Performance of Wiretap Rayleigh Fading Channels Under Statistical Delay Constraints

Farshad Naghibi, Sebastian Schiessl, Hussein Al-Zubaidy, James Gross
School of Electrical Engineering, KTH Royal Institute of Technology, Stockholm, Sweden
Emails:{farshadn,schiessl,hzubaidy,jamesgr}@kth.se

***Abstract*—In this paper, we investigate the performance of the wiretap Rayleigh fading channel in the presence of statistical delay constraints. We invoke tools from stochastic network calculus to derive probabilistic bounds on the delay. This method requires a statistical characterization of the wiretap fading service process, which we derive in closed form. We then validate these analytical bounds via simulations. Interestingly, the analysis of the wiretap fading channel reveals close structural similarities with the interference channel in terms of service process characterization, which is derived in our prior work. In our numerical evaluations, we show that the delay performance of the wiretap fading channel is in particular sensitive to bursty arrival processes due to the high variance of the service process.**

I. Introduction

As wireless access is becoming more prominent in communication networks, providing secrecy is increasingly becoming a predominant issue. This is mainly due to the broadcast nature of wireless channels which makes them vulnerable to malicious security attacks. As a consequence, information-theoretic security as a concrete framework for analyzing secrecy in physical layer has gained a notable attention among researchers in recent years [1], [2]. Information-theoretic security, which was initially introduced by Shannon [3], exploits different statistical characteristics of received information at the legitimate receiver and at the eavesdropper. Moreover, it makes no assumptions on the computational power of the eavesdropper, unlike the traditional cryptographic approaches for secrecy. Later, Wyner introduced the wiretap channel model in [4]. In this model, a source node wants to transmit confidential information to a destination node and wishes to keep an eavesdropper as ignorant as possible about this information. The performance measure of interest is the secrecy capacity, which is the largest reliable communication rate from the source node to the destination node with the eavesdropper obtaining no information. Wyner showed that perfectly secure communication without a shared secret key is possible if the channel from the transmitter to the legitimate receiver is stronger than the channel to the eavesdropper.

If both the main channel to the destination and the wiretap channel to the eavesdropper are Gaussian, the secrecy capacity was shown to be the difference between the capacity of the two channels in each transmission time instance [5]. Therefore in this case, secure communication is only possible if the main channel has a higher signal-to-noise ratio (SNR) than the eavesdropper's channel in the corresponding transmission time instance. The effect of fading in secrecy capacity of wireless channels was studied in [6]–[8] and it was shown that even when the wiretap channel is, on average, better than the main channel, non-zero secrecy capacity can be achieved.

Apart from the secrecy concerns in wireless networks, providing adequate quality-of-service (QoS) is a crucial requirement for various applications. For instance, machine-type communications, as one of the key technologies for the next generation of wireless networks, can pose strict end-to-end delay requirements on the network. In order to characterize the performance of wireless networks under such delay constraints, queuing effects should be taken into account. These effects are results of the random arrival of the traffic as well as the random service that is provided by the fading channel.

Due to the significant importance of both physical layer security and delay requirements in wireless networks, a rigorous performance model and analysis which jointly accounts for both aspects is of great interest and has attracted some attention in the last few years. The work in [9] proposed scheduling and power allocation policies where both secrecy and stability in terms of finite queue length are taken into account. The authors in [10] investigated the delay-limited secrecy capacity of a fading channel in which the source and destination share a secret key hidden from the eavesdropper. It was shown that using this secret key the transmitter can securely communicate with the destination even when the eavesdropper's channel is better than the main channel. Similar extensions to this work that consider a separate secret key queue can be found in [11]–[13]. Studies [14] and [15] investigated the effective capacity of a wiretap fading channel considering QoS constraint in terms of the queue length limitations. Effective capacity [16] is defined as the maximum constant arrival rate that a service process can support given a QoS constraint. The authors provided power control policies for achieving the boundary of this effective capacity region. The presented results in [14] and [15] are not in closed-form and need to be evaluated numerically, and thus, provide limited insight into the performance with respect to different system parameters.

In this paper, we provide an analytical performance model for Rayleigh fading wireless networks that takes into account both physical layer security and statistical delay constraint. For the analysis, we utilize the $(\min, \times)$ network calculus methodology for wireless network analysis provided in [17]. The main challenge in applying this methodology is the sta-

tistical characterization of the service offered by the wireless wiretap fading channel. We derive this characterization in closed form. Consequently, the delay bounds are tractable and easily computable, allowing us to gain insights into the system performance with respect to various parameters. Interestingly, we discovered in our analysis that the performance offered by the wiretap channel and that by the interference channel are related in the sense that the service characterization of the wiretap fading channel turns out to have structural similarities to that of the interference channel presented in our previous work [18]. Moreover, using the stochastic network calculus approach, we also investigate the effect of bursty arrival traffic on secure wireless communication with delay constraints. In addition, we show that for a specific delay constraint, even when the eavesdropper channel is on average better than the main channel, having secure communication may still be possible.

The rest of the paper is organized as follows: In Section II, we provide our system model. In Section III, a brief background on the $(\min, \times)$ network calculus is presented and the delay performance analysis of the wireless wiretap fading channel is derived. Numerical evaluations are presented in Section IV, and finally, we provide conclusions in Section V.

II. System Model

We consider a wireless wiretap channel in which a transmitter wishes to communicate confidential messages with a certain delay requirement to a legitimate receiver. In addition, there exists an eavesdropper in the system who, due to the broadcast nature of the wireless transmission, can listen in on the communication of the confidential messages.

We assume independent and Rayleigh-fading channels from the transmitter to the legitimate receiver and to the eavesdropper. We use a time-slotted model and assume that the fading coefficients stay constant for one transmission slot but vary independently from one slot to another (block-fading). All channel coefficients are assumed to be known at all nodes, i.e., at the transmitter, at the legitimate receiver and at the eavesdropper. This assumption is reasonable when the eavesdropper node is itself part of the network and its transmission can be monitored [6]. It was shown in [6] that the instantaneous secrecy capacity of the wiretap fading channel at time slot t is given by

$$C_{\mathrm{s},t} = \left[C_{\mathrm{m},t} - C_{\mathrm{e},t}\right]^+ = \left[N_c \log_2 \frac{1+\gamma_{\mathrm{m},t}}{1+\gamma_{\mathrm{e},t}}\right]^+, \quad (1)$$

where $[x]^+ \coloneqq \max(0, x)$ and N_c is the number of transmitted symbols per time slot. $C_{x,t}$ and $\gamma_{x,t}$ with $x \in \{\mathrm{m}, \mathrm{e}\}$ are instantaneous capacity and SNR of the main channel and the eavesdropper channel, respectively. For Rayleigh fading channels, the instantaneous SNRs are exponentially distributed: $\gamma_{\mathrm{m}} \sim \exp(\bar{\gamma}_{\mathrm{m}})$ and $\gamma_{\mathrm{e}} \sim \exp(\bar{\gamma}_{\mathrm{e}})$, where $\bar{\gamma}_{\mathrm{m}}$ and $\bar{\gamma}_{\mathrm{e}}$ denote the average SNRs. We assume that in time slot t, the transmitter can transmit $C_{\mathrm{s},t}$ bits without errors and without the eavesdropper obtaining any information.

Due to the time-varying nature of the fading channel, data must be queued at the transmitter. The queuing system is described by the bivariate functions $A(\tau, t)$, $D(\tau, t)$ and $S(\tau, t)$ for any $0 \leq \tau \leq t$, which denote the cumulative arrivals to the system, departures from the system, and service offered by the system, respectively, measured in bits in the interval $[\tau, t)$. In case the queue is handled in a first-come first-served order, the delay at time slot t is given by

$$W(t) = \inf\left\{u \geq 0 : A(0,t) \leq D(0, t+u)\right\}. \quad (2)$$

Thus, the delay $W(t)$ is the number of time slots it takes for a packet arriving at time slot t to be received at the legitimate receiver.

III. Delay Performance Bounds

In this section, we analyze the delay performance of the wiretap fading channel and provide probabilistic bounds that can be computed efficiently. However, we first give some brief introduction to $(\min, \times)$ network calculus.

A. Review of $(\min, \times)$ Network Calculus

In [17], it was shown that a probabilistic upper bound on the end-to-end delay $W(t)$ can be derived based on a transform of the cumulative arrival and service processes. In the transform domain, the cumulative arrival, departure, and service processes are denoted by calligraphic letters $\mathcal{A}$, $\mathcal{D}$, and $\mathcal{S}$, respectively, and are related to their bit domain counterparts through the exponential function. That is, we have $\mathcal{A}(\tau, t) \coloneqq e^{A(\tau,t)}$, $\mathcal{D}(\tau, t) \coloneqq e^{D(\tau,t)}$, and $\mathcal{S}(\tau, t) \coloneqq e^{S(\tau,t)}$. Due to the exponential function, these cumulative functions become products of the increments in the bit domain. Using this transform, the queuing behavior is analyzed directly in the domain of channel variations instead of the bit domain (see e.g., [19], [20]). This is referred to as the *SNR domain*. Using this transform, the delay bound is obtained by

$$\mathbb{P}\big(W(t) > w_\varepsilon\big) \leq \varepsilon, \quad (3)$$

where w_ε is the smallest $w_\varepsilon \geq 0$ satisfying

$$\inf_{s>0}\Big[\mathbb{K}(s, t+w_\varepsilon, t)\Big] < \varepsilon. \quad (4)$$

The function $\mathbb{K}(s, \tau, t)$, referred to as the *kernel*, is given by

$$\mathbb{K}(s, \tau, t) \coloneqq \sum_{i=0}^{\min(\tau,t)} \mathbb{M}_{\mathcal{A}}(1+s, i, t)\mathbb{M}_{\mathcal{S}}(1-s, i, \tau), \quad (5)$$

where $\mathbb{M}_{\mathcal{X}}(s)$ is the Mellin transform [21] of the random process $\mathcal{X}$, defined as

$$\mathbb{M}_{\mathcal{X}}(s, \tau, t) = \mathbb{M}_{\mathcal{X}(\tau,t)}(s) = \mathbb{E}\left[\mathcal{X}^{s-1}(\tau, t)\right], \quad (6)$$

for any complex-valued $s \in \mathbb{C}$. However, we restrict our derivations in this work to real-valued $s \in \mathbb{R}$.

In the following, we assume the cumulative arrival and service process in the SNR domain, i.e., $\mathcal{A}(\tau, t)$ and $\mathcal{S}(\tau, t)$, to have stationary and independent increments, denoted by a and $g\big(\gamma_{\mathrm{m},t}, \gamma_{\mathrm{e},t}\big)$, respectively. Hence, the Mellin transforms

become independent of the time instance. To simplify notation, we drop the arguments of g in the following. Then, we have

$$\mathbb{M}_{\mathcal{S}}(s,\tau,t) = \prod_{i=\tau}^{t-1} \mathbb{M}_g(s) = \mathbb{M}_g^{t-\tau}(s), \tag{7}$$

$$\mathbb{M}_{\mathcal{A}}(s,\tau,t) = \prod_{i=\tau}^{t-1} \mathbb{M}_a(s) = \mathbb{M}_a^{t-\tau}(s), \tag{8}$$

where $\mathbb{M}_g(s)$ and $\mathbb{M}_a(s)$ are the Mellin transform of the stationary and independent service increment g and arrival increment a, respectively, in the SNR domain.

Using (3)–(5), we can determine the probabilistic delay performance bound of the system with respect to some fixed violation probability $\varepsilon > 0$. Setting $\tau = t + w_\varepsilon$ and substituting (7) and (8) in (5), we obtain

$$\begin{aligned}
\mathbb{K}(s, t+w_\varepsilon, t) &= \sum_{i=0}^{t} \mathbb{M}_{\mathcal{A}}(1+s,i,t)\mathbb{M}_{\mathcal{S}}(1-s,i,t+w_\varepsilon) \\
&= \sum_{i=0}^{t} \big(\mathbb{M}_a(1+s)\big)^{t-i} \big(\mathbb{M}_g(1-s)\big)^{t+w_\varepsilon-i} \\
&= \sum_{u=0}^{t} \big(\mathbb{M}_a(1+s)\big)^{u} \big(\mathbb{M}_g(1-s)\big)^{u+w_\varepsilon} \\
&\overset{(a)}{\leq} \big(\mathbb{M}_g(1-s)\big)^{w_\varepsilon} \sum_{u=0}^{\infty} \big(\mathbb{M}_a(1+s)\mathbb{M}_g(1-s)\big)^{u} \\
&= \frac{\big(\mathbb{M}_g(1-s)\big)^{w_\varepsilon}}{1-\mathbb{M}_a(1+s)\mathbb{M}_g(1-s)},
\end{aligned} \tag{9}$$

for any $s > 0$ and under the stability condition

$$\mathbb{M}_a(1+s)\mathbb{M}_g(1-s) < 1. \tag{10}$$

In step (a) of (9), we let $t \to \infty$ as we are only interested in the steady-state kernel, then we evaluated the geometric sum in the last step.

To find the end-to-end delay bound w_ε, we first set the right-hand side of (9) equal to the violation probability ε, and solve for w_ε as a function of s. This results in

$$w_\varepsilon(s) = \frac{\ln\varepsilon + \ln\big(1-\mathbb{M}_a(1+s)\mathbb{M}_g(1-s)\big)}{\ln \mathbb{M}_g(1-s)}. \tag{11}$$

Then, the delay bound is

$$w_\varepsilon = \min_{s>0} w_\varepsilon(s). \tag{12}$$

Next, we proceed to derive the Mellin transforms of the arrival process and service process which are required for determining the above delay performance bound.

B. Characterization of the Arrival Process

In this work, we consider two different arrival models, namely, constant-rate traffic and Markov modulated ON-OFF traffic [17], [22]. Due to its bursty nature, the effect of the latter model on the delay performance is interesting to investigate in the context of secure communication in the wiretap fading channel.

In the constant-rate traffic model, the rate is denoted by ρ, and the cumulative arrival process in the SNR domain is characterized by its Mellin transform as

$$\mathbb{M}_{\mathcal{A}}(s,\tau,t) = \mathbb{M}_a^{t-\tau}(s) = e^{(s-1)\rho(t-\tau)}, \tag{13}$$

In the Markov modulated ON-OFF arrival model, there are two states. State 1 indicates the OFF state with arrival rate $r_1 = 0$, and State 2 indicates the ON state with arrival rate $r_2 = r$ which is referred to as the *burst rate*. The transition probabilities are denoted by $p_{12} = \alpha$ and $p_{21} = \beta$. Then, the cumulative arrival process in the SNR domain is characterized by [17]

$$\mathbb{M}_{\mathcal{A}}(s,\tau,t) \leq \Big(L(s-1,r,\alpha,\beta)\Big)^{t-\tau}, \tag{14}$$

with [22]

$$\begin{aligned}
L(s,r,\alpha,\beta) \coloneqq \frac{1}{2}\Big(&e^{sr}(1-\beta)+(1-\alpha) \\
&+\sqrt{(e^{sr}(1-\beta)+(1-\alpha))^2 - 4e^{sr}(1-\alpha-\beta)}\Big).
\end{aligned} \tag{15}$$

The upper bound for the Mellin transform of Markov modulated ON-OFF traffic thus has the same form as the Mellin transform for independent arrivals in (8), and the kernel (9) can be computed in the same fashion, replacing $\mathbb{M}_a(s)$ with $L(s-1,r,\alpha,\beta)$.

C. Characterization of the Service Process

The service process in our setup corresponds to the secrecy capacity that the wiretap fading channel provides. Therefore, we obtain the cumulative service process in the SNR domain as

$$\begin{aligned}
\mathcal{S}(\tau,t) = \prod_{i=\tau}^{t-1} e^{C_{\mathrm{s},i}} &= \prod_{i=\tau}^{t-1} \max\left(\left(\frac{1+\gamma_{\mathrm{m},i}}{1+\gamma_{\mathrm{e},i}}\right)^{\mathcal{N}}, 1\right) \\
&\coloneqq \prod_{i=\tau}^{t-1} g\big(\gamma_{\mathrm{m},i}, \gamma_{\mathrm{e},i}\big),
\end{aligned} \tag{16}$$

where $\mathcal{N} = N_c/\ln 2$. In order to simplify notations, we consider the case $\mathcal{N} = 1$ without loss of generality. The bounds for the general case can be obtained by appropriately scaling the derived results. For the analysis, we first define the random variable Z_t as

$$Z_t \coloneqq e^{C_{\mathrm{m},t} - C_{\mathrm{e},t}} = \frac{1+\gamma_{\mathrm{m},t}}{1+\gamma_{\mathrm{e},t}}. \tag{17}$$

For Rayleigh fading channels, the SNRs γ_{m} and γ_{e} are exponentially distributed. Therefore, the random variable Z_t is the division of two random variables with exponential distributions, for which the probability density function (PDF) is given by

$$f_Z(z) = \left(\frac{1}{\bar{\gamma}_{\mathrm{e}} z + \bar{\gamma}_{\mathrm{m}}} + \frac{\bar{\gamma}_{\mathrm{e}}\bar{\gamma}_{\mathrm{m}}}{(\bar{\gamma}_{\mathrm{e}} z + \bar{\gamma}_{\mathrm{m}})^2}\right) e^{-\frac{z-1}{\bar{\gamma}_{\mathrm{m}}}}, \tag{18}$$

and the cumulative distribution function (CDF) by

$$F_Z(z) = 1 - \frac{\bar{\gamma}_{\mathrm{m}}}{\bar{\gamma}_{\mathrm{e}} z + \bar{\gamma}_{\mathrm{m}}} e^{-\frac{z-1}{\bar{\gamma}_{\mathrm{m}}}}. \tag{19}$$

Now for the service process in the SNR domain in (16), we have

$$\mathcal{S}(\tau,t)=\prod_{i=\tau}^{t-1}\max\big(Z_i,1\big). \tag{20}$$

Furthermore, we define the truncated random variable

$$Y_t\coloneqq\{Z_t|Z_t>1\}, \tag{21}$$

with support $(1,\infty)$ and PDF

$$f_Y(y)=\frac{f_Z(y)}{1-F_Z(1)},\qquad \forall y>1. \tag{22}$$

To derive the delay performance bound in (12), we need to obtain the Mellin transform of the service process in the SNR domain. Using the independence property of the Mellin transform, we compute $\mathbb{M}_{\mathcal{S}}(s,\tau,t)$ in terms of the random variable Y as

$$\mathbb{M}_{\mathcal{S}}(s,\tau,t)=\Big(\big(1-F_Z(1)\big)\mathbb{M}_Y(s)+F_Z(1)\Big)^{t-\tau}. \tag{23}$$

This is based on the fact that, in each time slot t, with probability $1-F_Z(1)$ the system provides the service Y_t and with probability $F_Z(1)$ provides no service in the SNR domain (i.e., with probability $F_Z(1)$ the secrecy capacity is zero in the bit domain).

Before we continue to derive the Mellin transform of the service process in (23), we state the following lemma based on an insight from [18] in the interference channel.

Lemma 1: The solution to the integral

$$I(s)\coloneqq\int_1^{\infty}\frac{y^{s-2}}{1+\frac{\bar\gamma_{\rm e}}{\bar\gamma_{\rm m}}y}e^{-\frac{y}{\bar\gamma_{\rm m}}}\mathrm{d}y \tag{24}$$

is given by

$$I(s)=I_1^k(s)+I_\delta(s)+I_2^k(s) \tag{25}$$

for $k\to\infty$ and any small $\delta>0$, where

$$I_1^k(s)\coloneqq\sum_{n=0}^{k}(-1)^n\bar\gamma_{\rm e}^n\bar\gamma_{\rm m}^{s-1}\Bigg(\Gamma\bigg(s+n-1,\frac{1}{\bar\gamma_{\rm m}}\bigg)-\Gamma\bigg(s+n-1,\frac{\bar\gamma_{\rm m}/\bar\gamma_{\rm e}-\delta}{\bar\gamma_{\rm m}}\bigg)\Bigg), \tag{26}$$

for $k\geq 0$ and $\bar\gamma_{\rm m}/\bar\gamma_{\rm e}>1+\delta$; otherwise $I_1^k(s)=0$. $\Gamma(a,b)$ denotes the incomplete Gamma function.

$$I_\delta(s)\coloneqq\int_{\max(\frac{\bar\gamma_{\rm m}}{\bar\gamma_{\rm e}}-\delta,1)}^{\max(\frac{\bar\gamma_{\rm m}}{\bar\gamma_{\rm e}}+\delta,1)}\frac{y^{s-2}}{1+\frac{\bar\gamma_{\rm e}}{\bar\gamma_{\rm m}}y}e^{-\frac{y}{\bar\gamma_{\rm m}}}\mathrm{d}y, \tag{27}$$

and

$$I_2^k(s)\coloneqq\sum_{n=0}^{k}(-1)^n\bar\gamma_{\rm e}^{-(n+1)}\bar\gamma_{\rm m}^{s-1}\cdot\Gamma\bigg(s-n-2,\frac{\max\big(\frac{\bar\gamma_{\rm m}}{\bar\gamma_{\rm e}}+\delta,1\big)}{\bar\gamma_{\rm m}}\bigg), \tag{28}$$

for $k\geq 0$. □

Proof: To prove Lemma 1, we utilize the series expansion $\frac{1}{1+x}=\sum_{n=0}^{\infty}(-1)^nx^n$, for $|x|<1$. To make sure $|x|<1$, using a similar approach as in [18], we split the integration boundary into three parts and let $k\to\infty$. For the first part, we have for any small $\delta>0$ and $\bar\gamma_{\rm m}/\bar\gamma_{\rm e}>1+\delta$

$$\begin{aligned}I_1^{\infty}(s)&=\int_1^{\frac{\bar\gamma_{\rm m}}{\bar\gamma_{\rm e}}-\delta}\sum_{n=0}^{\infty}(-1)^n\big(\frac{\bar\gamma_{\rm e}}{\bar\gamma_{\rm m}}y\big)^ny^{s-2}e^{-\frac{y}{\bar\gamma_{\rm m}}}\mathrm{d}y\\&\overset{(a)}{=}\sum_{n=0}^{\infty}(-1)^n\bar\gamma_{\rm e}^n\bar\gamma_{\rm m}^{s-1}\int_{1/\bar\gamma_{\rm m}}^{(\frac{\bar\gamma_{\rm m}}{\bar\gamma_{\rm e}}-\delta)/\bar\gamma_{\rm m}}q^{s+n-2}e^{-q}\mathrm{d}q\\&\overset{(b)}{=}\sum_{n=0}^{\infty}(-1)^n\bar\gamma_{\rm e}^n\bar\gamma_{\rm m}^{s-1}\Bigg(\Gamma\bigg(s+n-1,\frac{1}{\bar\gamma_{\rm m}}\bigg)\\&\qquad-\Gamma\bigg(s+n-1,\frac{\bar\gamma_{\rm m}/\bar\gamma_{\rm e}-\delta}{\bar\gamma_{\rm m}}\bigg)\Bigg),\end{aligned} \tag{29}$$

where in (a), we use the change of variable $q=\frac{y}{\bar\gamma_{\rm m}}$. Step (b) follows from the definition of incomplete Gamma function $\Gamma(a,b)$. If $\bar\gamma_{\rm m}/\bar\gamma_{\rm e}\leq 1+\delta$, then the upper limit of the integral becomes 1 which leads to $I_1^{\infty}(s)=0$.

For the second integral term in (24), we have

$$I_\delta(s)=\int_{\max(\frac{\bar\gamma_{\rm m}}{\bar\gamma_{\rm e}}-\delta,1)}^{\max(\frac{\bar\gamma_{\rm m}}{\bar\gamma_{\rm e}}+\delta,1)}\frac{y^{s-2}}{1+\frac{\bar\gamma_{\rm e}}{\bar\gamma_{\rm m}}y}e^{-\frac{y}{\bar\gamma_{\rm m}}}\mathrm{d}y, \tag{30}$$

which tends to zero as $\delta\to 0$. The last term in (24) is obtained as

$$\begin{aligned}I_2^{\infty}(s)&=\int_{\max(\frac{\bar\gamma_{\rm m}}{\bar\gamma_{\rm e}}+\delta,1)}^{\infty}\sum_{n=0}^{\infty}(-1)^n\big(\frac{\bar\gamma_{\rm m}}{\bar\gamma_{\rm e}y}\big)^n\frac{\bar\gamma_{\rm m}}{\bar\gamma_{\rm e}y}y^{s-2}e^{-\frac{y}{\bar\gamma_{\rm m}}}\mathrm{d}y\\&\overset{(a)}{=}\sum_{n=0}^{\infty}(-1)^n\bar\gamma_{\rm e}^{-(n+1)}\bar\gamma_{\rm m}^{s-1}\\&\qquad\cdot\int_{\max(\frac{\bar\gamma_{\rm m}}{\bar\gamma_{\rm e}}+\delta,1)/\bar\gamma_{\rm m}}^{\infty}q^{s-n-3}e^{-q}\mathrm{d}q\\&=\sum_{n=0}^{\infty}(-1)^n\bar\gamma_{\rm e}^{-(n+1)}\bar\gamma_{\rm m}^{s-1}\\&\qquad\cdot\Gamma\bigg(s-n-2,\frac{\max\big(\frac{\bar\gamma_{\rm m}}{\bar\gamma_{\rm e}}+\delta,1\big)}{\bar\gamma_{\rm m}}\bigg),\end{aligned} \tag{31}$$

where in (a), we set $q=\frac{y}{\bar\gamma_{\rm m}}$. ■

This results in the following theorem for the Mellin transform of the cumulative service process of the wiretap Rayleigh fading channel.

Theorem 1: Given the wiretap Rayleigh fading channel and assuming block fading, the offered service is characterized by

$$\begin{aligned}\mathbb{M}_{\mathcal{S}}(s,\tau,t)&=\big(\mathbb{M}_g(s)\big)^{t-\tau}\\&=\Big(1+\big(I_1^{\infty}(s)+I_\delta(s)+I_2^{\infty}(s)\big)(s-1)e^{\frac{1}{\bar\gamma_{\rm m}}}\Big)^{t-\tau},\end{aligned} \tag{32}$$

for any $s<1$. □

Proof: We first proceed to derive $\mathbb{M}_Y(s)$ with Y defined in (20). We have

$$
\begin{aligned}
\mathbb{M}_Y(s) &= \mathbb{E}\big[Y^{s-1}\big] \\
&= \frac{1}{1-F_Z(1)} \int_1^\infty y^{s-1} \mathrm{d}F_Z(y) \\
&\overset{(a)}{=} \frac{1}{1-F_Z(1)} \Bigg(y^{s-1} F_Z(y)\Big|_1^\infty \\
&\qquad - (s-1) \int_1^\infty y^{s-2} \left(1 - \frac{\bar{\gamma}_\mathrm{m}}{\bar{\gamma}_\mathrm{e} y + \bar{\gamma}_\mathrm{m}} e^{-\frac{y-1}{\bar{\gamma}_\mathrm{m}}}\right) \mathrm{d}y \Bigg) \\
&= \frac{1}{1-F_Z(1)} \Bigg(- F_Z(1) - y^{s-1}\Big|_1^\infty \\
&\qquad + (s-1) \int_1^\infty \frac{y^{s-2}}{1 + \frac{\bar{\gamma}_\mathrm{e}}{\bar{\gamma}_\mathrm{m}} y} e^{-\frac{y-1}{\bar{\gamma}_\mathrm{m}}} \mathrm{d}y \Bigg) \\
&= 1 + \frac{(s-1) e^{\frac{1}{\bar{\gamma}_\mathrm{m}}}}{1-F_Z(1)} I(s), \qquad (33)
\end{aligned}
$$

for $s < 1$, where $I(s)$ is defined in (24). Step (a) follows from integration by part, in which, the first term converges to zero if $s < 1$. The solution to the integral $I(s)$ is given by Lemma 1.

Therefore, substituting $F_Z(1) = \frac{\bar{\gamma}_\mathrm{e}}{\bar{\gamma}_\mathrm{e}+\bar{\gamma}_\mathrm{m}}$ from (19) and $\mathbb{M}_Y(s)$ from (33) into (23) completes the proof. ∎

The above Mellin transform of the service process includes infinite sums (cf. Lemma 1), however, we are only interested in an upper bound of the service Mellin transform $\mathbb{M}_g(s)$ for $s < 1$ which provides an upper bound on the delay violation probability. Based on the result of [18, Corollary 1], truncating the sums at *even* values of k always gives an upper bound on the integral $I(s)$ in Lemma 1, and thus, leads to a valid closed-form delay bound which can be computed in a straightforward manner.

From the analysis of service process characterization of the wiretap fading channel above, we can observe that the Mellin transform of the service process, although not the same, is related to the Mellin transform of the service process in the interference channel presented in our prior work [18]. This observation provides an interesting relation between the wiretap and interference channels in the sense that having either eavesdropper(s) or interferer(s) in the system penalizes the service offered by the corresponding channels in a similar fashion. It also suggests that a general form for the service process of these and other types of channels may be possible. Although in the wiretap channel the secrecy capacity can be zero in certain transmission slots, analysis of the service process in both channels are tightly connected. Therefore, results obtained for one case can potentially offer some insights for the other.

IV. Numerical Evaluations

In this section, we study the delay performance of the wiretap Rayleigh fading channel via numerical evaluations based on the analytical model that we derived in the previous section. In particular, we first validate our analytical bound for the delay performance by means of simulations. Then, we proceed to investigate the effects of different arrival rates and eavesdropper's channel quality on the secure wireless transmission using the analytical results. We further study the impact of burstiness of the arrival traffic on the delay in this setup. Finally, we show that even when the eavesdropper's channel is on average better than the main channel, secure transmission with low delay is possible if the arrival rate, i.e. the rate at which traffic is generated at the source, is small enough.

First, we validate our analysis in Section III against simulations. The analytical bound is computed using (4) and (12), with the corresponding stability conditions, and the Mellin transforms of the constant-rate arrival process in (13) and the service process derived in (32) for the wiretap Rayleigh fading channel. In order to validate the analytical bound on the distribution of the delay, we empirically determined the actual distribution by simulating the queueing system over 10^{10} transmission slots. Fig. 1 shows the delay bound, w_ε, measured in transmission slots versus the delay violation probability, ε in (3), as well as the delay in the simulated system. The results are shown for a constant arrival rate of $\rho = 1$ bit/symbol, fixed average SNR of the main channel $\bar{\gamma}_\mathrm{m} = 15$ dB, and two different values of the average SNR of the eavesdropper's channel $\bar{\gamma}_\mathrm{e}$. The figure depicts that the computed delay bound is indeed an upper bound for the simulated delay performance for secure communication in the system. More importantly, in all cases the slope, i.e., the exponential decay, of the analytical and simulated curves are exactly the same, and therefore, the relative gap diminishes as the delay grows larger. Hence, our analytical bound is a good characterization of the system performance. In the remaining part of this section, we focus on characterizing the system performance based solely on the derived bounds.

In Fig. 2, we fix the delay violation probability to $\varepsilon = 10^{-4}$ and show the delay performance w_ε versus increasing arrival rate ρ of a constant-rate arrival process. The main channel's average SNR is set to $\bar{\gamma}_\mathrm{m} = 15$ dB and the eavesdropper's average SNR is chosen such that we have the ratio of the average SNRs (in linear scale) as $\frac{\bar{\gamma}_\mathrm{e}}{\bar{\gamma}_\mathrm{m}} = \{0.1, 0.2, 0.3, 0.5, 0.8\}$. First, it can be observed that as the arrival rate of the traffic increases the delay for secure transmission of this traffic increases drastically. In addition, the figure also depicts that as the average SNR ratio of the eavesdropper's channel to the main channel increases, which corresponds to the eavesdropper being closer to the source (assuming constant transmit power), the delay performance deteriorates. That is, as the eavesdropper's channel becomes better on average, for a specific delay constraint the source can only handle secure transmission of an incoming traffic with a much lower rate.

Next in Fig. 3, we show the delay performance versus the eavesdropper average SNR when the arrival traffic is bursty. More specifically, we consider the Markov modulated ON-OFF arrival process as described in Section III-B, with burst rate r and average rate $\bar{r}$. The burst-to-average rate ratio $r/\bar{r}$ is related to the Markov state transition probabilities as $r/\bar{r} = \frac{\alpha+\beta}{\alpha}$. Furthermore, α and β are chosen such that the

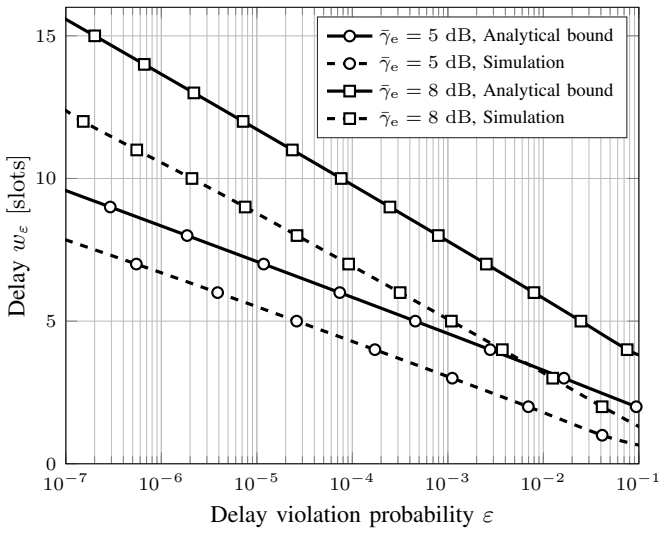

Fig. 1. Validation of the analytical bound with simulations for the delay performance of wiretap Rayleigh fading channel: Delay (w_ε) in slots versus delay violation probability (ε) with constant arrival rate $\rho = 1$ bit/symbol, main channel's average SNR $\bar{\gamma}_\mathrm{m} = 15$ dB, and different values of eavesdropper channel's average SNR $\bar{\gamma}_\mathrm{e} \in \{5, 8\}$ dB, and 10^{10} simulated transmission slots.

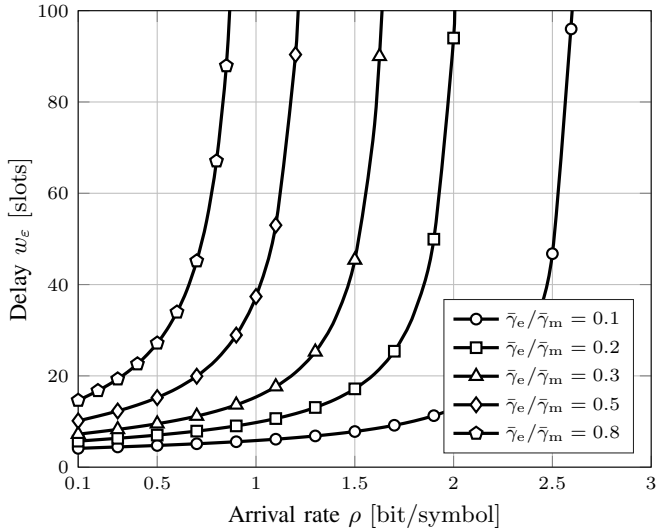

Fig. 2. Delay (w_ε) in slots versus arrival rate (ρ) in bit/symbol with fixed delay violation probability $\varepsilon = 10^{-4}$ and main channel's average SNR $\bar{\gamma}_\mathrm{m} = 15$ dB for different ratios of eavesdropper to main channel's average SNR $\frac{\bar{\gamma}_\mathrm{e}}{\bar{\gamma}_\mathrm{m}} = \{0.1, 0.2, 0.3, 0.5, 0.8\}$.

average cycle time of the Markov chain is 10 time slots, i.e., $\frac{1}{\alpha} + \frac{1}{\beta} = 10$. We plot the delay performance for different burst-to-average rate ratio of $\frac{r}{\bar{r}} = \{1, 1.5, 2.0\}$. Note that the case $r = \bar{r}$ corresponds to the constant-rate arrival model. First, we can see again that as the eavesdropper's channel average SNR increases, the delay increases. The second and more interesting observation from this figure is that when low latency is required, bursty arrival traffic is more difficult to handle than constant-rate traffic. For instance, if we consider systems that have:

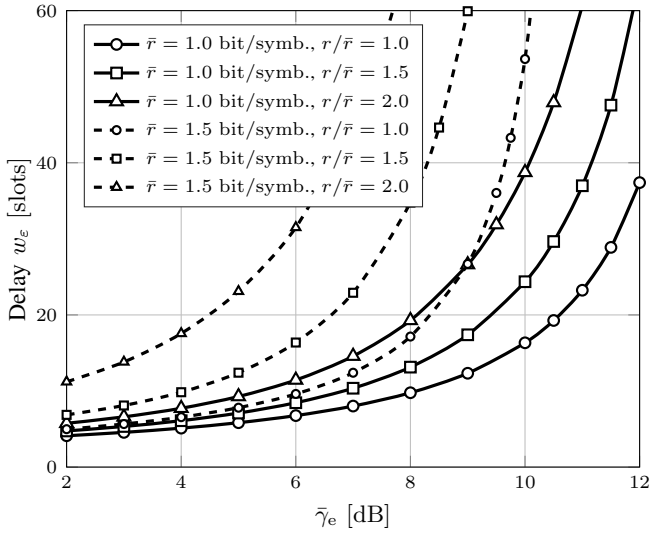

Fig. 3. Effect of bursty traffic with Markov modulated ON-OFF traffic model: Delay (w_ε) in slots versus eavesdropper channel's average SNR $\bar{\gamma}_e$ with fixed delay violation probability $\varepsilon = 10^{-4}$, main channel's average SNR $\bar{\gamma}_\mathrm{m} = 15$ dB, and different values of average arrival rate $\bar{r} = \{1, 1.5\}$ bit/symbol and burst-to-average rate ratio $\frac{r}{\bar{r}} = \{1, 1.5, 2\}$.

1) bursty arrival with $r/\bar{r} = 2.0$ and $\bar{r} = 1$ bit/symbol (the triangle-solid curve) and
2) constant-rate arrival ($r/\bar{r} = 1$), but with higher average rate $\bar{r} = 1.5$ bit/symbol (the circled-dashed curve),

we observe that when the eavesdropper's SNR is below 9 dB, the delay in the first system with bursty arrivals is worse than that in the second system, even though the average amount of data to be transmitted is much lower. Thus, the burstiness of the arrival traffic may have a severe impact on the delay.

Finally, in Fig. 4, we consider constant-rate traffic and show the delay violation probability versus the average SNR of eavesdropper's channel for a fixed average SNR in the main channel, which is set to $\bar{\gamma}_\mathrm{m} = 15$ dB, and different arrival rates. The vertical dashed-line depicts the point where $\bar{\gamma}_\mathrm{e} = \bar{\gamma}_\mathrm{m}$ resulting in zero secrecy capacity for the wiretap Gaussian channel. However, we can see that for the wiretap Rayleigh fading channel and for a certain delay constraint, it would still be possible to communicate securely in the region to the right side of the vertical line where the eavesdropper's channel is better than the main channel, on average, if the arrival rate of the traffic is low enough. This is also in line with previous findings, for instance in [6], for the wiretap fading channels.

V. Conclusions

In this paper, we considered delay bounds of the wiretap Rayleigh fading channel. We used stochastic network calculus to evaluate the delay performance, and derived the Mellin transform of the service in the wiretap fading channel. These derivations show structural relations between the wiretap channel and the interference channel. Our numerical results show in particular a high sensitivity of the wiretap delay performance to bursty arrival traffic.

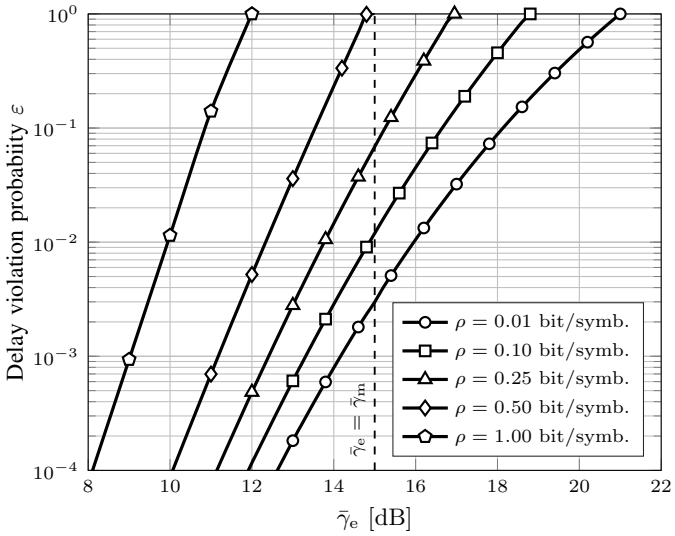

Fig. 4. Delay violation probability (ε) versus eavesdropper channel's average SNR $\bar{\gamma}_{\rm e}$ with fixed delay constraints $w_\varepsilon = 10$ slots, main channel's average SNR $\bar{\gamma}_{\rm m} = 15$ dB, and different values of arrival rate $\rho = \{0.01, 0.1, 0.25, 0.5, 1\}$ bit/symbol. The vertical dashed-line depicts the point where $\bar{\gamma}_{\rm e} = \bar{\gamma}_{\rm m}$ resulting in zero secrecy capacity in the Gaussian channel.

While this work analyzed single-hop transmission with a single eavesdropper, future analysis could include multi-hop channels with several eavesdroppers, as well as attack schemes that use a combination of interference/jamming and eavesdropping.

REFERENCES

[1] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Commun. and Inf. Theory*, vol. 5, no. 4-5, pp. 355–580, 2008.

[2] R. Liu and W. Trappe, Eds., *Securing Wireless Communications at the Physical Layer*. Springer, 2010.

[3] C. E. Shannon, "Communication for secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[4] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1335–1387, Jan. 1975.

[5] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[6] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[7] Y. Liang, H. V. Poor, and S. S. (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[8] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[9] Y. Liang, H. V. Poor, and L. Ying, "Wireless broadcast networks: Reliability, security, and stability," in *Proc. Inf. Theory and Applications Workshop (ITA)*, San Diego, CA, Jan. 2009, pp. 249–255.

[10] K. Khalil, M. Youssef, O. O. Koyluoglu, and H. E. Gamal, "On the delay limited secrecy capacity of fading channels," in *Proc. IEEE Int. Symp. on Inf. Theory (ISIT)*, Seoul, South Korea, Jun. 2009, pp. 2617–2621.

[11] O. Gungor, J. Tan, C. E. Koksal, H. El-Gamal, and N. B. Shroff, "Secrecy outage capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5379–5397, Sep. 2013.

[12] Z. Mao, C. E. Koksal, and N. B. Shroff, "Achieving full secrecy rate with low packet delays: An optimal control approach," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1944–1956, Sep. 2013.

[13] A. E. Shafie and N. Al-Dhahir, "On secure communications over a wiretap channel with fixed-rate transmission: Protocol design and queueing analysis," vol. 4, no. 4, pp. 453–456, Aug. 2015.

[14] D. Qiao, M. C. Gursoy, and S. Velipasalar, "Secure broadcasting over fading channels with statistical QoS constraints," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Miami, FL, Dec. 2010.

[15] ——, "Secure wireless communication and optimal power control under statistical queueing constraints," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 628–639, Sep. 2011.

[16] D. Wu and R. Negi, "Effective capacity: A wireless link model for support of quality of service," *IEEE Trans. Wireless Commun.*, vol. 2, no. 4, pp. 630–643, Jul. 2003.

[17] H. Al-Zubaidy, J. Liebeherr, and A. Burchard, "Network-layer performance analysis of multihop fading channels," *IEEE/ACM Trans. Netw.*, vol. 24, no. 1, pp. 204–217, Feb. 2016.

[18] S. Schiessl, F. Naghibi, H. Al-Zubaidy, M. Fidler, and J. Gross, "On the delay performance of interference channels," in *IFIP Networking Conference*, Vienna, Austria, May 2016, pp. 216–224.

[19] Y. Jiang and P. J. Emstad, "Analysis of stochastic service guarantees in communication networks: A server model," in *Proc. IEEE/ACM Int. Workshop on Quality of Service (IWQoS)*, Passau, Germany, Jun. 2005, pp. 233–245.

[20] M. Fidler, "A network calculus approach to probabilistic quality of service analysis of fading channels," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, San Francisco, CA, Nov. 2006.

[21] B. Davies, *Integral Transforms and Their Applications*. Springer-Verlag, 1978.

[22] C.-S. Chang, *Performance Guarantees in Communication Networks*. Springer-Verlag, 2000.