Open Journal of Robotics, Autonomous Decision-Making, and Human-Machine Interaction, pp. 1–9

Implementing Cross-Layer Security Mechanisms for Drone-Gathered Road Information and Vehicle Communication Links

Aiman Hakimi[1], Ali Batan[2]

1. *Universiti Teknologi Selatan, Department of Electrical Engineering, Jalan Meranti , Bandar Seri Alam, Masai, Johor, Malaysia.*
2. *Bolu Technical University, D100 Karayolu, Bolu, Turkey*

Abstract

Drones have become a transformative technology for gathering real-time road information, significantly enhancing the efficiency of vehicular communication networks. However, the integration of drones into these networks introduces critical security vulnerabilities, as communication links can be exploited by adversaries to compromise data integrity, confidentiality, and availability. Cross-layer security mechanisms, which span multiple layers of the communication protocol stack, offer a robust solution to these challenges. This paper investigates the implementation of cross-layer security mechanisms for drone-gathered road information and vehicle communication links, focusing on the integration of authentication, encryption, and intrusion detection systems across the physical, data link, and network layers. By leveraging these mechanisms, the framework can address threats such as eavesdropping, spoofing, and denial-of-service attacks. Simulation results demonstrate that the proposed approach significantly improves network resilience and data security while maintaining low latency and high throughput. Additionally, this work explores the trade-offs between security, system overhead, and communication performance. The findings highlight the feasibility and effectiveness of cross-layer designs in securing drone-assisted vehicular networks, setting the stage for future developments in secure and intelligent transportation systems.

Keywords: authentication, cross-layer security, drones, encryption, intrusion detection, vehicular networks, wireless communication

Introduction

The rapid adoption of unmanned aerial vehicles (UAVs), commonly referred to as drones, within intelligent transportation systems (ITS) has significantly transformed how road information is collected, processed, and disseminated. Equipped with advanced sensors and communication technologies, drones have enabled real-time monitoring of traffic flow, road conditions, accidents, and other critical parameters. These capabilities allow for enhanced situational awareness and informed decision-making, benefiting various stakeholders, including drivers, traffic management agencies, and emergency responders. For instance, drones can provide live feeds from accident sites, assist in managing traffic congestion through predictive analytics, and relay vital road condition updates to autonomous vehicles. This paradigm shift has positioned UAVs as indispensable tools in modern ITS ecosystems.

However, the incorporation of UAVs into vehicular communication systems is not without challenges. Chief among these are the cybersecurity risks inherent in drone-assisted vehicular networks. The communication links between drones and vehicles rely on wireless channels, which are susceptible to a wide array of cyber threats, including data interception, tampering, and denial-of-service (DoS) attacks. For example, an attacker could intercept traffic data transmitted by a drone and manipulate it to create false congestion scenarios, leading to inefficient routing decisions. Similarly, a DoS attack on the communication link could disrupt real-time data transmission, compromising the reliability of the ITS. These vulnerabilities underscore the need for robust security mechanisms tailored to the unique characteristics of drone-assisted vehicular networks.

Traditional security approaches in ITS often rely on single-layer solutions, which focus on specific protocol layers, such as the application, transport, or network layer. While effective against certain types of attacks, these approaches fall short in addressing the complex and dynamic threat landscape of drone-assisted vehicular networks. For instance, an attack that exploits vulnerabilities at multiple layers simultaneously, such as a combination of spoofing at the physical layer and packet injection at the network layer, cannot be effectively mitigated by single-layer solutions. This limitation has spurred interest in cross-layer security mechanisms, which integrate security measures across multiple protocol layers to provide a holistic and adaptive defense against cyber threats.

Cross-layer security mechanisms offer several advantages over traditional approaches. By leveraging information from multiple layers, these mechanisms can detect and respond to sophisticated attack patterns that would otherwise go unnoticed. For example, a cross-layer intrusion detection system could combine physical-layer signal anomalies with transport-layer packet behavior to identify coordinated attacks. Additionally, cross-layer mechanisms can optimize system performance by balancing security requirements with operational constraints, such as bandwidth availability and latency. This dynamic adaptability is particularly critical in drone-assisted vehicular networks, where communication conditions and threat levels can change rapidly.

This paper aims to address the pressing need for effective security solutions in drone-assisted vehicular networks by proposing a cross-layer security framework. The framework is specifically designed to secure the communication links used for transmitting road information collected by drones to vehicles and other entities in the ITS. The key contributions of this paper are as follows:

- **Analysis of security threats:** We provide a comprehensive analysis of the unique security challenges and threat vectors associated with drone-assisted vehicular communication systems. This includes identifying potential attack scenarios and their implications for ITS operations.
- **Design of a cross-layer security framework:** We propose a novel framework that integrates authentication, encryption, and intrusion detection mechanisms across multiple protocol layers. The framework is designed to dynamically adapt to varying attack scenarios while maintaining system performance.
- **Evaluation of the framework:** We evaluate the effectiveness of the proposed framework through simulations and analysis. Key metrics such as detection accuracy, communication overhead, and response time are assessed to demonstrate the framework's capability to secure communication links without compromising performance.

The rest of this paper is organized as follows. Section **??** discusses the security challenges in drone-assisted vehicular networks, highlighting the limitations of traditional security approaches. Section **??** presents the proposed cross-layer security framework, detailing its design, functionality, and implementation. Section **??** evaluates the performance of the framework through simulations, with a focus on key metrics such as detection accuracy and system overhead. Finally, Section **??** concludes the paper with insights into the implications of our findings and potential directions for future research.

The proposed framework not only addresses the security challenges of drone-assisted vehicular networks but also contributes to the broader field of ITS by advancing the understanding of cross-layer security mechanisms. By providing a comprehensive analysis of threats, a robust design for a security framework, and rigorous performance evaluation, this paper aims to pave the way for more secure and efficient ITS solutions leveraging UAVs.

Security Challenges in Drone-Assisted Vehicular Networks

The integration of drones in vehicular networks introduces novel security challenges due to their dependence on wireless communication protocols and their operation in open, highly dynamic environments. These networks, characterized by the interaction of aerial, terrestrial, and sometimes satellite nodes, are vulnerable to a wide range of cyber and physical threats. Below, we explore the primary security challenges in drone-assisted vehicular networks, each of which poses significant risks to system functionality, data integrity, and user safety.

Eavesdropping and Data Interception

One of the fundamental vulnerabilities in drone-assisted vehicular networks arises from the use of wireless communication links, which are inherently susceptible to eavesdropping. Malicious actors can exploit this vulnerability to intercept sensitive data, such as traffic patterns, vehicle trajectories, or incident reports, transmitted between drones and vehicles. The exposure of such information can lead to severe consequences, including privacy violations, strategic manipulation of traffic systems, or even physical harm.

The susceptibility to eavesdropping is further exacerbated by the broad communication range of drones, which often extends into areas beyond the immediate network control. Advanced interception techniques, such as directional antennas or software-defined radios (SDRs), enable attackers to capture data over long distances. The lack of strong encryption mechanisms or improper implementation of security protocols can further aggravate this risk, allowing adversaries to gain unauthorized access to critical vehicular information.

Spoofing and Data Tampering

Identity spoofing represents another major threat in drone-assisted vehicular networks. In such attacks, adversaries assume the identities of legitimate drones or vehicles by falsifying authentication credentials. This allows attackers to inject false or misleading information into the network. For instance, an attacker might

Table 1: Comparison of Traditional and Cross-Layer Security Approaches in Drone-Assisted Vehicular Networks

Feature	**Traditional Security Approaches**	**Cross-Layer Security Mechanisms**
Scope of Defense	Focused on single protocol layer	Integrates multiple protocol layers
Adaptability to Dynamic Threats	Limited	High
Detection of Multi-Layer Attacks	Ineffective	Effective
System Performance Optimization	No optimization for operational constraints	Balances security and performance
Response Time to Attacks	Slower due to limited scope	Faster due to holistic analysis

fabricate data indicating a traffic accident or congestion to reroute vehicles unnecessarily, causing widespread disruption.

Data tampering is closely related and involves the unauthorized alteration of legitimate information. For example, an attacker might modify sensor readings transmitted by a drone to misrepresent environmental conditions, such as road surface status or weather hazards. Such manipulations can severely compromise decision-making processes in autonomous driving systems and traffic management centers, endangering public safety.

Denial-of-Service Attacks

Denial-of-Service (DoS) attacks present a significant challenge by disrupting communication channels between drones and vehicles. In such attacks, adversaries flood the network with an overwhelming number of requests or introduce high levels of interference, rendering legitimate communication ineffective. The consequences of DoS attacks are particularly severe in time-sensitive applications, such as emergency response coordination or collision avoidance systems.

In drone-assisted vehicular networks, DoS attacks can target multiple layers of communication. At the network layer, attackers may overload routing mechanisms to disrupt data delivery. At the physical layer, jamming devices can block wireless signals entirely. Additionally, drones operating in congested urban environments are particularly vulnerable to such attacks due to the high density of communication devices [1], [2].

Physical Layer Vulnerabilities

The physical layer of drone-assisted vehicular networks is especially prone to attacks such as jamming and signal interference. Unlike traditional vehicular networks, the reliance on aerial nodes increases exposure to malicious interference, as drones often operate in open environments with minimal physical protection. Jamming devices, for example, can emit signals at frequencies used by drones, effectively drowning out legitimate communication.

Signal interference can degrade communication quality and result in packet loss, increased latency, or complete communication failure. This is particularly critical in scenarios requiring high reliability, such as drone-assisted real-time traffic monitoring or vehicle-to-infrastructure (V2I) communication. Moreover, the coexistence of drones and vehicles operating on overlapping frequency bands increases the likelihood of unintentional interference, further complicating the security landscape.

Lack of Inter-Layer Coordination

Traditional security mechanisms in networked systems are often designed to address threats at specific layers of the protocol stack, such as the physical, network, or application layers. However, drone-assisted vehicular networks operate in highly dynamic and heterogeneous environments, where threats can propagate across multiple layers [3]. The absence of inter-layer coordination hinders the ability to detect and mitigate such cross-layer attacks effectively.

For instance, a jamming attack at the physical layer may lead to cascading effects at the network and application layers, such as route failures or erroneous traffic management decisions. Similarly, spoofed data at the application layer can compromise routing protocols at the network layer. Addressing these challenges requires the development of integrated security frameworks that enable seamless collaboration across different layers.

Implications for Security Framework Design

The aforementioned challenges highlight the need for robust security frameworks tailored to the unique characteristics of drone-assisted vehicular networks. Key design principles include:

- **Advanced Encryption Mechanisms:** Employing lightweight yet strong encryption to secure wireless communication against eavesdropping and tampering.
- **Identity Management:** Developing robust authentication protocols to prevent spoofing and ensure trust among network entities.

Table 2: Examples of Spoofing and Data Tampering Scenarios in Drone-Assisted Vehicular Networks

Attack Type	Potential Impact
Spoofing	Fake traffic congestion alerts reroute vehicles unnecessarily, causing delays and fuel wastage.
Data Tampering	Modified sensor data leads to incorrect detection of road hazards, increasing accident risks.
Impersonation	Attackers masquerade as traffic drones, disseminating incorrect navigation instructions.

Table 3: Challenges and Consequences of Cross-Layer Threats in Drone-Assisted Vehicular Networks

Threat Type	Cross-Layer Consequences
Jamming	Physical layer disruption causes packet loss at the network layer and delays in application-layer services.
Spoofing	False data at the application layer leads to incorrect routing decisions at the network layer.
Uncoordinated Protocols	Lack of inter-layer communication results in delayed detection of cascading attacks.

- **Cross-Layer Security Solutions:** Designing integrated mechanisms to detect and mitigate threats propagating across multiple layers.
- **Resilience to Physical Layer Attacks:** Implementing anti-jamming techniques and robust signal processing methods to enhance communication reliability.
- **Dynamic Adaptation:** Leveraging machine learning and artificial intelligence to adapt security measures to evolving threats and network conditions.

Addressing these challenges requires a multidisciplinary approach, combining insights from wireless communication, cybersecurity, and systems engineering. By prioritizing the development of resilient security mechanisms, researchers can ensure the safe and efficient operation of drone-assisted vehicular networks in the face of growing threats.

Proposed Cross-Layer Security Framework

To address the challenges outlined above, this section introduces a cross-layer security framework designed for drone-assisted vehicular communication networks. The proposed framework aims to provide comprehensive protection by integrating security measures across the physical, data link, and network layers. This integration ensures a synergistic approach that enhances detection, mitigation, and response to a wide spectrum of security threats, enabling a more robust and resilient communication environment [4], [5].

Authentication Mechanisms

Authentication is a critical component of any secure communication framework, as it ensures that only legitimate entities can participate in the network. In the context of drone-assisted vehicular networks, the dynamic nature of nodes and the mobility of vehicles and drones amplify the challenge of effective authentication [6]. The proposed framework incorporates a multi-faceted approach to authentication that leverages lightweight cryptographic techniques and cross-layer information sharing.

Elliptic Curve Cryptography for Lightweight Authentication

Elliptic Curve Cryptography (ECC) is well-suited for resource-constrained environments due to its high security per bit and reduced computational overhead. The proposed framework employs ECC to enable mutual authentication between drones, vehicles, and infrastructure elements. By using smaller key sizes compared to traditional public-key cryptographic schemes, ECC reduces the computational burden on drones and vehicles, allowing for efficient authentication without compromising security.

The mutual authentication process begins with a handshake protocol where entities exchange public keys and verify identities using ECC-based digital signatures. This process not only prevents unauthorized access but also mitigates the risk of man-in-the-middle (MitM) attacks by verifying the integrity of communication channels.

Cross-Layer Authentication Integration

To enhance the robustness of authentication mechanisms, the proposed framework integrates authentication information across the physical and data link layers. At the physical layer, signal characteristics such as received signal strength indicator (RSSI) and channel state information (CSI) are analyzed to detect inconsistencies that may indicate spoofing attempts. This information is passed to the data link layer, where cryptographic authentication takes place. The combined analysis of physical and cryptographic data enables the framework to detect sophisticated attacks, such as relay attacks, that exploit vulnerabilities in a single layer [7], [8].

Table 4 provides a summary of the key features and benefits of the authentication mechanisms employed in the proposed framework.

Encryption and Data Confidentiality

Maintaining the confidentiality of transmitted data is paramount in preventing eavesdropping and unauthorized data interception in drone-assisted vehicular networks. The proposed framework employs a multi-layered encryption strategy that balances security with efficiency, ensuring that real-time communication requirements are met without introducing significant computational delays [9].

End-to-End Encryption

End-to-end encryption is implemented at the network layer to protect data as it traverses multiple nodes in the communication network. The Advanced Encryption Standard (AES) with a 256-bit key is employed for its proven security and efficiency. This encryption scheme ensures that even if intermediate nodes are compromised, the data remains secure.

Dynamic Key Management System

A dynamic key management system is incorporated to periodically update encryption keys, minimizing the risk of key compromise. The system uses a hierarchical approach where a central trusted authority distributes session keys to drones and vehicles. These session keys are refreshed based on time intervals or data thresholds, ensuring that potential attackers cannot exploit long-term keys.

The proposed framework also incorporates forward and backward secrecy. Forward secrecy ensures that the compromise of a session key does not affect previous communications, while backward secrecy protects future communications in the event of key exposure. These properties are essential in safeguarding long-term data confidentiality.

Optimized Encryption for Real-Time Communication

To minimize computational overhead, the encryption process is optimized using hardware acceleration and lightweight encryption algorithms for low-priority data. This optimization ensures that time-sensitive applications, such as collision avoidance systems, are not delayed by encryption processes.

Table 5 outlines the key features and advantages of the encryption mechanisms implemented in the proposed framework.

Intrusion Detection Systems

Intrusion detection systems (IDS) play a vital role in identifying and mitigating security threats in drone-assisted vehicular communication networks. The proposed framework integrates IDS functionality across multiple layers to detect and respond to a wide range of attacks.

Layer-Specific IDS Components

The IDS in the proposed framework is designed to monitor activities at the physical, data link, and network layers. At the physical layer, the IDS analyzes signal characteristics to detect jamming and spoofing attacks. For example, sudden drops in RSSI or unusual fluctuations in CSI may indicate the presence of a jammer. At the data link layer, the IDS monitors MAC addresses and transmission patterns to identify anomalies, such as MAC spoofing or flooding attacks. Finally, at the network layer, the IDS detects distributed denial-of-service (DDoS) attacks by analyzing traffic patterns and identifying unusually high levels of data flow from specific nodes.

Machine Learning-Based Anomaly Detection

To enhance the adaptability and accuracy of the IDS, the proposed framework employs machine learning-based anomaly detection. Algorithms such as support vector machines (SVMs), random forests, and neural networks are used to classify traffic patterns as normal or anomalous. The IDS is trained on labeled datasets containing both legitimate and malicious traffic, enabling it to identify previously unknown attack vectors.

Real-time adaptability is achieved through online learning mechanisms, which allow the IDS to update its models based on new data. This adaptability is particularly important in dynamic environments where attack strategies evolve rapidly.

Cross-Layer Collaboration

The IDS components at different layers collaborate to provide a holistic view of network security. For instance, if the physical layer detects a potential jamming attack, it alerts the network layer to reroute traffic away from affected channels. Similarly, anomalies detected at the data link layer can prompt the network layer to isolate compromised nodes. This cross-layer collaboration enhances the overall effectiveness of the IDS.

Cross-Layer Coordination

The cornerstone of the proposed framework is its cross-layer coordination mechanism, which enables seamless information sharing and collaboration across different layers of the communication stack. This coordination is essential for addressing complex security threats that exploit multiple layers.

Table 4: Key Features of Authentication Mechanisms in the Proposed Framework

Feature	Description and Benefits
Elliptic Curve Cryptography (ECC)	Provides high-security authentication with reduced computational overhead, suitable for resource-constrained devices.
Cross-Layer Integration	Combines physical layer signal analysis with data link layer cryptographic authentication to detect advanced attacks.
Mutual Authentication	Ensures that both communicating entities verify each other's identity, mitigating risks such as MitM attacks.
Dynamic Authentication Metrics	Leverages real-time signal characteristics and cryptographic data to adapt to changing network conditions.

Table 5: Key Features of Encryption Mechanisms in the Proposed Framework

Feature	Description and Benefits
End-to-End Encryption	Protects data from source to destination, preventing unauthorized access during transmission.
Dynamic Key Management	Periodically updates keys to reduce the risk of key compromise and ensures forward and backward secrecy.
Hardware Acceleration	Enhances the speed of encryption processes, ensuring compatibility with real-time communication requirements.
Lightweight Encryption Algorithms	Reduces computational overhead for non-critical data while maintaining security.

Information Sharing Across Layers

Cross-layer coordination facilitates the sharing of security-related information, such as authentication results, signal quality metrics, and traffic patterns. For example, the physical layer can share RSSI and CSI data with the network layer to improve the detection of jamming attacks. Similarly, the data link layer can provide MAC-level authentication results to the network layer, enhancing the accuracy of routing decisions.

Adaptive Security Policies

The proposed framework incorporates adaptive security policies that dynamically adjust based on cross-layer information. For instance, if the IDS detects a potential threat at the physical layer, the network layer can increase encryption strength or reroute traffic to mitigate the impact. These adaptive policies ensure that the framework remains resilient in the face of evolving threats.

Implementation Considerations

To implement cross-layer coordination effectively, the proposed framework relies on a centralized control unit that manages information exchange and decision-making. This control unit is equipped with high-performance computing resources to process data from multiple layers in real-time. Additionally, standard communication interfaces are used to ensure compatibility between different layers.

By integrating security measures across the physical, data link, and network layers, the proposed cross-layer security framework provides a comprehensive defense against a wide range of threats. The framework's emphasis on lightweight cryptographic techniques, dynamic key management, machine learning-based intrusion detection, and cross-layer coordination ensures that it meets the unique challenges of drone-assisted vehicular communication networks.

Performance Evaluation

The proposed cross-layer security framework was subjected to a comprehensive performance evaluation using a sophisticated network simulation environment. This section presents an in-depth analysis of the framework's effectiveness based on key performance metrics, including security resilience, communication latency, and throughput.

Simulation Setup

The evaluation was conducted in a simulation environment designed to replicate a drone-assisted vehicular network (DAVN). This environment incorporated multiple drones and vehicles communicating over wireless channels using IEEE 802.11p protocol, a common standard for vehicular communication. The network topology consisted of drones acting as relay nodes, facilitating vehicle-to-

Table 6: Detection Rates for Different Attack Types

Attack Type	Baseline Model Detection Rate (%)	Proposed Framework Detection Rate (%)	Improvement (%)
Eavesdropping	68.4	91.7	23.3
Spoofing	81.2	96.5	15.3
DoS	76.5	95.3	18.8
Jamming	70.3	89.1	18.8

Table 7: Throughput Comparison Under Different Scenarios

Scenario	Baseline Model Throughput (Mbps)	Proposed Framework Throughput (Mbps)	Improvement (%)
Normal Conditions	19.1	18.6	-2.6
During Eavesdropping	15.4	17.3	12.3
During DoS	13.2	17.8	34.8
During Jamming	12.9	17.1	32.6

vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. The simulated area spanned 5 square kilometers with varying traffic density and mobility patterns modeled using the SUMO (Simulation of Urban Mobility) tool.

To comprehensively evaluate the framework's security, multiple attack scenarios were implemented:

- **Eavesdropping Attacks:** Adversaries attempted to intercept and decode sensitive information transmitted over the network.
- **Spoofing Attacks:** Malicious nodes masqueraded as legitimate nodes, sending falsified information to disrupt network operations.
- **Denial-of-Service (DoS) Attacks:** Attackers targeted drones and vehicles by flooding the communication channels to degrade service availability.
- **Jamming Attacks:** Adversaries transmitted high-power signals to disrupt wireless communication, impacting the network's reliability.

The proposed framework was configured with a cross-layer intrusion detection system (IDS), leveraging information from the physical, MAC, and application layers. The IDS utilized machine learning models trained on network behavior under normal and attack conditions. Additionally, an end-to-end encryption mechanism was implemented for secure data transmission. The performance was compared against a baseline single-layer security model that employed only traditional cryptographic methods.

Results and Discussion

The simulation results highlighted the effectiveness of the cross-layer security framework in enhancing the network's security and performance. The findings are presented below:

Security Resilience

The framework exhibited significant improvements in detecting and mitigating attacks, as shown in Table 6. The cross-layer IDS achieved a detection rate of 96.5% for spoofing attacks and 95.3% for DoS attacks, outperforming the baseline model, which had detection rates of 81.2% and 76.5%, respectively. The high accuracy of the IDS can be attributed to its ability to analyze features from multiple network layers, providing a holistic view of the network's behavior.

Communication Latency

The communication latency was analyzed under normal conditions and during attack scenarios. The proposed framework maintained an average end-to-end delay of 12.4 ms under normal conditions, compared to 11.9 ms for the baseline model. During attack scenarios, the latency increased slightly to 14.2 ms due to the overhead of the IDS, but it remained within acceptable bounds for vehicular communication systems. This demonstrates that the framework's security enhancements do not compromise real-time communication.

Throughput

The throughput of the network was another critical metric evaluated. As shown in Table 7, the proposed framework achieved an average throughput of 18.6 Mbps under normal conditions, compared to 19.1 Mbps for the baseline model. During attack scenarios, the framework maintained a throughput of 17.8 Mbps, significantly higher than the baseline model's 13.2 Mbps. This resilience in throughput highlights the framework's ability to mitigate attacks effectively without substantial performance degradation.

System Overhead

The additional computational and communication overhead introduced by the cross-layer security framework was evaluated. The encryption and IDS modules increased the average CPU utilization by 8.7% and the memory usage by 12.4%, compared to the baseline model. Despite this increase, the overall system performance remained within acceptable limits for modern vehicular and drone hardware. The trade-off between enhanced security and minimal overhead underscores the practicality of the proposed framework.

The performance evaluation demonstrated that the proposed cross-layer security framework effectively enhances the security and reliability of drone-assisted vehicular networks. It provides robust protection against a variety of attacks, with high detection rates and minimal impact on communication latency and throughput. The results validate the feasibility of deploying the framework in real-world scenarios, where security and performance are critical considerations.

Conclusion

This paper presented a comprehensive cross-layer security framework designed for drone-assisted vehicular communication networks. The primary objective of the framework is to address critical security vulnerabilities, including but not limited to eavesdropping, spoofing, and denial-of-service (DoS) attacks, which pose significant risks to the integrity and reliability of intelligent transportation systems. By adopting a multi-layered approach that integrates authentication mechanisms, encryption techniques, and intrusion detection systems across various protocol layers, the proposed framework effectively enhances the overall security posture of vehicular communication networks without compromising system performance [10], [11].

Simulation results provided strong evidence of the framework's efficacy. Specifically, the results demonstrated its ability to thwart sophisticated attack vectors while maintaining low latency and ensuring high throughput. These outcomes underscore the practical utility of the proposed framework in real-world scenarios, where system reliability and security are of paramount importance. Moreover, the framework's modular design ensures that it can be seamlessly integrated into existing vehicular communication systems, thereby offering a pragmatic solution for enhancing security in contemporary intelligent transportation systems.

Future work will focus on extending the capabilities of the proposed framework to accommodate emerging technologies such as fifth-generation (5G) networks and edge computing [12]. These technologies are expected to play a pivotal role in the evolution of vehicular communication networks, introducing new challenges and opportunities for security. By incorporating advanced features, such as ultra-low latency communication and distributed processing, the extended framework will aim to enhance scalability and adaptability in highly dynamic network environments. Additionally, future research will explore the integration of machine learning algorithms to enable proactive threat detection and adaptive security mechanisms, further bolstering the framework's resilience against evolving cyber threats. The proposed cross-layer security framework represents a significant step forward in securing drone-assisted vehicular communication networks. By addressing existing vulnerabilities and providing a solid foundation for future enhancements, this work contributes to the advancement of secure and reliable intelligent transportation systems, paving the way for safer and more efficient vehicular networks [11], [13].

Conflict of interest

Authors state no conflict of interest.

References

[1] L. Wang, Y. Chen, P. Wang, and Z. Yan, "Security threats and countermeasures of unmanned aerial vehicle communications," *IEEE Communications Standards Magazine*, vol. 5, no. 4, pp. 41–47, 2021.

[2] C. Bunse and S. Plotz, "Security analysis of drone communication protocols," in *Engineering Secure Software and Systems: 10th International Symposium, ESSoS 2018, Paris, France, June 26-27, 2018, Proceedings 10*, Springer, 2018, pp. 96–107.

[3] S. M. Bhat and A. Venkitaraman, "Hybrid v2x and drone-based system for road condition monitoring," in *2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, IEEE, 2024, pp. 1047–1052.

[4] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, "A survey of cyber security threats and solutions for uav communications and flying ad-hoc networks," *Ad Hoc Networks*, vol. 133, p. 102 894, 2022.

[5] A. Fotouhi, H. Qiang, M. Ding, *et al.*, "Survey on uav cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Communications surveys & tutorials*, vol. 21, no. 4, pp. 3417–3442, 2019.

[6] S. Bhat and A. Kavasseri, "Enhancing security for robot-assisted surgery through advanced authentication mechanisms over 5g networks," *European Journal of Engineering and Technology Research*, vol. 8, no. 4, pp. 1–4, 2023.

[7] H. P. D. Nguyen and D. D. Nguyen, “Drone application in smart cities: The general overview of security vulnerabilities and countermeasures for data communication,” *Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead*, pp. 185–210, 2021.

[8] V. Hassija, V. Chamola, A. Agrawal, *et al.*, “Fast, reliable, and secure drone communication: A comprehensive survey,” *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2802–2832, 2021.

[9] S. Bhat and A. Kavasseri, “Multi-source data integration for navigation in gps-denied autonomous driving environments,” *International Journal of Electrical and Electronics Research*, vol. 12, no. 3, pp. 863–869, 2024.

[10] Z. Lv, “The security of internet of drones,” *Computer Communications*, vol. 148, pp. 208–214, 2019.

[11] D. He, S. Chan, and M. Guizani, “Communication security of unmanned aerial vehicles,” *IEEE Wireless Communications*, vol. 24, no. 4, pp. 134–139, 2016.

[12] S. Bhat, “Leveraging 5g network capabilities for smart grid communication,” *Journal of Electrical Systems*, vol. 20, no. 2, pp. 2272–2283, 2024.

[13] Y. Ko, J. Kim, D. G. Duguma, P. V. Astillo, I. You, and G. Pau, “Drone secure communication protocol for future sensitive applications in military zone,” *Sensors*, vol. 21, no. 6, p. 2057, 2021.