SMARTPHONE MODEL FINGERPRINTING USING WIFI RADIATION PATTERNS

Thomas Burton and Kasper Rasmussen

Department of Computer Science, University of Oxford, Oxford, UK

ABSTRACT

This paper aims to demonstrate the feasibility of our proposed method for fingerprinting different classes of wireless devices. Our method relies on the observation that different device types, or indeed different models of the same type, have different wireless radiation patterns. We show in detail how a small set of stationary receivers can measure the radiation pattern of a transmitting device in a completely passive manner. As the observed device moves, our method can gather enough data to characterize the shape of the radiation pattern, which can be used to determine the type of the transmitting device from a database of patterns. We demonstrate that the patterns produced by different models of smartphones are easily different enough to be identified. Our measurements are repeatably measurable using RSS with commercial-off-the-shelf hardware. We then use simulations to show the success of our method as a classifier.

KEYWORDS

Wireless Radiation Patterns, Device Fingerprinting, Identification.

1. INTRODUCTION

Antennas do not radiate power equally in all directions, and the resulting pattern of transmission energy is called a radiation pattern (or antenna pattern). The ability to remotely measure the radiation pattern of a device has a range of potential applications, from checking compliance with emission regulations and standards, optimising transmission power, smart routing and beamforming, to fingerprinting and identifying devices based on unique pattern shapes.

To demonstrate the power of the idea, we focus on fingerprinting smartphone models, which by itself has a number of interesting applications in intrusion detection; commercial analysis of the phone models in a group of users (e.g., for app development); and network analysis to understand what device types are using a network, for example, ensuring compliance with bring your own device to work policies. While fingerprinting provides a convenient application with which to demonstrate our radiation pattern measurement technique, the resulting fingerprinting scheme has a lot of benefits, making it a good competitor to existing approaches.

Existing approaches often focus on how the chipset or firmware behaves under certain circumstances. Fingerprinting in such schemes is conducted by either interrogating the device with differently formed packets or observing the device's particular behavioural characteristics. This can yield good results but will often require additional specialist hardware to inject packets or measure properties that cannot be achieved with commercial-off-the-shelf (COTS) networking infrastructure hardware. Additionally, when actively sending out probing packets, you alert the device to the use of fingerprinting.

David C. Wyld et al. (Eds): MLDS, NECO, SEMIT, IBCOM, SPPR, SCAI, CSIA, ICCSEA, WiMoA - 2021
pp. 283-303, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111823

Our method is entirely passive and relies on received signal strength (RSS), which is widely available across almost all networking hardware as it plays a vital role in network management and troubleshooting. This makes our fingerprinting method an ideal choice for situations where an existing wireless infrastructure already exists, e.g., a company WiFi installation or a LoRa city-wide network.

A receiver in a fixed location will measure the RSS of a transmission from another device differently depending on the transmitting device's radiation pattern, location, and orientation. When compared to measurements by other collaborating devices that form a measurement infrastructure, this will allow the calculation of several points on the radiation pattern of the transmitting device. In this paper, we use multiple receivers to measure several points on the pattern simultaneously for a single packet and attempt to find parts of known patterns that match the shape. We use this to create a fingerprinting method for smartphone models, exploiting the fact that each manufacturer has a slightly different antenna design and a different internal structure of the phone. As a by-product, the method also produces an estimate of the location and orientation of the device.

We summarize our main contributions as follows:

- We identify the challenges of using RSS for fingerprinting when not using location as a proxy for identity.
- We propose a methodology for passively measuring and reconstructing the radiation pattern of nearby wireless devices.
- We measure and analyze patterns from a range of smartphones to show that different models have significantly different patterns.
- We analyze how attacks on this type of system can be performed to break the model fingerprinting mechanism, and we discuss the required setup to mitigate those attacks.

The paper is organised as follows: in Section 2 we cover the necessary background knowledge to understand our proposal, followed by a discussion of related work in Section 3. In Section 4 we define the system model and adversary model. Section 5 presents the challenges to using radiation patterns for fingerprinting. In Section 6 we propose our method of fingerprinting. In Section 7and 8 we evaluate our solution with simulations and we compare patterns measured from a selection of smartphones. In Section 9 we perform an analysis to show the requirements to be secure against attacks. Finally, we conclude in Section 10.

2. TECHNICAL BACKGROUND

We now discuss the background knowledge related to radiation patterns necessary to understand our proposed method.

Directivity is a measure of how directional an antenna's pattern is, and it is one way to represent a radiation pattern. Directivity is defined as ``The ratio of the radiation intensity in a given direction from the antenna to the radiation intensity averaged over all directions'' [14]. From the definition, the directivity for a given elevation and azimuth, $D(\theta,\phi)$, is calculated by:

$$D(\theta,\phi) = \frac{U(\theta,\phi)}{P_{rad}/(4\pi)} \quad (1)$$

Where P_{rad} is the total radiated power output and U is the radiation intensity at the angle θ,ϕ. P_{rad} may be found through several methods, including: using the chipset specification; through

calculation using input power and efficiency; an estimate can be retrieved from the US Federal Communications Commission (FCC) certification test report; or by calculation of $U(\theta,\phi)$ integrated over the spherical surface if the pattern is represented by an equation [1].

$$P_{rad} = \int_0^{2\pi} \int_0^{\pi} U \sin\theta \; d\theta \, d \tag{2}$$

Directivity may be expressed as a ratio in dimensionless units or in decibels relative to another antenna. Most commonly, this is the theoretically perfect isotropic radiator, with a directivity of 1 expressed as a ratio or 0 dBi in all directions. The equations to convert between the two are as follows:

$$D_{dBi} = 10 \cdot log_{10} D \tag{3}$$

$$D = 10^{\left(\frac{D_{dBi}}{10}\right)} \tag{4}$$

3. RELATED WORK

There are two types of fingerprinting of interest: 1) unique device fingerprinting, where every unique device is distinguishable from every other; and 2) device type fingerprinting, where devices are categorised into groups based on some element of common hardware, software, or behaviour.

Unique device fingerprinting gives a very narrow and specific identity, whereas device type fingerprinting gives a very broad identity which may have further sub-categories.

3.1. Unique Device Fingerprinting

Existing fingerprinting or identification of wireless devices is done though a range of methods [29] that have different benefits and drawbacks when it comes to simplicity, computation, reliability, and required hardware. These methods range from simple addresses and cryptographic techniques to the analysis of signal properties.

The simplest method is for a sender to attach an identifier to their message. This is common across many types of networks and at different network layers. For example, TCP/IP uses IP addresses, and IEEE 802 uses MAC addresses. The downside is that an attached identifier can easily be spoofed or modified to achieve various goals. Cryptography can be used to supplement this approach by providing authentication when a device claims to have a particular identity. However, using cryptography leads to some issues, including initial key sharing and key revocation problems and cryptography being computationally expensive for low powered devices.

With access to a network, it has been shown that profiling the network traffic can be used to uniquely identify devices [9, 22]. While this may allow us to determine the software and operating system running on the device, it does not necessarily narrow the device down to one particular model. Also, an adversary can easily spoof this as network traffic is controlled by software that can be easily modified.

Unique device fingerprinting can fall into two categories at the PHY layer: 1) location-independent and 2) location-depended identity.

Location-independent techniques use radiometric properties of a signal for unique device fingerprinting. Radiometric fingerprinting methods can be broadly placed into three categories [11]: transient-based [12, 26], modulation-based [5, 23], and spectral-based techniques [3, 20]. These techniques have a very high accuracy rate, ranging from 70% to 99%, but the drawback of these methods is that they are difficult to deploy and need specialist hardware.

Location-dependent identity methods use a property where the location of a device produces some measurable change of that property. Existing work using received signal strength (RSS) [8, 6] and channel state information (CSI) [16, 17] has focused on using location as a proxy for identity. Using these methods, spatially distanced entities that claim to be the same entity can be distinguished. The downside of this method is that devices (or at least the genuine device in the case of an intruder detection system) must be static.

In order to use location-dependent properties (i.e. RSS or CSI) more generally on mobile devices, the location as a proxy for identity element must be removed. One such method proposed by Hua et al. [13] uses CSI data to infer the carrier frequency offsets (CFO), which arise due to fundamental physical properties of the device, which remains fairly consistent over time but differs significantly depending on the device. However, like many of these fingerprinting methods, the property is not inherent to a particular device type. To later determine the type, an enrolment step must first be performed.

Higher-level fingerprinting techniques have the advantage that they are easier to deploy as the data required is more accessible at the application layer of devices. Fingerprinting particular sensors onboard a device, e.g., the microphone or camera, is possible because applications running on a device can directly access the data feed from the sensors, and some sensors display unique characteristics even across devices of the same type [2]. The sensors can also be used to measure the properties of the device themselves. Perez et al. [24] demonstrated that the electromagnetic emissions of a smartphone can be measured onboard using the device's magnetometer or remotely and then be used to fingerprint the device providing 98.9% accuracy. However, with direct access to the application layer of smartphones, it is already possible to directly retrieve some identifiable information already, such as the manufacturer and model.

3.2. Device Type Fingerprinting

Device type fingerprinting aims to classify devices based on their hardware or software. This can be achieved by manipulating the preamble of packets to see how a receiver handles non-standard or malformed packets, for example, whether it drops the packet. Bratus et al. [4] demonstrated the feasibility for access point (AP) fingerprinting, and Ramsey et al. [25] showed a 99% accuracy when using this method to classify eight transceiver types. A different method by Gao et al. [15] classifies APs based on the time shift of a `packet train' when it is received and sent out by the AP. Although these methods have the advantage of being invariant with respect to the environment, they limit the number of possible unique fingerprints to the number of vendor implementations. For example, if Apple decided to use the same chips over their whole product range, the model would be indistinguishable if these methods were applied to smartphones.

We focus on using RSS for device fingerprinting because it has the large advantage that it is widely accessible across a range of hardware, making it easy to use and process without complex modifications to hardware or software. The focus is on WiFi antennas versus other communication technologies (e.g., Bluetooth and Zigbee) due to the ubiquity across the whole range of consumer electronic devices (including all smartphone models and generations), frequency of data transmission by background applications, and high probability of being in an active state.

3.3. Radiation Patterns

The work on using radiation patterns [7, 21] for improved localization supports the use of radiation patterns for device fingerprinting and model fingerprinting. Coca and Valentin [7] explored the impact of radiation patterns on range-based localization schemes. They found that devices exhibited their own subtle unique patterns, even among the same make and model devices. While Coca proposed additional onboard compasses and a calibration certificate for Wireless Sensor Network nodes, we think this can be leveraged for device fingerprinting. Mwila et al. [21] presented a Gauss-Newton approach to optimize localization. This approach also relies on knowing the orientation of the various entities and therefore relies on cooperation between the infrastructure and device to localize. We do not use this technique because applying it directly to our work is more challenging as there are more unknowns, making the optimization problem significantly harder.

For a device, such as a smartphone, the uneven distribution of energy may be caused by several factors, including the antenna pattern of the antenna itself [1] and the structure of the components packaged within the device causing reflection, diffraction, and attenuation. From now on, we use the term radiation pattern as we refer to the pattern produced by the device as a whole, not just the antenna.

4. SYSTEM AND ATTACKER MODEL

We consider a scenario based on a hybrid `bring your own device' to work and company-issued device environment. Some devices like desktops are company-issued, but most employees also bring in their personal smartphones. These devices are allowed to connect to the network, so they have Internet access away from their desks. However, the company has a policy that requires employees to keep software up-to-date if they want to use their personal devices. To enforce this, the company bans smartphones that cannot get the latest iOS and Android security updates, effectively banning some old models and some manufactures entirely. If a device not on the allowed list $\mathcal{L}$ is detected on the network, then it can be investigated further by other means.

4.1. System Model

The fingerprinting system is deployed in the area of interest $\mathcal{A}$. A set of receivers are in fixed positions around the environment. These sniff all network traffic on the network channel and they record the sender MAC address, received signal strength, and a packet identifier (e.g. a hash of the encrypted packet). The records are then sent to a central *calculation server* (CS) through wired connections. The packets are linked to a device using the MAC address, which we assume does not change while in use. Any attempt to modify the MAC address would cause communication problems at the network layer rendering an attack on identity pointless in this case. The multiple RSS measurements at the different receivers are linked together by the encrypted packet hash. CS knows the position of each receiver, has an RSS map of the environment, and has access to a public database of patterns, so enrolment of every device model is not required. However, an allowed model list $\mathcal{L}$ is maintained and only devices that are allowed on the network are listed. The CS performs the fingerprinting process we later discuss in Section 6, and the model with the closest match to a set of reference patterns will be found, and if a device fails to match a device from$\mathcal{L}$, it will be flagged for further investigation.

For the purpose of later descriptions, every transmitter and receiver has an x, y, and z position and each entity also has an orientation. Rotation is possible around the 3 axis azimuth ϕ (z-axis), pitch θ (x-axis), and roll ψ (y-axis).

The system has the following guarantees: 1) after a coverage metric c has been reached, a device will be flagged if it is classified as a device not in $\mathcal{L}$ for a set amount of time t (c and t are tuneable parameters); 2) if there is insufficient data to determine the model of the device, i.e. to many packets have been dropped (discussed in Section 6.1) or there is insufficient pattern coverage (discussed in Section 6.2), it will also be flagged.

4.2. Attacker Model

The attacker's goal is to access the network with a smartphone not in $\mathcal{L}$ and continue to use the network without being flagged. To achieve this, an adversary must trick the system into believing that the device not on the allowed list is one of the device models on the allowed list.

We make the following assumptions about the attacker's capabilities: the adversary is allowed A1) to choose any device on the not allowed list; A2) use the device in any location within $\mathcal{A}$; A3) full knowledge of how the system works; A4) access to the database of receiver positions and public database of patterns; A5) to make correct estimates of the RSS map for the environment; A6) to make external modifications to their device to modify the pattern using blocking materials placed externally onto the device (this includes a conventional off-the-shelf phone cover or custom made blocking materials).

The adversary may not N1) modify or prevent communications between the receivers and CS; N2) modify the hardware or software on the receivers or CS; N3) modify data in any of the databases used by CS; N4) interfere with the site survey phase; N5) modify the internals of their device or the operating system; N6) move objects in the environment to cause slow-fading in select directions at a distance; N7) perform beamforming to attack; N8) use multiple smartphones; N9) change their pattern once beginning their attack, as this would require them to re-measure their pattern after each change; N10) we must also make the assumption that if two models have the same pattern but are forced to run different software (i.e. the devices have the same hardware but for whatever reason one model cannot use the latest security updates), then they are both placed on the banned list.

5. CHALLENGES

Several challenges make the process of fingerprinting using radiation patterns difficult to perform in practice:

Measuring directivity at a distance. The core of this approach is being able to measure the directivity of a transmitter at a distance. This is not a value that can be measured on its own. Instead, it must be calculated by comparing the RSS measurements to samples measured for a *reference transmitter* with a known directivity. This is discussed in more detail in Section 6.

Resolving low resolution data. Ideally, RSS measurements would be taken using a huge number of receivers (i.e., hundreds) from different directions. This would give extensive coverage of the radiation pattern, which would give many points on the pattern to match and potentially, a machine learning approach could be taken to classify the devices. In reality, there would be a much smaller number of receivers, and with a small number of receivers, a close match for several reference patterns may be found for some orientation. Therefore, measurements need to be made for many packets over time as the device moves through the environment. This should then expose different parts of the radiation pattern to the receivers and give larger pattern coverage.

Temporary slow-fading and fast-fading. Objects moving around the environment may have a temporary effect on the received power from particular locations. By taking measurements from many packets, any temporary objects causing slow-fading will only temporarily affect a small number of measurements. Using many packets will also reduce the impact of fast-fading.

6. MODEL FINGERPRINTING METHOD

We will initially discuss the process at a high level to give an intuition of the process before going deeper into the details of each step.

Suppose the directivity is known for some directions from a device. In that case, this is matched to a known pattern by finding the pattern and orientation that has the smallest error to determine the model of the device, as shown in Figure 1. In this example, with the 4 data points, there is only one possible pattern it matches. However, calculating the directivity values from RSS measurements is the more complex part of the process. A set of receivers are used to measure RSS samples from a series of packets to achieve this. The RSS value measured by each receiver is a combination of many factors, including the device's directivity in the direction towards the receiver. It is impossible to calculate the directivity from a single measured RSS value as the device could be at any range, orientation, transmission power, and have any pattern shape. However, by combining multiple RSS measurements from multiple receivers, different candidate positions, orientations, and pattern shapes can be tested to minimise the RSS error from the expected values to estimate the most likely values for position and orientation for each candidate pattern. With an estimate for these values, there is enough information to estimate the directivity in the direction from the transmitter to each receiver by comparing the measurements to measurements previously collection from a reference transmitter with known directivity in the same environment. This is discussed further in Section 6.1.

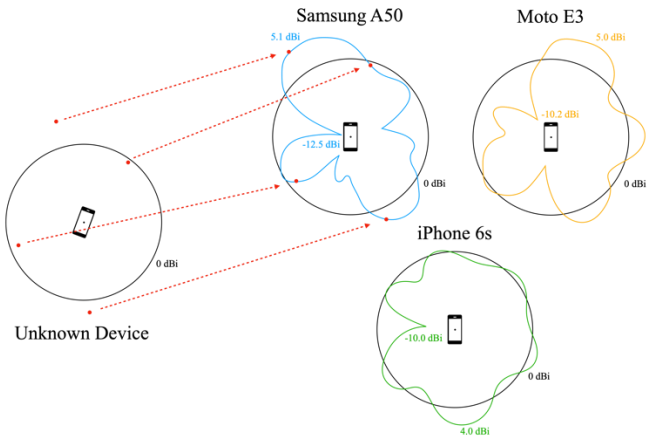


Figure 1. Diagram showing directivity measurements from an unknown device being matched to a known pattern. The patterns are shown in 2D relative to a black circle of 0dBi, representing a theoretical isotropic radiator. The largest and smallest directivity are also labelled.

To rebuild the shape of a pattern, RSS samples need to be collected for multiple packets as the device moves to increase the pattern coverage. The device is classified as the pattern with the lowest overall error. A series of packets and substantial pattern coverage is required to increase accuracy by reducing the impact of fast-fading and temporary slow-fading, ensuring important pattern artefacts are not missing from the inferred pattern, and increasing the difficulty of attacks. Therefore, classification will become more accurate with larger numbers of packets. The confidence of the classification result can be quantified by measuring the pattern coverage of all

the possible patterns, and this coverage can be represented as a coverage metric. Classification is discussed further in Section 6.2.

Before identification can be performed, there are some preliminary tasks that must be conducted: Firstly, the pattern of all the devices one may wish to identify must be enrolled (This first part of this step can be skipped if the operator has access to a public database of patterns). These patterns are called the *reference patterns* and are measured by rotating the devices around two axes at set increments at a fixed distance from a receiver to collect samples at all directions from the device. This measures the signal strength at different azimuths and elevations. The receiver must be in the far-field region of the transmitter to ensure the pattern has fully formed. During this phase, the *reference transmitter* pattern must also be enrolled. We will explain the purpose of the *reference transmitter* shortly. Although it has an omnidirectional pattern measuring the reference transmitter's pattern is an important calibration step because the directivity is only constant in one plane. The directivity is calculated using the measured RSS samples to create the pattern. Equation (1) is used to calculate the directivity. To calculate P_{rad}, a polynomial equation is fitted to the collected RSS data, and then the integration step is performed on this equation. We found that for 2D patterns, the number of coefficients required for a good fit varied between 20 and 45 depending on the pattern.

Secondly, a site survey must be performed using the *reference transmitter* that has a known pattern and orientation. RSS samples are collected from many points around the environment to form a power map in a similar way to many existing fingerprint-based localization schemes [18, 28]. The RSS map is built by placing the reference transmitter at different positions throughout the environment (the transmitter is placed at a fixed orientation α) and measuring the RSS at each receiver. For each location there is now a set of RSS values with 1 value for each receiver that is in range $\{P_{0_{ref}}, \dots, P_{n_{ref}}\}$.

Now that the preliminary tasks have been completed, we come to the actual identification. A device enters the area of operation $\mathcal{A}$ of the fingerprinting system. The aim is to classify it as one of the *reference patterns*. To match a device to a *reference pattern*, the directivity must be measured remotely and then the best matching *reference pattern* must be determined.

The number of receivers is variable and there is a trade-off of several factors including cost of hardware deployment, computational cost, number of packets required for accurate classification. At least n receivers are required to detect a packet for the calculations to proceed with that packet, with n being a configurable value. Enforcing a minimum n ensures that the number of receivers required to have a high classification accuracy is maintained. Depending on the receiver deployment, n may be smaller than the total number of receivers deployed. This is necessary if the area of operation is large and some areas would be out of range of some receivers. Throughout the remainder of the explanation, we use 4 receivers as an example and consider the 2-dimensional case for simplicity. For the 3D case, an extra component is added to any pattern access, and there are more possible orientations to consider.

The method is broken down into two parts: firstly, for every packet that is received, the RSS data measured by the receivers is processed to calculate the directivity, this is explained in Section 6.1; and secondly, at any time classification may be performed to find the best match along with a coverage metric c, explained in Section 6.2.

6.1. Remotely Measure Directivity

RSS values are measured for a packet recorded by each receiver to give$M = \{P_0, \ldots, P_n\}$. If less than n receivers receive the packet, the packet is dropped, but the packet still counts towards the number of packets used to calculate c.

For each possible *reference pattern*–which we refer to as the candidate *reference patterns* as we do not yet know which reference pattern is correct–the location and orientation with the best match to the measured data is found using the method we now describe.

We model RSS as a combination of transmission power (T_{px}), the directivity of the transmitter (D_t), the directivity of the receiver, slow-fading caused by the environment, path loss, and the effects of fast-fading [10, 27]. The impact of fast-fading is reduced by repeating this process for many packets, so we do not include this in our model equations. We assume that the slow-fading effects of the environment, path loss, and directivity of the receiver are constant from the same transmission location. Therefore, we simplify this by combining these constant values into the single constant E.

$$RSS = T_{px} + D_t + E \tag{5}$$

(5) is rearranged to separate the constant E.

$$E = RSS - T_{px} - D_t \tag{6}$$

Using (6), we can now compare different transmitters at a single location as the E from (6) will be the equal for both the correct reference pattern and the reference transmitter if the location is correct.

The values for the *reference transmitter* and each candidate *reference pattern* are substituted in to (6) so there is a system of n equations, one equation for each receiver, in the form:

$$L_{n_{ref}} - T_{px_{ref}} - D_{ref} = M_n - T_{px} - D_t \tag{7}$$

On the left-hand side of (7) there are the values for the reference transmitter, and on the right-hand side, there are the values for the candidate reference pattern. The sides are both equal because if they are at the same location, the environmental effects are also the same. Looking at each variable of (7) individually: $L_{n_{ref}}$ is the power received by the receiver n from the reference transmitter at location L, the reference transmitter transmission power $T_{px_{ref}}$, the directivity of the reference transmitter in the direction of the receiver D_{ref}, M_n is the actual RSS measured from the device to be identified by the receiver n,T_{px} the transmission power of the device corresponding to the candidate reference pattern, and D_t the directivity of the candidate reference pattern in the direction of receiver n.

To find the values D_{ref} and D_t we must fetch $pattern_{ref}[\alpha']$ and $pattern_{candidate}[\phi']$ respectively which are the directivity values from the patterns measured in phase 1. To calculate relative angles α' and ϕ' from the position of the various entities and the rotation values α and ϕ of the transmitters, the dot product of the transmitters rotation matrix and vector defining the relative position of the receiver and transmitter is calculated. The relative angle is then calculated between the two entities, converting from Cartesian coordinates to polar coordinates. In 2D space, these several steps are shown in the following equation for ϕ':

$$\phi' = atan2\Big(\sin\phi \cdot (R_x - T_x) + \cos\phi \cdot \big(R_y - T_y\big), \cos\phi \cdot (R_x - T_x) - \sin\phi \cdot \big(R_y - T_y\big)\Big) \quad (8)$$

(8) is the equation also used to calculate α'. Calculating the relative angles is more complex for 3D environments and radiation patterns as we must consider the rotation of the transmitter around 3 axes. However, this can be achieved relatively easily using the same method by adding an z component to the position vector and two additional rotation matrices for rotation around all 3 axes.

Using equation (7), the minimum squared difference between the two sides based on the RSS samples must be found to identify the closest location and orientation for each reference pattern. From the set of possible locations and orientations, the minimum value is found to determine location L and orientation ϕ:

$$\underset{L \in sampleLocations, \phi \in [-\pi, \pi]}{\operatorname{argmin}} \left(\sum_{n=0}^{R} \left(\left(L_{n_{ref}} - T_{px_{ref}} - D_{ref} \right) - \left(M_n - T_{px} - D_t \right) \right)^2 \right) \quad (9)$$

The values within the sum correspond to the values from (7). $\mathrm{M_n}$ is the actual measured RSS value for receiver n; $\mathrm{T_{px}}$ is the transmission power of the device corresponding to the reference pattern; $\mathrm{D_t}$ is the directivity from the reference pattern or more precisely $\mathrm{pattern_{candidate}}[\phi']$, where ϕ' is the relative angle to the receiver from the candidate location with a candidate rotation of ϕ; $\mathrm{L_{n_{ref}}}$ is the RSS value measured from the reference transmitter during the site survey by receiver n; $\mathrm{T_{px_{ref}}}$ is the transmission power of the reference transmitter; and $\mathrm{D_{ref}}$ is the directivity of the reference transmitter or more precisely $\mathrm{pattern_{ref}}[\alpha']$, where α' is the relative angle to the receiver when the site survey was performed.

Using the minimum value from (9), the location L and orientation ϕ of the best match has now been estimated for each reference pattern. For each reference pattern, the process is now reversed to estimate the *measured Directivity* in the direction of each receiver.

$$measuredDirectivity = M_n + T_{px_{ref}} + D_{ref} - T_{px} - L_{n_{ref}} \quad (10)$$

The (*measured Directivity*, *azimuth*) pair for each data point is calculated and stored for each reference pattern, where the azimuth is the direction to the receiver in the device's reference frame. If overlaid on the reference pattern database in 2D it may look something like Figure 2(a) with the red dots marking the *measuredDirectivity* values. In addition, the location and orientation can also be saved so the estimated movement can later be viewed for each possible pattern if desired. To be clear, the best matching location and orientation are found individually for each reference pattern, and therefore, the *measuredDirectivity* is calculated individually for each reference pattern. This can be seen in the Figure 2(a) example as the angles between the red dots on each pattern are different.

As previously stated, this process is performed on a series of packets to find the best reference pattern match later, so this process needs to be repeated for every received packet. As more packet samples are collected, the result will look more like Figure 2(b).

6.2. Classification

The identity is then resolved by finding the reference pattern with the closest match to the calculated *measuredDirectivity* data. This is performed by calculating the squared sum of the difference between the reference pattern directivity and the *measured Directivity* values. The reference pattern with the lowest average difference between the measured values and the actual pattern is the estimated device model.

To account for fast-fading and temporary slow-fading effects, this should only be performed when a sufficient number of measured points are taken. Ideally, the device should also have some movement during the collection time to expose more pattern segments to the receivers. As the location and orientation output correctness is not guaranteed, it is not possible to use these values to enforce movement, which is crucial for increasing the accuracy and, as discussed later on, preventing attacks on the system. However, if we look at each of the reference patterns and see that they all have significant coverage of the entire pattern, we can be confident that the transmitter has exposed a significant proportion of its pattern to various receivers. Therefore, a coverage metric c is used to give some indication of the confidence of the classification.

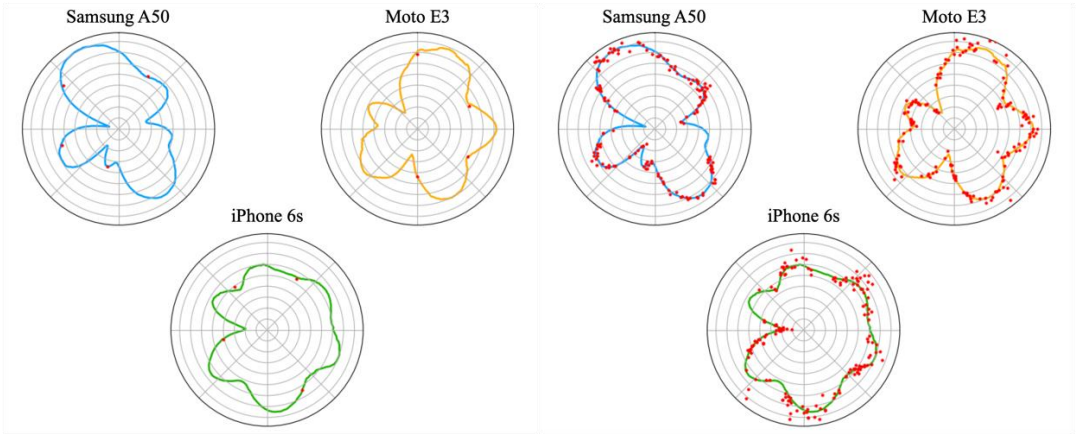


Figure 2. Examples of reference patterns database overlaid with (a) first set of *measuredDirectivity* data calculated after 1 packet and (b) after 40 packets with movement of the transmitter. The coloured lines show the whole pattern, and the red dots mark the *measuredDirectivity* values. Measurements are shown on a dBi scale.

To calculate the coverage metric c for any instance of classification, each reference pattern is split up into equal wedges with an angle of Ω, as shown in Figure 3, and the smallest value ofΩ is found that ensures that there are at least w% of data points in every wedge for all the reference patterns–we refer to w% as the wedge requirement and it is a tuneable parameter. For ease of comparison, Ω is normalised to between 0 and 1 and inverted so that a higher value indicates higher coverage, with 1 showing there is complete coverage with the wedges as small as the resolution of the pattern and 0 indicating that the coverage requirement is only met if Ω is 360°. It is important to note that if the operator is not careful, the coverage metric begins to break down past a certain point. For example, if the wedge requirement w is 1% then it is impossible to meet the wedge requirement if patterns are split into more than 100 wedges. The relationship between this coverage metric and classification accuracy is discussed further and evaluated in Section 7.3.

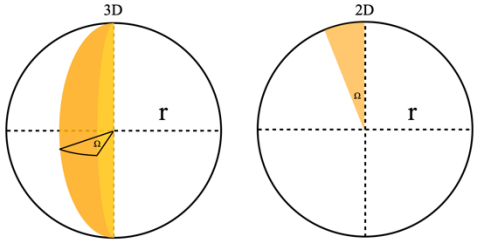


Figure 3. Radiation pattern sphere or circle sliced into wedges of Ω

The operator can use c in a variety of ways. For example, suppose a device cannot attain a threshold c after a set amount of time. In that case, the classification can be set to fail. Alternatively, the system can be configured only to accept classification results above the threshold.

6.3. Optimisations

This technique relies on an exhaustive search of the possible patterns, locations, and orientations, so optimisations are essential.

Firstly, the values for ϕ' and α' for each combination of location and orientation can be pre-calculated, so no matrix or trigonometric functions need to be computed at run time.

Secondly, a pattern can be stored in the form of a polynomial equation or as an array. Although storing a pattern as an equation saves some storage space, it comes at a high computational cost. Fetching a single directivity value requires calculating many exponents for the equation versus fetching a single array value. Storing patterns as arrays has a far lower computational cost, and the directivity value can be fetched using the azimuth and elevation as indexes.

Thirdly, during classification, the number of records to be stored for each device to be identified is approximately $nReceivers \times nPackets \times nReferencePatterns$.

With a huge number of reference patterns and/or devices to be identified, the data to be stored may grow to an unmanageable amount. To resolve this, once a storage size limit set by the operator is reached, the data from the bottom half of the matching patterns are deleted, and those reference patterns are no longer considered. Not only does this reduce the storage requirements, but it also reduces the computational cost of checking each reference pattern.

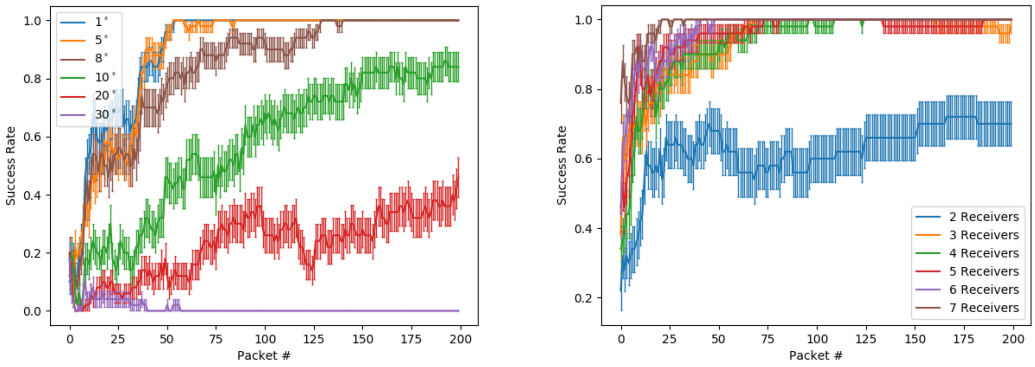
Fourthly, further processing time optimisations can be performed to reduce the number of locations to check, which may be expensive for large numbers of locations from the site survey and reference patterns. The computational requirements can be reduced in two ways 1) for the first i samples, the rough area can be calculated using a non-linear least squares optimiser for which it is assumed all patterns are isotropic and only the region with a high probability of being the locations with this less accurate method is searched thoroughly; and 2) after the first i samples a movement speed constraint can be added to prevent unnecessary checking of some locations that would be impossible to reach (e.g., locations more than 10m/s distance away from the previous packet can be discounted in the case of limited human movement).

7. EVALUATION

We evaluate our proposed method using radiation patterns collected from actual smartphones–we discuss the pattern collection further in Section 8–and simulations to explore the relationship between classification accuracy and several factors, including the number of packets, pattern fidelity, number of receivers, and our coverage metric.

For each of our simulations, we simulated 20m by 20m environments with receivers placed around the perimeter. We generated the simulated site survey data with 1m spacings between each survey point. A device to identify was then moved through the environment, and RSS samples were calculated, and random Gaussian noise with a standard deviation of 1.5dBm was added. The classification was then performed, and the results were outputted. 7 reference patterns collected from real devices as is discussed in Section 8.4 were used, this included the 2 modified patterns from the iPhone 6S, and only 1 pattern was used when there were multiple devices of the same make and model.

For the initial simulations, a device to simulate is selected from the list of reference patterns, and the success rate of classification is measured. Each simulation consisted of 50 runs, and the output plots we present show the mean result for the 50 runs with binomial proportion 95% confidence intervals marked for the success rate data. For each simulation, 200 sets of simulated RSS samples were used. Given that this is used for identity verification, we also tested it as a binary classifier and plotted the true positive rate (TPR) and false positive rate (FPR) on a receiver operating characteristic (ROC) curve for various coverage metrics c. Again, this used simulations with 200 sets of RSS data, but 420 runs of the simulation were performed.



(a) (b)

Figure 4. Success rate of classification using different (a) numbers of receivers and (b) pattern resolutions (i.e., the angle step between measurements) over 50 simulation runs with 95% confidence intervals marked.

7.1. Pattern Fidelity

The resolution of the pattern measurements impacts classification accuracy, as with more measurement points of the pattern, the pattern is of higher fidelity. With a lower pattern resolution, essential portions of patterns may be missed. This has the impact of significantly reducing the accuracy of classification. To demonstrate this, we performed simulations using various resolutions. We removed data between resolution steps and rounded the azimuth calculations to the nearest step to create the different fidelity patterns. The results in figure 4(a) show a significant increase in the number of packets required for accurate classification followed by degradation in classification accuracy as the resolution was reduced.

7.2. Number of Receivers

To demonstrate the relationship between the number of packets and the success rate of classification for different numbers of receivers, we varied the number of receivers in our simulations. The results are shown in figure 4(b) and–as expected–with 2 receivers, the success rate is significantly lower than with a larger number of receivers. For 3 receivers and above, the graph also shows that more receivers require fewer packets to achieve a higher success rate.

7.3. Coverage Metric

As already stated, exposing a greater proportion of the pattern is essential for increasing accuracy. However, there is no guarantee of movement or rotation, which is how greater pattern coverage is achieved. The coverage metric c is calculated for this reason, which is an indication of how much of the transmitter's pattern has been covered by the directivity measurements. Ideally, a high c would imply a high classification accuracy. That way, after any classification instance, one would have an estimated device identity and an indication of the likelihood of this being correct.

To demonstrate this increase in classification accuracy, simulations were performed. In each of the simulations, after every packet, classification was performed. This allowed the TPR and FPR to be recorded along with the coverage metric of that classification instance. The results of this are shown in Figure 5. The results demonstrate that as the coverage metric increases, the performance of the classifier improves. From this, we can conclude that with a higher coverage metric, we can be more confident in the accuracy of the classification.

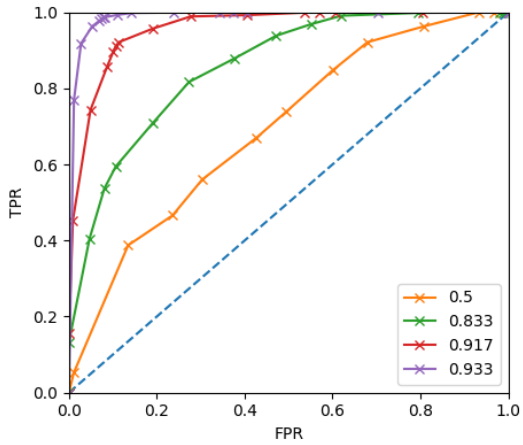


Figure 5. ROC curve of the classifier using a wedge requirement of 1%. Each line shows the curve for different output coverage metrics c.

8. SMARTPHONE PATTERN UNIQUENESS

To use WiFi radiation patterns for device type fingerprinting the patterns of each type must have the properties of 1) uniqueness and 2) repeatability. To explore these two properties in smartphone patterns we measured the pattern around 1 axis for 6 different smartphones.

8.1. Data Collection Framework

We used Raspberry Pi Model 4 boards running Ubuntu 19.10 (GNU/Linux 5.3.0-1022-raspi2 aarch64) as the platform for data collection. A USB external WiFi adapter with the Mediatek 7601u chipset placed into monitor mode was used for collecting wireless packet information, including sender MAC address and RSS. A separate Raspberry Pi controls a stepper motor that was used to rotate the phone 1º per second at a distance of 4m from the receiver. The transmitting device being measured is configured to transmit a packet approximately every 100ms. The Raspberry Pi clocks were synchronised to within 500ms and each packet received is matched to a rotation value by closest time. Therefore, the difference between the actual rotation value when the packet is transmitted and the measured rotation value should be $\pm 1°$ providing a pattern resolution of 1º.To prevent interference from other devices a wireless router was used to setup a network using a channel that did not overlap with any other surrounding networks. The MAC address of the device being measured was used to filter out packets from devices related to the data collection setup and rogue devices (e.g. probe requests).

The pattern in the horizontal plane with the device flat on its back was measured for 6 devices: 1) a Samsung Galaxy A50, 2) an iPhone X, 3) an iPhone 6S, 4) an iPhone 5S, 5) a Motorola Moto E3, and 6) another Motorola Moto E3.

8.2. Pattern Correlation

Firstly, we found that repeat pattern measurements collected on different days from a single device visually match and have a high linear correlation, as shown in Figure 6. Secondly, we found that devices of different models have a lower correlation. Each pattern was overlaid with one another and one was rotated in 1 degree increments while the normalised cross-correlation was calculated for each degree of rotation and the rotation that yielded the highest cross-correlation was taken as the best match. Figure 7 shows the maximum normalised cross-correlation between different pattern measurements of different devices. When multiple measurements of the pattern are made, the average maximum normalised cross-correlation of matching devices was 0.91. The average maximum for non-matching devices was 0.54.

This demonstrates that there is pattern uniqueness between the devices we measured and repeatability across devices of the same make and model.

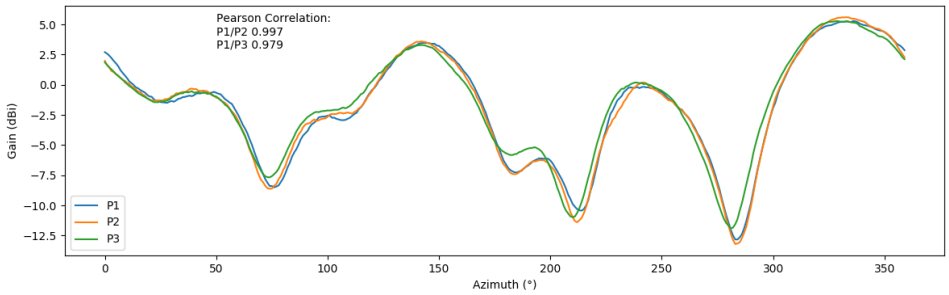


Figure 6. The diagram shows repeated measurements of the radiation pattern from the same Samsung Galaxy A50. This demonstrates that repeated pattern measurements result in the same pattern.

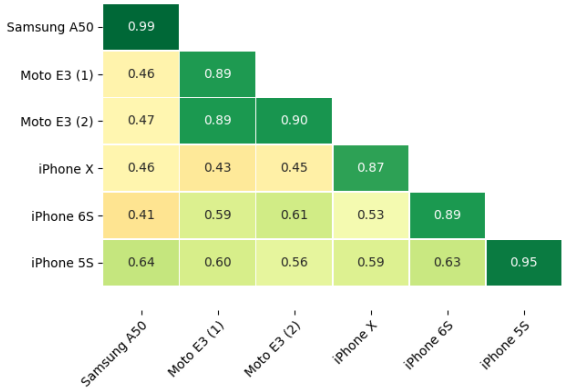


Figure 7. Normalised cross-correlation of smartphone radiation patterns. Each box gives an average of the cross-correlation when comparing the corresponding device on the y-axis with the device on the x-axis. Each device had its pattern measured at different times and was compared to every other device. The boxes on the diagonal consist of 3 averaged values as we do not compare a measurement run to itself. All the other boxes are the average of 9 values (3x3 runs).

8.3. Patterns from the Same Model

Coca [7] discussed the potential for devices to have their own unique patterns when compared to devices of the same model. However, in our experiments, conducted in an office environment, the patterns for the two Moto E3 devices did not show a significant difference. The level of difference was very similar to that of the repeat measurements for the iPhone X and 6S, which is likely caused by the effects of fast fading.

While our experiments for comparing two devices of the same model were limited, in that we only used two devices, the result shows that it is not always possible to uniquely distinguish devices of the same model based on the radiation pattern. However, it is possible that some models will exhibit larger differences across devices depending on other factors, such as manufacturing techniques and device construction. It is reasonable to expect devices that use an antenna that is part of an integrated circuit board or clamped to the chassis or other internal components would have very little manufacturing variations across devices. But in cases where a flexible wire that is not held into position is used, it is possible that patterns may vary across devices. The Samsung Galaxy A50, for example, uses a wire antenna for WiFi which is somewhat flexible as it is not clamped to the frame or circuitry.

8.4. Pattern Modifications

It is possible to modify a pattern using beamforming or by adjusting the device somehow, for example, adding additional material that will affect the energy distribution from the device. Only a tiny subset of current generation smartphones perform beamforming, so we do not consider this further.

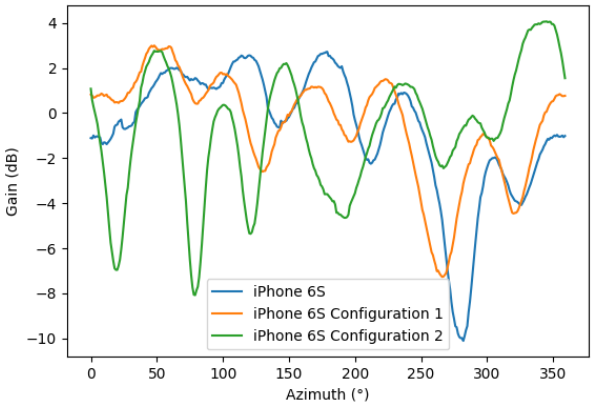


Figure 8. Pattern plots of iPhone 6S. The first without any blockers. The second and third have different configurations of blockers made from foil.

To explore how patterns can be modified we placed multiple layers of aluminium foil in two different configurations around the bottom end of an iPhone 6S. Figure 8 shows the pattern of the phone with different foil blocker configurations versus the unmodified pattern. Due to the complexity of modelling multipath fading effects, we would not expect the result to be as simple as reducing the gain in the direction of the blocker and an increasing gain proportionally in other directions. While noting we do not have the full picture, as the setup only measures power in one axis of rotation, as expected the blockers had some unpredictable effects on the pattern. Although at 180º–which was in the direction of the blocker–the gain was reduced, in other directions the increase is less clear. From 270º to 360º the results show an increase in gain with the blockers, but not by the same ratio and the alignment of peaks and troughs has changed. The other parts of the pattern have changed in an unpredictable way.

8.5. The Environment and Limitations of this Method

As with all schemes that utilise RSS, the environment plays a significant role and although we assume that the environment remains static using a constant E value, this will be affected by moving objects, such as people, doors, and furniture. As already mentioned, temporary changes are dealt with as the process is performed for many packets so the environment should return to its original state for some packets. In the case of long duration changes the site survey can be conducted with multiple states (e.g., with a door open), but the survey cannot be conducted with every possible state due to the state space explosion problem. However, multiple state surveys should be conducted when appropriate. Importantly, the movement of objects will have a limited impact to the RSS measurements in comparison to the pattern of the device which can cause differences of 14+ dBm.The limitation of this work is that in some settings, this assumption that the environment will return to the original site survey state may not apply.

9. SECURITY ANALYSIS

The adversary aims to break the fingerprinting mechanism, such that the system believes a smartphone that is not in $\mathcal{L}$ is a device in $\mathcal{L}$.Although the scheme produces quite a good location and orientation estimate as a by-product, we make no guarantees about those, so this is not considered in this analysis. For an attack to succeed, the attacker must find or produce a pattern that matches n points on a pattern from an allowed model where n is equal to the number of receivers. The angles between the matches in the pattern must correspond to a location in the environment where the angles to the receivers can be replicated. This must be done at multiple

orientations and/or locations so the calculated points meet the pattern coverage requirement for each reference pattern.

9.1. Misclassification Attack

In the simplest form of attack, an attacker would try to orient himself such that his transmissions would be mistaken for transmissions from a valid device. To do this, the attacker must find patterns with similarities and exploit those similarities. Although devices have significantly different patterns, as shown in Figure 7, there are overlaps in the patterns. These overlaps can be found easily, as shown in Figure 9, to make a pattern indistinguishable from another. The number of points of overlap between two patterns is the upper bound for the number of receivers that an attacker can trick the system into thinking one pattern is the other with a single packet. For example, the Samsung A50 and iPhone 6S have up to 12 points of overlap in 2D; in 3D, there would be lines of overlap with the full pattern. The attacker may need to consider the difference in transmission power of the devices, but this would have a limited change on the number of overlaps. Using the total number of points of overlap is the best-case scenario for the attacker and requires the reasonably strong assumption that the attacker has complete control over the angles from the transmitter to the receivers. In practice, an attacker does not control the position of the receivers as these are fixed and thus has limited control over the required angle between matching points on the pattern.

A more realistic approach to consider the attacker's capabilities is to present the attacker with a range of environments with different layouts of receivers and determine if the attacker can create a match with a different pattern at multiple locations that satisfies the required angles to the receivers, with some flexibility (e.g. $\pm$1dBm). As the number of receivers increases, the more difficult it is for an attacker to find patterns that match at the required angles. As expected, for a simulated $\mathcal{A}$ layout, we found that for 2 receivers, 539 combinations of positions and orientations matched for the Samsung A50 and Moto E3, 21 matches for 3 receivers, and 4 & 5 receivers resulted in 0 matches. The number of matches will vary depending on the layout and patterns used. However, critically, this type of attack can be effectively mitigated, as the overlaps can be pre-calculated before system deployment. The receivers can be positioned to prevent possible overlaps of patterns that would otherwise make the scheme susceptible to attacks. First, the angles between matches for allowed and banned patterns need to be calculated. Then a layout of receivers needs to be found that prevents any location within the environment from achieving those angles to the receivers. As more devices are added to the pattern database, the calculations may need to be rerun and receivers potentially moved.

Additionally, although the attacker can match an allowed device, the weakness with this attack is that the system will still recognise the banned device as a strong match. If the system returned the incorrect but allowed device on the first attack attempt, on subsequent checks, it may not. In addition, by forcing the attacker to achieve a high pattern coverage, they must find multiple combinations of points of overlap at the required angles, and the probability of remaining indistinguishable from another pattern reduces as each wedge is covered. The situation is even more hopeless for the attacker if the location of some, or all, of the receivers is unknown.

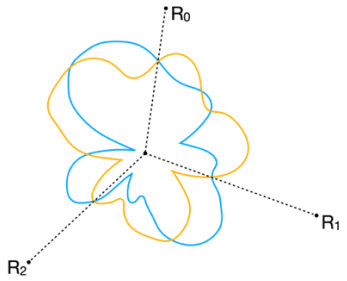


Figure 9. Example of an attacker finding matches that line up with 3 receivers. For a fixed transmission power, the overlap of directivity values will produce the same RSS values at the receivers, making the patterns indistinguishable from the perspective of the receivers.

9.2. Pattern Modification Attack

As described above, carefully crafting a situation where a device is misclassified is very difficult. Even if the attacker happens to succeed once, the attacker's actual pattern is still a strong match. To improve his chances, the attacker could modify his pattern to match an allowed pattern closely. However, as shown in Section 8.4, modifying a pattern by adding external blockers in a controlled way is difficult. This makes modifying a banned pattern to closely match an allowed pattern improbable.

An alternative way for the attacker to improve his chances is, somewhat counterintuitively, to modify the pattern, so that is it very different from any other pattern present in the database. Creating a new unique pattern with some overlap with existing patterns is not difficult. Once the attacker has created a new pattern, he can carry out attacks using the same methods discussed in the first attack. The greater the number of significant peaks and troughs, the easier it is for the attacker to maximise overlaps.

Noting what has already been discussed regarding matching patterns, the probability of successful attacks is reduced if the attacker is forced to find multiple matches at different points on the pattern–the coverage requirement introduced by the coverage metric forces this. Without very similar patterns, the attacker will not find many parts of the pattern that match at the required angles as dictated by the receivers' positions. The number of receivers n and the threshold coverage metric c the operator requires can be adjusted to prevent this attack because the attacker is subject to the following constraints: First, the pattern generated by the attacker must match an allowed device on at least n points simultaneously; Second, the attacker is forced to move to multiple locations or use multiple orientations due to the coverage requirement, i.e., they must find multiple matches. The larger the required c, the more matches they must find.

10. CONCLUSION

In this paper, we have proposed a new method for fingerprinting different models of smartphones using differences in their radiation patterns. We showed how a small set of stationary receivers could measure the radiation pattern of a transmitting device in a completely passive manner. Our novel measurement and pattern recreation method can obtain the radiation pattern of nearby devices and compare them to a database of known device fingerprints. Based on this, the presence of rogue devices can be detected without requiring any special-purpose hardware or collaboration from the devices themselves. Finally, we discussed how the proposed scheme can be configured by adjusting the number of receivers, coverage requirements, and the number of packets between identification checks to mitigate different forms of attacks on the scheme. There

is further scope for future work to explore how different environments affect the performance of the system.

REFERENCES

[1] C. A. Balanis, *Antenna Theory: Analysis and Design*. Hoboken, UNITED STATES: John Wiley & Sons, Incorporated, 2016. [Online]. Available: http://ebookcentral.proquest.com/lib/oxford/detail.action?docID=4205879

[2] G. Baldini and G. Steri, "A Survey of Techniques for the Identification of Mobile Phones Using the Physical Fingerprints of the Built-In Components," *IEEE Communications Surveys Tutorials*, vol. 19, no. 3, pp. 1761–1789, 2017, conference Name: IEEE Communications Surveys Tutorials.

[3] C. Bertoncini, K. Rudd, B. Nousain, and M. Hinders, "Wavelet Fingerprinting of Radio-Frequency Identification (RFID) Tags," *IEEE Transactions on Industrial Electronics*, vol. 59, no. 12, pp. 4843–4850, Dec. 2012, conference Name: IEEE Transactions on Industrial Electronics.

[4] S. Bratus, C. Cornelius, D. Kotz, and D. Peebles, "Active behavioral fingerprinting of wireless devices," in *Proceedings of the first ACM conference on Wireless network security*, ser. WiSec '08. New York, NY, USA: Association for Computing Machinery, Mar. 2008, pp. 56–61. [Online]. Available: https://doi.org/10.1145/1352533.1352543

[5] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp. 116–127, event-place: San Francisco, California, USA. [Online]. Available: http://doi.acm.org/10.1145/1409944.1409959

[6] Y. Chen and J. Yang, "Chapter 8 - Defending Against Identity-Based Attacks in Wireless Networks," in *Handbook on Securing Cyber-Physical Critical Infrastructure*, S. K. Das, K. Kant, and N. Zhang, Eds. Boston: Morgan Kaufmann, Jan. 2012, pp. 191–222. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B978012415815300008X

[7] E. Coca and P. Valentin, "Antenna Radiation Pattern Influence on the Localization Accuracy in Wireless Sensor Networks," *Advances in Electrical and Computer Engineering*, vol. 13, pp. 43–46, May 2013.

[8] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *Proceedings of the 5th ACM workshop on wireless security*, ser. WiSe '06. New York, NY, USA: Association for Computing Machinery, 2006, pp. 43–52, event-place: Los Angeles, California tex.numpages: 10. [Online]. Available: https://doi.org/10.1145/1161289.1161298

[9] J. François, H. Abdelnur, R. State, and O. Festor, "PTF: Passive Temporal Fingerprinting," in *12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011) and Workshops*, May 2011, pp. 289–296, iSSN: 1573-0077.

[10] H. T. Friis, "A Note on a Simple Transmission Formula," *Proceedings of the IRE*, vol. 34, no. 5, pp. 254–256, May 1946.

[11] X. Guo, Z. Zhang, and J. Chang, "Survey of Mobile Device Authentication Methods Based on RF Fingerprint," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Apr. 2019, pp. 1–6.

[12] J. Hall, M. Barbeau, and E. Kranakis, "Detection of Transient in Radio Frequency Finger printing using Signal Phase," *Wireless and Optical Communications*, p. 6, 2003.

[13] J. Hua, H. Sun, Z. Shen, Z.Qian, and S. Zhong, "Accurate and Efficient Wireless Device Fingerprinting Using Channel State Information," in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, Apr. 2018, pp. 1700–1708.

[14] IEEE, "IEEE Standard for Definitions of Terms for Antennas," *IEEE Std 145-2013 (Revision of IEEE Std 145-1993)*, pp. 1–50, Mar. 2014, conference Name: IEEE Std 145-2013 (Revision of IEEE Std 145-1993).

[15] Ke Gao, C. Corbett, and R. Beyah, "A passive approach to wireless device fingerprinting," in *2010 IEEE/IFIP International Conference on Dependable Systems Networks (DSN)*, Jun. 2010, pp. 383–392, iSSN: 2158-3927.

[16] F. J. Liu, X. Wang, and S. L. Primak, "A two dimensional quantization algorithm for CIR-based physical layer authentication," in *2013 IEEE International Conference on Communications (ICC)*, Jun. 2013, pp. 4724–4728, iSSN: 1938-1883.

[17] F.J. Liu, Xianbin Wang, and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *2011 - MILCOM 2011 Military Communications Conference*, Nov. 2011, pp. 538–542, iSSN: 2155-7586.

[18] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of Wireless Indoor Positioning Techniques and Systems," *IEEE Transactions on Systems, Man and Cybernetics, Part C (Applications and Reviews)*, vol. 37, no. 6, pp. 1067–1080, Nov. 2007.

[20] K. Merchant, S. Revay, G. Stantchev, and B. Nousain, "Deep Learning for RF Device Fingerprinting in Cognitive Communication Networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 1, pp. 160–167, Feb. 2018, conference Name: IEEE Journal of Selected Topics in Signal Processing.

[21] M. K. Mwila, K. Djouani, and A. Kurien, "The use of antenna radiation pattern in node localisation algorithms for wireless sensor networks," in *2014 International Wireless Communications and Mobile Computing Conference (IWCMC)*, Aug. 2014, pp. 856–862, iSSN: 2376-6506.

[22] C. Neumann, O. Heen, and S. Onno, "An Empirical Study of Passive 802.11 Device Fingerprinting," in *2012 32nd International Conference on Distributed Computing Systems Workshops*, Jun. 2012, pp. 593–602, iSSN: 2332-5666.

[23] L. Peng, A. Hu, J. Zhang, Y. Jiang, J. Yu, and Y. Yan, "Design of a Hybrid RF Fingerprint Extraction and Device Classification Scheme," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 349–360, Feb. 2019, conference Name: IEEE Internet of Things Journal.

[24] B. Perez, M. Musolesi, and G. Stringhini, "Fatal Attraction: Identifying Mobile Devices Through Electromagnetic Emissions," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '19. New York, NY, USA: ACM, 2019, pp. 163–173, event-place: Miami, Florida. [Online]. Available: http://doi.acm.org/10.1145/3317549.3319726

[25] B. W. Ramsey, B. E. Mullins, M. A. Temple, and M. R. Grimaila, "Wireless Intrusion Detection and Device Fingerprinting through Preamble Manipulation," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 5, pp. 585–596, Sep. 2015.

[26] K. B. Rasmussen and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks," in *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm 2007*, Sep. 2007, pp. 331–340.

[27] S. Y. Seidel and T. S. Rappaport, "914 MHz path loss prediction models for indoor wireless communications in multifloored buildings," *IEEE Transactions on Antennas and Propagation*, vol. 40, no. 2, pp. 207–217, 1992.

[28] P. Xiang, P. Ji, and D. Zhang, "Enhance RSS-Based Indoor Localization Accuracy by Leveraging Environmental Physical Features," Jul. 2018, iSSN: 1530-8669 Library Catalog: www.hindawi.com Pages: e8956757 Publisher: Hindawi Volume: 2018. [Online]. Available: https://www.hindawi.com/journals/wcmc/2018/8956757/

[29] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device Fingerprinting in Wireless Networks: Challenges and Opportunities," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 94–104, 2016, conference Name: IEEE Communications Surveys Tutorials.

© 2021 By AIRCC Publishing Corporation. This article is published under the Creative Commons Attribution (CC BY) license.