Development of HAODV algorithm for the multiple network layer attack detection and mitigation in the MANET

Margam Suthar[1], Ajay Kumar Vyas[2], Dharmendrasinh D Zala[3]*

[1]Assitant Professor, School of Engineering and Technology, Gujarat Technological University, Ahmedabad, Gujrat, India
[2]Assistant Professor, Adani Institute of Infrastructure Engg, Gujarat Technological University, Ahmedabad, Gujrat, India
[3]Assitant Professor, Department of Information and Communication Technology, Marwadi, University
Email : ap1_mcwt@gtu.edu.in
*Corresponding Author

Received: 19.04.2024 Revised : 20.05.2024 Accepted: 23.05.2024

ABSTRACT

Mobile nodes in mobile ad hoc networks (MANETs) move at random, are decentralized, and allow multi-hop communication by communicating between source and destination nodes via intermediary nodes. As a result, mobile ad hoc networks are vulnerable to a variety of assaults, such as wormhole attacks, rush attacks, black hole attacks, gray hole attacks, packet dropping attacks, sleep deprivation attacks, Sybil attacks, and others. Because of the ad hoc network's lack of infrastructure, the developed secure routing system for data transmission drew a lot of attention from the scientific community. The cutting-edge routing protocol HAODV (Hybrid Ad-Hoc On-Demand Distance Vector Protocol) was developed for various network-layer active packet dropping attack detection and mitigation and is based on a single-point detection approach.In this study, the influence of a random mobile environment with random mobility for 1800 seconds was compared to the performance of the routing protocol for large wireless ad hoc networks (100 nodes), producing ten different results for each node set. Packet delivery ratio, throughput, packet dropping ratio, routing overhead, and end-to-end delay quality of service (QoS) measurements are all included in the comparison. According to the simulation results, black hole and packet dropping attacks violate protocol standards and dramatically harm the functionality of good behavior protocols, resulting in throughput drops of up to 81% and network disruption. A single-point attack detection system was used in the development of the HAODV routing protocol to identify various attack types (BH and PDA attacks). The network's throughput and packet delivery ratio are now 90% and 82%, respectively.

Keywords: Ad hoc network; Routing Protocol; Random Waypoint Mobility; Throughput, Ad-hoc On-demand Distance Vector.

1. INTRODUCTION

The nodes in a wireless ad hoc network are self-configuring, self-locating, and communicate over the wireless link; the network has no fixed infrastructure [1]. In mobile ad-hoc networks (MANETs), mobile nodes move arbitrarily, carry out scattered operations, and communicate with one another via intermediary nodes to enable multi-hop communication. The two nodes will communicate the data directly if they are within the transmission range when it comes to data transfer. The use of ad hoc networks has increased during the previous few years. Currently, there is a lot of academic interest in developing efficient networking protocols for end-to-end wireless communication [2–3].

Proactive, reactive, and hybrid are the three categories used to classify routing protocols [4]. Because nodes in the MANET are connected via wireless links, the network has bandwidth limits, unpredictable link capacity, limited security, energy constraints, noise interference, and a variety of other issues. Mobile ad hoc networks are consequently subject to a wide variety of attacks, including wormhole, rush, black, gray, packet dropping, sleep deprivation, Sybil, and many others [4][5]. Through the use of single-point data collection, many scholars have developed techniques for identifying active packet-dropping network layer attacks. It provides real-time security in MANET by collecting security-related data for a given attack and routing protocol to react accordingly when malicious activity is detected in the network. HAODV is a novel routing protocol created for various network-layer active packet-dropping attack detection and mitigation. It is based on a single-point detection technique [7]. The overhearing-based strategy, despite it adding significant network routing cost, is used to detect packet-dropping assaults [8][9].

Overcome the disadvantage of the overhearing-based technique by determining the misbehavior tolerance value for the network efficiently using the Bayesian Approach [10].Simulation-based comparison of routing protocol performance for a small and dense network (100 nodes) under the impact of various packet-dropping attacks with the number of connections for 1800 seconds. Metrics including packet delivery ratio, throughput, packet dropping ratio, routing overhead, and end-to-end delay are included in the comparison.In the same environment, a comparison analyzed the performance of the HAODV and AODV (Ad-Hoc On-Demand Distance Vector Protocol) routing protocols using multiple performance metrics [11]. The AODV routing protocol provides more consistent performance than other routing protocols, but its performance suffers as a result when multiple packet-dropping attacks happen in the network.The HAODV routing protocol provides an advanced malicious node identification and isolation mechanism while also preserving Throughput, End-to-End Delay, and packet delivery ratio, and the simulation results are very close to the native AODV. Packet dropping ratio, throughput, delivery ratio, routing overhead, and end-to-end delay were the performance metrics utilized by the NS2.35 version to assess the ad hoc routing protocol's performance [12][13][14]. The article is divided into five sections: the compressive research of the Overhearing-based scheme, A Bayesian technique for the Reputation System 2, HAODV algorithm, 3. Experiment Workresults from analysis in section 4, and the conclusion in section 5.

2. Overhearing-based scheme

The researcher proposes Watchdog and path-rater techniques in [15] [16] [17] for the identification and prevention of malicious nodes in the MANET. The promiscuous mode is included in an overhearing-based system in which the node monitors the activities of the neighbor node and decides whether or not to transfer the packet to the other node. If the neighbor acts as a normal node and forwards the packet, the data packet is erased from the node's buffer [18] [19].

The malicious node activity detected by the source node and their misbehavior rate increase up to the threshold value when a data packet is only available in the buffer for a limited time. When the threshold value is reached, the node announces itself to be the malicious node. By avoiding the malicious node, the source node seeks another path utilizing the Path-rater. Path-rater keeps track of every path rate in its cache. The node's misbehavior is also known as the node's reputation, and the reputation system is calculated using the Bayesian Approach [20].

The Reputation System using a Bayesian approach: Reputation is an indication of a node's efficiency in forwarding data to subsequent nodes [21]. Observer nodes increase or reduce the node's reputation depending on the amount of data forwarded [21]. Packets are dropped by the node due to malicious activity or a variety of other factors such as collision, link bandwidth, or node mobility. As a result, the threshold of tolerance for node misbehavior must be determined [22].

A Bayesian strategy for the Reputation System constantly analyses node behavior and detects misbehaving activities. If the node efficiently forwards the data packet, its reputation value grows; otherwise, the reputation value decreases due to intentionally or unintentionally discarding the packet [22] [23]. Because the observer node only maintains updated information, memory does not need to store all of the observations [24] [25].

A Bayesian framework to Analise the misbehavior of the nodes [24] [25]: Node A keeps an eye on node B's actions. Node A assumes that the result may be inferred independently from one observation to the next and that node B behaves erratically in terms of probability because of the parameter [24]. By assuming that the parameter is drawn in accordance with a distribution that is updated when additional observations are made, Node A represents the uncertainty surrounding the parameter [25]. The traditional Bayesian framework is presented here.

A random variable estimated by a Beta distribution Beta (m,n) [25] is used to estimate the likelihood that each node A believes that each other node B is acting inappropriately.

The Probability Density Function (PDF) for a Beta $x \sim \mathrm{Beta}(m, n)$ is [25]:

$$f(x) = \begin{cases} \frac{1}{B(m,n)} X^{m-1}(1-X)^{n-m} & \text{if } 0 < X < 1 \\ 0 & \text{otherwise} \end{cases}$$

where $B(m, n) = \int_0^1 x^{m-1}(1-X)^{n-1} dx$

A Beta distribution has Mean

$$E[X] = \frac{m}{m+n} \text{ and}$$

Variance $r\,(X) = \frac{mn}{(m+n)^2\,(m+n+1)}$.

Standard Bayesian framework[27]

The initial prior is Beta (1,1), and the uniform distribution on [0,1] denotes the absence of information about the θ [28]. When a new observation is made or reported misbehavior is represented as s and normal observation as f, the prior or distribution is modified in accordance with:
$\alpha = \alpha + s$ and $\beta = \beta + f$.
If the θ is a true unknown value and is constant, then after a large number ofn of observations $\alpha \sim n\theta$ as per the expectations and $\beta \sim n\ (1\text{-}\ \theta)$ become close to a Dirat at θ, as expected [29]. The advantage of using the Beta function is that it only needs two continuously updated parameters as observations are made or reported [30].

Bayesian framework for the network[31]

Initially, No Prior information about the networks, so the Parameter θ is unknown, and it is assumed to be uniform in [0,1], which is equal to Beta (1,1) [31]. As observations are made (that follow a Bernoulli distribution with a parameter), a and b are updated as follows [32]:
$m = m + u,$ …………………………………………. (1)
$n = n + 1 - u$…………………………………………… (2)
where $u = 1$ if the observation consists of a dropping, and 0 otherwise.
When the appropriate two-hop ACK is not received (after a timeout), this is referred to as packet dropping in the network [33]. The decision will be taken after as many observations as possible, roughly speaking according to the mathematical expectation E(Beta(a,b)). The decision (or stationary) point is used to represent this, while m+n is used to represent the number of observations. Find the moment the accused was acting inappropriately, and this is indicated as:
$E\ (\text{Beta}\ (m,n)) > E_{max}$ ………………………………………….(3)
$E(\text{Beta}(m,n)) = \frac{m}{m+n}$…………………………………………….(4)
For the network to work more efficiently, it is necessary to find the E_{max} as follow:

- With the different scenarios, the simulation finds each node E without misbehaving in the network that assesses the E
- Find the maximum value from all the simulation evaluations, and that value consider as the E_{max}

The decision (Stationary) point in mathematical estimate methods is the point at which the difference between the two-subsequence observation could be insignificant. One common option is one that meets the criteria listed below [34]:
$\text{Var}\ (\text{Beat}\ (m, n)) < \epsilon$……………………………….. (5)
Such that Var is mathematical variance, and ϵ is a very small positive [34]:
$\text{Var}\ (\text{Beat}\ (m, n)) = \frac{m \text{ x } n}{(m+n+1) \text{ x } (m+n)^2}$……………………. (6)

3. HAODV algorithm

The mitigation technique HAODVidentifies and prevents multiple attacks in MANETs. For the Reputation System, the algorithm to detect multiple attacks (BH and PDA) is based on a Bayesian approach [35]. Considered System Parameters with specified values.

Efficiency Value (EV): It measures the efficiency of a node in routing data to another node and varies from zero to 1. It will drop or grow depending on the network's misbehaving node activity.

Maximum_RREQ: The source node begins calculating the misbehavior value for each node in its analysis table based on the node's maximum request count [36][37].

Misbehavior Value (MV): Promiscuous mode is activated to monitor node misbehavior. Because a malicious node does not forward the RREQ count is zero, this operation will enhance the node's MV. If the node MV equals the specified Misbehaviors Threshold Value, this node is verified to be a black hole node [37][38].

Mobility model: In a MANET, the mobile node can move freely within the network. It is challenging to record the mobile node's mobility pattern. Ad hoc networks have no fixed infrastructure, and all nodes move at unexpected speeds and directions. In a random waypoint mobility model, mobile node accurate real-life mobile patterns are created from all of the different mobility models. As a result, it is used to assess the performance of the routing protocol.

Detection of the Blackhole attack: Node A monitors node B's activities. Node A makes the erroneous assumption that the result may be derived independently from one observation to the next and that node B fluctuates irregularly in terms of probability due to the parameter [38]. Node A illustrates the uncertainty surrounding the parameter by supposing that the parameter is drawn in line with a distribution that is updated as new observations are made [37]. Here, the classic Bayesian framework is presented [39].

Packet dropping attack detection: It has comparable properties to the black hole attack, but it does not become part of the data transmission routing [38]. The packet is dropped due to the node's low battery, overhead condition, and selfishness. It is difficult to identify packet-dropping attacks since there are numerous other reasons for packet dropping in the network, such as a damaged link, wireless network mobility, energy limits, and transmission queue overflow [38]. To monitor data communication, a promiscuous mode was added to the network. Transmitter nodes monitor whether or not a neighbor node forwards data to another node. If the data is not transmitted, the node's efficiency value decreases. When a node's efficiency value reaches 0, it is declared malicious, and all neighbor nodes update their blacklist table. Normal nodes include the malicious node ID in their block list table. Stop sending the packet through the malicious node and start looking for a different route around it.

4. Experiment Work

Using the parameters listed in table 1, a comparative analysis of the proactive, source-initiated, and balanced-hybrid protocols is carried out using the Network Simulator 2.35 (NS2.35) platform.

Table 1. lists the parameters.

Parameter	**Typical Value**
Platform	NS-2.35
Routing Protocols	AODV, HAODV
Area of Network	800 m x 800 m
No. of nodes	10, 20, 30, 40, 50, 60, 70, 80, 90,100
Mobility Model	Random Waypoint Mobility
Traffic Type	UDP
MAC Protocol	IEEE 802.11
Period of Simulation	1800s
Packet Size	512

In the comparison study, we increase the network with random mobility's transmitter-to-receiver ratio and percentage of mobile nodes. In the original simulation setting, we created a network of 10 ad hoc nodes, each of which moved randomly and had two nodes that were constantly in communication with one another.

5. Results Analysis

The proposed study differs from earlier work in a number of ways, including random velocity, a large network, a protracted simulation time, an increased number of nodes, and others. With a 100-node network and random node mobility over a long simulation time, we compare AODV and HAODV approaches in this research (i.e., 1800 seconds). We also assess protocol performance in large (100 nodes) and small (10 nodes) multi-connection networks. By contrasting network characteristics, including packet delivery ratio, throughput, packet dropping ratio, routing overhead, and end-to-end delay, we can determine which protocol performs the best in a big, mobile network. The simulation also demonstrates how well the HAODV routing protocol functions in big mobile networks.

Four performance metrics, which are covered in more detail below, were used to compare mobile node network protocols:

Throughput: According to Eq (7), it specifies the ratio between the number of packets transmitted by the sender and the amount of time it takes for the receiver to receive all the data. Figure 1 depicts the throughput analysis of the AODV and HAODV approaches.

$$\mathrm{TH\,OUG\ \ H\,PUT} = \frac{1}{N}\sum_{I=1}^{N}\frac{B_I}{T_I} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.. \quad (7)$$

where bi represents the overall number of bits sent to the destination in time ti, n channel capacity, and i is the sequence number.

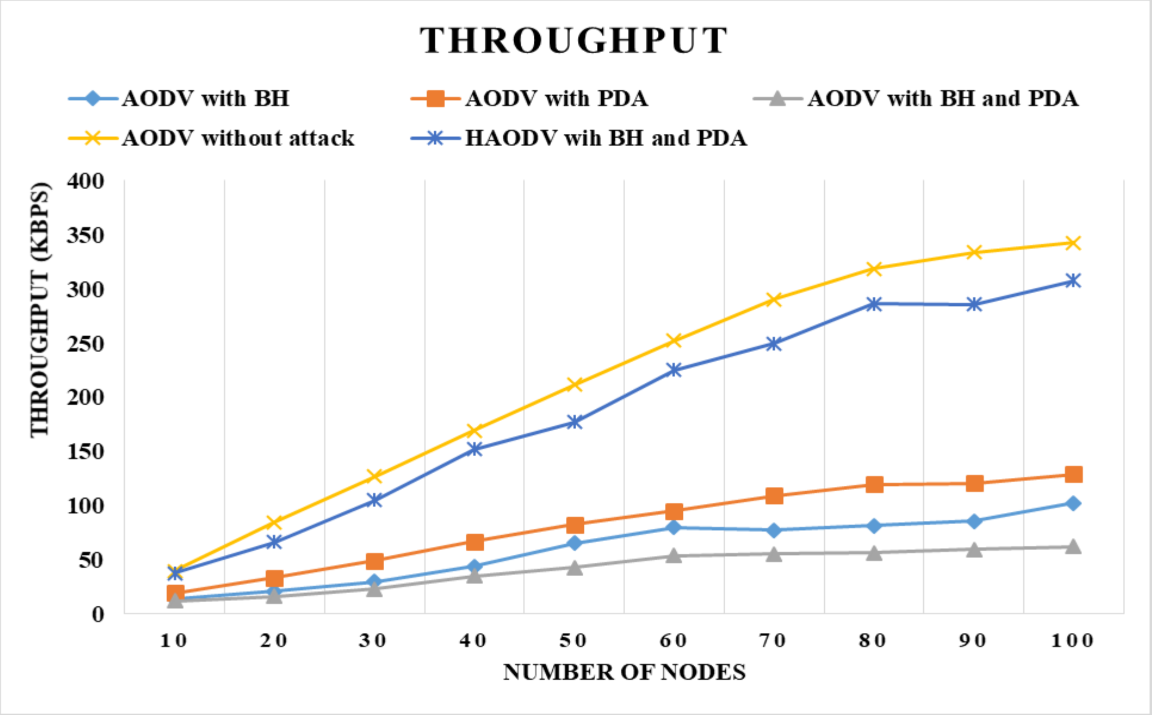

Figure 1: AODV and HAODV throughput comparison

A comprehensive examination of the throughput performance of the HAODV and AODV routing algorithms with and without network layer attacks (BH and PDA) is shown in Figure 1. In the presence of an attack (BH and PDA), the throughput of the AODV routing protocol drops because of the characteristics of the attacker node and a highly dynamic environment that results in break links, which also reduces performance.

The HAODV algorithm evaluates the RREQ Count of surrounding nodes first, and if the new value is equal to the maximum request count, it continues to calculate the node misbehavior, which involves checking the node's hop count and sequence number. If a node meets all of the requirements for malicious activity, it is classified as a black hole node; otherwise, if the misbehavior value falls below a specified level, a calculation of the node's efficiency value is initiated to look for packet-dropping assaults. After detecting the malicious node and routing data through the legitimate node to avoid the malicious node, the HAODV algorithm enhanced its performance. The mitigation method (HAODV) improves performance by up to 92 percent when compared to the original AODV routing protocol.

The packet delivery ratio is defined as the ratio of the packet delivered by the receiver to the packet transmitted by the sender, as shown in Eq (8). The network's speed and routing protocol are important for an improved packet delivery ratio.

$$\text{Packet Delivery Ratio} = \frac{1}{\text{N}}\sum_{\text{I}=1}^{\text{N}} \frac{\text{Pkt R}_{\text{I}}}{\text{Pkt S}_{\text{I}}} \qquad \dots\dots\dots\dots\dots\dots\dots\dots\dots.. \quad (8)$$

WherePktR_i is the Received Packets

Pkt$S_i$is theSend Packets

Figures 2 and 3 illustrate a simulation-based examination of the packet dropping ratio and packet delivery ratio metrics of the AODV and HAODV protocols in the presence and absence of the attack.Without an attack present in the network's original AODV routing protocol, it delivers up to 99 % of the packets to the destination for a small network, and form a dense network, performance is decreased owing to congestion but still delivers up to 95 % of the packets to the destination. When both attacks are present in the network, 88.12% and 89.82% of packets drop at the 10 nodes and 100-node networks, respectively.

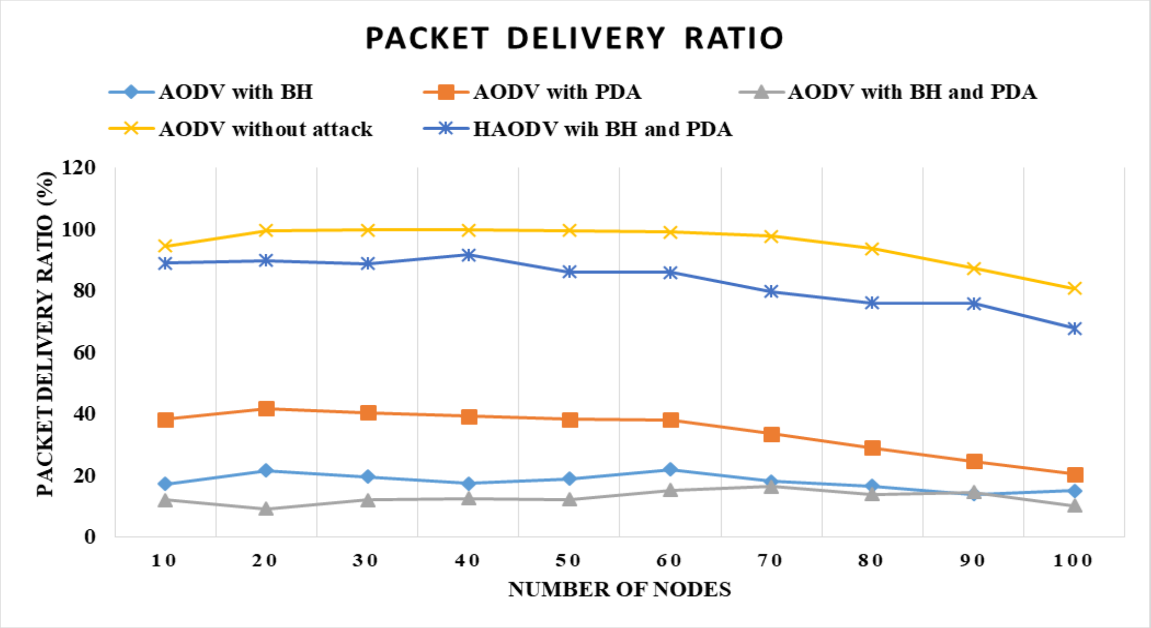

Figure 2: AODV and HAODV packet delivery ratio comparison

When both attacks were present in the network, the AODV routing protocol's performance suffered significantly, with just 12.73 % of packets delivered and 93 % of packets dropped on average. The HAODV routing protocol immediately detected the malicious nodes and created a new routing path that avoided the malicious node. As a result, when both malicious nodes are present in the network, it enhances data packet delivery by up to 85 %.

Packet dropping Ratio

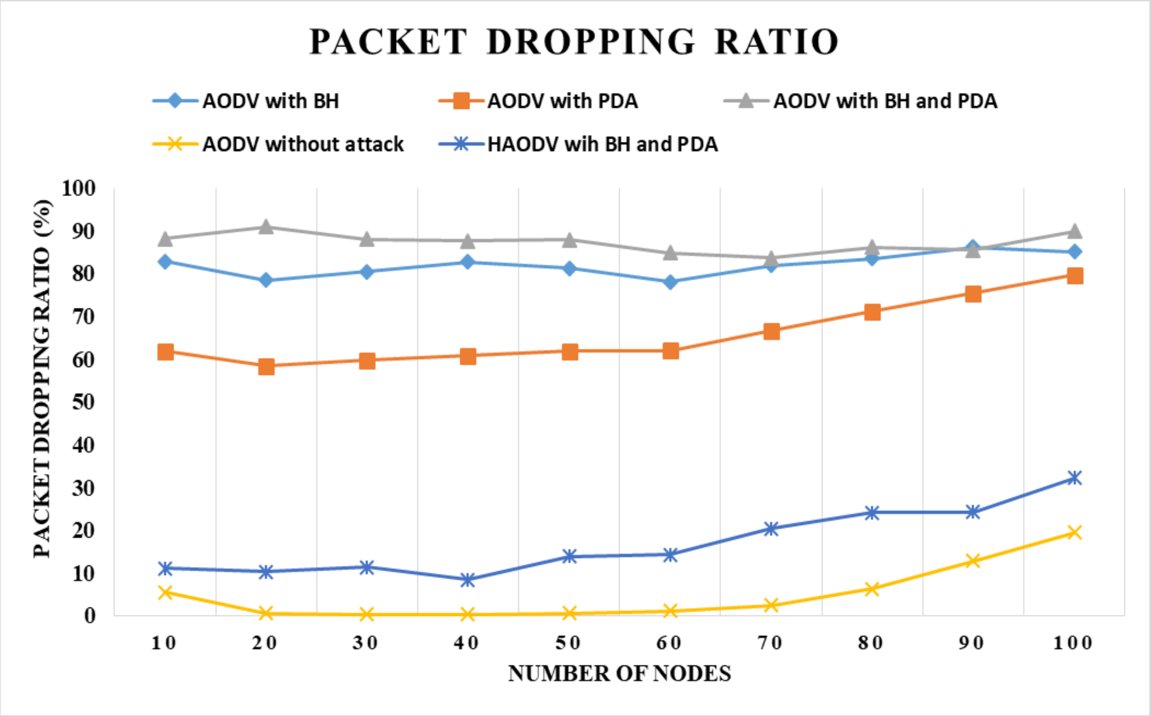

Figure 3: AODV and HAODV packet dropping ratio comparison

Routing Overhead

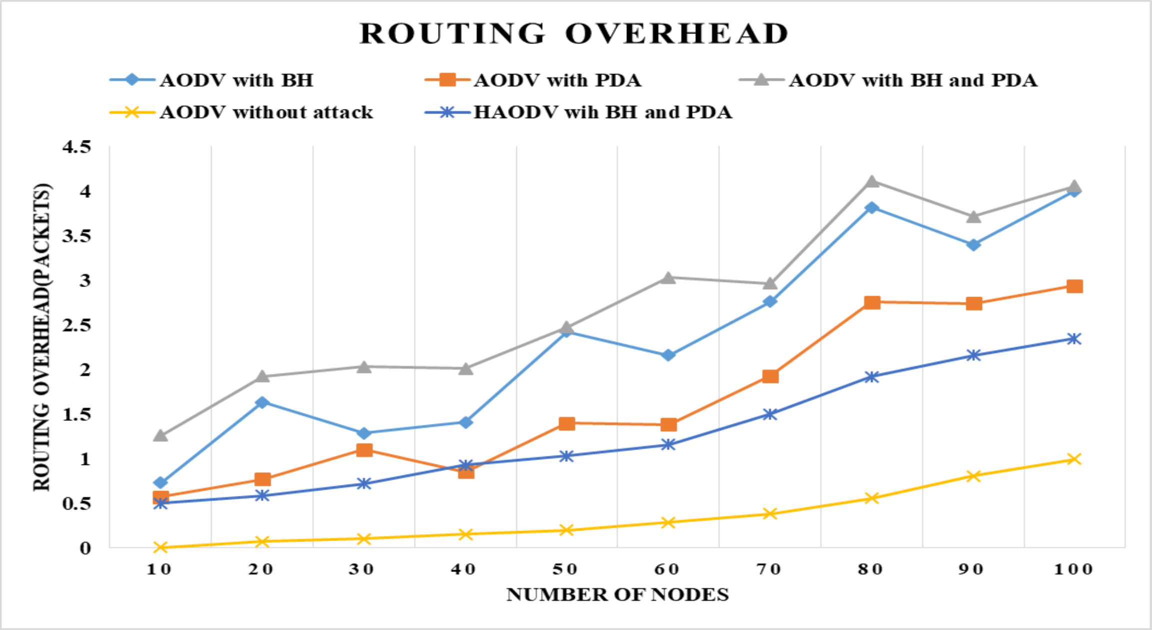

Figure 4: AODV and HAODV routing overhead comparison

The performance of a network with and without a malicious node is shown in Figure 4, along with a suggested HAODV for reducing routing overhead by adjusting the number of nodes and the dynamic environment. It has been noted that HAODV has greater routing overhead than AODV. As mobility and the number of nodes in the network grow, so will the routing overhead. Because high mobility is dynamic, there is an increase in path failure and route discovery, which raises the routing overhead.

At 100 nodes, the original AODV routing protocol performance is 0.995 percent, but if the overhearing base scheme with the efficiency value of 1 is used, the routing overhead increases to 27.91 %. To address this limitation of the overhearing-based technique, we set the efficiency or E max value in our research to 0.5 by determining the maximum value from all simulated evaluations. Our suggested HAODV method uses an efficiency value of 0.5, which reduces routing overhead to 0.75 % at 100 nodes by efficiently overcoming the effect of both attacks in the network.

End to End Delay

The end-to-end delay of a black hole attack on the network grows as node speed and mobility rise. In our investigation, we used dynamic mobility, which results in more frequent node movements and more frequent changes to network routing.

According to the graph in figure 5, the end-to-end delay decreased due to the black hole attack (Delay: 0.812 s at 100 nodes) and the node's high mobility compared to the original AODV attack (Delay: 1.078 s at 100 nodes), but it grew as the number of nodes increased in the case of the packet dropping attack (Delay: 2.38 s at 100 nodes).

When both attacks are active in the same network, similar effects are observed. Additionally, it has been noted that using the HAODV algorithm results in a higher delay (Delay: 1.42 s at 100 nodes) because it is based on an overhearing-based scheme, compared to the original AODV routing protocol (Delay: 1.078 s at 100 nodes), with a different attack, but it also increases throughput by up to 92 % and packet delivery ratio by 85 %.

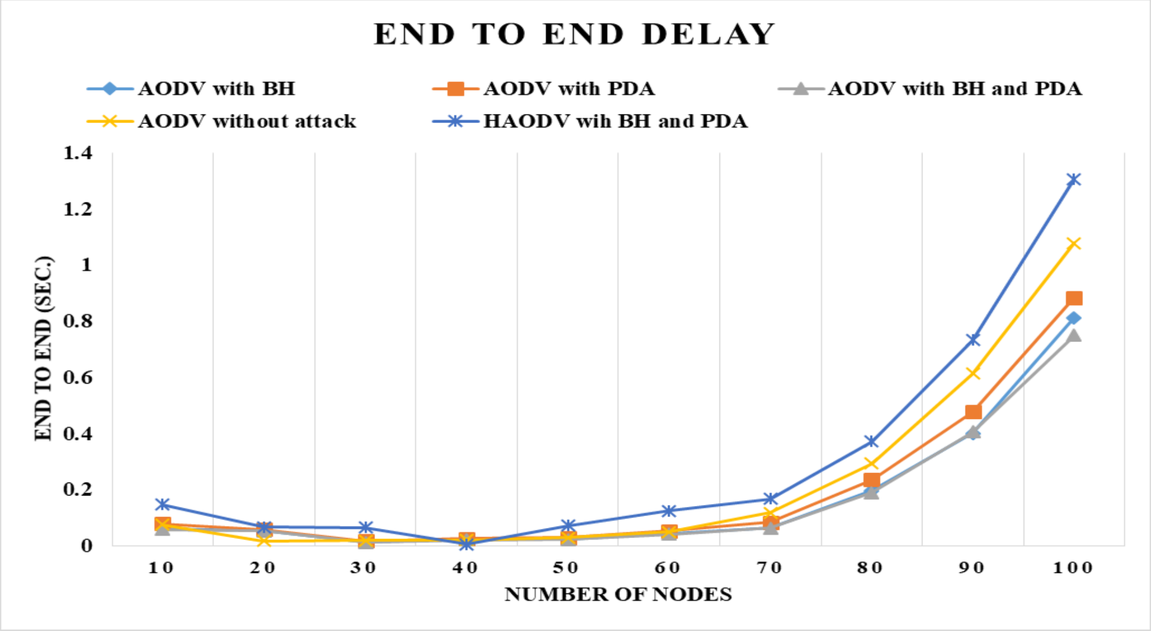

Figure 5: AODV and HAODV end to end delay comparison

5. CONCLUSION

In this study, the mitigation algorithm for HAODV is developed, and the network performance of the AODV and HAODV protocols is compared using a variety of metrics, including throughput, packet delivery ratio, packet dropping ratio, end-to-end delay, and routing overhead with the number of connections and nodes for the simulation period of the 1800s.

As traffic and nodes rise from 10 to 100 nodes, the AODV's total throughput performance (with BH and PDA) declines from 6.1 bits/sec (at 10 nodes) to 64.78 bits/sec. Throughput decreases by up to 81% at 100 nodes, putting the network's general security at risk. Only 12.73 percent of packets are delivered on average, and 93 percent of packets are discarded in the network. As demonstrated in the graph, black hole and packet dropping attacks break protocol requirements and dramatically degrade the performance of good behavior protocols.After detecting the malicious node and routing data through the legitimate node to avoid the malicious node, the HAODV algorithm enhanced performance. When both malicious nodes are present in the network, the mitigation technique (HAODV) improves network throughput by up to 92 % and packet delivery ratio by up to 85 % when compared to the original AODV routing protocol's performance.

Acknowledgment

The authors are thankful to DPC members, for their guidance and encouragement in research work.

Funding

No funding is received for the research work.

REFERENCE

[1] Subir Kumar Sarkar, T.G. Basavaraju and C. Puttamadappa, Ad hoc Mobile Wireless Networks: Principles, protocols, and application, Second Edition, Auerbach Publications, 2013.

[2] S. Misra, I.Woungang, and S. C. Misra, Guide to Wireless Ad hoc Networks, Computer Communication and networks Series, Springer –Verlag London, UK, February 2009.

[3] S. Misra, I.Woungang, and S. C. Misra, Guide to Wireless Sensor Networks, Computer Communication and networks Series, Springer –Verlag London, UK, June 2009.

[4] S. Misra, I.Woungang, and S. C. Misra, Guide to Wireless Mesh Networks, Springer –Verlag London, UK, December 2008.

[5] Gao Liua,Zheng Yan and Witold Pedrycz, "Data Collection for Attack Detection and Security Measurement in Mobile Ad," Journal of Network and Computer Application, no. doi: 10.1016/j.jnca.2018.01.004, 2018.

[6] M. Imran, F.A. Khan, H. Abbas, et al, "Detection and prevention of black hole attacks in mobile ad hoc networks," Ad-Hoc and Wireless Networks (AdHocNets), pp. pp. 111-122, 2014.

[7] S. Gurung and S. Chauhan, "A novel approach for mitigating grey hole attack in MANET," Wireless Networks, pp. pp. 1-15, 2016.

[8] S.B. Lee and Y.H. Choi, "A resilient packet-forwarding scheme against maliciously packet-dropping nodes in," ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), Vols. ACM, 2006., pp. 59-70, 2006.

[9] Parul Tyagi a and Deepak Dembla , "Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET)," Egyptian Informatics Journal Egyptian Informatics Journal 18, p. 133–139, 2017.

[10] Liu, G., Yan, Z., Pedrycz, W, "Data collection for attack detection and security measurement in Mobile Ad Hoc Networks: A survey," Journal of Network and Computer Applications, 2018.

[11] Siddharth Dhama, Sandeep Sharma, Mukul Saini, "Black Hole Attack Detection and Prevention Mechanism for Mobile Ad-Hoc Networks," IEEE, Vols. 978-9-3805-4421-2/16/$31.00, 2016.

[12] Shashi Gurung and Siddhartha Chauhan, "A survey of blackhole attack mitigation techniques in MANET: merits," Springer Science Wireless Networks, 2019.

[13] Shashi Gurung, and Siddhartha Chauhan, "A Review of Black-Hole Attack Mitigation Techniques and its Drawbacks in Mobile Ad-hoc Network," IEEE WiSPNET , 2017.

[14] Md Ibrahim Talukdar,RosilahHassan,Md Sharif Hossen,KhaleelAhmad,Faizan Qamar and Amjed Sid Ahmed, "Performance Improvements of AODV by Black Hole Attack Detection Using IDS and Digital Signature," Wireless Communications and Mobile Computing, p. 13, 2021.

[15] M. Strasser, B. Danev, and S. Apkun, "Detection of reactive jamming in sensor networks," ACM Transactions on Sensor Networks, Vols. vol. 7, no. 2, p. pp. 16, 2010.

[16] A. Hamieh and J. Ben-Othman, "Detection of jamming attacks in wireless ad hoc networks using error distribution," IEEE International Conference on Communications (ICC), pp. 1-6, 2009.

[17] Y.C. Hu, A. Perrig, and D.B. Johnson, "Wormhole attacks in wireless networks," IEEE Journal on Selected Areas in Communications, Vols. vol. 24, no. 2, pp. pp. 370-380, 2006.

[18] Y.C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A defense against wormhole attacks in wireless adhoc networks," IEEE International Conference on Computer Communications (INFOCOM), pp. pp.1976-1986, 2003.

[19] Sun Choi, Doo-young Kim, Do-Hyeon Lee, Jae-il Jung, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks," IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2008.

[20] S. Hazra and SK. Setua, "Rushing attack defending context-aware trusted AODV in an ad-hoc network," International Journal of Security, Privacy and Trust Management, Vols. vol. 1, no. 3, p. pp. 176, 2012.

[21] C. Pu and S. Lim, "A light-weight countermeasure to forwarding misbehavior in wireless sensor networks:Design, analysis, and evaluation," IEEE Systems Journal, pp. 1-9, 2016.

[22] M. Sarkar and D.B. Roy, "Prevention of sleep deprivation attacks using clustering," pp. 391-394, IEEE, 2011.

[23] C. Piro, C. Shields, and B. Levine,, "Detecting the sybil attack in mobile ad hoc networks," IEEE International Conference on Security and Privacy in Communication Networks (SecureComm),, pp. pp. 1-11, 2006.

[24] Sonja Buchegger and Jean -Yves le boudec, "A robust Reputation System for P2P and Mobile ad hoc networks," Nationa Competence in Research on Mobile Information and Communication System (NCCR- MICS), pp. 5005-67322.

[25] DjmelDjenouri, and NadjibBodache, "Struggling aganist selfishness and black hole attack in MANET," Wireless communication and mobile computing, pp. 687-704, 2008.

[26] S. Wang, Q. Sun, H. Zou, "Detecting SYN flooding attacks based on traffic prediction," Security and Communication Networks, vol. Volume 5 on 10, pp. 1131-1140, 2012.

[27] X. Long and B. Sikdar, "Wavelet based detection of session hijacking attacks in wireless networks," IEEE Global Communications Conference (GLOBECOM), pp. pp. 1-5, 2008.

[28] X. Long and B. Sikdar, "A mechanism for detecting session hijacks in wireless networks," IEEE Transactions on Wireless Communications, Vols. vol. 9, no 4, pp. 1380-1389, 2010.

[29] H.A. Kim and B. Karp, ""Autograph: Toward automated, distributed worm signature detection," Usenix Security Symposium (USENIX Security), pp. 271-286, 2004.

[30] Marti, S., Giuli, T. J., Lai, K., & Baker, M., "Mitigating routing misbehavior in mobile ad hoc networks," In Proceedings of the 6th annual international conference on mobile computing and networking, p. 255–265, 2000.

[31] Liu, K., Deng, J., Varshney, P. K., & Balakrishnan, K. (, "An acknowledgment-based approach for the detection of routing," p. 536–550, 2007.

[32] Peng, G., &Chuanyun, Z., "Routing attacks and solutions in mobile ad hoc networks. In Communication technology," ICCT'06. International conference, pp. 1-4, 2006.

[33] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., &, "Detecting blackhole attack on AODV-based," IJ Network, pp. 338-346.

[34] Raj, P. N., &Swadas, P. B. , "DPRAODV: A dyanamic learning system against blackhole attack in AODV based MANET," International Journal of Computer Science, p. 54–59.

[35] Jhaveri, R. H., Patel, S. J., &Jinwala, D. C. , "Improving route discovery for AODV to prevent blackhole and grayhole attacks in MANETs," INFOCOMP, pp. 1-121, 2012.

[36] Li, C., Wang, Z., & Yang, C., "SEAODV: A security enhanced AODV routing protocol for wireless mesh networks.," Transactions on computational science XI,Berlin:, pp. 1-16, 2010.

[37] Dhanalakshmi, K. S., Kannapiran, B., & Divya, In Electronics and communication system (ICECS), international conference on, pp. 1-5, 2014.

[38] Shi, F., Liu, W., Jin, D., & Song, J., "A cluster-based countermeasure against blackhole attacks in MANETs.," Telecommunication Systems,, p. 119–136, 59(2).

[39] Shashi Gurung, Siddhartha Chauhan, "A novel approach for mitigating gray hole attack in MANET," Springer Science Business Media New York, 2016.

[40] Fahad, T., Djenouri, D., & Askwith, R., "on detecting packets droppers in manet: A novel low cost approach.," In Information assurance and security, 2007. IAS 2007. Third international symposium on, vol. Piscataway: IEEE., pp. 56-64, 2007.

[41] Saha, H. N., Bhattacharyya, D., Bandhyopadhyay,A. K., & Banerjee, P. K., "Two-level secure re-routing (TSR) in mobile ad hoc networks.," In Advances in mobile network,communication and its applications (MNCAPPS), 2012 international conference on Piscataway: IEEE., p. 119–122, 2012.

[42] Deng, H. M., Li, W., & Agrawal, D. P., "Routing security in wireless ad hoc networks," IEEE Communication Magazine,, vol. 40 (10), p. 70–75..

[43] Ramaswamy, S., Fu, H., Sreekantaradhya, M., Dixon, J., & Nygard, K. E. , "Prevention of cooperative black hole attack in wireless ad hoc networks," In International conference on wireless networks, p. 570–575, 2003.

[44] Yu, C. W., Wu, T. K., Cheng, R. H., & Chang, S. C. , "A distributed and cooperative black hole node detection and elimination mechanism for ad hoc networks," In Pacific-Asia conference on knowledge discovery and data mining, vol. Berlin: Springer, p. 538–549, 2007.

[45] Weerasinghe, H., & Fu, H. , "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation," In Future generation communication and networking IEEE, vol. 2, pp. 362-367, 2007.

[46] Dorri, A., &Nikdel, H., "A new approach for detecting and eliminating cooperative black hole nodes in MANET," In Information and knowledge technology (IKT), 2015 7th conference on, pp. 1-6, 2015.

[47] Mui, L., Mohtashemi, M., Ang, C., Szolovits, P., & Halberstadt, A., "Ratings in distributed systems: A bayesian approach.," In Proceedings of the Workshop on Information Technologies and Systems (WITS), pp. 1-7, 2001.

[48] Buchegger, S. and Le Boudec, J.Y., , "A robust reputation system for mobile ad-hoc networks," REP WORK. , 2003.

[49] Sonja Buchegger and Jean -Yves le boudec, "A robust Reputation System for P2P and Mobile ad hoc networks," Nationa Competence in Research on Mobile Information and Communication System (NCCR- MICS), pp. 5005-67322.

[50] DjmelDjenouri, and NadjibBodache, "Struggling aganist selfishness and black hole attack in MANET," Wireless communication and mobile computing, pp. 687-704, 2008.

[51] Margam Suthar, Ajay Kumar Vyas. (2022), "Performance Investigation of Routing Protocol with the velocity of 30 m/s for Random Mobility Model", International journal on electrical engineering and informatics. Volume 14, No.2 June 2022 .

[52] Margam Suthar, Ajay Kumar Vyas. (2022), "Implement and Analysis the Impacts of Multiple Attacks & Connections in AODV Routing Protocol on MANETs." Journal of Optoelectronics Laser, 41(4), 500–507.