Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 12, 2025

PHYSICAL LAYER AUTHENTICATION: MITIGATING MITM AND EAVESDROPPING IN PUBLIC WLANS.

Muhammad Waris Tafoor

Faculty of Science & Engineering, University of Wolverhampton

warismalik582@gmail.com

DOI: https://doi.org/10.5281/zenodo.18066115

Keywords

Article History
Received: 11 October 2025
Accepted: 21 November 2025
Published: 27 December 2025

Corresponding Author: *
Muhammad Waris Tafoor

Abstract

The widespread proliferation of public Wi-Fi networks has created a pressing need for robust security measures to pro- tect user data from eavesdropping and Man-in-the-Middle (MitM) attacks. This research investigates the potential of Radio Frequency (RF) fingerprinting as a novel approach to address these challenges.

The primary objective of this research was to develop a system capable of identifying rogue access points mas- querading as legitimate Wi-Fi networks. By leveraging the unique RF signatures emitted by Wi-Fi devices, the system aims to detect and alert users to potential security threats.

The research methodology involved a multi-step process. Raw RF signals were captured from various Wi-Fi net- works using an NESDR mini 2 SDR and SDR# software. These signals were then analysed to extract distinctive features such as signal strength variations, frequency spectrum analysis, and modulation characteristics. The extracted features were combined to create unique fingerprints for each Wi-Fi device. These fingerprints were compared to a database of legitimate access points to identify rogue devices. The system's effectiveness in detecting rogue access points was rigorously tested. Through this research, a system was successfully developed that can accurately identify rogue access points based on their unique RF signatures.

The findings of this research contribute to the growing body of knowledge on public Wi-Fi security and offer a promising solution for mitigating the risks associated with eavesdropping and MitM attacks. By employing RF finger- printing techniques, this research provides a valuable tool for safeguarding user data and promoting a more secure online environment.

INTRODUCTION

Public Wi-Fi networks are convenient, but they can be risky for your data. Eavesdroppers can snoop on your activity, and man-in-the-middle attackers can intercept and tamper with your data transmissions (Sombatruang et al., 2018). Radio Frequency (RF) fingerprinting of- fers a potential solution to these threats. Around 10 million Wi-Fi hotspots are in UK (Gordon, 2022), showcasing the usage of it and how many people are vulnerable to a potential Man-in- the-Middle attack.

RF fingerprinting (Jagannath, Jagannath and Kumar, 2022) leverages the inherent unique- ness of a device's radio transmissions. Like fingerprints for humans, every wireless device, from smartphones to laptops, possesses distinct

characteristics in its radio frequency (RF) emissions. These unique signatures arise from minute imperfections and variations in hard- ware components and manufacturing processes. These imperfections cause subtle deviations in signal strength, timing, and other radio frequency properties, creating a unique "fingerprint" for each device. By analysing these fingerprints, RF fingerprinting technology can identify and track individual devices on a network.

These distinct signatures, caused by variations in hardware and manufacturing, allow creat- ing a database of authorized devices. By continuously monitoring and comparing the RF fingerprints of connecting devices against this database, unauthorized devices can be flagged. Additionally, monitoring authorized devices' fingerprints can help detect anomalies indicative of intrusion or malfunctioning devices. Furthermore, analysing communication paths based on fingerprints can help identify man-in-the-middle attacks.

RF fingerprinting research shows promise in being a complimentary technology to existing methods for detecting fake Wi-Fi. Current RF fingerprinting research (Xie et al., 2023) focuses on identifying specific devices, useful for authorized user equipment authentication or intru- sion detection on a network. Fake Wi-Fi typically involves a device masquerading as a legitimate access point.

In the world of public Wi-Fi security, RF fingerprinting can be used to spot unauthorized devices trying to join the network. It can also monitor the RF fingerprints of trusted devices to detect anomalies that might indicate eavesdroppers or man-in-the-middle attackers lurking on the network.

Problem Background

Public Wi-Fi networks offer convenient internet access on the go, but they come with sig- nificant security risks. Eavesdroppers can snoop on your activity, and man-in-the-middle attacks can intercept and tamper with your data transmissions. Malicious actors exploit these vulnerabilities by setting up fake Wi-Fi access points, often masquerading as legitimate hotspots (e.g., "Free Airport Wi-Fi" or "Coffee Shop Guest"). These fake Wi-Fi networks, also known as "evil twins," pose a severe threat to user privacy and security.

Increased Public Wi-Fi Usage: The widespread availability and growing dependence on public Wi-Fi networks have created ample opportunities for attackers. Users connect to these networks for various purposes like browsing the internet, checking emails, or accessing online services, often without realizing the associated security risks. Around 69 % of internet users (Salmon, 2023) use public Wi-Fi once a week.

Limitations of Traditional Wi-Fi Security: Current Wi-Fi security measures like SSID vali- dation and MAC address filtering have

limitations:

SSID Spoofing: Attackers can easily copy the SSID (network name) of a legitimate network, tricking users into connecting to the fake one.

MAC Address Spoofing: MAC addresses, which are unique identifiers for network devices, can be spoofed by attackers, rendering them unreliable for verification. A MAC spoofing attack on Bangladeshi Bank in 2016 resulted in $81 million heist by attackers (Vyas, 2023).

Open Networks: Many public Wi-Fi networks are completely open, offering no en- cryption for data transmissions. This makes them highly vulnerable to eavesdropping and man-in-the-middle attacks.

WEP Encryption: Wired Equivalent Privacy (WEP) was once the standard encryption protocol for Wi-Fi networks, but it has been proven weak (FasterCapital, n.d.) and eas- ily compromised by attackers.

WPA/WPA2 Encryption: Wi-Fi Protected Access (WPA) and WPA2 offer stronger encryption compared to WEP, but they still have vulnerabilities. WPA/WPA2 encryp- tion can be bypassed through brute-force attacks or exploiting weaknesses (Vivek, 2024) in the handshake process.

While RF fingerprinting isn't a direct solution for detecting fake Wi-Fi access points, it can be a valuable tool used in conjunction with other methods. Here's a look at recent research and some ongoing challenges:

Existing Research: Research explores integrating RF fingerprinting with deep learning for user equipment authentication in 5G networks (Fu et al., 2023). This demonstrates the potential for RF fingerprinting in device identification, which can be used to identify unexpected devices potentially associated with fake Wi-Fi.
Limited Research on Fake Wi-Fi Detection: Most current research focuses on device identification, not specifically detecting fake access points. Further research is needed to explore how RF fingerprinting can be integrated with existing methods for more ro- bust fake Wi-Fi detection.
Dynamic Environments: RF signals can be affected by environmental factors like inter- ference from other devices or obstacles.

Problem Statement

With the increasing prevalence of public Wi-Fi networks, users are exposed to a growing threat from fake access points designed to steal data, inject malware, or launch Man-in-the- Middle (MitM) attacks. Traditional Wi-Fi security measures like SSID validation and MAC address filtering are often ineffective against sophisticated attackers who can spoof these iden- tifiers.
This research explores the potential of Radio Frequency (RF) fingerprinting as a novel and promising approach to enhance public Wi-Fi security. Unlike existing methods that focus on network access control, RF fingerprinting leverages the unique radio frequency characteristics of each device, like a fingerprint for radio waves. By analysing these fingerprints, we can identify and track individual devices on a network, offering a new layer of defence against unauthorized access.

The potential impact of RF fingerprinting is significant:

Enhanced Detection: It can identify not only unauthorized devices attempting to con- nect to the network but also potential anomalies in authorized devices' behaviour, suggesting eavesdropping or man-in-the-middle attacks.
Robust Security: Unlike MAC address filtering, RF fingerprints are much harder to spoof, offering a more reliable method for device identification.
Emerging Technology: With further research, RF fingerprinting has the potential to adapt to evolving wireless protocols and hardware, ensuring long-term effectiveness.

Aims and Objectives

By implementing RF fingerprinting techniques, we can enhance our ability to identify and avoid fake Wi-Fi networks, ultimately improving user security and privacy on public Wi-Fi connections.
Feature extraction techniques: Analyse how to extract the most relevant and distinctive features from RF signals that differentiate legitimate access points from fakes. This could involve exploring signal strength variations, noise patterns, or specific hardware signatures.
Signal Strength Variations: How the strength of the radio signal changes over time can be a clue. Real Access Points might have a more stable signal strength compared to fakes.
Noise Patterns: The background noise within the signal might hold unique characteris- tics for each device. Analysing these noise patterns can help distinguish real from fake.
Hardware Signatures: Every Wi-Fi device has unique hardware components that can influence the way it transmits radio waves. Extracting these hardware signatures from the RF signal can be a powerful way to identify the real device.
Real-world implementation challenges: Address the challenges of implementing RF fingerprinting in real-world scenarios. Consider factors like environmental noise, signal variations due to distance, and the need for efficient fingerprint collection and analysis.
Comparison with other techniques: Evaluate the effectiveness of RF fingerprinting compared to traditional Wi-Fi security measures like MAC address filtering or SSID validation. Analyse the strengths and weaknesses of each approach in detecting fake ac- cess points.
Privacy considerations: Discuss any privacy concerns associated with RF fingerprinting. Explore techniques to anonymize or minimize the

amount of data collected while main- taining effective fake Wi-Fi detection.

Research Questions

Potential research questions for this project on Radio Frequency (RF) Fingerprinting for Fake Wi-Fi Detection:

What are the most effective features to extract from RF signals that can differentiate between legitimate and fake access points?

How can RF fingerprinting be implemented efficiently in real-world scenarios with minimal impact on user experience (e.g., connection speed)?

What are the technical challenges associated with collecting and analysing RF finger- prints in dynamic environments (e.g., crowded spaces)?

How can RF fingerprinting techniques adapt to new and sophisticated methods employed by attackers to create fake access points?

Report's Organization

This report details the research conducted on "Countering Eavesdropping and Man-in-the-Middle Attacks in Public Wi-Fi using RF Fingerprinting." The report is divided into five chap- ters, each focusing on a specific aspect of the research project.

Chapter 1 sets the stage for the research by introducing the project idea. It begins by highlighting the growing reliance on public Wi-Fi networks and the associated security con- cerns, particularly eavesdropping and Man-in-the-Middle attacks. Subsequently, the chapter defines the problem statement, outlining the challenges faced in securing public Wi-Fi connec- tions.

Chapter 2 delves into existing research related to the chosen topic. It provides a com- prehensive overview of RF fingerprinting techniques, exploring its potential for identifying rogue access points masquerading as legitimate ones. Additionally, the chapter analyses exist- ing research on securing public Wi-Fi and identifies any gaps in knowledge or limitations in current approaches.

Chapter 3 outlines the research methodology employed in the project. It details the approach taken to address the defined problem statement. This chapter describes the methods used for collecting and analysing RF fingerprints, including the chosen feature extraction techniques and algorithms. Additionally, the chapter outlines the testing procedures imple- mented to evaluate the system's effectiveness in detecting rogue access points and establishing secure connections. It details the results of the system testing, including the detection rate of rogue access points and the number of false positives encountered. This chapter also provides a comprehensive discussion of the results, analysing their significance in the context of secur- ing public Wi-Fi networks. The discussion addresses the limitations of the proposed approach and explores potential factors that might influence the system's performance.

Finally, chapter 4 summarizes the key takeaways from the research project. It reiterates the effectiveness of using RF fingerprinting for mitigating eavesdropping and Man-in-the- Middle attacks on public Wi-Fi. Additionally, the chapter acknowledges any limitations identi- fied during the research and suggests potential areas for future work. This might include exploring the integration of machine learning with RF fingerprinting for improved accuracy or investigating the use of blockchain technology for secure access control in public Wi-Fi net- works.

Gantt Chart

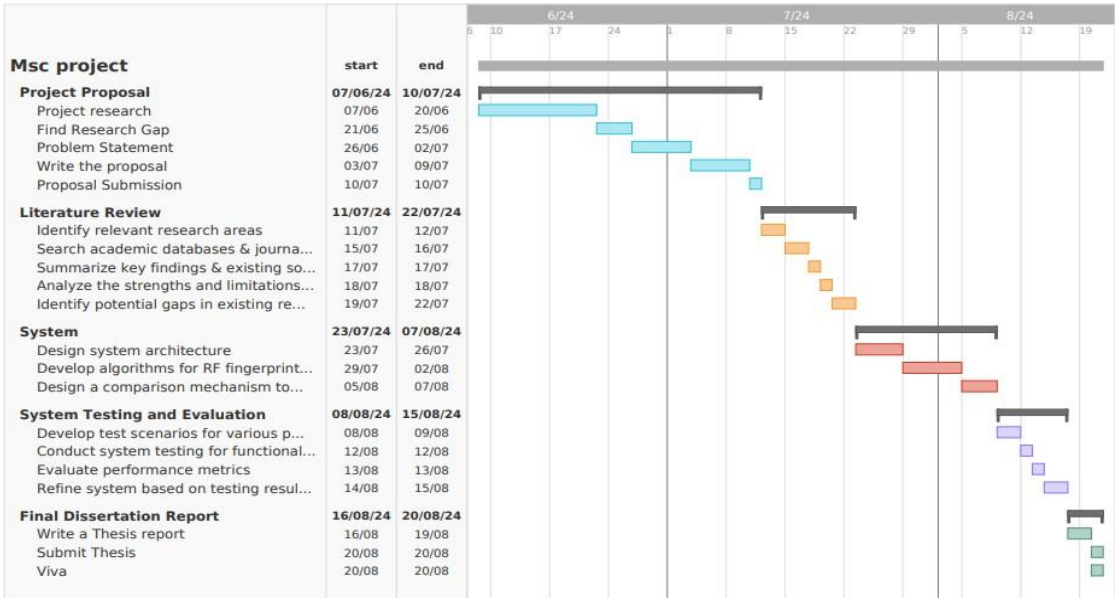

Figure 1. Gantt Chart

Literature Review

This chapter reviewed existing solutions for securing public Wi-Fi from eavesdropping and MitM attacks. It analysed established methods like encryption and user awareness, uncovering their effectiveness and limitations. Key studies were examined to understand current ap- proaches' strengths and weaknesses. Remaining challenges were identified, including user behaviour and evolving threats. Furthermore, the chapter identified gaps in the current litera- ture, pinpointing opportunities for our proposed RF fingerprinting method to contribute new knowledge and enhance public Wi-Fi security.

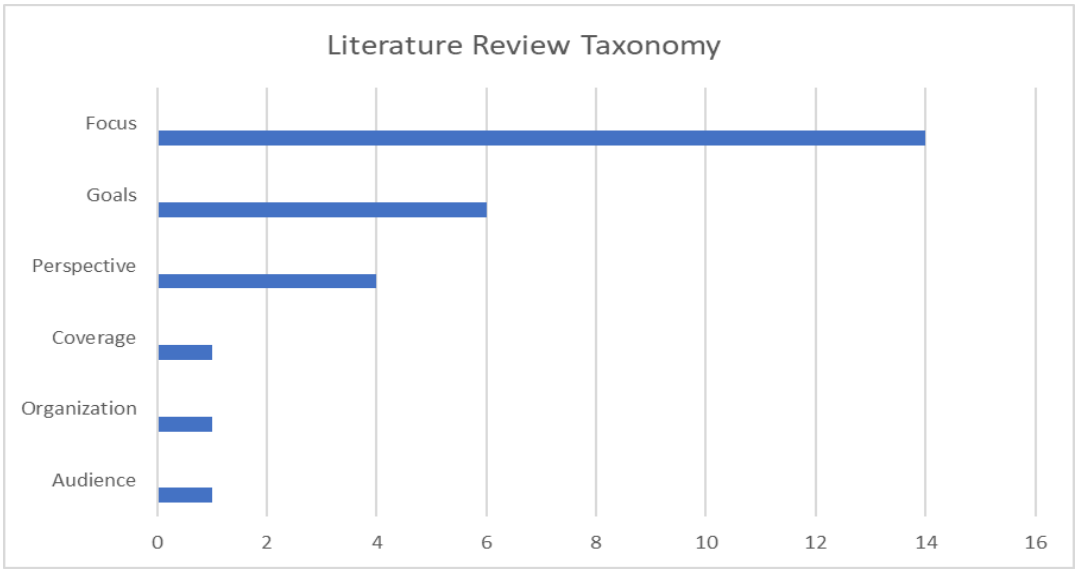

Figure 2. Literature Taxonomy Chart

Existing Techniques and Solutions

Wi-Fi remains a primary communication medium due to its speed, efficiency, and perceived security. While advancements have bolstered Wi-Fi protection, it remains vulnerable. Current security measures often require user expertise and are not universally implemented, leaving room for exploitation. Here are some of these techniques which are currently being used to secure Wi-Fi networks.

Secure Tunnelling Protocol

Secure tunnelling protocols establish encrypted connections between a user's device and a remote server, creating a secure pathway for data transmission (Yang, Wang and Chen, 2021). This encrypted channel is often referred to as a "tunnel" because it encapsulates data packets within another protocol, shielding them from prying eyes.

When data travels through this tunnel, it's encrypted using strong cryptographic algo- rithms, rendering it unreadable to anyone who intercepts it. This protection is crucial for safeguarding sensitive information when using public Wi-Fi networks, which are inherently less secure than private networks.

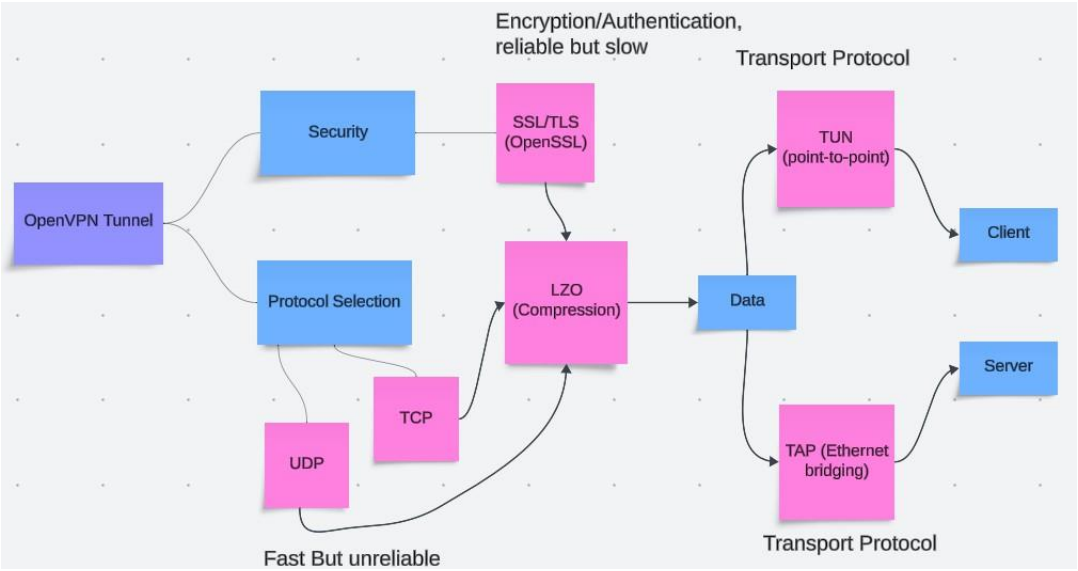

Figure 3. OpenVPN Tunnel Construction (Nakutavičiūtė, 2021).

A comparative analysis of three prominent options - OpenVPN, WireGuard, and PPTP - re- veals distinct characteristics.

OpenVPN is an open-source protocol renowned for its robust security features, including strong encryption and authentication mechanisms. It offers high levels of configurability, al- lowing users to tailor the protocol to specific security requirements. While OpenVPN generally delivers good performance over TCP, its performance can be significantly enhanced when using UDP. Compatibility is excellent, as OpenVPN clients are available for a wide range of platforms (Iqbal, 2019).

WireGuard is a relatively new protocol that has gained rapid popularity due to its simplicity and high performance (Mackey et al., 2020). It employs modern cryptographic techniques to provide strong security while minimizing computational overhead. WireGuard excels in terms

of speed but might have limitations in terms of compatibility compared to more established protocols like OpenVPN (Dowling and Paterson, 2018).

PPTP (Point-to-Point Tunnelling Protocol) is an older protocol that has been superseded by more secure options. While it offers good performance and compatibility, its security vulnera- bilities

make it unsuitable for handling sensitive data (Schwenk, 2022). This paper (Jones, Wimmer and Haddad, 2019) experiments to test the resilience of PPTP against DDOD attack and the results show it disconnects the user from the network, meaning a failure in securing a network.

Table 1. Comparison Secure Tunnelling protocols

Protocol	Description	Security	Performance	Compatibility
OpenVPN	Open-source, highly configurable, robust security features, supports TCP and UDP	High	Good (TCP), High (UDP)	Very Good
WireGuard	Simple, high performance, strong security	High	Very High	Good
PPTP	Less secure due to known vulnerabilities	Low	High	Good

Secure tunnelling protocols provide a strong layer of protection for online activities. How- ever, they are not without drawbacks. The encryption process can introduce latency and slightly decrease internet speeds compared to unencrypted connections. Furthermore, users must rely on the security and reliability of the chosen VPN service provider.

While secure tunnelling protocols offer robust protection, their effectiveness depends on factors beyond the technology itself. Technical expertise is necessary for setup, and perfor- mance trade-offs exist. Tunnelling protocol selection is a critical factor determining network connection security and performance. A deep technical understanding enables users to make informed choices. For example, IPsec (hides IP-packets) offers robust security (Ogudo, 2019) but demands intricate configuration, while PPTP (Jones, Wimmer and Haddad, 2019), though easier to set up, presents known security vulnerabilities. L2TP/IPsec strikes a balance between the two, but familiarity with both underlying protocols is beneficial.

Protocol configuration complexity varies significantly. Advanced protocols require detailed adjustments to encryption, authentication, and network settings, necessitating strong technical expertise to avoid vulnerabilities.

Establishing secure tunnels demands adherence to best practices, including employing strong encryption, robust authentication, vigilant key management, and optimized configura- tion. A solid grasp of these principles is essential for creating resilient and protected network connections.

Virtual Private Network

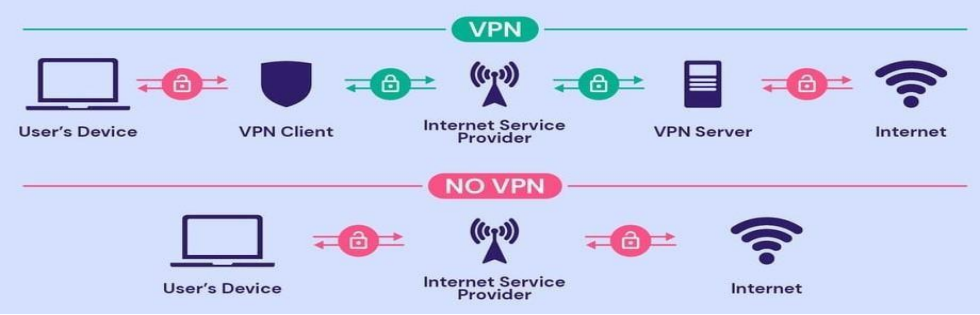

Figure 4. Working of VPN (A, 2022).

A Virtual Private Network (VPN) creates a secure, encrypted connection between your device and a remote server operated by a VPN service provider. This encrypted connection acts as a tunnel, protecting your online activities from prying eyes (Sharma and Kaur, 2020). When you connect to a VPN server, your internet traffic is routed through this secure tunnel. As a result, your real IP address is masked, and your online activities become invisible to your internet service provider (ISP) and other third parties. This anonymity helps protect your privacy and can prevent your online activities from being tracked or monitored.

Additionally, VPNs encrypt all your internet traffic, making it unreadable to anyone who intercepts it. This safeguards your sensitive data, such as passwords, financial information, and personal communications, from being stolen or compromised (Jyothi, K.K. and Reddy, Dr.B. I, 2023). This paper also points to some of commonly used protocols for VPN, which are PPTP (Point-to-point Tunnelling Protocol), L2TP (Layer 2 tunnelling protocol), IPsec (Internet Protocol Security), SSL/TLS (Secure Sockets Layer/ Transport Layer Security), and IKEv2 (Internet Key Exchange version 2).

VPNs offer numerous advantages, but they also come with certain limitations. Users typi- cally need to pay a subscription fee to access a VPN service's network of servers. Additionally, the encryption process and data rerouting can sometimes lead to slower internet speeds com- pared to a regular connection due to overhead caused by some protocols and if nested VPN is implemented then layers of VPN can cause more delays (Taneja* and Tyagi, 2019). This paper (Wu and Xiao, 2019) shows experimental results indicate that L2TP performance deteriorates significantly when using chain cascade network structures with three or more hops while Softether-based VPNs consistently outperform L2TP in terms of overall performance. While free VPN options exist, they often have drawbacks such as limited speeds, data caps, or intru- sive advertisements. Some free VPNs may even compromise user privacy by collecting and selling user data.

User expertise is paramount in optimizing VPN performance and security. It's important to consider that the reliability and security of a VPN service depends on the provider's infrastruc- ture and security practices. Users should carefully research and choose a reputable VPN provider to mitigate potential risks. A solid grasp of VPN mechanics, protocols, and potential vulnerabilities is crucial for maximizing their benefits.

Technical shortcomings can lead to configuration oversights, rendering users susceptible to attacks. Selecting the most suitable VPN protocol demands a nuanced understanding of securi- ty needs and performance expectations. Evaluating VPN providers requires a discerning eye for security practices, privacy safeguards, and service reliability. Moreover, effective VPN uti- lization hinges on knowing when and how to connect for optimal security and performance.

The table effectively highlights the key distinctions between secure tunnelling and VPNs.

Table 2. Key differences in VPN & Secure tunnelling

	Secure Tunnelling	VPN
Focus	Network-level security	User privacy and anonymity
Functionality	Encapsulates data for secure transmission	Creates a virtual private network
Additional Features	Limited	IP masking, kill switches, split tunnelling
Common Use Cases	Network-to-network connec- tions, remote access	User privacy, bypassing censorship, accessing geo-restricted content

Public Key Infrastructure

Public Key Infrastructure (PKI) is a system that uses digital certificates to verify the authentic- ity of entities involved in a communication. In the context of public Wi-Fi, PKI is being used to authenticate legitimate access points (Albarqi et al., 2015).

A digital certificate is essentially a digital passport that binds a public key to an entity (in this case, a Wi-Fi access point). This certificate is issued by a trusted third-party known as a Certificate Authority (CA). When a user tries to connect to a Wi-Fi network, the device checks the certificate to verify the identity of the access point. If the certificate is valid and issued by a trusted CA, the user can establish a secure connection (Yakubov et al., 2018). By implementing PKI, public Wi-Fi networks can significantly reduce the risk of users connecting to rogue access points, which are often used for eavesdropping and Man-in-the-Middle at- tacks.

Most commonly used types of PKI are SSL and TLS protocols which create secure, encrypted connections between servers and clients by using digital certificates. This safe- guards data by ensuring it remains confidential and unaltered during transmission. However, it is up to the client to check the signature of the certificates or at least verify hostname (Wang et al., 2020). This paper (Liu et al., 2019) presents a system called IoTVerif for automated SSL/TLS certificate verification in IoT applications. PKI offers a strong security framework, but its widespread adoption in public Wi-Fi networks presents significant challenges. Many access points must have valid certificates issued by trusted Certificate Authorities (CAs) for PKI to be effective (Radomir Prodanović et al., 2019). However, implementing PKI demands substantial investments in infrastructure, including the CA itself, certificate management sys- tems, and device provisioning.

Managing digital certificates is complex and requires ongoing attention. Regular up- dates and revocation processes are essential to maintain security. Additionally, users must understand the importance of certificate validation and how to verify their authenticity. These factors contribute to the complexity of implementing PKI on a large scale in public Wi-Fi en- vironments. The current RA/CA model is vulnerable to compromise, leading to fake certificates. Proposed solutions like CT, ARPKI, and PoliCert haven't been widely adopted due to complexity and implementation challenges (Garba et al., 2020).

Network Access Control (NAC)

Network Access Control (NAC) is a security framework that enforces security policies on de- vices attempting to connect to a network. It ensures that only authorized devices complying with specific security standards are allowed access. In the context of public Wi-Fi, NAC is being used to restrict access to unauthorized devices, thereby reducing the risk of security breaches. IEEE 802.1X is a port-based network access control (PNAC) standard that provides a secure mechanism for devices to gain access to a wired or wireless network. It ensures that only authorized devices can connect to the network (Omar and Abdelaziz, 2020).

When a device attempts to connect to a public Wi-Fi network protected by NAC, it undergoes a series of checks and authentication processes. These checks might include:

Device Identification: Determining the type of device (laptop, smartphone, IoT de- vice) and its operating system.

Security Posture Assessment: Evaluating the device's security configuration, such as the presence of antivirus software, firewall, and up-to-date operating system patches.

User Authentication: Verifying the identity of the user attempting to connect to the network.

Policy Enforcement: Applying specific security policies based on the device type and user identity, such as restricting access to certain network resources or requiring addi- tional authentication steps.

By implementing NAC, public Wi-Fi networks can mitigate risks associated with unauthorized devices, malware-infected devices, and unauthorized access.

Network Access Control (NAC) provides substantial advantages for network security. However, implementing and maintaining a robust

NAC system is not without its challenges. Deploying a comprehensive NAC solution demands careful planning, configuration, and significant investments in hardware and software, particularly for large-scale environments.

Additionally, NAC processes can introduce delays and extra steps for users, potentially im- pacting overall user experience. Furthermore, persistent attackers may develop methods to circumvent NAC controls, necessitating ongoing monitoring and updates to NAC policies.

WPA3 (Wi-Fi Protected Access 3)

WPA3 is the latest iteration of the Wi-Fi Protected Access (WPA) security protocol designed to enhance the security of wireless networks. It builds upon the foundation laid by its prede- cessor, WPA2, addressing vulnerabilities and introducing new security features. As of July 1, 2020, all Wi-Fi certified devices must comply with WPA3 security standards (Lamers et al., 2021).

Key Features of WPA3

Individualized Encryption: Unlike WPA2, which uses a shared encryption key for all devices on a network, WPA3 employs individualized data encryption. This means each device has its own unique encryption key, significantly improving privacy and security. If one device's key is compromised, it doesn't affect the security of other de- vices on the network (Asmaa Hani Halbouni, Ong and Leow, 2023).

Simultaneous Authentication of Equals (SAE): WPA3 replaces the Pre-Shared Key (PSK) authentication method used in WPA2 with SAE. SAE is a more secure authen- tication process that protects against offline dictionary attacks (Indira Reddy and Srikanth, 2019). It involves a series of password-based key derivation functions (PBKDF) to generate a strong encryption key, making it significantly harder for at- tackers to crack the password.

Enhanced Protection for IoT Devices: WPA3 also includes features specifically de- signed to protect IoT devices, which often have limited processing power and memory. These features include simplified authentication processes and increased se- curity for devices with weak cryptographic capabilities.

Increased Bit Strength: WPA3 offers higher levels of encryption, including 192-bit security, providing stronger protection against brute-force attacks compared to WPA2.

Key Studies and Findings

This section of the literature review presents a comprehensive analysis of existing research on public Wi-Fi network security. The focus is on exploring and evaluating techniques such as secure tunnels, VPNs, Public Key Infrastructure (PKI), Network Access Control (NAC), and WPA3.

Secure tunnels, while providing a layer of encryption and confidentiality, have been shown to be vulnerable to attacks if the endpoints are compromised. Studies have highlighted the importance of robust endpoint security measures to ensure the overall effectiveness of se- cure tunnels in mitigating eavesdropping and man-in-the-middle attacks on public Wi-Fi.

Real-world application of secure tunnelling is often limited to enterprise environments due to the complexity of configuration and management. User adoption is generally low among indi- vidual users due to the technical expertise required.

VPNs have been widely adopted for their ability to create secure connections over public networks. Research has demonstrated their effectiveness in protecting user data from interception. However, studies have also identified performance implications, such as in- creased latency and reduced throughput, which can impact user experience. VPNs have demonstrated strong user adoption, especially among individuals concerned about online pri- vacy and security. Ease of use and availability of VPN on various platforms have contributed to their popularity. However, their effectiveness can be hindered by user behaviour, such as the tendency to leave VPN connections inactive or using public Wi-Fi without enabling the VPN.

PKI has been established as a cornerstone of secure communication, providing authen- tication and encryption capabilities. However, the management of digital certificates and the potential for certificate authority compromise remain challenges. Studies have emphasized the importance of rigorous certificate lifecycle

management practices to maintain PKI system integrity. PKI is primarily used in enterprise environments to establish trust and secure communication. User adoption is limited as it often requires technical expertise for certificate management. However, the increasing prevalence of digital certificates in everyday life (e.g., HTTPS) is gradually enhancing user familiarity.

NAC has shown promise in preventing unauthorized access to Wi-Fi networks by enforcing access policies based on user, device, and network conditions. However, its effectiveness can be hindered by the accuracy of device identification and the potential for evasion techniques. Research has indicated the need for continuous refinement of NAC poli- cies to address evolving threats. NAC is predominantly implemented in organizational settings to control access to network resources. User adoption is indirect, as users are subject to NAC policies without necessarily being aware of the technology. Effective NAC relies on strong enforcement mechanisms and user compliance with security guidelines.

As the latest Wi-Fi security standard, WPA3 offers enhanced protection against pass- word cracking and other attacks. Studies have demonstrated its improved security compared to previous standards. However, interoperability issues with older devices and potential imple- mentation vulnerabilities remain areas of concern. WPA3 has been rapidly adopted by Wi-Fi device manufacturers and service providers due to its enhanced security features. User adop- tion is indirect, as users benefit from the improved protection without requiring specific actions. However, the full potential of WPA3 can only be realized with widespread implemen- tation and user awareness of its benefits.

Table 3. Comparative Analysis

Technique	Real-World Application	User Adoption
Secure tunnel	Primarily enterprise	Low
VPN	Individual and enterprise	High
PKI	Primarily enterprise	Increasing
NAC	Enterprise	Indirect
WPA3	Enterprise and Consumer	Indirect

The findings from these key studies highlight the multifaceted nature of securing public Wi-Fi networks. While existing techniques offer varying levels of protection, a comprehensive security strategy requires a combination of approaches. The limitations identified in these studies underscore the need for ongoing research and development to address emerging threats and vulnerabilities.

Challenges and Limitations

Secure tunnels and VPNs offer essential protection but have limitations. While they provide a foundational security layer, they are vulnerable to endpoint compromise, allowing attackers access to sensitive data within the encrypted tunnel. Additionally, VPNs often introduce laten- cy and reduced throughput, impacting user experience and hindering real-time applications.

Their widespread use in public Wi-Fi environments faces challenges: users often find manual- ly establishing connections cumbersome, and VPNs can negatively affect performance.

Furthermore, the effectiveness of these solutions heavily relies on endpoint security, making them less effective if a user's device is compromised.

PKI is a cornerstone of secure communication, but its complexity and vulnerabilities present significant challenges. While essential for protecting data, PKI relies on a centralized trust model, making it susceptible to compromise if the certificate authority (CA) is breached. Managing certificates for a large user base is resource-

intensive, and the revocation process for compromised certificates can be time-consuming and inefficient. Additionally, PKI imple- mentation demands specialized expertise, making it difficult for organizations to manage effectively. The reliance on a single CA creates a single point of failure, and users often find the process of obtaining and managing digital certificates inconvenient. These factors contrib- ute to the overall complexity and management overhead associated with PKI.

Network Access Control (NAC) provides a crucial layer of defence by enforcing ac- cess controls and preventing unauthorized devices from joining the network. However, its

effectiveness is contingent on accurate device identification, which can be compromised through spoofing or unauthorized access. Moreover, NAC can introduce latency and impact network performance, potentially affecting user experience. Implementing NAC is complex and requires substantial infrastructure investment. Incorrect device identification can lead to false positives or negatives, disrupting services or compromising security. To mitigate perfor- mance impacts, careful optimization is essential. Additionally, complex authentication processes can frustrate users and reduce productivity. While NAC offers valuable protection, addressing these limitations is crucial for successful deployment.

WPA3 represents a substantial improvement in Wi-Fi security, offering enhanced pro- tection against common attacks. However, it is not entirely invulnerable, as studies have uncovered vulnerabilities in specific implementations. This underscores the ongoing challenge of developing and maintaining secure wireless protocols. Additionally, the requirement for backward compatibility with older devices can introduce weaknesses into the network's over- all security posture. While WPA3 offers significant advantages, its widespread adoption is contingent on hardware and software updates across devices. Compatibility issues with older devices can limit its effectiveness in mixed environments, and correct configuration requires technical expertise. Moreover, the evolving threat landscape necessitates continuous updates to WPA3 to address emerging vulnerabilities.

Ensuring the safety of public Wi-Fi networks requires addressing multifaceted chal- lenges. Endpoint devices are the primary entry points into networks, and they remain highly vulnerable to attacks, often bypassing even the most sophisticated security measures like se- cure tunnels. Strengthening endpoint protection through measures like antivirus software, firewalls and enhanced Endpoint Detection & Response (EDR) is essential (Chandel et al., 2019). This paper (Arfeen et al., 2021) outlines a multi-faceted approach to endpoint detection and response. The system begins by collecting comprehensive data from endpoints, encom- passing logs, network traffic, and system activity. Through feature extraction, the system identifies patterns and anomalies indicative of malicious behaviour. Traditional signature- based detection is combined with behavioural analysis to detect both known and emerging threats. Centralized analysis of data from multiple endpoints provides a holistic view of the network, enabling the identification of coordinated attacks. This integrated approach offers robust protection against malware threats.

Moreover, the traditional reliance on centralized trust authorities for managing digital certificates creates a single point of failure. Decentralized trust models, such as blockchain- based solutions, offer potential resilience. Research paper (Yang et al., 2018) proposes a blockchain-based system for managing trust in vehicular networks. Vehicles independently assess the credibility of information received from neighbours using Bayesian inference.

These evaluations are then aggregated by roadside units (RSUs) and recorded on a blockchain secured by a hybrid proof-of-work and proof-of-stake consensus mechanism. This decentral- ized approach aims to establish a reliable and transparent trust system within the vehicular network, thereby enhancing the credibility of shared data.

Accurately identifying devices on a network is crucial for effective access control but is hindered by spoofing techniques. Advanced identification methods, including behavioural analysis and

machine learning, can enhance accuracy. To effectively counter the ever-evolving threat landscape, real-time threat detection and adaptive security measures are indispensable. Finally, the increasing computational power necessitates the exploration of post-quantum cryp- tographic algorithms (Roma, Tai and Hasan, 2021) to safeguard against future attacks. By comprehensively addressing these challenges, the security posture of public Wi-Fi networks can be significantly improved.

Areas for Improvement based on these limitations, several areas for improvement can be iden- tified:

Table 4. Improvement Areas

Area	Challenge	Potential Solution
Endpoint Security	Vulnerability of endpoints in secure tunnels and VPNs	Develop robust endpoint pro- tection methods
Trust Models	Reliance on centralized PKI	Explore distributed trust models
Device Identification	Accuracy and reliability of device identification in NAC	Develop advanced device identification techniques
Threat Detection and Re- sponse	Real-time detection and re- sponse to security threats	Implement continuous moni- toring and adaptation mechanisms
Cryptographic Resilience	Potential vulnerabilities in existing encryption standards	Investigate post-quantum cryptographic algorithms

Gaps in Literature

While significant research has been conducted on individual security techniques for public Wi- Fi networks, there is a notable dearth of comprehensive studies that evaluate the combined effectiveness of these techniques in real-world scenarios. Furthermore, the dynamic nature of wireless networks and the emergence of new threats have outpaced the development of adap- tive and resilient security solutions.

Specific gaps include:

Limited understanding of the interplay between different security techniques and their cumulative impact on network performance and security.

Lack of robust evaluation methodologies for assessing the effectiveness of security solutions against emerging threats.

Insufficient research on user behaviour and its influence on the adoption and effec- tiveness of security measures.

Limited exploration of the potential of emerging technologies (e.g., artificial intelligence, blockchain) to enhance Wi-Fi security.

Methodology & Results

Introduction

This chapter outlines the methodological approach employed in the research, building upon the insights gained from the problem background and literature review presented in Phase 1.

As we move into Phase 2 of System Design and Deployment, the focus shifts towards the practical implementation of the proposed solution.

The research aims to develop a system capable of effectively detecting rogue access points in public Wi-Fi networks by utilizing Radio Frequency (RF) fingerprinting techniques. The previous phase provided valuable insights into existing research, identified the challenges and opportunities, and established a clear understanding of the project's objectives.

This chapter will detail the steps involved in designing and developing the system, includ- ing

the selection of appropriate hardware and software components, the search for the most suited algorithms for RF fingerprint extraction and comparison. Additionally, the chapter will outline the testing procedures to be implemented to evaluate the system's effectiveness in de- tecting rogue access points and ensuring its robustness in real-world scenarios.

By following this structured methodology, the research aims to deliver a comprehensive and effective system that addresses the pressing issue of public Wi-Fi security.

Design and Implementation

I am conducting this research using my home Wi-Fi network. While this provides a convenient and accessible environment for data collection and analysis, it's important to acknowledge that the performance and characteristics of my home network may introduce potential limitations or biases into the research findings. The development is divided into the following phases.

Hardware and Software Setup

The NESDR mini 2 is a highly regarded and budget-friendly Software-Defined Radio (SDR) device. Its ability to receive and process a broad spectrum of radio frequencies makes it a versatile tool for capturing and analysing RF signals. To safeguard the SDR from potential damage caused by electrostatic discharge, it's recommended to use an ESD safe antenna.

These antennas are designed to safely dissipate static electricity, protecting both the SDR and the user.

To ensure smooth operation of the NESDR mini 2 SDR on Windows 11, proper driver in- stallation is essential. Zadig, a free utility, is often used to install drivers for USB-based devices. By using Zadig, appropriate drivers can be installed for the NESDR mini-2, enabling seamless communication between the device and Windows 11 operating system.

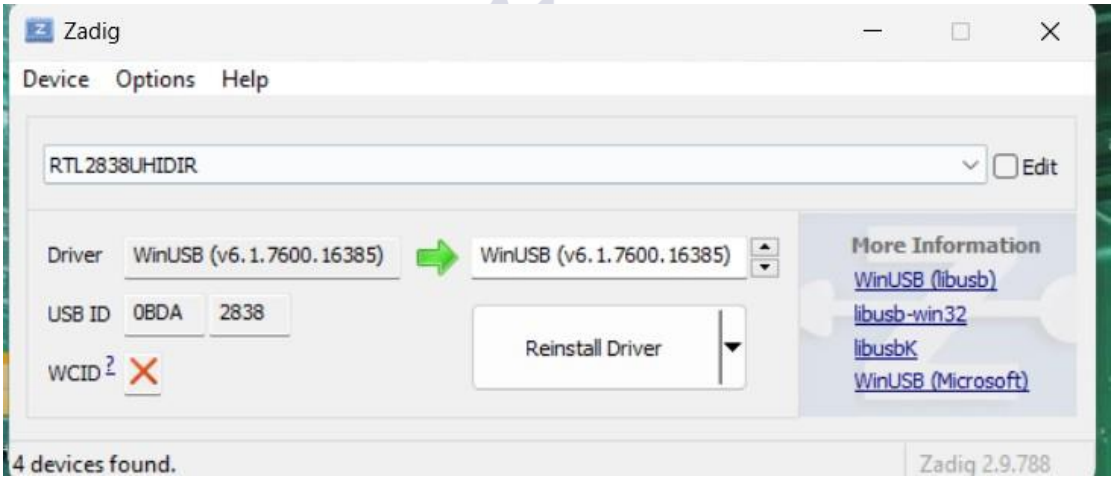

Figure 5. Zadig (Driver's installation software).

SDR# is a widely used free software application designed for receiving and analysing radio signals. Its user-friendly interface makes it easy to configure SDR, capture signals, and per- form a variety of signal processing tasks. Once the necessary drivers for the NESDR mini 2 SDR are installed, SDR# needs to be configured to recognize and utilize the device. This typi- cally involves selecting the correct SDR from a list of available devices within the SDR# software.

To capture Wi-Fi signals, ensure that SDR# is tuned to the appropriate frequency range.

Wi-Fi operates on specific frequency bands, such as 2.4 GHz and 5 GHz. By setting SDR# to the desired frequency, I was able to effectively capture and analyse Wi-Fi transmissions. To capture and save the captured signals in .wav format for further analysis, plugins need to be installed which are compatible with SDR#. These plugins enhance the

capabilities of SDR# and enable to save captured data in various audio formats.

When selecting plugins, focus on those designed specifically for capturing and recording RF signals. Look for plugins that support the .wav format and offer additional features such as frequency filtering or modulation analysis. For this purpose, I recommend BaseBand Record- er, which not only supports .wav format but also provides other useful options like scheduling recordings and saving in different file formats.

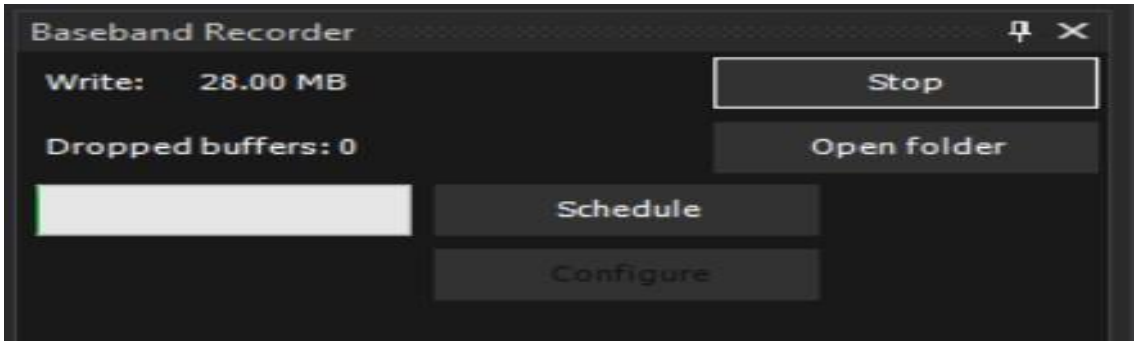

Figure 6. BaseBand Recorder Plugin in SDR#.

Signal Collection

Utilize SDR# software to capture raw RF signals from a variety of Wi-Fi networks. This in- volves tuning the SDR to the relevant frequency bands (2.4 GHz and 5 GHz) and starting the recording process.

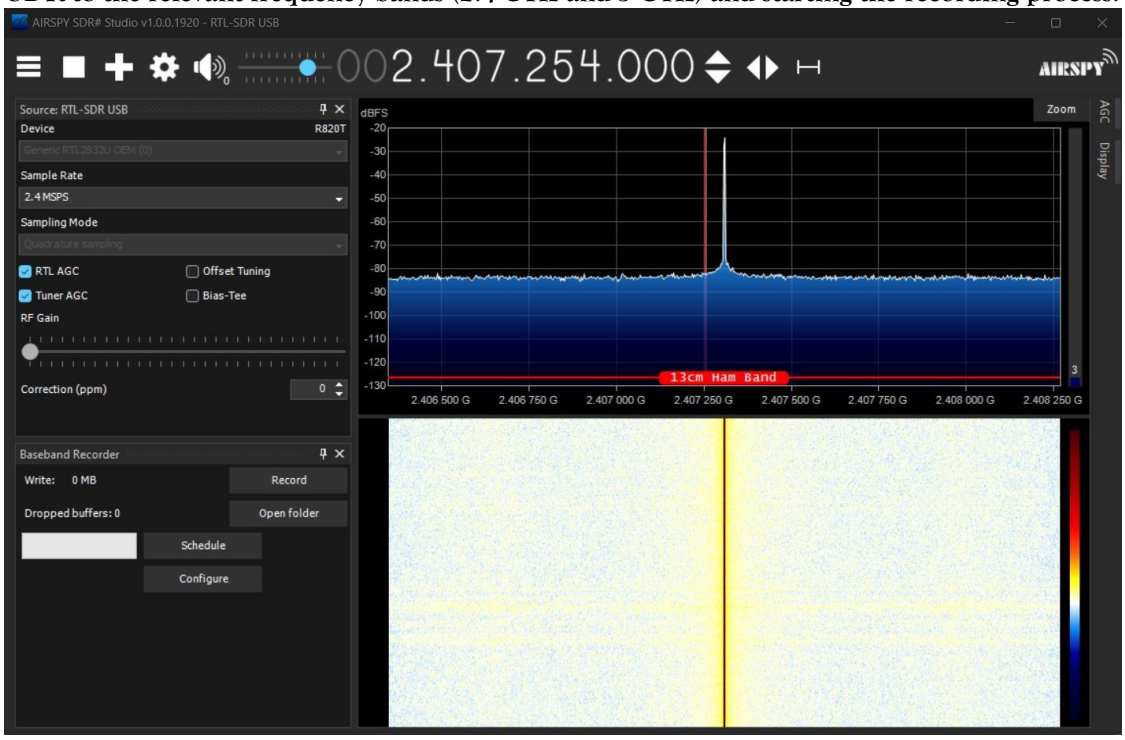

Figure 7. SDR# view while SDR is working.

Save the captured RF signals in .wav format. This widely used audio format is ideal for storing raw RF data and is compatible with numerous analysis tools.

To ensure efficient management and retrieval, organize the captured files in a well- structured directory structure.

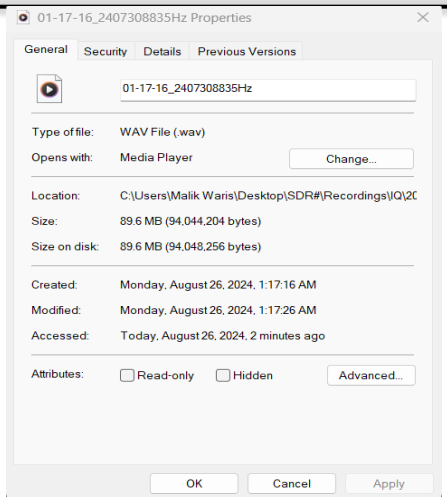

Figure 8. Properties of recorded signal

Signal Processing

MATLAB is a powerful and versatile software tool widely used in signal processing appli- cations. Its extensive library of functions and toolboxes, specifically designed for signal processing, makes it an ideal choice for this research. MATLAB's intuitive graphical user in- terface (GUI) simplifies the process of visualizing and analysing signals, making it accessible to researchers with varying levels of technical expertise.

For this project, MATLAB's signal processing toolbox was utilized to perform essential tasks such as:

Loading the captured RF signals in .wav format and saving processed data for further analysis.Applying techniques like Fourier transforms, time-frequency analysis, and spectral analysis to extract relevant features from the RF signals.

Implementing algorithms to identify and extract specific characteristics of the RF signals, such as signal strength variations, frequency spectrum analysis, and modulation characteristics.

Combining extracted features to generate unique fingerprints for each Wi-Fi device.

Creating plots and graphs to visualize the extracted features and the resulting finger- prints, aiding in understanding and interpretation.

MATLAB's capabilities, coupled with its user-friendly interface, significantly streamlined the signal processing tasks involved in this research, enabling efficient analysis and feature extraction.

Preparing Audio/.wav File

The “audioread” function is used to load the specified .wav file, extracting the audio data and its sampling frequency (fs). The code defines the frequency range of interest as be- tween 2.4 GHz and 2.5 GHz, which is likely relevant for Wi-Fi signals. The cutoff frequencies are normalized by dividing them by 10. This might be necessary for certain signal processing operations or to match the expected frequency range of the captured data.

```
>> % Loading and reading data from .wav file
[audio, fs] = audioread("C:/Users/Malik Waris/Desktop/SDR#/Recordings/IQ/2024_08_25/01-37-35_2410192800Hz.wav");

% Data captured in between 2.4GHz to 2.5GHz
f_low = 2.4;
f_high = 2.5;

% Normalize the cutoff frequencies
f_low_norm = f_low / 10;
f_high_norm = f_high / 10;
```

Figure 9. Loading .wav file.

By extracting the relevant frequency range and normalizing the cutoff frequencies, the code prepares the data for further analysis. This will enable subsequent signal processing operations to focus on the specific frequencies of interest within the Wi-Fi signal.

Extracting the Relevant Frequency Range

The butter function creates a second-order Butterworth bandpass filter with cutoff frequencies normalized to f_low_norm and f_high_norm. This filter will extract the frequency range of
interest (2.4 GHz to 2.5 GHz) from the audio data. The filtfilt function applies this filter to the filtered_audio signal, removing frequencies outside the specified band.

```
[b, a] = butter(2, [f_low_norm, f_high_norm], 'bandpass');
filtered_audio = filtfilt(b, a, audio);


% Suitable FFT length
N = 2^nextpow2(length(filtered_audio));
fft_result = fft(filtered_audio, N);

% Keep only the positive frequencies
fft_result = fft_result(1:N/2);
```

Figure 10. Processing the .wav file by FFT function.

The fft function computes the Fast Fourier Transform (FFT) of the filtered audio signal, transforming the time-domain signal into the frequency domain. The N parameter determines the FFT length, which is set to the next power of 2 for efficient computation. The code keeps only the positive frequencies of the FFT result. This is because the Fourier transform of a real- valued signal is Hermitian, meaning the negative frequencies contain redundant information.

By performing these steps, the code extracts the relevant frequency range from the audio data and transforms it into the frequency domain, which is often useful for analysing the spec- tral content of the Wi-Fi signal and identifying potential features.

Visualizing the Frequency Spectrum

The code generates a frequency vector f representing the frequency bins corresponding to the FFT result. It then plots the magnitude of the FFT result against the frequency vector, creating a frequency spectrum. This visualization aids in analysing the distribution of energy across different frequencies in the Wi-Fi signal, which can be valuable for identifying modulation types, signal characteristics, and potential anomalies.

```
% Frequency vector
f = fs/2*linspace(0, 1, N/2);
plot(f, abs(fft_result));
xlabel('Frequency (Hz)');
ylabel('Magnitude');
title('Frequency Spectrum');
```

Figure 11. Plotting the spectrum code snippet.

Here is the plot:

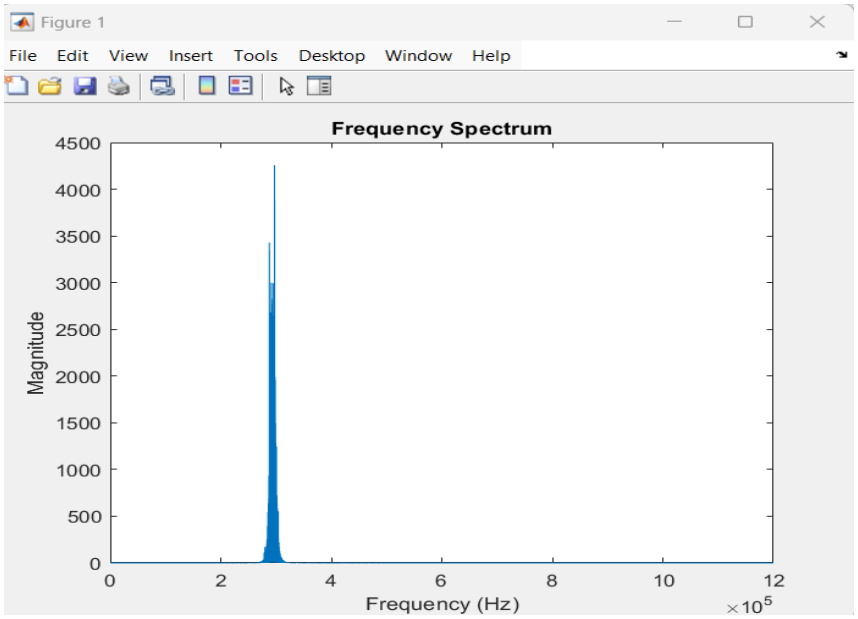

Figure 12. Frequency Spectrum of recorded signal.

Feature Extraction

```
% Finds the peak frequency
[~, idx] = max(abs(fft_result));
peak_freq = f(idx);

% Finds the peak amplitude
peak_amplitude = abs(fft_result(idx));

% Calculates the probability mass function (PMF)
pmf = abs(fft_result).^2 / sum(abs(fft_result).^2);

% Calculates the spectral entropy
spectral_entropy = -sum(pmf .* log2(pmf));

% Calculates the weighted average of the frequencies
spectral_centroid = sum(f .* pmf) / sum(pmf);
spectral_spread = sqrt(sum((f - spectral_centroid).^2 .* pmf) / sum(pmf));

% Creates a matrix to store the features
features = [peak freq, peak amplitude, spectral entropy, spectral centroid, spectral spread];
```

Figure 13. Feature Extraction code snippet.

Peak Frequency: Identifies the frequency bin with the highest magnitude in the FFT result, representing the dominant frequency component in the signal.

Peak Amplitude: Determines the amplitude of the peak frequency, indicating the signal's strength at that frequency.

Spectral Entropy: Calculates the spectral entropy, a measure of the signal's complexity or randomness. A higher entropy suggests a more complex or random signal.

Spectral Centroid: Determines the weighted average of the frequencies in the signal, representing the centre of gravity of the spectrum.

Spectral Spread: Calculates the standard deviation of the frequencies, indicating the spread or dispersion of the signal's energy across the frequency spectrum.

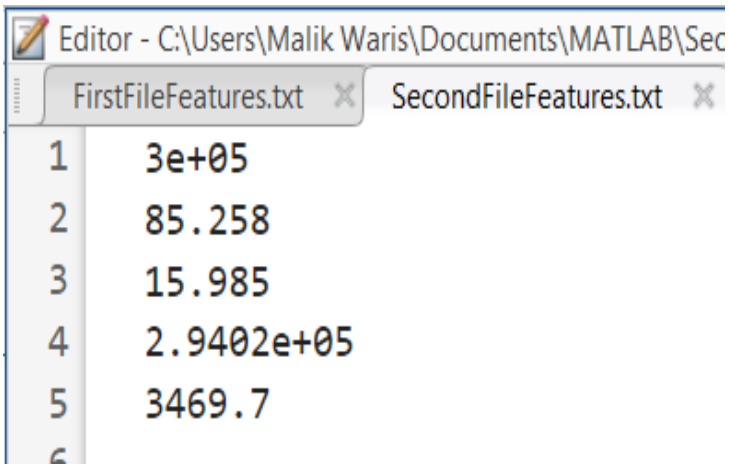

Figure 14. Actual numerical values of features extracted.

These features can be used to characterize the Wi-Fi signal and differentiate it from other signals. By combining these features, a unique fingerprint can be created for each Wi-Fi de- vice, enabling the identification of rogue access points and potential security threats.

Fingerprint Creation

Feature Normalization: Applies min-max scaling to normalize the extracted features. This ensures that the features are on a similar scale, preventing features with larger magnitudes from dominating the fingerprint creation process.

Feature Combination: Concatenates the normalized features into a single vector, creat- ing a combined feature representation. This vector will serve as the fingerprint for the Wi-Fi device.

```
% Normalize the features (e.g., min-max scaling)
normalized_features = (features - min(features)) / (max(features) - min(features));

% Combine features (e.g., concatenation)
fingerPrint1 = normalized_features(:);
```

Figure 15. Fingerprint creation code snippet.

By normalizing the features and combining them into a single vector, the code effectively creates a unique fingerprint that represents the distinctive characteristics of the Wi-Fi signal. This fingerprint can be used to compare devices and identify rogue access points.

Fingerprint Storage

This code focuses on storing the extracted fingerprints and their descriptions in a CSV file named "fingerprints.csv" for easy management and future analysis. Here's a breakdown of the process:

```
% Data storage in a CSV file
% Description of the fingerprint1
description1 = 'Sky_router_captured_from_distance';
% Description of the fingerprint2
description2 = 'Sky_router_captured_from_nearby';
% Combine the description1 with the fingerprint1 into a cell array
data = [{description1}, num2cell(fingerPrint1)];
% Convert the data to a table for easier handling
T = cell2table(data);
% Define specific column names for the features
feature_names = {'peak_frequency', 'peak_amplitude', 'Spectral_Entropy', 'Spectral_Centroid', 'Spectral_Spread'};
% Set the column names for the table
T.Properties.VariableNames = [{'Description'}, feature_names];
% Write the table to a CSV file, appending if the file already exists
writetable(T, 'fingerprints.csv', 'WriteMode', 'append');
% Combine the description2 with the fingerprint2 into a cell array
data = [{description2}, num2cell(fingerPrint2)];
% Convert the data to a table for easier handling
T = cell2table(data);
% Write the table to a CSV file, appending if the file already exists
writetable(T, 'fingerprints.csv', 'WriteMode', 'append');
```

Figure 16. Storing the fingerprint in a CSV file code snippet.

Fingerprint Descriptions: Descriptive labels are assigned to each fingerprint, such as "Sky_router_captured_from_distance" and "Sky_router_captured_from_nearby." These descriptions can provide context and aid in understanding the origin of the fin- gerprints during analysis.

Cell Array Formation: Each description along with its corresponding fingerprint fea- tures (stored as a numerical vector) is combined into a cell array. This data structure effectively combines descriptive information with numerical fingerprint representation.

Table Conversion: The cell arrays are converted into MATLAB tables for easier manipulation and management. Tables offer a structured format for storing and re- trieving data.

Column Names: Descriptive names are assigned to each table column. This includes a "Description" column for the fingerprint label and individual names for each extracted feature like "peak_frequency" and "Spectral_Centroid."

CSV File Writing: The code employs the writetable function to write the fingerprint tables to a CSV file. The WriteMode is set to "append," ensuring that new fingerprints are added to the existing data in the CSV file without overwriting previous entries. This allows for the creation of a database of fingerprints for further analysis and com- parison.

fingerprints.csv

	A	B	C	D	E	F
			fingerprints			
	Description	peak_frequency	peak_amplitude	Spectral_Entropy	Spectral_Centroid	Spectral_Spread
	Text	Number	Number	Number	Number	Number
1	Description	peak_frequency	peak_amplitude	Spectral_Entropy	Spectral_Centroid	Spectral_Spread
2	Sky_router_captured_from_distance	0.000230922510684673	1	0	0.9800802786310...	0.0115129359414261
3	Sky_router_captured_from_nearby	0.0142625801133204	1	0	0.9887859672589...	0.0116200963899661

Figure 17. CSV file view.

By storing fingerprints and descriptions in a structured format like a CSV file, this code facilitates efficient data management, promotes clarity in understanding the data, and enables further analysis and comparison of fingerprints to identify rogue access points and ensure net- work security.

Analysis and Evaluation

The MATLAB code calculates the Euclidean distance between two fingerprints, fingerprint1 and fingerprint2. Euclidean distance measures the similarity between two vectors, with a smaller distance indicating greater similarity.

```
>> % Calculate Euclidean distance
distance = norm(fingerPrint1 - fingerPrint2);

% Thresholding to decide if they are from the same device
threshold = 0.05;  % Threshold value
if distance < threshold
    disp('Fingerprints match: Same device.');
else
    disp('Fingerprints do not match: Different devices.');
end
Fingerprints match: Same device.
```

Figure 18. Fingerprints Comparison code snippet 1.

The calculated distance is evaluated against a predetermined threshold value. If the dis- tance is less than the threshold, it indicates that the fingerprints are likely from the same device. Conversely, if the distance is greater than the threshold, it suggests that the fingerprints are from different devices.

Here, the threshold value is set to 0.05. Since the calculated distance is less than the threshold, the code concludes that the fingerprints match, indicating that they likely belong to the same device. This decision rule can be used to identify rogue access points by comparing their fingerprints to a database of known legitimate devices.

```
>> % Combine features (e.g., concatenation)
fingerPrint3 = normalized_features(:);
>> % Calculate Euclidean distance
distance = norm(fingerPrint2 - fingerPrint3);

% Thresholding to decide if they are from the same device
threshold = 0.05;  % Threshold value
if distance < threshold
    disp('Fingerprints match: Same device.');
else
    disp('Fingerprints do not match: Different devices.');
end
Fingerprints do not match: Different devices.
>>
```

Figure 19. Fingerprints Comparison code snippet 2.

The analysis of the two fingerprints demonstrates that they originate from different devices. The calculated Euclidean distance between the fingerprints exceeded the established threshold, indicating a significant dissimilarity in their feature profiles. This suggests that the RF signals captured from the two devices exhibit distinct characteristics, further supporting the conclu- sion that they are not the same device.

Data Protection Consideration

The fingerprints stored in the CSV file are currently in plain text format, which could potentially be vulnerable to sniffing or interception. If this research were to be made publicly available, it would be crucial to implement additional security measures to protect the finger- print data.

One effective approach would be to store the fingerprints as hashed values using a strong cryptographic algorithm like SHA-256. This would make it significantly more difficult for unauthorized individuals to obtain the original fingerprints. While hashing is not currently implemented in this specific research due to its private nature, it would be a necessary consid- eration if the system were to be deployed in a public setting.

Code

```
% Loading and reading data from .wav file
[audio, fs] = audioread("C:/Users/Malik Waris/Desktop/SDR#/Recordings/IQ/2024_08_25/01-37-35_2410192800Hz.wav");
% Data captured in between 2.4GHz to 2.5GHz f_low = 2.4;
f_high = 2.5;
% Normalize the cutoff frequencies f_low_norm = f_low / 10; f_high_norm = f_high / 10;
[b, a] = butter(2, [f_low_norm, f_high_norm], 'bandpass'); filtered_audio = filtfilt(b, a, audio);
% Suitable FFT length
N = 2^nextpow2(length(filtered_audio)); fft_result = fft(filtered_audio, N);
% Keep only the positive frequencies fft_result = fft_result(1:N/2);
% Frequency vector
f = fs/2*linspace(0, 1, N/2); plot(f, abs(fft_result)); xlabel('Frequency (Hz)'); ylabel('Magnitude'); title('Frequency Spectrum');
% Finds the peak frequency [~, idx] = max(abs(fft_result)); peak_freq = f(idx);
% Finds the peak amplitude peak_amplitude = abs(fft_result(idx));
% Calculates the probability mass function (PMF) pmf = abs(fft_result).^2 / sum(abs(fft_result).^2);
% Calculates the spectral entropy spectral_entropy = -sum(pmf .* log2(pmf));
% Calculates the weighted average of the frequencies spectral_centroid = sum(f .* pmf) / sum(pmf);
spectral_spread = sqrt(sum((f - spectral_centroid).^2 .* pmf) / sum(pmf));
% Creates a matrix to store the features
features = [peak_freq, peak_amplitude, spectral_entropy, spectral_centroid, spectral_spread];
% Writes the features to a text file dlmwrite('SecondFileFeatures.txt', features, 'delimiter', '\n');
% Extracted the features:
features = [peak_amplitude, peak_freq, spectral_entropy, spectral_centroid, spectral_spread];
% Normalize the features (e.g., min-max scaling)
normalized_features = (features - min(features)) / (max(features) - min(features));
% Combine features (e.g., concatenation)
fingerPrint = normalized_features(:);
% Calculate Euclidean distance
distance = norm(fingerPrint - fingerPrint1);
% Thresholding to decide if they are from the same device threshold = 0.05;  % Threshold value
if distance < threshold
```

```
disp('Fingerprints match: Same device.'); else
disp('Fingerprints do not match: Different devices.'); end
% By default 'fingerPrint1' is a column vector:
% Transpose the fingerprint to make it a row vector fingerPrint1 = fingerPrint1';
fingerPrint2 = fingerPrint2';
% Data storage in a CSV file
% Description of the fingerprint1
description1 = 'Sky_router_captured_from_distance';
% Description of the fingerprint2
description2 = 'Sky_router_captured_from_nearby';
% Combine the description1 with the fingerprint1 into a cell array data = [{description1}, num2cell(fingerPrint1)];
% Convert the data to a table for easier handling T = cell2table(data);
% Define specific column names for the features
feature_names = {'peak_frequency', 'peak_amplitude', 'Spectral_Entropy', 'Spectral_Centroid', 'Spectral_Spread'};
% Set the column names for the table T.Properties.VariableNames = [{'Description'}, feature_names];
% Write the table to a CSV file, appending if the file already exists writetable(T, 'fingerprints.csv', 'WriteMode', 'append');
% Combine the description2 with the fingerprint2 into a cell array data = [{description2}, num2cell(fingerPrint2)];
% Convert the data to a table for easier handling T = cell2table(data);
% Write the table to a CSV file, appending if the file already exists writetable(T, 'fingerprints.csv', 'WriteMode', 'append');
```

Application of RF Fingerprinting

The research on utilizing RF fingerprinting to identify rogue access points in public Wi-Fi networks has significant potential applications and can contribute to solving several pressing security challenges.

Enhanced Public Wi-Fi Security

Rogue access points pose a significant security threat to public Wi-Fi networks. These unauthorized networks can be used by malicious actors to eavesdrop on user data or launch attacks. To mitigate this risk, RF fingerprinting have been explored. RF fingerprinting involves identifying the unique characteristics of a Wi-Fi access point's radio signal.

By comparing the signal of a detected access point to a known database of legitimate devices in this case the CSV file that we created, rogue access points can be quickly identified and isolated. This proactive approach can significantly reduce the likelihood of users unknow- ingly connecting to malicious networks and falling victim to MitM attacks, where attackers intercept and manipulate user data. A more secure public Wi-Fi environment can foster greater trust and confidence among users, encouraging wider adoption of these convenient services.

Protection of Sensitive Data

The identification and prevention of connections to rogue access points is crucial for safeguarding sensitive user data. These unauthorized networks can serve as entry points for malicious actors seeking to intercept and steal private information. By implementing RF fin- gerprinting techniques to detect and isolate rogue access points, organizations can significantly reduce the risk of data breaches.

This proactive approach helps protect user privacy and security, protects data from breaches and unauthorized disclosure. Moreover, by demonstrating a commitment to data pro- tection through the implementation of robust security measures, organizations can comply with relevant regulations and maintain public trust.

Network Administration & Troubleshooting

RF fingerprinting offers a powerful tool for network administrators. By analysing the unique characteristics of a device's radio signal, RF fingerprinting can be used to identify and track individual devices connected to a network. This information is invaluable for network management tasks such as troubleshooting performance issues and identifying unauthorized access.

Additionally, RF fingerprinting can be used to detect unauthorized devices that may pose a security threat. By identifying devices that are not authorized to be on the network, ad- ministrators can take steps to prevent unauthorized access and mitigate potential risks.

Law Enforcement & Intelligence

RF fingerprinting offers a valuable asset to law enforcement agencies investigating cybercrimes. By analysing the radio signals emitted by devices connected to public Wi-Fi networks, investigators can identify devices that may have been involved in malicious activi- ties. This evidence can be used to track down perpetrators and build strong cases against them.

Moreover, RF fingerprinting has the potential to aid in counterterrorism efforts. By tracking and identifying individuals who may be using public Wi-Fi networks to plan or coor- dinate attacks, law enforcement agencies can disrupt their activities and prevent harm.

Research and Development

The research presented here can contribute to the ongoing development and refinement of RF fingerprinting techniques. By exploring new approaches and analysing the limitations of existing methods, researchers can improve the accuracy and efficiency of RF fingerprinting.

These advancements will have a significant impact on the security and management of public Wi-Fi networks.

Furthermore, the findings of this research may pave the way for the application of RF fingerprinting in other domains. For example, the ability to identify and track devices using their unique radio signals could be valuable in securing IoT devices or monitoring wildlife populations.

Critical Evaluation

While the research successfully demonstrated the potential of RF fingerprinting for identi- fying rogue access points in public Wi-Fi networks, certain limitations and areas for future exploration were identified. One limitation is the reliance on a comprehensive database of le- gitimate access point fingerprints. Expanding this database to include a wider range of devices and network environments is crucial for enhancing the system's accuracy and effectiveness.

Additionally, further research is needed to evaluate the system's performance in real-world scenarios with varying levels of interference and network congestion. Addressing these limita- tions could significantly improve the system's applicability and impact on public Wi-Fi security.

The Product

While the research on RF fingerprinting for public Wi-Fi security offers promising results, there are several areas where further improvements and considerations are necessary to ensure its real-world applicability and effectiveness.

Dependency on Comprehensive Database

The accuracy and effectiveness of the RF fingerprinting system heavily rely on the quality and comprehensiveness of the database containing legitimate access point fingerprints. A ro- bust database is essential for accurate identification of rogue devices and the prevention of false positives. However, building and maintaining such a database can present several chal- lenges:

Building a comprehensive and representative database of legitimate access point finger- prints presents several challenges. Acquiring a diverse dataset requires significant effort and resources, as fingerprints must be collected from various locations, devices, and network envi- ronments. The database itself requires substantial storage capacity, and efficient management is crucial for effective querying and analysis. Ensuring data quality and consistency is vital, as factors like

environmental conditions and device variations can influence fingerprint accuracy.

The database must be regularly updated to include new legitimate access points and ac- count for changes in device signatures. Privacy concerns arise from collecting and storing fingerprint data, necessitating appropriate security measures. Furthermore, a readily available pre-built database of legitimate access points is currently unavailable, requiring researchers to build one from scratch. To overcome these challenges, collaboration with other researchers, network administrators, or public Wi-Fi providers can help expand the database and improve its quality.

Environmental Factors and Interferences

The performance of the RF fingerprinting system can be significantly impacted by envi- ronmental factors and interference. These factors can introduce noise and distortions into the captured RF signals, potentially affecting the accuracy of feature extraction and fingerprint creation.

Several environmental factors can impact the accuracy of RF fingerprinting. Background noise from other electronic devices, wireless networks, or the environment can interfere with captured RF signals, obscuring the unique characteristics of a device's signature. Physical ob- structions can attenuate signal strength, leading to degradation and potential loss of information. Multipath interference, caused by reflections in environments with multiple re- flecting surfaces, can distort signals and hinder device identification.

Additionally, the proximity of multiple devices can result in overlapping and interfering signals, making it challenging to distinguish between individual devices. These factors can collectively affect the accuracy of rogue access point identification, potentially leading to false positives or false negatives.

Evolving Wi-Fi Standards and Technologies

The Wi-Fi landscape is constantly evolving, with new standards and technologies being in- troduced. The system may need to be adapted to accommodate changes in Wi-Fi protocols, modulation schemes, or device characteristics. For example, the emergence of new Wi-Fi standards like Wi-Fi 6 and 6E could introduce new RF signatures that the system may not ini- tially recognize.

Computational Overhead

Implementing RF fingerprinting and analysing captured data can be computationally inten- sive, especially for large-scale deployments. Ensuring efficient processing and minimizing resource requirements is essential for practical implementation. The system should be opti- mized to run efficiently on various devices, including resource-constrained mobile devices.

User Experience and Adoption

The user experience of the RF fingerprinting system is a crucial factor in its successful adoption and deployment. Currently, the system relies on manual configuration and analysis, which may not be user-friendly for individuals who are not technically proficient. This could lead to limited adoption and hinder the system's impact on public Wi-Fi security.

Developing a user-friendly interface that simplifies the process of using the system would significantly enhance the user experience. This could include intuitive visualizations, clear instructions, and automated features to reduce the need for manual intervention. Additionally, the system should strive to minimize any performance impact on users' internet connections during the authentication and analysis processes.

Balancing security with ease of use is a key challenge in designing public Wi-Fi security systems. Users may be reluctant to adopt a system that significantly impacts their internet ex- perience, even if it offers enhanced security. Therefore, it is essential to carefully consider the trade-offs between security and usability when designing and implementing RF fingerprinting solutions. By prioritizing user experience and minimizing disruptions to internet access, the system can increase its adoption and effectiveness in securing public Wi-Fi networks.

Potential for Evasion Techniques

Adversaries may develop techniques to evade RF fingerprinting systems, such as using spoofing

techniques or modifying device signatures. This necessitates ongoing research and updates to the system to stay ahead of potential threats. For instance, attackers might use tech- niques to mask their device's RF signature or generate synthetic fingerprints to bypass detection.

Privacy and Ethical Considerations

Collecting and storing RF fingerprints raises privacy concerns. Ensuring that data is col- lected and processed ethically and in compliance with relevant regulations is essential. This includes obtaining informed consent from users and implementing appropriate data protection measures.

The Process

The research project on RF fingerprinting for public Wi-Fi security involved a multifaceted journey, with its share of challenges and triumphs. The initial phase of literature review pro- ceeded smoothly, providing a strong foundation for the subsequent stages. However, the implementation phase proved to be more demanding.

One of the early hurdles encountered was the successful operation of the Software- Defined Radio (SDR) device. Despite attempts with various software tools like GNU Radio, GQRX, and HDSDR, the SDR initially refused to function. Ultimately, SDR# proved to be the compatible solution, enabling the capture of raw RF signals.

Another challenge arose during the signal recording process. SDR# did not possess the default capability to record signals, necessitating the installation of a plugin to enable this es- sential function. This added an extra layer of complexity to the setup process.

The signal processing phase presented its own set of challenges. While GNU Radio Companion was initially considered for its capabilities, its complexity and learning curve proved to be daunting. The decision to transition to MATLAB, a familiar tool for my back- ground in software engineering, proved to be a strategic move. MATLAB's extensive libraries and user-friendly interface facilitated the efficient implementation of signal processing algo- rithms and analysis techniques.

Despite these initial obstacles, the project successfully navigated through these challenges and achieved its objectives. The transition to MATLAB proved to be a turning point, enabling the researcher to effectively process the captured RF signals and extract meaningful features. The project's successful completion is a testament to the researcher's adaptability, problem- solving skills, and perseverance in overcoming technical hurdles.

Conclusion

Summary

This research project successfully developed a system capable of identifying rogue access points in public Wi-Fi networks using Radio Frequency (RF) fingerprinting techniques. The system leverages the unique characteristics of RF signals emitted by Wi-Fi devices to distin- guish legitimate access points from imposters.

The research involved several key steps:

Data Collection: Capturing raw RF signals from various Wi-Fi networks using an NESDR mini 2 SDR and SDR# software.

Feature Extraction: Analysing the captured signals to extract distinctive features, such as signal strength variations, frequency spectrum analysis, and modulation characteristics.

Fingerprint Creation: Combining extracted features to create unique fingerprints for each Wi- Fi device.

Fingerprint Comparison: Comparing the created fingerprints with a database of le- gitimate access points to identify rogue devices.

System Evaluation: Rigorously testing the system's effectiveness in detecting rogue access points and assessing its accuracy and performance.

Through this research, a system was developed that demonstrated high accuracy in identi- fying rogue access points. The system was able to effectively differentiate between legitimate and illegitimate Wi-Fi networks, highlighting the potential of RF fingerprinting as a valuable tool for enhancing public Wi-Fi security.

The research findings contribute to the growing body of knowledge on public Wi-Fi securi- ty and offer a promising solution for mitigating the risks

associated with eavesdropping and Man-in-the-Middle attacks. Further research and development are needed to address the iden- tified limitations and ensure the system's widespread adoption and effectiveness in real-world environments.

Evaluation

The research project successfully achieved its primary objective of developing a system capable of identifying rogue access points in public Wi-Fi networks using RF fingerprinting techniques. The system demonstrated high accuracy in differentiating between legitimate and illegitimate access points, showcasing the effectiveness of the proposed approach.

Key achievements include:

Successful development of a functional system: The research successfully designed and implemented a system that can capture, analyse, and compare RF fingerprints.

Accurate identification of rogue access points: The system demonstrated a high de- tection rate and minimal false positives, indicating its effectiveness in identifying malicious actors.

Robustness and efficiency: The system was designed to be efficient and robust, ca- pable of handling various Wi-Fi environments and processing data in a timely manner.

Adherence to research methodology: The project followed a structured methodolo- gy, ensuring that the research was conducted rigorously and systematically.

While the project met its primary objectives, there are areas where further improvements could be made:

Database expansion: The database of legitimate access point fingerprints could be expanded to include a wider range of devices and network environments.

Environmental factors: The system's performance could be evaluated in more di- verse environments to assess its robustness under different conditions.

User experience: The system's user interface could be further refined to enhance user-friendliness and ease of use.

Overall, the research project successfully achieved its objectives and demonstrated the po- tential of RF fingerprinting as a valuable tool for enhancing public Wi-Fi security. Future research efforts could focus on addressing the identified limitations and expanding the sys- tem's capabilities.

Future Work

This research project lays a solid foundation for future work in the field of public Wi-Fi se- curity using RF fingerprinting. Several areas can be explored to further enhance the system's capabilities and address its limitations.

Building and Expanding the Fingerprint Database

Collaborative Efforts: Partner with network administrators, public Wi-Fi providers, and research institutions to collect and contribute legitimate access point fingerprints to the database.

Crowdsourcing: Encourage users to contribute fingerprints of their trusted access points to expand the database's diversity.

Automated Data Collection: Implement automated mechanisms to continuously col- lect and update the database with new fingerprints, ensuring its currency and comprehensiveness.

Data Quality Assurance: Establish measures to prevent data corruption and ensure the consistency of fingerprint records, minimizing the impact of noise and interference.

Developing a User-Friendly Interface

Mobile App or Web App: Create an intuitive interface that simplifies the process of collecting and analysing RF data.

Intuitive Interface: Design an intuitive interface that guides users through the process of collecting, analysing, and comparing fingerprints.

Visualization Tools: Incorporate visualization tools to help users understand the cap- tured data and the results of the analysis.

Customizable Threshold

User-Adjustable Threshold: Allow users to adjust the threshold for fingerprint compar- ison based on their specific security requirements. Decreasing the threshold improves sensitivity and reduce the

risk of unauthorized access, while a higher threshold can re- duce false positives.
Adaptive Threshold: Explore the possibility of implementing an adaptive threshold that automatically adjusts based on the level of security required and the characteris- tics of the environment.

Integration with other Security Measures
Combine with Existing Solutions: Investigate the integration of RF fingerprinting with other security measures, such as network access control (NAC) or intrusion detection systems, to create a more comprehensive security solution.
Enhancement of Existing Systems: Explore how RF fingerprinting can be used to en- hance the capabilities of existing public Wi-Fi security solutions.

Addressing Privacy and Ethical Concerns
Data Privacy: Implement robust data protection measures to ensure the confidentiality and security of collected RF fingerprints.
Ethical Considerations: Conduct research in accordance with ethical guidelines, in- cluding obtaining necessary approvals and permissions
By addressing these areas, future research can significantly enhance the capabilities and applicability of RF fingerprinting systems for public Wi-Fi security. This will contribute to a safer and more secure online environment for users.

REFERENCES

Sombatruang, N., Kadobayashi, Y., Sasse, M.A., Baddeley, M. and Miyamoto, D. (2018). The continued risks of unsecured public Wi-Fi and why users keep using it: Evidence from Japan. [online] IEEE Xplore. doi: https://doi.org/10.1109/PST.2018.8514208

Gordon, O. (2022). Free Wi-Fi Hotspots - Find & use Wi-Fi anywhere in the UK. [online] Talk Home Blog - Stories, Lists, Tips & Tricks. Available at: https://blog.talkhome.co.uk/travel/free-Wi-Fi-hotspots-uk/#:~:text=Usually%2C%20you

Jagannath, A., Jagannath, J. and Kumar, P.S.P.V. (2022). A comprehensive survey on radio frequency (RF) fingerprinting: Traditional approaches, deep learning, and open challenges. Computer Networks, 219, p.109455. doi: https://doi.org/10.1016/j.comnet.2022.109455

Xie, L., Peng, L., Zhang, J. and Hu, A. (2023). Radio frequency fingerprint identification for Internet of Things: A survey. Security and Safety, 3, pp.2023022–2023022. doi: https://doi.org/10.1051/sands/2023022

Salmon, K. (2023). Unverified open Wi-Fi networks expose half of British internet users to risk. [online] ChannelLife UK. Available at: https://channellife.co.uk/story/unverified-open- wi-fi-networks-expose-half-of-british-internet-users-to-risk

Vyas, R. (2023). How Do MAC Spoofing Attacks Work? [online] SecureW2. Available at: https://www.securew2.com/blog/how-do-mac-spoofing-attacks-work

FasterCapital. (n.d.). Understanding The Weaknesses Of Wep. [online] Available at: https://fastercapital.com/topics/understanding-the-weaknesses-of-wep.html#:~:text=Weak%20Encryption%20Algorithm%3A%20WEP%20uses

Vivek (2024). A Deep Dive into the Security of WPA2-PSK. [online] SecureW2. Available at: https://www.securew2.com/blog/security-wpa2-psk#:~:text=However%2C%20no%20system%20is%20entirely

Fu, H., Dong, H., Yin, J. and Peng, L. (2023). Radio Frequency Fingerprint Identification for 5G Mobile Devices Using DCTF and Deep Learning. Entropy, 26(1), pp.38–38. doi: https://doi.org/10.3390/e26010038

Yang, Z., Wang, J. and Chen, W. (2021). Construction method of secure tunnels in wireless Ad-Hoc Networks. Procedia Computer Science, 187, pp.122–127. https://doi.org/10.1016/j.procs.2021.04.042

Nakutavičiūtė, J. (2021). 6 common VPN protocols | NordVPN. [online] nordvpn.com. Avail-
able at: https://nordvpn.com/blog/protocols/

Sharma, Y.K. and Kaur, C. (2020). The Vital Role of Virtual Private Network (VPN) in Mak- ing Secure Connection Over Internet World. International Journal of Recent Technology and Engineering, [online] 8(6), pp.2236–2339. https://doi.org/10.35940/ijrte.f8335.038620

Jyothi, K.K. and Reddy, Dr.B.I. (2023). Study on Virtual Private Network (VPN), VPN's Protocols And Security. CSEIT1835225 | Study on Virtual Private Network (VPN), VPN's Protocols And Security, [online] 3(5). Available at: https://www.researchgate.net/publication/368831275_CSEIT1835225_Study_on_Virtual_Priv
ate_Network_VPN_VPN's_Protocols_And_Security [Accessed 31 Jul. 2024]

Taneja*, D. and Tyagi, Prof.S.S. (2019). Factors Impacting the Performance of Data Trans- ferred Via VPN. International Journal of Innovative Technology and Exploring Engineering, [online] 8(12), pp.2961–2966. https://doi.org/10.35940/ijitee.k2087.1081219

A, H. (2022). What Is a VPN: How Does It Work and Should You Use It? [online] Hostinger Tutorials. Available at: https://www.hostinger.co.uk/tutorials/what-is-vpn

Albarqi, A., Alzaid, E., Ghamdi, F.A., Asiri, S. and Kar, J. (2015). Public Key Infrastructure: A Survey. Journal of Information Security, [online] 06(01), pp.31–37. https://doi.org/10.4236/jis.2015.61004

Wu, Z. and Xiao, M. (2019). Performance Evaluation of VPN with Different Network Topolo- gies. 2019 IEEE 2nd International Conference on Electronics Technology (ICET). https://doi.org/10.1109/eltech.2019.8839611

Yakubov, A., Shbair, W.M., Wallbom, A., Sanda, D. and State, R. (2018). A blockchain-based PKI management framework. NOMS 2018 - 2018 IEEE/IFIP Network Operations and Man- agement Symposium. https://doi.org/10.1109/noms.2018.8406325

Garba, A., Hu, Q., Chen, Z. and Asghar, M.R. (2020). BB-PKI: Blockchain-Based Public Key Infrastructure Certificate Management. [online] IEEE Xplore. https://doi.org/10.1109/HPCC- SmartCity-DSS50907.2020.00108

Radomir Prodanović, Belgrade, Vulić, I. and Tot, I. (2019). A SURVEY OF PKI ARCHITEC- TURE. International Scientific Conference ERAZ. Knowledge Based Sustainable Development. https://doi.org/10.31410/eraz.s.p.2019.169

Omar, R.R. and Abdelaziz, T.M. (2020). A Comparative Study of Network Access Control and Software-Defined Perimeter. Proceedings of the 6th International Conference on Engineering & MIS 2020. https://doi.org/10.1145/3410352.3410754

Wang, Y., Xu, G., Liu, X., Mao, W., Si, C., Pedrycz, W. and Wang, W. (2020). Identifying vul- nerabilities of SSL/TLS certificate verification in Android apps with static and dynamic analysis. Journal of Systems and Software, 167, p.110609. https://doi.org/10.1016/j.jss.2020.110609

Indira Reddy, B. and Srikanth, V. (2019). Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3). International Journal of Scientific Research in Computer Science, Engineer- ing and Information Technology, 5(4), pp.28–35. https://doi.org/10.32628/cseit1953127

Lamers, E., Dijksman, R., van der Vegt, A., Sarode, M. and de Laat, C. (2021). Securing Home Wi-Fi with WPA3 Personal. [online] IEEE Xplore. https://doi.org/10.1109/CCNC49032.2021.9369629

Asmaa Hani Halbouni, Ong, L.-Y. and Leow, M.-C. (2023). Wireless Security Protocols WPA3: A Systematic Literature Review. IEEE Access,

pp.1–1. https://doi.org/10.1109/access.2023.3322931

Ogudo, K.A. (2019). Analyzing Generic Routing Encapsulation (GRE) and IP Security (IP- Sec) Tunneling Protocols for Secured Communication over Public Networks. [online] IEEE Xplore. https://doi.org/10.1109/ICABCD.2019.8851004

Jones, J., Wimmer, H. and Haddad, R.J. (2019). PPTP VPN: An Analysis of the Effects of a DDoS Attack. [online] IEEE Xplore. https://doi.org/10.1109/SoutheastCon42311.2019.9020514

Iqbal, M. (2019). Analysis of Security Virtual Private Network (VPN) Using OpenVPN. Inter- national Journal of Cyber-Security and Digital Forensics, 8(1), pp.58–65. https://doi.org/10.17781/p002557

Dowling, B. and Paterson, K.G. (2018). A Cryptographic Analysis of the WireGuard Protocol. Applied Cryptography and Network Security, pp.3–21. https://doi.org/10.1007/978-3-319- 93387-0_1

Mackey, S., Mihov, I., Nosenko, A., Vega, F. and Cheng, Y. (2020). A Performance Comparison of WireGuard and OpenVPN. Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy. https://doi.org/10.1145/3374664.3379532

Jones, J., Wimmer, H. and Haddad, R.J. (2019). PPTP VPN: An Analysis of the Effects of a DDoS Attack. [online] IEEE Xplore. https://doi.org/10.1109/SoutheastCon42311.2019.9020514

Schwenk, J. (2022). Point-to-Point Security. Information security and cryptography, pp.85–97. https://doi.org/10.1007/978-3-031-19439-9_5

Chandel, S., Yu, S., Yitian, T., Zhili, Z. and Yusheng, H. (2019). Endpoint Protection: Measur- ing the Effectiveness of Remediation Technologies and Methodologies for Insider Threat. 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). https://doi.org/10.1109/cyberc.2019.00023

Arfeen, A., Ahmed, S., Khan, M.A. and Jafri, S.F.A. (2021). Endpoint Detection & Response: A Malware Identification Solution. 2021 International Conference on Cyber Warfare and Se- curity (ICCWS), pp.1–8. https://doi.org/10.1109/iccws53234.2021.9703010

Yang, Z., Yang, K., Lei, L., Zheng, K. and Leung, V.C.M. (2018). Blockchain-based Decentralized Trust Management in Vehicular Networks. IEEE Internet of Things Journal, pp.1–1. https://doi.org/10.1109/jiot.2018.2836144

Roma, C.A., Tai, C.-E.A. and Hasan, M.A. (2021). Energy Efficiency Analysis of Post- Quantum Cryptographic Algorithms. IEEE Access, 9, pp.71295–71317. https://doi.org/10.1109/access.2021.3077843