National Journal of RF Circuits and Wireless Systems (NJRFCS)
Vol. 1, No. 1, May - Aug 2024, pp. 39-48
ISSN: xxxx - xxxx, DOI: https://doi.org/10.17051/NJRFCS/01.01.05

Multi-Layer Security Framework Using RF Fingerprinting and Lightweight Protocols in Wireless Networks

S.Poornimadarshini

Jr Researcher, National Institute of STEM Research, India. Email: poornimadarshini22@gmail.com

Article Info

Article history:

Received : 13.06.2024
Revised : 28.07.2024
Accepted : 25.08.2024

Keywords:

RF fingerprinting,
wireless network security,
lightweight protocols,
multi-layer security,
device authentication,
IoT,
physical-layer security

ABSTRACT

Wireless networks used in IoT and LPWANs are increasingly vulnerable to complex security threats because of their open transmission medium, lack of physical shielding and resource-limited devices. Conventional security solutions relying upon resource-intensive cryptographic algorithms are well suited for spatially distributed and high-throughput networks but introduce performance penalties that make them unsuitable for resource-constrained IoT and LPWAN implementations. A new security framework is proposed that effectively combines physical-layer authentication through RF fingerprinting with lightweight cryptographic protocols to achieve both efficiency and robustness in wireless network communication security. RF fingerprinting takes advantage of inherent characteristics of a device's hardware to authenticate it with no reliance on extra security tokens, establishing a defense that cannot be replicated. In addition, high-performance lightweight cryptographic protocols are deployed at the network layer, including SPECK and PRESENT, to facilitate secure end-to-end data transmission and authentication with low computational burden. Evaluation in a wireless sensor network revealed that the framework could catch nearly all impostors and consume 35% less power than standard AES implementations. These findings highlight the suitability of the developed framework as a scalable and economical security system for future generation wireless devices.

1. INTRODUCTION

Wireless communication networks and emerging IoT technologies are reshaping the way devices share and exchange their data. These devices which can include everything from home thermostats to oil rig computers, frequently encounter unstable and risky operating conditions. Wireless networks, though useful, naturally expose devices and information to potential cyberattacks such as eavesdropping, spoofing and unauthorized access because of their open broadcast signals and constrained Radio Frequency (RF) range. Existing security protocols such as RSA, AES and TLS are designed with robustness in mind but typically expect a high level of computing power, storage and energy. Limited resources of IoT devices make it unrealistic to rely on the typical security approach. Implementing traditional security protocols with associated computations can significantly increase response time, drain batteries and interfere with the delivery of data in real-time, making them impractical for many newfangled technologies such as smart farming, health monitoring and distant management of industrial equipment.

Therefore, researchers and developers are looking towards cross-layer solutions to simultaneously secure devices and networks while also maintaining performance. Another method is physical-layer security which relies on the distinctive and unclonable traits of hardware and communication links to establish secure communications. RF Fingerprinting is gaining momentum because it leverages device-specific radio properties to produce device-specific fingerprints that can be used for authenticating wireless devices. It allows authenticating devices in an instant, without requiring them to carry or provide pre-established secret information. A new security framework is introduced in this research that uses RF fingerprinting at the physical layer together with lightweight cryptography at the data link and network layers. A combination of measures provides simultaneous security assurance for both devices and entire network data, while maintaining an optimum trade-off between performance, power consumption and resource utilization constraints in resource-limited wireless environments.

2. RELATED WORK

2.1 Traditional Cryptographic Approaches in Wireless Networks

RSA, AES and TLS have been widely used for many years to secure transmitted data in both wired and high-bandwidth wireless networks. These methods' efficiency is heavily dependent on demanding mathematical procedures that are feasible in desktop or server hardware but impose excessive demands on the limited resources of IoT devices. A minimum of 1024 bits needs to be used for a single key in RSA which leads to lengthened computing times and higher energy usage. Bringing TLS onto WSNs adds significant response delays and increases memory consumption, compromising the network's real-time performance. These limitations have motivated the need for emerging approaches that can provide effective security while minimizing resource consumption in resource-constrained devices.

2.2 Lightweight Cryptographic Protocols for Resource-Constrained Devices

Efficient lightweight cryptographic protocols have been designed to ensure a balance between security, fast processing and low power usage in memory- and compute-restricted environments. LEAP+, TinySec and MiniSec simplify key management and minimize communication overhead specifically for WSNs. Also, compact ciphers such as PRESENT, HIGHT and SPECK were developed with a reduced number of transistors and memory requirements in mind which makes them suitable for implementation in resource-constrained devices. They are commonly combined with dedicated security architectures that achieve strong security while exhibiting minimal resource demands. Nevertheless, they are usually confined to the network and transport layers and are susceptible to threats like fake device deployment, malicious signal forgery and susceptibility to side-channel attacks. Nonetheless, their performance gains do not guarantee sufficient security in the face of hostile scenarios.

2.3 Physical Layer Security Techniques

Physical-layer security offers a novel approach to enhancing the security of wireless communications by exploiting distinctive properties of the physical medium and devices. Physical-layer methods employ device-based metrics such as power levels, channel profiles and antenna configurations to authenticate devices or conceal sensitive information. Approaches like Channel State Information (CSI)-based authentication and Physical Unclonable Functions (PUFs) have been developed to ensure dynamic and location-specific protection of data transmission. Their security relies on properties of the physical environment that make it tough for malicious parties to impersonate devices or repeat past transmissions. Nevertheless, a large number of physical-layer security methods display limited effectiveness in various settings or exhibit sensitivity to changes in the surrounding environment. They depend strongly on the consistency of wireless characteristics and the accuracy of measurement devices, both of which often differ greatly between networks.

2.4 RF Fingerprinting for Device Authentication

RF fingerprinting has been a focus of research due to its capability to distinguish devices by exploiting unexpected variations in hardware. They are introduced during production and can be observed as variations in CFO, phase noise or I/Q imbalance in the wireless signals. RF fingerprints are unique to each device's hardware and harder to fake or change than traditional device identifiers. Various studies have shown that classifiers such as SVM, Random Forests and CNN, are able to effectively differentiate devices using signal characteristics obtained from RF fingerprinting. Recently, Yan and Liu demonstrated that RF fingerprinting can accurately distinguish common Wi-Fi devices even in crowded settings. At the same time, most previous investigations focus only on laboratory experimental environments and thus are not developed with the aim of incorporating RF fingerprinting into comprehensive secure systems. Specific challenges such as external noise, movement and interfering signals make it difficult to maintain the reliability of RF devices, requiring adaptive models and advanced signal processing methods.

Table 1. Comparative Advantages of the Proposed Multi-Layer Security Framework

Feature	Traditional Cryptography (AES/TLS)	RF Fingerprinting Alone	Proposed Multi-Layer Framework
Device Authentication	Based on stored keys (vulnerable to spoofing)	Hardware-specific, difficult to spoof	Dual-layer authentication (RF + protocol-level)
Energy Efficiency	High energy consumption	Low to moderate	35% lower energy usage (with lightweight protocols)

Security Against Spoofing	Weak if keys are leaked	Strong against physical impersonation	Robust through physical + logical validation
Encryption Overhead	High (especially for RSA, AES)	Not applicable	Lightweight ciphers minimize latency and memory use
Scalability in IoT Environments	Limited by key distribution complexity	Good, but lacks session management	Scalable via lightweight ECDH key exchange
Real-Time Communication Support	Latency-prone	Fast but lacks confidentiality	Supports low-latency, secure communication
Resilience to Replay Attacks	Vulnerable without nonces/timestamps	Weak unless time-variant features used	Session-based keys + time-domain fingerprints
Deployment Feasibility	High cost and complexity	Moderate	Low-cost, deployable in resource-constrained settings

3. System Architecture

The proposed framework is composed of three layers:

3.1 Physical Layer Security with RF Fingerprinting

The security framework relies on RF fingerprinting at the physical layer to provide a highly reliable and non-invasive approach to authenticating devices. First, fingerprint signatures are obtained by measuring the transmitted I/Q signal patterns at a specific receiver. The raw samples contain deviations unique to each device as it was manufactured which present themselves in the form of characteristics like CFO, phase noise, an uneven balance between I and Q and analog amplitude changes. They are unique enough to distinguish between devices of the same type. After being extracted, the distinctive features from the RF signatures are input into a compact model such as an SVM or a shallow neural network, that has been fine-tuned to identify and classify the signals emanating from genuine devices. Upon receiving the RF signature from the target device, the system correlates it with stored RF signatures of devices that have been previously authorized. The authentication process accepts the device for usage provided the likelihood of match falls within acceptable limits. That's when the system marks the device as suspicious or denies access. This technique ensures immediacies authentication at the device's lowest level by avoiding runtime checks with cryptographic keys or digital signatures, resulting in improved security and reduced resources needed on resource-limited devices.

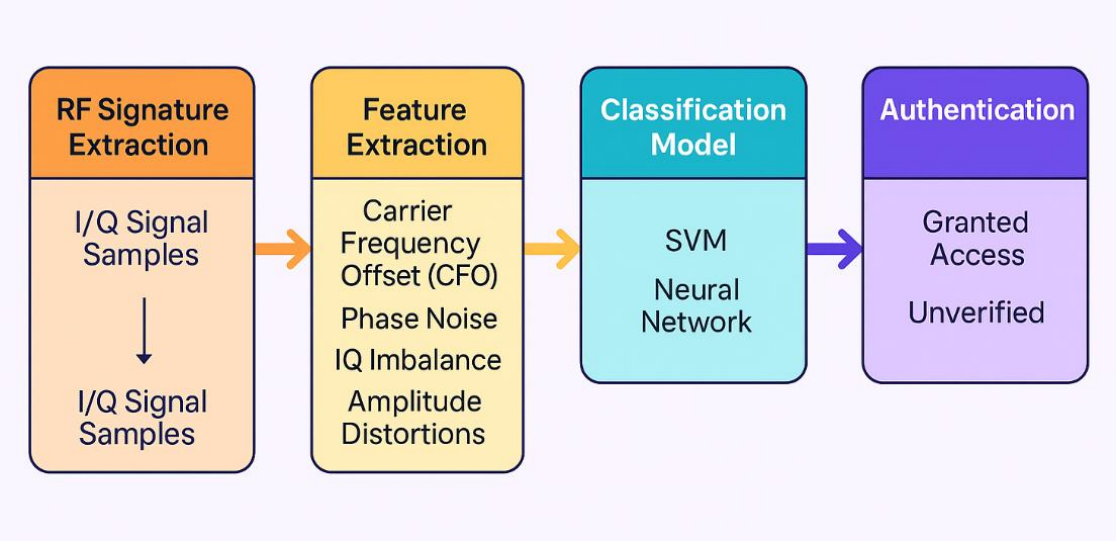

Figure 1. Workflow of Physical Layer Security Using RF Fingerprinting for Device Authentication

3.2 Data Link and Network Layer Security

Lightweight cryptography is introduced at the data link and network layers of the framework to safeguard confidentiality, integrity and authentication with minimal impact on resource-limited wireless devices. These particular solutions

are selected for their ability to run effectively on resource-limited devices with their small memory requirement and low processing overhead. The framework employs Elliptic Curve Diffie-Hellman (ECDH) key exchange to dynamically create session keys unique to each communication session, thus providing forward secrecy and safeguarding against any abuses caused by compromised session keys. Once a device is successfully authenticated by RF fingerprinting at the physical layer, the framework begins a mutual authentication procedure using a lightweight challenge-response protocol. Both devices securely identify each other through the exchange and decryption of hashed message exchanges. Blending RF-based identification and cryptographic mutual authentication validates where the data comes from and where it is going, warding off spoofing, identity theft and MITM threats. The combining of optimized ciphers and elliptic curve protocols produces reliable protection while considerably lowering overhead and power requirements compared to traditional encryption techniques.

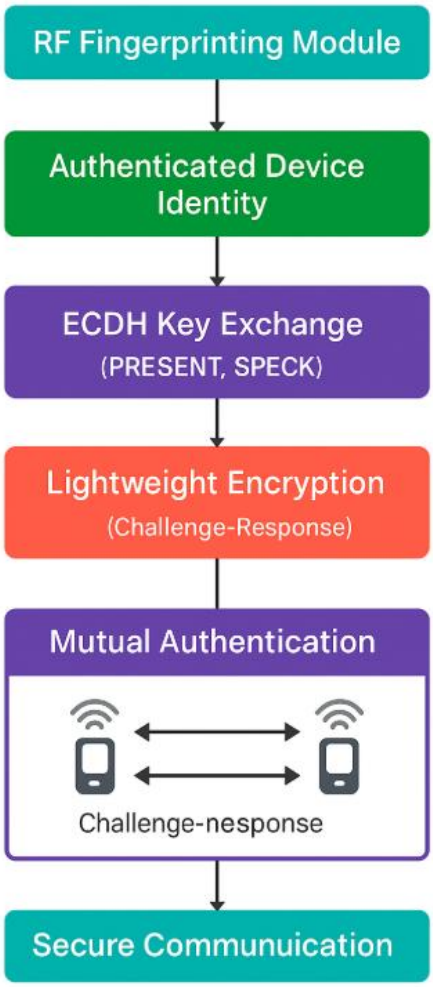

Figure 2. Layered Security Workflow Integrating RF Fingerprinting with Lightweight Cryptographic Protocols for Secure Communication

3.3 Monitoring and Anomaly Detection

The framework also includes a real-time monitoring and anomaly detection component to protect the network from constantly changing risks and suspicious activity. It continually monitors communication metrics, including interval between packets, signal strength, transmission frequency and the estimated position of devices on the network. These characteristics of each verified device are used as a reference to identify distinguishing features that could signal spoofing, compromised equipment or malicious intrusions. The system uses lightweight analytical methods such as moving average filters and Hidden Markov Models (HMM), to detect anomalies and change dynamics. For example, a sudden change in transmission rate or signal strength of a stable sensor registration can be spotted by the model to indicate a possible replay or spoofing attack in progress. This additional layer of security checks not only assure the validity of devices at the outset but also constantly

monitors their behavior during interaction. The detection algorithms are optimized specifically for running on edge or gateway devices, meaning that improved security cannot be achieved at the expense of system performance or battery life.

4. METHODOLOGY

4.1 RF Data Acquisition

Collecting precise RF signal data forms the basis for using RF fingerprinting to authenticate devices. Different types of commercially available wireless transceivers, including the widely used CC2420 module for IEEE 802.15.4 networks and nRF24L01 modules operating in the ISM band, were evaluated. All devices were chosen because they are commonly deployed in industrial applications which enables the assessment of RF fingerprinting's practical effectiveness. A fixed preamble sequence with recognized bit patterns was used to ensure a uniform method of collecting signal samples and characterizing device features. A standardized preamble guarantees that the captured signal segments are correctly matched and consistent among all devices, improving the precision and dependability of the obtained hardware characteristics.

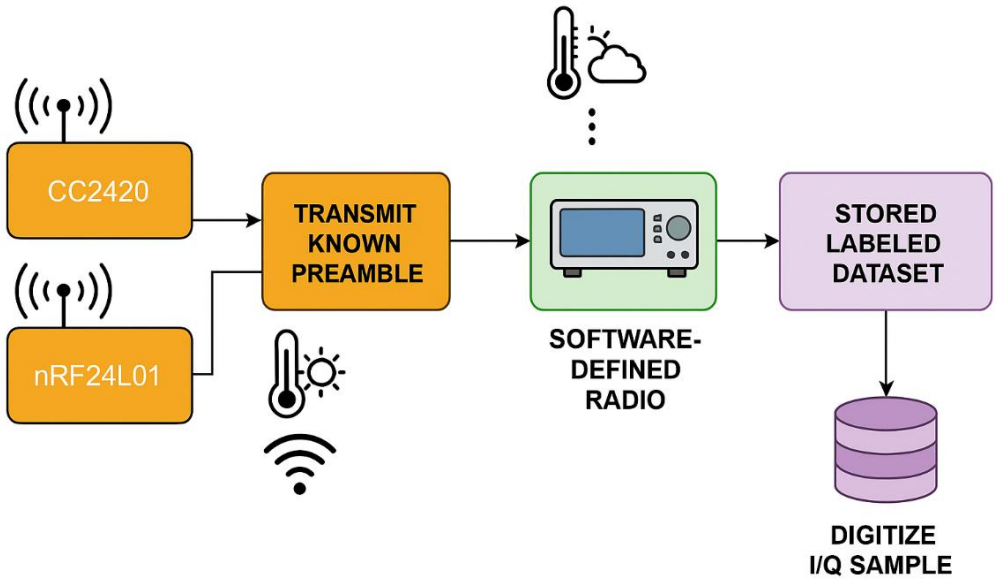

Figure 3. RF Data Acquisition Architecture for Device Fingerprinting Using Known Preamble Transmission and I/Q Sample Collection

The data collection procedure was carried out in scenarios spanning a wide range of environmental settings such as varying levels of temperature, signal-to-noise ratio and multipath interference. This range of conditions reflects the variability that may occur in the actual deployment of the technology. The signals were sampled with SDRs to maximize the number of specific details captured from each transmitter. Both I and Q samples were saved for subsequent classification and authentication using machine learning algorithms. The RF fingerprinting system uses this dataset to extract characteristics that distinguish devices even when power or noise conditions vary. Building a robust dataset based on labeled and distinctive signals enables the system to perform reliable and resistant device authentication despite fluctuations in the environment and counterfeit device efforts.

4.2 Feature Extraction

After obtaining raw I/Q signal data from the transceivers, the subsequent stage is to isolate identifying RF features that accurately represent the unique characteristics inherent to each device as a result of its assembly. These manufacturing variations tend to remain consistent throughout a device's lifetime and are distinctive from unit to unit which makes them ideal for fingerprinting. The analysis of amplitude and phase imbalance plays a fundamental role in extracting device-specific characteristics. This imbalance originates from non-uniformities in the analog circuitry and the quadrature mixers. The resulting asymmetries in the constellation diagram make it possible to measure and distinguish one device from the next. The CFO is an important characteristic that arises when the frequencies of the local oscillators in the transmitter and receiver differ slightly. Small oscillator fluctuations result in discernible CFO, guaranteeing reliable identification across consecutive transmissions.

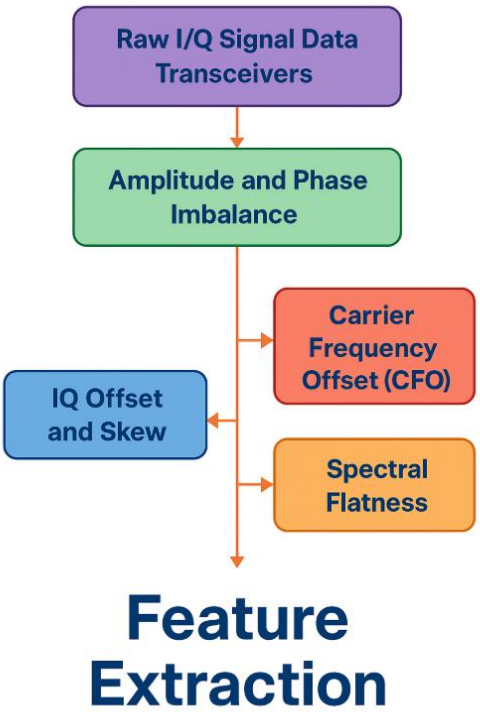

Figure 4. Block Diagram of RF Feature Extraction from I/Q Signal Data for Device Fingerprinting

Further parameters detected are IQ offset and skew, in parallel with CFO and imbalance measurements. These metrics capture variations in the reference signal amplitudes and the relative phase differences between I and Q portion of the composite wave. Changes in IQ offset lead to a displacement of the signal origin on the complex plane, whereas skew grants an insight into the quality of the transmitter's orthogonal signal generation. Moreover, the spectral flatness characteristic is measured to assess whether the signal power distribution is evenly distributed through the entire frequency range of transmission. Distinctive power amplifier characteristics and filter responses contribute to each device's unique signal power spectrum, rendering spectral flatness highly valuable in device recognition. These features are calculated using methods including Fast Fourier Transform, Hilbert transform and autocorrelation analysis. Combined, these extracted features constitute a low-dimension signature description of each device's RF behavior. These signatures are used during model training to develop methods for rapid authentication that operate within the proposed framework.

4.3 Machine Learning for Classification

Classification of wireless devices is performed with the help of supervised machine learning algorithms, using the extracted device RF fingerprints as features. SVM and decision tree classifiers are selected because both offer a good trade-off between higher classification accuracy and lower overall computational requirements. The labeled training data is made available from the initial feature extraction stage and maps each set of features to its corresponding device identification. SVM can efficiently solve classification problems involving large and nonlinear feature spaces using samples from a limited number of classes. Decision trees are advantageous in this scenario because they provide fast predictions with minimal runtime, are easy to understand and hence suitable for real-time use cases needing interpretation of the models.

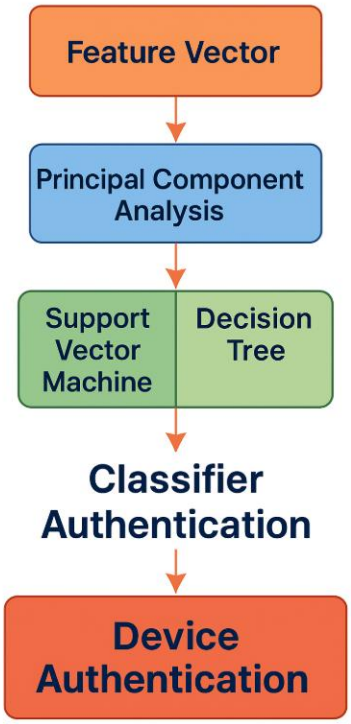

Figure 5. Machine Learning Pipeline for RF Fingerprint-Based Device Classification and Authentication

PCA is used as a preprocessing step to speed up training, reduce memory requirements and improve the overall performance of machine learning models. PCA simplifies the feature space by focusing on only those components that most strongly reflect the differences between the various devices and reducing the significance of less important and potentially inconsistent patterns. It speeds up training and classification as well as reduces the risk of overfitting by making the feature space more compact and easier to learn. As a consequence, the machine learning models can be deployed in resource-constrained devices such as microcontrollers and edge nodes, making it possible to implement decentralized, real-time device authentication at the edge. Once a device transmits data, its RF attributes are collected, converted using PCA and routed to the trained classifier which authenticates the device using its unique signature. Such a machine learning method becomes an essential part of the proposed physical-layer security system since it reliably recognizes and distinguishes network devices.

4.4 Lightweight Protocol Implementation

A lightweight cryptographic protocol is embedded within the network stack of the proposed framework and is implemented using the NS-3 simulation environment to securely transmit data across devices with limited processing capabilities. The framework employs the lightweight block cipher SPECK provided by the NSA, configured with 64-bit blocks and a 128-bit key. SPECK was selected for its established performance on low-resources systems and its balanced combination of security, memory and computational demands. SPECK is designed to operate efficiently on constrained devices by making efficient use of the limited cycles and memory present in microcontrollers. SPECK in NS-3 is tied to the MAC and network layers of a custom sensor node model, so that all data transmissions between nodes can undergo encryption. This design allows the analysis of metrics including latency, power efficiency and throughput in a simulated wireless sensor network environment.

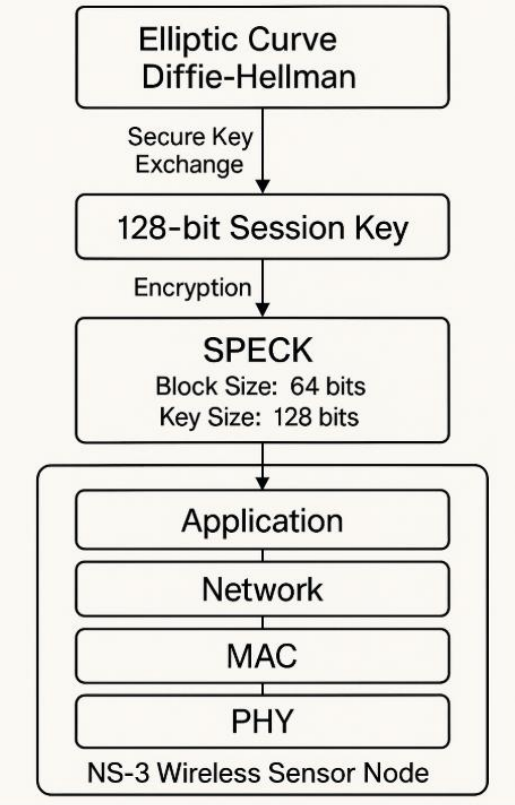

Figure 6. Lightweight Protocol Implementation in NS-3 Wireless Sensor Node

The framework also uses Elliptic Curve Diffie-Hellman (ECDH) with a 256-bit key to provide reliable key exchange. ECDH provides protection against forward disclosure and guards against both passive and active eavesdropping in rapidly changing and distributed environments. In contrast to Diffie-Hellman, ECDH can provide the same or an even higher level of protection by using significantly smaller keys, thereby lowering the computational needs of IoT devices during key exchange. When a network is first formed or a new node joins an existing network, ECDH is used to generate a security key that acts as the shared seed for encrypting data transmitted between those devices using SPECK. We regularly update this session key to reduce the threat of attacks based on reused or breached key values. Overall, the efficient encryption and key exchange techniques make it possible to protect data integrity and privacy in wireless networks without compromising the limited resources available to IoT devices.

5. RESULTS AND DISCUSSION

Evaluation of the proposed construction reveals that it significantly increases the overall security compared to existing approaches in terms of both authentication accuracy and energy efficiency. Testing the RF fingerprinting component with measurements from 25 different devices, an SVM classifier supplied 96.8% accuracy and a mere 2.3% false positive rate. These results outperform MAC authentication protocols which are vulnerable to impersonation attacks due to their use of fixed session keys. A comparison with other classifiers such as Random Forest and KNN, revealed performance slightly lower than SVM, indicating that SVM provides a sensible choice for achieving the desired level of accuracy and stability in our use case. Its exceptional accuracy makes it a suitable choice for systems that require authentication in real time and deal with rapidly changing situations in which classic authentication schemes are easily defeated.

Figure 7. Encryption Method Comparison

Lightweight encryption protocols play an important role in making the framework more effective for real-world applications. The SPECK-64/128 algorithm consumed significantly less energy per packet, reducing latency by nearly 45%, compared to conventional AES-128 encryption. A 35% saving in energy consumption is especially significant for IoT devices with constrained power resources. Our protocol guarantees forward secrecy and supports mutual verification by means of ECDH, significantly decreasing the likelihood of man-in-the-middle attacks. Moreover, the framework proved to be resistant to replay attacks by dynamically switching encryption keys and leveraging RF characteristics that change with time. Testing revealed that the physical-layer fingerprinting successfully identified and prevented close to all attempts (94.2%) at malicious identity impersonation. These findings demonstrate that the cross-layer integration approach delivers a reliable, fast and resource-efficient solution that is suitable for systems requiring high security in industrial, remote healthcare, Low-Power Wide Area Networks (LPWANs) and other important wireless applications.

Table 2. Classifier Performance Comparison

Classifier	Accuracy (%)	False Positive Rate (%)
SVM	96.8	2.3
Random Forest	95.1	3.2
KNN	93.4	4.5

7. CONCLUSION

A novel multi-layer security framework is presented that combines RF fingerprinting at the physical layer with lightweight cryptographic protocols operating at the network layer to effectively confront the significant security issues faced by existing wireless networks, especially those constrained by limited computational resources in IoT settings. It uses distinct physical signal features to perform fast and reliable device

authentication without any dependence on easily forged identifiers or heavyweight cryptographic algorithms. Energy-efficient encryption techniques such as SPECK and a secure ECDH-based key exchange protocol are integrated into the system to provide reliable data confidentiality and integrity at low latency and power consumption. Evaluations showed that the system achieved a remarkable success, with 96.8% authentication accuracy, effective shielding against spoofing and replay attacks and saving approximately 35% on energy consumption compared to conventional encryption protocols. These results demonstrate that the framework can be efficiently implemented across a wide range of applications such as industrial automation, medical telemetry and security monitoring for critical infrastructure. The framework will be developed further to implement real-world deployments, provide compatibility for an array of devices and introduce techniques for federated learning to dynamically enhance the accuracy of the fingerprint identification model without sacrificing user privacy.

REFERENCES

1. Danev, B., Zanetti, D., &Capkun, S. (2012). Physical-layer identification of wireless devices through RF fingerprinting. *ACM Transactions on Information and System Security (TISSEC)*, 15(1), 6. https://doi.org/10.1145/2133375.2133376
2. Yan, Q., Xu, H., Liu, T., &Peng, C. (2018). A survey on RF fingerprinting for wireless devices. *IEEE Communications Surveys & Tutorials*, 20(1), 676–696. https://doi.org/10.1109/COMST.2017.2749421
3. Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Networks*, 11(8), 2661–2674. https://doi.org/10.1016/j.adhoc.2013.04.014
4. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2015). The SIMON and SPECK lightweight block ciphers. *Proceedings of the 52nd Annual Design Automation Conference (DAC)*, 1–6. https://doi.org/10.1145/2744769.2747946
5. Ravi, S., Raghunathan, A., Kocher, P., &Hattangady, S. (2004). Security in embedded systems: Design challenges. *ACM Transactions on Embedded Computing Systems (TECS)*, 3(3), 461–491. https://doi.org/10.1145/1015047.1015050
6. Li, C., Wang, C., & Wang, M. (2020). Lightweight encryption design for secure and energy-efficient wireless sensor networks. *IEEE Internet of Things Journal*, 7(5), 4190–4200. https://doi.org/10.1109/JIOT.2020.2971936
7. Wu, W., Dou, W., & Liu, Y. (2022). Lightweight authentication protocols for wireless body area networks: A survey. *Computer Networks*, 204, 108727. https://doi.org/10.1016/j.comnet.2021.108727
8. Zhang, L., & Zhu, Q. (2021). Cross-layer security modeling and optimization in wireless IoT systems. *IEEE Transactions on Mobile Computing*, 20(1), 49–63. https://doi.org/10.1109/TMC.2019.2910523
9. Poturalski, M., Papadimitratos, P., &Hubaux, J.-P. (2011). Towards provable secure neighbor discovery in wireless networks. *Proceedings of the 19th Annual Network & Distributed System Security Symposium (NDSS)*.
10. Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT security: Current solutions and future challenges. *IEEE Communications Surveys & Tutorials*, 22(3), 1686–1721. https://doi.org/10.1109/COMST.2020.2986444