HYShield: A Multi-Layered Security Framework for Air-Space-Ground-Maritime Networks in 6G Scenarios

Miao Du, Peng Yang, Yinqiu Liu, Zehui Xiong, Dusit Niyato, and Biplab Sikdar

Abstract

The advent of 6G networks heralds unprecedented advancements in communication characterized by seamless integration across air, space, ground, and maritime (ASGM) domains. These networks aim to deliver ultra-high-speed connectivity, massive device interoperability, and real-time responsiveness, enabling critical applications such as drone logistics, autonomous driving, and smart marine operations. However, the multi-domain nature of ASGM networks introduces significant security challenges, including interception, tampering, distributed denial of service (DDoS), and advanced man-in-the-middle (MitM) attacks. To address these issues, we present HYShield, a novel multi-layered security framework tailored for ASGM networks in 6G scenarios. HYShield integrates advanced technologies such as federated learning, quantum key distribution (QKD), blockchain authentication, and AI-driven anomaly detection within a four-layer architecture comprising perception, transmission, processing, and application layers. In addition, we offer a comprehensive case study demonstrating HYShield's capability to defend against MitM attacks in drone communication, showcasing its effectiveness in enhancing resilience, privacy, and performance for critical ASGM applications in the era of 6G.

Introduction

With the advancement of 6G, the Air-Space-Ground-Maritime (ASGM) network has emerged as a transformative framework, combining high-speed connectivity with wide-reaching capabilities across diverse applications. Leveraging technologies such as real-time communication, AI, and secure data transmission, ASGM networks are now widely applied in drone logistics, satellite communications, unmanned driving, maritime transportation, smart marine fisheries, and emergency rescue [1]. These applications demonstrate the broad reach and transformative potential of ASGM, allowing for efficient resource distribution, enhanced security, and improved operational efficiency across multiple domains, as illustrated in Fig. 1.

However, as ASGM networks become integral to such critical applications, they also encounter significant security threats and challenges. For instance, satellite-ground links face risks of interception and signal interference, where unauthorized access to satellite data could expose sensitive information or disrupt essential services in remote regions, challenging existing encryption methods [2]. Drone networks are vulnerable to GPS spoofing attacks, which can lead to loss of navigation control, jeopardizing the reliability of drone-based logistics and emergency missions. Additionally, in autonomous driving, adversaries can introduce data poisoning into shared communication streams between vehicles, potentially leading to accidents by distorting traffic data. These cases underscore the limitations of current defense mechanisms, which often lack the adaptability and resilience needed to meet the complex, multi-domain security needs of ASGM environments [3].

In response to these security challenges, researchers and industry practitioners have proposed and implemented a variety of defense mechanisms tailored to the unique needs of ASGM networks.

Encryption Protocols: End-to-end encryption (E2EE) and Quantum Key Distribution (QKD) are widely used to secure data transmission across ASGM networks. E2EE ensures data remains encrypted during transmission, while QKD offers secure key exchange using quantum mechanics. However, E2EE may experience latency in high-speed environments, and QKD's hardware requirements and high costs limit its scalability [4].

Anomaly Detection through Artificial Intelligence: AI-driven systems monitor network traffic to detect suspicious patterns, protecting drones, unmanned vehicles, and maritime vessels from intrusions. These systems excel in identifying known attack patterns but depend on pre-existing data and require significant computational resources, making real-time deployment in constrained ASGM settings challenging.

Access Control and Authentication Mechanisms: Role-based access control (RBAC) and

Miao Du and Peng Yang (corresponding author) are with Southeast University, China; Yinqiu Liu and Dusit Niyato are with Nanyang Technological University, Singapore; Zehui Xiong is with Singapore University of Technology and Design, Singapore; Biplab Sikdar is with National University of Singapore, Singapore.

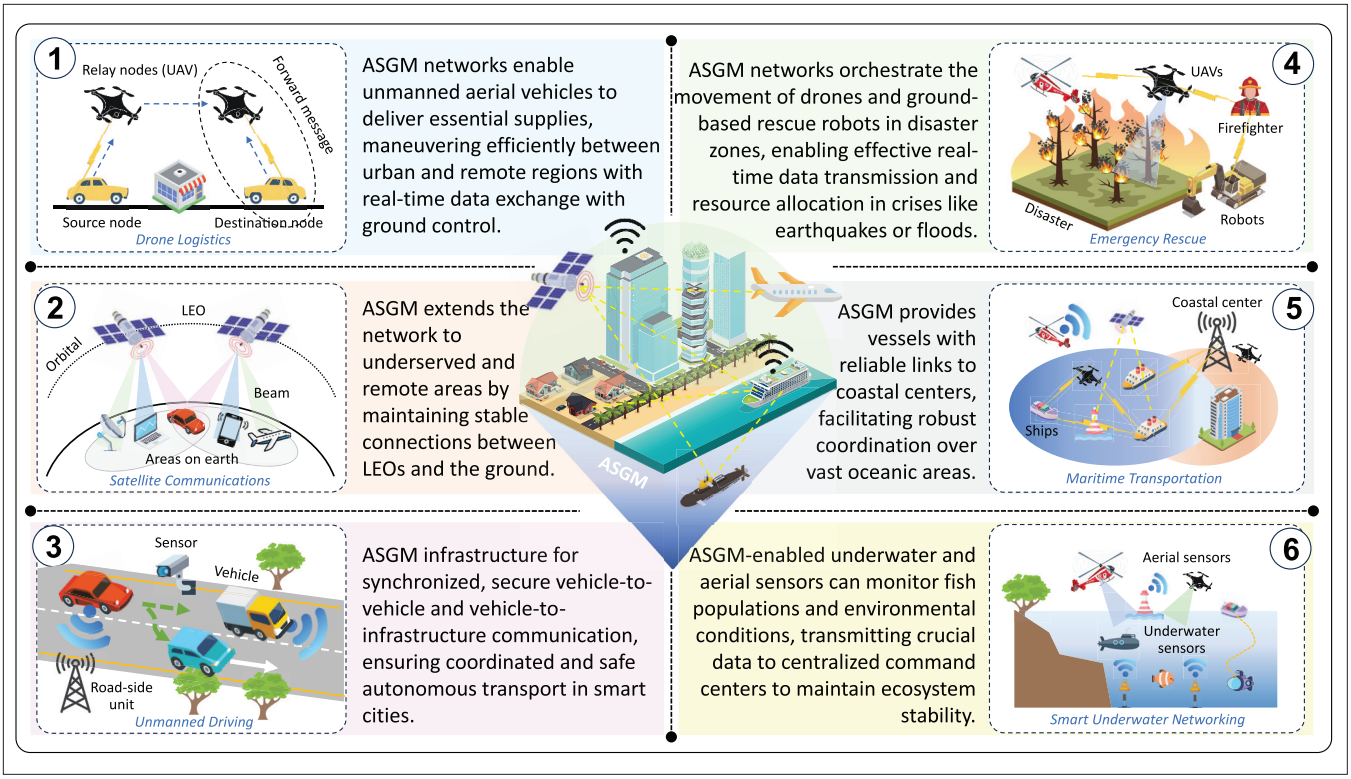

FIGURE 1. Diverse scenarios for ASGM applications in 6G networks. The central circle illustrates six representative scenarios of ASGM. More detailed scenarios and explanations are shown in (1)-(6).

blockchain-based authentication are used to restrict unauthorized access. RBAC assigns permissions by roles, and the blockchain provides tamper-resistant device identity records [5]. However, RBAC lacks adaptability for dynamic applications, and blockchain's computational demands can affect performance in bandwidth-limited scenarios.

Motivated by such facts, we propose HYShield, a novel multi-layered security framework that integrates advanced technologies such as federated learning, quantum key distribution (QKD), blockchain authentication, and AI-driven anomaly detection. HYShield is designed to safeguard communication and ensure data integrity in dynamic, multi-domain environments, offering resilience against evolving threats such as man-in-the-middle attacks. To accommodate low-resource environments, HYShield employs lightweight edge AI for anomaly detection and leverages federated learning to minimize computational overhead on constrained devices such as drones and IoT sensors. By providing a cohesive and adaptive defense mechanism, HYShield significantly enhances the security and reliability of ASGM networks in 6G environments. The main contributions can be summarized in the following:

- We analyze the unique security challenges faced by ASGM networks in 6G, highlighting the limitations of existing defense mechanisms and the necessity for an integrated approach.
- Based on the insightful analysis above, we propose HYShield, a comprehensive multi-layered security framework that incorporates advanced technologies to protect communication systems and ensure data integrity across diverse ASGM scenarios.
- We present a case study demonstrating HYShield's effectiveness in defending against MitM attacks in drone communication. Experimental results demonstrate that HYShield enhances communication security and improves the reliability of ASGM networks in various 6G applications.

Overview of Security Threats and Defense Mechanisms in ASGM Networks

In this section, we investigate and overview the existing security threats and defense mechanisms in ASGM networks, as illustrated in Fig. 2.

Security Threats

Signal Eavesdropping and Interception: In ASGM networks, open-air and satellite-based communication channels are highly vulnerable to eavesdropping. Adversaries with adequate equipment can intercept signals exchanged between aircraft, satellites, ground stations, and maritime vessels [6]. This interception exposes sensitive data and poses a significant threat to the privacy and security of transmitted information.

Jamming and Distributed Denial of Service (DDoS) Attacks: High reliance on wireless communication in ASGM networks makes them susceptible to jamming and DDoS attacks. Malicious actors can target specific frequency bands to disrupt communication in air, ground, or maritime networks. This interruption can lead to a loss of connectivity or prevent real-time data exchange, which is critical for navigation, control, and safety protocols.

GPS Spoofing and Navigation Deception: In ASGM systems, accurate positioning is crucial, especially for drones, maritime vessels, and aircraft. GPS spoofing attacks trick navigation systems into perceiving incorrect positions, which can lead to serious misdirection. This attack type

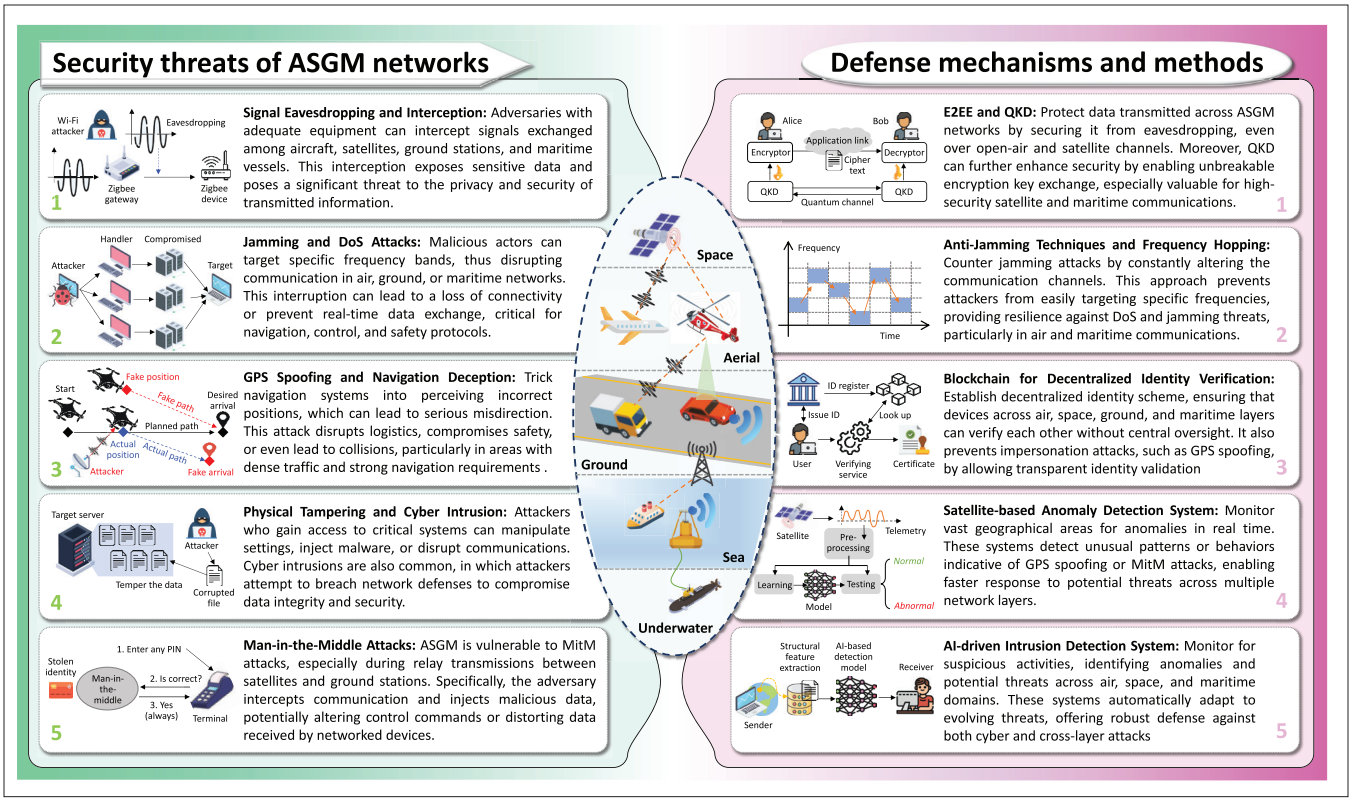

FIGURE 2. Security challenges and countermeasures in ASGM networks.

can disrupt logistics, compromise safety, or even lead to collisions, particularly in areas with dense traffic or challenging navigation requirements [7].

Physical Tampering and Cyber Intrusion: Physical infrastructure, such as ground stations and maritime base stations, may be vulnerable to direct tampering. Attackers who gain access to critical systems can manipulate settings, inject malware, or disrupt communications. Cyber intrusions are also common, as attackers attempt to breach network defenses to compromise data integrity and security.

Man-in-the-Middle (MitM) Attacks: ASGM communication channels are vulnerable to MitM attacks, especially during relay transmissions between satellites, ground stations, or airborne vehicles. In such attacks, the adversary intercepts communication and injects malicious data, potentially altering control commands or distorting data received by networked devices [8].

Defense Mechanisms

E2EE and QKD: E2EE protects data transmitted across ASGM networks by securing it from eavesdropping, even over open-air and satellite channels. Moreover, QKD can further enhance security by enabling unbreakable encryption key exchange, which is especially valuable for high-security satellite and maritime communications [9].

Anti-Jamming Techniques and Frequency Hopping: Dynamic frequency hopping and adaptive spectrum allocation can defend against jamming attacks by constantly altering communication channels. This approach prevents attackers from easily targeting specific frequencies, providing resilience against DDoS and jamming threats, particularly in air and maritime communications.

Blockchain for Decentralized Identity Verification: Using blockchain technology, ASGM networks can establish decentralized identity management, ensuring that devices across air, space, ground, and maritime layers can verify each other without central oversight. This solution prevents impersonation attacks, such as GPS spoofing, by allowing transparent and tamper-resistant identity validation [10].

Satellite-Based Anomaly Detection Systems: Leveraging AI and satellite sensors, ASGM networks can monitor vast geographical areas for anomalies in real time [11]. These systems detect unusual patterns or behaviors indicative of GPS spoofing or MitM attacks, enabling faster response to potential threats across multiple network layers.

AI-Driven Intrusion Detection Systems (IDS): AI-enhanced IDS solutions deployed in ground stations and edge devices within ASGM networks monitor for suspicious activities, identifying anomalies and potential threats across air, space, and maritime domains [12]. These systems automatically adapt to evolving threats, offering robust defense against both cyber and cross-layer attacks.

HYShield: A Multi-Layered Security Framework

In this section, we first outline the challenges that our proposed framework needs to address, followed by a detailed description of HYShield, as summarized in Fig. 3.

Challenges

Several considerations could be made to enhance the HYShield framework.

High Cost and Resource Demands: Advanced security measures, like QKD and AI-driven IDS, require significant computational resources, spe-

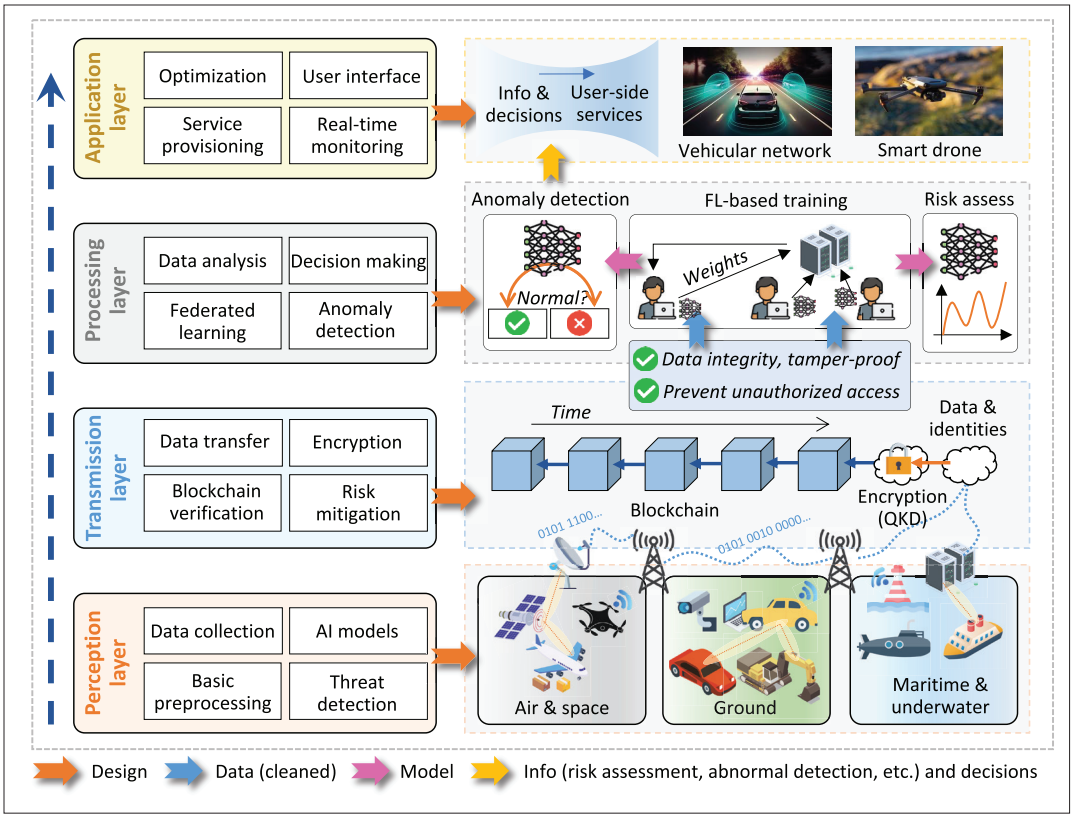

FIGURE 3. Illustration of the proposed HYShield framework: The perception layer collects and preprocesses data from diverse sources. The transmission layer ensures secure communication via encryption (including QKD) and blockchain-based verification. The processing layer applies AI-driven models to assess security risks and optimize responses. The application layer provides real-time monitoring, decision-making, and user-side services.

cialized hardware, and stable infrastructure. For ASGM networks, which often involve remote or mobile components (e.g., drones, maritime vessels, satellites), the high cost and energy consumption of these solutions are major limitations, making them challenging to deploy universally.

Latency and Real-Time Responsiveness: ASGM networks demand real-time responses to threats, especially in fast-moving environments like air and maritime. However, the current generation of intrusion detection systems and dynamic frequency adaptation mechanisms may introduce delays in detection or response. This latency can hinder the effectiveness of security protocols, especially in high-stakes scenarios where immediate countermeasures are required. HYShield can address this by leveraging edge AI for rapid local detection, ensuring minimal delay in threat response.

Vulnerability to Emerging Attacks: While existing defenses offer protection against many known threats, evolving tactics such as AI-driven attacks or quantum-based hacking could compromise ASGM networks. These emerging attacks exploit novel vulnerabilities across network layers, necessitating the constant adaptation of defense mechanisms, which can strain resources and require frequent updates to remain effective.

Limited Scalability Across Diverse Environments: ASGM networks are unique in their interconnection of air, space, ground, and maritime components, each with distinct environmental and operational challenges [13]. For instance, drones often face operational challenges such as sudden weather changes, GPS signal loss, or interference from other airborne objects. These factors can significantly disrupt communication and navigation, highlighting the need for adaptive security measures. Current defense mechanisms are often developed for specific layers and may not scale effectively across all domains. For example, anti-jamming protocols may work well in terrestrial settings but face performance limitations in high-altitude and maritime environments where signal interference is unpredictable.

Proposed Framework

To address the unique security challenges of ASGM networks, we propose HYShield, a multi-layered security framework tailored for comprehensive protection and adaptability across diverse applications in 6G-enabled ASGM environments. ASGM networks involve complex and heterogeneous domains, each with distinct security challenges, such as dynamic mobility, large-scale communication demands, and exposure to advanced attacks such as MitM and jamming. HYShield leverages QKD for real-time threat detection and secure key exchanges, addressing the critical need for rapid and reliable security in high-mobility scenarios. Additionally, HYShield incorporates blockchain to ensure decentralized trust management and tamper-resistant data integrity, overcoming the scalability and trust issues in heterogeneous environments. To enhance adaptability across diverse ASGM applications, HYShield integrates an adaptive anomaly detection mechanism that dynamically adjusts to changing network conditions, ensuring robust performance even in highly dynamic or unpredictable environments. Its lightweight and scalable

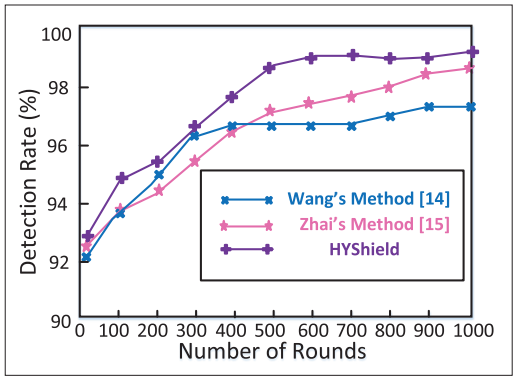

FIGURE 4. Detection rate comparison of HYShield and baseline methods over multiple rounds.

design allows seamless deployment across various ASGM scenarios, maintaining security without compromising efficiency. By addressing these challenges, HYShield ensures robust, efficient, and adaptive protection, enabling ASGM networks to securely support diverse 6G applications under challenging operational conditions. The specific design is as follows.

Perception Layer: The Perception Layer forms the foundation of the HYShield framework, focusing on data collection and preliminary threat detection. This layer interacts directly with network-connected devices, such as drones, satellites, and maritime sensors, which serve as primary data sources. By leveraging advanced sensors and edge AI technologies, the Perception Layer conducts real-time monitoring to detect anomalies at data entry points. For instance, drones and unmanned vehicles rely on sensor data to navigate safely, and any abnormal readings or inconsistencies are immediately flagged for inspection. By using machine learning algorithms optimized for edge processing, this layer minimizes latency in anomaly detection, providing a first line of defense against potential intrusions and enhancing real-time decision-making capabilities at the source.

Transmission Layer: The Transmission Layer ensures secure data transfer across ASGM network segments, maintaining data integrity and confidentiality as information moves between air, space, ground, and maritime nodes. This layer employs encryption methods such as homomorphic encryption and QKD to guard data against interception and unauthorized access during transmission. Additionally, a blockchain-based authentication system verifies device identities, adding an extra layer of trust among network nodes. These mechanisms prevent unauthorized manipulation of data streams and mitigate risks associated with eavesdropping, particularly across satellite-ground communication links where vulnerabilities to interception are high. By safeguarding the transmission pathway, this layer upholds a secure data flow across ASGM nodes.

Processing Layer: Once data is securely transmitted, the Processing Layer performs analysis and transforms it into actionable insights. This layer utilizes federated learning to enable edge devices, such as drones and autonomous vehicles, to collaboratively train machine learning models without sharing raw data, thereby preserving privacy. The Processing Layer also employs AI-driven anomaly detection and risk assessments, which identify unusual patterns or potentially malicious behaviors that may indicate an ongoing attack. For example, in autonomous vehicle networks, federated learning enables data sharing among vehicles to enhance traffic predictions without exposing individual vehicle data. This layer thus contributes to real-time intelligence generation, supporting informed decision-making while maintaining stringent privacy standards.

Application Layer: The Application Layer sits at the top of the HYShield framework, managing high-level security and meeting application-specific requirements. This layer evaluates the specific needs of applications, such as drone logistics or maritime surveillance, and applies adaptive security measures accordingly. Real-time risk assessments are conducted here, enabling the network to prioritize resources and modify protection strategies based on the criticality of each application. For example, during an emergency rescue operation, this layer ensures that communications receive heightened protection and dynamic response measures to counter any interference. Additionally, the Application Layer integrates feedback from the lower layers to continuously refine and optimize security policies, ensuring the system can adapt to evolving threats across ASGM environments.

Overall, the proposed HYShield framework can achieve a high level of resilience and adaptability. These four layers operate independently and collaboratively to create a cohesive security system that meets the stringent demands of 6G-enabled ASGM networks. Moreover, the interactions between layers ensure an adaptive and responsive security mechanism. For example, when the Perception Layer identifies an anomaly, it transmits the alert securely through the Transmission Layer while preserving data integrity. The Processing Layer then assesses the anomaly's impact using AI-based models and forwards critical insights to the Application Layer. This layer, in turn, refines security policies and resource allocations, ensuring real-time adaptive responses based on the severity and context of detected threats. Specifically, the perception layer enables early-stage anomaly detection, while the transmission layer protects data in transit. Moreover, the processing layer offers secure data analysis and intelligence, and the application layer provides application-specific protection. Therefore, the synergy of these layers forms a robust defense mechanism capable of addressing the security challenges inherent in ASGM networks, paving the way for a secure and reliable connectivity framework across diverse ASGM applications.

Case Study: Defending Against MitM Attacks with HYShield Framework

Experimental Configurations

The proposed HYShield framework is designed to address the multifaceted security challenges inherent in ASGM networks, offering robust solutions tailored to the dynamic and heterogeneous nature of these environments. To illustrate its effectiveness in real-world scenarios, we apply HYShield to secure drone communications within ASGM

networks, focusing on its ability to defend against MitM attacks. This case study highlights the critical risks posed by MitM attacks, as ASGM networks often rely on open and dynamic communication links, making them particularly susceptible to interception and manipulation. By mitigating these threats, HYShield strengthens data integrity, confidentiality, and trust in 6G-enabled ASGM systems. The experiment is set up as follows.

Hardware and Software Platform: We setup the experiments with Ubuntu 20.04 and the NS-3 simulator on an Intel Core i9-11900K with a 3.5GHz CPU and equipped with a NVIDIA Tesla V100 GPU accelerator. Moreover, the system uses high-performance servers equipped with Intel Xeon processors and NVIDIA GPUs for processing, and a Gazebo-PX4 simulator platform to emulate drone flight paths and communication scenarios.

Parameter Settings: The HYShield framework combines E2EE and QKD to counter MitM attacks, tested through rigorous simulations. Specifically, E2EE employs AES-256 for symmetric encryption, secured by RSA-4096 for key exchange, and integrates HMAC-SHA-256 for packet authentication. Sequence numbers prevent replay attacks, and session keys are rotated every 15 seconds. In addition, QKD uses the BB84 protocol in a simulated quantum channel with a photon loss rate of 5 percent. Quantum Bit Error Rate (QBER) is an indicator used to measure the error rate during the QKD process, specifically quantifying the number of erroneous bits in the quantum key exchange. If QBER exceeds a predefined threshold, it indicates the presence of noise or eavesdropping, potentially compromising the key's security. The QBER threshold for this setup is 11 percent, ensuring that the system only accepts secure keys. By achieving an average secure key generation rate of 20 kb/s, this rate allows for refreshing the E2EE session keys every 15 seconds.

Evaluation Metrics:

Attack Detection Rate: This metric measures the percentage of successful detections of MitM attacks, including cases where the attackers intercept or alter the communication. Variations in attack intensity and packet size are tested to evaluate detection reliability.

False Positive Rate: This metric measures the frequency at which legitimate communication is incorrectly flagged as malicious. It serves as an indicator of the precision of the detection algorithm, with lower rates signifying minimal disruption to normal operations.

Performance Analysis

We implement the HYShield framework alongside several other IDS schemes, including [14] and [15]. As shown in Fig. 4, HYShield achieves an average detection rate exceeding 95 percent, with a peak detection rate of 99 percent. Notably, after 500 rounds of detection experiments, HYShield maintains a stable detection rate of approximately 98 percent, whereas [14] fluctuates around 94 percent and [15] remains below 92 percent. This superior performance is attributed to HYShield's quantum key distribution (QKD) mechanism, which effectively detects eavesdropping or tampering through quantum error analysis. As the number of rounds increases, HYShield maintains a more stable and higher detection rate, demonstrating its robustness and reliability in long-term operations.

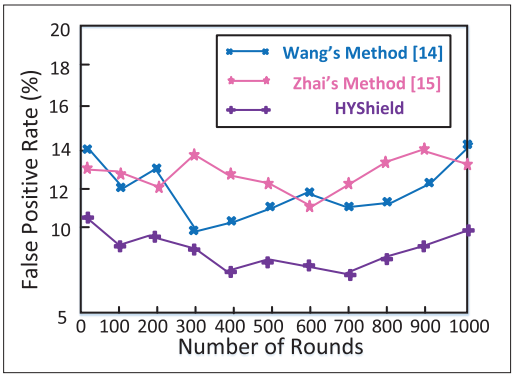

FIGURE 5. False positive rate analysis of HYShield and baseline methods across detection rounds.

In addition to high detection accuracy, HYShield significantly reduces false positive rates compared to the baseline methods, as illustrated in Fig. 5. The false positive rate of HYShield remains consistently low at around 6 percent, whereas [14] exhibits an average false positive rate of approximately 10 percent, and [15] fluctuates between 12 percent and 14 percent. Notably, even after 1000 rounds of testing, HYShield maintains its low and stable false positive rate, while the baseline methods show larger fluctuations. This improvement is due to HYShield's adaptive anomaly detection model, which dynamically adjusts detection thresholds, minimizing the misclassification of benign activities as threats. In real-world deployments, a lower false positive rate reduces unnecessary alerts, preventing disruptions to normal ASGM operations. For instance, in autonomous drone communication networks, excessive false alarms could lead to unnecessary security interventions, wasting resources and affecting mission efficiency. By maintaining a low false positive rate, HYShield ensures that security responses are both accurate and practical, enhancing its usability in operational environments.

Future Directions

In this section, we explore three promising future directions for enhancing communication security within ASGM networks in the 6G era.

Advanced Quantum-Resistant Encryption for Cross-Domain Security

With the advent of quantum computing, traditional encryption methods may become vulnerable, especially in ASGM networks where data often traverses multiple domains. Developing quantum-resistant encryption methods is critical to ensuring the long-term confidentiality of sensitive information across air, space, ground, and maritime layers. These new encryption approaches, such as lattice-based cryptography and post-quantum key distribution, must be designed to handle ASGM's specific demands, ensuring minimal latency and compatibility with the diverse infrastructure components of ASGM networks. In future iterations, HYShield could integrate lattice-based encryption into its QKD framework to enhance quantum resistance, ensuring secure key exchanges even against quantum-capable adversaries. Additionally, hybrid cryptographic schemes

Establishing unified security standards that enable interoperability across ASGM network layers will be essential for secure and efficient data exchange. Future research should focus on developing cross-layer security protocols tailored to a four-layer architecture comprising perception, transmission, processing, and application layers. For instance, ensuring that data integrity verified at the perception layer is preserved through the transmission and securely analyzed in the processing layer will be vital.

combining post-quantum and classical encryption could be explored to balance security and performance in different ASGM application scenarios.

Intelligent Autonomous Threat Detection and Response

To effectively defend ASGM networks against sophisticated attacks, such as GPS spoofing, signal jamming, and cross-layer vulnerabilities, future ASGM systems should incorporate intelligent autonomous detection and response mechanisms. Leveraging AI and machine learning, these systems can predict, identify, and mitigate threats in real time across air, space, ground, and maritime channels. A potential enhancement for HYShield involves incorporating federated learning to improve decentralized anomaly detection, allowing ASGM nodes to collaboratively refine threat models without exposing sensitive data. Additionally, reinforcement learning techniques could be applied to dynamically adjust defense strategies in response to changing attack patterns, making HYShield more adaptable to highly mobile environments such as drone swarms or fluctuating maritime networks. By adopting decentralized, adaptive AI-driven defenses, ASGM networks can improve resilience against dynamic attacks, ensuring the continuity of critical services in aviation, maritime navigation, and space operations.

Unified Security Standards and Interoperability for ASGM Applications

Establishing unified security standards that enable interoperability across ASGM network layers will be essential for secure and efficient data exchange. Future research should focus on developing cross-layer security protocols tailored to a four-layer architecture comprising perception, transmission, processing, and application layers. For instance, ensuring that data integrity verified at the perception layer is preserved through the transmission and securely analyzed in the processing layer will be vital. Additionally, HYShield can incorporate blockchain-based smart contracts to enforce secure interoperability rules between different ASGM domains, enabling automated verification and policy enforcement across heterogeneous infrastructures. Standardization in this area will foster a robust ecosystem to address the demands of ASGM communications in 6G networks.

Conclusion

In this article, we have presented HYShield, a novel security framework designed to protect 6G ASGM networks. Specifically, we have first analyzed the significant security challenges within ASGM networks, such as the need for secure communication and trust management across diverse layers. After reviewing existing security solutions and their limitations within 6G environments, we have proposed HYShield, a multi-layered framework integrating advanced QKD and blockchain technology to ensure robust security measures for ASGM networks. The effectiveness of this framework has been demonstrated through its defense against MitM attacks in secure drone communications. Finally, we have outlined three key research directions for further developing and applying HYShield in future 6G networks. We are certain that this article can inspire further innovations in securing 6G ASGM networks.

Acknowledgment

This work was supported in part by the Research and Development Project of China Railway Information Technology Group under Grant WJZG-CKY-2024040 (2024P01), the National Natural Science Foundation of China under Grant 62272100 and the Consulting Project of Chinese Academy of Engineering under Grant 2023-XY-09.

References

[1] X. Fang *et al.*, "Toward Physical Layer Security and Efficiency for SAGIN: A WFRFT-Based Parallel Complex-Valued Spectrum Spreading Approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, 2022, pp. 2819–29.
[2] Z. Yin *et al.*, "DT-Assisted Multi-Point Symbiotic Security in Space-Air-Ground Integrated Networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, 2023, pp. 5721–34.
[3] F. Tang *et al.*, "Blockchain-Based Trusted Traffic Offloading in Space-Air-Ground Integrated Networks: A Federated Reinforcement Learning Approach," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 12, 2022, pp. 3501–16.
[4] S. Yao *et al.*, "Toward Secure and Lightweight Access Authentication in SAGINs," *IEEE Wirel. Commun.*, vol. 27, no. 6, 2020, pp. 75–81.
[5] Y. Wang *et al.*, "Blockchain-Empowered Space-Air-Ground Integrated Networks: Opportunities, Challenges, and Solutions," *IEEE Commun. Surv. Tutorials*, vol. 24, no. 1, 2022, pp. 160–209.
[6] Y. Cai *et al.*, "Privacy-Driven Security-Aware Task Scheduling Mechanism for Space-Air-Ground Integrated Networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 5, 2024, pp. 4704–18.
[7] W. Sun *et al.*, "Collaborative Blockchain for Space-Air-Ground Integrated Networks," *IEEE Wirel. Commun.*, vol. 27, no. 6, 2020, pp. 82–89.
[8] J. Li *et al.*, "Secure and Efficient UAV Tracking in Space-Air-Ground Integrated Network," *IEEE Trans. Veh. Technol.*, vol. 72, no. 8, 2023, pp. 10,682–95.
[9] M. Xu *et al.*, "Quantum-Secured Space-Air-Ground Integrated Networks: Concept, Framework, and Case Study," *IEEE Wirel. Commun.*, vol. 30, no. 6, 2023, pp. 136–43.
[10] Q. Xu *et al.*, "Secure Federated Learning in Quantum Autonomous Vehicular Networks," *IEEE Netw.*, vol. 37, no. 6, 2023, pp. 240–47.
[11] Y. Zou *et al.*, "Cooperative Drone Communications for Space-Air-Ground Integrated Networks," *IEEE Netw.*, vol. 35, no. 5, 2021, pp. 100–06.
[12] Z. Liu *et al.*, "Establishing Trustworthy and Privacy-Preserving SAGIVNs in 6G: Architectures, Requirements, and Solutions," *IEEE Netw.*, vol. 38, no. 2, 2024, pp. 141–47.
[13] P. Zhang *et al.*, "AI-Enabled Space-Air-Ground Integrated Networks: Management and Optimization," *IEEE Netw.*, vol. 38, no. 2, 2024, pp. 186–92.
[14] D. Wang *et al.*, "Man-in-the-Middle Attacks Against Machine Learning Classifiers via Malicious Generative Models," *IEEE Trans. Dependable Secur. Comput.*, vol. 18, no. 5, 2021, pp. 2074–87.
[15] W. Zhai *et al.*, "ETD: An Efficient Time Delay Attack Detection Framework for UAV Networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, 2023, pp. 2913–28.