International Journal of Computational Methods and Experimental Measurements
Vol. 12, No. 1, March, 2024, pp. 61-67
Journal homepage: http://iieta.org/journals/ijcmem

Enhancing MANET Security: A Watch Dog Routing Algorithm Approach for Intruder and Black Hole Attack Detection

S. Hemalatha[1*], S Vijayakumar[2], Arunkumar Gurunathan[3], Anbarasi Masilamani[3], G Durga Prasad[4], Kiruthiga Balasubramaniyan[5], Chitra Devi D[6], Lakshmana Phaneendra Maguluri[7]

[1] Department of Computer Science and Business Systems, Panimalar Engineering College, Chennai 600123, India
[2] Department of Mathematics, RMK Engineering College, Kavaraipettai 601206, India
[3] School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India
[4] Department of Artificial Intelligence, Shri Vishnu Engineering College for Women, Vishnupur 534202, India
[5] Department of Electronics and Communication Engineering, K. Ramakrishnan College of Technology, Trichy 621112, India
[6] Department of Computer Science and Engineering, S.A. Engineering College, Chennai 600077, India
[7] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram 522302, India

Corresponding Author Email: pithemalatha@gmail.com

https://doi.org/10.18280/ijcmem.120107

Received: 6 February 2024
Revised: 13 March 2024
Accepted: 22 March 2024
Available online: 31 March 2024

Keywords:
MANET, attackers, intruder, black hole attackers, Watch Dog technique, forward time

ABSTRACT

When wireless nodes communicate without the use of infrastructure, the network is subject to security breaches. Mobile Adhoc Network (MANET) is one of the most vulnerable wireless networks in terms of security breaches. The most common types of security breaches are intruders and attackers, whose tasks are to reduce the internal performance of the network. Many research studies are focused on detecting and preventing these two security threads. This article focuses on intruder and black hole attackers and their communication. Several techniques were proposed for thwart the intruders and attackers in the Mobile Adhoc Network communication by using the modern technologies which are an additional load to the nodes operation and these techniques could not be able to predict the attacker before it was done. To achieve this goal, this article proposed the Watch Dog approach involves routing protocol to monitoring the forwarding time of all nodes in the transmission. Delays in forwarded time nodes could indicate an intruder, while discarding the forwarded node could indicate a black hole attacker. The proposed Watch Dog routing algorithm with classification technique was implemented with a network simulator with Adhoc On Demand Vector protocol named as WD-AODV, and the simulation results were compared to a modern techniques of Fuzzy Logic based AODV (FL-AODV), Machine Learning-based AODV (ML-AODV) and Artificial Intelligence based AODV (AI-AODV) routing protocol. The compared results of attack rates, attack detection time, Packet delivery ratio and End to End delay showed that the Watch Dog-based attacker and intruder detection methods perform better by more than 59%, with excellent performance factors of 69%.

1. INTRODUCTION

Due to this nature MANET was used in many applications like disaster management, earthquake, military etc, many external forces are trying to crumble the MANET application usage by creating the mitigation on MANET performance factor. One of the famous mitigation creations is done when the transmission of the packets. Several categories of attackers and intruders [1] are penetrated in the Network to mitigate packet transmission. Intruder and attacker are a kind of node which try to reduce the network performance by delaying the packet forwarding or dropping the packet forwarding as shown in the Figure 1. Intruder is a kind of attacker who tries to hold the packer or make a delay on forwarding the packet, whereas black hole attacker is a category of the attacker who drops the packers rather than forwarding to the next hope. Many research work was carried out for detection and preventing Intruder and Attackers in the MANET by introducing the novel techniques like deep learning based [2], trust-based [3], intrusion detection [4], crypto-based [5], and destination sequence number (DSN) [6] based methods and fuzzy logic [7], but still the MANET is lags on security.

Fuzzy based PCA-FELM scheme [4] for detecting intruder in MANET, Vijayalakshmi et al. [8] proposed the IDS system based on the novel game theory with neighbor trust table approach which classifies the nodes in to defect node or cooperate node approach they achieved packet delivery ratio in 42%. Sultan et al. [9] used deep learning based ANN technique to make detection of IDS. Set of research work was carried out to detect the attack using protocol, an optimal

routing algorithm proposed in the study [10] providing a security route path for communication to avoid intruders interfering in the communication. Hybrid routing multipath algorithm for intruder detection provided trusty communication between the nodes [11]. Ghodichor et al. [12] proposed the routing algorithm for internal and external attack prevention in MANET node communication. Clustering routing approach for finding routing misbehavior nodes to identify the intruder was invented in the study [13].

Teli et al. [14] detected the black hole and gray hole attack using mitigating techniques. Khanna and Sachdeva [15] used a taxonomy technique to detect black hole attackers. Pandey and Singh [16] did black hole detection using a machine learning algorithm. Rajeshkumar et al. [17] used cluster trust adaptive ack, Kalman filtering technique, and swarm optimization to identify black hole attacker, outcome of this research provides 3.3% improvement in PDR and 3.5% improvement in male ware detection when compared with CTAAPSO methods. Black hole detection algorithm proposed in the study [5] using DHMD 5 and compute the performance metric which yields 23% and reduce the memory overhead. Sarao [18] addressed multiple attack solutions like rushing attack, gray hole attack and black hole attack. They concluded that above attacks affect the performance of the network. Block chain based routing protocol proposed by Ghodichor et al. [12] to mitigate attacks in MANET and the research work achieves good improvement in delay. Along with spider monkey optimization and swarm Intelligence technique proposed by the study [19] to detect the black hole attackers and proved the result performs better performance. Fuzzy logic scheme based black hole and gray hole attack detection method proposed by the study [20] and simulation results achieved greater performance improvement.

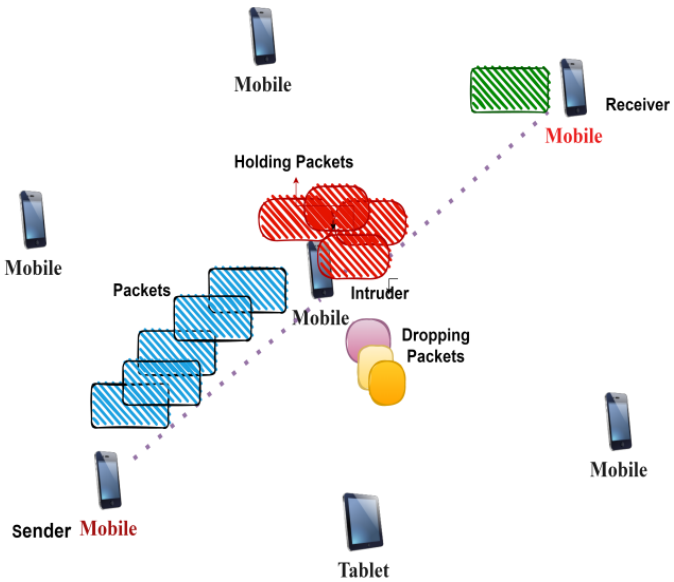

Figure 1. Intruder and black hole attacker

The objective of the research work was to carry out Intruder and black hole attacker nodes in the MANET while making communication. Black hole attack means that the intermediate nodes could drop the packet to reduce the MANET performance. The narrow research work is needed to pigeonhole the attackers who are participating in the MANET communication. This could be achieved by simple monitoring of forwarding time of each MANET node. For instance the node forward time for a specific packet is delayed, not forwarding selective the packet constantly classified into Intruder, Black hole attacker.

This research work could be achieved by adding techniques called Watch Dog to monitor the forwarding time of each packet on every node which participates in the communication. This research article is organized as follows: survey related to research work talked in Section 2, techniques discussed in Section 3 studies, proposed research work simulation work mentioned in Section 4, and conclusion in Section 5.

2. LITERATURE SURVEY

Shafi et al. [3] introduced the machine learning and trust based AODV Routing Protocol to prevent intruders and black hole attacks in the MANET. To do this, the author employs an Artificial Neural Network (ANN) with a Support Vector Machine (SVM) classifier to identify the node as a trust node. To choose the trust node, the ANN algorithm employs the Hop Count (HC), Residual Energy (RE), and Link Expiration Time parameter values to determine the intermediate route path between the source and destination nodes. This approach relies on too many parameters to determine the travel path. Furthermore, the modeling results show only a little increase in throughput and overall characteristics, ranging from 10 to 15%.

Murali and Sathya [21] created the Enhanced Black Hole Resistance approach, which employs cryptographic techniques to transport packets over an encrypted path with the shortest round-trip time. The simulation results perform better in terms of end-to-end latency, efficiency, energy consumption, and packet delivery ratio. However, picking the shortest round-trip time among the nodes is not practicable.

Dhanke et al. [6] presented a strategy for repelling a black hole attacker by leveraging the destination sequence number to prevent the attacker from delivering a counterfeit RREP and dropping the packet. The simulation results produced only 98.15% Packet Delivery Ratio (PDR), whereas the other known approaches reach 98% PDR in the case of a single black hole assault, 98.12% PDR for cooperative black hole attacks, and 98.04% PDR for normal AODV. Furthermore, this method's DSN number is entirely dependent on the threshold calculation, which is impossible to compute in all cases, such as congestion.

Olanrewaju et al. [5] developed the enhanced on-demand distance vector (AODV) routing protocol to prevent black hole attackers from invading into the network, dropping the original packet, and fabricating a new packet for forwarding it to the destination. This approach encrypts the packet using Diffie Hellman and Message Digest 5, enabling the destination node to authenticate the packet received by the sender. The work's shortcoming was the packet acknowledgement provided by the recipient; if the attacker, acting as an intermediary node, omitted the packet acknowledgement, the entire research would be flawed.

Kouanou et al. [22] created secure communication, which can avoid wormhole and black hole attacks in any wireless communication network. This strategy employs recent machine learning techniques to create a prototype for attacker avoidance. NetSim simulation with 26 nodes reaches 99% accuracy, however the method's limitations need the use of a deep learning methodology to monitor the rising data set.

Sivanesan and Rajesh [23] created a machine learning categorization model for mitigating nodes and DoS attacks in MANET. This approach divides attacks into the following categories: Gray hole, black hole, TDMA, flood. The simulation results showed a 96.75% greater accuracy than the ANN models.

Abdelhamid et al. [24] suggested a lightweight detection technique to identify black hole attackers in wireless nodes utilizing anomaly detection based on a support vector machine (SVM) using the nodes' transmission power and number of answers. The OMNET++ simulator was used to replicate the environment, and black hole attackers were detected with great accuracy. The drawbacks of this study include that the simulation was performed with a restricted number of systems (seven) and one attacker node, however the research was unable to forecast the black hole attacker when there were a large number of systems.

Sampada and Shobha [25] introduced the Smart & Secure Adhoc OnDemand Distance Vector technique (S2-AODV) with secondary CH (S-CH), primary CH (P-CH), and a super cluster head (SCH) node included. S2-AODV improves security by utilizing Honey-pot AODV (H-AODV) and avoiding the CH re-election procedure, extending the total network lifespan. The network's CH nodes gather statistics such as the Received Signal Strength Indicator (RSSI), transmission power, battery level, distance, and number of transmission retries. Machine learning (ML) methods provide a look-up table that indicates the transmission power (TXP) that the CH nodes should set. In online mode, SCH uses H-AODV to detect and delete malicious CH (black hole / gray hole) nodes (ns-2.34).

Rathod and Kotari [26] invented a novel Kangaroo-based intrusion detection system was proposed to eliminate malicious nodes from the network using Bidirectional-Long Short-Term Memory (Bi-LSTM). This increases data transmission security. For graphical user authentication, encryption based on ASCII values of the Reflection tree (E-ART algorithm) is employed. Fire Hawk Optimization Algorithm (FHO) to obtain optimal multipath by contemplating trust, node connectivity, throughput, node degree, bandwidth, energy and distance where this protocol.

From the literature survey the many authors did the research on finding the intruder and black hole attacker by following some kind of algorithms, methods, novel techniques and MANET nodes parameters etc. All the existing methods were able to predict the intruder and attacker by providing an additional overload to the nodes operation, this research article proposed a novel technique called Watch Dog without need of the additional computation and the latest technique could be able to predict the intruder and attacker node in the MANET communication. This is done by monitoring the forward time of each node to predict the attacker and intruder in the MANET.

3. RESEARCH METHODS

MANET nodes are vulnerable to many kinds of attacks which could be done by the internal nodes which are taking part of communication. The research method focuses on MANET node forming to find out if the attackers are present in the communication or not. Assuming MANET is a Graph which has vertices and Edges are connected in an undirected graph.

Let us Assume Graph G (V, E),

Vertices represent the total number of nodes in the MANET.

Let's say V={n1, n2, n3….Nn}

Edges are connecting n number of nodes

The transmission range of N nodes are two dimensions metric of N

Let Assume Source node S wants to send Data P to the Destination node D.

The data is a collection of packets named as Pi={P1, P2, and P3…..Pm}.

Every packet passes several intermediate nodes to reach the destination.

Let have Collection of intermediate nodes from S to D={Im1, Im2, Im3 ...Imn} Watch Dog technique used for monitoring the every node activity forwarded time. This estimated forwarded time only support for classifying the node is an intruder, black hole attacker. Every node forwarded time is calculated from the Eq. (1).

$$ForwardTimeFt = \sum_{i=1}^{n} \text{tt Pi} \quad (1)$$

where, tt is the Transmission time of the all packets Pi of every nodes.

The time taken for a packet to reach the destination is computed with the principle of time of flight. A threshold value is determined, when the Forwarded time below the threshold value them conclude the nodes is normal, otherwise classify the nodes in to attacker category or intruder category. The distance between the sources to destination is calculated using time of flight. This is done with the support of beacon signal generation for route Request (RREQ) and Route Reply (RREP). Two categories of beacon signal named as Beacon signal arrival time B_{at}, Beacon signal Transmission time B_{tt}. The difference between these two times is called distance from Source to Destination d from the Eq. (2).

$$d = (Bat - Btt) \quad (2)$$

Algorithm I

The algorithm for determine the Watch Dog role as follows

1. Let S be the source node and D be the destination node.
2. The AODV routing algorithm determines the path between the source to destination using RREQ and RREP procedure.
3. Collect the All the intermediate nodes and forward time and time of flight using the forward to the Watch Dog classification.
4. Watch Dog perform the comparison using the following process
   - Source Node RREQ→Intermediate Node→Destination Node
   - Destination Node RREP→Intermediate Node RREP→Source Node
   - To differentiate malicious and normal node along with the route path
   - Malicious Node where Ft > threshold value δ
   - Normal Node where Ft ≤ threshold value δ
5. If any malicious node detected call classification technique.
6. Alert malicious node.
7. Start finding new path and forwarding the packets.

Classification Technique (Malicious Node)

{
//Here the classification of malicious node in to intruder or attacker
If (Forward time>threshold Value)
{
Check forward time for all the packets from the malicious node
if (selective packet forward time varies)
return Node M is an Intruder
elseif (Forward time is not occur for few packets)
Node M is a black hole attacker
else M is a normal node
}
return M
}

Watch Dog algorithm stages defined in the Algorithm I and working flow chart shown in Figure 2. First few stages the route selection is done using the traditional routing technique of route request and reply. This algorithm uses on demand AODV protocol for finding the best path since it is on demand and does not require any route overhead. After the reliable route is selected then the calculation of Forward time for the entire intermediate route (which include the source node as well as destination node) and time to flight is done. This information is forwarded to the Watch Dog for processing the nodes and finding out any intruder or attacker present in the route. All the computation is done once the variation of the threshold values is detected.

When the threshold values vary, the suspected node forward to the classification function where the nodes will be finalized is an intruder or an attacker. Classification function is established to check the forwarded time of the malicious node. If the node forwarded time is delayed then it is an intruder who tries to degrade the MANET performance.

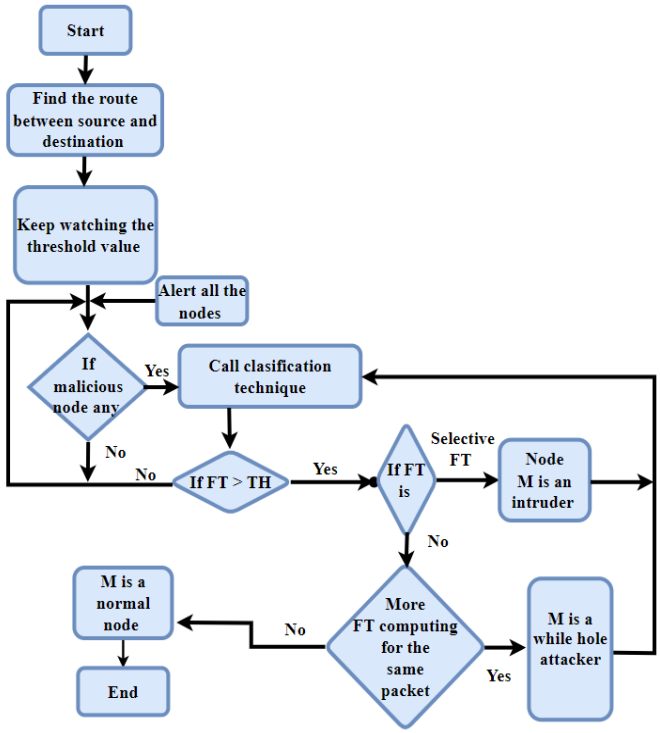

Figure 2. Watch Dog routing and classification technique flow chart

4. SIMULATION RESULT

The Simulation of the proposed intruder and black hole attacker detection with the support of Watch Dog technique is simulated using the network simulator NS2.34, the AODV was chosen as a routing protocol since it is on demand and the proposed work was named as WD-AODV. Simulation value set for the testing is shown in the Table 1, Network area 1000m×1000m, Simulation time is 300sec, nodes speed 25m/s. Total nodes is 300 nodes, initially the testing was set by using 50 nodes and slowly the nodes count is increased by 50 in each 5ns.

Table 1. Metric value

Metric	Value
Network simulator	NS 2.34
Protocol selected	AODV
Number of nodes	50,100,150,200,250,300
Simulation time	300sec
Model of mobility	Random
Speed of node	0-25m/s
Network area	1000m×1000m
Initial sending data packets	10,20,30,40,50,60,70
Traffic	Constant bit rate

The working of the proposed work, the source node send the Route Request to all the nodes for getting the Reliable path between the source and destination using the RREQ signal, Destination nodes send the Route reply to the source with the shortest path between the Source to destination as per AODV working design. Next the source node identifies the path between and all the intermediate nodes. Once the packet starts sending from the source, the Watch Dog techniques initiated to check the forward time of the each packets in all the nodes, when any nodes forward time is more than a threshold value, the node information is passed to the classification technique to classify whether the node is an intruder node or an black hole attacker. If the node is an intruder the delay in forward time, if the node is a black hole attacker the packet dropped and forward time is missing of the packets. Finally the MANET malicious nodes are alerted to the MANET, and find a new route part then start transmitting the packets as new.

The data received from the NS 2.34 node ID, data send, transmission time, data received, types of attack nodes. The parameters considered for the simulation comparison are Attack rate, attack detection time, Packet delivery ratio and end to end delay. The proposed work simulated in AODV and names as WD-AODV, and other modern techniques of FL-AODV, ML-AODV and AI-AODV routing protocol.

4.1 Attack rate

The ratio between the total nodes currently detected as a normal or malicious node is called attack rate. To simulate the attack rate the nodes are defined initially 50 nodes and slowly increase the node count by 50 to teach to 300 nodes in each 5ms.Compare the attack rate, initially 8 attacker nodes are set to make the packet dropping and packet delaying for 50 nodes, and when the nodes get increased the attacker nodes also increase by 17,29,28,29. The proposed WD-AODV predicted the exact 8 attacker nodes whereas the other method FL-AODV), ML-AODV and AI-AODV predicted only 4, 5, 6, nodes. When the nodes increased the proposed WD-AODV was able to predict the exact malicious nodes where other nodes failed to predict the exact malicious nodes. The

Simulation value and comparison graph are shown in the Table 2, and Figure 3.

Table 2. Attack rate

Nodes	FL-AODV	ML-AODV	AI-AODV	WD-AODV
50	4	5	6	8
100	13	14	15	17
150	25	26	27	29
200	24	25	26	28
250	25	26	27	29
300	30	31	32	34

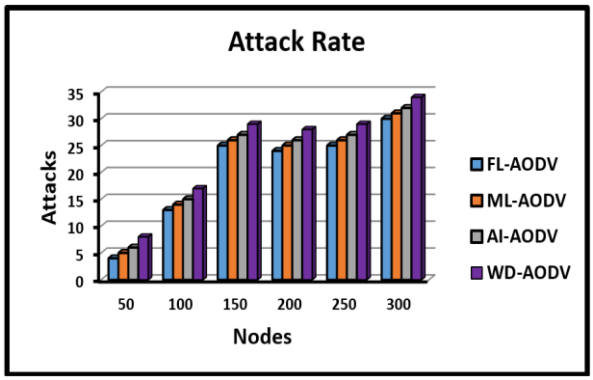

Figure 3. Attack rate

4.2 Attack detection time

Table 3. Attack detection time

Nodes	FL-AODV	ML-AODV	AI-AODV	WD-AODV
50	0.3	0.29	0.28	0.1
100	0.32	0.31	0.3	0.12
150	0.36	0.35	0.34	0.16
200	0.39	0.38	0.37	0.19
250	0.4	0.39	0.38	0.2
300	0.43	0.42	0.41	0.23

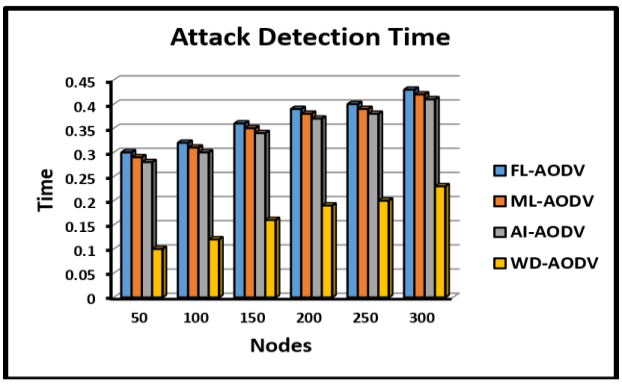

Figure 4. Attack detection time

Attack detection time is a measurement to find out the method taking time for detecting the attack. To predict the attack detection time rate the nodes are defined initially 50 nodes and slowly increase the node count by 50 to teach to 300 nodes in each 5ms.Initially 8 attacker nodes are set to make the packet dropping and packet delaying for 50 nodes. The proposed WD-AODV predicted the exact first attack on 0.1ms whereas the other methods FL-AODV, ML-AODV and AI-AODV predicted the first attack on 0.3ms, 0.29ms and 0.28ms. When the nodes increased the proposed WD-AODV was able to predict the exact malicious nodes in lesser time compared with other methods FL-AODV, ML-AODV and AI-AODV. The Simulation value and comparison graph are shown in the Table 3, and Figure 4.

4.3 Packet delivery ratio

The ratio between the number of packets sent by the sender and received by the receiver is called packet delivery ratio. Initially 50 nodes with 10 packets were set to send from the sender, and finding out the packet received by the receiver node with other methods. WD-AODV received 8 packets, other methods FL-AODV, ML-AODV and AI-AODV received the 6,4, and 5 packets respectively, the proposed methods packet delivery ratio is always higher even though the number of nodes increases parallel the total packets send also increased. Table 4 and Figure 5 depicted the simulation values and comparison graph among all the methods, in which the proposed WD-AODV model packet delivery ratio is high ranging from 70% to 84% whereas traditional Packet Delivery ratio is 40% to 70%.

Table 4. Packet delivery ratio

Nodes	Total Packet	FL-AODV	ML-AODV	AI-AODV	WD-AODV
50	10	6	4	5	8
100	20	12	10	11	14
150	30	19	20	21	24
200	40	28	29	32	35
250	50	32	32	32	42
300	60	37	42	47	50

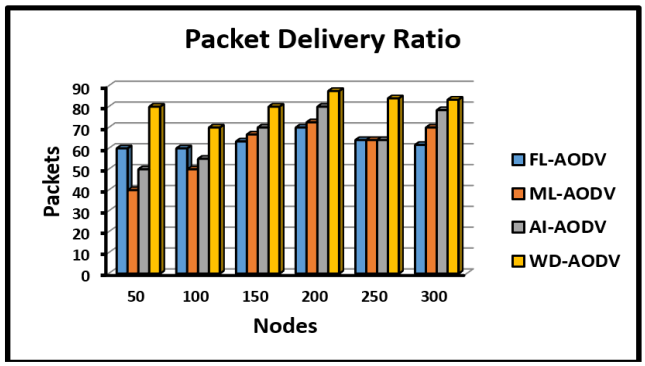

Figure 5. Packet delivery ratio

4.4 End to end delay

The time difference between packet sent from the source to packet arrival at destination is called end to end delay. Initially 10 packets were sent from the sender with 50 nodes, and the delay set from the sender side was 0ms, and receiver side packet arrival was computed to compute the delay between the sender and the receiver. The proposed WD-AODV method delay was 3ms due to the intruder and the black hole attacker presents, whereas other methodsFL-AODV, ML-AODV and AI-AODV delay was 5ms,5ms and 4.8ms respectively, this shows that the proposed methods delay was less even though the number of packets increases along with number of nodes. Table 5 and Figure 6 depicted the simulation values and comparison graph among all the methods, in which the proposed WD-AODV model delay is less varies from 3% to 29% whereas the other methods delay 4ms to 47ms.

Table 5. End to end delay

Total Packet	FL-AODV	ML-AODV	AI-AODV	WD-AODV
10	5	5	4	3
20	7	6	5	2
30	19	18	16	12
40	22	19	18	11
50	31	28	26	18
60	45	41	39	29
70	47	43	40	29

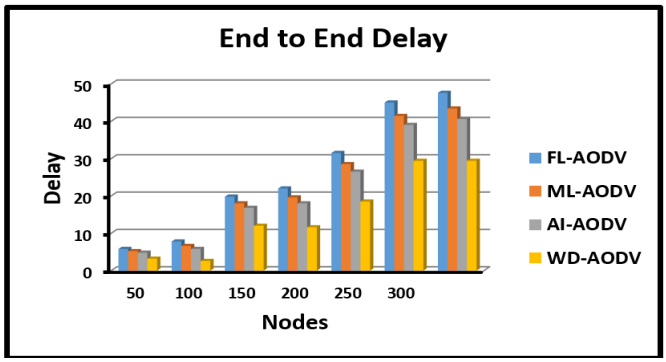

Figure 6. End to end delay

5. CONCLUSION

This article focuses on predicting the intruder and Black hole attacker using the simple Watch Dog classification technique with the node's simple parameter of forward time rather than using the complex methods in the existing technique. The proposed work was named as Watch Dog based Adhoc On Demand Vector protocol (WD-AODV) and compared to a modern techniques of Fuzzy Logic based AODV (FL-AODV), machine learning-based AODV (ML-AODV) and Artificial Intelligence based AODV (AI-AODV) with the parameters of attack rate, attack detection time, packet delivery ratio and end to end delay. The proposed work proved the best in finding all the attacks nodes, WD-AODV predicted the exact first attack on 0.1ms whereas the other methods FL-AODV, ML-AODV and AI-AODV predicted the first attack on 0.3ms, 0.29ms and 0.28ms, WD-AODV PDR was 70% to 84% whereas traditional Packet Delivery ratio is 40% to 70%. WD-AODV model delay varies from 3% to 29% whereas the other methods delay 4ms to 47ms. In feature this work could be enhanced into detecting the gray hole and white hole attackers using the forward time monitoring.

REFERENCES

[1] Verma, S., Mehra, R. (2017) Intrusion detection and prevention systems in MANET-A review. International Journal for Scientific Research & Development, 5(5): 2001-2003.

[2] Abbood, Z.A., Atilla, D.Ç., Aydın, Ç. (2023). Intrusion detection system through deep learning in routing manet networks. Intelligent Automation & Soft Computing, 37(1): 269-281. https://doi.org/10.32604/iasc.2023.035276

[3] Shafi, S., Mounika, S., Velliangiri, S.J.P.C.S. (2023). Machine learning and trust based AODV routing protocol to mitigate flooding and blackhole attacks in MANET. Procedia Computer Science, 218: 2309-2318. https://doi.org/10.1016/j.procs.2023.01.206

[4] Singh, C.E., Vigila, S.M.C. (2023). WOA-DNN for intelligent intrusion detection and classification in MANET services. Intelligent Automation & Soft Computing, 35(2). https://doi.org/10.32604/iasc.2023.028022

[5] Olanrewaju, O.M., Abdulwasiu, A.A.A., Nuhu, A. (2023). Enhanced on-demand distance vector routing protocol to prevent blackhole attack in MANET. International Journal of Software Engineering and Computer Systems, 9(1): 68-75. https://doi.org/10.15282/ijsecs.9.1.2023.7.0111

[6] Dhanke, J., Rastogi, S., Singh, K., Saxena, K., Kumar, K., Mishra, P. (2024). An efficient approach for prevention of blackhole attack in MANET. International Journal of Intelligent Systems and Applications in Engineering, 12(12s): 743-752. https://ijisae.org/index.php/IJISAE/article/view/4560

[7] Kumari, A., Dutta, S., Chakraborty, S. (2023). Detection and prevention of black hole attack in MANET using node credibility and andrews plot. Research Square, Version 1. https://doi.org/10.21203/rs.3.rs-1528078/v1

[8] Vijayalakshmi, S., Bose, S., Logeswari, G., Anitha, T.J.C.S. (2023). Hybrid defense mechanism against malicious packet dropping attack for MANET using game theory. Cyber security and Applications, 1: 100011. https://doi.org/10.1016/j.csa.2022.100011

[9] Sultan, M.T., Sayed, H.E., Khan, M.A. (2023). An intrusion detection mechanism for manets based on deep learning artificial neural networks (ANNs). arXiv Preprint arXiv: 2303.08248. https://doi.org/10.5121/ijcnc.2023.15101

[10] Veeraiah, N., Krishna, B.T. (2022). An approach for optimal-secure multi-path routing and intrusion detection in MANET. Evolutionary Intelligence, 15: 1313-1327. https://doi.org/10.1007/s12065-020-00388-7

[11] Veeraiah, N., Khalaf, O.I., Prasad, C.V.P.R., Alotaibi, Y., Alsufyani, A., Alghamdi, S.A., Alsufyani, N. (2021). Trust aware secure energy efficient hybrid protocol for manet. IEEE Access, 9: 120996-121005. https://doi.org/10.1109/ACCESS.2021.3108807

[12] Ghodichor, N., Namdeoe, V., Borkar, G. (2022). Secure routing protocol against internal and external attack in MANET. In Proceedings of the International Conference on Emerging Trends in Artificial Intelligence and Smart Systems, THEETAS 2022, Jabalpur, India. http://doi.org/10.4108/eai.16-4-2022.2318163

[13] Rajendran, A., Balakrishnan, N., Ajay, P. (2022). Deep embedded median clustering for routing misbehaviour and attacks detection in ad-hoc networks. Ad Hoc Networks, 126: 102757. https://doi.org/10.1016/j.adhoc.2021.102757

[14] Teli, T.A., Yousuf, R., Khan, D.A. (2022). MANET routing protocols attacks and mitigation techniques: A review. International Journal of Mechanical Engineering, 7(2): 1468-1478.

[15] Khanna, N., Sachdeva, M. (2019). A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs. Computer Science Review, 32: 24-44. https://doi.org/10.1016/j.cosrev.2019.03.001

[16] Pandey, S., Singh, V. (2020). Blackhole attack detection using machine learning approach on MANET. In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, pp. 797-802. https://doi.org/10.1109/ICESC48915.2020.9155770

[17] Rajeshkumar, G., Kumar, M.V., Kumar, K.S., Bhatia, S., Mashat, A., Dadheech, P. (2023). An improved multi-objective particle swarm optimization routing on MANET. Computer Systems Science & Engineering, 44(2). http://doi.org/10.32604/csse.2023.026137

[18] Sarao, P. (2022). Performance analysis of MANET under security attacks. Journal of Communications, 17(3): 194-202. https://doi.org/10.12720/jcm.17.3.194-202

[19] Arunmozhi, S.A., Rajeswari, S., Venkataramani, Y. (2023). Swarm intelligence based routing with black hole attack detection in MANET. Computer Systems Science & Engineering, 44(3). https://doi.org/10.32604/csse.2023.024340

[20] Maheswari, S., Vijayabhasker, R. (2023). Fuzzy reputation based trust mechanism for mitigating attacks in MANET. Intelligent Automation & Soft Computing, 35(3). https://doi.org/10.32604/iasc.2023.031422

[21] Murali, S., Sathya, V. (2024). Reliability assessment and detection of nodes causing a blackhole attack in portable informal networks. International Journal of Intelligent Systems and Applications in Engineering, 12(8s): 173-185.

[22] Kouanou, A.T., Fonzin, T.F., Zanga, F.M., Mouelas, A.N., Ndenoka, G.N., Ekonde, M.S. (2024). Machine learning for intrusion detection in ad-hoc networks: Wormhole and blackhole attacks case. Cloud Computing and Data Science, 62-79. https://ojs.wiserpub.com/index.php/CCDS/article/view/3516

[23] Sivanesan, N., Rajesh, A. (2023). Mitigating intruder detection system in mobile adhoc network (MANET) using optimizer based ANN model. Research Square, Version 1. https://doi.org/10.21203/rs.3.rs-3199495/v1

[24] Abdelhamid, A., Elsayed, M.S., Jurcut, A.D., Azer, M.A. (2023). A lightweight anomaly detection system for black hole attack. Electronics, 12(6): 1294. https://doi.org/10.3390/electronics12061294

[25] Sampada, H.K., Shobha, K.R. (2024). Co-Ordinated blackhole and grayhole attack detection using smart & secure ad hoc on-demand distance vector routing protocol in MANETs. International Journal of Computer Networks and Applications (IJCNA), 11(1). https://doi.org/10.22247/ijcna/2024/224433

[26] Rathod, J.A., Kotari, M. (2024). TriChain: Kangaroo-based intrusion detection for secure multipath route discovery and route maintenance in MANET using advanced routing protocol. International Journal of Computer Networks and Applications, 11(1). https://doi.org/10.22247/ijcna/2024/224436