Performance Analysis of Distributed SIMO Physical Layer Authentication

Henrik Forssell, Ragnar Thobaben, James Gross
Dept. of Information Science and Engineering, KTH Royal Institute of Technology
SE-100 44 Stockholm, Sweden
E-mail: {hefo, ragnart, jamesgr}@kth.se

***Abstract*—This paper proposes a new approach for physical layer authentication where transmissions are authenticated based on the single-input/multiple-output channel-states observed at multiple distributed antenna-arrays. The receiver operating characteristics (ROC) are derived in terms of closed form expressions for the false alarm and missed detection probability in order to evaluate the effectiveness compared to single-array authentication. To this end, we study the worst-case missed detection probability based on the optimal attacker position. Finally, we apply our previously developed queueing analytical tools, based on stochastic network calculus, in order to assess the delay performance impacts of the physical layer authentication scheme in a mission-critical communication scenario. Our results show that the distributed approach significantly outperforms single-array authentication in terms of worst-case missed detection probability and that this can help mitigating the delay performance impacts of authentication false alarms.**

I. Introduction

Authenticating transmissions at the physical layer (PHY) is an alternative method for fast and lightweight verification of transmitter identities and detection of impersonation attacks in wireless systems. The advantages of low security overhead and low complexity make such schemes interesting for many future use-cases in arising mission-critical machine type communications (MTC) where high reliability and low latency are key requirements [1].

A physical layer authentication scheme verifies the transmitter identity using hypothesis testing based on dedicated features of the communication pair, like e.g., the location-specific channel frequency response [2], received signal strength, or multiple-antenna angle-of-arrival (AoA). Authentication based on diverse and multi-dimensional features provides security in the sense that estimation and impersonation of the legitimate transmitter features is very difficult which, in contrast to cryptographic techniques, does not presuppose any computational limitations of the attacker. On the other hand, physical layer authentication schemes suffer from inevitable false alarms which might require retransmissions that could be detrimental in delay critical applications.

In our previous work [3], we studied the detection and delay performance of physical layer authentication in a MTC network with a multiple-antenna access point for various attack strategies based on queueing theory and stochastic network calculus [4]. This work concluded that, compared to the single-antenna case, introducing 4-8 receiver antennas significantly improved both detection rate and delay performance. However, we also observed a degradation in the detection performance for certain attacker positions due to the inability of the linear receive array to distinguish between transmissions from similar AoAs. In this work, we resolve this problem by introducing physical layer authentication based on multiple spatially distributed antenna arrays. By characterizing the detection performance with closed form expressions, we are able to quantify the benefits of the distributed approach over a conventional deployment and to provide important insights into deployment strategies.

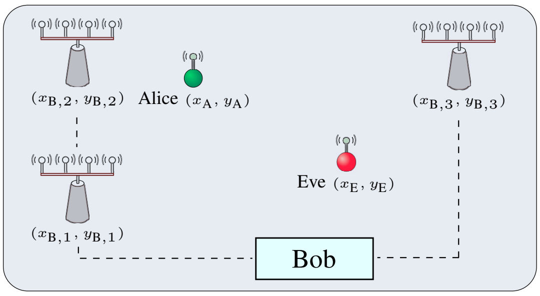
To the best of our knowledge, distributed physical layer authentication has only been studied in [5] where multiple receivers forward the observed, possibly compressed, features which are then authenticated by a central processing unit. Our work differs from [5] in that we consider multiple antennas at each receiver, spatial modeling of the physical layer channels, and the delay impacts in a mission-critical communication scenario. Applying physical layer authentication for mission-critical MTC was first mentioned in [1]. However, this work does not consider the authentication-induced delays that are highly relevant in such scenarios. Furthermore, queuing theory has been employed for studying delay impacts of physical layer security techniques in [6–8]; however, besides our own work in [3, 9], none has studied the impact of authentication delays.

In order to be able to characterize the benefits of the distributed antenna array architecture proposed in this paper, we provide as one of our main contributions a closed form expression for the missed detection probability, given as a series expansion in terms of non-central χ^2 distributions. To get a location independent metric for the detection performance, we introduce the worst-case missed detection rate based on an optimally positioned attacker. We furthermore combine the derived detection performance results with our previously developed delay analysis tools in [3] in order to assess the baseline delay performance impacts of the scheme with the attacker remaining inactive. Our results show that distributing antenna arrays significantly improves the performance of physical layer authentication for a fixed total number of receive antennas, both in terms of security and delay performance impacts.

This paper is organized as follows: Section II introduces the system model, the proposed distributed physical layer authentication scheme, and the problem formulation. Section III analyses the authentication scheme in terms of false alarm probability, missed detection probability, and worst-case missed detection probability. Section IV introduces the queueing and delay analysis tools employed in [3] and its application in this paper. Section V provides numerical results studying the performance under different deployment scenarios. Finally, the paper is concluded in Section VI.

Notation: We let $\mathbf{X}$, $\mathbf{X}^T$, $\mathbf{X}^\dagger$, and $\operatorname{tr}(\mathbf{X})$ denote matrices, their transpose, conjugate transpose, and trace, $\mathbf{I}_N$ denotes the $(N \times N)$ identity matrix, and bold symbols $\mathbf{x}$ represent vectors with entries x_i. The operation $\|\mathbf{x}\| = \sqrt{|x_1|^2 + \ldots + |x_n|^2}$ represents the Euclidian norm. For an event E, we let $\mathbb{P}(E)$ and $\mathbb{I}(E)$ denote the probability and indicator function, respectively, and for a random variable X, $\mathbb{E}[X]$ denotes its expected value. By $\mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$, we denote the multivariate complex Gaussian distribution with mean $\boldsymbol{\mu}$ and covariance matrix $\boldsymbol{\Sigma}$. We denote by $\chi_k^2(\lambda)$ a non-central χ^2 distribution with k degrees of freedom and non-centrality parameter λ and let $F_{\chi^2}(k; \nu; x)$ and $f_{\chi^2}(k; \nu; x)$ denote its cumulative distribution function (CDF) and probability density function (PDF), respectively.

II. System Model and Physical Layer Authentication Scheme



$(x_{\mathrm{B},2}, y_{\mathrm{B},2})$
Alice $(x_{\mathrm{A}}, y_{\mathrm{A}})$
$(x_{\mathrm{B},3}, y_{\mathrm{B},3})$
Eve $(x_{\mathrm{E}}, y_{\mathrm{E}})$
$(x_{\mathrm{B},1}, y_{\mathrm{B},1})$
Bob

Fig. 1. System deployment consisting of central processing unit Bob equipped with distributed antenna arrays, legitimate single-antenna MTC device Alice, and adversary MTC device Eve.

As depicted in Fig. 1, we study a system consisting of a single-antenna device Alice positioned at (x_A, y_A), communicating uplink data to a central processing unit equipped with multiple antenna arrays, referred to as Bob. We propose a physical layer authentication scheme, described in detail in Section II-B, in which Bob verifies the legitimacy of the transmissions based on the line-of-sight (LOS) single-input/multiple output (SIMO) channel-states between the transmitter and the distributed antenna arrays. The adversary Eve, also depicted in Fig. 1, is a single antenna device positioned at (x_E, y_E) with the intention of impersonating Alice in order to communicate fraudulent messages to Bob. For the queueing analysis of a stream of authenticated messages from Alice to Bob, presented in detail in Section IV, we assume that a constant flow of data is arriving at a local buffer at Alice and that this data needs to be communicated to Bob within a strict delay deadline.

A. Line-of-Sight Channel Model

We assume that Bob is equipped with K_{a} linear antenna arrays consisting of N_{Rx} antennas each and that Alice has a line-of-sight path to each array. The line-of-sight paths are required for the proposed authentication scheme and may be considered a limitation. However, such assumptions also exist in related work, for instance for line-of-sight beamforming for secret key agreement [10]. The jth array is positioned at $(x_{B,j}, y_{B,j})$ and with horizontal rotation Θ_j. The channels are modeled as narrowband Rice fading SIMO channels, i.e., the complex channel vector from Alice to array j, denoted by $\mathbf{h}_{A,j}$, is modeled as a circular-symmetric complex Gaussian (CSCG) vector with mean denoted by $\boldsymbol{\mu}_{A,j}$ and covariance matrix by $\boldsymbol{\Sigma}_{A,j}$. The arrays are furthermore assumed to be spaced sufficiently far apart so that the channel realizations can be seen as independent (i.e., $\mathbf{h}_{A,j} \perp\!\!\!\perp \mathbf{h}_{A,j'}$ for $j \neq j'$). Denoting by $d_{A,j}$ and $\Phi_{A,j}$ the distance and angle-of-arrival from Alice w.r.t. array j, respectively, and assuming that $d_{A,j} \gg \lambda_c \Delta_r$ where Δ_r denotes the normalized antenna spacing, the channel mean $\boldsymbol{\mu}_{A,j}$ can be modeled as a phased array antenna

$$\boldsymbol{\mu}_{A,j} = A e^{-\frac{j2\pi d_{A,j}}{\lambda_c}} \mathbf{e}(\Omega_{A,j}), \tag{1}$$

where $\Omega_{A,j} = \sin(\Phi_{A,j})$ is the directional sine, $\mathbf{e}(\Omega) = \frac{1}{\sqrt{N_{\mathrm{Rx}}}} \left[z^0, z^\Omega, \cdots, z^{(N_{\mathrm{Rx}}-1)\Omega}\right]$ is the unit spatial signature in terms of the complex number $z = e^{-j2\pi\Delta_r}$, and $A = \sqrt{\frac{P_{A,j} N_{\mathrm{Rx}} K_{A,j}}{K_{A,j}+1}}$ with $K_{A,j}$ denoting the Rice factor. $P_{A,j} = P_0 d_{A,j}^{-\beta/2}$ is the received power per antenna element according to a path-loss model with exponent β and transmit power P_0. The array-specific covariance matrix is given by $\boldsymbol{\Sigma}_{A,j} = \sqrt{\frac{P_{A,j}}{K_{A,j}+1}} \boldsymbol{\Lambda}$ where $\boldsymbol{\Lambda}$ is a correlation matrix with unit diagonal so that $\mathbb{E}[\|\mathbf{h}_{A,j}\|^2] = P_{A,j}$. In this paper, we model the correlation matrix according to $\boldsymbol{\Lambda}_{A,j} = \mathbf{I}$, i.e., we assume that the antenna spacing is large enough so that no antenna correlation is present.

Adversary Assumptions: The channel from Eve to array j, denoted by $\mathbf{h}_{E,j} \sim \mathcal{CN}(\boldsymbol{\mu}_{E,j}, \boldsymbol{\Sigma}_{E,j})$, is modeled similarly to Alice's channels with $d_{E,j}$ and $\Phi_{E,j}$ denoting the distance and angle-of-arrival of Eve w.r.t. array j, respectively, and $K_{E,j}$ denoting the Rice factor. We assume that Eve transmits with the same power P_0 as Alice.

In the rest of this paper, we will let vector $\mathbf{h}$ with index j excluded denote the $(1 \times N_{\mathrm{Rx}} K_{\mathrm{a}})$ concatenated vector $\mathbf{h} = \begin{bmatrix}\mathbf{h}_1^T & \ldots & \mathbf{h}_{K_{\mathrm{a}}}^T\end{bmatrix}^T$, i.e., $\mathbf{h}_A$ and $\mathbf{h}_E$ represent the concatenated channel state from Alice and Eve, respectively, to all antenna arrays. For the CSCG mean and covariance matrices, we similarly let

$$\boldsymbol{\mu} = \begin{bmatrix} \boldsymbol{\mu}_1 \\ \vdots \\ \boldsymbol{\mu}_{K_{\mathrm{a}}} \end{bmatrix}, \quad \text{and} \quad \boldsymbol{\Sigma} = \begin{bmatrix} \boldsymbol{\Sigma}_1 & \mathbf{0} & \cdots & \mathbf{0}. \\ \mathbf{0} & \boldsymbol{\Sigma}_2 & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0}. & \cdots & \boldsymbol{\Sigma}_{K_{\mathrm{a}}} \end{bmatrix} \tag{2}$$

denote the concatenated mean and covariance matrix. The diagonal form of $\mathbf{\Sigma}$ is sufficient for our purposes since we assume that fading is independent between antenna arrays.

B. Physical Layer Authentication with Distributed Receive Arrays

Bob performs hypothesis testing to verify the identity of the source of each transmission. We denote the observed channel state at array j by $\tilde{\mathbf{h}}_j$ and let $\mathcal{H}_0$ represent the hypothesis that the distribution of $\tilde{\mathbf{h}}_j$ is parameterized by $\boldsymbol{\mu}_A$ and $\mathbf{\Sigma}_A$ (i.e., the transmission is legitimate), and $\mathcal{H}_1$ that $\tilde{\mathbf{h}}_j$ is parameterized by $\boldsymbol{\mu}_E$ and $\mathbf{\Sigma}_E$ (i.e., originating from the adversary). The legitimate distribution parameters $\boldsymbol{\mu}_{A,j}, \mathbf{\Sigma}_{A,j}$ are assumed to be available to Bob in a feature bank[1]. However, the distribution of Eve's channel remains unknown to Bob. To authenticate a new transmission, Bob constructs the concatenated vector $\tilde{\mathbf{h}}$, and given that the transmission is legitimate, Bob knows that $\tilde{\mathbf{h}}_j \sim \mathcal{CN}(\boldsymbol{\mu}_{A,j}, \mathbf{\Sigma}_{A,j})$. Consequently, Bob also knows that $\tilde{\mathbf{h}}|\mathcal{H}_0 \sim \mathcal{CN}(\boldsymbol{\mu}_A, \mathbf{\Sigma}_A)$.

Bob uses a generalized likelihood ratio test (GLRT)

$$d(\tilde{\mathbf{h}}) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} T, \tag{3}$$

with a threshold T as a design parameter and the discriminant function $d(\tilde{\mathbf{h}}) = 2(\tilde{\mathbf{h}} - \boldsymbol{\mu}_A)^\dagger \mathbf{\Sigma}_A^{-1}(\tilde{\mathbf{h}} - \boldsymbol{\mu}_A)$ that quantifies the similarity between the observation and the legitimate distribution [3]. If Bob decides $\mathcal{H}_0$, the transmission is considered authentic and the data is accepted. If Bob on the other hand decides $\mathcal{H}_1$, it is declared as a fraud and the data is rejected. We assume that Bob's decision is reported back to the transmitting device via an error free feedback channel.

Error events: There are two types of errors that can occur in the physical layer authentication scheme: i) a false alarm, when a legitimate message from Alice is rejected, and ii) a missed detection, when a fraudulent message from Eve is accepted. The probabilities of these events can mathematically be formulated as

$$\begin{aligned} &p_{\text{FA}}(T) = \mathbb{P}(d(\tilde{\mathbf{h}}) > T|\mathcal{H}_0) \quad \text{and} \\ &p_{\text{MD}}(T) = \mathbb{P}(d(\tilde{\mathbf{h}}) < T|\mathcal{H}_1). \end{aligned} \tag{4}$$

Bob can freely choose the authentication threshold T in (3). However, minimizing the false alarm and missed detection probabilities in (4) are generally two conflicting objectives.

C. Problem Formulation

In this paper we address two problems with respect to the proposed multiple antenna-array authentication scheme described in this section: i) we wish to characterize the detection performance in terms of false alarm and missed detection probabilities in closed form, and ii) we wish to evaluate the performance improvements from the proposed multiple antenna-array authentication scheme in terms of detection and delay performance. Problem i) arises due to the block structure of the covariance matrices in (2) which makes a straightforward extension of previous works for calculating the missed detection probability impossible. We solve this issue in Section III by a series expansion in terms of non-central χ^2 distributions. Problem ii) is addressed by combining the results from Section III with our previously developed delay analysis tools in [2], summarized in Section IV, and by illustrating the results in a numerical study for different deployment strategies in Section V.

III. Performance Analysis of Distributed Physical Layer Authentication

We begin this section by providing closed form expressions for the false alarm and missed detection probabilities in (4) for a given attacker distribution. Next, since a given distribution of Eve's channel is dependent on a specific attack position, we introduce the worst-case missed detection rate based on the optimal attack position outside a physical exclusion region.

A. False Alarm and Missed Detection Probabilities

The false alarm probability is given by the following proposition:

Proposition 1. *The false alarm probability in the test* (3) *with threshold T is given by*

$$p_{FA}(T) = 1 - F_{\chi^2}(2N_{Rx}K_a; 0; T), \tag{5}$$

Proof. The fact that under $\mathcal{H}_0$ we have $d(\tilde{\mathbf{h}}) \sim \chi^2_{2N_{\text{Rx}}K_{\text{a}}}(0)$ is a standard result, for instance proven in [11]. It is from this observation clear that $p_{\text{FA}}(T) = \mathbb{P}(d(\tilde{\mathbf{h}}) > T|\mathcal{H}_0)$ is given by (5). □

Next, we turn to the analysis of the missed detection probability which is more involved due to the spatial distribution of the antenna arrays. First, we provide a general expression for the missed detection probability given a particular attacker distribution in the following proposition:

Proposition 2. *The missed detection rate in the test* (3) *can be written in integral form*

$$p_{MD}(T) = \int \cdots \int_{\mathcal{Y}} \prod_{j=1}^{K_a} f_{\chi^2}(k_i, \nu_j, y_j) dy_j \cdots dy_{K_a}, \tag{6}$$

with $\mathcal{Y} = \{y_1, \cdots, y_{K_a}; \sum_{j=1}^{K_a} \alpha_j y_j < T\}$, $\alpha_j = \sqrt{\frac{P_{E,j}(K_{A,j}+1)}{P_{A,j}(K_{E,j}+1)}}$, $\nu_j = 2(\boldsymbol{\mu}_{E,j} - \boldsymbol{\mu}_{A,j})^\dagger \mathbf{\Sigma}_{E,j}^{-1}(\boldsymbol{\mu}_{E,j} - \boldsymbol{\mu}_{A,j})$, and $k_i = 2N_{Rx}$.

Proof. From the block structure of the covariance matrix in (2) it is trivial to see that

$$d(\tilde{\mathbf{h}}) = \sum_{j=1}^{K_{\text{a}}} 2(\tilde{\mathbf{h}}_j - \boldsymbol{\mu}_{A,j})^\dagger \mathbf{\Sigma}_{A,j}^{-1}(\tilde{\mathbf{h}}_j - \boldsymbol{\mu}_{A,j}). \tag{7}$$

Through the observation that $\mathbf{\Sigma}_{E,j} = \sqrt{\frac{P_{E,j}}{K_{E,j}+1}}\mathbf{\Lambda}$ and $\mathbf{\Sigma}_{A,j} = \sqrt{\frac{P_{A,j}}{K_{A,j}+1}}\mathbf{\Lambda}$, we get that $\mathbf{\Sigma}_{E,j} = \alpha_j \mathbf{\Sigma}_{A,j}$ with

[1] Such distributions can be obtained in a training phase or from channel prediction. However, the details of this process are omitted in this work.

$\alpha_j = \sqrt{\frac{P_{E,j}(K_{A,j}+1)}{P_{A,j}(K_{E,j}+1)}}$ and it is clear that $d(\tilde{\mathbf{h}}) = \sum_{j=1}^{K_\mathrm{a}} \alpha_j Y_j$ with $Y_j = 2(\tilde{\mathbf{h}}_j - \boldsymbol{\mu}_{A,j})^\dagger \boldsymbol{\Sigma}_{A,j}^{-1}(\tilde{\mathbf{h}}_j - \boldsymbol{\mu}_{A,j})$. It is straightforward to prove that Y_j is distributed according to $\chi^2_{2N_\mathrm{Rx}}(\nu_i)$ [3]. What remains is to note that $p_\mathrm{MD}(T) = \mathbb{P}(d(\tilde{\mathbf{h}}) < T|\mathcal{H}_1)$, i.e., $p_\mathrm{MD}(T) = \mathbb{P}(\sum_{j=1}^{K_\mathrm{a}} \alpha_j Y_j < T)$ which is given by (6) since the χ^2 random variables Y_j are independent. □

Solving the integral (6) is complicated except for the special case $\alpha_1 = \alpha_2, \cdots, \alpha_{K_\mathrm{a}} = \alpha$ which yields $d(\tilde{\mathbf{h}}) \sim \chi^2_{2N_\mathrm{Rx}K_\mathrm{a}}(\nu)$ with $\nu = \sum_{i=1}^{K_\mathrm{a}} \nu_i$ and the missed detection probability $p_\mathrm{MD}(T) = F_{\chi^2}(2N_\mathrm{Rx}K_\mathrm{a}; \nu; T)$. For the general case, we instead note that $p_\mathrm{MD}(T)$ is equivalent to the CDF of the weighted sum of non-central χ^2 given by $d(\tilde{\mathbf{h}}) = \sum_{j=1}^{K_\mathrm{a}} \alpha_j Y_j$ for which approximative solutions exist in previous literature. Approximate methods are based on inverse Laplace-transform of an approximate moment generating function [12], χ^2 approximations with cumulant matching [13], or truncated series expansions in terms of central χ^2 CDFs [14]. The latter approach is utilized to provide a closed form expression for the missed detection probability in the following theorem:

Theorem 1. *The missed detection rate in the test* (3) *can be written*

$$p_{MD}(T) = \sum_{i=0}^{\infty} c_i F_{2(i+\bar{k})}(y/\beta) \tag{8}$$

for any $0 < \beta \leq \min(\alpha_1, \cdots, \alpha_{K_a})$ *with* $\bar{k} = \sum_{i=0}^{K_a} k_i$, $\kappa_i = 1 - \beta/\alpha_i$, $g_k = N_{Rx} \sum_{i=0}^{K_a} \kappa_i^k + k/2 \sum_{i=0}^{K_a} \nu_i \kappa_i^{k-1}(1 - \kappa_i)$, $c_0 = \prod_{i=0}^{K_a} (\beta/\alpha_i)^{N_{Rx}} \exp(-1/2 \sum_{i=0}^{K_a} \nu_i)$, *and* $c_k = k^{-1} \sum_{r=0}^{k-1} g_{k-r} c_r$ *for* $k \geq 1$.

Proof. From Proposition 2, we know that $p_\mathrm{MD}(T) = \mathbb{P}(\sum_{j=1}^{K_\mathrm{a}} \alpha_j Y_j < T)$ with Y_j distributed according to $\chi^2_{k_i}(\nu_i)$. The series expansion (8) of its CDF is provided in Section VI in [14]. □

For a computable expression for the missed detection rate, we can truncate the sum in (8) and write $p_\mathrm{MD}^\mathrm{approx}(T) = \sum_{i=0}^{N} c_i F_{2(i+K_\mathrm{a}N_\mathrm{Rx})}(T/\beta)$. The truncation error $\epsilon(N) = p_\mathrm{MD}(T) - p_\mathrm{MD}^\mathrm{approx}(T)$ is shown in [14] to be bounded by

$$0 < \epsilon(N) \leq 1 - \sum_{k=1}^{N} c_k. \tag{9}$$

B. Worst-Case Missed Detection Probability

The derived missed detection rate is dependent on the particular position of Eve through the channel distribution and Eve can choose her position to optimize her success probability (e.g, a location close to Alice or with similar angle-of-arrival w.r.t. the receive array). Therefore, in this paper we adopt a worst-case detection performance metric based on a physical exclusion region[2] $\mathcal{R}(R) = \{(x, y) \in \mathbb{R}^2; (x - x_A)^2 + (y - y_A)^2 \leq R^2\}$ and let Eve optimize her position outside the exclusion region:

$$p_\mathrm{MD}^{(\max)}(T, R) = \max_{(x_E, y_E) \in \mathcal{R}(R)^\mathrm{c}} p_\mathrm{MD}(T, x_E, y_E). \tag{10}$$

In other words, $p_\mathrm{MD}^{(\max)}(T, R)$ captures the highest success-rate an adversary can achieve given that it cannot get closer to the legitimate device than a distance of R. Note that in this work, we only consider grid search methods for optimizing the attacker position.

IV. Queueing Analysis of Authentication Delays

Authentication false alarms during a stream of messages transmitted from Alice might cause unwanted retransmissions resulting in delays. In our previous work [3], we developed a queueing model taking the inevitable false alarms into account. In this section, we present how this analysis can be applied to the system model considered in this paper. For complete details, we refer the reader to [3]. We note that in this paper, the focus is on the baseline queueing performance on the single link from Alice to Bob and Eve is remaining inactive not interfering with the transmissions.

A. Queueing Modelling of Authentication Delays

We model a flow of data from Alice to Bob as a queueing system with a stochastic service process due to authentication false alarms and channel fading. The bivariate stochastic processes $A(\tau, t) = \sum_{k=\tau}^{t} a_k$ and $D(\tau, t) = \sum_{k=\tau}^{t} d_k$ represent the cumulative arrivals to and departures from the queue in the time interval $[\tau, t)$ for all $0 \leq \tau \leq t$. In frame k, a_k represents the instantaneous arrivals to Alice's buffer measured in bits, and d_k represents the instantaneous departures from the queue (i.e., information successfully received at Bob). The links ability to transfer data from the buffer at Alice to the destination at Bob is characterized by the cumulative service process $S(\tau, t) = \sum_{k=\tau}^{t} s_k$, where s_k represent the instantaneous service in frame k (i.e., the available resources for transmitting information bits over the wireless channel with error-free reception at Bob).

In this paper, we assume a frame based medium access scheme where the uplink grants transmission of M complex symbols in each frame. We consider a deterministic arrival process where $a_k = a$ bits arrive in each frame. The transmission in each frame is modeled by: i) Alice adopts a coding rate $R^{(k)}$ and encodes $MR^{(k)}$ information bits from the buffer that are transmitted over the channel, ii) Bob employs maximal ratio combining (MRC) using the received symbols from each antenna array, iii) Bob authenticates the transmission using the observed channel state $\mathbf{h}_A^{(k)}$ and reports the decision through an error-free feedback link. According to the channel model in Section II-A, the channel from Alice to Bob is a Rice fading SIMO channel with $\mathbf{h}_A^{(k)} \sim \mathcal{CN}(\boldsymbol{\mu}_A, \boldsymbol{\Sigma}_A)$ and we assume that the frame period is long enough such that $\mathbf{h}_A^{(k)}$ is i.i.d fading across frames. Given MRC at Bob, we adopt the Shannon capacity $R^{(k)} = \log\left(1 + \frac{\|\mathbf{h}_A^{(k)}\|^2}{N_0}\right)$ as a proxy for the adopted

[2] Obviously, $p_\mathrm{MD} \approx 1$ at positions very close to Alice where the channel distribution is close to the legitimate (i.e., $\boldsymbol{\mu}_E \approx \boldsymbol{\mu}_A$). The rationale behind this region is to exclude such points from Eve's choices.

rate in frame k where N_0 is AWGN noise power. Given these assumptions, the service model can be written as

$$s_k = \begin{cases} M \log\left(1 + \frac{\|\mathbf{h}_A^{(k)}\|^2}{N_0}\right), & \text{if } X_k \\ 0 & \text{if } X_k^{\mathsf{c}}, \end{cases} \tag{11}$$

where we let X_k denote the event that frame k is successfully authenticated (i.e., $\mathbb{P}(X_k = 0) = p_{\text{FA}}(T)$).

Delay performance can be evaluated through the delay violation probability

$$p(w) = \mathbb{P}(W(t) > w), \tag{12}$$

i.e., the probability the the delay exceeds a defined deadline w, where $W(t) \triangleq \inf\{u > 0; A(0,t) \leq D(0,t+u)\}$ represent the queueing delay at time t (i.e., the frames required to serve the bits in the queue at time t).

B. Delay Violation Bound Using Stochastic Network Calculus

Stochastic network calculus is a mathematical framework that allows us to analyze input-output relationships of stochastic queueing systems. The work in [15] developed the stochastic network calculus framework for wireless fading links by observing that the analysis can be conducted conveniently by converting the bivariate stochastic processes $A(\tau,t)$, $S(\tau,t)$ and $D(\tau,t)$ into $\mathcal{A}(\tau,t) \triangleq e^{A(\tau,t)}$, $\mathcal{S}(\tau,t) \triangleq e^{S(\tau,t)}$ and $\mathcal{D}(\tau,t) \triangleq e^{D(\tau,t)}$, referred to as the SNR-domain processes. Performance bounds are derived in terms of Mellin transforms, defined as $\mathcal{M}_X(s) = \mathbb{E}[X^{s-1}]$ for a random variable X, of the involved SNR-domain processes. An upper bound on the delay violation probability is given in [15], recapitulated in the following lemma:

Lemma 1. *The delay violation probability is upper bounded by*

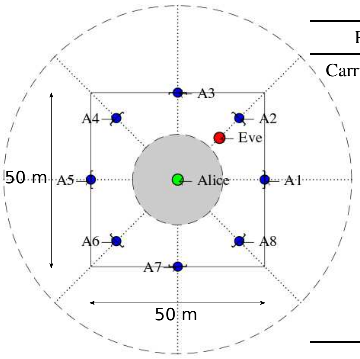
$$p(w) \leq \inf_{s>0} \left\{ \frac{\mathcal{M}_{\mathcal{S}}(1-s)^w}{1 - \mathcal{M}_{\mathcal{A}}(1+s)\mathcal{M}_{\mathcal{S}}(1-s)} \right\}, \tag{13}$$

where $\mathcal{M}_{\mathcal{S}}(s) \triangleq \mathbb{E}[e^{s_k(s-1)}]$ *and* $\mathcal{M}_{\mathcal{A}}(s) \triangleq \mathbb{E}[e^{a_k(s-1)}]$ *under the stability condition* $\mathcal{M}_{\mathcal{A}}(1+s)\mathcal{M}_{\mathcal{S}}(1-s) < 1$.

Proof. See Theorem 1 in [15] and [3] for details. □

The steady-state kernel in (13) has been shown to be a convex function for every s in the stability interval $\mathcal{M}_{\mathcal{A}}(1+s)\mathcal{M}_{\mathcal{S}}(1-s) < 1$ (see Theorem 1 in [16]). However, no previous works have provided an analytical solution to this minimization problem, so one typically resorts to grid search methods.

In [3], we derived the service-process Mellin transform $\mathcal{M}_{\mathcal{S}}(s)$ for a service model of the form (11). In the following Section V, we apply the bound (13) to the authentication scheme presented in this paper to evaluate the delay performance impacts of the distributed physical layer authentication scheme.



Parameter	Value
Carrier frequency	2.4 GHz
Δ_r	0.5
$K_{\text{a}}N_{\text{Rx}}$	8
β	4
P_0	100 mW
$K_{\text{a}} = 1$	{A1}
$K_{\text{a}} = 2$	{A1, A3}
$K_{\text{a}} = 4$	{A1, A3, A5, A7}
$K_{\text{a}} = 8$	{A1-A8}

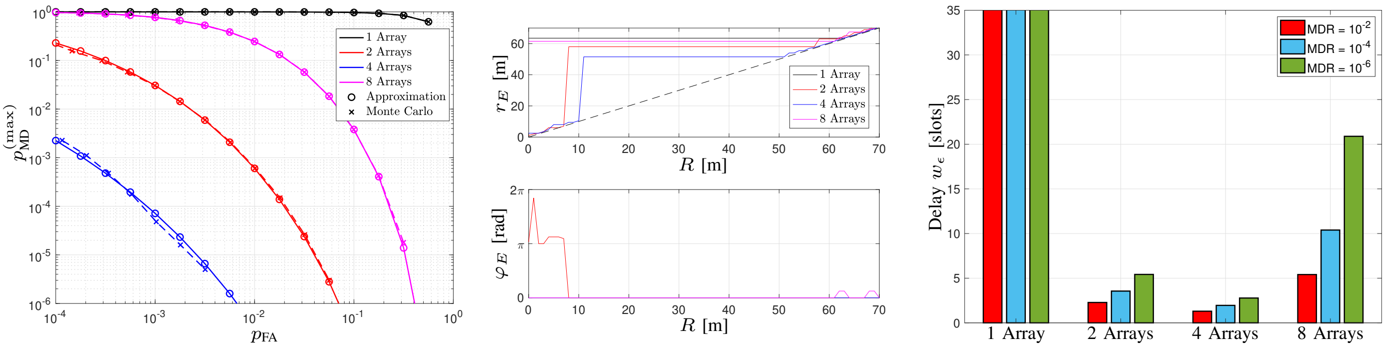
Fig. 2. Deployment scenario and system parameters.

V. Numerical Results

In this section, we numerically study the performance of the distributed authentication approach with $K_{\text{a}} = \{1, 2, 4, 8\}$ arrays. It is important to note that in this section we always consider a fixed total number of antennas $K_{\text{a}}N_{\text{Rx}} = 8$ distributed over the K_{a} arrays. The system deployment, relevant parameter values, and the array deployment mapping can be seen in Fig. 2. The arrays are deployed 25 m from and directed towards the center where Alice is situated at $(x_A, y_A) = (25, 25)$ m. For positioning of Eve, the optimal coordinates are obtained according to (10) through an exhaustive search due to lack of an analytical solution. Note that due to symmetry, the deployment in Fig. 2 contains many equivalent attacker positions which help reduce the size of the search.

In Fig. 3(a), we show the ROC performance curve for each deployment scenario when Eve is located at the optimal position outside the exclusion region with $R = 20$ m. A truncation at $N \approx 200$ terms is sufficient for (8) to get an approximation error $\epsilon(N) < 10^{-6}$. With a single array, the performance is poor since Eve can mimic the channel of Alice by positioning herself at the same distance from A1 at the opposite side in order to mirror the position of Alice. However, we also see that the distributed approaches are outperforming the single array scenario with the highest performance gain achieved for $K_{\text{a}} = 4$ arrays of $N_{\text{Rx}} = 2$ antennas each. The reason that performance degrades from $K_{\text{a}} = 4$ to $K_{\text{a}} = 8$ is that the latter setup consists of single-antenna receivers which cannot resolve the direction of the received signal.

Fig. 3(b) illustrates the optimal polar coordinates for Eve w.r.t. Alice's position as functions of the radius R of the physical exclusion region. We observe that for $R > 10$, Eve is constantly choosing the angle $\phi_E = 0$ i.e., she is placed at the opposite side of array A1 (see Fig. 2). We also see that Eve is choosing positions approximately mirroring the distance from Alice to array A1 (positioned 25 m from Alice in the considered deployment scenario). However, our results show that the mirroring point is not fixed but depending on the number of antenna arrays. The variations of ϕ_E for $K_{\text{a}} = 2$ are due to numerical imprecisions and the asymmetry of the $K_{\text{a}} = 2$ array configuration (see Fig. 2).



(a) (b) (c)

Fig. 3. Nummerical results: (a) ROC curves considering Eve at optimal position. $K_{\text{Rice}} = K_{\text{Rice},E} = 7$ dB. (b) Optimal Eve position in polar coordinates w.r.t. Alices position, (c) Delay w_ϵ for $\epsilon = 10^{-6}$ for various worst-case missed detection rates (MDR).

In Fig. 3(c), we illustrate the delay performance impacts of the different deployment scenarios considering the optimal attacker position. We have assumed $M = 100$ complex symbols/frame and a fixed arrival rate of $a = 500$ bits/frame. We evaluate the delay w_ϵ that is guaranteed not to be violated with a confidence of $\epsilon = 10^{-6}$, i.e., $p(w_\epsilon) \leq \epsilon$. Fig. 3(c) shows again that the performance of the single array scenario is poor when the attacker position is optimal. The reason for this is frequent false alarms due to the fact that the threshold T needs to be very low to achieve the missed detection rates (MDR) in Fig. 3(c). On the other hand, we can observe that the distributed approach can guarantee much lower delays even at fairly low worst-case missed detection rates (i.e., MDR = 10^{-6}). Again, the performance is optimized for $K_{\text{a}} = 4$ arrays which is expected since this scheme can achieve the lowest false alarm rate for a given missed detection rate (see Fig. 3(a)).

The numerical study verifies that our proposed physical layer authentication approach improves detection and delay performance for a fixed total number of antennas. Furthermore, it illustrates that the completely distributed approach of $K_{\text{a}} = 8$ single antenna receivers is suboptimal, and hence, there is an optimal array deployment (i.e., $K_{\text{a}} = 4$ in our case). Positioning of Eve through the exhaustive grid search method seems to indicate that the optimal position is at the opposite side of any of the antenna arrays, regardless of the number of arrays. Investigation of more sophisticated optimization tools for finding worst-case attacker positions is left for future work.

VI. Conclusions

In this paper, we have proposed and studied a new approach for physical layer authentication using multiple distributed antenna arrays. We have provided closed expressions for the ROC, formulated a detection performance metric based on the optimal attacker position, and applied our previous delay analysis tools to the new scheme. As our results have shown, our proposed approach outperforms the single-array scheme, both in terms of worst case missed-detection rate and delay impact. Moreover, the results illustrate that the completely distributed approach of single antennas is suboptimal, and hence there is an optimal choice of number of and antennas per array.

For future work, we wish to extend the queueing analysis to include an active adversary and show the effectiveness of this distributed approach in mitigating various attacks. We will also investigate analytical tools for finding the optimal attacker position. Furthermore, we will introduce and analyze different system architectures (e.g., independent decoding and authentication at the remote arrays with fusing at the central processing unit).

References

[1] A. Weinand, M. Karrenbauer, R. Sattiraju, and H. Schotten, “Application of machine learning for channel based message authentication in mission critical machine type communication,” in *European Wireless Conference*, May 2017, pp. 1–5.

[2] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “Fingerprints in the ether: Using the physical layer for wireless authentication,” in *IEEE International Conference on Communications*, June 2007, pp. 4646–4651.

[3] H. Forssell, R. Thobaben, H. Al-Zubaidy, and J. Gross, “Physical layer authentication in mission-critical MTC networks: A security and delay performance analysis,” *ArXiv e-prints*, Jun. 2018.

[4] M. Fidler and A. Rizk, “A guide to the stochastic network calculus,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 92–105, Firstquarter 2015.

[5] A. Mahmood, W. Aman, M. O. Iqbal, M. M. U. Rahman, and Q. H. Abbasi, “Channel impulse response-based distributed physical layer authentication,” in *IEEE Vehicular Technology Conference*, June 2017, pp. 1–5.

[6] M. Ozmen and M. C. Gursoy, “Secure transmission of delay-sensitive data over wireless fading channels,” *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 9, pp. 2036–2051, Sept 2017.

[7] ——, “Energy-delay-secrecy tradeoffs in wireless communications under channel uncertainty,” in *IEEE Wireless Communications and Networking Conference*, April 2018, pp. 1–6.

[8] F. Naghibi, S. Schiessl, H. Al-Zubaidy, and J. Gross, “Performance of wiretap Rayleigh fading channels under statistical delay constraints,” in *IEEE International Conference on Communications*, May 2017, pp. 1–7.

[9] H. Forssell, R. Thobaben, H. Al-Zubaidy, and J. Gross, “On the impact of feature-based physical layer authentication on network delay performance,” in *IEEE Global Communications Conference*, Dec 2017, pp. 1–6.

[10] A. Abdelaziz, R. Burton, and C. E. Koksal, “Message authentication and secret key agreement in VANETs via angle of arrival,” *CoRR*, Sep. 2016. [Online]. Available: http://arxiv.org/abs/1609.03109

[11] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “Using the physical layer for wireless authentication in time-variant channels,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2571–2579, July 2008.

[12] P. Ramírez-Espinosa, L. Moreno-Pozas, J. F. Paris, J. A. Cortés, and E. Martos-Naya, “A new approach to the statistical analysis of non-central complex gaussian quadratic forms with applications,” *CoRR*, vol. abs/1805.09181, 2018. [Online]. Available: http://arxiv.org/abs/1805.09181

[13] H. Liu, Y. Tang, and H. H. Zhang, “A new chi-square approximation to the distribution of non-negative definite quadratic forms in non-central normal variables,” *Computational Statistics Data Analysis*, vol. 53, no. 4, pp. 853 – 856, 2009.

[14] S. Kotz, N. L. Johnson, and D. W. Boyd, “Series representations of distributions of quadratic forms in normal variables. i. central case,” *Ann. Math. Statist.*, vol. 38, no. 3, pp. 823–837, 06 1967. [Online]. Available: https://doi.org/10.1214/aoms/1177698877

[15] H. Al-Zubaidy, J. Liebeherr, and A. Burchard, “Network-layer performance analysis of multihop fading channels,” *IEEE/ACM Transactions on Networking*, vol. 24, no. 1, pp. 204–217, Feb 2016.

[16] N. Petreska, H. Al-Zubaidy, R. Knorr, and J. Gross, “Power-minimization under statistical delay constraints for multi-hop wireless industrial networks,” *CoRR*, vol. abs/1608.02191, 2016. [Online]. Available: http://arxiv.org/abs/1608.02191