Collision-free Jamming for Enhanced Wireless Secrecy

João P. Vilela
CISUC, Department of Informatics Engineering
University of Coimbra, Coimbra, Portugal.
Email: jpvilela@dei.uc.pt

João Barros
Instituto de Telecomunicações
Departamento de Engenharia Electrotécnica e de Computadores
Faculdade de Engenharia da Universidade do Porto, Porto, Portugal.
Email: jbarros@fe.up.pt

***Abstract*—We present a collision-free jammer selection policy for enhanced wireless secrecy. Jammers, selected from the neighbors of a source, are friendly in the sense that they are willing to help the source to transmit securely by causing interference/collisions to possible eavesdroppers. The proposed jammer selection policy results in the selection of the largest number of jammers that do not cause collisions among themselves. This enables jammers to assist the source to transmit securely by causing interference to eavesdroppers, while sending their own traffic into the network.**

***Keywords*-wireless secrecy, physical-layer security, jamming, eavesdropping, interference, throughput-security tradeoffs.**

I. Introduction

Providing secrecy in wireless communications remains a significant challenge. In particular, even a small number of eavesdroppers was shown to dramatically reduce the ability to communicate securely [1], [2]. Recent contributions on physical-layer security suggest that the physical characteristics of wireless channels can be relied upon to enhance the secrecy level of these networks [3].

Physical-layer security sparked an interest on the use of otherwise silent devices (e.g. due to a time-division channel access mechanism) to cause interference to possible eavesdroppers in a shared wireless medium. These devices can be seen as jammers, but are considered friendly in the sense that their goal is to assist legitimate communication by causing interference to eavesdroppers, as illustrated in Figure 1. The idea of jamming for secrecy appeared in [4] and was extended in [5], whereby a transmitter with multiple antennas or, alternatively, a set of amplifying relays introduce noise in the system that results in low outage probabilities of secrecy capacity. In [6], a cooperative jamming scheme is proposed in which an otherwise disadvantaged user can help improve the secrecy rate by jamming a nearby eavesdropper. [7] presents a set of cooperation strategies for a relay node to improve the achievable secrecy rate. Interference-assisted secret communication in which an interferer improves the secrecy rate by injecting independent interference is considered in [8].

In [9], [10], we perform a system analysis of the impact of jamming on the secrecy level of wireless networks. The first contribution [9] provides insight on the optimal configurations of jammers under different levels of channel state information, showing that a single jammer is not sufficient to maximize secrecy objectives. The second contribution [10] considers multi-terminal environments and proposes a scheme for selection of jammers according to their location, showing that (i) contention of jammers near legitimate receivers is necessary, and (ii) there is a large energy-cost associated with jamming. In [11] we propose a jamming protocol that includes jammer selection policies leading to different levels of secrecy–energy trade-offs.

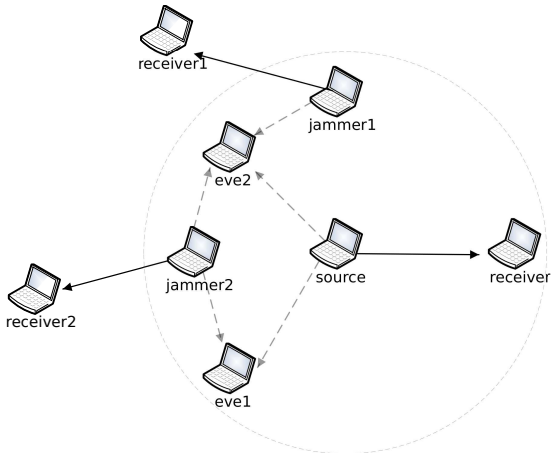


Figure 1. Example of a wireless network, where filled lines correspond to legitimate receptions, while dashed lines correspond overhearing of information by eavesdroppers. When the source transmits to its receiver, selected jammers can send traffic to their own receivers while causing interference/collisions on eavesdroppers eve1 and eve2.

A relay selection scheme for inter-session interference is proposed in [12]. Unlike previous contributions, this work provides secrecy from inter-session interference of regular devices, instead artificially generated interference. The proposed relay selection is not necessarily optimal with respect to some network metric (e.g. number of hops), and the maximum number of eavesdroppers allowed for a secrecy criterion to be achieved is derived asymptotically on the number of nodes in the network.

Our work also deals with inter-session interference, however it differs from [12] by providing a scheme where relays are selected as usual by a routing protocol that aims at optimizing a metric such as the hop count. Security comes, instead, by having the sources select a set of neighbor devices that can act as jammers while transmitting their own

traffic. Jammers are selected so as to avoid collisions among themselves, therefore causing interference to possible eavesdroppers while transmitting their own traffic. Our scheme is applicable to networks with finite number of devices and does not restrict the selection of relays.

In Section II we describe the system model considered and inherent assumptions. Section III presents the proposed scheme for selection of jammers that ensures the selection of the maximum number of jammers without collisions among themselves. This scheme is evaluated in Section IV, and Section V concludes the paper.

II. System model and assumptions

We consider a network composed of regular single antenna nodes and eavesdroppers (Eve). Among the regular nodes, we have packet transmitter nodes (Tx) and their corresponding receivers (Rx). During transmission from Tx other nodes remain silent (e.g. because of a time-division scheme for channel access) and can serve as jammers if called upon.

Our adversaries are eavesdroppers that are alien to the network operation. These eavesdroppers lie silently within network range and try to overhear as much information as possible. This maximizes the probability of successful eavesdropping, specially when wireless nodes are not able to transmit and receive simultaneously, as is usually the case. We consider that eavesdroppers are not able to collude and possess the same single-antenna capabilities as the other nodes. The effect of multiple antennas and collusion of eavesdroppers is considered in works such as [5].

We assume that the locations of eavesdroppers are unknown and treat them as uniformly distributed. This way, no specific eavesdropper location is favored, and the results obtained encompass a wide range of scenarios, ranging from less-favorable to more-favorable eavesdropper locations. We admit that this neglects the fact that continued transmission can give clues to the eavesdroppers about favorable spots. However, this can be prevented through the use of traffic anonymity schemes, such as [13].

The location of jammers is also assumed unknown. Although jammers may not be silent, their location is still unknown in the sense that they can be regular nodes communicating in the network, as is the case here. We assume that jammers are cooperative and honest, such that if they are asked to cause interference, they will do so. Moreover jammers are not interested in eavesdropping. Cooperation enforcement schemes are out of the scope of this paper, but some proposals exist in the context of mobile ad-hoc networks [14], [15].

For the selection of collision-free jammers by Tx, we view the network as a graph in which nodes are neighbors if they can communicate with one-another – information usually conveyed by routing protocols. Under this setup, we say that a collision occurs if two or more nodes transmit to a same neighbor destination.

This work on jamming for wireless secrecy finds applicability in spontaneous networks with unknown receivers, in which sharing a secret between devices for cryptography-based security may not be feasible. In this case, these techniques can be applied to reduce the probability that a malicious eavesdropper is able to overhear communication.

III. Collision-free data packet jamming

We now present a selection policy for the Tx to choose a set of neighbor devices to act as jammers. These jammers will cause interference by sending their own data concurrently with Tx. Successful communication requires that jammers (1) are selected so as to avoid causing interference to the legitimate receiver, as observed in [10], and (2) avoid causing collisions among themselves, this being assured by a *collision-free jammer selection policy*. The process of selection of jammers consists of three main steps:

1) selection of jammers by Tx through the collision-free jammer selection policy (illustrated in Figure 2);
2) selection of next-hops by the jammers;
3) generation and processing of jamming data packets.

The successful delivery of jamming data packets depends on every jammer to have at least one available neighbor that does not suffer collisions from other active jammers. We call such jammer a *collision-free node*. Also, since more jammers generally improve the secure throughput, we are interested in the largest set of such jammers. For that, we introduce the collision-free jammer selection policy.

A. Collision-free jammer selection policy

Let $\mathcal{C} = (\mathcal{N}, \mathcal{L})$ be a connectivity graph that represents links between nodes of the two-hop neighborhood of Tx in Figure 2 (i.e. possible jammers and their neighbors)[1], where $\mathcal{N}$ is the set of nodes, and $\mathcal{L}$ the set of links connecting those nodes. Also, let $nbs(i)$ represent the set of one-hop neighbors of a certain node i, and l_{ij} the link from source i to receiver j. We say that a collision happens if two links $l_{ij}, l_{ab} \in \mathcal{L}$ are active and $a \in nbs(j)$, or $i \in nbs(b)$.

Definition 1 (Collision-free node): We say that a node $i \in \mathcal{F}$ is collision-free in $\mathcal{F}$ if

$$\exists j \in nbs(i) : j \notin nbs(a), \forall a \in \mathcal{F} \backslash \{i\}.$$

This means that i is able to transmit to j without suffering a collision from any other transmitting node in $\mathcal{F}$. We also call the corresponding link l_{ij} a collision-free link.
The fact that a node is collision-free depends on the set of nodes $\mathcal{F}$ under consideration, and we are interested in the largest set of such nodes to be used as jammers.

The collision-free jammer selection policy relies on the concept of conflict graph [16]. The conflict graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is a graph whose vertices correspond to links in the connectivity graph $\mathcal{C}$. A vertex $l_{ij} \in \mathcal{V}$ is connected to another

[1]This selection policy requires knowledge of the two-hop neighborhood of Tx.

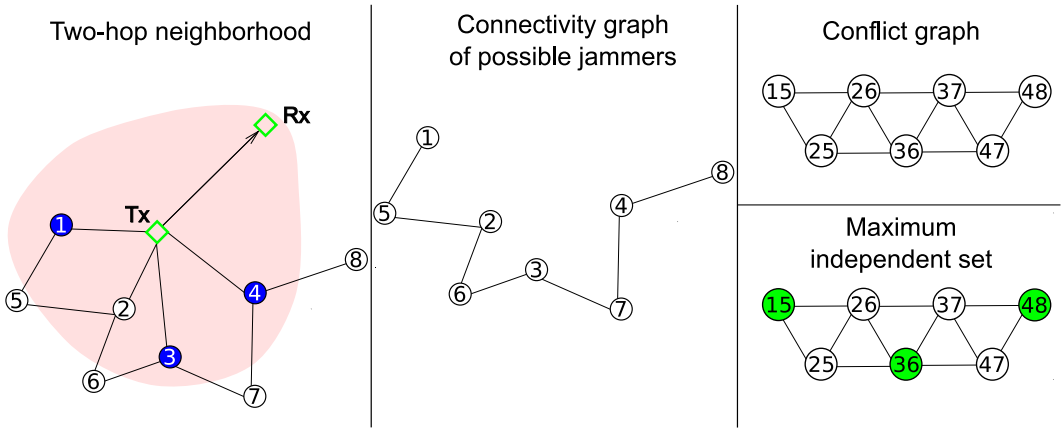


Figure 2. Operation of data packet jamming under collision-free jammer selection policy. The sequence of figures illustrates steps 1, 2, and 3 of Table I. Nodes in the shaded area on the left are the one-hop neighbors of Tx that may serve as jammers. Each node of the conflict graph corresponds to a link in the connectivity graph. Highlighted nodes in the maximum independent set graph are the determined collision-free links, and the corresponding collision-free jammers are highlighted in the two-hop neighborhood graph.

vertex $l_{ab} \in \mathcal{V}$ if both links cannot be active simultaneously, as this would lead to a collision. More formally, following the definition of collision-free node, the set of edges of $\mathcal{G}$ is

$$\mathcal{E} = \left\{ \overline{l_{ij} l_{ab}} : i \in nbs(b) \text{ in } \mathcal{C} \bigvee a \in nbs(j) \text{ in } \mathcal{C} \right\}. \quad (1)$$

For a set of links $\mathcal{W}$, we say that a link l_{ij} is collision-free if $\nexists l_{ab} \in \mathcal{W} \backslash \{l_{ij}\}$ such that $j \in nbs(a)$. If all links in $\mathcal{W}$ are collision-free, then all links in $\mathcal{W}$ can be scheduled for transmission simultaneously without any collision happening.

Definition 2 (Maximum independent set): An independent set, $\mathcal{I}$, of a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is a set of vertices from $\mathcal{V}$ such that there is no edge connecting any two vertices in $\mathcal{I}$. A maximal independent set is an independent set that is not a subset of any other independent set. A graph can have several maximal independent sets, and the largest of the maximal independent sets is the maximum independent set.

Proposition 1: The maximum set of collision-free nodes is the set of sources $\{i\}$ of all links l_{ij} belonging to the maximum independent set $\mathcal{I}^{\max}$ of a conflict graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where every vertex $l_{ij} \in \mathcal{V}$ is connected to every other vertex $l_{ik} \in \mathcal{V}$, for $k \neq j$.

Proof: The maximum independent set $\mathcal{I}^{\max}$ of a conflict graph is the maximum set of collision-free links. A collision-free link $l_{ij} \in \mathcal{W}$ is a link that does not suffer collision from any other link in $\mathcal{W}$, i.e. $\nexists l_{ab} \in \mathcal{W} \backslash \{l_{ij}\}$ such that $j \in nbs(a)$. According to this definition, $\mathcal{I}^{\max}$ can have multiple links with the same source, as these do not cause collisions among themselves.

We now create a modified conflict graph to rule out multiple links with the same source from $\mathcal{I}^{\max}$. This is achieved by creating edges in the conflict graph between all pairs of links with a common source, i.e. $(l_{ij}, l_{ik}) \in \mathcal{V} \times \mathcal{V}$, for $k \neq j$. The edge set of this modified conflict graph is then

$$\mathcal{E} = \left\{ \overline{l_{ij} l_{ab}} : i \in nbs(b) \text{ in } \mathcal{C} \quad \bigvee \quad a \in nbs(j) \text{ in } \mathcal{C} \right. \\ \left. \bigvee \quad (a = i \wedge j \neq b) \right\} \quad (2)$$

With this modified conflict graph, links from the same source cannot, by definition, belong to $\mathcal{I}^{\max}$. The maximum independent set of the conflict graph then becomes the maximum set of links with distinct sources that can be scheduled to transmit simultaneously without any collision happening. The maximum set of collision-free nodes then corresponds to the sources of links belonging to $\mathcal{I}^{\max}$ of a conflict graph with edge set (2). ■

The collision-free jammer selection policy relies on finding this set of collision-free jammers that can be scheduled to transmit simultaneously. The procedure is described in Table I.

Table I
COLLISION-FREE JAMMER SELECTION POLICY
(ILLUSTRATED IN FIGURE 2)

1) Tx creates a connectivity graph $\mathcal{C} = (\mathcal{N}, \mathcal{L})$ from the two-hop neighborhood, by omitting connections between possible jammers and jammers connected to Rx;
2) The connectivity graph is converted to a conflict graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with edge set (2);
3) The maximum independent set $\mathcal{I}^{\max}$ of the conflict graph is determined;
4) The collision-free jammers are given by the set of sources of links in the maximum independent set, $\{i : l_{ij} \in \mathcal{I}^{\max}\}$.

After determining the list of active jammers, the source can pass that information to the respective jammers through a S-RTS signaling message such as introduced in [11].

B. Selection of next-hop by jammers

Upon reception of the signaling message, all jammers are informed about the list of collision-free jammers, but not on

which neighbor to transmit to in order to form a collision-free link. This can, however, be distilled from the two-hop neighborhood information and the list of active jammers as follows.

Let $\mathcal{F}$ be the set of collision-free jammers received by a jammer node i through the signaling message. The possible next-hops forming a collision-free link from jammer i is given by the set of nodes

$$\{a \in nbs(i) : \underbrace{a \notin nbs(j)}_{(1)} \wedge \underbrace{j \notin nbs(a)}_{(2)}, \forall j \in \mathcal{F} \backslash \{i\}\}.$$

This gives the set of possible next-hops that (1) are not neighbors of any jammer, and (2) do not have jammers as neighbors. Condition (2) is relevant since two jammers may not be neighbors, thus making condition (1) unverifiable because $nbs(j)$ is not known. Condition (2) assumes reciprocity of wireless channels, such that if a jammer is not neighbor of a possible next-hop, the next-hop is also not a neighbor of the jammer and, therefore, will not suffer a collision. If more than one possible next-hop exists, one of them is chosen according to some criteria (e.g. selected at random, or the next-hop closest to the final destination).

The transformations among the several types of graphs in the proposed method are easily performed in polynomial time. For the determination of the maximum independent set of a graph, we used the algorithm in [17] that allows us to obtain results for a reasonable number of nodes in real-time.

IV. Evaluation

We now present evaluation results of collision-free data packet jamming, performed with the network simulator ns-3 [18] with the following system model.

A. System model and metrics

For the evaluation of our scheme, we resort to the 802.11b physical layer model of ns-3, with network interface cards in ad-hoc mode and Optimized Link State Routing (OLSR) as the routing protocol. The link-state information required for the collision-free jammer selection policy is obtained from OLSR, whose operation provides every node with link-state information on its two-hop neighborhood. The channels follow a log-distance channel propagation model where the pathloss PL is given by

$$PL(dB) = PL(d_0) + 10\alpha \log_{10}(d/d_0),$$

where α is the path loss exponent, d is the transmitter-receiver distance and d_0 is the reference close-in distance. Modeling the environment as a building with obstructions [19] (e.g. from walls) we set the path loss exponent to 4 and reception gain to -10dB. The path loss at the reference distance of $d_0 = 1$m is evaluated based on free space propagation. The remaining parameters take the default values defined in ns-3. In this setup, the signal strength of a received packet is affected by the transmission of any neighbor and a packet is successfully received if it meets a minimum required signal strength level.

Regular nodes and eavesdroppers are placed uniformly at random in a squared region of 10000 m^2 according to a Poisson point process with densities λ_{r} and λ_{e}, respectively. A minimum density of regular nodes of $\lambda_{\mathrm{r}} = 0.2\text{e-}2$ m^{-2} is considered, so that sufficient nodes are available for communication. From these nodes, every 2 seconds five transmitter-receiver pairs are randomly selected and exchange packets of 500 bytes at a rate of 25 packets/sec. The jammers cause interference by sending their own traffic packets with equal size to the Tx data packets (500 bytes). Following the insight gained in [10], the jammers transmit with low power ($P_j = 10$mW) and follow a near-receiver contention strategy, meaning that jammers that are neighbors of the legitimate receiver do not transmit to avoid causing interference on legitimate communication.

Since jammers are sending regular data packets instead of dummy jamming packets, we present results according to two perspectives: (i) *dummy* perspective in which only traffic from Tx is considered data, and (ii) *data* perspective in which traffic from jammers is also considered as data traffic. The dummy perspective relates to the case in which jammers send artificial interference without any meaning, whereas the data perspective captures the fact that jammers are now sending data packets that must also be considered in the calculations of the respective metrics.

For simplicity, we assume that the destination of data packets from jammers is a randomly selected next-hop from the set of neighbors of the jammers. If the jammers desire to send packets further ahead in the network, it is possible that these next-hops are not optimal with respect to some routing metric (e.g. hop-count). However, our focus here is to provide a proof-of-concept of the benefits of having jammers cause interference by sending their own regular data packets.

Metrics: Recognizing that the jammers can harm both the eavesdroppers as well as the legitimate receivers and their operation comes at an energy cost, we consider metrics to capture secrecy, communication and energy expenditure aspects. In particular,

1) Secrecy metric:
   - secure throughput, $\mathcal{T}_{\mathrm{s}}$, defined as the fraction of packets delivered successfully without any eavesdropper having access to them;
2) Communication metric:
   - goodput, G, i.e. the average throughput at the application level for all nodes in the network;
3) Energy expenditure metrics:
   - energy efficiency,

$$\mathsf{E}_{\mathrm{eff}} = \frac{\mathcal{N}_{\mathrm{app}}}{\mathcal{N}_{\mathrm{data}} + \mathcal{N}_{\mathrm{jam}}}, \quad (3)$$

where $\mathcal{N}_{\text{app}}$ represents the total number of end-to-end data bytes received at the application level. $\mathcal{N}_{\text{data}}$ and $\mathcal{N}_{\text{jam}}$ are the total number of data and jamming bytes, respectively, transmitted at the physical layer. The energy efficiency captures the relation between the total number of delivered end-to-end data bytes and the number of bytes (data or jamming) required to be transmitted at the physical layer so that end-to-end transmission is successful.

B. Secure throughput

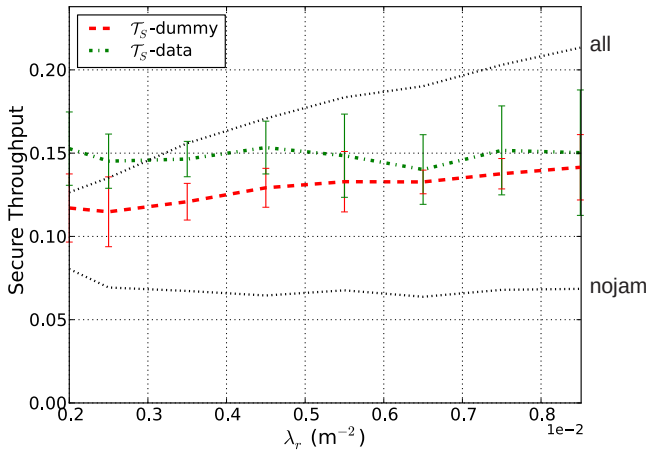
The results of Figure 3(a) show that the secure throughput of data packet jamming is better than when no jammer is active (nojam), yet scales slowly with the density of nodes in the network when compared to the case in which all jammers are active (all). This is explained by the fact that there are not many collision-free jammers available. Actually, our results show that the average number of jammers stays below 2 for the entire range of λ_{r}.

When data packets from jammers are also considered for the secure throughput calculations ($\mathcal{T}_{\text{s}}$-data), we observe that the secure throughput is above $\mathcal{T}_{\text{s}}$-dummy. This makes sense because, in the same way that some nodes behave as jammers for Tx, so does Tx with respect to the jammers, as well as the jammers among themselves, therefore protecting data from every source (jammers and Tx) alike. Notice that the $\mathcal{T}_{\text{s}}$-dummy increases with the density of nodes, whereas $\mathcal{T}_{\text{s}}$-data remains relatively steady, therefore reducing the gap between the two.

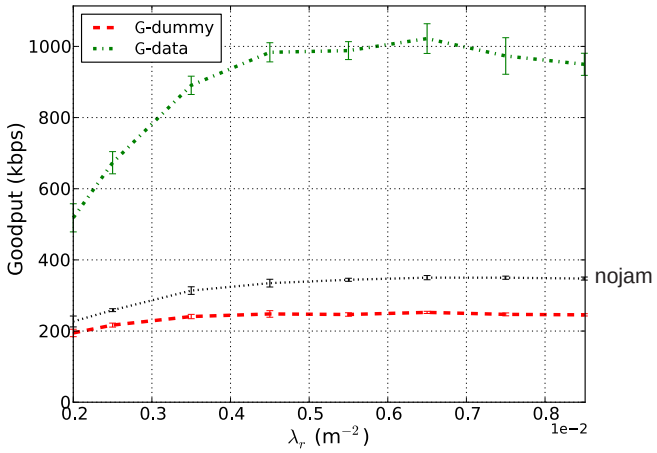
In brief, data packet jamming does not provide secure throughput improvements up to the level of all jammers active (best case identified in [11]). It does, however, more than double the secure throughput when compared to the case without jammers, and also provides relevant gains in terms of goodput and energy efficiency, as we will now see.

C. Goodput

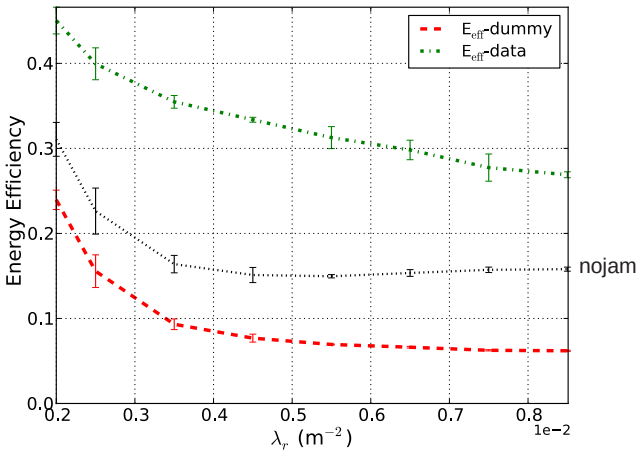
Looking at the goodput results of Figure 3(b), we see that the goodput when the jammers' traffic is considered as dummy (G-dummy) turns out worse than the goodput with no jammers active. This happens because of the effect of interference from the jammers on the legitimate receivers. However, the goodput when jammers' traffic is considered as regular data traffic (G-data) is greatly improved. This happens because data traffic from jammers is also contributing to the overall goodput by increasing the number of successful transmissions in a given area. However, such a large difference must be analyzed with care. In fact, it does not make sense to compare the data perspective with the dummy perspective directly, as more data is being injected into the network by jammers. Still, these results do show that it is possible to have some selected neighbors of Tx causing interference by sending their own data packets, without much decline in the goodput of the transmitters as shown by G-dummy.



(a) Secure throughput.



(b) Goodput.



(c) Energy efficiency.

Figure 3. Simulation results for varying λ_j ($\lambda_{\text{e}} = 0.15\text{e-}2$ m^{-2}, $P_j = 40$mW). The case with all jammers active (all) and no jammers active (nojam) are shown for reference.

Moreover, this leads to a major gain in terms of aggregate goodput (G-data) of sources and jammers in the network.

D. Energy efficiency

Having jammers transmit data packets also leads to a major benefit in terms of energy efficiency, as seen in Figure 3(c). This plot shows that by jamming with data packets, the energy efficiency of the network is greatly improved even with respect to the case without jammers. This happens because the term $\mathcal{N}_{\text{app}}$ of (3) now includes traffic delivered successfully by jammers, therefore compensating the increase in $\mathcal{N}_{\text{jam}}$ due to the jammers.

For these results, we consider that jammers always have data packets to send. If this is not the case, jammers can fallback to generate dummy jamming packets. In that case, more jammers can be active and results would tend towards the results of the case in which all jammers are active, i.e. higher secure throughput at the cost of reduced goodput and energy-efficiency.

V. Conclusions

We presented a jammer selection policy that enables sources of data in wireless networks to choose the largest set of neighbors that can act as jammers without causing collisions among themselves. These jammers are then used to send their own data concurrently with data from the source with the goal of causing interference to possible eavesdroppers. Our results show that both the jammers as well as the sources benefit from this concurrent transmission, as the number of secure transmissions is higher than when jammers are causing interference with dummy data. This highlights the potential of collision-free jamming to increase the secrecy level of wireless networks, while providing benefits in terms of energy efficiency and goodput.

References

[1] Martin Haenggi. The secrecy graph and some of its properties. In *Proc. IEEE International Symposium on Information Theory*, pages 539–543, Toronto, Canada, July 2008.

[2] Pedro C. Pinto, João Barros, and Moe Z. Win. Secure Communication in Stochastic Wireless Networks–Part I: Connectivity. *IEEE Transactions on Information Forensics and Security (accepted for publication)*, 7(1):125–138, February 2012.

[3] Matthieu Bloch and João Barros. *Physical Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[4] R. Negi and S. Goel. Secret communication using artificial noise. In *Proc of IEEE Vehicular Technology Conference*, pages 1906–1910, Texas, USA, September 2005.

[5] Satashu Goel and Rohit Negi. Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications*, 7(6):2180–2189, June 2008.

[6] Ender Tekin and Aylin Yener. The General Gaussian Multiple-Access and Two-Way Wire-Tap Channels: Achievable Rates and Cooperative Jamming. *IEEE Transactions on Information Theory*, 54(6):2735–2751, June 2008.

[7] Lifeng Lai and Hesham El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Transactions on Information Theory*, 54(9):4005–4019, September 2008.

[8] X. Tang, R. Liu, P. Spasojevic, and H.V. Poor. Interference-assisted secret communication. In *IEEE Information Theory Workshop (ITW)*, pages 164–168, Porto, Portugal, 2008.

[9] João P. Vilela, Matthieu Bloch, João Barros, and Steven W. McLaughlin. Wireless secrecy regions with friendly jamming. *IEEE Transactions on Information Forensics and Security*, 6(2):256–266, June 2011.

[10] João P. Vilela, Pedro C. Pinto, and João Barros. Position-based Jamming for Enhanced Wireless Secrecy. *IEEE Transactions on Information Forensics and Security*, 6(3):616–627, September 2011.

[11] João P. Vilela and João Barros. A cooperative protocol for jamming eavesdroppers in wireless networks. In *IEEE International Conference on Communications*, Ottawa, Canada, June 2012.

[12] Azadeh Sheikholeslami, Dennis Goeckel, Hossein Pishro-Nik, and Don Towsley. Physical layer security from inter-session interference in large wireless networks. In *Proceedings of the IEEE INFOCOM 2012, Orlando, FL, USA, March 25-30, 2012*, pages 1179–1187. IEEE, 2012.

[13] Azzedine Boukerche, Khalil El-Khatib, Li Xu, and Larry Korba. A novel solution for achieving anonymity in wireless ad hoc networks. In *Proceedings of the 1st ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, PE-WASUN*, October 2004.

[14] Pietro Michiardi and Refik Molva. Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Proc. of the IFIP-Communication and Multimedia Security Conference*, Copenhagen, June 2002.

[15] Levente Buttyán and Jean-Pierre Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. *Mobile Networks and Applications*, 8(5):579–592, October 2003.

[16] Kamal Jain, Jitendra Padhye, Venkata N. Padmanabhan, and Lili Qiu. Impact of interference on multi-hop wireless network performance. *Wireless Networks*, 11(4):471–487, 2005.

[17] Janez Konc and Dusanka Janezic. An improved branch and bound algorithm for the maximum clique problem. *MATCH Communications in Mathematical and in Computer Chemistry*, 58(3):569–590, 2007.

[18] Network simulator 3, version 3.7.1. `http://www.nsnam.org/`.

[19] Patrick Stuedi, Oscar Chinellato, and Gustavo Alonso. Connectivity in the presence of shadowing in 802.11 ad hoc networks. In *IEEE Wireless Communications and Networking Conference*, volume 4, pages 2225–2230, New Orleans, LA, USA, March 2005.