IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 1, 2016, accepted August 11, 2016, date of publication August 30, 2016, date of current version September 16, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2601629

Enhanced Transmit Antenna Selection Scheme for Secure Throughput Maximization Without CSI at the Transmitter

HIRLEY ALVES[1], MAURICIO DE CASTRO TOMÉ[1], PEDRO HENRIQUE JULIANO NARDELLI[1], CARLOS H. M. DE LIMA[2], AND MATTI LATVA-AHO[1]

[1]Centre for Wireless Communications, University of Oulu, 90014 Oulu, Finland
[2]São Paulo State University (UNESP), 13876-750 São João da Boa Vista, Brazil

Corresponding author: H. Alves (halves@ee.oulu.fi)

This work was supported in part by the Academy of Finland through the Project SAFE under Grant 303532, in part by the Strategic Research Council/Aka BCDC Project under Grant 292854, and in part by the joint Aka and CNPq/Brazil Project SUSTAIN under Grant 490235/2012-3.

ABSTRACT This paper addresses the establishment of secure communication links between Alice and Bob in the presence of an eavesdropper (Eve). The proposed scenario assumes: 1) MIMOME wiretap channel; 2) transmit antenna selection at the Alice; 3) no channel state information at the transmitter; 4) fixed Wyner codes; and 5) guarantee of secure throughput by both quality of service and secrecy outage constraints. We propose a simple protocol to enhance security via transmit antenna selection, and then assess its performance in a closed form by means of secrecy outage and successful transmission probabilities. We assume these probabilities are our constraints and then maximize the secure throughput, establishing a security-reliability tradeoff for the proposed scenario. Our numerical results illustrate the effect of this tradeoff on the secure throughput as well as on the number of antennas at Alice, Bob, and Eve. Interestingly, a small sacrifice in reliability allows secrecy enhancement in terms of secure bps/Hz. We apply this idea in our smart grid application (where Alice represents a smart meter and Bob an aggregator) to exemplify that, although Eve may acquire some samples of the average power demand of a household, it is not enough to properly reconstruct such curve.

INDEX TERMS Physical layer security, secure throughput, secrecy outage probability, smart-grids.

I. INTRODUCTION

Wireless networks have become an indispensable part of our daily life through several applications that allows us to remotely monitor and control different processes within our homes, workplaces or even modern power grids. In this context, each application has its own set of requirements and performance targets, which should be considered whenever designing communication systems. For instance, smart meters sending information about energy consumption have looser reliability and latency requirements than grid control and demand menagement applications in the aggregator [1]–[3].

One downside of wireless systems relates to information security and secrecy as they more susceptible to eavesdropping and denial of service attacks (e.g. jamming and spoofing) than wired systems due to its own nature [4]–[6]. To cope with such issue, current security systems are mainly based on cryptographic methods employed at the upper layers of communication protocols, while assuming limited computational power at the eavesdropper [5], [6].

This assumption, nonetheless, is becoming an issue nowadays since the computational power of devices are steadily growing. Another weak point is that cryptographic solutions often overlook the physical properties of the wireless medium, the relative locations of the network elements and the actual transmitted information [5]–[7].

Information-theoretic security at the physical layer has reemerged to cope with such issues and complement cryptography by adding reliability and confidentiality at lower layers [6]. Physical layer (PHY) security can also open new ways to enhance robustness and reduce the complexity of conventional cryptography as far as it is built to be unbreakable and quantifiable (in confidential bps/Hz), regardless of the eavesdropper's computational power [6]. The notion of

PHY-security was first introduced by Shannon in his seminal work in 1949 [8]. But it was only later, in 1975, that Wyner proposed in [9] the wiretap channel where the eavesdropper attempts to decode the information based on a degraded version of the legitimate link signal. Later in [10], authors showed the existence of a transmission rate that guarantees confidentiality based only on the statistics of the wireless channel.

In 2008, after a long period, those initial results are extended to account for the effects of fading channels [11], [12]. Thereafter, different established techniques in wireless systems have been analyzed, for instance multiple antenna wiretap channel is characterized in [13], cooperative diversity is investigated in [14]–[16], while multi antenna diversity schemes are analyzed in [17]–[20]. Besides, PHY-security is point out as a key technology to safeguard future wireless communications networks [21]. Notwithstanding all these fundamental results and advances, most works have quite restrictive assumptions on the eavesdropper, for instance, it is common to assume some (or even full) knowledge of the channel state information (CSI) of the eavesdropper [6], which turns out to be not feasible in practice since the legitimate transmitter may not be aware of the eavesdroppers. Alternatively, few works consider the case where no CSI is available at the transmitters [16], [22]–[25]; however perfect secrecy cannot be achieved at all times and then secrecy outage characterization is performed in order to capture the probability of having a reliable and secure transmission.

Consequently, PHY-security is neglected as a suitable option, even when the application in consideration presents the characteristics that would make such an approach viable. Some applications of the smart energy grid are good examples where PHY-security appears as an attractive solution to enhance security and confidentiality [26]. PHY-security enables an enhanced secure communication network (i) within smart-homes, (ii) between smart-meters and aggregators, and (iii) between aggregators and the local (cloud-)controller; and these three levels of communications are in fact the information backbone of the modern electricity distribution grid [1], [2], [4], [5]. Besides [5], which summarizes the wireless network architecture in smart grid and proposes a key establishment protocol, few works consider PHY-security in this context.

In this work we attempt to fill this gap and focus on the secure communication between smart meters and aggregators in the presence of an eavesdropper (known as Eve). We assume that the smart meter poses as a legitimate transmitter (also known as Alice), while the aggregator acts as the legitimate receiver (known as Bob). Both receivers (Bob and Eve) are able to estimate their own CSI, but Alice does not possess any CSI and resorts to adaptive encoder with constant transmit rate (which can be optimally chosen). We build upon [17], [18], which introduces a scheme that allows only Bob to exploit diversity from Alice's transmission and thus limiting Eve's attack by design; therefore, we assume that all nodes have multiple antennas, but Alice employs transmit antenna selection (TAS) while Bob and Eve employ maximal ratio combining (MRC). Then, we characterize the secrecy outage and secure throughput. Finally, we put our results in the context of smart grids, and thus resort to actual measured data and evaluate the impact of outages in the reconstruction of the average power demand by the aggregator.

Our results show that the proposed scheme achieves high reliability while restricting Eve capabilities by design and therefore enhancing security. Our main contributions are summarized next:

- we extend the results in [18] and [24] by (i) assuming multi antenna wire-tap channel (all nodes have multiple antennas), (ii) characterizing in closed-form the secrecy outage probability for the case without CSI at the transmitter, thus extending also the results in [16], [22], and [23] to the MIMOME wire-tap channel; (iii) provide a secure throughput analysis;
- we analyze the trade-off between security and reliability by introducing a parameter that reflects the quality of service of the legitimate link;
- we propose a secure throughput maximization problem, and we evaluate the respective system performance with respect to the network configuration parameters;
- we investigate how the trade-off between secrecy and reliability affects performance in terms of secure throughput;
- we apply our results to smart grids, resorting to actual data to support and exemplify our findings; we show that even if Eve acquires some information, it will not be enough to reconstruct the power demand curve of a household.

The rest of this paper is organized as follows: Section II introduces the system model and our main assumptions, Section III presents the secure outage probability analysis focusing on the optimization problem, and illustrates how the system performance changes with respect to the configuration parameters. Then, Section IV addresses the secure reconstruction of the average power demand curve as a function of the outage events, while Section V discuss how our results might be used in actual deployments. Section VI draws the final remarks and concludes this 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, then $(\mathbf{x})^T$ and $(\mathbf{x})^\dagger$ denote transpose and conjugate transpose operations, respectively. The $m \times m$ identity matrix is represented as $\mathbf{I}_m$. 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 its expectation is denoted as $\mathbb{E}[\cdot]$. Gamma function is defined as $\Gamma(z)$ [27, Ch. 6, Sec. 6.1.1], and the regularized lower incomplete gamma function is denoted as $\mathrm{P}(s, z) = \frac{\gamma(s,z)}{\Gamma(z)}$ [27, Ch. 6, Sec. 6.5.1].

II. SYSTEM MODEL

We assume multiple antenna wiretap channel where a legitimate pair attempts to communicate securely in the presence of an eavesdropper. The transmitter is known as Alice and represents a smart meter and possesses N_A antennas. An smart meter is a device with limited processing capabilities, whose main characteristics encompass monitoring of power consumption, data exchange between customer and aggregator or vise versa, besides guaranteeing privacy [1]. Therefore, we assume that Alice employs TAS, which is simplest diversity scheme as well as energy efficient [18].

On the other hand, the aggregator is responsible for acquiring information from smart meters, performing control and management actions, and act as well in the electric market [3], [28]. Thus is reasonable to assume that the aggregator has much more hardware capabilities and processing power than an smart meter. In this context, we assume that Bob acts as an aggregator with N_B antennas and is able to perform MRC. The untrusted node, commonly named as Eve, is assumed to have N_E antennas. Eve may eavesdrop and attempt to acquire data from Alice's transmissions. Herein, we assume that Alice sends its average power demand to the aggregator, which by its turn reconstructs this signal in order to perform control and power demand management of its grid.

This scenario is depicted in Fig. 1, where the solid black line represents the communication between Alice and Bob, while eavesdropper link is depicted in as a dashed red arrow. Moreover, both receivers are able to estimate their own CSI, but no CSI is fed back to Alice. However, there is a open and error-free feedback channel between Bob and Alice which is used to convey the index of Alice's antenna with the best signal-to-noise-ratio (SNR) and enable on-off transmission.

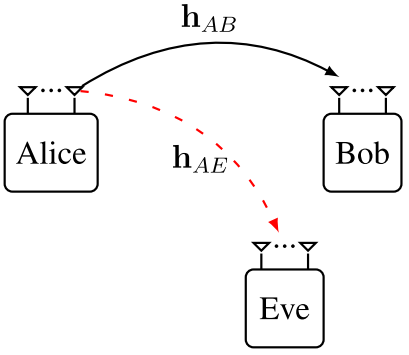


FIGURE 1. Network deployment illustration: Alice employs TAS, while Bob and Eve resort to MRC, but only Bob is able to exploit diversity from Alice's antennas. An error-free open channel is assumed between Bob and Alice, so that Bob can enable the Alice's transmission and inform the best antenna index.

As in [16] and [18], such channel is open and error-free, and even if Eve acquires this feedback and knows the antenna index an optimum TAS scheme with respect to Bob is a random TAS scheme concerning Eve. Therefore, Eve is not able to exploit diversity from Alice's multiple antennas since legitimate and eavesdropper channels are uncorrelated. Another advantage of this approach is that the feedback channel can have limited capacity, and the number of bits necessary for this channel is $n_{bits} = \lceil \log_2 N_A \rceil$.

A. TRANSMISSION PROTOCOL AND ENCODING SCHEME

The aggregator schedules and requests each smart meter to send its average power demand. Such a request is performed though the feedback channel, which not only carries the signaling to start the transmission but also the antenna index. Since no CSI is fed back to Alice, we resort to fixed Wyner codes, with constant transmission rate, which can be optimally chosen given the network configuration parameters as we shall see in the next section.

Let us first define the capacity of the legitimate and eavesdropper links as C_b and C_e, respectively. Then, Bob chooses two rates: a transmission rate R_b and a confidential rate R_s, and we define the cost of securing a transmission as $R_e = R_b - R_s$ [22]–[24]. Then, two conditions arise in order to guarantee secrecy and reliability: (i) whenever $C_b > R_b$ the message is correctly decoded at Bob; and (ii) an information leakage occurs whenever $C_e > R_e$ [22]–[24]. These conditions guarantee that there is a Wyner code that ensures a reliable (small error probabilities) and secure communication link. Further details of fixed Wyner codes and code construction can be found in [22] and [23]. Furthermore, in this context we adopt a probabilistic measure of security, namely *secrecy outage probability*, and then we are able to characterize the secure throughput maximization problem analyzed in Section III.

B. LEGITIMATE AND EAVESDROPPER CHANNEL MODELS

We assume that all channels coefficients are independent and the squared-envelope is exponentially distributed, thus we consider Rayleigh fading. In the legitimate channel, a single transmit antenna is selected at Alice to maximize the SNR at Bob, which applies MRC at the received signal. The best antenna index is defined as i^*:

$$i^* = \underset{1 \leqslant i \leqslant N_A}{\operatorname{argmax}} \; ||\mathbf{h}_{iB}||, \tag{1}$$

where $\mathbf{h}_{iB} = \left[h_{i1}, h_{i2}, \cdots, h_{iN_B}\right]^T$ denotes the $N_B \times 1$ channel vector between the ith transmit antenna at Alice and the N_B antennas at Bob with independent and identically distributed (i.i.d.) Rayleigh fading.

Then, Alice encodes the message with the codeword $\mathbf{x} = [x(1, \cdots, x(i), \cdots, x(n))]$, using the aforementioned Wyner codes [23]. We also assume that the codeword transmitted is subject to an average power constraint $\frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[|x(i)|^2\right] \leqslant P_A$, where P_A denotes Alice's transmit power. Then, Bob combines the signal vectors using MRC, which yields the following received signal at time i:

$$y_B(i) = \mathbf{h}_{AB}^{\dagger}\mathbf{h}_{AB}x(i) + \mathbf{h}_{AB}^{\dagger}\mathbf{n}_{AB}, \tag{2}$$

where $\mathbf{h}_{AB} = \mathbf{h}_{i^*B}$ represents the legitimate channel vector, $\mathbf{n}_{AB}$ is the $N_B \times 1$ additive white Gaussian noise vector at Bob, assuming $\mathbb{E}\left[\mathbf{n}_{AB}\mathbf{n}_{AB}^{\dagger}\right] = \mathbf{I}_{N_B}\sigma_{AB}^2$, with σ_{AB}^2 being the noise

variance at each antenna. Thus, from (2) the instantaneous SNR of the legitimate link is

$$\gamma_B = \frac{||\mathbf{h}_{AB}||^2 P_A}{\sigma_{AB}^2}, \tag{3}$$

and its PDF and CDF are defined, respectively, as

$$f_{\gamma_B}(\gamma) = \frac{N_A\, \gamma^{N_B-1}}{\Gamma(N_B)\, \overline{\gamma}_B^{N_B}} \exp\left(-\frac{\gamma}{\overline{\gamma}_B}\right) \mathrm{P}\left(N_B, \frac{\gamma}{\overline{\gamma}_B}\right)^{N_A-1}, \tag{4}$$

$$F_{\gamma_B}(\gamma) = \mathrm{P}\left(N_B, \frac{\gamma}{\overline{\gamma}_B}\right)^{N_A}, \tag{5}$$

where $\overline{\gamma}_B$ denotes the average SNR and we recall that $\mathrm{P}(\cdot,\cdot)$ denotes the regularized lower incomplete gamma function [27, Ch. 6, Sec. 6.5.1] Notice from (4) and (5) that the legitimate channel exploits diversity from Alice and Bob's multiple antennas.

On the other hand, Eve perceives a random TAS scheme, thus can only exploit diversity from its own antennas. Therefore, Eve combines the eavesdropped signal vectors using MRC, which yields the following received signal at time i

$$y_E(i) = \mathbf{h}_{AE}^{\dagger}\mathbf{h}_{AE}x(i) + \mathbf{h}_{AE}^{\dagger}\mathbf{n}_{AE}, \tag{6}$$

where $\mathbf{h}_{AE} = \mathbf{h}_{i^*B}$ represents the eavesdropper channel vector, $\mathbf{n}_{AE}$ is the $N_E \times 1$ additive white Gaussian noise vector at Eve, assuming $\mathbb{E}\left[\mathbf{n}_{AE}\mathbf{n}_{AE}^{\dagger}\right] = \mathbf{I}_{N_E}\sigma_{AE}^2$, with σ_{AE}^2 being the noise variance at each antenna. Similarly to the legitimate link, all channels undergo Rayleigh fading. In this context, we write the instantaneous SNR at Eve as $\gamma_E = \frac{||\mathbf{h}_{AE}||^2 P_A}{\sigma_{AE}^2}$, which follows Gamma distribution, and its PDF and CDF are given receptively as [18], as in (4) and (5), but with the following substitutions $\gamma_B = \gamma_E$, $\overline{\gamma}_B = \overline{\gamma}_E$, $N_A = 1$ and $N_B = N_E$, where $\overline{\gamma}_E$ denotes the average SNR at Eve.

III. SECRECY OUTAGE AND SECURE THROUGHPUT

As discussed above there are two conditions so as to guarantee secrecy and reliability [23], [24]. With respect to the former, the channel capacity has to be greater than the transmission rate, thus $C_b > R_b$ which ensures that the message is decoded. Therefore, we define the probability of successful transmission for the proposed scheme in the following lemma.

Lemma 1: The probability of successful transmission for the system model of Section II assuming that an on-off transmission scheme, which occurs whenever γ_B exceeds an SNR threshold μ, is $p_{suc} = \Pr[C_b > R_b] = \Pr[\gamma_B > \mu] = 1 - F_{\gamma_B}(\mu)$, where $F_{\gamma_B}(\cdot)$ is given in (5) *and $\mu \geqslant 2^{R_b} - 1$, which reflects the minimum value that guarantees reliability at the legitimate link.*

On the other hand, regarding security, an information leakage occurs whenever $C_e > R_e$, where $R_e = R_b - R_s$, and thus we have secrecy outage which can be defined as follows.

Lemma 2: Given the system model of Section II and fixed Wyner codes, the probability of secrecy outage is $p_{so} = \Pr[C_e > R_b - Rs] = \Pr\left[\gamma_E > 2^{R_b-R_s} - 1\right] = 1 - F_{\gamma_E}(2^{R_b-R_s} - 1)$, where $F_{\gamma_E}(\cdot)$ is the CDF of γ_E.

Let us introduce an example of Lemmas 1 and 2. Fig. 2 illustrates the performance of the success probability (p_{suc}) and secrecy outage probability (p_{so}) as a function of the transmission rate R_b. As expected, the performance improves by increasing the number of antennas either at the legitimate link or at the Eve. However, Eve can only change its own diversity, and thus outage probability (we recall that higher secrecy outage, means that more information is acquired by the eavesdropper), by adding more antennas, since it cannot exploit diversity from Alice's antennas. In its turn, the legitimate channel performance enhances even more if the aggregator dedicates more antennas to reception. Additionally, notice that we assume a multiple antenna scenario, encompassing the single antenna case introduced in [24].

After presenting Lemmas 1 and 2, we are able to define the secure throughput and the maximization problem.

Definition 1 (Secure Throughput): The secure throughput T_s of the legitimate link (between smart meter and aggregator) is defined as

$$T_s \triangleq R_s\, p_{suc} = R_s \left(1 - \mathrm{P}\left(N_B, \frac{\mu}{\overline{\gamma}_B}\right)^{N_A}\right). \tag{7}$$

With respect to Alice, our goal is to determine the best transmission rate that ensures both reliability and secrecy. This thus maximizes the secure throughput to Bob, while respecting secrecy outage ($p_{so}(R_b, R_s) \leqslant \epsilon$) and QoS constrains ($p_{suc}(\mu) \geqslant \sigma$). Then, we can define the following maximization problem as

$$\begin{aligned} &\underset{R_s, R_b, \mu}{\text{argmax}} \; T_s \\ &\text{subject to } p_{so}(R_b, R_s) \leqslant \epsilon \\ &\qquad p_{suc}(\mu) \geqslant \sigma \\ &\qquad \mu \geqslant 2^{R_b} - 1 \\ &\qquad R_s > 0, \end{aligned} \tag{8}$$

where $0 \leqslant \sigma \leqslant 1$ is the minimum acceptable success probability, reflecting the QoS constraint on the legitimate channel, and $0 \leqslant \epsilon \leqslant 1$ is the maximum acceptable information leakage.

Note that Alice is aware that eavesdropping may occur, and thus protects its transmission by optimally selecting a proper rate while minimizing the secrecy outage. We will further discuss the impact of these assumptions in Section IV. From (12) and Lemma 2, we can see that $p_{so}(R_b, R_s)$ is independent of μ. Thereby, we first maximize $p_{suc}(\mu)$, which is monotonically decreasing with respect to μ, by minimizing μ. Hence, its optimal value is $\mu = 2^{R_b} - 1$.

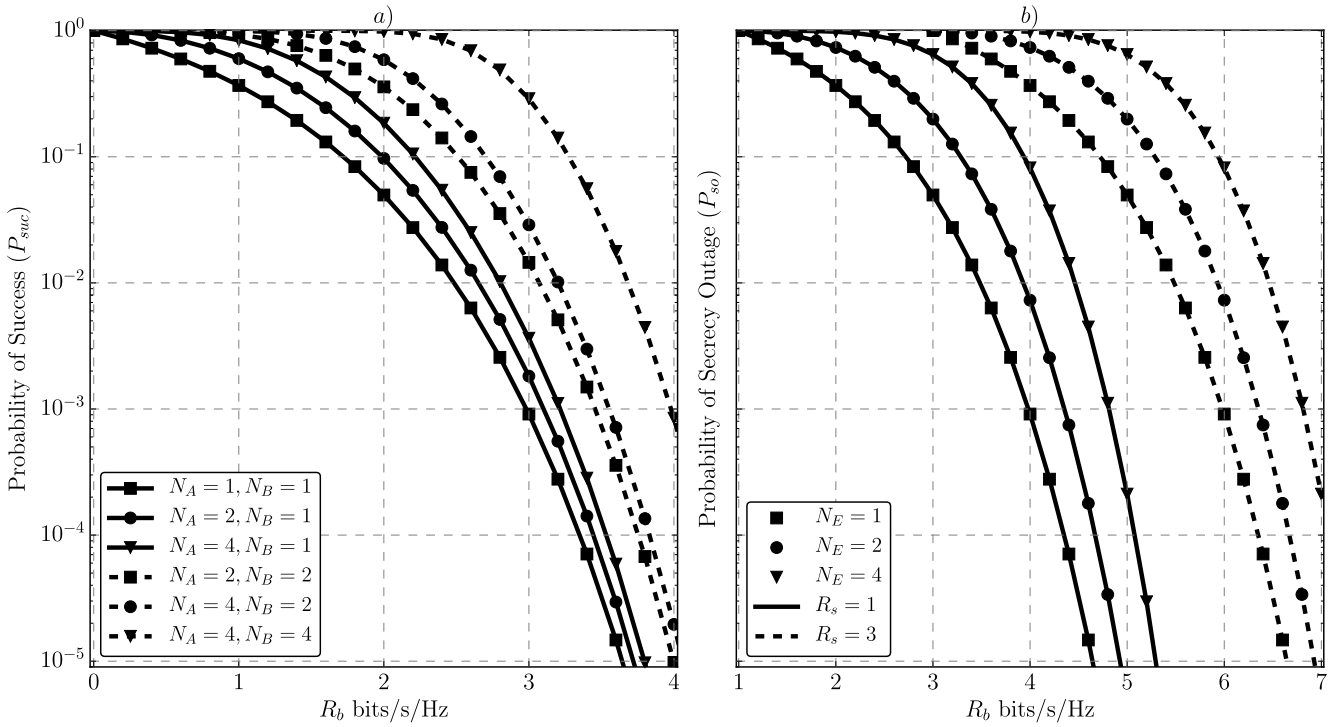


FIGURE 2. Example of the success and secrecy outage probabilities vs. the transmission rate R_b: *a*) distinct antenna arrangements at the legitimate link with $\overline{\gamma}_B = 10$ dB; *b*) secrecy outage for different number of antennas and for two secure rates $R_s \in \{1, 3\}$ bits/s/Hz with $\overline{\gamma}_E = 0$ dB

Proposition 1: Assuming optimal $\mu = 2^{R_b} - 1$*, the transmission rate* R_b *that ensures* $p_{suc}(\mu) \geqslant \sigma$ *is*

$$R_b \leqslant \log_2\left(1 + \overline{\gamma}_B\, \alpha\, \log\left(\left(1 - (1-\sigma)^{\frac{1}{N_A N_B}}\right)^{-1}\right)\right), \tag{9}$$

where $\alpha = \Gamma(N_B + 1)^{\frac{1}{N_B}}$.

Proof: Please see Appendix A. ∎

Corollary 1: Assuming $N_A \in \mathbb{Z}^*$ *and* $N_B = 1$*, which is the case when only TAS is employed at the legitimate channel, then* $R_b \leqslant \log_2\left(1 + \overline{\gamma}_B\, \log\left(\left(1 - (1-\sigma)^{\frac{1}{N_A}}\right)^{-1}\right)\right)$. *While for* $N_A = N_B = 1$ *(single antenna case),* (9) *reduces to* $R_b \leqslant \log_2\left(1 + \overline{\gamma}_B\, \log\left(\sigma^{-1}\right)\right)$ *as in [24].*

Next, we tackle the restriction on the information leakage $p_{so}(R_b, R_s) \leqslant \epsilon$.

Proposition 2: For any $R_b > R_s$ *the secrecy outage is monotonically decreasing with* R_b*, while monotonically increasing with respect to* R_s*. Thus, satisfying* $p_{so}(R_b, R_s) \leqslant \epsilon$*, the throughput maximizing* R_s *is*

$$R_s = R_b - \log_2\left(1 + \overline{\gamma}_E\, \mathrm{P}^{-1}\left(N_E, 1-\epsilon\right)\right), \tag{10}$$

where $\mathrm{P}^{-1}(a, x)$ *is the inverse of the generalized regularized incomplete gamma function [29].*[1]

[1]It is noteworthy that $\mathrm{P}^{-1}(a, x)$ is an analytic function of a and x and can be easily evaluated through standard mathematical frameworks such as Mathematica [29] as well as SciPy [30].

Proof: Since for any $R_b > R_s$ the secrecy outage is a decreasing function of R_b, the maximizing throughput R_s occurs when $p_{so}(R_b, R_s) = \epsilon$. In the equality $\mathrm{P}(a, z) = x$ is invertible [29], which allow us to isolate $z = 2^{R_b - R_s} - 1$ and then attain R_s as in (10). ∎

We are about to state the simplified version of our maximization problem given Propositions 1 and 2 discussed above. But first, let us introduce an important result that allows us to assess the trade-off between reliability and security.

Proposition 3: Given a positive secrecy rate $R_s > 0$*, we establish the trade-off between reliability and security as*

$$\sigma < 1 - \left(1 - \exp\left(-\frac{\mathrm{P}^{-1}\left(N_E, 1-\epsilon\right)}{\rho\, \alpha}\right)\right)^{N_A N_B}, \tag{11}$$

where $\rho \triangleq \overline{\gamma}_B / \overline{\gamma}_E$ *defines the relative gain between the average SNR of the legitimate* ($\overline{\gamma}_B$) *and eavesdropper* ($\overline{\gamma}_E$) *channels.*

Proof: Please see Appendix B. ∎

Corollary 2: Assuming $N_A \in \mathbb{Z}^*$ *and* $N_B = 1$*, then* $\sigma < 1 - \left(1 - \exp\left(-\mathrm{P}^{-1}\left(N_E, 1-\epsilon\right)/\rho\right)\right)^{N_A}$*, whilst for the single antenna case,* (9) *reduces to* $\sigma < \epsilon^{1/\rho}$*, which was also attained in [24].*

Fig. 3 illustrates the trade-off between reliability and security stated in Proposition 3. We evaluate σ, which can be seen as a QoS/reliability indicator, as a function of ϵ, which denotes how much secrecy outage the system tolerates, as well as ρ, which captures how good is

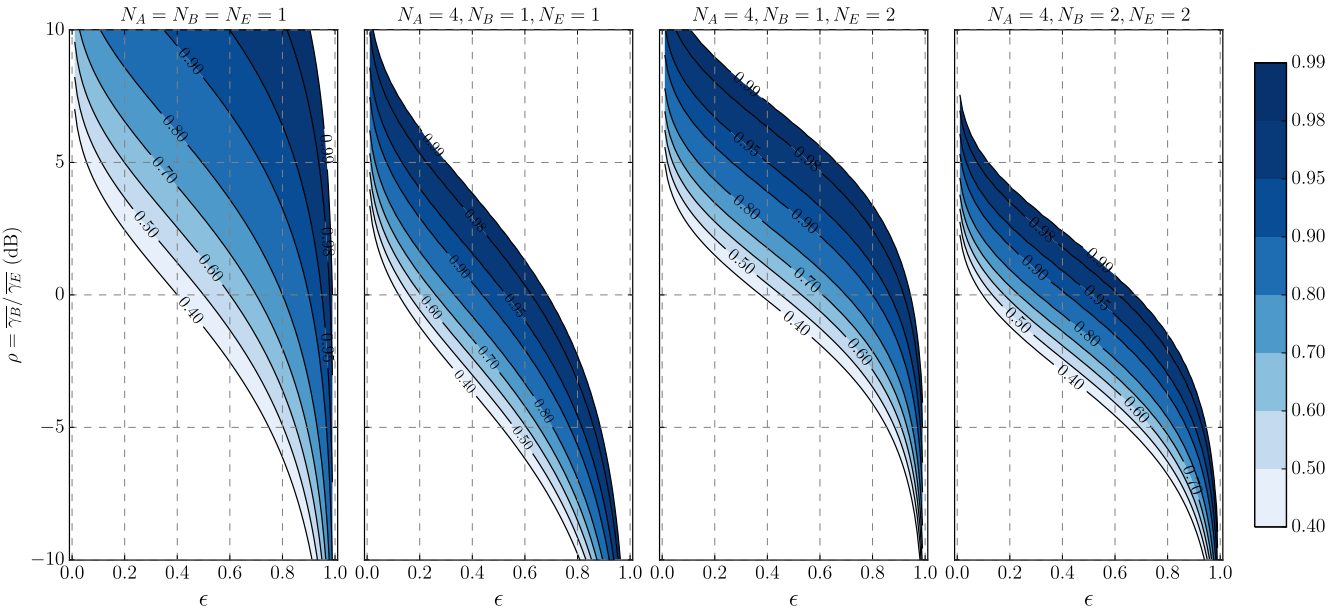


FIGURE 3. Illustrative example of the trade-off between reliability and security for distinct sets of antennas, from the single (left) to multiple (right) antennas. Contour plots indicate the value of $.4 \leqslant \sigma \leqslant 0.99$ as a function of the relative gain between the average SNR of the legitimate and eavesdropper channels, namely $\rho = \frac{\overline{\gamma}_B}{\overline{\gamma}_E}$, and ϵ.

the main channel with respect to the eavesdropper's channel. Fig. 3 has four settings: from single to multi antenna configuration.

For instance, if Alice employs only TAS ($N_A = 4$), Bob and Eve are single antenna, there is a great gain in reliability with respect to the single antenna case, in fact, reliability grows from 60% to about 97.5% for $\epsilon = .2$ and $\rho = 5$ dB. However, as N_E increases the feasibility region diminishes. For instance, if Eve has one more antenna, thus $N_E = 2$, σ drops from 97.5% to about 86%. This effect can be counteracted by adding more antennas to the legitimate link, thus enhancing reliability through diversity. This case is exemplified on the rightmost plot of Fig. 3, where Bob now has $N_B = 2$ antennas, which renders more than 99% of reliability for $\epsilon > 0.1$ and $\rho > 5$ dB.

In this discussion we set $\epsilon = 0.2$, which is somewhat a high value for secrecy constraints. As we shall discuss in the next section, such high secrecy outage constraint may be feasible (acceptable) depending on the application. Of course, the less information lost the better, especially if the information is critical. We recall that herein we are only evaluating security at PHY layer as a way to complement some cryptographic method implemented in the higher layers of the protocol stack. Nonetheless, our results also show ways to increase security at PHY layer, thus smaller values of ϵ, by increasing the number of antennas as well as guaranteeing high SNR at the main link (larger ρ).

Finally, one more way to increase performance of the legitimate link is to maximize the secure throughput, which is hereby our goal and we are now ready to state the simplified version of our maximization problem given Propositions 1 to 3. Therefore, the secure throughput maximization problem is rewritten as,

$$\begin{aligned} &\underset{R_b}{\text{argmax}}\ T_s = (R_b - R_e)\left(1 - \mathrm{P}\left(N_B, \frac{2^{R_b}-1}{\overline{\gamma}_B}\right)^{N_A}\right) \\ &\text{subject to } R_e < R_b \end{aligned} \tag{12}$$

where R_b is given in (9) from Proposition 1, and $R_e = \log_2\left(1 + \overline{\gamma}_E\, \mathrm{P}^{-1}\left(N_E, 1-\epsilon\right)\right)$ comes from Proposition 2.

Proposition 4: The optimal secure throughput of our proposed scheme is given as

$$T_s^* = \left(R_b^* - R_e\right)\left(1 - \mathrm{P}\left(N_B, \frac{2^{R_b^*}-1}{\overline{\gamma}_B}\right)^{N_A}\right), \tag{13}$$

where the optimal transmission rate R_b^* is the solution for the following transcendental equation

$$1 - \mathrm{P}\left(N_B, y\right)^{N_A} = \beta y^{N_B - 1} e^{-y}\, \mathrm{P}\left(N_B, y\right)^{N_A - 1}, \tag{14}$$

where $y = \frac{2^{R_b}-1}{\overline{\gamma}_B}$ given the domain $R_e < R_b$ and respecting the condition (11)*, where $\beta = \frac{\log(2) N_A (R_b - R_e) 2^{R_b}}{\Gamma(N_B)\overline{\gamma}_B}$.*

Proof: Please refer to Appendix C. ■

We illustrate Proposition 4 with the following numerical example depicted in Fig. 4 where the optimal rate allocation R_b^* is depicted as a function of ϵ. Fig. 4 also compares the proposed scheme as in (14) to the numerical optimization of (12). Notice that the proposed scheme and numerical solution match well and are well within the R_b rate region. As we can see from the figure, allocating R_b^{max} is not optimal,

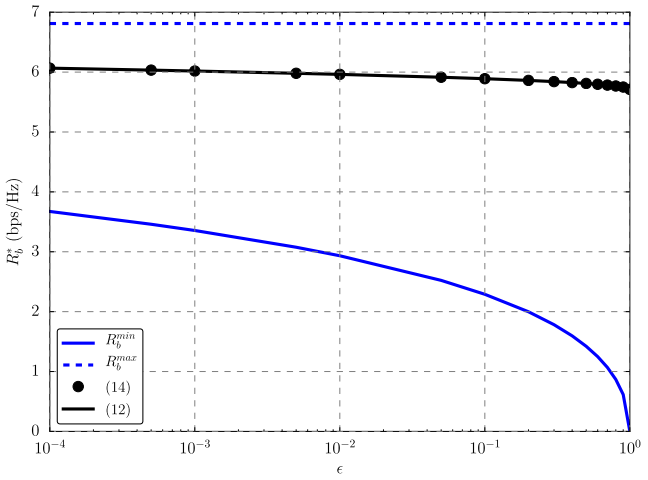


FIGURE 4. Optimal R_b as a function of ϵ, for $\sigma = 0.5$, $N_a = 4$, $N_b = 2$, $N_a = 2$, and $\rho = 10$ dB.

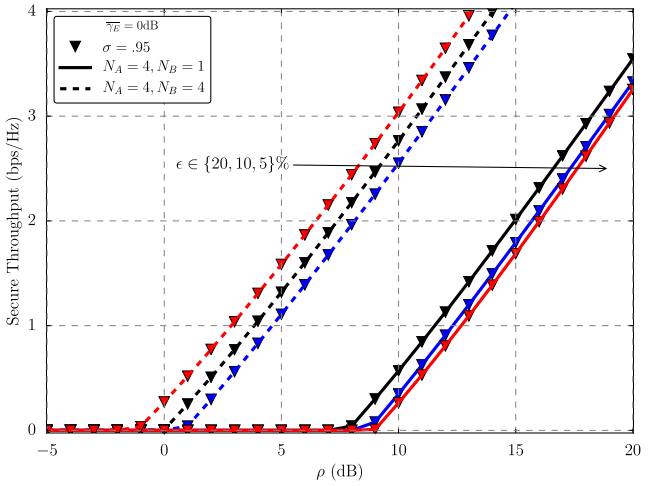


FIGURE 5. Secure throughput as a function of the SNR of the legitimate link $\overline{\gamma}_B$, assuming $\overline{\gamma}_E = 0$ dB, $\sigma = 95\%$ and distinct antenna configurations and secrecy outage thresholds.

even though there is an increase in the effective secrecy rate, there is a considerable decrease in success probability, for instance, setting $R_b^* = R_b^{max} = 6.81$ bps/Hz (considering $\sigma = 0.5$, $\epsilon = 0.1$) renders a throughput of approximately $\eta \approx 1.26$ bps/Hz, while $R_b^* \approx 5.89$ renders $\eta \approx 1.85$ bps/Hz. Another example is given in Fig. 5, where secure throughput is evaluated as a function of the SNR of the legitimate link $\overline{\gamma}_B$, assuming $\overline{\gamma}_E = 0$ dB (thus $\rho = \overline{\gamma}_B$), $\sigma = 95\%$ for $N_A = 4$, $N_B \in \{1, 4\}$ and $N_E = 2$. As expected, by relaxing the constraint on the secrecy outage ϵ, larger throughput can achieved. Similar effect can be also observed if we relax the QoS constraint (σ). An significant improvement can be observed as the number of antennas at the legitimate channel grows.

Fig. 6 further shows the secure throughput as a function of the legitimate link QoS (σ) on the left, and as a function of the secrecy outage threshold (ϵ) on the right. We assume $\rho = 10$ dB and distinct antenna configurations. Again, the higher the number of antennas at the legitimate link, greater throughput is achieved, for instance by increasing by one the number of antennas at Bob the throughput more than doubles ($\times 2.33$) for $\epsilon = .10$ and $\sigma = .90$.

Such throughput enhancement can be also observed by relaxing the constraint on the secrecy outage. Interestingly, some performance floors are achieved with respect to our constraints. Notice that for $N_A = 4, N_B = 4, N_E = 2$ throughput saturates for different σ, which allows us to relax the QoS constraint, from 98% to 90% for example, and yet achieve the same throughput, as we can observe from Fig. 6. This conclusion is a consequence of Proposition 3, which establish the trade-off between reliability and security, thus in this case by relaxing the QoS constraint, we can tighten security (reducing ϵ).

All in all, our results show the trade-off between security and reliability, and thus depending on the application more relaxed secrecy constraints can ensure great reliability. Likewise, we are also able to trade reliability for secrecy, which in this case goes against current standards for smart grids that requires at least 98% reliability in the communication link [1]. Nonetheless, [1] do not account for security and herein we show that such constraint can be achieved and even higher security can be guaranteed if the reliability constraint is relaxed.

In the following section, we illustrate our framework with a practical smart grid example. As we will see later, the information to be transmitted is average power demand of a household where the aggregator and the eavesdropper need to reconstruct the load profile curve.

IV. SECURE RECONSTRUCTION OF THE AVERAGE POWER DEMAND CURVE

In the previous section, we commented that if we allow a larger secrecy outage, higher throughput in the legitimate link can be attained. Consequently, larger secrecy outage means that the Eve will decode more information and become more knowledgeable about our system. As pointed out in [31], joint sampling-communication strategies are needed to improve the reconstruction of the average power demand curve with low deviation, but such models often neglect security aspects and possible eavesdropping. Such issue is tackled herein and we demonstrate that Eve will not be able to acquire enough information in order to reconstruct the average power demand curve completely as we shall see next.

Let us first exemplify how Alice transmits its average power demand to Bob, relying on a time-based sampling-communication scheme as in [31]. Then, let $x[n]$ denote the average power demand, where $n = 1, \ldots, N$ is the index and N total number of samples. Transmissions are schedule in fixed period of time τ, herein we assume 15-minute based sampling and a transmission and thus $\tau = 0.25$ hour, which renders $N = 96$ samples per day. If an outage occurs, Bob reconstructs the signal via linear interpolation between two adjacent points. Thus, Bob will interpolate the missing value(s) using the latest two received samples. Similarly, we assume that Eve also attempts to estimate and

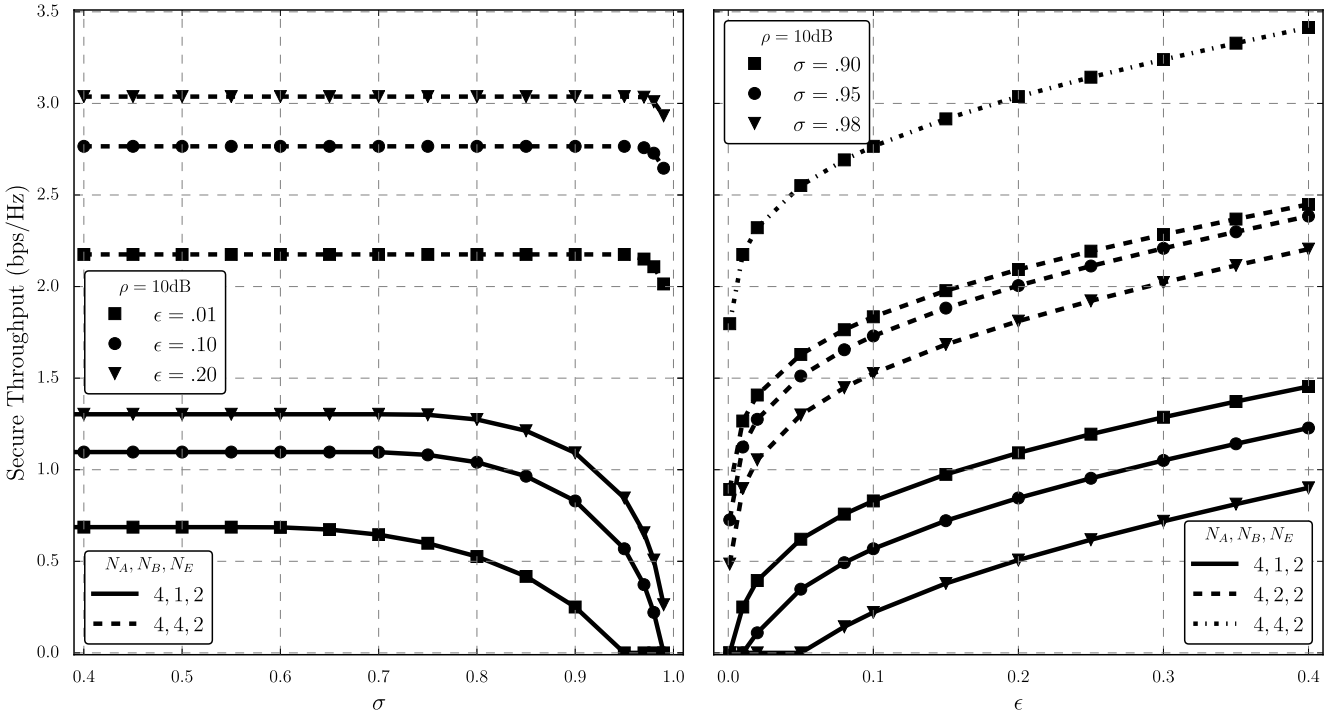


FIGURE 6. Secure throughput as a function of the σ on the left and ϵ on the right, for fixed $\overline{\gamma}_B = 10$ dB, assuming $\overline{\gamma}_E = 0$ dB, and distinct antenna configurations.

reconstruct the signal via linear interpolation. For example, consider the transmitted sequence: $x[k-2], x[k-1], x[k]$ with $k = 2, \ldots, N$, and let $y[k]$ denote the received signal, $k = 1, \ldots, N$. Then, if the samples $x[k-2]$ and $x[k]$ are successfully received but $x[k-1]$ is not, the reconstruction is based on the linear interpolation and the estimated point is denoted by $y[k-1] = (y[k] + y[k-2])/2$.

In order to perform our analysis we resort to "The Reference Energy Disaggregation Data Set" (REDD) database [32], [33] to build the signal $x[n]$, which is a 15-minute average power demand over a timespan of 24 hours.[2] We assume that both Bob and Eve use linear interpolation to reconstruct the power demand curve. In order to estimate the error due to the signal reconstruction we adopt the root mean square deviation (RMSD), which is calculated based on the received (and estimated when needed) samples and the actual data, and is given as

$$\text{RMSD} = \sqrt{\frac{1}{N}\sum_{k=1}^{N}(y[k] - x[k])^2}. \tag{15}$$

In order to facilitate the comparison among household power demand profiles, we choose to normalize the RMSD (NRMSD) by the average of the transmitted signal power, thus NRMSD $=$ RMSD$/\bar{y}$, which is commonly known as the coefficient of variation of the RMSD.

Further, from the database selected 3 households that provide a significant representation of the dataset, namely House 1, House 2 and House 3, since each of these households presents a distinct average power demand profile. Fig. 7 exemplifies the average power demand of these three distinct houses over 24 hours with transmissions every 15 minutes. For instance, House 1 presents a low power demand profile, which means that few appliances are on (e.g. fridge, lights). House 2 has higher average compared to House 1 and presents peak demand, which is also observed in House 3. For instance, from the data of House 2 we can infer that there is more activity in the house in early morning (e.g. showering, preparing breakfast) and at the end of the day, around the time where people are having dinner, doing the house chores, and watching TV. House 3 has similar patterns, but shifted in time and concentrated during the afternoon. Fig. 7 also assumes that an eavesdropper is able to decode 10% (red square) or 20% (blue circle) of the packages, due to the secrecy outages occurred in this period. Note that if Eve can obtain 20% of the packets, she is still not able to reconstruct the power demand curve and then infer the presence and activities within a given house. On the other hand, with $\sigma \geqslant 90\%$ few points are lost such that the aggregator can estimate them through linear interpolation without larger estimations errors. It is noteworthy that a malicious eavesdropper may acquire this information and perform a series of cyber (and even physical)

[2]The REDD database is composed of 6 households, monitored during several days with a frequency of 1Hz. After processing the data (namely, the sum of the power of phases A and B), we identified 53 slices of 24-hour periods (all aligned in time among themselves) which provide us a full set of average power measures. In other words, each of these slices can be seen as a single household and then these measures are used to simulate the daily transmissions

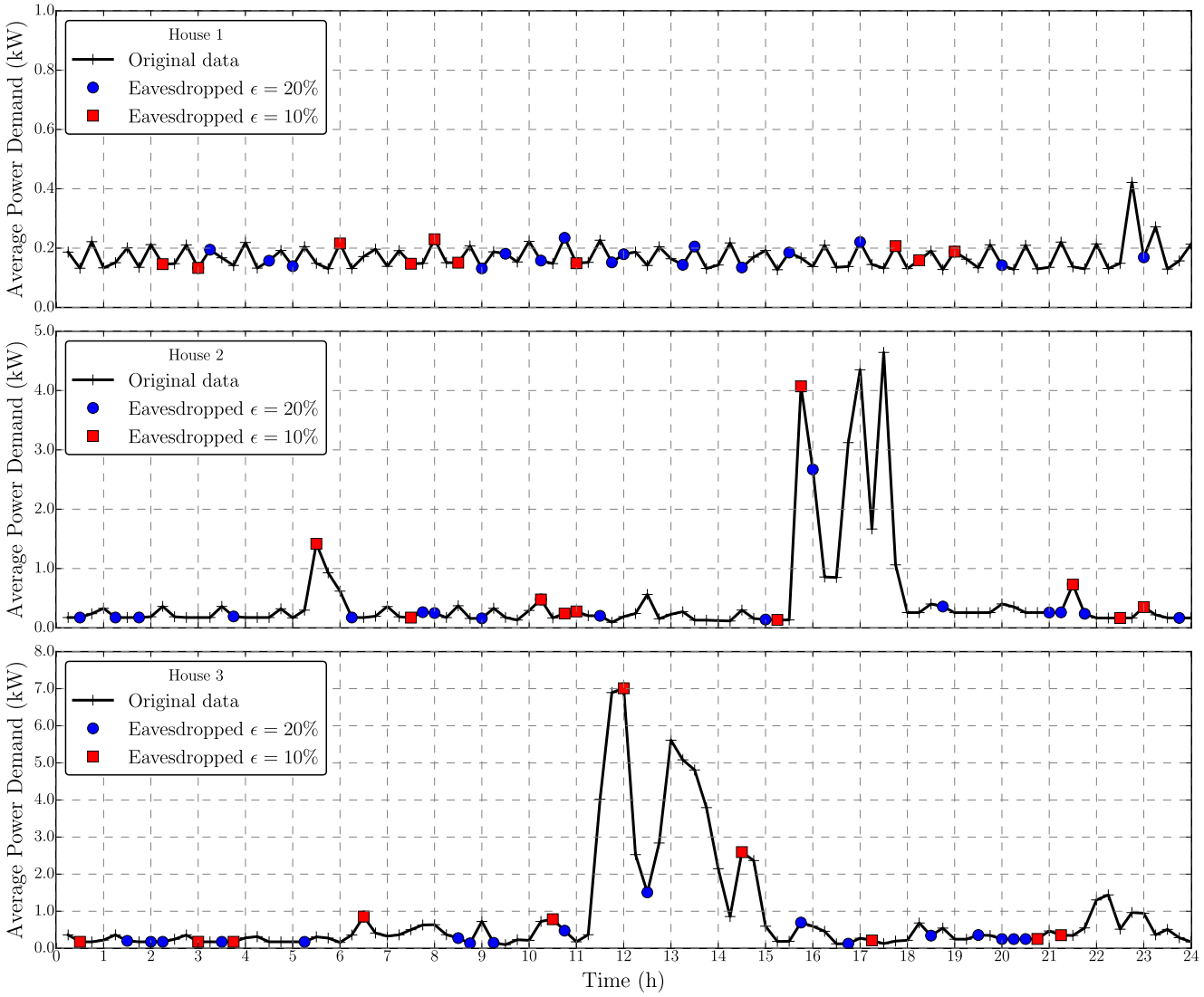


FIGURE 7. Examples of average power demand curves for three distinct houses from REDD database over 24 hours with transmissions every 15 minutes. House 1 presents a low power demand (few appliances (e.g. fridge) are on), House 2 has higher average and presents peak demand, which is also observed in House 3. The cases where the eavesdropper acquires 10% and 20% of the packages if also depicted.

attacks on a neighborhood by exploiting the smart meters transmissions. Given enough intercepted points, it is possible to infer personal information and inhabitants behavior and activities (for instance, presence and absence hours, sleeping hours) from the power demand curve [2]. Thus the necessity of protecting the transmission against eavesdropping and any other type information leakage.

Fig. 8 depicts the normalized RMSD as a function of the outages, which represents the outage either at the legitimate link or information leakage to Eve. In terms of reliability, the region of interest lies on the left-hand side of the plot and it is delimited by the σ threshold (blue line). We assume Monte Carlo simulations with 10^5 repetitions for each house (each house has $N = 96$ samples). After the linear interpolation used to estimate the missing points, we calculate the RMSD and then normalize by the average power. As we can observe from the figure, if during a day the legitimate link perceives outages of up to $\sigma = 10\%$, the demand power curve can be reconstructed with low error. For instance, for $\sigma = 10\%$, the normalized RMSD for each house is respectively 0.12, 0.18 and 0.35, and these values can be seen as coefficient of variation indicating that there is a low variance in the reconstruction of the power demand curve. Eve, on the other hand, has a greater outage, which increases the error in the signal reconstruction leading to high coefficient of variation. For example, secrecy outages of at most $\epsilon \leqslant 20\%$ (which means that, on average, Eve intercepts up to 20% of the transmissions) correspond to outages greater than 80% and therefore a higher coefficient of variation of the RMSD as indicated by red line ($1 - \epsilon$ threshold) on the rightmost

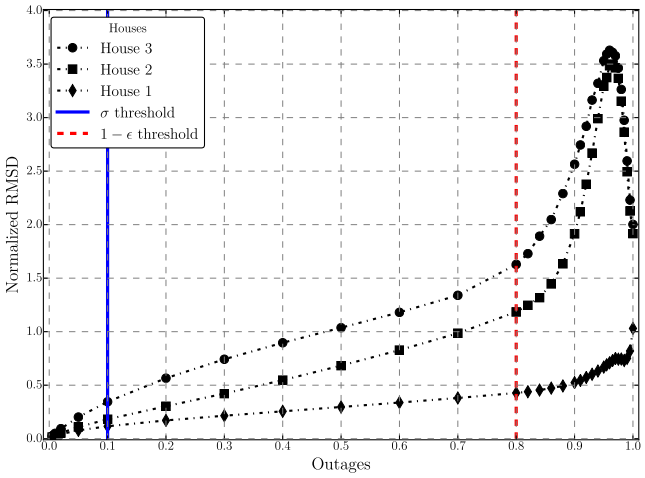


FIGURE 8. Normalized RMSD as a function of the outage, which encompass reliability and secrecy outages. Note that σ (blue line on the left) and $1-\epsilon$ (dashed red line on the right) thresholds delimit the regions that guarantee secrecy and reliability.

side of Fig. 8. Notice that Eve acquires few points, and thus her estimation and reconstruction is very poor, as a result of Alices strategy when setting the secrecy outage threshold and optimizing the secure throughput. It is worth mentioning that the reduction on the normalized RMSD on the extreme right (more than 97% of outages) occurs because the number of points available at Eve is small. In this cases the RMSD is calculated with respect to zero or to a line that lies close to average of the actual signal, which decreases the RMSD. To illustrate this point assume that Eve only attained a point around hours 3 and 21 from House 3, as depicted in Fig. 7. Based only on that, Eve estimates that all points lie within this line, and as we can see from Fig. 7 the majority of the points is closer to the marginal power demand rather than to the peak consumption hours.

V. DISCUSSIONS

We proposed a physical layer security scheme that enhances the communication link between a pair of legitimate nodes in the presence of an eavesdropper. In our scenario, an eavesdropper may attempt to acquire information from the smart meters from a given neighborhood. However, the transmitter does not have any CSI from the Eve, but is still able to optimize its transmission rate such that secure throughput can be achieved. Notice that the results attained herein are not limited to smart grid applications, thus we provide an general framework that can be extended to other contexts. In the previous sections we have discussed how we can improve the secure throughput, reliability and security of the system and we connect our analytical results with actual data and signal reconstruction. Herein, we discuss some pros and cons of this proposed method and future work.

A. RELIABILITY AND SECRECY OUTAGE CONSTRAINTS

We set the reliability constraint (σ) to ensure a minimum robustness for the legitimate link. Likewise, the secrecy outage constraint (ϵ) envisages a maximum information leakage to the eavesdropper. Then, we present the trade-off between security and reliability, in which we can choose to sacrifice robustness of the legitimate link for security, or relax the secrecy constraint in order to achieve higher reliability. Current standards foresee a reliability greater than 98% for the communication link in the smart grid (smart meter–aggregator) [1]. As discussed above, such constraint is stringent especially if we want add security at physical layer while enhancing the performance of the system.

Then, *how big would be the sacrifice of robustness of the legitimate link for security?* A more appropriate answer can be given only if we know the information that is sent to the aggregator, so that different information flows have distinct priorities and allocation. In our case, we assume that the information sent is the average power demand, then we show that the signal reconstruction is possible even with relatively loose outage constraints (e.g. $\sigma \geqslant 90\%$), while Eve cannot attain much information at secrecy outages of $\epsilon \leqslant 10\%$. Notice that this result is dependent on the inherent characteristic of the transmitted signal, for instance, as we can observe from Fig. 7 the average power demand presents overall low variation around the average (see House 1), except for relatively short periods of peak consumption as in House 2 and House 3. Therefore, design the whole system for higher outage probabilities in the legitimate link as well as high secrecy outages may not be prudent for other kind of signals or if the aggregator should provide some kind of feedback to the smart meter (e.g. change the power demand behavior, as in strategies of demand-side management [3], [28]). Thus, the necessity of classifying the information flows from smart meters to aggregator with respect to signal characteristics, as well as reliability and security.

B. ENHANCING ROBUSTNESS OF THE LEGITIMATE LINK

Herein, we assume that transmissions are scheduled every 15 minutes, and if a package does not meet our outage constraint, it is considered lost and then Bob will estimate the power demand via interpolation. Alternatively, as future work, another scenario may include Hybrid Automatic Repeat Request (HARQ) strategies in order to enhance the communication link, which reduces outage events while enhancing throughput as show in [34] and [35]. Cooperation may also be an extension to enhance secure throughput and reliability [15], [16]. Thus, these more advanced communication techniques combined may be used to enhance secure throughput and would be an interesting next step for the present work.

C. SIGNAL PROCESSING AND TRANSMISSION

Fig. 7 exemplifies a 15 minute sampling interval of the power demand of a household. Due to the characteristics of this signal, a time-based sampling might not be the most effective way to collect and sent data to the aggregator. Then,

as pointed out in [36] event based sampling may be more suitable, once it reduces the amount of redundant information transmitted. However, such approach requires a more robust communication link, due to the lack of redundant data, and therefore the loss of any sample will have a more dramatic effect on the signal reconstruction. At the same time, this scheme is more secure once Eve acquires even less information. As pointed out in [37] transmission strategies and outage constraints should be evaluated in combination with the sampling procedure, due to the amount of redundant information generated in each case.

It is worth noting that even though we analyze the situation for a 24-hour period and a simple interpolation technique. Due to the daily habits of the dwellers, it would be possible to recover the usage profile (or activities) by superimposing the missing data from one day with data from similar days. However, this would require more sophisticated signal processing at Eve as well as large time window that could range from days to months depending on the settings of the network. Such process is also hampered by slight variations in the habits and activities of the inhabitants if we consider a sufficiently high outage for Eve. Recently, [31] compares usual time-based, periodic, sampling against a event-based strategy, and the authors show that latter strategy provides an accurate way to represent the power demand data, which leads to a lower number of samples (in average) to reconstruct average power demand curve. Thus, such strategy reduces the amount of data to transmit and to store as well as the number of transmissions, which may enhance security as well.

VI. CONCLUSIONS AND FINAL REMARKS

Herein we assess the secure communication link between smart-meters and an aggregator in the presence of a potential eavesdropper (Eve). We assume MIMOME wiretap channel, where Alice employs transmit antenna selection and has no channel state information of Bob and Eve. Therefore, we resort to fixed Wyner codes and then optimize Alice's transmission rate so that secure throughput can be guaranteed subject to quality of service and secrecy outage constraints. We assess in closed-form both secrecy outage and successful transmission probabilities, and then maximize the secure throughput and establish the secrecy-reliability trade-off. Our numerical results illustrate the effect of this trade-off on the secure throughput as well as number of antennas at Alice, Bob and Eve. Our results show that a small sacrifice in reliability allows secrecy enhancement. Even though Eve may acquire some information, we show that it will not be enough to reconstruct the average power demand curve of a household.

We plan to study in future works how the secure throughput will be affected under different sampling strategies, extending the initial results introduced in [31]. In this way, we plan to build a joint sampling-transmission technique that can improve the system efficiency, as discussed in Section V.

APPENDIX A
PROOF OF PROPOSITION 1

Let us first recall Lemma 1 which renders us $p_{suc}(\mu)$, which constrained on σ can be written as follows

$$1 - \mathrm{P}\left(N_B, \frac{\mu}{\overline{\gamma}_B}\right)^{N_A} \geqslant \sigma \tag{16}$$

$$\mathrm{P}\left(N_B, \frac{\mu}{\overline{\gamma}_B}\right) \overset{(a)}{\leqslant} (1-\sigma)^{\frac{1}{N_A}} \tag{17}$$

$$\left(1 - \exp\left(-\frac{\mu}{\overline{\gamma}_B\,\alpha}\right)\right)^{N_B} \overset{(b)}{\leqslant} (1-\sigma)^{\frac{1}{N_A}} \tag{18}$$

$$\mu \overset{(c)}{\leqslant} \overline{\gamma}_B\,\alpha\,\log\left(\xi^{-1}\right), \tag{19}$$

(a) since $0 \leqslant \sigma \leqslant 1$ we isolate the regularized gamma function, which is invertible only for the equality, thus $\mu = \overline{\gamma}_B\,\mathrm{P}^{-1}\left(N_B, (1-\sigma)^{\frac{1}{N_A}}\right)$, where $\mathrm{P}^{-1}(a,x)$ is the inverse of the generalized regularized incomplete gamma function defined in [29] and [30]; otherwise,

(b) since $N_B > 0$ $\frac{\mu}{\overline{\gamma}_B} > 0$, we rewrite ($a$) by resorting to the following inequality $(1-\exp(-\alpha_a x))^a \leqslant \mathrm{P}(a,x)$, where $\alpha_a = \Gamma(1+a)^{1/a}$ (equality holds for $a=1$) [38, Ch. 8, Sec. 8.10.11],

(c) last, since all variables are positive we isolate the variable μ, where $\xi = \left(1-(1-\sigma)^{\frac{1}{N_A N_B}}\right)$

Finally, we know that $\mu = 2^{R_b} - 1$, thus we readily attain (9).

APPENDIX B
PROOF PROPOSITION 3

Notice that in order to achieve a positive secrecy rate $R_s > 0$, we have to guarantee that $R_b > \log_2\left(1+\overline{\gamma}_E\,\mathrm{P}^{-1}\left(N_E, 1-\epsilon\right)\right)$. From (9) we attain R_b, and then we isolate σ as follows

$$-\overline{\gamma}_B\alpha\,\log\left(1-(1-\sigma)^{\frac{1}{N_A N_B}}\right) > \overline{\gamma}_E\,\mathrm{P}^{-1}\left(N_E, 1-\epsilon\right) \tag{20}$$

$$\log\left(1-(1-\sigma)^{\frac{1}{N_A N_B}}\right) \overset{(a)}{<} \frac{\mathrm{P}^{-1}\left(N_E, 1-\epsilon\right)}{\rho\,\alpha}, \tag{21}$$

(a) since $0 \leqslant \epsilon \leqslant 1$, $N_A > 0$, $N_B > 0$, we isolate the function of σ in the right-side and then define ρ; then

since all variables are positive and grater than zero, we perform some algebraic manipulations and isolate σ as in (11).

APPENDIX C
PROOF OF PROPOSITION 4

The function T_s is continuous and concave in the domain $R_e < R_b$ (with $N_A, N_B \in \mathbb{Z}^*$ and $\overline{\gamma}_B > 0$), where R_b is given in (9), since its second derivative with respect to R_b is negative, thus $\partial^2 T_s/\partial R_b^2 < 0$, therefore R_b^* is attained by solving the first derivative of T_s with respect to R_b and equating to zero, $\partial T_s/\partial R_b = 0$, which after some algebraic manipulations yields (14).

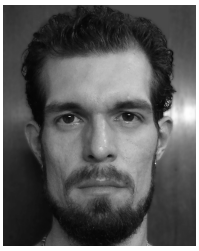
Unfortunately, (14) does not have a closed-form expression, though it is noteworthy that (14) can be easily evaluated

numerically using mathematical frameworks such as Mathematica and SciPy [39]. For the single antenna case an closed-from expression for R_b^* can be attained as in [24].

REFERENCES

[1] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, "Communication network requirements for major smart grid applications in HAN, NAN and WAN," *Comput. Netw.*, vol. 67, pp. 74–88, Jul. 2014.
[2] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart Grid—The new and improved power grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, 4th Quart., 2012.
[3] L. Gkatzikis, I. Koutsopoulos, and T. Salonidis, "The role of aggregators in smart grid demand response markets," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1247–1257, Jul. 2013.
[4] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Netw.*, vol. 57, no. 5, pp. 1344–1371, 2013.
[5] E.-K. Lee, M. Gerla, and S. Y. Oh, "Physical layer security in wireless smart grid," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 46–52, Aug. 2012.
[6] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.
[7] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.
[8] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[9] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[10] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
[11] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.
[12] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[13] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
[14] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359–368, Feb. 2012.
[15] H. Alves, G. Brante, R. D. Souza, D. B. D. Costa, and M. Latva-aho, "On the performance of secure full-duplex relaying under composite fading channels," *IEEE Signal Process. Lett.*, vol. 22, no. 7, pp. 867–870, Jul. 2015.
[16] G. Brante, H. Alves, R. D. Souza, and M. Latva-aho, "Secrecy analysis of transmit antenna selection cooperative schemes with no channel state information at the transmitter," *IEEE Trans. Commun.*, vol. 63, no. 4, pp. 1330–1342, Apr. 2015.
[17] H. Alves, R. D. Souza, and M. Debbah, "Enhanced physical layer security through transmit antenna selection," in *Proc. IEEE GLOBECOM Workshops (GC Wkshps)*, Dec. 2011, pp. 879–883.
[18] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.
[19] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-*m* fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054–6067, Nov. 2014.
[20] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2170–2181, Apr. 2016.
[21] 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, Apr. 2015.
[22] X. Tang, R. Liu, and P. Spasojevic, "On the achievable secrecy throughput of block fading channels with no channel state information at transmitter," in *Proc. 41st Annu. Conf. Inf. Sci. Syst.*, Mar. 2007, pp. 917–922.
[23] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.
[24] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.
[25] B. He, X. Zhou, and A. L. Swindlehurst, "On secrecy metrics for physical layer security over quasi-static fading channels," *IEEE Trans. Wireless Commun.*, vol. PP, no. 99, pp. 1–1, doi: 10.1109/TWC.2016.2593445.
[26] P. H. J. Nardelli *et al.*, "Models for the modern power grid," *Eur. Phys. J. Special Topics*, vol. 223, no. 12, pp. 2423–2437, 2014.
[27] M. Abramowitz and I. A. Stegun, Eds., *Handbook of Mathematical Functions: With Formulas, Graphs, and Mathematical Tables*, 9th ed. New York, NY, USA: Dover, 1965.
[28] G. Strbac, "Demand side management: Benefits and challenges," *Energy Policy*, vol. 36, pp. 4419–4426, Dec. 2008.
[29] Wolfram Research. *Inverse of the Generalized Regularized Incomplete Gamma Function*, accessed on Oct. 30, 2015. [Online]. Available: http://functions.wolfram.com/GammaBetaErf/InverseGammaRegularized3/
[30] SciPy.Org. *Inverse of the Generalized Regularized Incomplete Gamma Function*, accessed on Oct. 30, 2015. [Online]. Available: http://docs.scipy.org/doc/scipy-0.14.0/reference/generated/scipy.special.gammainccinv.html#scipy.special.gammainccinv
[31] M. C. Tomé, P. H. J. Nardelli, H. Alves, and M. Latva-aho, "Joint sampling-communication strategies for smart-meters to aggregator link as secondary users," in *Proc. IEEE ENERGYCON*, Apr. 2016, pp. 1–6.
[32] J. Z. Kolter and M. J. Johnson, "REDD: A public data set for energy disaggregation research," in *Proc. Workshop Data Mining Appl. Sustainability (SIGKDD)*, San Diego, CA, USA, vol. 25. 2011, pp. 59–62.
[33] *REDD: The Reference Energy Disaggregation Data Set*, accessed on Aug. 29, 2016. [Online]. Available: http://redd.csail.mit.edu/
[34] P. H. J. Nardelli, M. Kaynia, P. Cardieri, and M. Latva-aho, "Optimal transmission capacity of ad hoc networks with packet retransmissions," *IEEE Trans. Wireless Commun.*, vol. 11, no. 8, pp. 2760–2766, Aug. 2012.
[35] H. Alves, R. D. Souza, G. Fraidenraich, and M. E. Pellenz, "Throughput performance of parallel and repetition coding in incremental decode-and-forward relaying," *Wireless Netw.*, vol. 18, no. 8, pp. 881–892, 2012.
[36] M. Simonov, H. Li, and G. Chicco, "Gathering process data in low-voltage systems by enhanced event-driven metering," *IEEE Syst. J.*, vol. PP, no. 99, pp. 1–12, doi: 10.1109/JSYST.2015.2390073
[37] P. H. J. Nardelli, M. de Castro Tomé, H. Alves, C. H. M. de Lima, and M. Latva-aho, "Maximizing the link throughput between smart meters and aggregators as secondary users under power and outage constraints," *Ad-Hoc Netw.*, vol. 41, pp. 51–68, 2016.
[38] F. W. J. Olver, D. W. Lozier, R. F. Boisvert, and C. W. Clark, *NIST Handbook of Mathematical Functions*, 1st ed. Cambridge, U.K.: Cambridge Univ. Press, 2010.
[39] Sympy.org. *Solvers Module in SymPy*, accessed on Oct. 30, 2015. [Online]. Available: http://docs.sympy.org/dev/modules/solvers/solvers.html

HIRLEY ALVES received the B.Sc., M.Sc., and D.Sc. degrees from Universidade Tecnológica Federal do Paraná, Brazil, in 2010, 2011, and 2015, respectively. He has jointly graduated from the University of Oulu in a double degree program, and received the D.Sc. (Tech) degree in 2015. He is currently a Post-Doctoral researcher with the Centre for Wireless Communications, Oulu. His current research focuses on ultrareliable communications, physical layer security, full-duplex networks, and applications to IoT and 5G.



MAURICIO DE CASTRO TOMÉ received the B.S and M.Sc. degrees in electrical engineering from the University of Campinas, Brazil, in 2011 and 2014, respectively. He is currently pursuing the Ph.D. degree with the University of Oulu, Finland, researching power and energy measurements and load estimation in smart grids.

PEDRO HENRIQUE JULIANO NARDELLI received the B.S. and M.Sc. degrees in electrical engineering from the State University of Campinas, Brazil, in 2006 and 2008, respectively, and the Ph.D. degree from the University of Oulu, Finland, and State University of Campinas following a dual-degree agreement, in 2013. He holds a post-doctoral position with the University of Oulu, and his studies are mainly focused on the efficiency of wireless networks and spatio-temporal dynamics of complex systems, and smart grids.

CARLOS H. M. DE LIMA received the B.Sc. and M.Sc. degrees in electrical engineering from the Federal University of Ceará, Fortaleza, Brazil, in 2002 and 2004, respectively, and the D.Sc. degree in telecommunications engineering from the University of Oulu, Finland, in 2013. From 2000 to 2005, he was a Research Scientist with the Wireless Telecommunications Research Group, Fortaleza. In 2005, he was a Visiting Researcher with the Ericsson Research Center, Lulea, Sweden, where he was engaged in power control techniques for enhanced high-speed packet access systems. In 2006, he was with the Nokia Institute of Technology, Brazil, where he was engaged in the evaluation of the system performance of WiMAX systems. He is currently an Assistant Professor with São Paulo State University, São João da Boa Vista-SP, Brazil, and also a Research Staff Member with the Centre for Wireless Communications, University of Oulu. His research interests include statistical signal processing and analysis of interference networks using stochastic geometry.

MATTI LATVA-AHO was born in Kuivaniemi, Finland, in 1968. He received the M.Sc., Lic.Tech., and Dr. Tech (Hons.) degrees in electrical engineering from the University of Oulu, Finland, in 1992, 1996, and 1998, respectively. From 1992 to 1993, he was a Research Engineer with Nokia Mobile Phones, Oulu, Finland. From 1994 to 1998, he was a Research Scientist with the Telecommunication Laboratory and Centre for Wireless Communications, University of Oulu. He was the Director of Centre for Wireless Communications, University of Oulu, from 1998 to 2006. He is currently the Department Chair Professor of Digital Transmission Techniques and the Head of the Department for Communications Engineering with the University of Oulu. He is also the Head of the Centre for Wireless Communications and leads the activities related to 5G and 5G test network. He has published over 200 conference or journal papers in the field of wireless communications. His research interests are related to mobile broadband wireless communication systems. He has been TPC Chairman for PIMRC06, TPC Co-Chairman for ChinaCom07, and General Chairman for WPMC08.