International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 May 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Trust-Based Routing Selection Policy on Mobile Ad-Hoc Network Using Aodv Routing Protocol

Mrs. Versha Matre
Research Scholar
Department of Computer Science and Engineering
Dr. A.P.J. Abdul Kalam University
Indore, India
versha.matre@gmail.com

Dr. Pradnya A. Vikhar
Research Supervisor, Department of Computer Science and Engineering
Dr. A.P.J. Abdul Kalam University
Indore, India
pradnyav123@gmail.com

Abstract— This study presents an enhanced Ad-hoc On-demand Distance Vector (AODV) routing protocol, termed Proposed_TAODV, designed to improve security in Mobile Ad-Hoc Networks (MANETs) of 150 nodes by incorporating trust-based mechanisms. Through a comprehensive simulation, the Proposed_TAODV is evaluated against existing AODV and Dynamic Source Routing (DSR) protocols under conditions of increasing malicious node presence. The results reveal that Proposed_TAODV maintains a higher Packet Delivery Ratio, experiences lower Average End-to-End Delay, and achieves greater Throughput compared to the benchmarks, indicating its superior performance and robustness. The integration of Direct Trust Evaluation, Indirect Trust Evaluation, and Trust Aggregation methods into the AODV protocol clearly enhances the MANET's resilience to security threats, establishing the Proposed_TAODV as a promising approach for securing MANETs against various forms of attacks and network disruptions.

Keywords- Ad-hoc On-demand Distance Vector , Mobile Ad-Hoc Networks, Dynamic Source Routing, Direct Trust Evaluation, Indirect Trust Evaluation.

I. INTRODUCTION

In the evolving landscape of Mobile Ad-Hoc Networks (MANETs), the imperative for robust and secure routing protocols is paramount due to the network's dynamic nature and vulnerability to malicious entities.[1] Traditional protocols such as AODV and DSR, while efficient under standard operating conditions, often fall short in the presence of adversarial nodes, leading to compromised network integrity and performance.[2] Addressing these challenges, this research introduces an innovative Trust-based Routing Selection Policy, integrated within the AODV routing protocol—dubbed Proposed_TAODV. This novel approach weaves a trust assessment framework into the routing mechanism, leveraging both Direct and Indirect Trust Evaluations alongside a sophisticated Trust Aggregation system to discern and preferentially select the most reliable paths through the network. Comprehensive simulations within a 150-node MANET environment expose the Proposed_TAODV to increasing levels of security threats, quantifying its performance against existing protocols. The Proposed_TAODV consistently outperforms its predecessors by achieving superior Packet Delivery Ratios, minimizing End-to-End Delays, and maximizing Throughput. These enhancements in network performance metrics not only exemplify the efficacy of trust-based routing policies but also underscore the potential of Proposed_TAODV to fortify MANETs against the spectrum of security threats, thus paving the way for more resilient communications in decentralized wireless systems.

II. LITERATURE REVIEW

Wireless ad hoc networks, specifically Mobile Ad-hoc Networks (MANETs), are gaining significance in the field of wireless communication systems due to their notable absence of infrastructure and capacity for self-organization. Mobile Ad hoc Networks (MANETs), in contrast to traditional wireless networks, operate independently without relying on a central hub. These attributes make them highly suitable for certain applications such as military operations, disaster relief, and emergency situations [3].

MANETs have proven indispensable in several fields, serving as a structure for the exchange of multimedia data in mobile environments. However, the lack of a centralised management in these networks poses substantial security challenges. The incidence of vulnerabilities like as eavesdropping, impersonation, and denial of service attacks [4] is enhanced due to the dynamic nature, limited resources such battery power and bandwidth, and high mobility.

Addressing these security risks is intricate. The study in this domain include examining various security vulnerabilities and protocols with the aim of enhancing the efficiency of Mobile Ad hoc Networks (MANETs). Recognising and mitigating complicated assaults, such as wormhole attacks, is crucial in Mobile Ad hoc Networks (MANETs) due to the substantial danger they offer. One major focus [5] is the creation of algorithms that can accurately and safely detect attacks in commonly used routing protocols like Ad-hoc On-Demand Distance Vector (AODV). Furthermore, with the increasing integration of the Internet of Things (IoT) and mobile networks, new network security challenges are emerging.

Given the MANET nodes' ability to independently adjust to changes in network structure, it is crucial to include advanced security mechanisms to protect against various routing attacks and provide secure communication [6].

The widespread use of wireless networking technology has significantly expanded the range of potential applications for Mobile Ad hoc Networks (MANETs). These networks, which consist of mobile devices like computers, smartphones, and sensors, operate together in a decentralised manner to provide necessary network functionalities without depending on permanent infrastructure. This has potential for use in several fields, including home automation and wireless sensor networks [7].

Mobile Ad-hoc Networks (MANETs) are being used for diverse multimedia applications over wireless networks due to their distinctive attributes. MANET nodes has the ability to collaborate with neighbouring nodes in order to disseminate data. However, this collaboration is often exploited by malicious nodes, who collude with normal nodes to undermine network operations and hinder efficacy. The assailants use the mobility of nodes in MANETs to evade detection. This poses a significant security challenge in such environments that lack infrastructure, have limited battery capacity, and lack coordination among nodes [8].

To address these dangers, many strategies have been developed. The effectiveness of game theory in detecting malicious nodes has been shown, while several routing methods have been studied to enhance both security and routing performance. This work does a comprehensive analysis of several security attacks and proposes strategies to mitigate them [9].

Furthermore, the increasing occurrence of wireless sensor networks, which are prone to various security vulnerabilities, has led to the development of novel techniques for detecting and mitigating attacks such as wormhole attacks. These include fast connections among malicious sensor nodes that have a substantial influence on routing paths. Scientists are now examining the use of artificial intelligence (AI) and machine learning (ML) methods to effectively oversee and safeguard networks that are impervious to many cryptographic algorithms and challenging to identify [10].

One other challenge with Mobile Ad hoc Networks (MANETs) is their susceptibility to routing attacks, which is due to the unrestricted communication channel and lack of a centralised authority. Wormhole attacks pose a substantial threat since they create pathways between malicious nodes to disrupt network connectivity. Various methodologies for detecting and preventing these attacks are now under assessment [11].

The Optimised Link State Routing Protocol (OLSR) is notable among routing protocols because to its proactive and table-driven approach, which depends on Multipoint Relays (MPRs). However, the inappropriate behaviour of MPRs might potentially endanger network connectivity, leading to the development of new MPR selection algorithms that provide improved coverage and support for changing topologies [12].

In order to provide safe communication in Mobile Ad hoc Networks (MANETs), it is essential to implement strong security measures, given the absence of infrastructure and the presence of hostile conditions. Gaining comprehension and recognition of wormhole assaults is crucial, since these attacks have the potential to result in significant disruptions to the delivery of data packets in multi-hop wireless networks. Current research endeavours to enhance the security of Mobile Ad hoc Networks (MANETs) by using protocols like AODV to effectively detect and thwart attacks [13].

Mobile Ad Hoc Networks (MANETs) provide versatile communication capabilities for mobile devices, enabling them to communicate independently of a fixed infrastructure. However, the existence of fluidity in the network introduces complexities in the packet routing process. The increased node density may lead to significant interference and instability, particularly in areas where nodes are constantly moving. This study introduces a novel iteration of the Ad hoc On-Demand Distance Vector (AODV) protocol, referred to as Dynamic Power-Ad hoc On-Demand Distance Vector (DP-AODV). DP-AODV dynamically adapts the transmission power based on variations in the density of nodes. DP-AODV reduces latency and improves efficiency in congested networks, leading to better packet transmission, lower control overheads and jitter, and reduced end-to-end delay in situations with medium to high density [14].

The importance of energy efficiency in wireless networking cannot be overstated, since wireless devices possess limited power resources. This work presents the development of an Energy Aware On-Demand Routing Protocol (EAORP), an innovative approach that addresses the energy limitations of Dynamic Source Routing (DSR). EAORP is designed to particularly adapt to the energy levels, traffic loads, and power management of nodes. Reference [15] states that the routing system provided is both scalable and energy-efficient.

The Ad-hoc On-Demand Distance Vector (AODV) protocol is a reactive protocol used in ad-hoc mobile networks, specifically designed to construct routes only when they are required. The system utilises traditional routing tables and sequence numbers to ensure current routing information and prevent routing loops, showcasing its efficacy in dynamic network environments [16].

Mobile Ad hoc Networks (MANETs) depend only on the connectivity of mobile nodes, since they do not possess a permanent infrastructure. The nodes' mobility leads to fast and unpredictable changes in network configurations, underscoring the need for robust routing techniques. This study also investigates the compatibility of Mobile Ad hoc Networks (MANETs) with both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). IPv6 offers enhanced security and a wider pool of accessible addresses. The Qualnet simulator is used to evaluate the efficacy of the Ad Hoc On Demand Vector and Dynamic Manet On Demand routing protocols, taking into account both IPv4 and IPv6 standards. The research primarily examines important performance measures including as throughput, end-to-end latency, and average jitter. These indicators are used to assess the effectiveness of MANET deployments [17].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 May 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

III. PROPOSED METHODOLOGY

3.1 Direct Trust Evaluation in the context of a Trust-based Routing Selection Policy for Mobile Ad-Hoc Networks (MANETs) focuses on assessing the reliability and integrity of nodes based on their historical interactions. This evaluation is crucial for establishing secure and efficient routes in the network. The criteria for Direct Trust Evaluation involve several key metrics and behaviors that can quantitatively and qualitatively measure the trustworthiness of nodes. Here are the primary criteria often considered:

1. Packet Forwarding Behavior

Successful Packet Forwarding Rate: The ratio of successfully forwarded packets to the total packets received for forwarding. This rate indicates a node's reliability in transmitting data to the next hop.
Packet Dropping Rate: Frequency of packet drops by a node, either due to malicious intent (e.g., black hole attack) or network congestion. A lower rate is indicative of a more trustworthy node.

2. Communication Reliability

Link Stability: Frequency of link failures or link breaks with other nodes. A stable link suggests a reliable communication partner.
Latency: The average time taken for a packet to traverse from one node to another. Lower latency may indicate a more efficient and reliable node.

3. Energy and Resource Usage

Remaining Energy Level: The current energy level of a node. Nodes with higher remaining energy may be deemed more reliable as they are less likely to drop out of the network.
Resource Allocation: The efficiency in utilizing computational and bandwidth resources. Nodes that manage their resources effectively are often considered more trustworthy.

4. Behavioral Consistency

History of Behavior: Consistency in a node's behavior over time, indicating its reliability. Nodes with stable and consistent behavior are usually more trusted.
Response to Network Dynamics: Adaptability and performance consistency in response to changes in network topology or density.

5. Security Attributes

Absence of Malicious Activities: Lack of participation in known malicious activities such as packet tampering, creation of routing loops, or impersonation.
Cryptographic Measures: Effectiveness in employing cryptographic measures like authentication and encryption to secure communications.

6. Contribution to Network Operations

Routing Information Accuracy: The accuracy and timeliness of routing information provided by a node. Accurate and up-to-date routing information contributes positively to trust.
Assistance in Network Recovery: The role and effectiveness of a node in aiding the network to recover from failures or attacks.

3.2 Indirect Trust Evaluation in the context of a Trust-based Routing Selection Policy for Mobile Ad-Hoc Networks (MANETs) is the process of assessing the trustworthiness of nodes based on recommendations or feedback from other nodes in the network. Unlike Direct Trust Evaluation, which relies on firsthand observations, Indirect Trust Evaluation leverages the collective intelligence of the network to infer the reliability of nodes. This approach is particularly useful for evaluating nodes with which a direct interaction history is limited or non-existent. Here are the primary criteria and considerations for implementing Indirect Trust Evaluation:

1. Recommendation Credibility

Source Trustworthiness: The trust level of the node providing the recommendation. Recommendations from highly trusted nodes are given more weight.
Recommendation Consistency: The degree to which recommendations about a node from different sources are consistent. High consistency may indicate a more accurate assessment of the node's trustworthiness.

2. Recommendation Freshness

Time Sensitivity: The relevance of a recommendation based on its age. Newer recommendations are often more reflective of the current state and thus may be given more weight.
Dynamic Network Conditions: Consideration of the network's current state, as past recommendations might not be relevant under new network conditions or configurations.

3. Recommendation Context

Contextual Relevance: The similarity between the conditions under which the recommendation was generated and the current conditions. Recommendations made under similar conditions are more valuable.
Interaction Context: The nature and outcomes of the interactions that led to the recommendation, considering the specific tasks or communication patterns involved.

4. Aggregation Methodology

Weighted Aggregation: Combining multiple recommendations using a weighted average, where weights are based on factors like source trustworthiness and recommendation freshness.
Fusion Techniques: Employing advanced data fusion techniques to integrate diverse recommendations, potentially using methods from statistics or machine learning.

5. Handling Conflicting Recommendations

Conflict Resolution Strategies: Methods to resolve discrepancies in recommendations, such as prioritizing more recent data or using consensus mechanisms.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 May 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Anomaly Detection: Identifying and filtering out outlier recommendations that significantly deviate from the majority, which might indicate false or malicious feedback.

6. Security Considerations

Sybil Attack Protection: Mechanisms to detect and mitigate the impact of Sybil attacks, where a malicious node creates multiple fake identities to influence the network's trust evaluation.
Recommendation Tampering Detection: Ensuring the integrity of recommendations against tampering or man-in-the-middle attacks during transmission.

3.3 Trust Aggregation in the context of a Trust-based Routing Selection Policy for Mobile Ad-Hoc Networks (MANETs) involves combining Direct Trust Evaluation and Indirect Trust Evaluation to form an overall trust score for each node. This comprehensive trust score is then used to make informed decisions about route selection, with a preference for routes that involve nodes with higher overall trust scores. Trust Aggregation is a critical step in ensuring that the routing protocol can effectively balance the trade-offs between relying on firsthand experiences and the collective insights of the network.

IV. IMPLEMENTATION

Implementing a Trust-based Routing Selection Policy using AODV in NS2 (Network Simulator 2) involves integrating Direct Trust Evaluation, Indirect Trust Evaluation, and Trust Aggregation into the AODV routing protocol. Start by modifying the AODV source code to include additional fields in routing packets for trust information. Implement Direct Trust Evaluation by recording and analyzing packet forwarding behavior, link stability, and other metrics directly observed during communication. For Indirect Trust Evaluation, introduce a mechanism for nodes to share trust recommendations, incorporating a credibility assessment based on the source's trustworthiness and the recommendation's freshness. Develop a Trust Aggregation algorithm that dynamically combines direct and indirect trust scores, using weighted averages or other aggregation methods, and adjust these weights based on network conditions and interaction history. Ensure the aggregated trust scores are normalized and incorporate a temporal decay factor to reflect the most current evaluation of a node's trustworthiness. Optimize the code for computational efficiency and test the modified AODV protocol in NS2 by simulating various network scenarios, comparing performance and security metrics against the standard AODV protocol to validate the effectiveness of the trust-based routing approach. This implementation requires a deep understanding of NS2's architecture, proficiency in C++ (used for NS2 simulation scripts), and a solid background in network security principles.

Table 1: Key Parameters for Trust-based Routing in AODV

Parameter	Description	Method/Value
Direct Trust Score (DTS)	Reflects the trustworthiness of a node based on direct interactions.	Calculated using metrics such as packet forwarding rate, link stability, and energy level.
Indirect Trust Score (ITS)	Derived from recommendations or feedback from other nodes.	Aggregated using credibility, consistency, and freshness of recommendations.
Weight for Direct Trust (WDT)	Determines the influence of direct trust scores in the overall trust calculation.	Dynamic, adjusted based on interaction history and network conditions.
Weight for Indirect Trust (WIT)	Determines the influence of indirect trust scores in the overall trust calculation.	Dynamic, similar to WDT, adjusted based on network conditions.
Aggregated Trust Score (ATS)	The combined trust score from both direct and indirect evaluations.	Calculated using weighted averages or non-linear methods of DTS and ITS.
Trust Threshold (TT)	The minimum trust score required for a node to be considered trustworthy.	Set based on network security requirements and performance goals.
Temporal Decay Factor (TDF)	Reflects the reduction in relevance of trust scores over time.	A predetermined value or formula that reduces trust scores gradually.
Recommendation Freshness (RF)	Measures the relevance of indirect trust recommendations based on their age.	A time-based decay function to decrease the value of older recommendations.
Link Stability Metric (LSM)	Assesses the reliability of a communication link.	Calculated based on the frequency of link failures or breaks.
Packet Forwarding Rate (PFR)	The ratio of successfully forwarded packets to the total received packets.	Measured directly from routing activities within the simulation.

V. RESULT ANALYSIS

5.1 Concerning No Malicious Nodes and the number of nodes 150 fixed

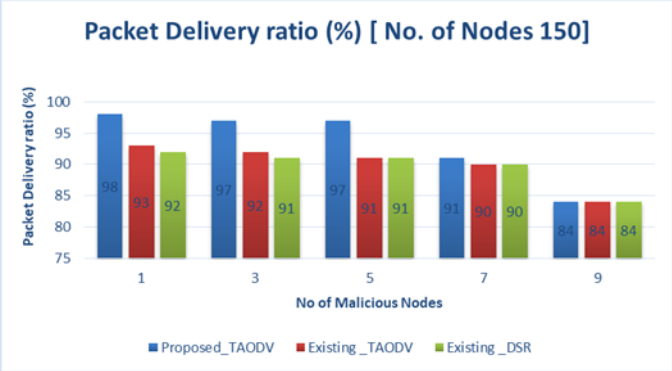

Figure 1. Packet Delivery ratio (%) [No. of Nodes 150]

The figure 1 presents a comparison of the Packet Delivery Ratio (PDR) for two existing routing protocols, AODV and DSR, against a Proposed_TAODV protocol within a network of 150 nodes under varying conditions of malicious node presence. The PDR is measured as a percentage and is shown for scenarios with 1, 3, 5, 7, and 9 malicious nodes. The Proposed_TAODV consistently maintains a higher PDR across all scenarios, demonstrating its robustness against malicious activities within the network. The existing AODV and DSR protocols show a decline in PDR as the number of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 May 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

malicious nodes increases, with DSR experiencing a more pronounced drop. This trend illustrates the enhanced effectiveness of the Proposed_TAODV in sustaining reliable packet delivery even in the presence of security threats.

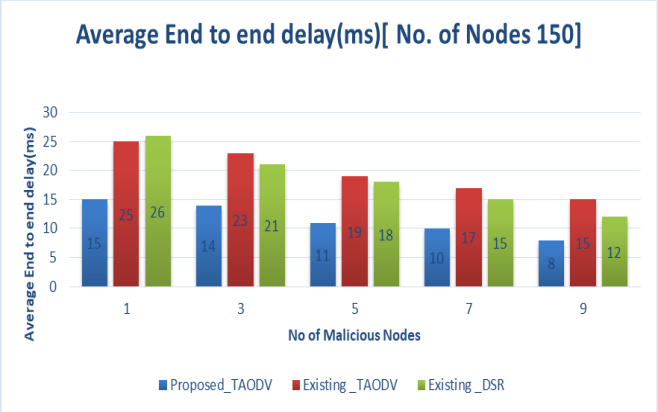

Figure 2. Average End to end delay(ms) [No. of Nodes 150]

The Figure 2 compares the Average End-to-End Delay in milliseconds (ms) of the Proposed_TAODV protocol with two existing routing protocols, AODV and DSR, in a MANET consisting of 150 nodes. The comparison is conducted under varying conditions with 1, 3, 5, 7, and 9 malicious nodes present in the network. As the number of malicious nodes increases, the Proposed_TAODV shows a consistently lower or comparable delay, indicating its efficiency in maintaining timely data transmission despite security threats. Both existing AODV and DSR protocols exhibit higher delays, especially as the number of malicious nodes grows, with the DSR protocol generally incurring the most significant increase. This suggests that the Proposed_TAODV protocol is better optimized for minimizing delay in adverse conditions, highlighting its potential for reliable and efficient communication in compromised MANET environments.

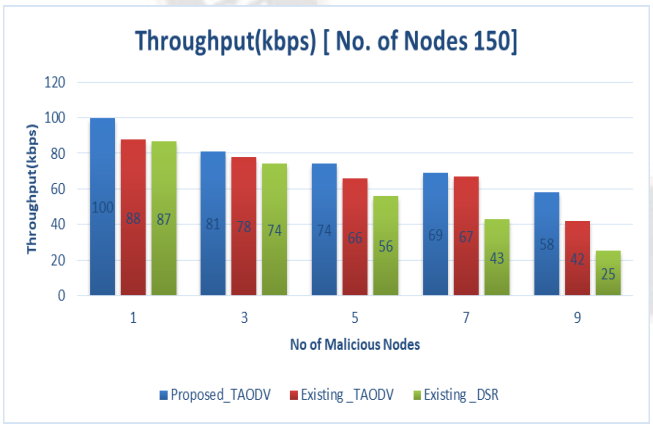

Figure 3. Throughput(kbps) [No. of Nodes 150]

The figure 3 illustrates the network throughput measured in kilobits per second (kbps) for three different routing protocols—Proposed_TAODV, Existing_TAODV, and Existing_DSR—within a network of 150 nodes while varying the number of malicious nodes from 1 to 9. The Proposed_TAODV maintains higher throughput compared to the other protocols across all scenarios, indicating its robust capability in handling malicious activities. The throughput for all protocols decreases as the number of malicious nodes increases, but the decline is more pronounced for the Existing_TAODV and even more so for the Existing_DSR. This suggests that the Proposed_TAODV protocol is more resilient and effective in sustaining network performance under adverse conditions characterized by security threats.

6. Conclusions

The comparative analysis of the Proposed_TAODV protocol with Existing_TAODV and Existing_DSR protocols within a 150-node MANET environment under varying security threats demonstrates the superior performance of Proposed_TAODV. The visual data indicates that the Proposed_TAODV consistently outperforms the existing protocols in terms of maintaining a higher Packet Delivery Ratio, ensuring lower Average End-to-End Delay, and achieving greater Throughput, even as the number of malicious nodes increases. These results suggest that the integration of trust-based routing mechanisms significantly enhances network resilience against malicious activities, thereby improving the reliability, efficiency, and overall security of mobile ad-hoc networks. The Proposed_TAODV's robustness against security threats makes it a promising solution for secure and dependable communication in dynamic and potentially hostile wireless network environments.

References

1. T. Varshney, T. Sharma, and P. Sharma, “Implementation of watchdog protocol with AODV in mobile ad hoc network,” *Proceedings - 2014 4th International Conference on Communication Systems and Network Technologies, CSNT 2014*, pp. 217–221, 2014, doi: 10.1109/CSNT.2014.50.
2. A. O. Bang and P. L. Ramteke, “MANET : History , Challenges And Applications,” no. March, 2019.
3. P. Chitra, “A Study on Manet: Applications, Challenges and Issues,” *IJERT Journal International Journal of Engineering Research and Technology*, Accessed: Oct. 20, 2022. [Online]. Available: www.ijert.org
4. B. Banerjee and S. Neogy, “A brief overview of security attacks and protocols in MANET,” *Proceedings of the 2021 IEEE 18th India Council International Conference, INDICON 2021*, 2021, doi: 10.1109/INDICON52576.2021.9691554.
5. N. Dubey and K. Kumar Joshi, “An Approach to Detect Wormhole Attack in AODV based MANET,” *Int J Comput Appl*, vol. 114, no. 14, pp. 32–39, 2015, doi: 10.5120/20049-2098.
6. M. Rath, J. Swain, B. Pati, and B. K. Pattanayak, “Network Security: Attacks and Control in MANET,” *https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-5225-4100-4.ch002*, pp.19–37, Jan. 1AD, doi: 10.4018/978-1-5225-4100-4.CH002.
7. Raja L, Baboo SS. An overview of MANET: Applications, attacks and challenges. International journal of computer science and mobile computing. 2014 Jan;3(1):408-17.
8. R. Krishnan, “1-4 Rahul Krishnan. A Survey on Game Theory Approaches for Improving Security in MANET,” *American Journal of Electrical and Computer Engineering*, vol. 2, no. 1, pp. 1–4, 2018, doi: 10.11648/j.ajece.20180201.11.
9. Hanif M, Ashraf H, Jalil Z, Jhanjhi NZ, Humayun M, Saeed S, Almuhaideb AM. AI-based wormhole attack detection techniques in wireless sensor networks. Electronics. 2022 Jul 26;11(15):2324.
10. Gohil Y, Sakhreliya S, Menaria S. A review on: detection and prevention of wormhole attacks in MANET. International Journal of Scientific and Research Publications. 2013 Feb;3(2):1-6.

11. Zougagh, H., Idboufker, N., El Mourabit, Y., Saadi, Y. and Elouaham, S., 2021. Avoiding Wormhole Attack in MANET Using an Extending Network Knowledge. In *Innovations in Bio-Inspired Computing and Applications: Proceedings of the 11th International Conference on Innovations in Bio-Inspired Computing and Applications (IBICA 2020) held during December 16-18, 2020 11* (pp. 217-230). Springer International Publishing.
12. Mishra P, Kispotta A. "Identification of Worm Hole Attack in MANET using Cluster basedApproach".
13. S. Singh and H. S. Saini, "Intelligent Ad-Hoc-On Demand Multipath Distance Vector for Wormhole Attack in Clustered WSN," *Wirel Pers Commun*, vol. 122, no. 2, pp. 1305–1327, 2022, doi: 10.1007/s11277-021-08950-x.
14. A. M. Bamhdi, "Efficient dynamic-power AODV routing protocol based on node density," *Comput Stand Interfaces*, vol. 70, Jun. 2020, doi: 10.1016/j.csi.2019.103406.
15. Tarus HS, Alias SB, Parthasarathy R. A review of energy efficient on-demand routing protocols and the design of energy efficient algorithm in mobile ad hoc networks. InAIP Conference Proceedings 2023 Nov 27 (Vol. 2847, No. 1). AIP Publishing.
16. V. Sahu, P. Kumar Maurya, G. Sharma, A. Roberts, and M. Srivastava, "An Overview of AODV Routing Protocol," *International Journal of Modern Engineering Research (IJMER) www.ijmer.com*, vol. 2, no. 3, Accessed: Oct. 21, 2022. [Online]. Available: https://www.researchgate.net/publication/252068339
17. J. H. Majeed, N. A. Habeeb, and W. K. Al-Azzawi, "Performance investigations of internet protocol versions for mobile Ad-hoc network based on qualnet simulator," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, pp. 497–504, 2021, doi: 10.11591/ijeecs.v21.i1.pp497-504.