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

WHITE HOLE ATTACKER DETECTION IN MOBILE ADHOC NETWORK

Dr.S.HEMALATHA[1], SONIA MARIA D'SOUZA[2], KHADRI SYED FAIZZ AHMAD[3], M.RAJASEKARAN[4], PANKAJ RANGAREE[5], P. SUKANIA[6], M.POMPAPATHI[7], ASHOK BEKKANTI[8]

[1] Department of Computer Science and Business Systems, Panimalar engineering College, Chennai, Tamil nadu , India .
[2] Department of Artificial Intelligence and Machine Learning, New Horizon College of Engineering, Bengaluru, Karnataka 560103, India.
[3] Department of Computer Science, SRM University, Andhra Pradesh 522502, India.
[4] Department of Computer Science & Engineering, Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh 517325, India.
[5] Department of Electronics and Communication Engineering, Vaagdevi College of Engineering, Warangal, Telangana 506002, India.
[6] Department of Mathematics, R.M.K. Engineering College, Kavarapettai, Tamil Nadu 601206, India.
[7] Department of Information Technology, RVR & JC College of Engineering, Andhra Pradesh , India.
[8] Department of Computer Science & Engineering, Koneru lakshmaiah Education Foundation, Andhra Pradesh 520002, India.
Email : pithemalatha@gmail.com[1], s1985md@gmail.com[2], faizzkhadri@gmail.com [3], rajasekaranm@mits.ac.in [4], phrangaree247@gmail.com[5], psa.sh@rmkec.ac.in[6], manasani.pompapathi@gmail.com [7], ashok.bakkanti@gmail.com[8]

ABSTRACT

While making communication among the wireless nodes, which relies on without making infrastructure less network are vulnerable to security fall. One of the most affecting vulnerable security falling wireless networks is Mobile Adhoc Network. The most predominant kind of security falls are intruders and attackers whose roles are trying to diminish the internal performance of the Network. Many research works are concentrating to detect and prevent these two factors. This article concentrates on predicting white hole attackers inside the communication or not. White hole attackers is a kind of attacker whose role is to send the many duplicate packets to the neighboring node to increase the load of the neighbor nodes which affect the overall Mobile Adhoc network performance . Many existing research used the latest technique to predict the attackers which are additional overload to the network .To achieve this objective the WatchDog method introduces to monitoring the forwarded time of the every nodes present in the communication a node which make plenty of times forwarded the packet to the many nodes assumes as white hole attackers. The proposed Watchdog Algorithm with Classification Technique was implemented with Network simulator and the simulation results are compared with Machine learning based routing protocol then the compared results are proved the WatchDog based attacker methods performs well is more than 30 % better also the performance factors are excellent in 60%.

Keywords: *MANET, Attackers, White Hole Attackers, WatchDog Technique, Forward time, Threshold Value*

1. INTRODUCTION

One of the on demanding wireless networks for making instant communication without support of any basic infrastructure is Mobile Adhoc Network (MANET) as shown in the Figure 1. This Kind of Networks can easily moved instantly to any place and also has an advantage of limiting layers in the protocol stack. Due to this nature MANET was using in many applications like disaster management, earth quake, 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 are penetrated in the

Network make the mitigation on packet transmission.

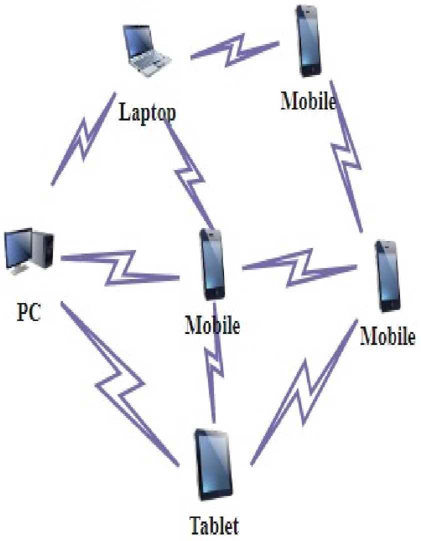

Figure 1 Manet Nodes Architecture

Many research work was carried out for detection and preventing white hole Attackers in the MANET by introducing the novel techniques like Artificial based [9], Machine learning algorithms[21], deep learning algorithms[9] , Data analytic method[16], and Fuzzy logic[19] shown in the Figure 2 ,but still the MANET is lags on security.

Motivation of the Research work

The objective of the research work to carried out white hole attacker in the MANET while making communication. White hole attackers are inverse to the black hole attacker; they send multiple packets to the neighboring node to make the MANET in to disintegrate. The narrow research work is needed to classify what kinds of attacker are participating in the MANET communication. This could be achieved by simple monitoring of forwarding time of the each MANET node. For instant the node forward time for a specific packet is delay , not forwarding selective the packet constantly , and not at all forwarding the packet or forwarding the packet many times are classified in to white hole attacker.

This research work could be achieving my adding WatchDog technique to monitoring the forwarding time of each packets on every node which participating in the communication. This research article is organized as follows: survey related to research work talked in chapter 2, WatchDog Algorithm and classification techniques discussed in chapter 3 studies, proposed research work simulation work mentioned in chapter 4, and conclusion in chapter 5.

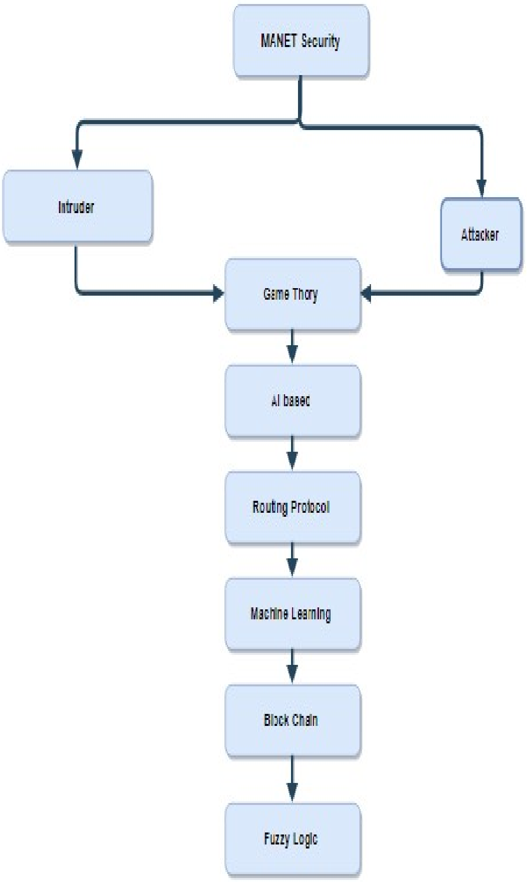

Figure 2 Manet Security Research Classifications

2. LITERATURE SURVEY

Vijayalakshmi et al. [1] 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 %. Set of research work was carried out to detect the attack using protocol. Hanif et al [2] detect wormhole attacker detection in using AI based techniques, Teli et al.[3]detect the black hole and gray hole attack using mitigating techniques.

Shankar [4] proposed secured data transmission using ZRP protocol to provide better QOS while gray whole attack. Hussain et al. [5] proposed AI enabled routing protocol for secured communication. Khanna and Sachdeva [7] uses a taxonomy technique to detect black hole attackers, Sultan, [9] uses deep learning based ANN technique to make detection of IDS, Pandey and Singh [10] done black hole detection using machine learning algorithm , Location aided routing techniques proposed by suma et al. [7] for attackers in MANET .

Rajeshkumar et al. [6] uses cluster trust adaptive ack , Kalman filtering technique, and swarm optimization identify black hole attacker , outcome of this research provides 3.3 % improvement in PDR and 3.5% improvement in male ware detection when comparing with CTAAPSO methods. Khaled Ahmed [11] made research on jelly fish attack in TCP based MANET, jelly fish nodes target the TCP communication mechanism. Black hole detection algorithm proposed by Olanrewaju et al. [12] Using DHMD 5 and compute the performance metric which yield 23% and reduce the memory overhead .Research work done by the authors Pushpender Sarao [13] for multiple attacks solutions like rushing attack, gray hole attack and black hole attack. They conclude that above attacks affect the performance of the network. Block chain based routing protocol proposed by Nitesh Ghodichor [14] to mitigate attacks in MANET and the research work achieves good improvement in delay.

SDPEGH algorithm proposed by the authors Thabiso Khosa et al.[15], result produced 90.9% throughput, 89% Packet delivery ratio, and 5.7% overhead comparing with RSet Theory and GA_BFO algorithms. Along with spider monkey optimization and swarm Intelligence technique proposed by the authors Arunmozhi et al. [16] to detect the black hole attackers and proved the result performs better performance. Timer Entrenched Baited Scheme proposed by the authors Padmapriya [17] to locate the attacker and remove from the network communication also support intelligent dark opening recognition and detachment technique in MANET . Whale Optimized Deep Neural Network Model, Whale Optimization Algorithm) and Deep Neural Network invented by the authors Edwin Singh and Maria Celestin Vigila [18] for detecting intruder in MANET the simulation result of this work produced 99.1% accuracy. S. Fuzzy logic scheme based black hole and gray hole attacker detection method proposed by the Maheswari and R. Vijayabhasker [19] and simulation results achieved greater performance improvement.

Fuzzy based PCA-FELM scheme proposed by the authors Edwin Singh and Maria [20] for detecting intruder in MANET; proposed work was simulated using MAT LAB and results produces 99.08% higher accuracy comparing with DBN-IDS, GOA-SVM and SDAE-ELM.ML-AODV method proposed by haik Shafi et al. [21] for detecting flood and black hole attacks detection simulation results achieves throughput reliability routing over head and pack loss ratio to 4%, 44%, 10 to 15 % respectively. Optimal routing algorithm proposed by Veeraiah and Krishna [22] providing security route path for communication to avoid intruder interfere in the communication. Hybrid routing multipath algorithm for intruder detection proposed by N. Veeraiah *et al [23] to provide trusty communication between the nodes* . Borkar, G. M., & Mahajan [24] discuss the different article supports secure data communication for prevention attack in MANET. Nitesh Ghodichor et al. [25] proposed the routing algorithm for against internal and external attack prevention in MANET nodes communication.

Research related to malicious nodes isolation was done by the authors Thiagarajan et al. [26] with secure optimized approach. Clustering routing approach for finding routing misbehaviour node to indentify the intruder was invented by the authors in Nagaraj et al. [27]. AI with Swarm algorithm with AI for detecting black hole and gray hole attacker proposed by the authors Rani et al. [28] .AI technique incorporated in to MANET to predict the Black hole attacker for making secure communication was proposed by the authors Hassan et al. [29]. Kumari et al. [30] invented the method for creating black hole attack in AODV routing protocol and S. Gurung and S. Chauhan [31] discussed the challenges and survey about black hole attacks techniques in MANET . Trust based techniques were proposed by the authors in Goswaalcmi et al. [31] for black hole detection technique in MANET. Ant colony approach method was discussed in Khan et al [33] for preventing black hole attacker in MANET.

From the literature review many authors uses the different techniques like AI based, machine learning based, clustered based, block chain based and even the trust based methods for preventing and detecting black hole , gray hole and warm hole attacker. Still the research work is more focusing on the MANET to provide solution for preventing such an attacker in MANET.

3. RESEARCH METHODS

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

Let us Assume Graph G (V, E),
Vertices represent the total number of nodes are 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 collection of packets named as Pi = {P1, P2, and P3…..Pm}.
Every packet pass several intermediate node to reach to the destination.
Let have Collection of intermediate nodes from S to D = {I1, I2, I3 …In}

WatchDog technique used for monitor the every node activity forwarded time. This estimated forwarded time only support for classifying the node is white hole attacker . Every node forwarded time is calculated from the equation

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

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

The time taken for a packet reach to the destination is computed with the principle of time of flight. A threshold value δ 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 normal node 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 category of beacon signal named as Beacon signal arrival time B_{at} , Beacon signal Transmission time $B_{tt.}$ the difference between this two times is called distance from Source to Destination d.

d=(Bat - Btt) *(Eq 2)*

Source Node RREQ →Intermediate Node →Destination Node (Eq 3)

Destination Node RREP →Intermediate Node RREP →Source Node (Eq 4)

To differentiate malicious and normal node along with the route path

Malicious Node where Ft > threshold value δ (Eq5)

Normal Node where Ft ≤ threshold value δ (Eq 6)

Algorithm 1

The algorithm for determine the WatchDog role as follows

1. Let S be the source node and D be the destination node
2. Using 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 WatchDog classification,
4. WatchDog perform the comparison using the Eq 1 to 6.
5. If any malicious node detected call classification technique
6. Alert malicious node
7. Start finding new path and forwarding the packets

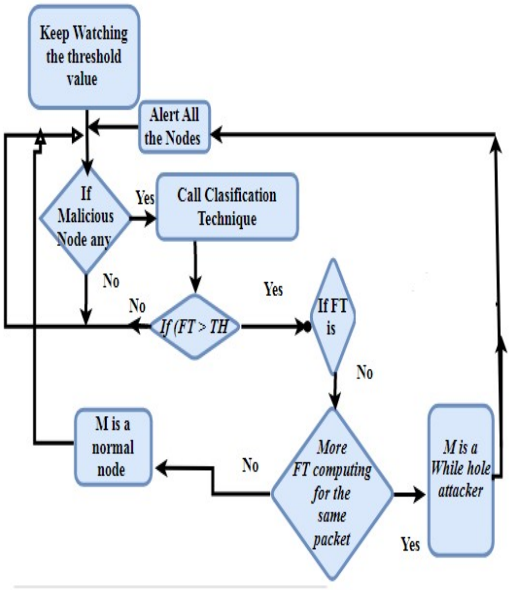
Keep Watching the threshold value
Alert All the Nodes
If Malicious Node any
Yes
Call Clasification Technique
No
No
If (FT > TH
Yes
If FT is
No
M is a normal node
No
More FT computing for the same packet
Yes
M is a While hole attacker

Figure 3 Watchdog And Classification Technique Flow Chart

Classification technique (Malicious Node)

```
{
//Here the classification of malicious node in to White hole attacker or a normal node
If (Forward time > threshold Value)
{
Check forward time for all the packets form the malicious node
        if (selective packet forward time varies)
        return Node M is a normal node
        Elseif (More forward time computing for
the same packet)
                Node M is a White hole attacker
        else M is a normal node
}
return M
}
```

WatchDog algorithm stages define in the Algorithm 1 and working flow chart shown in the Figure 3. 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 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 WatchDog for processing the nodes and find out any attacker present in the route. All the computation is done once the variation of the threshold vales detected.

When the threshold values varies suspected node forward to the classification function where the nodes will be finalized it is a normal node or an attacker. Classification function is established to check the forwarded time of the malicious node.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 more than one forward time is estimated for the single packet then the node is a white hole attacker since which try to flood the packet to many nodes.

4. SIMULATION RESULT

Simulation of WatchDog technique based White hole attacker classification is named as WDWHA model (WDWHA -AODV) which is simulated using Network simulator 2.34. Table 1 for metric value defined used for simulation. Defined Network area is 1000 m* 1000m and nodes are varying ranges from 50, 100, and 150 and so on up to 300. Simulation time 300 sec and random mobility among the nodes are set .Speed of the mobility node is maximum 25 ms, and protocol used for route selection is AODV.

Figure 4 depict stages to carry out the proposed model in the simulation. Well defined system model done from the chapter 3, outcome of the system model with the WatchDog algorithm and simulation set up pass to the NS 2.34.Simulator done the classification of the nodes, in to the normal or malicious node. Malicious node is forwarded to the classification, classifier detect that malicious is a normal node or white hole attacker .Data set receive from the simulation are plotted as a graph by comparing with ML-AODV [7] protocol. Finally conclude the proposed work outcomes.

Table 1 Metric Value Used For Simulation

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*

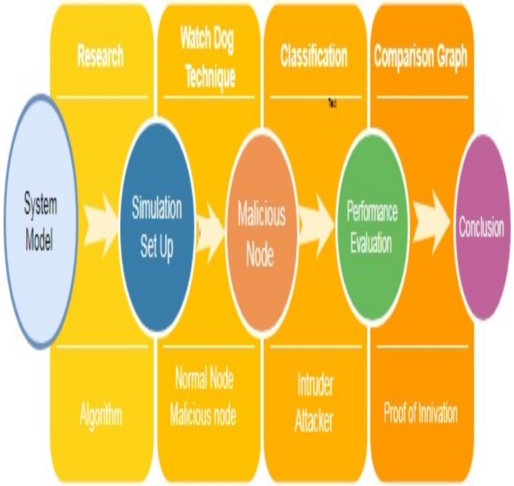

Figure 4 Proposed Model Simulation Stage

Initially, the proposed work will be work by setting the source node and destination node .when the simulation starts running the Route Request is send from the source to reach to destination, destination node send route reply. This makes the route path between the sources to the destination. Second stage the Source send the packet one by one parallel the WatchDog start collecting the forwarded time of the all intermediate node, when the threshold level greater the forwarded time then classification function invoked to classify the node is a normal node or white hole attacker. Finally the MANET malicious node are alert in to the MANET , and find a new route part then start transmitting of the packets as new.

The data received from the NS 2.34 node ID, data send, transmission time, Data received, types of attack nodes. ML-AODV protocol without WatchDog and classification algorithm values are taken for the performance comparison.

Attack Rate Comparison

Attack rate is computed as a ratio between the total number of nodes currently detected as a normal or malicious with total number of nodes in percentage. Simulation result shows high attack rate when the proposed work is more efficient. The data collected from the simulation is shown the comparisons result in pictorial representation is depicted in the Figure 5, the results proven that proposed AODV with WDWHA -AODV model works 30 percent than existing ML-AODV.

$$Attack\ Detection = \frac{Total\ number\ of\ normal\ or\ malicious\ node}{Number\ of\ Nodes} X100 \qquad (Eq7)$$

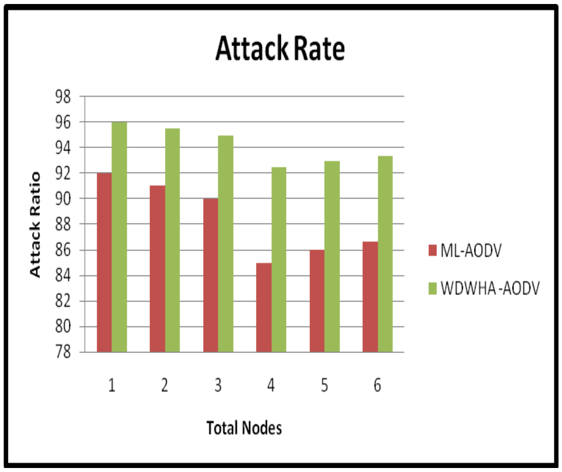

Figure 5 Attack Rate

Attack Detection Time

This is the measurement time taken for identification of first malicious node.
ADT = n* t (Detecting First Malicious Node)

Where n is the total node and t is time taken for detecting first malicious node.

Simulation result lesser attack detection method is efficient. The ML-AODV without WDWHA -AODV model detect the attacker in 0. 3ms where proposed AODV WDWHA -AODV model detect the attacker in 0.2 ms. which exhibit that proposed WDWHA -AODV model comparing with AODV good in 25% performance. The Figure 6 depicted the simulation value received and comparison graph plotted between the estimated values which shows that proposed WDWHA -AODV model attacker detection time is less 0.4m/s of traditional ML-AODV 0.7m/s.

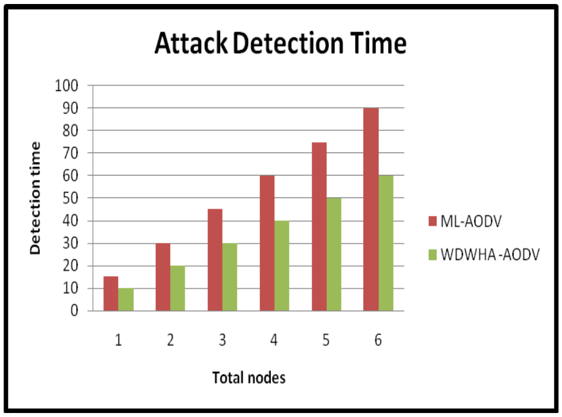

Figure 6 Attack Detection Time

Packet Delivery Ratio

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

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

Initially the packet are started send is set from 10,and slowly increasing by 20,30,40,50,60,70, The dropped packet are listed in the comparison chart shown in the Figure 7 , in which the proposed WDWHA -AODV model packet delivery ratio is high ranging from 70 % to 84% where as traditional Packet Delivery ratio is 60% to 70% .

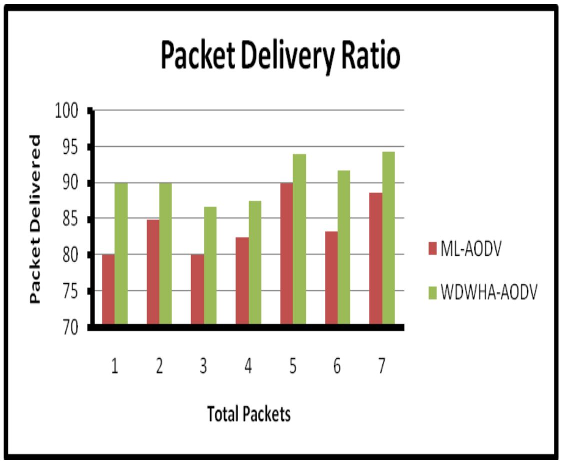

Figure 7 Packet Delivery Ratio

End to End Delay

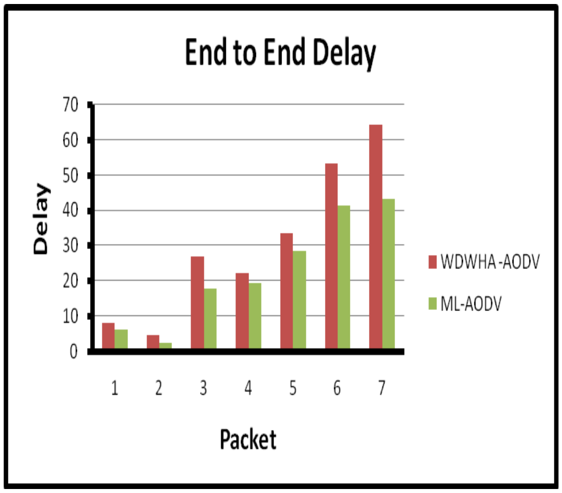

Figure 8 End To End Delay

End to End delay estimated as the time difference between packet send from the source to packet arrival at destination. Packet send from the sender side delay is 0ms but there is varies delay at the destination node which is shown in the Figure 8 shows the comparison chart of delay between the traditional ML-AODV and Proposed WDWHA - AODVT model where the proposed model delay is less varies from 6.2% to 43.4 % .

5. CONCLUSION

This article focuses on detecting White hole attackers are present in the communication of the MANET routing. This is achieved by introducing the WatchDog Algorithm and classification technique based on the forward time and threshold value. The outcome of the research out whether the malicious node is a normal node or white hole attacker. Simulation of the proposed work done with NS2.34 and the revealed result are computed with the metric of attack rate, attack detection time, packet delivery ratio and End to End Delay. Simulation result in all the factors the proposed methods proved best result overall MANET metric value are increased to 30 % better also the performance factors are excellent in 60%.

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 26659174,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..