5-2023

The Identification of Rogue Access Points Using Channel State Information

Irene McGinniss

Abstract

Today's wireless networks (Wi-Fi) handle more significant numbers of connections, deploy efficiently, and provide increased reliability and high speeds at low cost. The ability of rogue access points (RAPs) to mimic legitimate APs makes them the most critical threat to wireless security. APs are found in coffee shops, supermarkets, stadiums, buses, trains, airports, hospitals, theaters, and shopping malls.

Rogue access points (RAP) are unauthorized devices that connect to legitimate access points and networks and bypass authorized security procedures. RAP detection has been attempted using hardware and software-based solutions requiring the developing of dedicated tools or beacon frame modification. (Arisandi, 2021). The effectiveness of software-based tools such as Aircrack-ng, Kismet, and InSSIDER is diminished as customized configurations are required for each environment. (VanSickle, 2019).

Channel State Information (CSI) are characteristics of the communication link between a Wi-Fi transmitter and receiver and facilitates reliable communication in multi-antenna systems. The data contained in CSI can be analyzed and used to detect motion and activity based on interference in the line of sight (LoS) between the transmitter and receiver. CSI has been used to recognize human activity (Wang, 2015) and recognize differences in gaits based on the speed of motion (Wang, 2016).

This paper proposes identifying RAPs by detecting differences in CSI characteristics due to interference in the (LoS) path between the Wi-Fi transmitter and the receiver.

Keywords: Rogue Access Point (RAP), Channel State Information (CSI), Wi-Fi, Machine Learning.

MONTCLAIR STATE UNIVERSITY

The Identification of Rogue Access Points

Using Channel State Information

By

Irene McGinniss

A Master's Thesis Submitted to the Faculty of

Montclair State University

In Partial Fulfillment of the Requirements

For the Degree of

Master of Science

May 2023

College of Science and Mathematics
Department of Computer Science

Thesis Committee

[redacted]

Dr. Jiacheng Shang
Thesis Sponsor

[redacted]

Dr. Bharath Samanthula
Committee Member

[redacted]

Dr. John Jenq
Committee Member

The Identification of Rogue Access Points Using Channel State Information

A THESIS

Submitted to the Faculty of

Montclair State University in partial fulfillment

of the requirements

for the degree of Master of Science

by

Irene McGinniss

Montclair State University

Upper Montclair, NJ

May 2023

Thesis Sponsor: Dr. Jiacheng Shang

Table of Contents

List of Figures

List of Tables

Chapter One

Introduction

With the increased reliance on mobile devices, the number of IoT devices is expected to reach 27 billion by 2025. (Hasan, 2022) Isolation caused by Covid-19 accelerated the adoption of real-time communications platforms to manage and monitor health, remote online learning, and virtual business meetings. The addition of IoT devices to support the changes in society resulted in the exponential growth of wireless networks. The convenience, accessibility, and flexibility for users fueled the high demand and proliferation of APs. Due to the increased demand, APs are being deployed without consideration of network or user security.

The IEEE 802.11n (802.11n) protocol standard introduced in 2009 supports 2.4 GHz and 5GHz band frequencies, is backward compatible with IEEE 802.11a/b/g and has a maximum speed of 600 Mbps. The supported frequencies are higher than those for cell phones and televisions, allowing the signal to carry more data. The 2.4 GHz band travels farther and is best for online activities like surfing the web. The backward compatibility and increased throughput allow for a more extensive range of devices (both old and new) to connect, expanding its appeal. While 802.11n is an older protocol, it supports MIMO (Multiple Input and Multiple Output), which multiplies the capacity by using multiple antennas for transmitting and receiving several streams simultaneously.

Access points are network devices that transmit and receive signals using radio waves at specific frequencies and modulations. These signals are subject to factors that affect signal strength, such as distance, obstacles, and interference. Wi-Fi signals can change direction (reflect) off objects they encounter, such as metal which can weaken the signal. Signals can be absorbed and weakened by materials in the environment like wood, ceramic tiles, and the human body. Refraction of WiFi signals occurs when the signal passes *through* some medium like a glass of water causing the signal to change direction. Signals can also suffer from scattering; after encountering an object, the wave splits into multiple waves. Decreased power levels at the receiver can also affect signal strength.

The Wi-Fi signal range can be maximized by placing the AP in a location that provides a clear LoS for most users. APs are usually mounted to ceilings in the center of a room, away from corners, heating and cooling vents, and electronic devices that can cause interference. Most newer APs can easily cover an area of 1,500 square feet.

Access point placement advocates for creating a clear LoS where the largest number of users can easily connect without interference from other devices or objects. RAPs are rarely installed near an AP due to the logistical challenges (including physical site security) of placing the RAP in the exact location of the AP. The difference in placement can be used to identify interference in the LoS between the transmitter and receiver.

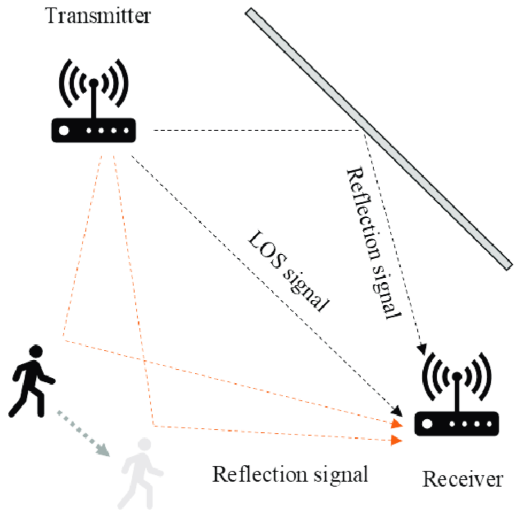


Figure 1- Schematic diagram of WiFi signal propagation path (ResearchGate)

The AP sends a beacon with an SSID (Service Set Identifier) to uniquely identify it from other APs. The client sends a probe request to discover any network in close proximity. After the client receives a response to the probe request, it will determine which AP to join. Public Wi-Fi APs use encryption. When the client joins, it will be prompted to enter a password; the authentication process will begin if encryption is enabled on the AP. Once the client is authenticated, it is connected and can access the internet. For public Wi-Fi APs, passwords are required to log in for legitimate users and malicious actors.

With the increased number of threats and sophistication of hacking tools, securing wireless networks is becoming more complex. Setting up a wireless network takes minimal effort compared with the effort and experience required to secure it. As businesses offer free Wi-Fi to entice customers, the risks to trusting users are ever-increasing. Hackers exploit the behaviors of APs and users to intercept communications, steal credentials and install malware. Android and iOS Wi-Fi devices create a PNL (Preferred Network List) of all networks they connected to before. These devices are presumed to be "safe," and the device will broadcast a probe using the identical SSID to reconnect. After receiving responses to the probe requests sent, all APs that respond will be displayed in order of signal strength. Malicious actors use this to their advantage in setting up a RAP, usually an Evil Twin that will mimic the SSID, BSSID, and MAC address of the legitimate AP. Users are lured to the rogue device, unknowingly not being able to discern the legitimate AP from the RAP and the closer proximity of the RAP facilities the device preferring this wireless network over others.

RAPs are used to steal credentials, compromise networks, and attack network infrastructures. Rogue access points can be innocuous, such as an employee setting up a Wi-Fi router to connect a wireless device or a malicious attacker looking to gain access or intercept data. Both result in security vulnerabilities for the organization, with higher risks for those involved in the healthcare or financial industries.

Users connected to the legitimate AP will be disconnected when the RAP sends a deauthorization packet. The client will send out a probe, receive a response from the RAP (masquerading as the AP the client was just connected to), and the user thinks they are connected to the original AP. For clients not previously connected, the RAP will be closer to the victims, have a higher RSSI, and be listed first. The users will try to connect to the AP with the strongest signal.

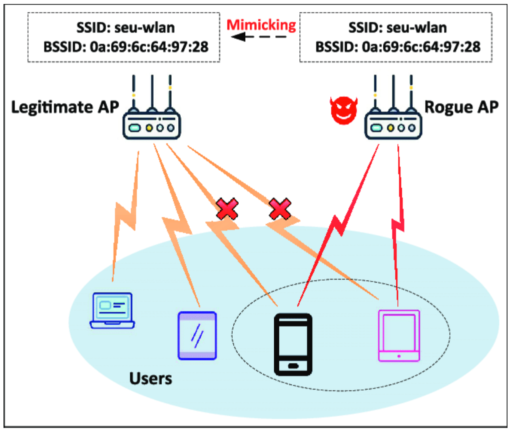


Figure 2- Attack model of Rogue APs (Wu, 2018)

Chapter Two

Related work

Wireless Network Security

Mechanisms for securing Wi-Fi networks include hiding the SSID, using encryption, using MAC address filtering, updating the AP software, enabling any embedded firewall on the AP, using complex Wi-Fi passwords, and monitoring network activity and devices. The challenge for smaller venues is the need for more expertise in securing the network and the trade-off between investing in securing the network and ease of use for users. The current encryption standards available for APs include WEP, WPA, WPA2, and WPA3. WEP and WPA have been deprecated since the encryption has been broken. WPA2 is generally used with pre-shared keys (shared passcode). WPA3 is more robust but requires newer equipment and devices.

The challenge in securing a public Wi-Fi network where the password is posted or well-known is that it indiscriminately invites all users. Once a rogue actor joins a Wi-Fi network, tools freely available could be used to easily compromise the network or, more commonly, hijack users' communications. A study by Attipoe (2022) found that 40% of users of public Wi-Fi networks felt they had no control over security. A majority of mobile device users choose convenience over security.

Another vulnerability in APs is Universal Plug and Play (UPnP), enabled by default. UPnP is a protocol that allows UPnP compatible devices to discover and communicate with each other and open direct channels to the internet. This feature could lead to command and control attacks.

Joining a password-protected Wi-Fi network does not necessarily ensure security. A researcher easily hacked 70% of a pool of 5,000 Wi-Fi networks in Tel Aviv. (Lakshmanan, 2021). Most of these networks were "protected" with passwords and were easily cracked using a dictionary attack. With public Wi-Fi, the passwords are already given, opening the door to hackers. Given the scenario of a coffee shop or bookstore, a rogue actor could be at the next table from a victim, and neither the victim nor the Wi-Fi network provider is aware of their presence. Twenty percent of public Wi-Fi users perform financial transactions over these networks. (Hann, 2023) Mitigating damages from a rogue actor is critical as WiFI networks expand.

Users understand the inherent risks of joining public Wi-Fi networks, as evidenced by increased personal VPN use. Forty-seven percent of those VPN users are opting for free services. (Crail, 2023). A study showed that 20% of public Wi-Fi users perform financial transactions over these public networks. Even when users employ VPNs, there are inherent risks, as seen in 2022 when seven VPN service providers were hacked, and customers' user information was collected and posted unprotected on a cloud server. (Wagenseil, 2022). The majority of users still take risks.

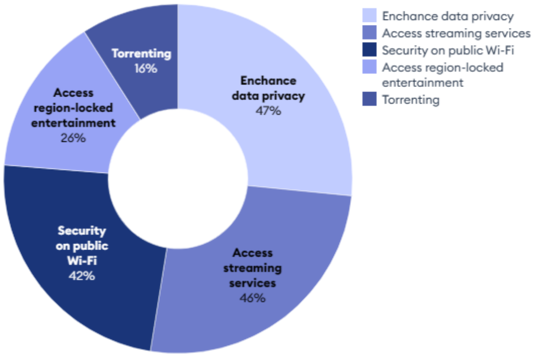


Figure 3- VPN Statistics and Trends in 2023

Rogue Access Points (RAPs)

The most common wireless exploit comes in the form of a rogue access point (RAP). RAPs mimic the SSID, MAC address, and IP address of legitimate APs and can disconnect all users by sending a deauthorization packet. The users will try to connect to the last known network or the AP with the strongest signal. As the RAP will be closer to the users/victims, the RAP's signal will likely be stronger.

Wireless communications have become a necessity. As most websites use HTTPS for security, the ability for malicious actors to insert themselves between a victim and a legitimate AP is via the use of an Evil Twin. Evil Twins will mimic the legitimate AP's SSID, MAC address, and IP address; the victim is unaware of the difference. The biggest threat to legitimate APs is the ability of a hacker to interfere with communications and intercept traffic. The hacker can be used to capture login information, install malware, intercept traffic, steal credentials, and even force all communications over HTTP, removing the perceived protection of encryption.

When establishing connections to Wi-Fi devices, Android and iOS-based devices have algorithms that generate a list of nearby APs and rank them according to signal strength for users to auto-join. While both will prefer known networks over private or public, in a coffee shop, the only networks available to users are those with the strongest signal (RSSI). If the public AP a user wants to connect to has a password, those passwords are posted somewhere to make connecting easy. Malicious actors looking for an easy way to penetrate a network will deploy rogue access points (RAP) and exploit these devices' inherent trust in nearby networks. The evolution of hacking tools and the proliferation of online tutorials demonstrate the need for identifying RAPs.

RAPs are not always the result of malicious actions. A worker who plugs an AP into the corporate network for convenience or to bypass corporate policy is not uncommon, and while not malicious, the threat remains. The corporate network could be compromised without IT knowing the device was added.

An Evil Twin attack was launched on the US Department of the Interior. (Boyd, 2020). The results demonstrated how a single attack vector could compromise the wireless network and allow attackers access to the other parts of the enterprise network. The test conducted by white hat hackers revealed that the Department did not properly secure its network never maintained an inventory of legitimate devices, nor did they perform any intrusion detection testing. Large organizations with dedicated IT departments struggle to deal with WLAN security, and the task is even more significant for businesses trying to provide a service for their customers.

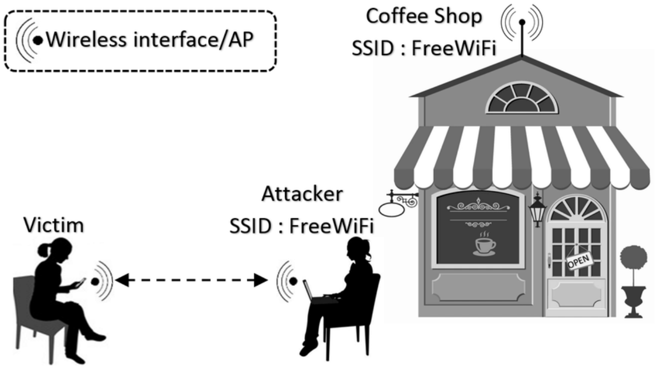


Figure 4- Exposing Vulnerabilities in Mobile Networks (ResearchGate)

Rogue AP Detection

Lu, et al. (2017) attempted to create a passive client-based approach to Evil Twin detection. Utilizing a laptop with 2 Wi-Fi interfaces, the team set out to detect RAPs by focusing on the 802.11 forwarding frames between the legitimate AP and RAP. The hypothesized data flow rate of the forward frames between the AP and RAP should equal the frames between the RAP and the client. There were limitations to the solution in that the client must be running two separate Wi-Fi network cards and distance them to avoid interference. The ET-spotter application requires at least one victim on the RAP, and that victim must open a browser and surf the internet.

Fingerprinting is considered another option in identifying RAPs. The challenge is creating and maintaining the database of unique characteristics used for identification. There is also the possibility of misidentification of devices if the RAP used is the same brand and firmware version as a legitimate AP. With passive fingerprinting, the APs broadcasting their beacons are assessed, and their characteristics are classified. Fingerprinting does address issues with APs hiding their SSIDs. However, it cannot differentiate an Evil Twin from a legitimate AP.

Wired fingerprinting is independent of any frequency or Wi-Fi range, but there is no way to classify the Wi-Fi traffic. If TCP Ack arrival times are used, this only works with TCP traffic. If Round Trip Time (RTT) deviation is used, this presumes the variation is caused by Wi-Fi traffic and not congestion on the Wi-Fi network or signal interference.

While RSSI is one of 3 methods of using Wi-Fi to recognize activity (Tian, 2021), relying on the same as a means of identifying a RAP falls short as the proximity of the RAP to the victim is closer than the AP. The signal from the RAP can be boosted as well.

Intrusion Detection Systems (IDS) can detect rogue devices on the network by learning and scanning for specific traffic patterns. While not depending on the Wi-Fi frequency or range, using

IDS to detect a rogue device requires a learning curve for non-technical people; the rogue actor can evade it by using non-standard ports for traffic, or the RAP could be powered off immediately after exfiltrating data. Probes/nodes can be used, but equipment must be deployed and maintained.

A distinction needs to be made between detecting rogue devices and identifying same. These studies can confirm that a RAP is connected to a wireless network, but distinguishing same from legitimate APs or locating same has proven to be more difficult.

Channel State Information (CSI)

Channel State Information (CSI) is a wireless communication parameter that captures the characteristics of the wireless channel between the transmitter and the receiver. As the wireless signal propagates through the channel, CSI's attenuation, phase shift, and delay metrics are measured from a known signal sent by the transmitter and collected at the receiver. CSI frequency response data is represented as a matrix with the state of the channel subcarriers recorded at a given instance in time. CSI is ideal for this application as the characteristics of the wireless signal between a user and AP and a user and the RAP will differ significantly due to the device's position.

Several features of CSI can be used to extract additional information from the data. Variance is the representation of the deviation of the amplitude value from the average amplitude. The average amplitude is the mean amplitude over a specific period and estimates the signal strength. Peak-to-Peak amplitude is the difference between the minimum and maximum amplitude values over a certain period of time.

Features of CSI can be used to differentiate between a legitimate AP and a RAP, as the characteristics will be different due in part to the position of the respective access point and the interference with the LOS caused by motion.

Problem Statement

WLAN utilization has increased exponentially with the reliance on mobile devices. Rogue access points are one of the principal security threats for WLANs. Many studies have been conducted on the tools and techniques that can be used to identify rogue access points. Most require special hardware or software, are not cost-effective, and must be managed. Despite extensive research, more progress has yet to be made in consistently identifying RAPs. RAPs used for Man-in-the-Middle attacks can result in fraudulent transactions, stolen credentials, unauthorized access to confidential information, widespread DDoS, malware attacks, and compromising internal infrastructure. Given the magnitude of the harm a RAP can cause, solutions to accurately identify rogue access points are paramount to the IoT industry.

This research study aims to determine if a rogue access point can be identified on a network based on changes in CSI characteristics due to Wi-Fi signal interference.

Research Question

RQ1: Can interference in the line of sight between an Access Point and a client (based on placement) cause changes in signal attenuation that can be used to identify rogue access points?

The null hypothesis is:

H1: Changes in signal attenuation cannot accurately be attributed to rogue access points.

RQ1 will be evaluated using the Support Vector Model machine learning to determine the accuracy of the training classification.

Chapter Three

Methodology

This section details the hardware and software components used in the experimental environment. A large *.avi file was installed on both the AP and RAP, and the client/CSI collector downloaded the file to generate sustained traffic. Each collection was run for approximately 60 seconds, and each set of tests ran for 80 iterations. Both the AP and RAP were restricted to using the 802.11n 2.4 GHz frequency band, and due to the requirements of the CSI collector, the Wi-Fi networks were not secured. All nearby Bluetooth devices were powered off so as not to cause additional unwanted interference.

The RAP was a Raspberry PI (RPi) Model 4B+, with 8 GB of memory running Debian 11 (Bullseye. The hardware used for the legitimate AP was a TP-Link Archer 7 v 5.0 router with three antennas running firmware version 1.1.2 Build 202100125. An Aiibe 6 Ports Super High-Speed USB 3.0 powered hub was connected to the RPi, and connected to the hub was a dual antenna Linux compatible Wi-Fi adapter model ALFA AWUS036ACM. The external Wi-Fi adapter was used instead of the RPi onboard adapter for stronger signal strength.

The CSI collector/victim ("victim") was an IBM Thinkpad T400 with an Intel 5300 chipset Wi-Fi adapter required for use with the CSI collector software – Linux 802.11 CIS Toolkit. (Halperin, 2010). The resultant data was exported into MatLab (The MathWorks Inc., 2022), where a lowpass filter was applied and signal features extracted. The resulting *.csv files were imported into SciKit-Learn (SciKit-learn, 2011) for classification and predictions.

The choice of using a Raspberry Pi with an external Wi-Fi adapter was made as this is a common real-world scenario for hackers to compromise networks in coffee houses or other public places.

Data Collection

CSI values for 30 subcarriers of each receiving antenna were collected. Before each test, commands were run to unload the Intel Wi-Fi driver, reload the driver with logging enabled, and stop the wpa_supplicant service before capturing CSI data to a file.

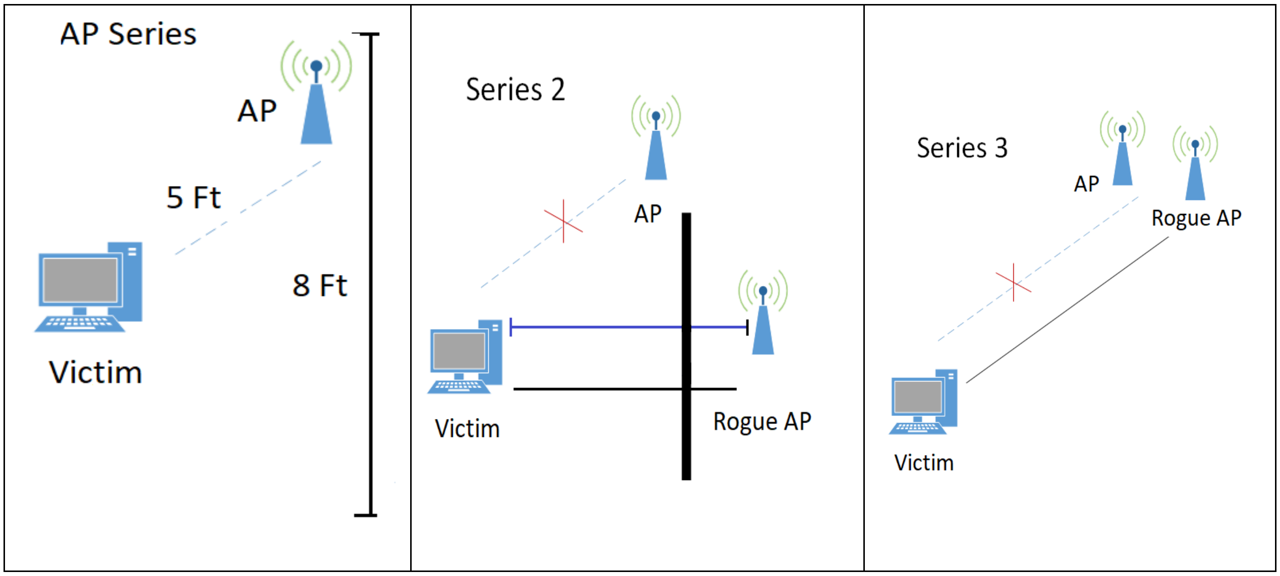
A large file was uploaded to both access points. The file was transferred from the AP to the victim using secure copy. Due to the CSI collection application requirements, the 2.4GHz frequency band was used, and no security or encryption was applied to either the AP or RAP.

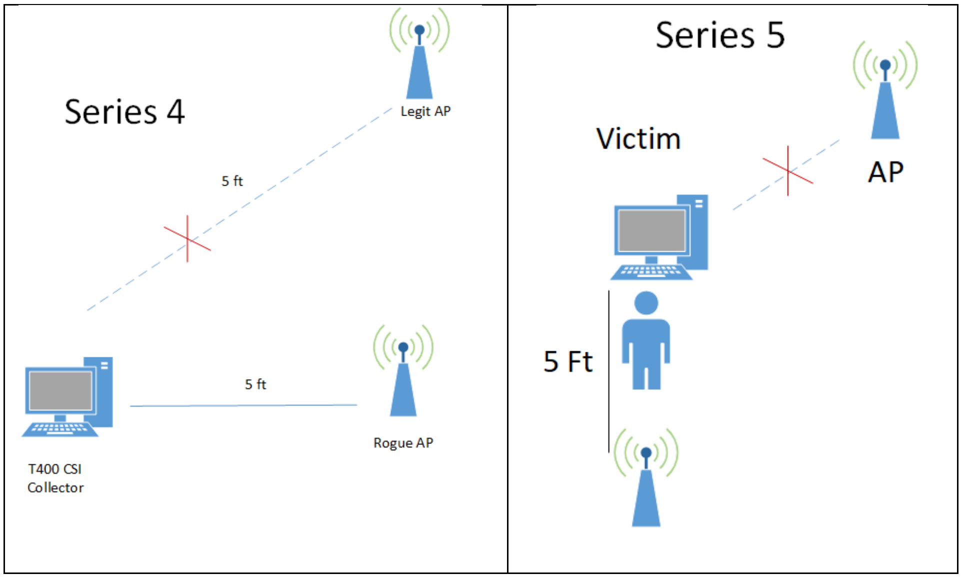
The decision to use an external Wi-Fi adapter connected to the RAP was based on the need for a stronger signal than the internal Raspberry Pi Wi-Fi adapter. In addition, to ensure consistent power to the external adapter, a powered USB hub was used.

The placement of the RAPs in the various experiments mimics a scenario where a rogue actor would sit in a coffee shop, connect to Wi-Fi, and launch an Evil Twin attack.

Positioning of the Rogue Access Points

For each series of tests, the RAP was positioned in several locations with the "coffee shop" scenario in mind. The legitimate AP was positioned near the ceiling with the victim five feet away. There was a clear, unobstructed LoS between the transmitter and receiver. The RAP in Series 2 tests was placed in the next room with a wall separating the transmitter and receiver. The distance between the AP and the victim was ten feet. This test was run to see how much of a signal could be sustained through a wall. Most users are unaware of the range of their APs, and the test replicated a scenario where a rogue actor would position themselves outside the coffee shop. In the Series 3 tests, the RAP was placed next to the legitimate AP, five feet from the victim. This test was done to determine if the RAP sharing the same LoS as the AP would see the same signal strength. For the Series 4 tests, the RAP was placed next to the victim at a distance of five feet. This test emulates the scenario in a coffee shop where the rogue actor could be at the next table. For Series 5, the RAP was placed behind the victim.   This test was to emulate a scenario where the rogue actor sat behind the victim.





CSI Preprocessing

The raw CSI data needs to be processed before any filters can be applied or features extracted. The raw CSI data is processed in Matlab. Arrays are defined for CSI and time as data is extracted from subccarriers of 3 antennas. A lowpass filter is applied to the full signal using 3.0 Hz as the cutoff value to compensate for any noise from the wireless adapter and other interference. This "denoising" allowed the low-frequency components to pass through while higher frequencies were attenuated. The value of 3 Hz was selected to detect average motion, given that the fastest arm movement tracked was 8 Hz, and the actions were natural and not grandiose or deliberate. (Qiao, 2008). After the lowpass filter was applied, features were explicitly extracted to enhance characteristics associated with changes associated with LOS interference. After applying the filters and features, the raw data for each test was plotted along with the results. Once the data was processed in Matlab, it was exported as *.csv files. The signal retained critical characteristics and data as seen below:

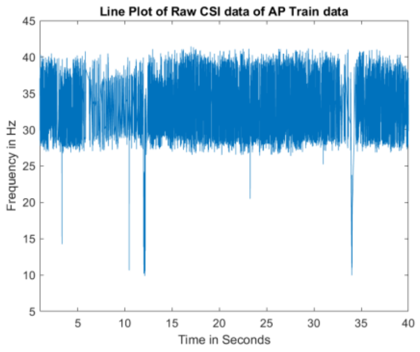


Figure 5- CSI Raw Data AP Train Set

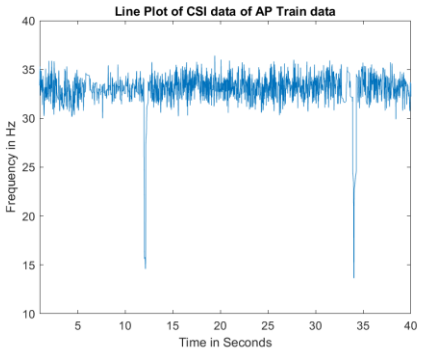


Figure 6- CSI Filtered Data AP Train Set

Feature Selection and Extraction

Variance

Variance helps to quantify the dispersion of the signal generated by an object in between the transmitter or receiver. Signal variance measures the fluctuations in the signal as well as the distribution of the signal's values. As changes can be caused by interference (or motion), the variance function returns normalized elements of the array.

Root-Mean-Square (RMS*)*

RMS is used as a feature for signal comparison and characterization based on the average amplitude of the signal. It is the process used to determine the average power output over a period of time and is used to measure Wi-Fi signal noise. RMS allows for the normalization of the Wi-Fi signal when extreme peaks vary between waveforms.

Peak (local maxima)

A peak can be used for event detection as they represent significant changes in the signal, anomalies, or events in the data. The peak features identify local maxima, which are higher based on neighboring values. It is the maximum absolute value of the signal. The difference between the peak signal minus the background signal can be used to calculate the noise-to-signal ratio.

Average Amplitude

The average amplitude (mean) of a Wi-Fi signal is the average calculated over a period of time. It can be used to determine the minimum strength needed to maintain a reliable connection.

Peak to Peak

The Peak to Peak function returns the difference between the maximum and minimum values within a specific time interval. The range can be indicative of the signal's intensity. A significant peak-to-peak value can be used to determine the signal-to-noise ratio (SNR) quality.

Model Training & Evaluation

Support Vector Machine (SVM) is a machine learning algorithm used for data classification of complex datasets. A hyperplane – or decision boundary – is used to distinguish two classes of data points: data points from the AP and data points from the RAP. The algorithm aims to maximize the distance between the decision boundary and the closest data point from each class. A critical factor in an SVM's performance is the kernel choice. (Chappelle, 2002). The kernel used for the SVM is the Gaussian Radial Basis Function (RBF).

Half of the data collected from each test series was used for training. First, a classifier was defined using the RBF kernel. The model was trained using the CSI train data set and the vector array. The predicted vector array for the test set was generated using the *predict* function. The accuracy of the training model is determined by comparing the vector test set value and the original vector array.

The same data was analyzed using the SVM mode to randomly select 80% of the data for training and 20% for testing with the random state value set to 42. The classification accuracy was the same.

Chapter Four

Results and Analysis

All data collected from each experiment were processed using Support Vector Machine with RBF kernel. The RBF kernel's maximum value is 1 when the points are the same. The accuracy of the classification model was calculated using the known vector array and the predicted array when the test data was processed. The accuracy of the classification model is listed below:

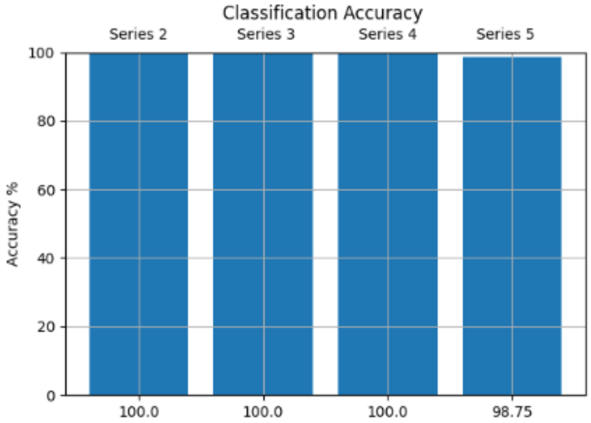


Table 1 - Classification Accuracy

Plotting the data comparing the legitimate AP with each RAP Series test shows the distinct distribution between the two classes. The drop in frequency for all the RAP data sets indicates the distortion of CSI magnitude or interference in the signal.

The scatter plot for data points from the legitimate AP shows many points above 25Hz, indicating little to no frequency or signal drop. With an unobstructed LOS to the receiver, the legitimate AP had a higher frequency for most of its data points.

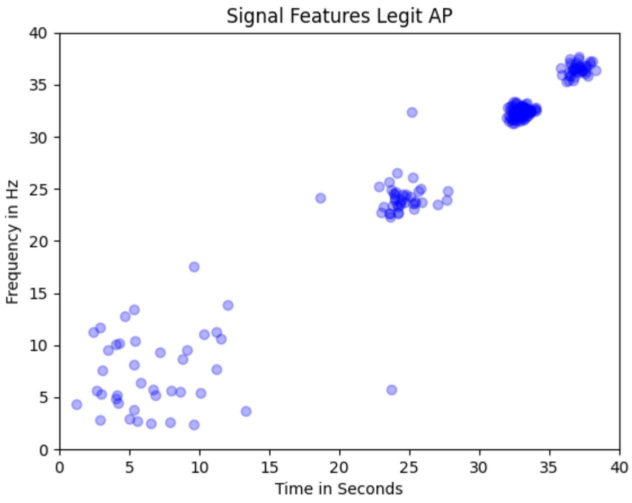


Figure 7- AP Data Points

The scatter plot for Series 2, where the RAP was in the next room, shows a consistently low frequency with no points above 22 Hz. The structure (wall) between the RAP and the victim receiver degraded the Wi-Fi signal for the test period.

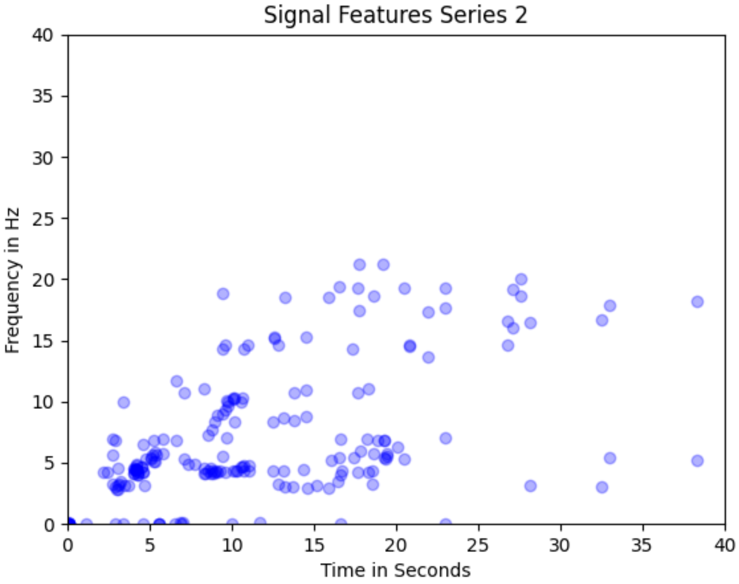


Figure 8- Series 2 Data Points

The scatter plot for Series 3, where the RAP was placed next to the legitimate AP, showed most data points between 8 and 16 Hz. The expectation was that a clear LOS would have resulted in little or no drop in frequency. The signal strength of the antennas used on the external adapter connected to the RAP was less than the legitimate AP, or interference was caused by the legitimate AP's antennas.

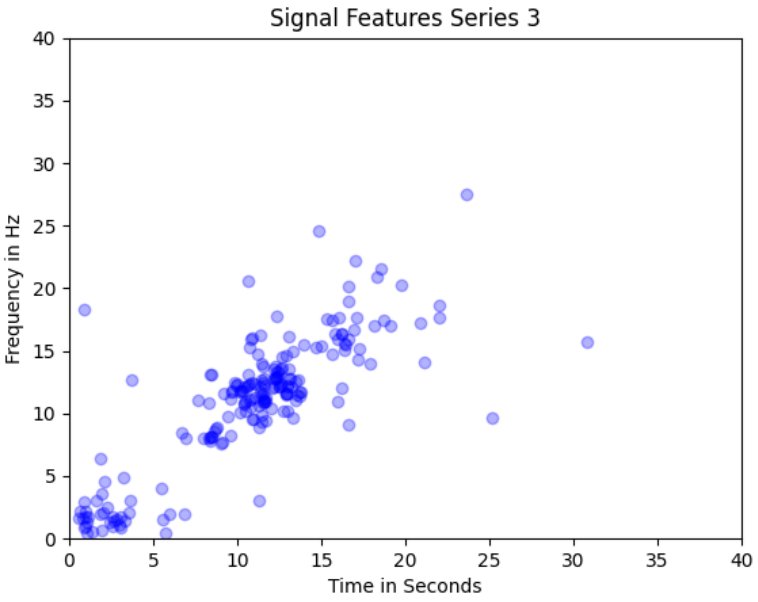


Figure 9- Series 3 Data Points

The plot representing Series 4 testing (where the RAP was on the same plane as the victim) recorded considerable interference based on activity. The interference is evidenced by the decreased frequency levels resulting in lower frequency numbers. The scatter plot for Series 4 shows no data past 20 seconds, and the plotted data is below 20Hz.

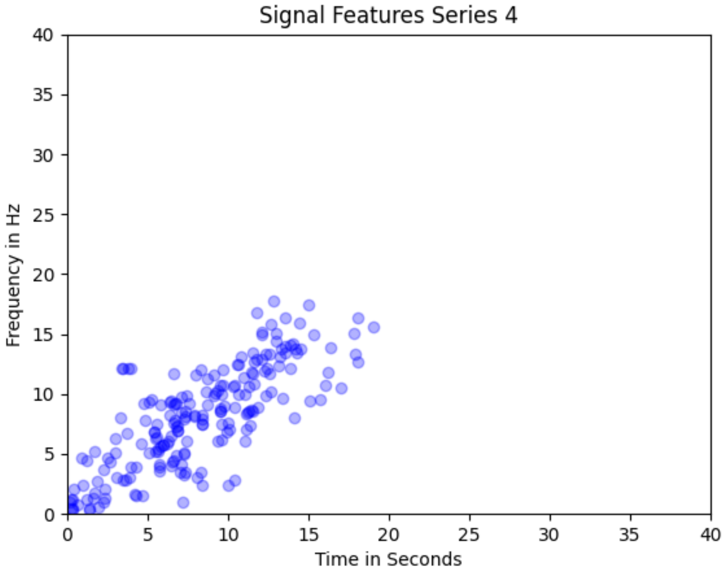


Figure 10- Series 4 Data Points

The scatter plot representing the results from the Series 5 test with the RAP behind the victim PC had the widest distribution of data points. There was a cluster between 10 and 25 seconds in the 10-20 Hz range, with some frequency measurements recorded at 40 Hz. As the victim was sitting directly in the LOS between the RAP and receiver, the expectation was a consistently lower overall frequency sustained for the time period of the test. This would be the result of both absorption of the signal and reflection.

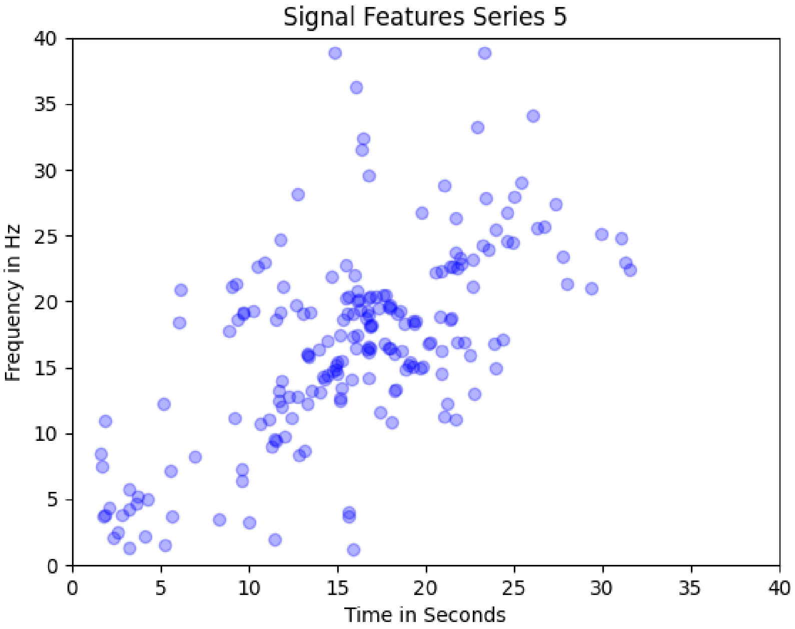


Figure 11- Series 5 Data Points

Chapter Five

Conclusion

In this paper, using CSI to identify a rogue access point was investigated with the specific scenario of a rogue access point being deployed in a coffee shop in mind. The classification accuracy confirms that the model to train the test data was correct. Two variables that may have skewed the results are (a) the limited number of iterations of each test and (b) the features extracted. Another consideration is the power of the antennas of the legitimate AP versus the RAP and whether the frequency response was limited.

Summary of results

The approach in this paper focused on the specific scenario of a RAP being deployed in a coffee shop setting as an Evil Twin. Capturing and analyzing CSI data demonstrated significant changes in signal attenuation due to interference of the LoS between the AP and RAP. The LoS of the AP will be mostly undisturbed due to its placement. Significant changes in signal strength via low frequency were seen only in the RAP dataset.

The SVM classification accuracy substantiates that the model could determine what data obtained from the receiver was from a rogue or legitimate AP. With the limited data available, rogue access points' Wi-Fi signal characteristics are significantly altered due to the motion between the transmitter and receiver. These changes in signal characteristics were not seen in the AP, where the LoS was primarily unobstructed.

Practical Implications

Wireless security can benefit from an accurate means of identifying RAPs. The solution must be simple to deploy, accurate and efficient. The solution proposed does more than detect a RAP; it can identify and distinguish it from a legitimate AP based on the signal attenuation due to interference in the LoS.

Future Exploration

We propose collecting larger data samples to substantiate the accuracy of the classification and replace the RPi with a more robust PC with an external WiFI adapter to mitigate any variables that may result in decreased signal power from the rogue access point.

Further, neural networks can be employed to expand data classification from tests. Adding extract features as variables for additional classification may help with scenarios outside the one tested for this paper.

References

Arisandi, D., Ahmad, N.M., and Kannan, S. (2021, Sept). *The rogue access point identification: a model and classification review.* Indonesian Journal of Electrical Engineering and Computer Science, Vol 23, No.3, Sept 2012, pp 1527-1537

Attipoe, E. (2022). *End User's Perception about Security of the Public Wireless Network.* Retrieved April 17, 2023, from https://www.researchgate.net/profile/Elliot-Attipoe/publication/358729487_End_User's_Perception_about_Security_of_the_Public_Wireless_Network/links/6211419808bee946f38ec598/End-Users-Perception-about-Security-of-the-Public-Wireless-Network.pdf

Boyd, A. (2020, Sept.16). *Interior IG Team Used Evil Twins and $200 Tech to Hack Department Wi-Fi Networks*. NextGov. Retrieved May 3, 2023, from https://www.nextgov.com/cybersecurity/2020/09/interior-ig-team-used-evil-twins-and-200-tech-hack-department-wi-fi-networks/168521/

Cai, X., Li, X., Yuan, R., and Hei, Y., "Identification and mitigation of NLOS based on channel state information for indoor Wi-Fi localization," *2015 International Conference on Wireless Communications & Signal Processing (WCSP)*, Nanjing, China, 2015, pp. 1-5, doi: 10.1109/WCSP.2015.7341172.

Chapelle, O., Vapnik, V., Bousque, O., et al., *Choosing Multiple Parameters for Support Vector Machines* Machine Learning 46, 131–159 (2002). https://doi.org/10.1023/A:1012450327387

Crail, C., (2023, Feb 9). *VPN Statistics and Trends in 2023*, ForbesAdvisor, Retrieved March 19, 2023, from https://www.forbes.com/advisor/business/vpn-statistics/

Exposing Vulnerabilities in Mobile Networks: A Mobile Data Consumption Attack - Scientific Figure on ResearchGate. Retrieves May 10, 2023, from: https://www.researchgate.net/figure/Illustration-of-an-Evil-Twin-Attack-The-attacker-can-successfully-lure-a-victim-into_fig5_321122614

Haan, K. (2023, February 9*). The Real Risks Of Public Wi-Fi: Key Statistics And Usage Data*. Forbes Advisor. Retrieved May 9, 2023, from: https://www.forbes.com/advisor/business/public-wifi-risks/

Halperin, D., Hu, W., Sheth, A., & Wetherall, D. (2010). Linux 802.11 n CSI tool. *ACM SIGCOMM Computer Communication Review*, *41*(1), 53.

Hasan, M. (2022, June 14). *State of IOT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally*. IoT Analytics. Retrieved May 3, 2023, from https://iot-analytics.com/number-connected-iot-devices/

Hunter,J., "*Matplotlib: A 2D Graphics Environment*", Computing in Science & Engineering, vol. 9, no. 3, pp. 90-95, 2007.

Jang, R., Kang, J., Mohaisen, A., and Nyang, D. (2017, June 5). *Rogue Access Point Detector Using Characteristics of Channel Overlapping in 802.11n,* 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 2017, pp. 2515-2520, doi: 10.1109/ICDCS.2017.153.

Kitisriworapan, S., Jansang, A. & Phonphoem, (2020). *A. Client-side rogue access-point detection using a simple walking strategy and round-trip time analysis*. J Wireless Com Network 2020, 252 (2020). https://doi.org/10.1186/s13638-020-01864-5

Lakshmanan, R., *Israeli Researcher Cracked Over 3,500 Wi-Fi Networks in Tel Aviv City.* The Hacker News. (2021, Oct/ 28). Retrieved May 9, 2023, from: https://thehackernews.com/2021/10/israeli-researcher-cracked-over-3500-wi.html

Lu, Q. Qu, H., Zhuang, Y., Lin, X, Zhu, Y, and Liu, Y. *A Passive Client-based Approach to Detect Evil Twin Attacks*, 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, NSW, Australia, 2017, pp. 233–239, doi: 10.1109/Trustcom/BigDataSE/ICESS.2017.242.

Ma., Y., Zhou, G. and Wang, S. (2019) *Wi-Fi Sensing with Channel State Information: A Survey*. ACM Comput. Surv. 52, 3, Article 46 (May 2020), 36 pages. https://doi.org/10.1145/3310194

Qiao, D., Pang, G., Kit, M. M., & Lam, D. S. (2008). *A new PCB-based low-cost accelerometer for human motion sensing*. Retrieved May 2, 2023, from: https://doi.org/10.1109/ical.2008.4636119

Security Wireless Networks (2021, Feb 01). *Securing Wireless Networks*. CISA. Retrieved May 3, 2023,
from https://www.cisa.gov/news-events/news/securing-wireless-networks

Schematic diagram of WiFi signal propagation path. | Download Scientific Diagram. (n.d.). ResearchGate Retrieved May 9, 2023, from: . https://www.researchgate.net/figure/Schematic-diagram-of-WiFi-signal-propagation-path_fig2_343250194/actions#reference

Scikit-learn: Machine Learning in Python, Pedregosa, *et al.*, JMLR 12, pp. 2825-2830, 2011.

Tian, Y., Li, Sr., Chen, C., Zhang, Q., Zhuang, C., and Ding. X. (2021) *Small CSI Samples-Based Activity Recognition: A Deep Learning Approach Using Multidimensional Features*, Security and Communication Networks, vol. 2021, Article ID 5632298 https://doi.org/10.1155/2021/5632298

The MathWorks Inc. (2022). MATLAB version: 9.13.0 (R2022b), Natick, Massachusetts: The MathWorks Inc. https://www.mathworks.com

VanSickle, R., Abegaz, T, Payne, B (2019, Oct 12). *Effectiveness of Tools in Identifying Rogue Access Points on a Wireless Network.* KSU Proceedings on Cybersecurity Education, Research and Practice. Retrieved April 29, 2023, from https://digitalcommons.Kennesaw.edu/ccerp/2019/education/5

Wagenseil, P. (2022, March 14). *20 million VPN users have private data leaked online: What to do*. Tom's Guide. Retrieved May 4, 2023, from https://www.tomsguide.com/news/seven-vpns-user-data.

Wang, W, Liu, A., Shazad, M., Ling, K, and Lu, S. (2015). *Understanding and Modeling of Wi-Fi Signal Based Human Activity Recognition.* In Proceedings of the 21st Annual International Conference on Mobile Computing and Networking (MobiCom '15). Association for Computing Machinery, New York, NY, USA, 65–76. https://doi.org/10.1145/2789168.2790093

Wang, W., Liu, A. and Shahzad, M. (2016). *Gait recognition using Wi-Fi signals*. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '16). Association for Computing Machinery, New York, NY, USA, 363–373. https://doi.org/10.1145/2971648.2971670

Wu, Wenjia & Gu, Xiaolin & Dong, Kai & Shi, Xiaomin & Yang, Ming. (2018). *PRAPD: A novel received signal strength–based approach for practical rogue access point detection.* International Journal of Distributed Sensor Networks. 14. 155014771879583. 10.1177/1550147718795838.