INTEGRATION OF SDR AND UAS FOR MALICIOUS WI-FI HOTSPOTS DETECTION

Jian Wang, Embry-Riddle Aeronautical University, Daytona Beach, FL
Nicolas Juarez, Jacksonville University, Jacksonville, FL
Emma Kohm, Yongxin Liu , Jiawei Yuan, and Houbing Song, Embry-Riddle Aeronautical University, Daytona Beach, FL

Abstract

With the explosive growth in the number of smartphones and other mobile devices, free Wi-Fi service has become very attractive to these devices' users. Due to the high demands of Internet services for mobile users, many public locations offer free Wi-Fi services today, such as restaurants, shopping malls, events, etc. However, the prevalent free Wi-Fi service also introduces additional hacking channels for malicious entities by deploying fake Wi-Fi access points. While research efforts have been spent on detecting rogue Wi-Fi access points, the mobility of existing systems are very limited, and hence making them inefficient to cover multiple locations.

In this paper, we propose an unmanned aerial vehicle (UAV)-based detection system for rogue Wi-Fi access points. By uniquely leveraging the high mobility feature of UAVs and wireless analysis feature of software-defined radio (SDR), our system turbocharges the efficiency and coverage of detecting rogue Wi-Fi access points.

1. Introduction

Free Wi-Fi service has become increasingly popular given the fact that smartphones and mobile devices are ubiquitous. According to the data recent statistical data [1], the number of public Wi-Fi APs is forecast to rise to 454 million by the end of 2020. A threat called rogue access points (APs) has emerged as an important security problem in WLANs [2,3,4,5]. When connecting to a public Wi-Fi AP, many mobile users do not check whether this access point is legitimate or not. As a result, deploying rogue Wi-Fi APs has become a popular channel for hackers to attack mobile device users. In fact, 25% of all public Wi-Fi APs are found to be rogue and used by hackers to gain access to your personal information. For example, during the Sochi Olympics in 2014, a reporter from NBC News reported how his laptop was hacked within a few moments of being connected to a Wi-Fi network at Russian Olympic Village. Another similar attack happened in Rio Olympics when tons of free rogue Wi-Fi APs were found stealing personal data of tourists [6].

A rogue AP is defined as an illegal access point that is not deployed by the WLAN administrator. There are two major types of rogue APs can be set with different equipment. The first type uses a typical wireless router connected directly into an Ethernet jack on a wall. The second type of rogue APs is set on a portable laptop with two wireless cards, one connected to a real AP and the other configured as an AP to provide Internet access to WLAN stations. By creating rogue Wi-Fi APs, hackers and other cybercriminals are able to eavesdrop on network traffic and insert themselves into the data conversation between their victims and the servers that the victims access while connected. As a result, hackers will have a great chance to launch various network attacks, including stealing usernames and passwords, accessing sensitive information, redirecting victims to malware sites and phishing sites, etc. As a comparison to the huge potential value hackers may obtain using a rogue Wi-Fi AP, the cost of setting up a rogue Wi-Fi AP is less than $100. Such a fact further leads to the prevalence of rogue Wi-Fi APs.

When deploying a rogue Wi-Fi AP, hackers usually imitating a legitimate AP with the same SSID, which will help them confuse mobile users and attract more users to select the rogue one. To avoid being detected, hackers may also go a step further and spoof the MAC address of the true access point so that will be seen as a base station clone, which strengthens the illusion. In addition, when multiple Wi-Fi APs are associated with the same SSID, the majority of today's devices are configured to connect to the one that provides higher signal strength. When mobile devices are closer to the rogue Wi-Fi AP than

978-1-7281-1893-2/19/$31.00 ©2019 IEEE

the genuine one, the rogue one is like to have higher signal strength and hence is selected for connection. As the example shown in Figure 1, hackers can deploy a rogue Wi-Fi AP near to Starbucks Coffee store and change the SSID to "Starbucks Free Wi-Fi". For users who do not check it carefully, there is a high probability for them to choose this rogue Wi-Fi AP.

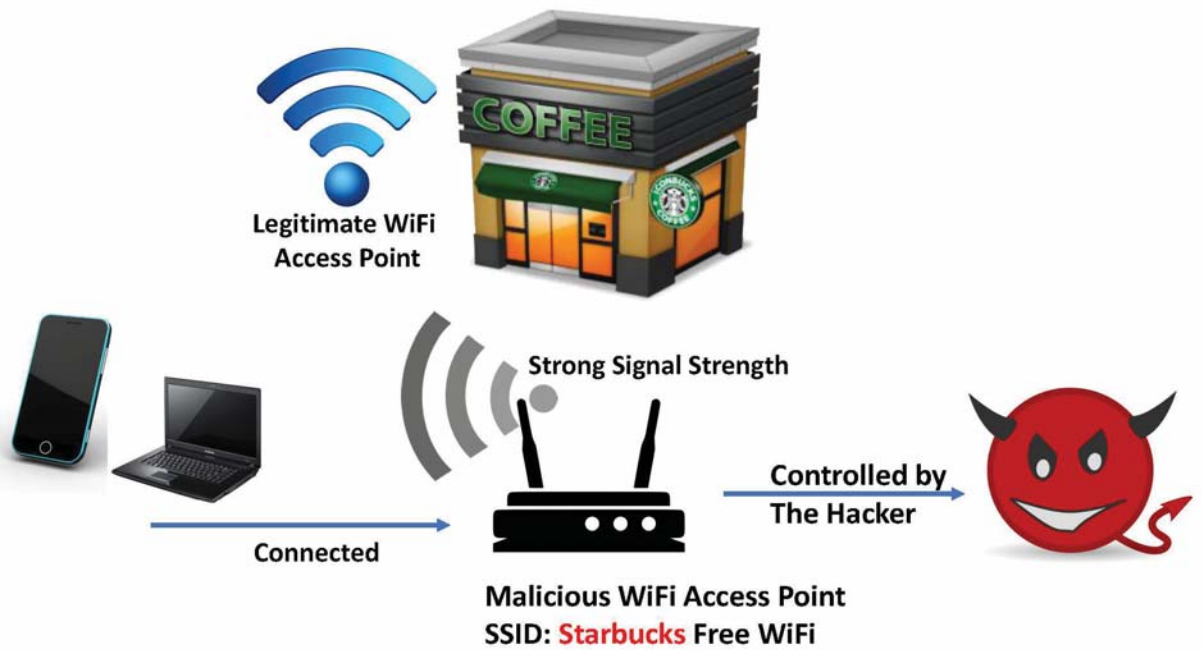

Figure 1. An Example of Rogue Wi-Fi Access Point

In this paper, we propose to design a rogue Wi-Fi access point (AP) detection system using a UAV. To detect and analyze Wi-Fi signals for potential attacks, our system embeds the lightweight USRP B210 SDR kit and a Raspberry Pi into the UAV. Different from traditional detection systems on the ground, which need to be deployed close enough to the rogue Wi-Fi AP for detection, our proposed system can significantly increase the detection range by utilizing the advantage of UAVs. Specifically, the quality of wireless signals captured in the ground-based detection system can be greatly affected by different types of blocking objects, e.g., buildings, traffic, trees, etc. To ensure the detection accuracy, the distance between the detection system and the target has to be close enough. Our UAV-based design overcomes this limitation since it can easily establish the free-space communication environment given its flying nature. By integrating SDR into our system, it can further enhance the detection distance. In addition, thanks to the high mobility of UAV, our proposed system is not only suitable for quickly checking multiple locations as planned, but also launching ad-hoc checks on demands.

The rest of this paper is organized as follows. Section 2 discusses the background information of rogue Wi-Fi AP deployment and the corresponding attacks. In Section 3, we present the detailed construction of our proposed system, which is followed by the evaluation in Section 4. We review the related work in Section 5 and conclude this paper in Section 6.

2. Background

2.1 Four-Way Handshake

The four-way handshake protocol [7] that enables the Wi-Fi access point and wireless users to independently prove to each other that they know the pre-shared key (PSK) and pairwise master key (PMK) without disclosing the key. The four-way handshake is critical for the protection of the PMK from the rogue AP. For example, when an attacker's

SSID impersonating a real access point, the user does not need to tell the AP its PMK.

There are four major steps in this protocol. In the first two steps, the user sends an authentication request to the AP, and the AP replies with an authentication response. The authentication fails if the user's MAC address is filtered by the AP's blacklist, or the AP is overloaded with a large number of connections. In step 3 and 4, the user sends an association request to the AP and the AP returns the corresponding response. The user is authenticated and associated with the AP once these four steps are completed.

2.2 Attack using Rogue Wi-Fi Access Point

For attacks launched by deploying rogue Wi-Fi APs, there are four major parties as shown in Figure 1: a genuine AP, a regular Wi-Fi service user, a rogue AP, and an attacker. To launch the attack, the rogue Wi-Fi AP just simply sniffs the first three steps of the four-way handshake protocol between the user and the genuine AP. As the authentication process is in an open Wi-Fi network that does not involve any key exchange, the attacker is able to obtain the parameters sent by the genuine AP to the user. Then, by injecting an association response to the user right after its request is sent out in step 3 of the four-way handshake protocol, the rogue Wi-Fi AP will be associated with the user. This is because the user associated with the AP whose association response arrives first. This attack process is also illustrated in Figure 2.

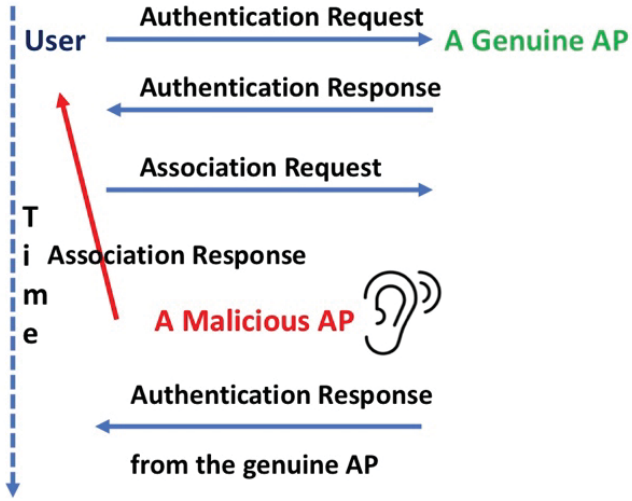

Figure 2. Attack Process Using a Rogue Wi-Fi AP

3. Detailed Construction

3.1 System Architecture

The system architecture of our design is depicted in Figure 3. To initialize the system, a map with target locations will be generated. In our system, we consider locations that are popularly selected by hackers to deploy rogue Wi-Fi APs as potential targets, such as coffee shops, restaurants, shopping malls, etc. Ad-hoc targets will also be added for special events that are hosted for a period of time. The map will be classified into multiple regions based on the density of targets. Different UAV-based detection systems can be deployed to cover multiple regions simultaneously. When checking a target location, the detection system first sniffs all available Wi-Fi signals and captures packets to analyze. These captured packets will be filtered and further analyzed to determine whether they are from rogue Wi-Fi APs. We now present the detailed construction of each module in our system.

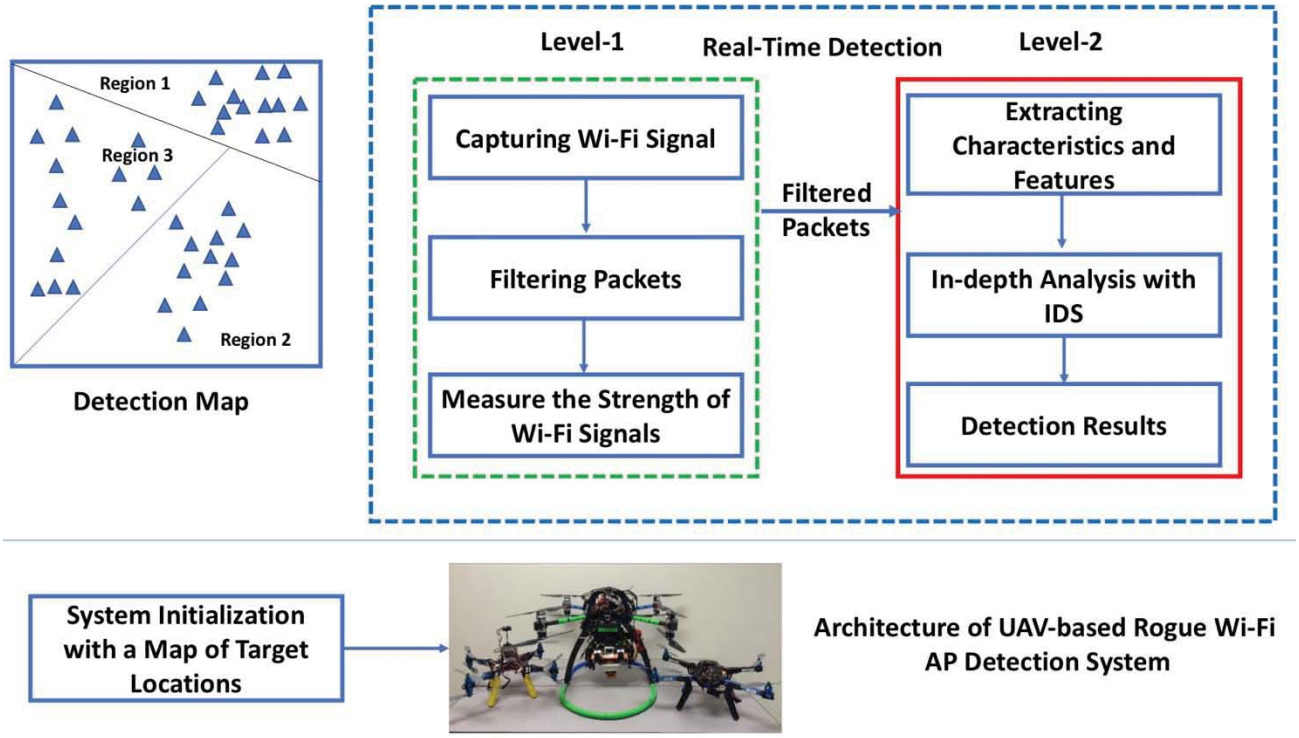

Figure 3. Architecture of UAV-based Rogue Wi-Fi AP Detector

3.2 UAV-based Rogue Wi-Fi AP Detector

The detection process of our design contains the three major modules: sniffing Wi-Fi signals, rogue behavior detection, and rogue AP information update. The UAV keeps checking pre-defined target locations and sniffing Wi-Fi signals around these locations. Wi-Fi signals captured will be further analyzed to determine whether the AP is rogue or not.

Sniffing Wi-Fi Signals: To enable long-distance detection, our design utilizes SDR to develop the Wi-Fi sniffer. Considering the limited lifting capacity of small-scale UAVs, a lightweight SRD - USRP B210 is adopted in our design, which is only 350 grams. USRP B210 has two channels with continuous RF coverage from 70 MHz – 6 GHz, and hence supports the sniffing of both 2.4GHz and 5GHz Wi-Fi signals. Currently, a set of SRD-based Wi-Fi solutions [8,9] have been proposed, which have been demonstrated to be effective in terms of receiving and decoding Wi-Fi signals. A Raspberry Pi 3 model B+ is also integrated with the UAV to conduct wireless signal decoding using GNU Radio [10] and follow up analysis.

Rogue Behavior Detection: Our design performs a two-level detection for Wi-Fi APs that might be rogue.

- **Level-1**: The first level of detection is based on the observation that a rogue Wi-Fi AP typically provides higher signal strength, which makes it easier to be selected by users. Thus, our detection system will measure the strength of each signal that can be detected in the target location using received-signal-strength-indicator (RSSI). Special attention will be given for these APs that have the same SSID but are using different channels. For these APs with high RSSI from multiple directions, we mark them as suspicious, and additional weight will be placed on them during the Level-2 analysis.
- **Level-2**: The second level of our detection will utilize existing intrusion detection system (IDS) for rogue Wi-Fi AP [11,12,13]. For example, by utilizing the lightweight IDS proposed in [13],

our system will extract the characteristics (e.g., retry bits, sequence number, and AID of both responses) and then perform in-depth analysis on it to determine whether the AP that sends out this frame is rogue or not. To be specific, raw frames captured by our Wi-Fi sniffer will be filtered first to discard these frames that are directed to other APs that are not being monitored. If the IDS finds the user device receives two association responses, these responses are marked as suspicious. These suspicious activities will be further analyzed to make the decision of whether the AP is rogue or not. More details about the IDS is available in [13].

Rogue AP Information Update: Once a rogue Wi-Fi AP is detected at the target location, our UAV-based system will send the information back to the ground station. The ground station then reports this detected rogue AP with the location information to the corresponding organization (e.g., local police department) for further process. The map for detection will also be updated based on the information of detected rogue Wi-Fi AP. Instead of marking the target location as completed, a re-check sign will be placed on it, which needs to be revisited later. Correspondingly, the route of checking will also be updated to minimize the detection cost.

4. Evaluation

In this section, we evaluate our proposed UAV-based rogue AP detection system with a proof of concept simulation. We mainly focus on the measurement of Wi-Fi signals using the SDR deployed on the UAV. In our evaluation, USRP B210is adopted as the SDR device. As our system can adopt existing in-depth Wi-Fi signal analysis modules [13] in our Level-2 design, its accuracy can be assured if the Level-1 Wi-Fi signal measurement is accurate.

In our evaluation, the SDR could detect two different band Wi-Fi signals in 2.4 GHz and 5.8 GHz. As shown in Figure 4 and Figure 5, we simulate genuine and rogue Wi-Fi APs that can generate 2.4GHz WiFi signal. The average power of energy of the genuine Wi-Fi AP is weaker than the rogue one. The rogue Wi-Fi AP broadcasts packets more frequently than the genuine one. Therefore, the packets from the Rogue Wi-Fi AP could occupy the channels and attract users to connect it.

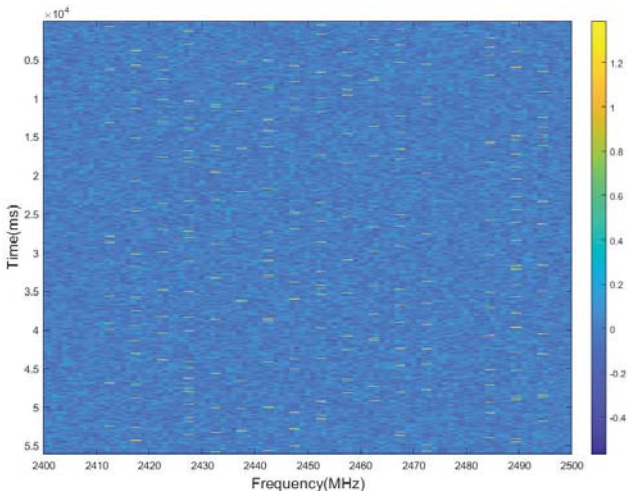

Figure 4. Genuine Wi-Fi AP in 2.4GHz

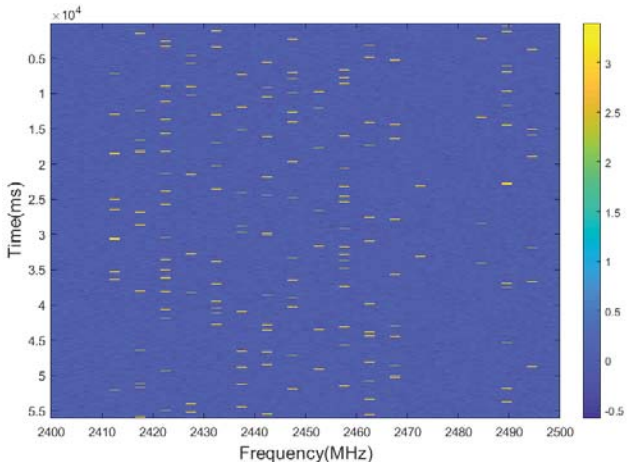

Figure 5. Rogue Wi-Fi AP in 2.4GHz

Figure 6 and Figure 7 presents the spectrum distribution of the Wi-Fi signal from the genuine and rogue Wi-Fi APs in 5.8 GHz respectively. The Wi-Fi APs in 5.8GHz have more channels than that in 2.4GHz. These APs are randomly distributed to a 20 miles X 20 miles area, in which there is a pre-defined flying route for the UAV to perform detection tasks. As shown in Figure 8, the detection accuracy is affected by the flying speed of the UAV. Figure 8 shows that with the increment of UAV' speed, the accuracy of detection based on both greedy path and fixed path reduce. Thus, we suggest that the speed of UAVs shall be controlled in a pre-defined limit to ensure the SDR's accurate measurement of Wi-Fi single.

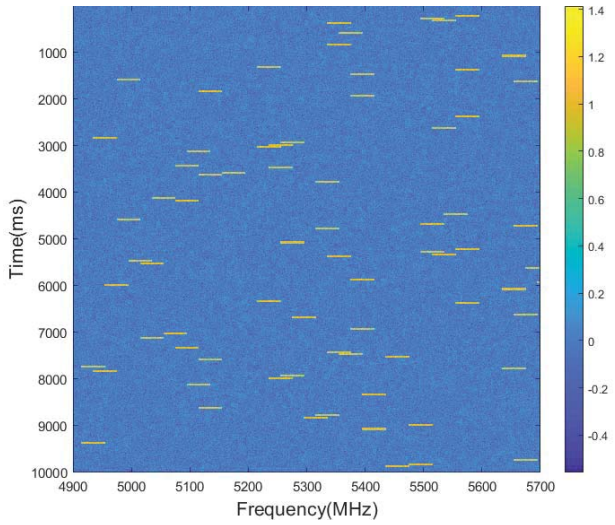

Figure 6. Genuine Wi-Fi AP in 5GHz

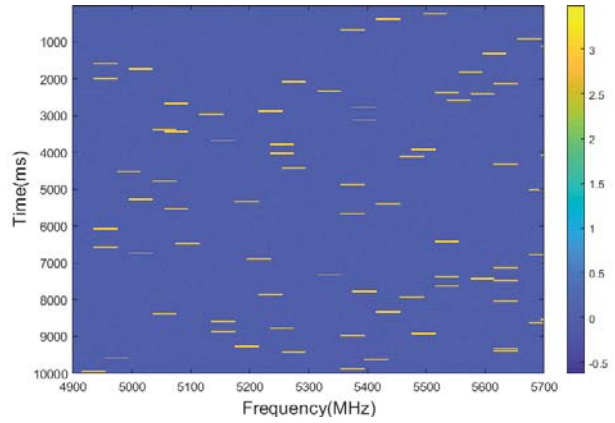

Figure 7. Rogue Wi-Fi AP in 5GHz

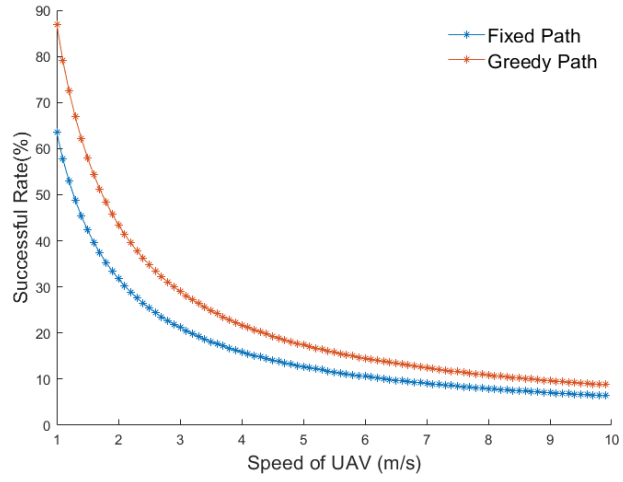

Figure 8. Wi-Fi Measurement Accuracy vs. UAV Speed

5. Related Work

The problem of detecting rogue APs has attracted significant attention from both industry and academy. To address this problem, a straightforward approach is to maintain a whitelist (or blacklist) by checking the MAC addresses of Wi-Fi APs. For example, [14] detects the presence of rogue AP by maintaining a whitelist of authorized MAC addresses of legitimate APs in the network. If the network sniffer captures packets from AP whose MAC address is not in the whitelist, then it is marked as malicious. In [15, 16], agent-based IDS solutions are proposed to detect rogue APs. In these solutions, the agent monitors the network and detect the presence of new APs, which are marked as malicious if they are not in the whitelist. While these solutions are easy to deploy, the MAC address spoof techniques make them easy to fail.

To enhance the effectiveness of detection, characteristics of wireless communication are used for detecting rogue Wi-Fi APs. Several commercial products have been proposed [17, 18] to distinguish between a genuine Wi-Fi AP and a rogue one by analyzing the wireless characteristics including MAC addresses, vendor name, and SSID. In addition, researchers also propose a fingerprint-based approach for rogue Wi-Fi AP detection [19, 20, 21], in which wireless characteristics including RSS values, radio frequency variations, and clock skews are extracted to generate a unique fingerprint for AP. For example, if a Wi-Fi AP's clock skew is different from existing clock skews in the database, the AP is then considered as a rogue one [21]. In [22], researchers utilized temporal characteristics (e.g., inter-packet arrival time) for rogue AP detection. In [20], the arrival time of consecutive Acknowledge pairs in TCP traffic is utilized. By examine the CSMA/CA mechanism and physical properties of half-duplex channel, [24, 25] are able to detect rogue APs using the round-trip time of TCP traffic. There is also a line of research that utilizes a hybrid approach that combines the analysis from both wireless and wired networks. In particular, [4] proposed to generate special packets and send them to a specified wired station through a wired network. Later on, if this kind of special packets is captured by the wireless sniffer, the corresponding Wi-Fi AP is considered as malicious.

6. Conclusion

Wireless attack via rogue Wi-Fi APs is a serious security problem, especially due to the ease of deployment. In this paper, we propose a UAV-based rogue Wi-Fi AP detection system, which utilizes the advantages of both UAV and SDR. Our system can provide detection with high mobility and enhanced detection range. The modular design of our system makes it can be easily combined with the existing Wi-Fi signal analysis solutions to ensure the detection accuracy.

For the future research of this project, we will fully implement a prototype of our proposed system and tune the system to optimize the detection performance in terms of efficiency and coverage.

References

[1] The Statistics Portal, 2018, "Number of Public Wi-Fi Hotspots Worldwide from 2016 to 2021", Available at: https://www.statista.com/statistics/677108/global-public-wi-fi-hotspots/

[2] L. Ma, A. Y. Teymorian, and X. Cheng, "A Hybrid Rogue Access Point Protection Framework for Commodity Wi-Fi Networks," in Infocom 2008.

[3] W. Wei, K. Suh, B. Wang, Y. Gu, J. Kurose, and D. Towsley, "Passive Online Rogue Access Point Detection Using Sequential Hypothesis Testing with TCP ACK-pairs," in IMC 2007.

[4] H. Yin, G. Chen, and J. Wang, "Detecting Protected Layer-3 Rogue APs," in Broadnets 2007.

[5] S. Shetty, M. Song, and L. Ma, "Rogue Access Point Detection by Analyzing Network Traffic Characteristics," in Milcom 2007.

[6] Hackread, 2016, "Internet Minefield: Beware of Fake Wi-Fi Spots in Rio Stealing User Data", available at: https://www.hackread.com/fake-Wi-Fi-spots-in-rio-stealing-data/

[7] IEEE Standards Association, 2004, "IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements".

[8] Bastian Bloessl, Michele Segata, Christoph Sommer, Falko Dressler, August 2013, "An IEEE 802.11a/g/p OFDM Receiver for GNU Radio", Proceedings of the Second Workshop on Software Radio Implementation Forum, Hong Kong, China, pp. 9-16.

[9] Bastian Bloessl, Michele Segata, Christoph Sommer, Falko Dressler, September 2013, "Decoding IEEE 802.11a/g/p OFDM in Software Using GNU Radio", Proceedings of the 19th Annual International Conference on Mobile Computing & Networking (MobiCom), Miami, Florida, pp: 159-162.

[10] GNU Radio, 2019, available at: https://www.gnuradio.org/

[11] Chao Yang, Yimin Song, Guofei Gu, September 2011, "A Timing-Based Scheme for Rogue AP Detection", IEEE Transactions on Parallel and Distributed Systems, Volume: 22, Issue: 11, pp: 1912 - 1925.

[12] Chao Yang, Yimin Song, Guofei Gu, September 2012, "Active User-Side Evil Twin Access Point Detection Using Statistical Techniques", IEEE Transactions on Information Forensics and Security, Volume: 7, Issue: 5, pp: 1638 - 1651.

[13] Chao Yang, Yimin Song, Guofei Gu, September 2012, "An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802.11 Wi-Fi Networks", International Journal of Wireless Information Networks, Volume: 2, Issue: 25, pp: 130 - 145.

[14] K. F. Kao, T. H. Yeo, W. S. Yong, and H. H. Chen, A Location-Aware Rogue AP Detection System Based on Wireless Packet Sniffing of Sensor APs. In: Proceedings of the 2011 ACM Symposium on Applied Computing, SAC '11, pp. 32–36. ACM, New York, USA 2011.

[15] V. Sriram, G. Sahoo, and K. Agrawal, Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN—A Multi-Agent Sourc- Ing Methodology. In: Advance Computing Conference (IACC), 2010 IEEE 2nd International, pp. 256 –260, 2010.

[16] M. K. Chirumamilla, Agent Based Intrusion Detection and Response System for Wireless LANs. In: Proceedings of IEEE International Conference on Communications, pp. 492–496, 2003.

[17] Rogue Access Point Detection, available at: https://www.solarwinds.com/topics/rogue-access-point-detection

[18] Rogue Device Detection & Access Point Protection, available at: https://www.pwnieexpress.com/rogue-device-detection

[19] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell., "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," in Infocom 2008.

[20] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," in Mobicom 2008.

[21] S. Jana and S. Kasera, "On Fast and Accurate Detection of Unau- Thorized Wireless Access Points Using Clock Skews," in Mobicom 2008.

[22] R. Beyah, S. Kangude, G. Yu, B. Strickland, and J. Copeland, "Rogue Access Point Detection Using Temporal Traffic Characteristics," in Globecom 2004. [23] W. Wei, S. Jaiswal, J. F. Kurose, and D. F. Towsley, "Identifying 802.11 Traffic from Passive Measurements Using Iterative Bayesian Inference," in INFOCOM, 2006.

[24] L. Watkins, R. Beyah, and C. Corbett, "A Passive Approach to Rogue Access Point Detection," in Globecom 2007.

[25] C. D. Mano, A. Blaich, Q. Liao, Y. Jiang, D. A. Cieslak, D. Salyers, and A. Striegel, "Ripps: Rogue Identifying Packet Payload Slicer Detecting Unauthorized Wireless Hosts Through Network Traffic Conditioning," ACM Trans. Inf. Syst. Secur., vol. 11, no. 2, 2008.

Acknowledgement

This project was supported by National Science Foundation REU grant (CNS-1757781)