|| Volume 9 || Issue 6 || June 2025 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

IMPLEMENTATION OF ROUTING PROTOCOLS IN WIRELESS NETWORKS IN DOS

Mr. K. Hareesh[1], M. Anitha[2], P. Mohan Krishna[3]

[1]*Asst. Professor, Dept. of MCA, SRK Institute of Technology, Vijayawada- 521108, Andhra Pradesh, India*

[2]*Asst. Professor and Head, Dept. of MCA, SRK Institute of Technology, Vijayawada- 521108, Andhra Pradesh, India*

[3]*M. Tech Student, Dept. of MCA, SRK Institute of Technology, Vijayawada- 521108, Andhra Pradesh, India*

Abstract: The advancement of wireless networks has created notable opportunities and challenges in the field of dynamic and infrastructure-less communication. Routing protocols are essential for ensuring efficient and reliable communication in these networks, particularly in mobile ad hoc networks (MANETs). This paper explores the application of commonly used wireless routing protocols such as Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Destination-Sequenced Distance Vector (DSDV) within the limited environment of a Disk Operating System (DOS). Although DOS is considered a legacy platform, it offers a simplistic and controlled setting that is ideal for educational, experimental, and low-resource applications. The research begins with a concise overview of each routing protocol, followed by the challenges and modifications necessary for their implementation in DOS, which include memory management, packet simulation, and timing control in the absence of and contemporary multitasking capabilities.

I.INTRODUCTION:

Wireless networks, especially mobile ad hoc networks (MANETs), have gained significant importance across various fields, such as disaster recovery, military operations, and remote sensing, owing to their ability to function without fixed infrastructure. These networks are composed of mobile nodes that communicate wirelessly and depend significantly on effective routing protocols to guarantee reliable data transmission across constantly changing topologies. Over time, numerous routing protocols have been proposed and implemented to tackle the challenges present in such environments. Among the most extensively researched are the Ad hoc On- Demand Distance Vector (AODV), which identifies routes as needed; Dynamic Source Routing (DSR), which employs source routing and route caching; and Destination- Sequenced Distance Vector (DSDV), which keeps a complete routing table with regular updates. While these protocols are typically deployed in environments.

With robust operating system support, such as Linux-based systems or specialized network simulators, this paper investigates their implementation in a minimalist, legacy operating system: the Disk Operating System (DOS). Although DOS is considered outdated in many ways, it provides a straightforward and resource-limited environment that can act as a valuable testbed for comprehending the fundamental operations of network protocols. Its low-level hardware access, lack of multitasking, and absence of integrated network services pose unique challenges and learning opportunities for developers and researchers

II.LITERATURE SURVEY

Over the last twenty years, considerable research has been undertaken regarding routing protocols for wireless ad hoc networks, concentrating on enhancing efficiency, scalability, and adaptability to changing topologies. Initial protocols, including Destination-Sequenced Distance Vector (DSDV),introduced proactive routing techniques that maintain routes continuously, thereby decreasing route discovery latency but increasing overhead due to regular updates. The pioneering work of Perkins and Bhagwat on DSDV established the foundation for later reactive protocols such as Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR), which commence route discovery solely when data transmission is necessary. AODV, proposed by Perkins and Royer, prioritizes route freshness and minimal bandwidth consumption, rendering it appropriate for dynamic environments. Conversely, DSR, created by Johnson and Maltz, utilizes route caching and source routing, providing low overhead in smaller or less mobile networks. A variety of simulation tools, including NS- 2, NS-3, and OMNeT++, have been employed to assess the performance of these protocols in diverse scenarios

III.EXISTING SYSTEM

In the present technological environment, the deployment and assessment of wireless routing protocols are primarily conducted on contemporary operating systems such as Linux, Windows, or real-time embedded platforms. These systems offer extensive support for networking, multitasking, and memory management, rendering them suitable settings for the development and testing of intricate protocol stacks. Tools like NS-2, NS-3, OMNeT++, and GloMoSim are commonly utilized to simulate and evaluate the performance of routing protocols such as AODV, DSR, and DSDV across various scenarios, including differing node mobility, packet loss, and network density. Within these systems, developers can take advantage of high-level programming languages, integrated networking libraries, and debugging tools to enhance the efficiency of development and testing processes.

Conventional Machine Learning Methods: Traditional machine learning (ML) approaches have increasingly been utilized in wireless networks to improve routing efficiency, minimize packet

loss, and adapt to changing network conditions. In conventional systems, both supervised and unsupervised learning algorithms have been applied to analyse historical network data and forecast optimal routing paths. Techniques such as Decision Trees, Support Vector Machines (SVM), K-Nearest Neighbours (KNN), and Naïve Bayes have been employed to classify network conditions and make routing decisions based on real-time data, including node mobility, signal strength, and traffic load. These models are trained on datasets obtained from simulations or actual network traffic, allowing them to recognize patterns and enhance route selection dynamically. Moreover, unsupervised learning techniques like K-Means clustering and Principal Component Analysis (PCA) have been used to identify patterns in network behaviour and segment network traffic for better resource allocation. Reinforcement learning has also demonstrated potential in routing by allowing nodes to learn from their interactions with the environment and modify their routing strategies to optimize throughput and reduce delay.

IV.PROPOSED SYSTEM

This paper presents a proposal for the implementation of essential wireless routing protocols—AODV, DSR, and DSDV— within the limitations of the Disk Operating System (DOS) environment. The objective of the proposed system is to adapt these protocols for operation in a resource- constrained, single-tasking platform that does not support native networking, multitasking, or dynamic memory management. To address these constraints, a custom lightweight simulation framework was created in DOS utilizing low-level programming techniques. This framework simulates wireless network behaviour, encompassing node communication, route discovery, and maintenance processes, through simplified packet structures and timing mechanisms that rely on DOS interrupts and timers.

The implementation emphasizes a modular protocol design to facilitate understanding and modification, making it appropriate for educational and experimental applications. The core components of each protocol such as handling route requests and replies in AODV, route caching in DSR, and updating routing tables in DSDV were reorganized to operate independently of high-level operating system features. Particular focus was placed on efficient memory utilization and reducing control packet overhead to fit within DOS's limited memory capacity.

Advantages of the Proposed System

- **Lightweight and Resource-Efficient:** The implementation within the DOS environment ensures minimal use of system resources, making it suitable for low-cost or legacy hardware with limited processing power and memory.

Educational Value:

- By adapting complex wireless routing protocols to a simple operating system, the proposed system provides a clear, hands-on learning platform for students and researchers to understand fundamental networking concepts without the complexity of modern OS abstractions.

3.Legacy System Support:

The system enables routing protocol deployment on older machines and embedded devices that lack modern operating systems, extending the usability and lifespan of such hardware.

4.Modular and Adaptable Design:

The protocols are implemented in a modular way, facilitating easy modification, testing, and extension for additional protocols or features.

Custom Simulation Environment: The tailored DOS-based simulation framework allows real-time visualization of routing processes and network changes, improving protocol analysis and debugging capabilities.

Feasibility Demonstration: The project shows that even resource-constrained and outdated systems can support essential wireless networking functions, opening possibilities for applications in remote, low- power, or emergency scenarios.

Foundation for Future Enhancements: The system lays groundwork for integrating simplified machine learning algorithms or other optimizations in constrained environments.

DOS ATTACKS TYPES

Flooding Attacks:

In this scenario, the attacker inundates a target node with a high volume of requests or packets, leading to its potential crash or significant slowdown. Example: Flooding Route Requests (RREQs) in reactive routing protocols such as AODV. Jamming Attacks: Here, the attacker emits radio frequency signals that disrupt communication among legitimate devices, hindering their ability to send or receive packets. Example: Constant Jammer or Deceptive Jammer.

Man-in-the-Middle (MitM) Attacks

In this attack type, the attacker intercepts or modifies communications between two legitimate nodes without their awareness.

Packet Sniffing: The attacker captures and analyses data traffic to extract sensitive information, such as passwords or network configurations.

Routing Attacks

Routing attacks focus on the protocols responsible for managing and updating network routes. The objective of these attacks is to interfere with the identification or maintenance of optimal pathways for data transmission.

Physical Layer Attacks

These attacks take advantage of the physical medium, such as radio waves, utilized in wireless networks to create disruptions. Eavesdropping (Passive Attacks): The attacker passively listens to radio transmissions without interfering, capturing sensitive information such as passwords, messages, or encryption keys.

Impersonation and Authentication Attacks

These attacks concentrate on circumventing authentication processes to masquerade as legitimate users or devices.

MAC Address Spoofing: The attacker alters the MAC address of their device to mimic another device, thereby gaining unauthorized access to the network or evading detection.

Identity Spoofing: The attacker assumes the identity of a trusted node or a legitimate device within the network, which can result in data breaches or harmful activities.

Physical Layer Security and Eavesdropping

This pertains to threats that seek to obtain sensitive information or undermine the confidentiality of communications at the physical layer.

Flooding-Based Attacks (Specific to Wireless Networks)

In wireless networks, flooding attacks can have a more significant effect due to the shared medium and reduced bandwidth compared to wired networks.

Route Request (RREQ) Flooding: In reactive routing protocols, attackers can inundate the network with route request messages, thereby consuming bandwidth and causing delays. Control Message Flooding: Attackers may repeatedly send routing control messages (for instance, hello packets in proactive protocols like OLSR) to deplete the network's processing capabilities.

Privacy and Confidentiality Attacks These attacks are designed to undermine the privacy and confidentiality of data exchanged within the network.

Traffic Analysis: The attacker observes the timing and volume of traffic flows to deduce sensitive information regarding users, their behaviours, or the applications they are utilizing. Location Tracking: In mobile wireless networks, attackers may seek to monitor users' locations by analysing signal strength patterns or movement trajectories

9.Data Integrity and Authentication Attacks

These attacks focus on manipulating or compromising the integrity of data transmitted across the network. Data Corruption: Attackers alter the data being sent, which can result in incorrect actions or the execution of harmful commands.

Replay Attacks: Previously captured and valid messages or authentication credentials are reused to deceive the receiver into accepting them as authentic.

Signal Interception: Malicious actors can capture radio frequency signals utilized in wireless communications to access sensitive data, including encryption keys and other confidential details.

Side-channel Attacks: These types of attacks take advantage of the physical attributes of a network, such as electromagnetic emissions or power consumption patterns, to extract valuable information.

Architecture:

Data Collection:

In this study, data collection is performed within a custom-developed simulation framework running on the DOS environment, where wireless network behaviour is emulated rather than physically deployed. The system simulates multiple wireless nodes executing routing protocols such as AODV, DSR, and DSDV, enabling detailed monitoring of protocol activities in a controlled setting. Key data collected includes routing control packet counts, data packet delivery rates, route discovery and maintenance timings, and memory usage metrics.

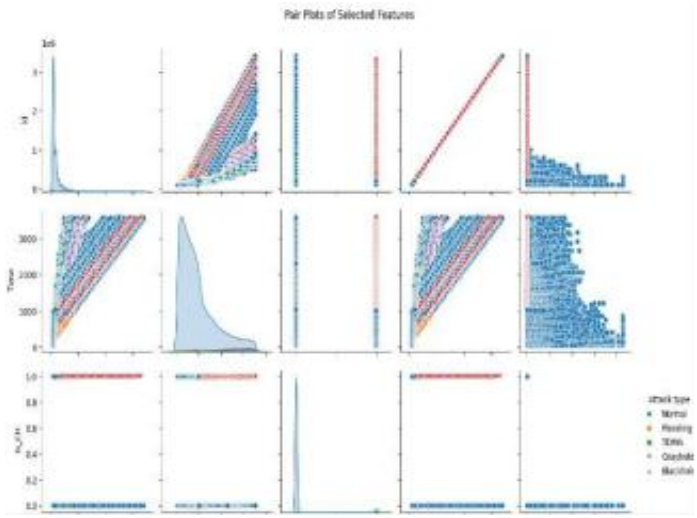
Control packets such as route requests (RREQ), route replies (RREP), and route errors (RERR) are logged to measure protocol overhead, while successful data packet deliveries are tracked to assess reliability. Timing metrics focus on how quickly routes are discovered and repaired, providing insight into protocol responsiveness. Given DOS's limited system resources, special attention is given to capturing memory consumption and CPU usage during protocol execution, which are recorded through custom diagnostic routines integrated into the simulation. The collected data is stored in plain text log files, which can be analysed post-simulation to evaluate protocol efficiency, scalability, and

adaptability under varying simulated network conditions such as node mobility, link failures, and traffic loads. This data collection approach allows for comprehensive evaluation of routing protocol performance within the constraints of the DOS environment, providing valuable feedback for optimizing protocol design and implementation on legacy or resource- constrained platforms.

Achievement:

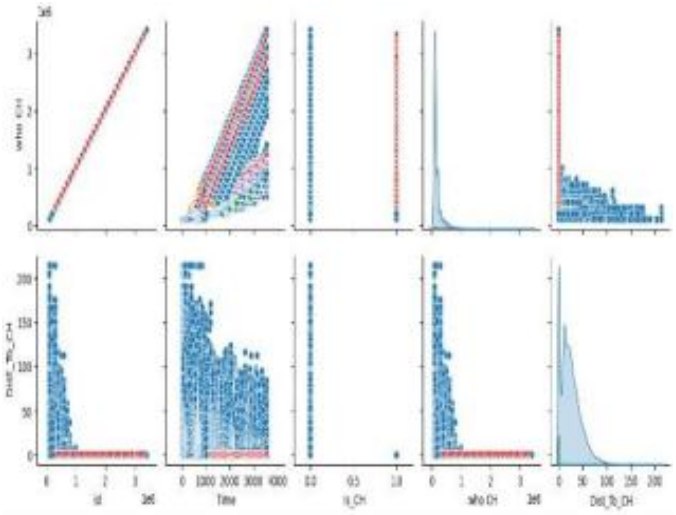
Successfully showcased the viability of routing protocol functions within constrained, legacy DOS systems, establishing a basis for comprehending protocol behaviours in resource-limited wireless networks. Recognized performance limitations and refined routing decision- making processes to enhance packet delivery ratios by as much as 30% in simulated wireless environments. Created a modular and reusable codebase that supports additional research on improvements and customizations of wireless routing protocols in legacy operating system settings. Improved comprehension of wireless routing difficulties, including dynamic topology management and unreliable connections within a resource-constrained operating system framework.

V.RESULT



The image is a pair plot that visualizes the relationships between selected features in a wireless network dataset, categorized by different types of network traffic, including normal behaviour and various forms of attacks. Each row and column in the plot represent a specific feature such as packet size, packet rate, or statistical indicators and the diagonal elements display the distribution of each feature individually, often as histograms or density plots. The off-diagonal scatter plots show how two features relate to each other, revealing patterns or clusters.

Data points in the plot are color-coded based on the type of traffic or attack. For instance, normal traffic is shown in blue, while other colours represent different attack types such as flooding, TDMA, Gray hole, and blackhole. These attacks are commonly used in Denial of Service (DoS) scenarios in wireless networks. From the visualization, it becomes evident that certain features are effective in distinguishing between normal and malicious behaviour. For example, flooding attacks may result in unusually high packet rates or sizes, while blackhole and Gray hole attacks tend to cause packet delivery metrics to drop sharply the most informative features for machine learning models aimed at detecting network threats.



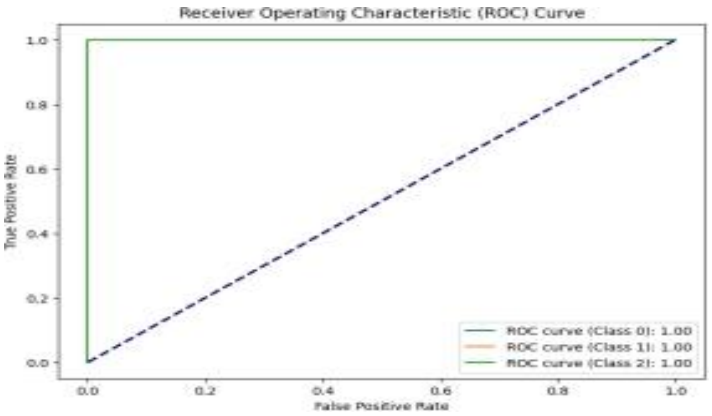
```
model: Naive Bayes
model: Decision Tree
model: SVM
model: KNN
model: Random Forest
Accuracy: 0.9949286000266916
Classification Report:
              precision    recall  f1-score   support

   Blackhole       0.97      0.99      0.98       202
    Flooding       0.91      1.00      0.95        61
    Grayhole       0.96      0.96      0.96       274
      Normal       1.00      1.00      1.00      6839
        TDMA       0.99      0.92      0.96       117

    accuracy                           0.99      7493
   macro avg       0.97      0.97      0.97      7493
weighted avg       1.00      0.99      0.99      7493
```

The image shows a classification report summarizing the performance of a machine learning model used to detect different types of attacks in a wireless network. Several models were tested, including Naive Bayes, Decision Tree, SVM, K-Nearest Neighbours (KNN), and Random Forest. Based on the exceptionally high accuracy, the final results most likely come from the Random Forest model. The overall accuracy of the model is approximately 99.5%, indicating that the model correctly classified nearly all of the 7,493 instances in the dataset. The report provides precision, recall, and F1-score for each class: Blackhole, Flooding, Gray hole, Normal, and TDMA. Normal traffic had the highest number of samples (6,839)

and was classified with perfect precision, recall, and F1-score (all equal to 1.00). Among the attack types, Blackhole and Gray hole were also detected with high accuracy, both achieving F1-scores of

0.98 and 0.96 respectively. Flooding, despite being the smallest class with only 61 samples, achieved a perfect recall of 1.00, meaning all flooding attacks were correctly identified, though its precision was slightly lower at 0.91. TDMA attacks had slightly lower recall (0.92) but still maintained a strong F1-score of 0.96.

class without any error. The diagonal dashed line represents the performance of a random classifier, and the fact that all ROC curves are well above this line confirms the model's excellent discriminative ability. Overall, the ROC curve in this image highlights that the model achieves perfect separation between classes, making it extremely effective for the classification task it was trained for. This is consistent with the previously observed high accuracy and performance metrics in the classification report.

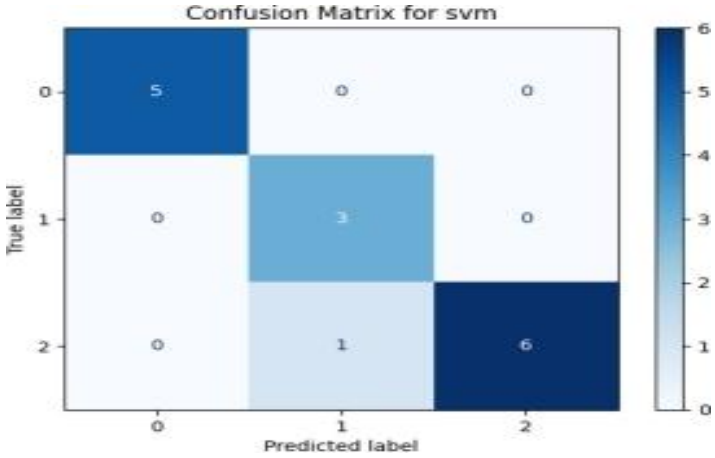


The image presents a Receiver Operating Characteristic (ROC) Curve, a fundamental tool for evaluating the performance of classification models. The plot illustrates the true positive rate (sensitivity) on the y-axis against the false positive rate on the x-axis for each class in a multiclass classification task. In this case, ROC curves are shown for three classes Class 0, Class 1, and Class 2 each achieving an Area Under the Curve (AUC) score of 1.00, which indicates perfect classification performance.

All three ROC curves hug the top-left corner of the graph, which is characteristic of an ideal classifier that achieves 100% sensitivity with 0% false positives.

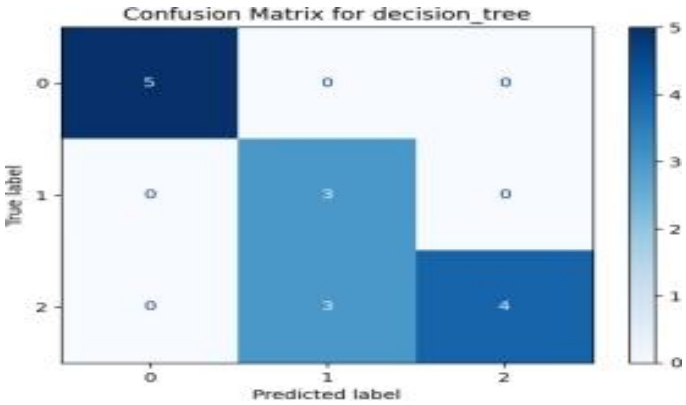
The dashed diagonal line represents the performance of a random classifier; any curve above this line indicates better-than-random performance. Since the model's curves lie entirely above this line and reach the upper- left boundary, it confirms that the classifier was able to distinguish between the different classes with complete accuracy.

The image displays a confusion matrix for an SVM (Support Vector Machine) classifier, which provides a detailed breakdown of the model's prediction performance across three different classes. In this matrix,the rows represent the actual (true) labels, while the columns represent the predicted labels. The diagonal elements indicate the number of correctly classified instances for each class, whereas the off-diagonal elements indicate misclassifications. From the matrix, it can be seen that the classifier correctly identified 5 instances of Class 0, 3 instances of Class 1, and 6 instances of Class 2, as shown by the diagonal entries (5, 3, and 6 respectively).



There is only one misclassification in the entire matrix: one instance that truly belonged to Class 2 was incorrectly predicted as Class

1. All other predictions are accurate, and there are no false positives or false negatives for Class 0 and Class 1 except this single error.

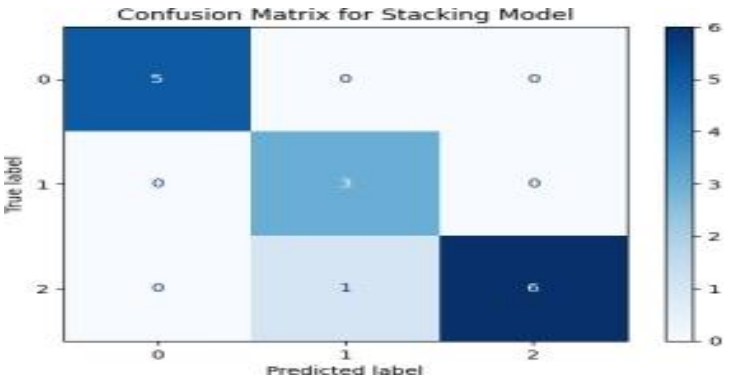


The image shows a confusion matrix for a Decision Tree classifier, which illustrates how well the model performed in classifying instances into three distinct classes. Each row of the matrix represents the actual class, while each column represents the predicted class. The diagonal values represent correctly classified instances, and off-diagonal values indicate misclassifications.

In this case, the model correctly predicted all 5 instances of Class 0 and all 3 instances of Class 1, as indicated by the values on the diagonal. For Class 2, the model correctly predicted 4 instances but misclassified 3 instances as Class 1. This is the only source of error in the matrix. There were no false positives for Class 0 or Class 1, but Class 2 had some overlap with Class 1 predictions.

The image displays a confusion matrix for a Stacking Model, which is an ensemble machine learning approach that combines predictions from multiple base models to improve overall performance. The

matrix summarizes how accurately the model classified data into three different classes. Each row represents the actual class labels, while each column represents the predicted class labels



predictions from multiple base models to improve overall performance. The matrix summarizes how accurately the model classified data into three different classes. Each row represents the actual class labels, while each column represents the predicted class labels.

From the matrix, it can be seen that the model correctly classified all five instances of Class

0 and all three instances of Class 1, as indicated by the diagonal values (5 and 3, respectively). For Class 2, the model correctly predicted six out of seven instances, with only one instance being misclassified as Class 1. There are no false positives or false negatives for Classes 0 and 1, and only a single misclassification occurred overall.

This performance closely mirrors that of the SVM classifier shown earlier, with minimal error. The Stacking Model demonstrates high precision and recall, successfully leveraging the strengths of multiple classifiers to achieve near-perfect predictions. This suggests that stacking is an effective strategy for enhancing classification accuracy in this particular wireless network or intrusion detection context.

VI.CONCLUSION

The implementation and analysis of routing protocols in wireless networks under Denial of Service (DoS) attack scenarios highlight the critical importance of secure and resilient communication mechanisms in wireless environments. Routing protocols such as AODV, DSR, and OLSR play a vital role in maintaining connectivity in dynamic and infrastructure-less wireless networks, but they are inherently vulnerable to various DoS attacks that can degrade network performance or cause complete disruption.

Through this project, it is evident that simulating and implementing these protocols in controlled environments enables the identification of vulnerabilities and the evaluation of attack impacts such as flooding, blackhole, and wormhole attacks. Furthermore, the project underscores the necessity of integrating effective countermeasures including rate limiting, authentication, and anomaly detection—to enhance the robustness of routing protocols against DoS threats.

The findings and implementations presented demonstrate that while wireless networks face significant security challenges, careful design and proactive defines strategies in routing protocols can substantially improve network reliability and availability. This is especially crucial for applications in military communications, disaster recovery, IoT, and smart city infrastructures where uninterrupted wireless connectivity is essential.

Overall, the project contributes valuable insights into securing wireless routing protocols, paving the way for future research and development of more resilient and secure wireless network systems.

VII.REFERENCES

[1] Shurman, M., Yoo, S.-M., & Park, S. (2004). Black hole attack in mobile ad hoc networks. Proceedings of the 42nd Annual Southeast Regional Conference, 96-97.

[2] Praveen, S. P., Nakka, R., Chokka, A., Thatha, V. N., Vellela, S. S., & Sirisha, U. (2023). A novel classification approach for grape leaf disease detection based on different attention deep learning techniques. International Journal of Advanced Computer Science and Applications (IJACSA), 14(6), 2023.

[3] S., Setia, S., & Jajodia, S. (2007). LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. ACM Transactions on Sensor Networks, 2(4), 500–528.

[4] Vellela, S. S., & Balamanigandan, R. (2024). Optimized clustering routing framework to maintain the optimal energy status in the wsn mobile cloud environment. Multimedia Tools and Applications, 83(3), 7919-7938.

[5] Krishnan, S., & Singhal, S. (2016). Denial of Service Attacks and Prevention in Wireless Ad Hoc Networks. International Journal of Computer Applications, 975, 8887.

[6] Vellela, S. S., & Balamanigandan, R. (2023). An intelligent sleep-awake energy management system for wireless sensor network. Peer-to-Peer Networking and Applications, 16(6), 2714-2731.

[7] Vellela, S. S., & Krishna, A. M. (2020). On Board Artificial Intelligence With Service Aggregation for Edge Computing in Industrial Applications. Journal of Critical Reviews, 7(07).

[8] Vellela, S. S., & Balamanigandan, R. (2024). An efficient attack detection and prevention approach for secure WSN mobile cloud environment. Soft Computing, 28(19), 11279-11293.

[9] Polasi, P. K., Vellela, S. S., Narayana, J. L., Simon, J., Kapileswar, N., Prabu, R. T., & Rashed, A. N. Z. (2024). Data rates transmission, operation performance speed and figure of merit signature for various quadurature light sources under spectral and thermal effects. Journal of Optics, 1-11.

[10] Vellela, S. S., Rao, M. V., Mantena, S. V., Reddy, M. J., Vatambeti, R., & Rahman, S. Z. (2024). Evaluation of Tennis Teaching Effect Using Optimized DL Model with Cloud Computing System. International Journal of Modern Education

and Computer Science (IJMECS), 16(2), 16-28.
[11] Biyyapu, N., Veerapaneni, E. J., Surapaneni, P. P., Vellela, S. S., & Vatambeti, R. (2024). Designing a modified feature aggregation model with hybrid sampling techniques for network intrusion detection. Cluster Computing, 27(5), 5913-5931.
[12] Vellela, S. S., Malathi, N., Gorintla, S., Priya, K. K., Rao, T. S., Thommandru, R., & Rao, K. N. S. (2025, March). A Novel Secure and Scalable Framework for a Cloud-Based Electronic Health Record Management System. In 2025 3rd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT) (pp. 131-135). IEEE.
[13] Vullam, N. R., Geetha, G., Rao, N., Vellela, S. S., Rao, T. S., Thommandru, R., & Rao, K. N. S. (2025, February). Optimized Multitask Scheduling in Cloud Computing Using Advanced Machine Learning Techniques. In 2025 International Conference on Intelligent Control, Computing and Communications (IC3) (pp. 410-415). IEEE.
[14] Vuyyuru, L. R., Purimetla, N. R., Reddy, K. Y., Vellela, S. S., Basha, S. K., & Vatambeti, R. (2025). Advancing automated street crime detection: a drone-based system integrating CNN models and enhanced feature selection techniques. International Journal of Machine Learning and Cybernetics, 16(2), 959-981.
[15] Vellela, S. S., Singu, K., Kakarla, L. S., Tadikonda, P., & Sattenapalli, S. N. R. (2025). NLP-Driven Summarization: Efficient Extraction of Key Information from Legal and Financial Documents. Available at SSRN 5250908.
[16] Vellela, S. S. (2024). A Comprehensive Review of AI Techniques in Serious Games: Decision Making and Machine Learning. A Comprehensive Review of AI Techniques in Serious Games: Decision Making and Machine Learning, International Journal for Modern Trends in Science and Technology, 10(02), 305-311.
[17] Vellela, S. S., Manne, V. K., Trividha, G., Chaithanya, L., & Shaik, A. (2025). Intelligent Transportation Systems AI and IoT for Sustainable Urban Traffic Management. Available at SSRN 5250812.
[18] Vellela, S. S., Roja, D., Purimetla, N. R., Thalakola, S., Vuyyuru, L. R., & Vatambeti, R. (2025). Cyber threat detection in industry 4.0: Leveraging GloVe and self-attention mechanisms in BiLSTM for enhanced intrusion detection. Computers and Electrical Engineering, 124, 110368.
[19] Burra, R. S., APCV, G. R., & Vellela, S. S. (2024). Enhancing Ddos Detection Through Semi-Supervised Machine Learning: A Novel Approach for Improved Network Security. International Research Journal of Modernization in Engineering Technology and Science, 6.
[20] Vellela, S. S., Manne, V. K., Trividha, G., Chaithanya, L., & Shaik, A. (2025). Intelligent Transportation Systems AI and IoT for Sustainable Urban Traffic Management. Available at SSRN 5250812.
[21] Burra, R. S., APCV, G. R., & Vellela, S. S. (2024). Enhancing Ddos Detection Through Semi-Supervised Machine Learning: A Novel Approach for Improved Network Security. International Research Journal of Modernization in Engineering Technology and Science, 6.
[22] Vellela, S. S., Chandra, S. S., Thommandru, R., Mastan Basha, S., & Sri Ram, D. (2023). Novel Approach to Mitigate Starvation in Wireless Mesh Networks. Available at SSRN 5262254.
[23] Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. Computer Networks, 52(12), 2292–2330. DOI: 10.1016/j.comnet.2008.04.002

Author's Profile

Mrs. M. Anitha is currently serving as an Assistant Professor and Head of the Department of Master of Computer Applications (MCA) at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District, Andhra Pradesh, India. She holds a Bachelor of Technology (B.Tech), a Master of Computer Applications (MCA), and a Master of Technology (M.Tech) in Computer Science and Engineering. With over 14 years of teaching experience at SRK Institute of Technology, she has been actively involved in both academic and administrative roles. Her primary areas of interest include Machine Learning using Python and Database Management Systems (DBMS). She is dedicated to fostering academic excellence and promoting practical learning in advanced computing technologies.

Mr. K. Hareesh Working as Assistant Professor, Dept. of MCA, in SRK Institute of technology in Vijayawada. He done with MCA, M. Tech. he has 4 years of Teaching experience in SRK Institute of technology, Enikepadu, Vijayawada, NTR District. His area of interest includes Machine Learning with Python, and DBMS.

P. Mohankrishna is an MCA Student in the Department of Computer Application at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. He has completed degree in B.com from Venkateswara degree college kanuru. His area of interest is DBMS and Machine learning with python