Computer Networks 109 (2016) 13–20

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Throughput maximization in multi-hop wireless networks under a secrecy constraint

Pedro H.J. Nardelli[a], Hirley Alves[a,*], Carlos H.M. de Lima[b], Matti Latva-aho[a]

[a] Depto. of Communications Engineering (DCE), Centre for Wireless Communications (CWC), University of Oulu, Oulu, Finland
[b] São Paulo State University (UNESP), São João da Boa Vista, Brazil

ARTICLE INFO

Article history:
Received 16 December 2015
Revised 31 March 2016
Accepted 17 June 2016
Available online 23 June 2016

Keywords:
Multi-hop wireless networks
Stochastic geometry
Machine-to-machine communications
Throughput
Security and jamming

ABSTRACT

This paper analyzes the achievable throughput of multi-hop sensor networks for industrial applications under a secrecy constraint and malicious jamming. The evaluation scenario comprises sensors that measure some relevant information of the plant that is first processed by an aggregator node and then sent to the control unit. To reach the control unit, a message may travel through relay nodes, which form a multi-hop wireless link. At every hop, eavesdropper nodes attempt to acquire the messages transmitted through the legitimate link. The communication design problem posed here is how to maximize the multi-hop throughput from the aggregator to the control unit by finding the best combination of relay positions (i.e. hop length: short or long) and coding rates (i.e. high or low spectral efficiency) so that the secrecy constraint is satisfied. Using a stochastic-geometry formulation, we show that the optimal choice of coding rate is normally high and depends on the path-loss exponent only, while a greater number of shorter hops are preferable to smaller number of longer hops in any situation. For the investigated scenarios, we prove that the optimal throughput subject to the secrecy constraint achieves the unconstrained optimal performance – if a feasible solution exists.

1. Introduction

The industrial environment imposes challenging conditions on radio propagation due to their commonplace reflective and absorbent surfaces, as well as electromagnetic interference from the machinery [1]. Recently, wireless solutions for industrial applications have gained considerable attention from both academia and industry, using the concept of machine-to-machine communications [2–6]. Such an idea enables seamless exchange of information between autonomous devices without any (direct) human intervention. Another advantage of wireless machine-to-machine communications is its scalability, which reduces deployment and maintenance costs.

In industrial plants, exchange of information is often needed among the machinery, monitoring devices and control unit; thereby, reliability, low latency and security become major concerns in the communication system design [7]. In this context, multi-hop machine-to-machine communications appear as a promising technology to tackle the industrial environment challenges. As pointed out in [3], multi-hop schemes are more suitable in such environments with additional interference.

In a typical plant, the design of a multi-hop link between the aggregator and the control unit can be simplified by setting two parameters: position of relay nodes and coding rate (spectral efficiency). The most straightforward design option would be to use long-hops (less use of network resources) and to set high coding rates (i.e. more efficient messages in bits/s/Hz).

Industrial networks usually employ unlicensed frequency bands and consequently are exposed to stronger co-channel interference. If this is the case, using long hops in conjunction with high rates may not be the best choice as far as the former leads to lower signal-to-interference ratio (SIR) while the latter leads to higher SIR thresholds needed to successfully decode a message [8].

In large industrial deployments, there are various sensors and machines continuously monitoring several processes. The resulting information that needs to be exchanged is frequently confidential, which requires the communication to be reliable, efficient, and secure at all levels of the network infrastructure [7,9]. Due to the broadcast nature of the wireless medium, non-intended nodes – commonly named eavesdroppers – within the communication range of a given transmitter can overhear the so-called legitimate transmission and possibly extract private information [9]. To avoid that, cryptographic techniques are usually implemented in the higher layers of the communication protocols to ensure confidentiality [10].

* Corresponding author.
E-mail addresses: nardelli@ee.oulu.fi (P.H.J. Nardelli), halves@ee.oulu.fi (H. Alves), carlos.lima@sjbv.unesp.br (C.H.M. de Lima), matla@ee.oulu.fi (M. Latva-aho).

http://dx.doi.org/10.1016/j.comnet.2016.06.020
1389-1286/

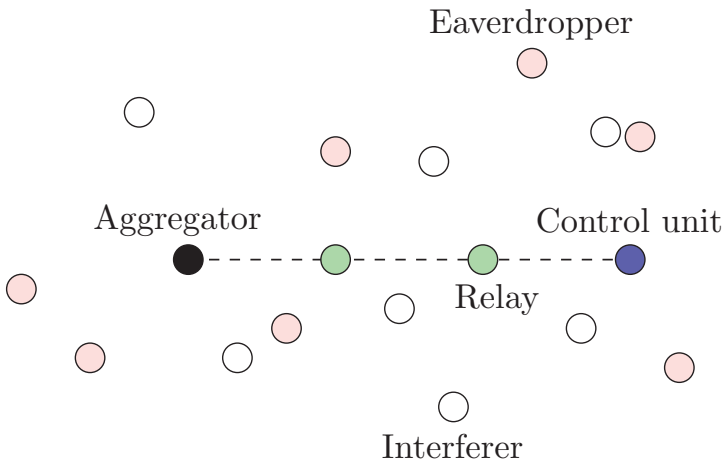

Fig. 1. Schematic example of the proposed scenario. The black node is the aggregator (source), the blue node is the control unit (destination) and the green nodes are the relays, all of them defining the legitimate link. The white nodes are the interferers while the red nodes are the eavesdroppers, which attempt to illegitimately acquire the messages send through the multi-hop link. The network designer aims at maximizing the multi-hop throughput by properly deploying the relays and setting the coding rate used while respecting a given secrecy constraint. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

Such techniques, however, depend on secret keys and rely on the limited computational power of eavesdroppers, as well as the reliability guaranteed by channel coding at the physical-layer design. These assumptions may not always hold since devices with high computational power are getting cheaper and widespread. Moreover, they become expensive and difficult to achieve as the network scales [9,11]. In this context, physical-layer security comes as a promising alternative to complement cryptographic solutions, by adding not only security at the physical-layer with strategies that guarantee reliability, but also confidentiality regardless of eavesdroppers' computational power [9,11].

Another interesting solution when dealing with wireless communication over multiple hops are the well-known cooperative relaying strategies [12,13]. As pointed out in [12], such schemes are robust to fading and interference impairments due to the enhanced diversity. Additionally, as discussed in [14,15,16], cooperative diversity schemes also enhance the performance of networks secured at the physical-layer.

All in all, the existence of multiple hops, interferers and eavesdroppers further complicate the design of wireless communication systems in industrial applications. Fig. 1 exemplifies an industrial deployment, where several sensors communicate to an aggregator (black node), which by its turn communicates via relays with the control unit (blue node). For instance, an aggregator can act as a relay and help to convey the information to the control unit. The legitimate link is composed by an aggregator (black node), relays (green nodes) and the control unit (blue node). All other randomly distributed nodes in the network are assumed to be either interferers (white nodes) or (potential) eavesdroppers (red nodes).

We assume that sensors are scattered throughout the industrial facility to measure relevant information, which is processed by an aggregator node and then sent to the control unit. Note that the sensor measurements, their communication with the aggregator and the information processing are all assumed to be perfect. To reach the control unit, the message may travel through relay nodes, forming a multi-hop, wireless link. At every hop, eavesdropper nodes attempt to acquire the messages transmitted through the legitimate link.

For instance, the aggregator could attempt a single transmission via long hops, which means that the channel is used less times and then there is a lower chance of the message being decoded by the eavesdropper. At the same time this increases the chance that an eavesdropper, which is closer to the transmitter than the desired receiver, intercepts and acquires the information being transmitted.

As we can observe, there are trade-offs regarding possible eavesdropper locations, number of hops, transmit power and decoding capabilities, which are function of the interference level perceived at the receivers. To assess such trade-offs, we introduce a tractable model based on stochastic geometry [17–20] to characterize the uncertainty related to interferers (jammers) and eavesdroppers positions and then proceed with a throughput optimization subject to a secrecy constraint. Moreover, similar to [21], we model the location of the eavesdroppers as a Poisson point process, due to the uncertainty of their presence and position.

Often in the literature [14,15,16,22] Wyner encoding schemes are adopted together with the notion of secrecy capacity. Conversely, herein we adopt conventional encoding schemes, thus practical coding schemes (such as BCH, and low-density-parity-check codes) in order to evaluate the performance of the network. Our goal is to show that some level of security can be achieved even with conventional coding, raising a more practical implementation aspect for physical layer security. A similar approach has been reported in [23,24], where information-theoretic security metrics are attained based on conventional codes, imposing guarantees on the eavesdropper error probability.

Then, the main contributions of this paper can be summarized as follows:

- Analysis of the throughput of industrial communication networks under a secrecy constraint by employing a model that characterizes the uncertainty related to interferers (jammers) and eavesdroppers' positions, accounting for conventional and more practical coding schemes[1]
- Closed-form solutions for the optimal multi-hop throughput considering or not the secrecy constraint as a function of network parameters.
- Identification of the operational regions proving that the optimal throughput subject to the secrecy constraint achieves the optimal performance if a feasible solution exists.

It is worth saying that this work is novel in the sense the legitimate link is unaware of both the positions and the number of

[1] An overview of state of the art on physical layer security schemes based on Wyner encoding and secrecy capacity metrics can be found in [9,11]. Distinct secrecy capacity-based metrics and applications can be found in [14,15,16,22].

eavesdroppers. As mentioned before, these uncertainties are quantified using stochastic geometry by modeling the eavesdroppers positions as a Poisson point process.

The remainder of this paper is organized as follows: Section 2 introduces the system model and the main metrics used to evaluate the performance of the network. Sections 3 and 4 evaluate the trade-offs involved in the design and deployment of the network. Both sections offer comprehensive numerical results and discussions. Next, Section 5 contextualizes our results and current industrial standards. Finally, in Section 6 conclusions and final remarks are drawn.

2. System model

Let $D > 0$ be the distance from the aggregator to the central unit, assuming that there exist in-between relay nodes employing a decode-and-forward strategy [12]. We consider that the relay nodes are deployed in the straight line defined by the aggregator and the central unit such that the distance $d > 0$ between any two nodes is the same. The number of hops is then computed as $h = D/d$. We assume that randomly scattered nodes attempt to jam the communication between the aggregator and the central unit. Then, if we assume that the jamming signals experienced by each receiver node along the multi-hop link are independent, the respective throughput $\mathcal{T}$, with respect to the multi-hop link, can be computed as [8]:

$$\mathcal{T} = \frac{\log(1+\beta)}{h}\,(P_{\text{suc}})^h, \tag{1}$$

where P_{suc} is the probability that the message is successfully decoded by the receiver and $\beta > 0$ is the minimum required SIR for a successful reception. If we assume point-to-point Gaussian codes and interference-as-noise decoding rule [25], the spectral efficiency of $\log(1+\beta)$, measured in bits/s/Hz, in the single-hop links is achievable if SIR $> \beta$.

If the network designer chooses one long hop $h = 1$, the throughput is $\log(1+\beta)\,P_{\text{suc}}$. If more hops are desired, then more network resources are required and the overall spectral efficiency decreases in relation to the number of hops (i.e. the same information is transmitted at the expense of more channel usage). Nevertheless, if more hops are added, P_{suc} is expected to increase. These contradictory effects are captured by (1).

We assume a field of jammers (malicious interferers) that is characterized by a 2-dimension uniform Poisson point process Φ_{int} with intensity $\lambda_{\text{int}} > 0$, measured in transmitters per unit of area [17]. We assume that the channel has two components: one related to the distance-dependent path-loss such that the received power decays with the distance and other related to fading. The received power at the node of interested can be computed as $g_i r_i^{-\alpha}$, where r_i is the distance between the reference receiver and the ith node, g_i is the channel gain between them, and $\alpha > 2$ the path-loss exponent [26].

We consider the communication occurs on a time-slot basis so that the slot length is the time required to transmit one packet [27]. If the nodes' positions and the channel gains do not change during the packet transmission, the signal-to-interference ratio (SIR) is computed as[2]

$$\text{SIR} = \frac{g_0 d^{-\alpha}}{\sum_{i\in\Phi_{\text{int}}} g_i r_i^{-\alpha}}. \tag{2}$$

To compute P_{suc}, we assume that the channel gains g_i are independent and identically distributed exponential random variables (Rayleigh fading) and that the interferers' positions change every time slot. In this way, each time-slot is a different realization of the point processes Φ_{int} and the channel gains g_i. From this assumptions, the success probability is [17]:

$$P_{\text{suc}} = e^{-\lambda_{\text{int}}\kappa\pi d^2\beta^{2/\alpha}}, \tag{3}$$

where $\kappa = \Gamma(1+2/\alpha)\Gamma(1-2/\alpha)$.

Let us now consider that there are eavesdroppers that are capable of decoding the transmitted messages if the SIR experienced by them are greater than the threshold $\beta_{\text{eav}} > 0$.[3] Their spatial distribution are modeled as a 2-dimensional uniform Poisson point process Φ_{eav} with intensity $\lambda_{\text{eav}} > 0$, measured in eavesdroppers per unit of area. The channel gains in relation to the transmitter are modeled as in the interferers' process described above (quasi-static Rayleigh fading and distance-dependent path-loss). As before, a different realization of the point process and channel gains are assumed at every different time-slot. In this scenario, due to the lack of any side information regarding the specific position and the channel gains, it is not possible to guarantee 100% of secrecy in the communication of the desired link.

Herein, we assume a secrecy constraint referring to the aggregator–control unit multi-hop link. In this case, the probability that the eavesdropper illegitimately acquires the message should be, statistically, lower than or equal to ϵ%. To compute such a probability, we need to evaluate the outage probability in the eavesdropper.[4] The probability density function $f_{R_1}(r)$ of distance r between an arbitrary point to the closest point of a Poisson point process with intensity λ_{eav} is given by [17]:

$$f_{R_1}(r) = \lambda_{\text{eav}}\, 2\pi r e^{-\lambda_{\text{eav}}\pi r^2}. \tag{4}$$

Similar to (3), the outage probability $P_{\text{out: eav}}$ (i.e. the probability that the packet is not successfully decoded) at the eavesdropper can be computed as [17]:

$$\begin{aligned} P_{\text{out:eav}} &= \mathbb{E}_r\left[1 - e^{-\lambda_{\text{int}}\kappa\pi r^2(\beta_{\text{eav}})^{2/\alpha}}\right] \\ &= \frac{\lambda_{\text{int}}\kappa(\beta_{\text{eav}})^{2/\alpha}}{\lambda_{\text{int}}\kappa(\beta_{\text{eav}})^{2/\alpha} + \lambda_{\text{eav}}}, \end{aligned} \tag{5}$$

where $\mathbb{E}_r[\cdot]$ is the expected value in regard to the distance r given by (4).

We are now ready to state the optimization problem of interest as follows: *What are the hop length d and SIR threshold β that jointly optimize the multi-hop throughput $\mathcal{T}$ given by (1) while the secrecy constraint ϵ is satisfied?* Mathematically, we have the following:

$$\begin{aligned} \max_{(\beta,d)} \quad & \mathcal{T} = \frac{d\log(1+\beta)}{D}\left(e^{-\lambda_{\text{int}}\kappa\pi d^2\beta^{2/\alpha}}\right)^{D/d} \\ \text{s.t.} \quad & d \le D \\ & \left(\frac{\lambda_{\text{int}}\kappa(\beta_{\text{eav}})^{2/\alpha}}{\lambda_{\text{int}}\kappa(\beta_{\text{eav}})^{2/\alpha} + \lambda_{\text{eav}}}\right)^{D/d} \ge 1-\epsilon \end{aligned}, \tag{6}$$

where the constraint is the probability that the eavesdropper links are in outage at every hop of the multi-hop link with a probability greater than equal to $1-\epsilon$.

3. Unconstrained optimization

Let us start presenting the solution of the unconstrained optimization problem assuming that the number of hops h can be

[2] We assume here interference-limited networks. As pointed in [28], the inclusion of the noise power leads to a more complex analysis without providing any significant qualitative difference.

[3] This threshold may reflect how powerful the eavesdroppers are: a low β_{eav} indicates that the eavesdroppers are able to successfully decode messages even with low SIR, reflecting a powerful decoding scheme.

[4] In fact this is an approximation since there will be closer eavesdroppers that experience a better channel. This, however, is a good approximation and holds in most of the cases for the spatial densities considered here since the probability that the closest eavesdropper cannot decode the message while any other can is very low [18].

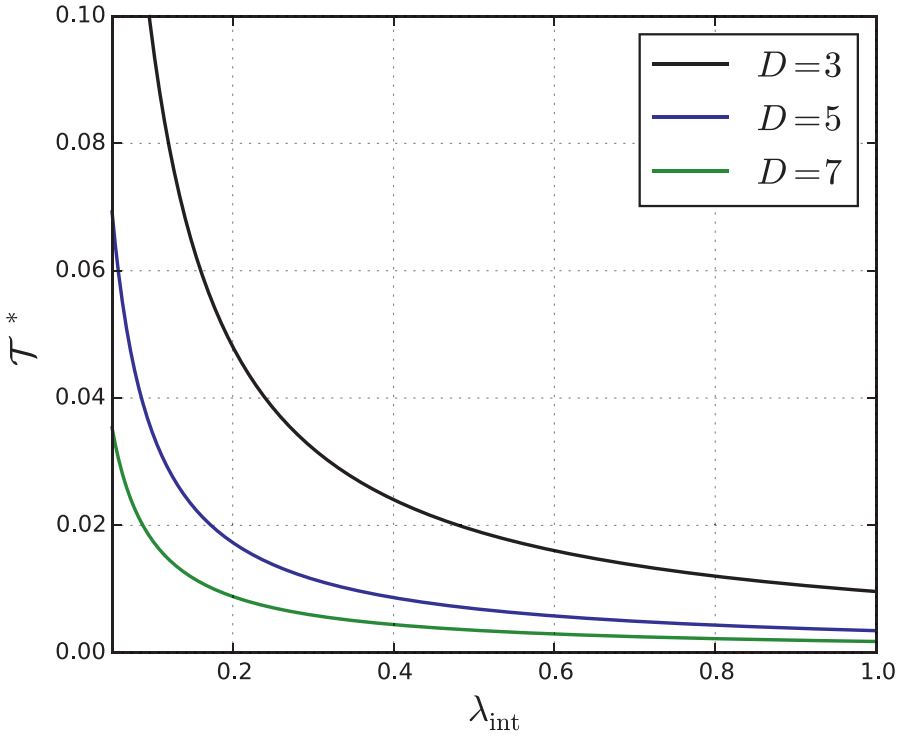

Fig. 2. Optimal multi-hop throughput $\mathcal{T}^*$, given by (9), as a function of the density of interferers λ_{int} for different values of multi-hop distance D, considering $\alpha = 4$.

a real number so that the hop length d can assume any positive value for a given D.

Proposition 1. *The pair (β^*, d^*) of the unconstrained version of the optimization problem given by (6) is:*

$$\beta^* = -1 + e^{\mathcal{W}_0\left(-\frac{\alpha}{2}e^{-\alpha/2}\right)+\frac{\alpha}{2}} \tag{7}$$

$$d^* = \frac{1}{D\lambda_{\text{int}}\kappa\pi\,(\beta^*)^{2/\alpha}}, \tag{8}$$

where $\mathcal{W}_0(\cdot)$ is the principal branch of the Lambert W function[5] [27], which is defined as $x = \mathcal{W}_0(x)e^{\mathcal{W}_0(x)}$ such that $x \geq -e^{-1}$ and $\mathcal{W}_0(x) \geq -1$.

The optimal throughput $\mathcal{T}^*$ is then:

$$\mathcal{T}^* = \frac{\log\left(e^{\mathcal{W}_0\left(-\frac{\alpha}{2}e^{-\alpha/2}\right)+\frac{\alpha}{2}}\right)}{e\log(2)D\lambda_{\text{int}}\kappa\pi\left(-1+e^{\mathcal{W}_0\left(-\frac{\alpha}{2}e^{-\alpha/2}\right)+\frac{\alpha}{2}}\right)}. \tag{9}$$

Proof. (Outline of proof). The first step is to show that multi-hop throughput $\mathcal{T}$ in (6) is a quasi-concave function in terms of both d and β. Then, the pair (β^*, d^*) that leads to the optimal unconstrained throughput $\mathcal{T}^*$ can be found as the joint solution of the following partial derivative equations $\partial\mathcal{T}/\partial d = 0$ and $\partial\mathcal{T}/\partial\beta = 0$.

Solving that system of equation, we find the equilibrium point (β^*, d^*) that is given by (7) and (8). Inserting these values into multi-hop throughput given by (6), we obtain equation (9). □

Fig. 2 exemplifies how the optimal throughput $\mathcal{T}^*$ varies with the density of interferers λ_{int} for different multi-hop distances D. One can see that the lower densities λ_{int} yields higher optimal throughputs, regardless of the multi-hop distance considered. Looking at the multi-hop distances, we find that the lower the distance D, the higher the throughput $\mathcal{T}^*$.

[5] We have used the function LambertW(·) from the library SymPy [29].

Although those results are somehow expected, it is interesting to analyze the reasons behind this behavior, which will later help us to understand the solution of the constrained optimization. From (7), the optimal value of β^* is independent of any other parameter of the system, but the path-loss exponent α, which is not under the designer control. Therefore, β^* is fixed if α is fixed and the single-hop distance d^* is the variable that changes with λ_{int} and/or D, as indicated by (8).

Eq. (9) shows that the optimal throughput $\mathcal{T}^*$ is inversely proportional to λ_{int} and D. It is worth noting that for small values of D and/or λ_{int}, $\mathcal{T}^*$ tends to infinity. This is a byproduct of our assumptions and clearly does not represent actual scenarios. Although, we understand this limitation, we still believe that the simplicity of our results can provide clear, and reasonable, guidelines on the network design.

When the same λ_{int} is considered, the optimal throughput $\mathcal{T}^*$ is determined only by D: if a packet needs to travel longer source-destination distances, the single-hops should be surprisingly smaller to support the optimal coding rate β^*. This happens because the smaller the single-hop distance, the higher the SIR experienced by the receiver nodes. In this case, having more shorter hops is statistically more advantageous than having less longer hops. A similar analysis is also valid when assessing the case when the same multi-hop distance is assumed D and the intensity λ_{int} is varying.

Although the results showing that longer distances D and higher intensity of interferer nodes λ_{int} degrade the throughput are expected, the design choices (β^*, d^*) that optimize the multi-hop throughput $\mathcal{T}$ are rather surprising. In the next section, we will see how the secrecy constraint will affect the optimal system design.

4. Constrained optimization

Let us now focus on the optimization problem subject to the secrecy constraint stated in (6). We first recall that the network

designer does not have any control on the eavesdropper parameters so that λ_{eav} and β_{eav} are input variables (i.e. external factors).

Lemma 1. *The secrecy constraint given by (6) can be rewritten as*

$$d \leq d_c \leq D, \tag{10}$$

where the new constraint d_c is given by:

$$d_c = \frac{D \log\left(\frac{\lambda_{int}\kappa(\beta_{eav})^{2/\alpha}}{\lambda_{int}\kappa(\beta_{eav})^{2/\alpha}+\lambda_{eav}}\right)}{\log(1-\epsilon)}. \tag{11}$$

Proof. We start by manipulating the secrecy constraint from (6) as follows:

$$\frac{D}{d}\log\left(\frac{\lambda_{int}\kappa(\beta_{eav})^{2/\alpha}}{\lambda_{int}\kappa(\beta_{eav})^{2/\alpha}+\lambda_{eav}}\right) \geq \log(1-\epsilon) \Rightarrow$$

$$\Rightarrow \frac{D \log\left(\frac{\lambda_{int}\kappa(\beta_{eav})^{2/\alpha}}{\lambda_{int}\kappa(\beta_{eav})^{2/\alpha}+\lambda_{eav}}\right)}{\log(1-\epsilon)} \geq d. \tag{12}$$

We now use the fact that the single-hop must have a length lower than or equal to the multi-hop $d \leq D$ and that the distances are strictly positive to conclude this proof. □

Proposition 2. *The solution of the constrained optimization problem stated in (6) is given in Proposition 1 with* $\log(\frac{\lambda_{int}\kappa(\beta_{eav})^{2/\alpha}}{\lambda_{int}\kappa(\beta_{eav})^{2/\alpha}+\lambda_{eav}}) \leq \log(1-\epsilon) \leq D^2\lambda_{int}\kappa\pi(\beta_{eav})^{2/\alpha}\log(\frac{\lambda_{int}\kappa(\beta_{eav})^{2/\alpha}}{\lambda_{int}\kappa(\beta_{eav})^{2/\alpha}+\lambda_{eav}})$.

Proof. Let us start by considering the second part of the secrecy constraint given by Lemma 1, namely $d_c \leq D$. If $\log(\frac{\lambda_{int}\kappa(\beta_{eav})^{2/\alpha}}{\lambda_{int}\kappa(\beta_{eav})^{2/\alpha}+\lambda_{eav}}) > \log(1-\epsilon)$, then $d_c > D$, the secrecy constraint is then violated and the problem has no feasible solution.

In the case where $\log(\frac{\lambda_{int}\kappa(\beta_{eav})^{2/\alpha}}{\lambda_{int}\kappa(\beta_{eav})^{2/\alpha}+\lambda_{eav}}) \leq \log(1-\epsilon)$, we need to verify the constraint $d \leq d_c$. As stated in Proposition 1, the optimal choice of β^* only depends on α. Therefore we focus on the optimal single-hop distance d^* given by (8): the optimal solution can be only obtained if the inequality $d^* = \frac{1}{D\lambda_{int}\kappa\pi(\beta^*)^{2/\alpha}} \leq d_c$ is satisfied. □

Corollary 1. *The solution of the constrained optimization problem stated in (6) does not exist if* $\log(\frac{\lambda_{int}\kappa(\beta_{eav})^{2/\alpha}}{\lambda_{int}\kappa(\beta_{eav})^{2/\alpha}+\lambda_{eav}}) > \log(1-\epsilon)$ *and then* $\mathcal{T}^* = 0$.

Proof. This proof follows from the first part of the proof of Proposition 2, when $\log(\frac{\lambda_{int}\kappa(\beta_{eav})^{2/\alpha}}{\lambda_{int}\kappa(\beta_{eav})^{2/\alpha}+\lambda_{eav}}) > \log(1-\epsilon)$ implies that the problem has no feasible solution. □

Remark 1. In the scenarios under investigation, the inequality $d^* \leq d_c$ holds due to the combination of the system parameters and target variables.

From this remark and the analytic results previously stated, the solution of optimization problem with secrecy constraint only depends on the relation between d_c and the multi-hop distance D for the cases studied here. More specifically, Corollary 1 tells us that the optimal solution exists if the secrecy constraint ϵ is achievable for the network density of interferers λ_{int}, density of eavesdroppers λ_{eav} and their SIR threshold β_{eav} considered.

Fig. 3 (presented in the next page) shows the distance constraint d_c as a function of the eavesdroppers' SIR threshold β_{eav} for different combination of densities λ_{int} and λ_{eav}. One can see that lower SIR thresholds β_{eav} cause the unfeasibility of the optimal solution. As expected, if the eavesdroppers are able to decode messages with low SIR, then their chance of correctly decoding the information of the legitimate link grows, regardless of the densities λ_{int} and λ_{eav}.

The effects of λ_{int} and λ_{eav} are the following. The higher the density of eavesdroppers λ_{eav}, the stricter is the distance constraint d_c. This is due to the fact that big values of λ_{eav} lead to greater probabilities that a eavesdropper node is closer to the legitimate link. This, in turn, requires a more stringent d_c to satisfy the secrecy constraint ϵ.

The increase of the density of interferers λ_{int}, on the other hand, helps the secrecy of the legitimate link. This is in line with the general literature on physical layer security (e.g. [22]) since higher λ_{int} leads to probabilistically lower SIR. This will then result in more outages in the eavesdropper links, making the distance constraint d_c less stringent.

Fig. 4 shows an example of the optimal constrained multi-hop throughput,[6] in relation to the unconstrained case. The optimal multi-hop throughput $\mathcal{T}^*$ is plotted as a function of λ_{int} for $D = 3$, $\alpha = 4$ and $\epsilon = 10\%$. One can verify that the constrained optimization can achieve the unconstrained performance if the solution of the problem is within its feasibility region, which can be analytically determined as predicted in Corollary 1.

5. Implementation and deployment aspects

As previously mentioned, the scenario under analysis is a simplified, abstract, version of an actual industrial communication network. In any case, we would like to reinforce the value of our results, which are simple enough to characterize important trade-offs on the system design. In the proposed model, we do not assume any information about interferers and (malicious) eavesdroppers, which might be a more practical consideration. For example, the design of a physical-layer secured network assumes some information about eavesdroppers as in [9,11]. Therein, each transmitter attempts to convey its message in a reliable and confidential way, once they are aware that non-intended receivers may be overhearing their transmission. In the case of interference, there are well-established approaches that use the channel and/or location information to increase the system throughput.

In what follows, we briefly discuss some of the major standardization efforts, which could benefit from our results. For instance, ZigBee (IEEE 802.15.4) and Bluethooth (Low Energy) network standards serve not only for industrial applications, but also for home automation for instance [7,31]. Both standards are low-power and have limited communication range (few tens of meters in indoor environments), and thus could take advantage of our guidelines: a large number of hops in short range communication is preferable over long hops. Another possible alternative for wireless industrial is WirelessHART [31], which has already embedded functionalities that allow information relaying.

It is worthy noting that our discussions so far are based on industrial environments; however, our results also extend to modern (smart) power grids due to the similarities of the communication environment. For instance, smart grids also present a distinct profile of interference due to the highly reflective materials and electromagnetic interference from the machinery, especially at the distribution side. Besides, communication links suffer additional interference from concurrent transmissions from neighboring devices and aggregations as discussed in [32]. This initial assessment is then extended in order to include not only reliability analysis but also security and privacy in [33]. This evinces the potential applications and relevance of our results.

[6] To solve the constrained optimization, we have used the numerical function fmin_l_bfgs_b from the library SciPy [30].

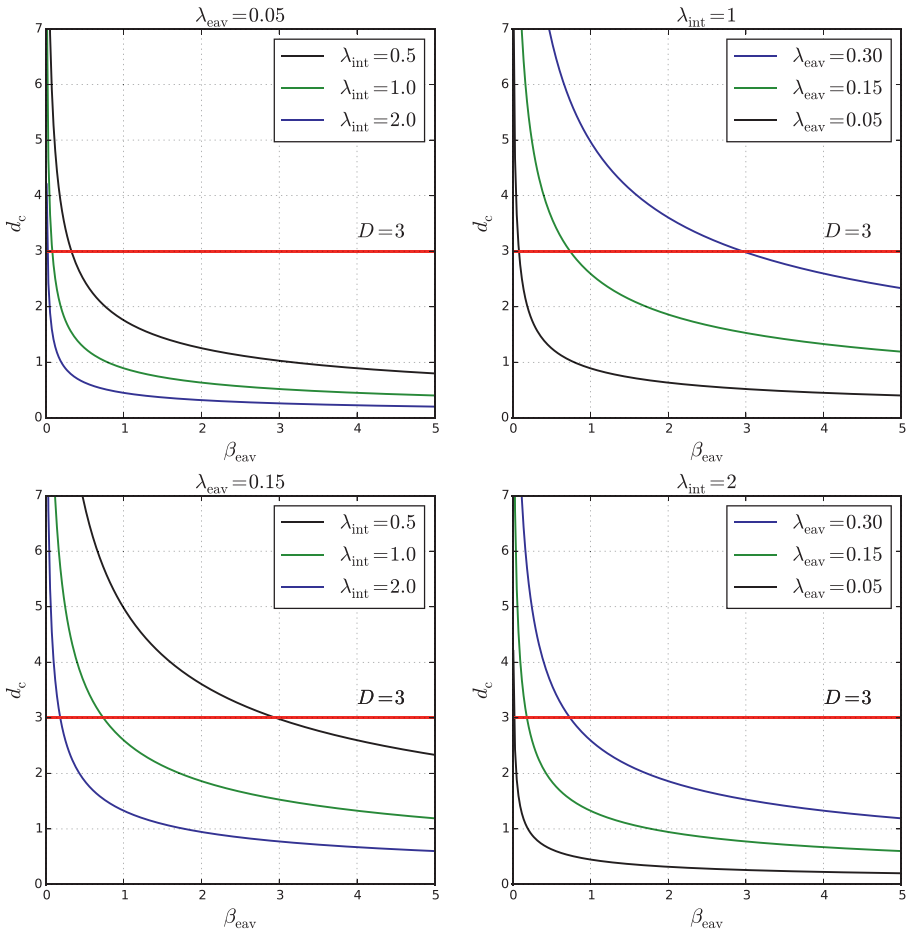

Fig. 3. Distance constraint d_c as a function of the eavesdroppers' SIR threshold β_{eav} for different combination of densities λ_{int} and λ_{eav}, assuming the path-loss exponent $\alpha = 4$ and secrecy constraint $\epsilon = 10\%$. We consider the multi-hop distance $D = 3$ that is presented by the red line. When the $d_c \leq D = 3$, then the optimal solution of (6) exists and it is given by Proposition 1.

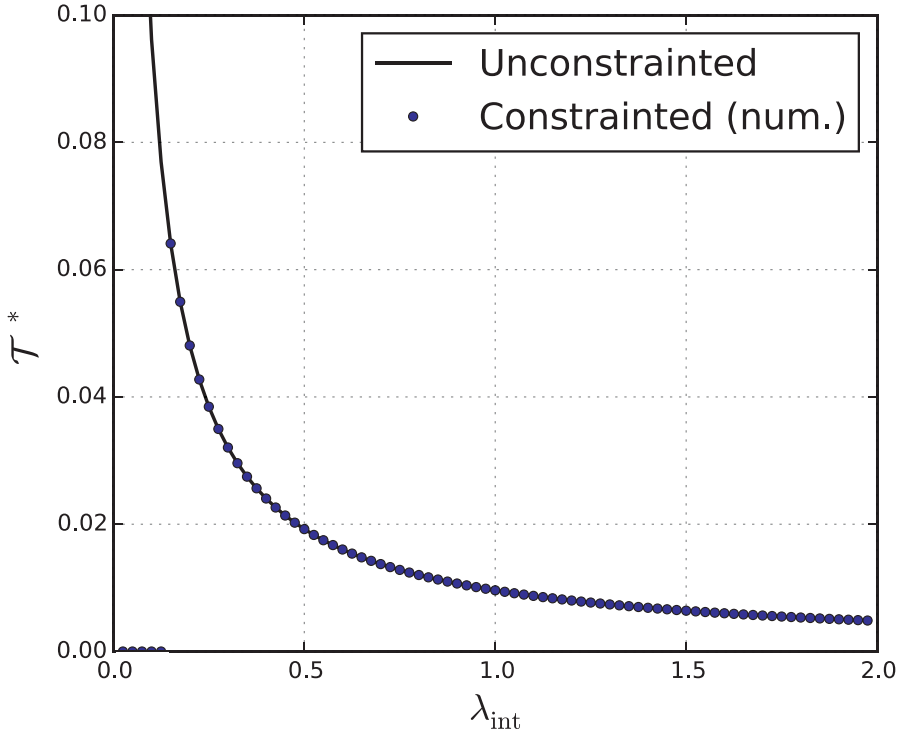

Fig. 4. Optimal multi-hop throughput $\mathcal{T}^*$ as a function of the density of interferers λ_{int} for $D = 3$, $\alpha = 4$ and $\epsilon = 10\%$. We consider the unconstrained optimization given by (9) and the numerical solution of (6).

6. Conclusions and final remarks

This paper analyzes the throughput of industrial multi-hop machine-to-machine networks under a secrecy constraint subject to malicious jamming. The scenario under analysis consists in an aggregator node, which collects and processes the sensor measurements, and a control unit that needs the proceeded information. This communication is wireless and may occur over multiple hops, and the communication engineer is expected to find the optimal position of the relay nodes and the coding rates used in the single-hop links so as to maximize the throughput in [bits/s/Hz] while respecting a given secrecy constraint and accounting for malicious jamming.

By employing our stochastic-geometric-based model to characterize the uncertainties involved in the eavesdroppers' and jammers' positions, we first showed that the optimal choice without any secrecy constraint of coding rate (spectral efficiency) depends only on the path-loss exponent and normally assumes a high value. To sustain such a high rate, a great number of shorter hops are then preferable to a small number of longer hops. When the secrecy constraint is assumed, we proceeded with the throughput optimization and proved that the unconstrained performance can be achieved with the same optimal relay positions and coding rates only if a feasible solution exists. Otherwise, there is no solution for the problem that satisfies the minimum level of secrecy required.

As a next step, we expect to evaluate our guidelines in actual industrial environments by following the insights provided herein. To do so, we aim at designing a feasible experimental deployment that utilizes established standards for industrial wireless systems. It is also important to point out that, although this analysis has been presented focusing on industrial deployments, our framework can be also extended to different kind of smart applications such as homes, cities, energy grids or highways.

Acknowledgments

The authors also would like to thank Aka and Infotech Oulu Graduate School from Finland, CNPq 490235/2012-3, and Strategic Research Council/Aka BCDC Energia project (n.292854).

References

[1] P. Stenumgaard, et al., Challenges and conditions for wireless machine-to-machine communications in industrial environments, IEEE Commun. Mag. 51 (6) (2013) 187–192.
[2] I. Stojmenovic, Machine-to-machine communications with in-network data aggregation, processing, and actuation for large-scale cyber-physical systems, IEEE Internet Things J. 1 (2) (2014) 122–128, doi:10.1109/JIOT.2014.2311693.
[3] H. Goh, et al., Development of bluewave: A wireless protocol for industrial automation, IEEE Trans. Ind. Inf. 2 (4) (2006) 221–230, doi:10.1109/TII.2006.885186.
[4] A. Rajandekar, B. Sikdar, A survey of MAC layer issues and protocols for machine-to-machine communications, IEEE Internet Things J. Early Access (99) (2015) 1.
[5] A. Osseiran, et al., Scenarios for 5G mobile and wireless communications: The vision of the METIS project, IEEE Commun. Mag. 52 (5) (2014) 26–35.
[6] F. Boccardi, et al., Five disruptive technology directions for 5G, IEEE Commun. Mag. 52 (2) (2014) 74–80, doi:10.1109/MCOM.2014.6736746.
[7] V. Gungor, G. Hancke, Industrial wireless sensor networks: Challenges, design principles, and technical approaches, IEEE Trans. Ind. Electron. 56 (10) (2009) 4258–4265.
[8] P.H.J. Nardelli, et al., Efficiency of wireless networks under different hopping strategies, IEEE Trans. Wireless Commun. 11 (1) (2012) 15–20, doi:10.1109/TWC.2011.111211.101963.
[9] Y. Shiu, et al., Physical layer security in wireless networks: A tutorial, IEEE Wireless Commun. 18 (2) (2011) 66–74.
[10] C. Kaufman, et al., Network security: Private communication in a public world, 2 edition, Prentice Hall, Upper Saddle River, NJ, USA, 2002.
[11] A. Mukherjee, et al., Principles of physical layer security in multiuser wireless networks: A survey, Commun. Surveys Tuts. 16 (3) (2014) 1550–1573.
[12] F. Gomez-Cuba, et al., A survey on cooperative diversity for wireless networks, Commun. Surv. Tut. 14 (3) (2012) 822–835.
[13] F. Mansourkiaie, M. Ahmed, Cooperative routing in wireless networks: A comprehensive survey, Commun. Surv. Tut. PP (99) (2015), doi:10.1109/COMST.2014.2386799. 1–1.
[14] Y. Zou, et al., Improving physical-layer security in wireless communications using diversity techniques, IEEE Netw. 29 (1) (2015) 42–48.
[15] H. Alves, et al., On the performance of secure full-duplex relaying under composite fading channels, IEEE Sig. Process. Lett. 22 (7) (2015) 867–870.
[16] T.X. Zheng, H.M. Wang, F. Liu, M.H. Lee, Outage constrained secrecy throughput maximization for df relay networks, IEEE Trans. Commun. 63 (5) (2015) 1741–1755.
[17] M. Haenggi, Stochastic geometry for wireless networks, Cambridge University Press, Cambridge, UK, 2012.
[18] F. Baccelli, B. Blaszczyszyn, Stochastic geometry and wireless networks: Theory, NOW 3 (3–4) (2009) 249–449.
[19] F. Baccelli, B. Blaszczyszyn, Stochastic geometry and wireless networks: Applications, NOW 4 (1–2) (2009) 1–312.
[20] A. Baddeley, Spatial point processes and their applications, in: Stochastic Geometry, Springer, 2007, pp. 1–75.
[21] T.X. Zheng, H.M. Wang, J. Yuan, D. Towsley, M.H. Lee, Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers, IEEE Trans. Commun. 63 (11) (2015) 4347–4362.
[22] H. Alves, et al., On the secrecy of interference-limited networks under composite fading channels, IEEE Sig. Process. Lett. 22 (9) (2015) 1306–1310.
[23] J.P.V.M.G. Willie K. Harrison, Dinis Sarmento, Analysis of short blocklength codes for secrecy, ArXiv: http://arxiv.org/abs/1509.07092 (2015).
[24] J.P. Vilela, M. Gomes, W.K. Harrison, D. Sarmento, F. Dias, Interleaved concatenated coding for secrecy in the finite blocklength regime, IEEE Sig. Process. Lett. 23 (3) (2016) 356–360.
[25] F. Baccelli, et al., Interference networks with point-to-point codes, IEEE Trans. Inf. Theory 57 (5) (2011) 2582–2596, doi:10.1109/TIT.2011.2119230.
[26] H. Inaltekin, et al., On unbounded path-loss models: Effects of singularity on wireless network performance, IEEE J. Sel. Areas Commun. 27 (7) (2009) 1078–1092, doi:10.1109/JSAC.2009.090906.
[27] P.H.J. Nardelli, et al., Throughput optimization in wireless networks under stability and packet loss constraints, IEEE Trans. Mob. Comput. 13 (8) (2014) 1883–1895.
[28] S. Weber, et al., An overview of the transmission capacity of wireless networks, IEEE Trans. Commun. 58 (12) (2010) 3593–3604.
[29] URL http://docs.sympy.org/0.7.1/modules/mpmath/functions/powers.html.
[30] URL http://docs.scipy.org/doc/scipy/reference/generated/scipy.optimize.fmin_l_bfgs_b.html.
[31] K. Al Agha, et al., Which wireless technology for industrial wireless sensor networks? The development of OCARI technology, IEEE Trans. Ind. Electron. 56 (10) (2009) 4266–4278, doi:10.1109/TIE.2009.2027253.
[32] P.H.J. Nardelli, et al., Maximizing the link throughput between smart meters and aggregators as secondary users under power and outage constraints, Ad-hoc Netw. PP (99) (2015) 1–20.
[33] H. Alves, et al., Enhanced transmit antenna selection scheme for secure throughput maximization without CSI at the transmitter and its applications on smart grids, IEEE Trans. Inf. Forensics Security (2015). Submitted.

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. In 2013 he received his doctoral degree from University of Oulu, Finland, and State University of Campinas following a dual-degree agreement. Nowadays he holds a postdoctoral position at University of Oulu, and his studies are mainly focused on the efficiency of wireless networks and spatio-temporal dynamics of complex systems.

Hirley Alves received the B.Sc., M.Sc. and D.Sc. degrees from Federal University of Technology – Paranß (UTFPR), Brazil, in 2010, 2011 and 2015, respectively. Hirley has jointly graduated from University of Oulu, and received his D.Sc. in 2015. Hirley is postdoctoral researcher at Centre for Wireless Communications (CWC), Oulu. His current research focuses on: performance analysis of full-duplex networks and relaying and its applications on 5G, 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. In 2013 he is received his D.Sc. degree in of Telecommunications Engineering from University of Oulu, Finland. He is currently an assistant professor at São Paulo State University, São João da Boa Vista–SP, Brazil, and a member of the research staff with the Centre for Wireless Communications, University of Oulu. From 2000 to 2005, he was a Research Scientist with the Wireless Telecommunications Research Group (GTEL), Fortaleza. In 2005, he was a Visiting Researcher with the Ericsson Research Center, Lulea, Sweden, engaged in power control techniques for enhanced high-speed packet access systems. In 2006, he was with Nokia Institute of Technology (INdT), Brazil, engaged in the evaluation of the system performance of WiMAX systems. 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 at Nokia Mobile Phones, Oulu, Finland. During the years 1994 - 1998 he was a Research Scientist at Telecommunication Laboratory and Centre for Wireless Communications at the University of Oulu. Prof. Latva-aho was Director of Centre for Wireless Communications at the University of Oulu during the years 1998–2006. Currently he is the Chair of the Department of Communications Engineering and Professor of Digital Transmission Techniques at the University of Oulu.