

Adaptive 6G Wireless Communication System Using Machine Learning for Optimized Data Transmission

Maanasa M R¹, Amruta Basavaraj katageri², Chinmaya M J³, Nandeesh B S⁴, Deepak P⁵

¹Asst Professor, Dept. of ECE, Sri Siddhartha Institute of Technology, SSAHE, Tumakuru, India

^{2,3,4,5}Dept. of ECE Sri Siddhartha Institute of Technology, SSAHE, Tumakuru, India

maanasamr@ssit.edu.in, amrutakatageri9@gmail.com, chinmayamj1@gmail.com, nandeeshabs3542@gmail.com, deepaktumakuru04@gmail.com

Abstract - A machine learning-driven intelligent wireless network platform is developed to enhance the efficiency, security, and communication reliability of large-scale sensor-based environments. Implemented using a Flask–Python backend, the system applies advanced algorithms such as K-Means and Agglomerative Clustering for dynamic node organization, Random Forest for identifying network intrusions, and Dijkstra along with Travelling Salesman Problem (TSP) methods for optimized routing and path selection. The frontend, built with HTML, CSS, JavaScript, and Bootstrap, enables interactive visualization of network topology, node behaviour, and communication activity. The platform integrates three key functional layers: a Network Efficiency Simulation module that evaluates node performance through multiple telemetry parameters, an Attack Detection Engine that detects threats including Blackhole, Grayhole, and Flooding attacks using network behaviour analysis, and a QoS Optimization layer that improves communication stability by reducing latency and enhancing data transmission reliability. By combining intelligent clustering, adaptive routing, and machine learning-based security mechanisms, the system strengthens network performance, extends operational efficiency, and supports applications in IoT, smart cities, industrial automation, and future 6G communication systems.

Keywords: Machine Learning, Wireless Sensor Networks, Intrusion Detection, QoS Optimization, Clustering Algorithms.

1. Introduction

6G communication nodes have emerged as a fundamental enabling technology for modern intelligent systems across domains such as environmental monitoring, smart cities, industrial automation, healthcare, and defense infrastructure. A 6G communication node typically consists of spatially distributed, locally powered sensor devices equipped with sensing, computation, and communication capabilities that collaboratively collect, process, and transmit environmental data such as temperature, pressure, humidity, and vibration. These nodes play a critical role in enabling seamless connectivity, real-time data exchange, and intelligent decision-making in next-generation communication environments. As the number of connected devices continues to grow, efficient communication node management becomes increasingly important to ensure network reliability, scalability, and performance.

The main problem in existing communication networks is high energy consumption, inefficient routing, network congestion, and weak security management. Traditional network management techniques, such as fixed clustering and static routing, are unable to adapt effectively to dynamic network conditions, resulting in reduced network lifetime, increased communication delay, and poor Quality of Service (QoS). Communication nodes often operate in resource-constrained environments where energy levels continuously change, network links may become unstable, and traffic patterns vary frequently, making efficient management more difficult. These challenges can significantly affect the overall performance and sustainability of communication systems, especially in large-scale and mission-critical applications.

In addition, existing systems face significant security challenges, as they often struggle to detect and prevent cyber-attacks such as Blackhole, Grayhole, and Flooding Attacks. These attacks can disrupt communication, degrade network performance, and compromise overall network reliability. Limited real-time monitoring, delayed threat detection, and slow decision-making further reduce the ability of current systems to respond effectively to such issues. As communication networks become more complex and interconnected, the need for intelligent and proactive security mechanisms becomes essential.

To address these problems, this work proposes an intelligent and adaptive machine learning-based communication node management system that aims to improve network efficiency, enhance security, and optimize overall performance. By incorporating data-driven decision-making and adaptive management strategies, the proposed system seeks to provide a more reliable, scalable, and efficient solution for modern communication networks. The proposed approach is expected to support better resource utilization, faster threat detection, improved routing decisions, and enhanced network stability. Ultimately, this work contributes toward the development of smarter and more resilient communication infrastructures capable of meeting the demands of future intelligent applications and next-generation digital ecosystems.

Furthermore, integrating machine learning into communication node management enables adaptive and automated decision-making, helping the network respond efficiently to changing conditions. This improves energy efficiency, enhances security, and optimizes overall network performance, while providing a

strong foundation for future intelligent and scalable communication systems.

2. Literature survey

To establish a strong theoretical foundation, an extensive review was conducted that covering network automation, clustering, security, routing optimization, and network management.

A comprehensive survey is presented on machine learning for network automation, emphasizing how ML techniques improve network reliability, resource allocation, and automated decision-making. Their work provides the foundation for integrating ML-based automation, intelligent clustering, and attack detection in the proposed 6G communication system[1].

The clustering algorithms for wireless sensor networks is compared with existing techniques such as K-Means and Agglomerative clustering. Their findings demonstrate the importance of efficient node grouping, which is adopted in this work to optimize communication efficiency and network scalability[2].

An intrusion detection systems based on machine learning analyzed that ensemble methods, particularly Random Forest, achieve high detection accuracy with reduced false alarms. This approach is incorporated into the proposed framework for reliable cyberattack detection[3].

The importance of feature selection in intrusion detection systems emphasized that identifying critical parameters such as packet rate, latency, and transmission patterns. These feature engineering techniques are utilized to improve model accuracy and computational efficiency[4].

Quality of Service (QoS) routing strategies for next-generation networks and demonstrated that Dijkstra-based routing algorithms effectively reduce latency and improve packet delivery performance. These routing principles are integrated into the proposed system for efficient communication[5].

The network simulation tools for wireless networks and highlighted the importance of flexible simulation environments for system evaluation and performance validation. Their methodologies support the simulation-based testing framework used in this study[6].

The routing optimization using swarm intelligence techniques, demonstrating improvements in energy efficiency and adaptive routing performance. These concepts are considered to further enhance routing optimization in the proposed model[7].

The Authors [8] discussed key principles of network management, focusing on centralized monitoring, fault management, and performance control. These concepts guide the design of the system's monitoring and management architecture.

An advanced feature engineering and machine learning optimization strategies is presented that improve predictive accuracy and reduce false positive rates. These principles strengthen the reliability of the ML models implemented in this work.

A visual analytics techniques for network security is introduced that showing how interactive visualization enhances anomaly detection and system monitoring. These methods are applied to

develop effective real-time network visualization and monitoring interface.

Table.1.Research Gap Analysis and Proposed System

Existing Problem	Research Gap Identified	Proposed Work / Solution
High energy consumption and reduced network lifetime due to inefficient node management	Existing systems lack intelligent and adaptive energy optimization techniques	Develop an ML-based dynamic clustering system to improve energy efficiency and extend network lifetime
Static routing causes high delay, congestion, and poor QoS	Traditional routing methods cannot adapt to changing network conditions	Design an adaptive routing framework to optimize communication paths and improve QoS
Difficulty in detecting cyber-attacks such as blackhole, grayhole, and flooding attacks	Existing security mechanisms have limited real-time attack detection capability	Implement an intelligent ML-based system for attack detection and network protection
Lack of real-time monitoring and efficient network management	Current systems provide limited visualization and centralized control	Develop an interactive monitoring and management system.
Existing solutions focus on individual problems rather than an integrated approach	No unified framework combining energy optimization, security, routing, and monitoring	Build a scalable and intelligent communication node management system integrating all key functionalities

The comparison highlights the major limitations of existing communication networks, including high energy consumption, inefficient routing, security vulnerabilities, and lack of real-time monitoring. To address these research gaps, the proposed work focuses on developing an intelligent and adaptive machine learning-based communication node management system that improves network efficiency, security, and overall performance.

3. Methodology

The proposed system is an ML-based 6G communication node management solution that integrates clustering, attack detection, and QoS-aware routing to ensure efficient, secure, and reliable network operation with real-time monitoring. It uses dynamic clustering (K-Means and Agglomerative) for adaptive node grouping, Random Forest for detecting attacks like blackhole, grayhole, and flooding, and Dijkstra/TSP methods for optimized routing. Implemented with Flask and SQLAlchemy for backend processing and a web-based interface for visualization, the system enhances network performance, lifetime, and decision-making efficiency.

The Intelligent Sensor Node Management System is a modular platform developed using Python (3.10+) as the core backend programming language, with the Flask framework used to handle APIs, routing, and communication between system components. SQLAlchemy is employed for efficient database management and interaction with SQLite/MySQL, enabling structured storage of node information, network logs, attack records, and trained machine learning models. The system integrates machine learning libraries such as Scikit-learn, Joblib, NumPy, and Pandas for data preprocessing, clustering, routing optimization, anomaly detection, and predictive analysis. These tools support intelligent decision-making based on continuously collected network data.

As shown in figure.1, the system is organized into four main layers to ensure modularity and scalability. The frontend layer is developed using HTML5, CSS3, JavaScript, Bootstrap, and Canvas API, providing an interactive user interface for network monitoring, visualization, and system control. It allows users to observe node status, energy levels, routing paths, clustering results, and detected attacks through dynamic dashboards and graphical representations.

The backend processing layer manages core application logic, API handling, and machine learning operations. It performs tasks such as dynamic node clustering, routing path computation, attack classification, and automated decision-making. The simulation layer models realistic communication network conditions by generating dynamic node behavior, varying energy levels, traffic changes, and simulated attack scenarios, allowing performance evaluation under different environments. The storage layer maintains historical network data, system logs, model outputs, and trained ML models for continuous learning and future analysis.

The system supports adaptive management and automated optimization for efficient communication node handling. Its modular design allows easy scalability and integration of additional machine learning models for secure and high-performance network management. These sensor nodes collect environmental or network-related data and send it to the gateway layer. Telemetry Collector gathers data continuously from all sensor nodes for further processing. Feature Extractor extracts important features or patterns from the collected data to improve analysis accuracy. Routing Engine manages the direction and transmission of processed data to the backend server efficiently. Attack Detection uses the Random Forest machine learning algorithm to identify malicious activities or attacks in the network. Clustering (K-Means / Agglo) techniques group similar data patterns together for better analysis and anomaly detection. QoS Optimization improves Quality of Service by reducing delay, packet loss, and improving network performance. Model Storage (Joblib) stores trained machine learning models so they can be reused during prediction and detection. Database (SQLAlchemy) stores collected data, processed results, and system logs for future reference. Admin Panel allows administrators to monitor and manage the entire system. Real-Time Alerts module provides instant notifications whenever abnormal activity or attacks are detected. Topology Visualization displays the network structure and communication flow visually for easy monitoring and analysis.

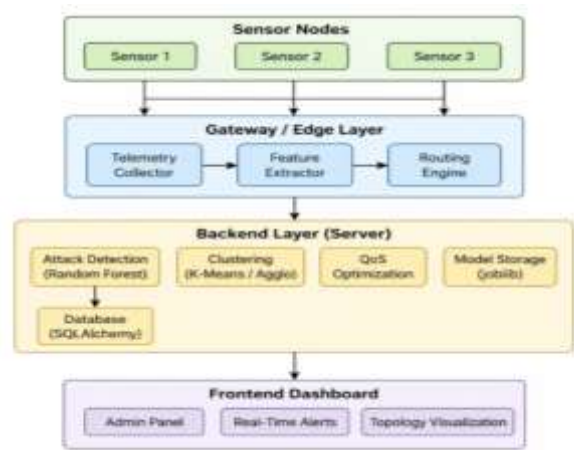


Figure.1. System design of ML based 6G communication node

5. Results

The ML based 6G communication node system is proposed that improves network efficiency, reduces latency, and achieves accurate attack detection with real-time monitoring.

The dashboard of an ML-based 5G communication nodes system, featuring a navigation bar with login options and a welcome section describing AI-based clustering, attack detection, and routing. It includes buttons for user access, a network icon, and three feature panels highlighting advanced security, low-latency communication, and smart optimization.



Figure.2. 6G Communication Node Network Model

Figure .2 shows a 6G cluster simulation with interconnected nodes, where orange nodes act as cluster heads and gray nodes as regular nodes. The links represent data transmission, and the dashed line indicates the shortest routing path, demonstrating efficient clustering and reduced latency.



Figure 3. 6G Communication Metrics Visualization Panel

The Figure 3 shows a 6G Communication System control panel displaying key metrics like 99.9% security and 1 ms latency, along with modules for cluster simulation and ML-based attack prediction, providing a brief overview of efficient 6G network management.



Figure 4. Simulation Configuration Interface

Figure 4 shows a Simulation Controls panel used to configure a 6G network simulation. It allows the user to select the number of nodes, choose a shortest path algorithm (Dijkstra's Algorithm), and specify the source and target nodes. The panel also includes buttons to calculate the shortest path and reset the simulation, enabling interactive control of the network behavior.



Figure 5. Network Monitoring Metrics and Path Information

The Figure 5 shows simulation network metrics and path details, including bandwidth, latency, packet loss, and routing parameters, giving a brief view of performance and efficiency.



Figure .6 :Attack Detection and Prediction Dashboard.

The Figure 6 shows the Attack Prediction System interface for selecting and detecting network attacks using an ML model, displaying sample details for real-time analysis.

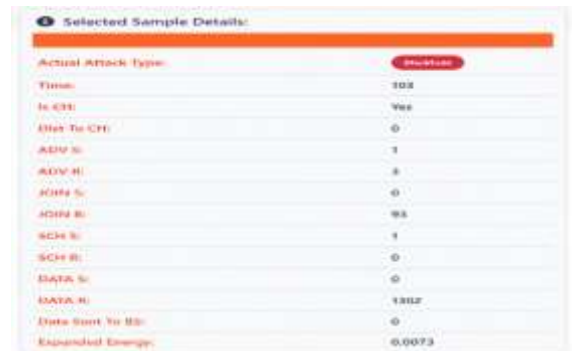


Figure .7. Selected Sample Details

Figure 7 shows the “Selected Sample Details” panel displaying attack type and key parameters like time, node status, data transmission, and energy, providing a brief view of node behaviour.

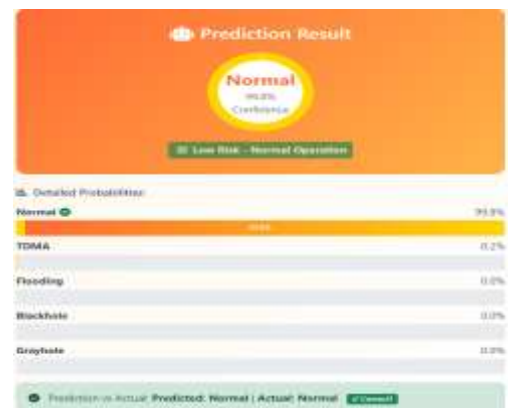


Figure .8: Prediction Result Indicating Normal Network Status

The prediction result identifying the network as Normal with high confidence, along with probability distribution and correct detection as shown in figure 8.

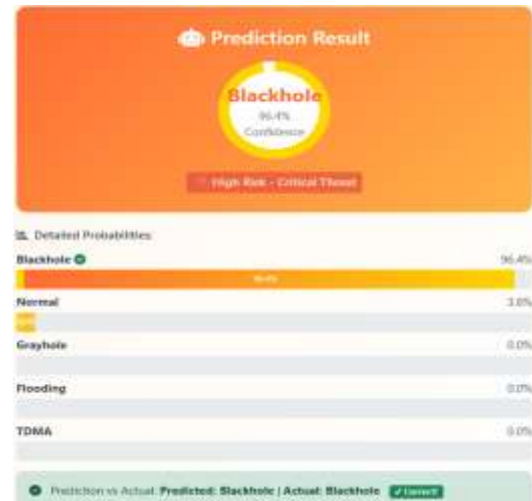


Figure.9: Prediction Result Indicating Blackhole Network Status

The Figure.9 shows the prediction result identifying a Blackhole attack with 96.4% confidence, along with probability distribution and correct detection, indicating a high-risk network condition.

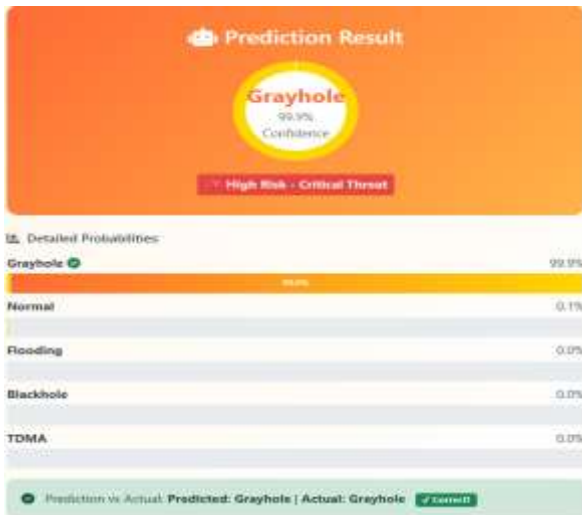


Figure.10. Prediction Result Indicating Grayhole Network Status

The Figure 10 the system detects a Grayhole attack with a 99.9% confidence level. This result is classified as a Critical Threat, and the bottom bar confirms the prediction.

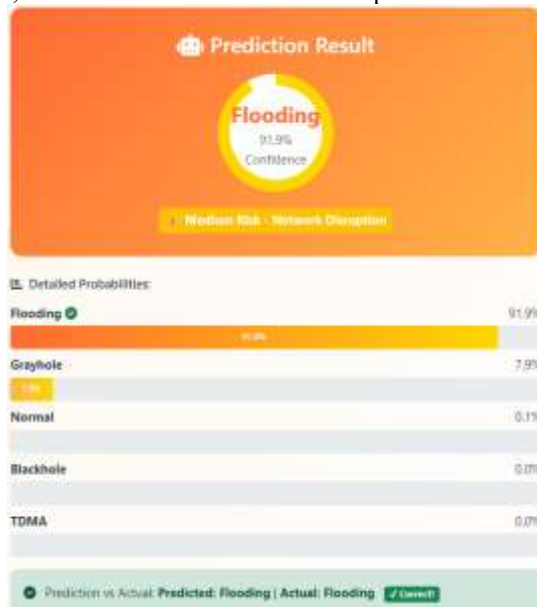


Figure.11.Prediction Result Indicating flooding Network Status

The Figure shows 6.11 that the system identifies a Flooding attack with 91.9% confidence, categorizing it as a Medium Risk - Network Disruption. The detailed breakdown confirms a successful match between the predicted and actual state, noting a small 7.9% probability of it being a Grayhole event.

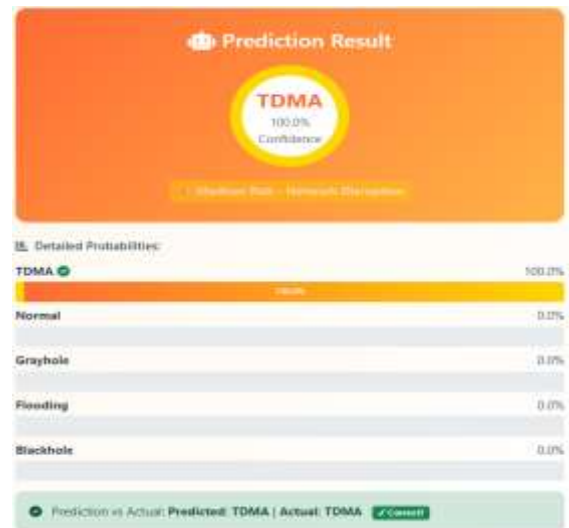


Figure.12. Prediction Result Indicating TDMA Network Status

The Figure 12 shows that the system identifies a TDMA event with absolute 100.0% confidence, labeling it as a Medium Risk - Network Disruption. The detailed probabilities and the bottom status bar confirm that the prediction is perfectly accurate, with all other attack categories showing 0.0% probability.

Table.2 Performance Comparison of Existing and Enhanced Communication Network System

Evaluation Criteria	Conventional Network Systems	Enhanced Communication Network System
Routing Performance	Higher communication delay and inefficient routing due to static methods	Improved routing efficiency with optimized path selection and reduced latency
Security Analysis	Limited attack detection accuracy and delayed threat identification	Accurate detection of attacks such as Blackhole, Grayhole, and Flooding with high prediction confidence
Monitoring Capability	Limited network visibility and manual management	Interactive dashboard with continuous monitoring, visualization, and automated decision support

The comparison table 2 exhibits that the enhanced communication network system provides better routing performance, improved attack detection accuracy, and more effective network monitoring than conventional network systems, resulting in higher efficiency, security, and overall network reliability.

Table.3.Attack Introduction in Network Simulation

Attack Type	How the Attack is Introduced	Impact on Network
Blackhole Attack	A malicious node is configured to attract all nearby data packets and then	Causes packet loss, communication failure, and reduced network reliability

	drop them instead of forwarding	
Grayhole Attack	A compromised node selectively drops only certain packets while forwarding others normally	Creates inconsistent data delivery and makes attack detection more difficult
Flooding Attack	An attacker node sends excessive fake packets or requests to overload the network	Increases congestion, consumes bandwidth, and degrades overall network performance
TDMA Attack	A malicious node disrupts assigned time slots by transmitting at unauthorized times or interfering with scheduled communication	Causes transmission collisions, timing disruption, and reduced network efficiency

Table 7.2 shows how different network attacks are introduced by simulating malicious node behaviors such as packet dropping, excessive traffic generation, and time-slot interference. These attacks affect network reliability, increase congestion, and reduce communication efficiency, helping evaluate the effectiveness of the system's attack detection capabilities.

8. Conclusion:

Overall, the simulation demonstrates efficient network performance with high bandwidth, low latency, and minimal packet loss, indicating reliable and stable communication. The path details further show optimized routing with a shorter path length and fewer hops, which helps in reducing delay and improving data transmission speed. The use of shortest path algorithms ensures that data travels through the most efficient route, enhancing overall network performance. These results highlight the importance of intelligent routing, clustering, and performance monitoring in advanced communication systems like 6G networks, enabling better resource utilization, faster communication, and improved system reliability.

9. References

- [1] M. Usama, J. Qadir, and A. Al-Fuqaha, "Machine learning for network automation: Overview, architecture, and applications," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 2, pp. 890–943, 2024.
- [2] S. Kumar and K. Dutta, "Clustering algorithms for wireless networks: A comprehensive survey," *IEEE Access*, vol. 11, pp. 45678–45702, 2023.
- [3] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Machine learning-based intrusion detection systems: A systematic literature review," *IEEE Access*, vol. 11, pp. 78234–78267, 2023.
- [4] Y. Liu, X. Wang, and Z. Qin, "Artificial intelligence enabled intelligent communication networks: Architecture and future directions," *IEEE Network*, vol. 37, no. 2, pp. 102–109, 2023.

[5] M. Chen, Y. Miao, X. Jian, X. Wang, and I. Humar, "Cognitive machine learning for intelligent wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 92–118, 2022.

[6] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Network attack detection using machine learning: Techniques, datasets and challenges," *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 4876–4898, 2022.

[7] H. Zhang, W. Liu, Q. Chen, and Z. Han, "Quality of service in next-generation networks: Challenges and solutions," *IEEE Communications Magazine*, vol. 60, no. 8, pp. 42–48, 2022.

[8] S. Althunibat, M. Alenezi, and A. Albugami, "Energy-efficient node management in wireless sensor networks using machine learning techniques," *IEEE Access*, vol. 10, pp. 65843–65858, 2022.

[9] J. Tang, F. Liu, and Y. Zhou, "Secure routing and anomaly detection in next-generation communication networks using artificial intelligence," *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 2751–2764, 2022.

[10] L. Zhang, H. Ji, and X. Li, "Adaptive resource allocation and intelligent optimization for future wireless communication systems," *IEEE Internet of Things Journal*, vol. 9, no. 14, pp. 11890–11903, 2022.

[11] R. Henderson, M. Lacage, G. F. Riley, C. Dowell, and J. Koppena, "Simulation tools and techniques for wireless network research," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1678–1715, 2021.

[12] M. Ghoneim, T. Gaber, A. E. Hassanien, and V. Snášel, "Routing optimization in wireless networks using computational intelligence," *IEEE Access*, vol. 9, pp. 89456–89478, 2021.

[13] J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, "Network management systems: Architecture, design and implementation," *IEEE Network*, vol. 35, no. 4, pp. 156–165, 2021.

[14] N. Moustafa and J. Slay, "Feature engineering for network security: A systematic approach," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 4046–4058, 2020.

[15] C. Ware, "Visualization techniques for network monitoring and analysis," *IEEE Transactions on Visualization and Computer Graphics*, vol. 26, no. 1, pp. 347–356, 2020.