PACKET HIDING MECHANISM FOR SELECTIVE JAMMING TECHNIQUES

Ashish Ladda[1], K. Reethika[2], G. Sunny[3], G. Pravalika[4], M. Shirisha[5], Dr. V.Venkateshwarlu[6]

[1,2,3,4,5,6] Department of CSE, Balaji Institute of Technology and Science, Laknepally, Warangal, India

ABSTRACT

Wireless networks are vulnerable to intentional interference attacks, known as jamming, which can facilitate Denial-of-Service attacks. While traditional jamming security focus on external risks, internal adversaries can launch low-effort, selective jamming attacks targeting high-priority messages. This work addresses selective jamming attacks, demonstrating their effectiveness through case studies on TCP and routing. We propose three schemes combining cryptographic primitives with physical-layer attributes to avoid real-time packet classification, thereby reducing selective jamming attacks. We examine the security of methods and evaluate their computational and communication over.

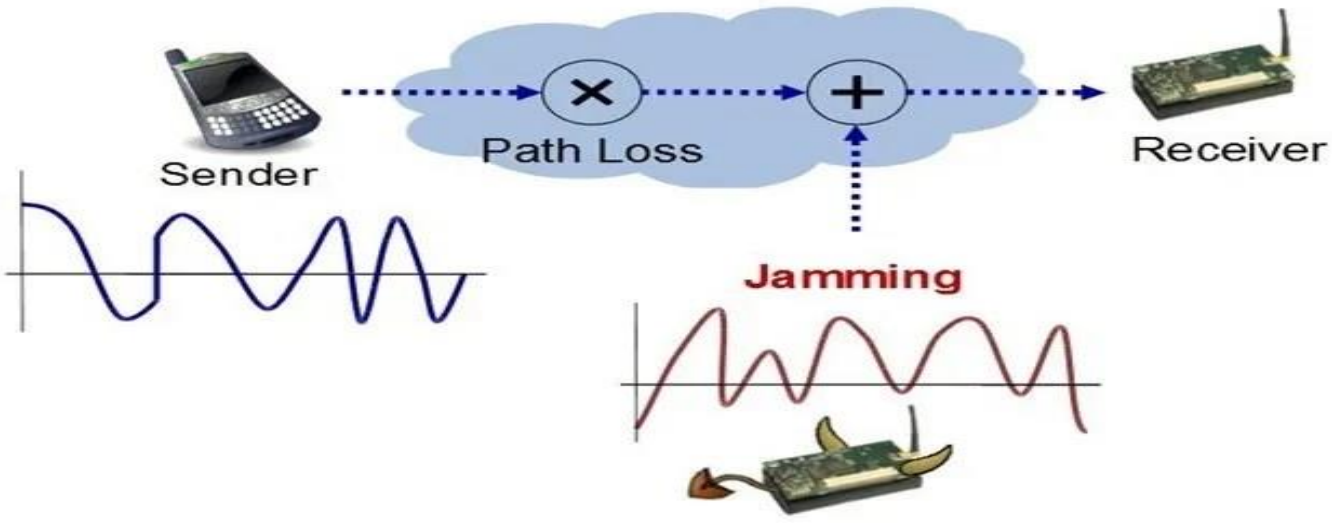
Keywords: selective jamming attacks, Denial-of-service attacks, cryptographic, physical layer.

1. INTRODUCTION

In today's digital world, wireless communication is essential for various applications, from personal devices to critical infrastructure. However, this efficiency comes with significant security challenges, particularly from attackers who employ selective jamming techniques. Selective jamming involves disrupting specific data packets while allowing others to pass through, making it a more targeted and efficient form of attack. To counter these threats, packet hiding mechanisms are crucial. These mechanisms aim to hide the presence and content of important data packets, making it difficult for attackers to identify which packets to jam. By implementing strategies such as packet fragmentation, encryption, and randomization, we can enhance the resilience of wireless communication against selective jamming. This project explores various packet hiding techniques, evaluates their effectiveness, and propose new methods to improve the security of wireless network. By understanding and reducing the risks connecting with selective jamming, we can secure more stable and secure communication in an increasingly interconnected world[1-15].

In a selective jamming attack, the adversary does not blindly jam all transmissions but instead targets specific high-value packets, such as TCP acknowledgments or routing control messages. This allows the attacker to degrade network performance with minimal effort while remaining undetected. Such an attack requires real-time packet classification, which can be achieved by manipulating protocol semantics or by decoding packet headers on fly to retrieve critical identifiers. Once target packet is identified, the attacker can introduce bit error, modeling the massage unusual for the receiver[16-25].

doi: 10.48047/ijiee.2025.15.4.44



2. LITERATURE REVIEW

Title: Enhanced Packet Delivery Techniques Using Packet Hiding Schemes on Jamming Attacks (2021)

This study explores the use of cryptographic puzzle-based hiding schemes to enhance packet delivery in the presence of jamming attacks. The proposed methods aim to prevent adversaries from classifying and selectively jamming packets by making it algorithmically impossible to decode packet contents in real-time.

Limitations:

- Computational delays due to cryptographic puzzles
- Increased processing overhead and energy consumption
- Ineffective against advanced attackers with significant computational resources

Title: Selective Jamming Attacks Based On Swarm Intelligence Optimized Multi-Metric Packet Hiding Method (2022)

This research introduces a packet-hiding method optimized using swarm intelligence techniques. The approach improves the toughness of wireless networks against selective jamming by dynamically adjusting packet-hiding parameters based on network conditions, thereby enhancing efficiency and packet delivery ratios.

Limitations:

- Performance depends on accurate optimization of swarm intelligence parameters
- Increased computational complexity may introduce latency
- Effectiveness against evolving jamming techniques not extensively evaluated

Title: Jamming And Anti-Jamming Techniques In Wireless Networks (2023)

This comprehensive survey reviews various jamming attacks and corresponding anti-jamming strategies, providing a detailed analysis of existing techniques and their effectiveness.

Limitations:

- Primarily a survey paper, lacking experimental validation or simulation results
- Limited discussion on AI-based detection and mitigation strategies

doi: 10.48047/ijiee.2025.15.4.44

Advanced countermeasures and techniques for mitigating attacks in wireless communication networks (2024)

This research provides an in-depth analysis of various jamming attacks and introduces advanced anti-jamming techniques, including spread spectrum modulation and beam forming, to enhance network security.

Limitations:

- Primarily theoretical analysis, lacking real-world implementation and testing
- Spread spectrum and beamforming techniques require additional hardware, increasing system costs
- Effectiveness against adaptive jammers not fully explored

Jamming Attacks And Anti-Jamming Strategies In Wireless Networks (2024)

This survey explores into the evolution of jamming attacks and the development of sophisticated anti-jamming strategies, highlighting the role of software –defined radio technology in enhancing spectral and energy efficiency.

Limitations:

- Lacks detailed comparative analysis of performance metrics
- Does not provide implementation guidelines or best practices for real-World deployment
- Does not discuss quantum cryptography and next-generation wireless technologies

3. PROBLEM STATEMENT

Wireless networks are vulnerable to selective jamming attacks by insiders who interrupt high-priority packets. Existing anti-jamming techniques are ineffective against such risks, this project aims to design a secure packet hiding mechanism to avoid real-time packet classification and reduce selective jamming attacks. The consequences of selective jamming attacks can be severe, leading to significant disruptions in critical applications such as real-time communication, financial transactions, and healthcare services. Furthermore, the lack of effective countermeasures against selective jamming attacks can erode trust in wireless networks, ultimately undermining their widespread adoption. Therefore, it is mandatory to develop creative solutions that can effectively reduce selective jamming attacks and ensure the reliability and security of wireless networks.

4. REQUIREMENTS

Hardware Requirements:

- High-performance computing system with multi-core processor.
- Network simulator software (eg., NS-3, OMNeT++)

doi: 10.48047/ijiee.2025.15.4.44

- Testbed with wireless communication devices.

Software Requirements:

- Programming languages (e.g., C++, Python).
- Network simulator software.
- Data analysis and visualization tools (e.g., MATLAB, Python)

5. PROPOSED SYSTEM

This research paper explores the critical issue of jamming attacks with wireless networks, focusing on internal threats. Wireless networks have become essential in today's interconnected world, but their convenience and flexibility also introduce vulnerabilities that can be exploited by malicious entities.

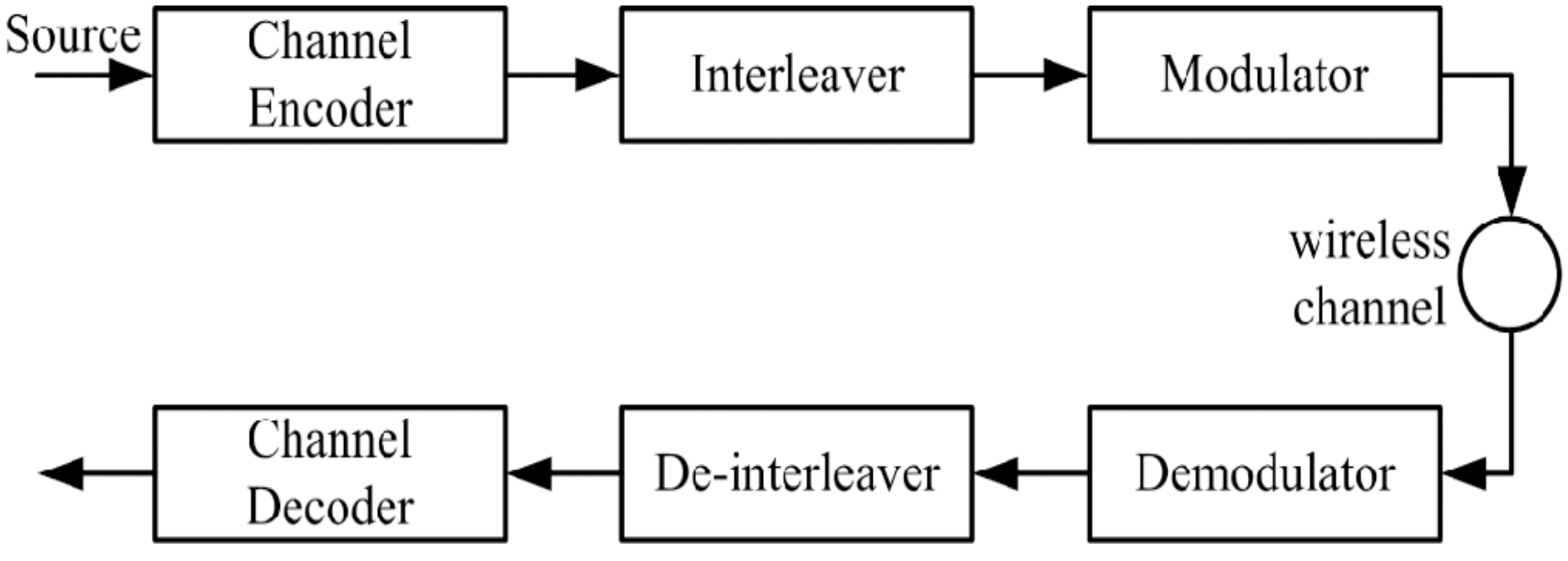
A sophisticated adversary with knowledge of network secrets and protocol implementation details can launch selective jamming attacks, targeting high-importance messages crucial for network functioning. For instance, they can disrupt route discovery by targeting route-request messages or severely degrade network throughput by targeting TCP acknowledgments. To execute such attacks, the adversary must employ a "classify-then-jam" strategy, involving packet classification using protocol semantics or real-time decoding. This requires an in-depth understanding of both physical and upper layer protocols, as well as quick packet analysis and processing.

The ability of an adversary to launch selective jamming attacks highlights the need for effective countermeasures. Implementing robust security protocols, using spread-spectrum techniques, or employing machine learning algorithms can detect and implementing such countermeasures, we can ensure the reliability and security of wireless networks and prevent the devastating consequences of selective jamming attacks. This research aims to contribute to the development of effective countermeasures and improve the overall security of wireless networks.

6. ARCHITECTURE

Consider the generic communication system depicted in below figure. At the Physical layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, de-interleaved, and decoded, to recover the original packet m.

doi: 10.48047/ijiee.2025.15.4.44



7. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation designing of methods to achieve changeover and evaluation of changeover methods.

7.1 MODULES

7.1.1 Network module

Solves the issue of stopping jamming nodes from classifying packets in real-time. The network is composed of nodes connected through wireless links, and nodes exchange information directly or indirectly through multiple hops. Exchanges may be unicast, broadcast, unencrypted, or encrypted.

7.1.2 Real Time Packet Classification

Take into account the generic communication system. Packet classification can be achieved by utilizing static parts of transmitted packets. However, a malicious user can utilize static parts of transmitted packets. However, a malicious user can utilize static cipher text parts for packet classification.

7.1.3 Selective Jamming Module

Describe the effects of selective jamming attacks in two multi-hop wireless network scenarios, demonstrating the potential damage caused by such attacks.

7.1.4 Strong Hiding Commitment Scheme (SHCS)

doi: 10.48047/ijiee.2025.15.4.44

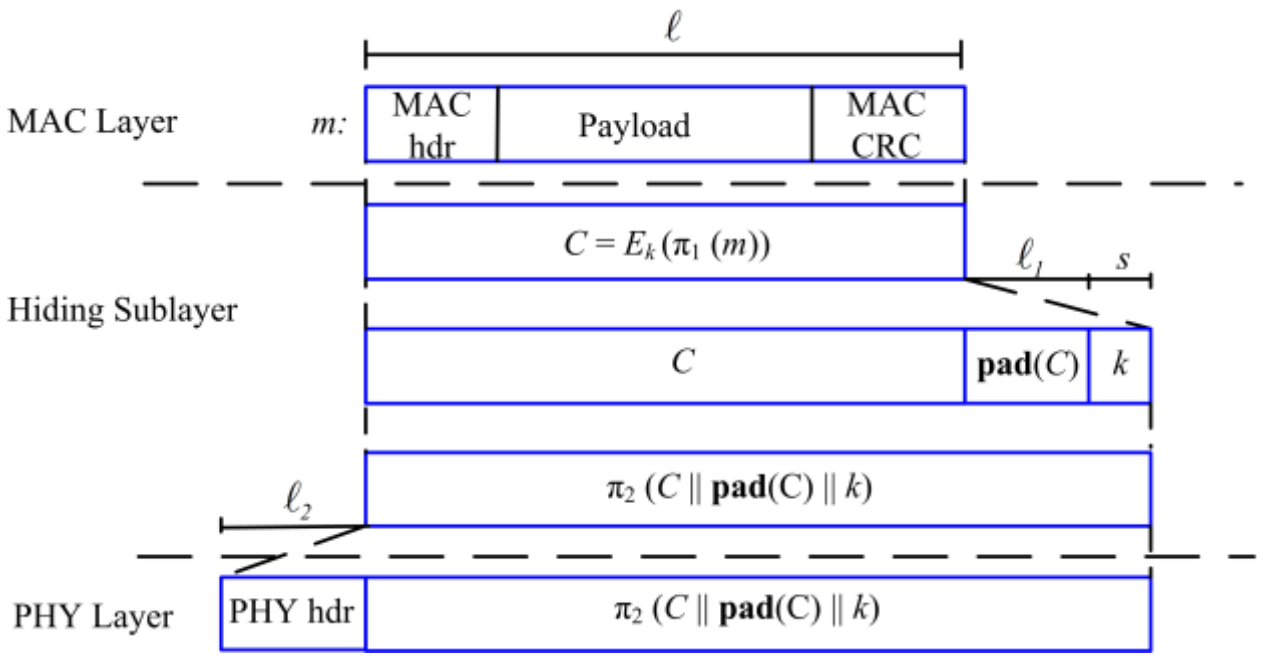


Fig 3: Strong hiding commitment scheme

It presents a strong hiding commitment scheme with symmetric cryptography. This scheme supports the strong hiding property with minimum computation and communication overhead, requiring only one symmetric decryption at the receiver.

7.1.5 Cryptographic Puzzle Hiding Scheme (CPHS)

It provides a packet hiding scheme using cryptographic puzzles. This scheme compels the receiver to perform pre-determined computations prior to extracting a secret. While security does not depend on physical layer parameters, this approach incurs increased computation and communication overhead.

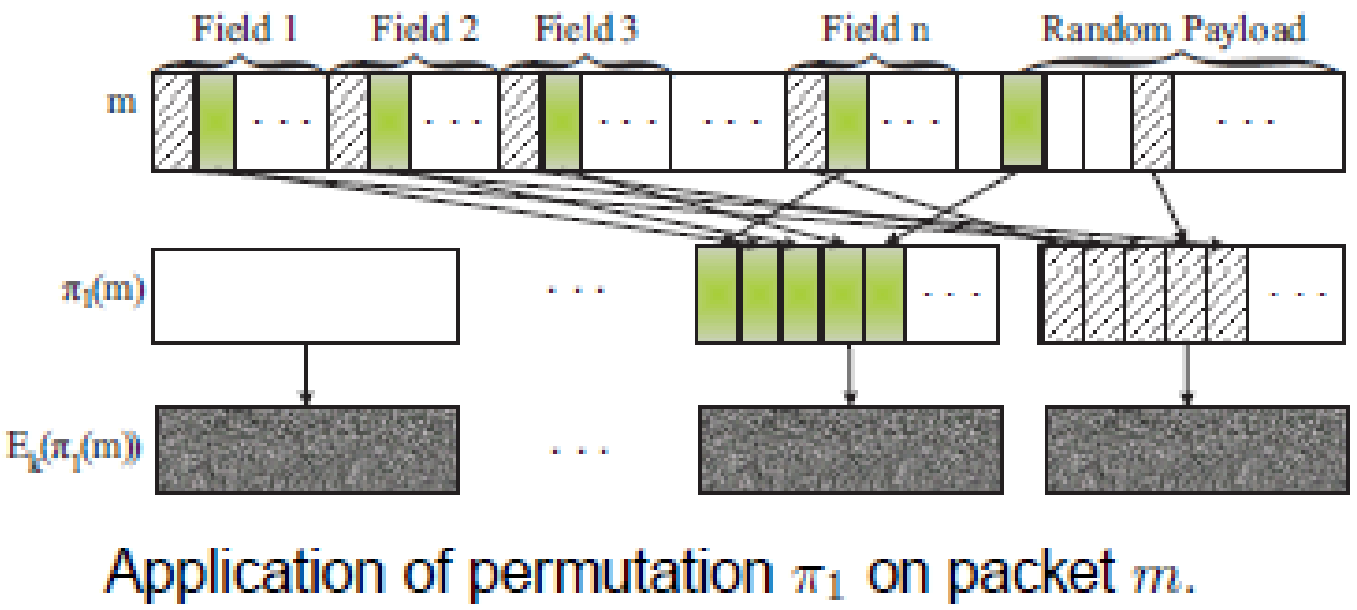
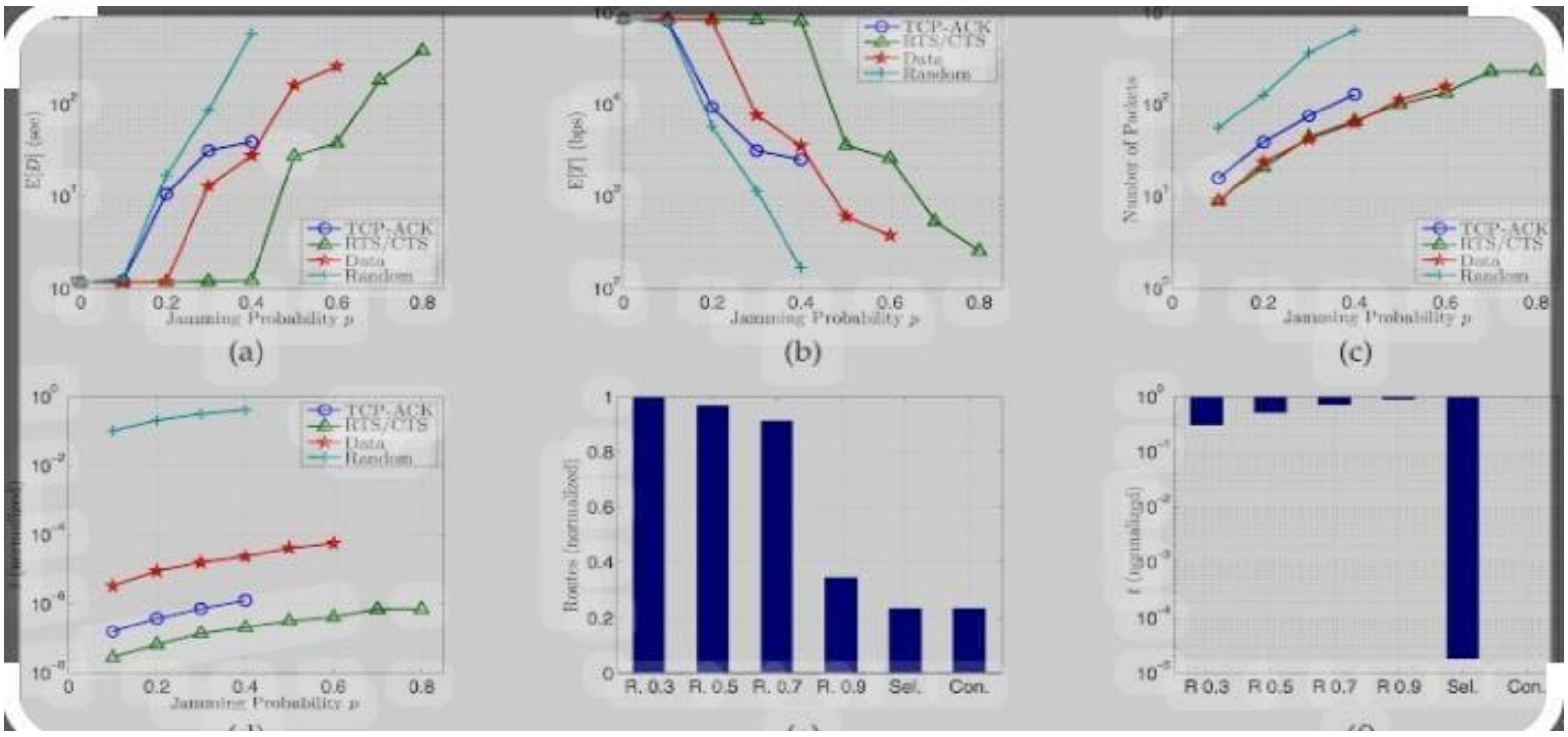


Fig 4: Cryptographic Puzzle Hiding Scheme

doi: 10.48047/ijiee.2025.15.4.44

8. RESULT



9. CONCLUSION

In conclusion, selective jamming attacks pose a significant threat to wireless networks, particularly when launched by internal adversaries. Our research demonstrated the devastating impact of such attacks on network performance. To mitigate this threat, we develop three novel schemes that effectively transform a selective jammer into random one, thereby preventing real-time packet classification. By combining cryptographic primitives with physical layer characteristics, our solutions provide a robust defense against selective jamming attacks, ensuring the reliability and security of wireless networks.

10. REFERENCES

1. Goldreich Foundations of cryptography: Basic applications. Cam-bridge University Press, 2004.

doi: 10.48047/ijiee.2025.15.4.44

2. A. Juels,J. Brainard. Client puzzles,"A cryptographic countermeasure against connection depletion attcks", In Proceedings of NDSS, 1999.
3. L. Lazos, S. Liu, M. Krunz,"Mitigating control-channel jamming attackes in multi-channel Ad-Hoc networks", In proceedings of the 2nd ACM conference on wireless network security, 2009.
4. G. Noubir, G. Lin,"Low-power DoS attacks in data wireless lans and countermeasures", Mobile Computing and Communication Review, 2003.
5. R. C. Merkle,"Secure communications over insecure channels", Communications of the ACM, 1978.
6. R. Rivest, A. Shamir, D. Wagner,"Time-lock puzzles and timed-release crypto", Massachusetts Institute of Technology, 1996.
7. W. Trappe, Y. Zhang, t. wood,"The feasibility of launching and detecting jamming attacks in wireless network", In Proceedings of MobiHoc, 2005.
8. W.Xu, T.Wood, W. Trappe, Y. Zhang,"Channel surfing and spatiall retreats: defences against wireless denial of service", In Proceedings of the 3rd ACM workshop on Wireless security, 2004.
9. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima" A Brain Tumor Identification and Classification Using Deep Learning based on CNN-LSTM Method" Computers and Electrical Engineering , 101 (2022) 107960
10. Ramdas Vankdothu,.Mohd Abdul Hameed "Adaptive features selection and EDNN based brain image recognition on the internet of medical things", Computers and Electrical Engineering , 103 (2022) 108338.
11. Ramdas Vankdothu,.Mohd Abdul Hameed,Ayesha Ameen,Raheem,Unnisa " Brain image identification and classification on Internet of Medical Things in healthcare system using support value based deep neural network" Computers and Electrical Engineering,102(2022) 108196.
12. Ramdas Vankdothu,.Mohd Abdul Hameed" Brain tumor segmentation of MR images using SVM and fuzzy classifier in machine learning" Measurement: Sensors Journal,Volume 24, 2022, 100440 .
13. Ramdas Vankdothu,.Mohd Abdul Hameed" Brain tumor MRI images identification and classification based on the recurrent convolutional neural network" Measurement: Sensors Journal,Volume 24, 2022, 100412 .
14. Bhukya Madhu, M.Venu Gopala Chari, Ramdas Vankdothu,.Arun Kumar Silivery,Veerender Aerranagula " Intrusion detection models for IOT networks via deep learning approaches " Measurement: Sensors Journal,Volume 25, 2022, 100641
15. Mohd Thousif Ahemad ,Mohd Abdul Hameed, Ramdas Vankdothu" COVID-19 detection and classification for machine learning methods using human genomic data" Measurement: Sensors Journal,Volume 24, 2022, 100537
16. S. Rakesh [a], NagaratnaP. Hegde [b], M. VenuGopalachari [c], D. Jayaram [c], Bhukya Madhu [d], MohdAbdul Hameed [a], Ramdas Vankdothu [e], L.K. Suresh Kumar "Moving object detection using modified GMM based background subtraction" Measurement: Sensors ,Journal,Volume 30, 2023, 100898
17. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Efficient Detection of Brain Tumor Using Unsupervised Modified Deep Belief Network in Big Data" Journal of Adv Research in Dynamical & Control Systems, Vol. 12, 2020.
18. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Internet of Medical Things of Brain Image Recognition Algorithm and High Performance Computing by Convolutional Neural Network" International Journal of Advanced Science and Technology, Vol.

doi: 10.48047/ijiee.2025.15.4.44

29, No. 6, (2020), pp. 2875 – 2881

19. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Convolutional Neural Network-Based Brain Image Recognition Algorithm And High-Performance Computing", Journal Of Critical Reviews,Vol 7, Issue 08, 2020(Scopus Indexed)
20. Ramdas Vankdothu, Dr.Mohd Abdul Hameed "A Security Applicable with Deep Learning Algorithm for Big Data Analysis",Test Engineering & Management Journal,January-February 2020
21. Ramdas Vankdothu, G. Shyama Chandra Prasad " A Study on Privacy Applicable Deep Learning Schemes for Big Data" Complexity International Journal, Volume 23, Issue 2, July-August 2019
22. Ramdas Vankdothu, Dr.Mohd Abdul Hameed, Husnah Fatima " Brain Image Recognition using Internet of Medical Things based Support Value based Adaptive Deep Neural Network" The International journal of analytical and experimental modal analysis, Volume XII, Issue IV, April/2020
23. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima" Adaptive Features Selection and EDNN based Brain Image Recognition In Internet Of Medical Things " Journal of Engineering Sciences, Vol 11,Issue 4 , April/ 2020(UGC Care Journal)
24. Ramdas Vankdothu, Dr.Mohd Abdul Hameed " Implementation of a Privacy based Deep Learning Algorithm for Big Data Analytics", Complexity International Journal , Volume 24, Issue 01, Jan 2020
25. Ramdas Vankdothu, G. Shyama Chandra Prasad" A Survey On Big Data Analytics: Challenges, Open Research Issues and Tools" International Journal For Innovative Engineering and Management Research,Vol 08 Issue08, Aug 2019

doi: 10.48047/ijiee.2025.15.4.44

BIBLIOGRAPHY

I am Kolipaka Reethika from the Department of Computer Science and Engineering. Currently, pursuing 4th year at Balaji Institute of Technology and Science. My research is done based on “Packet Hiding Mechanism for Selective Jamming Techniques”.

I am Gogikar Sunny from the Department of Computer Science and Engineering. Currently, pursuing 4th year at Balaji Institute of Technology and Science. My research is done based on “Packet Hiding Mechanism for Selective Jamming Techniques”.

I am Gurrala Pravalika from the Department of Computer Science and Engineering. Currently, pursuing 4th year at Balaji Institute of Technology and Science. My research is done based on “Packet

doi: 10.48047/ijiee.2025.15.4.44

Hiding Mechanism for Selective Jamming Techniques".

I am Manubothula Shirisha from the Department of Computer Science and Engineering. Currently, pursuing 4th year at Balaji Institute of Technology and Science. My research is done based on "Packet Hiding Mechanism for Selective Jamming Techniques".

doi: 10.48047/ijiee.2025.15.4.44