A Cooperative Protocol for Jamming Eavesdroppers in Wireless Networks

João P. Vilela
CISUC, Department of Informatics Engineering
University of 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 jamming protocol for secrecy-enhanced wireless networks in which otherwise silent devices are selected as jammers to cause interference to potential eavesdroppers. This cooperative protocol includes several jammer selection policies that lead to different levels of secrecy–energy tradeoffs. Our results show that there is some advantage over selecting well-connected jammers and there is a need for a minimum number of jammers for the energy cost of jamming to payoff.**

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]. Examples include jamming schemes with secrecy purposes, as proposed in [4], [5]; other techniques such as directional antennas and neutralization of eavesdroppers are proposed in [6].

In [7], [8], we perform a system analysis of the impact of jamming on the secrecy level of wireless networks. The first contribution [7] 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 [8] considers multi-terminal environments and proposes a basic 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.

Here we specify and evaluate a practical jamming protocol for enhancing wireless secrecy. This protocol relies on the well-known RTS(request-to-send)/CTS(clear-to-send) channel reservation scheme as a signaling scheme to detect when to jam; the protocol includes several jammer selection policies, leading to different secrecy-gain–energy-cost tradeoffs.

A. Network Scenario

We consider a network composed of regular 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. The eavesdroppers are external devices in that they are alien to the network operation and just lie silently with the intent of overhearing as much information as possible.

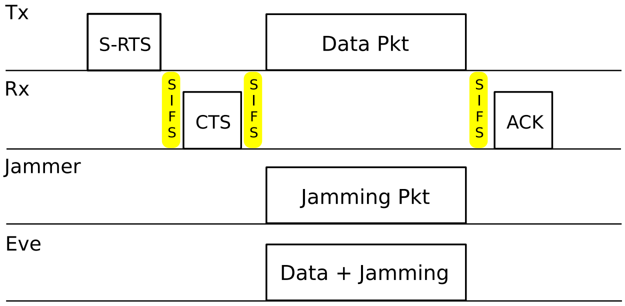


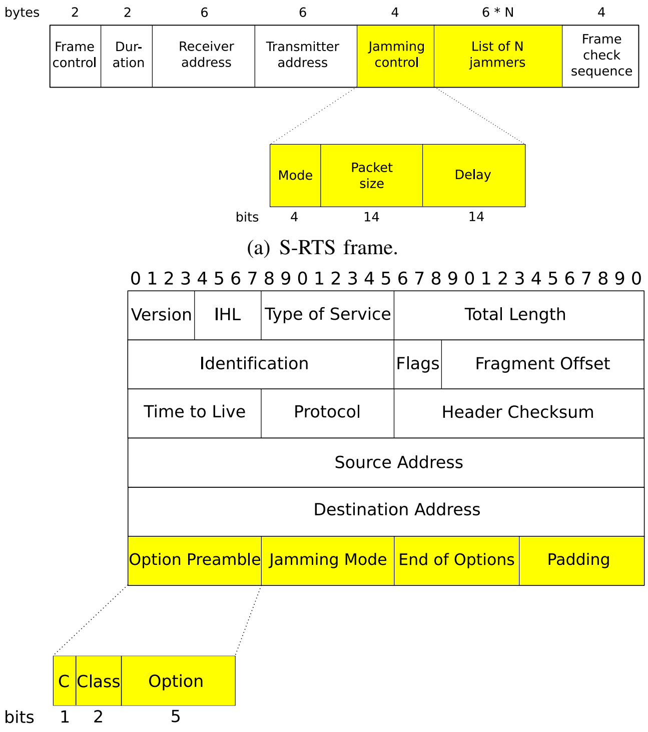
Fig. 1. Message passing for the jamming protocol. Messages are separated by short inter-frame space (SIFS) time intervals, as in the original RTS/CTS protocol.

II. Protocol Design

This protocol inherits and extends the operation of the RTS/CTS handshake as depicted in *Figure 1*. Prior to communication Tx sends a RTS message augmented with security-related fields (henceforth referred to as S-RTS). Among other information, the S-RTS contains a list of active jammers, whose selection is in charge of Tx. Once a jammer that figures in the list of active jammers receives the S-RTS, it performs carrier sensing to detect the beginning of transmission by Tx. Then, interference is generated by the jammer according to the selected jamming mode.

The operation of the jamming protocol can be divided in two phases:

1) prior to communication:
   - selection of jammers: according to the adopted jammer selection policy, Tx selects a set of jammers that shall cause interference to possible eavesdroppers;
   - generation and processing of S-RTS: a S-RTS frame is generated to convey relevant information to the jammers. In particular, the S-RTS contains a list of active jammers, specifies the jamming mode, size of the data packet from Tx and transmission delay;
   - carrier sensing: after processing the S-RTS, the jammers enter a carrier sensing mode to detect the beginning of transmission from Tx.



(a) S-RTS frame.

(b) Jamming datagram.

Fig. 2. S-RTS frame format in (a) and jamming datagram header format in (b). New fields with respect to the original versions are highlighted.

2) during communication:

- jamming: during transmission from Tx the role of the selected jammers is to cause interference to potential eavesdroppers by sending a jamming datagram according to the adopted jamming mode.

Note that most decisions are on behalf of Tx. Namely, Tx selects a set of jammers according to the adopted jammer selection policy. Tx can also indicate a jamming mode and send other relevant information to the jammers via the S-RTS. In this section we provide a detailed description of the several phases of the jamming protocol and a specification of its corresponding messages (S-RTS and jamming datagram).

A. Packet formats

The jamming protocol is based on two packet types. The S-RTS is a signaling frame exchanged at the MAC level between neighbor devices, whereas the jamming datagram is an adapted IP datagram that can possibly traverse multiple hops.

1) S-RTS: the S-RTS frame (*Figure 2(a)*) contains four fields of information from the jamming protocol. These are:

- mode: indicates the mode used to cause interference by the jammers (up to 16 different jamming modes allowed);
- packet size: size of the packet that Tx intends to send (packet sizes up to 16384 bytes);
- delay: expected time interval until the transmission of the data packet by Tx (delays of up to 16384 microseconds);
- list of jammers: the list of jammers chosen according to the adopted jammer selection policy.

With respect to the regular operation of the RTS/CTS handshake, these new fields induce a fixed overhead of 4 bytes and a variable overhead of $6*N$ bytes, where N is the number of selected jammers[1].

2) Jamming datagram: the jamming datagram (*Figure 2(b)*) follows the same structure of any other IP datagram. It can be of any size and the header includes an extra option field indicating the jamming mode of the packet. A final padding is added assuring that the IP header is a multiple of 32 bits.

The option field is composed by a preamble of three fields, followed by the option data itself (the jamming mode) and an indicator of the end of options (a sequence of eight 0 bits). The three preamble fields are as follows.

- copy flag (1 bit): indicates whether this option is copied into all fragments on fragmentation. Takes the value 1, meaning that all fragments should be treated according to the specified jamming mode;
- class (2 bits): defines the option class. Takes value 0, meaning that this is a control parameter;
- option (5 bits): defines the number associated to this option (set to one of the available numbers (e.g. 26), as defined by the Internet Assigned Numbers Authority[9]).

The jamming datagram is then an IPv4 datagram with an extra option field that leads to a per-packet overhead of 4 bytes.

B. Node configuration

Tx and jammers have an active role in the jamming protocol. Their operation can be tuned according the desired secrecy goals and the configurable parameters for Tx are:

- jammer selection policy: the jammer selection policy is a set of rules used to select the batch of active jammers among the one-hop neighbors of Tx;
- jamming mode: the jamming mode specifies the type of jamming employed by the jammers. Although the jammers themselves have a default jamming mode, this can also be determined by Tx. Possible jamming modes are described in Section II-F.

For the jammers, we have:

- jamming mode: jamming at the physical level can be performed in several ways. The jamming mode specifies how jamming is performed in practice;
- jamming strategy: jammers can also choose to cause interference according to a given strategy, such as the near-source jamming and near-receiver contention strategies introduced in [8];
- transmission power.

C. Selection of jammers by Tx

The selection of jammers is performed according to the information available at Tx. Several policies can be used with different requirements in terms of available information. A common type of information usually available is link state information, and this enables several policies. We now provide a set of jammer selection policies along with their information requirements. These policies may adjust to different types of environments, according to the available information and the security objectives.

[1] Each jammer is identified through its MAC address, which takes 6 bytes.

1) Multipoint relay jammers: the multipoint relay (MPR) is a concept borrowed from the Optimized Link State Routing Protocol (OLSR) [10] for mobile ad-hoc networks, and corresponds to the smallest set of one-hop neighbor nodes ensuring connectivity to every two-hop neighbor of a given node. Flooding through MPRs ensures that every two-hop neighbor receives the intended information and minimizes redundant local retransmissions by performing scoped flooding instead of a full node-to-node flooding. Although the goal of MPRs is to provide connectivity to two-hop neighbors (which are unable to eavesdrop on Tx), given the well connected nature of MPRs we consider a policy in which these nodes are selected as jammers.

This policy requires knowledge of the two-hop neighborhood of Tx, so that the selection of MPRs can take place. Finding the MPRs is a NP-complete problem, however, efficient heuristics[11] have been proposed and applied.

2) k most connected jammers: this policy selects the k most connected one-hop neighbors as jammers (k is a configurable parameter). In contrast with the previous policy, this does not necessarily lead to covering all two-hop neighbors of Tx. The reasoning behind this policy is that most connected jammers can potentially overcome a larger number of eavesdroppers. This policy requires knowledge of the two-hop neighborhood.

3) Random fraction $F\%$ of jammers: recognizing that eavesdroppers can appear anywhere in the vicinity of Tx, this policy selects a fraction $F\%$ of the possible jammers uniformly at random. To implement this policy, knowledge of the one-hop neighborhood of Tx suffices.

4) No jammers and all jammers: these are basically two reference policies in which (i) no jammers are active, and (ii) all jammers are active.

These policies require no network information and no selection of jammers is needed. The case without jammers corresponds to the regular network operation in which the secrecy fields of the S-RTS are nonexistent (or no S-RTS is sent), whereas the policy of all jammers can be made active by sending a S-RTS with an empty list of jammers.

D. Generation and processing of S-RTS

The secrecy-related fields of the S-RTS are determined by the node configuration of Tx and the characteristics of the data to send. When processed by the jammers, the S-RTS conveys information about the transmission of a packet by Tx. The transmission of this data packet takes place only if a CTS from Rx is received by Tx in response to the S-RTS. The beginning of transmission from Tx triggers the jammers, who must perform some form of carrier sensing to detect the ongoing transmission by Tx.

E. Carrier sensing by the jammers

The detection of an ongoing transmission from Tx by the jammers is crucial to prevent the generation of unnecessary interference and waste of resources. This can be achieved through carrier sensing, which usually takes two flavors:

- *physical carrier sensing* is a layer 1 mechanism to physically detect an ongoing transmission, usually by measuring energy levels. All stations that are not transmitting or receiving perform physical carrier sensing with the intent of either detecting a free medium or receiving incoming traffic;
- *virtual carrier sensing* is a virtual form of sensing normally performed through the exchange of signaling packets for notification of some event.

The RTS/CTS is actually a form of virtual carrier sensing. A CTS indicates that a transmission is about to take place and can be used by jammers in the vicinity of Rx to determine when to start causing interference. This, however, assumes that Tx will receive the CTS successfully and is limited to jammers that are neighbors of Rx. Therefore, physical carrier sensing is preferable. In particular, after reception of the S-RTS, the jammer senses the channel until detection of an ongoing transmission. After that, the jammer switches to transmit mode, thus interfering with possible eavesdroppers according to the chosen jamming mode.

F. Jamming modes

Different jamming modes can be employed according to the desired goals. Some relate to the duration of activity by the jammers [12], such as constant jamming and pulse jamming, while others are pertained with the nature of traffic being targeted, such as protocol-specific control packets or data packets. Constant jamming is performed by having a jammer generate constant noise for a given time period. The signal from the jammer can be modulated with a random noise waveform with the intent of adding noise to the eavesdropper's signal. Pulse jamming is characterized by the pulse length, interval between pulses and jammer transmission power. In this case, the jammer sends a pulse of a defined length and transmission power, with a silence period between pulses.

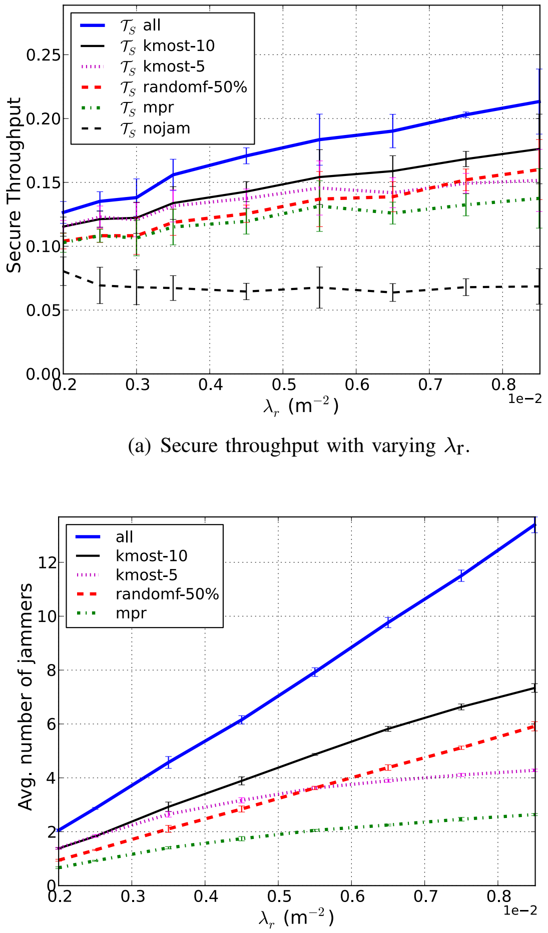
Our jamming protocol targets data packets and jamming is performed for the duration of transmission from Tx by generating jamming packets of the same size of the source-generated data packet. This jamming packet is a dummy packet generated with the sole intent of causing interference and, therefore, it is not destined to any node in the network.

III. Evaluation

The jamming protocol was completely implemented in the network simulator ns-3[13]. This section presents a comparison of the different jammer selection policies.

A. System setup

We consider the network scenario described in Section I-A. 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 $\lambda_\mathrm{r} = 0.2\mathrm{e}\text{-}2\ \mathrm{m}^{-2}$ 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



(a) Secure throughput with varying λ_{r}.

(b) Average number of jammers per transmission.

Fig. 3. Simulation results ($\lambda_{\text{e}} = 0.15\text{e-}2\ \text{m}^{-2}$, $P_J = 10\text{mW}$.)

500 bytes at a rate of 25 packets/sec. Each Tx is configured with a chosen jammer selection policy. Following the insight gained in [8], the jammers follow the near-receiver contention strategy and transmit with low power, i.e. $P_J = 10\text{mW}$.

For the ns-3 simulations, we resort to a 802.11b physical layer model with the network interface cards in ad-hoc mode and Optimized Link State Routing as the routing protocol. The link-state information required for the different jammer selection policies 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 with path loss exponent 4 and reception gain -10dB. 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.

B. *Metrics*

We consider metrics to capture secrecy and energy expenditure aspects. In particular,

1) Secrecy metric:
   - secure throughput, $\mathcal{T}_{\text{s}}$, defined as the fraction of packets delivered successfully without any eavesdropper having access to them;
2) Energy expenditure metrics:
   - energy efficiency, $\mathsf{E}_{\text{eff}} = \dfrac{\mathcal{N}_{\text{app}}}{\mathcal{N}_{\text{data}} + \mathcal{N}_{\text{jam}}}$, 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;
   - energy-per-secure-bit, $\mathsf{E}_{\text{sb}}(\mu\text{J/bit}) = \dfrac{P_J\ S_j\ T}{\overline{N}_{sec}}$, where P_J (μW) is the transmit power of the jammer, S_j the size of jamming packet in bits, T is the time to transmit one bit in seconds, and $\overline{N}_{sec}$ the average number of secure bits per transmission. This metric captures the energy required from a jammer to enable the secure transmission of one bit.

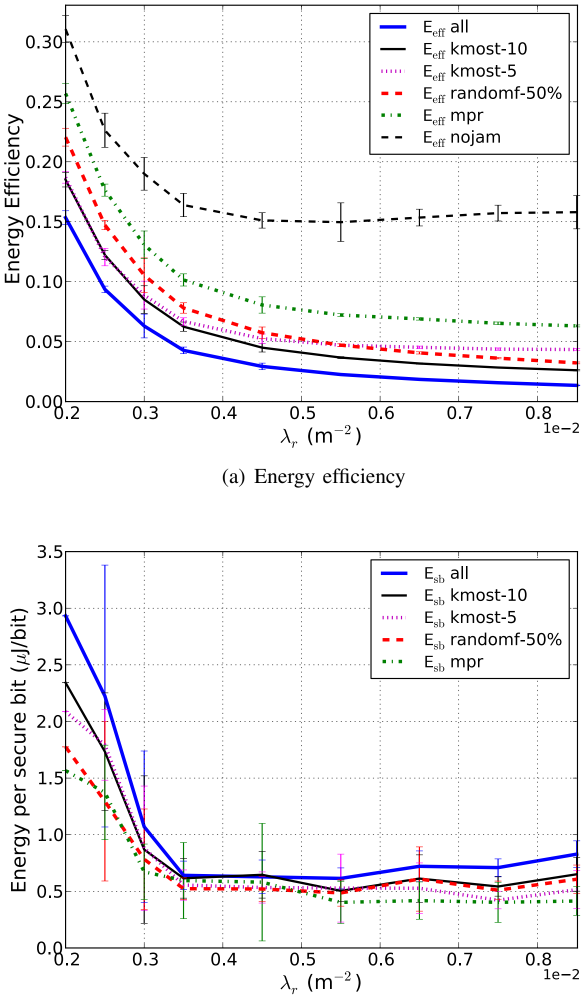
We also considered the effect of jamming on communication via a goodput metric, i.e. the end-to-end throughput at the application level. These results, which are omitted for brevity, show that there is some loss of goodput, which is contained as result of employing a near-receiver contention strategy. The goodput loss varies with the density of regular nodes, leading a maximum loss of 35.5% on one extreme when all jammers are active, and a maximum loss of 19.4% on the other extreme when mpr jamming is used.

C. *Results*

1) Secure throughput: Figure 3(a) shows the variation of the secure throughput with the density of nodes. The policy of all jammers active leads to a steady $\mathcal{T}_{\text{s}}$ growth with λ_{r} as observed in [8]. The remaining policies exhibit smaller growth with λ_{r} and there appears to be a mapping between the average number of active jammers and the secrecy gain. This is supported by *Figure 3(b)*, which shows that the policy with maximum secure throughput (all jammers) is also the one with highest average number of jammers per transmission. Conversely, the MPR policy leads to the lowest secure throughput as result of the having the lowest average number of jammers per transmission among all strategies.

The policies of k most connected with $k = 5$ (kmost-5) and $k = 10$ (kmost-10) show a similar behavior for initial values of λ_{r}, after which the policy with larger k lifts off, both in terms of average number of jammers per transmission, as well as secure throughput. This happens because the initial the pool of possible jammers is small, thus leading to a similar number of jammers per transmission for both cases. Once the pool of jammers increases, the advantage of a higher k value kicks in.

Comparing the results of the kmost-5 policy with the random fraction with $f = 50\%$ (randomf-50%) policy, we see that although the average number of jammers of randomf-



(a) Energy efficiency

(b) Energy-per-secure-bit

Fig. 4. Energy plots for jammer selection policies ($\lambda_{\rm e} = 0.15\text{e-}2\text{m}^{-2}$).

50% surpasses kmost-5 at nearly $\lambda_{\rm r} = 0.55\text{e-}2\text{m}^{-2}$, the secure throughput of randomf-50% overcomes that of kmost-5 only for $\lambda_{\rm r} > 0.7\text{e-}2\text{m}^{-2}$, suggesting that there is some advantage of selecting the most connected jammers over selecting jammers at random, even for a uniformly distributed eavesdropper.

2) Energy costs: due to the different average number of jammers per transmission, these policies are bound to have separate energy efficiency results, as depicted in *Figure 4(a)*. Notice that $\mathrm{E}_{\rm eff}$ results are inversely correlated with the average number of jammers of *Figure 3(b)*. In particular, policies with largest average number of jammers lead to the lowest $\mathrm{E}_{\rm eff}$, and vice-versa. Moreover, $\mathrm{E}_{\rm eff}$ of randomf-50% becomes lower than $\mathrm{E}_{\rm eff}$ for kmost-5 at nearly $\lambda_{\rm r} = 0.55\text{e-}2\text{m}^{-2}$ which is the turning point after which randomf-50% surpasses kmost-5 in terms of average number of jammers. This shows that in this setup the predominant factor on the energy efficiency comes from having jammers transmitting. Also, although there is an improvement in terms of energy efficiency from using fewer jammers, there is still a severe penalty for all policies, specially for large density of nodes.

An alternative perspective focused on the secrecy-gain–energy-cost tradeoff of individual jammers is presented in *Figure 4(b)*. The plot shows that for all policies the cost of jamming with respect to the number of bits transmitted securely is high for low density of nodes, and drops to a somewhat steady value for a large range of $\lambda_{\rm r}$ values. This means that, either there is a reasonable number of jammers available, or the cost of jamming with respect to the attained secrecy gain is high. After initial values of $\lambda_{\rm r}$ that lead to a high energy-per-secure-bit, this measure exhibits a small variability among all policies. Although this ultimately leads to very different overall energy costs depending on the average number of jammers per transmission of each policy, this means that the energy cost of having extra jammers in the system is alleviated by the resulting secrecy gain from those jammers.

IV. Conclusion

We provided the complete specification of a jamming protocol for secrecy-enhanced wireless networks. The specification of the protocol includes several jammer selection policies that rely on distinct levels of available link-state information. These policies exhibit different secrecy-gain–energy-cost tradeoffs and show that selecting well-connected jammers is beneficial; also, for a small number of jammers the individual energy-cost is high with respect to the obtained secrecy-gain, meaning that either there is a minimum number of jammers available or the secrecy benefit may not justify the associated energy cost.

References

[1] M. Haenggi, “The secrecy graph and some of its properties,” in *Proc. IEEE International Symposium on Information Theory*, Toronto, Canada, July 2008, pp. 539–543.

[2] P. C. Pinto, J. Barros, and M. Z. Win, “Secure Communication in Stochastic Wireless Networks–Part I: Connectivity,” *IEEE Transactions on Information Forensics and Security (accepted for publication)*, 2011.

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

[4] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[5] E. Tekin and A. Yener, “The General Gaussian Multiple-Access and Two-Way Wire-Tap Channels: Achievable Rates and Cooperative Jamming,” *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.

[6] P. C. Pinto, J. Barros, and M. Z. Win, “Techniques for Enhanced Physical-Layer Security,” in *IEEE Global Telecommunications Conference (GLOBECOM)*, Miami, FL, USA, December 2010.

[7] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, “Wireless secrecy regions with friendly jamming,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 256–266, June 2011.

[8] J. P. Vilela, P. C. Pinto, and J. Barros, “Position-based Jamming for Enhanced Wireless Secrecy,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 616–627, September 2011.

[9] I. A. N. A. (IANA), “IP Option Numbers,” last updated April 5th, 2011, http://www.iana.org/assignments/ip-parameters.

[10] T. Clausen and P. Jacquet, “Optimized link state routing protocol (OLSR),” IETF Internet Draft, http://www.ietf.org/rfc/rfc3626.txt, Tech. Rep., 2003.

[11] A. Qayyum, L. Viennot, and A. Laouiti, “Multipoint Relaying for Flooding Broadcast Messages in Mobile Wireless Networks,” in *35th Annual Hawaii International Conference on System Sciences*, Hawaii, United States, January 2002.

[12] R. A. Poisel, *Modern communications jamming principles and techniques*. Artech House, 2004.

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