A Novel Method for Physical-Layer Authentication via Channel State Information

Scott Lord and John Roth
Dept. of Electrical and Computer Engineering
Naval Postgraduate School
Monterey, CA, USA
sflord, jdroth@nps.edu

John McEachen and Murali Tummala
Dept. of Electrical and Computer Engineering
Naval Postgraduate School
Monterey, CA, USA
mceachen, mtummala@nps.edu

Abstract—The channel response between a wireless transmitter node and a receiver node changes as the nodes move and the environment changes. Recent studies have suggested several approaches to leverage such changes in channel response to enable authentication of a communication node’s reported location by comparing measured transmission channel characteristics to those expected for emissions from the reported location. This work focuses on how a specular reflecting plane can be estimated from the multipath time delay measurements over multiple transmitter positions presenting theoretical limits to estimating such a reflecting plane. Additionally, we provide a brief example to illustrate the value such a reflecting plane can bring in regards to authenticating a transmission’s claimed position of origin.

Index Terms—Physical-layer security, authentication, single bounce refraction, optimization algorithm, multipath

I. INTRODUCTION

A broad spectrum of security vulnerabilities have been proposed and cataloged as devices have become more interconnected. The vulnerabilities present themselves in every layer of the Open Systems Interconnected (OSI) Model from the application layer to the physical layer. As new communication technologies are introduced, additional previously infeasible security vulnerabilities often present themselves. In an effort to address not only the recognized security vulnerabilities but also potential new vulnerabilities, several papers have been recently published from a security focused perspective on the broad spectrum of physical-layer security approaches. For our purposes, we will focus on authentication; however, [2] provides an excellent survey of key-based cryptographic security use in 3G and LTE networks.

Beyond identifying and characterizing the various security vulnerabilities, multiple solutions may be appropriate for any particular vulnerability. Different mitigation approaches yield various advantages and disadvantages depending on the needs of the system, and so a range of security approaches for a single vulnerability may be appropriate. We propose that one such security feature is the ability to verify the reported location of a communication node via physical layer attributes.

To motivate the value of such a security feature consider the standard authentication problem. Two entities, typically labeled “Alice” and “Bob,” conduct a communication where Alice sends a message to Bob. To achieve authentication of Alice’s message Bob has to determine if the received message is actually from Alice vice some other masquerading entity, typically labeled “Eve”. Bob must leverage some information regarding the message to ascertain whether the message is legitimately from Alice.

A common approach for Bob to authenticate Alice is via cryptographic techniques. Typically, a shared secret is established between Bob and Alice which Alice uses to generate a digital signature via an enciphering algorithm. Bob then deciphers the digital signature to verify it matches an expected result to authenticate the message is from Alice. Such cryptography-based security schemes have been leveraged in many different capacities to great effect; [5] provides a robust description of key-based security use in 3G and LTE networks. However, there are some challenges inherent to their use:

- Unique key sets are required between each pair of nodes for each communication session. For LTE security 11 unique keys are generated for each session between a mobile terminal and a base station [5].
- Latency required for key processing may be prohibitive for certain applications.
- It remains mathematically unproven that the cryptography cannot be computationally broken [6].
- Cryptographic techniques typically operate on data at levels above the physical layer in the OSI Model. If an attacker is able to obtain an unauthorized security key; the system cannot easily detect the security violation when the physical-layer attributes are disregarded [7].

Given the need for flexible security schemes and the challenges inherent to key-based cryptographic security schemes, substantial research has gone into physical-layer security. Physical-layer security can be summarized as security techniques which leverage phenomena inherent to the physical medium through which information is being transmitted to achieve various security needs. For our purposes, we will focus on authentication; however, [2] provides an excellent survey on the broad spectrum of physical-layer security approaches. Regarding physical-layer authentication in our example with Alice and Bob, Bob must leverage some feature about the received message which can identify Alice and is difficult for Eve to imitate. Several techniques to achieve this goal have
been proposed which fall into the following categories:

- Leverage the random nature of the channel response between two communication nodes and the phenomena that the channel response is often reciprocal between two nodes to generate a shared secret seed from which typical cryptographic keys are generated [8].
- Leverage previously captured radio frequency (RF) fingerprint-like characteristics of a particular transmitter to identify if a current transmission originated from that same transmitter because it exhibits a similar RF fingerprint [9].
- Leverage recent channel response measurements to identify if the current channel response has changed too drastically to be the same identity as previously verified [10].

Our proposed approach falls into the last category. By leveraging transmission channel characteristics that strongly depend on the relative geometry between a mobile communication node and a fixed node, we propose that a map of planar specular reflectors can be generated for various operating regions of mobile node positions. After the map of planar reflectors has been generated, subsequent communications received by the fixed node can be assessed to verify the anticipated channel features caused by the mapped planar reflectors are present for the reported location of the mobile node.

Our contributions are two-fold. First, based on a survey of recent work in physical layer authentication, we propose a framework to separate authentication features into channel-based features and transmitter-based features. Furthermore, we propose the channel-based features be reduced to fundamental channel-model parameters in order to enable better review of a scheme’s applicability to a new environment. Our second contribution is a proposed methodology and analysis of its theoretical estimation limits to transform the channel state information (CSI) regarding select multi-path delays over multiple transmitter positions into regionally defined reflecting planes.

The organization of this paper is as follows: We summarize recent channel-based authentication publications highlighting the challenge of considering their application to new environments. We present an argument for transforming the variety of proposed physical-layer authentication features to their constituent physical model components where possible. We follow with our proposed mapping scheme to transform measured channel features into planar specular reflectors. We present the theoretical limits of estimating such reflecting planes. Finally, we provide a brief example at how such reflecting planes can be leveraged to verify the claimed position of transmission.

II. CHANNEL-BASED AUTHENTICATION

Of the three general implementation strategies to achieve physical authentication listed in the introduction, we will focus on recent work regarding physical authentication which leverages various forms of CSI. Regarding approaches which use an RF fingerprint for physical authentication we refer the reader to [9] for insights into the basic limits of such an approach. Regarding approaches which generate secret keys leveraging the CSI as a shared secret seed, we refer the reader to [8] for insights into the practical limits of such an approach.

The premise of physical authentication based on CSI depends on two fundamental features, differentiation and continuity. For differentiation, the information regarding the transmission channel from Alice to Bob, CSI-AB, is different than the information regarding the channel from Eve to Bob, CSI-EB. For continuity, CSI-AB is in some way related from one transmission to the next. Without differentiation it would not be feasible to tell Alice from Eve, and without continuity it would not be feasible to tell if a new transmission was still from Alice. For differentiation, Jake's uniform scattering model [11] predicts that the correlation of a received signal envelope will rapidly diminish when Alice and Eve are physically separated by a distance of at least half the carrier wavelength. And for continuity, several works in channel estimation confirm that there are channel features which vary slowly from one data symbol to the next such as multipath time delay and angle of arrival (AoA) [12]–[14].

As both foundational features for CSI-based physical authentication have been observed in wireless transmission environments, several physical authentication schemes have been proposed and explored. Typically, an authentication scheme is proposed which leverages CSI and often some other additional measure(s) of the transmission. For example, [10] explored a system based on the frequency response of the transmission channel and a temporal variance measurement predetermined from environmental modeling. Another approach proposed in [15] is based on the received power spectral density (PSD) of a signal. An approach based on received signal strength (RSS) was developed and evaluated by [16], and a physical authentication scheme leveraging the channel impulse response and the measured signal-to-noise ratio (SNR) was considered by [17]. Finally, a physical authentication scheme based on RSS, time of arrival (TOA), and a measure of the correlation of cyclic features in the received signal was proposed and simulated by [18]. With such a variety of features already proposed, [7] proposed a multi-attribute multi-observation (MAMO) approach where as many of the physical-layer attributes as possible are leveraged to achieve the authentication goal. However, engineering constraints typically limit which data can be made available and how much processing can performed. As such, it is valuable to be able to reduce the various measures of physical layer phenomena down to a minimal set of irreducible features. Such a reduction not only reduces data and processing needs, it also creates a framework by which different authentication schemes can be more easily compared and their applicability better predicted.

We propose that for the purposes of wireless physical-layer authentication, the minimal set of irreducible features to describe the channel should be the parameters defining each resolvable multipath component of a received signal assuming a specular reflecting model for the environment. Those features are derived from the frequency-domain parametric channel
The response yielded due to the sum of $P$ and a non-LOS (NLOS) path bouncing off a building $p$ has 2 paths to traverse: a direct line of sight (LOS) path and a non-LOS (NLOS) path bouncing off a building $p_1$. Figure 1 depicts an example where the transmission can traverse and still have significant energy upon reaching the receiver. This model is motivated by the concept of specular reflectors in the environment creating multiple paths which the transmission can traverse and still have significant energy upon reaching the receiver. Figure 1 depicts an example where the transmission has 2 paths to traverse: a direct line of sight (LOS) path $p_0$ and a non-LOS (NLOS) path bouncing off a building $p_1$.

By condensing the CSI down to a set of environmental features, we argue that it is simpler to evaluate how applicable a proposed physical-layer authentication scheme is for a new environment. Instead of considering the mathematical abstraction of complex gains at various frequencies $H(t, f)$, we believe it is more intuitive to consider how the transmission channel is composed of multiple physical paths where each path consists of a gain $|\alpha_p|$, a phase offset $\angle \alpha_p$, an AoA $\Theta_{R_p}$, an AoD $\Theta_{T_p}$, a time delay $\tau_p$, and a Doppler shift $\nu_p$. Furthermore, if those paths can be associated with physical structures in the environment such as floors and walls upon which the transmission is reflecting then it becomes quite intuitive to consider how a proposed physical authentication scheme will behave in a new environment. The challenge becomes estimating the various parameters of each multipath component and determining which structures in the environment are creating which multipath components.

Fortunately, there has been substantial work in channel estimation techniques to estimate the parameters of the various multipath components from 1. To highlight some of the more popular techniques we refer the reader to [19], [20] for approaches leveraging algorithms dubbed ESPRIT and MUSIC, and we refer the reader to [13] for a technique dubbed compressed channel sensing. To inform our error models in section IV we will use the results from [12] which presented an approach that estimated multipath components via ESPRIT and subsequently refined the estimate for each multipath component via delay locked loop tracking. We leveraged the results of [12] because their tracking approach to each multipath component naturally lends itself to our proposed approach to identifying which environmental structures are causing a particular multipath component and because their delayed lock loop approach yielded rather precise estimation of the $\tau_p$ parameter which we focus on for identifying planar reflectors in the environment.

One last aspect we highlight about converting CSI to the form of 1 is that it separates the CSI into features which vary due to different phenomena. For example, the parameter $|\alpha_p|$ represents the strength of a particular multipath component, and it is affected by phenomena such as the distance of the path traveled and the reflectivity of surfaces off which it bounced. The parameter $\tau_p$ on the other hand is only affected by the distance of the path traveled, and it is not significantly affected by the reflectivity of encountered surfaces. The Doppler shift encountered along each path $\nu_p$ is due to the path length changing over the transmission duration, and thus it is affected by relative motion between the transmitter, receiver, or scattering surface. The AoA $\Theta_{R_p}$ and AoD $\Theta_{T_p}$ depend on the orientation of the transmitter and receiver and the geometry of scatterers in the environment. And finally the phase offset of each multipath component $\angle \alpha_p$ depends on factors such as the phase of the transmitter upconverter, the phase of the receiver downconverter, and phase changes due to interactions with scatterers in flight.

Because the parameters depend on different phenomena, some parameters may perform better in regards to the authentication needs of differentiation and continuity. In particular, we note that the phase offset of each multipath component $\angle \alpha_p$ varies so unpredictably that it is typically modeled as a uniform random variable in the range $[0, 2\pi)$. We highlight this because as such it provides essentially no information to Bob regarding Alice. While it is rather unlikely that Eve and Alice would have the same $\angle \alpha_p$, indicating the potential for differentiation, we argue $\angle \alpha_p$ varies so much that it does not exhibit useful continuity for Bob to assess whether the next transmission is still from Alice. Other features provide such continuity such as $|\alpha_p|$ and $\tau_p$, but the unpredictable nature of $\angle \alpha_p$ causes it to act as essentially white noise in regards to information about Alice. This is significant because many of the proposed physical-layer authentication schemes in the literature leverage at least one feature which strongly depends on $\angle \alpha_p$ from each multipath component. Features such as $H(t, f)$, RSS, and PSD can all be rather strongly affected by $\angle \alpha_p$ simply because a significant multipath component can be completely out of phase with the other multipath components.

\[ H(t, f) = \sum_{p=0}^{P-1} \alpha_p a_R(\Theta_{R_p}) a_T(\Theta_{T_p}) e^{-j2\pi f \tau_p e^{j2\pi \nu_p t}} \]
destructively interfering and significantly reducing the overall gain at a particular frequency. Thus, the unpredictable nature of $\alpha_p$ manifests as unpredictable changes in each feature dependent on $\alpha_p$ similar to noise.

To conclude, there is significant value in converting the various features proposed for channel based physical authentication into the multipath parameters of $\mathbf{I}$. By converting to a common feature set, it is easier to compare different physical authentication schemes against each other. Also, because the features of $\mathbf{I}$ correspond to physical structures in the environment, it is easier to assess the applicability of a physical layer authentication scheme to a new environment. And finally, by separating the CSI into its constituent multipath components, the various phenomena which affect each parameter can be more aptly leveraged for the authentication of Alice.

III. ESTIMATING A SPECULAR REFLECTOR LOCATION AND ORIENTATION

We now shift to the previously mentioned challenge of determining which structures in the environment are causing the various multipath components of $\mathbf{I}$. We propose that a map of stationary planar specular reflecting surfaces can be resolved through a processing sequence that uses the delay parameter $\tau_p$ and position data of the transmitter over a variety positions with a fixed receiver position. We pursue mapping large persistent planar reflectors because such planes are rather common in most environments (i.e. walls and floors) and because such large surfaces tend to be stable and persistent over time (i.e. the floor does not typically move). This allows for the authentication scheme to continue to function even when potential changes to the environment occur; if Bob only uses the anticipated features from the large surfaces that should not change over time, then new environmental scatterers causing additional multipath features would simply be ignored. The challenge we anticipate arising in such cases is the potential for scatterers to occlude the anticipated multipath component from the apriori mapped reflector; however, for the purposes of this paper, we are going to focus on the ability to identify and map such reflectors. It is our intention to consider how occluding scatterers as well as the quantity and orientation of mapped planar reflectors affect Bob’s authentication decision in subsequent work.

A. Noiseless Estimation

The methodology we propose to generate a map of such specular reflectors is an optimization scheme where a planar reflector is estimated which would yield time delays closest to those measured for a set of known transmitter locations assuming standard ray propagation. Leveraging such an optimization scheme we ensure we only map surfaces that consistently reflect detectable energy over a variety of geometries. Also, such a mapping technique assists the case where a particular transmitter position has several propagation paths that are all rather weak gain paths but have identical time delays and thus constructively add to create the effect of a single high gain transmission path. The time delays of each of those weak paths lose alignment as the transmitter moves and thus their effect of a singular high gain path is lost, and the optimization scheme will not be able to resolve a plane as inadequate energy detection will occur over too many of the geometries. As such, spurious planar reflectors are not mapped as resolvable time delays do not persist over a broad enough range of transmitter positions.

We consider a simple case with only a single plane of reflection to be estimated and a fixed receiver position. The plane is defined by 4 parameters in Cartesian coordinates: the $x$, $y$, and $z$ components of the planes unit magnitude normal vector $\mathbf{n} = [x_n, y_n, z_n]^T$ as well as the height of the receiver from the plane $h_{Rx}$. Note, that for a fixed receiver location and fixed reflecting plane position and orientation, $h_{Rx}$ fixes the $x$, $y$, and $z$ coordinates of a point in the reflecting plane $\mathbf{P}_n$ such that

$$\mathbf{P}_n = \mathbf{P}_{Rx} - h_{Rx}\mathbf{n}$$

where $\mathbf{P}_{Rx}$ is the receiver location $\mathbf{P}_{Rx} = [x_{Rx}, y_{Rx}, z_{Rx}]^T$. To estimate the plane parameters our mapping process leverages measurements from $N$ mobile transmitter positions $\mathbf{P}_{Tx_i} = [x_{Tx_i}, y_{Tx_i}, z_{Tx_i}]^T$ and the time delay of the NLOS path relative to the LOS path $\tau_i = \tau_{iNLOS} - \tau_{iLOS}$ for each of the $N$ geometries. The $i^{th}$ geometry is the defined by $\mathbf{P}_{Rx}$, $\mathbf{P}_{Tx_i}$, $\mathbf{n}$, and $h_{Rx}$.

Initially, we consider a case where there is no noise in our measurements and there is only a single geometry of measurements: $\mathbf{P}_{Rx}$, $\mathbf{P}_{Tx_0}$, and $\tau_0$. For the case of only this single geometry, there are many different plane positions and orientations that are possible which would produce the measured time delay $\tau_0$. Geometrically, the possible locations for the point of reflection $\mathbf{P}_R = [x_R, y_R, z_R]^T$ form an ellipsoid defined by the following

$$|\mathbf{P}_R - \mathbf{P}_{Rx}| + |\mathbf{P}_R - \mathbf{P}_{Tx_0}| - |\mathbf{P}_{Rx} - \mathbf{P}_{Tx_0}| = c\tau_0$$

where $c$ is the speed of light, $|\mathbf{P}_R - \mathbf{P}_{Tx_0}|$ is the distance from the transmitter to the point of reflection, $|\mathbf{P}_R - \mathbf{P}_{Rx}|$ is the distance from the receiver to the point of reflection, and $|\mathbf{P}_{Tx_0} - \mathbf{P}_{Rx}|$ is the distance from the transmitter to the receiver. Each distance can be described mathematically from the Pythagorean equation. For example, $|\mathbf{P}_R - \mathbf{P}_{Rx}| = \sqrt{(x_R - x_{Rx})^2 + (y_R - y_{Rx})^2 + (z_R - z_{Rx})^2}$ is the distance from $\mathbf{P}_R$ to $\mathbf{P}_{Rx}$.

With only the delay from the geometry of a single transmitter position measured, the reflecting plane could be any plane tangent to the ellipsoid of (3). More measurements in different geometries are required to resolve the specular reflecting plane. For those additional measurements, we assume the specular reflector plane is unmoving throughout the $N$ geometries and that a ray model describes the the behavior of the path traversed by the specularly reflected transmission component. As such the direction of the reflected component upon reflecting off the specular reflecting plane is

$$\frac{\mathbf{b}}{|\mathbf{b}|} = \frac{\mathbf{a}}{|\mathbf{a}|} - 2\left(\frac{\mathbf{a}}{|\mathbf{a}|} \cdot \mathbf{n}\right)\mathbf{n}$$

where $|\mathbf{a}|$, $|\mathbf{b}|$, and $\mathbf{n}$ are the length of the vector $\mathbf{a}$, the length of the vector $\mathbf{b}$, and the unit normal vector respectively.
where \( \mathbf{b} \) is the vector to the receiver from the point of reflection \( \mathbf{b} = \mathbf{R}_x - \mathbf{R} \), \( \mathbf{a} \) is the vector to the point of reflection from the transmitter \( \mathbf{a} = \mathbf{R} - \mathbf{T}_{x_0} \), \( \mathbf{n} \) is the normal vector of the reflecting plane with unit magnitude, and \( \cdot \) is the dot product operator.

Leveraging (4), the point of reflection for each geometry \( \mathbf{P}_{R_i} \) can be represented as a function of the transmitter position, receiver position, and reflecting plane parameters

\[
\mathbf{P}_{R_i} = \frac{(h_{Tx_i} \mathbf{CA}_{Rx} + h_{Rx} \mathbf{CA}_{Tx_i})}{h_{Tx_i} + h_{Rx}}
\]

(5)

where for the \( i^{th} \) geometry \( h_{Tx_i} = (\mathbf{P}_{Tx_i} - \mathbf{n}) \cdot \mathbf{n} \) is the distance from the transmitter to the closest point of approach (CPA) in the reflecting plane, \( \mathbf{CPA}_{Tx_i} = \mathbf{P}_{Tx_i} - h_{Tx_i} \mathbf{n} \) is the point in the reflecting plane at the CPA to the transmitter, and \( \mathbf{CPA}_{Rx} = \mathbf{P}_{Rx} - h_{Rx} \mathbf{n} \) is the point in the reflecting plane at CPA to the receiver.

By substituting (5) into (3), the mathematical model can be manipulated into the following form

\[
Q(\mathbf{P}_{Tx_i}, \mathbf{P}_{Rx}, \mathbf{n}, h_{Rx}) = \tau_{i,1}
\]

(6)

where \( Q(\mathbf{P}_{Tx_i}, \mathbf{P}_{Rx}, \mathbf{n}, h_{Rx}) = \frac{1}{\tau_i} |\mathbf{P}_{Rx} - \mathbf{P}_{Tx_i} - \frac{1}{\tau_i} |\mathbf{P}_{Rx} - \mathbf{P}_{Tx_i}|. \) Note that \( Q \) is a unique function for each geometry of the form

\[
Q(\mathbf{P}_{Tx_i}, \mathbf{P}_{Rx}, \mathbf{n}, h_{Rx}) = \sqrt{P^6(\mathbf{P}_{Tx_i}, \mathbf{P}_{Rx}, \mathbf{n}, h_{Rx}) + P^4(\mathbf{P}_{Tx_i}, \mathbf{P}_{Rx}, \mathbf{n}, h_{Rx})} - \sqrt{P^2(\mathbf{P}_{Tx_i}, \mathbf{P}_{Rx})}
\]

(7)

where \( P^i(\ldots) \) represents a multivariate polynomial of degree \( i \). It is also worth noting that of the two degree-6 polynomials of (7) only the unit-less normal vector components \( (x_n, y_n, z_n) \) are degree-6 while the various position components \( (x_{Rz}, x_{Tx_i}, x_{Pz}, y_{Rx}, \ldots, z_{Pn}) \) which have units of distance are degree-4. Additionally, in the degree-4 polynomials of (7) only the normal vector components are degree-4 while the position components are degree-2.

Despite the complexity of (7), it is a continuous differentiable multi-variate function. Furthermore, we have assumed that the reflecting plane and receiver position are constant across all \( N \) geometries. Thus, to simplify notation we denote

\[
Q_i(\Theta) = Q(\mathbf{P}_{Tx_i}, \mathbf{P}_{Rx}, \mathbf{n}, h_{Rx})
\]

(8)

where \( \Theta = [x_n, y_n, z_n, h_{Tx_i}]^T \) and the \( i \) subscript indicates unique coefficients exist for the polynomials of \( Q_i \) due to the unique transmitter position of the \( i^{th} \) geometry.

Because \( Q_i(\Theta) = \tau_i \) for each geometry, an optimization approach is feasible to resolve \( \Theta \). Our approach is to minimize the sum of squared errors across all \( N \) geometries with the constraint that the worst case error is within some threshold \( \epsilon_{max} \). The error of the \( i^{th} \) geometry is defined as

\[
\epsilon_i = \hat{\tau}_i - Q_i(\Theta)
\]

(9)

where \( \hat{\tau}_i \) is the measured time delay for the \( i^{th} \) geometry. The goal of the optimization is to find

\[
\arg\min_{\Theta} \sum_{i=0}^{N-1} \epsilon_i^2, \quad s.t. \quad n \cdot n = 1, \quad \epsilon_i \leq \epsilon_{max}, \quad h_{Rx} > 0, \quad h_{Tx_i} > 0; \quad 0 \leq i \leq N - 1
\]

(10)

satisfying all \( N \) geometries. Essentially, the optimization problem is finding the parameters for a reflecting plane which yields time delays closest to those observed for each transmitter position not to exceed a selected threshold \( \epsilon_{max} \). The condition \( h_{Rx} > 0 \) and \( h_{Tx_i} > 0 \) is due to our definition where they represent the distance to the reflecting plane. If the reflecting plane is above the receiver position for a given perspective, \( n \) will be oriented such that it points away from the reflecting plane towards the side of the reflecting plane to which both the receiver and transmitter are positioned.

Leveraging (10) we produced the results displayed in Figure 2 which illustrates the receiver position as a blue star, the various transmitter positions for each geometry as red circles, the theoretical reflection points for each geometry off of the \( xy \)-plane as yellow triangles, and the estimated reflection plane from the optimization as purple x’s. It should be noted that even with perfect theoretical measurements \( \hat{\tau}_i = \tau_i \) for each geometry the optimization computation does not yield a perfect result for the reflecting plane. This is a result of different configuration settings of the optimization algorithm. For example, the geometries in Figure 2 yielded a perfect result for the reflecting plane. This is a result of the theoretical \( \Theta \) was such that \( n = [0, 0, 1]^T \) and \( h_{Rx} = 5 \).
Our intent is not to examine the various configuration settings and their effects on the proposed optimization results, but rather our goal is demonstrate that despite the non-linear nature of the error function $e_i$ a resolvable solution can be computed with relatively few geometries in the absence of noise. We do highlight that the geometries of the transmitter positions should not all be co-planar with the receiver position, otherwise, multiple planes may be possible which would yield exactly the same $\tau_i$ values. To best illustrate this, consider the case where the reflecting plane is the $xy$-plane as in Figure 2. If all transmitter positions were the same height from the $xy$-plane as the receiver and thus co-planar, a plane parallel to the $xy$-plane but at a height of twice the transmitter height, $h_{Tx} = 2z_{Tx}$, would yield the same time delays as those bouncing off the $xy$-plane for every receiver position. In other words, if all $N$ transmitter positions were the same height from the ground plane, a ceiling plane could exist that would yield the same time delays. From a geometric perspective, an ellipsoid of possible reflection points exists for each of the $N$ transmitter positions and associated time delays. Our proposed optimization scheme finds a plane tangent to all $N$ ellipsoids, and if the geometries are such that there are multiple planes which are tangent to all $N$ ellipsoids, ambiguous solutions may result from the computation.

B. Noisy Estimation

Next we introduce noise to the measurement of $\tau_i$ and analyze its effects on the optimization computation. We assume independent identically distributed, i.i.d., additive Gaussian noise $Z \sim \mathcal{N}(0, \sigma^2_z)$ is present in each measurement, $\hat{\tau}_i = \tau_i + z_i$. To discuss the influence of noise on the optimization computation it is insightful to consider the function for calculating $\tau_i$ for a given geometry from (7). We highlight the components of $n$ are the highest degree variables at degree-6, and thus $\tau_i$ can be quite sensitive to the orientation of the reflecting plane especially when $h_{Tx_i}$ is the same order of magnitude as $h_{Rx_i}$. However, if the transmitter is much further from the reflecting plane than the receiver $h_{Rx_i} \gg h_{Tx_i}$ analysis of (5) indicates the point of reflection is well approximated as the CPA of the receiver $P_{Rx_i} \approx \text{CPA}_{Rx_i}$, and $\tau_i$ is dominated by $\text{CPA}_{Rx_i}$. Additionally, if instead the receiver is much further from the reflection plane than the transmitter $h_{Rx_i} \gg h_{Tx_i}$, then $P_{Rx_i} \approx \text{CPA}_{Tx_i}$, and $\tau_i$ is dominated by $\text{CPA}_{Tx_i}$.

Beyond the insights into the general dependence of $\tau_i$ on the above mentioned geometry, as mentioned earlier (7) is a continuous differentiable function. This provides a means to evaluate the Cramer Rao Lower Bound (CRLB) for estimating $\Theta$ from $N$ delay measurements $\hat{\tau} = [\tau_0, \tau_1, \ldots, \tau_N]^T$, $N$ transmitter positions $P_{Tx} = [P_{Tx_0}, P_{Tx_1}, \ldots, P_{Tx_N}]$, and the receiver position $P_{Rx}$. The probability density function (pdf) for $\hat{\tau}$ given $\Theta$, $P_{Tx}$, and $P_{Rx}$ is

$$p(\hat{\tau}; \Theta, P_{Tx}, P_{Rx}) = \prod_{i=0}^{N-1} \frac{1}{\sqrt{2\pi \sigma_{\tau}^2}} e^{-\frac{(\tau_i - Q_i(\Theta))^2}{2\sigma_{\tau}^2}}$$

(11)

due to the i.i.d. nature of $z_i$, and in Appendix A we show that “regularity” conditions are met. As such, the CRLB states that the minimum covariance of any unbiased estimator of $\Theta$ is bounded by the inverse of the Fisher Information Matrix $I(\Theta)$ which has the following element-wise definition

$$[I(\Theta)]_{j,k} = -E \left[ \frac{\partial^2}{\partial \Theta_j \partial \Theta_k} \ln(p) \right]$$

(12)

where $\Theta_i$ is the $i^{th}$ parameter of $\Theta$. In Appendix A we derive $I(\Theta)$ as the following

$$[I(\Theta)]_{j,k} = \frac{1}{\sigma^2_\tau} \sum_{i=0}^{N-1} \frac{\partial Q_i(\Theta)}{\partial \Theta_j} \frac{\partial Q_i(\Theta)}{\partial \Theta_k}$$

(13)

where $[I(\Theta)]_{j,k}$ represents the element of the $I(\Theta)$ matrix at the $j^{th}$ row and $k^{th}$ column. From 13 we note that each entry in $I(\Theta)$ is a sum of $N$ unique functions of $\Theta$. Each of the unique partial derivatives is of the following form

$$\frac{\partial Q_i(\Theta)}{\partial \Theta_j} = (P_i^6(\ldots) P_i^{10}(\ldots))^{-1/2} P_i^{10}(\ldots)$$

(14)

yielding large degree polynomials for each entry of $I(\Theta)$. As such, it quickly becomes untenable to calculate the inverse of $I(\Theta)$ symbolically even with computational methods. However, it is feasible to evaluate $I(\Theta)$ numerically under conditions which are likely to represent the intended environment of use which we present in the following section.

IV. SIMULATION

We present conditions where the planar reflector is assumed to be the ground with the receiver at an elevated position of 25 m and the transmitter locations are close to the reflecting plane at heights between 1 m and 3 m as they traverse a 5 m by 5 m area. We select the initial 8 transmitter locations as the corners of the rectangular prism containing the possible transmitter locations. Subsequent transmitter locations are added by randomly selecting any point in the rectangular prism via a uniform distribution. In Figure 3 we illustrate such conditions.

Constrained to the geometry of Figure 3 we simulated our proposed optimization scheme 800 times for various subsets of transmitter positions. The minimum number of transmitter positions used was 8 and the maximum number of transmitter positions was 408. The noise introduced to the reflecting path was the noise positions was 408. The noise introduced to the reflecting path
delay measurement was Gaussian zero mean i.i.d. noise with \( \sigma_t = 2 \text{ nsec} \) for all simulations, and the reflecting plane being estimated was the \( xy \)-plane, \( n = [0, 0, 1]^T \); \( h_{Rx} = 25 \text{ m} \). For the optimization algorithm, we constrained \( |\epsilon_i| < 7\sigma_t \) and we uniformly varied the initial guess of the optimization algorithm with the following bounds: \( |n_x| \leq 0.2, |n_y| \leq 0.2, n_z \geq 0.6 \), \( h_{Rx} = h_{\text{max}} \) where \( h_{\text{max}} \) is the maximum possible height of the receiver based on the transmitter positions and their time delays, \( h_{\text{max}} = \max \{ |\mathbf{P}_{Rx} - \mathbf{P}_{Tx_i}| + \tau_i/2 \} \). Our intention with such a simulation is to imitate a setting where an access point has an elevated field of view of a region with mobile traffic in which occasional mobile users provide high accuracy geo-location data as they progress through the region. Our goal is to resolve the reflecting ground plane of the region from the time delay measurements of the mobile users.

The mean of each estimated parameter from the optimization scheme is displayed in Figure 4 with error bars representing the standard deviation of the results across all simulations. One can see from the sizable error bars that for a single optimization output, the result is prone to error. However, over many repetitions with unique noise insertion, a reasonable estimate of the reflecting plane is established. Of note, increasing the number of geometries included in the optimization does not appear to improve the estimation. We conclude that the estimation does not improve with more geometries due to the algorithmic challenge of meeting the constraints described by (10). The constraint that the error for each delay measurement \( \epsilon_i \) must be within a strict tolerance causes the optimization result to occasionally fail, meaning it yields a normal plane which fails to meet the constraints of (10). In such cases, our approach was to restart the optimization algorithm up to 2 times with a different initial guess randomly selected with the same first guess constraints. Our conclusion for such behavior is that the initial guess of the optimizer would cause the algorithm to progress to a potential solution region that was isolated from regions which actually met the problem constraints. The gradient descent approach of the optimizing algorithm would not be able to leave the isolated region yielding an estimate which did not meet the constraints. For cases when the constraints were met, this also explains the mediocre performance of the optimizer when adding more geometries. Adding more geometries principally just created more isolated regions where the optimizer would become trapped and produce an estimate with error similar to the fewer geometry cases. Such optimizer results indicate there are potential improvements to be made in the application of the optimizing algorithm. However, our current intention is to demonstrate the feasibility of such a mapping scheme.

In regards to the best possible performance of an optimizing algorithm to estimate the reflecting plane, we present the CRLB as a function of each added transmitter location in Figure 5. One can see that our intuition of the reflecting plane estimation improving with more geometries is supported theoretically for an optimal estimator. More geometries provide a better theoretical limit for estimating the normal plane. Of note, the slightly jagged nature of the CRLB at fewer geometries (< 150) is due to the method new transmitter positions were selected. By randomly selecting each new transmitter position constrained to the 5 m x 5m x 2m region bounded by the 8 initial transmitter positions, occasionally a position would be selected which did not significantly improve the CRLB. For example, selecting a position close to a position already chosen typically does not improve the CRLB as much as selecting a position distant from previous positions. However, once enough positions have been randomly selected that the region is effectively saturated geometrically, the rate at which the CRLB decreases becomes quite slow as indicated by the meager difference between the CRLB at 200 geometries and the CRLB at 400 geometries.
While our optimization implementation did not achieve the CRLB, it did demonstrate that a reasonable estimate of a reflecting plane could be generated for a receiver collecting nothing more than various transmitter positions and multipath delay measures. The noise we simulated created error in the delay measurements substantially higher than the delay error reported in channel estimation schemes focused on multipath delay estimation. We simulated $\sigma_\tau = 2 \text{ nsec}$ while [12] reported a standard deviation in delay error of $\sigma_\tau = 0.8 \text{ nsec}$ indicating that our assumptions for delay estimation are achievable. Finally, the geometric constraints of a 5 m x 5 m x 2m sampling region are conservative in our estimation as it seems quite plausible to establish a similar collection scenario over a much larger region.

As such, we conclude that an estimation scheme for planar specular reflectors is achievable leveraging position data and channel estimation data. We propose that mapping such planar specular reflectors has direct value in regards to the capacity to authenticate the reported location of a transmitter, recognizing there may additional value beyond authentication purposes. Furthermore, we acknowledge that theoretical limits of the CRLB indicate there are improvements to be achieved regarding our optimization algorithm implementation.

V. Value for Authentication

In this work we focused on the estimation theory limits for mapping a reflecting plane which could be subsequently used for authentication purposes. We have not completed a rigorous analysis of how valuable such mapped reflecting planes are in regards to verifying Alice’s claimed position. However, to illustrate the potential of leveraging the mapped reflecting plane for authentication purposes, we have included a simple example. In the example we maintain the $xy$-plane as the only reflecting plane in the environment but now consider the transmitter positions which had been used for mapping as the claimed positions of Alice (a 5x5x2 m box). We add additional transmitter positions in an elevated position to represent potential Eve positions $P_{Eve}$ from which Eve could attempt to impersonate Alice. For the example, we chose Eve positions in a (1x1x1 m) box centered at $(9.5, 3, 15.5)$.

The positions are displayed in Figure 6, and though partially occluded by the transmitter positions representing Alice $P_{Tx}$, one can see the points of reflection for the Eve positions $P_{R_{Eve}}$ overlap with the Alice points of reflection $P_{R_i}$. We subsequently illustrate in Figure 7 the histogram of time delays $\tau_i$ that would occur from the mapping transmitter positions $P_{Tx}$, overlaid with the histogram of time delays $\tau_i$ that would occur from the chosen Eve positions $P_{Eve}$. For the example geometry it is quite apparent that the multipath delays caused from the Eve positions away from the reflecting plane produce a distinguishable feature that can be leveraged to identify Eve is not transmitting from a position near the reflecting plane. For such a geometry, delay resolution as coarse as 25 nsec appears to be adequate to separate Eve’s position from Alice’s position.

![Fig. 6. Example case where Eve attempts to claim she is transmitting from the transmitter locations near the reflecting plane while actually positioned 15 m to 16 m above the reflecting plane.](image)

![Fig. 7. Histogram of time delays from the mapping positions overlayed with a histogram of the time delays from the Eve positions to illustrate potential of identifying falsely claimed positions of transmission.](image)

We reiterate that this example does not entail a rigorous evaluation of the many intricacies involved with our proposed authentication scheme. There are many different geometries to consider for the positions of Alice and Eve. There are several forms of measurement error to consider: error in Alice’s reported position, error in the mapped reflecting plane, and error in the measured time delay. Additionally, it is not obvious how the addition of multiple reflecting planes affects the proposed scheme. Finally, this example does not consider the capacity of Eve or Alice to change their position and how such movement affects Doppler measurements or how lack of movement may improve the resolution with which time delay can be measured. The example simply highlights that there is substantial potential for Bob to leverage delay measurements and knowledge of anticipated reflection planes to verify Alice is transmitting from a claimed position.

VI. Summary

We provided a review of recent physical-layer authentication schemes and posited a framework where physical-
layer authentication is decomposed into RF-fingerprint like features and CSI features. Furthermore, we proposed the CSI features be reduced to the fundamental parametric channel model features to enable better assessment of their value as authenticating features. To support an authentication scheme where a transmitter’s reported location is to be verified, we proposed a methodology to estimate large planar specular reflectors from multi-path delay measurements in different geometries. We presented the CRLB of such a planar estimator in a simulated scenario. And finally, we presented a simple example to illustrate the potential value in identifying transmissions emanating from falsely claimed positions.

VII. CHALLENGES AND FUTURE WORK

There are several avenues to explore further for this research. As is the case with many optimization algorithm implementations, there is space to improve the algorithm’s performance. Related to the optimization algorithm implementation is the inclusion of additional reflecting planes and methods to correctly group time delays with their respective reflecting plane. Also, there is value in exploring the estimation of each reflecting plane’s boundaries. Additionally, it is our intention to establish a physical experiment to validate our proposed methodology. Regarding our proposed authentication scheme, substantial work remains exploring its practical limits. Finally, there may be potential to improve geolocation services by leveraging our proposed mapping of planar specular reflectors in a region.

VIII. APPENDIX A

For “regularity” conditions to exist, the $\mathbb{E}[\partial^2 \ln(p(\hat{\mathbf{\Theta}}; \mathbf{P}_{Tx}, \mathbf{P}_{Rx}))] = 0$ for all $\mathbf{Q}_j$. In order to show this is true, we start with taking the natural log of (11) where $\ln(p)$ is shortened notation for $\ln(p(\hat{\mathbf{\Theta}}; \mathbf{P}_{Tx}, \mathbf{P}_{Rx}))$. We then take the first partial derivative with respect to the $j$th parameter of $\mathbf{\Theta}$ yielding

$$\frac{\partial}{\partial \mathbf{\Theta}_j} \ln(p) = \frac{1}{\sigma^2} \sum_{i=0}^{N-1} (\hat{\tau}_i - Q_i(\mathbf{\Theta})) \frac{\partial Q_i(\mathbf{\Theta})}{\partial \mathbf{\Theta}_j}$$

where $\mathbf{\Theta}_i$ is the $i$th parameter of $\mathbf{\Theta}$. We follow by taking the expectation of (15) yielding

$$\mathbb{E}[\frac{\partial}{\partial \mathbf{\Theta}_j} \ln(p)] = \frac{1}{\sigma^2} \sum_{i=0}^{N-1} (\hat{\tau}_i - Q_i(\mathbf{\Theta})) \frac{\partial Q_i(\mathbf{\Theta})}{\partial \mathbf{\Theta}_j}$$

Lastly, $\mathbb{E}[\hat{\tau}_i] = Q_i(\mathbf{\Theta})$ and thus $\mathbb{E}[\frac{\partial}{\partial \mathbf{\Theta}_j} \ln(p)] = 0$.

Regarding the elements of the Fisher Information Matrix, the second partial partial derivative of (15) with respect to the $k$th parameter yields

$$\frac{\partial^2}{\partial \mathbf{\Theta}_j \partial \mathbf{\Theta}_k} \ln(p) = \frac{1}{\sigma^2} \sum_{i=0}^{N-1} (\hat{\tau}_i - Q_i(\mathbf{\Theta})) \frac{\partial^2 Q_i(\mathbf{\Theta})}{\partial \mathbf{\Theta}_j \partial \mathbf{\Theta}_k} - \frac{\partial Q_i(\mathbf{\Theta})}{\partial \mathbf{\Theta}_j} \frac{\partial Q_i(\mathbf{\Theta})}{\partial \mathbf{\Theta}_k}$$

Leveraging $\mathbb{E}[\hat{\tau}_i] = Q_i(\mathbf{\Theta})$, the negative expectation of (17) yields

$$-\mathbb{E}[\frac{\partial^2}{\partial \mathbf{\Theta}_j \partial \mathbf{\Theta}_k} \ln(p)] = \frac{1}{\sigma^2} \sum_{i=0}^{N-1} \frac{\partial^2 Q_i(\mathbf{\Theta})}{\partial \mathbf{\Theta}_j \partial \mathbf{\Theta}_k} - \frac{\partial Q_i(\mathbf{\Theta})}{\partial \mathbf{\Theta}_j} \frac{\partial Q_i(\mathbf{\Theta})}{\partial \mathbf{\Theta}_k}$$

REFERENCES