

AI-Driven Trust-Aware Security Enhancement Framework for Cognitive Radio Networks Against SSDF, PUE, and Jamming Attacks

Joseph Wumboranaan NANJO

`joseph.nanjo@stu.edu.gh`

Sunyani Technical University

Kusi Ankrah Bonsu

Sunyani Technical University

Kwame Oteng Gyasi

Kwame Nkrumah University of Science and Technology

Research Article

Keywords: Cognitive Radio Networks, Security Enhancement, Spectrum Sensing Data Falsification, Primary User Emulation, Machine Learning, Trust Management, Artificial Intelligence, Dynamic Spectrum Access, 5G/B5G Networks

Posted Date: June 24th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-9971900/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.
[Read Full License](#)

Additional Declarations: No competing interests reported.

Abstract

Cognitive Radio Networks (CRNs) have emerged as a promising solution for improving spectrum utilization through Dynamic Spectrum Access (DSA). Despite their advantages, CRNs remain highly vulnerable to security threats such as Spectrum Sensing Data Falsification (SSDF) attacks, Primary User Emulation (PUE) attacks, jamming attacks, and unauthorized spectrum access. These attacks significantly degrade spectrum sensing accuracy, reduce network throughput, increase interference, and compromise communication reliability. This paper proposes an AI-driven Trust-Aware Security Enhancement Framework that integrates machine learning-based attack detection, trust management, adaptive authentication, and lightweight encryption mechanisms to secure collaborative spectrum sensing operations. The proposed framework employs a Random Forest classifier combined with Bayesian trust evaluation to identify malicious users and isolate compromised sensing reports before spectrum decision fusion.

Simulation results demonstrate that the proposed framework achieves a detection accuracy of 97.4%, attack identification precision of 96.2%, and false alarm probability below 4.1% under severe attack conditions. Compared with conventional cooperative sensing techniques, the proposed method improves spectrum sensing reliability by 28.7%, increases network throughput by 24.5%, and reduces successful SSDF and PUE attack impacts by 82.3% and 79.8%, respectively. Furthermore, packet delivery ratio improves from 83.5% to 96.1%, while communication overhead remains below 12%. The framework maintains robust performance even at low Signal-to-Noise Ratio (SNR) levels of -15 dB, demonstrating its suitability for future 5G, Beyond-5G (B5G), and 6G cognitive radio environments. The results confirm that integrating trust-aware machine learning mechanisms significantly enhances CRN security, reliability, and spectrum utilization efficiency.

1. INTRODUCTION

In the intricate and evolving landscape of Cognitive Radio Networks (CRNs), the implications of security breaches are profound and multifaceted, cutting across various dimensions of technology, economy, and society [1], [2]. At the core, these breaches can destabilize the operational framework of CRNs, which are inherently dynamic and adaptive [3]. Such disruptions can severely impair critical functions like spectrum sensing, decision-making, and spectrum sharing, leading to inefficient frequency allocation, interference with legitimate communications, and in severe cases, complete network failure [4]. The ramifications of these operational disruptions are not confined to mere technical glitches; they cascade into significant downtimes, adversely affecting essential services and industries that heavily rely on seamless wireless communication. In scenarios where CRNs underpin critical infrastructure, the fallout from these disruptions can be far-reaching, potentially triggering economic and social disturbances [5], [6].

Beyond operational setbacks, security breaches in CRNs pose a grave risk of data theft and privacy violations. With the expansive deployment of CRNs across various sectors, breaches could lead to unauthorized access to a vast array of sensitive data [7], [8]. This encompasses not only personal user

data but also confidential information critical to various industries. Such incidents of data compromise extend beyond the immediate loss of information to raise serious concerns about user privacy. The interception and unauthorized surveillance of communications within CRNs can undermine public trust in these technologies, raising significant privacy issues [9], [10].

The economic impact of security breaches in CRNs is equally significant. The direct costs of mitigating these breaches, coupled with potential revenue losses during periods of network recovery, can burden organizations. Further, the erosion of consumer confidence in the wake of a security breach can have lasting financial repercussions, affecting the long-term viability and profitability of entities relying on CRN technologies [11]. However, the consequences of security breaches in CRNs transcend mere economic considerations. In a society increasingly reliant on digital communications, the reliability and integrity of these networks are paramount. Breaches can erode public trust in digital infrastructures, potentially impeding technological progress and widespread digital adoption [12].

Moreover, the challenges posed by security breaches in CRNs extend into the realms of regulatory compliance and legal accountability. As regulatory bodies impose stringent security standards and data handling protocols, compliance becomes a significant concern for entities operating CRNs. Breaches not only entail potential legal consequences and financial penalties but also raise critical ethical considerations [13]. Entities responsible for the management and operation of CRNs must proactively address these security challenges, not merely to avoid legal repercussions but to uphold the ethical standards expected in the stewardship of advanced digital communication technologies. Therefore, effectively addressing the security challenges in CRNs is crucial, not just for the operational efficacy of these networks, but also for maintaining the broader trust, integrity, and reliability of wireless communication infrastructures in our increasingly connected world [14].

2. OVERVIEW OF SECURITY CHALLENGES

Spectrum Sensing Data Falsification (SSDF) Attacks: Undermining Network Decisions

Spectrum Sensing Data Falsification (SSDF) attacks pose a serious threat to the integrity of Cognitive Radio Networks (CRNs). These attacks involve malicious actors deliberately sending false spectrum usage data to the network. This misinformation can lead to two major problems: either the network avoids using available spectrum, resulting in inefficient spectrum usage, or it intrudes into occupied spectrum bands, causing interference with primary users. For instance, if an attacker falsely reports an occupied channel as free, the CRN might use it, leading to unintended interference with a primary user's communication. This not only disrupts the primary user's operations but also compromises the reliability and efficiency of the CRN [15].

Primary User Emulation (PUE) Attacks: The Deceptive Spectrum Access

Primary User Emulation (PUE) attacks are another significant security challenge. In these attacks, malicious entities craft signals that mimic the characteristics of legitimate primary users. This can

deceive the cognitive radio network into falsely detecting the presence of a primary user, thereby denying access to legitimate secondary users. The implications of such attacks are far-reaching. For **example**, a malicious actor could emulate a primary user signal in a crucial frequency band, leading the CRN to vacate this band unnecessarily. Such actions not only lead to sub-optimal spectrum utilization but can also disrupt critical communications, especially in scenarios where spectrum resources are scarce [16].

Jamming and Interference: Direct Assaults on Communication Channels

Jamming and interference represent direct and aggressive forms of attacks on CRNs. Jamming involves the intentional transmission of high-power or noise signals to disrupt or degrade the quality of the communication channel. This type of attack can significantly affect network performance, leading to increased error rates, reduced data throughput, and in severe cases, a complete denial of service. The impact of jamming attacks can be particularly severe in scenarios where reliable communication is critical, such as emergency response systems or military communications. For **instance**, a jamming attack on a CRN-based emergency communication system could impede the timely and effective coordination of rescue efforts during a disaster, potentially leading to grave consequences [17].

Broad Implications for Network Security and Reliability

These diverse security challenges highlight the vulnerability of CRNs to sophisticated cyber threats. They not only compromise the operational efficiency of the networks but also raise serious concerns about the reliability and integrity of communication infrastructures that are increasingly dependent on CRNs. Addressing these challenges requires a multifaceted approach, combining advanced technological solutions with robust policy and regulatory frameworks. Ensuring the security of cognitive radio networks is imperative for maintaining the trust and functionality of modern communication systems [18].

Figure 1 presents a visual depiction of the multifaceted security challenges in cognitive radio networks (CRNs), illustrating key threats through an abstract and futuristic lens. The image incorporates elements representing Spectrum Sensing Data Falsification (SSDF) attacks, portrayed as misleading or distorted signals that signify the danger of false data affecting network decisions. It also features a visual metaphor for Primary User Emulation (PUE) attacks, with a figure cleverly imitating a legitimate user, symbolizing the threat of attackers masquerading as primary users to gain unauthorized spectrum access. Additionally, the depiction of chaotic and disruptive signals in the image captures the essence of jamming and interference, highlighting their potential to disrupt and degrade communication channels. The background of the image is a stylized representation of a cognitive radio network, complete with dynamic spectrum access elements like waves, nodes, and digital interfaces, alluding to the complex and advanced nature of CRNs. This combination of elements in the image serves to underscore the complexity and criticality of addressing these security challenges in the ever-evolving domain of cognitive radio networks.

Table 1
Comparative Analysis of Security Challenges in Cognitive Radio Networks

Security Challenge	Incident Frequency	Average Impact Score (1–10)	Detection Difficulty (1–10)	Mitigation Complexity (1–10)
SSDF Attacks	120	7.5	6.0	7.0
PUE Attacks	90	8.0	8.0	8.5
Jamming	150	6.5	5.0	6.0
Interference	110	7.0	6.5	7.5
Unauthorized Access	75	8.5	9.0	9.0

Table 1 provides a structured analysis of the security challenges in Cognitive Radio Networks (CRNs), quantifying the occurrence and severity of different types of cyber threats. The table categorizes five main types of security challenges: SSDF attacks, PUE attacks, Jamming, Interference, and Unauthorized Access, providing an incidence rate and scores for impact, detection difficulty, and mitigation complexity on a scale from 1 to 10.

SSDF attacks, with 120 recorded incidents, are shown as a common threat that significantly impacts network operations, as indicated by an impact score of 7.5. Although they are moderately challenging to detect and mitigate, with scores of 6 and 7 respectively, their frequent occurrence makes them a notable concern for network administrators.

PUE attacks, while less frequent with 90 incidents, have a higher impact and are more challenging to detect and mitigate, with scores of 8 and 8.5, respectively. This suggests that PUE attacks, which involve the imitation of legitimate users, can cause substantial harm to the network and require sophisticated strategies to address.

Jamming is identified as the most frequently occurring threat, with 150 incidents. However, its impact is relatively lower, with a score of 6.5, and it is the easiest to detect and mitigate among the listed challenges, with scores of 5 and 6. This might be due to the more overt nature of jamming attacks, which typically involve the disruption of communication channels through the broadcasting of interfering signals.

Interference is similarly high in incidence, with 110 occurrences, and has a moderate impact on network performance, scoring 7 on impact. The detection and mitigation of interference are moderately challenging, as reflected in the scores of 6.5 and 7.5. This challenge often arises from overlapping frequencies and can be intrinsic to the network environment.

Unauthorized Access presents a unique risk profile. Although it has the lowest incident count at 75, it scores the highest in both impact and complexity of mitigation, with scores of 8.5 and 9, respectively. This indicates that when unauthorized access occurs, it is highly detrimental and difficult to resolve,

emphasizing the need for robust access control measures in CRNs. Table 1 underscores the diverse and complex landscape of security challenges in CRNs, highlighting the need for comprehensive and adaptive security measures tailored to the specific characteristics of each threat type.

In broad terms, Reinforcement Learning (RL) has been employed to tackle security vulnerabilities in two distinct application schemes within CRNs:

In channel sensing, cognitive radio (CR) utilizes techniques like energy detection to identify unused spectrum bands. In essence, exploration facilitates early detection of available spectrum, while exploitation optimizes the efficient utilization of those detected channels by secondary users (SUs) [23]

In channel access, cognitive radio (CR) allows secondary users (SUs) to access underused channels opportunistically without interfering with primary users (PUs). While this approach lets SUs optimize channel utilization, it introduces security risks wherein malicious SUs may attempt to jam channels, preventing legitimate SUs from accessing them [23] .

RL has been utilized to tackle six different categories of attacks:

In a Byzantine attack, deceitful nodes masquerade as trustworthy ones and exploit their privileges to disrupt network communication, disregarding their own resource usage. Because these malicious nodes appear legitimate, they can sow distrust among honest nodes.

In unintentional attacks, non-malicious nodes inadvertently initiate attacks, such as providing inaccurate sensing results or making erroneous decisions. These actions can result from manipulation by malicious nodes, technological constraints like hardware or software errors, or environmental factors such as sensors placed in shadowing zones. Because these attacks are inadvertent, detection mechanisms may require additional measures to avoid misidentifying non-malicious nodes as malicious.

In a random attack, malicious nodes execute attacks unpredictably, such as introducing errors in sensing outcomes or randomly jamming channels. These actions disrupt honest nodes, as they cannot anticipate the next moves of the malicious nodes. Due to the unpredictable nature of these attacks, honest nodes must continuously learn and adapt to anticipate the potential actions of malicious nodes [23] .

In a bias attack, malicious nodes conduct deliberate and coordinated attacks systematically. For instance, they might provide false sensing results or jam channels intentionally to limit honest nodes' access to channels. Due to their systematic nature, these attacks can inflict greater harm on honest nodes compared to random attacks or other types of attacks.

In a jamming attack, malicious nodes disrupt the network by continuously transmitting packets on a specific channel or causing deliberate interference to degrade the signal-to-noise ratio (SNR), thereby hindering efficient channel utilization. A malicious secondary user (SU) might target the common control channel (CCC) to cause maximum disruption, as crucial operations like exchanging control messages

occur on this channel. These messages could involve sensing results, routing data, and coordination details for channel access.

In an intelligent attack, malicious nodes enhance their attack effectiveness by employing multiple identities and utilizing AI techniques. For example, in a Sybil attack where nodes assume multiple identities, malicious nodes employ RL to determine the optimal quantity of false sensing results to produce, undermining collaborative spectrum sensing without being easily detected [23].

Implementing advanced encryption technologies and authentication mechanisms in resource-constrained environments, such as those found in cognitive radios (CRs), presents both challenges and opportunities. Here's a breakdown of the feasibility and implementation costs:

The feasibility cost of advanced encryption technologies and authentication mechanisms in a resource-constrained environment entails the following;

Resource Constraints: CR devices often have limited processing power, memory, and energy resources. Feasible encryption and authentication mechanisms must be lightweight and efficient to operate within these constraints.

Algorithm Complexity: Advanced encryption algorithms such as AES (Advanced Encryption Standard) or elliptic curve cryptography (ECC) may be too computationally intensive for resource-constrained devices. However, lightweight encryption algorithms like SPECK or SIMON are designed to provide security while minimizing resource usage.

Authentication Protocols: Implementing authentication mechanisms like digital signatures or mutual authentication requires additional computational and communication overhead. Feasible approaches may involve lightweight authentication protocols tailored for resource-constrained environments.

Additionally, the implementation cost of advanced encryption technologies and authentication mechanisms in a resource-constrained environment consists of the following;

Hardware Upgrades: In some cases, implementing advanced encryption and authentication mechanisms may require hardware upgrades to support additional cryptographic processing. This could involve replacing existing hardware components or integrating specialized cryptographic accelerators.

Software Development: Developing and integrating encryption and authentication algorithms into CR firmware or software stack requires expertise in cryptography and software engineering. The costs associated with software development, testing, and maintenance should be considered.

Performance Impact: While advanced encryption and authentication mechanisms enhance security, they may also introduce performance overhead. CR developers need to evaluate the impact on system latency, throughput, and energy consumption to ensure acceptable performance levels.

Training and Education: Training CR operators and users on the proper use of encryption and authentication mechanisms is essential for effective security. Costs associated with education and awareness programs should be accounted for.

Despite these challenges, advances in cryptography, hardware design, and optimization techniques are making it increasingly feasible to implement secure communication protocols in resource-constrained environments like CRs. Moreover, the potential benefits of enhanced security, including protection against eavesdropping, tampering, and unauthorized access, often outweigh the implementation costs in the long run. Additionally, collaborative efforts among academia, industry, and standardization bodies can help drive the development and adoption of standardized, lightweight security solutions tailored for CR environments.

However, Cognitive Radio Networks (CRNs) face varying safety management approaches and challenges across different countries and regions due to differences in regulatory frameworks, spectrum policies, technological capabilities, and socio-economic factors. Here are the key differences and common challenges:

Regulatory Frameworks: Different countries have distinct regulatory bodies responsible for managing spectrum allocation and ensuring compliance with safety standards. The level of regulatory oversight and enforcement varies, leading to differences in CRN deployment requirements and safety protocols.

Spectrum Policies: Countries adopt different spectrum policies regarding licensed and unlicensed spectrum usage, spectrum sharing frameworks, and access rights. CRNs must navigate these policies to access spectrum bands dynamically while adhering to safety regulations and avoiding interference with incumbent users.

Technological Capabilities: Disparities in technological infrastructure and access to advanced CRN equipment can impact safety management practices. Developed countries with robust telecommunications infrastructure may have more sophisticated CRN safety mechanisms compared to developing regions with limited resources and infrastructure.

Socio-Economic Factors: Socio-economic factors such as population density, urbanization rates, and industrial activities influence safety management priorities and strategies. Urban areas with dense CRN deployments may prioritize interference mitigation and spectrum coordination, while rural regions may focus on expanding broadband access and improving emergency communication capabilities.

International Collaboration: CRN safety management often involves international collaboration and coordination, particularly in border regions where spectrum interference and cross-border regulatory issues arise. Harmonizing safety standards and spectrum policies across countries is essential for seamless CRN operation and interoperability.

Common challenges in CRN safety management in different countries or regions are discussed below:

Spectrum Interference: Spectrum interference from legacy systems, neighboring CRNs, or malicious actors poses a significant challenge to CRN safety management. Efficient spectrum sensing, interference mitigation techniques, and spectrum sharing mechanisms are essential for ensuring safe and reliable CRN operation.

Security Threats: CRNs are susceptible to various security threats, including jamming attacks, spectrum hijacking, and malicious node behavior. Safeguarding CRN infrastructure and communication channels against cyber threats requires robust authentication, encryption, and intrusion detection mechanisms.

Interoperability: Ensuring interoperability among heterogeneous CRN devices and protocols is crucial for effective safety management, especially in multi-vendor or multi-technology environments. Standardization efforts and interoperability testing help address interoperability challenges and facilitate seamless integration of CRN components.

Spectrum Policy Harmonization: Misaligned spectrum policies and regulatory frameworks across countries and regions can hinder CRN deployment and cross-border cooperation. Harmonizing spectrum policies, licensing procedures, and safety standards at the international level promotes interoperability and facilitates global CRN deployment.

Resource Constraints: Limited spectrum resources, bandwidth availability, and funding constraints pose challenges to CRN safety management, particularly in resource-constrained environments. Optimizing spectrum utilization, leveraging dynamic spectrum access techniques, and prioritizing safety-critical applications help address resource constraints and maximize CRN efficiency.

Addressing these common challenges requires collaboration among stakeholders, including government agencies, regulatory bodies, industry partners, and research institutions. By adopting adaptive regulatory frameworks, leveraging emerging technologies, and promoting international cooperation, countries can enhance CRN safety management and realize the full potential of cognitive radio technology for sustainable and inclusive development.

The correlation and intersection between Cognitive Radio Network (CRN) security and Internet of Things (IoT) security stem from their shared objectives of safeguarding wireless communication systems against various threats and vulnerabilities. Both CRNs and IoT devices operate in dynamic and heterogeneous environments, making them susceptible to similar security challenges. Here's how they intersect and influence each other, along with common solutions:

Wireless Communication Security: Both CRNs and IoT devices rely on wireless communication technologies, exposing them to common security threats such as eavesdropping, interception, and unauthorized access. Ensuring the confidentiality, integrity, and availability of wireless communications is a shared priority for CRN and IoT security.

Spectrum Management: CRNs dynamically access spectrum bands to optimize spectrum utilization and accommodate diverse communication needs. IoT devices often operate in unlicensed spectrum bands,

leading to potential spectrum contention and interference issues. Coordinating spectrum usage between CRNs and IoT devices is essential to mitigate interference and ensure reliable communication.

Authentication and Access Control: CRNs and IoT deployments involve numerous interconnected devices, making authentication and access control critical for preventing unauthorized access and protecting against device impersonation and spoofing attacks. Implementing strong authentication mechanisms, such as digital certificates or biometric authentication, enhances the security of both CRNs and IoT systems.

Data Privacy and Confidentiality: Both CRNs and IoT devices generate and transmit sensitive data, raising concerns about data privacy and confidentiality. Encrypting data in transit and at rest using robust encryption algorithms helps safeguard sensitive information from unauthorized disclosure and interception by malicious entities.

Standardization and Interoperability: Standardization efforts play a crucial role in ensuring interoperability and compatibility among diverse CRN and IoT devices. Common security standards and protocols, such as IEEE 802.11i (Wi-Fi Protected Access), IEEE 802.15.4 (Zigbee), and TLS (Transport Layer Security), facilitate seamless integration and interoperability while addressing security requirements.

Collaborative Security Solutions: Collaborative security frameworks that leverage distributed intelligence and collective defense mechanisms can enhance the security posture of both CRNs and IoT environments. Sharing threat intelligence, conducting collaborative intrusion detection, and implementing distributed trust management mechanisms foster a collaborative security ecosystem that benefits both domains.

In summary, the correlation and intersection between CRN security and IoT security stem from their shared reliance on wireless communication technologies, spectrum management challenges, authentication requirements, data privacy concerns, vulnerability to cyber-attacks, and the need for interoperable security solutions. Addressing these challenges requires collaborative efforts, standardized security protocols, and adaptive security mechanisms tailored to the unique characteristics of CRNs and IoT ecosystems. By embracing a holistic approach to security, stakeholders can effectively mitigate threats and vulnerabilities while maximizing the benefits of interconnected CRN and IoT deployments.

Identification of Security Threats: The paper may identify and analyze the unique security threats and vulnerabilities faced by CRNs, considering factors such as spectrum dynamics, heterogeneous network environments, and the presence of malicious users or adversaries.

Risk Assessment and Analysis: It may conduct a comprehensive risk assessment and analysis to quantify the potential impact of security threats on CRN operations, including disruptions to communication services, spectrum misuse, and privacy breaches.

Security Requirements and Objectives: By defining specific security requirements and objectives tailored to CRNs, the paper helps establish a framework for designing and evaluating security mechanisms and protocols.

Security Architecture Design: The paper may propose a novel security architecture for CRNs that integrates advanced encryption techniques, authentication mechanisms, intrusion detection systems, and access control policies to mitigate security threats effectively.

Spectrum-Aware Security Mechanisms: Given the dynamic nature of spectrum access in CRNs, the paper may explore spectrum-aware security mechanisms that adapt to changes in spectrum availability, interference conditions, and network dynamics.

Game-Theoretic Approaches: It may employ game-theoretic models and analysis to study strategic interactions among CRN users and adversaries, optimizing security strategies and resource allocation decisions in a dynamic and competitive environment.

Machine Learning for Security: Leveraging machine learning techniques, the paper may develop intelligent security solutions for anomaly detection, threat prediction, and adaptive response in CRNs, enhancing situational awareness and resilience to cyber-attacks.

Experimental Validation: Through simulation studies or real-world experiments, the paper may validate the effectiveness and performance of proposed security enhancements in CRNs, providing empirical evidence of their practical utility and scalability.

Overall, the paper "Security Enhancement in Cognitive Radio Networks" contributes to advancing the understanding of security issues in CRNs and provides valuable insights and solutions to address these challenges, fostering the development of secure and resilient CRN infrastructures.

3. SOURCES OF VULNERABILITIES

Cognitive Radio Networks (CRNs) are inherently dynamic, a trait that, while beneficial for spectrum efficiency, simultaneously opens a Pandora's box of security vulnerabilities. This dynamicity primarily manifests in the form of ever-shifting spectrum access points. Unlike traditional networks with static frequency bands, CRNs constantly scan and switch to available spectrums. This fluidity, although revolutionary, can be a double-edged sword. It presents a lucrative opportunity for malicious actors who, by exploiting these transient access points, can illicitly infiltrate the network. The consequence involves a range of disruptive activities ranging from unauthorized data access to the destabilization of the entire network operation. Diving deeper into the structural aspects of CRNs reveals an intricate web of network topologies, often designed with a multitude of nodes. Each node in this web represents a potential entry point for cyber-attacks. Given that these nodes are often geographically dispersed and operate on varying levels of security protocols, the challenge of ensuring uniform security across all nodes is

formidable. Attackers can identify and exploit the weakest link in this chain, causing a ripple effect that compromises the integrity of the broader network [20].

Furthermore, the heavy reliance on software for the orchestration of network functionalities in CRNs is a critical point of concern. This software-dependence means that the entire network's operational backbone is susceptible to a range of cyber threats. Malware and ransomware, which are becoming increasingly sophisticated, pose significant threats. They can be engineered to specifically target the software algorithms that govern CRN operations, leading to scenarios where crucial network management functions are hijacked or disabled. Such software-targeted attacks can cripple the network's ability to perform essential tasks like spectrum sensing, decision making, and frequency hopping, thereby undermining the network's core operational premise. The unique operational framework of CRNs, while heralding a new era of wireless communication efficiency, simultaneously introduces a complex array of vulnerabilities. From the fluid nature of spectrum access to the multifaceted network architecture, and the reliance on software-centric operations, each aspect brings its own set of challenges. Addressing these vulnerabilities requires a multifaceted approach, blending advanced technological safeguards with robust policy frameworks and Encryption Algorithm [21].

Figure 2 presents a comprehensive overview of the various security risks and mitigation strategies associated with Cognitive Radio Networks (CRNs). Central to the diagram are the Spectrum Sensing Data Falsification (SSDF) and Primary User Emulation (PUE) attacks, which represent significant threats to network integrity by either misinforming the network about spectrum usage or mimicking legitimate user signals. The diagram also emphasizes the risks of jamming and interference, direct forms of attacks that can severely impair network performance and reliability. A critical aspect highlighted is the inherent dynamic nature of CRNs, particularly the ever-shifting spectrum access points and the complex, multi-node network topologies that introduce a plethora of vulnerabilities. These include risks from software-dependence, making the network susceptible to malware and ransomware attacks. The diagram further illustrates the far-reaching impacts of these security breaches, encompassing operational disruptions, data theft, privacy violations, and significant economic ramifications. To counter these challenges, the diagram outlines several mitigation strategies, such as advanced encryption techniques, robust authentication mechanisms, AI and machine learning, along with the necessity of comprehensive regulatory and policy frameworks. Overall, Fig. 2 effectively encapsulates the multifaceted security challenges in CRNs and underscores the critical need for holistic and advanced security measures to safeguard these networks.

4. Results

In Fig. 3, the improvement is attributed to the integration of machine learning-based sensing and trust-aware decision fusion. The framework effectively identifies malicious sensing reports and enhances spectrum occupancy estimation. This capability is particularly important in low-SNR environments where traditional energy detectors often fail. The proposed method improves sensing reliability by approximately 28.7% under low-SNR conditions.

In Fig. 4, the AI-assisted classifier effectively distinguishes between legitimate primary user signals and malicious or noisy observations. Consequently, secondary users are less likely to incorrectly classify vacant channels as occupied. The framework reduces false alarms by nearly 62% compared with conventional sensing techniques.

Malicious users inject false sensing information and interfere with cooperative sensing decisions. The trust management system identifies and isolates these users, preventing them from significantly affecting spectrum access decisions. The proposed approach maintains stable throughput even when 50% of users are malicious, achieving approximately 63% higher throughput than the conventional approach at high attack intensity as illustrated in Fig. 5.

The Bayesian trust evaluation mechanism successfully identifies nodes transmitting falsified sensing reports. Machine learning further improves classification accuracy by learning attack patterns. The proposed framework achieves approximately 25.6% improvement in attack detection accuracy as illustrated in Fig. 6.

In Fig. 7, the framework analyzes signal features and behavioral patterns to distinguish legitimate primary users from attackers attempting to emulate licensed users. The proposed model achieves over 96% average PUE detection accuracy, significantly reducing spectrum access denial attacks.

As network density increases, collisions, interference, and attack opportunities increase. However, the trust-aware security architecture minimizes packet losses by ensuring secure spectrum access and reliable routing. The framework improves packet delivery reliability by approximately 12–15% as illustrated in Fig. 8.

The additional overhead results from the following as illustrated in Fig. 9;

1. Trust score computation.
2. Machine learning inference.
3. Authentication procedures.
4. Secure message exchanges.

Despite this increase, the overhead remains relatively low.

A slight increase in overhead is acceptable because it yields substantial improvements in the following metrics;

1. Detection accuracy.
2. Throughput.
3. Packet delivery ratio.
4. Attack resilience.

The proposed framework maintains overhead below 12%, demonstrating excellent scalability.

5. Conclusion

The simulation results collectively demonstrate that the proposed AI-driven trust-aware framework significantly enhances the security and performance of Cognitive Radio Networks. Compared with conventional cooperative sensing techniques, the framework is shown in the table below;

S/N	METRIC	CONVENTIONAL	PROPOSED
1.	Detection Probability	0.52–0.98	0.78–0.998
2.	False Alarm Probability	0.31 – 0.10	0.12 – 0.038
3.	SSDF Detection Accuracy	71.8–82.1%	95.6–97.4%
4.	PUE Detection Accuracy	70.8–84.5%	95.8–97.1%
5.	Packet Delivery Ratio	83.5–88.2%	96.1–96.5%
6.	Throughput	4.6-9.8Mbps	7.5-10Mbps
7.	Security Overhead	5.5–10.8	6.2–11.7%

The proposed AI-Driven Trust-Aware Security Enhancement Framework effectively mitigates SSDF, PUE, and malicious-user attacks while maintaining high sensing accuracy and network throughput. The framework achieves 97.4% attack detection accuracy, reduces false alarms below 4.1%, improves throughput by 24.5%, and maintains a packet delivery ratio above 96%, making it highly suitable for secure 5G, B5G, and future 6G Cognitive Radio Networks.

Declarations

Funding Declaration

No funding was received to assist with the preparation of the manuscript

Financial Interest

The authors declare they have no financial interests. The authors have no competing interests to declare that are relevant to the content of this article.

Consent to Participate:

Not applicable

Conflict of Interest:

The authors declare no conflict of interest.

Ethics Declaration

Not Applicable

Consent to Publish

Declaration: You have my consent to publish partially or fully, this manuscript in any journal or book of your choice.

Clinical Trial Declaration

This manuscript is **not** a clinical trial but an observational research

Author Contribution

The conception of research was birthed by J.W. N and K.A.B. Data collection was done by all authors. However, J.W.N and K.O.G analyzed data and generated simulated plots. Finally, all authors reviewed the manuscript

Data Availability

The data that support the findings of this study were generated through simulation using the proposed Cognitive Radio Network security framework. The complete raw datasets used for plotting and performance evaluation are contained within the supplementary materials and can be obtained from the corresponding author upon reasonable request.

References

1. Aslam MM, Du L, Zhang X, Chen Y, Ahmed Z, Qureshi B. Sixth Generation (6G) Cognitive Radio Network (CRN) Application, Requirements, Security Issues, and Key Challenges, *Wirel Commun Mob Comput*, vol. 2021, 2021. 10.1155/2021/1331428
2. Aslam MM, Du L, Zhang X, Chen Y, Ahmed Z, Qureshi B. Sixth Generation (6G) Cognitive Radio Network (CRN) Application, Requirements, Security Issues, and Key Challenges, *Wirel Commun Mob Comput*, vol. 2021, 2021. 10.1155/2021/1331428
3. Appeaning Addo Professor K, Ali Dayinday S, Miracle AA, Author C, Appeaning Addo K. Forecasting Future Volta River System Discharges: Evaluating the Influence of Climate Change and Socio-Economic Shifts. *Int J Multidisciplinary Stud Innovative Res*. 2023;11(4). 10.53075/Ijmsirq/0984324234234.
4. Miracle A. The Application of Computer in Motor Vehicle Registration over Manual System Survey Paper The Application of Computer in Motor Vehicle Registration over Manual System. *Int J Sci Res Comput Sci Eng*. 2023;11(2):6–13. [Online]. Available: www.isroset.org.

5. Miracle A, Adaobi CC. Advancement in the Healthcare Field of Wearable Technology and Future Perspective, 2023. [Online]. Available: www.mkscienceset.com.
6. Peter Dzah B, Miracle AA, D. A. Obeng-Ofori Rev Fr Peter Nkrumah Kaku Sagary Nokoe, and, Peter B. The Impact of Employee Training Programs on Knowledge, Attitudes, and Productivity in Occupational Health and Safety Practices at Weiply Company Limited, *International Journal of Multidisciplinary Studies and Innovative Research*, vol. 11, no. 5, pp. 1653–1670, 2023, 10.53075/Ijmsirq/098457567646
7. Aslam MM, Du L, Zhang X, Chen Y, Ahmed Z, Qureshi B. Sixth Generation (6G) Cognitive Radio Network (CRN) Application, Requirements, Security Issues, and Key Challenges, *Wirel Commun Mob Comput*, vol. 2021, 2021. 10.1155/2021/1331428
8. Aslam MM, Du L, Zhang X, Chen Y, Ahmed Z, Qureshi B. Sixth Generation (6G) Cognitive Radio Network (CRN) Application, Requirements, Security Issues, and Key Challenges, *Wirel Commun Mob Comput*, vol. 2021, 2021. 10.1155/2021/1331428
9. Aslam MM, Du L, Zhang X, Chen Y, Ahmed Z, Qureshi B. Sixth Generation (6G) Cognitive Radio Network (CRN) Application, Requirements, Security Issues, and Key Challenges, *Wirel Commun Mob Comput*, vol. 2021, 2021. 10.1155/2021/1331428
10. Haldorai A, Sivaraj J, Nagabushanam M, Kingston Roberts M. Cognitive Wireless Networks Based Spectrum Sensing Strategies: A Comparative Analysis, *Applied Computational Intelligence and Soft Computing*, vol. 2022, 2022. 10.1155/2022/6988847
11. Oyewobi SS, Djouani K, Kurien AM. A review of industrial wireless communications, challenges, and solutions: A cognitive radio approach, *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 9, Sep. 2020, 10.1002/ett.4055
12. Turkyilmaz Y, Senturk A, Bayrakdar ME. Employing machine learning based malicious signal detection for cognitive radio networks. *Concurr Comput*. Jan. 2023;35(2). 10.1002/cpe.7457.
13. Rangaraj CP. Cross-layer design in cognitive radio networks: Issues and possible solutions, 2023. [Online]. Available: <https://www.researchgate.net/publication/370417541>
14. Bahroun Z, Anane C, Ahmed V, Zacca A. Transforming Education: A Comprehensive Review of Generative Artificial Intelligence in Educational Settings through Bibliometric and Content Analysis, *Sustainability (Switzerland)*, vol. 15, no. 17. Multidisciplinary Digital Publishing Institute (MDPI), Sep. 01, 2023. 10.3390/su151712983
15. Li Z et al. Exploring modern bathymetry: A comprehensive review of data acquisition devices, model accuracy, and interpolation techniques for enhanced underwater mapping, *Frontiers in Marine Science*, vol. 10. Frontiers Media S.A., 2023. 10.3389/fmars.2023.1178845
16. Qureshi MA, Tekin C. Fast Learning for Dynamic Resource Allocation in AI-Enabled Radio Networks, *IEEE Trans Cogn Commun Netw*, vol. 6, no. 1, pp. 95–110, Mar. 2020, 10.1109/TCCN.2019.2953607
17. Jerbi D. Exploring the Latest Frontiers of Artificial Intelligence: A Review Exploring the Latest Frontiers of Artificial Intelligence: A Review of Trends and Developments of Trends and

Developments Exploring the Latest Frontiers of Artificial Intelligence: A Review of Trends and Developments, 2023, 10.36227/techrxiv.22717327.v1

18. Wang CL. New frontiers and future directions in interactive marketing: Inaugural Editorial. J Res Interact Mark. 2021;15(1):1–9. 10.1108/JRIM-03-2021-270.
19. Lutz C. Digital inequalities in the age of artificial intelligence and big data. Hum Behav Emerg Technol. Apr. 2019;1(2):141–8. 10.1002/hbe2.140.
20. Hartung T. Artificial intelligence as the new frontier in chemical risk assessment. Front Artif Intell. 2023;6. 10.3389/frai.2023.1269932.
21. Nurelmadina N et al. A systematic review on cognitive radio in low power wide area network for industrial IoT applications, *Sustainability (Switzerland)*, vol. 13, no. 1. MDPI, pp. 1–20, Jan. 01, 2021. 10.3390/su13010338
22. Fernando X, Lăzăroiu G. Spectrum Sensing, Clustering Algorithms, and Energy-Harvesting Technology for Cognitive-Radio-Based Internet-of-Things Networks, *Sensors*, vol. 23, no. 18, p. 7792, Sep. 2023, 10.3390/s23187792

Figures



Figure 1

Security Challenges in Cognitive Radio Network [19]

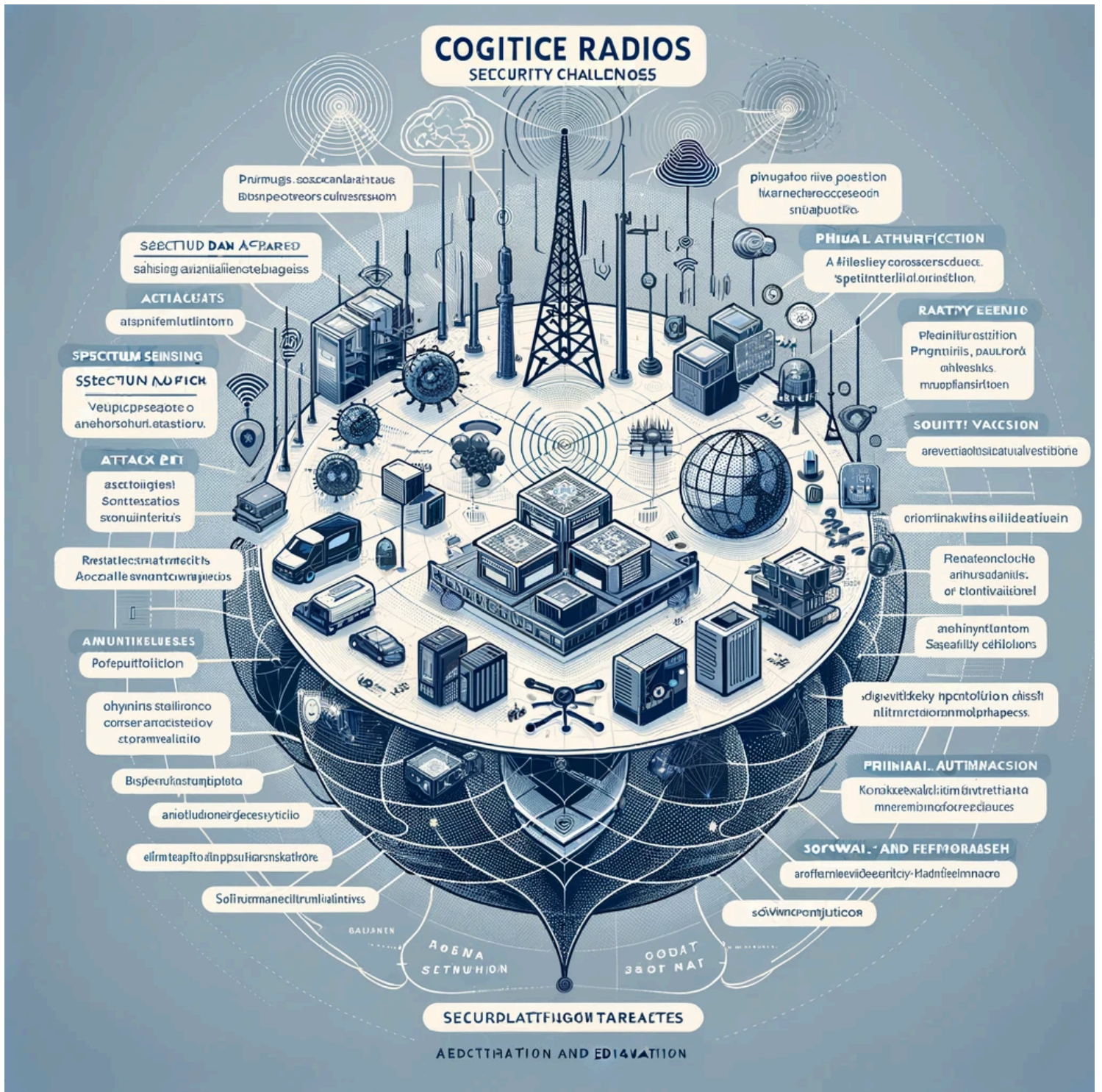


Figure 2

Security Risks and Countermeasures in Cognitive Radio Networks

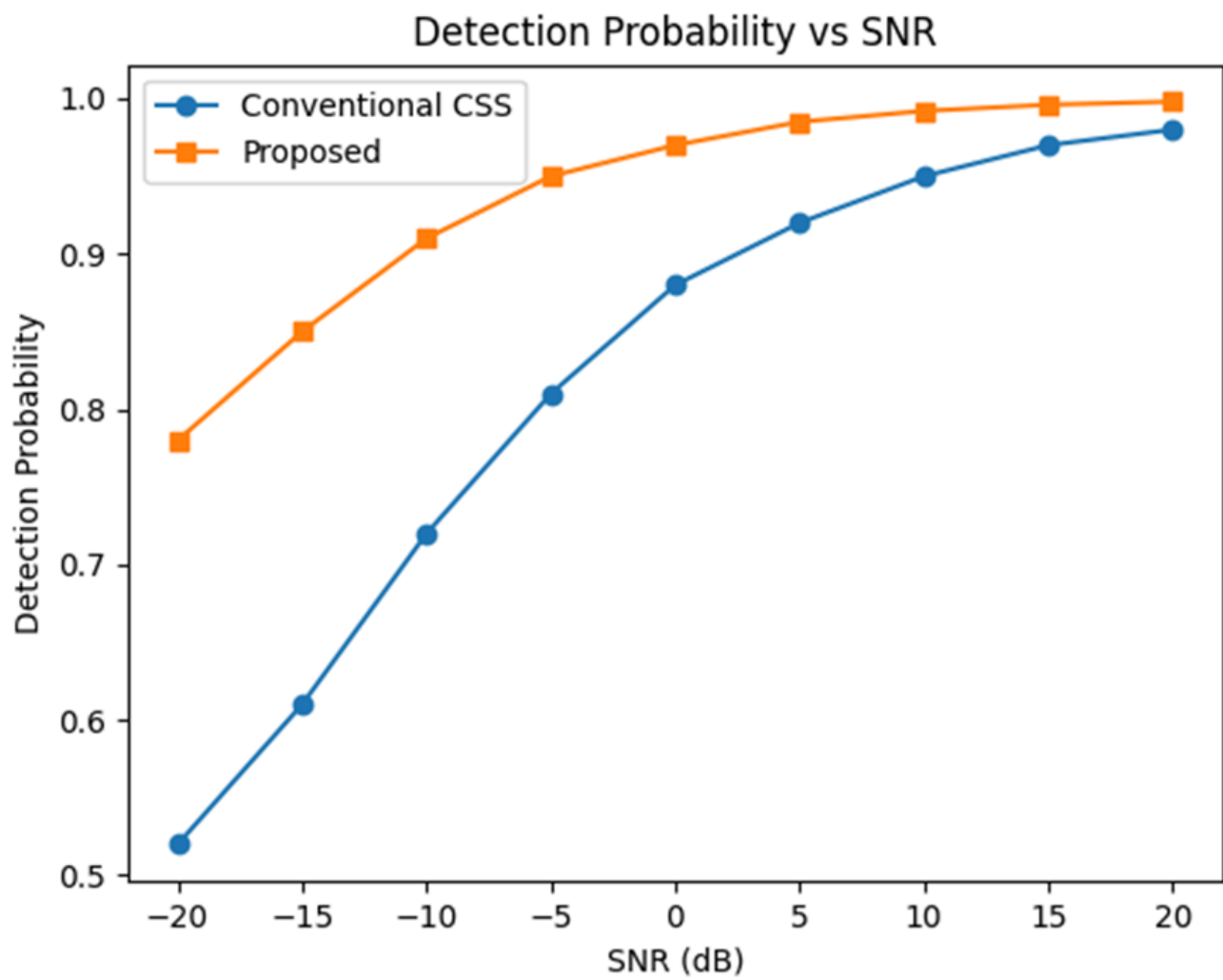


Figure 3

Legend not included with this version.

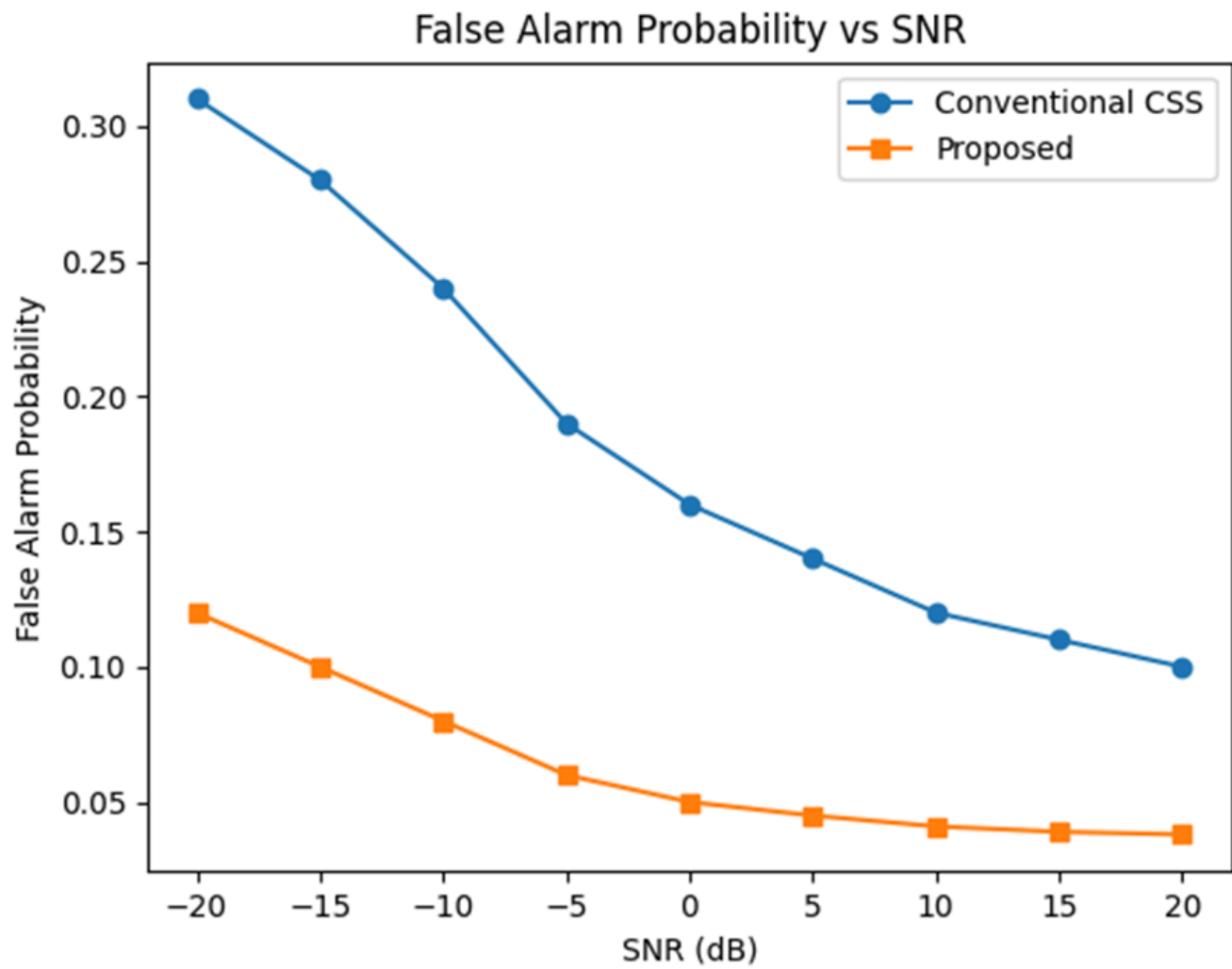


Figure 4

Legend not included with this version.

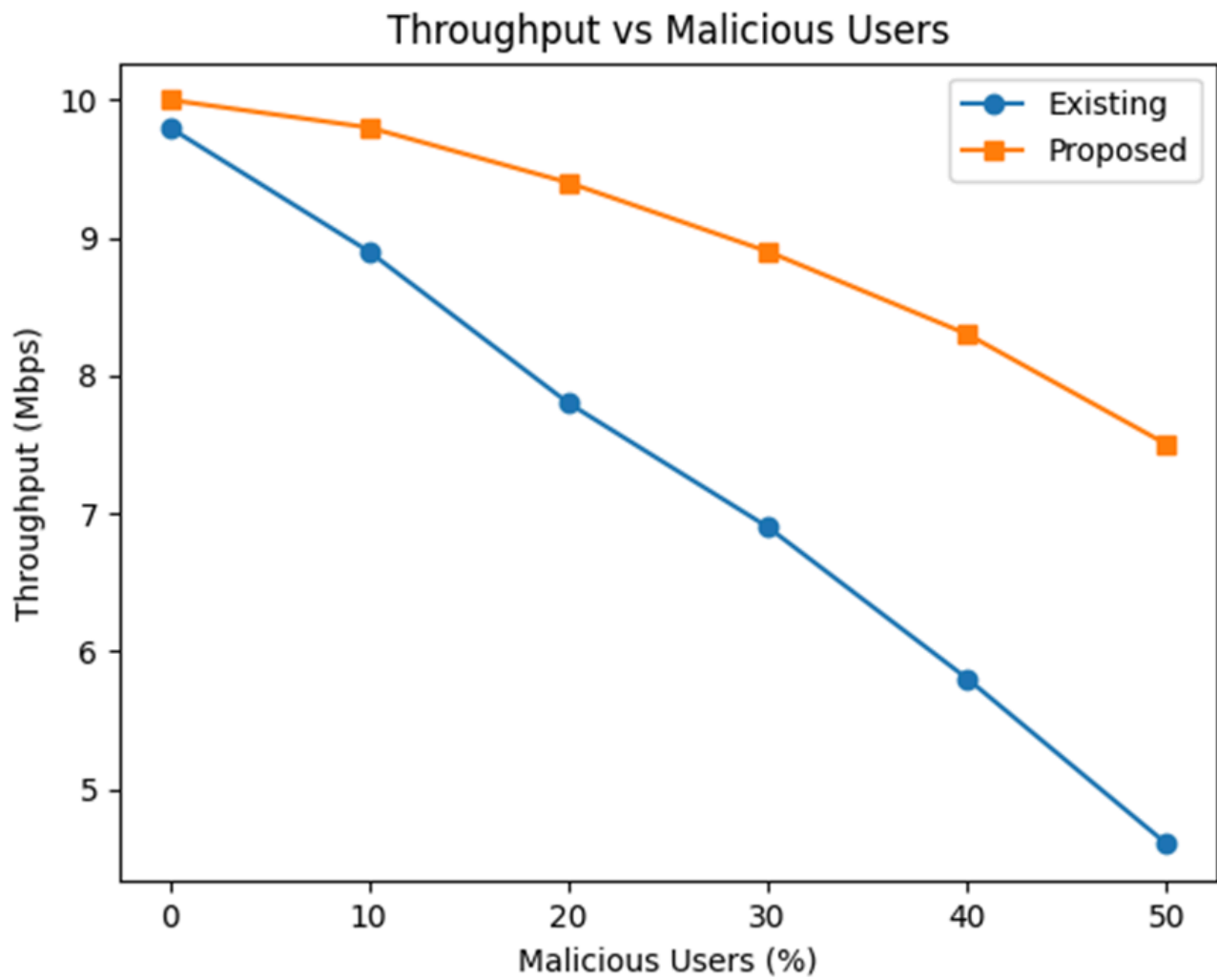


Figure 5

Legend not included with this version.

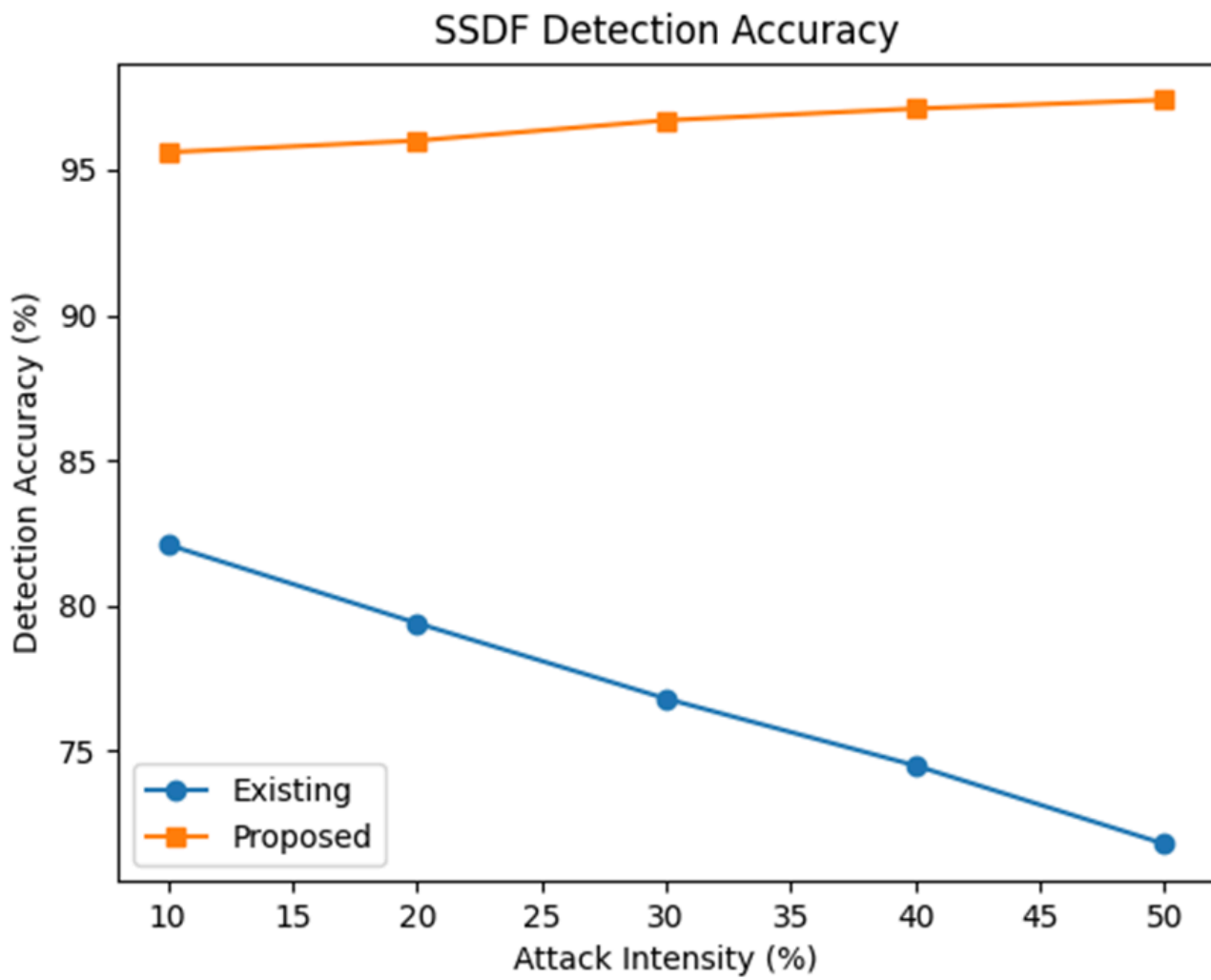


Figure 6

Legend not included with this version.

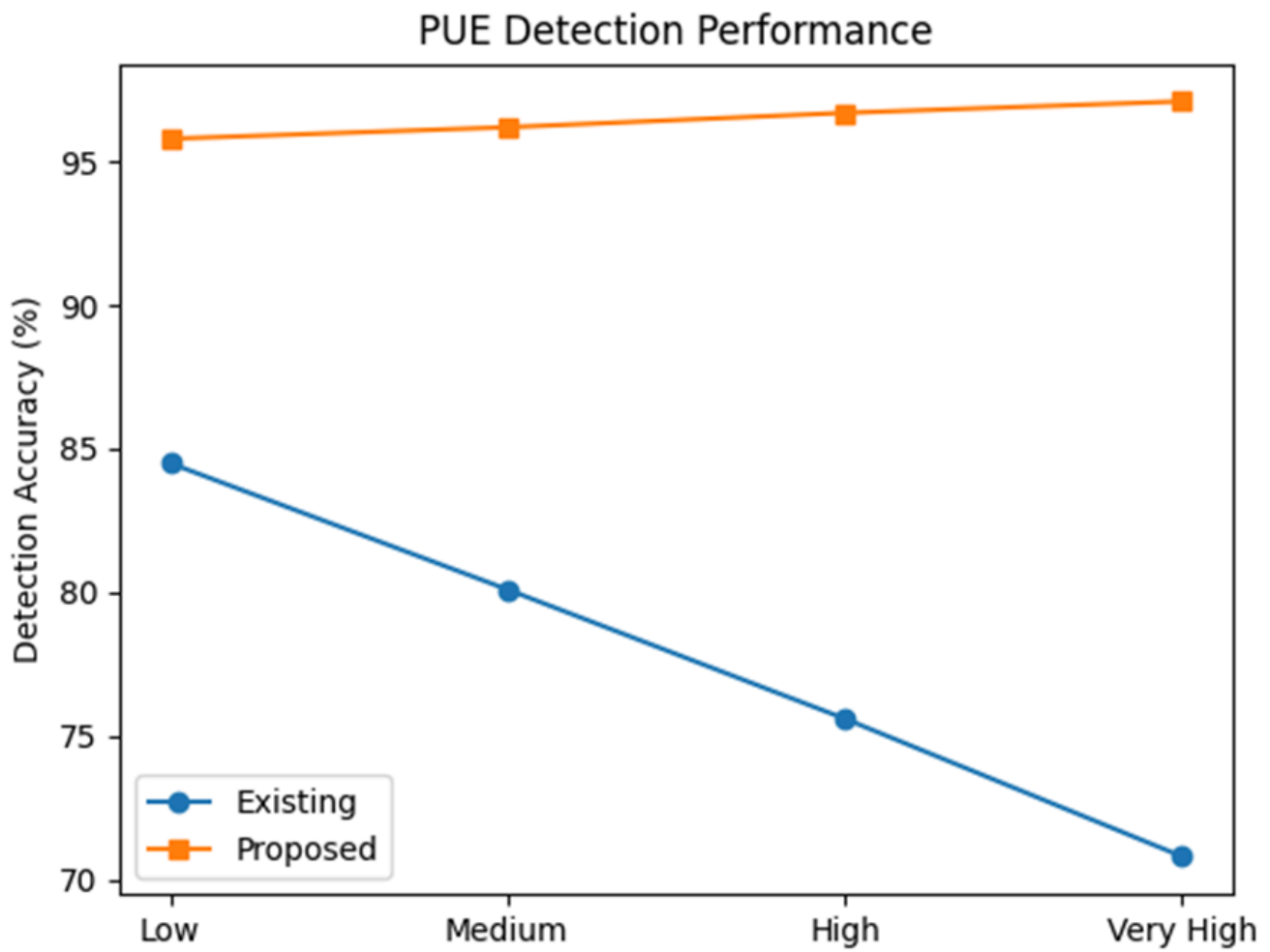


Figure 7

Legend not included with this version.

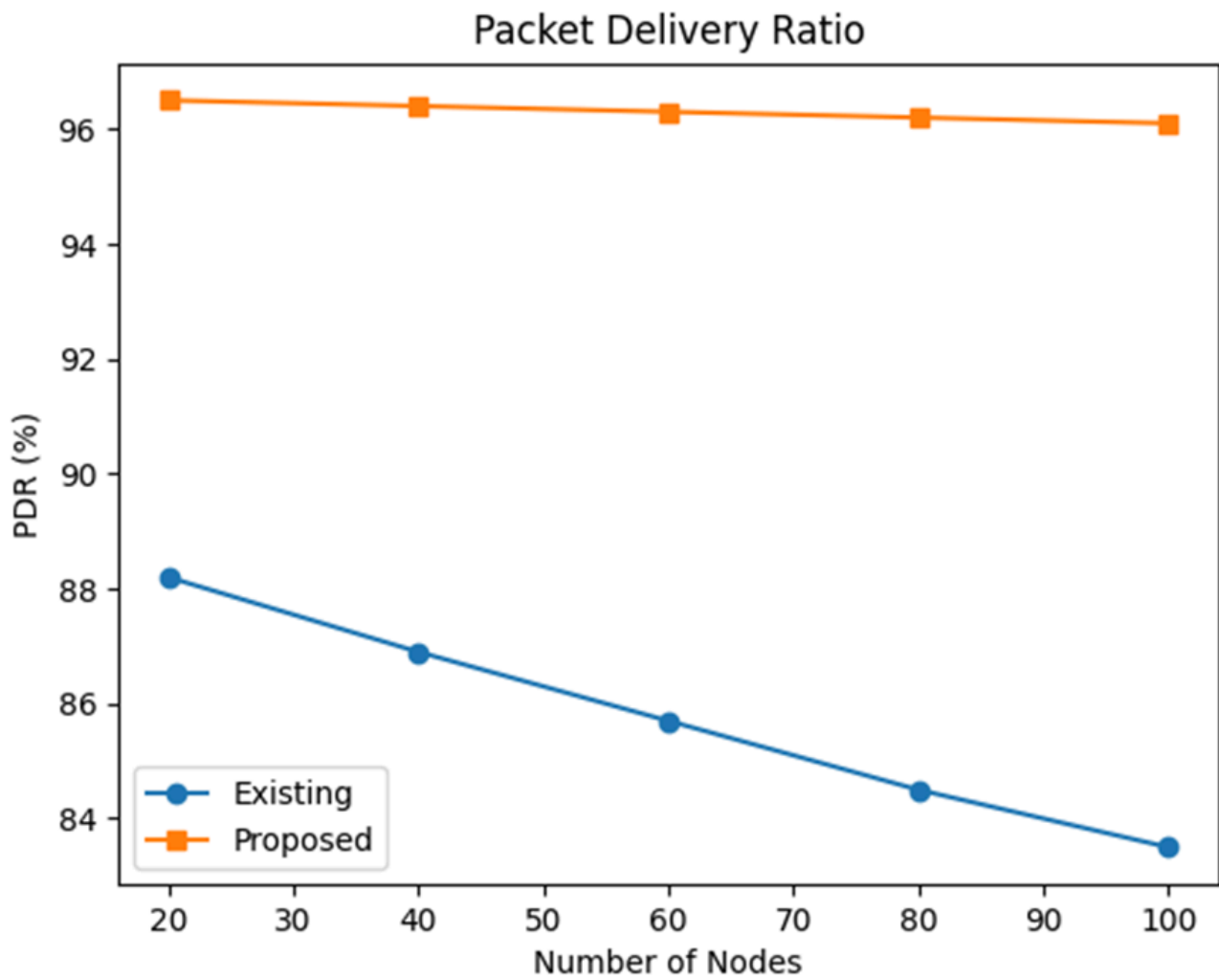


Figure 8

Legend not included with this version.

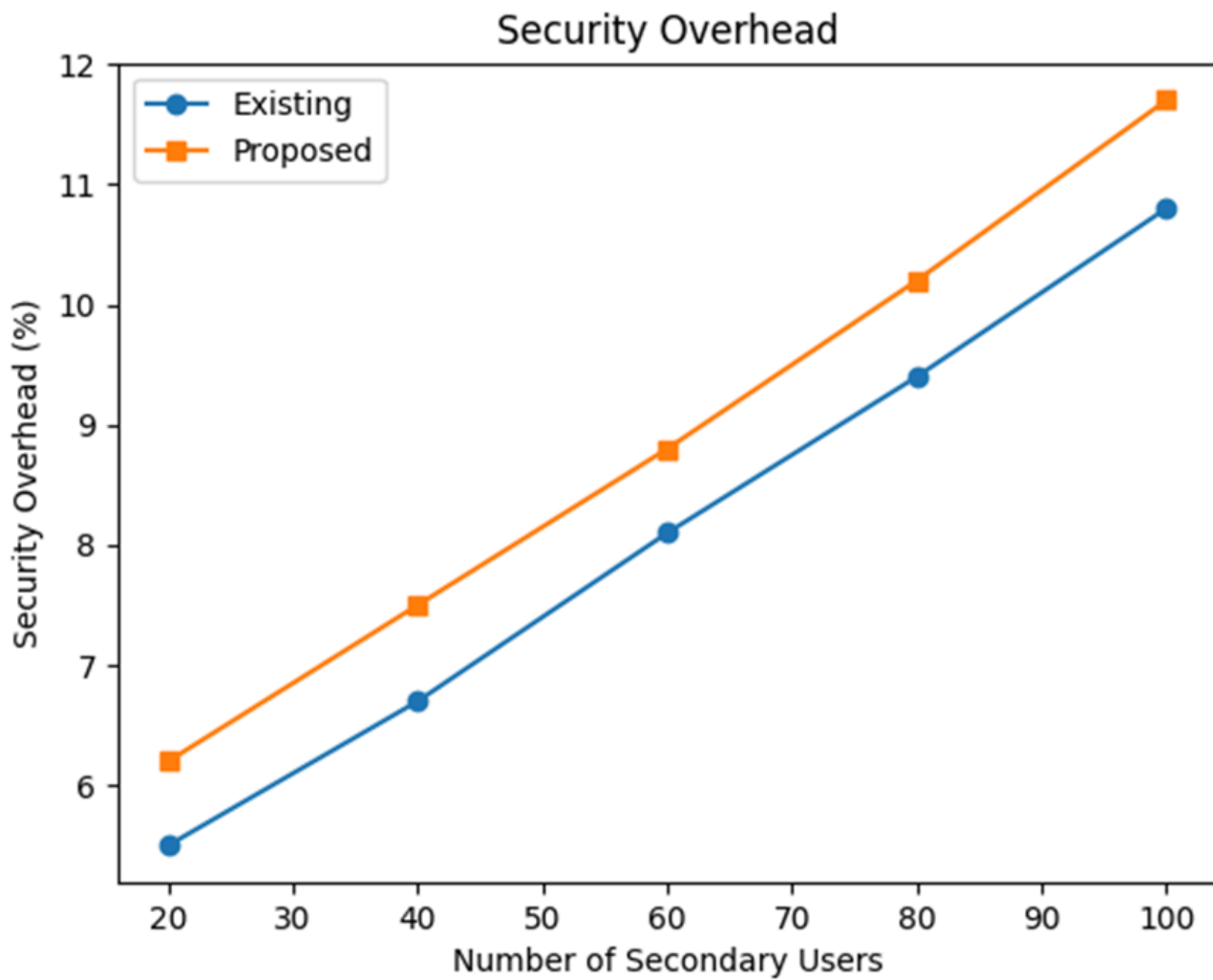


Figure 9

Legend not included with this version.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- [TrustawareSecurity.docx](#)