Hindawi
Security and Communication Networks
Volume 2021, Article ID 8650272, 19 pages
https://doi.org/10.1155/2021/8650272

Research Article

Secure Rate Control and Statistical QoS Provisioning for Cloud-Based IoT Networks

Irfan Muhammad, Hirley Alves, Onel Alcaraz López, and Matti Latva-aho

Centre for Wireless Communications (CWC), University of Oulu, Oulu, Finland

Correspondence should be addressed to Irfan Muhammad; irfan.muhammad@oulu.fi

Received 22 July 2021; Accepted 23 September 2021; Published 29 October 2021

Academic Editor: Shehzad Ashraf Chaudhry

The Internet of Things (IoT) facilitates physical things to detect, interact, and execute activities on-demand, enabling a variety of applications such as smart homes and smart cities. However, it also creates many potential risks related to data security and privacy vulnerabilities on the physical layer of cloud-based Internet of Things (IoT) networks. These can include different types of physical attacks such as interference, eavesdropping, and jamming. As a result, quality-of-service (QoS) provisioning gets difficult for cloud-based IoT. This paper investigates the statistical QoS provisioning of a four-node cloud-based IoT network under security, reliability, and latency constraints by relying on the effective capacity model to offer enhanced QoS for IoT networks. Alice and Bob are legitimate nodes trying to communicate with secrecy in the considered scenario, while an eavesdropper Eve overhears their communication. Meanwhile, a friendly jammer, which emits artificial noise, is used to degrade the wiretap channel. By taking advantage of their multiple antennas, Alice implements transmit antenna selection, while Bob and Eve perform maximum-ratio combining. We further assume that Bob decodes the artificial noise perfectly and thus removes its contribution by implementing perfect successive interference cancellation. A closed-form expression for an alternative formulation of the outage probability, conditioned upon the successful transmission of a message, is obtained by considering adaptive rate allocation in an ON-OFF transmission. The data arriving at Alice's buffer are modeled by considering four different Markov sources to describe different IoT traffic patterns. Then, the problem of secure throughput maximization is addressed through particle swarm optimization by considering the security, latency, and reliability constraints. Our results evidence the considerable improvements on the delay violation probability by increasing the number of antennas at Bob under strict buffer constraints.

1. Introduction

Recent advancements in communication technologies and antenna design have drastically increased the amount of data collected from Internet of Things (IoT) environments. They have also catalyzed the growing trend towards big data, where data acquisition and posterior data processing are actionable and trigger intelligent decision-making [1]. Although IoT devices are advancing in terms of their sensing functions, enhanced decision-making capabilities and ubiquitous processing are still not possible as they require a higher quantum of computer power. Cloud-based IoT infrastructure is a potential setup that can offer such capabilities and provide higher reliability as cloud computing can collect, process, and store huge amounts of data. However, before such a system can be fully realized, they need to ensure data security and privacy and handle the heterogeneity of IoT devices and networks. In particular, cloud-based IoT networks currently suffer from physical attacks that include interference, eavesdropping, and jamming, making quality-of-service (QoS) provisioning complicated for cloud-based IoT.

The newly launched fifth generation new radio (5G NR) facilitates the digital transformation of communication infrastructure and particularly increases the overall performance of various vertical sectors. It is apparent that 5G networks are not able to sufficiently meet most of the stringent specifications of communication technologies. In turn, the continued growth of the community through 2030 would lead to new and more strict demands on wireless

communications [2]. With the rise of the sixth generation (6G) of cellular systems, which targets a fully digitized and hyperconnected society for the coming years, IoT would play a predominant role. However, IoT imposes a large variety of critical challenges since it differs significantly from traditional human-type communications. Therefore, the transmission schemes and traffic management strategies for IoT networks must consider their unique traffic characteristics [3]. For instance, different IoT applications may have different requirements, such as priority and delay constraints; thus, there is a need for considering mixed traffic models with event-driven and periodic traffics. The different traffic pattern properties of IoT devices demand the study of accurate traffic models that can capture their behaviour. A traffic model for automotive IoT, considering the spatially and temporally correlated bursty traffic, was proposed in [4]. Such a model is based on a coupled Markovian arrival process (CMAP) and can capture burstiness and multimodality of arrival rates. In [5], authors examined IoT traffic using traditional Markovian arrival processes since they are able to capture the traffic burstiness inherent to many IoT use cases. Moreover, authors in [6] analyzed different types of traffic generated by IoT devices through effective rate transmission and the effective capacity for single-antenna point-to-point communication systems.

Due to enormous growth in IoT devices, an increasing requirement of private and confidential data transmission has made security a critical issue for cloud-based IoT networks. Traditionally, security is realized via cryptography techniques, i.e., public key infrastructure (PKI) [7]. However, cryptography and its associated techniques have shown vulnerability to secure information as they rely on an assumption of infinite computational capability available at the adversary side for their operation. Furthermore, they require high bandwidth and computational complexity. Different challenges in key management schemes for decentralized wireless networks have been identified in [8]. Therefore, physical layer (PHY) security (or in other words, information-theoretic security) has become an attractive candidate to offer alternative security solutions by adding an extralayer of security [9]. While security issues in the physical layer are typically addressed by reducing the risk of information leakage to an external bad actor [10], the more alarming threat to user privacy from the discovery of the existence of a message has not been mitigated yet. Therefore, this paper addresses this threat by considering rate control and quality-of-service (QoS) provisioning to minimize the outage secrecy probability and mitigate privacy leakage in IoT networks. A fundamental issue lies in efficiently providing QoS guarantees in wireless channels, which are drastically affected with the randomness induced by the environment. Therefore, it is imperative to model a wireless channel for satisfying certain QoS metrics such as data rate, delay, and delay violation probability. In that sense, statistical QoS provisioning, where many applications or services can tolerate a small probability of QoS violation [11,12], is a viable tool for characterizing and satisfying delay bound QoS guarantees in real-time wireless traffic [13]. Authors in [14] proposed to move the channel model from PHY to the link layer by introducing a link-layer performance metric called effective capacity that captures a link-level capacity notion of the fading channel in the presence of statistical QoS limitations. Furthermore, effective capacity is defined as the maximum constant arrival rate that the service rate can support to guarantee the specified statistical delay-bounded requirement over a wireless channel. Thus, effective capacity is equivalent to effective bandwidth that helps in analyzing the resources needed for supporting different time-varying arrival processes. Recently, the effective capacity theory has been used as a relevant cross-layer designing tool that allows to link PHY to the statistical QoS performance of upper layers in several different scenarios [15–17], while ensuring high security fidelity.

For instance, two resource allocation algorithms based on effective capacity for multiple-input multiple-output (MIMO) networks serving multiple users with different statistical QoS requirements were proposed in [15]. A detailed analysis of the effective capacity for a MIMO wireless system with low-power, wideband, and high signal-to-noise ratio (SNR) regimes was carried out in [16], where statistical queuing constraints were imposed as a limitation on buffer violation probabilities in the large-queue-length regime. Meanwhile, the authors in [17] investigated the throughput and energy efficiency of a MIMO system subject to a statistical QoS constraint. However, as the traffic originated from IoT devices is massive due to the large number of devices in a IoT network, such networks require the support of per-link bit rate, delay and reliability, and security, which is not addressed in the above works. IoT devices also have additional constraints with respect to limited computational and energy capabilities [18]. Specifically, challenges regarding privacy and secrecy are highly critical in IoT as these networks are prone to eavesdropping due to the large-scale deployment of vulnerable devices. Hence, providing security and reliability in this context proves to be a challenging and demanding task.

1.1. Motivation and Contribution. In order to fill in the gap above in the literature, herein we propose the use of PHY security, which has emerged as a promising way to achieve security against any level of computational power [19], thus being attractive to safeguarding future networks. The basic idea behind PHY security is to provide secure communications by taking advantage of fading and interference phenomena. We obtained a novel exact expression for the secrecy outage probability conditioned upon a message being transmitted for the considered wiretap system with CSI at the transmitter. In this work, inspired by [20–22], we rely on the effective capacity theory in order to examine the joint impact of security, latency, and reliability constraints of cloud-based IoT networks for the four-node multiantenna scenario. To the best of our knowledge, traffic models with secure effective capacity and jamming have not been yet analyzed under security, reliability, and latency constraints in the literature. As novel contributions, herein

(i) A novel and exact closed-form expression for the secrecy outage probability is provided for the proposed scenario, conditioned upon a message

actually being transmitted. As a byproduct, we also provide a simpler closed-form expression of secrecy outage probability when all nodes are equipped with a single antenna.

(ii) We further extend [21] to the multiantenna wiretap channel and analyze the secure effective capacity for an ON-OFF transmission under jamming while analyzing the traffic originated by a massive number of IoT devices through Markovian sources.

(iii) We solve the design problem of maximizing the secure throughput by considering both security and reliability constraints for an adaptive rate allocation scheme in an ON-OFF fashion through particle swarm optimization (PSO).

(iv) We show that the number of antennas at Bob as compared with Alice and Wiley plays a significant role in meeting stringent requirements of reliability and security, while it also decreases delay violation probability under strict QoS exponent.

The remainder of this paper is organized as follows. Section 2 discusses the related work. Section 3 introduces the system model and our main assumptions. Section 4 presents the secrecy outage probability analysis. Section 5 provides the traffic models and statistical QoS provisioning. Section 6 presents the analysis of the source models, while Section 7 shows the secure effective capacity maximization. Section 8 discusses the numerical results, and Section 9 concludes the paper.

Notation. Hereafter, we denote scalar variables by italic symbols, while vectors and matrices are denoted by lowercase and upper-case boldface symbols, respectively. Given a complex vector $\mathbf{x}$, $\|\mathbf{x}\|$ denotes the Euclidean norm, while $\mathbf{x}^T$ and $\mathbf{x}^\dagger$ denote transpose and conjugate transpose operations, respectively. The $m \times m$ identity matrix is represented as $\mathbf{I}_m$. The probability density function (PDF) and cumulative distribution function (CDF) of a given random variable X are denoted as $f_X(x)$ and $F_X(x)$, respectively, while the expectation operator is denoted as $\mathbb{E}[\cdot]$. The gamma function is denoted as $\Gamma(z)$ (see Section 6, Equation 6.1.1 in [23]), while the regularized lower incomplete gamma function is denoted as $P(s,z) = \gamma(s,z)/\Gamma(z)$ (see Section 6, Equation 6.5.1 in [23]), and the regularized upper incomplete gamma function is represented as $Q(s,z) = \Gamma(s,z)/\Gamma(z)$ (see Equation 26.4.19 in [23]), where $\gamma(s,z)$ and $\Gamma(s,z)$ are the lower and upper incomplete gamma functions (see Section 6, Equation 6.5 in [23]), respectively. The Gauss hypergeometric function is denoted as ${}_2F_1(a,b;c;z)$ (see Equation 15.1.1 in [23]), while the inverse of the generalized regularized incomplete gamma function is represented as $P^{-1}(s,z)$ [24]. We also use the common notation $[z]^+ = \max\{0,z\}$, while the probability of event A is represented as $\Pr\{A\}$.

2. Literature Review

The idea of using artificial noise to degrade further the wiretap channel was initially introduced by [25]. Several works have been shown to be effective for enhancing the secrecy of wireless networks at the PHY [20,26–29]. In [27], the throughput of securely transmitted delay-sensitive data originated from random sources was analyzed while the secrecy capacity for MIMO wiretap channel in the low-SNR regime was studied in [28]. Moreover, multiantenna diversity techniques have been shown to enhance the secrecy performance in [20, 29]. Particularly, the MIMO multiple eavesdropper (MIMOME) scenario has renewed attention in the last years [30–32]. In [30], the impact of transmit antenna selection (TAS) over a massive MIMO scenario by considering no information about Eve's channel state information (CSI) at the transmitter was studied. In [32], authors carried out secrecy performance of MIMOME scenario using TAS at the transmitter and either maximum-ratio combining (MRC) or selection combining (SC) at the receiver and an eavesdropper with perfect feedback. While in [31], the effect of imperfect feedback on secrecy performance was studied using TAS/MRC-based PHY security scheme for MIMO wiretap channels. Furthermore, the authors in [33] utilized jamming strategy for the MIMOME system using TAS/MRC schemes over κ-μ fading channels.

Regarding IoT QoS constraints, the authors in [34] proposed the concept of effective secure throughput based on effective capacity metric in order to take into account security and reliability issues, while satisfying certain buffer or delay constraints. Furthermore, authors in [27] extended the results of [34] by analyzing the energy efficiency and the throughput of secure transmissions by looking into the delay-sensitive data that are generated by Markovian sources. Although the work in [27] is designed for broadband applications, its results are also applicable to IoT as Markovian processes can incorporate the properties of IoT devices traffic [21].

Despite the recent advances, the works above focused on the classical secrecy outage probability metric for evaluating the secrecy performance, i.e., the probability that the instantaneous secrecy capacity is less than a target secrecy rate [35]. Such formulation fails to capture the actual security level alone as it does not reflect the failure to attain perfect secrecy. An alternative formulation is presented in [22] which takes into account the rate of the transmitted code words as well as the condition under which message transmissions take place; thus, it is able to differentiate between a failure on attaining a secrecy transmission from a failure on attaining reliability. While authors in [22, 36] study the trade-off between security and reliability, the trade-off among security, latency, and reliability has not been studied yet. Moreover, a secure effective capacity metric was analyzed in [21] without considering friendly jammer, inspired on [27, 34]. The scenario comprises a single-antenna legitimate pair of IoT devices communicating in the presence of an eavesdropper and using an ON-OFF transmission where secrecy is conditioned on the actual transmission. The metric captures the impact of the source's arrival traffic, where security, latency, and reliability constraints were considered to evaluate the optimal secure communication rates.

3. System Model

We consider a four-node wiretap system as illustrated in Figure 1, where legitimate nodes, namely, Alice (transmitter) and Bob (receiver), communicate confidentially in the presence of a passive eavesdropper Eve, who intends to overhear the confidential communication between them. Additionally, we assume a friendly jammer named Wiley is deployed to transmit artificial noise, aiming to worsen the eavesdropper's channel quality.

All system nodes are equipped with multiple antennas, where N_A, N_B, N_E, and N_W denote the number of antennas at Alice, Bob, Wiley, and Eve, respectively. We assume that Bob and Eve can perfectly estimate their individual CSI, while Alice knows Bob's channel perfectly (we assume there is a separate and reliable mechanism to accurately acquire the CSI, for instance, by assuming channel reciprocity in time-division duplex (TDD) systems or by using dedicated pilot sequences [37]) but has just a statistical knowledge of Eve's CSI. Additionally, Bob and Alice share an open error-free feedback channel, which Bob utilizes to send back the index of Alice's antenna that allows achieving the best SNR at Bob, along with its corresponding value to enable ON-OFF transmissions, i.e., Alice transmits only when Bob's SNR exceeds some SNR threshold μ. Alice utilizes the index sent by Bob to implement TAS. Since legitimate and eavesdropper channels are not correlated, Eve is not able to exploit such information and cannot attain any diversity gain. Moreover, we consider a cloud (or centralized) radio access network (C-RAN) architecture, wherein Alice is connected to the edge cloud, as illustrated in Figure 1. It should be noted, in the C-RAN architecture, a common baseband processing unit (BBU) performs all the digital signal processing functionalities, while Alice implements limited radio operations [38]. Such centralized processing provides more processing capabilities and thus enables more effective implementation of cloud-based IoT networks. Besides, all channels in this system undergo block Rayleigh fading; thus, the channels coefficients remain unchanged over the block interval, and they vary independently for the subsequent block. We further assume that Bob decodes the artificial noise perfectly and thus removes its contribution by implementing perfect successive interference cancellation (SIC). The channel coefficients are represented by h_{ij}, with $i \in \{1, \ldots, N_A\}$ and $j \in \{1, \ldots, N_X\}$, with $X \in \{B, E, W\}$.

Hence, the index received by Alice from Bob is given by

$$i^* = \text{argmax}_{1 \le i \le N_A} \left\| \mathbf{h}_{iB} \right\|, \tag{1}$$

where $\mathbf{h}_{i_B} = [h_{i1}, h_{i2}, \ldots, h_{iN_B}]^T$ is the $N_B \times 1$ legitimate channel vector between the i–th transmit antenna at Alice and the N_B antennas at Bob. After TAS, Alice transmits the encoded message $x = [x(1), x(2), \ldots, x(n)]$ to Bob. The power of the transmitted message is limited by an average power constraint, that is, $1/n \sum_{j=1}^{n} \mathbb{E}[|x(j)|^2] \le P_A$, where P_A represents the transmit power of Alice. Then, Bob employs MRC, and the received signal becomes

$$y_B = \mathbf{h}_{i_B}^{\dagger} \mathbf{h}_{i_B} x + \mathbf{h}_{i_B}^{\dagger} \mathbf{n}_{i_B}, \tag{2}$$

where $\mathbf{n}_{i_B}$ is the $N_B \times 1$ additive white Gaussian noise vector at Bob such that $\mathbb{E}[\mathbf{n}_{i_B} \mathbf{n}_{i_B}^{\dagger}] = \mathbf{I}_{i_B} \sigma_B^2$ and σ_B^2 is the noise variance at each antenna. Thus, the instantaneous received SNR at Bob is given by

$$\gamma_B = \left\| \mathbf{h}_{iB} \right\|^2 \bar{\gamma}_{AB}, \tag{3}$$

where $\bar{\gamma}_{AB} = P_A / \sigma_B^2$ is the average SNR of legitimate link. The PDF and CDF of γ_B are, respectively, as follows [36]:

$$f_{\gamma B}(\gamma) = \frac{N_A \gamma^{N_B - 1}}{\Gamma\left(N_B \bar{\gamma}_{AB}^{N_B}\right)} \exp\left(-\frac{\gamma}{\bar{\gamma}_{AB}}\right) P\left(N_B, \frac{\gamma}{\bar{\gamma}_{AB}}\right)^{N_A - 1}, \tag{4}$$

$$F_{\gamma B}(\gamma) = P\left(N_B, \frac{\gamma}{\bar{\gamma}_{AB}}\right)^{N_A}. \tag{5}$$

Meanwhile, the received signal at Eve is given by

$$yE = \mathbf{h}_{i_E}^{\dagger} \mathbf{h}_{i_E} x + + \mathbf{h}_{i_w}^{\dagger} \mathbf{h}_{i_E} V + \mathbf{h}_{i_E}^{\dagger} \mathbf{n}_{i_E}, \tag{6}$$

where $\mathbf{h}_{i_E}$ is the $N_E \times 1$ eavesdropper channel vector, $\mathbf{n}_{i_E}$ is the $N_E \times 1$ additive white Gaussian noise vector at Eve such that $\mathbb{E}[\mathbf{n}_{i_E} \mathbf{n}_{i_E}^{\dagger}] = \mathbf{I}_{i_E} \sigma_E^2$, and σ_E^2 is the noise variance at each antenna. $\mathbf{h}_{i_W}$ is the $N_W \times 1$ artificial noise channel, and v is the artificial noise signal. Thus, the instantaneous received SNR at Eve is given by

$$\gamma_E = \frac{\left\| \mathbf{h}_{i_E} \right\|^2 \bar{\gamma}_{AE}}{1 + \left\| \mathbf{h}_{i_W} \right\|^2 \bar{\gamma}_{WE}}, \tag{7}$$

where $\bar{\gamma}_{AE} = P_A / \sigma_E^2$ is the average SNR of Alice to Eavesdropper link and $\bar{\gamma}_{WE} = 1 - P_A / \sigma_{WE}^2$. The PDF and CDF of γ_E are given, respectively, by

$$f_{\gamma_E}(\gamma) = \frac{\gamma_E^{N_e - 1} \exp\left(-\gamma_E / \bar{\gamma}_{AE}\right)}{\Gamma(N_e) \bar{\gamma}_{AE}^{N_e} \bar{\gamma}_{WE}^{N_w}} \left(\frac{\gamma_E}{\bar{\gamma}_{AE}} + \frac{1}{\bar{\gamma}_{WE}}\right)^{-N_w} \sum_{d=0}^{N_e} \binom{N_e}{d} \frac{\Gamma(N_w + d)}{\Gamma(N_w)} \left(\frac{\gamma_E}{\bar{\gamma}_{AE}} + \frac{1}{\bar{\gamma}_{WE}}\right)^{-d}, \tag{8}$$

$$F_{\gamma_E}(\gamma) = \sum_{d=0}^{N_e} \binom{N_e}{d} \frac{\Gamma(N_w + d)}{\Gamma(N_w)} \frac{\exp\left(-\gamma_E / \bar{\gamma}_{AE}\right)}{\Gamma(N_e) \bar{\gamma}_{WE}^{N_w}} \sum_{J=0}^{N_e - 1} \binom{N_e - 1}{J} \left(-\frac{1}{\bar{\gamma}_{WE}}\right)^{Ne - 1 - J} \left[\Gamma\left(1 + J - Nw - d, \frac{1}{\bar{\gamma}_{WE}}\right) - \Gamma\left(1 + J - Nw - d, \frac{\gamma}{\bar{\gamma}_{AE}} + \frac{1}{\bar{\gamma}_{WE}}\right)\right]. \tag{9}$$

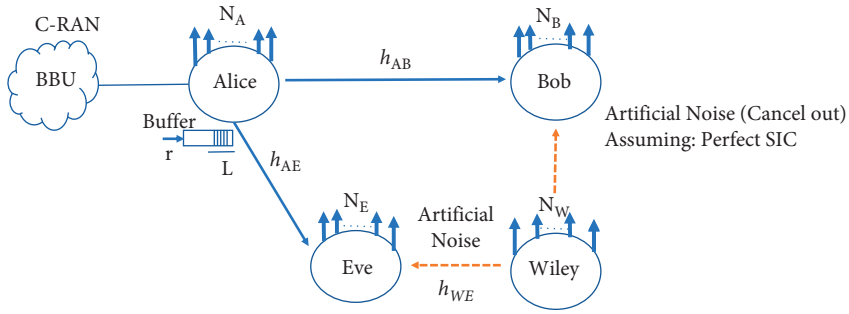

FIGURE 1: System model shows that Alice employs TAS while Bob and Eve resort to MRC. Herein, r is the arrival rate at source, L is queue length at the Alice, while h_{AB} and h_{AE} are channel coefficients of legitimate and wiretap channels.

This work aims to provide secure throughput maximization under security, reliability, and latency constraints. For that purpose, we consider the effective capacity model to link PHY with QoS constraints. We analyze the secure throughput for an ON-OFF transmission where secrecy is conditioned on actual transmission. Therefore, we first derive the secrecy outage probability for an adaptive rate allocation scheme to take security and reliability constraints into account as described in Section 4. Then, we assume Markovian arrivals at Alice, and we characterize the effective bandwidth under statistical QoS constraints such that we are able to capture the effects of latency and reliability in the secure throughput as discussed in Section 5.

4. Secrecy Outage Probability Analysis

We present the formulation for the secrecy outage probability proposed in [22], by considering an adaptive rate allocation scheme. For that purpose, we consider Wyner's encoding scheme, where the rate of transmitted code words is R_b and the secrecy rate is R_s. The resulting capacity of the legitimate and eavesdropping link is $C_b = \log_2[1+\gamma_B]$ and $C_e = \log_2[1+\gamma_E]$, respectively. Thus, $C_s = [C_b - C_e]^+$ is the secrecy capacity, and $R_e = R_b - R_s$ represents the rate penalty for securing the transmission against eavesdropping. Moreover, $C_b > R_b$ is the requirement for Bob to decode the information correctly. The probability of successful transmissions for this system is as follows:

$$\begin{aligned} P_{\text{tx}}(\mu) &= \Pr\{C_b > R_b\} \\ &= \Pr\{\gamma_B > \mu\} \\ &= 1 - F_{\gamma_B}(\mu), \end{aligned} \tag{10}$$

where $F_{\gamma_B}(\cdot)$ is given in (5). It is assumed that $\mu \geq 2^{R_s} - 1$ since the transmission will only occur whenever $C_b > R_s$. Then, the secrecy outage probability given that the transmission is successful on the legitimate channel can be expressed as follows [22]:

$$\begin{aligned} P_{\text{out}}(\mu, R_s) &= \Pr\{C_e > C_b - R_s | \gamma_B > \mu\} \\ &\overset{(a)}{=} \frac{\Pr\{\mu < \gamma_B < 2^{R_s}(1+\gamma_E) - 1\}}{p_s(\mu)} \\ &\overset{(b)}{=} \int_{((1+\mu)/2^{R_s})-1}^{\infty} \frac{F_{\gamma_B}\left(2^{R_s}(1+\gamma_E) - 1\right) f_{\gamma_E}(\gamma_E)\mathrm{d}\gamma_E}{1 - F_{\gamma_B}(\mu)} - \frac{\left(1 - F_{\gamma_E}\left((1+\mu)/2^{R_s} - 1\right)\right) F_{\gamma_B}(\mu)}{1 - F_{\gamma_B}(\mu)}, \end{aligned} \tag{11}$$

where step (a) comes from Equation (7) in [22] and step (b) is obtained by assuming independent random variables. A closed-form expression for the secrecy outage probability for the proposed scenario is presented next.

Theorem 1. *The secrecy outage probability, conditioned upon a successful transmission, for the considered wiretap system, where Alice employs TAS while Bob and Eve perform MRC, is*

$$
\begin{aligned}
P_{\text{out}}(\mu, R_s)_1 = {} & \frac{1}{P_{\text{tx}}(\mu)} \sum_{K=0}^{N_A} \binom{N_A}{K} (-1)^K \exp\left(\frac{\left(K 2^{R_s} \bar{\gamma}_{AE} + \bar{\gamma}_{AB}\right) - \bar{\gamma}_{WE} K \left(2^{R_s} - 1\right)}{\bar{\gamma}_{AB} \bar{\gamma}_{WE}} \right) \\
& \times \sum_{s_0 + s_1 + \cdots + s_{N_B - 1} = K} \binom{K}{s_0, s_1, \ldots, s_{N_B - 1}} \left(\prod_{t=0}^{N_B - 1} \frac{1}{(t!)^{s_t}} \right) \times \sum_{p=0}^{\alpha} \binom{\alpha}{p} \left(\frac{2^{R_s} - 1}{\bar{\gamma}_{AB}} \right)^{\alpha - p} \left(\frac{2^{R_s}}{\bar{\gamma}_{AB}} \right)^{p} \frac{1}{\Gamma(N_E) \bar{\gamma}_{AE}^{N_E} \bar{\gamma}_{WE}^{N_w}}, \\
& \sum_{d=0}^{N_e} \binom{N_e}{d} \frac{\Gamma(N_w + d)}{\Gamma(N_w)} \left(\bar{\gamma}_{AE}\right)^{p + N_E} \sum_{J=0}^{P + N_e - 1} \binom{p + N_e - 1}{J} \left(-\frac{1}{\bar{\gamma}_{WE}} \right)^{p + N_e - 1 - J}, \\
& \left(\frac{K 2^{R_s} \bar{\gamma}_{AE} + \bar{\gamma}_{AB}}{\bar{\gamma}_{AB}} \right)^{-1 - p + d + Nw} \Gamma\left[1 + p - Nw - d, \left(\frac{K 2^{R_s} \bar{\gamma}_{AE} + \bar{\gamma}_{AB}}{\bar{\gamma}_{AB}} \right) \left(\frac{1 + \mu - 2^{R_s}}{2^{R_s} \bar{\gamma}_{AE}} + \frac{1}{\bar{\gamma}_{WE}} \right) \right] \\
& - \frac{1}{P_{\text{tx}}(\mu)} P\left(N_B, \frac{\mu}{\bar{\gamma}_{AB}} \right)^{N_A} \left(1 - \sum_{d=0}^{N_e} \binom{N_e}{d} \frac{\Gamma(N_w + d)}{\Gamma(N_w)} \frac{\exp\left(1/\bar{\gamma}_{WE}\right)}{\Gamma(N_e) \bar{\gamma}_{WE}^{N_w}} \sum_{J=0}^{N_e - 1} \binom{N_e - 1}{J} \left(-\frac{1}{\bar{\gamma}_{WE}} \right)^{Ne - 1 - J} \right. \\
& \left. \left[\Gamma\left(1 + J - Nw - d, \frac{1}{\bar{\gamma}_{WE}} \right) - \Gamma\left(1 + J - Nw - d, \frac{1 + \mu - 2^{R_s}}{2^{R_s} \bar{\gamma}_{AE}} + \frac{1}{\bar{\gamma}_{WE}} \right) \right] \right).
\end{aligned}
\tag{12}
$$

Proof. See Appendix A.

We are aware that the formulation shown in Theorem 1 is quite intricate. Therefore, in the following, we provide simpler and easy to evaluate single-antenna case closed-form expression of secrecy outage probability when all nodes have a single antenna:

$$
\begin{aligned}
P_{\text{out}}(\mu, R_s) = {} & \frac{\exp\left(-\left(\left(\mu + 1 - 2^{Rs} \right) \bar{\gamma}_{AE} / 2^{Rs} \right) \right) \bar{\gamma}_{AE}}{\bar{\gamma}_{AE} + \left(\left(\mu + 1 - 2^{Rs} \right) \bar{\gamma}_{WE} / 2^{Rs} \right)} \\
& - \frac{1}{\bar{\gamma}_{WE}} \exp\left(\frac{\left(\mu + 1 - 2^{Rs} \right) \bar{\gamma}_{WE} + \bar{\gamma}_{AB} + 2^{Rs} \bar{\gamma}_{AE} \bar{\gamma}_{WE}}{\bar{\gamma}_{AB}} \right) \left[\frac{2^{Rs} \bar{\gamma}_{WE}}{\left(\mu + 1 - 2^{Rs} \right) \bar{\gamma}_{AE} \bar{\gamma}_{WE} + 2^{Rs}} \right. \\
& \exp\left(-\left(\frac{\bar{\gamma}_{AB} + 2^{Rs} \bar{\gamma}_{AE}}{\bar{\gamma}_{AB}} \right) \left(\frac{\left(\mu + 1 - 2^{Rs} \right) \bar{\gamma}_{AE} \bar{\gamma}_{WE} + 2^{Rs}}{\bar{\gamma}_{WE} 2^{Rs}} \right) \right) \\
& \left. - \frac{2^{Rs}}{\bar{\gamma}_{AB}} \bar{\gamma}_{AE} E_1 \left(\left(\frac{\bar{\gamma}_{AB} + 2^{Rs} \bar{\gamma}_{AE}}{\bar{\gamma}_{AB}} \right) \left(\frac{\left(\mu + 1 - 2^{Rs} \right) \bar{\gamma}_{AE} \bar{\gamma}_{WE} + 2^{Rs}}{2^{Rs} \bar{\gamma}_{WE}} \right) \right) \right].
\end{aligned}
\tag{13}
$$

□

4.1. Special Case. Now, we suppose the case where no CSI is available at Alice, such scheme is known as nonadaptive rate allocation [22]. In this scheme, the transmitted code words R_b are constant over time (but require to be selected optimally). Unlike, adaptive scheme which demands the feedback of instantaneous SNR, this scheme only needs the feedback of $\log_2(N_A)$ bits to enable on-off transmission. The secrecy outage probability for given values of μ, R_s, and R_b is given as follows:

$$
\begin{aligned}
P_{\text{out}}(R_b, R_s) &= \Pr\left[C_e > R_b - R_s | \gamma_B > \mu \right] \\
&= \Pr\left[C_e > R_b - R_s \right] \\
&= \int_{2^{R_b - R_s} - 1}^{\infty} f_{\gamma_e}(\gamma) \mathrm{d}\gamma_e.
\end{aligned}
\tag{14}
$$

Theorem 2. *The secrecy outage probability of nonadaptive scheme for the considered wiretap system, where Alice employs TAS while Bob and Eve perform MRC, is*

$$P_{\text{out}}(R_b, R_s) = \frac{\exp\left(1/\bar{\gamma}_{WE}\right)}{\Gamma(N_E)\bar{\gamma}_{WE}^{N_W}} \sum_{s=0}^{N_E} \binom{N_E}{s} \frac{\Gamma(N_W + s)}{\Gamma(N_W)} \sum_{v=0}^{N_E-1} \binom{N_E - 1}{v} \left(-\frac{1}{\bar{\gamma}_{WE}}\right)^{Ne-1-v} \Gamma\left[1 - N_W - s + v, \left(\frac{2^{R_b-R_s}-1}{\bar{\gamma}_{AE}} + \frac{1}{\bar{\gamma}_{WE}}\right)\right]. \tag{15}$$

Proof. See Appendix B.

Note that when all nodes are equipped with a single antenna, (15) simplifies to the following:

$$P_{\text{out}}(R_b, R_s) = \frac{\bar{\gamma}_{AE} \exp\left(2^{R_b-R_s} - 1/\bar{\gamma}_{AE}\right)}{\left(2^{R_b-R_s} - 1\right)\bar{\gamma}_{WE} + \bar{\gamma}_{AE}}. \tag{16}$$

In the next section, in order to investigate the impact of the arrival and service processes at Alice, we assume that the information to be transmitted is stored in a buffer before actual transmission as shown in Figure 1. Then, the statistical QoS guarantees are considering by relying on the effective capacity model. □

5. Statistical QoS Provisioning

5.1. Preliminaries. We assume that the data to be transmitted are originated from random sources, and it is accumulated in a buffer prior to transmission. It is also assumed that the queue length is constrained, and then the buffer overflow probability of a queue with finite buffer size q satisfies the following [39]:

$$\lim_{q\longrightarrow\infty} \frac{\ln \Pr\{L \geq q\}}{q} = -\theta, \tag{17}$$

where the length of the stationary queue is represented by L, θ denotes the decay rate, and q is the buffer threshold. For a large $q \longrightarrow q_{\max}$, the probability of buffer overflow can be approximated as $\Pr\{L \geq q\} \approx \zeta e^{-\theta q}$, where $\zeta = \Pr\{L > 0\}$ is the probability of nonempty buffer. It can be observed that for a large enough q, the probability of buffer overflow can be estimated as an exponentially decay at rate θ, which is also known as QoS exponent.

In this sense, strict QoS limitations are applied for large values of θ, while small values of θ mean that looser QoS constraints are imposed [39]. The range of θ goes from 0 to ∞. Additionally, D indicates the queue delay in the buffer at a steady state and the maximum tolerated delay is d, then the delay violation probability is given by [14] as $\Pr\{D \geq d\} \approx \zeta e^{-\theta a(\theta) d}$, where $a(\theta)$ is the effective bandwidth, which is defined as follows.

5.2. Effective Bandwidth. The effective bandwidth models asymptotically the stochastic behaviour of a source traffic process, by describing the minimum constant service rate that can be sustained by a random arrival process while satisfying the statistical queuing constraints. Therefore, by assuming a sequence of nonnegative random arrival rates $\{a(k), k = 1, 2, 3, \ldots\}$ and letting $A(t) = \sum_{k=1}^{t} a(k)$ be the accumulated arrival process at time t, the effective bandwidth is $a(\theta) \triangleq \lim_{t\longrightarrow\infty} 1/\theta t \ln \mathbb{E}\{e^{\theta A(t)}\}$ [39].

5.3. Effective Capacity. The effective capacity is a dual concept of the effective bandwidth that can be used to model a relation between the source rate and the service by considering both link layer and PHY layer parameters. This model defines the maximum constant arrival rate that the wireless channel supports (service rate) while satisfying a delay constraint requirement as given by θ. Let $\{s[k], k = 1, 2, \ldots\}$ be the discrete-time stationary and ergodic stochastic service process, while $S[t] \triangleq \sum_{k=1}^{t} s[k]$ be the time accumulated service process. Then, we represent the effective capacity for a given QoS exponent by the following [14]:

$$\begin{aligned} E_C(\theta, \gamma) &= -\lim_{t\longrightarrow\infty} \frac{1}{\theta t} \ln \mathbb{E}\left\{e^{-\theta S[t]}\right\} \\ &\overset{(a)}{=} -\lim_{t\longrightarrow\infty} \frac{1}{\theta t} \ln \mathbb{E}\left\{e^{-\theta R}\right\}. \end{aligned} \tag{18}$$

Here, θ is related to delay outage probability as in probability of buffer overflow [40]. Step (a) comes from using the maximum service rate R since the service process depends on the fading coefficients that vary independently every block. We are interested in finding the maximum average arrival rate of Markovian sources that can support a certain fading channel while satisfying the QoS requirement in (17). Regarding this, the QoS requirements are satisfied when the effective bandwidth of the arrival process becomes equal to the effective capacity of the service process, i.e., $a(\theta, \gamma) = E_C(\theta, R)$ [39]. Therefore,

$$a(\theta, r) = E_C(\theta, R). \tag{19}$$

Herein, we focus on a secure communication; thus, in the following, instead of R in (18) we will consider the secrecy rate R_s, thus defining the secure effective capacity as in [21].

6. Analysis of the Source Models

Since Markovian processes can incorporate the typical characteristics of the traffic generated by IoT devices, which is comprised of small and burst packets [5, 21, 41], herein we present the models for four different types of Markov arrival sources. The Markovian described herein are (i) discrete-time Markov source (DTMS), (ii) fluid Markov source (FMS), (iii) discrete-time Markov modulated Poisson source (DMMPS), and (iv) continuous-time Markov modulated Poisson source (CMMPS).

6.1. Discrete Markov Source. This model describes a discrete-time data arrival, which is modeled as a discrete-time Markov chain. Data arrive at r bits/block during ON state, while no arrivals occur during OFF state. The transition probability matrix $\mathbf{J}$ for this source is $\mathbf{J} = \begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix}$, where p_{11} indicates the probability of staying in the OFF state from one block to another. Similarly, p_{22} is the probability of staying in ON state, while the transition probabilities are $p_{21} = 1 - p_{22}$ and $p_{12} = 1 - p_{11}$. The probability of ON state in the steady state is $P_{\mathrm{ON}} = 1 - p_{11}/2 - p_{11} - p_{22}$.The effective bandwidth for this two-state (ON-OFF) model is as follows:

$$a(\theta, r) = \frac{1}{\theta}\ln\left(\frac{1}{2}\left(p_{11} + p_{22}e^{\theta r} + \sqrt{\left(p_{11} + p_{22}e^{\theta r}\right)^2 - 4\left(p_{11} + p_{22} - 1\right)e^{\theta r}}\right)\right) \overset{(a)}{=} \frac{1}{\theta}\ln\left(1 - s + se^{\theta r}\right), \tag{20}$$

where (a) comes from using $p_{11} = 1 - s$ and $p_{22} = s$. Hence, $p_{\mathrm{ON}} = s$, which becomes the measure of burstiness, and it is relevant to model different IoT devices traffic patterns. The maximum average arrival rate is $\bar{r}_{\max}(\theta, R_s) = rP_{\mathrm{ON}}$. By using (19), we obtain the average arrival rate that supports secure transmissions at given SNR γ and θ as follows:

$$r = \frac{1}{\theta}\ln\left(\frac{1}{s}e^{\theta E_C(\theta,R)} - (1 - s)\right). \tag{21}$$

Then, we get $\bar{r}_{\max}$, in terms of θ and R_s, for discrete-time Markov source as follows:

$$\bar{r}_{\max}(\theta, R_s) = \frac{s}{\theta}\ln\left(\frac{1}{s}e^{\theta E_C(\theta,R_s)} - (1 - s)\right). \tag{22}$$

6.2. Markov Fluid Source. The arrival process of a Markov fluid source is considered as a continuous-time Markov process, where the generating matrix for a two-state (ON-OFF) case is $\mathbf{G} = \begin{bmatrix} -\alpha & \alpha \\ \beta & -\beta \end{bmatrix}$, and the transition rates from one state to another state are denoted by α and β. During ON state, r bits arrive, while no bits arrive during OFF state. The effective bandwidth for this source is defined as follows [39]:

$$a(\theta, r) = \frac{1}{2\theta}\left(\theta r - (\alpha + \beta) + \sqrt{(\theta r - (\alpha + \beta))^2 + 4\alpha\theta r}\right). \tag{23}$$

The steady state probability for ON and OFF states is $P_{\mathrm{ON}} = \alpha/\alpha + \beta$ and $P_{\mathrm{OFF}} = \beta/\alpha + \beta$, respectively. Then, by using (19) and (23), we obtain r as follows:

$$r = \frac{\theta E_C(\theta, R) + (\alpha + \beta)}{\theta E_C(\theta, R) + \alpha}E_C(\theta, R). \tag{24}$$

Then, we are able to state $\bar{r}_{\max}(\theta, R_s)$ for an ON-OFF fluid Markov source model as follows:

$$\bar{r}_{\max}(\theta, Rs) = P_{\mathrm{ON}}\frac{\theta E_C(\theta, Rs) + (\alpha + \beta)}{\theta E_C(\theta, Rs) + \alpha}E_C(\theta, Rs). \tag{25}$$

6.3. Discrete-Time Markov Modulated Poisson Source. A source is modeled as a discrete-time Markov modulated Poisson process (MMPP), whenever the data arrival is modeled as a Poisson process in which the intensity is determined by a discrete Markov chain. The discrete-time MMPP is the same as a discrete Markov process; however, the data rate of instantaneous arrival in every Markov state is Poisson distributed rather than being fixed. MMPP is able to capture burstiness or uncertainity. In MMPP, the arrival intensity is r during ON state, while no data arrive during OFF state (intensity is equal to zero). This model presents the same transition probability matrix $\mathbf{J}$, as in Section 6.1, and the effective bandwidth for this source is given as follows [27]:

$$a(\theta, r) \overset{(a)}{=} \frac{1}{\theta}\ln\left(1 - s + se^{r\left(e^{\theta} - 1\right)}\right). \tag{26}$$

which is similar to (20) except that we replace the term $e^{r\theta}$ by $e^{r(e^{\theta}-1)}$; as in the previous case, we attain (a) after considering $p_{11} = 1 - s$ and $p_{22} = s$; hence, $P_{\mathrm{ON}} = s$. Now, we proceed similar as before to obtain the average arrival rate r for this source as

$$r = \frac{1}{\left(e^{\theta} - 1\right)}\ln\left(\frac{1}{s}e^{\theta E_C(\theta,R)} - (1 - s)\right). \tag{27}$$

Then, the maximum average arrival rate $\bar{r}_{\max}(\theta, R_s)$ is given by

$$\bar{r}_{\max}(\theta, R_s) = \frac{s}{\left(e^{\theta} - 1\right)}\ln\left(\frac{1}{s}e^{\theta E_C(\theta,R_s)} - (1 - s)\right). \tag{28}$$

6.4. Continuous-Time Markov Modulated Poisson Source. In continuous-time Markov modulated Poisson source, the data arrival rate has Poisson distribution and the intensity changes according to a continuous-time Markov chain. Similar to the other sources, it is also assumed that this source uses the simple ON-OFF model, where r is the Poisson arrival density during ON state, but there is zero

Poisson arrival intensity during OFF state. For the continuous-time Markov chain, the same generator matrix can be employed as in Section 6.2 to obtain the following:

$$a(\theta, r) = \frac{1}{2\theta}\left(\left(e^{\theta} - 1\right)r - (\alpha + \beta)\right) + \frac{1}{2\theta}\sqrt{\left(\left(e^{\theta} - 1\right)r - (\alpha + \beta)\right)^2 + 4\alpha\left(e^{\theta} - 1\right)r}. \tag{29}$$

Then, $\bar{r}_{\max}(\theta, R_s)$ is given by

$$\bar{r}_{\max}(\theta, R_s) = P_{\mathrm{ON}}\frac{\theta\left(\theta E_C(R_s, \theta) + (\alpha + \beta)\right)}{\left(e^{\theta} - 1\right)\left(\theta E_C(R_s, \theta) + \alpha\right)}E_C(R_s, \theta). \tag{30}$$

7. Secure Effective Capacity Maximization

Herein, we assess the maximum average arrival rate that Alice can support while transmitting with secrecy. This can be accomplished by maximizing the secure throughput while determining the effect of burstiness on the performance of the system. Since we use an ON-OFF transmission model, the transmission service can be as well modeled as an ON-OFF Markov chain. Hence, $P_{tx}(\mu)$ can be described as the steady probability of ON state, which is given as a probability of successful transmission in (10). Notice that V_{11} and V_{22} are the probabilities of being in OFF and ON state, respectively. Meanwhile, $V_{21} = 1 - V_{22}$ and $V_{12} = 1 - V_{11}$ are transition probabilities. The probability of ON state in the steady state is $P_{\mathrm{ON}} = 1 - V_{11}/2 - V_{11} - V_{22}$. Then, the secure effective capacity is as follows:

$$\begin{aligned} E_C(\theta, R_s) &= -\lim_{t\longrightarrow\infty}\frac{1}{\theta t}\ln\mathbb{E}\left\{e^{-\theta R}\right\} \\ &= -\frac{\Lambda(-\theta)}{\theta}. \end{aligned} \tag{31}$$

Meanwhile, for the ON-OFF model, we have that (see Ch.7 in [42])

$$E_C(\theta, R_s) = -\frac{1}{\theta}\ln\left(\frac{1}{2}\left(V_{11} + V_{22}e^{\theta r} + \sqrt{\left(V_{11} + V_{22}e^{\theta r}\right)^2 + 4\left(V_{11} + V_{22} - 1\right)e^{\theta r}}\right)\right). \tag{32}$$

Note that in our model, $V_{11} = 1 - w$, $V_{22} = w$, and $V_{11} + V_{22} = 1$; hence, $P_{\mathrm{ON}} = w$ and (31) becomes

$$\begin{aligned} \mathrm{SE}_C(\theta, R_s) &= -\frac{1}{\theta}\ln\left(1 - w + we^{-\theta R_s}\right) \\ &= -\frac{1}{\theta}\ln\left(1 - P_{tx}(\mu)\left(1 - e^{-\theta R_s}\right)\right) \\ &= -\frac{1}{\theta}\ln\left(1 - \left(1 - P\left(N_B, \frac{\mu}{\bar{\gamma}_B}\right)^{N_A}\right)\left(1 - e^{-\theta R_s}\right)\right). \end{aligned} \tag{33}$$

Remark 1. According to (31), note that

$$\begin{aligned} \lim_{\theta\longrightarrow 0}\mathrm{SE}_C(\theta, R_s) &= P_{tx}(\mu)R_s, \\ \lim_{\theta\longrightarrow\infty}\mathrm{SE}_C(\theta, R_s) &= 0. \end{aligned} \tag{34}$$

The novel secure effective capacity formulation in (33) gives the security level of each transmission, and it also enables the legitimate pair to have higher effective capacity at secure rate R_s. Moreover, for $N_A = 1$, $N_B = 1$, $N_W = 0$, and $N_E = 1$, $\mathrm{SE}_C(\theta, R_s)$ in (33) reduces to Equation (9) in [21]. This metric is different than Section 4 in [27], which considers no CSI at Alice, while we assume that Alice knows the legitimate link CSI and can adapt transmission rate accordingly. It enables us model the services as an ON-OFF Markov chain as we conditioned security on the actual transmission. Later, we will see that large arrival rates are not served by wireless fading channels, thus increasing the queue length and delay of the network. This effect can be minimized by maximizing the secure effective capacity in terms of secrecy rate under security and reliability constraints, which also maximizes the maximum average arrival rate $\bar{r}_{\max}$ since the latter is an increasing function of the secure effective capacity. Besides this, all Markovian sources have the same optimal secure rate, which consequently maximizes $\bar{r}_{\max}$ of each source.

The problem of maximizing the secure effective capacity given the reliability constraint σ and security constraint ϵ for a positive secrecy rate $R_s > 0$ is presented next.

7.1. Constrained Optimization. We consider the adaptive rate transmission scheme in [22]. The adaptive scheme relies on the knowledge of the legitimate channel's CSI at Alice in order to adapt its secure rate according to the quality of the channel. The encoder adapts the transmit rate R_b to an arbitrary value close to C_b according to the instantaneous CSI of the legitimate channel. It is pertinent to observe that the constraint $\mu \geq 2^{R_s} - 1$ is always satisfied since transmission only occurs whenever $C_b \geq R_s$. We determine the

values of μ and R_s that maximize the secure throughput, which is given by $T = \mathrm{SE}_C(\theta, R_s)$ under a reliability constraint $\sigma \in [0,1]$ and security constraint $\epsilon \in [0,1]$. Therefore, the design problem is given by

$$\begin{aligned} &\arg\max_{R_s,\mu} \mathrm{SE}_C(\theta, Rs), \\ &\quad P_{\mathrm{out}}(\mu, R_s) \le \epsilon, \\ &\quad P_{tx}(\mu) \ge \sigma, \\ &\text{s.t.} \quad \mu \ge 2^{R_s} - 1, \\ &\quad R_s > 0. \end{aligned} \tag{35}$$

Due to the complexity of this optimization problem, a closed-form solution cannot be obtained. However, we solve this problem through the population-based stochastic optimization algorithm, known as particle swarm optimization (PSO). PSO is simple to implement and already present in many standard mathematical software. Note that we verify our results through numerical solvers as those available in Matlab such as Fmincon, wherein we resort to interior point algorithm that converts the original problem into a sequence of approximate problems as described in [43–45] (Algorithm 1).

8. Numerical Analysis

In this section, we analyze the performance of our system through some illustrative cases and validate our analytical results via Monte Carlo simulations. In Subsection 8.1, we analyze the secrecy outage performance in terms of secrecy rate and average SNR of legitimate and eavesdropper channels under different antenna configurations. Meanwhile, in Subsection 8.2, we evaluate the impact of security, reliability, and latency constraints on maximum average arrival rate for IoT generated traffic.

8.1. On the Secrecy Outage Performance. Figure 2 shows the secrecy outage probability as a function of the average SNR at Bob $\bar{\gamma}_{AB}$, for a fixed secrecy rate $R_s = 2$ bits/s/Hz, $\bar{\gamma}_{AE} = 0$ dB, $\bar{\gamma}_{WE} = 5$ dB, and different configurations of the number of antennas at each node. The SNR threshold is set to its minimum value of $\mu = 2^{R_s} - 1$. First, notice that simulations perfectly match with our analytical results, thus corroborating the correctness of our expressions. Note also that while an increase in N_A or N_B causes a significant decrease in the secrecy outage probability, an increase in N_E degrades the system's secrecy performance to a lesser extent. This can be explained due to the TAS technique, which prevents the eavesdropper from exploiting diversity from Alice. In addition, it can be observed that a greater number of receive antennas are more beneficial than a greater number of transmit antennas in the legitimate link. In fact, when $N_A > N_B$, it is required at least 2 dB gain of $\bar{\gamma}_{AB}$ to attain the same secrecy performance while Figure 3 shows the comparison between adaptive and nonadaptive schemes. We also perform Monte Carlo simulation for the nonadaptive scenario, which matches exactly with analytical expression and corroborates its correctness. We notice that adaptive scheme outperforms its counterpart. Therefore, we only focus on adaptive scheme for the rest of numerical analysis.

Figure 4 shows the level curves of the secrecy outage probability as a function of N_A and N_E. For $N_B = 2$, $N_W = 2$, $\bar{\gamma}_{AB} = 10$ dB, $\bar{\gamma}_{WE} = 5$ dB, and $\bar{\gamma}_{AE} = 0$ dB, we see that by increasing the average SNR between legitimate and eavesdropper channel and the number of antennas at Alice, it is possible to achieve much lower secrecy outage probability, i.e., less than 0.1%, even if Eve has several antennas. Therefore, we conclude that increasing the power ratio between legitimate and Eve's channel plays a crucial role in the performance of the network.

8.2. Statistical QoS Evaluation. Figure 5 illustrates the maximum average arrival rate $\bar{r}_{\max}$ and secrecy outage probability P_{out} as a function of a secure rate R_s, for different Markovian sources and two different configurations of antennas, where $N_A \in \{3,2\}$, $N_B \in \{3,2\}$, $N_E = 2$, and $N_W = 2$. We considered $\theta = 1$, i.e., strict QoS limitations, $P_{\mathrm{ON}} = 0.5$, $\bar{\gamma}_{AB} = 10$ dB, $\bar{\gamma}_{WE} = 5$ dB, and $\bar{\gamma}_{AE} = 0$ dB. The SNR threshold for ON-OFF transmission of the legitimate link is set to its minimum value of $\mu = 2^{R_s} - 1$. Increasing the number of antennas at Alice or Bob consequently increases the maximum average arrival rate and reduces the secrecy outage probability. Note that by increasing R_s, the maximum arrival rate also increases up to a maximal point, after which it starts to decrease. Therefore, there is an optimal R_s that maximizes $\bar{r}_{\max}$. On the other hand, the secrecy outage probability increases always with R_s as expected. Besides, it is observed that all Markovian sources present the same optimal R_s, as shown by red triangular markers, while attainable secrecy outage probability at the optimal rate is indicated by blue triangular markers for three different settings of antennas. It can be also observed that for $N_B = 3$, $\bar{r}_{\max}$ is larger and P_{out} is smaller than in case of $N_A = 3$. The FMS experiences high $R_{\max}$, while DMMPS encounters lower $\bar{r}_{\max}$.

In Figure 6, we analyze the maximum average arrival rate as a function of the target reliability for different Markovian sources and different numbers of antennas at all nodes, where $N_A \in \{1,2\}$, $N_B \in \{1,2\}$, $N_W \in \{1\}$, and $N_E \in \{1\}$. We assume 20 dB gain, $\epsilon = 1\%$, source's burstiness $\mathrm{P_{ON}} = 0.5$, and QoS constraint $\theta = 1$. Notice that as $\theta \longrightarrow 0$, which implies longer delays, effective capacity will converge to capacity, which in this case is a fixed rate R_s. It is worth noticing that for the ultrareliable region, i.e., $\sigma >$ 99.9% or stringent reliability requirement, $\bar{r}_{\max}$ along with optimal secure rate becomes very small for all Markovian sources, so for given parameters, it is impractical to operate in the ultrareliable region with secrecy. As previously mentioned, each setting of antennas has a unique optimal secure rate for all Markovian sources. $\bar{r}_{\max}$ along with the optimal secure rate tends to zero for $\sigma >$ 99% in a scenario where Eve is equipped with more antennas than Alice and Bob. Note that higher $\bar{r}_{\max}$ can be maintained for loose reliability requirements for FMS, while DMMPS experiences more degradation in all cases.

(1) **Initialization**: flag = 0, $\epsilon = 10^{-4}$, $\sigma = 99\%$, $\theta = 10^{-3}$, GBestCost = $-\infty$, pBest = 0, particles = 10,000, iter = 10,000, $w = 0.8$, $c1 = 1.5$, and $c2 = 2$;
(2) **for** i from 1 to particles **do**
(3) **while** flag $\longleftarrow$ 0 **do**
(4) Rs, $\mu \longleftarrow$ U(1,50), U(1,100)
(5) **if** $\mu \geq 2^{Rs} - 1$ **then**
(6) flag $\longleftarrow$ 1
(7) **end if**
(8) **end while**
(9) p.v.Rs, p.v. $\mu \longleftarrow$ 0,0; ▷ Initialize particle Velocity for Rs, μ
(10) cost, P_{out}, $P_{tx} \longleftarrow$ compute (28), (12), (10)
(11) **if** $P_{\text{out}} < \epsilon$ AND $P_{tx} > \sigma$ **then**
(12) Rs$^* \longleftarrow$ Rs, $\mu^* \longleftarrow \mu$
(13) **end if**
(14) pBest.Rs $\longleftarrow$Rs* , pBest. $\mu \longleftarrow \mu^*$, pBest.cost $\longleftarrow$cost* ▷ Set Personal Best
(15) **end for**
(16) **for** i from 1 to particles **do**
(17) **if** pBest.cost >$r$bin GBestCost **then** ▷ Set Global Best
(18) GBest.Rs $\longleftarrow$ pBest.Rs, GBest. $\mu \longleftarrow$ pBest. μ, GBest.cost $\longleftarrow$ pBest.cost
(19) **end if**
(20) **end for**
(21) **for** i from 1 to iter **do**
(22) **for** j from 1 to particles **do**
(23) p.v.Rs = w^*p.v.Rs + $c1$∗rand∗(pBest.Rs - Rs*)+$c2$∗rand∗(GBest.Rs- Rs*)
(24) p.v. μ = w^*p.v. μ +$c1$∗rand(1)∗(pBest. μ - μ^*)+$c2$∗rand∗(GBest. μ - μ^*) ▷ Update Velocity
(25) Rs$^* \longleftarrow$Rs* + p.v.Rs, $\mu^* \longleftarrow \mu^*$ + p.v. μ ▷ Update Position
(26) cost$^* \longleftarrow$ compute (28) based on Rs* & μ^* ▷ Evaluation
(27) **if** cost* < pBest.Cost **then**
(28) pBest.Rs = Rs*, pBest. μ = μ^*, pBestCost = cost* ▷ Update Personal Best
(29) **if** pBest.Cost >$r$bin GBest.Cost **then**
(30) Gbest = pBest ▷ Update Global Best
(31) **end if**
(32) **end if**
(33) **end for**
(34) BestCost = GBest.Cost
(35) **end for**

Algorithm 1: Particle swarm optimization.

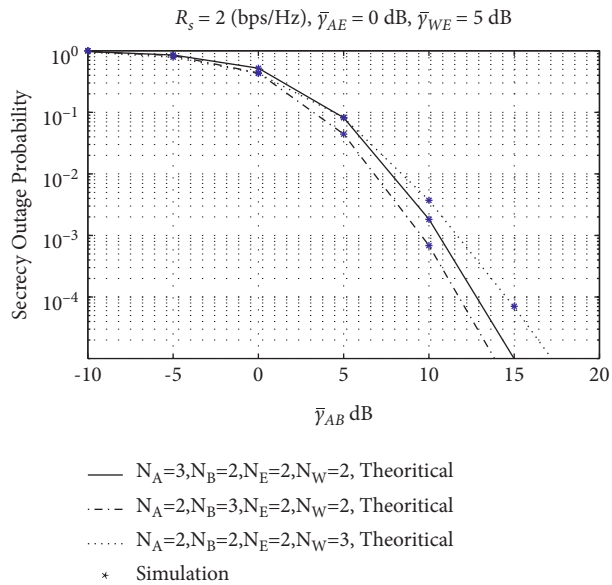

Figure 2: Conditioned secrecy outage probability as a function of average SNR at Bob for different number of antennas at Alice, Bob, Wiley, and Eve, for R_s = 2 bits/s/Hz, $\bar{\gamma}_{WE}$ = 5 dB, and $\bar{\gamma}_{AE}$ = 0 dB.

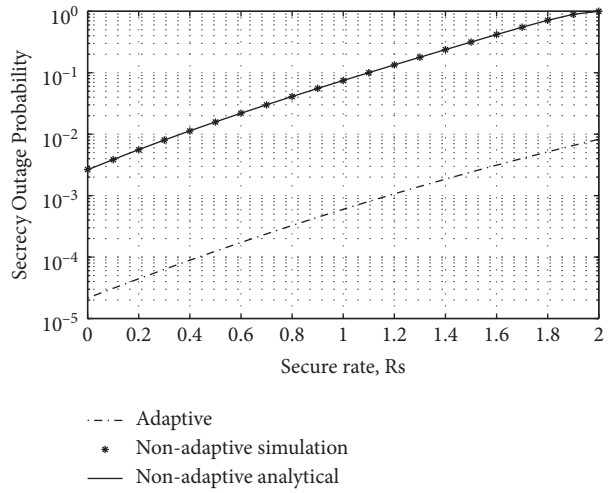

Figure 3: Conditioned secrecy outage probability as a function of secure rate R_s for different number of antennas at Alice, Bob, Wiley, and Eve, for $R_b = 2$ bits/s/Hz, $\overline{\gamma}_{AB} = 20$ dB, $\overline{\gamma}_{WE} = 5$ dB, and $\overline{\gamma}_{AE} = 0$ dB.

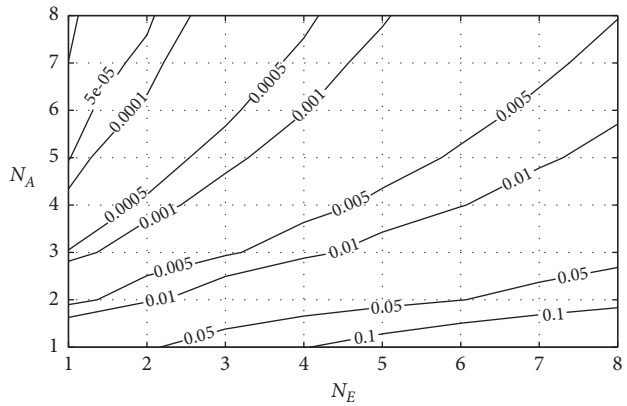

Figure 4: Conditioned secrecy outage probability as a function of N_A and N_E for $N_B = 2$, $N_W = 2$, $R_s = 2$ bits/s/Hz, $\overline{\gamma}_{AB} = 10$ dB, $\overline{\gamma}_{AE} = 0$ dB, and $\overline{\gamma}_{WE} = 5$ dB.

In Figure 7, we fix the target reliability σ to 90%, and we focused on the variation of the threshold of secrecy outage probability and optimal R_s. Note that a higher $\overline{r}_{\max}$ and a higher optimal R_s can be attained for a loose security constraint. These results show the intuition that optimal R_s and $\overline{r}_{\max}$ are sacrificed to guarantee high reliability and security. Furthermore, this figure illustrates that even under strict requirement, i.e., $\epsilon = 0.1\%$, $\sigma = 90\%$, and $\theta = 1$, a positive secrecy rate is still achievable. Moreover, a higher number of antennas at Bob provide significant gains to the system. It is also noticeable that DMMPS and CMMPS are less prone to strict reliability and security constraints.

After analyzing the impact of security and reliability constraints on the system performance, we next assess the effect of latency. In Figure 8, we show the probability of delay violation versus maximum average arrival rate for $\theta \in [0, 2]$, $P_{\text{ON}} = 0.5$, different antenna settings, and distinct values of

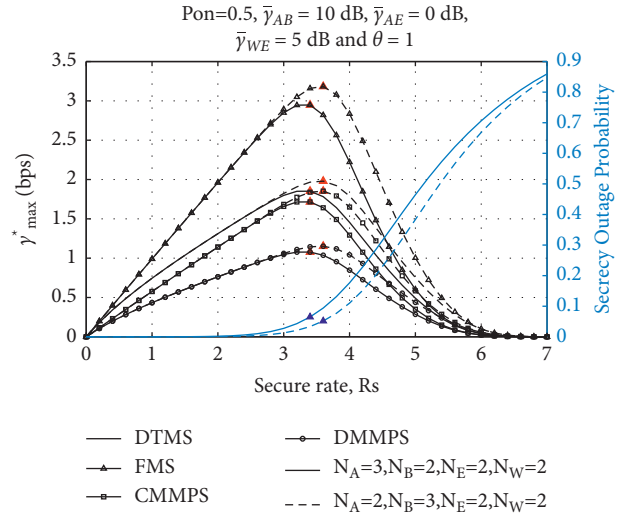

Figure 5: Maximum average arrival rate and conditioned secrecy outage probability as a function of secure rate for different configurations of antennas and different Markovian sources, for $P_{\text{ON}} = 0.5$, $\overline{\gamma}_{AB} = 10$ dB, $\overline{\gamma}_{AE} = 0$ dB, $\overline{\gamma}_{WE} = 5$ dB, and $\theta = 1$. Note that black lines shows $\overline{r}_{\max}$ and blue lines indicate ε, and red $\triangle$ denotes optimum $\overline{r}_{\max}$ while blue $\triangle$ represents ϵ corresponding to optimum $\overline{r}_{\max}$ at secure rate.

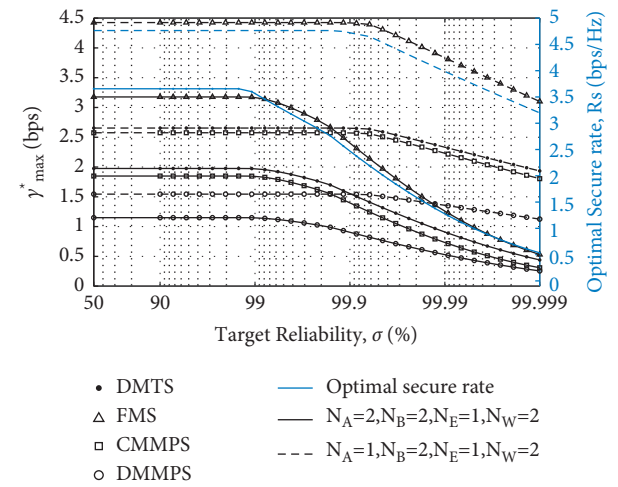

Figure 6: Maximum average arrival rate as a function of target reliability σ and optimal secure rate R_s for different Markov sources and different number of antennas at all nodes, for $P_{\text{ON}} = 0.5$, $\varepsilon = 1\%$, $\overline{\gamma}_{AB} = 20$ dB, $\overline{\gamma}_{WE} = 5$ dB, $\overline{\gamma}_{AE} = 0$ dB, and $\theta = 1$. Maximum average arrival rate is plotted on the left y-axis and optimal secure rate on the right y-axis.

delay threshold $d \in \{5, 8\}$. We examine the different Markovian sources to determine achievable security, latency, and reliability performance since this is an important issue in industrial control systems. Interestingly, for $\sigma = 90\%$, lower security constraints, $\epsilon = 0.1\%$, delay threshold $d = 8$, and 1% delay violation probability, $\overline{r}_{\max}$ is compromised for all Markovian sources and larger values of $\overline{r}_{\max}$ cannot be supported for larger values of θ. Besides this, in order to have low delay violation probability, the delay threshold d needs

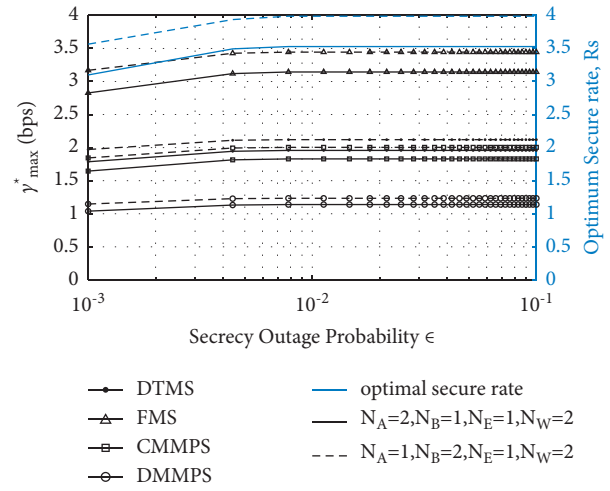

Figure 7: Maximum average arrival rate and optimal secure rate as a function of secrecy outage probability ε for different Markovian sources and three different configurations of antennas, for $P_{\text{ON}} = 0.5$, $\sigma = 99\%$, $\overline{\gamma}_{AB} = 20$ dB, $\overline{\gamma}_{WE} = 5$ dB, $\overline{\gamma}_{AE} = 0$ dB, and $\theta = 1$. Black lines indicate the maximum average arrival rate while cyan color shows the optimum secure rate.

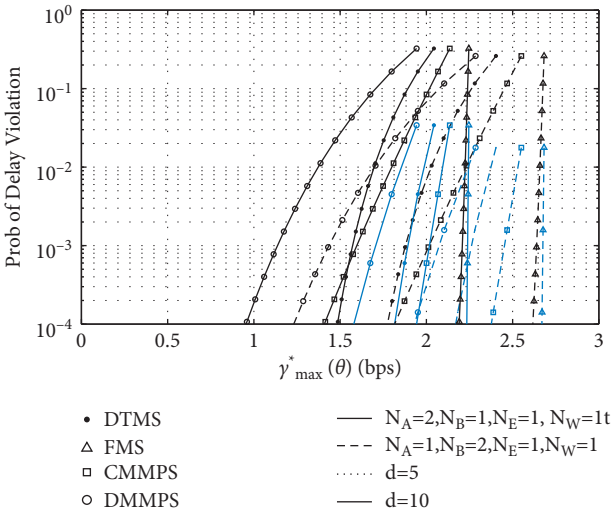

Figure 8: Delay violation probability vs. maximum average arrival rate for different Markovian sources for $\theta \in [0, 2]$ with three distinct antenna arrangements and for two distinct delay thresholds $d \in \{5, 10\}$, $P_{\text{ON}} = 0.5$, $\varepsilon = 0.1\%$, $\sigma = 90\%$, $\alpha = 50$, $\beta = 50$, $\overline{\gamma}_{AB} = 20$ dB, $\overline{\gamma}_{WE} = 5$ dB, $\overline{\gamma}_{AE} = 0$ dB, and $\theta = 1$. Black lines are for $d = 5$, and cyan lines are for $d = 8$.

to be flexible. The larger delay threshold we have, the less delay violation probability a system can have, which consequently increases $\bar{r}_{\max}$. Obviously, the delay violation probability is large in the SISOME and less in SIMOSE scenarios.

Figure 9 shows the maximum average arrival rate as a function of QoS exponent θ for different Markovian sources and distinct antenna arrangements. We set $P_{\text{ON}} = 0.5$ with 90% reliability and 0.1% secrecy outage. We notice a degradation in $\bar{r}_{\max}$ when stricter buffer constraints are

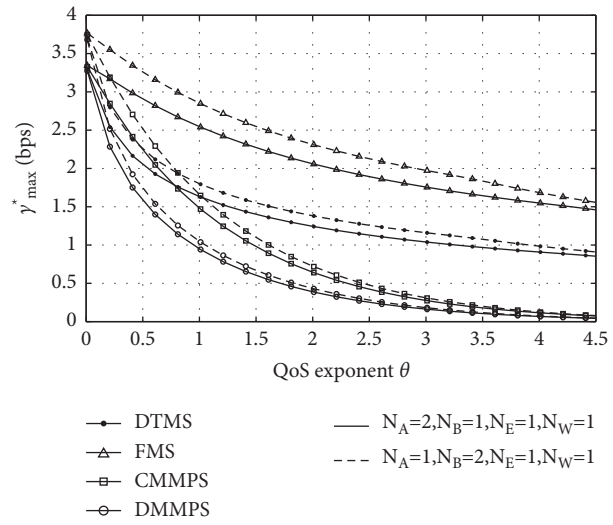

Figure 9: Maximum average arrival rate as a function of QoS exponent θ for different Markovian sources and different settings of antennas, for $P_{\text{ON}} = 0.5$, $\sigma = 90\%$, $\varepsilon = 1\%$, $\overline{\gamma}_{AB} = 20$ dB, $\overline{\gamma}_{WE} = 5$, and $\overline{\gamma}_{AE} = 0$ dB.

imposed. Consequently, it is observed that lower $\bar{r}_{\max}$ can be tolerated for stringent delay requirements ($\theta \gg 0$). We also observe that FMS and DTMS have better performance even under high QoS constraints, while CMMPS and DMMPS perform poorly at very tight buffer constraints (higher values of θ). Similar to previous intuitions, we see that the for higher number of antennas at Bob, cases attain high $\bar{r}_{\max}$, while it reduces in when jammer is equipped with a single antenna.

In Figure 10, we examine the effect of the source's burstiness on arrival rate for different Markovian sources to sustain the optimal secure effective capacity for different antenna configurations at $\overline{\gamma}_{AB} = 20$ dB and $\overline{\gamma}_{AE} = 0$ dB. We set the reliability indicator σ to 90%, security constraint $\epsilon = 0.1\%$, and $\theta = 1$. Note that the source's burstiness (lesser values of P_{ON}) increases the arrival rate. In the case of DTMS and FMS, we notice that the arrival rate becomes equal to the optimal secure effective capacity when $P_{\text{ON}} = 1$, which means the source is always ON and there is a constant arrival rate. The DMTS and FMS need larger arrival rates to sustain the optimal secure effective capacity. Furthermore, the $N_B = 2$ case also requires higher arrival rates as compared with $N_A = 2$. We further show that as P_{ON} reduces, the arrival rate in ON state needs to increase with a specific level to keep average arrival rate nondecreasing. When the source is bursty, the higher arrival rate is needed to attain secure effective capacity. Note that the DTMS and FMS are affected by the source's burstiness, so to ensure QoS, these two sources need a significant adaptation of arrival rate. The CMMPS is suitable to model bursty traffic. Moreover, the probability of ON state is not the only measure of burstiness for FMS and CMMPS; the low values of α and β also show that the source is bursty as transition does not frequently occur between ON and OFF states, which also indicates that OFF state is more persistent. Large values of α and β indicate

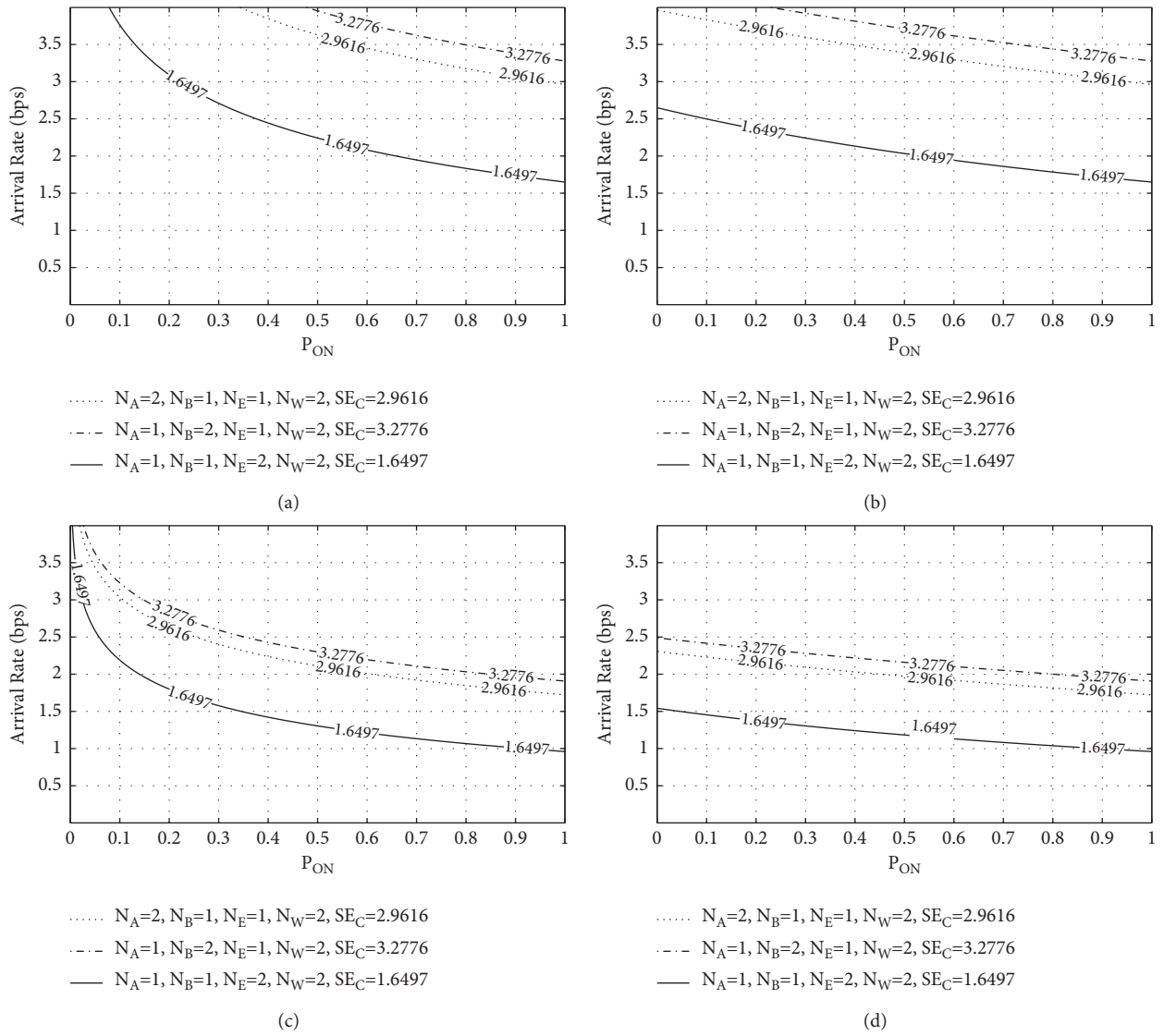

Figure 10: Arrival rate as a function of P_{on} for secure effective capacity of Markovian sources for three combinations of antennas, for $\sigma = 90\%$, $\varepsilon = 0.1\%$, $\overline{\gamma}_{AB} = 20$ dB, $\overline{\gamma}_{WE} = 5$ dB, $\overline{\gamma}_{AE} = 0$ dB, and $\theta = 1$: (a) DTMS, (b) FMS, (c) DMMPS, and (d) CMMPS.

the fast transition between ON and OFF states, which minimizes the SNR requirement levels.

9. Conclusion

In this work, we investigated the statistical QoS provisioning for cloud-based IoT networks under security, reliability, and latency constraints. To do so, we relied on the secure effective capacity model and considered a wiretap channel, where the legitimate pair, Alice and Bob, communicates in the presence of an eavesdropper who attempts to breach the transmission originated from Alice, while a friendly jammer Wiley emits the artificial noise to degrade Eve's channel. This is a relevant scenario in the context of massive IoT deployments where nodes have limited computational capabilities. Nodes are equipped with multiple antennas, which are exploited by Alice to perform TAS, while Bob and Eve employ MRC technique. Furthermore, we assumed that Bob applies perfect SIC to cancel out artificial noise coming from Wiley. Our model was inspired by the alternative secrecy outage formulation conditioned upon a successful transmission, which provides a more thorough measure of the system's security since the conventional secrecy outage formulation fails to differentiate between the system's security and reliability level. We derived exact closed-form expression for the secrecy outage probability for the proposed scenario. We examined the secure effective capacity for an ON-OFF transmission by analyzing the traffic generated by IoT devices through Markovian sources. This metric is capable of capturing the source's burstiness. Furthermore, a secure throughput maximization was performed by considering an adaptive rate, according to Bob's received SNR, subject to reliability and security constraints. The maximized secure throughput consequently enhanced the maximum average arrival rate. Simulation results showed that the number of antennas at Bob has a significant

impact on security performance compared with that at Alice and Wiley. Moreover, higher average SNR at the legitimate link led to a greater security even if Eve is equipped with several antennas. It was also observed that secure throughput experiences reduction when stringent QoS requirements are imposed. Besides, the delay violation probability could be reduced by relaxing the delay threshold and also by increasing the number of antennas at Bob as compared with Alice. However, it gets seriously affected when Eve is equipped with more antennas than Alice and Bob. Finally, the legitimate link's SNR gain plays a crucial role for system performance to meet the stringent security, reliability, and latency requirements.

Appendix

A. Proof of Theorem 1

From (11), the secrecy outage probability can be expressed as the difference of two terms, as follows:

$$P_{\text{out}}(\mu, R_s)_1 = I_1 - \Psi_1, \tag{A.1}$$

where

$$\begin{aligned}
I_1 &\overset{(a)}{=} \frac{1}{P_{\text{tx}}(\mu)} \int_{\infty} F_{\gamma_B}\left(2^{R_s}(1+\gamma_E)-1\right) f_{\gamma_E}(\gamma_E)\mathrm{d}\gamma_E \\
&\overset{(b)}{=} \frac{1}{P_{\text{tx}}(\mu)} \sum_{K=0}^{N_A} \binom{N_A}{K} (-1)^K \int_{((1+\mu)/2^{R_s})-1}^{\infty} \exp\left(-\frac{K\left(2^{R_s}(1+\gamma_E)-1\right)}{\bar{\gamma}_B}\right) \sum_{s_0+s_1+\cdots+s_{N_B-1}=K} \\
&\binom{K}{s_0, s_1, \ldots, s_{N_B-1}} \times \left(\prod_{t=0}^{N_B-1} \frac{1}{(t!)^{s_t}}\right) \left(\frac{2^{R_s}(1+\gamma_E)-1}{\bar{\gamma}_B}\right)^{s_t t} f_{\gamma_E}(\gamma_E)\mathrm{d}\gamma_E\%. \\
&\overset{(c)}{=} \sum_{K=0}^{N_A} \binom{N_A}{K} (-1)^k \int_{((1+\mu)/2^{R_s})-1}^{\infty} \exp\left(-\frac{K\left(2^{R_s}(1+\gamma_E)-1\right)}{\bar{\gamma}_B}\right) \sum_{s_0+s_1+\cdots+s_{N_B-1}=K} \binom{K}{s_0, s_1, \ldots, s_{N_B-1}} \left(\prod_{t=0}^{N_B-1} \frac{1}{(t!)^{s_t}}\right) \\
&\times \prod_{t=0}^{N_B-1} \left(\frac{\left(2^{R_s}(1+\gamma_E)-1\right)}{\bar{\gamma}_B}\right)^{s_t t} f_{\gamma_E}(\gamma_E)\mathrm{d}\gamma_E \overset{(d)}{=} \frac{1}{P_{\text{tx}}(\mu)} \sum_{K=0}^{N_A} \binom{N_A}{K} (-1)^K \exp\left(-\frac{K\left(2^{R_s}-1\right)}{\bar{\gamma}_B}\right) \\
&\times \sum_{s_0+s_1+\cdots+s_{N_B-1}=K} \binom{K}{s_0, s_1, \ldots, s_{N_B-1}} \left(\prod_{t=0}^{N_B-1} \frac{1}{(t!)^{s_t}}\right) \\
&\times \sum_{p=0}^{\alpha} \binom{\alpha}{p} \left(\frac{2^{R_s}-1}{\bar{\gamma}_B}\right)^{\alpha-p} \left(\frac{2^{R_s}}{\bar{\gamma}_B}\right)^{p} \frac{1}{\Gamma(N_E)\bar{\gamma}_E^{N_E}\bar{\gamma}_{we}^{N_w}} \int_{((1+\mu)/2^{R_s})-1}^{\infty} (\gamma_E)^p \exp\left(-\frac{K2^{R_s}\gamma_E}{\bar{\gamma}_B}\right)\gamma_E^{N_E-1} \\
&\times \exp\left(-\frac{\gamma_E}{\bar{\gamma}_E}\right)\left(\frac{\gamma_E}{\bar{\gamma}_E}+\frac{1}{\bar{\gamma}_{we}}\right)^{-N_w} \sum_{d=0}^{N_e} \binom{N_e}{d} \frac{\Gamma(N_w+d)}{\Gamma(N_w)} \left(\frac{\gamma_E}{\bar{\gamma}_E}+\frac{1}{\bar{\gamma}_{we}}\right)^{-d} \mathrm{d}\gamma_E.
\end{aligned} \tag{A.2}$$

Note that in step (b), we have applied the binomial theorem, while in step (c), we have applied the multinomial theorem. Next, after some simplifications, in step (c), we used this property $\prod_{j=0}^{J} x_j y_j = \prod_{j=0}^{J} x_j \prod_{j=0}^{J} y_j$ and $\prod_{t=0}^{N_B-1} (X)^{s_t t} = X^{s_0 0} \cdot X^{s_1 1} \cdots X^{s_{N_B-1} N_B-1} = (X)^{\sum s_t t}$; thus, let $\sum s_t t = \alpha$. In step (d), we have applied the binomial expansion to $((2^{R_s}-1/\bar{\gamma}_B)+(2^{R_s}\gamma_E/\bar{\gamma}_B))^{\alpha}$ and used (B.2). Next, the integral in (A.2) is solved as follows:

$$\begin{aligned}
I_1 &\overset{(a)}{=} \frac{1}{P_{\text{tx}}(\mu)} \int_{((1+\mu)/2^{R_s})-1}^{\infty} F_{\gamma_B}\left(2^{R_s}(1+\gamma_E)-1\right) f_{\gamma_E}(\gamma_E)\mathrm{d}\gamma_E \\
&\overset{(b)}{=} \frac{1}{P_{\text{tx}}(\mu)} \sum_{K=0}^{N_A} \binom{N_A}{K} (-1)^K \int_{((1+\mu)/2^{R_s})-1}^{\infty} \exp\left(-\frac{K\left(2^{R_s}(1+\gamma_E)-1\right)}{\bar{\gamma}_B}\right) \sum_{s_0+s_1+\cdots+s_{N_B-1}=K} \binom{K}{s_0, s_1, \ldots, s_{N_B-1}} \\
&\times \left(\prod_{t=0}^{N_B-1} \frac{1}{(t!)^{s_t}}\right) \left(\frac{2^{R_s}(1+\gamma_E)-1}{\bar{\gamma}_B}\right)^{s_t t} f_{\gamma_E}(\gamma_E)\mathrm{d}\gamma_E\%.
\end{aligned} \tag{A.3}$$

Now, we let $(\gamma_E/\bar{\gamma}_E + 1/\bar{\gamma}_{we}) = y$, which leads to $\gamma_E = (y - 1/\bar{\gamma}_{we})\bar{\gamma}_E$, when $\gamma_E = (1+\mu)/2^{R_s} - 1$, => $y = 1 + \mu - 2^{R_s}/2^{R_s}\bar{\gamma}_E + 1/\bar{\gamma}_{we}$, and when $\gamma_E = \infty$, => $y = \infty$, and we also suppose $(1 + \mu - 2^{R_s}/2^{R_s}\bar{\gamma}_E + 1/\bar{\gamma}_{we}) = \beta$:

$$\begin{aligned}
&\overset{(f)}{=} \frac{1}{P_{\text{tx}}(\mu)} \sum_{K=0}^{N_A} \binom{N_A}{K} (-1)^K \exp\left(-\frac{K\left(2^{R_s}-1\right)}{\bar{\gamma}_B}\right) \times \sum_{s_0+s_1+\ldots+s_{N_B-1}=K} \binom{K}{s_0, s_1, \ldots, s_{N_B-1}} \left(\prod_{t=0}^{N_B-1} \frac{1}{(t!)^{s_t}}\right) \\
&\times \sum_{p=0}^{\alpha} \binom{\alpha}{p} \left(\frac{2^{R_s}-1}{\bar{\gamma}_B}\right)^{\alpha-p} \left(\frac{2^{R_s}}{\bar{\gamma}_B}\right)^{p} \frac{1}{\Gamma(N_E)\bar{\gamma}_E^{N_E}\bar{\gamma}_{we}^{N_w}} \sum_{d=0}^{N_e} \binom{N_e}{d} \frac{\Gamma(N_w+d)}{\Gamma(N_w)} \left(\bar{\gamma}_E\right)^{p+N_E-1} \int_{\beta}^{\infty} \left(y - \frac{1}{\bar{\gamma}_{we}}\right)^{p+N_E-1} \\
&\times \exp\left(-\frac{\left(y - 1/\bar{\gamma}_{we}\right)\bar{\gamma}_E\left(K2^{R_s}\bar{\gamma}_E + \bar{\gamma}_B\right)}{\bar{\gamma}_B\bar{\gamma}_E}\right) (y)^{-N_w-d} \bar{\gamma}_E \mathrm{d}y\%.
\end{aligned} \tag{A.4}$$

Now, we apply Binomial theorem on $(y - 1/\bar{\gamma}_{we})^{p+Ne-1} = \sum_{J=0}^{p+N_e-1} \binom{p+N_e-1}{J} (-(1/\bar{\gamma}_{we}))^{p+N_e-1-J} (y)^J$ and simplify it further as follows:

$$\begin{aligned}
&\overset{(g)}{=} \frac{1}{P_{\text{tx}}(\mu)} \sum_{K=0}^{N_A} \binom{N_A}{K} (-1)^K \exp\left(\frac{\left(K2^{R_s}\bar{\gamma}_E + \bar{\gamma}_B\right) - \bar{\gamma}_{we}K\left(2^{R_s}-1\right)}{\bar{\gamma}_B\bar{\gamma}_{we}}\right) \\
&\times \sum_{s_0+s_1+\cdots+s_{N_B-1}=K} \binom{K}{s_0, s_1, \ldots, s_{N_B-1}} \left(\prod_{t=0}^{N_B-1} \frac{1}{(t!)^{s_t}}\right) \sum_{p=0}^{\alpha} \binom{\alpha}{p} \left(\frac{2^{R_s}-1}{\bar{\gamma}_B}\right)^{\alpha-p} \left(\frac{2^{R_s}}{\bar{\gamma}_B}\right)^{p} \\
&\frac{1}{\Gamma(N_E)\bar{\gamma}_E^{N_E}\bar{\gamma}_{we}^{N_w}} \sum_{d=0}^{N_e} \binom{N_e}{d} \frac{\Gamma(N_w+d)}{\Gamma(N_w)} \left(\bar{\gamma}_E\right)^{p+N_E} \sum_{J=0}^{P+N_e-1} \binom{p+N_e-1}{J} \left(-\frac{1}{\bar{\gamma}_{we}}\right)^{p+N_e-1-J} \int_{\beta}^{\infty} (y)^{J-Nw-d} \\
&\exp\left(-\frac{y\left(K2^{R_s}\bar{\gamma}_E + \bar{\gamma}_B\right)}{\bar{\gamma}_B}\right) \mathrm{d}y.
\end{aligned} \tag{A.5}$$

After solving the integral with further algebraic manipulation and replacing β, we get

$$\begin{aligned}
I_1 = &\frac{1}{P_{\text{tx}}(\mu)} \sum_{K=0}^{N_A} \binom{N_A}{K} (-1)^K \exp\left(\frac{\left(K2^{R_s}\bar{\gamma}_E + \bar{\gamma}_B\right) - \bar{\gamma}_{we}K\left(2^{R_s}-1\right)}{\bar{\gamma}_B\bar{\gamma}_{we}}\right) \\
&\times \sum_{s_0+s_1+\cdots+s_{N_B-1}=K} \binom{K}{s_0, s_1, \ldots, s_{N_B-1}} \left(\prod_{t=0}^{N_B-1} \frac{1}{(t!)^{s_t}}\right) \times \sum_{p=0}^{\alpha} \binom{\alpha}{p} \left(\frac{2^{R_s}-1}{\bar{\gamma}_B}\right)^{\alpha-p} \left(\frac{2^{R_s}}{\bar{\gamma}_B}\right)^{p} \\
&\frac{1}{\Gamma(N_E)\bar{\gamma}_E^{N_E}\bar{\gamma}_{we}^{N_w}} \sum_{d=0}^{N_e} \binom{N_e}{d} \frac{\Gamma(N_w+d)}{\Gamma(N_w)} \left(\bar{\gamma}_E\right)^{p+N_E} \sum_{J=0}^{P+N_e-1} \binom{p+N_e-1}{J} \left(-\frac{1}{\bar{\gamma}_{we}}\right)^{p+N_e-1-J} \\
&\left(\frac{K2^{R_s}\bar{\gamma}_E + \bar{\gamma}_B}{\bar{\gamma}_B}\right)^{-1-J+d+Nw} \Gamma\left[1 + J - Nw - d, \left(\frac{K2^{R_s}\bar{\gamma}_E + \bar{\gamma}_B}{\bar{\gamma}_B}\right)\left(\frac{1+\mu-2^{R_s}}{2^{R_s}\bar{\gamma}_E} + \frac{1}{\bar{\gamma}_w}\right)\right].
\end{aligned} \tag{A.6}$$

Finally,

$$\Psi_1 = \frac{1}{P_{\text{tx}}(\mu)} P\left(N_B, \frac{\mu}{\bar{\gamma}_B}\right)^{N_A} \left(1 - \sum_{d=0}^{N_e} \binom{N_e}{d} \frac{\Gamma(N_w + d)}{\Gamma(N_w)} \frac{\exp\left(1/\bar{\gamma}_{we}\right)}{\Gamma(N_e)\bar{\gamma}_{we}^{N_w}} \sum_{J=0}^{N_e-1} \binom{N_e - 1}{J} \left(-\frac{1}{\bar{\gamma}_{we}}\right)^{Ne-1-J} \left[\Gamma\left(1 + J - Nw - d, \frac{1}{\bar{\gamma}_{we}}\right) - \Gamma\left(1 + J - Nw - d, \frac{1 + \mu - 2^{R_s}}{2^{R_s}\bar{\gamma}_E} + \frac{1}{\bar{\gamma}_{we}}\right)\right]\right). \tag{A.7}$$

By substituting (A.5) and (A.6) into (A.1), we attain the secrecy outage probability of the MIMOME wiretap channel in closed form as in (12), thus concluding the proof.

B. Proof of Theorem 2

We substitute (8) into (14); hence,

$$P_{\text{out}}(R_b, R_s) = \int_{2^{R_b - R_s} - 1}^{\infty} \frac{\gamma_e^{N_E - 1} \exp\left(-\left(\gamma_e/\bar{\gamma}_{AE}\right)\right)}{\Gamma(N_E)\bar{\gamma}_{AE}^{N_E}\bar{\gamma}_{WE}^{N_W}} \left(\frac{\gamma_e}{\bar{\gamma}_{AE}} + \frac{1}{\bar{\gamma}_{WE}}\right)^{-N_W} \sum_{s=0}^{N_E} \binom{N_E}{s} \frac{\Gamma(N_W + s)}{\Gamma(N_W)} \left(\frac{\gamma_e}{\bar{\gamma}_{AE}} + \frac{1}{\bar{\gamma}_{WE}}\right)^{-s} \mathrm{d}\gamma_e$$

$$= \frac{1}{\Gamma(N_E)\bar{\gamma}_{AE}^{N_E}\bar{\gamma}_{WE}^{N_W}} \sum_{s=0}^{N_E} \binom{N_E}{s} \frac{\Gamma(N_W + s)}{\Gamma(N_W)} \int_{2^{R_b - R_s} - 1}^{\infty} \gamma_e^{N_E - 1} \exp\left(-\frac{\gamma_e}{\bar{\gamma}_{AE}}\right) \left(\frac{\gamma_e}{\bar{\gamma}_{AE}} + \frac{1}{\bar{\gamma}_{WE}}\right)^{-N_W} \left(\frac{\gamma_e}{\bar{\gamma}_{AE}} + \frac{1}{\bar{\gamma}_{WE}}\right)^{-s} \mathrm{d}\gamma_e. \tag{B.1}$$

We let $y = (\gamma_e/\bar{\gamma}_{AE} + 1/\bar{\gamma}_{WE})$, which implies $\gamma_e = (y - 1/\bar{\gamma}_{WE})\bar{\gamma}_{AE}$ and $d\gamma_e = dy\ \bar{\gamma}_{AE}$, hence changing the limits.

When $\gamma_e = 2^{R_b - R_s} - 1$, then $y = (2^{R_b - R_s} - 1/\bar{\gamma}_{AE} + 1/\bar{\gamma}_{WE})$; suppose $(2^{R_b - R_s} - 1/\bar{\gamma}_{AE} + 1/\bar{\gamma}_{WE}) = A$.

When $\gamma_e = \infty$, then $y = \infty$.

$$= \frac{1}{\Gamma(N_E)\bar{\gamma}_{AE}^{N_E}\bar{\gamma}_{WE}^{N_W}} \sum_{s=0}^{N_E} \binom{N_E}{s} \frac{\Gamma(N_W + s)}{\Gamma(N_W)} \int_A^{\infty} \left(\left(y - \frac{1}{\bar{\gamma}_{WE}}\right)\bar{\gamma}_{AE}\right)^{N_E - 1} \exp\left(-\frac{\left(y - \left(1/\bar{\gamma}_{WE}\right)\right)\bar{\gamma}_{AE}}{\bar{\gamma}_{AE}}\right) (y)^{-N_W - s} \mathrm{d}y\bar{\gamma}_{AE}$$

$$= \frac{1}{\Gamma(N_E)\bar{\gamma}_{AE}^{N_E}\bar{\gamma}_{WE}^{N_W}} \sum_{s=0}^{N_E} \binom{N_E}{s} \frac{\Gamma(N_W + s)}{\Gamma(N_W)} \left(\bar{\gamma}_{AE}\right)^{N_E - 1} \bar{\gamma}_{AE} \int_A^{\infty} \left(y - \frac{1}{\bar{\gamma}_{WE}}\right)^{N_E - 1} \exp\left(-\left(y - \frac{1}{\bar{\gamma}_{WE}}\right)\right) (y)^{-N_W - s} \mathrm{d}y \tag{B.2}$$

$$= \frac{\exp\left(1/\bar{\gamma}_{WE}\right)}{\Gamma(N_E)\bar{\gamma}_{WE}^{N_W}} \sum_{s=0}^{N_E} \binom{N_E}{s} \frac{\Gamma(N_W + s)}{\Gamma(N_W)} \int_A^{\infty} \left(y - \frac{1}{\bar{\gamma}_{WE}}\right)^{N_E - 1} \exp(-y)(y)^{-N_W - s} \mathrm{d}y.$$

Now, we apply Binomial theorem on $(y - 1/\bar{\gamma}_{WE})^{N_E - 1} = \sum_{v=0}^{N_E - 1} \binom{N_E - 1}{v} (y)^v (-(1/\bar{\gamma}_{WE}))^{Ne-1-v}$.

$$= \frac{\exp\left(1/\bar{\gamma}_{WE}\right)}{\Gamma(N_E)\bar{\gamma}_{WE}^{N_W}} \sum_{s=0}^{N_E} \binom{N_E}{s} \frac{\Gamma(N_W + s)}{\Gamma(N_W)} \int_A^{\infty} \sum_{v=0}^{N_E - 1} \binom{N_E - 1}{v} (y)^v \left(-\frac{1}{\bar{\gamma}_{WE}}\right)^{Ne-1-v} \exp(-y)(y)^{-N_W - s} \mathrm{d}y$$

$$= \frac{\exp\left(1/\bar{\gamma}_{WE}\right)}{\Gamma(N_E)\bar{\gamma}_{WE}^{N_W}} \sum_{s=0}^{N_E} \binom{N_E}{s} \frac{\Gamma(N_W + s)}{\Gamma(N_W)} \sum_{v=0}^{N_E - 1} \binom{N_E - 1}{v} \left(-\frac{1}{\bar{\gamma}_{WE}}\right)^{Ne-1-v} \int_A^{\infty} (y)^{v - N_W - s} \exp(-y) \mathrm{d}y \tag{B.3}$$

$$= \frac{\exp\left(1/\bar{\gamma}_{WE}\right)}{\Gamma(N_E)\bar{\gamma}_{WE}^{N_W}} \sum_{s=0}^{N_E} \binom{N_E}{s} \frac{\Gamma(N_W + s)}{\Gamma(N_W)} \sum_{v=0}^{N_E - 1} \binom{N_E - 1}{v} \left(-\frac{1}{\bar{\gamma}_{WE}}\right)^{Ne-1-v} \Gamma(1 - N_W - s + v, A).$$

By substituting A into (B.3), we obtained the closed-form expression of secrecy outage probability for nonadaptive scheme as in (15). Thus, concluding the proof.

Data Availability

The data used to support this study are available upon request.

Disclosure

This paper is the extended version of the work appearing in ISWCS 2019 [26], but the authors do not incorporate or reproduce any result from [26] in the current manuscript.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was financially supported by Academy of Finland 6Genesis Flagship (grant 318927), EE-IoT (grant 319008), and AKProf (grant 307492).

References

[1] I. H. Witten, E. Frank, and M. A. Hall, *Data Mining: Practical Machine Learning Tools and Techniques*, Morgan Kaufmann, MA, USA, 2011, https://www.sciencedirect.com/science/article/pii/B9780123748560000237, 3rd edition.

[2] N. H. Mahmood, "White paper on critical and massive machine type communication towards 6g," in *6G Flagship White Paper Series*, http://urn.fi/urn, 2020.

[3] N. H. Mahmood, S. Böcker, I. Moerman et al., "Machine type communications: key drivers and enablers towards the 6G era," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, pp. 1–25, 2021.

[4] E. Grigoreva, M. Laurer, M. Vilgelm, G. Thomas, and W. Kellerer, "Coupled Markovian arrival process for automotive machine type communication traffic modeling," in *Proceedings of the 2017 IEEE International Conference on Communications (ICC)*, pp. 1–6, Paris, France, May 2017.

[5] M. Z. Shafiq, L. Ji, A. X. Liu, J. Pang, and J. Wang, "Large-scale measurement and characterization of cellular machine-to-machine traffic," *IEEE/ACM Transactions on Networking*, vol. 21, no. 6, pp. 1960–1973, 2013.

[6] F. Qasmi, M. Shehab, H. Alves, and L.A. Matti, "Fixed rate statistical qos provisioning for Markovian sources in machine type communication," in *Proceedings of the 2019 16th International Symposium on Wireless Communication Systems (ISWCS)*, pp. 474–479, Oulu, Finland, August 2019.

[7] J. L. Massey, "An introduction to contemporary cryptology," *Proceedings of the IEEE*, vol. 76, no. 5, pp. 533–549, 1988.

[8] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security," *Foundations and Trends™ in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, 2009.

[9] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Wireless Communications*, vol. 19, no. 1, pp. 40–47, 2012.

[10] M. Bloch and J. Barros, *Physical-layer Security: From Information Theory to Security Engineering*, Cambridge University Press, Cambridge, United Kingdom, 2011.

[11] D. Wu, "QoS provisioning in wireless networks," *Wireless Communications and Mobile Computing*, vol. 5, no. 8, pp. 957–969, 2005.

[12] I. Muhammad, H. Alves, L.A. Matti, O. A. Lopez, and N. H. Mahmood, "Mission effective capacity - a novel dependability metric: a study case of multi-connectivity enabled urllc for IIoT," *IEEE Transactions on Industrial Informatics*, no. 1–1, , 2021.

[13] W. Cheng, X. Zhang, and H. Zhang, "Heterogeneous statistical QoS provisioning for downlink transmissions over mobile wireless cellular networks," in *Proceedings of the 2014 IEEE Global Communications Conference*, pp. 4622–4628, Austin, TX, USA, December 2014.

[14] D. Wu and R. Negi, "Effective capacity: a wireless link model for support of quality of service," *IEEE Transactions on Wireless Communications*, vol. 2, no. 4, 2003.

[15] M. O. Memis, O. Ercetin, O. Gurbuz, and S. V. Azhari, "Resource allocation for statistical QoS guarantees in MIMO cellular networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, no. 1, 2015.

[16] M. C. Gursoy, "MIMO wireless communications under statistical queueing constraints," *IEEE Transactions on Information Theory*, vol. 57, no. 9, pp. 5897–5917, 2011.

[17] M. Hammouda, S. Akin, M. C. Gursoy, and J. Peissig, "Effective capacity in MIMO channels with arbitrary inputs," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 4, pp. 3252–3268, 2018.

[18] S. K. Sharma and X. Wang, "Toward massive machine type communications in ultra-dense cellular iot networks: current issues and machine learning-assisted solutions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 426–471, 2020.

[19] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5g wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[20] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Processing Letters*, vol. 19, no. 6, pp. 372–375, 2012.

[21] H. Alves, P. H. J. Nardelli, and C. H. M. D. Lima, "Secure statistical QoS provisioning for machine-type wireless communication networks," in *Proceedings of the 2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, pp. 1–5, Porto, Portugal, June 2018.

[22] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: a secure transmission design perspective," *IEEE Communications Letters*, vol. 15, no. 3, pp. 302–304, 2011.

[23] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, Dover, IL, USA, 9th edition, 1965.

[24] "Wolfram Alpha, ," 2019.

[25] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proceedings of the VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, 2005*, vol. 62, no. 3, Dallas, TX, USA, September 2005.

[26] I. Muhammad, L. A. L. Onel, H. Alves, P. M. O. Diana, E. E. B. Olivo, and L. A. Matti, "Adaptive secure rate allocation via TAS/MRC under multi-antenna eavesdroppers," in *Proceedings of the 2019 16th International Symposium on Wireless Communication Systems (ISWCS)*, pp. 666–671, Oulu, Finland, August 2019.

[27] 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, 2017.

[28] M. C. Gursoy, "Secure communication in the low-SNR regime," *IEEE Transactions on Communications*, vol. 60, no. 4, pp. 1114–1123, 2012.

[29] H. Alves, G. Brante, R. D. Souza, D. B. Costa, and M. A. Latva, "On the performance of secure full-duplex relaying under composite fading channels," *IEEE Signal Processing Letters*, vol. 22, no. 7, pp. 867–870, 2015.

[30] S. Asaad, A. Bereyhi, A. M. Rabiei, R. R. Muller, and R. F. Schaefer, "Optimal transmit antenna selection for massive MIMO wiretap channels," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 817–828, 2018.

[31] J. Y. Tang, M. Dongtang, P. Xiao, and K. K. Wong, Secrecy performance analysis for TAS-MRC system with imperfect feedback," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1617–1629, 2015.

[32] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Transactions on Communications*, vol. 61, no. 1, pp. 144–154, 2013.

[33] J. D. V. Sánchez, D. P. M. Osorio, F. J. M. Lopez, C. Paredes, and F. U. A. Luis, *Physical Layer Security of Tas/mrc over κ-μ Shadowed Fading Channel*, 2020, https://arxiv.org/abs/2005.02441.

[34] D. Qiao, M. C. Gursoy, and S. Velipasalar, "Secure communication over fading channels with statistical QoS constraints," in *Proceedings of the 2010 IEEE International Symposium on Information Theory*, pp. 2503–2507, Austin, TX, USA, June 2010.

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

[36] H. Alves, M. D. C. Tome, P. H. J. Nardelli, C. H. M. D. Lima, and M. A. Latva, "Enhanced transmit antenna selection scheme for secure throughput maximization without CSI at the transmitter," *IEEE Access*, vol. 4, pp. 4861–4873, 2016.

[37] H. Minn and D. Munoz, "Channel knowledge acquisition in relay and multipoint-to-multipoint transmission systems," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 4, pp. 1416–1434, 2015.

[38] A. Checko, C. L. Henrik, Y. Yan et al., "Cloud ran for mobile networks—a technology overview," *IEEE Communications surveys & tutorials*, vol. 17, no. 1, pp. 405–426, 2014.

[39] M. Ozmen and M. C. Gursoy, "Wireless throughput and energy efficiency with random arrivals and statistical queuing constraints," *IEEE Transactions on Information Theory*, vol. 62, no. 3, 2016.

[40] M. Amjad, L. Musavian, and M. H. Rehmani, "Effective capacity in wireless networks: a comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 4, 2019.

[41] M. Laner, N. Nikaein, P. Svoboda, M. Popovic, D. Drajic, and S. Krco, "Traffic models for machine-to-machine (M2M) communications," in *Machine-To-Machine (M2M) Communications*, pp. 133–154, Elsevier, Amsterdam, Netherlands, 2015.

[42] S. Cheng, *Performance Guarantees in Communication Networks*, Springer-Verlag, London, U.K., 2000.

[43] R. A. Waltz, J. L. Morales, J. Nocedal, and D. Orban, "An interior algorithm for nonlinear optimization that combines line search and trust region steps," *Mathematical Programming*, vol. 107, no. 3, pp. 391–408, 2006.

[44] Mathworks, *Constrained Nonlinear Optimization Algorithms*, Wiley, Hoboken, NJ, USA, 2016.

[45] D. Simon, *Evolutionary Optimization Algorithms*, Wiley, NJ, USA, 1st edition, 2013.