Computer Networks 000 (2016) 1–8

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 xxx

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/

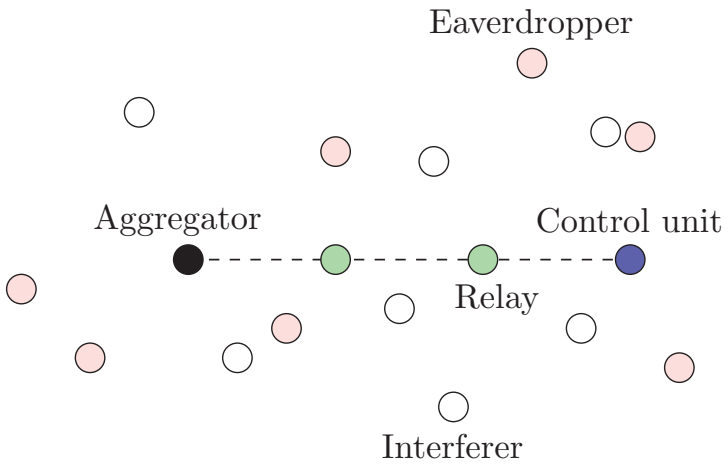

Fig. 1. Schematic example of the proposed scenario. The black node is the aggregator (source), the blue node is the control unit (destination) and the green nodes are the relays, all of them defining the legitimate link. The white nodes are the interferers while the red nodes are the eavesdroppers, which 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].

Please cite this article as: P.H.J. Nardelli et al., Throughput maximization in multi-hop wireless networks under a secrecy constraint, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.06.020