received: 06-06-2024 Revised: 15-07-2024 Accepted: 28-08-2024

[10]. A. Nadeem and M.P. Howarth, "A survey of MANET intrusion detection and prevention approaches for network layer attacks," IEEE Communications Surveys and Tutorials, vol. 15, no. 4, pp. 2027-2045, 2013.
[11]. S. Jain and A. Khunteta, "Detection techniques of blackhole attack in mobile ad hoc network: A survey," in 2015 International Conference on Advanced Research in Computer Science Engineering and Technology (ICARCSET), pp. 1-5, ACM, 2015.
[12]. E. Amiri, H. Keshavarz, H. Heidari, et al., "Intrusion detection systems in MANET: A review," Procedia - Social and Behavioral Sciences, vol. 129, no. 2, pp. 453-459, 2014.
[13]. Mohebi, A., Scott, S.: A survey on detecting black-hole methods in mobile ad hoc networks. Int. J. Innovative Ideas. 13(2), 55–63 (2013)
[14]. Mandala, S., Abdullah, A.H., Ismail, A.S., Haron, H., Ngadi, M.A., Coulibaly, Y.: A review of blackhole attack in mobile ad hoc network. In: 3rd International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME), Bandung, pp. 339–344 (2013)
[15]. Tseng, F.-H., Chou, L.-D., Chao, H.-C.: A survey of black hole attacks in wireless mobile ad hoc networks. Hum. -Centric Comput. Inf. Sci. 1(4), 1–16 (2011)
[16]. Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., Nemoto, Y.: Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. Int. J. Netw. Secur. 5(3), 338–346 (2007)
[17]. Weerasinghe, H., Fu, H.: Preventing cooperative black hole attacks in mobile ad hoc networks: simulation implementation and evaluation. Int. J. Softw. Eng. Appl. 2(3), 39–54 (2008)
[18]. Djenouri D, Badache N. New power-aware routing for mobile ad hoc networks. The International Journal of Ad Hoc and Ubiquitous Computing (Inderscience Publisher) 2006; 1(3): 126–136.
[19]. Srinivasan V, Nuggehalli P, Chiasserini CF, Rao RR. Cooperation in wireless ad hoc networks. In The 22nd IEEE Annual Joint Conference on Computer Communications and Networking (INFOCOM'03), San Francisco, California, USA, April 2003.
[20]. David B, David A. Dynamic source routing in ad hoc wireless networks. In Mobile Computing (vol. 353), Imielinski T, Korth H (eds). Kluwer Academic: Norwell, MA, USA, 1996; 153–181.
[21]. Buchegger S, Le-Boudec J-Y. A robust reputation system for p2p and mobile ad-hoc networks. In Second Workshop on the Economics of Peer-to-Peer Systems, Harvard university, Cambridge, MA, USA, June 2004.
[22]. J.J. Garcia-Luna-Aceves, Marcelo Spohn, and David Beyer. Source Tree Adaptive Routing (STAR) Protocol (Internet-Draft). Mobile Ad hoc Network (MANET} Working Group, IETF, October 1999.
[23]. F. Stajano and R. Anderson. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. B. Christianson, B. Crispo, and M. Roe (Eds.)., Security Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science, 1999.

Power System Technology
ISSN:1000-3673
Received: 06-06-2024 Revised: 15-07-2024 Accepted: 28-08-2024

[24]. C.-K. Toh. Associativity Based Routing for Ad-Hoc Mobile Networks. Wireless Personal Communications Journal, Special Issue on Mobile Networking and Computing Systems, Vol. 4, No. 2, pp.103-139, March 1997.
[25]. W.R. Heinzelman, J. Kulik, H. Balakrishnan, Adaptive Protocols for Information Dissemination in Wireless Sensor Networks, ACM MobiCom99, pp. 174.185, 1999.
[26]. A. Perrig, J. Stankovic, and D. Wagner, Security in Wireless Sensor Networks, Communications of the ACM, 47(6), Special Issue on Wireless sensor networks, pp.53-57, Jun. 2004
[27]. B. Przydatek, D. Song, and A. Perrig, SIA: Secure Information Aggregation in Sensor Networks, 1st International Conference on Embed
[28]. A. Woo, T. Tong, and D. Culler, Taming the Underlying Challenges of Reliable Multhop Routing in Sensor Networks, ACM SenSys03, Nov 2003
[29]. D. Johnson, D.A. Maltz, and J. Broch, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (Internet-Draft), Mobile Ad-hoc Network (MANET) Working Group, IETF, Oct. 1999
[30]. Mr. Margam K. Suthar, Dr Ajay Kumar Vyas, Dharmendrasinh D Zala, "Development of HAODV algorithm for the multiple network layer attack detection and mitigation in the MANET", scopus indexed Journal of Computational Analysis and Applications, ISSN:1521-1398E-ISSN:1572-9206, Vol. 33 No. 06 (2024)
[31]. Dr. Margam Suthar, Dharmendrasinh D Zala, "Development of modified random waypoint mobility model of routing protocol for the mobile ad-hoc network", scopus indexed Power System Technology, ISSN: 1000-3673, Volume 48 Issue 1 (March 2024).
[32]. Mr. Margam K. Suthar, Dr Ajay Kumar Vyas, "Performance Investigation of Routing Protocol with the velocity of 30 m/s for Random Mobility Model", scopus indexed International Journal on Electrical Engineering and Informatics, Printed ISSN 2085-6830/ online e-ISSN 2087-5886, Volume 14, Number 2, June 2022.
[33]. Mr. Margam K. Suthar, Dr Ajay Kumar Vyas, "Implement and Analysis the Impacts of Multiple Attacks & Connections in AODV Routing Protocol on MANETs", scopus indexed Journal of Optoelectronics Laser, ISSN: 1005-0086, Volume 41 Issue 4, 2022.
[34]. Sharma Hitesh Omprakash, Margam K. Suthar,"Implementation of Black hole Attack for Random Mobility for Single and Multiple Connection in MANET", scopus indexed International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Vol. 9, Issue 03, 2019.