August 2023

# ENHANCED WI-FI FINGERPRINTING FOR SECURITY

Vishal S Desai

Shayne Miel

Ardalan Alizadeh

Akshaya Nagarajan

# ENHANCED WI-FI FINGERPRINTING FOR SECURITY

AUTHORS:
Vishal S Desai
Shayne Miel
Ardalan Alizadeh
Akshaya Nagarajan

## ABSTRACT

Techniques described herein provide for an enhanced risk-based authentication method that greatly improves the quality of identifying the Wi-Fi identity associated with a remote worker and significantly reduces necessity of multiple multifactor authentication attempts. Techniques described herein support enhanced Wi-Fi-based user identification while still maintaining compliance with user privacy by not collecting user location information. Techniques described herein enhance Wi-Fi fingerprinting solutions by using unique physical layer signatures to curtail false positives and improve accuracy for detection of device identities.

## DETAILED DESCRIPTION

Wi-Fi fingerprinting is a minimally intrusive risk-based authentication feature that is an effective location proxy for converged, cloud-delivered security service edge systems. Wi-Fi fingerprinting optimizes zero trust multifactor authentication (MFA) via processing Wireless Local Area Network (LAN) information (e.g., service set identifiers (SSIDs)) derived from a secure access device and comparing the information against historical benchmarks at a similar location with a MinHash function. Wi-Fi fingerprinting provides additional inputs to a mobile authentication application for multifactor authentication and aims to reduce successive MFA attempts, which creates a better usage experience for remote and hybrid workers.

The dependence of Wi-Fi fingerprinting on Wi-Fi parameters provided by a mobile/laptop client chipset creates several issues. First, different vendors have unique Wi-Fi drivers that sometimes allow only a subset of information to be available to the mobile authentication application. For example, some companies do not allow access to basic SSID (BSSID) information unless location privileges are fully enabled by the end user of the mobile authentication application, which may not happen often.

Moreover, most of the wireless clients prioritize battery saving policies and, therefore, their scans are triggered based on roaming conditions only. Furthermore, a large number of use cases for mobile authentication applications involve remote workers working at home, cafes, and other public venues where the remote workers are susceptible to ad hoc networks, impersonators, and rogues.

In addition, benchmarks collected from the SSIDs can greatly vary from chipset to chipset, which leads to significantly more false positives. For example, SSID lists and signals (e.g., received signal strength indicators (RSSIs)) in certain laptops vary greatly, which calls to question the reliability of these historical benchmarks used for the comparison. While the MinHash function typically provides higher tolerance against deviations in the sets of SSID lists, there needs to be some level of consistency expected to avoid false positives. Unfortunately, mobile authentication applications do not have the authority to define acceptable levels of tolerance for the Wi-Fi chipset vendors, and enforcement of such levels is not practical.

Figure 1, below, illustrates an example in which a single SSID is mapped to multiple BSSIDs.


*Figure 1: Example of a Single SSID Mapped to Multiple BSSIDs*

As illustrated in Figure 1, in enterprise environments, a single SSID may be mapped to multiple BSSIDs to provide seamless roaming and load balancing across multiple access points in the enterprise deployment. The SSID is the name of the network while the BSSID is the base radio MAC address of each access point. In enterprise Wi-Fi deployments (e.g., campuses and retail stores), a single SSID is mapped to multiple BSSIDs to provide seamless roaming and load balancing across multiple access points. A non-trivial percentage of mobile authentication application users operate in carpeted enterprise environments and, due to the mapping of the single SSID to multiple BSSIDs, current

SSID-based filtering may not work well in these environments. For example, the current SSID-based Wi-Fi fingerprinting does not perform well in such environments since any location in the enterprise can be detected as a similar fingerprint. Single radios advertising multiple BSSIDs (MBSSIDs) may end up listed as multiple access points.

Techniques described herein address the above concerns and greatly reduce false positives. According to one technique described herein, MBSSIDs are used to identify the presence of the user in a certain location in an enterprise for an enterprise Wi-Fi network. MBSSIDs are very common as most of the Wi-Fi access points advertise multiple SSIDs to differentiate guest network versus, for example, a store or campus network.

Techniques described herein provide for an enhanced risk-based authentication method that greatly improves the quality of identifying the Wi-Fi identity associated with the remote worker and, therefore, significantly reduces the necessity of multiple MFAs. Techniques described herein enhance Wi-Fi-based user identity while still maintaining compliance with user privacy by not collecting user location information. Techniques described herein provide for a new mechanism of BSSID masking to support enterprise access points with dual radios in the same 802.11 spectrum. To avoid false positives triggered by dual radios in the same access points, techniques described herein support BSSID masking to generate a single BSSID for the radios supporting these multi-BSSIDs. Techniques described herein include four salient distinctions from the legacy method, including biasing toward radio frequency (RF) proximity, isolating ad-hoc networks, BSSID management, and 802.11 inspection.

Figure 2, below, illustrates a system that may implement the techniques described herein.

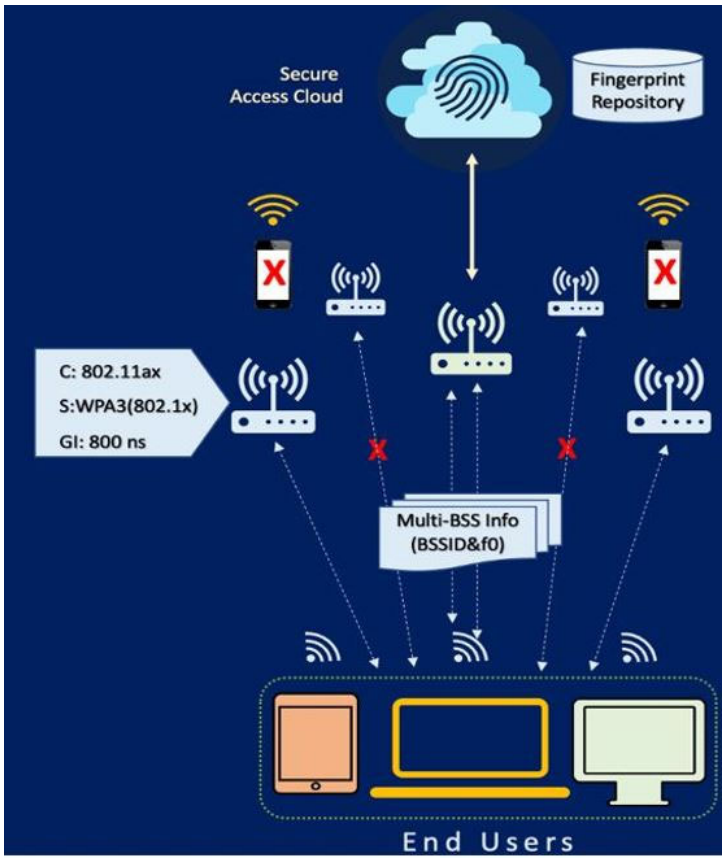


*Figure 2: Example System*

**RF Proximity-Based Filtering**

Previous methods evaluate the top 100 Wi-Fi signals at a user's location. Unfortunately, for most public venues, there is an increased potential of weaker Wi-Fi signals, which tend to fluctuate at a greater degree when a user moves few feet away from the source. Furthermore, as explained above, due to variations in the client vendor chipset front ends, RSSIs tend to vary even when the client doesn't move its location. To tackle both of these problems, techniques described herein introduce RF proximity-based filtering with a binning technique.

Figure 3, below, illustrates RSSI variation of a wireless station at a constant location.

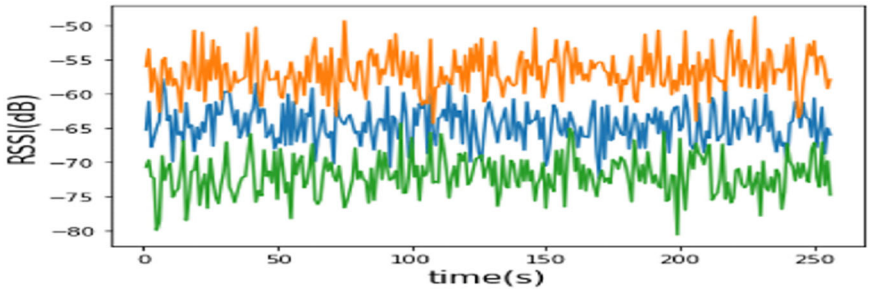


*Figure 3: Example RSSI Variation*

Techniques described herein evaluate Wi-Fi signals only above a certain RSSI cutoff. Signal cutoff can change based on a density of the RF signals observed by the station as well as SSID inspection. In one embodiment, the cutoff or threshold can be dependent on the user location and density of the Wi-Fi networks in the vicinity. For example, in stadiums/public venues, the threshold can be lower to be more conservative while in an enterprise campus this threshold can be higher. For example, in an enterprise with an observed high density of Wi-Fi signals, the SSID cutoff can be -70dBm and in a public venue with sparse coverage, the SSID cutoff may have a more conservative threshold of -85dBm.

Within a list of collected Wi-Fi signals, instead of using absolute RSSI/SNR samples (which tend to vary), the techniques described herein perform signal binning either on RSSI or SNR (if available) samples. Binning is conducted in either fixed sample bins (example: 6dB) or vary based on the RF density. For example, if more than 15 W-Fi signals are available between an SNR of 25db and 40dB, techniques described herein may introduce granular bins of 3dB. Otherwise, de facto 5dB bins may be used. Binning of the RSSI values may be based on fixed or variable ranges. For example, binning granularity will be based on the number Wi-Fi networks observed in the vicinity. For sparse network, techniques described herein support sparse binning of 6-10 dBm, while dense RF networks will support more granular binning of 3-5dBm.

**Ad-hoc Networks**

Today, with the proliferation of Wi-Fi, most of the public venues also suffer from massive presence of ad hoc networks. These ad hoc Wi-Fi networks are temporarily

enabled to either support peer-to-peer transfer (document or application transfer between two mobile devices) or support temporary Wi-Fi for basic connectivity.

Figure 4, below, is an example table illustrating example peer-to-peer mobile ad hoc networks. A peer-to-peer mobile ad hoc network may be created, for example, when a smart phone uses Wi-Fi tethering for laptops or tablets.

| SSID | BSSID | RSSI | IBSS | PROTOCOL | GI | SECURITY |
|---|---|---|---|---|---|---|
| a | d2:94:35:6b:5d:81 | -91 | 0 | 6 | 400 | RSN(802.1x/AES/AES) |
| b | ca:94:35:6b:5d:81 | -91 | 0 | 6 | 400 | NONE |
| c | 0a:b4:b1:b0:1c:1c | -90 | 1 | 6 | 400 | RSN(PSK,SAE/AES/AES) |
| d | 10:0c:6b:d4:c2:cd | -74 | 0 | 5 | 800 | RSN(PSK/AES/AES) |
| e | 98:9d:5d:d2:bc:b0 | -68 | 1 | 6 | 400 | RSN(PSK/AES/AES) |
| f | 10:0c:6b:d4:c2:ce | -59 | 1 | 5 | 800 | RSN(PSK/AES/AES) |
| g | 30:b6:2d:10:40:91 | -51 | 0 | 5 | 800 | NONE |
| h | 30:b6:2d:10:40:90 | -51 | 0 | 5 | 800 | RSN(PSK/AES/AES) |

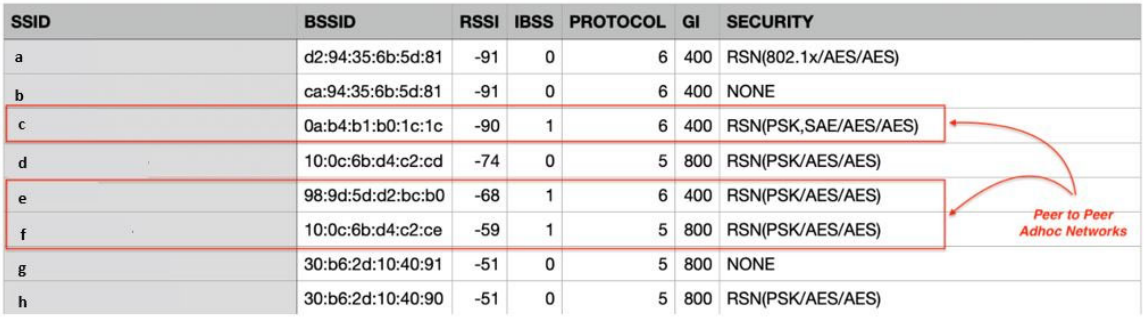


*Figure 4: Example Peer-to-Peer Mobile Ad Hoc Networks*

The mobile ad hoc networks have short sessions of operation, therefore they tend to create significant fluctuations in the sample set used for Wi-Fi identity. Techniques described herein distinguish mobile hotspots (marked under SSID 802.11 with the independent BSS (IBSS) set to 0) from Wi-Fi infrastructure access points (IBSS = 1) in 802.11 management frames. This will ensure Wi-Fi signals used for sampling don't fluctuate and, therefore, avoid false positives due to sample variation.

**BSSID Management**

As described above, one-to-one mapping of SSID to BSSID is not the case for most enterprise deployments. This is primarily done to separate guest Wi-Fi networks from retail/warehouse/cafe infrastructure Wi-Fi networks. Therefore, simply relying on SSID for validation isn't enough. Furthermore, in order to meet today's demands of the high efficiency wireless stations, access point models designed for enterprise Wi-Fi experience support multiple (dual) radios within the same spectrum (e.g., dual 5Ghz, dual 6GHz, etc.). With dual radios, in order to avoid station scanning delays, most of the WLAN vendors flip last nibbles of the BSSID to distinguish WLANs broadcasts.

In order to avoid false positives triggered by dual radios within a spectrum with the same access points and multi-BSSID support, techniques described herein support BSSID

masking for access points with dual radios. Techniques described herein also support built-in MAC nibble masking for multi-BSSID support. Techniques described herein better identity a single access point based on multiple MAC addresses corresponding to the multiple (dual) radios working in the same band based on masking the nibble of the radios and considering all of them as a single Wi-Fi fingerprint. This enhancement will address MBSSID and multi-radio operations in the same 802.11 spectrum. For example, when a dual radio access point advertises WLANs aa:bb:cc:dd:ee:**f0**, aa:bb:cc:dd:ee:**f1** & aa:bb:cc:dd:ee**:fc** for WLAN ID 1, 2 and 4 respectively, techniques described herein simply mask the last nibble and will consider a single entry (aa:bb:cc:dd:ee**:ff**) for the radio supporting these multi-BSSIDs.

**802.11 Inspection**

To support enhanced security profiling, techniques described herein inspect 802.11 WLAN capabilities, communication protocols, and security profiles associated with the WLAN. These additional attributes further filter out duplicate entries and, most importantly, curtail false positives due to malicious rogue and impersonator access points.

Inspection of following (but not limited to) attributes have been completed: Security Profile (example: WPA2 Enterprise/WPA2 Personal, WPA3 802.1x etc. can be used to associate deployment in which the user is operating. Typically, public venues/home locations tend to support more primitive version of sec enforcement compared to enterprise and Ed-Sector.), Communication Protocol (802.11ax, 802.11acw1, 802.11acw2, 802.11n, 802.11a/b/g etc.), Guard Interval (GI): 400ns, 800ns or 1600ns.

In summary, techniques described herein enhance Wi-Fi fingerprinting solutions with unique physical layer signatures to curtail false positives and improve detection accuracy for device identities. According to techniques described herein, BSSID masking filters false positives for MBSSID use cases and increases robustness in the dual radio enterprise deployments. Parameters that are used in the techniques described herein (e.g., ad hoc network filtering (IBSS), RSSI, security profile, communication protocol, guard interval, etc.) are not personally identifiable information, are available to mobile authentication applications without needing special permissions from the end user, and can be used by the application.