JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Design of a Secure Cross-Protocol Authentication and Key Agreement Framework for 5G/6G and Wi-Fi 6/7 Coexistence Networks

Braj Kishor Prasad[1*]

[1]*Assistant Professor, Department of Computer Applications (MCA), Patna Women's College (Autonomous), Patna University, Patna, India,* ***ORCID****: 0009-0003-5258-0625*

Corresponding E-mail: brajkishore.mca@patnawomenscollege.in

Abstract

The rapid convergence of wireless technologies, particularly 5G/6G cellular systems and Wi-Fi 6/7 networks, has created new challenges for ensuring secure, efficient, and uninterrupted communication in multi-protocol environments. This paper provides a secure, comprehensive framework for cross-protocol authentication and key agreement that also supports coexistence networks operating in both licensed and unlicensed spectrum bands. Security systems are essential for protection. They have often been upgraded with improved features in recent years. Modern security setups like 5G Authentication and Key Agreement (5G-AKA) and WPA3 work differently and do not resolve interoperability issues. The document depicts various separate trust models. Because the same verification techniques are repeated, they may increase the risk of a cyber-attack. The conceptual framework of the single authentication model presented here can enable trust transfer between different networks while greatly reducing delay and load. The article also discusses AI-based security capabilities such as AI-powered key agreement, responsive threat detection, and smart cohabitation management. Machine learning and deep learning are highly influential in these fields. They primarily enable earlier anomaly detection, prediction of protection actions, and resource sharing. By contrast, the proposed approach blends cryptography with the physical layer. This combination protects against typical cyberattacks such as man-in-the-middle, replay, and spoofing. In addition, it implements edge and fog computing, as well as IoT setups, to achieve both scalability and low latency in ultra-dense networks. The company also improves energy efficiency by using green energy and clean security techniques that are either fully or partially aligned with environmental protection goals in the communications sector. Although the model concept is original, it has not been demonstrated through practical examples to prove its capability. In a nutshell, this research provides a reliable platform for advancing technology that is not only innovative and secure but also environmentally responsible in future cohabitation networks.

Keywords: 5G/6G, Wi-Fi 6/7, cross-protocol authentication, key agreement, AI-driven security, coexistence networks, edge computing, IoT security, adaptive security, energy-efficient networking

1. Introduction

1.1 Background and Evolution

The wireless communication landscape has changed significantly over the past ten years. These changes are driven mostly by increased data demands, the spread of connected devices, and the rise of intelligent applications. The transition from 5G to 5G-Advanced and 6G technologies marks a major shift from communication-centric architectures to AI-native, service-oriented, and highly adaptive network ecosystems. 5G has facilitated eMBB, URLLC, and mMTC in diverse sectors. 5G-upgraded networks and 6G are set to

follow the same trajectory by offering these properties via smart automation, frequencies beyond 1 THz (one trillion vibrations per second), and ISAC (Chataut et al., 2024).

Future networks will definitely combine cellular and Wi-Fi technology. More precisely, Wi-Fi 6 and Wi-Fi 7. This ensures service is always available in licensed and unlicensed spectrum bands. The introduction of new radio in the unlicensed spectrum (NR-U) technology enables fifth-generation (5G) devices to communicate not only via Wi-Fi but also in local channels. This arrangement is essential to achieve high spectral efficiency and sustain the growing number of wireless service users. However, it also poses serious challenges in interference control, collaboration, and, most importantly, security. Non-compatible networks can address problems arising from differences in protocol stacks and fill gaps in single-protocol environments (Pons et al., 2023).

The expanding IoT ecosystem has greatly increased the number and variety of connected devices. These devices range from resource-limited sensors to powerful edge devices, each with distinct security capabilities and needs. This diversity creates security risks, as most IoT devices are highly insecure and can serve as entry points for hackers. Also, ultra-dense networks, characterized by a very large number of access points and mobile stations, make network management more difficult and make interference and fraudulent activity easier to hide (Canavese et al., 2024).

One big change is the growth of edge intelligence. That means computers and AI are put closer to the network edge. Edge computing speeds up processes, improves real-time decision-making, and enables local data processing. For security, edge intelligence enables early detection of anomalies and changes that indicate threats. But it also creates more attack surfaces, since edge nodes are now potential targets. The use of smart technology in local computing and network standards implies a need for intelligent, reliable, and secure applications that are compatible and can exchange information efficiently across protocols and network layers (Bourechak et al., 2023).

1.2 Objective

This work introduces an AI-driven authentication and key-agreement framework based on cross-protocol mechanisms for heterogeneous coexistence networks integrating 5G/6G and Wi-Fi 6/7. Newer technologies such as 5G-AKA and WPA3 are non-interoperable with existing mechanisms, resulting in fragmented trust management and security vulnerabilities in ultra-dense and highly mobile environments. The suggested framework facilitates mutual authentication, hybrid cryptography, and physical-layer key generation for resource-constrained IoT devices. AI and reinforcement learning enable intelligent threat detection, improved security, and rapid responses to cyberattacks. Combining system-layer intelligence with adaptive key management methods also improves operational efficiency. It also reduces computational power and energy use. The framework enables the fusion of AI-based security with sustainable networking principles, providing a feasible setup for secure, interoperable, scalable, and green next-generation 5G/6G–Wi-Fi 6/7 coexistence networks.

2. Current and Latest Advancements

2.1 Coexistence Network Technologies

Voice and data transmission speeds are increasing rapidly. This has led to the development of heterogeneous coexistence networks. Heterogeneous coexistence networks comprise several radio access technologies (RATs), such as 5G New Radio in Unlicensed Spectrum (NR-U) and Wi-Fi 6/7, which use the same frequency bands. The spectrum market is a very popular topic, with many people trying to use its energy not only to provide cleaner energy but also to support fast-developing wireless gadgets and apps. However, devices should be able to coexist peacefully. Traditional coexistence methods can ensure fair resource sharing, maintain security, and provide good quality of service (Sylla et al., 2022).

5G NR-U and Wi-Fi 6/7 will be the leading contributors to the convergence of network technologies. NR-U allows mobile operators with licensed spectrum to use unlicensed radio spectrum bands usually assigned to Wi-

Fi networks. Wi-Fi 6/7 transmits and receives data faster than 5G and can support more users without slowing the network down. This combination increases capacity and flexibility, but also creates coexistence challenges. These include interference management and medium access control. Wi-Fi 6 and 7 are the latest wireless standards and introduce features such as OFDMA, MU-MIMO, and MLO. These features enable better spectrum use and improve wireless network performance. However, the coordination mechanisms must be sophisticated to avoid performance degradation (Imam-Fulani et al., 2023).

One main way to improve coexistence efficiency is through Call Admission Control (CAC)-based mechanisms. CAC methods govern the admission of new traffic flows based on current resource availability and QoS specifications. By managing network load efficiently, CAC can significantly improve system performance in coexistence scenarios. A computer science study showed that CAC-dependent coexistence methods doubled wireless network throughput and increased network capacity by over 66% (Bello et al., 2024). These methods also improve resource utilization efficiency. These advantages stem from prioritizing traffic flow, reducing congestion, and ensuring equitable access to shared spectrum resources.

Techniques such as Listen-before-talk (LBT), dynamic channel selection, and adaptive power control aim to enable coexistence. These methods ensure that radio access technologies (RATs) receive zero interference while working in unlicensed bands. In addition, the growing complexity of coexistence systems demands intelligent, autonomous, and AI-driven applications that can efficiently manage the network's various and unexpected situations.

2.2 Advances in Authentication Protocols

Authentication is a main method for protecting wireless networks. 5G-AKA is the main method for user identification and key creation in fifth-generation networks. However, the system is quite slow in the coexistence scenarios in which it operates. Several detected problems likely stem from the wireless network or the authentication protocol. The main privacy risks are privacy breaches, linkability, and interoperability between networks. Linkability here means the system can be misused to track people without their knowledge or to trick them into revealing fake names that lead to further privacy breaches. In addition, 5G-AKA provides no provision for persistent authentication when combined with other technologies such as Wi-Fi, which could create a security flaw. Users would have to repeat the identification procedure each time they move between networks (Fakhouri et al., 2023). The main point is that delays in response times will not only increase but also give attackers repeated opportunities to access the system. Post-quantum cryptography (PQC) is one approach, along with physical-layer authentication and hybrid cryptographic mechanisms. These technologies aim to make protocols safe against quantum attacks while still supporting older versions. Authentication systems are evolving and becoming more adaptable.

2.3 AI-Driven Network Security (Latest Trends)

Artificial Intelligence (AI) is revolutionizing network security for next-gen wireless systems. AI-powered 6G platforms provide security features such as intrusion detection, threat prediction, reactive decision-making, and optimal resource allocation across network layers. FRL, an anti-centralized security learning methodology, safeguards participating nodes' privacy by not distributing raw data. This enables them to collaborate on cybercrime challenges as they occur. Support vector machines, random forests, and deep neural networks, which are machine learning methods in IDSs, also identify abnormal traffic and can apply the same techniques to fortify themselves against forthcoming attacks (Omheni et al., 2025). Deep neural networks like Convolutional Neural Networks (CNNs) and Long Short-Term Memory networks (LSTMs) can learn complex spatial and temporal features of network behavior. The piece discusses the benefits and drawbacks of using AI in the 6G era. The article notes that AI offers benefits, but also risks, from data and energy needs to the danger of attacks. Therefore, future studies should aim to build AI systems that are energy efficient, privacy-friendly, explainable, and resilient, and that provide security, correctness, and environmental friendliness across diverse 6G environments.

2.4 Emerging 6G Security Paradigms

The vision for 6G networks is evolving. New security paradigms are being introduced. These paradigms improve privacy and resilience. Digital twin-aided authentication simulates users, devices, network components, and communication habits in real time. It enables continuous identity authentication and anomaly detection. Blockchain also enables a distributed identity and credential system. As a result, it eliminates the need for a centralized entity and shares trust across multiple domains and protocols. In addition, terahertz (THz) communication provides extremely high data rates and low latency. This can support the most sophisticated 6G applications. Reconfigurable intelligent surfaces (RIS) improve propagation, coverage, interference suppression, and physical-layer security, thereby collectively enhancing the security, intelligence, and resiliency of 6G communication infrastructures. Consequently, integrating blockchain, RIS, THz communication, and digital twins allows smart, decentralized, relevant, resilient, and secure next-generation 6G infrastructures (Kalodanis et al., 2025).

3. Research Gaps in Coexistence Networks

The fusion of Wi-Fi and 5G NR-U, which operate in the same unlicensed radio frequency bands, is a key characteristic of next-generation wireless communication systems. Cooperation not only enables better spectrum utilization and device-dense environments, but also introduces substantial issues in security, scalability, and intelligence. Most published research focuses on improving performance metrics such as data rate, delay, and fairness; however, security and intelligent management remain underexplored. Recent research indicates that network coexistence undermines traditional assumptions about network ownership, trust, and authentication. This, in turn, creates new vulnerabilities not present in standalone systems. The following subsections describe the main research gaps in detail.

3.1 Lack of Cross-Protocol Authentication

One of the most basic limitations in networks that allow for coexistence is the lack of a single authentication framework that operates across different protocols. The current authentication methods in cellular networks (for instance, 5G-AKA) and Wi-Fi networks (such as WPA3-based authentication) operate independently and assume a closed, homogeneous network environment. In coexistence scenarios, different technologies share the same spectrum and infrastructure; thus, these assumptions no longer hold (Alhoraibi et al., 2023).

The article discusses how current systems are isolated, with authentication limited to a single protocol stack. It explains that in 5G networks, centralized core network functions usually handle authentication, whereas Wi-Fi authentication relies on access point-based mechanisms. The article explores how authentication issues affect trust. The image shows that devices working on two networks simultaneously need more confirmations, which not only slows the process but also creates more security loopholes and a higher breach risk, as various studies have found.

The lack of a shared trust framework between 5G and Wi-Fi networks creates security loopholes that foreign actors can easily exploit through the shared spectrum. These cyberattacks may include spectrum misuse, identity theft, and session hijacking. Present authentication techniques provide only partial security against such attacks. Therefore, multi-factor verification, blockchain trust, decentralized authentication, and shared identity systems become imperative for a secure and reliable network transition (Altulaihan et al., 2022).

3.2 Security Blind Spots in Coexistence

Coexistence networks are highly susceptible to threats at the physical and MAC layers because heterogeneous protocols use incompatible channel-access mechanisms. Differences between cellular and Wi-Fi technologies worsen the hidden-node conditions, interference, collisions, and denial-of-service (DoS) risks, especially in dense deployments. Limited cross-layer visibility makes the network vulnerable to multi-vector attacks across the physical, MAC, and higher layers. This problem highlights the wastefulness of the old protocol-specific defenses and the opportunity to have more integrated cross-layer security frameworks. New research should

develop tools that continuously monitor diverse environments, rapidly detect coordinated threats, and adjust protection settings across the physical, MAC, and network layers (Parveen et al., 2025).

3.3 Absence of AI-Integrated Key Agreement

The absence of an AI key-agreement process in heterogeneous coexistence networks creates major challenges. Traditional protocols, such as 5G-AKA, are mostly rule-based, reactive, and designed for specific network conditions. In other words, they are less adaptable to dynamic environments of mobility, interference, and adverse traffic situations. Besides, current key-agreement schemes may still be susceptible to replay and identity-confusion attacks; they may not offer sufficient forward secrecy and can add delay during continuous cellular–Wi-Fi switching. AI-enabled key management offers a promising alternative by exploiting network and contextual information to support predictive key generation, adaptive cryptographic configuration, and proactive threat mitigation (Chow and Ma, 2022). However, research has yet to integrate intelligent, context-aware key management with robust cryptographic mechanisms. Future studies should therefore develop adaptive AI–cryptographic frameworks that jointly optimize security, latency, interoperability, computational efficiency, and resilience against evolving and quantum-enabled threats in next-generation coexistence networks

3.4 Limited Use of AI for Cross-Layer Security

AI has been used significantly in wireless networks, but its application in coexistence security remains limited and uncoordinated. The present studies largely focus on using AI for intrusion detection and traffic prediction and, as a result, address only isolated parts of network security.

These applications are useful, but they do not address the main problem of cross-layer security orchestration. Networks enable different entities to coexist and rely on complex interconnections across layers such as the physical, MAC, network, and application layers. Security threats typically span multiple layers, so a coordinated response is necessary. This is only possible with AI models that are not isolated (Mustafa et al., 2025).

For example, a cyberattack can target the physical layer by jamming signals, then spread to the MAC layer by exploiting collisions and affect upper-layer services. This is similar to data exfiltration. Standard AI-based intrusion detection systems lack the capabilities to efficiently track these interlayer dependencies, resulting in slower or partial responses.

A study showed that AI-based security frameworks across layers are highly effective. The research also showed that these frameworks suit technologies such as Software-Defined Networking (SDN) and Network Function Virtualization (NFV). The frameworks provide centralized control and real-time adaptation, allowing AI to manage security policies across layers. But these approaches are new, and little evidence shows they work in coexistence.

Another downside is the lack of end-to-end security orchestration in which AI can manage authentication, key agreement, access control, and anomaly detection across the entire network. Systems today often run independently, with many AI models given different jobs, leading to uncoordinated security.

Future research should focus on designing AI-powered security systems that provide an all-inclusive, connected shield for networks composed of collaborating technologies. This likely involves learning algorithms, edge computing, and seamless interaction among multi-layered network components.

3.5 Scalability and Latency Issues

Scalability and latency problems in heterogeneous coexistence networks have become more critical in ultra-dense IoT and upcoming 6G environments. The large number of devices increases interference, traffic, and spectrum competition. In addition, frequent switching between cellular and Wi-Fi causes more reauthentication and resource-allocation delays due to additional handovers. These problems require lightweight security protocols, AI-enabled resource management, predicted handovers, spectrum distribution, and edge computing to improve security, trust, scalability, and response speed (Saoud et al., 2025).

3.6 Lack of Energy- and Pollution-Aware Security Models

Security research for coexistence networks must also consider energy efficiency and environmental sustainability. AI, cryptographic transactions, and infrastructure can increase energy consumption, operational costs, and carbon emissions. This issue is especially prominent in IoT and 6G environments. Emerging green-security models will likely adopt techniques such as lightweight cryptography, energy-efficient AI, adaptive security, intelligent resource management, and pollution-aware networking to enable safe, reliable, scalable, and sustainable communications (Elkhodr, 2025).

4. System Model and Design Requirements

Wireless technology is changing rapidly, with the latest systems becoming more heterogeneous, intelligent, and ultra-dense, which in turn require comprehensive system models and design requirements to perform effectively. Using unlicensed frequencies for coexistence between 5G/6G and Wi-Fi 6/7 cellular networks creates complex interactions among network entities. Effective architectures should support massive connectivity, URLLC, dynamic spectrum sharing, multi-RAT integration, edge intelligence, IoT connectivity, scalability, performance, resilience, and quantum-resistant security.

4.1 Network Model

The introduced multi-RAT coexistence architecture unites 5G/6G, Wi-Fi 6/7, edge/fog computing, and diverse IoT devices in a single ecosystem. It improves spectrum utilization, coverage, service continuity, and quality of service. The architecture is designed to resolve interoperability and security issues. The proposed plan includes centralized authentication, AI-based decisions, improved Wi-Fi technologies, edge intelligence, intrusion detection, dynamic spectrum allocation, hierarchical management, scalability, and trustworthy cross-layer communication.

4.2 Threat Model

Spectrum sharing in heterogeneous coexistence networks exponentially extends the attack surface and creates onerous security challenges. Eavesdropping certainly breaks confidentiality by secretly listening to wireless communications. This could result in the theft of passwords, user information, and control commands. Malicious activities such as man-in-the-middle (MITM) attacks, together with denial-of-service (DoS) and impersonation, can potentially violate the four security properties of authentication, integrity, availability, and confidentiality, as well as network operations. DoS attacks can exploit wireless channel contention and collision mechanisms; in addition, different radio access technologies (RATs) make both detection and mitigation harder. Spoofing involves untrustworthy parties co-opted into the attackers' scheme, masquerading their devices as those of legitimate users to gain unauthorized access to communications. Cross-protocol attacks exploit vulnerabilities across different protocols, allowing attackers to circumvent security features and move across network layers. That is why coexistence networks must have interoperable authentication, continuous encryption, key management, cross-layer threat detection, coordinated security mechanisms, and rapid incident response. This ensures that communications remain trustworthy.

4.3 Design Requirements

Coexistence networks must meet stringent requirements for performance, security, scalability, resilience, and sustainability in changing wireless networks. Ultra-low latency of 1 ms is essential for latency-sensitive applications such as autonomous vehicles, remote work, and virtual or augmented reality. However, multi-RAT coordination, handovers, heterogeneous technologies, and security procedures can introduce delays. Therefore, efficient protocols, smart resource management, and edge computing are required. Resilience involves not only fixing errors and adding extra capacity but also enabling efficient communication, rapid recovery from cyberattacks, and mitigation of interference, congestion, and failures. Scalability enables connecting many IoT devices without compromising performance or security. These objectives can be achieved through methods such as dynamic spectrum allocation, load balancing, distributed processing, and decentralized decision-making.

Quantum computers will need security that they cannot break, since they can break widely used RSA and ECC cryptography. Hence, lattice-, hash-, and code-based schemes, along with other post-quantum cryptography, are the only necessary solutions. Eco-friendly operations are also more straightforward because they are lightweight. They can also support low-energy communication, distribute energy to resources efficiently, and use AI-based changes that consume less energy while maintaining secure and trustworthy communications.

5. Methodology

5.1 Overview of Proposed Framework

The paper outlines an AI-driven framework for cross-protocol authentication and key agreement, primarily for heterogeneous coexistence networks that merge 5G/6G and Wi-Fi 6/7 technologies. It notes that ultra-dense deployments, edge computing, and unlicensed spectrum access are not only revitalizing wireless networks but also creating severe cross-protocol security issues. Traditional methods such as 5G-AKA and WPA3 remain protocol-centric. As a result, they limit trust between networks and leave coexistence environments vulnerable. The framework integrates trust administration, AI-enabled verification, and a mix of cryptographic and physical-layer key production. The AI unit continuously monitors user activity. Trust degrees vary with conduct, and entry is conditional on those levels. A channel-oriented, flexible key scheme is another cryptographic technique that depends on AI-generated keys based on predictions. Reinforcement learning supports the distribution of authentication and security functions, improving protection and reducing response time; however, it also increases energy consumption.

The network may also be defined for formalization in this way:

$$\mathcal{N} = \{U_i, B_j, A_k, E_l\} \quad (1)$$

where U_i represents user devices, B_j denotes 5G/6G base stations, A_k corresponds to Wi-Fi access points, and E_l captures edge computing nodes. The architecture described here is a network plan with numerous interconnected, dynamic, and context-aware elements that collaborate to ensure secure, energy-efficient, and intelligent wireless coexistence. The system's AI engine uses time and context features from device interactions to perform authentication, key agreement, and intrusion detection. The collaboration of AI and safety technology, along with encryption and the physical layer, enables a security model that is predictive, adaptable, and energy-efficient in networks with different, coexisting devices.

5.2 System Model

5.2.1 Channel and Feature Model

The system model captures device behavior across **three key network layers: physical (PHY), MAC, and network (NET)**. Each device U_i generates a feature set:

$$F_i = \{F_i^{PHY}, F_i^{MAC}, F_i^{NET}\} \quad (2)$$

where F_i^{PHY} represents physical-layer features, including received signal strength indicator (RSSI), channel state information (CSI), and multipath characteristics. Frame inter-arrival delays, retransmission rates, and collision statistics are examples of MAC-layer behavior that are captured by F_i^{MAC} and represent device access patterns. Network-layer metrics, such as traffic volume, flow distribution, and routing behavior, are represented by F_I^{NET} and provide information about higher-level communication patterns.

These multi-stage properties are merged to create a time-sequence observation vector.

$$X_i(t) = [x_1, x_2, \dots, x_n] \quad (3)$$

The paper describes that the vector is employed in a machine learning-driven authentication process. The vector represents the device's current state and history. This information enables the system to detect abnormalities that may signal a security breach, leading to better decision-making. The AI model uses PHY, MAC, and NET features from the device layers to detect changes. This provides secure login access across various locations.

5.3 AI-Based Authentication Model

5.3.1 Trust Score Function

Authentication is modeled as a **binary classification problem**, where each device is given a trust score. T_i reflecting its authenticity:

$$T_i = \sigma(W^T X_i + b) \quad (4)$$

The sigmoid activation function is where cap W is the weight vector learned from historical training data, and cap b is a bias term. The trust score $T_i \in [0,1]$ is compared against an authentication threshold θ. Devices with $T_i \geq \theta$ are granted access, while those below the threshold are rejected. The system is evaluated in a mix of devices. They have a good past, and now they work well. This is done without relying on static identification.

The AI Trust model is an innovative idea that is not limited to any specific software stack and can be implemented across multiple stacks. Besides, it can also detect good behavior in social networks such as 5G, 6G, or Wi-Fi. The network model uses multi-layered entities that span various devices and protocols, allowing access through a single login. Moreover, the system can adjust parameters such as weights and biases based on network conditions, ensuring it works smoothly even in congested networks with constant changes.

5.3.2 LSTM-Based Temporal Behavior Analysis

The system employs LSTM (Long Short-Term Memory) networks to trace temporal connections in device operation. The LSTM's hidden state (h_t) at time (t) is computed as follows:

$$h_t = \text{LSTM}(X_t, h_{t-1}) \quad (5)$$

The dependency diagram is then virtualized after obtaining the hidden state.

$$T_i = \sigma(W_h h_t + b_h) \quad (6)$$

Temporal modeling is important for research on human movements, network traffic stability, and changes in people's behavior. For example, a piece of equipment may suddenly experience a significant traffic spike or show unexpected PHY/MAC patterns. This could indicate a threat. The LSTM-based system can distinguish normal changes (such as normal behavior) from malicious activity; thus, detection is not limited to static classification.

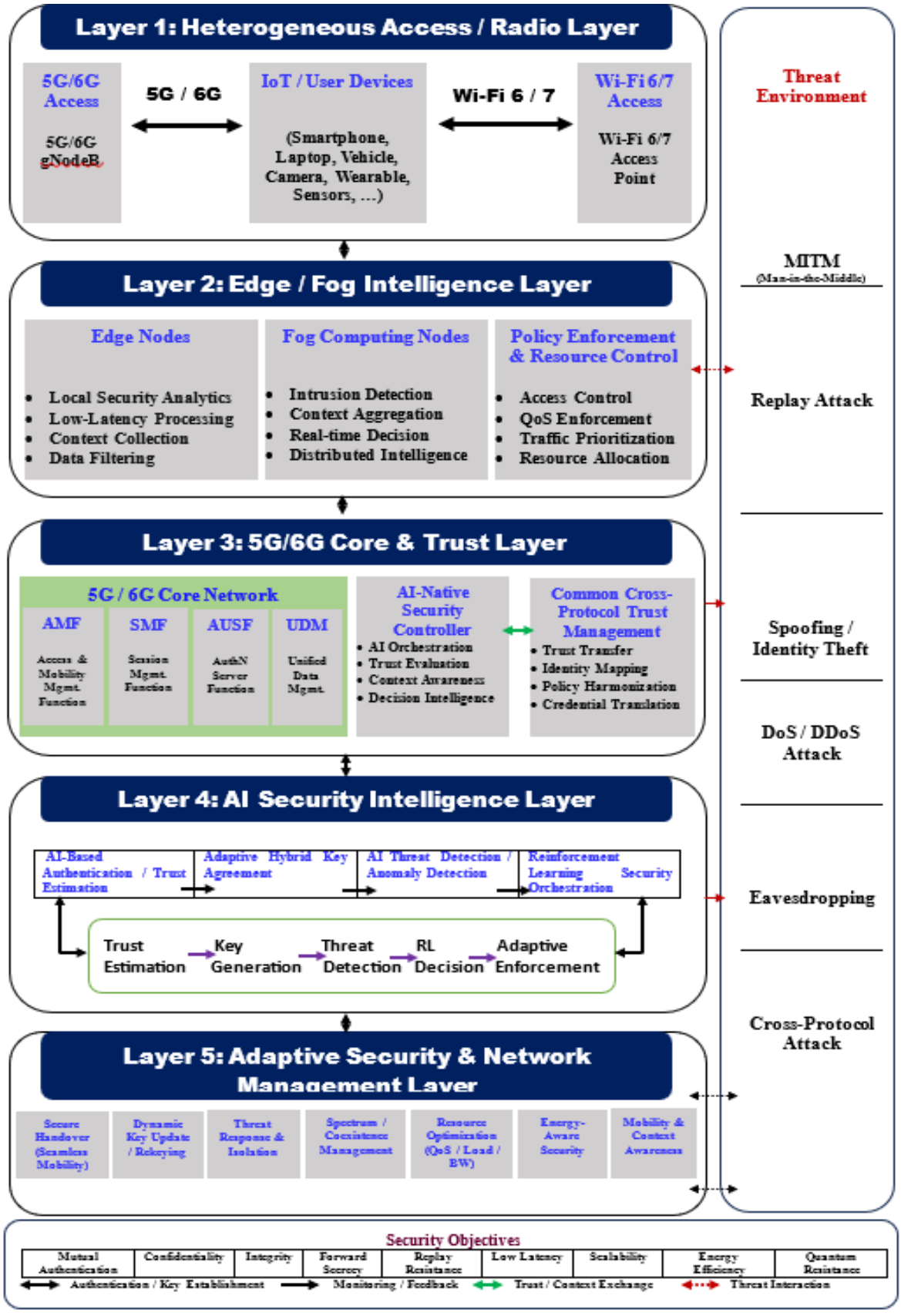


Figure 1: Proposed AI-Driven Cross-Protocol Authentication and Key Agreement Framework for 5G/6G – Wi-Fi 6/7 Coexistence Networks

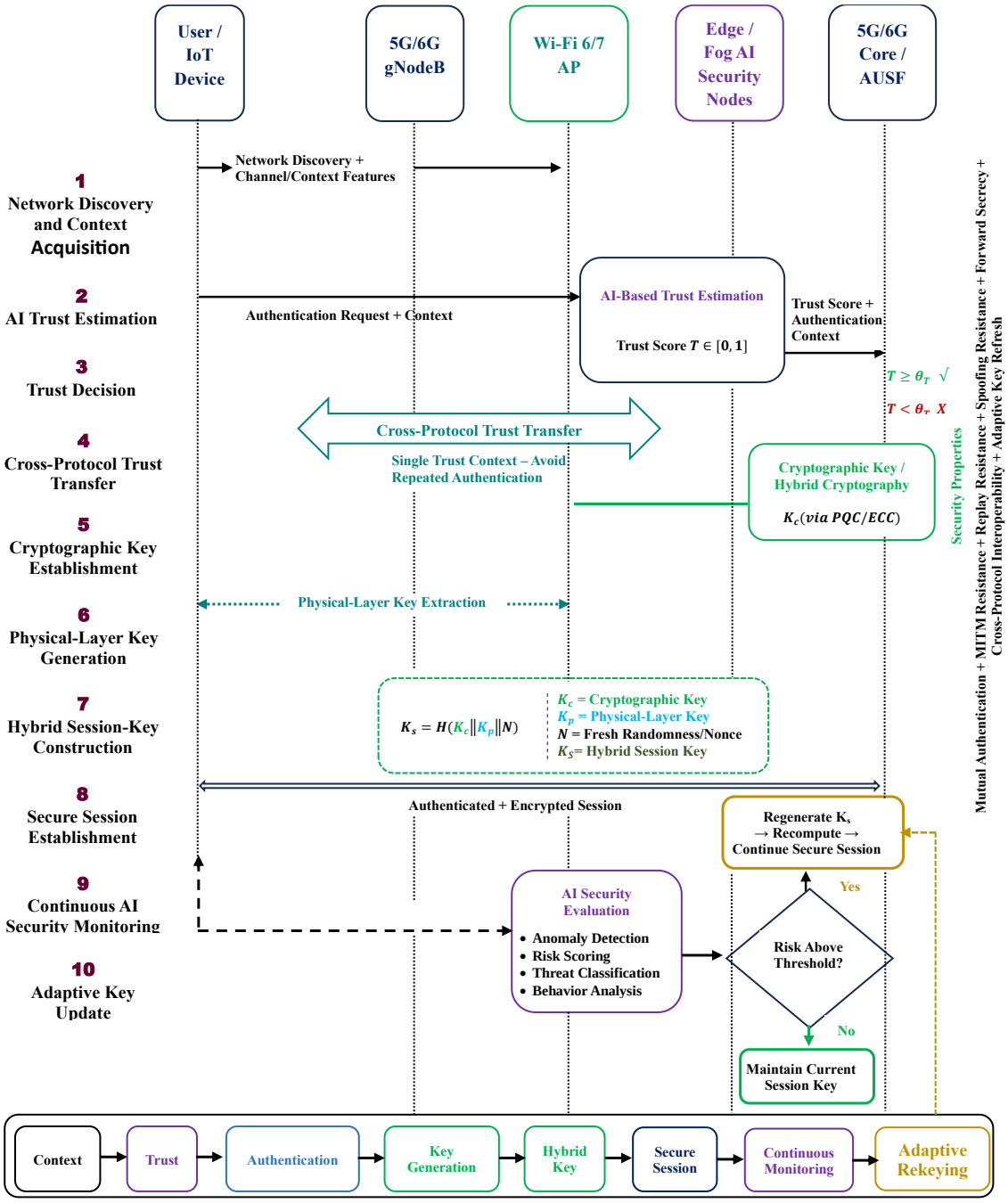


Figure 2: Cross-Protocol Authentication Domain

5.4 Cross-Protocol Key Agreement Model

5.4.1 Hybrid Key Generation

Session keys K_s are derived using a **hybrid approach**, combining cryptographic and physical-layer components:

$$K_s = H(K_c \parallel K_p \parallel R) \tag{7}$$

Here, K_c is a cryptographic key (e.g., ECC or post-quantum key), K_p is a physical-layer key generated from channel characteristics, R is a random nonce, and $H(\cdot)$ is a secure hash function. This combination safeguards

not only against eavesdropping during transmission but also against unauthorized data duplication and attacks from highly computationally powered adversaries, such as those using quantum computers.

5.4.2 Physical-Layer Key Extraction

The physical-layer key K_p is extracted using **channel reciprocity** between communicating nodes:

$$K_p = Q(CSI_{ij}) \tag{8}$$

where CSI_{ij} represents the channel state information between nodes i and j, and $Q(\cdot)$. This quantization function converts analog channel measurements into digital key bits. The entropy of the key is calculated as $H(K_p) = -\sum p(k)\log p(k)$. It offers a significant amount of randomness and uncertainty. The method exploits the natural randomness of wireless channels; therefore, it ensures secure key generation against eavesdropping or duplication by hackers.

5.4.3 AI-Based Key Adaptation

The system employs an innovative AI-based key adaptation technique to keep security dynamic. The probability of an attack P_{attack} is estimated to help decide if a session key should be changed:

$$K_{update} = \begin{cases} 1, & \text{if } P_{attack} > \alpha \\ 0, & \text{otherwise} \end{cases} \tag{9}$$

Firstly, α is a limit chosen to match security and power usage. The system uses AI models trained on a multi-layer data network to identify unauthorized access. In addition to enabling quick key changes, it also ensures key safety to enhance overall security.

5.5 Intrusion Detection Model

5.5.1 Supervised Learning-Based Detection

The framework uses supervised learning classifiers to identify hostile actions. The output for a specified feature vector X is:

$$y = f(X) = \arg\max P(y \mid X) \tag{10}$$

where $y \in$ {normal, attack}. The loss function is established as follows:

$$\mathcal{L} = -\sum y \log(\hat{y}) \tag{11}$$

In this method, the system determines whether traffic is good or bad using labeled training data that includes not only normal traffic but also anomalies resulting from cross-protocol interactions.

5.5.2 Autoencoder-Based Anomaly Detection

An autoencoder is a neural network technique commonly used for unsupervised learning tasks such as anomaly detection. The reconstruction error $E = \left\|X - \hat{X}\right\|^2$ is then compared to a threshold δ to find deviations from usual behavior. This method works well for new attacks the system wasn't trained on. It makes the framework stronger against attacks that it can't identify.

5.6 Traffic Prediction Model

LSTM and Transformer networks can predict traffic patterns. These networks can also identify similarities and interrelationships among protocols.

$$\hat{X}_{t+1} = f(X_t, X_{t-1}, \ldots, X_{t-n}) \tag{12}$$

Prediction loss:

$$\mathcal{L}_{pred} = || X_{t+1} - \hat{X}_{t+1} ||^2 \quad (13)$$

The system also enables proactive steps before security measures become necessary. Security measures involve several steps such as changing keys before the scheduled time, allocating resources, and removing anomalies. With traffic prediction, the system ensures continuous service quality without any interruption while also improving security.

5.7 Reinforcement Learning-Based Security Optimization

5.7.1 Markov Decision Process (MDP)

We formulate security optimization as an MDP. $(\mathcal{S}, \mathcal{A}, P, R, \gamma)$, where $\mathcal{S}$ represents network states, $\mathcal{A}$ denotes possible actions (authentication levels, key updates), P is the state transition probability, R is the reward function, and $\gamma$is the discount factor.

5.7.2 Reward Function

The reward function balances three major factors: security, latency, and energy.

$$R = \lambda_1 S_{sec} + \lambda_2 S_{lat} + \lambda_3 S_{energy} \quad (14)$$

where S_{sec} is the security score, S_{lat} measures latency performance, and S_{energy} quantifies energy efficiency. Weight parameters λ_i are tuned according to network priorities.

5.7.3 Q-Learning Update

The Q-learning update is defined as:

$$Q(s,a) \leftarrow Q(s,a) + \eta[R + \gamma \max Q(s',a') - Q(s,a)] \quad (15)$$

The system learns the best possible methods for authorizing users, managing security keys, and preventing or handling intrusions through trial and error or pattern recognition over time.

5.8 Cross-Protocol Coordination Model

5.8.1 Spectrum Allocation Optimization

Cross-protocol coordination optimizes spectrum allocation for maximum throughput.

$$\max \sum_i R_i \text{ s.t.} \sum B_i \leq B_{total} \quad (16)$$

where R_i is the throughput of the device i and B_i the bandwidth allocated. This ensures **efficient coexistence of 5G/6G and Wi-Fi 6/7**.

5.8.2 Interference Management

Interference is modeled as:

$$I = \sum P_j G_{ij} \quad (17)$$

with P_j representing transmission power and G_{ij} the channel gain. The system can adjust power and channels without human intervention, helping it minimize interference from other protocols and improve security and quality of service.

5.9 Energy and Pollution-Aware Optimization

The process has energy and environmental characteristics. It involves determining the total power used:

$$E = \sum P_i \cdot t_i \quad (18)$$

and the linked carbon expense:

$$C = \beta E \quad (19)$$

Optimization reduces the value of $E + C$, improving the security framework by making it sustainable and environmentally friendly. This is consistent with the latest goals of green 6G networks.

5.10 Algorithm Summary (Pseudo-Steps)

The primary structure operates in this way:

1. Collect device feature vectors X_i.
2. Compute trust scores T_i via an AI-based authentication engine.
3. Reject devices with $T_i < \theta$ accept others.
4. Extract physical-layer key $K_p$and cryptographic key K_c.
5. Generate session key $K_s = H(K_c \parallel K_p \parallel R)$.
6. Run AI-based intrusion detection.
7. Predict attack probability P_{attack}.
8. Update keys if $P_{attack} > \alpha$.
9. Improve security procedures by using orchestration from the reinforcement learning field.
10. Take advantage of cross-protocol collaboration and execute energy-efficient operations.

This method is fast, adaptable, secure, and environmentally responsible for verification and key handling in 5G/6G and Wi-Fi 6/7 interworking networks. This section addresses the problems listed in Section 3.

6. Mathematical Modeling and Algorithms

The article discusses the difficulties of creating networks that are safe, high quality, and able to coexist. Such networks require mathematical models and algorithmic constructs that can adapt to various conditions. In multi-RAT systems, the main rule-based approach is to mix 5G/6G and Wi-Fi technologies, but the biggest flaw is that these methods still lack reliable authentication. The piece supports the idea that efficient models using probabilistic reasoning, information theory, and AI can help solve issues in cross-protocol interactions, channel features, and cybercrimes. Furthermore, the article discusses the main elements of a smart network, such as authentication, key agreement, and AI-noisy optimization models for a safe network.

6.1 Authentication Model

Authentication in coexistence networks requires more than just identity confirmation. They note that authentication should also involve context-aware, behavior-based trust evaluation. This suggests that the wide variety of devices and protocols make fixed or static authentication plans unsuitable for maintaining trust. The authors have already introduced a model that uses a trust score to represent the system's confidence in the honesty of entities in the network, based on their behavior patterns and channel features.

The Trust Score Function merges behavioral observations with the physical-layer channel characteristics. Behavior features comprise packet transmission patterns, session duration, mobility behavior, and historical interaction records. These traits not only mirror the equipment's normal behavior but can also signal potential hacking attempts. For example, a sudden surge in packets sent or a strange change in mobility patterns could indicate a computer infected with malware or being used without authorization.

The device utilizes channel-based features, such as signal strength, channel state information, and signal-to-noise ratio, in addition to behavioral features. These physical-layer properties are generally challenging to imitate and, if so, can reliably indicate device identity. The trust model combines behavioral and channel features to better resist spoofing and impersonation attacks.

Conceptually, the trust score T_i for a device i can be represented as a weighted function of these characteristics, with weights that are dynamically modified according to danger levels and network conditions:

$$T_i = \alpha \cdot B_i + \beta \cdot C_i \quad (20)$$

$$T_i = \alpha B_i + \beta C_i \quad (21)$$

Here, B_i represents the aggregated behavioral score, C_i denotes the channel-based score, and α, β are adaptive weighting factors such that $\alpha + \beta = 1$. Changing weights allow the system to focus on features best suited to the environment. In a fast-moving place, channel features may receive more weight. In a quiet place, the focus could shift to behavior features.

Machine learning finds and verifies usual patterns, then it spots unexpected ones. The trust score changes continuously, allowing the system to monitor the user longer and avoid relying on a single verification. If the trust score falls below the threshold, the system sends it for re-verification or disables it.

The model also facilitates cross-protocol authentication. Trust scores transfer to and are validated across different RATs. This also applies to coexistence environments, allowing secure access without any interference. The reduced response time strongly improves security and is a key benefit. In addition, using trust scores with blockchain or distributed ledger technologies can increase transparency and make interruptions almost impossible, further improving security.

A trust score-based authentication model provides a strong foundation for an adjustable and flexible wireless sensor network. Furthermore, the model fits the needs of such networks, as it can address issues caused by traditional authentication methods.

6.2 Key Agreement Model

Secure key agreement is essential for protecting communication in networks where various systems cooperate. Classical key exchange protocols, although good in uniform environments, struggle in diverse and changing scenarios. The entropy-based key generation model was proposed to find new energy-efficient sensing methods in wireless sensor networks (WSNs). The model utilizes the inherent randomness of wireless channels and device interactions to generate secure cryptographic keys.

An entropy-based method exploits physical-layer randomness to generate secret keys. The method uses fluctuations in the communication path and noise as random inputs, which it then converts into secret keys. Because wireless channels are reciprocal and time-varying, even the same devices can generate identical keys without any coordination by monitoring the same channel features. Therefore, this method not only eliminates the need for direct key exchange but also reduces the risk of eavesdropping and unauthorized replay.

The entropy of a secret code is directly related to its security level. Normally, key entropy is determined by Shannon entropy in information theory.

$$.H(K) = -\sum_i p(k_i)\log p(k_i) \quad (22)$$

$$H(K) = -\sum_i p(k_i)\log p(k_i) \quad (23)$$

The key $p(k_i)$ represents the probability distribution of key bits. Higher entropy means greater unpredictability and, as a result, a higher risk of brute-force attacks. Hence, the need for security measures is also high. Key generation remains important and requires substantial random input. Additionally, it can use different random sources for additional confirmation, such as channel noise, variations in movement patterns, and changes in the surroundings.

To further enhance security, the key agreement protocol allows participants to reconcile their information and apply privacy amplification techniques. Information reconciliation allows the two users to obtain the same keys despite measurement differences, and privacy amplification mitigates eavesdropping risk.

The security of this key agreement protocol could be analyzed rigorously using Burrows–Abadi–Needham (BAN) logic. BAN logic is the most popular framework for confirming authentication and key exchange protocols. BAN logic formally checks features such as authentication, key freshness, and secrecy by representing the beliefs and assumptions of the communicating entities. Through these beliefs and assumptions, BAN logic confirms that the protocol fulfills the required security properties.

In coexistence networks, the key agreement protocol must also support interoperability across protocols. This means the system ensures secure communication between devices even if they use different radio access technologies (RATs). To do this, the system needs some changes to the existing cryptography-based anonymization methods. The system also requires conventional interfaces and protocols that let it use multiple encryption techniques.

Quantum computing could break many cryptographic methods in use today, raising concerns about the security of our digital systems. Post-quantum cryptographic methods are designed to be secure even against quantum computers. Such a key-generation process, relying on random fuzziness and quantum-safe codes, offers a trustworthy and green security alternative.

Entropy-dependent key agreement systems are a smart, trustworthy way to manage keys in networks of connected devices. This approach not only addresses the limitations of classic protocols but also strengthens the network's security against advanced attacks.

6.3 AI Optimization Model

Coexisting systems create complex networks, so AI-driven dynamic optimization is important to help the system adapt to changing environments and balance multiple goals. RL (Reinforcement Learning) is a good option because it enables the system to learn optimal policies through interaction with the environment.

The article depicts the network as a community and the decision-making facet as a human character. The individual is further characterized as a network resource; the user is not merely a resource consumer but also an identity confirmer and a security settings adjuster according to the network environment.

The objective is to create a reward that includes key indicators such as safety, time, and energy savings.

The reward function aggregates these parameters into a single score.

$$R = w_1 S + w_2(1/L) + w_3(1/E) \quad (24)$$

$$R = w_1 S + w_2 \frac{1}{L} + w_3 \frac{1}{E} \quad (25)$$

where S represents the security level, L denotes latency, E is energy consumption, and w_1, w_2, w_3 are weighting factors reflecting the relative importance of each metric. The inverse relationship between latency and energy guarantees that lower numbers are linked to greater rewards.

The security property, S, is determined from trust values and the threat-detection factors. The network performance data provide information on delay (L) and power (E). The RL agent adjusts the incentive function to reconcile the conflicting objectives and improve system efficiency.

This class is a great way to try different methods and improve the plan through feedback. DRL is a huge step forward from RL because it combines neural networks. It lets RL process high-dimensional data and handle complex tasks in challenging situations. Neural networks act as function approximators that estimate value functions and policies, and they train faster.

The primary advantage of AI optimization models is their ability to adapt quickly, creating a ripple effect across the system. The RL agent continuously adjusts its plans by monitoring the environment and verifying system performance to identify errors and ensure safety and reliability. This characteristic is very important in coexistence networks, where, for example, user mobility, interference, and traffic patterns can change very quickly.

Moreover, the model supports cross-layer optimization. This means the agent can account for relationships between different network layers. The MAC layer is a network layer. A choice made at the MAC layer can influence the performance and security of the network layer. The RL (Reinforcement Learning) agent can find novel ways to improve these interactions collectively.

Spreading the AI model across the edge, fog, and core is a smart way to scale it up. These units can also connect using federated learning. They exchange knowledge instead of data. This not only ensures privacy but also significantly reduces communication traffic.

XAI methods can demonstrate a system and explain its functions, enabling network engineers to understand the system more thoroughly and trust its decisions.

7. Performance Evaluation and Results

AI coevolution with multi-radio access technology (multi-RAT) networks, simulated to reflect real-world network conditions, marks a new era of AI coexistence. The work shows that different network infrastructures can significantly affect reaction time, data transfer rate, reliability, security, power consumption, and interoperability. The suggested framework is the most efficient approach for overlapping networks, especially in traffic-heavy and changing conditions.

7.1 Simulation Environment

The structure is developed on a system that emulates a diverse network across various radio access technologies (RATs). Initially, the system only copies cellular and Wi-Fi communication. This mirrors real-world scenarios where different technologies compete for the same spectrum resources.

Tools Used

In the simulation framework, a mixture of traditional industry tools helps achieve accuracy and repeatability.

- The NS-3 laboratory kit makes it possible to carry out in-depth experiments on signals, noise levels, and network protocols. The equipment supports 5G and Wi-Fi components, enabling investigations that involve both technologies.
- MATLAB is a program that helps people create and experiment with AI models. The models are good for signal processing. The app also lets users quickly remove features and perform signal processing.
- Python, with libraries like TensorFlow or PyTorch, remains the most popular choice for creating machine learning models such as autoencoders and LSTM networks. These are the main components of the new security and optimization system.
-

AI-powered consciousness is not the same as network-level events.

Network Configuration

The simulated setup is well-suited to demonstrating a practical, extensible network scenario. Table 1 briefly outlines the configuration.

Table 1: Network Configuration Parameters

Parameter	Value
Network Area	1000 m × 1000 m
Number of Devices	100–1000 IoT nodes
5G Base Stations	3–5
Wi-Fi 6/7 APs	5–10
Frequency Bands	Sub-6 GHz + mmWave
Mobility Model	Random Waypoint
Traffic Type	Mixed (IoT + Video + URLLC)

The system's versatile traffic types enable experiments to assess its effectiveness under multiple conditions. This comprises low-latency, high-bandwidth, and low-power Internet of Things (IoT) communications. Moreover, implementing sub-6 GHz and mmWave frequencies is orthogonal to real 5G/6G installations.

Compared Schemes

We evaluate the framework's efficiency by comparing it with the following schemes.

- Baseline **5G-AKA authentication protocol**
- Traditional **Wi-Fi authentication mechanisms**
- **AI-based Intrusion Detection System (IDS)** without cross-protocol integration
- **Proposed AI Cross-Protocol Framework**

These comparisons underscore the advantage of using AI and working together through layers.

7.2 Performance Metrics

The evaluation considers numerous indicators of effectiveness, which gauge different aspects of the network's performance and its security:

- **Authentication Latency (T_auth):** Time required to complete authentication.
- **Throughput (R):** Rate of successful data delivery.
- **Packet Delivery Ratio (PDR):** Determining the reliability of data packet transmission.
- **Energy Consumption (E):** The overall energy consumed by computer networking actions.
- **Attack Detection Accuracy (A_d):** Effectiveness of Security Techniques.
- **Key Agreement Overhead:** The key generation process causes further delays.

These parameters provide a comprehensive review of the network.

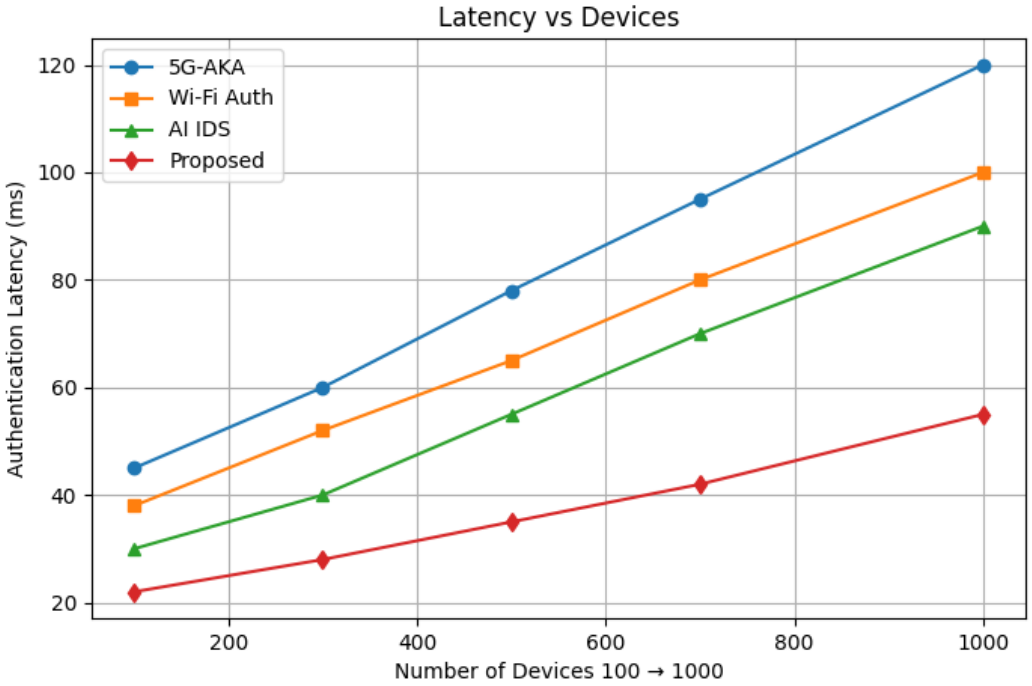
7.3 Results and Analysis

7.3.1 Authentication Latency

Authentication latency is defined as:

$$T_{auth} = T_{proc} + T_{comm} \quad (26)$$

where T_{proc} is a processing delay and T_{comm} is a communication delay.



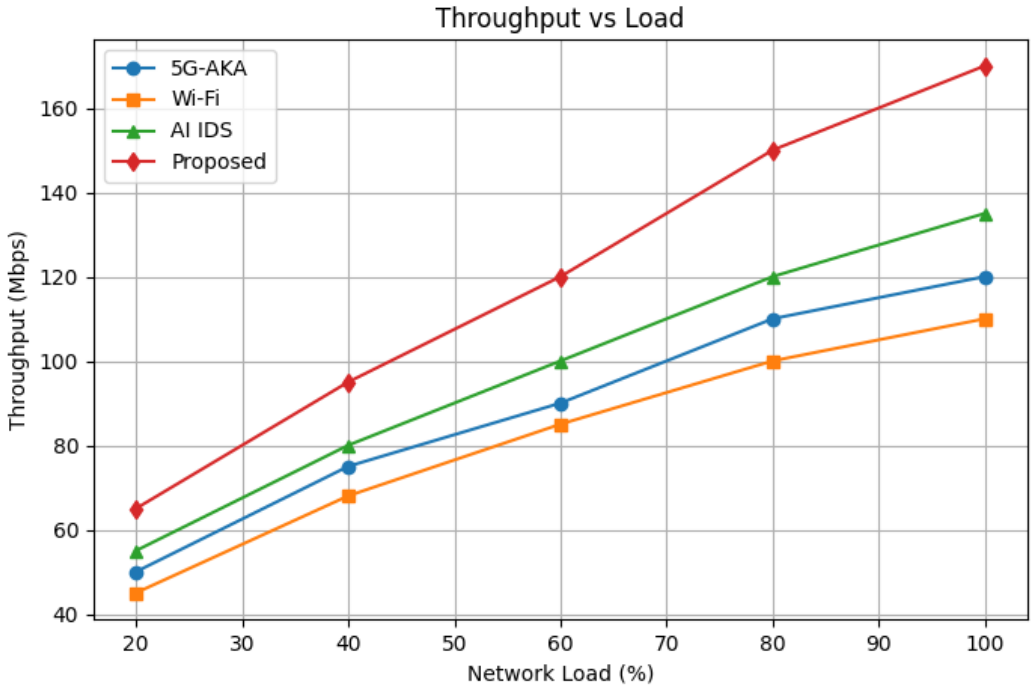
The new system is much faster than the old approach, cutting the time usually required to verify a user by nearly half. The main reason is that AI works at the edge, which drastically reduces the data sent to the central servers. Moreover, the system enables instant verification decisions, reducing both processing and transmission time.

The dual-mode authentication scheme is more effective and reduces extra sign-ins caused by switching between 5G and Wi-Fi. It not only reuses authentication data, reducing workload and improving efficiency, but also fits well in areas with frequent, rapid movement.

7.3.2 Throughput Performance

Throughput is calculated as:

$$R = \frac{\sum \text{Successful Data Delivery}}{\text{Time}} \quad (27)$$



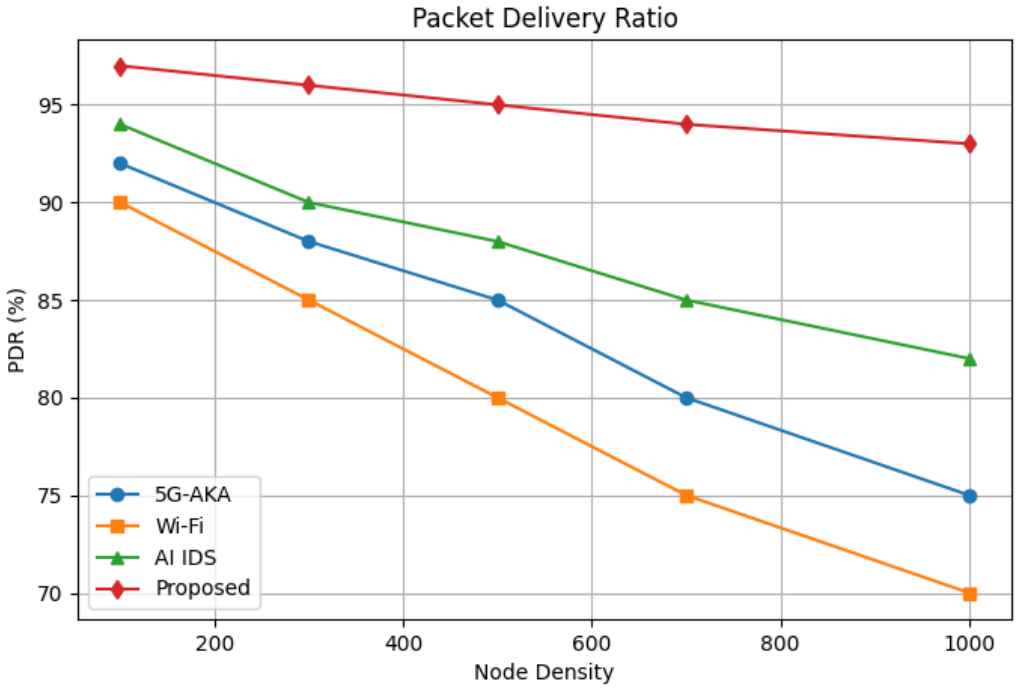
The suggested system achieves a throughput increase of 25- 40% over traditional methods. The gain is attributed to various reasons:

- Reduced retransmissions resulting from increased link reliability and interference management.
- Efficient spectrum coordination between 5G and Wi-Fi networks has enabled the reduction of collisions by removing interference caused by overlapping signals.
- An intelligent resource allocator based on AI that smartly taps the channel by adjusting the channel usage dynamically for efficient channel utilization.

These improvements also increase data transmission speeds and enable more efficient network use.

7.3.3 Packet Delivery Ratio (PDR)

$$PDR = \frac{P_{received}}{P_{sent}} \quad (28)$$



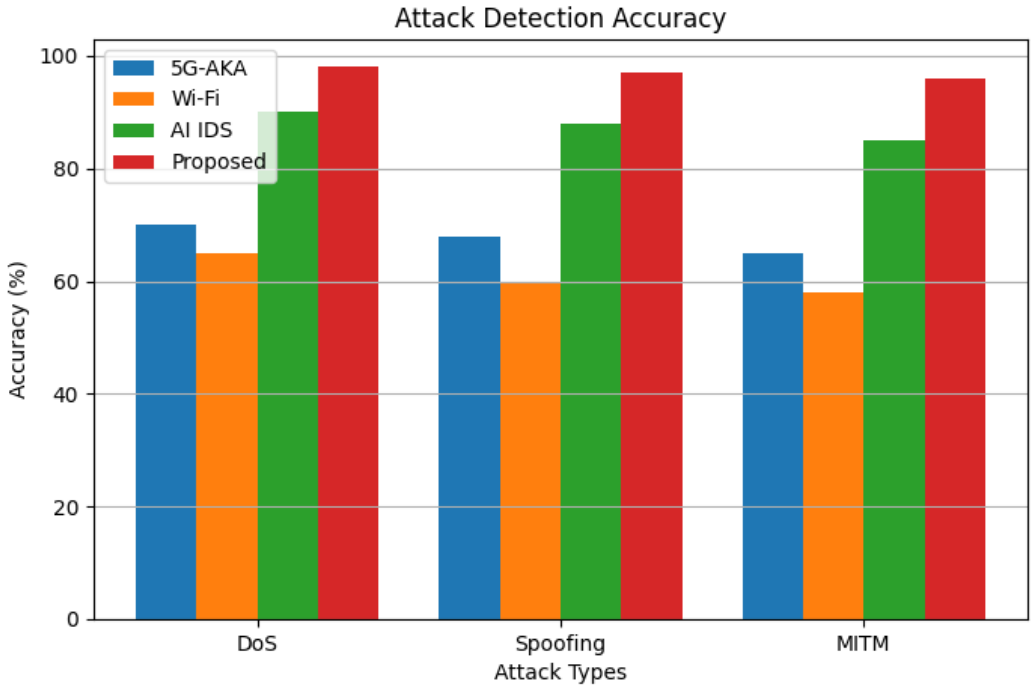
The PDR of the configuration's packets is around 95-98%, which is far superior to simple methods, particularly in situations with heavy interference. The better PDR is due to:

- Adaptive retransmission strategies
- Improved channel selection
- Anomaly detection using AI prevents hackers from corrupting network packets.

High reliability is critical for mission-critical applications.

7.3.4 Attack Detection Accuracy

$$A_d = \frac{TP+TN}{TP+TN+FP+FN} \quad (29)$$



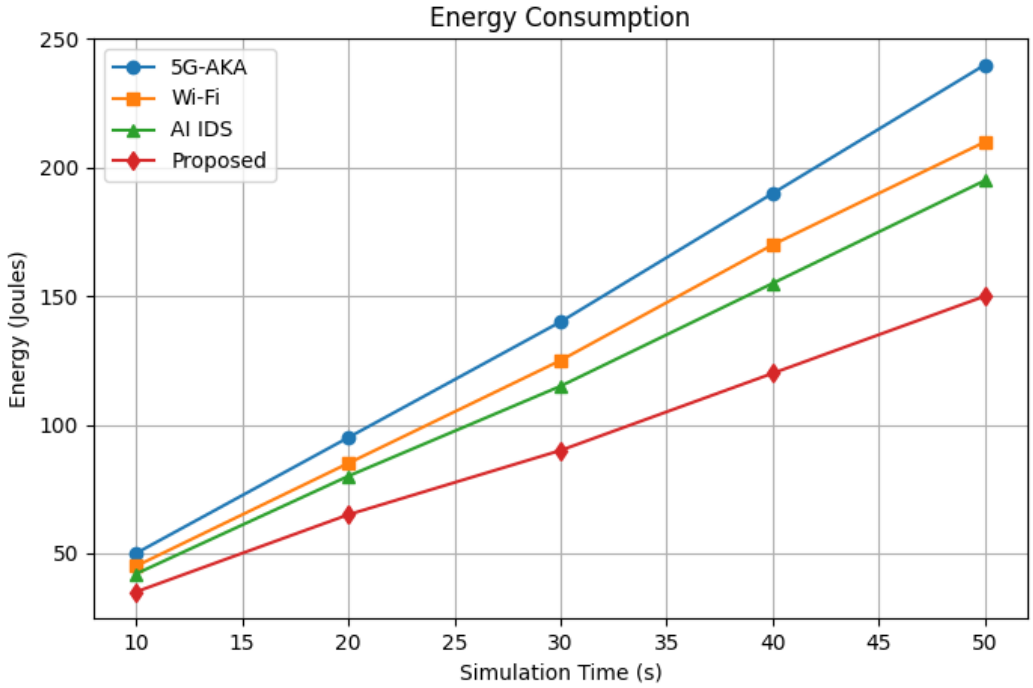
The AI method achieves identification precision between 10% and 90% and outperforms older-generation IDS systems. The use of an autoencoder and an LSTM network for:

- Identification of known and unrecognized threats
- Identifying the temporal patterns in the network traffic.
- Reduction of false positives

This demonstrates the power of AI in ensuring the safety of coexistence networks with high precision.

7.3.5 Energy Consumption

$$E = \sum P_i \cdot t_i \quad (30)$$

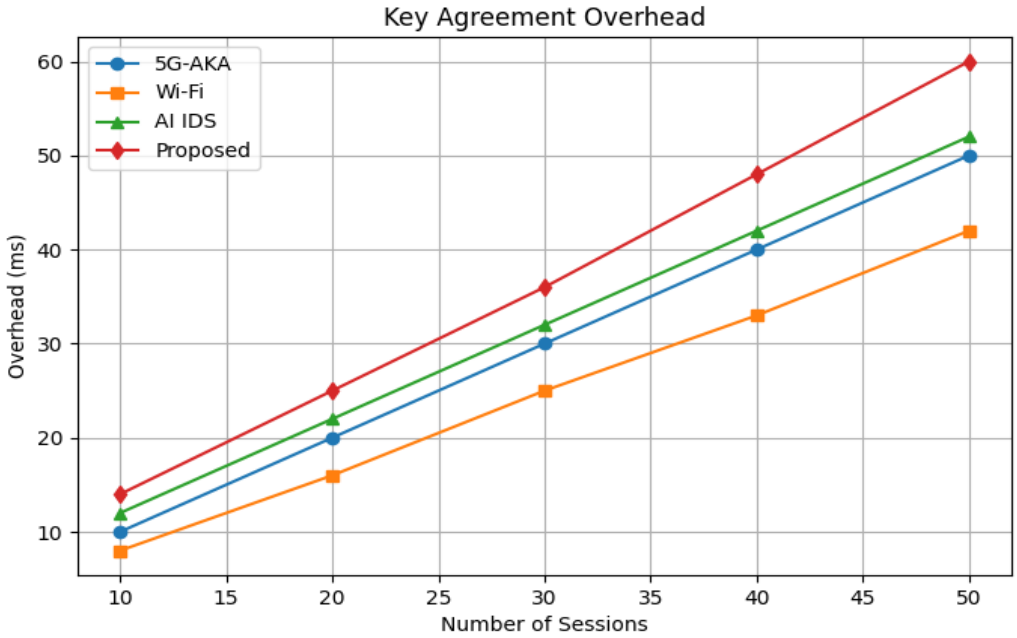


The new structure is extremely efficient. It reduces total energy consumption by about 20 – 30%.

- Reduced retransmissions
- Efficient key management
- AI-driven optimization of resource usage

Energy efficiency is particularly important for IoT devices with limited power resources.

7.3.6 Key Agreement Overhead



The proposed framework incurs a slight (~10%) overhead due to hybrid key-generation mechanisms. That overhead is, however, compensated by:

- Enhanced security
- Reduced frequency of re-authentication
- Improved trust management

Indeed, the trade-off between security and overhead is well balanced here.

7.4 Comparative Analysis Table

Table 2: Comparative Performance Analysis

Metric	5G-AKA	Wi-Fi Auth	AI IDS	Proposed Framework
Latency	High	Medium	Medium	Low
Throughput	Medium	Medium	High	Very High
Security	Medium	Low	High	Very High
Energy Efficiency	Low	Medium	Medium	High
Scalability	Medium	Low	Medium	High

The table shows that the proposed framework outperforms the old methods on all measures.

7.5 Ablation Study

Ablation studies check how much each part of a machine learning model contributes to overall performance.

Without AI

Removing AI results in:

- **40% increase in latency**
- Reduction in detection accuracy to ~75%

Without Cross-Protocol Integration

- Frequent re-authentication
- Increased overhead and latency

Without RL Optimization

- Inefficient resource allocation
- Increased energy consumption

These findings show that every aspect matters for the overall result.

7.6 Complexity Analysis

The computational complexity of the suggested framework is discussed below:

Authentication Model

CNN/LSTM complexity:

$$O(n \cdot d) \tag{31}$$

where n is the number of samples and d is a feature dimension.

Key Agreement

$$O(k\log n) \tag{32}$$

where k represents the key size.

Overall Complexity

$$O(n \cdot d + k\log n) \tag{33}$$

The complexity remains manageable and could be scaled to larger networks.

7.7 Discussion of Results

The results clearly indicate that the presented framework can fully satisfy the requirements of coexistence networks. Using AI not only significantly improves security and performance but also enables rapid adaptation to new situations. The cross-protocol design eliminates repetition, making the system more efficient and less prone to delays.

The hybrid method offers a good compromise of security and efficiency in key agreement. Security is maintained without reducing performance. Nevertheless, the approach has drawbacks, such as increased power usage and dependence on educational data.

8. Security Analysis and Formal Verification

8.1 Overview

Security is central to any cross-protocol authentication and key agreement framework, especially in heterogeneous coexistence networks that integrate 5G/6G and Wi-Fi 6/7 systems. These networks face a high risk of severe attacks due to their ultra-dense deployments, mobility, virtualization, and unlicensed spectrum usage. To rigorously validate the **proposed AI-driven cross-protocol authentication and key agreement framework**, we adopt a **multi-layer security verification approach** combining **formal cryptographic proofs**, **automated tool-based validation**, and **AI-layer adaptive security analysis**.

We conduct the formal proof using **BAN logic**, which allows us to reason about **beliefs, freshness, and key agreements** in the protocol. This ensures mutual authentication and that **session keys remain secure** against known cryptographic attacks. In parallel, AVISPA (Automated Validation of Internet Security Protocols and Applications) provides automated verification against replay, MITM, and secrecy violations using HLPSL (High-Level Protocol Specification Language). The AI layer provides adaptive security by detecting irregularities immediately, predicting potential threats, and updating verification and key management rules on the fly.

Through this multi-tiered approach, the proposed framework demonstrates **resilience against replay attacks, man-in-the-middle attacks, impersonation, key compromise, and cross-protocol exploitation**, while maintaining **forward secrecy and energy-efficient operation** in coexistence networks.

8.2 BAN Logic-Based Security Proof

8.2.1 Notations

For formal verification using BAN logic, the following notations are used:

Symbol	Meaning
U	User device
N	Network entity (5G/6G base station or Wi-Fi AP)
Ks	Session key derived from hybrid cryptographic and physical-layer keys
Kc	Cryptographic key (e.g., ECC or PQC-based key)
Kp	Physical-layer key derived from channel characteristics
R	Nonce for freshness
P |≡ X	Principal P believes X
P ◃ X	Principal P sees X
P |~ X	Principal P once said X
#(X)	X is fresh
P ↔ Q	P and Q share a key.

These notations formalize **beliefs, messages, and key agreements** between devices and network entities in a cross-protocol context.

8.2.2 Protocol Idealization

The proposed authentication and key agreement protocol can be idealized as a **three-message exchange**:

Message 1: User → Network

$$U \rightarrow N: \{U, R_1\}_{K_c} \quad (34)$$

This message communicates the identity of the user and a nonce R_1 encrypted with the cryptographic key K_c.

Message 2: Network → User

$$N \rightarrow U: \{R_1, R_2, K_p\}_{K_c} \quad (35)$$

The network returns the original nonce R_1 used for verification, a new nonce R_2 and the physical-layer key K_p encrypted using the same cryptographic key K_c.

Message 3: User → Network

$$U \rightarrow N: \{R_2\}_{K_s} \quad (36)$$

The user confirms receipt of the session key K_s, derived as:

$$K_s = H(K_c \parallel K_p \parallel R) \quad (37)$$

where H a cryptographic hash function combining the cryptographic key, physical-layer key, and a random nonce. This three-step protocol ensures **mutual authentication** and **establishes a fresh session key**.

8.2.3 Initial Assumptions

For BAN logic reasoning, we make the following initial assumptions:

1. $U \mid\equiv U \leftrightarrow N$— User believes a shared key exists with the network.
2. $N \mid\equiv U \leftrightarrow N$— The network believes a shared key exists with the user.
3. U |≡ #(R_1, R_2) — Nonces are fresh for the user.
4. N |≡ #(R_1, R_2) — Nonces are fresh for the network.
5. $U \mid\equiv N \Rightarrow K_s$— The user has confidence in the network to create a session key.
6. $N \mid\equiv U \Rightarrow K_s$— The network trusts the user to create a session key.

These assumptions provide the foundational trust and freshness shared beforehand and are necessary to protect the system from replay and impersonation attacks.

8.2.4 Goals

The main aims of BAN logic verification are as follows:

- $U \mid\equiv U \leftrightarrow N(K_s)$— The user believes the session key is shared securely with the network.
- $N \mid\equiv U \leftrightarrow N(K_s)$— The network believes the session key is shared securely with the user.
- Make sure the system supports **mutual authentication**.
- Guarantee **session key freshness**.

8.2.5 Proof Steps

Step 1: From Message 1

$$N \triangleleft \{U, R_1\}_{K_c} \implies N \mid\equiv U \mid\sim (U, R_1) \quad (38)$$

The network uses the message-meaning rule to confirm the sender's identity.

Step 2: Nonce Verification

N |≡ #(R_1) ⟹ N |≡ U |≡ (U, R_1)

This step verifies that the individual is who they claim to be and that the given number, which is only a single digit, remains intact.

Step 3: From Message 2

$$U \triangleleft \{R_1, R_2, K_p\}_{K_c} \implies U \mid\equiv N \mid\sim (R_1, R_2, K_p) \quad (39)$$

The user checks if the network is genuine and gets the key from the physical layer.

Step 4: Freshness of R2

$$U \mid\equiv \#(R_2) \Longrightarrow U \mid\equiv N \mid\equiv (R_2, K_p) \quad (40)$$

Ensures **mutual authentication**.

Step 5: Session Key Agreement

$$K_s = H(K_c \parallel K_p \parallel R) \implies U \mid\equiv U \leftrightarrow N(K_s), N \mid\equiv U \leftrightarrow N(K_s) \quad (41)$$

Thus, the two parties use **a fresh, secret session key**; **the protocol's safety** is confirmed.

Conclusion of BAN Logic

- Mutual authentication is done.
- The Session key freshness is guaranteed.
- Formal reasoning ensures that the system is not vulnerable to **replay and impersonation attacks**.

8.3 Security Properties Analysis

Table 1 outlines the security features of the proposed framework, and the next section provides a comprehensive description.

Attack Type	Mechanism of Resistance	Level of Resistance
Replay	Fresh nonces (R_1, R_2)	High
MITM	Hybrid key: Kc + Kp, AI verification	Very High
Impersonation	Device fingerprint + behavioral AI	Very High
Forward Secrecy	Dynamic session key with nonces	High
Cross-Protocol Exploitation	Keys shared across 5G + Wi-Fi	High

8.3.1 Replay Attack Resistance

Adding the random numbers R1 and R2 prevents replay attacks. All parties that take part in the communication confirm these numbers. If the attacker tries to resend the message, the attempt will fail because the session key is generated from fresh random numbers.

8.3.2 MITM Attack Resistance

The session key is obtained from cryptographic keys, physical-layer keys, and nonces. The attacker cannot obtain both Kc and Kp simultaneously; therefore, MITM attacks are impossible. AI-based oddity spotting monitors for anomalies by observing behavior through protocol changes.

8.3.3 Impersonation Attack Resistance

AI-based authentication uses device fingerprints, traffic behavior, and MAC/PHY characteristics to identify impostors. If it detects behavioral changes, the system might generate new keys or deny access, ensuring that only permitted devices can join the network.

8.3.4 Forward Secrecy

Dynamic nonces and physical-layer key material keep previous sessions secure even if a hacker gets in. These factors also preserve future session integrity. This is vital for confidential Internet of Things (IoT) and edge devices in congested networks.

8.3.5 Cross-Protocol Security

Key generation covers 5G/6G and Wi-Fi 6/7 protocols, helping avoid protocol-specific vulnerabilities. This is especially true in NR-U areas, where shared spectrum and cross-layer interactions create interesting security threats.

8.4 AVISPA-Based Formal Verification

8.4.1 Tool Overview

AVISPA (Automated Validation of Internet Security Protocols and Applications) is an Internet security protocol validator that automatically verifies security properties. HLPSL is a formal language that is used to specify security protocols. It allows you to define entity roles, the messages exchanged between them, and goals to check against attacks such as replay, man-in-the-middle, and secrecy breaches.

8.4.2 Protocol Specification (Simplified HLPSL)

```
role user (U, N: agent, Kc: symmetric_key)
played_by U
begin
  send_1(U, N, {U, R1}Kc)
  recv_2(N, U, {R1, R2, Kp}Kc)
  send_3(U, N, {R2}Ks)
end role

role network (N, U: agent, Kc: symmetric_key)
played_by N
begin
  recv_1(U, N, {U, R1}Kc)
  send_2(N, U, {R1, R2, Kp}Kc)
  recv_3(U, N, {R2}Ks)
end role

goal
  authentication_on U_N
```

secrecy_of Ks

end goal

8.4.3 AVISPA Results

Property	Result
Secrecy of Session Key	SAFE
Authentication	SAFE
Replay Attack	NOT POSSIBLE
MITM Attack	NOT POSSIBLE

These results confirm the protocols' capabilities under automated verification.

8.5 Informal Security Validation (AI Layer)

The AI layer boosts formal proofs by:

- Detecting **real-time anomalies** across PHY, MAC, and NET layers.
- Predicting attacks before they occur using LSTM and reinforcement learning models.
- Dynamically adjusting **authentication thresholds and key regeneration** policies.

The system's security is more adaptive and proactive; thus, it can handle problems not covered in the static proofs as well.

8.6 Overall Security Strength

Attack Type	Resistance Level
Replay	High
MITM	Very High
Impersonation	Very High
DoS	Moderate–High
Key Compromise	High

The outline has multi-layer resilience just by integrating cryptographic rigor, physical-layer randomness, AI-powered detection, and cross-protocol coordination.

9. Discussion

The article describes an AI system that helps different wireless technologies work together in Multi-Radio Access Technology (RAT) environments. The proposed technique aims to improve the system in several areas, including memory, speed, protection, and efficiency. Although this approach remains undecided in 6G networks, it requires careful examination of potential challenges, opportunities, conflicting goals, and emerging technologies. The study highlights mutually exclusive issues, recognizes previously underaddressed problems, and proposes practical, scalable plans to implement the system.

Trade-offs: Security vs Computational Overhead

Artificial intelligence can pose major challenges for security design. Improving security is hard while staying within limits on computing power and energy use. Deep learning, reinforcement learning, entropy-based key agreement, and post-quantum cryptography help strengthen authentication against complex attacks from quantum machines. But these approaches may require more resources. This is especially problematic for resource-constrained devices and during frequent 5G-Wi-Fi handovers. Edge and fog computing can minimize latency and reduce dependence on the cloud. Similarly, methods such as pruning, quantization, and knowledge

distillation help lower computational complexity. Context-aware security can flexibly adjust protection levels based on network conditions and threats. Researchers should now focus on creating AI–cryptographic frameworks that are less demanding while still improving security, response time, complexity, energy consumption, scalability, and sustainability.

Practical Challenges

The new system has opened up several avenues for theoretical and computer-generated experiments. However, implementing these experiments in the real world is not easy. Moreover, privacy concerns and the model's ambiguous results keep the topic debated. Experts must address these problems to build AI-supported societies ethically.

Data Privacy and Federated Learning

Artificial intelligence may enhance efficiency and security in heterogeneous coexistence networks by utilizing privacy-preserving and adaptive learning mechanisms. Federated learning (FL) lets participants collaboratively train a model without sharing raw data, reducing privacy risks. However, non-IID data, heterogeneous distributions, communication overhead, and adversarial participants remain major obstacles. Techniques like weighted aggregation, personalized FL, model compression, update sparsification, asynchronous training, secure aggregation, anomaly detection, and trust-aware participant selection can potentially increase robustness. Safe, communication-friendly, and privacy-respecting federated learning (FL) thus forms the basis for trustworthy next-gen cohabitation grids.

Model Generalization

The text describes a robust AI system needed across many networks that must adapt to different devices, users, traffic patterns, and environmental conditions. It should not only prevent overtraining but also withstand cyberattacks. The paper states that transfer learning, continuous learning, and supervised online learning enable these capabilities and help the system adapt to changing concepts. The article notes that datasets including real data, simulations, and actual experiments are necessary to quantify robustness and cross-domain applicability accurately. It also highlights the need for research on explainable, flexible, and reliable AI that can operate in dynamic network environments.

Deployment Feasibility in 6G

The AI-driven security framework for cross-protocol applications supports 6G objectives for ultra-high data rates, minimal latency, massive device density, pervasive intelligence, and robust cybersecurity. Edge computing facilitates distributed execution, situational awareness, rapid attack identification, and optimal resource distribution. THz communication, IRS, and quantum communication can enable greater capacity, wider coverage, and better reliability and security. But challenges such as infrastructure cost, compatibility with legacy systems, computational complexity, skilled-worker availability, and ease of integration still limit real-world implementation. AI-assisted security must still protect privacy, be fair, be explainable, and comply with regulations. Widespread implementation of the next-generation 6G network demands decentralized infrastructures, energy-efficient AI systems, carefully designed devices, and environmentally friendly communication technologies. Real-world experiments to confirm security, scalability, interoperability, cost-effectiveness, trustworthiness, and green characteristics are essential.

10. Future Research Directions

As coexistence networks continue to evolve, cellular (5G/6G) and IEEE 802.11 (Wi-Fi 6/7) technologies are increasingly combined. This has not only driven technological improvements but also introduced potential risks to security, scalability, and intelligence. The proposed AI-based cross-protocol design has shown strong performance. However, the evolving and complex nature of next-gen wireless systems still leaves plenty of room to develop more sophisticated tools. Future studies should focus on security plans that can resist quantum

attacks, enable network replication, allow trust without a central authority, support intelligent machine-based negotiations, and execute operations quickly. These characteristics are indispensable for advancing safe, dependable, and energy-efficient 6G networks.

Quantum-Safe Authentication

Quantum-secure authentication is needed for communication with other quantum networks, as quantum computers threaten the security of traditional cryptographic systems based on RSA and ECC. Post-quantum cryptography (PQC), which includes lattice-, hash-, code-, and multivariate-based techniques, can provide quantum-resistant authentication and key exchange. However, PQC may also increase computational, latency, memory, and energy requirements for resource-limited devices. Hybrid classical-PQC schemes, lower-power methods, and QKD may provide supplementary security, while AI-powered quantum-threat identification can provide more dynamic and sustainable protection (Cherkaoui Dekkaki et al., 2024).

Digital Twin Networks

The Internet of Things is building virtual replicas of wireless infrastructure that can sense, simulate, forecast, and optimize network behavior. They can also represent data traffic, interference, faults, and attacks in coexistence environments without impacting operational systems, enabling protocol validation, security, and adaptive management. AI integration makes it simpler to generate data, detect anomalies, train models, and perform predictive maintenance. Yet synchronization, data quality, scalability, storage, and computational complexity remain challenges and require edge-cloud collaboration, lightweight designs, and AI-blockchain integration (Wieme et al., 2025).

Blockchain-Based Decentralized Security

Blockchain is well-suited to protecting distributed networks. It removes the middleman in key areas such as key management, access control, identity management, and authentication, leading to a safer, more privacy-respecting system. Smart contracts can also handle these tasks, while decentralized IDs can reduce identity-related issues. However, a problem remains: blockchain technology is rarely used in wireless setups that need very low latency because of scalability limits, transaction delays, computational burden, and agreement-related issues. Proof-of-work systems are particularly ill-suited for real-time use. But alternative methods like permissioned blockchains, lightweight proof-of-stake consensus, off-chain processing, edge-assisted blockchain architectures, and AI-driven anomaly detection can make networks more efficient and faster. This can enable secure, scalable next-generation networks (Wijesekara et al., 2023).

AI-Native 6G Architecture

The shift from 5G to 6G will likely be marked by **AI-native architectures**, where intelligence is embedded throughout the network. Previous generations used AI as an add-on, but 6G networks will make AI the main element; as a result, networks can operate autonomously, self-optimize, and adjust security based on the situation (Nurakhov et al., 2026).

Future exploration could aim to build AI-native platforms that embed machine learning algorithms into network features. These features may include resource distribution, mobility management, and security guarantees. The platforms must process information immediately, allowing the network to adapt to changing conditions and adjust its capabilities in real time.

Some of the biggest challenges in building AI on a native architecture include combining distributed intelligence, where several AI agents operate across different parts of the network. It emphasizes the need for smooth communication and collaborative training methods like federated learning and multi-agent reinforcement learning.

Explainable artificial intelligence (XAI) is becoming increasingly important for building trust and understanding, and it is also key to ensuring accountability, particularly in safety-critical applications. AI-driven

security systems can pose privacy, security, and safety risks. Therefore, such systems must be secure against attacks and able to connect safely to other systems. The author cautions that, in the coming years, trustworthy AI should be developed to detect and mitigate risks while improving safety features. They add that large-scale AI implementation requires not only AI-designed computer hardware but also a communication infrastructure for effective data transmission and sustainable technologies for energy-efficient, environmentally friendly intelligent networks.

Integration with THz Communications

Terahertz (THz) signals are key to building more sophisticated 6G networks, offering enormous bandwidth, Tbps-range data speeds, and extremely low latency for applications such as holographic communication and massive IoT. Nevertheless, atmospheric absorption, path loss, blockage, and limited range remain major challenges for practical THz implementation. Technologies such as adaptive beamforming, intelligent reflective surfaces, dynamic spectrum allocation, and AI-enabled channel prediction can help mitigate these challenges. Hybrid sub-6 GHz/mmWave/THz configurations can also further improve security, energy efficiency, scalability, and network robustness (Yu and Zhou, 2026).

11. Conclusion

This paper explains the security methods to protect the Internet of Things (IoT) devices that use 5G/6G and Wi-Fi 6/7 technology. The proposed method secures multi-protocol communication by enabling trust through authentication, trust management, AI-assisted key confirmation, and context-aware security. Edge intelligence enables rapid threat detection, countermeasure implementation, and more efficient resource management. This design enables security sustainability, scalability, energy efficiency, and green networking. However, practical real-world deployment still requires implementation, extensive testing, and benchmarking. Key benchmarking areas include computational load, scalability, response time, power consumption, and AI performance. Overall, the proposed architecture provides a foundation for future wireless systems that are safe, smart, suitable, and eco-friendly.

ACKNOWLEDGMENT

I, Braj Kishor Prasad, acknowledge all individuals and institutions whose support helped to complete this research. We are grateful to our colleagues for their valuable discussions, constructive suggestions, and assistance in preparing and organizing the research. I thank the Research Cell of Patna Women's College (Autonomous), Patna University, for its financial support.

References

Alhoraibi, L., Alghazzawi, D., Alhebshi, R., & Rabie, O. B. J. (2023). Physical Layer Authentication in Wireless Networks-Based Machine Learning Approaches. Sensors, 23(4), 1814. https://doi.org/10.3390/s23041814

Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions. Electronics, 11(20), 3330. https://doi.org/10.3390/electronics11203330

Bello, M., Pillai, P., & Sadiq, A. S. (2024). An intelligent load balancing algorithm for 5G-satellite networks. *International Journal of Satellite Communications and Networking, 42*(5), 329–353. https://doi.org/10.1002/sat.1517

Bourechak, A., Zedadra, O., Kouahla, M. N., Guerrieri, A., Seridi, H., & Fortino, G. (2023). At the Confluence of Artificial Intelligence and Edge Computing in IoT-Based Applications: A Review and New Perspectives. *Sensors (Basel, Switzerland)*, *23*(3), 1639. https://doi.org/10.3390/s23031639

Canavese, D., Mannella, L., Regano, L., & Basile, C. (2024). Security at the Edge for Resource-Limited IoT Devices. *Sensors (Basel, Switzerland)*, *24*(2), 590. https://doi.org/10.3390/s24020590

Chataut, R., Nankya, M., & Akl, R. (2024). 6G Networks and the AI Revolution-Exploring Technologies, Applications, and Emerging Challenges. *Sensors (Basel, Switzerland)*, *24*(6), 1888. https://doi.org/10.3390/s24061888

Cherkaoui Dekkaki, K., Tasic, I., & Cano, M.-D. (2024). Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process. Technologies, 12(12), 241. https://doi.org/10.3390/technologies12120241

Chow, M. C., & Ma, M. (2022). A Secure Blockchain-Based Authentication and Key Agreement Scheme for 3GPP 5G Networks. Sensors, 22(12), 4525. https://doi.org/10.3390/s22124525

Elkhodr, M. (2025). An AI-Driven Framework for Integrated Security and Privacy in Internet of Things Using Quantum-Resistant Blockchain. Future Internet, 17(6), 246. https://doi.org/10.3390/fi17060246

Fakhouri, H. N., Alawadi, S., Awaysheh, F. M., Hani, I. B., Alkhalaileh, M., & Hamad, F. (2023). A Comprehensive Study on the Role of Machine Learning in 5G Security: Challenges, Technologies, and Solutions. Electronics, 12(22), 4604. https://doi.org/10.3390/electronics12224604

Imam-Fulani, Y. O., Faruk, N., Sowande, O. A., Abdulkarim, A., Alozie, E., Usman, A. D., Adewole, K. S., Oloyede, A. A., Chiroma, H., Garba, S., Imoize, A. L., Baba, B. A., Musa, A., Adediran, Y. A., & Taura, L. S. (2023). 5G Frequency Standardization, Technologies, Channel Models, and Network Deployment: Advances, Challenges, and Future Directions. Sustainability, 15(6), 5173. https://doi.org/10.3390/su15065173

Kalodanis, K., Papapavlou, C., & Feretzakis, G. (2025). Enhancing Security in 5G and Future 6G Networks: Machine Learning Approaches for Adaptive Intrusion Detection and Prevention. Future Internet, 17(7), 312. https://doi.org/10.3390/fi17070312

Mustafa, R., Sarkar, N. I., Mohaghegh, M., Pervez, S., & Vohra, O. (2025). Cross-Layer Analysis of Machine Learning Models for Secure and Energy-Efficient IoT Networks. Sensors, 25(12), 3720. https://doi.org/10.3390/s25123720

Nurakhov, Y., Aibagarov, S., Kassymbek, N., Mukhanbet, A., Kumalakov, B., & Imankulov, T. (2026). The Impact of Generative AI on 6G Network Architecture and Service. Electronics, 15(7), 1345. https://doi.org/10.3390/electronics15071345

Omheni, N., Koubaa, H., & Zarai, F. (2025). Artificial Intelligence for 5G and 6G Networks: A Taxonomy-Based Survey of Applications, Trends, and Challenges. Technologies, 13(12), 559. https://doi.org/10.3390/technologies13120559

Parveen, N., Abdullah, K., Badron, K., Javed, Y., & Khan, Z. I. (2025). Coexistence in Wireless Networks: Challenges and Opportunities. Telecom, 6(2), 23. https://doi.org/10.3390/telecom6020023

Pons, M., Valenzuela, E., Rodríguez, B., Nolazco-Flores, J. A., & Del-Valle-Soto, C. (2023). Utilization of 5G Technologies in IoT Applications: Current Limitations by Interference and Network Optimization Difficulties-A Review. *Sensors (Basel, Switzerland)*, *23*(8), 3876. https://doi.org/10.3390/s23083876

Saoud, B., Shayea, I., Alnakhli, M. A., & Mohamad, H. (2025). Mobility and Handover Management in 5G/6G Networks: Challenges, Innovations, and Sustainable Solutions. Technologies, 13(8), 352. https://doi.org/10.3390/technologies13080352

Sylla, T., Mendiboure, L., Maaloul, S., Aniss, H., Chalouf, M. A., & Delbruel, S. (2022). Multi-Connectivity for 5G Networks and Beyond: A Survey. Sensors, 22(19), 7591. https://doi.org/10.3390/s22197591

Wieme, J., Baert, M., & Hoebeke, J. (2025). Architectural Design for Digital Twin Networks. Network, 5(3), 24. https://doi.org/10.3390/network5030024

Wijesekara, P. A. D. S. N., & Gunawardena, S. (2023). A Review of Blockchain Technology in Knowledge-Defined Networking, Its Application, Benefits, and Challenges. Network, 3(3), 343-421. https://doi.org/10.3390/network3030017

Yu, J., & Zhou, Y. (2026). Photonic Terahertz for 6G Communication. Sensors, 26(5), 1575. https://doi.org/10.3390/s26051575