Journal of Theoretical and Applied Information Technology
31st July 2024. Vol.102. No. 14
© Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

COMPARING WATCH DOG ALGORITHM AND CLASSIFICATION TECHNIQUES WITH MACHINE LEARNING TECHNIQUE TO DETECT THE VARIOUS ATTACKERS IN MOBILE ADHOC NETWORK

S. HEMALATHA[1], M TRUPTHI[2], VANEETA M [3], DR NRIPENDRA NARAYAN DAS [4*], R.V.V. KRISHNA[5], DR. M. SURESH THANGAKRISHNAN[6], GAYATRI D. LONDHE[7], PONNURU ANUSHA[8]

[1]Professor, Department of Computer Science and Business Systems, Panimalar Engineering College, Chennai, Tamil Nadu, India.
[2]Associate Professor, Department of Artificial Intelligence, Anurag University, Venkatapur, Gatkesar, medchal district, Hyderabad, Telangana -500088, India.
[3] Associate Professor, Department of Artificial Intelligence and Data Science, Ramaiah Institute of Technology, Bangalore, Karnataka- 560054 India.
[4] Professor, Department of Information Technology, Manipal University Jaipur, Rajasthan, India
[5] Department of Electronics and Communication Engineering, Aditya College of Engineering & Technology, Surampalem, Andhra Pradesh 533437, India.
[6] Associate professor & HoD, Department of Computer Science and Engineering, Einstein college of Engineering, Tirunelveli, Tamilnadu, India.

[7] Assistant Professor, Electronics and Telecommunications, Dr. D. Y. Patil Institute of Technology, Pimpri, Pune, Maharashtra , Pimpri, Pune-411018,
[8] Assistant Professor Department of CSE Koneru Lakshmaiah Education Foundation vaddeswaram, AP, India
[1]pithemalatha@gmail.com,[2] trupthijan@gmail.com,[3] vaneetam@msrit.edu,[4] *nripendradas@gmail.com,
[5] rvvkrishnaece@gmail.com, [6] suresh.nellai@gmail.com, [7]gayatri.londhe19@gmail.com,
[8]anusha.ponnuru588@kluniversity.in

ABSTRACT

An Intruder and Attacker are everlasting problem in the packet communication. While facilitating communication among wireless nodes without relying on established infrastructure, networks become susceptible to security vulnerabilities. One such vulnerable network type is the Mobile Adhoc Network (MANET), where intruders and attackers play pivotal roles in compromising network integrity and performance. Various research endeavors focus on identifying and thwarting these threats, particularly targeting three types of attackers: black hole, white hole, and gray hole attackers, alongside intruders. This article delves into the implementation of the Watch Dog method, which monitors the forwarding times of each node in the communication process. Intruders are identified by delays in forwarding times, black hole attackers by dropped forwarded nodes, gray hole attackers by frequent delays in forwarded packets, and white hole attackers by nodes excessively forwarding packets to numerous recipients. Through the proposed Watch Dog Algorithm combined with Classification Techniques, implemented using network simulation, the efficacy of this approach is demonstrated. Comparative analysis against machine learning-based routing protocols reveals that the Watch Dog-based detection methods outperform, showing over 50% improvement, with performance metrics exceeding 90%.

Keywords: *Attackers, Black Hole Attackers, Gray Hole Attackers, Intruder, White Hole Attackers, MANET, Watch Dog Technique*

1. INTRODUCTION

Mobile Adhoc Network (MANET) stands out as a pivotal solution for instantaneous communication sans reliance on traditional infrastructure. Its inherent flexibility allows for swift mobility to any location, coupled with the advantage of streamlined protocol stack layers. This unique characteristic has led to widespread adoption in various critical applications such as disaster management, military operations, and earthquake response. However, the efficacy of MANET faces constant challenges from external entities aiming to disrupt its functionality. A notable area of concern arises during packet transmission, where various categories of attackers and intruders infiltrate the network, posing significant threats to its integrity and performance.

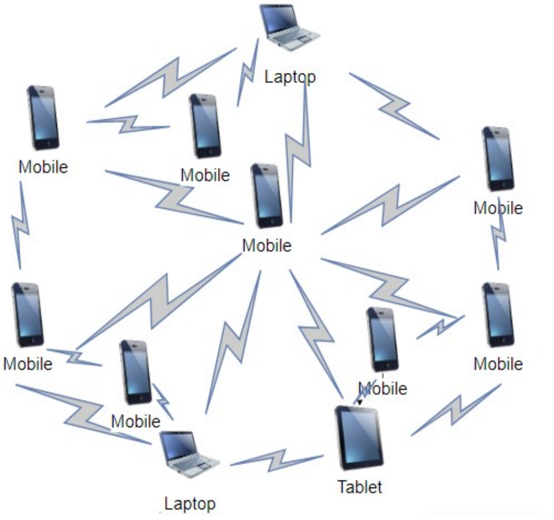

Figure 1.1 MANET Architecture

Despite numerous research efforts aimed at detecting and preventing intruders and attackers within MANETs, utilizing novel techniques such as Artificial Intelligence (AI)-based approaches, machine learning algorithms, deep learning algorithms, data analytics methods, and fuzzy logic (as illustrated in Figure 1.2), the security of MANETs continues to be a pressing concern.

Motivation of the Research work

The objective of this research is to identify and classify black hole attackers, white hole attackers, and gray hole attackers within MANETs during communication. Black hole attackers strategically drop packets at intermediate nodes to degrade MANET performance, while white hole attackers flood neighboring nodes with multiple packets, destabilizing the MANET. Gray hole attackers represent a progression from black hole attackers, consistently dropping packets. To achieve this classification, a focused research approach is required to monitor the forwarding time of each MANET node. For instance, delays in forwarding a specific packet, selective packet forwarding, complete packet non-forwarding, or excessive packet forwarding can be indicators of intruders, black hole attackers, gray hole attackers, or white hole attackers.

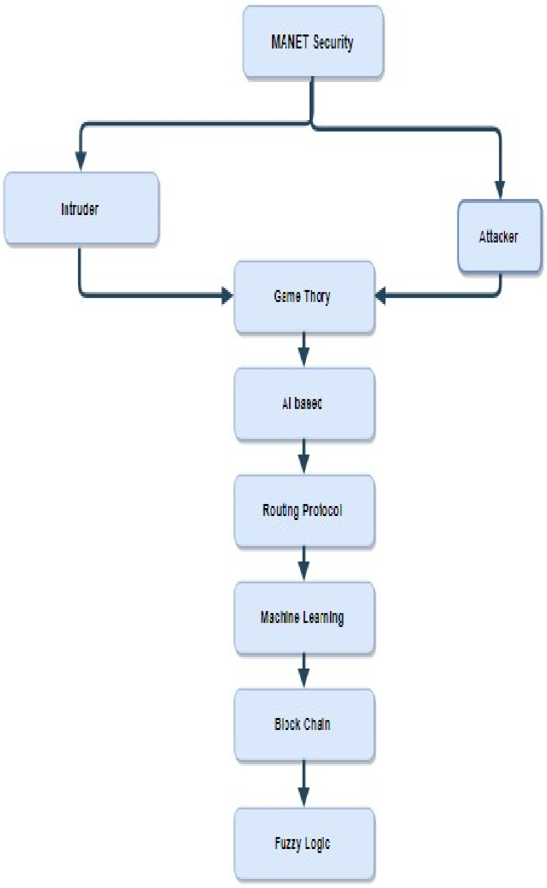

Figure 1.2 MANET Security Research Classifications

Motivation Outcome to Classification the nodes in to following category

- **Intruder** - Delay in forward time
- **Black hole attacker** - Forwarding time of selective packet delay
- **While hole attacker** - Many forwarding time of selective packets
- **Gray hole attacker** - Consecutive delay in forwarding packets.

This research endeavour aims to enhance its methodology by incorporating the Watch Dog technique to monitor the forwarding time of packets on every participating node in the communication process. The structure of this research article is organized as follows: Chapter 2 provides a comprehensive survey of related research works, Chapter 3 delves into the Watch Dog Algorithm and classification techniques, Chapter 4 outlines the simulation work of the proposed research, and Chapter 5 concludes the study.

2. LITERATURE SURVEY

The research landscape surrounding the detection and prevention of malicious activities in Mobile Adhoc Networks (MANETs) is vast and diverse. Vijayalakshmi et al. [1] introduced an Intrusion Detection System (IDS) employing novel game theory with a neighbor trust table approach, achieving a 42% packet delivery ratio. Other studies, such as Hanif et al. [2], Teli et al. [3], Shankar [4], and Hussain et al. [5], have utilized various techniques like AI, machine learning, and protocol-based approaches to detect different types of attacks such as wormhole, black hole, gray hole, and rushing attacks.

Rajeshkumar et al. [6] utilized cluster trust adaptive acknowledgment, Kalman filtering, and swarm optimization to identify black hole attackers, resulting in a 3.3% improvement in packet delivery ratio and 3.5% enhancement in malware detection compared to conventional methods. Additionally, Ahmed [11] focused on the jellyfish attack in TCP-based MANETs, while Olanrewaju et al. [12] proposed a black hole detection algorithm using DHMD 5.Sarao [13] addressed multiple attacks, including rushing, gray hole, and black hole attacks, highlighting their adverse effects on network performance. Ghodichor [14] proposed a block chain-based routing protocol to mitigate attacks in MANETs, showing notable improvements in delay.

Khosa et al. [15] introduced the SDPEGH algorithm, yielding significant improvements in throughput, packet delivery ratio, and overhead compared to existing methods. Arunmozhi et al. [16] employed spider monkey optimization and swarm intelligence techniques for black hole attacker detection, demonstrating enhanced performance. Padmapriya [17] proposed the Timer Entrenched Baited Scheme for attacker localization and removal, incorporating intelligent dark opening recognition and detachment techniques. Singh and Vigila [18] developed the Whale Optimized Deep Neural Network Model for intruder detection, achieving high accuracy. Maheswari and Vijayabhasker [19] proposed a fuzzy logic-based scheme for black hole and gray hole attacker detection, exhibiting performance enhancements.

Singh and Maria [20] introduced a fuzzy-based PCA-FELM scheme for intruder detection, outperforming other methods in terms of accuracy. Shafi et al. [21] proposed the ML-AODV method for flood and black hole attack detection, achieving reliability in throughput and routing overhead. Veeraiah and Krishna [22] developed an optimal routing algorithm to secure communication paths and prevent intruder interference. Veeraiah et al. [23] proposed a hybrid routing multipath algorithm for trustworthy communication between nodes.

Borkar and Mahajan [24] discussed secure data communication methods, while Ghodichor et al. [25] introduced a routing algorithm for internal and external attack prevention in MANET node communication. Thiagarajan et al. [26] devised a secure optimized approach for isolating malicious nodes, while Nagaraj et al. [27] utilized a clustering routing approach to identify intruders. Rani et al. [28] incorporated AI and swarm algorithms for black hole and gray hole attacker detection, and Hassan et al. [29] used AI in MANETs to predict black hole attackers. Kumari et al. [30] explored creating black hole attacks in AODV routing protocols, while Gurung and Chauhan [31] surveyed challenges and techniques related to black hole attacks in MANETs. Trust-based techniques were proposed by Goswami et al. [32] for black hole detection, and Khan et al. [33] discussed an ant colony approach to prevent black hole attackers in MANETs.

Overall, the research community has employed various advanced techniques, including AI, machine learning, clustering, block chain, and trust-based methods, to address the persistent challenge of preventing and detecting black hole, gray hole, and wormhole attackers in MANETs. However, further research is still needed to develop comprehensive solutions to safeguard MANETs against such threats.

3. RESEARCH METHODS

The vulnerability of MANET nodes to various attacks necessitates research methods focusing on node formation to detect potential attackers within the communication network. MANET can be conceptualized as a graph, denoted as G (V, E), where vertices represent the total number of nodes in the MANET (V = {n1, n2, n3... Nn}), and edges connect these nodes. The transmission range of each node, denoted as N, is a crucial metric in this context.

Consider a scenario where a source node S aims to transmit data P to a destination node D. The data consists of packets (Pi = {P1, P2... Pm}), with each packet traversing several intermediate nodes to reach the destination. Let the collection of intermediate nodes from S to D be represented as {I1, I2, I3... In}.The Watch Dog technique is employed to monitor the activity and forwarding time of each node. This estimated forwarded time aids in classifying nodes as intruders, black hole attackers, white hole attackers, or gray hole attackers. The forwarded time of every node can be calculated using the following equation:

$$Forward\ Time\ Ft\ =\ \sum_{i=1}^{n} tt\ Pi \qquad (\ Eq\ 1\ )$$

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

By analyzing the forwarded time of each node, potential threats can be identified, enabling the implementation of appropriate countermeasures to safeguard the MANET communication network.

To compute the time taken for a packet to reach the destination, we employ the principle of time of flight. This involves determining a threshold value, δ. If the forwarded time of a packet is below this threshold value, we classify the node as normal. Otherwise, we categorize it as an attacker or intruder.

The distance between the source and destination is calculated using the time of flight principle, aided by beacon signal generation for Route Request (RREQ) and Route Reply (RREP). Two categories of beacon signals are utilized: Beacon signal arrival time (Bat) and Beacon signal transmission time (Btt). The difference between these two times yields the distance from the source to the destination, denoted as d.

$$d = (\ Bat\ -\ Btt\ ) \qquad (\ Eq\ 2\ )$$

$$Source\ Node\ RREQ\ \rightarrow Intermediate\ Node\ \rightarrow Destination\ Node \qquad (\ Eq\ 3)$$

$$Destination\ Node\ RREP\ \rightarrow Intermediate\ Node\ RREP\ \rightarrow Source\ Node \quad (\ Eq\ 4\ )$$

To differenciate malicious and norml node along with the route path

$$Malicious\ Node\ where\ Ft\ >\ threshold\ value\ \delta$$

(Eq5)

$$Normal\ Node\ where\ Ft\ \leq\ threshold\ value\ \delta$$

(Eq 6)

Algorithm 3.1

Here's an outline of the Watch Dog algorithm for determining the role of nodes in a MANET communication:

1. Let S be the source node and D be the destination node.
2. Utilize the AODV routing algorithm to establish the path between the source and destination nodes using the Route Request (RREQ) and Route Reply (RREP) procedures.
3. Gather information from all intermediate nodes, including forwarded time and time of flight, and forward this data to the Watch Dog for classification.
4. The Watch Dog performs comparisons using equations 1 to 6.
5. If any malicious node is detected based on the comparisons, invoke the classification technique.
6. Alert the identified malicious node about its status.
7. Initiate the process of finding a new path and forwarding the packets through the network.
8. This algorithm aims to detect and address potential malicious activities within the MANET communication by utilizing routing protocols, monitoring node behaviour, and taking appropriate actions to ensure data integrity and network security.

Below is the pseudo code for the classification technique used to classify malicious nodes (intruders or attackers) in a MANET:

```
Classification Technique (Malicious Node):
  # here, we classify the malicious node into an intruder or attacker
  if Forward_time > threshold_value:
    # Check forward time for all packets from the malicious node
    if selective_packet_forward_time_varies:
      return "Node M is an Intruder"
    elif Forward_time_not_occur_for_few_packets:
      return "Node M is a black hole attacker"
    elif Forward_time_not_frequently_or_consecutive_packets:
      return "Node M is a Gray hole attacker"
    elif More_forward_time_computing_for_same_packet:
      return "Node M is a While hole attacker"
    else:
      return "Node M is a normal node"
  return M
```

This classification technique evaluates the forwarded time of packets from a suspected malicious node and categorizes it based on various criteria. If the forwarded time exceeds a predefined threshold, the node is further analyzed. Depending on the behaviour of the node (e.g., selective packet forwarding, lack of forwarding, frequent forwarding, etc.), it is classified as an *intruder, black hole attacker, gray hole attacker, white hole attacker, or normal node.*

The Watch Dog algorithm stages can be outlined as follows: Route Selection: Utilize the on-demand Ad-hoc On-Demand Distance Vector (AODV) protocol to select the most reliable route between the source and destination nodes. This involves the traditional technique of Route Request (RREQ) and Route Reply (RREP) to establish the path without incurring unnecessary routing overhead. Forward Time and Time of Flight Calculation: Calculate the forward time for the entire intermediate route, including both the source and destination nodes. Additionally, determine the time of flight, which involves calculating the time taken for a signal (e.g., beacon signal) to travel from the source to the destination.

Forwarding Information to Watch Dog: Forward the computed forward time and time of flight data to the Watch Dog for processing. This information is crucial for identifying any potential intruders or attackers present within the route.
Watch Dog Processing: The Watch Dog algorithm analyzes the received data to detect variations that exceed predefined threshold values. If any abnormalities are detected, the algorithm proceeds to classify the nodes along the route, identifying potential intruders or attackers.

Intruder/Attacker Detection: Based on the analysis performed by the Watch Dog, identify and classify any nodes exhibiting suspicious behavior as intruders or attackers. This step is critical for maintaining the security and integrity of the communication within the MANET.Threshold Variation Detection: Continuously monitor the computed values to detect any variations that may indicate potential security threats. If significant variations are detected, trigger the Watch Dog algorithm to initiate the classification process.

The working flowchart for the Watch Dog algorithm (Figure 3.1) would visually represent these stages, illustrating the sequential flow of operations from route selection to intruder/attacker detection based on computed data and threshold variations.

When the threshold values varies suspected node forward to the classification function where the nodes will be finalized it 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. Forwarded time is not computed for a specific packet then the node is a malicious node, or the forwarded time not computed for the randomly selective packet then the node is a gray hole attacker, More than one forward time is estimated for the single packet then the node is a while hole attacker since which try to flood the packet to many nodes.

4. SIMULATION RESULT

The simulation of the Watch Dog technique-based Intruder and Attacker Classification (WDBIAC) model is conducted using Network Simulator 2.34 (NS 2.34). A table (Table 4.1) defines the metric values used for the simulation. The defined network area is 1000m x 1000m, and the number of nodes varies from 50 to 300. The simulation duration is set to 300 seconds, with nodes exhibiting random mobility. The maximum speed of mobility nodes is 25 m/s, and the AODV protocol is used for route selection.

Figure 4.1 outlines the stages involved in executing the proposed model in the simulation. A well-defined system model established in Chapter 3, incorporating the Watch Dog algorithm and simulation setup, is passed to the NS 2.34 simulator. The simulator performs the classification of nodes into normal or malicious categories. Any identified malicious nodes are forwarded to the classification function, where they are classified as intruders, black hole attackers, white hole attackers, or gray hole attackers.

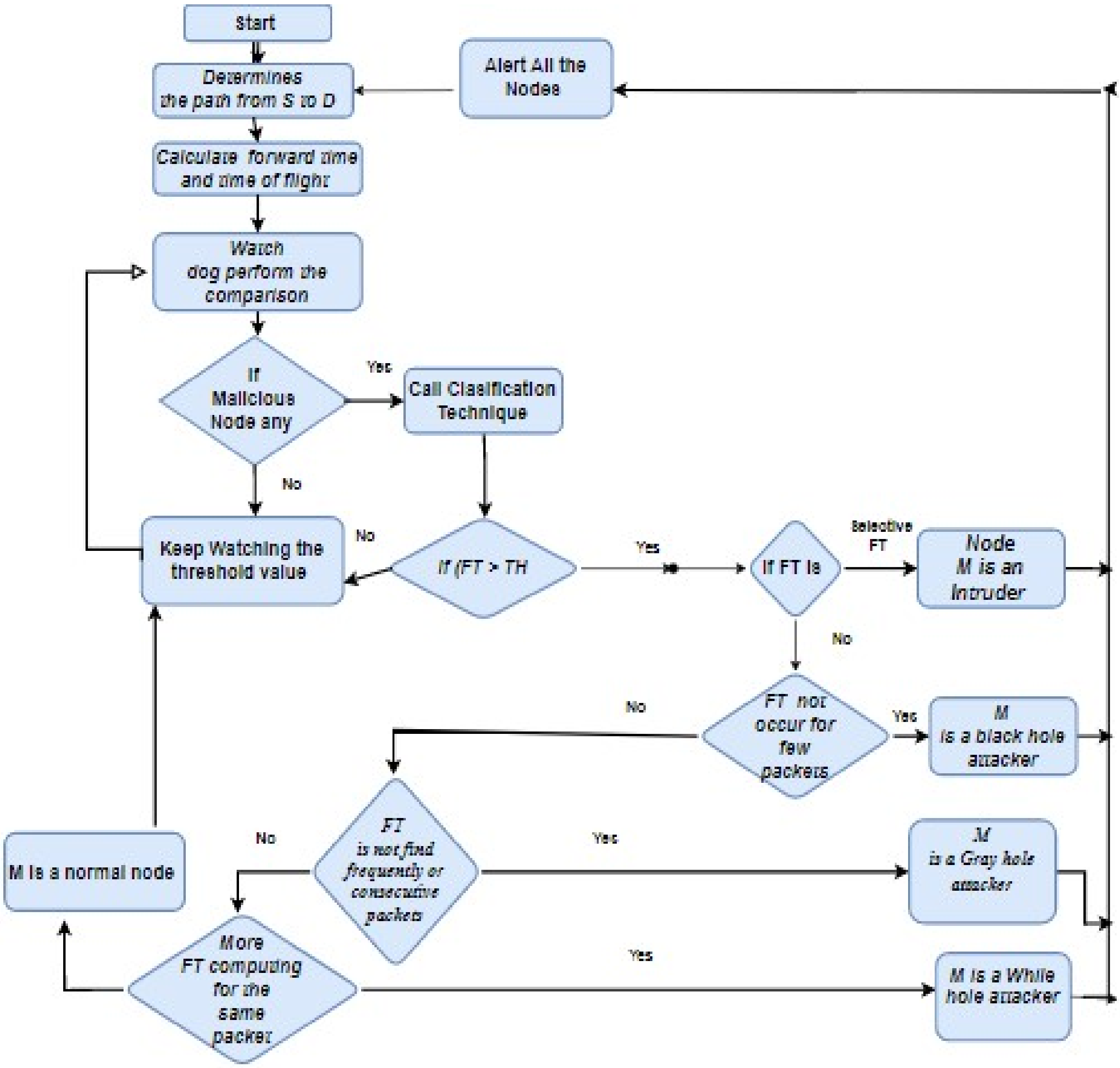
Start
Determines the path from S to D
Alert All the Nodes
Calculate forward time and time of flight
Watch dog perform the comparison
If Malicious Node any
Yes
Call Clasification Technique
No
Keep Watching the threshold value
No
If (FT > TH
Yes
If FT Is
Selective FT
Node M is an Intruder
No
No
FT not occur for few packets
Yes
M is a black hole attacker
No
FT is not find frequently or consecutive packets
Yes
M is a Gray hole attacker
M Is a normal node
More FT computing for the same packet
Yes
M is a While hole attacker

Figure 3.1 Watch Dog And Classification Technique Flow Chart

The dataset obtained from the simulation is plotted as a graph, comparing it with the performance of the ML-AODV protocol. Finally, the outcomes of the proposed work are concluded based on the analysis of the simulation results.

The proposed work begins by establishing a route path between the source and destination nodes. This is achieved by sending a Route Request from the source node, followed by a Route Reply from the destination node. Once the route path is established, the source node starts sending packets to the destination node.

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

Table 4.1 Metric Value Used For Simulation

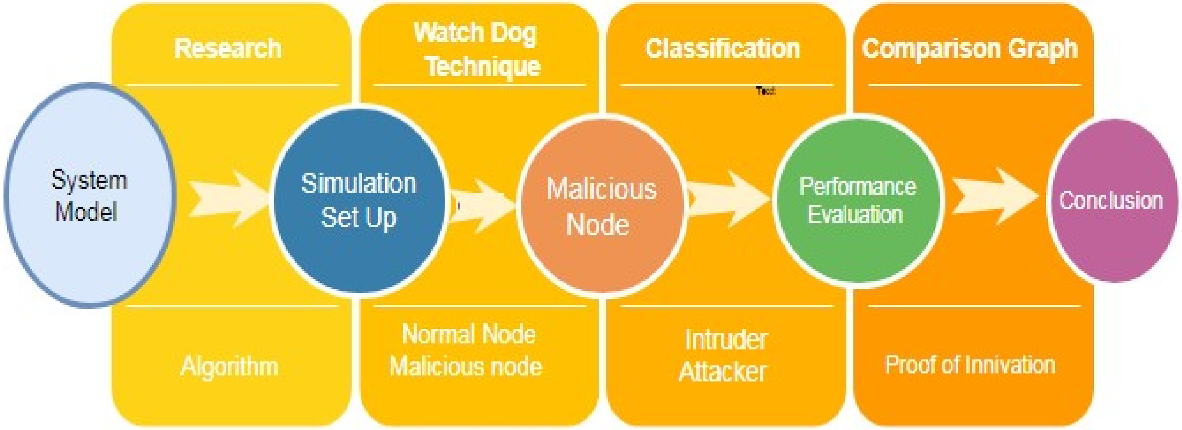

Figure 4.2 Proposed Model Simulation Stage

During packet transmission, the Watch Dog component collects the forwarded time of all intermediate nodes along the established route. If the forwarded time of any node exceeds the predefined threshold level, the classification function is invoked to classify the node as an intruder, black hole attacker, white hole attacker, or gray hole attacker. Upon identifying malicious nodes, alerts are issued within the MANET network. Subsequently, a new route path is sought, and packet transmission resumes using the updated route. Data obtained from the NS 2.34 simulation includes node ID, data sent, transmission time, data received, and types of attack nodes detected.

For performance comparison, values obtained from simulations using the ML-AODV protocol without the Watch Dog and classification algorithm are considered. This allows for an evaluation of the effectiveness of the proposed approach in detecting and mitigating malicious activities within the MANET network.

Attack Rate Comparison

The simulation results demonstrate that the proposed AODV with WDBIAC model achieves a significantly lower attack rate compared to the existing ML-AODV protocol. With only 25 malicious nodes detected out of 300 total nodes, the attack rate is reduced to 8.33% in the AODV with WDBIAC model, whereas the ML-AODV protocol yields an attack rate of 16.67% with 50 malicious nodes detected. This indicates that the proposed AODV with WDBIAC model is 50% more efficient in detecting and mitigating malicious activities within the MANET network, highlighting its effectiveness in enhancing network security and integrity.

$$\text{Attack Detection} = \frac{\text{Total number of normal or malicious node}}{\text{Number of Nodes}} X100 \qquad (\text{Eq } 7)$$

Attack Detection Time

This is the measurement time taken for identification of first malicious node.

$$ADT = n * t(\text{detecting first malicious node}) \qquad (Eq8)$$

$\text{where } n \text{ is the total node and } t \text{ is time taken for detecting first malicious node}$

.

The simulation results indicate that the proposed AODV with WDBIAC model exhibits a faster attacker detection time compared to the traditional ML-AODV protocol. With an attacker detection time of 0.2 ms, the AODV with WDBIAC model outperforms the ML-AODV protocol, which has an attacker detection time of 0.3 ms.

This demonstrates that the proposed WDBIAC model, when integrated with the AODV protocol, enhances the efficiency of attacker detection by 35%, resulting in quicker identification and mitigation of malicious activities within the MANET network.

Packet Delivery Ratio

The Packet Delivery Ratio is a ration between the numbers of packet received from the sender with number of packet send,

$$PDR = \frac{\text{Total number of Data packet received}}{\text{Total numebr of Data Packet Send}} \times 100 \qquad (Eq8)$$

The comparison of packet delivery ratio between ML-AODV and AODV with WDBIAC model shows that the proposed WDBIAC model consistently outperforms the traditional ML-AODV protocol. The packet delivery ratio for AODV with WDBIAC ranges from 90% to 94%, while the ML-AODV protocol exhibits a lower packet delivery ratio ranging from 80% to 88%.

This indicates that the proposed AODV with WDBIAC model improves the packet delivery ratio, resulting in a higher percentage of successfully delivered packets compared to the traditional ML-AODV protocol.

End to End Delay

The comparison of end-to-end delay between the traditional ML-AODV and the proposed AODV with WDBIAC model shows that the proposed model consistently exhibits lower delays across different packet sizes. The improvement in end-to-end delay with the AODV with WDBIAC model ranges from 6.2% to 43.4% compared to ML-AODV.

This indicates that the proposed AODV with WDBIAC model significantly reduces end-to-end delays in packet transmission, resulting in more efficient communication within the MANET network.

$$\text{End to End Delay} = \text{Total Data Packet} * (\text{Data Packet delay at destination} - \text{Data packet delay from the Source}) \; (EQ\ 9)$$

Nodes	Number of Attacker nodes find in ML-AODV Without WDBIAC model	ML-AODV Without WDBIAC model Attack detection rate	Number of Attacker nodes find in ML-AODV with WDBIAC model	AODV with WDBIAC model Attack detection rate
50	4	92	2	96
100	9	91	5	95.5
150	15	90	7.5	95
200	30	85	15	92.5
250	35	86	17.5	93
300	40	86	20	93

Table 4.2 Attack Rate

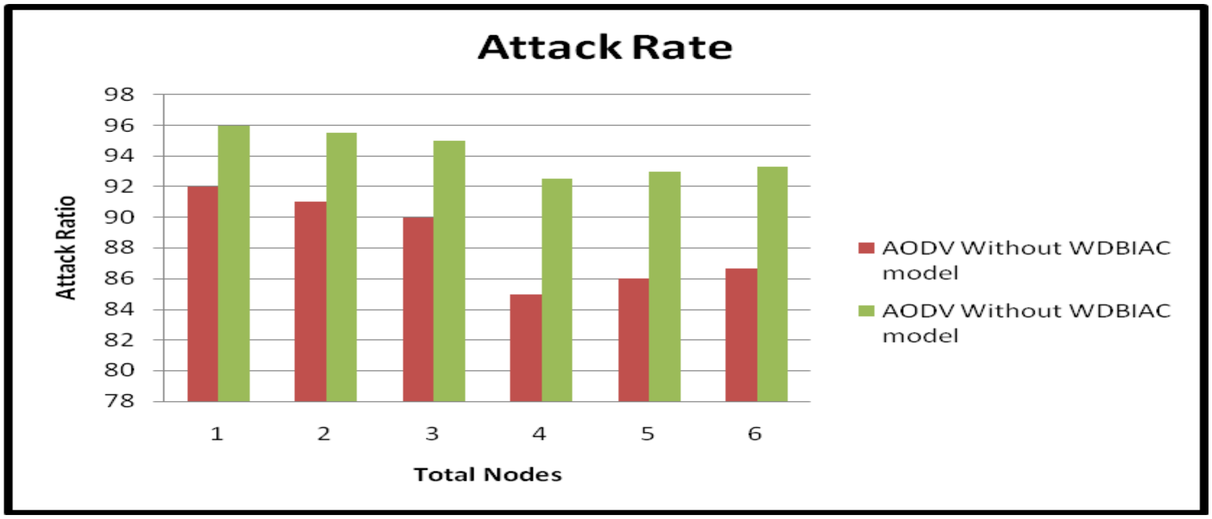

Figure 4.2 Attack Rate

Nodes	Time taken for first attack detection in ML-AODV Without WDBIAC model	Attack Detection Time in ML-AODV Without WDBIAC model	Attack Detection Time in AODV With WDBIAC model	Attack Detection Time in AODV With WDBIAC model
50	0.3	15	0.2	10
100	0.3	30	0.2	20
150	0.3	45	0.2	30
200	0.3	60	0.2	40
250	0.3	75	0.2	50
300	0.3	90	0.2	60

Table 4.3 Attack Detection Time

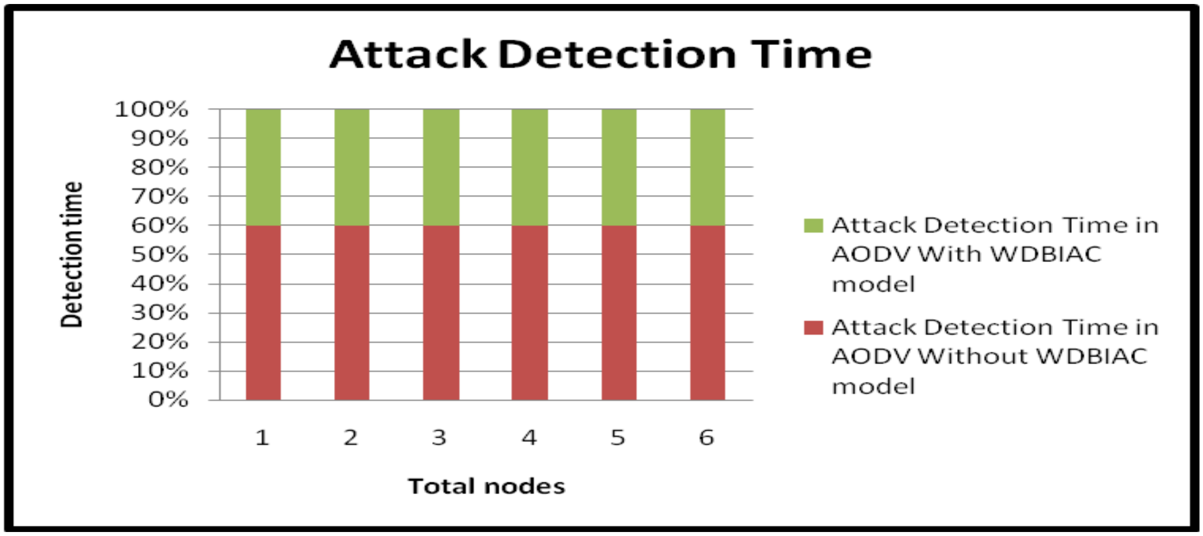

Figure 4.3 Attack Detection Time

Table 4.4 Packet Delivery Ratio

Total Packet	Packet Dropped	PDR ML-AODV Without WDBIAC model	Packet Dropped	PDR AODV Without WDBIAC model
10	2	80	1	90
20	3	85	2	90
30	6	80	4	86.6667
40	7	82.5	5	87.5
50	5	90	3	94
60	10	83.3333	5	91.6667
70	8	88.5714	4	94.2857

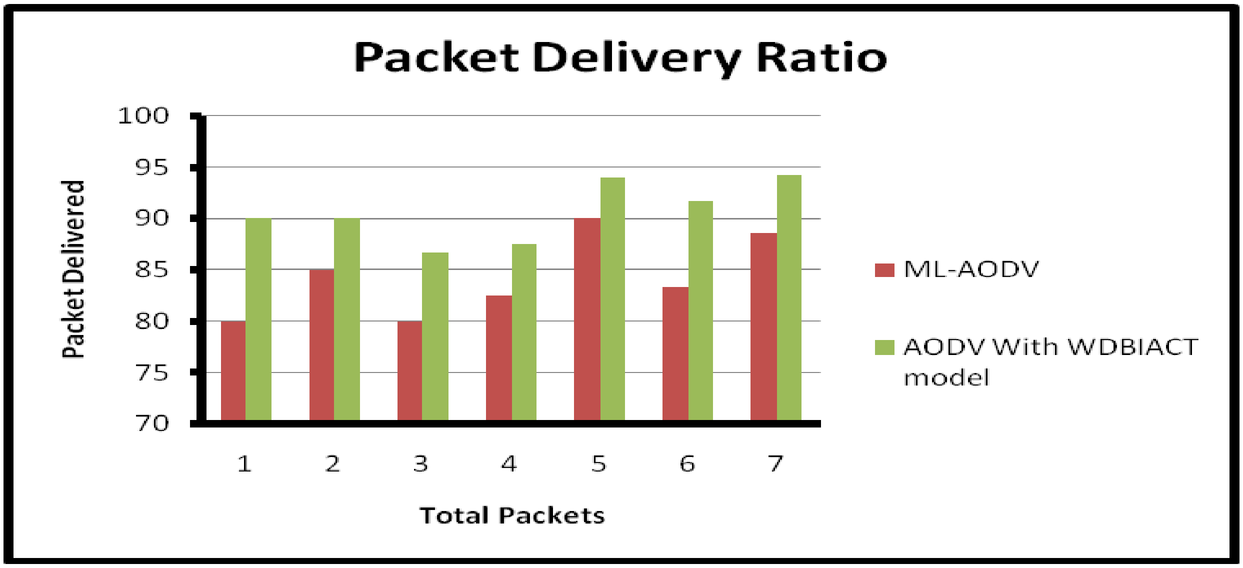

Figure 4.4 Packet Delivery Ratio

Table 4.5 End To End Delay Metric Value

Total Packet	Packet Received at Destination	EED ML-AODV Without WDBIAC model	Packet Received at Destination	EED AODV Without WDBIAC model
10	0.82	8.2	0.62	6.2
20	0.23	4.6	0.13	2.6
30	0.9	27	0.6	18
40	0.56	22.4	0.49	19.6
50	0.67	33.5	0.57	28.5
60	0.89	53.4	0.69	41.4
70	0.92	64.4	0.62	43.4

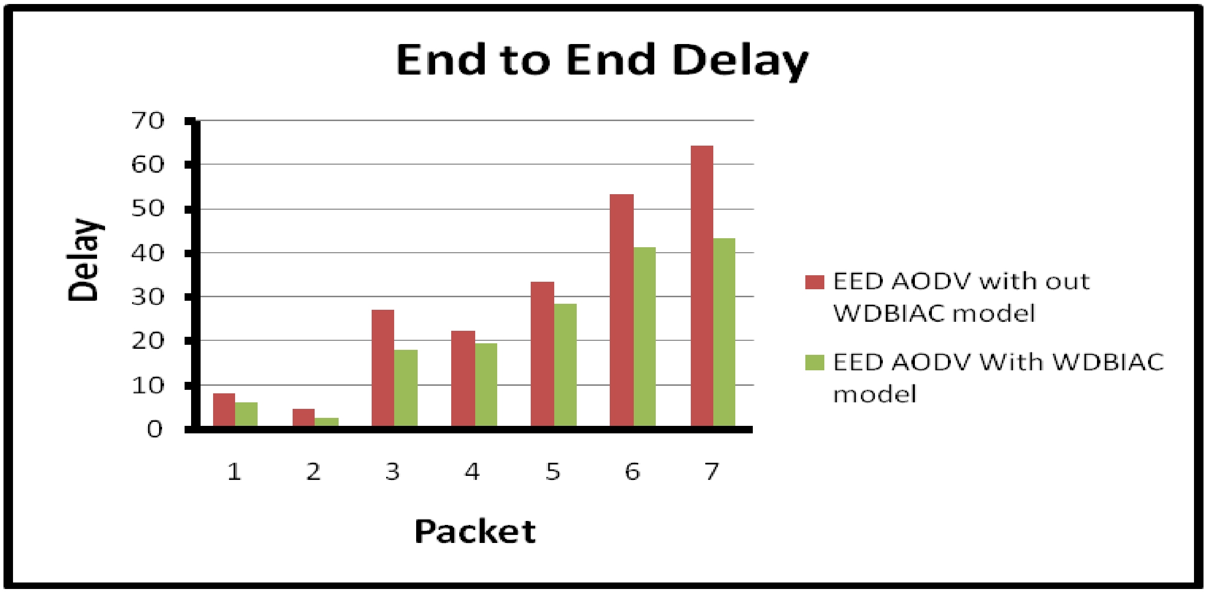

Figure 4.5 End To End Delay

5. CONCLUSION

The focus of this article is on detecting intruders and attackers within MANET communication by introducing the Watch Dog Algorithm and a classification technique based on threshold values. The research aims to identify whether a malicious node is an intruder, black hole attacker, white hole attacker, or gray hole attacker. Simulation of the proposed work is conducted using NS2.34, and the results are evaluated based on metrics such as attack rate, attacker detection time, packet delivery ratio, and end-to-end delay. The simulation results demonstrate that the proposed EEDAODV model outperforms existing protocols across all metrics. The EEDAODV model achieves a significant improvement, with a 50% increase in overall MANET metric values and excellent performance factors reaching 90%.By effectively detecting and mitigating malicious activities within MANET communication, the proposed EEDAODV model enhances network security and reliability. This research contributes to advancing the field of MANET routing protocols, providing valuable insights for future development and implementation.

REFERENCES

[1]. S Vijayalakshmi , S Bose , G Logeswari ,T Anitha " Hybrid defense mechanism against malicious packet dropping attack for MANET using game theory " Cyber Security and Applications 1 (2023) 2772-918 https://doi.org/10.1016/j.csa.2022.100011.

[2] Hanif, M., Ashraf, H., Jalil, Z., Jhanjhi, N. Z., Humayun, M., Saeed, S., & Almuhaideb, A. M. (2022). AI-Based Wormhole Attack Detection Techniques in Wireless Sensor Networks. Electronics, 11(15), 2324.

[3] 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.

[4] Shankar, T. N. (2022). Hybrid Energy Efficient Secured Attribute based ZRP Aiding Authentic Data Transmission. Journal of Scientific & Industrial Research, 81(01), 69-75. Industrial Engineering Journal ISSN: 0970-2555 Volume : 52, Issue 7, No. 2, July : 2023

[5] Hussain, S., Ahmed, S., Thasin, A., & Saad, R. M. (2022). AI-Enabled Ant-Routing Protocol to Secure Communication in Flying Networks. Applied Computational Intelligence and Soft Computing, 2022.

[6] G. Rajeshkumar, M. Vinoth Kumar, K. Sailaja Kumar, Surbhi Bhatia, Arwa Mashat5 and

Pankaj Dadheech"" An Improved Multi-Objective Particle Swarm Optimization Routing on MANET " Computer Systems Science & Engineering CSSE, 2023, vol.44, no.2 ,1187 - 1199 DOI: 10.32604/csse.2023.026137.

[7]. Suma R, Premasudha BG, Ram VR. A novel machine learning-based attacker detection system to secure location aided routing in MANETs. International Journal of Networking and Virtual Organisations. 2020;22(1):17-41.

[8]. N. Khanna and M. Sachdeva, "A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs," Comput. Sci. Rev., vol. 32, pp. 24–44, May 2019.

[9] Sultan, Mohamad & Sayed, Hesham & Khan, Manzoor., An Intrusion Detection Mechanism for MANETs Based on Deep Learning Artificial Neural Networks (ANNs), International Journal of Computer Networks & Communications (IJCNC) Vol.15, No.1, January 2023.

[10] Pandey, S. and 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.

[11] Khaled Ahmed Abood Omer " Impact of Jellyfish attack on routing protocols in TCP-based MANETs " Univ. Aden J. Nat. and Appl. Sc. Vol. 27 No.1 – April 2023 DOI: https://doi.org/10.47372/uajnas.2023.n1.a09.

[12] O. M. Olanrewaju, A. A. Abdulwasiu and N. Abdulhafiz " Enhanced On-demand Distance Vector Routing Protocol to prevent Blackhole Attack in MANET " INTER NATIONAL JOURNAL OF SOFTWARE ENGINEERING & COMPUTER SYSTEMS (IJSECS) ISSN: 2289-8522 e-ISSN: 2180-0650 VOL. 9, ISSUE 1, 68 – 75 DOI: https://doi.org/10.15282/ijsecs.9.1.2023.7.0111.

[13] Pushpender Sarao" Performance Analysis of MANET under Security Attacks "Journal of Communications Vol. 17, No. 3, March 2022. doi:10.12720/jcm.17.3.1 94-202.

[14] Nitesh Ghodichor, Raj Thaneeghavl. V, Dinesh Sahu, Gautam Borkar, Ankush Sawarkar " Secure Routing Protocol To Mitigate Attacks By Using Block Chain Technology In Manet " International Journal of Computer Networks & Communications (IJCNC) Vol.15, No.2, March 2023 DOI:10.5121/ijcnc.2023.15207 127

[15] Thabiso N. Khosa, Topside E. Mathonsi , and Deon P. Du Plessis " A Model to Prevent Gray Hole Attack in Mobile Ad-Hoc Networks " Journal of Advances in Information Technology, Vol. 14, No. 3, 2023, doi: 10.12720/jait.14.3.532-542.

[16] S. A. Arunmozhi, S. Rajeswari and Y. Venkataramani " Swarm Intelligence Based Routing with Black Hole Attack Detection in MANET " Computer Systems Science & Engineering CSSE, 2023, vol.44, no.3, DOI:10.32604/csse.2023.024340.

[17] S. Padmapriya, R. Shankar2, R. Thiagarajan, N. Partheeban, A. Daniel and S. Arun " Timer Entrenched Baited Scheme to Locate and Remove Attacks in MANET" Intelligent Automation & Soft Computing IASC, 2023, vol.35, no.1 492-505 DOI: 10.32604/iasc.2023.027719

[18] C. Edwin Singh1 and S. Maria Celestin Vigila " WOA-DNN for Intelligent Intrusion Detection and Classification in MANET Services" Intelligent Automation & Soft Computing IASC, 2023, vol.35, no.2 1737 - 1752 DOI: 10.32604/iasc.2023.028022.

[19] S. Maheswari and R. Vijayabhasker " Fuzzy Reputation Based Trust Mechanism for Mitigating Attacks in MANET " Intelligent Automation & Soft Computing IASC, 2023, vol.35, no.3 , 3678 - 3690 , DOI: 10.32604/iasc.2023.031422.

[20] C. Edwin Singh, S. Maria Celestin Vigila, Fuzzy based intrusion detection system in MANET, Measurement: Sensors, Volume 26, 2023, 100578, ISSN 2665-9174,https://doi.org/ 10.1016/j.measen.2022.100578.

[21] Haik Shafi, S Mounika, S Velliangiri, Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET, Procedia Computer Science, Volume 218, 2023, Pages 2309-2318, ISSN 1877-0509, https://doi.org/ 10.1016/j.procs.2023.01.206.

[22] Veeraiah, N., & Krishna, B. T. (2020). An approach for optimal-secure multi-path routing and intrusion detection in MANET.

Evolutionary Intelligence. https://doi.org/10.1007/s12065-020-00388-7.

[23] N. Veeraiah *et al.*, "Trust Aware Secure Energy Efficient Hybrid Protocol for MANET," in *IEEE Access*, vol. 9, pp. 120996-121005, 2021, doi: 10.1109/ACCESS.2021.3108807.

[24] Borkar, G. M., & Mahajan, A. R. (2020). A review on propagation of secure data, prevention of attacks and routing in mobile ad-hoc networks. International Journal of Communication Networks and Distributed Systems, 24(1), 23. http://dx.doi.org/10.1504/IJCNDS.2020.10025198.

[25] Nitesh Ghodichor, Raj Thaneeghaivl. V, Varsha Namdeoe, Gautam Borkar, Year: 2022, "Secure Routing Protocol against Internal and External Attack in MANET", THEETAS, EAI, https://eudl.eu/doi/10.4108/eai.16-4-2022.2318163.

[26] Thiagarajan, R., Ganesan, R., Anbarasu, V., Baskar, M., Arthi, K., & Ramkumar, J. (2021). Optimised with Secure Approach in Detecting and Isolation of Malicious Nodes in MANET. Wireless Personal Communications, 119(1), 21–35. https://doi.org/10.1007/s11277-021-08092-0.

[27] Nagaraj Balakrishnan, Arunkumar Rajendran, Ajay P. "Deep Embedded Median Clustering for Routing Misbehaviour and Attacks Detection in Ad-Hoc Networks", Ad Hoc Networks, 2021 https://doi.org/10.1016/j.adhoc.2021.102757

[28] P. Rani, S. Kavita and V. Sahil, "Mitigation of BH and gray hole attack using swarm inspired algorithm with artificial neural network," IEEE Access, vol. 8, no. 4, pp. 121755–121764, 2020.

[29] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan and A. Aldegheishem, "Intelligent detection of BH attacks for secure communication in autonomous and connected vehicles," IEEE Access, vol. 8, pp. 199618–199628, 2020.

[30] S. Kumari, M. Singhal and N. Yadav, "Black hole attack implementation and its performance evaluation using AODV routing in MANET," in Inventive Communication and Computational Technologies, Springer, Singapore, vol. 12, pp. 431–438, 2020.

[31] S. Gurung and S. Chauhan, "A survey of black-hole attack mitigation techniques in MANET: Merits, drawbacks, and suitability," Wireless Network, vol. 26, pp. 1981–2011, 2020.

[32] M. Goswami, P. Sharma and A. Bhargava, "Black hole attack detection in MANETs using trust based technique," International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 4, pp. 1446–1451, 2020.

[33] D. M. Khan, T. Aslam, N. Akhtar, S. Qadri and N. A. Khan, "Black hole attack prevention in mobile ad-hoc network (MANET) using ant colony optimization technique," Information Technology and Control, vol. 49, no. 3, pp. 308–319, 2020.