Artificial Noise-Aided MIMO Physical Layer Authentication With Imperfect CSI

Jake Bailey Perazzone, *Student Member, IEEE*, Paul L. Yu, *Senior Member, IEEE*, Brian M. Sadler, *Life Fellow, IEEE*, and Rick S. Blum, *Fellow, IEEE*

***Abstract*— Fingerprint embedding at the physical layer is a highly tunable authentication framework for wireless communication that achieves information-theoretic security by hiding a traditional HMAC tag in noise. In a multiantenna scenario, artificial noise (AN) can be transmitted to obscure the tag even further. The AN strategy, however, relies on perfect knowledge of the channel state information (CSI) between the legitimate users. When the CSI is not perfectly known, the added noise leaks into the receiver's observations. In this article, we explore whether AN still improves security in the fingerprint embedding authentication framework with only imperfect CSI available at the transmitter and receiver. Specifically, we discuss and design detectors that account for AN leakage and analyze the adversary's ability to recover the key from observed transmissions. We compare the detection and security performance of the optimal perfect CSI detector with the imperfect CSI robust matched filter test and a generalized likelihood ratio test (GLRT). We find that utilizing AN can greatly improve security, but suffers from diminishing returns when the quality of CSI knowledge is poor. In fact, we find that in some cases allocating additional power to AN can begin to decrease key security.**

***Index Terms*— Authentication, fingerprint embedding, physical layer security, multiple-input, multiple-output (MIMO), artificial noise (AN).**

I. Introduction

THE need for authentication in communication systems is readily apparent. By enabling trusted users to verify the source of received transmissions, the integrity of the system can be maintained and trustworthy communication can take place. Its importance is further amplified in the wireless setting where potential adversaries can easily observe and interact with the legitimate parties in an attempt to communicate under the guise of a legitimate transmitter. Traditionally, authentication is handled via cryptographic protocols in the MAC layer or above. Recently, though, it has been shown that authenticating at the physical layer can offer many benefits, including not requiring a secret key, offering information-theoretic guarantees, and/or providing covertness, e.g., [1]–[10].

The typical message authentication model consists of three parties, the legitimate transmitter, legitimate receiver, and an adversary whom we will refer to as Alice, Bob, and Eve, respectively. In the model, Alice sends a message to Bob who wishes to decode it and determine whether it came from Alice or not. Authentication is required here because of the presence of Eve who may try to impersonate Alice by sending messages of her own. In order for Bob to authenticate the message, Alice must include, deliberately or not, some evidence in the transmission that identifies her as the sender. The effectiveness of an authentication system is measured by its ability to accurately identify authentic transmissions and reject inauthentic ones. Its success is complicated by the fact that Eve can learn the unique identifying information used by Alice and Bob to establish authenticity by observing authentic transmissions. Therefore, it is important to both limit and keep track of Eve's knowledge before the system is compromised.

In this article, we consider key-based authentication in which a shared secret key between Alice and Bob is used to facilitate authentication. Existing key-based cryptographic methods [11], however, rely only on computational complexity to protect the key from Eve and are instantly defeated by a computationally unlimited adversary. Meanwhile, other key-based works that do consider such adversaries over noiseless channels, e.g., [12], [13], still reveal the key in relatively few observations depending on key length [14], [15]. Therefore, exploiting physical layer security for information-theoretic authentication is a worthwhile endeavor that can extend the amount of times a key can be used securely.

Authentication via fingerprint embedding is a physical layer authentication framework that combines the practicality of the cryptographic methods with the advantages of the physical layer to provide information-theoretic guarantees and covertness [5]. In the traditional hash-based message authentication code (HMAC) approach, a tag is generated from both the message and a shared secret key using a cryptographic hash function [11]. The tag is then transmitted with the message to Bob who computes the expected tag using the received message and shared key. Bob authenticates if the expected tag matches the received tag. The fingerprint embedding framework follows the same concept, but hides the tag from adversaries by superimposing it upon the message waveform

Manuscript received June 5, 2020; revised October 23, 2020; accepted December 22, 2020. Date of publication January 11, 2021; date of current version February 9, 2021. This work was supported by the U.S. Army Research Laboratory and the U.S. Army Research Office under Grant Number W911NF-17-1-0331, the National Science Foundation under Grant ECCS-1744129, and a Grant from the Commonwealth of Pennsylvania, Department of Community and Economic Development, through the Pennsylvania Infrastructure Technology Alliance (PITA). The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Ragnar Thobaben. *(Corresponding author: Jake Bailey Perazzone.)*

Jake Bailey Perazzone and Rick S. Blum are with the Electrical and Computer Engineering Department, Lehigh University, Bethlehem, PA 18015 USA (e-mail: jbp215@lehigh.edu; rblum@lehigh.edu).

Paul L. Yu and Brian M. Sadler are with the U.S. Army Research Lab, Adelphi, MD 20783 USA (e-mail: paul.l.yu.civ@mail.mil; brian.m.sadler6@mail.mil).

Digital Object Identifier 10.1109/TIFS.2021.3050599

at low power. The deliberate low signal-to-noise ratio (SNR) of the tag ensures that even with computationally unlimited resources, Eve will be mostly unsuccessful in her attempts to extract the correct key while allowing Bob to still detect its presence. While the framework has been shown to work well in single-input, single-output (SISO) scenarios in both simulation [5] and practice [16], its capabilities can be further improved by utilizing multiple-input, multiple-output (MIMO) communications [17] and employing a secrecy technique known as artificial noise [18]. In the SISO case, the only degree of freedom available to increase detection performance is the total energy of the transmitted tag. MIMO communications, on the other hand, offer more degrees of freedom to achieve desired results.

In this article, we study the use of artificial noise (AN) [19], [20], called masked beamforming in some articles [21], which is a technique in which a jamming signal that only affects Eve is broadcast simultaneously with the traditional signal. This is achieved by designing the AN to be orthogonal to the main channel, i.e., the channel from Alice to Bob. The role of AN is to further increase the security of the shared key such that we can increase the amount of times a single key can be used before it is compromised. This is the first use of beamforming-based AN in an authentication setting. Some other works that deploy artificial noise to aid authentication are different from our approach. For example, Wu *et al.* use it in such a way that it affects both Bob and Eve evenly in a SISO setting [22] and also apply it in a different challenge-response authentication model [23], while Tugnait uses added noise to aid detection rather than enhance security [24].

Since the design of this type of AN is deeply dependent on knowledge of the channel state information (CSI) of the main channel, we address the very practical problem of having only imperfect CSI knowledge. In doing so, we make the framework more robust to channel estimation errors, and present analysis that allows users to identify when and how much AN is worth using depending on the quality of their channel estimate and desired performance. More specifically, we provide the following contributions in the context of MIMO systems with imperfect CSI:

1) A highly tunable authentication framework that utilizes AN to increase security and is robust to channel estimation error
2) A new security analysis that precisely tracks the vulnerability of the key by analyzing an adversary's ability to infer the secret key from observations
3) Numerical results that show the design trade-offs of the framework, show that desirable operating regimes exist, and show that allocating additional power to AN is not always beneficial

The article is organized as follows. Section II provides background on MIMO secrecy capacity, authentication, and artificial noise. Next, Section III details the specific procedures and analysis of the MIMO framework while Section IV considers security from an adversarial capabilities perspective. Finally, numerical results are provided in Section V before making concluding remarks in Section VI.

II. Background

In this section, we briefly review secrecy in MIMO systems, including artificial noise and levels of CSI knowledge, and how it pertains to authentication.

A. Notation

Matrices are represented by bold capital letters while vectors are bold lower case letters and scalars are non-bolded upper and lower case letters. Subscripts of matrices denote particular elements, i.e., $\mathbf{A}_{ij}$ is the i^{th} column, j^{th} row element of $\mathbf{A}$. Additionally, $\mathbf{A}_i^j$ denotes the columns i through j of matrix $\mathbf{A}$. The operators $E[\cdot]$, $\text{Var}(\cdot)$, $\det(\cdot)$, $\text{Tr}(\cdot)$, $\Re(\cdot)$, and $\dagger$ denote the expectation, variance, determinant, trace, real, and Hermitian transpose of their arguments, respectively. Probability distribution functions and cumulative distribution functions are denoted as $p(X)$ and $P(X)$, respectively.

B. MIMO Secrecy Capacity, Authentication, and Artificial Noise

The main focus of physical layer security research is the analysis of secret communications in which a message is sent between trusted parties that must not be successfully decoded by an eavesdropper. The maximum possible rate at which the message can be sent securely and reliably is known as secrecy capacity [25]. A lot of work has been dedicated to characterizing secrecy rate and capacity while information-theoretic authentication, on the other hand, has not received nearly the same amount of attention, especially in MIMO communications with imperfect CSI. Since authentication has different goals and thus has different performance metrics than secrecy, the existing analysis does not readily apply. Recently, though, physical layer authentication has received more interest and different approaches and models have been proposed. For example, some work derives its authentication capabilities from a shared key only [13], [26], [27] in a noiseless setting while some utilize a noisy channel only [1], [3], [10], [28]. Some even utilize both [2], [9], [29].

Our framework falls into the final category where the advantage over the adversary is in the form of a shared secret key and where differences between the main and adversarial channel are exploited. Since the key is the source of authentication, it must be protected from the adversary to maintain security. So, rather than using secrecy techniques and analysis to protect a message, we instead apply them to the key by way of the tag in order to keep it secret from the adversary. One of the major issues with applying information-theoretic security concepts in practice, though, is the assumptions that must be made about the model or adversary. For example, in the wire-tap channel [25], it must be assumed that the main channel is "less noisy" than the channel to the adversary, denoted the adversarial channel, in order to extract any secrecy from the channel. These types of strong assumptions also extend to analysis of the MIMO wire-tap channel in which it is assumed that the main and adversarial channels, denoted as $\mathbf{H}$ and $\mathbf{G}$, respectively, are perfectly known [30], [31].

Fortunately, in MIMO systems, some secrecy can still be guaranteed even when $\mathbf{G}$ is unknown, through the use of a

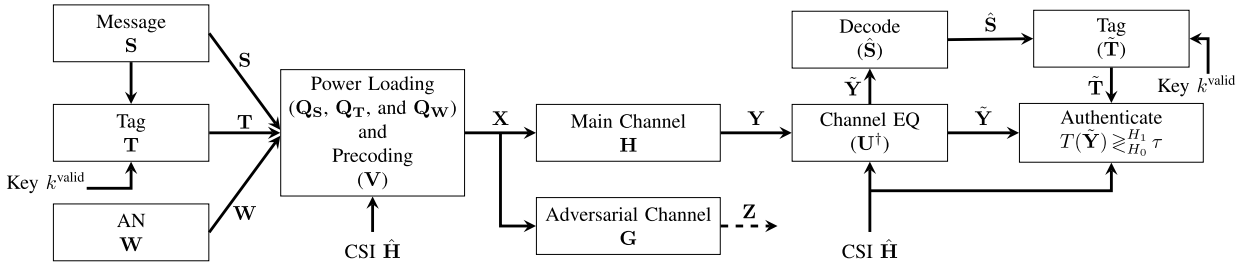

Fig. 1. System diagram of the physical layer fingerprinting authentication framework. A legitimate transmitter-receiver pair share the same secret key that is then used to create an identifying tag that enables authentication.

technique called artificial noise which requires only knowledge of $\mathbf{H}$. First introduced in [19] and [20], the technique achieves secrecy by simultaneously transmitting additional noise that is orthogonal to the main channel such that it cancels out at the receiver. In doing so, it degrades an adversary's channel, but not the legitimate receiver's, effectively lowering the adversary's SNR and thereby increasing security. This scheme can sustain rates that approach secrecy capacity in the high SNR MISO regime [21], but unfortunately bounds rates arbitrarily far from secrecy capacity in the MIMO regime [31]. Nonetheless, artificial noise is a viable approach to increasing secrecy in MIMO communications with the more realistic assumption that communicating parties know their channel $\mathbf{H}$, but not the adversary's $\mathbf{G}$.

In practice, however, even $\mathbf{H}$ cannot be perfectly known, further complicating the deployment of AN. In this case, the null space of $\mathbf{H}$, which is needed to design an orthogonal signal, will not be known exactly. Then, if the imperfect CSI is used to design the AN, it will leak into the legitimate receiver's observations degrading their channel in addition to the adversary's, albeit to a lesser degree. Some work to address imperfect CSI in regards to physical layer authentication has been done using machine learning [8] and in regards to secrecy capacity with and without artificial noise [32]. In the studies, the imperfection of CSI knowledge is due to things such as general channel estimation errors [33], limited feedback [34], and delayed feedback [35]. Since the optimal secrecy coding approach cannot be determined and secrecy capacity itself cannot be calculated in these scenarios, most works instead attempt to first optimize performance of the main channel under some metric, e.g., minimum mean squared error (MMSE) of the message [36] or maximizing signal-to-interference-plus-noise (SINR) [37], and then allocate any remaining power to AN after a certain performance metric is met, essentially maximizing the amount of power available for AN.

In this article, we utilize AN to increase the secrecy of the key. We will primarily focus on optimizing authentication/detection performance, before analyzing the trade-offs with security. The straightforward approach of allocating as much power to AN after certain metrics are met, as in [35] and [37], does not always result in the best security in our framework.

III. MIMO With an Authentication Framework

In this section, we present the fingerprint embedding authentication framework with artificial noise for the imperfect CSI MIMO regime.

We follow the same basic principles of tag embedding as the SISO framework [5] and the overall structure of its MIMO extension [17], but enhance it to include artificial noise and to be robust to imperfect CSI. A brand new security analysis is given in Section IV. A block diagram of the authentication framework can be found in Figure 1. The goal still remains to enable Bob to successfully decode and authenticate messages from Alice while rejecting messages from Eve, but the presence of imperfect CSI requires major changes to the detection procedure to maintain optimality and other desired properties.

A. MIMO System and CSI Model

We first give the basic structure of the transmitted signal and the channel and then detail the design of each component in the subsequent subsections. The framework is primarily based on the HMAC protocol [11], but adapts it for the physical layer to take advantage of the noise inherent in the wireless medium. Before communications begin, Alice and Bob generate and share a κ-bit secret key k^{valid} that is chosen uniformly at random from $\mathcal{K}$, the set of all κ-bit keys. Eve begins ignorant of the shared key, but can learn it by observing Alice and Bob's communications. Additionally, besides possibly sending messages of her own, we assume that Eve is not actively jamming or interfering with Alice's transmissions. Alice, Bob, and Eve are equipped with N_T, N_R, and N_A antennas, respectively.[1]

When Alice is ready to communicate, she generates an $N_D \times L$ complex message $\mathbf{S}$ where $N_D \leq \min\{N_T, N_R\}$ and each of the LN_D symbols are drawn from any desired modulation constellation, e.g., QPSK or 16-QAM, with average unit power. The number of dimensions, N_D, is chosen by the designer and provides a trade-off between message rate and security. A larger N_D allows more streams of data (higher rate), but leaves less dimensions for AN. It has been shown that increasing the number of dimensions of AN increases security [20]. The parameter N_D is important in that it allows Alice to send AN in the range space of $\mathbf{H}$ in cases where transmitting AN in only the null space is not sufficiently secure for her needs or if there is no null space at all, i.e., $N_R \geq N_T$.

Then, following the HMAC protocol, an $N_D \times L$ complex tag $\mathbf{T}$ is generated using the tag-generating function $g(\cdot, \cdot)$ as

$$\mathbf{T} = g(\mathbf{S}, k^{\text{valid}}), \tag{1}$$

[1]Eve can also be interpreted as being multiple colluding adversary's that have a total of N_A antennas with a fusion center that has access to all observations.

where the symbols of $\mathbf{T}$ can be from a different constellation than $\mathbf{S}$. The function $g(\cdot,\cdot)$, commonly implemented in practice via a cryptographic hash function, is specifically designed to appear as though the outputs are chosen uniformly at random, but are actually deterministic for fixed inputs. The effect of this is that minor variations in the input cause very different outputs with high probability. For authentication purposes, this means that producing $\mathbf{T}$ for a given $\mathbf{S}$ without knowledge of the specific key k^{valid} is unlikely. The determinism of the function ensures that anyone with access to k^{valid} will produce the same tag $\mathbf{T}$ for the same $\mathbf{S}$, enabling authentication.

Next, Alice generates the $(N_T - N_D) \times L$ artificial noise matrix $\mathbf{W}$ whose entries are zero-mean complex Gaussian with unit variance. She then embeds the tag into the message waveform using power allocation parameters p_s^2 and p_t^2 for the message and tag, respectively, and loads the AN into the remaining transmit dimensions with power allocation p_w^2. The final transmitted $N_T \times L$ matrix $\mathbf{X}$ is of the form

$$\mathbf{X} = \mathbf{V}\begin{bmatrix} \mathbf{Q}_{\mathbf{S}}^{\frac{1}{2}} p_s \mathbf{S} + \mathbf{Q}_{\mathbf{T}}^{\frac{1}{2}} p_t \mathbf{T} \\ p_w \mathbf{Q}_{\mathbf{W}}^{\frac{1}{2}} \mathbf{W} \end{bmatrix}, \tag{2}$$

where $\mathbf{V}$ is the $N_T \times N_T$ precoding matrix, $\mathbf{Q_S}$ and $\mathbf{Q_T}$ are the $N_D \times N_D$ diagonal power loading matrices of the message and tag, respectively, and $\mathbf{Q_W}$ is the $(N_T - N_D) \times (N_T - N_D)$ diagonal power loading matrix of the AN. The precoding and power loading will be designed such that $\mathbf{X}$ satisfies a total power constraint P_0 where $\text{Tr}(E[\mathbf{X}\mathbf{X}^\dagger])/L = p_s^2 \,\text{Tr}(\mathbf{V}_1^{N_D}\mathbf{Q_S}{\mathbf{V}_1^{N_D}}^\dagger) + p_s^2 \,\text{Tr}(\mathbf{V}_1^{N_D}\mathbf{Q_T}{\mathbf{V}_1^{N_D}}^\dagger) + p_w^2 \,\text{Tr}(\mathbf{V}_{N_D+1}^{N_T}\mathbf{Q_W}{\mathbf{V}_{N_D+1}^{N_T}}^\dagger) \leq P_0$. The power allocation of the tag is typically chosen such that $p_t^2 \ll p_s^2$ as to have negligible impact on message decoding [16], [38].

Bob observes the transmitted vector through the $N_R \times N_T$ channel matrix $\mathbf{H}$ while Eve observes it through the $N_A \times N_T$ channel matrix $\mathbf{G}$. In other words, Bob will receive the $N_R \times L$ matrix

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{N}_\text{b} \tag{3}$$

while Eve will receive the $N_A \times L$ matrix

$$\mathbf{Z} = \mathbf{G}\mathbf{X} + \mathbf{N}_\text{e}\,, \tag{4}$$

where $\mathbf{N}_\text{b}$ and $\mathbf{N}_\text{e}$ are the $N_R \times L$ and $N_A \times L$ matrices of i.i.d. zero-mean circularly-symmetric complex white Gaussian noise (CWGN) with variance σ_b^2 and σ_e^2, respectively. From $\mathbf{Y}$, Bob tries to detect the presence of $\mathbf{T}$ to determine authenticity, while Eve tries to determine which key was used from $\mathbf{Z}$. It is assumed that the entries of both $\mathbf{H}$ and $\mathbf{G}$ are i.i.d. zero-mean complex Gaussian distributed with unit variance and are determined before each round of communication such that they remain constant for the entire message. We consider the case where $\mathbf{H}$ and $\mathbf{G}$ are independent. The gain of the channel is accounted for in the transmit power of $\mathbf{X}$.

We assume that Alice and Bob have (im)perfect knowledge of $\mathbf{H}$ and no knowledge of $\mathbf{G}$ while the adversary has perfect knowledge of both channels. In this article, we consider the case where the CSI imperfection is due to channel estimation errors. Specifically, we model the channel estimate $\hat{\mathbf{H}}$ as a perturbation of the true channel with an error matrix defined as

$$\mathbf{E} = \mathbf{H} - \hat{\mathbf{H}}\,. \tag{5}$$

We assume that $\hat{\mathbf{H}}$ is found through minimum mean square error (MMSE) estimation and is thus uncorrelated with the error matrix [39]. We then assume that $\hat{\mathbf{H}}$ and $\mathbf{E}$, are both i.i.d. zero-mean complex Gaussian with variances $1 - \sigma_{\mathbf{E}}^2$ and $\sigma_{\mathbf{E}}^2$, respectively [39]. The value of $\sigma_{\mathbf{E}}^2$ characterizes the quality of the estimate and can be determined from estimation parameters such as training interval length, pilot symbol transmit power, and channel coherence time depending on the technique used [39]. The case of perfectly known $\mathbf{H}$ is included in this model by setting $\sigma_{\mathbf{E}}^2 = 0$. We consider the cases where the value of $\sigma_{\mathbf{E}}^2$ is either known or unknown to all. In both cases, we assume that Alice and Bob have access to the same estimate $\hat{\mathbf{H}}$. Mismatched estimates can be explored in future work.

We will focus on optimizing authentication/detection performance first, before analyzing the trade-offs with security. This strategy is motivated by the fact that the adversarial channel is unknown to the legitimate parties so design can only be catered to the main channel. Additionally, optimal tag detection by the receiver results in a lower tag power requirement to achieve a given detection probability. This increases security since a lower tag power makes it more difficult for the adversary to recover the key. For the perfect CSI case, optimal tag detection/authentication is easily obtained and feasible, whereas for imperfect CSI, the optimal test is infeasible due to the lack of a closed-form expression of the underlying distributions. Therefore, we provide alternative sub-optimal tests for two different CSI scenarios in Section III-E and compare them to the perfect CSI test to judge the performance loss. More specifically, when all distributions and their parameters, such as error variance, are known, we propose using a robust matched filter tag detection test, while for cases where the distribution of the error is unknown, we propose the GLRT.

B. Legitimate Transmitter Design

We now discuss the design of the precoding and power loading matrices in the transmitted vector in Eq. (2). The matrices $\mathbf{V}$, $\mathbf{Q_S}$, $\mathbf{Q_T}$, and $\mathbf{Q_W}$ are determined by the framework and the given channel $\mathbf{H}$ while p_s^2, p_t^2, p_w^2, and N_D are parameters that are chosen by the user. The parameter N_D, in particular, controls the number of dimensions over which data is sent and allows users to sacrifice data rate in order to send AN over additional dimensions. This flexibility is especially important for cases like $N_T = N_R$ in which there is no null space to send the artificial noise and AN must be sent over dimensions in the range space of $\mathbf{H}$ normally reserved for data. Without knowledge of $\mathbf{G}$, we design the precoding and power loading for the message, tag, and AN to optimize reception at Bob.

When $\mathbf{H}$ is perfectly known, the singular value decomposition (SVD) precoding approach along with water-filling for power loading achieve main channel capacity [40]. The use of SVD allows for the decomposition of the MIMO channel into independent parallel channels while water-filling optimally

allocates power to those parallel channels by prioritizing the stronger ones. In the case of imperfect channel knowledge, however, these two strategies cannot be executed precisely. For example, performing SVD with the channel estimate $\hat{\mathbf{H}}$ will cause the individual channels to not be fully orthogonal leading to leakage between them while naively performing water-filling using $\hat{\mathbf{H}}$ will lead to suboptimal rate. Additionally, the estimated null space will cause the artificial noise to leak into Bob's observations since it will not cancel perfectly. Nonetheless, the optimal design of $\mathbf{V}$ still begins with SVD of $\hat{\mathbf{H}}$ [39]:

$$\hat{\mathbf{H}} = \mathbf{U}\mathbf{D}\mathbf{V}^{\dagger}, \tag{6}$$

where $\mathbf{D}$ is an $N_R \times N_T$ diagonal matrix of singular values and $\mathbf{U}$ and $\mathbf{V}$ are unitary matrices of singular vectors. The precoding matrix $\mathbf{V}$ is then the right singular matrix of $\hat{\mathbf{H}}$. The unitary structure of $\mathbf{V}$ reduces the power constraint to $\mathrm{Tr}(E[\mathbf{X}\mathbf{X}^{\dagger}])/L = p_s^2\,\mathrm{Tr}(\mathbf{Q_S}) + p_t^2\,\mathrm{Tr}(\mathbf{Q_T}) + p_w^2\,\mathrm{Tr}(\mathbf{Q_W}) \le P_0$.

Next, for the design of $\mathbf{Q_S}$, we adopt the approach in [39] in which a spatio-temporal modified water-filling algorithm is presented that maximizes a lower bound on the main channel capacity under an average transmit power constraint. While there are two parts of the approach, we only consider the spatial aspect which slightly modifies the traditional water-filling algorithm depending on the quality of the channel estimate via $\sigma_{\mathbf{E}}^2$ and with constant P_0. For a channel estimate $\hat{\mathbf{H}}$, the modified water-filling algorithm produces a diagonal $N_D \times N_D$ power loading matrix $\mathbf{Q_S}$ as follows

$$\mathbf{Q_S}(i,i) = \left(\mu - \frac{(\sigma_{\mathrm{b}}^2 + \sigma_{\mathbf{E}}^2 P_0)}{\lambda_i}\right)^{+} \tag{7}$$

$$\text{s.t. } P(\mu) = \sum_{i=1}^{N_D} \mathbf{Q_S}(i,i) \le P_0\,, \tag{8}$$

where λ_i is the i^{th} eigenvalue of $\hat{\mathbf{H}}^{\dagger}\hat{\mathbf{H}}$, μ is chosen to satisfy the data and tag power constraint such that $\mathrm{Tr}(\mathbf{Q_S}) = P(\mu) = P_0$, and $(\cdot)^+ = \max\{\cdot, 0\}$. When considering perfect CSI, i.e., when $\sigma_{\mathbf{E}}^2 = 0$, the modified water-filling approach reduces to standard water-filling. Note that there are cases in which the algorithm decides that not all desired dimensions should be used for optimal data transmission. In that event, N_D in the subsequent analysis should be changed to the number of nonzero entries in $\mathbf{Q_S}$ from (7) and (8) rather than the value chosen by Alice and Bob.

For the tag, we consider two embedding strategies as in [17] termed the all mode (AM) and strongest mode only (SM) embedding approaches. In the first, the tag is embedded across the same eigenmodes as the message, so the power loading is the same as the message, i.e., $\mathbf{Q_T} = \mathbf{Q_S}$, just scaled by p_t^2. In the second approach, the tag is embedded in only the strongest mode in which only the first diagonal element of $\mathbf{Q_T}$ is nonzero and is set to P_0. For an analysis of optimal joint message and tag precoding, see [41]. Finally, since $\mathbf{G}$ is unknown, the artificial noise is transmitted isotropically such that $\mathbf{Q_W} = \frac{P_0}{N_T - N_D}\mathbf{I}_{N_T - N_D}$. Therefore, the final transmit power satisfies the constraint, $\mathrm{Tr}(E[\mathbf{X}\mathbf{X}^{\dagger}])/L = p_s^2\,\mathrm{Tr}(\mathbf{Q_S}) + p_t^2\,\mathrm{Tr}(\mathbf{Q_T}) + p_w^2\,\mathrm{Tr}(\mathbf{Q_W}) = p_s^2\,P_0 + p_t^2 P_0 + p_w^2 P_0 = P_0$, when $p_s^2 + p_t^2 + p_w^2 = 1$.

C. Authentication and Tag Detection Assumptions

Bob's goal is to decode the message $\mathbf{S}$ and determine its authenticity by detecting the presence of the valid tag $\mathbf{T}$ in the received signal $\mathbf{Y}$. He is successful when he correctly accepts a message containing a valid tag or when he rejects a message that does not. The problem is a binary hypothesis test where

$$\begin{aligned} H_0:&\quad \text{valid tag is not present in received signal}\\ H_1:&\quad \text{valid tag is present in received signal}\,. \end{aligned}$$

Choosing the hypotheses as such allows us to provide security guarantees such that the probability of falsely accepting an inauthentic message is limited to a user-specified level while providing the best detection of authentic signals as possible. This is achieved through the Neyman-Pearson style approach to detection which maximizes the probability of detection P_{D} for a given false alarm probability P_{FA}, which in this case represents the false acceptance of an inauthentic message. When the value of P_{FA} is guaranteed, the detector is said to have a constant false alarm rate (CFAR) which is very valuable in authentication.

Since the Neyman-Pearson approach utilizes the likelihood ratio, the structure and distributions under each hypothesis must be well-defined to determine the optimal test. While the structure of the signal under H_1 is known since it is explicitly designed by Alice and Bob, the structure under H_0 depends on Eve's attack strategy, or lack thereof. Since her goal is to have one of her messages accepted as though it was from Alice, we assume that she selects a key, either naively or based on her observations, and then follows the same procedure as Alice via Eq. (2) following the design from Section III-B. According to consequences of Sanov's theorem [42], the best way to cause errors in Bob's test, i.e., have him accept Eve's message, is to induce a distribution at Bob that is as close to H_1 as possible. Another way to justify this attack model as opposed to allowing Eve to do anything is that any transmission that does not adhere to the communication protocol/standard used by Alice and Bob will likely be flagged or cause errors, so Eve's possible signal structures are restricted. Alternatively, game theory could be used to formulate the attack model and detector as a game to determine a possible Nash equilibrium like in [6], but this is out of the scope of this article. Since a correct key choice will have a high probability of being accepted, we model H_0 as a uniformly random tag generated by an incorrect key choice to create a baseline level of security. This ensures that Eve is limited to P_{FA} until she gains enough information about the key to guess with probability greater than P_{FA}.

The random tag may be allocated a different power level than Alice's, so we denote the tag power as p_{eve}^2 in H_0 to differentiate it from p_t^2 in H_1. However, we will assume that p_{eve}^2 is known and $p_{\mathrm{eve}}^2 = p_t^2$ unless otherwise specified since Bob might be able to detect the increased power using a simple energy detector thereby decreasing the success probability of an attack. The amount of additional power Eve could allocate to her random tag is also limited by its interference with the

message which would cause more errors in Bob's decoder. The assumption of known p_{eve}^2 is removed later on for the GLRT detector and the performance of such an energy detector is omitted for conciseness. Eve's randomly chosen tag in noise is distributed as a Gaussian mixture model where each component represents a tag in $\mathcal{T}$, i.e.,

$$p(y|H_0) = \frac{1}{|\mathcal{T}|}\sum_{i=1}^{|\mathcal{T}|}\frac{1}{\pi^L\sigma_{\text{b}}^{2L}}\exp\left(-\frac{1}{\sigma_{\text{b}}^2}(y-p_{\text{eve}}t_i)^\dagger(y-p_{\text{eve}}t_i)\right) \tag{9}$$

To simplify the problem, our final assumption under H_0 is that the random tag symbols are distributed as zero-mean complex Gaussian with variance p_{eve}^2. This allows us to develop closed-form, i.e., feasible, tests that are easily implemented in practice. The assumption is motivated by the fact that the modes of the Gaussian mixture tend to overlap one another and tend towards a zero-mean Gaussian since the tag SNR, $\frac{p_{\text{eve}}^2}{\sigma_{\text{b}}^2}$, is designed to be very low. In other words, as p_{eve}^2 becomes small, (9) is well approximated as zero-mean complex Gaussian with variance $\sigma_{\text{b}}^2 + p_{\text{eve}}^2$.

D. Legitimate Receiver Procedure: Perfect CSI

We first describe the fairly straightforward perfect CSI, i.e., $\sigma_{\mathbf{E}}^2 = 0$, authentication/detection procedure before discussing the imperfect case. After having received

$$\mathbf{Y} = \mathbf{HV}\begin{bmatrix}\mathbf{Q}_{\mathbf{S}}^{\frac{1}{2}}p_s\mathbf{S}+\mathbf{Q}_{\mathbf{T}}^{\frac{1}{2}}p_t\mathbf{T}\\ p_w\mathbf{Q}_{\mathbf{W}}\mathbf{W}\end{bmatrix}+\mathbf{N}_{\text{b}}, \tag{10}$$

Bob performs SVD receiver beamforming by multiplying by $\mathbf{U}^\dagger$ to obtain

$$\begin{aligned}\tilde{\mathbf{Y}} &= \mathbf{U}^\dagger\mathbf{Y}\\ &= \mathbf{D}\begin{bmatrix}\mathbf{Q}_{\mathbf{S}}^{\frac{1}{2}}p_s\mathbf{S}+\mathbf{Q}_{\mathbf{T}}^{\frac{1}{2}}p_t\mathbf{T}\\ p_w\mathbf{Q}_{\mathbf{W}}\mathbf{W}\end{bmatrix}+\mathbf{U}^\dagger\mathbf{N}_{\text{b}}\\ &= \mathbf{D}'(\mathbf{Q}_{\mathbf{S}}^{\frac{1}{2}}p_s\mathbf{S}+\mathbf{Q}_{\mathbf{T}}^{\frac{1}{2}}p_t\mathbf{T})+\mathbf{U}^\dagger\mathbf{N}_{\text{b}},\end{aligned} \tag{11}$$

where $\mathbf{D}'$ is an $N_D \times N_D$ diagonal matrix of singular values creating N_D independent parallel channels. In the case of $N_D \leq N_R$, the last $N_R - N_D$ rows of $\tilde{\mathbf{Y}}$ are ignored since AN will be loaded into those channels leaving an $N_D \times L$ matrix. The remaining artificial noise is not present in the final equation since it is loaded into the null space of the channel, i.e., the all zero columns of $\mathbf{D}$. Since U is unitary, the distribution of $\mathbf{U}^\dagger\mathbf{N}_{\text{b}}$ is the same as $\mathbf{N}_{\text{b}}$ and no adjustments must be made.

Next, Bob obtains a message estimate $\hat{\mathbf{S}}$ by conventional demodulation techniques, ignoring the presence of the tag. He then forms the $N_D \times L$ residual

$$\begin{aligned}\mathbf{R} &= \tilde{\mathbf{Y}} - \mathbf{D}'\mathbf{Q}_{\mathbf{S}}^{\frac{1}{2}}p_s\hat{\mathbf{S}}\\ &= \mathbf{D}'\mathbf{Q}_{\mathbf{T}}^{\frac{1}{2}}p_t\mathbf{T}+\mathbf{U}^\dagger\mathbf{N}_{\text{b}},\end{aligned} \tag{12}$$

by removing $\hat{\mathbf{S}}$ from the observation. By assuming that decoding is successful, $\hat{\mathbf{S}} = \mathbf{S}$, Bob is left with N_D independent blocks of noisy tags with varying SNR due to the gains of the channel. The optimal detector for the hypothesis test outlined in Section III-C in this case is a weighted combination of a matched filter and an energy detector [43]. From our assumption that $p_{\text{eve}}^2 = p_t^2$, the distribution of the total energy of the signal will be the same under both hypotheses. Therefore, for simplicity, we omit the energy detector portion of the test and only use a matched filter test since the performance will be approximately equal. Accounting for the channel gain and power loading, the matched filter (MF) test can be written in matrix form as

$$T(\mathbf{Y}) \triangleq \Re[\text{Tr}(\mathbf{R}^\dagger\tilde{\mathbf{R}})] \underset{H_0}{\overset{H_1}{\gtrless}} \tau \tag{13}$$

where $\tilde{\mathbf{R}} = \mathbf{D}'\mathbf{Q}_{\mathbf{T}}^{\frac{1}{2}}p_t\tilde{\mathbf{T}}$ is the expected residual with $\tilde{\mathbf{T}}$ being the expected tag computed from (1) using k^{valid} and $\hat{\mathbf{S}}$. Since $\mathbf{Y}$ is Gaussian and (13) is a linear transformation, the distribution of the test statistic $T(\mathbf{Y})$ under both H_0 and H_1 is also Gaussian. Then, the threshold τ given a desired false alarm probability P_{FA} and the detection performance can be easily calculated using the Q-function [17].

E. Legitimate Receiver Procedure: Imperfect CSI

We now focus on developing the authentication test in the case of imperfect CSI knowledge, i.e., $\sigma_{\mathbf{E}}^2 > 0$. The goal still remains to find the best test possible such that minimal tag power p_t^2 is required for a desired probability of detection P_D. Finding the optimal test is complicated by the artificial noise leakage in the main channel and the imperfect parallelization of channels. This necessitates a different approach to detection since unknown imperfections are introduced.

There are two main approaches to dealing with unknowns in hypothesis testing, the choice of which depends on the model. If the distributions of the unknowns are available, then optimal performance in the Neyman-Pearson sense can be developed through the Bayesian approach to composite hypothesis testing. If, instead, the unknowns are simply treated as deterministic values or the distributions are not known, then the generalized likelihood ratio test (GLRT) can be employed. Although the Bayesian approach is known to be optimal, it has some undesirable properties and can often lead to solutions that are not closed-form and thus difficult to implement, as is the case here. Therefore, we recommend two alternatives that address two different scenarios. More specifically, a matched filter robust to the channel uncertainties is recommended for known error distributions and p_{eve}^2 while the GLRT is recommended for when the structure/distribution of $\mathbf{E}$ is unknown or parameters $\sigma_{\mathbf{E}}^2$ or p_{eve}^2 are unknown.

Before forming our tests for either approach, we first determine the specific structure of $\mathbf{Y}$ under each hypothesis such that the distributions can be obtained. First, let $\tilde{\mathbf{E}} = \mathbf{U}^\dagger\mathbf{EV}$ where $\mathbf{U}$ and $\mathbf{V}$ are the singular vectors from the SVD of the channel estimate, $\hat{\mathbf{H}} = \mathbf{UDV}^\dagger$. Since $\mathbf{U}$ and $\mathbf{V}$ are both unitary, $\tilde{\mathbf{E}}$ will have the same distribution as $\mathbf{E}$. This allows us to write the actual channel as $\mathbf{H} = \hat{\mathbf{H}} + \mathbf{E} = \mathbf{U}(\mathbf{D}+\tilde{\mathbf{E}})\mathbf{V}^\dagger$. Then, after multiplying $\mathbf{Y}$ from (10) by $\mathbf{U}^\dagger$, Bob receives

$$\begin{aligned}\tilde{\mathbf{Y}} &= \mathbf{U}^\dagger\mathbf{Y}\\ &= (\mathbf{D}+\tilde{\mathbf{E}})\begin{bmatrix}\mathbf{Q}_{\mathbf{S}}^{\frac{1}{2}}p_s\mathbf{S}+\mathbf{Q}_{\mathbf{T}}^{\frac{1}{2}}p_t\mathbf{T}\\ p_w\sqrt{\frac{P_0}{N_T-N_D}}\mathbf{W}\end{bmatrix}+\mathbf{U}^\dagger\mathbf{N}_{\text{b}}.\end{aligned} \tag{14}$$

In the perfect CSI case, the presence of only the diagonal matrix $\mathbf{D}$ ensured that each row of the data matrix separated perfectly and that the artificial noise canceled out successfully. In this case, however, the error matrix $\tilde{\mathbf{E}}$ causes the individual data streams to interfere with each other in addition to the AN leaking into the observation.

If we separate the matrix $\mathbf{D}+\tilde{\mathbf{E}}$ into the first N_D columns as the $N_R \times N_D$ matrix $\mathbf{A}$ and the last $N_T - N_D$ columns as the $N_R \times (N_T - N_D)$ matrix Λ, we can rewrite the observation as

$$\tilde{\mathbf{Y}} = \mathbf{A}\mathbf{Q}_{\mathbf{T}}^{\frac{1}{2}} p_t \mathbf{T} + \Lambda p_{\mathrm{AN}} \mathbf{W} + \mathbf{U}^{\dagger}\mathbf{N}_{\mathrm{b}}\,, \tag{15}$$

with $\mathbf{S}$ removed and where $p_{\mathrm{AN}}^2 = p_w^2 \frac{P_0}{N_T - N_D}$. The perfect removal of $\mathbf{S}$ is justified by the fact that after successfully decoding, it can be used to estimate its unknown amplitude using maximum likelihood estimation before subtracting it from (14). Since L and $p_s^2 P_0$ are large relative to $\sigma_{\mathbf{E}}^2$, the estimate will be very good and $\mathbf{S}$ will be canceled almost perfectly. After this process, $\tilde{\mathbf{Y}}$ can be interpreted as a deterministic signal with a random/unknown complex amplitude matrix $\mathbf{A}$ in the presence of complex Gaussian noise with random/unknown covariance $\Sigma_1 = p_{\mathrm{AN}}^2 \Lambda\Lambda^{\dagger} + \sigma_{\mathrm{b}}^2 \mathbf{I}$. The probability distribution function (PDF) of (15) under H_1 and H_0 conditioned on the actual amplitude and covariance is then

$$p(\tilde{\mathbf{Y}}|H_i, \mathbf{A}, \Sigma_1) = \frac{1}{\pi^{LN_D} \det(\Sigma_i)^L} \exp\left(-\mathrm{Tr}\left(\Sigma_i^{-1}\tilde{\mathbf{Y}}_i\tilde{\mathbf{Y}}_i^{\dagger}\right)\right) \tag{16}$$

for $i = 0, 1$ where $\tilde{\mathbf{Y}}_1 = \tilde{\mathbf{Y}} - \mathbf{A}\mathbf{Q}_{\mathbf{T}}^{\frac{1}{2}} p_t \mathbf{T}$, $\tilde{\mathbf{Y}}_0 = \tilde{\mathbf{Y}}$, and $\Sigma_0 = p_{\mathrm{eve}}^2 \mathbf{A}\mathbf{Q}_{\mathbf{T}}\mathbf{A}^{\dagger} + p_{\mathrm{AN}}^2 \Lambda\Lambda^{\dagger} + \sigma_{\mathrm{b}}^2 \mathbf{I}$. Now that our hypotheses are defined, we can construct our tests.

1) Robust Matched Filter: Since the optimal Bayesian detector lacks a closed-form expression in this problem, we propose adjusting the MF to account for the channel estimate error and AN leakage. Although it is suboptimal, we will show that it performs well. The premise is that the matched filter is tuned as though the channel estimate is correct, but the threshold calculation is modified to ensure that the desired probability of false alarm is maintained. The change in threshold calculation is due to the change in the test statistic's distribution caused by the unknown parameters. The test, denoted as the robust matched filter (RMF), is given as

$$T^{\mathrm{RMF}}(\mathbf{Y}) \triangleq \Re[\mathrm{Tr}(\mathbf{R}^{\dagger}\tilde{\mathbf{R}})] \underset{H_0}{\overset{H_1}{\gtrless}} \tau^{\mathrm{RMF}} \tag{17}$$

where $\mathbf{R}$ is the residual of $\mathbf{Y}$ after the contribution of $\mathbf{S}$ is removed and $\tilde{\mathbf{R}} = \mathbf{D}\mathbf{Q}_{\mathbf{T}}^{\frac{1}{2}} p_t \tilde{\mathbf{T}}$ is the expected residual with $\tilde{\mathbf{T}}$ being the expected tag computed from (1) using k^{valid} and $\hat{\mathbf{S}}$. The test differs from (13) in the calculation of the threshold τ^{RMF}.

For sufficiently large tag length L, we can invoke the central limit theorem (CLT) to approximate the distribution of (17) as Gaussian under both hypotheses. Since our zero-mean Gaussian approximation of H_0 (introduced in Section III-C) has the same mean and variance as the true distribution of a randomly chosen tag, the distribution of the test statistic under H_0 will be the same for both the approximation and the true distribution. In other words, the presented distributions apply to both a random tag and a random zero-mean Gaussian signal. For the sake of brevity, we do not include proofs for the following identities. Let $\tilde{\mathbf{T}} = \mathbf{A}\mathbf{Q}_{\mathbf{T}}^{\frac{1}{2}} p_t \mathbf{T}$, where once again $\mathbf{A}$ is the first N_D columns of $\mathbf{D}+\tilde{\mathbf{E}}$, then the mean and variance under H_0 is

$$E\left[T^{\mathrm{RMF}}(\mathbf{Y}|\hat{\mathbf{H}})\middle|H_0\right] = \mu_{0,\mathrm{b}} = 0 \tag{18}$$

$$\begin{aligned}\mathrm{var}\left(T^{\mathrm{RMF}}(\mathbf{Y}|\hat{\mathbf{H}})\middle|H_0\right) &= \sigma_{0,\mathrm{b}}^2 \\ &= \frac{1}{2} p_{\mathrm{eve}}^2 \,\mathrm{Tr}\left(\mathbf{A}\mathbf{Q}_{\mathbf{T}}\mathbf{A}^{\dagger}\tilde{\mathbf{T}}\tilde{\mathbf{T}}^{\dagger}\right) \\ &\quad + \frac{1}{2}\left(p_{\mathrm{eve}}^2 \sigma_{\mathbf{E}}^2 P_0' + \sigma_{\mathrm{b}}^2\right)\mathrm{Tr}\left(\tilde{\mathbf{T}}\tilde{\mathbf{T}}^{\dagger}\right)\end{aligned} \tag{19}$$

while for H_1 it is

$$E\left[T^{\mathrm{RMF}}(\mathbf{Y}|\hat{\mathbf{H}})\middle|H_1\right] = \mu_{1,\mathrm{b}} = \mathrm{Tr}\left(\tilde{\mathbf{T}}\tilde{\mathbf{T}}^{\dagger}\right) \tag{20}$$

$$\begin{aligned}\mathrm{var}\left(T^{\mathrm{RMF}}(\mathbf{Y}|\hat{\mathbf{H}})\middle|H_1\right) &= \sigma_{1,\mathrm{b}}^2 \\ &= \frac{1}{2}\sigma_{\mathbf{E}}^2 p_t^2 \,\mathrm{Tr}\left(\mathbf{T}^{\dagger}\mathbf{Q}_{\mathbf{T}}\mathbf{T}\tilde{\mathbf{T}}^{\dagger}\tilde{\mathbf{T}}\right) \\ &\quad + \frac{1}{2}\left(p_{\mathrm{AN}}^2 \sigma_{\mathbf{E}}^2 + \sigma_{\mathrm{b}}^2\right)\mathrm{Tr}\left(\tilde{\mathbf{T}}\tilde{\mathbf{T}}^{\dagger}\right).\end{aligned} \tag{21}$$

The threshold τ^{RMF} and performance P_D^{RMF} are then calculated as

$$\tau^{\mathrm{RMF}} = \min \tau \text{ s.t. } \Phi\left(\frac{\tau - \mu_{0,\mathrm{b}}}{\sigma_{0,\mathrm{b}}}\right) \leq 1 - P_{\mathrm{FA}}, \tag{22}$$

$$P_D^{\mathrm{RMF}} = 1 - \Phi\left(\frac{\tau^{\mathrm{RMF}} - \mu_{1,\mathrm{b}}}{\sigma_{1,\mathrm{b}}}\right), \tag{23}$$

where $\Phi(\cdot)$ is the cumulative distribution function (CDF) of the standard normal distribution.

2) GLRT Approach: When the variables are modeled as deterministic unknowns, the GLRT can be utilized for detection. The GLRT is especially useful when the assumption that p_{eve}^2 is known is no longer made as the test accounts for any value of p_{eve}^2 while maintaining the CFAR property. It is also useful when the structure of the error $\mathbf{E}$ or the error variance $\sigma_{\mathbf{E}}^2$ is unknown. Instead of marginalizing out the unknown variables, the GLRT replaces the unknown variables with their maximum likelihood estimates (MLE) in the likelihood function to create

$$L_{\mathrm{GLRT}}(\mathbf{Y}) = \frac{p(\mathbf{Y}|\hat{\boldsymbol{\theta}}_1)}{p(\mathbf{Y}|\hat{\boldsymbol{\theta}}_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \tau\,, \tag{24}$$

where $\hat{\boldsymbol{\theta}}_1$ and $\hat{\boldsymbol{\theta}}_0$ are the MLEs of the unknown parameters $\boldsymbol{\theta}_1$ and $\boldsymbol{\theta}_0$ in H_1 and H_0, respectively. A major advantage of the GLRT is that if the parameter space of the null hypothesis $\boldsymbol{\Theta}_0$ is a proper subset of the alternate hypothesis parameter space $\boldsymbol{\Theta}_1$, then $2\log L_{\mathrm{GLRT}}(\mathbf{Y})$ is asymptotically χ_d^2 distributed under H_0 with degrees of freedom $d = |\boldsymbol{\Theta}_1| - |\boldsymbol{\Theta}_0|$ [44]. For sufficiently large L, this fact, known as Wilks' theorem, can be utilized to produce a CFAR detector since the test statistic under H_0 will always be χ_d^2 regardless of the channel estimate or Eve's transmit power.

Whenever $N_R > N_T - N_D$, though, the null hypothesis parameter space will not be a proper subset of the full parameter space and Wilks' theorem will not apply. This is due to the difference in structure of the covariance matrices under each hypothesis and the fact that $\Lambda\Lambda^\dagger$ will not be full-rank when $N_R > N_T - N_D$. When this is the case, Σ_1 will have less than $2N_R^2$ unknowns since it is derived from the $N_R \times (N_T - N_D)$ matrix Λ whereas Σ_0 will always have $2N_R^2$ unknowns since it is derived from the full rank $N_R \times N_D$ matrix $\mathbf{A}$. Specifically, based on the number of dimensions in which AN is loaded, Σ_1 will contain $\min\{2N_R(N_T - N_D), 2N_R^2\}$ unknowns. While taking advantage of the unique structure of Σ_1 will lead to better estimates and thus better detection performance, we will lose the desired CFAR property afforded by Wilks' Theorem. Nevertheless, we can ignore this structure of the AN interference, $\Lambda\Lambda^\dagger$, in Σ_1 and treat it as a full-rank covariance matrix to apply Wilks' theorem and obtain a CFAR detector.

After invoking Wilks' theorem, the final GLRT test is

$$T_{\text{GLRT}}(\mathbf{Y}) = -2L \log\det\left(\mathbf{I}_{N_R} - \left(\mathbf{Y}\mathbf{Y}^\dagger\right)^{-1}\mathbf{Y}\mathbf{T}^\dagger\left(\mathbf{T}\mathbf{T}^\dagger\right)^{-1}\mathbf{T}\mathbf{Y}^\dagger\right), \quad (25)$$

and it follows that the distribution under each hypothesis is approximately

$$T_{\text{GLRT}}(\mathbf{Y}|H_0) \sim \chi^2_{2N_R N_D} \quad (26)$$

$$T_{\text{GLRT}}(\mathbf{Y}|H_1) \sim \chi^2_{2N_R N_D}(\lambda), \quad (27)$$

where $\lambda = 2\,\text{Tr}\left(\Sigma_1^{-1}\mathbf{A}\mathbf{T}\mathbf{T}^\dagger\mathbf{A}^\dagger\right)$ is the non-centrality parameter and Σ_1 and $\mathbf{A}$ are the true values [45]. These distributions hold for both the zero-mean Gaussian approximation of H_0 and the true distribution due to the CLT. The detection threshold τ^{GLRT} as well as the detection performance P_D^{GLRT} can then be found via

$$\tau^{\text{GLRT}} = \min\tau \text{ s.t. } P_{\chi^2_{2N_R^2}(0)}(\tau) \le 1 - P_{\text{FA}}, \quad (28)$$

$$P_D^{\text{GLRT}} = 1 - P_{\chi^2_{2N_R^2}(\lambda)}(\tau^{\text{GLRT}}), \quad (29)$$

where $P_{\chi^2_{2N_R^2}(\lambda)}(\cdot)$ is the CDF of the $\chi^2_{2N_R^2}$ distribution with non-centrality parameter λ. Since the distributions hold for the actual H_0, the CFAR property holds in practice and performance remains the same whether the adversary transmits a random tag or a zero-mean Gaussian signal.

IV. Security: Adversarial Perspective

In this section, we analyze a computationally unlimited adversary's ability to launch successful attacks as a means of quantifying authentication security. The adversary's main goal is to deceive Bob into falsely accepting one of her messages as if it was from Alice. Due to the collision resistance property of the tag generating function and the structure of Bob's test, the only guaranteed way to successfully fool Bob is to obtain the shared secret key k^{valid}, which allows her to perfectly impersonate Alice. The justification for this attack model was given in Section III-C, where we designed the hypothesis test such that an incorrect key guess is limited to a success probability of P_{FA}. Once Eve's ability to recover the correct key P_{K} exceeds P_{FA}, we can no longer guarantee security at that level. Therefore, we will quantify security by both P_{FA} and the *key lifespan* which we define as the number of observations required by Eve before $P_{\text{K}} > P_{\text{FA}}$.

Eve's key recovery problem is equivalent to a multiple hypothesis testing problem where each hypothesis corresponds to a key in $\mathcal{K}$. It is well known that maximum likelihood (ML) estimation is optimal in terms of minimizing the probability of error for uniform priors [43], therefore we analyze its performance as it is the optimal key recovery algorithm. We directly compute the expected performance of the ML estimator of the key for a given channel pair $\mathbf{H}$ and $\mathbf{G}$ while the key lifespan itself is computed numerically in Section V-B by performing Monte Carlo runs over $\mathbf{H}$ and $\mathbf{G}$. For more discussion on using this as a security metric and its relationship to the information-theoretic quantity min-entropy, please refer to [46].

In order to provide guarantees for any adversary, we assume the worst-case scenario (from a security perspective) in which Eve has complete knowledge of her channel $\mathbf{G}$ as well as Alice and Bob's channel estimate $\hat{\mathbf{H}}$. Due to her knowledge of $\hat{\mathbf{H}}$, Eve is also able to derive both $\mathbf{V}$ and $\mathbf{Q_T}$ in the same way as Alice. If Alice transmits a tagged signal as in (2), Eve observes

$$\mathbf{Z} = \mathbf{G}\mathbf{V}\begin{bmatrix}\mathbf{Q}_{\mathbf{S}}^{\frac{1}{2}} p_s \mathbf{S} + \mathbf{Q}_{\mathbf{T}}^{\frac{1}{2}} p_t \mathbf{T} \\ p_w \mathbf{Q}_{\mathbf{W}}^{\frac{1}{2}} \mathbf{W}\end{bmatrix} + \mathbf{N}_{\text{e}}, \quad (30)$$

which can be rewritten with the message removed as

$$\mathbf{Z} = \mathbf{A}_{\mathbf{G}} p_t \mathbf{T} + \Lambda_{\mathbf{G}} p_{\text{AN}} \mathbf{W} + \mathbf{N}_{\text{e}}, \quad (31)$$

where $p_{\text{AN}}^2 = p_w^2 \frac{P_0}{N_T - N_D}$, $\mathbf{A_G} = \mathbf{G}\mathbf{V}_1^{N_D}\mathbf{Q}_{\mathbf{T}}^{\frac{1}{2}}$ and $\Lambda_{\mathbf{G}} = \mathbf{G}\mathbf{V}_{N_D+1}^{N_T}$ with $\mathbf{V}_i^j$ indicating columns i through j of $\mathbf{V}$. Upon reception of Alice's tagged signal, Eve decodes the message as $\hat{\mathbf{S}}$ and, similarly to Bob, obtains a residual by removing the contribution of $\hat{\mathbf{S}}$ from $\mathbf{Z}$. From the remaining residual signal matrix, Eve wishes to estimate which tag is present so that she can obtain the key by inverting the tag generating function (1). Unlike traditional information-theoretic authentication [12], [13], we generally consider the case where $|\mathcal{K}| < |\mathcal{T}|$ such that we can assume each tag has a single unique key that could have produced it. Therefore, determining the most likely key is tantamount to determining the most likely tag. This assumption is made because large tag sizes are needed in order to offer covertness while achieving desirable detection performance. The larger tag space also allows easier analysis of multiple uses of the same key.

From the residual, Eve formulates the MAP/ML estimation problem

$$\arg\max_{k:\,\mathbf{T}_k = g(\hat{\mathbf{S}},k)} p(\mathbf{Z}|\mathbf{T}_k, \mathbf{A_G}, \Lambda_{\mathbf{G}}) \quad (32)$$

where

$$p(\mathbf{Z}|\mathbf{T}_k, \mathbf{A_G}, \Lambda_{\mathbf{G}}) = \frac{1}{\pi^{LN_D}\det\left(\Sigma_{\mathbf{G}}\right)^L}\exp\left(-\text{Tr}\left(\Sigma_{\mathbf{G}}^{-1}\bar{\mathbf{Z}}\bar{\mathbf{Z}}^\dagger\right)\right), \quad (33)$$

$\bar{\mathbf{Z}} = \mathbf{Z} - \mathbf{A}_{\mathbf{G}} p_t \mathbf{T}_k$, and $\Sigma_{\mathbf{G}} = p_{\text{AN}}^2 \Lambda_{\mathbf{G}} \Lambda_{\mathbf{G}}^{\dagger} + \sigma_{\text{e}}^2 \mathbf{I}_{N_A}$. The maximization in (32) can be recast as a hypothesis testing problem consisting of $|\mathcal{K}|$ hypotheses corresponding to each possible key. The optimal test and equivalent ML detector in this case is given by a bank of $|\mathcal{K}|$ generalized matched filters (GMF) that are tuned to the tags from each possible key, i.e., tuned to each $\mathbf{T}_k = g(\hat{\mathbf{S}}, k)$ for all $k \in \mathcal{K}$. The final key is then chosen by the tag associated with the GMF with the largest output.[2]

Eve uses multiple observations of Alice's transmissions in order to gain a satisfactory amount of information about the key to launch a successful attack. For multiple observations, the optimal test maintains a similar structure, but where outputs are summed across each observation such that each MF bank consists of a separate stage for each observation. The test consists of concatenating all observations and then matching it with filters that are each tuned to a concatenation of tags created from a given key and each observed message $\mathbf{S}_i$. The maximum output determines the most likely key. Since GMFs prewhiten the noise, the test remains optimal by accounting for the varying channel quality of each observation by essentially weighing the better channels more than the poorer channels in the final summations.

More formally, let $\mathbf{Z}_i$ denote the i^{th} observation and let $\mathbf{G}_i$, and $\hat{\mathbf{H}}_i$ be its corresponding realizations of the adversarial channel and main channel estimate for each observation, respectively. Then, let $\mathbf{Z} = \{\mathbf{Z}_i\}_{1 \le i \le N_o}$, $\mathbf{G} = \{\mathbf{G}_i\}_{1 \le i \le N_o}$, and $\hat{\mathbf{H}} = \{\hat{\mathbf{H}}_i\}_{1 \le i \le N_o}$ now represent the collection of channel realizations for observations 1 to N_o. Then, Eve's procedure using N_o observations gives the key estimate

$$\hat{k} = \arg\max_k T_k(\mathbf{Z}|\mathbf{G}, \hat{\mathbf{H}}), \tag{34}$$

where

$$T_k(\mathbf{Z}|\mathbf{G}, \hat{\mathbf{H}}) = \sum_{i=1}^{N_o} \Re\left[\text{Tr}\left(\mathbf{Z}_i^{\dagger} \Sigma_{\mathbf{G}_i}^{-1} \tilde{\mathbf{T}}_{k,i}\right)\right] \tag{35}$$

is the sum of GMFs tuned to $\tilde{\mathbf{T}}_{k,i} = \mathbf{A}_{\mathbf{G}_i} p_t \mathbf{T}_{k,i}$ with $\mathbf{T}_{k,i} = g(\hat{\mathbf{S}}_i, k)$ being the expected tag for key k and message $\hat{\mathbf{S}}_i$ precoded according to the given channel $\mathbf{G}_i$ and channel estimate $\hat{\mathbf{H}}_i$. Since we follow the information-theoretic approach to security where Eve has unlimited computational power, we do not consider the complexity of such an estimator, but can compute its expected performance to determine the security of the framework.

In order for the estimator in (34) to produce the correct key, the output of the statistic attributed to the correct key, $T_k^{\text{valid}}(\mathbf{Z}|\mathbf{G}, \hat{\mathbf{H}})$, must be larger than the output of all $|\mathcal{K}| - 1$ other keys. Since we model the key and tags as being uniformly and independently chosen in (1), the expected probability of correct key recovery for a given collection of channels, averaged over all possible keys, is given by

$$P_K(\mathbf{G}, \hat{\mathbf{H}}) = \int_{-\infty}^{\infty} p\left(T_k(\mathbf{Z}|\mathbf{G}, \hat{\mathbf{H}}) \middle| k = k^{\text{valid}}\right) \cdot P^{|\mathcal{K}|-1}\left(T_k(\mathbf{Z}|\mathbf{G}, \hat{\mathbf{H}}) \middle| k \neq k^{\text{valid}}\right) dT_k, \tag{36}$$

where $p(T_k|k = k^{\text{valid}})$ is the PDF of (35) when $k = k^{\text{valid}}$ and $P(T_k|k \neq k^{\text{valid}})$ is the CDF of (35) for an incorrect key $k \neq k^{\text{valid}}$. Since the distribution of $\mathbf{Z}$ in (31) is complex Gaussian for both cases and the GMF is a linear transformation, the resulting test statistic (35) is also Gaussian. The mean and variance of (35) when $k \neq k^{\text{valid}}$ are

$$\begin{aligned} &E\left[T_k(\mathbf{Z}|\mathbf{G}, \hat{\mathbf{H}}) \middle| k \neq k^{\text{valid}}\right] \\ &\quad = \mu_{0,\text{e}} = 0 \end{aligned} \tag{37}$$

$$\begin{aligned} &\text{var}\left(T_k(\mathbf{Z}|\mathbf{G}, \hat{\mathbf{H}}) \middle| k \neq k^{\text{valid}}\right) \\ &\quad = \sigma_{0,\text{e}}^2 \\ &\quad = \sum_{i=1}^{N_o} \frac{1}{2} \text{Tr}\left(\Sigma_{\mathbf{G}_i}^{-1} \tilde{\mathbf{T}}_{k^{\text{valid}},i} \tilde{\mathbf{T}}_{k^{\text{valid}},i}^{\dagger}\right) \\ &\qquad + \frac{1}{2} \text{Tr}\left(p_t^2 \Sigma_{\mathbf{G}_i}^{-1} \mathbf{A}_{\mathbf{G}_i} \mathbf{A}_{\mathbf{G}_i}^{\dagger} \Sigma_{\mathbf{G}_i}^{-1} \tilde{\mathbf{T}}_{k^{\text{valid}},i} \tilde{\mathbf{T}}_{k^{\text{valid}},i}^{\dagger}\right), \end{aligned} \tag{38}$$

while for the correct tag they are [43]

$$\begin{aligned} &E\left[T_k(\mathbf{Z}|\mathbf{G}, \hat{\mathbf{H}}) \middle| k = k^{\text{valid}}\right] \\ &\quad = \mu_{1,\text{e}} \\ &\quad = \sum_{i=1}^{N_o} \text{Tr}\left(\Sigma_{\mathbf{G}_i}^{-1} \tilde{\mathbf{T}}_{k^{\text{valid}},i} \tilde{\mathbf{T}}_{k^{\text{valid}},i}^{\dagger}\right) \end{aligned} \tag{39}$$

$$\begin{aligned} &\text{var}\left(T_k(\mathbf{Z}|\mathbf{G}, \hat{\mathbf{H}}) \middle| k = k^{\text{valid}}\right) \\ &\quad = \sigma_{1,\text{e}}^2 \\ &\quad = \sum_{i=1}^{N_o} \frac{1}{2} \text{Tr}\left(\Sigma_{\mathbf{G}_i}^{-1} \tilde{\mathbf{T}}_{k^{\text{valid}},i} \tilde{\mathbf{T}}_{k^{\text{valid}},i}^{\dagger}\right) \\ &\quad = \frac{1}{2} \mu_{1,\text{e}}. \end{aligned} \tag{40}$$

Therefore,

$$p\left(T_k(\mathbf{Z}|\mathbf{G}, \hat{\mathbf{H}}) \middle| k = k^{\text{valid}}\right) = \phi\left(\frac{T - \mu_{1,\text{e}}}{\sigma_{1,\text{e}}}\right) \tag{41}$$

$$P\left(T_k(\mathbf{Z}|\mathbf{G}, \hat{\mathbf{H}}) \middle| k \neq k^{\text{valid}}\right) = \Phi\left(\frac{T - \mu_{0,\text{e}}}{\sigma_{0,\text{e}}}\right), \tag{42}$$

where $\phi(\cdot)$ and $\Phi(\cdot)$ are the PDF and CDF of the standard normal distribution, respectively. The final expected probability of correct key recovery using (34) is

$$P_K(\mathbf{G}, \hat{\mathbf{H}}) = \int_{-\infty}^{\infty} \phi\left(\frac{T - \mu_{1,\text{e}}}{\sigma_{1,\text{e}}}\right) \Phi^{|\mathcal{K}|-1}\left(\frac{T - \mu_{0,\text{e}}}{\sigma_{0,\text{e}}}\right) dT. \tag{43}$$

Numerical examples will be given in Section V-B

V. Numerical Results

We now present numerical results to show the advantages of utilizing artificial noise in the fingerprint embedding framework for MIMO communications even when channel

[2]We assume that $\mathbf{S}$ is recovered correctly by Eve, otherwise, the computed tags used in Eq. (32) will be incorrectly reconstructed. In practice, though, the addition of AN will induce more decoding errors at Eve resulting in improperly tuned GMFs. When this occurs, Eve's key uncertainty will be larger than what is presented here. This is an additional indirect security benefit of AN.

TABLE I

PARAMETERS FOR EVE PERFORMANCE RESULTS (UNLESS OTHERWISE SPECIFIED)

Parameter	Description	Value
N_T	# of transmit antennas	4
N_R	# of receive antennas	4
N_A	# of adversary antennas	4
$\sigma^2_{\mathbf{E}}$	Channel error variance	0.1
p^2_w	Artificial noise allocation	0.1
P_0	Transmit power constraint	14 dB
L	Number of Message Symbols	1024
κ	# of key bits	512
P_{FA}	False alarm probability	10^{-4}
P_D	Bob Probability of detection	0.999
p^2_t	Tag power allocation	-
N_D	# of data dimensions	-
AM	All mode embedding	-
SM	Strongest mode embedding	-

state information isn't known perfectly. We will compare the performance of the different tag detection approaches proposed in Section III and the perfect CSI optimal estimation approach proposed for the adversary in Section IV. While performance is calculated numerically for a given channel instance, the expected performance over different channel realizations is found using Monte Carlo methods. For all presented plots, a 4×4 MIMO system will be considered and relevant parameters are given above each plot or in the legend. The more interesting and relevant parameters will be referenced in the text. We consider normalized CWGN where $\sigma^2_{\text{b}} = 1$ so that transmit SNR is solely controlled by P_0. Although the channel estimation error is related to the transmit power and the resulting SNR for the pilots at the receiver, we will assume that $\sigma^2_{\mathbf{E}}$ is constant and independent of P_0 for simplicity. Finally, we consider the case where $\mathbf{H}$ and $\mathbf{G}$ are independent and are both i.i.d. zero-mean complex Gaussian distributed with unit variance. Please refer ahead to Table I for a reminder on parameter notation and descriptions.

A. Legitimate Receiver Authentication/Detection Performance

We begin with demonstrating the impact of imperfect CSI on Bob's tag detection performance for two different levels of channel uncertainty where $\sigma^2_{\mathbf{E}} = 0.1$ represents moderate channel estimation error and $\sigma^2_{\mathbf{E}} = 0.5$ represent severe estimation error. The performance of all three tests with increasing transmit power can be found in Figure 2. Since we consider a 4×4 MIMO system, there is no null space over which to transmit the AN. In this case, AN is transmitted over the weakest mode while the data is transmitted over the remaining $N_D = 3$ modes. Additionally, the tag is embedded on all N_D data modes. For $\sigma^2_{\mathbf{E}} = 0.1$, the RMF is fairly close in performance to the optimal perfect CSI matched filter, but suffers greatly from increased error and performs worse than the GLRT at high P_0. The GLRT is less affected by additional uncertainty, but still performs poorly compared to the perfect CSI case.

Next, in Figure 3, we compare the two tag embedding approaches and examine how the number of AN dimensions affects detection. The performance of the AM embedding approach is depicted by the dashed line while the SM approach is depicted by both the solid and dotted curves. The dotted

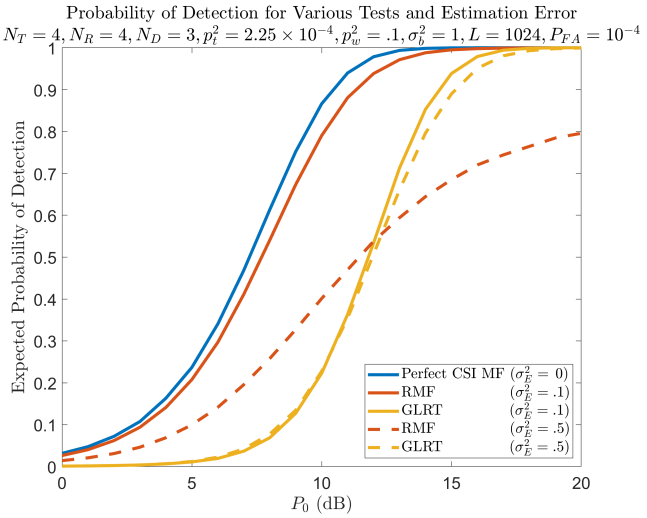

Fig. 2. Transmit SNR versus probability of detection/authentication. The robust matched filter is affected more by increased channel estimation error than the GLRT, but is close to the optimal perfect CSI performance for lower $\sigma^2_{\mathbf{E}}$. GLRT generally performs worst except at higher $\sigma^2_{\mathbf{E}}$ and P_0.

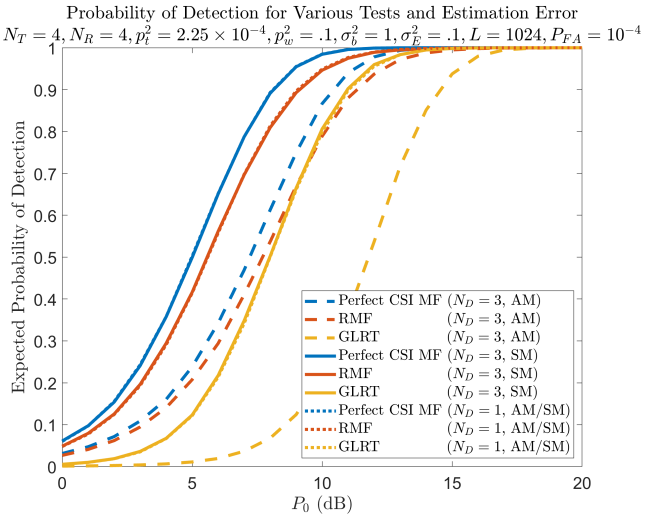

Fig. 3. Transmit SNR versus probability of detection/authentication. Embedding the tag in the strongest eigenmode produces better detection performance.

curve differs from the solid curve in that more dimensions are allocated towards AN rather than data. The similarity in performance between the two show that spreading the AN across more dimensions does not affect Bob's performance. This is useful since increasing the AN dimensions decreases Eve's ability to recover the key, so we can do this freely. The results also show that in this scenario, the strongest mode only approach has better detection performance for a given p_t^2.

B. Security Performance (Adversary Performance)

Next, we evaluate the security of the framework which is quantified by the performance of the adversary's key estimator. The main metric is the key lifespan which is the number of observations the adversary requires before her probability of successful key recovery exceeds the desired false alarm probability, P_{FA}. Note that in the noiseless case, a computationally unlimited adversary will recover the key

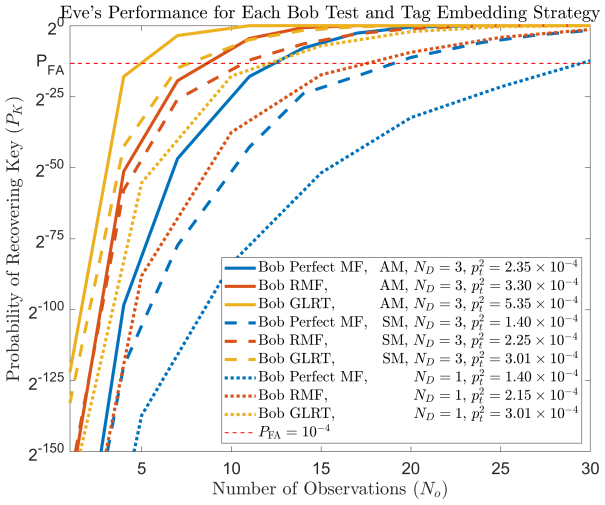

Fig. 4. Number of observations versus probability of successful key recovery. For constant P_D with appropriately adjusted p_t^2, the strongest mode only embedding strategy has superior security performance. As expected, the less CSI knowledge Bob has, the lesser the key lifespan. More AN dimensions universally increases security.

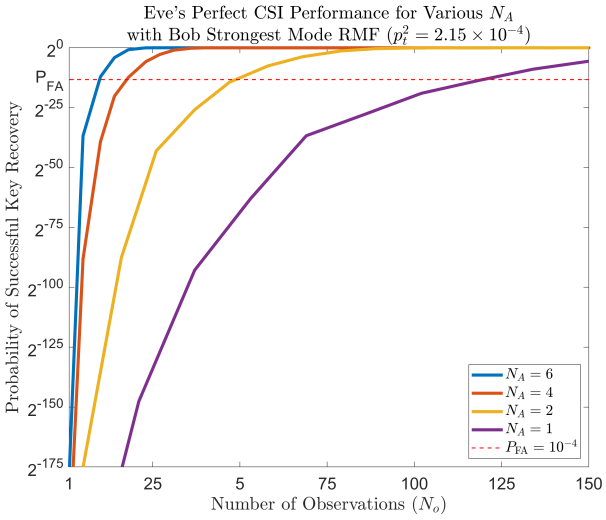

Fig. 5. Number of observations versus probability of successful key recovery. Eve's number of antennas greatly affects her ability to recover the key from observations.

perfectly with only one observation since the tag generating function is one-to-one with high probability when $|\mathcal{K}| < |\mathcal{T}|$, where $|\mathcal{T}|$ is the total number of possible tags. In other words, the key lifespan is only 1 for a traditional (non-embedded) HMAC since the noiseless tag uniquely identifies the key. The goal of this section is to determine if AN is still effective when only imperfect CSI is available and how it affects the rate vs. security trade-off. To fairly compare the security performance for Bob's different detection schemes and embedding strategies, we adjust p_t^2 for each case such that Bob's probability of detection always remains at $P_D = 0.999$. This leads to some interesting conclusions regarding the better embedding strategy. The appropriate p_t^2 is found using the bisection method. Table I contains the other parameters values that were used to obtain the discussed results unless otherwise specified.

First, in Figure 4, we compare the key lifespans for the two different tag embedding strategies and all three of Bob's tests. The first two sets of curves are the case when $N_D = 3$ in which AN is only transmitted along one dimension whereas the last set of three curves are the case where $N_D = 1$ in which data is sent over only one dimension and AN over three. The tag embedding strategy of the last set isn't denoted since the two provided strategies are equivalent when $N_D = 1$ in which only 1 dimension is available for embedding. The plot contains two fairly obvious results, but also one surprising result. The first result is that as Bob's CSI knowledge worsens (switches from RMF to GLRT), he must increase p_t^2 in order to maintain $P_D = 0.999$, thus leaking more key information to Eve. The second result is that transmitting AN over more dimensions increases the lifespan of the key as seen by comparing the $N_D = 3$ curves with the $N_D = 1$ curves. This increase, though, comes with the caveat of reduced data rate since data dimensions are sacrificed to accommodate the AN.

Finally, the surprising result in Figure 4 is that the SM tag embedding strategy has superior security to the AM strategy. The result is surprising since for the straightforward MIMO system without AN, it was concluded in [17] that for constant p_t^2, SM favors detection while AM favors security. But, if instead P_D is held constant as it is here, SM becomes more favorable in both cases as demonstrated in the plot. Intuitively, spreading the tag over more dimensions should make Eve's problem more difficult, but the better detection afforded by SM allows Alice to transmit using a lower p_t^2 for the same P_D. That decrease is tag power then hinders Eve's ability to recover the key to a greater extent than any increase in the number of dimensions of the tag. Therefore, for the same P_D, the SM strategy outperforms the AM strategy in terms of key security.

Next, Figure 5 shows the varying levels of security depending on the number of antennas with which Eve, or a group of colluding Eves, is equipped. Naturally, the fewer antennas, the harder it is for Eve to recover the key. For example, in the case of $N_A = 1$, the 512-bit key can be used approximately 140 times before being deemed vulnerable, a great improvement over previous results. Alice and Bob must be careful in their calculation of the key lifespan, though, since it relies on knowledge of Eve's antenna count which is the assumption made here. For all other plots, we assume that $N_A = N_T = 4$ since in order to impersonate Alice, Eve would most likely desire at least the same number of antennas as Alice.

Finally, Figure 6 shows the decaying effectiveness of AN when the channel estimate is poor. In fact, allocating additional AN power does not necessarily always increase security when Bob uses the RMF for constant $P_D = 0.999$. In this case, when $\sigma_{\mathbf{E}}^2 = 0.1$, even though allocating additional power towards AN initially increases the key lifespan, it eventually begins to decrease it. This is due to the fact that the increase in p_t^2 required to compensate for the leaked AN in Bob's observation outweighs the advantage of having additional AN in Eve's signal. When compared to the no AN case, though, adding AN does not decrease security at any point in this case, but makes it less effective at higher power allocations. For $\sigma_{\mathbf{E}}^2 = 0$ and $\sigma_{\mathbf{E}}^2 = 0.01$, on the other hand, increasing p_w^2 always increases the key lifespan. However, it is less effective for $\sigma_{\mathbf{E}}^2 = 0.01$.

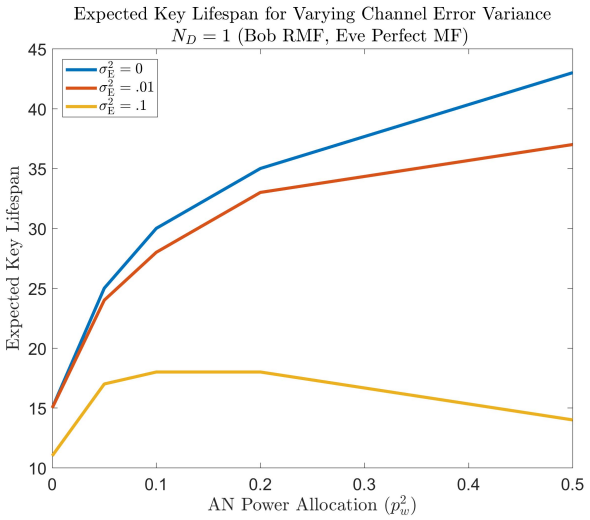

Fig. 6. Key lifespan versus AN power allocation for different quality of channel estimate. Additional AN does not necessarily increase security performance.

Finding the optimal p_w^2 for such a case, as in $\sigma_{\mathbf{E}}^2 = 0.1$, is the subject of future research.

VI. Conclusion

Although perfect CSI knowledge is required for perfect cancellation of artificial noise at the intended receiver, the authentication process can be made robust to imperfect CSI and the resulting AN leakage. The results presented here show that great security gains can still be obtained for the fingerprint embedding framework for MIMO systems even with the practical assumption of channel estimation errors. We show it is better to transmit the tag over a single mode rather than over all modes for constant P_{D} and that allocating additional AN power does not always increase the key lifespan. In fact, increasing the power allocation of AN can sometimes decrease the key lifespan which is a surprising result. Our numerical results indicate that there are desirable operating regimes that effectively utilize AN to allow users to maximize the use of a single key while guaranteeing the security of the system. The new security analysis precisely tracks Eve's knowledge of the key such that Alice and Bob can determine when key refreshes are necessary to maintain the desired level of security. Furthermore, Eve's probability of recovering the key is related to her min-entropy of the key which has possible future application in privacy amplification. Finally, although not analyzed here, the increase in AN also has the potential to cause errors in the adversary's decoding of $\mathbf{S}$ which disrupts their construction of their key recovery algorithm since the tags will not be reconstructed properly.

Acknowledgment

The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

References

[1] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008.
[2] L. Lai, H. El Gamal, and H. V. Poor, "Authentication over noisy channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 906–916, Feb. 2009.
[3] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over MIMO fading wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2564–2573, Jul. 2012.
[4] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016.
[5] P. L. Yu, B. M. Sadler, G. Verma, and J. S. Baras, "Fingerprinting by design: Embedding and authentication," in *Digital Fingerprinting*, C. Wang, R. M. Gerdes, Y. Guan, and S. K. Kasera, Eds. Cham, Switzerland: Springer, 2016, pp. 69–88.
[6] L. Xiao, T. Chen, G. Han, W. Zhuang, and L. Sun, "Game theoretic study on channel-based authentication in MIMO systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7474–7484, Aug. 2017.
[7] N. Wang, T. Jiang, S. Lv, and L. Xiao, "Physical-layer authentication based on extreme learning machine," *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1557–1560, Jul. 2017.
[8] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2260–2273, Mar. 2019.
[9] J. Perazzone, E. Graves, P. Yu, and R. Blum, "Inner bound for the capacity region of noisy channels with an authentication requirement," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2018, pp. 126–130.
[10] O. Kosut and J. Kliewer, "Authentication capacity of adversarial channels," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Nov. 2018, pp. 1–5.
[11] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.
[12] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," *J. Comput. Syst. Sci.*, vol. 22, no. 3, pp. 265–279, Jun. 1981.
[13] G. J. Simmons, "Authentication theory/coding theory," in *Proc. Adv. Cryptol.*, Santa Barbara, CA, USA, Aug. 1984, pp. 411–431.
[14] U. Rosenbaum, "A lower bound on authentication after having observed a sequence of messages," *J. Cryptol.*, vol. 6, no. 3, pp. 135–156, Mar. 1993.
[15] B. Smeets, "Bounds on the probability of deception in multiple authentication," *IEEE Trans. Inf. Theory*, vol. 40, no. 5, pp. 1586–1591, Sep. 1994.
[16] G. Verma, P. Yu, and B. M. Sadler, "Physical layer authentication via fingerprint embedding using software-defined radios," *IEEE Access*, vol. 3, pp. 81–88, 2015.
[17] P. L. Yu and B. M. Sadler, "MIMO authentication via deliberate fingerprinting at the physical layer," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 606–615, Sep. 2011.
[18] J. B. Perazzone, P. L. Yu, B. M. Sadler, and R. S. Blum, "Fingerprint embedding authentication with artificial noise: MISO regime," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 1–5.
[19] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE Veh. Technol. Conf.*, Dec. 2005, vol. 62, no. 3, p. 1906.
[20] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[21] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
[22] X. Wu, Z. Yang, C. Ling, and X.-G. Xia, "Artificial-Noise-Aided message authentication codes with information-theoretic security," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1278–1290, Jun. 2016.
[23] X. Wu, Z. Yang, C. Ling, and X.-G. Xia, "Artificial-Noise-Aided physical layer phase challenge-response authentication for practical OFDM transmission," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6611–6625, Oct. 2016.
[24] J. K. Tugnait, "Using artificial noise to improve detection performance for wireless user authentication in time-variant channels," *IEEE Wireless Commun. Lett.*, vol. 3, no. 4, pp. 377–380, Aug. 2014.
[25] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[26] M. Walker, "Information-theoretic bounds for authentication schemes," *J. Cryptol.*, vol. 2, no. 3, pp. 131–143, Jan. 1990.
[27] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1350–1356, Jul. 2000.

[28] A. Beemer, O. Kosut, J. Kliewer, E. Graves, and P. Yu, "Authentication against a myopic adversary," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 1–5.
[29] O. Gungor and C. E. Koksal, "On the basic limits of RF-Fingerprint-Based authentication," *IEEE Trans. Inf. Theory*, vol. 62, no. 8, pp. 4523–4543, Aug. 2016.
[30] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
[31] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
[32] A. Hyadi, Z. Rezki, and M.-S. Alouini, "An overview of physical layer security in wireless communication systems with CSIT uncertainty," *IEEE Access*, vol. 4, pp. 6121–6132, 2016.
[33] Z. Rezki, A. Khisti, and M.-S. Alouini, "On the secrecy capacity of the wiretap channel with imperfect main channel estimation," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3652–3664, Oct. 2014.
[34] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y.-W.-P. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 901–915, Mar. 2011.
[35] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Trans. Commun.*, vol. 63, no. 8, pp. 2959–2971, Aug. 2015.
[36] M. Pei, J. Wei, K.-K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 544–549, Feb. 2012.
[37] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.
[38] P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 38–51, Mar. 2008.
[39] T. Yoo and A. Goldsmith, "Capacity and power allocation for fading MIMO channels with channel estimation error," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2203–2214, May 2006.
[40] E. Telatar, "Capacity of multi-antenna Gaussian channels," *Eur. Trans. Telecommun.*, vol. 10, no. 6, pp. 585–595, Nov. 1999.
[41] B. K. Chalise and B. M. Sadler, "Joint data and tag precoder optimization for MIMO physical layer authentication with embedded fingerprinting," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 1–5.
[42] T. M. Cover and J. A. Thomas, *Elements Information Theory*. Hoboken, NJ, USA: Wiley, 2012.
[43] S. M. Kay, "Fundamentals of statistical signal processing, volume II:, Detection theory," in *Signal Processing*. Upper Saddle River, NJ, USA: Prentice-Hall, 1998.
[44] S. S. Wilks, "The large-sample distribution of the likelihood ratio for testing composite hypotheses," *Ann. Math. Stat.*, vol. 9, no. 1, pp. 60–62, Mar. 1938.
[45] A. De Maio and M. Lops, "Design principles of MIMO radar detectors," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 43, no. 3, pp. 886–898, Jul. 2007.
[46] J. B. Perazzone, P. L. Yu, B. M. Sadler, and R. S. Blum, "Physical layer authentication via fingerprint embedding: Min-entropy analysis : Invited presentation," in *Proc. 53rd Annu. Conf. Inf. Sci. Syst. (CISS)*, Mar. 2019, pp. 1–6.

Jake Bailey Perazzone (Student Member, IEEE) received the B.S. degree in electrical engineering from The College of New Jersey, Ewing, NJ, USA, in 2015, and the M.S. and Ph.D. degrees in electrical engineering from Lehigh University, Bethlehem, PA, USA, in 2017 and 2020, respectively. He is currently a Post-Doctoral Researcher with the Computational and Information Sciences Directorate, U.S. Army Research Laboratory (ARL), Adelphi, MD, USA. His research interests include signal processing, wireless security, and distributed analytics in tactical networks. He was a recipient of the Graduate Assistance in Areas of National Need (GAANN) Fellowship.

Paul L. Yu (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Maryland at College Park, College Park. He is currently an Electronics Engineer with the U.S. Army Research Laboratory (ARL). His research interests include signal processing and security for wireless tactical networking. He has several patents in these areas.

Brian M. Sadler (Life Fellow, IEEE) received the B.S. and M.S. degrees from the University of Maryland at College Park, College Park, and the Ph.D. degree from the University of Virginia, Charlottesville, all in electrical engineering. He is currently the U.S. Army Senior Scientist for Intelligent Systems and a fellow of the U.S. Army Research Lab (ARL), Adelphi, MD, USA. He has more than 400 publications in these areas with 17,000 citations and h-index of 56. His research interests include information science and networked collaborative autonomous intelligent systems. He received Best Paper Awards from the IEEE Signal Processing Society in 2006 and 2010, several ARL and Army R/D awards, and the 2008 Outstanding Invention of the Year Award from the University of Maryland. He was a General Co-Chair of the IEEE GlobalSIP'16. He has been an Associate Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING, the IEEE SIGNAL PROCESSING LETTERS, and *EURASIP Signal Processing*, and a Guest Editor for several journals including the IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING (JSTSP), the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (JSAC), the IEEE TRANSACTIONS ON ROBOTICS (T-RO), the *IEEE SP Magazine*, *Autonomous Robots*, and the *International Journal of Robotics Research*. He was and the IEEE Signal Processing Society Distinguished Lecturer from 2017 to 2018 and an IEEE Communications Society Distinguished Lecturer from 2020 to 2021.

Rick S. Blum (Fellow, IEEE) received the B.S. degree in electrical engineering from Pennsylvania State University in 1984 and the M.S. and Ph.D. degrees in electrical engineering from the University of Pennsylvania in 1987 and 1991, respectively.

From 1984 to 1991, he was a Member of Technical Staff with General Electric Aerospace, Valley Forge, PA, USA. He graduated from GE's Advanced Course in Engineering. Since 1991, he has been with the Electrical and Computer Engineering Department, Lehigh University, Bethlehem, PA, USA, where he is currently a Professor and holds the Robert W. Wieseman Endowed Professorship in electrical engineering. He holds several patents. His research interests include signal processing for security, smart grid, communications, sensor networking, radar, and sensor processing.

Dr. Blum was a member of the SAM Technical Committee (TC) of the IEEE Signal Processing Society. He was a member of the Signal Processing for Communications TC of the IEEE Signal Processing Society and is a member of the Communications Theory TC of the IEEE Communication Society. He was on the awards Committee of the IEEE Communication Society. He is an IEEE Third Millennium Medal winner, Eleanor and Joseph F. Libsch Research Award winner, and a member of Eta Kappa Nu and Sigma Xi. He was awarded an ONR Young Investigator Award in 1997 and an NSF Research Initiation Award in 1992. His IEEE Fellow Citation "for scientific contributions to detection, data fusion and signal processing with multiple sensors" acknowledges contributions to the field of sensor networking. He was on the Editorial Board of the *Journal of Advances in Information Fusion* of the International Society of Information Fusion. He was an Associate Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING and of the IEEE COMMUNICATIONS LETTERS. He has edited special issues of the IEEE TRANSACTIONS ON SIGNAL PROCESSING, the IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING, and the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He served two terms as an IEEE Signal Processing Society Distinguished Lecturer.