Securing delay-tolerant IoT uplink communications against eavesdropping

Stefano Iellamo
ICS-FORTH
Leof. Plastira 100, Greece
siellamo@ics.forth.gr

Raoul Guiazon
University College London,
EEE Department, UK
raoul.guiazon.13@ucl.ac.uk

Marceau Coupechoux
LTCI, CNRS, Telecom ParisTech,
University Paris-Saclay, France
coupecho@enst.fr

Kai-Kit Wong
University College London,
EEE department, UK
kai-kit.wong@ucl.ac.uk

***Abstract*—We consider a network of Internet of Things devices transmitting to an IoT Gateway (IoT-GW). Such communications can potentially be overheard by one or multiple eavesdroppers whose position is unknown. Our goal is to design an artificial noise (AN)-aided transmit strategy such that the secrecy capacity always be positive everywhere across the served region, subject to power and interference cancellation constraints. We thus propose a communication design where the potential eavesdroppers are deactivated by means of jamming operations performed by 1) an In-Band Full Duplex (IBFD) IoT-GW and/or by 2) cooperative helpers featuring multiple antennas. We show that the solution where only the IBFD IoT-GW generates AN is feasible in the smart-home use case, i.e., when a neutralization zone around each IoT-device is assumed. In the case with helpers instead, we show that the Average number of Secure Connections (ASC) increases at least exponentially with the density of the helpers.**

I. Introduction

The Internet of Things (IoT) is regarded as the next big revolution in digital communications. Billions of old and new physical objects (aka Things) - embedded with sensors, controllers and actuators - will soon become IoT-augmented, i.e., will be enabled to sense, process and transmit data; with a tremendous impact on industrial processes, business services and people 's everyday life. In this new context, wireless communications are the key to provide connectivity to the Things; the latter are by definition extremely limited in terms of battery/processing power and architecture, so that the unique opportunities linked to IoT come along with unique challenges.

In this paper, we address the problem of protecting IoT delay-tolerant uplink data, consisting of users' private information, from eavesdropping. Motivated by the fact that using traditional cryptographic tools is not practical nor realistic with IoT networks (seen the extremely limited amount of resources available at the IoT-devices and IoT-gateways IoT-GW) we propose the use of PHY layer security achieved by smart jamming operations. We assume that the position of the eavesdropper(s) is unknown so that we aim to ensure the secrecy across a whole region around the IoT-GW. We will show how this is made possible by leveraging In-Band Full-Duplex (IBFD) technology and/or cooperative jamming, and will present a first methodic study which points out the practicability of the presented solutions. To the best of our knowledge, this is the first study bridging the gap between information-theoretical tools and practical IoT applications.

S.Iellamo is supported by the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement no 612361.
R. Guiazon is supported by the EPSRC and BT under Grant EP/K504610/1.
M. Coupechoux is partly supported by the french ANR project NETLEARN ANR-13-INFR-004.

PHY layer security is an information-theoretic approach that allows to achieve secrecy by using channel codes and signal processing techniques. The seminal work of Wyner [1] dated 1975 introduced the degraded wiretap channel and the fundamental notion of secrecy capacity. Three years later, Wiener's secrecy capacity formulation was generalized to non-degraded broadcast channels with confidential information [2] and Gaussian wiretap channels [3]; and more recently to MIMO wiretap channels [4]. In the meantime, the literature on secrecy capacity has been growing: Many papers can be found on the secrecy rate maximization problem with one or more eavesdroppers (see [5], [6] and references therein) and with different assumptions on transmitter/receiver/eavesdropper antenna configurations and channel state information (CSI).

A few works focus on the case where there is no Eve's CSI (i.e., the position of the eavesdropper is unknown): In [7] the authors present scaling results on the per-node secure throughput in a network of transmitter-receiver pairs. In [8] a stochastic cooperative jamming strategy to thwart the eavesdropper(s) anywhere in the network is proposed. Compared to this strategy, the cooperative scheme we propose in this paper does not cause data rate degradation to the legacy IoT users and does not require protocol modifications. In [9] the authors propose a secure transmission design between a secondary transmitter- receiver pair in the presence of randomly distributed eavesdroppers under an interference constraint set by the primary user. In [10] the authors present a scheme for compensating non-altruistic SUs for providing jamming service by providing variable spectrum resources. This can be used in conjunction with stochastic protocols to optimize CR performance [11], [12].

As for In-Band Full-Duplex (IBFD) technology, this was firstly thought as a way to enhance spectrum efficiency

[13]. It was then proposed as a way to provide PHY layer secrecy by letting legacy nodes receive and at the same time transmit AN (see, e.g., [14] and references therein). However, the biggest practical impediments to IBFD operation is the presence of self-interference, i.e., the interference caused by an IBFD nodes own transmissions to its desired receptions [15]. In this paper, we take the self-interference cancellation constraint into account and provide results accordingly.

With this paper, our contribution is three-fold:

- We consider a realistic IoT network and formulate a power optimization problem by taking into account interference cancellation, secrecy capacity and power constraints (Section II).
- We provide simple design rules for achieving a positive secrecy capacity everywhere across the served region, regardless of Eve's position, in the cases where:
  - the AN is broadcasted by the IoT-GW only (Section III).
  - the AN is broadcasted by the IoT-GW and by a set of cooperative jammers featuring multiple antennas (Section IV).
- We analyze the effectiveness of our solutions by means of an extensive numerical analysis with real NB-IoT settings (Section V).

II. Model and Problem Statement

A. Network Model

Let $\mathcal{B}(x,\rho)$ be a disk centered at node position x with radius ρ. We define our network over a disc $\mathcal{B}(0,R)$, where 0 is the origin and corresponds to the location of the IoT-GW. Let $\mathcal{X}\{1,..,x,..\#\mathcal{X}\}$ and $\mathcal{X}_{\text{📍}} = \{x_i\}_{i\in\mathcal{X}} \subset \mathcal{B}(0,R)$ denote the set of IoT devices and of their locations respectively. Similarly, let $\mathcal{E} = \{1,..,e,..\#\mathcal{E}\}$ and $\mathcal{E}_{\text{📍}} = \{x_e\} \subset \mathcal{B}(0,2R)$ be the set of eavesdroppers and of their locations; and let $\mathcal{K}$ and $\mathcal{K}_{\text{📍}} = \{x_k\}_{k\in\mathcal{K}} \subset \mathcal{B}(0,2R)$ denote the set of helpers and of their locations. The IoT devices transmit data to the IoT-GW which for convenience will be referred to as device 0 located at x_0. The IoT-GW features IBFD technology and is therefore able to receive and transmit on the same frequency band for security purposes. All operations occur on the same frequency band B_1 centered at f_1 and characterized by background noise power $N_1 = N_0 B_1$. The resulting network is sketched in Fig. 1. Nodes in $\mathcal{E}_{\text{📍}}$, $\mathcal{K}_{\text{📍}}$ and $\mathcal{X}_{\text{📍}}$ are distributed according to an independent Poisson Point Process (PPP) [16] with intensities λ_E, λ_K and λ_X respectively across a disk of radius R centered at the IoT-GW. The Euclidean distance between two nodes x and y is denoted by d_{xy} and the channel gain g_{xy} is assumed to be strictly decreasing on the distance d_{xy} and not dependent on the considered nodes. Each node has no idea of the information of surrounding nodes. All nodes are assumed to be static, and the eavesdroppers are passively operating independently of each other. That is, there exists no collusion among eavesdroppers.

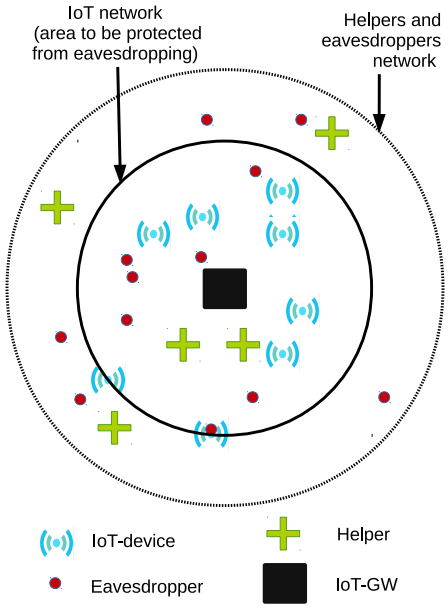

Fig. 1. Sketch of the considered IoT network.

B. Secure communications

In order for the data transmission from an IoT device i to be securely received at a destination node j in the presence of an eavesdropper e, the signal to interference plus noise ratio (SINR) ie at the eavesdropper's place x_e should be smaller than the SINR experienced at the destination node x_j, i.e., $SINR_{ie} < SINR_{ij}$. In particular, given SINR $ij \geqslant \gamma_j$ and $SINR_{ie} < \gamma_e$, where $\gamma_e < \gamma_j$ and γ_e can be arbitrarily small, the secrecy capacity [3], [4] of the communication between i and j at each separate transmission can be determined by:

$$\mathbf{C}_{ij} = \max\{0, \log_2(1+SINR_{ij}) - \log_2(1+SINR_{ie})\} \quad (1)$$

That is, i and j can achieve secure communication with secrecy rate $\mathbf{R}_{ij} < \mathbf{C}_{ij}$ by agreeing on a code.
Recalling that the eavesdroppers follow a PPP process $\mathcal{E}$, a secure data link can be defined as follows [8]:

Definition 1 (Secure Data Link)**.** *The data link from x_i to x_j is secure if and only if*

$$SINR_{ij} \geqslant \gamma_j \qquad \textit{and} \qquad SINR_{ie} < \gamma_e, \qquad \forall e \in \mathcal{E}. \quad (2)$$

In our model, the above security conditions are met thanks to *jamming operations* which generate *neutralization zones*.

Definition 2 (Neutralization zone)**.** *A neutralization zone is an area across which conditions* (2) *are satisfied, i.e., where no eavesdropper is able to overhear transmissions performed by any IoT device of the network .*

We model the neutralization zones by disks $\mathcal{B}(x,\rho)$, $x \subset \mathcal{B}(0,2R), \rho > 0$. The jamming operation are performed

by the IBFD IoT-GWs emitting artificial noise (AN) with power P_0 and/or a set of cooperative helpers which are capable of steering their jamming signal away of the IoT-GW (by means of multiple antenna techniques such as beamforming). The IBFD IoT-GW is then able to partially cancel the related self-interference from its in-band receive antenna. We say partially because self-interference cancellation is a complex operation and so far it has only been proven the possibility to cancel up to 110dB [15].

C. Problem Formulation

We formulate the problem of minimizing the IoT-GW transmit power while securing the uplink IoT data in the case of unknown eavesdroppers location. We focus on the case where all IoT devices transmit with the same power P and all the helpers transmit with the same power Q and set-up the following optimization problem:

$$\begin{aligned}
\textbf{minimize} \quad & P_0 && (3)\\
\textbf{s.t.} \quad & SINR_{i0} \geqslant \gamma_0 && \forall i \in \mathcal{X} \quad (4)\\
& SINR_{ie} < \gamma_E && \forall i \in \mathcal{X}, \forall e \in \mathcal{E} \quad (5)\\
& P_0 \leqslant P_0^{max} && (6)
\end{aligned}$$

where

$$SINR_{i0} = \frac{P g_{i0}}{N_1 + P_0 h_0}, \tag{7}$$

$$SINR_{ie} = \frac{P g_{ie}}{N_1 + P_0 g_{0e} + \sum_{k \in \mathcal{K}} Q g_{ke}} \tag{8}$$

where h_0 denotes the IoT-GW self-interference reduction factor, P_0^{max} denote the maximum power the IoT-GW can use for jamming operations. Note that $\gamma_E = \min_e\{\gamma_e\}$, meaning that no eavesdropper is able to decode messages if the experienced SINR is less than γ_E.

III. Jamming from the IoT-GW only

Let us firstly focus on the case where there are no cooperative jamming nodes. This is equivalent to setting $Q = 0$ in (8). In this scenario a worst case communication can be defined as follows:

Definition 3 (Worst case communication)**.** *The worst case communication is the one occurring from the farthest IoT-device (from the IoT-GW) when an eavesdropper e^* is co-located with it.*

The following proposition is straightforward.

Proposition 1. *An IoT network is fully secure (i.e., all of its data links are secure) if all IoT-devices transmit at a secrecy rate which is less than the secrecy capacity calculated wrt to the worst case communication.*

From the Proposition, a solution to the optimization problem (3)-(6) exists if the IoT-GW can guarantee secure data links to all of its associated IoT-devices. This is possible by generating a neutralization zone covering the whole IoT network.

Theorem 1. *Assume $g_{xy} = f(d_{xy})$ is a monotone function (strictly decreasing in Euclidean distance d_{xy} and not dependent on the position of x and y). Further, assume i^* is the farthest IoT-device from the IoT-GW and e^* is its co-located eavesdropper. Then:*

1) *The IoT-GW can guarantee a positive secrecy rate to all its associated IoT-devices if*

$$h_0 < \frac{\gamma_E g_{i*0}(P g_{i*0} - N_1\gamma_0)}{\gamma_0(P - N_1\gamma_E)} \tag{9}$$

2) *When such inequality holds, there exists a solution to the optimization problem* (3)-(6)*. Such solution is*

$$P_0 = \frac{P - N_1\gamma_E}{g_{i*0}\gamma_E} + \epsilon \tag{10}$$

where ϵ is the smallest power increasing step.

Proof. See Appendix. □

However, as shown in the numerical section (Section V) fully secure communications even in small areas come at the cost of extremely high IoT-GW AN transmit power. This reduces drastically the business potential of the proposed technique (for instance, it would be unrealistic to install such power-hungry IoT-GW at the users' premises) and motivates us to seek other ways to improve the IoT network secrecy capacity while reducing the IoT-GW power consumption. Thus, we now study the cases with protected surroundings and with helpers.

A. Protected surroundings

In some scenarios, each legitimate IoT-node may be able to physically inspect its surroundings and deactivate the eavesdroppers falling inside some neutralization region. With each node, we associate a neutralization region inside which all eavesdroppers have been deactivated. This can be the case for indoor IoT nodes (e.g., within the smart home walls).

For finite neutralization regions, we need to define a new worst case communication case:

Definition 4 (Worst case communication with neutralization areas)**.** *In the presence of finite neutralization areas around each IoT-device the worst case communication occurs when an eavesdropper e^* is located just outside the neutralization region, on the farthest point from the IoT-GW.*

Theorem 2. *Consider a neutralization region around each IoT-node of minimum radius $d_{x_i x_e^*} - \epsilon$, where ϵ is a very small constant. Assume $g_{xy} = f(d_{xy})$ is a monotone function (strictly decreasing in Euclidean distance d_{xy} and not dependent on the position of x and y). Let i^* be the farthest IoT-device from the IoT-GW and e^* be the eavesdropper located on the farthest point from the IoT-GW which is just outside the neutralization region. Then,*

1) *the IoT-GW can guarantee a positive secrecy rate to all its associated IoT-devices if*

$$h_0 < \frac{\gamma_E g_{0e*}(P g_{i*0} - N_1\gamma_0)}{\gamma_0(P g_{i*e*} - N_1\gamma_E)} \tag{11}$$

2) When such inequality holds, there exists a solution to the optimization problem (3)-(6)*. Such solution is*

$$P_0 = \frac{P g_{i*e*} - N_1 \gamma_E}{g_{i*0} \gamma_E} + \epsilon \tag{12}$$

where ϵ is the smallest power increasing step.

We will show in the simulation section how even a neutralization region of limited size allows to greatly reduce the IoT-GW power consumption.

IV. Cooperative approaches

A simple and yet powerful strategy for lowering the IoT-GW transmit power while guaranteed a certain degree of secrecy is cooperative jamming [17]. In cooperative jamming, the IoT-GW artificial noise is complemented by the jamming signal(s) emitted by a set of of friendly jammers or helpers. We propose in the following subsections two cooperative jamming strategies and provide a systematic study of their performance.

A. Based on the location of eavesdroppers

In this section we consider a cooperative model where the IoT network is populated by helpers which are able to neutralize potential eavesdroppers located within a certain radius. The resulting IoT network is sketched in Fig. 2, where the white areas are the neutralization zones generated by the helpers.
Note that the considered model with neutralization regions is general enough to include different sorts of physical realizations. For example, the helpers can be radio transceivers able to sense even passive eavesdroppers from their leaked local oscillator power as described in [18] then, using directional antennas they can send a jamming signal towards these eavesdroppers. Using the same model, the neutralization regions can be viewed as trusted areas where no eavesdropper can be found, for example this could be locations where physical security measures dissuades the eavesdroppers.

In the following, we will rate the level of confidentiality of an IoT network by its Average number of Secure Connections (ASC) to the IoT-GW. However, due to the fact that a practical IoT network is envisioned to comprise thousands of IoT devices, running a Monte Carlo simulation to obtain the ASC can be very daunting and could take days. Therefore, we aim to obtain a closed-form expression of the ASC lower bound as this can indeed provide a powerful tool to analyze IoT networks within shorter terms and limited resources.

Let us recall that helpers, eavesdroppers and IoT devices are PPP distributed with intensities λ_K, λ_E and λ_X. And let us adapt a few definitions from graph theory and from [19] to our case:

Definition 5 (Poisson iS-Graph for IoT networks)**.** *The Poisson intrinsically Secure graph ($i\mathcal{S}-graph$) for IoT networks*[1] *is the directed graph $G = \{\mathcal{X} \cup \{x_0\}, \mathcal{T}\}$ with vertex set $\mathcal{X} \cup \{x_0\}$ and edge set*

$$\mathcal{T} = \{\overrightarrow{x_i x_0} : \boldsymbol{C}_{i0} > 0\}. \tag{13}$$

[1]The $i\mathcal{S}$-graph was defined in [19] in a setting where every node in the network could potentially want to talk to any other node.

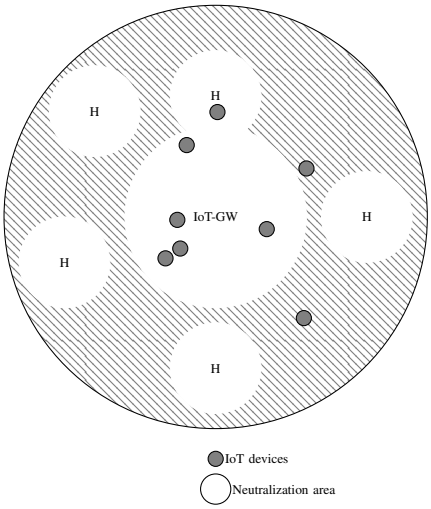

Fig. 2. Neutralization region in IoT networks. Note that the eavesdroppers and the helpers can be in an area much larger than the IoT network itself.

Definition 6 (IoT-GW in-degree N_{in})**.** *In the Poisson iS-Graph for IoT networks, the IoT-GW in-degree N_{in} is the number of edges entering the IoT-GW vertex. In other words, it is the average number of secure connections in the IoT network.*

Definition 7 (IoT-GW In-isolation)**.** *In the Poisson iS-Graph for IoT networks, the IoT-GW In-isolation is the probability that the IoT-GW cannot receive from anyone with positive secrecy rate.*

By the definitions above, we want the IoT-GW to be the least In-isolated possible by letting each helper generate a neutralization zone of finite size.

We approximate the neutralization zones as in [19] by associating to each helper k_i a neutralization zone Θ_i inside of which all eavesdroppers will be neutralized. Thus the total neutralization region Θ is given as

$$\Theta \approx \bigcup_{i=1}^{\#\mathcal{K}} (k_i + \Theta_i) \tag{14}$$

Where $\#\mathcal{K}$ is the number of element in $\mathcal{K}$.
The area around the IoT-GW is most sensitive because, the closer an eavesdropper is to the IoT-GW the higher the probability of In-isolation. Therefore, we assume that the IoT-GW is protected inside a neutralisation region of radius ρ_{IoT}. With this model, no protection for the IoT-GW is equivalent to $\rho_{IoT} = 0$.

Considering generic path losses g_{xy}, we provide a full characterization of the proposed cooperative model with the following theorem.

Theorem 3. *The average number of secure communication connections in the Poisson iS-Graph for IoT networks is lower bounded by*

$$\mathbb{E}\{N_{in}\} \geqslant \frac{\lambda_x}{\lambda_e}\Big(\pi\lambda_e\bar{\rho}_{IoT}^2 + \frac{1}{p_{\bar{\Theta}}}\left[\exp(-\lambda_e\pi p_{\bar{\Theta}}\bar{\rho}_{IoT}^2) - \exp(-\lambda_e\pi p_{\bar{\Theta}}R^2)\right]\Big) \quad (15)$$

With $p_{\bar{\Theta}} = e^{-\lambda_k\pi\rho_k^2}$ *and* $\bar{\rho}_{IoT} = \frac{\rho_{IoT}}{2}$

Proof. See Appendix. □

This result shows how the network parameters are linked to the number of secure connections. Compared to the result shown in [19] our result takes into account the physical size of the network, the presence of helpers, as well as generic channel gains.

B. Blind Jamming Strategies

We now turn our attention to the case where jamming operations are performed by the IoT-GW in cooperation with a set of helpers in the form of multi-antenna friendly jammers. This could model a 5G LTE small cell network (5G) where each small cell base station additionally operates as an IoT-GW and each served multi-antenna LTE terminal additionally operates as an IoT helper by steering the jamming beam away of the IoT-GW.

In a first approach, we can assume that each eavesdropper is jammed only by the closest helper node to its location. This approximation is even more realistic in the case where the IoT-devices use the technique Divide-and-Conquer [8] for their data transmission, provided that the messages are encoded across a sufficiently large number of blocks and the helpers are sending jamming signals sporadically.

A second approach is to assume that all the eavesdroppers are receiving a jamming signal from all the helpers at the same time. In this scenario also, we consider that the helpers are able to steer their interference away from the IoT-GW. The performance of the two approaches above will be shown and compared in the numerical section (Section V). A more detailed analysis of this work will be presented in a future publication.

V. Numerical analysis

For the simulation we consider a NB-IoT network whose IoT devices transmit with constant power $P = 0$dBm across a bandwidth B_1 which is $200kHz$ wide and is centered at $900MHz$. We calculate the channel gains according to $g_{xy}(d) = A\log(d) + B + C\log(f_c)$ with $A = 22$, $B = 28$, $C = 20$ (typical urban LOS [20]) and we set in all simulations $\gamma_0 = 6$ and $\gamma_E = 3$.

In this real world scenario, we want to analyze the results presented in the form of Theorem 1 and Theorem 2. In Fig. 3 and Fig. 4 we show the minimum required IoT-GW performance (in terms respectively of dB to be canceled from the self-interference signal and artificial noise transmit power) needed in order to fully secure a disk area of radius R around the IoT-GW. From the figures it is easy to notice that the case with co-located eavesdropper is very unrealistic in practice as a state-of-the-art self-interference cancellation mechanism and 50 dBm of AN transmit power are required to fully secure a disk area of only 20m radius. On the other hand, by considering even a small neutralization region it is possible to secure much wider areas with much less resources. For instance a 70m radius area can be fully secured by means of a 70 dB self-interference cancellation mechanism and 36 dBm AN transmit power for the 1m protected surroundings case.

In Fig. 5 we show the secrecy capacity lower bound for IoT communications within a network of radius R. We say lower bound because that will be the maximum secrecy rate that can be achieved by an IoT-device in the worst case communication scenario (with and without neutralization areas). Note that this holds true because all the IoT devices transmit with the same power.

Fig. 6 shows the ASC from the IoT devices to the IoT-GW in percentage of the total number of IoT-devices against the size of the neutralization regions generated by the helpers. The neutralization region of the IoT-GW is fixed at $\rho_{IoT} = 0m$ and the network size is $R = 100m$. The Monte carlo simulation and theoretical curves are shown for $\lambda_x = 0.1$, which corresponds to an average number of 3141 IoT devices. We see that the simulation curves and the lower bounds are very close.

In Fig. 7 we show the ASC when the eavesdroppers are jammed by the closest helper only. Three different cases are shown, first, when the IoT-GW is not sending jamming signal in the network we see that with helpers power of -5dBm only 40% of the IoT devices are secured in average. This number grows to almost 60% when the IoT-GW sends a 0dBm jamming signal and 90% when the IoT-GW jamming signal power is 15dBm. However, even without IoT-GW jamming, the helpers are able to secure 90% of the IoT-devices with a power of just 5dBm whereas the IoT-GW would need at least 15dBm to obtain the same results.

In Fig. 8 we compare the scenario where an eavesdropper is jammed by its closest helper to the one where the eavesdropper is jammed by all the helpers. The first obvious result is that the performance is higher when all the helpers are considered at the same time. However, the gap between the two scenario is smaller if the helpers are transmitting at higher power, and the aggregate interference created by the network to potential neighboring networks is much less if only one helper is jamming at one time.

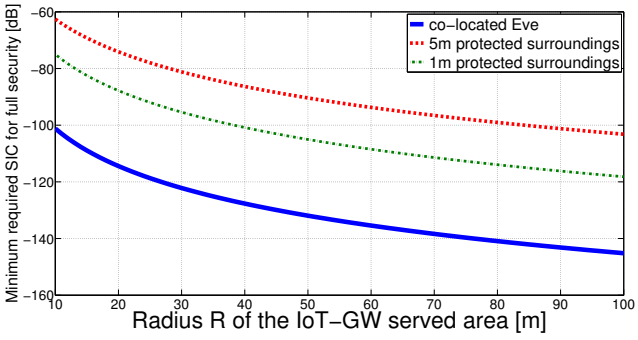

Fig. 3. Minimum self-interference cancellation (SIC) performance required at the IoT-GW in order to achieve fully secure NB-IoT communications across a disk-shaped area of radius R around the IoT-GW.

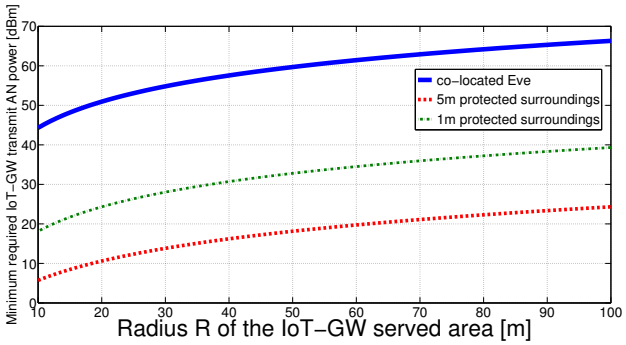

Fig. 4. Minimum required IoT-GW transmit power performance to achieve fully secure NB-IoT communications across a disk-shaped area of radius R around the IoT-GW.

VI. Conclusion and Future Work

In this paper we have studied the confidentiality of the communications flowing from a network of IoT devices to a reference IoT-GW when the position of the potential eavesdropper(s) is unknown. By building on the concepts of jamming by artificial noise (AN) and In band full duplex we have proposed smart jamming strategies aimed at minimizing the IoT-GW AN power consumption while guaranteeing a

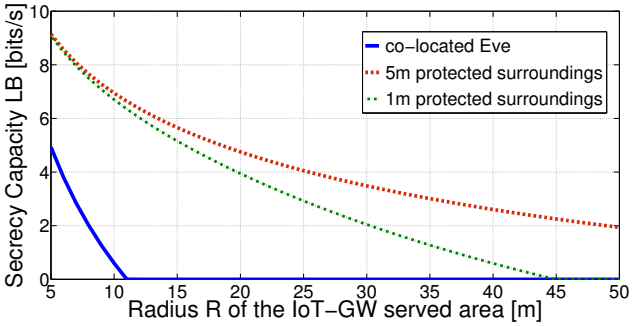

Fig. 5. Secrecy capacity Lower Bound when the IoT-devices use NB-IoT radios. Settings: $h_0 = 10^{-10}$, $P_0 = 30$dBm

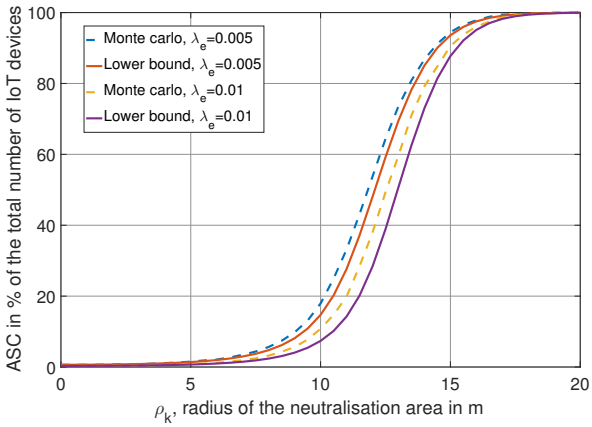

Fig. 6. Average number of secure connections to the IoT-GW against the size of de neutralization regions of the helpers. Settings: $\rho_{IoT} = 0m$, $\lambda_x = 0.1$, $\lambda_k = 1.10^{-2}m^{-2}$, $R = 100m$.

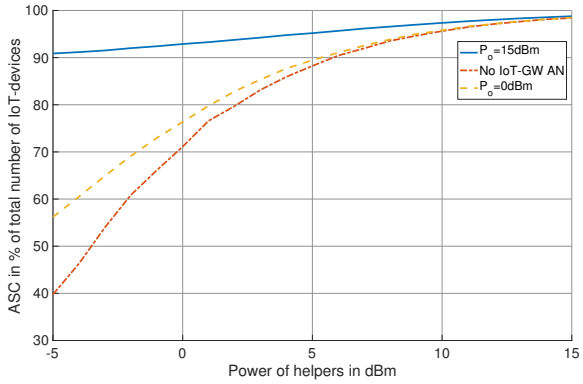

Fig. 7. Average number of secure connections to the IoT-GW against the transmit power of the helpers and for different transmit AN power at the IoT-GW, settings: $\lambda_x = 0.1$, $\lambda_e = 5.10^{-4}m^{-2}$, $\lambda_k = 5.10^{-4}m^{-2}$, $R = 100m$, $\gamma_E = 3$, $\gamma_0 = 6$, $h_0 = 10^{-10}$.

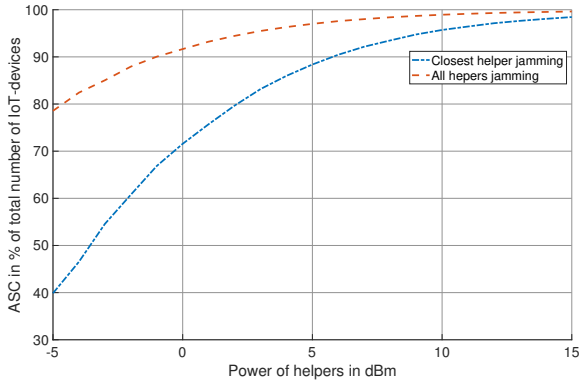

Fig. 8. Comparison of the ASC against the transmit power of the helpers in the case where only the closest helper AN is considered with the case where all helpers AN are considered, settings: $\lambda_x = 0.1$, $\lambda_e = 5.10^{-4}m^{-2}$, $\lambda_k = 5.10^{-4}m^{-2}$, $R = 100m$, $\gamma_E = 3$, $\gamma_0 = 6$, $h_0 = 10^{-10}$.

positive secrecy rate across the IoT-GW served region. To study the proposed jamming strategies, we have used the concept of neutralization regions, which are areas within the IoT network where all eavesdroppers are deactivated (i.e., they are not able to decode information). We have shown that the solution where only the IBFD IoT-GW generates AN is viable in the smart-home use case, i.e., when a neutralization zone around each IoT-device is assumed. In the case with helpers and punctual jamming instead, we have shown that the Average number of Secure Connections (ASC) increases at least exponentially with the density of the helpers.
In our parallel ongoing work, we are studying AN-based smart jamming strategies for downlink IoT communications, for the backhaul (i.e., from the IoT-GW to an IoT cloud receiver), and for delay-sensitive applications.

REFERENCES

[1] A. D. Wyner. The wire-tap channel. *The Bell System Technical Journal*, 54(8):1355–1387, October 1975.

[2] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, May 1978.

[3] S. Leung-Yan-Cheong and M. Hellman. The Gaussian wire-tap channel. *IEEE Transactions on Information Theory*, 24(4):451–456, July 1978.

[4] F. Oggier and B. Hassibi. The Secrecy Capacity of the MIMO Wiretap Channel. *IEEE Transactions on Information Theory*, 57(8):4961–4972, August 2011.

[5] Qiang Li and Wing-Kin Ma. Spatially Selective Artificial-Noise Aided Transmit Optimization for MISO Multi-Eves Secrecy Rate Maximization. *IEEE Transactions on Signal Processing*, 61(10):2704–2717, May 2013. arXiv: 1303.1915.

[6] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst. Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey. *IEEE Communications Surveys Tutorials*, 16(3):1550–1573, 2014.

[7] apar, D. Goeckel, B. Liu, and D. Towsley. Secret communication in large wireless networks without eavesdropper location information. In *2012 Proceedings IEEE INFOCOM*, pages 1152–1160, March 2012.

[8] Z. Liu, J. Liu, N. Kato, J. Ma, and Q. Huang. Divide-and-conquer based cooperative jamming: Addressing multiple eavesdroppers in close proximity. In *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, pages 1–9, April 2016.

[9] X. Xu, B. He, W. Yang, X. Zhou, and Y. Cai. Secure Transmission Design for Cognitive Radio Networks With Poisson Distributed Eavesdroppers. *IEEE Transactions on Information Forensics and Security*, 11(2):373–387, February 2016.

[10] I. Stanojev and A. Yener. Improving Secrecy Rate via Spectrum Leasing for Friendly Jamming. *IEEE Transactions on Wireless Communications*, 12(1):134–145, January 2013.

[11] Stefano Iellamo, Ekaterina Alekseeva, Lin Chen, Marceau Coupechoux, and Yuri Kochetov. Competitive location in cognitive radio networks. *4OR*, pages 1–30, August 2014.

[12] S. Iellamo, L. Chen, and M. Coupechoux. Imitation-based spectrum access policy for CSMA/CA-based cognitive radio networks. In *2012 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 2780–2785, April 2012.

[13] Dinesh Bharadia, Emily McMilin, and Sachin Katti. Full Duplex Radios. In *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, SIGCOMM '13, pages 375–386, New York, NY, USA, 2013. ACM.

[14] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten. Improving Physical Layer Secrecy Using Full-Duplex Jamming Receivers. *IEEE Transactions on Signal Processing*, 61(20):4962–4974, October 2013.

[15] D. Kim, H. Lee, and D. Hong. A Survey of In-Band Full-Duplex Transmission: From the Perspective of PHY and MAC Layers. *IEEE Communications Surveys Tutorials*, 17(4):2017–2046, 2015.

[16] Sung Nok Chiu, Dietrich Stoyan, Wilfrid S. Kendall, and Joseph Mecke. *Stochastic Geometry and Its Applications*. John Wiley & Sons, June 2013.

[17] M. Atallah, G. Kaddoum, and L. Kong. A Survey on Cooperative Jamming Applied to Physical Layer Security. In *2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB)*, pages 1–5, October 2015.

[18] A. Mukherjee and A. L. Swindlehurst. Detecting passive eavesdroppers in the MIMO wiretap channel. In *2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 2809–2812, March 2012.

[19] P. C. Pinto, J. Barros, and M. Z. Win. Secure Communication in Stochastic Wireless Networks #x2014;Part I: Connectivity. *IEEE Transactions on Information Forensics and Security*, 7(1):125–138, February 2012.

[20] 3rd Generation Partnership Project. 3gpp 36tr 36 .814 V 9.0.0 (20 10 - 03). Technical report, 3GPP, 2010.

APPENDIX

Proof of Theorem 1

Recall that the secrecy rate capacity of IoT-device i wrt eavesdropper e is $\mathbf{C}_{i0} = \max\{0, \log_2(1+SINR_{i0}) - \log_2(1+SINR_{ie})\}$, where

$$SINR_{i0} = \frac{Pg_{i0}}{N_1 + P_0 h_0}$$

Assuming reciprocal channel gains (i.e., e.g., $g_{i0} = g_{0i}$) and for the worst case where an eavesdropper e^* is co-located with a transmitting IoT-device i (i.e., $g_{i0} = g_{e*0} = g_{0e*}$), $SINR_{ie*}$ can be written as follows:

$$SINR_{ie*} = \frac{P}{N_1 + P_0 g_{i0}}$$

According to constraints (4) and constraints (5) (which reflect conditions (2)) an IoT-device experiences positive secrecy rate if $SINR_{i0} \geqslant \gamma_0$ and $SINR_{ie*} < \gamma_E$, i.e.,

$$\begin{cases} \frac{Pg_{i0}}{N_1+P_0 h_0} \geqslant \gamma_0 \\ \frac{P}{N_1+P_0 g_{i0}} < \gamma_E \end{cases}$$

It is easy to verify that the system of inequalities above is solved for $\frac{P-N_1\gamma_E}{g_{i0}\gamma_E} < P_0 \leqslant \frac{Pg_{i0}-N_1\gamma_0}{h_0\gamma_0}$.
Thus a finite P_0 exists only if $\frac{Pg_{i0}-N_1\gamma_0}{h_0\gamma_0}$ is strictly greater than $\frac{P-N_1\gamma_E}{g_{i0}\gamma_E}$, which holds for $h_0 < \frac{\gamma_E g_{i0}(Pg_{i0}-N_1\gamma_0)}{\gamma_0(P-N_1\gamma_E)}$ (point 1 of the Theorem). From this one can easily infer that 1) if g(.) is strictly decreasing as a function of the distance d_{xy} between positions x and y, the most stringent condition for h is wrt the farthest IoT-device i^* from the IoT-GW. Thus, if the inequality holds for such worst case, then it holds for all the IoT devices of the network (point 1 of the Theorem) 2) The minimum feasible P_0 is $\frac{P-N_1\gamma_E}{g_{i0}\gamma_E} + \epsilon$, where ϵ is the smallest possible power increasing step (point 2 of the Theorem).

Proof of Theorem 3

In order for a device (say x) to be able to establish a secure communication link to the IoT-GW there must not be any eavesdropper within a disc of radius d_{xo} around the device.
If there is an eavesdropper within $\mathcal{B}(x, d_{xo})$ then to keep the link secure that eavesdropper must be neutralized by a helper or by the IoT-GW.

Hence, the set of users able to achieve a secure communication link to the IoT-GW is given as

$$\mathcal{S} = \left\{ x \ ; \ x \in \mathcal{X} \ and \ \overset{\circ}{\mathcal{B}}(x, d_{xo}) \cap \bar{\Theta} \cap \mathcal{K} = \varnothing \right\} \tag{16}$$

Where $\overset{\circ}{\mathcal{B}}(x, d_{xo}) = \mathcal{B}(x, d_{xo}) / \mathcal{B}(0, \rho_{IoT})$ is the disc centered on x of radius d_{xo} without the zone neutralized by the IoT-GW.

We can write the number of secure links from the IoT devices to the IoT-GW as

$$\begin{aligned} N_{in} &= \sum_{x \in \mathcal{X}} \mathbb{1}\{x \in \mathcal{S}\} \\ &= \iint_{\mathcal{B}(0,R)} \mathbb{1}\{x \in \mathcal{S}\} \, \mathcal{X}(dx) \end{aligned}$$

Therefore

$$\mathbb{E}\{N_{in}\} = \lambda_x \iint_{\mathcal{B}(0,R)} \mathbb{P}_x\{x \in \mathcal{S}\} \, dx \tag{17}$$

$$= \lambda_x \left(\pi \bar{\rho}_{IoT}^2 + \iint_{\mathcal{D}(\bar{\rho}_{IoT}, R)} \mathbb{P}_x\{x \in \mathcal{S}\} \, dx \right) \tag{18}$$

Where $\mathcal{D}(\bar{\rho}_{IoT}, R)$ is the annulus centered at the origin with inner radius $\bar{\rho}_{IoT}$ and outer radius R with $0 \leqslant \bar{\rho}_{IoT} \leqslant R$.
Now let's find the palm probability $\mathbb{P}_x\{x \in \mathcal{S}\}$

$$\mathbb{P}_x\{x \in \mathcal{S}\} = \mathbb{P}_{\Theta,\mathcal{K}} \left\{ \overset{\circ}{\mathcal{B}}(x, d_{xo}) \cap \bar{\Theta} \cap \mathcal{K} = \varnothing \right\} \tag{19}$$

$$= \mathbb{E}_\Theta \left\{ \exp(-\lambda_e \mathbb{A}(\overset{\circ}{\mathcal{B}}(x, d_{xo}) \cap \bar{\Theta}) \right\} \tag{20}$$

$$\geqslant \exp\left(-\lambda_e \mathbb{E}_\Theta \left\{ \mathbb{A}(\overset{\circ}{\mathcal{B}}(x, d_{xo}) \cap \bar{\Theta}) \right\} \right) \tag{21}$$

Where (21) is obtained using Jensen's inequality, $\mathbb{E}_X$ is the average according to the random variable X, $\mathbb{A}()$ gives the area of a specified random region.

$$\mathbb{E}_\Theta \left\{ \mathbb{A}(\overset{\circ}{\mathcal{B}}(x, d_{xo}) \cap \bar{\Theta}) \right\} = \iint_{\overset{\circ}{\mathcal{B}}(x, d_{xo})} \mathbb{P}\{y \in \bar{\Theta}\} \, dy \tag{22}$$

$$\leqslant \iint_{\mathcal{B}(x, d_{xo})} \mathbb{P}\{y \in \bar{\Theta}\} \, dy \tag{23}$$

$$= \pi d_{xo}^2 \underbrace{e^{-\lambda_k \pi \rho_k^2}}_{\triangleq p_{\bar{\Theta}}} \tag{24}$$

Therefore

$$\mathbb{P}_x\{x \in \mathcal{S}\} \geqslant \exp(-\lambda_e \pi p_{\bar{\Theta}} d_{xo}^2) \tag{25}$$

And finally we can obtain equation (15) by plugging this last result back into equation (18).