On the Impact of Feature-Based Physical Layer Authentication on Network Delay Performance

Henrik Forssell, Ragnar Thobaben, Hussein Al-Zubaidy, James Gross
KTH Royal Institute of Technology and ACCESS Linnaeus Centre
SE-100 44 Stockholm, Sweden
E-mail: {hefo, ragnart, hzubaidy, jamesgr}@kth.se

***Abstract*—Feature-based authentication schemes that verify wireless transmitter identities based on physical-layer features allow for fast and efficient authentication with minimal overhead. Hence, they are interesting to consider for safety-critical applications where low latency and high reliability is required. However, as erroneous authentication decisions will introduce delays, we propose to study the impact of feature-based schemes on the system-level performance. In this paper, we therefore study the queuing performance of a line-of-sight wireless link that employs a feature-based authentication scheme based on the complex channel gain. Using stochastic networks calculus, we provide bounds on the delay performance which are validated by numerical simulations. The results show that the delay and authentication performance is highly dependent on the SNR and Rice factor. However, under good channel conditions, a missed-detection rate of 10^{-8} can be achieved without introducing excessive delays in the system.**

I. Introduction

Impersonation attacks pose a serious threat in wireless networks since once a devices identity is spoofed the adversary is able to perform various follow-up attacks [1]. Resilience to such attacks becomes increasingly important as we allow more and more systems to rely on wireless technology (e.g., monitoring and control of critical infrastructures).

Feature-based authentication exploits hardware or channel specific features available at the physical (PHY) layer for verifying transmitter identities and detecting impersonation attacks. It is part of the broader area of PHY-layer security consisting of techniques that provide security by exploiting randomness at the PHY layer, as opposed to traditional higher layer security techniques (e.g., cryptographic authentication).

While high guarantees on authentication reliability can be achieved with cryptographic methods, it comes at a cost of protocol complexity and overhead for verifying and distributing authentication keys [2]. An alternative technique that authenticates transmitters at the PHY-layer has the advantage of reduced complexity and overhead since it utilizes inherent features that are already available at the receiver for other purposes. Additionally, by using diverse features that are impossible or very difficult for an adversary to observe/replicate, one can ensure that successfully impersonating a legitimate device is a highly complex task.

Safety-critical scenarios such as machine-to-machine type communication in critical infrastructures are typically characterized by low rate, sporadic transmissions with very high requirements on reliability. In such scenarios extensive security overhead becomes an issue since performance is constrained by the amount of control signaling [3]. This observation indicates that feature-based authentication could be a practical solution to ensure resilience against impersonation attacks, while at the same time keeping overhead and latency within a limit. On the downside, erroneous authentication decisions (false alarms and missed detections in the underlying hypothesis test) will impact the system performance due to packet-drops and in the worst case, admission of illegitimate data. A fundamental question relates to the significance of this impact and under which circumstances a feature-based scheme is a viable option. Studying the relations between system-level performance and authentication security allows us to answer such questions and increase our understanding of which schemes that would provide necessary guarantees for a safety-critical application.

Authentication at the PHY layer is a relatively new area of research (see e.g., [4] and references therein) where authentication generally is based on hypothesis testing. Proposed schemes based on hardware features utilize device specific offset in carrier frequency [5] or reciprocity of phase response in a multi-carrier system [6]. Schemes based on channel features employ the location specific channel frequency-response [7, 8], impulse-response [9] or multi-antenna channel [10]. In [11], the authors propose a feature-based authentication algorithm that is combined with cryptographic authentication to reduce latency in 5G small cell handovers, they however ignore the impact on the latency due to false alarms. Their paper is, to the best of our knowledge, the only work that considers system-level performance of a feature-based authentication scheme.

In this paper, we propose a queuing model to analyze the system-level performance of a wireless fading link with authentication of packets based on the observed complex channel coefficients. We consider a fixed deployment in a closed environment with line-of-sight (LOS) communication between the legitimate nodes. To bound the security level (probability of missed detection) we assume that a potential adversary is physically prohibited to access the closed environment where the system is deployed. For a given security

This work is supported in part by the Swedish Civil Contingencies Agency, MSB, through the CERCES project.

level, we derive the corresponding false alarm rate and its impact on the queueing model. We focus our attention on the baseline performance when no adversary is taking action and measure the system performance in terms of probabilities of violating certain delay requirements. Transforms of the queueing processes are used for bounding the delay violation probability by using tools from stochastic network calculus: an approach for analysing queuing systems over wireless fading links [12].

The contributions of this paper are the following, we provide:

1) Probabilistic bounds on the system-level delay performance for a given security level of the feature-based authentication scheme. Simulation results confirm that the derived bounds are valid with a gap of 1-2 orders of magnitude.
2) Numerical results that quantify the delay impact of the feature-based authentication scheme in a system that requires both strict latency/reliability guarantees as well as high security level.
3) A closed-form solution for the Mellin transform of the cumulative service process for a block fading LOS-link. To our knowledge, this problem has not been solved before in the literature.

The rest of the paper is organized as follows: Section II introduces the system model, assumptions, and problem formulation. In Section III we provide a detailed description of the authentication hypothesis test and in Section IV we briefly describe the stochastic network calculus framework followed by derivation of the relevant transforms. The numerical results are presented in Section V and our conclusions are summarized in Section VI.

II. System Model

We consider a wireless communication link from the legitimate transmitter (Alice) to receiver (Bob), and a potential attacker (Eve) as depicted in Figure 1. We assume a frame-based communication structure where a sequence of transmission symbols are divided into blocks of N symbols and the channel between Alice and Bob is modelled as a block fading LOS channel with average SNR γ. We further assume a stationary system so that the average SNR remains constant and known to Bob.

The fading in block k is given by the instantaneous SNR $\gamma_k = \gamma |h_k|^2$ where the channel gain realizations are i.i.d complex Gaussian $h_k \sim \mathcal{CN}(\mu_A, \sigma_A^2)$ and $|\mu_A|^2 + \sigma_A^2 = 1$; hence, the channel is completely characterized by the average SNR γ and the Rician factor $K = \frac{|\mu_A|^2}{\sigma_A^2}$. We assume that Alice and Bob have perfect knowledge of the channel distribution and perfect estimates of the channel realizations.

A. Feature-Based Authentication

For detection of impersonation attacks, we assume that the system is using a feature-based authentication scheme that aims to determine whether the frames are actually transmitted from Alice. We employ an authentication scheme where the observed channel gain h_k is used as feature in a binary hypothesis test. We denote the hypothesis that the frame is legitimate by $\mathcal{H}_0$ and the alternative hypothesis $\mathcal{H}_1$. For authentication of block k Bob computes a test statistic $Z(h_k)$ and employs a hypothesis test defined by

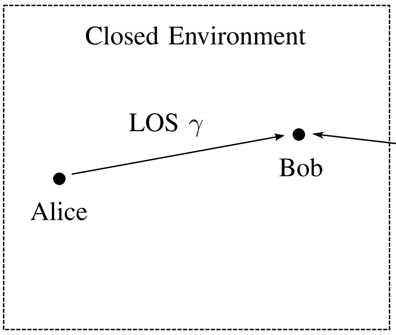


Fig. 1. Legitimate user Alice communicate to receiver Bob (LOS channel). A potential adversary Eve (NLOS channel) is physically prohibited to enter the closed system environment.

$$Z(h_k) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} T, \tag{1}$$

where T is a design parameter/threshold. The performance of the scheme for a given threshold can be evaluated through the probabilities of the two possible error events:

- **Type-I:** False alarm i.e., the receiver Bob rejects a legitimate frame from Alice.
- **Type-II:** Missed detection i.e., Bob accepts a frame that is not from Alice.

The test threshold T is chosen by Bob in order to bound the probability of missed detection $p_{\mathrm{MD}}(T)$ that defines a certain security level of the system. However, as the corresponding probability of false alarm $p_{\mathrm{FA}}(T)$ indicates, Bob may also reject a frame that is actually legitimate. Further assumptions on the hypothesis test and analytical expressions for the probabilities $p_{\mathrm{MD}}(T)$ and $p_{\mathrm{FA}}(T)$ will be defined/derived in Section III.

B. Queueing Model

In order to analyse the effect of the authentication scheme on the system-level performance we define a queuing model of the system depicted in Figure 2. We denote the cumulative arrival, service, and departures during the period $k \in [\tau, t]$ by

$$A(\tau,t) = \sum_{k=\tau}^{t} a_k, \quad S(\tau,t) = \sum_{k=\tau}^{t} s_k, \quad D(\tau,t) = \sum_{k=\tau}^{t} d_k,$$

where a_k, s_k, and d_k respectively represent the instantaneous arrival, service, and departure of the queueing system in frame k. For the arrival process we assume a constant arrival of α bits per frame.

The service process is dependent on the channel fading and the authentication false alarms. Given the instantaneous SNR γ_k, the transmitter chooses an appropriate coding rate

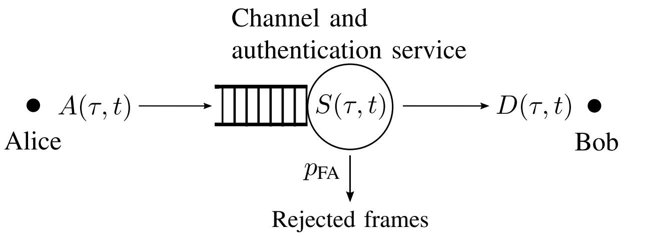


Fig. 2. Queuing model of the channel in conjunction with PHY-layer authentication.

R_k which we define here as the Shannon capacity, expressed as follows

$$R_k = \log_2(1+\gamma_k). \tag{2}$$

Given that the frame is accepted by the authentication test, the number of bits served in frame k will be $s_k = NR_k$. However, due to the false alarm probability, there is a possibility that a frame is dropped which implies that $s_k = 0$.

C. Problem Formulation

In this work, we are interested in quantifying the effect of authentication false alarms on the delay performance. A well-known result from binary hypothesis testing (Neyman-Pearson lemma) states that picking another threshold T^* in (1) such that $p_{\text{MD}}(T^*) < p_{\text{MD}}(T)$ implies that $p_{\text{FA}}(T^*) > p_{\text{FA}}(T)$ i.e., demanding a higher security level will cause an increase in false alarm probability.

From the queuing perspective, an increase in the number of false alarms will cause potentially significant delays in the queuing system and hence we have a trade-off between security level (bound on $p_{\text{MD}}(T)$) and the delay performance of the system. The delay function $W(t)$ describes the number of blocks it takes for a bit received at time t to depart from the system and is defined as

$$W(t) \triangleq \inf\{u > 0; A(0,t) \leq D(0,t+u)\}. \tag{3}$$

To assess the effects of false alarms on the delay performance we are here interested in deriving upper bounds on the probability that a bit is not received within a defined deadline w, referred to as the delay violation probability which is defined as

$$p(w) = \mathbb{P}(W(t) > w). \tag{4}$$

Evaluating bounds on the delay violation probability for various security levels of the feature-based authentication scheme allows us to determine the impact of the authentication on the system-level delay performance.

III. Authentication Performance

For authentication of each frame, Bob utilizes the log-likelihood ratio test

$$\log \frac{p(h_k|\mathcal{H}_0)}{p(h_k|\mathcal{H}_1)} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\gtrless}} \eta, \tag{5}$$

for some threshold η. Assuming that Bob has no explicit knowledge of the distribution $p(h_k|\mathcal{H}_1)$ he assigns a zero-mean complex Gaussian distribution $\mathcal{CN}(0,\sigma^2)$ and let $\sigma^2 \to \infty$ (uniform distribution over $\mathbb{C}$), which results in the test statistic $Z(h_k) = |h_k - \mu_A|$ in (1). Hence, the hypothesis test of (1) can be interpreted as determining whether the Euclidian distance between the observed channel gain and the mean is below a certain threshold.

Finding the probability of false alarm is now straightforward since under $\mathcal{H}_0$ we have $Z(h_k) \sim \text{Rayleigh}(\sqrt{\frac{\sigma_A^2}{2}})$ and hence

$$p_{\text{FA}}(T) = \mathbb{P}(Z_k > T|\mathcal{H}_0) = e^{-\frac{T^2}{\sigma_A^2}}. \tag{6}$$

To quantify the security level of the authentication scheme we seek the worst case probability of missed detection assuming that a potential attacker (Eve) does not have physical access to the closed environment where the system is deployed (see Figure 1). Communicating from outside this closed environment Eve's channel can be modelled as NLOS where we denote the best average SNR that the attacker can achieve by γ_E [1].

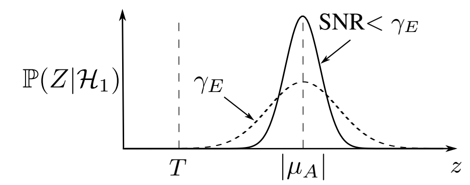


Fig. 3. Rician probability distribution of test statistic $Z(h_k)$ given alternative hypothesis $\mathcal{H}_1$.

Mathematically this means that under $\mathcal{H}_1$ we have $h_k \sim \mathcal{CN}(0,\sigma_E^2)$ where $\sigma_E^2 = \gamma_E/\gamma$. Now since $Z(h_k|\mathcal{H}_1) \sim \text{Rice}(\nu_1,\sigma_1)$ with $\nu_1 = |\mu_A|$ and $\sigma_1 = \sqrt{\frac{\sigma_E^2}{2}}$, we can easily obtain the corresponding probability of missed detection from the Rician distribution according to:

$$p_{\text{MD}}(T) = \mathbb{P}(Z_k < T|\mathcal{H}_1) = 1 - Q_1\left(\frac{\nu_1}{\sigma_1}, \frac{T}{\sigma_1}\right), \tag{7}$$

where $Q_1()$ denotes the Marcum Q function. Moreover as illustrated in Figure 3, an attacker with worse channel conditions (average SNR lower than γ_E) will reduce the variance of the Rician distribution of $Z(h_k|\mathcal{H}_1)$. Therefore, given that $T < |\mu_A|$, the expression (7) serves as the worst case probability of missed detection.

Remark 1. *We note here that having a more accurate knowledge of an attacker's channel distribution can improve the detection performance of the authentication scheme. However, knowing or learning this distribution would in reality require observations in terms of actions from the attacker. Since we restrict ourselves to the case with no impersonated frames, we*

[1] For example an attacker transmitting with commodity hardware for which PHY layer properties cannot be altered, resulting in limits on path loss and available transmission power.

believe that the most realistic assumption is that the channel distribution of the attacker is unknown to Bob.

Extending the feature dimension by using multiple or vector-valued features such as multi-carrier frequency responses can also improve the detection performance. However, for the sake of simplifying the queuing analysis, we have chosen the complex channel gain feature in this paper.

IV. Stochastic Network Calculus

In this section, we use tools from stochastic network calculus in order to provide a bound on the delay violation probability of (4) in terms of transforms of the arrival and service processes of the queuing model. Due to the logarithmic expression for the service process in (2), the analysis is simplified by using Network Calculus framework for the SNR-domain 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 $\mathcal{D}(\tau,t) \triangleq e^{D(\tau,t)}$.

Stochastic network calculus provides a bound for the delay violation probability based on the SNR-domain processes using a moment bound. For a given target delay w, it can be shown that

$$p(w) \leq \inf_{s>0}\{\mathcal{K}(s,t+w,t)\}, \tag{8}$$

where the function $\mathcal{K}(s,\tau,t)$ is called the kernel. The kernel is defined as

$$\mathcal{K}(s,\tau,t) \triangleq \sum_{u=0}^{\min(\tau,t)} \mathcal{M}_{\mathcal{S}}(1+s,u,t)\mathcal{M}_{\mathcal{A}}(1-s,u,\tau), \tag{9}$$

where $\mathcal{M}_X(s) = \mathbb{E}[X^{s-1}]$ denotes the Mellin transform of a random variable X.

Since we assume constant arrivals of α bits per frame, the arrival process is deterministic and the Mellin transform of the SNR-domain arrival process can easily be found to be

$$\mathcal{M}_{\mathcal{A}}(s,\tau,t) = e^{\alpha(\tau-t)}. \tag{10}$$

The Mellin transform of the cumulative service process is derived in the following subsection. For a more detailed description of stochastic network calculus and the utilized bound, see [13].

A. Mellin Transform of the Service Process

In this section we derive the Mellin transform of the SNR-domain cumulative service process $\mathcal{M}_{\mathcal{S}}(s,\tau,t)$.

As described in Section II, the instantaneous service in frame k is

$$s_k = \begin{cases} N\log_2(1+\gamma_k), & \text{if} \quad X_k = \text{"success"} \\ 0, & \text{if} \quad X_k = \text{"false alarm"}, \end{cases} \tag{11}$$

where we similarly to the analysis in [14] introduce a Bernoulli random variable $X_k \in \{\text{"success"}, \text{"false alarm"}\}$ to indicate whether the transmission is successful or not. By fixing the threshold T of the hypothesis test we can obtain $\Pr(X_k = \text{"false alarm"}) = p_{\text{FA}}$ independent of the instantaneous SNR γ_k.

We define the functions $h(\gamma_k, X_k) \triangleq e^{s_k}$ and $g(\gamma_k) = 1+\gamma_k$ so that

$$h(\gamma_k, X_k) = \begin{cases} g(\gamma_k)^{\frac{N}{\ln(2)}}, & \text{if} \quad X_k = \text{"success"} \\ 1, & \text{if} \quad X_k = \text{"false alarm"}. \end{cases}$$

First we provide the Mellin transform of $g(\gamma_k)$ for the LOS case in the following theorem:

Theorem 1. *For the Rice-fading channel with average SNR γ and Rician factor K we have*

$$\mathcal{M}_{g(\gamma_k)}(s) = \left(\frac{\gamma}{K+1}\right)^{s-1} e^{\frac{K+1}{\gamma}-K} \sum_{k=0}^{\infty} \frac{K^k}{k!^2} S_k, \tag{12}$$

where

$$S_k = \sum_{m=0}^{k} \binom{k}{m} \left(\frac{-\gamma}{K+1}\right)^{-m} \Gamma\left(s+k-m, \frac{K+1}{\gamma}\right),$$

and $\Gamma(s,x)$ denotes the upper incomplete Gamma function.

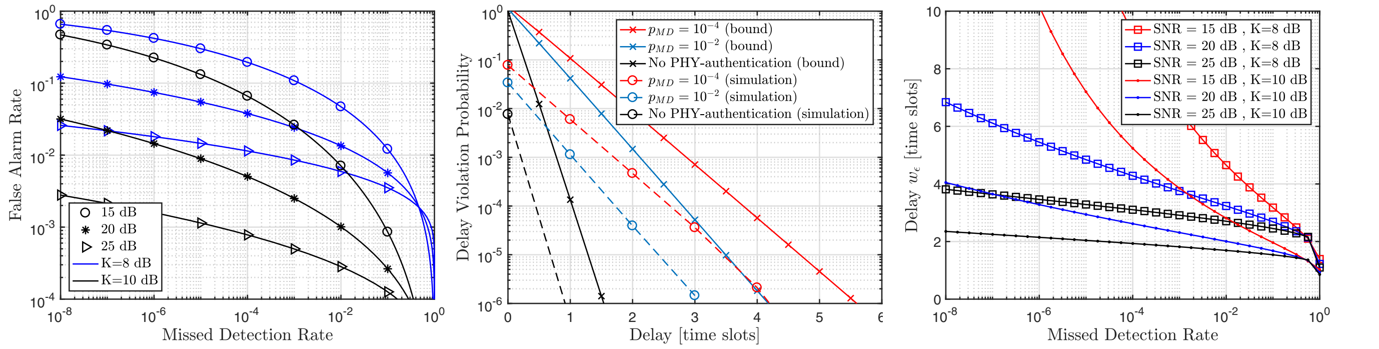
Proof. To simplify notation we define the constant $a = \frac{2\gamma}{K+1}$ and introduce a change of variable $z = \frac{\gamma_k}{a}$ so that $z \sim \chi_2^2(2K)$, where $\chi_2^2(\nu)$ denotes the non-central chi-squared distribution with two degrees of freedom and non-centrality parameter ν. This implies that $g(\gamma_k) = 1 + az$ and now we observe that

$$\begin{aligned} \mathcal{M}_{g(\gamma_k)}(s) &= \mathbb{E}[g(\gamma_k)^{s-1}] = \int_0^{\infty} (1+az)^{s-1} f_{\chi_2^2}(z)dz \\ &= \int_0^{\infty} (1+az)^{s-1} \frac{1}{2} e^{-(z+2K)/2} \sum_{k=0}^{\infty} \frac{(\frac{Kz}{2})^k}{k!^2} dz \\ &= \frac{1}{2a} e^{1/2a-K} \sum_{k=0}^{\infty} \frac{\left(\frac{K}{2a}\right)^k}{k!^2} \underbrace{\int_1^{\infty} t^{s-1}(t-1)^k e^{-\frac{t}{2a}} dt}_{=I_k}. \end{aligned} \tag{13}$$

The integral I_k does not have a standard solution, but we can use the Binomial series expansion

$$(t-1)^k = \sum_{m=0}^{k} \binom{k}{m} (-1)^m t^{k-m} \qquad |t| > 1. \tag{14}$$

With this expansion we get



(a)

(b)

(c)

Fig. 4. Numerical results: (a) Authentication performance for $\gamma_E = 0$ dB. (b) Delay bound compared to simulation for $\gamma_E = -5$ dB, average SNR $\gamma = 15$dB and $\alpha = 80$ bits/frame. (c) Delay as a function of security level. Delay target w_ϵ that is met with violation probability $\epsilon = 10^{-6}$ as function of missed-detection rate, $\gamma_E = 0$ dB, $N = 100$ and $\alpha = 100$ bits/frame.

$$\begin{aligned} I_k &= \int_1^\infty t^{s-1}\sum_{m=0}^{k}\binom{k}{m}(-1)^m t^{k-m}e^{-\frac{t}{2a}}dt \\ &= \sum_{m=0}^{k}\binom{k}{m}(-1)^m\int_1^\infty t^{s-1+k-m}e^{-\frac{t}{2a}}dt \\ &= (2a)^{s+k}\underbrace{\sum_{m=0}^{k}\binom{k}{m}(-2a)^{-m}\Gamma(s+k-m,1/2a)\,.}_{=S_k} \end{aligned} \tag{15}$$

Plugging this into Equation (13) yields (12) which completes the proof. □

Remark 2. *For validation we can see that by setting $K = 0$ (reducing the fading to the NLOS case), the sum in the right-hand side of* (12) *contains only one term ($k = 0$). Hence the expression reduces to*

$$\mathcal{M}_{g(\gamma_k)}(s) = \gamma^{s-1}e^{\frac{1}{\gamma}}\Gamma(s, 1/\gamma), \tag{16}$$

which is the known result for the NLOS (Rayleigh) fading channel.

Next we utilize a previously provided result for Bernoulli packet drops [14] in the following lemma:

Lemma 1. *For a fading channel with packet-drops indicated by $X_k \sim$ Bernoulli(p_{FA}) we have*

$$\mathcal{M}_{h(\gamma_k,X_k)}(s) = (1-p_{FA})\mathcal{M}_{g(\gamma_k)}\left(1+\frac{N(s-1)}{\ln 2}\right)+p_{FA}.$$

Finally we can find that

$$\begin{aligned} \mathcal{M}_{\mathcal{S}}(s,\tau,t) = \mathbb{E}\left[\left(\prod_{k=\tau}^{t}e^{s_k}\right)^{s-1}\right] &= \mathbb{E}\left[h(\gamma_k,X_k)^{s-1}\right]^{t-\tau} \\ &= \left(\mathcal{M}_{h(\gamma_k,X_k)}(s)\right)^{t-\tau} \end{aligned} \tag{17}$$

where we in the second equality have used that the services s_k are independent due to the i.i.d fading. Lemma 1 and Theorem 1 allows us to evaluate the Mellin transform of the SNR-domain service process according to (17).

V. Numerical Results

As outlined in Section I, we seek to study the trade-off between authentication security level and the system-level delay performance by numerically evaluating the derived bounds. The procedure is to fix a certain security level p_{MD}, compute the test threshold from (7) and use the corresponding false-alarm rate of (6) for computing the Mellin transform of the service process, which is then used for evaluating the bound (8) on the delay violation probability for a certain delay target w. Numerically, the minimization of (8) is performed through an exhaustive search and the infinite sum in (12) is truncated.

Firstly, we show in Figure 4a the relation between the authentication false-alarm and missed-detection rate for various SNR and Rice factors. We observe that in order to give strict guarantees on missed-detection rates while keeping the false-alarm rate low, we need a high SNR and Rician factor (K) (strong LOS component on the link from Alice to Bob). We also note that the line-crossing on the right-hand side of Figure 4a corresponds to a missed-detection rate of 50% (when the test threshold is at the peak of the $Z(h_k|\mathcal{H}_1)$ distribution).

In Figure 4b we show the evaluated bounds on delay violation probability as functions of delay target where the simulated curves (dashed lines) validate the bounds. The gaps between bound and simulation are between 1-2 orders of magnitude which is a typical behavior of these bounds. In this figure we also see a substantial impact on the delay performance by introducing the feature-based authentication. We observe that without the feature-based authentication, a delay target of 1 time slot can be guaranteed with violation probability of around 10^{-4}. However, introducing authentication with a stronger security level ($p_{\text{MD}} = 10^{-4}$) increases the delay target to around 4 time slots in this scenario.

In a safety-critical application we would typically require both high security levels and strict guarantees on delay performance. To asses what security levels we can achieve under a given delay requirement we compute the delay target w_ϵ that can be met with a certain violation probability ϵ. In Figure 4c we show the delays w_ϵ for $\epsilon = 10^{-6}$ as functions of the missed-detection rate. We find that for low SNR and Rician K, a reduced missed-detection rate quickly introduces unacceptable delays in the system due to the high false-alarm rates. However, when SNR and Rician factor increase, the introduced delays are only moderate. For example, we can see from the bottom curve in Figure 4c that a missed-detection rate in the order of 10^{-8} can be achieved without exceeding a delay of 3 time slots. Figure 4a reveals the reason for this, as we can see that the missed-detection rates are associated with lower false-alarm rates yielding less rejected packets and lower delays.

Alleviating the introduced delays at lower SNR and Rician factors requires improved detection performance of the feature based scheme (e.g., through knowledge of attackers distribution or multi-feature authentication as discussed in Section III).

VI. Conclusion

In this paper we have studied the impact of feature-based authentication on the delay performance of a wireless LOS fading link. We have assumed that the system is deployed in a closed environment where a potential intruder is physically prohibited to enter and the analysis is restricted to the baseline queueing performance when no attacker is taking action.

Two fundamental analytical results are presented: (I) the Mellin transform of the cumulative service process under LOS block fading; (II) a characterization of the service process when the receiver authenticates frames based on the complex channel gain. These results have been achieved with respect to the stochastic network calculus framework, which allows us to bound the delay violation probability.

The numerical results include simulations that validate the derived bounds and evaluations of the bounds for various authentication security levels. The results show that demanding a low delay violation probability (in the order of 10^{-6}) can result in target delays that quickly grow out of proportion at low missed-detection rates. However from the studied scenario we have observed that under certain conditions a simple feature-based scheme such as the one studied in this paper can achieve a missed-detection rate of 10^{-8} without introducing significant delays in the system.

We conclude that mitigation of the introduced delays at lower SNR and Rician factors can be achieved by improving the detection performance of the feature-based scheme, for example by having an accurate knowledge of the attackers channel distribution or by increasing the dimension of the authenticated feature. The effectiveness of such extensions are left for future work. Finally, we have observed two main directions in which this work can be extended:

1) Introducing actions from the attacker Eve in terms of impersonated data frames. Under an attack scenario, missed-detections will influence the system performance either through accepted illegitimate data, or causing entire frames to be dropped at higher layers.
2) As discussed above, we aim to evaluate enhancements of the feature-based authentication by increasing the dimension of the authenticated feature. Therefore, an extension of the analysis in this paper to a single-input-multiple-output system, using the received channel vector as a feature is one direction we want to investigate.

References

[1] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 56–62, October 2010.

[2] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sept 2016.

[3] N. K. Pratas, S. Pattathil, Č. Stefanović, and P. Popovski, "Massive machine-type communication (mMTC) access with integrated authentication," in *2017 IEEE International Conference on Communications (ICC)*, May 2017, pp. 1–6.

[4] E. Jorswieck, S. Tomasin, and A. Sezgin, "Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1702–1724, Oct 2015.

[5] W. Hou, X. Wang, J-Y. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Transactions on Communications*, vol. 62, no. 5, pp. 1658–1667, May 2014.

[6] X. Wu and Z. Yang, "Physical-layer authentication for multi-carrier transmission," *IEEE Communications Letters*, vol. 19, no. 1, pp. 74–77, Jan 2015.

[7] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *Communications, 2007. ICC '07. IEEE International Conference on*, June 2007, pp. 4646–4651.

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

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

[10] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over MIMO fading wiretap channels," *IEEE Transactions on Wireless Communications*, vol. 11, no. 7, pp. 2564–2573, July 2012.

[11] X. Duan and X. Wang, "Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer," in *2016 IEEE International Conference on Communications (ICC)*, May 2016, pp. 1–6.

[12] 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.

[13] 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.

[14] S. Schiessl, J. Gross, and H. Al-Zubaidy, "Delay analysis for wireless fading channels with finite blocklength channel coding," in *Proceedings of the 18th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, New York, NY, USA, 2015, MSWiM '15, pp. 13–22, ACM.