Secure Statistical QoS Provisioning for Machine-type Wireless Communication Networks

Hirley Alves*, Pedro. H. J. Nardelli* and Carlos H. M. de Lima‡
*Centre for Wireless Communications (CWC), University of Oulu, Finland
†Laboratory of Control Engineering and Digital Systems, Lappeenranta University of Technology, Finland
‡São Paulo State University (UNESP), São João da Boa Vista, Brazil
hirley.alves@oulu.fi, pedro.nardelli@lut.fi, carlos.lima@sjbv.unesp.br

***Abstract*—This work assesses the performance of secure machine-type communication networks composed of a legitimate pair of devices communicating in the presence of an eavesdropper. We evaluate the impact of legitimate source's arrival traffic in the design of secure communication protocol. Our approach is based on the secrecy outage probability framework, which identifies the security level of transmissions. We then characterize the secrecy transmission rate that includes the arrival traffic, evaluating its impact on the secrecy performance of the network. We introduce ON-OFF adaptive and non-adaptive transmission schemes that maximizes both the secure effective capacity and the maximum average arrival rate at the source node. Our numerical results provide insights on the interplay between the different traffic originated from MTC devices and security in the system.**

I. Introduction

Internet of Things (IoT) is already changing many aspects of our daily life, opening opportunities for new business models and revolutionizing the whole value chain of several industries; estimates say these have an economic potential in the order of trillions of dollars [1], [2]. The widespread of wireless connectivity allowing for machine-type communications (MTC) networks is at the core of the IoT revolution, consistent with the ambitious goals planned for the 5th generation of wireless networks (5G) [2]. In contrast to the previous generations, 5G proposes solutions for MTC based on two different application classes, namely massive MTC (mMTC) and ultra-reliable, low latency communication (URLLC). These two new modes enable MTC networks to operate with heterogeneous requirements – massive connectivity, or ultra-reliability and low latency – challenging current understanding of conventional techniques for wireless communications [2]–[4].

Many applications in MTC networks present devices with limited computational and power capabilities. This raises concern on privacy and secrecy, even more so due to large scale deployment of such devices as wireless transmissions are susceptible to eavesdropping. Hence, solutions that preclude such issues from design should be always welcome. One promising alternative to complement lightweight cryptography solutions (often used at higher layers of the communication protocol stack) is physical layer (PHY) security, which is built to be unbreakable and quantifiable (in confidential bps/Hz), regardless of the eavesdropper's computational power [5]–[7]. In this case, the legitimate pair of transmitter and receiver (dubbed Alice and Bob, respectively) are able to communicate securely regardless of the presence of an eavesdropper (dubbed Eve). Surveys on the most recent advances PHY security are presented in [5], [6], while [7] indicates PHY security as key technology to safeguard future wireless networks.

A common performance metric available in PHY security is secrecy outage probability [8]. This metric, however, is incapable of distinguishing between reliability and secrecy as far as an outage event occurs whenever Bob could not decode (unreliable transmission), or when information leaked (secrecy has been comprised). As a result, we are unable to know the level of security each transmission possesses. To fill this gap, the authors in [9] proposed a secure throughput metric capable of quantifying reliability and secrecy, separately, by assessing the security-reliability trade-off. In [10], we focused on MTC networks to shed light into a smart grid use-case investigating transmit antenna selection schemes at the Alice without channel state information (CSI) at the transmitter. Extending [9], the secure throughput is maximized and a security-reliability trade-off is established for multi-input, multi-output, multi-eavesdropper wiretap channel. The results showed that a small sacrifice in reliability allows secrecy enhancement, thus keeping an unintended eavesdropper unable to reconstruct the daily average power demand curve of an arbitrary household.

Even though security-reliability trade-off was establish in [9], [10], the trade-offs involved between security, ultra-reliability and latency were not discussed. In [11], the authors introduced the *effective secure throughput*, based on the effective capacity metric [12], which allows to investigate trade-offs between secrecy and latency subject to inherent characteristics of the wireless medium. In [13], the authors extended the analysis of [11], by investigating both throughput and energy efficiency of secure transmissions of delay sensitive data generated by Markovian sources. This allows for modeling the arriving traffic, while capturing its effects in the design of the secure communication link. Although [13] focused on broadcasting for broadband applications, the results can be also applied in MTC since Markovian sources can characterize different type of traffic generated by MTC devices, which are often composed of small, burst package transmissions [3], [14]. Both works looked at broadcast channels whose transmissions are composed by confidential and common messages. They mainly dealt with secrecy capacity as a metric assuming perfect CSI of all nodes. This, however, limits the

possible applications as the transmitters might not be aware of the eavesdroppers presence. Additionally, those works focus primarily on secure throughput-latency trade-off without any constraint on reliability.

In this work, we assess the performance of a MTC network composed of a legitimate pair of MTC devices communicating in the presence of an eavesdropper by evaluating the impact of the source's arrival traffic in the design of the secure communication rates. Different from [11], [13], we assume that CSI is available at the receivers and Alice can only estimate the legitimate channel. We build our contribution upon the secrecy outage probability framework proposed in [9], [10]. This approach allows us to identify the level of security each transmission possess and therefore design the appropriate secrecy transmission rate. We follow the recent contribution [13] to incorporate arrival traffic so its impact on the secrecy performance of the network can be evaluated. Therefrom, we propose the *secure effective capacity* metric based on an ON-OFF adaptive and non-adaptive transmission schemes that maximizes not only secure effective capacity but also the maximum average arrival rate at source. By doing so, we then provides insights about the effects of different traffic originated from MTC devices on the system performance.

II. System model

We consider a block-fading (Rayleigh) wiretap channel so that its coefficients remain constant over the coherence time of the block though change independently for the next block. A legitimate transmitter-receiver pair, namely Alice and Bob, is assumed to communicate in the presence of a passive eavesdropper, known as Eve. The aforesaid configuration is illustrated in Fig. 1. Note that Alice does not acquire Eve CSI (e.g. [9]), and receivers can only estimate their own channel. The received signal at Bob is $y_b = h_{ab}x + w_b$, while Eve perceives $y_e = h_{ae}x + w_e$, where x is the transmitted signal, h_{ij}, $i \in \{a\}$ and $j \in \{b, e\}$, denotes the Rayleigh distributed channel coefficients, while w_j represents receiver noise, which is considered to be a zero-mean, circularly symmetric complex Gaussian random variable with variance N_0.

From [5], [6] we known that Alice and Bob communicate with secrecy capacity defined as

$$C_s = [C_b - C_e]^+ = [\log_2(1+\gamma_{ab}) - \log_2(1+\gamma_{ae})]^+ \quad (1)$$

where C_b and C_e denotes the Bob' and Eve's channel capacities, respectively, while γ_{ab} and γ_{ae} are exponentially distributed random variables that represent the signal-to-noise ratio (SNR) at Bob and Eve, respectively, hence $\gamma_{ab} \sim \mathsf{Exp}(1/\Gamma_{ab})$ and $\gamma_{ae} \sim \mathsf{Exp}(1/\Gamma_{ae})$.

The secrecy outage probability is defined as $p_{\text{so}} \triangleq \Pr[C_s < R_s]$, where $R_s > 0$ is the target secrecy rate [5], [6], [9]. As aforesaid, p_{so} does not distinguish between reliability and secrecy, hence it implies that an outage event occurs: *i)* because Bob could not decode, therefore unreliable transmission; or *ii)* because there was an information leakage, thus secrecy has been comprised. Either way, we are unable to identify each transmission security level.

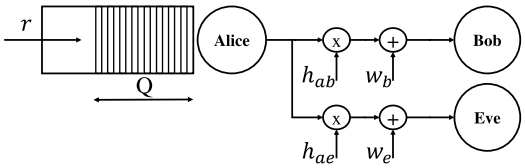

Fig. 1. System model. Consider a transmitter, Alice, with a buffer with Q with constant arrival rate communicating under block-fading channel with Bob, in the presence of a passive eavesdropper, Eve.

An alternative formulation was proposed in [9], defining secrecy outage probability where secrecy is assessed conditioned on the actual transmission, thus revealing the secrecy-reliability trade-off [9], [10]. Alice then chooses two code rates: transmission rate R_b and confidential rate R_s, where $R_e = R_b - R_s$; thereby, secrecy outage occurs if $C_e > R_e$ [9]. Then, p_{tx} in (2) denotes the conditional probability of transmission defined as $p_{\text{tx}} = \Pr[\gamma_{ab} > \mu] = \exp(-\mu/\Gamma_{ab})$, where a transmission takes places whenever the SNR of the legitimate channel (γ_{ab}) is above a certain threshold μ. Then, the secrecy outage probability can be written as [9]:

$$\begin{aligned} p_{\text{so}} &= \Pr[C_e > C_b - R_s \,|\gamma_{ab} > \mu] \\ &= \frac{2^{R_s}\Gamma_{ae}}{2^{R_s}\Gamma_{ae} + \Gamma_{ab}} \exp\left(-\frac{\mu + 1 - 2^{R_s}}{2^{R_s}\Gamma_{ae}}\right). \end{aligned} \quad (2)$$

In order to assess both the arrival and service processes at Alice, we assume that the corresponding secure information to be conveyed is stored in a buffer before actual transmission. The arrival rate of discrete-time Markovian source is characterized next.

A. Discrete-time Markovian Arrival

To evaluate the arrival process we resort to the effective bandwidth theory, which characterizes the minimum constant transmission rate required to sustain a random data arrival process, subject to queuing constraints, such as buffer overflow and delay violation [13], [15]. We assume that Markovian sources generate data which are stored in a buffer before transmission, as well as statistical quality of service (QoS) constraints are imposed.

Let Q be the stationary queue length, then θ represents the decay rate of the tail of the respective distribution, so that $\lim_{q\to\infty} \frac{\log \Pr[Q \geq q]}{q} = -\theta$, which translates to how strict are the QoS constraints of the system. For large $q \to q_{\max}$ the buffer violation probability can be approximated by $\Pr[Q \geq q_{\max}] \approx \Pr[Q > 0] \exp(-\theta\, q_{\max})$, where $\Pr[Q > 0]$ denotes the probability of non-empty buffer [12]. Notice that the QoS exponent θ, can be interpreted as a QoS measure, thus large values of θ represent strict QoS (delay) constraints, and if $\theta \to \infty$ no delay is tolerated. On the other hand, low values of θ imply in looser QoS constraints [12], [13], [15].

Next, let D denote the queuing delay in the buffer at steady state, while d is the delay threshold, then the delay violation probability is characterized as [13]

$$\Pr[D \geq d] \approx \Pr[Q > 0]\; e^{-\theta\, a(\theta)\, d}, \quad (3)$$

where $a(\theta)$ is the effective bandwidth of the arrival process $a(k), k \in \mathbb{N}^+$, which describes the random arrival rates (non-negative random variables).

Then, the time accumulated arrival process at the source is $A(t) = \sum_{k=1}^{t} a(k)$, and the effective bandwidth is characterized by the asymptotic logarithmic moment generating function of $A(t)$ [16]:

$$a(\theta) \triangleq \lim_{t\to\infty} \frac{1}{\theta t}\mathbb{E}\left[e^{-\theta A(t)}\right], \tag{4}$$

where $\mathbb{E}[\cdot]$ denotes mathematical expectation. As in [13], we employ a two-state (ON-OFF) Markovian model, namely discrete Markov source. In this model, the data arrival process is described as a two state discrete-time Markov chain, where during the ON state r bits arrive with a arrival rate of r bits/block, while no arrivals occur during the OFF state. Such system has a transition probability matrix $\mathbf{J} = (p)_{i\,j}$, where $p_{11} \in [0,1]$ denotes the probability of staying in the off state, while $p_{22} \in [0,1]$ denotes the probability of staying on the ON state, while the transition probabilities are $p_{21} = 1 - p_{22}$ and $p_{12} = 1 - p_{11}$. At the steady state, the probability of ON state is $p_{\text{ON}} = \frac{1-p_{11}}{2-p_{11}-p_{22}}$. The effective bandwidth is

$$a(\theta, r) = \frac{1}{\theta}\log\left(\tfrac{1}{2}\phi + \tfrac{1}{2}\sqrt{\phi^2 - 4(p_{11}+p_{22}-1)e^{r\theta}}\right) \tag{5}$$

$$\overset{(a)}{=} \frac{1}{\theta}\log\left(1 - s + se^{r\theta}\right), \tag{6}$$

where $\phi = p_{11} + p_{22}e^{r\theta}$, and (a) comes from a simplified version of the source with $p_{11} = 1 - s$ and $p_{22} = s$, hence $p_{\text{ON}} = s$ (refer to [15]). From (6), note that s becomes a measure of the burstiness, which is relevant to model different traffic generated by a MTC device. Given that the maximum average arrival rate is $\overline{r}_{\max} = r\,p_{\text{ON}}$. Next, we describe the service process.

B. Effective capacity

The effective capacity is defined as the maximum constant arrival rate that a process tolerates in order to guarantee a statistical QoS requirement defined by the exponent θ [12]. Similar to the arrival process, let us define the service process as $s(k), k \in \mathbb{N}^+$, which describes a discrete-time stationary and ergodic stochastic service process, while $S(t) = \sum_{k=1}^{t} s(k)$ is the time accumulated service process. Then, the effective capacity is defined as [12]:

$$E_c(\theta) = -\lim_{t\to\infty}\frac{1}{\theta}\log\mathbb{E}\left[e^{-\theta S(t)}\right] \overset{(a)}{=} -\frac{1}{\theta}\log\mathbb{E}\left[e^{-\theta R}\right], \tag{7}$$

where the effective capacity is simplified in (a) due to the dependence of the service process on the fading coefficients that change independently every block, R denotes the maximum service rate, which in this context is given as in (1).

To determine the maximum secure throughput in the following session, we first need to identify the maximum average arrival rate that can be supported by the wiretap fading channel. As pointed out in [13], the buffer violation probability as in (3) decays exponentially with rate controlled by the QoS exponent θ. If the effective bandwidth of the arrival process is equal to the effective capacity, the condition $a(\theta) = E_c(\theta)$ shall hold. Bearing this in mind, we solve such an equality, with $p_{\text{ON}} = s$, and obtain the maximum average arrival rate of the discrete-time Markov source as:

$$\overline{r}_{\max} = \frac{s}{\theta}\log\left(\frac{1}{s}\left(\exp\left(\theta\,E_c(\theta)\right) - (1-s)\right)\right). \tag{8}$$

III. Secure Throughput and Delay Analysis

We aim here at maximizing the secure throughput and identify the maximum arrival rate that can be sustained at Alice, while evaluating the impact of traffic burstiness on system performance. The secure throughput is defined as [9] $\eta = p_{\text{tx}}Rs$, where p_{tx} is the transmission probability – a condition to assess the level of security of conveyed messages as defined in (2). If the service process is a two-state Markov modulated process and remembering that the fading coefficients are independent, the ON state probability is then p_{tx} while the secure effective capacity becomes

$$SE_c(R_s, \theta) = -\frac{1}{\theta}\log\left(1 - p_{\text{tx}}(1 - e^{-\theta R_s})\right). \tag{9}$$

Remark 1. *Differently from [13, Sect. IV], which assumes no CSI at Alice, we assume that Alice knows only the legitimate link CSI, and thus is able to adapt its transmission rate accordingly. We are then able to model the services as an ON-OFF Markov chain, because we conditioned security on the an actual transmission, thus steady probability of the ON state is p_{tx}. Therefore,* (9) *differs from [13, Eq. (65)] because steady probability of the ON state is considered as a function of the secrecy outage probability (e.g. $1 - \Pr[C_s < R_s]$) rather than p_{tx}. However, as discussed above, such metric do not allow one to infer the security level achieved in each transmission.*

Remark 2. *Note that as $\theta \to 0$ the secure effective capacity converges to $\lim_{\theta\to 0} SE_c(R_s, \theta) = p_{\text{tx}}R_s$, as in [9].*

Fig. 2 illustrates the difference between formulations of the conventional secure effective capacity in [13, Eq. (65)] and the proposed one in (9). We assume the worst case scenario for (9) (thus, $\mu = 2^{R_s} - 1$) and $10\log_{10}\Gamma_{ab}/\Gamma_{ae} = 10$ dB, as well as $\theta = 10^{-3}$ (loose) and $\theta = 1$ (tight) QoS exponents. The formulation in (9) captures the level of security that can be achieved within each transmission, as well as allows Alice and Bob to communicate with larger secure rates for a given secure effective capacity or to achieve higher secure effective capacity at fixed R_s. We also observe that tight delay constraints induce an effective capacity reduction. Thus, for more stringent delay requirements $\theta \gg 0$, we observe that lower $\overline{r}_{\max}$ can be tolerated, while the source burstiness reduces $\overline{r}_{\max}$. In other words, the wireless fading channel is not able to cope with larger arrival rates, thus increasing the queue length and delay of the network. We attempt to reduce this effect by maximizing the secrecy effective capacity, which also optimizes $\overline{r}_{\max}$.

As the maximum average arrival rate is an increasing function of $E_c(\theta)$, we can optimize $SE_c(R_s, \theta)$ subject to a

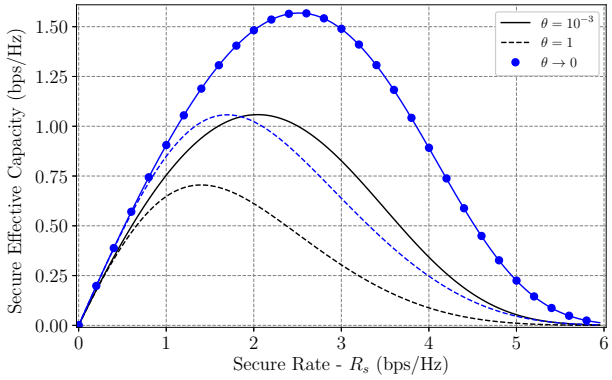

Fig. 2. Secure effective capacity from [13, (65)] (in black), and the proposed in (9) (in blue). The gain between legitimated and eavesdropper links is 10 dB. The asymptotic case $\lim_{\theta\to 0} SEC(R_s, \theta)$ is shown by the markers.

minimal reliability $p_{\text{tx}} \geq \sigma$ and a maximum security leakage $p_{\text{so}} \leq \epsilon$ for a positive secrecy rate – $R_s > 0$. Then,

$$\begin{aligned} &\underset{R_s,\mu}{\text{argmax}} \quad SE_c(R_s, \theta) \\ &\text{subject to} \quad p_{\text{so}} \leq \epsilon, p_{\text{tx}} \geq \sigma, \mu \geq 2^{R_s} - 1, R_s > 0. \end{aligned} \tag{10}$$

Remark 3. *We evaluate adaptive and non-adaptive rate allocation schemes, as in [9] but with a distinct objective function as in* (10)*. The adaptive scheme resorts to the CSI available at Alice to adapt its secure rate for the duration of the fading block, while the non-adaptive scheme does not require CSI, but relies on a* 1*-bit feedback so as to enable ON-OFF transmissions. Moreover, since no CSI is available, Alice resorts to fixed Wyner codes, and thus fixes the transmission rates R_b and R_s, and in this case the secrecy outage probability becomes $p_{so} = \exp\left(-(2^{R_b - R_s} - 1)/\Gamma_{ae}\right)$.*

Note that the constraint $\mu \geq 2^{R_b} - 1$ holds, since a transmission only occurs when $C_b > R_s$. From those constraints, we attain the secrecy-reliability trade-off as $\epsilon > \frac{1}{1+\alpha}\sigma^{\alpha}$ where $\alpha = \frac{\Gamma_{ab}}{\Gamma_{ae}}$, and the solution follows similar steps as in [9], but non-adaptive case cannot be solved in closed-form. The solution is found numerically using the Sequential Least SQuares Programming (SLSQP) library from Scipy[1].

Fig.3 shows the optimal secure effective capacity as function of the targeted reliability for distinct values of secrecy outage probability ϵ and QoS exponents. Note that higher secure effective capacity can be sustained for loose security. When reliability requirement becomes too stringent, the secure throughput tends to zero since the assigned rate capable of meeting both the security and reliability requirements becomes too small. Strict reliability, latency and security constraints can be only met if the legitimate link experiences much higher SNR values when compared to the eavesdropper, i.e. $\Gamma_{ab}/\Gamma_{ae} \ggg 1$. For this setting we have assumed 20 dB gain. In what follows, we fixed the target reliability and focus on variations of the secrecy outage probability threshold, as depicted in Fig. 4. These results confirm our intuition that to

[1]Further documentation is found here https://docs.scipy.org/doc/scipy-0.19.1/reference/index.html.

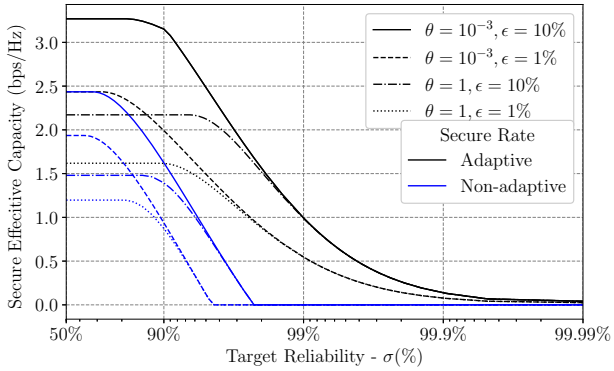

Fig. 3. Secure effective capacity as a function of the targeted reliability σ for different combinations of secrecy outage probability ϵ and QoS exponents θ values.

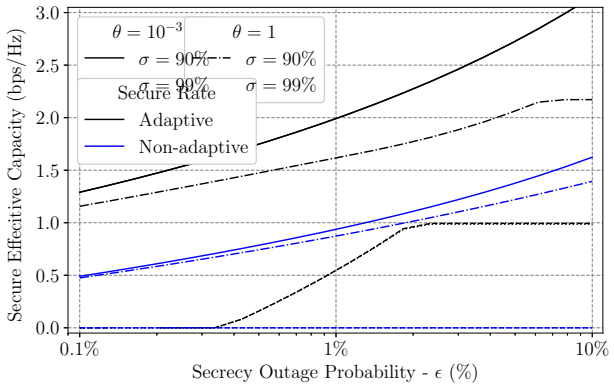

Fig. 4. Secure effective capacity as a function of the targeted secrecy outage probability ϵ for distinct values of reliability requirements σ and QoS exponents θ.

guarantee high reliability and security, we need to sacrifice throughput, in this case secure effective capacity, and increase SNR. From this figure we can also observe that positive secure rates are attained even under stringent requirements (e.g. $\theta = 1$, $\sigma \geq 90\%$ and $\epsilon = 1\%$). As we can observe from those figures, the non-adaptive case offers lower performance compared to its counterpart; however, the performance loss is compensated whenever the communication overhead needs to be minimized. In this case, the non-adaptive scheme does not require CSI at Alice, but a single bit of feedback so as to enable the ON-OFF transmission.

So far, we have observed mainly the impact of security and reliability, we now evaluate the effects of latency as in Fig. 5, where delay violation probability (as in (3)) is shown as a function of the targeted reliability for distinct values of secrecy outage probability, source's burstiness, for $d = 10$ and $\theta = 1$, since smaller values of $\theta \to 0$ impose longer delays as effective capacity converges to capacity, and in this context delay violation probability tends to 1. Fig. 5 shows that burst traffic increases the delay violation probability, since lower maximum average arrival rates are tolerated. Notice as well that security constraints increase the delay violation probability, since lower secrecy outage probability imply lower secure effective capacity as discussed above. Further, Fig. 6 shows

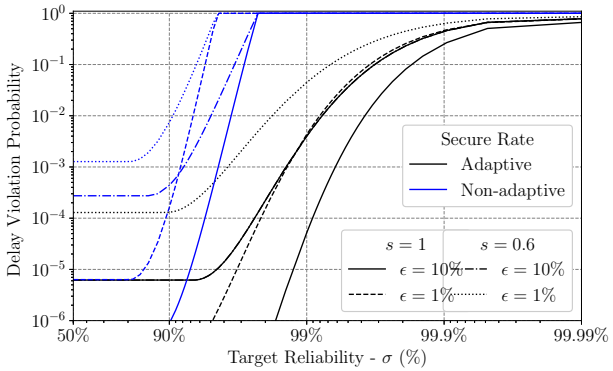

Fig. 5. Delay violation probability as function of the targeted reliability for distinct values of secrecy outage probability, source's burstiness.

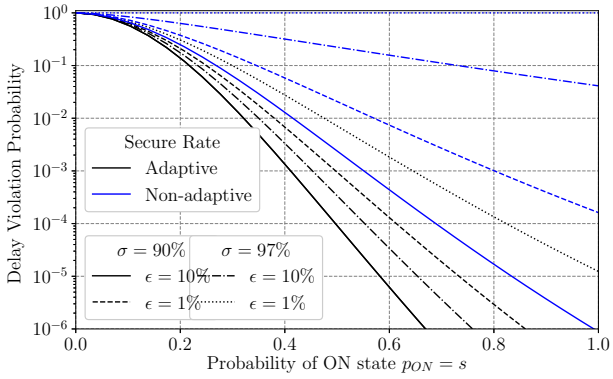

Fig. 6. Delay violation probability vs. ON state probability for different secrecy outage probabilities and QoS exponents.

the delay violation probability as a function of the burstiness measure of the sources' arrivals, the parameter $p_{\text{ON}} = s$ for fixed target reliability and secrecy outage probability. The source burstiness (small s) reduces the maximum average arrival rate, which in its turn impacts the delay violation probability. With such configuration, it becomes impractical to operate in the ultra reliable region (high to ultra reliability $> 99.9\%$), since the secure effective capacity tends to zero as $\sigma \to 1$ and hence delay violation probability tends to unity in that region. However, for applications that do not require ultra-reliability ($< 99.9\%$), e.g. sensor network, smart metering [10], reasonable performance is achieved in terms of secure transmission rates, reliability and secrecy outage probability. For instance, $\sigma < 99\%$ and $\epsilon = 1\%$ renders delay violation probabilities lower than 10%, which can be reduced even further by slight decreasing the reliability target. Even though the non-adaptive is outperformed by the adaptive scheme, its analysis is still relevant given the reduced overhead of the secure communication protocol and for applications that have mild requirement in terms of reliability and latency, such scheme appears as a suitable strategy. However, as observed in Fig.6 the delay violation probability increases considerably as the security and reliability levels become tighter.

IV. Discussion and Conclusions

We assess MTC networks composed by a legitimate pair of machine-type devices communicating in the presence of an eavesdropper node, and then evaluate their performance considering the impact of source's arrival traffic in the design of secure communication rates. Moreover, we introduce a new metric that captures the impact of source's burstiness in the design of a secure communication link when constrained on some level of reliability and security. Our results show that the aforementioned levels can be met for mild reliability and latency constraints. In order to cope with stringent reliability, latency and security requirements, the legitimate link needs to be designed so to provide high SNR gain over Eve's link. This, for instance, could be achieved via spatial diversity or friendly jamming at the Eve, which are the future directions from the present contribution.

Acknowledgments

This work is partially supported by Academy of Finland (n.303532 and SRC/n.292854).

References

[1] B. R. Haverkort and A. Zimmermann, "Smart Industry: How ICT Will Change the Game!" *IEEE Int. Comput.*, vol. 21, no. 1, 2017.
[2] Ericsson, "5G Systems," Tech. Rep. January, 2017.
[3] Nokia, "5G for Mission Critical Communication:Achieve ultra-reliability and virtual zero latency," *Nokia White Pap.*, 2016.
[4] P. Popovski, J. J. Nielsen, C. Stefanovic, E. de Carvalho, E. Ström, K. F. Trillingsgaard, A.-S. Bana, D. M. Kim, R. Kotaba, J. Park, and R. B. Sørensen, "Ultra-Reliable Low-Latency Communication (URLLC): Principles and Building Blocks," pp. 1–7, aug 2017.
[5] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Commun. Surv. Tut.*, vol. 16, no. 3, 2014.
[6] R. F. Schaefer, H. Boche, and H. V. Poor, "Secure Communication under Channel Uncertainty and Adversarial Attacks," *Proc. IEEE*, vol. 103, no. 10, pp. 1796–1813, 2015.
[7] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, 2015.
[8] J. Barros and M. D. Rodrigues, "Secrecy Capacity of Wireless Channels," *2006 IEEE Int. Symp. Inf. Theory*, vol. 1, pp. 356–360, 2006.
[9] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the Secrecy Outage Formulation: A Secure Transmission Design Perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, mar 2011.
[10] H. Alves, M. De Castro Tome, P. H. J. Nardelli, C. H. M. De Lima, and M. Latva-Aho, "Enhanced Transmit Antenna Selection Scheme for Secure Throughput Maximization Without CSI at the Transmitter," *IEEE Access*, vol. 4, no. 2, pp. 4861–4873, 2016.
[11] D. Qiao, M. C. Gursoy, and S. Velipasalar, "Secure Wireless Communication and Optimal Power Control Under Statistical Queueing Constraints," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, 2011.
[12] Dapeng Wu and R. Negi, "Effective capacity: A wireless link model for support of quality of service," *IEEE Trans. Wirel. Commun.*, vol. 24, no. 5, pp. 630–643, may 2003.
[13] M. Ozmen and M. C. Gursoy, "Secure Transmission of Delay-Sensitive Data Over Wireless Fading Channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 9, pp. 2036–2051, sep 2017.
[14] M. Laner and *et al.*, *Traffic models for machine-to-machine (M2M) communications: types and applications*. Book chapter "Machine-to-machine communications, architecture, performance and applications", Edited by M. Dolher and C. Anton, Woodhead Publishing, 2014.
[15] M. Ozmen and M. C. Gursoy, "Wireless throughput and energy efficiency with random arrivals and statistical queuing constraints," *IEEE Trans. Inf. Theory*, vol. 62, no. 3, pp. 1375–1395, 2016.
[16] Cheng-Shang Chang, "Stability, queue length, and delay of deterministic and stochastic queueing networks," *IEEE Trans. Automat. Contr.*, vol. 39, no. 5, pp. 913–931, may 1994.