I.J. Wireless and Microwave Technologies, **2024, 3, 50-60**
Published Online on June 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2024.03.04

Improved Route Discovery Scheme under Blackhole Attack in MANET

Priyanka Pandey*
Department of Computer Science and Engineering, Harcourt Butler Technical University, Kanpur, India
E-mail: priyankapandey07@gmail.com
ORCID: https://orcid.org//0000-0001-5187-5796
*Corresponding author

Raghuraj Singh
Department of Computer Science and Engineering, Harcourt Butler Technical University, Kanpur, India
E-mail: rrsingh@hbtu.ac.in
ORCID: https://orcid.org//0000-0003-2360-8038

Received: 07 January, 2024; Revised: 12 February, 2024; Accepted: 14 March, 2024; Published: 08 June, 2024

Abstract: A Mobile Ad Hoc Network (MANET) consists of numerous wireless mobile devices. It is a self-organizing network and does not require any pre-established infrastructure. Communication between devices sets up without any dedicated centralized server. A malicious node takes advantage of this vulnerability and attempts to integrate into the network in order to lower its overall performance. In MANET, one of the most dangerous types of attacks is the blackhole node assault. In order to join the route, a node with blackhole assault wrongly sends route information to the source node during the route discovery process and degrades the network performance. In order to address this problem, a novel Blackhole Detection Algorithm (BHDA) has been proposed in this work. To determine the existence of blackhole nodes, the protocol takes into account various factors including number of route request packets (RREQ) received, number of RREQ packets forwarded, and number of route reply packets (RREP) transmitted by nodes throughout the route discovery process. Apart from this, each node maintains a local neighbourhood information and for that all neighbourhood node has to pass the check before becoming a neighbour. The simulation results prove that the proposed technique BHDA shows drastic improvement in network performance under blackhole attack.

Index Terms: MANET, Blackhole Attack, Routing, Security, AODV, Blackhole Detection.

1. Introduction

MANET is a wireless network in which mobile devices communicate among themselves through wireless links. It is a self-configuring network with no existence of centralized server. Thus, each device in the network operates without any central monitoring and controlling. It may be used in a wide range of applications, including disaster recovery operations, battlefields etc. without pre-existing infrastructure [1]. Some of the most popular routing protocols such as AODV [2], DSR [3], OLSR [4], DSDV [5] etc. are used in transmitting data packets from the source to the target. These kinds of protocols are further categorized as reactive and proactive. Reactive routing protocols construct the path only when needed. While, in proactive, each node has complete route information about other nodes in the network.

Due to the absence of centralized server, continuous node mobility and dynamic topology, these routing protocols are vulnerable to many types of attacks. A blackhole attack has shown its severe impact on network performance [6]. The description of blackhole attack has been given below.

Blackhole attack is one of the most dangerous attacks in MANET environment [7] Route discovery procedure which includes both normal and blackhole nodes is shown in Figure 1.

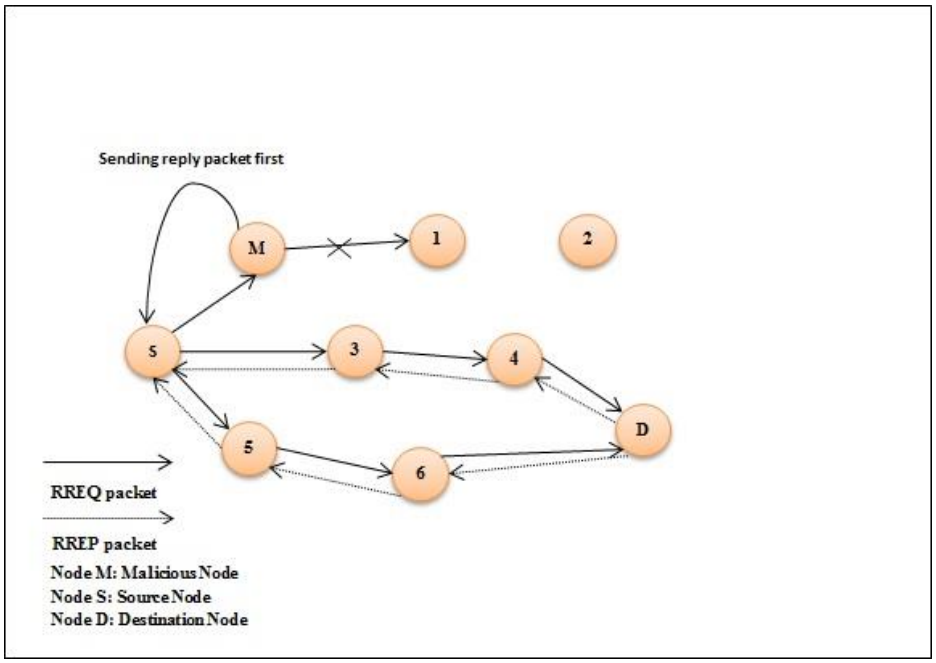

Fig.1. Route Discovery Operation

Such kind of malicious node gets activated during route discovery operation. After receiving RREQ packet, the malicious node abruptly increases sequence number and re-sets the hop count wrongly to a lower value. It then subsequently replies to the source node by sending RREP packet. This malicious node even does not enquire in its routing table. Due to this, the source node gets first response about the path from the malicious node and considers it as the most appropriate node to carry out data transmission process. Once the source node initiates the data transmission process, the blackhole node starts dropping all the received data packets. This degrades the performance of routing protocols in terms of packet delivery ratio, routing load, delay and throughput.

In this paper, a blackhole node has been launched on AODV routing protocol. Further, both schemes i.e. AODV with blackhole node attack and its proposed remediation technique i.e. BHDA have been analyzed after implementing them on the network simulator. In the proposed technique, during route discovery operation factors such as quantity of RREQ packets transmitted, quantity of RREQ packets received, quantity of RREP packets sent and trust value have been taken into account. The trust value of a node is used to identify its legitimacy. Any node with trust value as zero has to go through a check while maintaining the neighbourhood information. Thus, the suggested approach BHDA is able to reduce the adverse effect of such a malicious node.

The rest of the paper is organized as follows: Section 2 discusses about previous work proposed for preventing the network from blackhole attack. Section 3 elaborates the proposed BHDA technique which provides secure routing in AODV in the existence of blackhole node. Section 4 evaluates and analyzes the performances of both AODV protocol with blackhole attack and BHDA technique. Results have thoroughly been represented through graphs and the last section concludes this work alongside giving its future prospective.

2. Background

One of the worst malicious node assaults in a network is the blackhole attack. It leads to overall degradation of network performance specifically in MANET environment. During route discovery operation, malicious node gets activated and pretends itself as the most promising node. During routing operation it drops all the received data packets causing less delivery ratio, less throughput, more routing load and extra delay. In order to mitigate its impact on routing protocols, several works have been proposed. AODV routing protocol is often used in the MANET environment for transmitting data packets. However, when the blackhole node attacks on the network it degrades the overall network routing performance. The contribution by researchers to enhance the performance of such protocol is given in the subsequent part of this section.

Payal N. Raj et. al. [8] proposed a DPRAODV technique to detect and prevent a network from blackhole attack. The suggested method looks at whether or not the route reply packet's sequence number (SN) is over threshold. The node is thought to be malicious if the sequence number exceeds the threshold. This threshold value is modified dynamically. Results show improvement in performance. However, routing overhead is slightly increased. In order to improve the security of AODV, Nital Misty et. al. [9] proposed a technique which identifies a malicious node by modifying an operation of source node using an additional function. Results show improvement in PDR (Packet Delivery Ratio) and throughput, but with a higher delay. Work proposed in [10] detects a blackhole nodes using intrusion detetction technique and digital signature. The timestamp is used during IDS technique and malicious node is

detected by digital signature using key comparison. Simulation results show improved performance in terms of PDR and overhead. However, delay is higher.

Shweta Pandey et. al. [11] proposed a technique i.e. Secure AODV (SAODV) which makes use of Artificial Neural Network and SVM (Support Vector Machine) for the discovery of blackholes. SVM ensures that new operation of new path is same as earlier path and ANN is used for the classification of malicious node. Results showed improved performance. However, control overhead has not been considered for analysis. Similarly the scheme presented in [12] mitigates blackhole attack using firefly and artificial neural network techniques. Working of firefly algorithm depends upon light intensities and degree of attractiveness of flies. Results show improved delay, throughput and PDR. Another technique suggested in [13] uses Hidden Markov Model (HMM) for detection of blackhole nodes. After simulation, results show improvement in PDR and delay. However, routing overhead has not been analyzed.

In [14], Srijan Shrestha et. al. proposed a technique based on sequence number for detection of blackhole. During route reply phase, if an abrupt rise is seen in sequence number, the source node again broadcasts the RREQ packet with the destination sequence number set equal to the received RREP sequence number. If received number shows higher increments, then the node is detected as malicious. Results show improvement in terms of throughput and PDR. However, delay performance has not been considered for analysis.

In [15], authors proposed fuzzy based intrusion detection system which identifies the presence of both blackhole and greyhole nodes in the network. The proposed detection system consists of four modules i.e. extraction of parameters, fuzzy inference part, decision module and response module. Simulation results prove that the blackhole attack affects the network performance more as compared to the greyhole. By applying the proposed strategy, performance is improved in terms of PDR and routing overhead. However, delay has not been analyzed. Vidya Kr. Saurabh et.al. [16] presented a cluster based technique to detect the presence of blackhole attack in the network. Energy node in the cluster sends the message to its cluster head about the difference between data received and forwarded. If fault is detected, the particular node is isolated from the network. Results give improved performance in terms of delay and packet delivery ratio. However, normalized routing load performance has not been considered for analysis.

Enhanced Blackhole Resistence (EBR) [17] detect and resist blackhole nodes. It uses the Time To Live (TTL) and Round Trip Time (RTT) factors to determine the existence of blackhole attacks. The algorithm preserves energy and gives better performance. However, the proposed approach has not been analyzed in highly dynamic network environment. Anant Ram [18] proposed a dynamic threshold based blackhole detection approach. The scheme, examines the sequence number in the route reply message and compares against threshold. If it is greater than or equal to threshold, the node is considered as a part of routing path. Throughput and PDR performance has shown improvement. However, other performance metrics such as delay and control overhead has not been considered for analysis.

Varun Talati et. al. [19] proposed a technique which minimizes the effect of blackhole attack. When the node receives second route reply packet, a check is initiated based on broadcasted and sequence number. If the difference between both messages is greater than half of the highest possible sequence number, the packet is discarded. Results show improved performance. However, performance in terms of delay has not been analyzed. The work presented in [20] uses the reliability factor value to identify the malicious node in the network. The reliability value is compared to the threshold by the source node upon receiving the route reply packet; if it is less, a false RREQ packet is sent to identify malicious node. If the response is received from the node, the particular is considered as malicious and discarded from the route. Simulation results show improvement in performance. However, routing load has not been considered for analysis.

From the literature review it is revealed that several approaches have been proposed to minimize the impact of blackhole node in AODV routing protocol. However, performance has not been improved in all major aspects such as delivery ratio, routing load, throughput and delay. For instance, either the delay is higher i.e. [9, 10] or has not been considered for analysis [14, 15], [19]. In [8] routing load is more or in [16] and [20] it has not been considered during performance evaluation. The approach presented in this work aims to improve performance of routing protocol in all major aspects.

3. Proposed Scheme for Blackhole Mitigation

The proposed technique i.e. Blackhole Attack Detection Algorithm (BHDA) aims to mitigate impact of blackhole attack on routing protocol in MANET environment. In this paper, an AODV routing protocol has been considered as the basic mechanism of data transfer in which, when the source node needs to send a packet to the goal node, it first enquires in its routing table. If a path to the goal node exists, the source node starts forwarding data packets. Otherwise, a route discovery process gets initiated.

3.1 Route Discovery Operation:

During route discovery operation, if any blackhole node attacks in the network, the node tries to acquire all the data packets by pretending itself as the most promising node for data transmission. After receiving RREQ packet, it sets the value of hop count as 1 and abruptly increases the sequence number. Later, when the source node receives RREP

packet, it starts transmitting data packets destined towards malicious node. Consequently, the malicious node starts dropping all received data packets leading to degradation in network routing performance.
In order to identify the presence of such kinds of harmful nodes, in this work, a new approach i.e. Blackhole Node Detection Algorithm) has been proposed. Each network node's trust value is initialized to zero. In addition, the technique keeps track of how many RREQ packets are forwarded, how many RREQ packets are received and how many RREP packets are sent by a particular node.

Whenever a node receives an RREQ packet, it goes through a check in which total number of RREQ packet forwarded is examined. If the value is greater than threshold (in this work it is set to 10), trust value of a node is changed to 1. The node having trust value 1 is considered as a legitimate node and hence can take part in route discovery operation. The Algorithm 1 shows the whole sequence of operation during forwarding of RREQ packets.

Algorithm 1: Process during route discovery operation

1) *If an Intermediate node receives RREQ packet.*
If (Packet == RREQ)
// Increase the count of RREQ Packet received (RREQR)
RREQR++
// Check the number of route request packet forwarded RREQPF against threshold value $RREQPF_{TH}$
If (RREQPF > $RREQPF_{TH}$*)*
// Set the trust value as 1.
Trust_Value =1
Else
Value remains same i.e. 0
Update the routing table
Increase the hop count and destination sequence number
//At last, before forwarding RREQ packet increase the value of number of RREQ packet forwarded (RREQPF).
RREQPF++
End
2) *If source Node receives RREP packet.*
Estimate the difference (DSS_{Diff}*) between destination sequence numbers stored in RREP packet received and routing table.*
// Compare the difference (DSS_{Diff}*) against threshold (*DSS_{TH}*).*
If (DSS_{Diff} *>* DSS_{TH}*)*
Drop the packet.
Else
Forward the packet.
End.

After receiving route reply packet, the source node checks the difference between sequence number present in the RREP packet and in its routing table. If the difference exceeds the threshold, the received route reply packet is dropped.

3.2 Neighbour Table Updating:

In order to update information about neighbour node, each node sends a hello message continuously. If the message is received for the first time, a sender node is added to the table. Otherwise, its expiration time is updated in the neighbour table.

In the proposed technique, a slight modification has been done in order to keep the list of trusted node. Upon receiving a hello message, the sender with a trust value of 1 is immediately added to the neighbour table. On the other hand, sender node with a trust value zero has to go through an examination before being added to the table. The whole process is shown in Figure 2.

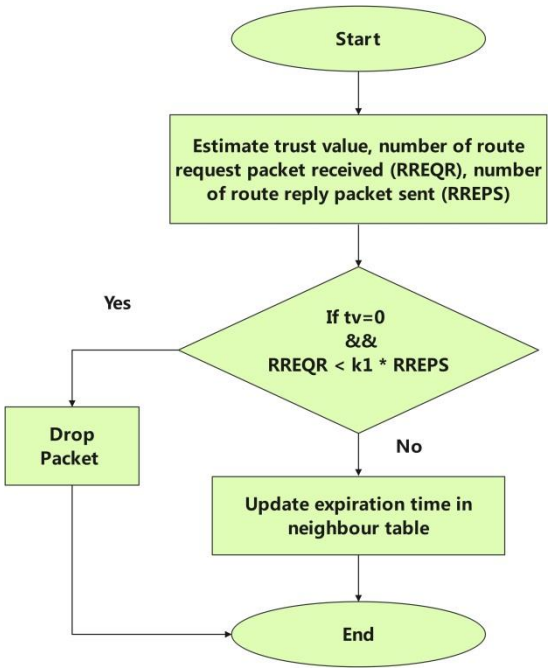

Fig.2. Maintenance of Neighbourhood Information

After receiving hello message, a receiving node estimates trust value (tv), number of route request packet received (RREQR) and number of route reply packet sent (RREPS). Information about the transmitting node is immediately added to the table if the trust value is one; if not, a check is made. If the variable, or k1* RREPS, where k1 is the multiplication factor, is greater than the value of RREQR, the hello packet is dropped, otherwise, the table is updated.

4. Simulation Overview

In this paper, for validating the effectiveness of proposed BHDA approach, network simulator NS2.35 [21] has been used. Nodes are randomly distributed in the region of 700 m x 800 m. For node mobility RWP [22] mobility model is used. In the network one of the normal nodes has been chosen as a blackhole node. Two ray radio propagation model [23] and Constant Bit Rate traffic type are used during implementation. The network performance has been analyzed at speeds 5, 10, 15, 20 and 25m/s and by varying number of nodes as 20, 40, 60, 80 and 100.

The performance of AODV with blackhole and after applying BHDA has been evaluated in terms of packet deliver ratio (PDR), packet loss ratio (PLR), throughput, routing load (NRL) and delay. In this paper, the blackhole node has been launched in such a way that in initial 3 seconds it acts as a normal node and after that it starts behaving as a blackhole node. The main simulation parameters considered during implementation have been shown in the Table 1.

Table 1. Simulation Parameters

Simulation area	700 x 800 m
Simulation time	120 seconds
Propagation model	Two ray ground
MAC type	IEEE 802.11
Mobility speeds	5, 10, 15, 20 and 25 m/s
Number of nodes	20, 40, 60, 80 and 100
Pause time	5.0 seconds
Protocols	AODV with blackhole, BHDA
Traffic Type	CBR

Performance of the protocols has been evaluated using aforementioned performance metrics and results obtained after simulation has been discussed in the next section.

5. Result Analysis

In this section, results obtained after simulation have been represented through graphs. These results are obtained on the basis of different network conditions i.e. by varying number of nodes as 20, 40, 60, 80 and 100 and by varying node speed as 5, 10, 15, 20 and 25 m/s.

5.1 Packet Delivery Ratio (PDR)

As shown in Figure 3, average PDR on varying number of nodes in case of AODV with blackhole node is about 28.07% while it is 56.15% in BHDA which proves that the PDR is improved twice against the AODV under blackhole attack.

PDR performance has also been evaluated on varying mobility speed and represented in Figure 4. As per the results, the average PDR of AODV with blackhole is 27.91% while by applying BHDA on AODV it is 66.07% which shows drastic improvement in performance. This is due to the fact that the proposed work examines the legitimacy of node during route request packet forwarding.

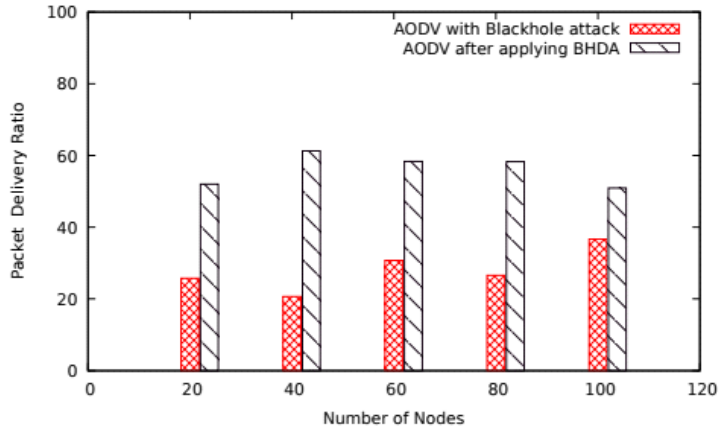

Fig. 3. Number of Nodes Vs PDR

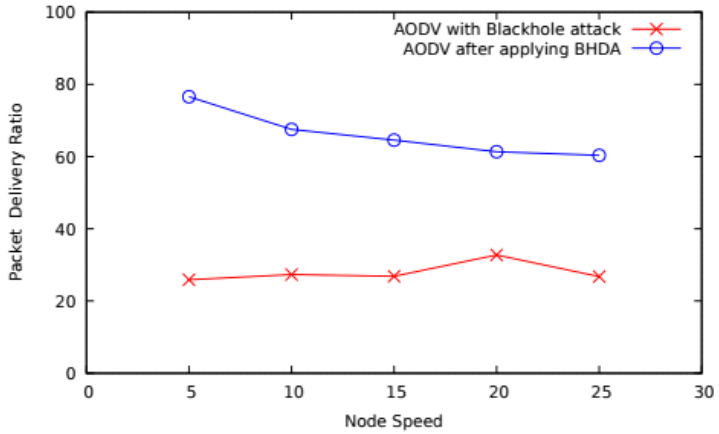

Fig. 4. Node Speed Vs PDR

5.2 Packet Loss Ratio

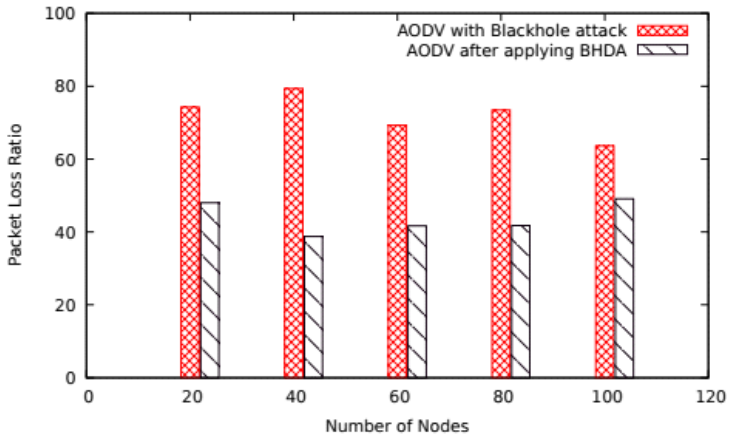

Fig.5. Number of Nodes Vs PLR

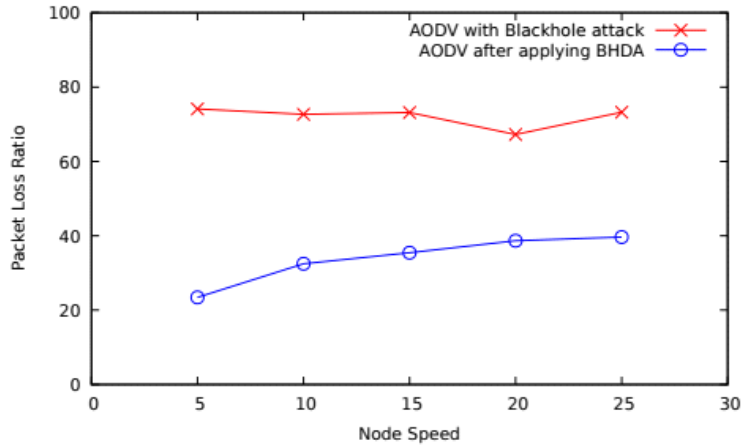

Fig.6. Node Speed Vs PLR

The average PLR on varying number of nodes in presence of blackhole node in AODV as depicted in Figure 5 is about 71.93% which after applying BHDA is reduced to 43.85%. Hence, the scheme proves overall 39% of improvement.

On varying mobility speed as shown in Figure 6 the proposed BHDA has shown 52.93% reduction of average PLR as compared to AODV in presence of blackhole node. This is because, the scheme is able to effectively identify and isolates blackhole node during route discovery and local neighbourhood maintenance operation.

5.3 Throughput

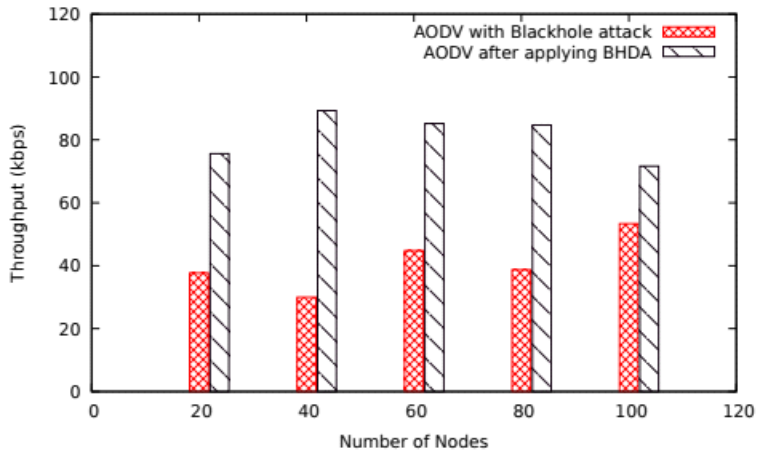

Fig.7. Number of Nodes Vs Throughput

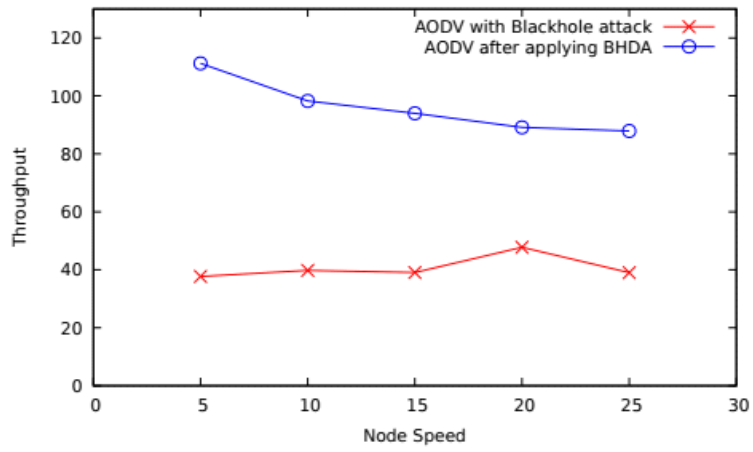

Fig.8. Node Speed Vs Throughput

The graphs represented in Figure 7 and Figure 8 show throughput performance by varying number of nodes and speed respectively. The throughput on varying number of nodes in case of AODV with blackhole attack is about 40.89% while in BHDA it is 81.28%. Overall, on average 98.77 % of improvement has been achieved.

On varying mobility speed average throughput of BHDA has been improved to 136.26% against AODV with blackhole attack. This is because the scheme discards the malicious node by identifying and isolating it during route discovery operation.

5.4 Normalized Routing Load

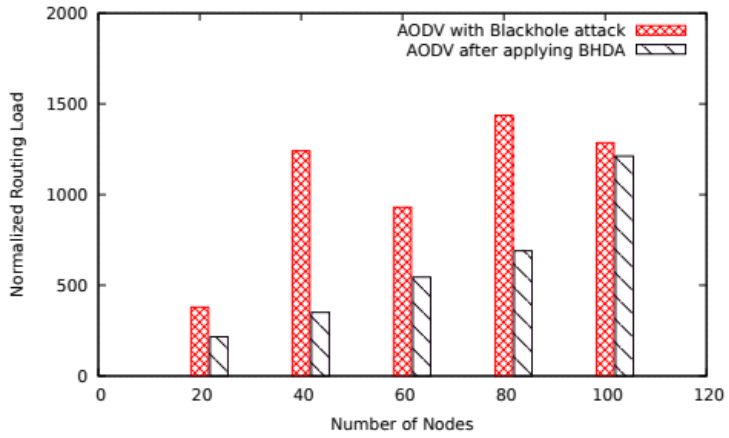

Fig.9. Number of Nodes Vs NRL

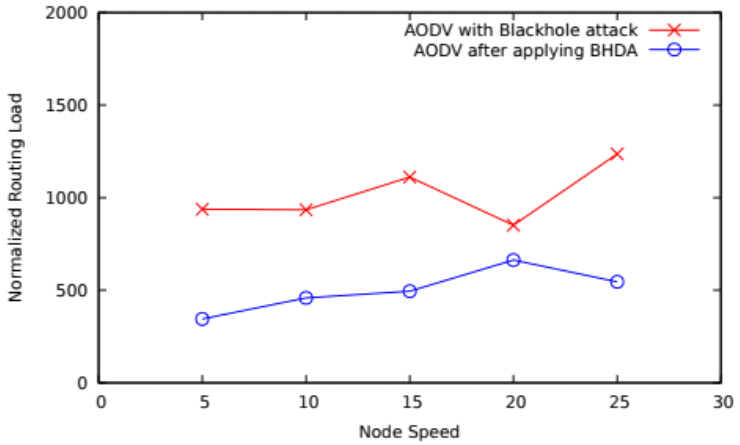

Fig.10. Node Speed Vs NRL

The proposed approach is able to minimize routing load which basically represents total number of control message required in transmitting a single data packet. From the Figure 9 it can be concluded that on varying number of nodes, the BHDA is able to minimize up-to 42.88% of routing load on the network as compared to the AODV with blackhole attack.

On varying mobility speed as depicted in Figure 10, the average routing load of BHDA has been reduced to 50.56% as compared to the other one. This is because; the scheme effectively detects malicious node and thus leading less number of incorporation of control message.

5.5 End to end delay

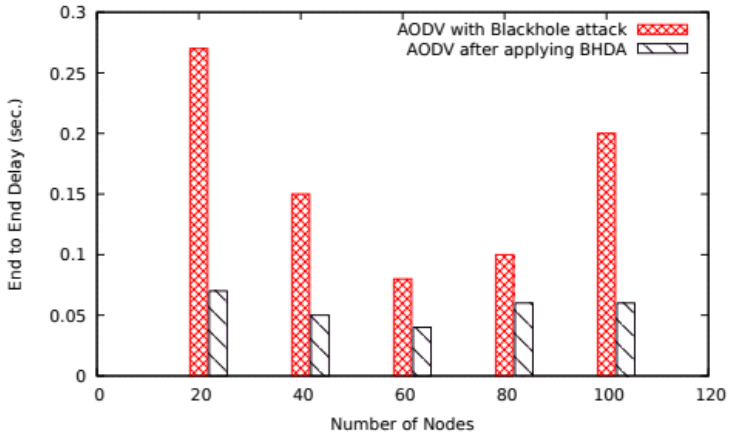

Fig.11. Number of Nodes Vs Delay

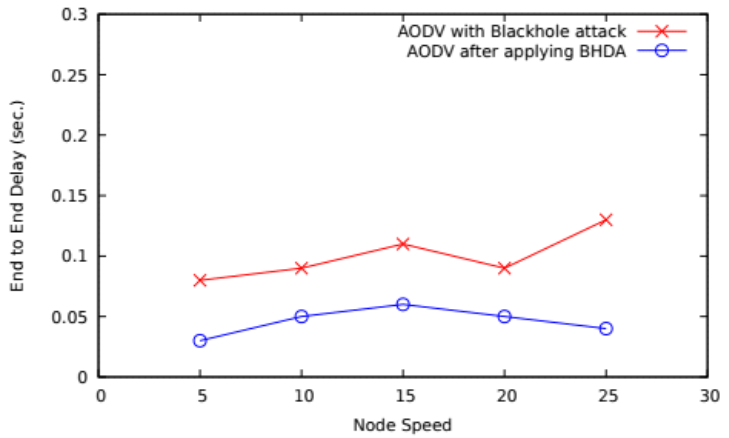

Fig.12. Node Speed Vs Delay

As shown in Figure 11, on varying number of nodes, the scheme BHDA is able to reduce delay up-to 62.5% as compared to AODV with blackhole. Similarly, on varying mobility speed, the performance of both schemes has been represented in Figure 12. The proposed scheme BHDA is able to minimize the delay up-to of 50% as compared to AODV with blackhole.

6. Conclusion

In this paper, a new BHDA approach for mitigating the impact of blackhole attack has been presented. A blackhole node has been launched in the network which on receiving RREQ packet pretends itself as the legitimate node and tries to acquire all data packets. After receiving the data packets, it starts dropping them. The proposed approach has been designed in such a way that during route discovery and maintenance of local connectivity information, it identifies this kind of node. In this scheme, at the time of route discovery process, a trust value based on number of RREQ packet forwarded is used to indicate legitimate node. When updating local connectivity information, nodes with zero trust value are identified as legitimate nodes based on characteristics such as the number of RREQ and RREP packets they send. Simulation results show significant improvement in performance in terms of PDR, PLR, NRL, throughput and delay as compared to the AODV with blackhole node. In future we will try to improve routing performance under other attacks such as grayhole, wormhole, Sybil attacks etc.

References

[1] Loo, J., Lloret Mauri, J., & Hamilton Ortiz, J. (2011). Mobile ad hoc networks: current status and future trends.
[2] Perkins, C., Belding-Royer, E., & Das, S. (2003). RFC3561: Ad hoc on-demand distance vector (AODV) routing.
[3] Johnson, D. B., Maltz, D. A., & Broch, J. (2001). DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. Ad hoc networking, 5(1), 139-172.
[4] Clausen, T., & Jacquet, P. (Eds.). (2003). RFC3626: Optimized link state routing protocol (OLSR).
[5] Perkins, C. E., & Bhagwat, P. (1994). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. ACM SIGCOMM computer communication review, 24(4), 234-244.

[6] H. Moudni, M. Er-rouidi, H. Mouncif and B. El Hadadi, "Performance analysis of AODV routing protocol in MANET under the influence of routing attacks," 2016 International Conference on Electrical and Information Technologies (ICEIT), Tangiers, Morocco, 2016, pp. 536-542, doi: 10.1109/EITech.2016.7519658.
[7] Sharma, S., & Gupta, R. (2009). Simulation study of blackhole attack in the mobile ad hoc networks. Journal of Engineering Science and Technology, 4(2), 243-250.
[8] Raj, P. N., & Swadas, P. B. (2009). Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet. arXiv preprint arXiv:0909.2371.
[9] Mistry, N., Jinwala, D. C., & Zaveri, M. (2010, March). Improving AODV protocol against blackhole attacks. In international multiconference of engineers and computer scientists (Vol. 2, No. 6, pp. 1-6).
[10] Talukdar, M. I., Hassan, R., Hossen, M. S., Ahmad, K., Qamar, F., \& Ahmed, A. S. (2021). Performance improvements of AODV by black hole attack detection using IDS and digital signature. Wireless Communications and Mobile Computing, 2021, 1-13.
[11] Pandey, S., & Singh, V. (2020, July). Blackhole attack detection using machine learning approach on MANET. In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 797-802). IEEE.
[12] Rani, P., Kavita, Verma, S., Rawat, D. B., & Dash, S. (2022). Mitigation of black hole attacks using firefly and artificial neural network. Neural Computing and Applications, 34(18), 15101-15111.
[13] Kalkha, H., Satori, H., & Satori, K. (2019). Preventing black hole attack in wireless sensor network using HMM. Procedia computer science, 148, 552-561.
[14] Shrestha, S., Baidya, R., Giri, B., & Thapa, A. (2020, March). Securing blackhole attacks in MANETs using modified sequence number in AODV routing protocol. In 2020 8th International Electrical Engineering Congress (iEECON) (pp. 1-4). IEEE.
[15 Abdel-Azim, M., Salah, H. E. D., & Eissa, M. E. (2018). IDS Against Black-Hole Attack for MANET. Int. J. Netw. Secur., 20(3), 585-592.
[16] Saurabh, V. K., Sharma, R., Itare, R., & Singh, U. (2017, April). Cluster-based technique for detection and prevention of black-hole attack in MANETs. In 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA) (Vol. 2, pp. 489-494). IEEE.
[17] Kancharakuntla, D., & El-Ocla, H. (2022). EBR: Routing Protocol to Detect Blackhole Attacks in Mobile Ad Hoc Networks. Electronics, 11(21), 3480.
[18] Ram, A., Kulshrestha, J., \& Gupta, V. (2021). Secure routing-based aodv to prevent network from black hole attack in manet. In Proceedings of 6th International Conference on Recent Trends in Computing: ICRTC 2020 (pp. 633-642). Springer Singapore.
[19] Talati, V., Thorat, M., Yadav, K., & Mane, R. (2021). Detection and Prevention of Blackhole Attack in MANET Network, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056,Volume(08), Issue(05)
[20] Gupta, P., Goel, P., Varshney, P., & Tyagi, N. (2019). Reliability factor based AODV protocol: Prevention of black hole attack in MANET. In Smart Innovations in Communication and Computational Sciences: Proceedings of ICSICCS-2018 (pp. 271-279). Springer Singapore.
[21] Issariyakul, T., Hossain, E., Issariyakul, T., & Hossain, E. (2009). Introduction to network simulator 2 (NS2) (pp. 1-18). Springer US.
[22] Bettstetter, C., Hartenstein, H., & Pérez-Costa, X. (2004). Stochastic properties of the random waypoint mobility model. Wireless networks, 10, 555-567.
[23] Sarkar, T. K., Ji, Z., Kim, K., Medouri, A., & Salazar-Palma, M. (2003). A survey of various propagation models for mobile communication. IEEE Antennas and propagation.

Authors' Profiles

Priyanka Pandey received her B. Tech. and M. Tech. degree in Computer Science and Engineering from Dr. A.P.J. Abdul Kalam Technical University, Lucknow. She is completed Ph.D. in Computer Science and Engineering, Harcourt Butler Technical University, Kanpur, India. Her research area is Mobile Ad hoc Network and has published research papers in reputed journals and conferences.
Email: priyankapandey07@gmail.com

Raghuraj Singh received his Ph.D. degree from U. P. Technical University, Lucknow, India in 2006 and M. S. from BITS, Pilani, India in 1997. He has received B. Tech. in Computer Science and Engineering from Harcourt Butler Technological Institute, Kanpur, India in 1990. He is currently working as Professor at Computer Science and Engineering, Harcourt Butler Technical University, Kanpur, India. His research interest includes Software Engineering, Human Computer Interaction and Mobile Ad hoc Networks. Dr. Singh has published about 140 research papers in International Journals and Conferences including IEEE, Springer etc.
Email: rrsingh@hbtu.ac.in

How to cite this paper: Priyanka Pandey, Raghuraj Singh, "Improved Route Discovery Scheme under Blackhole Attack in MANET", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.14, No.3, pp. 50-60, 2024. DOI:10.5815/ijwmt.2024.03.04