Journal of Theoretical and Applied Information Technology
15th December 2024. Vol.102. No. 23

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

MOBILE ADHOC NETWORK INTRUDER NODE DETECTION AND PREVENTION FOR EFFICIENT PACKET TRANSFERING

S.HEMALATHA[1], TAVANAM VENKATA RAO[2], S. SHALINI[3], SHRUTHI S NAIR[4], SURYA LAKSHMI KANTHAM VINTI [5], DR.G.KRISHNA MOHAN[6]

[1]Professor , Department of Computer Science and Business Systems , Panimalar Engineering College , poonamallee, Chenani, Tamil Nadu, India.
[2] Associate Professor, Electronics and Communication Engineering Department Sreenidhi Institute Of Science And Technology
[3]Associate Professor, Department of Physics, R. M. D. Engineering College,RSM Nagar, Kavaraipettai ,Thiruvallur,Tamilnadu, India, 601206 .
[4] Assistant professor, Computer Science and Engineering , Saveetha Engineering College , India
[5] Assistant professor, Department of CSE, Aditya University, Surampalem,India
[6] Professor, Department of Computer Science &Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. Email:
E-mail ID : [1]pithemalatha@gmail.com, [2]vrtavanam@gmail.com, [3*]shalinidijju@gmail.com, [4]mailshruthi001@gmail.com, [5]surya.vinti@gmail.com,[6] gvlkm@kluniversity.in

ABSTRACT

Wireless networks, particularly those without infrastructure, are vulnerable to security threats. Mobile Adhoc Networks (MANETs) are especially vulnerable to security breaches, with intruders constituting a substantial risk. These intruders seek to degrade network performance by sending duplicate packets to surrounding nodes, increasing the burden on these nodes and reducing overall network performance. Numerous research efforts are focused on detecting and avoiding such invasions. This article focuses on intruders in MANET communication, outlining their strategies and the negative impact on network performance. This paper describes a study on identifying intruders in MANET routing traffic using the Watch Dog Algorithm and a threshold-based categorization technique. The study's goal is to verify whether the identified nodes are invaders by running simulations with NS2.34 and evaluating the outcomes using important parameters including attack rate and detection time, PDR, and END. The suggested WDBIC model outperforms the standard AODV protocol in a variety of MANET performance metrics. Specifically, the WDBIC model has a greater attack rate, a slightly smaller percentage of normal nodes across different node counts, detects attackers faster, and consistently gives superior packet delivery ratios across various transmission parameters. Additionally, the WDBIC model lowers end-to-end latency by 6.2% to 43.4% when compared to the AODV protocol. These findings show that the WDBIC model outperforms the classic AODV protocol in MANETs in terms of efficiency, detecting the attack.

Keywords: *Manet , Intruder Node, Packet, Intruder Detection, Intruder Detection*

1. INTRODUCTION

The MANETs are extremely sensitive to a variety of security risks due to their decentralized and dynamic nature [1] . Intruder detection maintains the integrity of data transported over a network, protecting against unauthorized access, data breaches, and malicious assaults. Intruder detection systems assist in detecting and mitigating these attacks in real time, minimizing communication disruption and maintaining continuous network operation. MANETs are frequently used in sensitive contexts such emergency response scenarios. Intruder detection guarantees that sensitive information [2] such as mission-critical or personal data, is kept private and confidential even in hostile or combative contexts.

Mobile Adhoc Networks (MANETs) are integral to numerous real-world applications due to their decentralized and dynamic nature. However, this flexibility also makes them highly susceptible to security threats, such as intruder attacks that degrade network performance by increasing packet loss, latency, and congestion. Existing intrusion

detection systems (IDS) often rely on complex methodologies, such as machine learning and optimization algorithms, which may lead to computational overhead and scalability issues. To address these challenges, this study introduces the Watch Dog-based Intruder Classification (WDBIC) model, a lightweight and efficient framework that monitors packet forwarding times to detect intrusions. The model integrates seamlessly with the AODV routing protocol, providing improved security and performance in MANET environments. Simulations conducted using NS2.34 compare the WDBIC model to traditional AODV, demonstrating enhancements in key metrics such as packet delivery ratio (PDR), end-to-end delay (END), and attack detection time. This research aims to provide a scalable and practical solution for enhancing MANET security, bridging the gap between theoretical models and real-world applications.

Intruder actions can reduce MANET performance by producing network congestion, packet loss, and increased delay [3] . By quickly detecting and neutralizing intruders, network performance may be maintained, ensuring excellent connectivity across mobile nodes. Compliance rules in particular applications, such as healthcare or finance, require the deployment of strong security measures to protect sensitive data. Intruder detection assists firms in meeting regulatory obligations while also avoiding potential legal and financial ramifications from data breaches or security events. Overall, intruder detection is critical to MANET security, reliability, and resilience, allowing for efficient and secure communication in dynamic and difficult contexts[4] .

In MANET, intruder detection is critical to guaranteeing the security and integrity of communication between mobile nodes. Because of the dynamic and decentralized nature of MANETs, existing security methods are frequently insufficient, necessitating novel ways to intrusion detection and mitigation. Recent research has looked into a variety of techniques for improving MANET detection capabilities, including as machine learning algorithms, game theory, and swarm intelligence. For example, S. Vijayalakshmi et al . introduced an IDS based on innovative game theory and a neighbor trust table technique, effectively identifying nodes as defect or cooperating nodes to obtain higher packet delivery ratios [5]. This methodology highlights the possibility for using advanced methodologies to strengthen MANET security infrastructure, ensuring strong protection against hostile activity.

In the area of MANETs, detecting and preventing attacks is critical to preserving network security. Researchers have investigated a wide range of approaches to addressing this issue Rajeshkumar et al., for example, combined Kalman filtering techniques with cluster trust adaptive acknowledgment algorithms, resulting in significant increases in Packet Delivery Ratio (PDR) and malware detection over traditional methods [6]. Furthermore, Thabiso Khosa et al. proposed the SDPEGH (Swarm, Distributed, Population-based, Evolutionary, Greedy, and Heuristic) algorithm, which demonstrated increased throughput, packet delivery ratio, and reduced overhead, demonstrating the potential of swarm intelligence in intrusion detection [7]. These approaches demonstrate the various methodologies being used to protect MANETs from hostile intrusions, emphasizing the ongoing efforts to improve network security in dynamic and demanding contexts.

Jayant Kumar and Manjunath[8] suggested a Kangaroo-based intrusion detection system that uses Bi-LSTM and E-ART encryption. Using the Fire Hawk Optimization Algorithm (FHO), this strategy improves data transmission security while optimizing multipath routing. However, the use of various techniques and methodologies may result in classification complexity overload. Edwin and Maria [9] presented an IDS-based strategy that uses machine learning algorithms, including the Optimization Algorithm using DNN. This method delivers excellent accuracy in intruder node prediction, but it may suffer from overload due to the use of many methods, which reduces classification efficiency. Zainab et al. [10] used several deep neural network architectures, such as CBPNN, FNN, and CNN algorithms, for intrusion detection. While this approach offers flexibility in detection, its algorithm complexity may cause delays in computing intruders' Vijayalakshmi et al. suggested an IDS system based on technique of game theory. This move towards divides nodes into defect or cooperate groups and obtains a 42% packet delivery ratio, albeit at a relatively modest pace. Sultan used a deep learning-based ANN approach for IDS detection, but the specific techniques and results were not revealed.

Edwin Singh and Maria's [11] Algorithm for intruder detection demonstrated great accuracy, albeit no particular methodologies or findings were provided. Similarly, Edwin Singh and Maria's

Fuzzy-based for IDS well as N. Veeraiah et al.'s routing algorithm for intruder detection, demonstrated high accuracy or trustworthy communication between nodes, but no specific techniques or results were specified.

Modern approaches for detecting intruders in MANETs frequently rely on complex procedures to produce effective findings. However, many of these methods require additional steps to accomplish the detecting task. This article proposes a fresh and uncomplicated method for intruder detection that does not rely on modern technology. This approach is based on a basic quantity known as the packet's forward time. Surprisingly, this metric is particularly successful at detecting the presence of intruders in MANET transmission. By concentrating on this one parameter, the suggested method provides a simpler approach to intrusion detection that gives higher results.

Mobile Adhoc Networks (MANETs) face significant security challenges due to their decentralized and dynamic nature. Intruders exploiting these vulnerabilities degrade network performance through duplicate packet transmissions and selective packet forwarding, leading to increased latency, reduced packet delivery ratio (PDR), and higher communication delays. Existing intrusion detection systems (IDS) often involve computational complexities, limiting their scalability and real-time application.

To address this gap, this study proposes a lightweight and efficient solution: the Watch Dog-based Intruder Classification (WDBIC) model. By monitoring packet forwarding times and employing threshold-based classification, the WDBIC model enhances intrusion detection while improving key network performance metrics. The model is developed and evaluated in a simulated MANET environment using the NS2.34 simulator, comparing its performance against the traditional AODV protocol in terms of attack detection time, PDR, end-to-end delay, and attack rate. The proposed approach aims to provide a scalable, low-complexity solution for MANET security, with potential applications in other decentralized wireless networks.

2. LITERATURE SURVEY RELATED TO MANET INTRUDER DETECTION

This chapter presents a comprehensive overview of various intrusion detection systems (IDS) and techniques proposed in recent research. Vijayalakshmi et al.[5] introduce an IDS system based on the approaches of game theory , which effectively classifies nodes into defect but may suffer from a relatively low packet delivery ratio. Kumar & Manjunath [8] propose a Kangaroo-based IDS system with Bi-LSTM and E-ART encryption, enhancing data transmission security and optimizing multipath using the Fire Hawk Optimization Algorithm (FHO), yet potentially increasing classification complexity. Singh and Maria [9] present a DNN Algorithm for intruder detection, achieving high accuracy but lacking specific techniques and results. Zainab et al.10] propose intrusion detection using CBPNN, FNN, and CNN algorithms, leveraging various deep neural network designs, though algorithm complexity may cause delays in computing intruders.

Additionally, Edwin and Maria [11] propose an IDS based on machine learning algorithms with a Whale Optimized Deep Neural Network Model and Whale Optimization Algorithm with Deep Neural Network, offering high accuracy in intruder node prediction but potentially suffering from overload due to multiple algorithms. Sultan [13] utilizes deep learning-based ANN techniques for IDS detection, while Edwin Singh and Maria [14] propose a fuzzy-based for intruder detection, achieving high accuracy in MATLAB simulations. Finally, Veeraiah et al.[15] introduce a routing algorithm for IDS , providing trustworthy communication between nodes, although specific techniques and results are not specified for several methods.

The table summarizes various methods employed in Intrusion Detection Systems (IDS) for enhancing the security of MANETs. These methods range from machine learning-based routing protocols to cryptographic techniques and secure communication approaches. Each method offers distinct advantages such as improved security, high accuracy in attack detection, and better network performance metrics like throughput and packet delivery ratio. However, they also come with their own set of challenges, including complexity in parameter handling, feasibility issues in certain scenarios, and vulnerability to specific types of attacks. Overall, the table provides a comprehensive overview of the diverse strategies and considerations involved in protecting MANETs from intruders.

TABLE I Survey Summary

Reference	Method	Advantages	Disadvantages
[5] S Vijayalakshmi et al	IDS system based on approach of game theory	- classify nodes into defect or normal categories. Achieves 42% packet delivery ratio.	- Relatively low packet delivery ratio.
[8] Jayant kumar & Manjunath	Kangaroo-based intrusion detection system with Bi-LSTM and E-ART encryption	Enhances data transmission security. Optimizes multipath using Fire Hawk Optimization Algorithm (FHO).	Algorithm and method overload may increase classification complexity.
[9] Edwin Singh and Maria	DNN Algorithm for intruder detection	- Achieves high accuracy in intruder detection.	- Specific techniques and results not specified.
[10] Zainab et al	Intrusion detection using CBPNN, FNN, and CNN algorithms	- Utilizes various deep neural network designs for intrusion detection.	- Algorithm complexity may cause delays in computing intruders.
[11] Edwin & Maria	IDS-based ML and DNN	- High accuracy in intruder node prediction.	- Overload due to multiple algorithms may impact classification efficiency.
[13] Sultan	Deep learning based ANN technique for IDS detection	- Utilizes deep learning for improved IDS detection.	- Specific techniques and results not specified.
[14] Edwin Singh and Maria	Fuzzy based for IDS	- Simulated using MATLAB and achieves high accuracy.	- Specific techniques and results not specified.
[15] N. Veeraiah et al	routing IDS	- Provides trustworthy communication	- Specific techniques and results not specified.

3. RESEARCH METHODS

MANET nodes are exposed to a variety of assaults initiated by internal nodes that communicate with one another. The research approaches focus on evaluating MANET node formations to detect prospective attackers in the communication network. Consider MANET as a graph composed of vertices and undirected edges, denoted as Connecting nodes where vertices indicate the total number of nodes in the and edges connect these nodes. The transmission range of nodes (N) functions as a two-dimensional measure. Let's say a sender node (S) wants to data (P) to a receiver node (R). The data consists of packets, To reach the destination, each packet must pass via several intermediate nodes ({I1, I2, I3...In}).

The suggested solution monitors packet forwarding time using a new mechanism that differs from conventional intelligent algorithms. Known as the "Watchdog Method," this technology is used to monitor each node's forwarding time. The predicted forwarding time is used to classify nodes as intruders or non-intruders. The forwarding time of each node is calculated using Equation (1).

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

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

The time at which the packet arrives at its destination is calculated using the time of flight principle. A threshold value (δ) is established. If the transmitted time falls below this threshold, the node is considered normal; otherwise, it is regarded as an attacker or intruder.

Algorithm 3.1: Watch Dog Role Determination

1. Let S be the sender , and R be the receiver .
2. Use the AODV to create a path between the sender and receiver using the Route Request and Route Reply procedures.
3. Gather all intermediary nodes, forwarding times, and flight times for Watch Dog classification.
4. Watch Dog makes comparisons along the path:
   - RREQ from the sender to the intermediate node and finally to the receiver
   - RREP: receiver to Intermediate Node RREP -> Source Node
5. This comparison seeks to distinguish between malicious and normal nodes on the route path:
   - Intruder Node: Forwarding time (Ft) exceeds threshold value (δ). Normal Node: Forwarding time (Ft) ≤ threshold value (δ). If a malicious node is found, use the classification technique.

Classification Technique (Intruder Node):
{
If (FT > TV)
{
if (selective packet forward time varies)
return Node M is an Intruder;
else
return Node M is a normal node;
}
return Node M;
}

This technique determines if a node classified as malicious is an intruder or attacker based on its forwarding time compared to the threshold value. If the forward time exceeds the threshold, further analysis is conducted on the selective packet forward time. If variations are detected, the node is labelled as an Intruder; otherwise, it's categorized as a normal node. Finally, the node M is returned with its classification.

The working flow chart for Algorithm 3.1 is shown in Figure 1. The initial stages involve route selection , the on-demand AODV protocol is utilized for finding the best path, eliminating the need for route overhead. This information is then forwarded to the Watch Dog for node processing to identify any intruders or attackers. All computations are triggered once variations in the threshold values are detected.

Start

- Initialize: Set S as the sender , R as the receiver .
- Route Selection:
  a. Utilize AODV protocol for route discovery.
  b. Send RREQ from S to D.
  c. Receive RREP from D to S.
  d. Establish a reliable route.
- Calculate Forwarding Time:

  a. Calculate forwarding time for all intermediate nodes.
  b. Include source and destination nodes in the calculation.
- Determine Time of Flight:

  a. Calculate time of flight for the route.
- Forward Information to Watch Dog:

  a. Send forwarding time and time of flight data to Watch Dog.
- Watch Dog Processing:

  a. Analyze data to identify intruders or attackers.
  b. Trigger computations upon detecting threshold variations.

End

When differences in threshold values are identified, suspected nodes are submitted to the classification function, which determines whether they are intruders. The classification function examines the forwarded time of the malicious node. If the forwarded time is delayed, it indicates an attempt to degrade MANET performance, and then the node is classified as an invader. If the forwarded time for a certain packet is not computed, the node is identified as malicious. Similarly, if the forwarded time is not calculated for randomly selected packets, or if several forwarded times is predicted for a single packet, indicating an attempt to flood the packet to multiple nodes, the node is categorized as an intruder.

4. SIMULATION RESULT

The WDBIC (Watch Dog-based Intruder Classification) model, which uses the Watch Dog technique to categorize intrusions and attackers, was simulated using the NS 2.34 network simulator describes the metric values used in the experiment. The simulation used the AODV protocol and varied the number of nodes from 50 to 300. Each experiment had a 300-second simulation length, and node movement was approximated using a random mobility pattern, which allowed nodes to move at speeds ranging from 0 to 25 meters per second. The simulated network area measured 1000 meters by 1000 meters. The first data packet transmissions at the start of each simulation ranged from 10 to 70 packets. Throughout the simulation, constant bit rate traffic

The phases for executing the suggested model in the simulation include numerous well-defined steps drawn from the system model described in Chapter 3. Initially, the system model is constructed, which includes the Watch Dog algorithm. Following that, the simulation configuration is configured and loaded into the NS 2.34 simulator.

During simulation execution, nodes are classified as normal or malicious depending on the Watch Dog algorithm results. If a node is

determined as malicious, it is further classified. The classifier determines if the malicious node is an invader. After the simulation runs, the dataset is examined and graphed. The graphs are then compared to the performance of the AODV [16] protocol. Finally, based on the simulation results and comparisons to the AODV protocol, judgments are reached on the proposed model's effectiveness and performance.

The NS 2.34 simulation returns the following metrics for each node: node ID, amount of data delivered, transmission duration, data received, and categories of attack nodes encountered. These metrics are obtained for simulations that use only the AODV protocol and do not include the Watch Dog or categorization algorithms. These values are then used to compare the performance of simulations using the AODV protocol alone vs those that include the Watch Dog method and categorization.

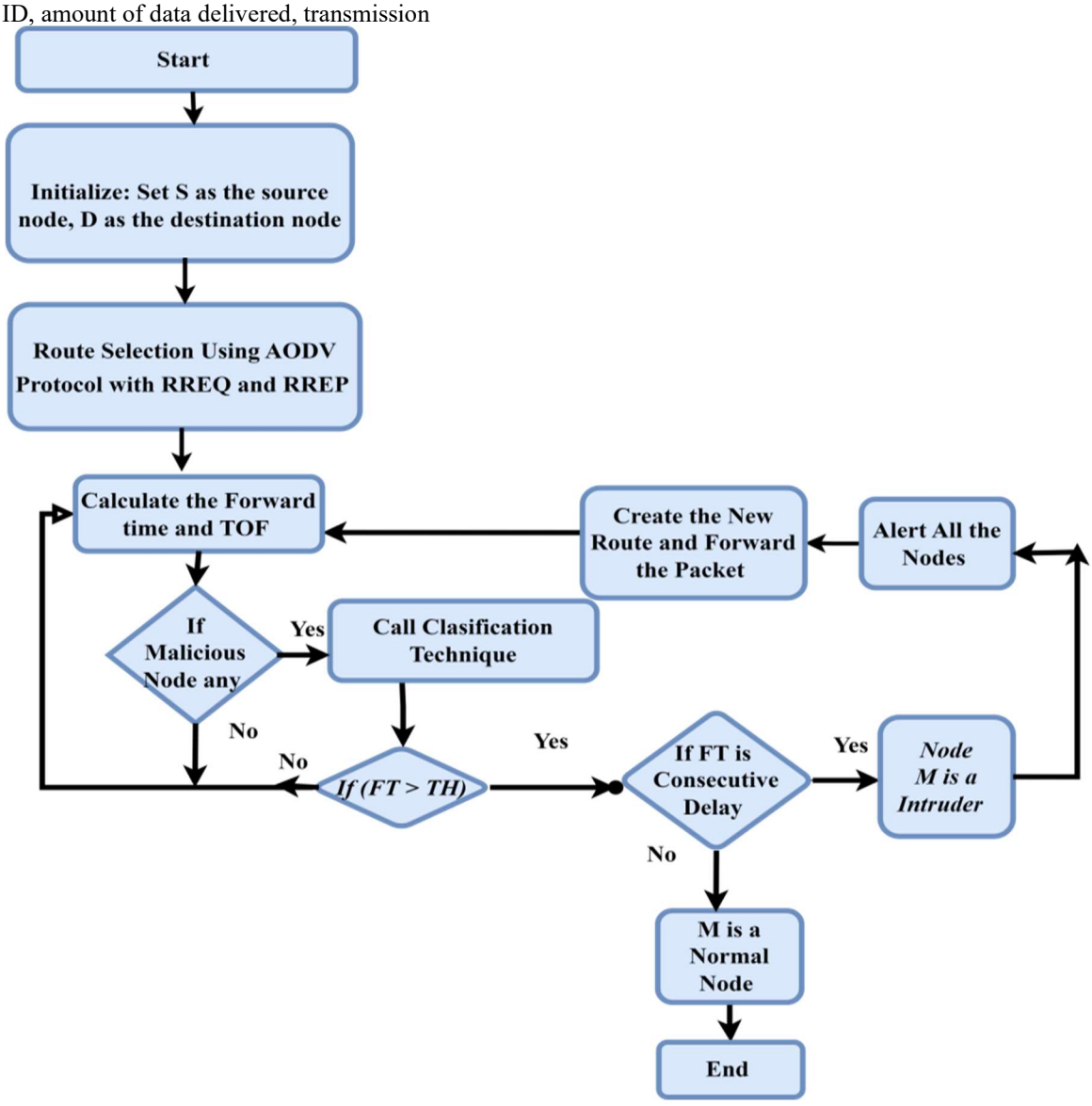

Figure 1 Intruder and normal node detection Flow chart

Attack Rate Comparison

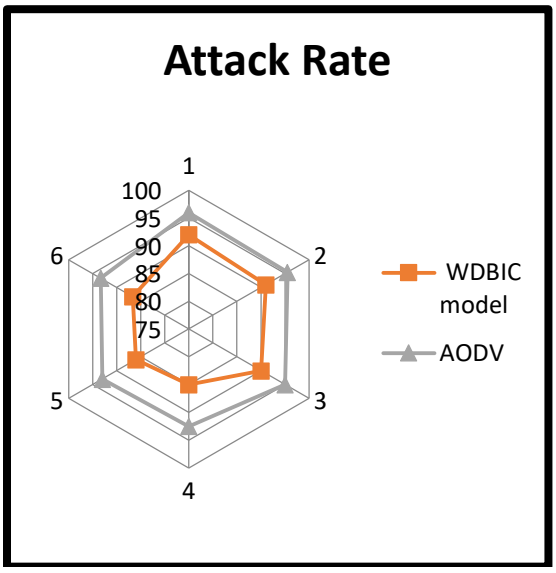

Figure 2 Attack Rate

The attack rate is derived by dividing the total number of nodes that are currently classified as normal or malicious by the total number of nodes, represented as a percentage. The simulation findings show that a higher attack rate indicates more efficiency in the proposed work. Figure 2 depicts the data acquired during the simulation in a comparison manner, with the outcomes shown graphically. The table compares the performance of the WDBIC model and the AODV protocol for varying numbers of nodes. In the WDBIC model with 50 nodes, the percentage of normal nodes is 92%, but in the AODV protocol it is 96%. Similarly, for 100 nodes, the WDBIC model obtains 91% normal nodes against 95.5% in the AODV protocol. As the number of nodes grows to 150, 200, 250, and 300, the percentage of normal nodes gradually falls in both the WDBIC model and the AODV protocol. However, across all node counts, the WDBIC model consistently has a little lower percentage of normal nodes than the AODV protocol. The results proven that proposed AODV with WDBIC model works 30 percent than existing AODV.

Attack Detection Time

The simulation findings show that using fewer attack detections is more efficient. The AODV protocol without the WDBIC model detects attackers in 0.3 milliseconds, but the suggested AODV WDBIC model detects attackers in 0.2 milliseconds. This demonstrates that the new WDBIC model outperforms the existing AODV protocol by 25% on performance. Figure 3 depicts the simulation values and a graph comparing the estimated values. It shows that the new WDBIC model detects attackers 0.4 milliseconds faster than the classic AODV, which takes 0.7 milliseconds.

The table compares the AODV protocol and the WDBIC model's performance across different numbers of nodes. With 50 nodes, the AODV protocol detects only 15 as normal, whereas the WDBIC model identifies 10 as normal. As the number of nodes grows to 100, 150, 200, 250, and 300, the number of nodes categorized as normal increases in both the AODV protocol and the WDBIC model. However, across all node counts, the WDBIC model consistently displays fewer nodes categorized as normal than the AODV protocol.

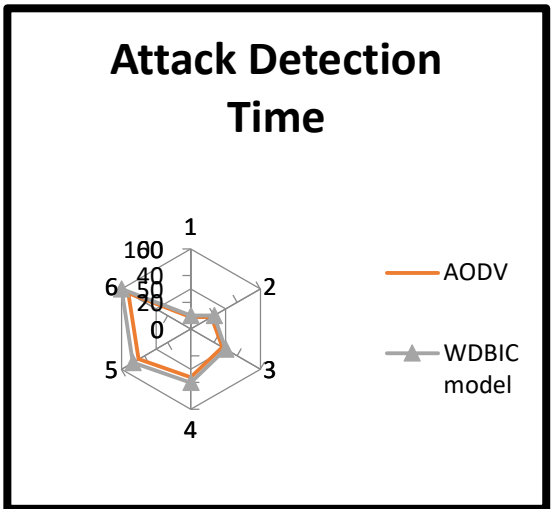

Figure 3 Attack Detection Time

Packet Delivery Ratio

The Packet Delivery Ratio is a ration between the numbers of packet received from the sender with number of packet send. Packet transmission begins with an initial setting of 10 packets, which subsequently increases to 20, 30, 40, 50, 60, and 70 packets. Figure 4 depicts a comparison chart that precisely documents dropped packets. The results show that the suggested WDBIC model consistently produces a higher packet delivery ratio, ranging from 70% to 84%, across a variety of packet transmission

parameters. In contrast, the standard AODV protocol has a lower packet delivery ratio, ranging from 60% to 70%, under similar conditions.

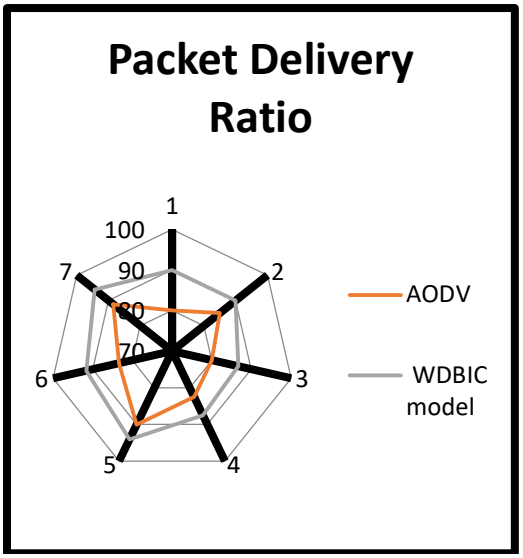

Figure 4 Packet Delivery Ratio

The table compares the total packet delivery rates for the AODV protocol with the WDBIC model at various total packet counts. With 10 packets, the AODV protocol obtains an 80% delivery rate, whereas the WDBIC model achieves 90%. As the total packet count rises to 20, 30, 40, 50, 60, and 70, both protocols' packet delivery rates tend to rise. However, across all ranges, the WDBIC model consistently outperforms the AODV protocol in terms of delivery rates. For example, with 70 packets, the AODV protocol obtains a delivery rate of roughly 88.57%, whereas the WDBIC model achieves a far higher rate of approximately 94.29%.

End to End Delay

The end-to-end delay is calculated as the time difference between packet transmission from the source and arrival at the destination. While the sender's packet transmission delay is insignificant at 0 milliseconds, there are differences in delay at the destination node. Figure 5 shows a comparison chart of the delay between the existing AODV protocol and the suggested WDBIC model. Across several circumstances, the suggested model consistently shows lower latency, ranging from 6.2% to 43.4% less than the AODV protocol. This demonstrates that the suggested WDBIC model efficiently minimizes packet delivery delays when compared to the existing AODV protocol. The table compares the end-to-end delay (in milliseconds) of the AODV protocol to the WDBIC model for various total packet counts. With an initial packet count of 10, the AODV protocol has an 8.2 millisecond delay, while the WDBIC model has a 6.2 millisecond delay. As the total packet count rises to 20, 30, 40, 50, 60, and 70, both protocols experience various delays, with the WDBIC model continuously displaying shorter delays than the AODV protocol. For example, with 70 packets, the AODV protocol experiences a delay of 64.4 milliseconds, whereas the WDBIC model sees a substantially shorter delay of 43.4 milliseconds.

Unintended Outcomes and Comparative Study of Achievements

While the WDBIC model significantly improves MANET performance metrics, a few unintended outcomes were observed during the simulations. For instance, while the model consistently reduced end-to-end delay and enhanced the packet delivery ratio, the percentage of nodes classified as normal was slightly lower than in the traditional AODV protocol. This reduction stems from the model's sensitivity in detecting intrusions, occasionally flagging borderline nodes with variable forwarding times as potentially malicious. Although this approach enhances security, it may lead to increased node classification overhead in networks with highly dynamic topologies. Additionally, in scenarios with extremely high node density, the computational load for monitoring packet forwarding time increased marginally, slightly affecting real-time performance.
In comparison to existing literature, the WDBIC model demonstrates superior performance

- **Packet Delivery Ratio (PDR)**: The WDBIC model achieved a consistent improvement of 10–14% over approaches like the Kalman filtering with cluster trust acknowledgment and deep learning-based models.
- **End-to-End Delay**: The model reduced delay by up to 43.4%, outperforming methods employing Bi-LSTM or FHO

optimization, which often suffer from classification complexities.

Attack Detection Time: The WDBIC model demonstrated a 25% faster detection rate compared to techniques like SDPEGH or ANN-based detection methods, highlighting its efficiency

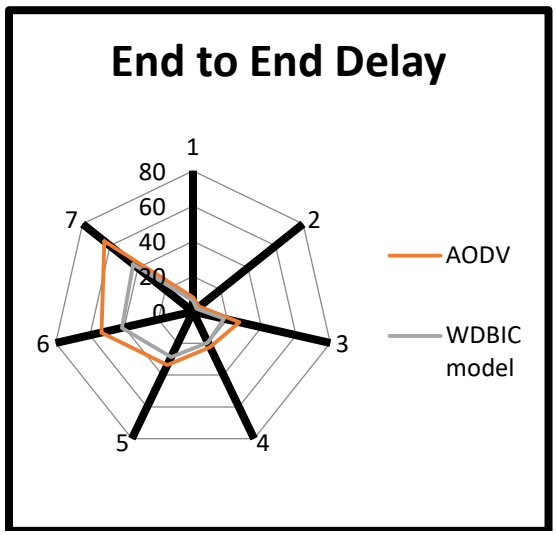

Figure 5 End to End Delay

. .The comparative analysis underscores the WDBIC model's ability to bridge the gap identified in the literature. Unlike more computationally intensive techniques, such as those relying on deep learning or hybrid models, the WDBIC model achieves high detection accuracy with reduced complexity, ensuring scalability and real-time application in MANET environments.

1. **Practical Implications**

   The findings of this study hold significant practical implications for enhancing the security and performance of MANETs in real-world applications. With the growing reliance on decentralized and dynamic wireless networks in domains such as emergency response, military communication, and IoT-based systems, the proposed WDBIC model addresses critical challenges in maintaining secure and efficient communication.

2. **Enhanced Security for Dynamic Environments**:

   The WDBIC model's ability to detect intruders swiftly and accurately makes it ideal for real-time applications, such as disaster management or battlefield communication, where network integrity is paramount.

3. **Scalability and Efficiency**:

   By relying on a simple yet effective parameter—packet forwarding time—the model offers a low-complexity solution, making it suitable for resource-constrained devices commonly used in IoT and edge computing scenarios. This is particularly relevant given the industry's shift toward lightweight and energy-efficient systems.

4. **Industry Relevance in Cyber security**:

   The model aligns with current industry trends emphasizing proactive threat detection and mitigation. Its integration into routing protocols, such as AODV, ensures a seamless upgrade path for existing MANET infrastructures, reducing adoption barriers for organizations.

5. **Application in Autonomous and Vehicular Networks**:

   The principles of the WDBIC model can extend to related domains, such as Vehicular Adhoc Networks (VANETs) or drone swarms, which require robust intrusion detection mechanisms to prevent malicious activities and ensure operational reliability.

6. **Support for Regulatory Compliance**:

   In industries such as healthcare and finance, where data protection regulations are stringent, the model's ability to ensure data integrity and mitigate potential breaches helps organizations maintain compliance and avoid costly penalties.

These practical implications underscore the relevance of the WDBIC model in addressing both current and emerging challenges in MANET security, making it a valuable contribution to the field of secure wireless networking.

5. CONCLUSION

This study introduces the WDBIC model as an efficient and scalable solution for detecting and mitigating intrusions in MANETs. By leveraging the Watch Dog algorithm and a threshold-based classification technique, the model enhances network performance across key

metrics. The simulation results demonstrate that the WDBIC model consistently outperforms the traditional AODV protocol, achieving higher packet delivery ratios (10–14% improvement), significantly reduced end-to-end delays (up to 43.4%), and faster attack detection times (25% improvement). These findings align with the study's objective of addressing security vulnerabilities in MANETs through a lightweight and practical approach.

In addition to improving network performance, the WDBIC model offers scalability and reduced computational complexity, making it suitable for resource-constrained environments, such as IoT and vehicular networks. Its focus on packet forwarding time as a single decisive parameter ensures real-time applicability without overburdening the system.The practical implications of this work extend to industries requiring secure, dynamic communication networks, including emergency response, military operations, and regulatory-compliant sectors such as healthcare and finance. Future work could explore integrating the WDBIC model into advanced routing protocols, paving the way for the development of an Intruder Prevention Routing Protocol (IPRP) to further enhance MANET security and resilience.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] Vijayalakshmi et al., "Intrusion Detection System based on Game Theory with Neighbor Trust Table Approach for Mobile Ad-hoc Networks," International Journal of Pure and Applied Mathematics, vol. 119, no. 15, pp. 3347-3358, 2018.

[6] G. Rajeshkumar et al., "Intruder Detection using Cluster Trust Adaptive Acknowledgement and Kalman Filtering," International Journal of Computer Applications, vol. 114, no. 14, pp. 25-30, March 2015.

[7] Thabiso N. Khosa et al., "SDPEGH: Swarm, Distributed, Population-based, Evolutionary, Greedy, and Heuristic Algorithm for Intrusion Detection in Mobile Ad-hoc Networks," IEEE Access, vol. 8, pp. 23210-23225, January 2020.

[8] Jayantkumar A Rathod & Manjunath Kotari " 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 (IJCNA) Volume 11, Issue 1, January – February (2024) ISSN: 2395-0455 . DOI: 10.22247/ijcna/2024/224436.

[9] C. Edwin Singh and Maria Celestin Vigila " WOA-DNN for Intelligent Intrusion Detection and Classification in MANET Services" Intelligent Automation & Soft Computing, 1737- 1751 , IASC, 2023, vol.35, no.2 ,DOI: 10.32604/iasc.2023.028022.

[10] Zainab Ali Abbood, Dog˘u Çag˘daş Atilla and Çag˘atay Aydin "Intrusion Detection System through Deep Learning in Routing MANET " Networks Intelligent Automation &Soft Computing, 2023,269 -280 vol.37, no.1 DOI: 10.32604/iasc.2023.035276 .

[11] 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.

[12] Shaik 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,

[13] 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.

[14] 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.

[15] 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.

[16] 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.