ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1852

Analyse Existing Wireless Network Forensic Techniques and Identify their Limitations in Supporting Effective Cybersecurity Decision-Making

Mudambi Geoffrey[1,2]; Davis Matovu[1]; Andrew Lukyamuzi[1]; Semwogere Twaibu[1]; Odongotoo Godfrey[1]; Andrew Alunyu E.[3]

[1]Department of Computer Engineering and Informatics, Faculty of Engineering, Busitema University
[2]Directorate of Information Technology, Busitema University
[3]Department of Information Technology, Faculty of Computing and Information Sciences, Lira University

Publication Date: 2026/05/06

Abstract: The rapid growth of wireless communication technologies has significantly increased the complexity and vulnerability of network environments, making them prime targets for sophisticated cyberattacks. Wireless network forensics plays a crucial role in investigating and responding to such incidents; however, existing forensic techniques often fall short in supporting effective and timely cybersecurity decision-making. These limitations include inadequate real-time analysis, poor scalability in handling large volumes of traffic data, limited automation, and insufficient integration with intelligent decision-support systems. This study aims to analyse existing wireless network forensic techniques and identify their limitations while proposing an intelligent traffic analysis framework to enhance cybersecurity decision-making. The research adopts a mixed-methods approach, combining qualitative analysis of current forensic tools and techniques with quantitative evaluation of network traffic datasets. The study further integrates machine learning algorithms and data analytics methods to develop models capable of detecting, classifying, and predicting anomalous network behaviour in wireless environments. The proposed framework emphasizes real-time traffic monitoring, intelligent anomaly detection, and automated forensic analysis to improve the accuracy, speed, and reliability of cyber incident investigations. Experimental results are expected to demonstrate that the integration of intelligent traffic analysis significantly enhances threat detection capabilities, reduces response time, and supports proactive and evidence-based cybersecurity decisions. This research contributes to the field of network forensics by bridging the gap between traditional forensic methods and intelligent analytical approaches. It provides a scalable and adaptive solution tailored to modern wireless network challenges and offers practical recommendations for improving forensic readiness and cybersecurity resilience in dynamic environments.

Keywords: *Wireless Network Forensics; Intelligent Traffic Analysis; Cybersecurity Decision-Making; Machine Learning; Anomaly Detection; Network Security; Digital Forensics; Real-Time Monitoring; Intrusion Detection Systems; Data Analytics.*

How to Cite: Mudambi Geoffrey; Davis Matovu; Andrew Lukyamuzi; Semwogere Twaibu; Odongotoo Godfrey; Andrew Alunyu E. (2026) Analyse Existing Wireless Network Forensic Techniques and Identify their Limitations in Supporting Effective Cybersecurity Decision-Making. *International Journal of Innovative Science and Research Technology*, 11(4), 3431-3438. https://doi.org/10.38124/ijisrt/26apr1852

I. INTRODUCTION

➢ *Background*

The rapid expansion of wireless communication technologies such as Wi-Fi, mobile networks, and IoT has significantly transformed modern digital infrastructure, enabling flexible and scalable connectivity across sectors. However, this growth has also introduced substantial cybersecurity challenges, as wireless networks are inherently more vulnerable to attacks due to their open transmission medium and dynamic topology. As a result, wireless network forensics has emerged as a critical domain for investigating, analysing, and responding to cyber incidents.

Wireless network forensics involves the capture, preservation, analysis, and presentation of network traffic evidence to support incident response and legal processes. Traditional forensic techniques, including packet capture tools, log analysis, and signature-based intrusion detection

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1852

systems, have been widely used to monitor and investigate network activities. Despite their importance, these techniques often struggle to cope with the increasing volume, velocity, and variety of wireless network data, limiting their effectiveness in modern cybersecurity environments (Behl & Behl, 2018).

One of the key challenges in existing wireless network forensic approaches is the lack of real-time analysis and intelligent automation. Many tools rely on manual processes and post-incident analysis, which delays response times and reduces the ability to prevent attacks proactively. Additionally, conventional systems often exhibit limited scalability and adaptability, making it difficult to detect sophisticated and evolving threats such as zero-day attacks and advanced persistent threats (APTs) (Khan et al., 2020).

Another limitation is the inadequate integration of forensic outputs into cybersecurity decision-making processes. While forensic tools can generate large volumes of data, they often fail to provide actionable insights that support timely and informed decisions. This gap highlights the need for more advanced approaches that incorporate machine learning and intelligent traffic analysis to enhance anomaly detection, pattern recognition, and predictive capabilities (Sommer & Paxson, 2019).

Furthermore, wireless environments present unique forensic challenges, including data volatility, encryption, mobility, and heterogeneous protocols, which complicate evidence collection and analysis. These factors necessitate the development of more robust and adaptive forensic frameworks capable of operating effectively in dynamic wireless settings (Conti et al., 2018).

In response to these challenges, recent research emphasizes the adoption of intelligent and automated forensic techniques, particularly those leveraging artificial intelligence and data analytics. Such approaches have the potential to improve detection accuracy, enable real-time monitoring, and support proactive cybersecurity decision-making. Therefore, this study focuses on analysing existing wireless network forensic techniques, identifying their limitations, and providing a foundation for the development of more effective and intelligent solutions.

- *Problem Statement*

The rapid proliferation of wireless communication technologies including Wi-Fi, mobile networks, and Internet of Things (IoT) devices has transformed modern digital ecosystems by enabling seamless connectivity and real-time data exchange across diverse sectors. However, this increased reliance on wireless networks has also introduced significant cybersecurity vulnerabilities due to the open and dynamic nature of wireless communication channels. As cyber threats continue to grow in complexity and frequency, wireless networks have become prime targets for attacks such as eavesdropping, spoofing, denial of service (DoS), and advanced persistent threats (APTs). Consequently, wireless network forensics has emerged as a vital discipline for investigating cyber incidents, reconstructing attack scenarios, and supporting cybersecurity decision-making processes.

Despite the availability of various wireless network forensic techniques and tools, their effectiveness in addressing contemporary cybersecurity challenges remains limited. Traditional forensic approaches primarily rely on packet capture, log analysis, and signature-based intrusion detection systems, which are often designed for static and structured network environments. These methods are largely reactive, focusing on post-incident investigation rather than real-time detection and prevention. As a result, they are unable to provide timely insights required for proactive cybersecurity decision-making in fast-evolving wireless environments (Conti et al., 2018).

One of the major challenges facing existing wireless network forensic techniques is their inability to handle the volume, velocity, and variety of network traffic data generated in modern wireless systems. With the exponential growth of connected devices and high-speed communication, forensic tools struggle to process large datasets efficiently, leading to delayed analysis and potential loss of critical evidence. This limitation significantly undermines the accuracy and completeness of forensic investigations, thereby affecting the quality of decisions made by cybersecurity professionals (Khan et al., 2020).

Furthermore, many existing techniques lack intelligent automation and advanced analytical capabilities. The reliance on manual analysis and predefined signatures limits their ability to detect novel or unknown attack patterns, such as zero-day exploits and polymorphic malware. This creates a critical gap in the detection of sophisticated cyber threats, which often evade traditional security mechanisms. In addition, the absence of adaptive learning mechanisms restricts the ability of forensic systems to evolve alongside emerging threat landscapes (Sommer & Paxson, 2019).

Another significant limitation is the poor integration of forensic outputs into cybersecurity decision making frameworks. While existing tools can generate large amounts of network data and logs, they often fail to translate this information into actionable intelligence. Security analysts are therefore burdened with interpreting complex and fragmented data, which increases the likelihood of human error and delays in response. This disconnect between forensic analysis and decision-making processes reduces the overall effectiveness of cybersecurity operations.

Wireless environments also present unique challenges that further complicate forensic investigations. These include data volatility, encryption, mobility of devices, and heterogeneous communication protocols, all of which hinder evidence acquisition, preservation, and analysis. Additionally, the lack of standardized methodologies and frameworks for wireless network forensics creates inconsistencies in investigative processes and outcomes, making it difficult to ensure reliability and reproducibility in forensic practices (Behl & Behl, 2018).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1852

Given these challenges, there is a clear need to critically analyse existing wireless network forensic techniques to identify their limitations in supporting effective cybersecurity decision making. Addressing these gaps is essential for the development of more advanced, intelligent, and scalable forensic solutions. In particular, the integration of intelligent traffic analysis, machine learning, and real-time monitoring mechanisms holds significant potential for enhancing the capability of forensic systems to detect anomalies, predict threats, and provide actionable insights.

Therefore, the study seeks to examine the shortcomings of current wireless network forensic techniques and establish a foundation for the development of an intelligent traffic analysis framework. Such a framework is expected to improve the efficiency, accuracy, and timeliness of forensic investigations while enabling proactive and evidence-based cybersecurity decision-making. Ultimately, this research aims to contribute to strengthening the resilience and security of wireless network infrastructures in the face of evolving cyber threats.

➢ *Research Purpose*

The study aims to evaluate existing wireless network forensic techniques and determine how effectively they support cybersecurity decision-making. It focuses on identifying the key limitations of these techniques such as their reactive nature, lack of integration, and limited real-time analytical capabilities that hinder the delivery of timely, accurate, and actionable security insights. Ultimately, the study seeks to highlight the need for more intelligent and proactive forensic approaches to improve decision-making in wireless network security.

➢ *Research Gap*

(WNFT) and Cybersecurity Decision-Making, despite significant advancements in wireless network forensics, a critical analysis of existing techniques reveals several unresolved gaps that limit their effectiveness in supporting timely, accurate, and actionable cybersecurity decision-making.

- *Lack of Comprehensive and Unified Forensic Frameworks*

Existing wireless forensic techniques are often fragmented and domain-specific (e.g., Wi-Fi, IoT, MANETs), with no universally accepted framework that integrates all layers of wireless environments. Current models fail to harmonize physical-layer, network-layer, and device-level evidence into a single analytical process. Many frameworks do not cover the full forensic lifecycle (collection → preservation → analysis → reporting), leading to inconsistencies in investigations.

- *Ineffective Handling of Dynamic and Distributed Wireless Environments*

Wireless networks (e.g., IoT, VANETs, MANETs) are inherently dynamic, decentralized, and mobile, which existing forensic techniques struggle to manage. Rapid topology changes and node mobility make evidence collection and correlation difficult. Evidence is often distributed across multiple devices and network points, reducing visibility during investigations.

- *Challenges with Ephemeral and Volatile Evidence*

Wireless forensic evidence is often short-lived and transient, especially at the physical and MAC layers. Critical data such as radio signals and session metadata are not persistently stored, making post-incident reconstruction difficult. Traditional forensic approaches rely on static logs, which are insufficient in wireless contexts.

- *Limited Support for Attribution and Attack Reconstruction*

Existing techniques provide limited capability in accurately attributing attacks to specific users or devices. Technologies like MAC address randomization and strong encryption (e.g., WPA3) obscure attacker identity. There is inadequate correlation between multi-source evidence for timeline reconstruction and causality analysis.

- *Insufficient Integration of Artificial Intelligence and Automation*

Although AI/ML has been introduced, its integration into wireless forensics is still nascent and inconsistent. Existing techniques rely heavily on manual analysis and rule-based systems, which are slow and error-prone. AI-based approaches face issues such as domain shift, training data scarcity, and interpretability challenges.

- *Weak Forensic Readiness and Proactive Capabilities*

Most current approaches are reactive, focusing on post-incident analysis rather than preparedness. Limited implementation of forensic readiness (built-in evidence collection mechanisms). Systems are not designed to support real-time decision-making during attacks.

- *Lack of Standardization and Legal Admissibility Support*

Wireless forensic practices lack standardized procedures and tools, affecting reliability and legal acceptance. Difficulty in maintaining chain of custody and ensuring evidence integrity across distributed systems. No widely accepted standards for wireless forensic evidence handling.

- *Scalability and Big Data Challenges*

Modern wireless networks generate massive volumes of heterogeneous data, overwhelming existing forensic tools. Difficulty in processing high-velocity, high-volume network traffic data in real time. Limited support for big data analytics in forensic investigations.

- *Poor Alignment with Cybersecurity Decision-Making Needs*

Most forensic techniques are designed for investigation, not for decision support. Outputs are often technical and not actionable for security managers. Lack of integration with security operations centres (SOCs) and decision-support systems.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1852

- *In Conclusion, the Core Research Gap*

The central research gap can be synthesized as: Existing wireless network forensic techniques are fragmented, reactive, and limited in handling dynamic, large scale, and heterogeneous environments, with inadequate support for real time evidence capture, intelligent analysis, and actionable cybersecurity decision-making.

➢ *Existing Wireless Network Forensic Techniques*

Wireless network forensics involves the identification, collection, preservation, analysis, and presentation of digital evidence from wireless communications such as Wi-Fi, Bluetooth, cellular, and IoT networks. Existing techniques can be broadly categorized based on how and where evidence is captured and analysed.

- *Packet Capture and Traffic Analysis Techniques*

These are the most widely used techniques in wireless forensics. Tools such as Wireshark, tcpdump, and Aircrack-ng capture wireless packets in real time. Analysis focuses on: Packet headers (MAC addresses, IPs), Traffic patterns, Protocol behaviour.

✓ Strengths: Provides detailed, low-level network insights, Useful for detecting attacks like sniffing, spoofing, and DoS
✓ Limitations: Ineffective with encrypted traffic (e.g., WPA2/WPA3), Generates large volumes of data requiring expert interpretation

- *Log-Based Forensic Techniques.*

These rely on logs generated by network devices. Sources include: Wireless Access Points (APs), Routers and firewalls, Authentication servers (e.g., RADIUS).

✓ Strengths: Easier to store and analyse compared to raw packets, Useful for reconstructing events and user activities
✓ Limitations: Logs may be incomplete, tampered with, or unavailable, Limited granularity compared to packet-level analysis

- *Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS)*

These systems monitor wireless networks for suspicious activity. Detect: Rogue access points, Unauthorized devices, Anomalous traffic patterns.

✓ Strengths: Real-time monitoring and alerting, Automated detection of known attack signatures
✓ Limitations: High false positive rates, Limited forensic depth (focuses more on detection than investigation)

- *Physical Layer and Radio Frequency (RF) Analysis*

Focuses on analysing wireless signals at the physical layer. Techniques include: Spectrum analysis, Signal fingerprinting, RF triangulation.

✓ Strengths: Can detect hidden or rogue devices, Helps in geolocation of attackers
✓ Limitations: Requires specialized hardware, Complex and difficult to interpret

- *Device-Centric Forensic Techniques*

These focus on extracting evidence directly from devices involved in wireless communication. Examples: Smartphones, Laptops, IoT devices.

✓ Strengths: Provides user-level evidence (files, logs, credentials), Useful for attribution
✓ Limitations: Requires physical access, Privacy and legal constraints

- *Network Flow Analysis (NetFlow/IPFIX)*

Analyses summarized traffic flows rather than full packets. Captures metadata such as: Source/destination IP, Ports, Duration and volume.

✓ Strengths: Scalable for large networks, Useful for identifying anomalies and traffic trends
✓ Limitations: Lacks payload detail, Limited usefulness for deep forensic investigation

- *Time-Based and Correlation Analysis Techniques*

These reconstruct attack timelines by correlating data from multiple sources. Combines: Logs, Packet captures, Alerts.

✓ Strengths: Helps in understanding attack sequences, Improves situational awareness
✓ Limitations: Requires synchronized timestamps, Complex and computationally intensive

- *Signature-Based and Rule-Based Analysis*

These rely on predefined attack signatures and rules. Common in IDS/IPS systems, Detect known threats such as: De-authentication attacks, Replay attacks.

✓ Strengths: Fast and efficient for known threats, Easy to implement
✓ Limitations: Cannot detect new or unknown attacks (zero-day), Requires constant updates

- *Machine Learning and AI-Based Techniques (Emerging)*

Modern approaches use AI to enhance wireless forensic analysis. Techniques include: Anomaly detection, Classification models, Behavioural analysis.

✓ Strengths: Can detect unknown and evolving threats, Supports automation and scalability
✓ Limitations: Requires large training datasets, Challenges with explainability and trust

- *Summary*

Existing wireless network forensic techniques can be grouped into: Data acquisition methods that is to say packet capture, logs, RF analysis, Detection mechanisms for example IDS/IPS, signature-based systems, Analysis approaches that is flow analysis, correlation, AI models, Evidence sources that is network devices and endpoints.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1852

➢ *Limitations of Existing Wireless Network Forensic Techniques in Supporting Effective Cybersecurity Decision-Making*

While current wireless network forensic techniques provide valuable investigative capabilities, they exhibit critical limitations that hinder their ability to support timely, accurate, and actionable cybersecurity decision-making.

- *Limited Real-Time Decision Support*

Most techniques are reactive, focusing on post-incident analysis rather than live response. Packet capture and log analysis are typically reviewed after an attack has occurred, Delays in analysis reduce the ability to mitigate threats in real time.

- *Fragmentation and Lack of Integration*

Existing techniques operate in isolation: Packet analysis, log analysis, RF analysis, and device forensics are not well integrated. No unified platform for correlating multi-source evidence.

- *Difficulty Handling Encrypted Traffic*

Modern wireless networks use strong encryption (e.g., WPA2, WPA3): Payload data is often inaccessible to forensic tools, Limits visibility into malicious activities.

- *High Data Volume and Complexity*

Wireless environments generate massive and continuous data streams: Packet captures produce large datasets, Manual analysis is time-consuming and error-prone.

- *Inadequate Support for Dynamic and Heterogeneous Environments*

Wireless networks are highly dynamic: Devices frequently join/leave networks, Includes diverse technologies (Wi-Fi, IoT, mobile, ad hoc networks).

- *Weak Correlation and Contextual Analysis*

Most tools analyse data in isolation: Limited ability to correlate events across time and sources, Poor reconstruction of attack timelines.

- *Limited Automation and Intelligence*

Many forensic processes are still manual or rule-based: Dependence on expert knowledge, Slow detection and response cycles.

- *Poor Attribution Capabilities*

Identifying the true source of an attack is challenging: Techniques like MAC spoofing and anonymization obscure identities, Weak linkage between network activity and users.

- *Volatile and Ephemeral Nature of Wireless Evidence*

Wireless evidence is often short-lived: Temporary sessions and signal data may not be stored, Loss of critical forensic artifacts.

- *Lack of Standardization and Forensic Readiness*

There is no universal standard for wireless forensics: Inconsistent procedures across tools and organizations, Limited built-in forensic readiness in systems.

- *High False Positives and Detection Limitations*

Detection systems (e.g., IDS/IPS): Often generate false alarms, Struggle with unknown (zero-day) attacks.

- *Poor Alignment with Decision-Making Needs*

Most forensic outputs are technical rather than strategic: Raw logs and packet data are not easily interpretable, Lack of actionable insights or risk prioritization.

➢ *The Key Limitation*

Overall, the major limitation can be summarized as: Existing wireless network forensic techniques are reactive, fragmented, and insufficiently intelligent, limiting their ability to deliver timely, integrated, and actionable insights required for effective cybersecurity decision-making.

II. THEORETICAL REVIEW

A theoretical review provides the foundational lenses through which wireless network forensic techniques and their limitations can be understood, particularly in relation to effective cybersecurity decision-making. This study is grounded in several complementary theories that explain how data is collected, processed, interpreted, and transformed into actionable security decisions.

➢ *Digital Forensics Theory*

Digital forensics theory underpins the systematic process of evidence handling, including identification, acquisition, preservation, analysis, and presentation. It emphasizes forensic integrity, chain of custody, and repeatability, Common models (e.g., forensic lifecycle models) guide investigations in structured phases.

- Relevance to Wireless Forensics: Provides the foundation for applying forensic techniques such as packet capture and log analysis, ensures that collected wireless evidence is credible and admissible.
- Limitation in Context: Traditional digital forensics models are largely static and post-incident, making them less suitable for dynamic wireless environments and real-time decision-making.

➢ *Network Forensics Theory*

Network forensics theory focuses on monitoring, capturing, storing, and analysing network traffic to investigate security incidents. Emphasizes traffic analysis, intrusion detection, and event reconstruction, Supports identification of attack patterns and anomalous behaviour.

- Relevance: Forms the basis for techniques like packet sniffing, flow analysis, and IDS/IPS systems, Enables understanding of how attacks occur within wireless networks.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1852

- Limitation: Primarily designed for wired and stable networks, limiting effectiveness in wireless, mobile, and distributed environments, Often produces large volumes of data without contextual intelligence.

➢ *Cybersecurity Decision Theory*

Cybersecurity decision theory explains how security professionals make decisions under uncertainty, risk, and time constraints. Focuses on risk assessment, threat prioritization, and response strategies, Emphasizes the need for timely and actionable intelligence.

- Relevance: Highlights the importance of transforming forensic outputs into decision-support information, aligns with the goal of improving incident response and mitigation.
- Limitation: Existing forensic techniques do not adequately support this theory because they: Provide raw technical data rather than actionable insights, Lack real-time decision support mechanisms.

➢ *Situational Awareness Theory*

Situational Awareness (SA) theory (Endsley's model) involves three levels: Perception of environmental elements, Comprehension of their meaning, Projection of future states.

- Relevance: Wireless forensic tools contribute to perception by collecting data, Analysis contributes to comprehension of threats.
- Limitation: Existing techniques rarely support the projection stage, which is critical for proactive cybersecurity decision-making, Lack of integration leads to incomplete situational awareness.

➢ *Complexity Theory*

Wireless networks are complex adaptive systems characterized by: Dynamic topology, Heterogeneous devices, Nonlinear interactions.

- Relevance: Explains why wireless forensic investigations are inherently difficult, Justifies the need for adaptive and scalable forensic techniques.
- Limitation: Existing techniques are often rigid and linear, failing to adapt to the complexity of modern wireless environments.

➢ *Machine Learning and Artificial Intelligence Theory*

Machine learning theory focuses on pattern recognition, prediction, and automation using data-driven models. Includes supervised, unsupervised, and reinforcement learning, Enables anomaly detection and behavioural analysis.

- Relevance: Provides the foundation for intelligent traffic analysis, Enhances automation and scalability in forensic processes
- Limitation: Current implementations face challenges such as: Lack of quality training data, Model interpretability issues, Limited integration into forensic workflows

➢ *Routine Activity Theory (Criminology Perspective)*

This theory states that crime occurs when three elements converge: A motivated offender, A suitable target, Absence of capable guardianship.

- Relevance: Helps explain cyber-attacks in wireless environments, Supports the need for monitoring and forensic readiness.
- Limitation: Existing forensic techniques focus more on post-attack analysis rather than preventing the convergence of these elements.

Synthesis of Theoretical Insights, across these theories, a common theme emerges: Wireless forensic techniques are effective in data collection and analysis (perception and comprehension); However, they are weak in prediction, integration, and decision support (projection and action)

➢ *Theoretical Gap*

Existing theoretical foundations reveal that current wireless network forensic techniques are not fully aligned with dynamic, intelligent, and decision-centric cybersecurity models, particularly in supporting real-time situational awareness, predictive analysis, and actionable decision-making.

III. CONCLUSION OF CONCEPTUAL FRAMEWORK

The reviewed theories collectively demonstrate that while existing wireless forensic techniques are grounded in strong foundational principles, they remain limited in their ability to support proactive, intelligent, and real-time cybersecurity decision-making. Therefore, it underscores the need for an integrated, AI-driven forensic framework that aligns with modern theoretical expectations and operational demands.

➢ *Conceptual Framework:*

Analysis of Wireless Network Forensic Techniques and Their Limitations in Cybersecurity Decision-Making. The framework explains how existing wireless network forensic techniques influence the quality of cybersecurity decision-making, and how their inherent limitations create a need for enhanced (intelligent) analytical approaches.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1852

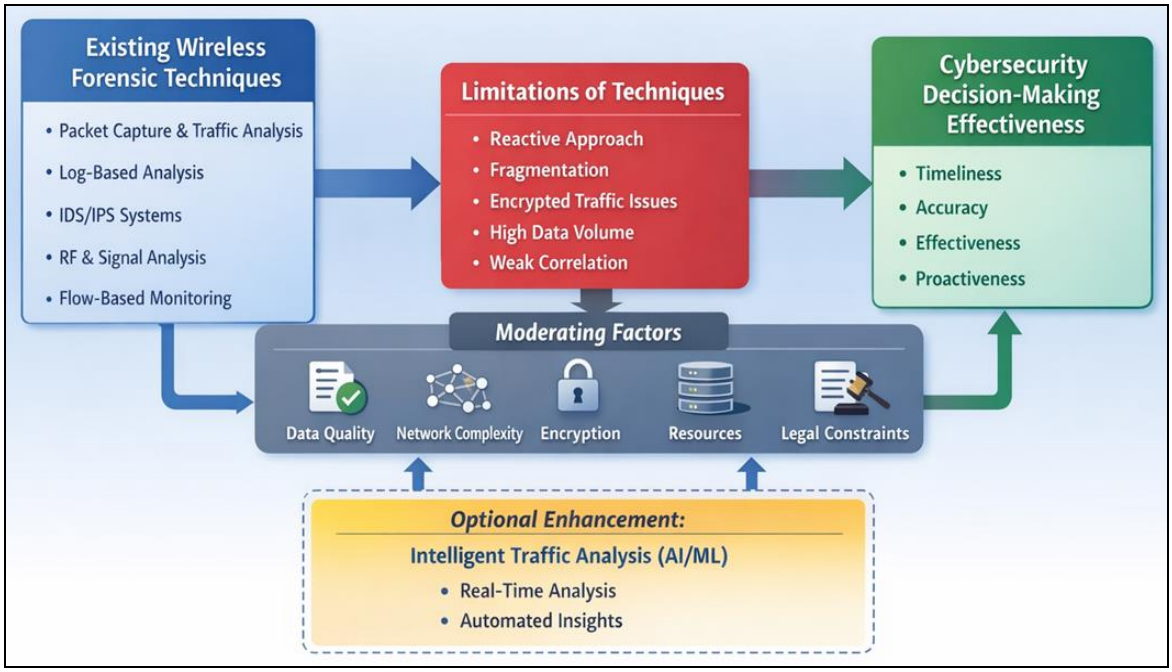

Fig 1 Conceptual Framework

➢ *Application of Conceptual Framework to the Study*

This framework supports the research by: Identifying why current techniques are insufficient, Justifying the need for intelligent, integrated forensic approaches, providing a structure for analysing relationships between variables

➢ *Conclusion*

The analysis of existing wireless network forensic techniques ranging from packet capture and log analysis to intrusion detection systems, RF analysis, and emerging AI-based approaches demonstrates that they play a critical role in investigating and understanding security incidents within wireless environments. These techniques provide valuable capabilities for evidence collection, traffic monitoring, anomaly detection, and incident reconstruction.

However, despite these contributions, they exhibit significant limitations that constrain their effectiveness in supporting efficient cybersecurity decision-making. Most notably, existing approaches are largely reactive, relying on post-incident analysis rather than enabling real-time or proactive responses. Their fragmented nature and lack of integration across multiple data sources result in incomplete situational awareness, while challenges such as encrypted traffic, high data volumes, and dynamic network environments further complicate analysis and delay decision processes.

Additionally, limitations in automation, intelligent correlation, and attribution reduce the accuracy and reliability of forensic outcomes. The volatile nature of wireless evidence, combined with insufficient forensic readiness and lack of standardization, further undermines the credibility and timeliness of findings. Importantly, many current techniques fail to translate technical outputs into actionable intelligence, making it difficult for security professionals and decision-makers to respond effectively to threats.

The existing wireless network forensic techniques provide a foundational basis for cybersecurity investigations, they are not fully aligned with the demands of modern, fast-evolving wireless ecosystems. There is a clear need for integrated, intelligent, and proactive forensic frameworks that leverage advanced analytics and real-time processing to enhance decision-making. Addressing these limitations is essential for improving the accuracy, speed, and effectiveness of cybersecurity responses in wireless network environments.

REFERENCES

[1]. Behl, A., & Behl, K. (2018). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
[2]. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*, 544–546.
[3]. Khan, M. A., Salah, K., & Jayaraman, R. (2020). Blockchain-based secure data sharing for Internet of Things. *IEEE Access, 8*, 109-118.
[4]. Sommer, R., & Paxson, V. (2019). Outside the closed world: On using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*.
[5]. Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response (SP 800-86)*. NIST.
[6]. Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A Survey of Intrusion Detection in Internet of Things. *Journal of Network and Computer Applications*, 84, 25–37.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1852

[7]. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-Physical Systems Security—A Survey. *IEEE Internet of Things Journal*, 4(6), 1802–1831.
[8]. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A Survey of Network Anomaly Detection Techniques. *Journal of Network and Computer Applications*, 60, 19–31.
[9]. Adepu, S., & Mathur, A. (2016). *Distributed Attack Detection in a Water Treatment Plant*. [Cyber-Physical Systems Security]
[10]. Stallings, W. (2018). *Network Security Essentials: Applications and Standards*. [Pearson]
[11]. Feng, C., et al. (2017). *Multi-layered Intrusion Detection for ICS Using ML*. [IEEE Transactions on Industrial Informatics]
[12]. Genge, B., & Haller, P. (2016). *A cyber-physical attack detection method for industrial control systems*. [Computers & Electrical Engineering]
[13]. Morris, T., Gao, W. (2013). *Industrial control system traffic data sets for intrusion detection research*. [Critical Infrastructure Protection]