Uncoordinated Frequency Hopping for Secrecy with Broadband Jammers and Eavesdroppers

João Sá Sousa
CISUC, Department of Informatics Engineering
University of Coimbra, Coimbra, Portugal.
Email: jagsousa@dei.uc.pt

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

***Abstract*—Uncoordinated Frequency Hopping (UFH) has been proposed as a mechanism to address denial-of-service attacks, and consists of legitimate devices hopping uniformly at random between frequencies to cope with an attacker that aims to disrupt communication. We consider the use of UFH against an eavesdropper adversary that aims to overhear as much information as possible. We characterize the secrecy level of wireless networks under UFH, showing the harmful security effect of broadband eavesdropper adversaries capable of overhearing in multiple frequencies. To counter such eavesdroppers, we consider the use of broadband friendly jammers that are available to cause interference on eavesdroppers. Our results show that adding a limited number of broadband friendly jammers effectively improves the security level of such systems.**

I. Introduction

As wireless systems become widely available, security in these environments is regarded as something of the utmost importance. These systems have always been a target for a number of different attacks that, more than often, are capable of breaching the security mechanisms implemented and threaten the reliability, safety and robustness of communications. Attacks such as Denial of Service (DoS) and eavesdropping are constantly ravaging these systems and surpassing the security techniques employed, using ingenious tactics and/or capable devices. Most solutions imply the use of sophisticated encryption techniques to fend off some types of attackers, such as eavesdroppers, but usually depend on a shared secret between involved parties, which can be impracticable to carry out in some situations (e.g. degraded channel). Other attackers which aim to disrupt communications (e.g. jammers) are usually addressed through spread spectrum systems such as frequency hopping (FH) that also depends on a shared hopping sequence. Researchers have tried to bolster these techniques and have developed new mechanisms by trying to tackle some of the problems and liabilities of the previous settings, such as the need for a shared secret or the presence of malicious colluding insiders or adversaries [1]. Methods such as Uncoordinated Frequency Hopping (UFH) [2], [3] and friendly jamming [4] have been regarded as possible ways of improving secrecy and reliability of wireless communications without the need for a shared secret.

Uncoordinated Frequency Hopping implies the communication between transmitter and receiver through a randomly chosen frequency channel unknown for both agents. Therefore, both intervenients randomly and independently hop between a set of frequencies, briefly transmitting chunks of data when both of them land in the same canal. Since adversaries are unaware of the random hopping sequence, this enables adversary-free periods of communication whenever the transmitter and receiver lie in the same frequency without the adversary doing so. This scheme acts, in some way, like regular FH, although it tries to offer a key-independent service (no previous hopping scheme is established between nodes). This leads to a significant reduction of the average throughput and, consequently, significantly decreases its performance (transmission ratio) at the benefit of adversarial-free information exchange. Originally thought out for protection against DoS jammers, these periods of adversary-free communication can then be used, for example, for exchanging a hopping sequence for regular FH communication.

Interference/jamming generation schemes for wireless secrecy have been proposed and recent works suggest that jamming can improve the secrecy level of wireless networks by reducing the received signal quality of adversary eavesdroppers. In [5] the authors introduced a scheme for generating artificial noise using a transmitter with multiple transmission antennas or relay nodes, whereas in [6] jammers are used as defensive nodes willing to assist legitimate communication by using a cooperative jamming scheme in which an otherwise disadvantage user can help improve the secrecy rate by jamming a nearby eavesdropper or by carefully placing jammers as to maximize the security level for a particular region. In [4], [7], jammers are employed as defensive devices and optimal configurations and placement are studied as to provide sufficient coverage using minimum resources in multi-terminal environments. Finally, [8], [9] analyze jammer selection schemes for inter-session interference, therefore reducing the energetic burden of jamming for secrecy.

In [10] we evaluated the combined usage of jamming with narrowband (single frequency) UFH for secrecy against eavesdroppers. This showed that the number of available frequencies can be adjusted so as to reduce the effect adversary eavesdroppers; and jammers can greatly aid in providing higher levels of security by causing interference to eavesdroppers. This revealed UFH with jamming to be an effective counter-measure against eavesdropping without the need for a previously exchanged key.

In our present work we focus on the security level of uncoordinated frequency hopping with eavesdroppers and friendly jammers which are able to respectively listen and transmit in several frequencies at a time. We will, therefore, evaluate how these broadband jammers can hamper the ability of one or more eavesdroppers that are able to overhear in multiple frequencies at the same time. Doing this provides us with a greater insight into the impact that these defensive jammer agents can have in the secure throughput (i.e. the fraction of securely transmitted messages) of this system, according to different parameters, such as the number of receive/transmit channels, number of jammers and eavesdroppers, and number of hopping frequencies.

The remainder of the paper is divided into four other sections: Section II describes the system and attacker model, where we specify the characteristics of the proposed scheme and some of the assumptions considered. In Sections III and IV we perform the analysis of the security level of UFH respectively with and without friendly jammers, and compare those results with the narrowband scenario. Section V concludes the paper and highlights key issues and findings.

II. System and Attacker Model

This system comprises one transmitter (Tx) and one receiver (Rx) deployed within reach of each other and capable of consistently communicating between themselves. Furthermore, it includes a set Π_e of E broadband eavesdroppers able to listen to C_E different canals and J broadband jammers able to transmit in C_J different channels. Each node is capable of jumping through N possible frequencies following the Uncoordinated Frequency Hopping (UFH) Scheme.

Let x $\rightarrow$ y denote the event of *successful reception* by device y of a message sent by x. Similarly, let x $\not\rightarrow$ y denote the event of *unsuccessful reception*, i.e. the complementary event of x $\rightarrow$ y. Successful communication happens when Tx and Rx land on the same frequency channel.

A. Assumptions

We assume that all devices share the same physical characteristics (e.g. transmission power and rate), and jump synchronously between frequencies. All devices belonging to this system are within reach of each one another, meaning that all eavesdroppers can potentially listen to communication between Tx and Rx, while all jammers are capable of causing interference to those same eavesdroppers.

We consider that jammers coordinate with Tx and Rx , using for example a RTS(request-to-send)/CTS(clear-to-send) handshake as presented in [11], to avoid harming legitimate communication, while causing interference to potential eavesdroppers. Although this is a strong assumption, it may be achieved through different mechanisms, such as steered/sectorized [12] transmission towards regions of potential eavesdroppers via directional antennas, or distributed beamforming schemes that have been recently incorporated into regular wireless networks [13], therefore allowing jammers' signals to add up coherently at an intended receiver, while causing interference to potential eavesdroppers.

B. Attacker Model

For the attackers we consider a passive eavesdropper adversary, who lies silently within transmission range to overhear legitimate communication. The adversary eavesdroppers have the same characteristics as other agents and are able to detect and overhear communication in several frequencies, depending on their broadband capacity. The eavesdroppers also jump independently at random among the different frequencies searching for the legitimate communication channel. Eavesdroppers hop between frequencies at the same rate as the remaining devices. If eavesdroppers could hop between frequencies much faster than other devices, this would allow them to rapidly detect legitimate communication on a given frequency and remain on that frequency overhearing communication until the Tx jumps to another frequency. However, the same kind of reasoning can be applied to jammers, in the sense that if jammers were able to hop between frequencies much faster this would allow them to affect eavesdroppers more frequently with corresponding security benefits. Whenever communication is possible (i.e. Tx and Rx are in the same frequency), we say that secure communication happens if:

1) Tx and Rx are in the same frequency while no jammer or eavesdropper is present in that channel.
2) Tx, Rx and jammers are in the same frequency while there is no eavesdropper listening in that band.
3) Tx, Rx and jammers are in the same frequency, as well as eavesdroppers, with jammers avoiding interference on legitimate communication, while causing interference on eavesdroppers' so as to limit their ability to overhear information.

III. Secure Throughput

We consider a secure throughput security metric. The secure throughput measures the transmission rate at which Tx can communicate with Rx without eavesdroppers being able to acquire any information, as described in the previous three situations.

Definition 1 (Secure Throughput). *The secure throughput* $\mathcal{T}_\mathrm{s}$ *from* Tx *to* Rx *is the probability that a message transmitted by* Tx *is* successfully *received by* Rx*, and* unsuccessfully *received by every eavesdropper in any frequency,*

$$\mathcal{T}_\mathrm{s} \triangleq \mathbb{P}\left\{ \mathrm{Tx} \rightarrow \mathrm{Rx} \ \wedge \bigwedge_{e_i \in \Pi_e} \mathrm{Tx} \nrightarrow e_i \right\}.$$

The secure throughput quantifies the probability of secure communication between Tx and Rx, depending on parameters such as the number of frequency channels, and the number of eavesdroppers and jammers in the system.

Proposition 1. The secure throughput for a setup with one Tx-Rx pair hopping uniformly at random through N frequencies, and E broadband eavesdroppers capable of simultaneously overhearing from C_E of those N frequencies is given by

$$\mathcal{T}_{\rm s} = \frac{N\binom{N-1}{C_E}^E}{N^2\binom{N}{C_E}^E}, \quad C_E < N,$$

where

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}, \quad n \geq r \wedge r > 0$$

represents the combination of r non-repeated elements selected from a group of n members, such that the order of selection does not matter.

Proof. This formula results from the ratio of favorable cases over possible cases, where N represents the number of matching frequency channels between Tx and Rx, and $\binom{N-1}{C_E}^E$ the combination of the C_E frequencies being listened to by the eavesdroppers so that none of them is capable of overhearing legitimate communication. As for $N^2 * \binom{N}{C_E}^E$, it encompasses all the possible permutations between all the devices currently selected for this setup (E eavesdroppers, plus Tx and Rx). □

A. Analysis

To carefully analyze the system's throughput and study the impact of broadband eavesdropping for Uncoordinated Frequency Hopping we started by elaborating a set of different situations using a varying number of adversary eavesdroppers and their capabilities. In order to validate the results we performed some simulations using Monte Carlo experiments. Both *Figure 1* and *Figure 2* depict a rather low secure throughput. This results from the negative effect of eavesdroppers on security, but also from the low throughput (i.e. probability that Tx and Rx land on the same frequency) between Tx and Rx, as depicted in *Figure 1*.

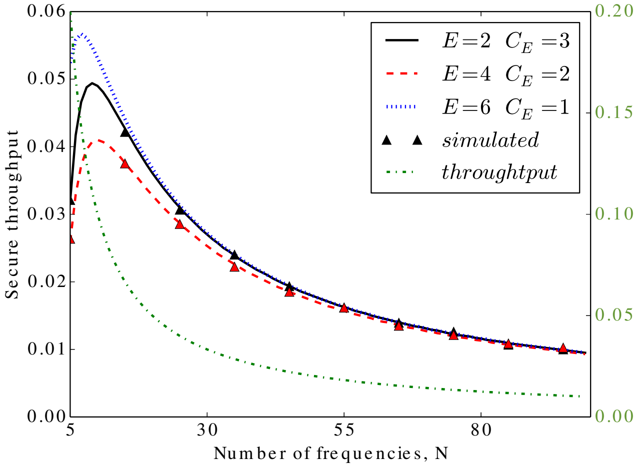

Fig. 1. Secure throughput in the presence of $E = 2$, $E = 4$ and $E = 6$ eavesdroppers capable of, respectively, listening to $C_E = 3$, $C_E = 2$ and $C_E = 1$ frequencies at the same time for different number of possible frequency channels, N. Simulation results are also provided and validate the analytic results. The second y-axis and consequent curve represent the throughput associated with the Uncoordinated Frequency Hopping Scheme.

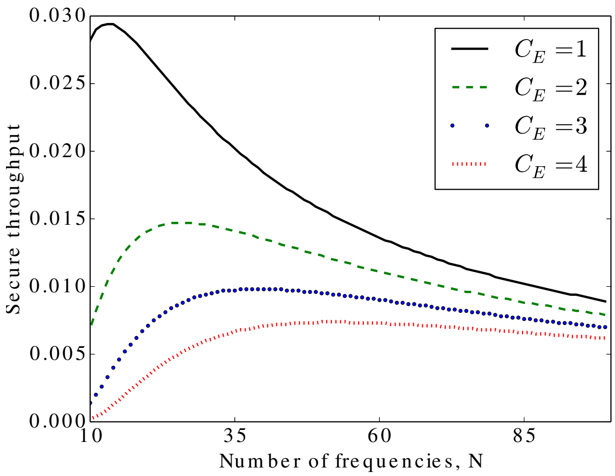

Fig. 2. Secure throughput in the presence of $E = 12$ eavesdroppers listening between 1 and 4 different channels at the same time for a varying number of frequency channels, N.

Figure 1 shows that there are two main factors limiting the secure throughput:

1) the increase in the number of frequencies N which, incidentally, reduces the throughput (probability of communication) between Tx and Rx;
2) the increase in the broadband capability (C_E) of eavesdroppers.

In particular, with respect to the second factor we can observe that the ability to overhear in more than one channel ($C_E = 3$ and 2) even for a lower number of eavesdroppers ($E = 2$ and 4) leads to a lower secure throughput when compared to the narrowband setup with more eavesdroppers ($E = 6$). This phenomenon is mostly due to the fact that, instead of having several eavesdroppers jumping independently through the N frequencies and possibly repeating some frequencies among them, these broadband devices are capable of eavesdropping while individually avoiding repetition among the C_E frequencies they listen to, therefore encompassing a larger number of independent frequencies under eavesdropping.

Figure 2 further depicts the extreme low values of secure throughput obtained, resulting from a larger number of eavesdroppers (E =12). Again the secure throughput decreases with the number of frequencies N. More importantly, this graph illustrates the quite negative effect of increased broadband capabilities of eavesdroppers (C_E) on security. It is also important to mention that these very small values are also the result of the secure throughput being a very demanding metric, in the sense that it takes a single eavesdropper on a unique frequency to tamper the communication and deem the transmission of data insecure; even if other eavesdroppers are unable to overhear communication.

As suggested by *Figure 1* and *Figure 2* and already determined in [10], it is possible to adapt the number of frequencies in order to maximize the secure throughput. In particular, for

Figure 2 the right shift in the maximum is quite noticeable when comparing broadband with narrowband ($C_E = 1$) eavesdropping. In fact, as the number of eavesdropped frequencies increases (due to the broadband characteristics of the devices) so does the amount of necessary hopping frequencies to obtain the maximum secure throughput.

IV. Secure Throughput with Broadband Jamming

In this section we include an analysis of a scenario where we have added a number of J broadband jammers capable of transmitting on C_J frequency channels. The purpose of these defensive agents is to combat eavesdroppers by causing interference on the frequencies where they overhear communication.

Proposition 2. The secure throughput for a setup with one Tx-Rx pair, E broadband eavesdroppers listening in C_E frequencies and J broadband jammers transmitting in C_J frequencies, all of them hopping uniformly at random through N frequency channels is given by

$$\mathcal{T}_s = \frac{N\left(\binom{N-1}{C_E}^E\binom{N-1}{C_J}^J + \binom{N-1}{C_E}^E \neg\binom{N-1}{C_J}^J + \neg\binom{N-1}{C_E}^E \neg\binom{N-1}{C_J}^J\right)}{N^2\binom{N}{C_E}^E\binom{N}{C_J}^J}$$

where

$$C_E < N \wedge C_J < N,$$

and

$$\neg\binom{x-1}{y}^z = \binom{x}{y}^z - \binom{x-1}{y}^z$$

Proof. This formula is divided in three parts, each of which corresponds to one of the three situations described in Section II-B. Again, N corresponds to the number of matching frequencies between the Tx-Rx pair, while:

$\binom{N-1}{C_E}^E\binom{N-1}{C_J}^J$ corresponds to the situation where none of these devices (eavesdroppers and jammers) are listening to the communication channel;

$\binom{N-1}{C_E}^E\neg\binom{N-1}{C_J}^J$ represents the number of cases in which all E eavesdroppers are not listening to the communication channel, and at least one jammer lands on the frequency being used by the Tx-Rx pair (i.e. the complementary of $\binom{N-1}{C_J}^J$);

$\neg\binom{N-1}{C_E}^E\neg\binom{N-1}{C_J}^J$ refers to the number of cases in which at least one eavesdropper and one jammer land on the frequency being currently used by the Tx-Rx pair.

Finally $N^2\binom{N}{C_E}^E\binom{N}{C_J}^J$ represents, once more, all the possible permutations of all the devices present in the system (the Tx-Rx pair, J broadband jammers and E broadband eavesdroppers) hopping through N frequencies. □

A. Analysis

By introducing jammers, we can assess the impact of these defensive agents on the secure throughput of the system. For *Figure 3* we have added one broadband jammer, so that we could highlight the secure throughput improvement of using these warding devices against harmful broadband eavesdroppers. As expected, the difference between both situations (jamming and no jamming) is quite significant for lower values of number of frequencies N and fades away with increasing N due to the reduction in the throughput, as observed in *Figure 1*. It becomes noticeable the advantage of broadband jamming to secure these systems, especially for lower values of number of frequencies.

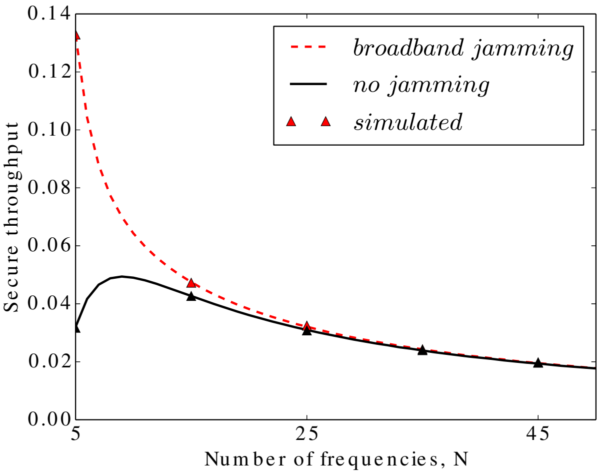

Fig. 3. Secure throughput in the presence of $E = 2$ broadband eavesdroppers listening to $C_E = 3$ frequencies and $J = 1$ broadband jammer transmitting on $C_J = 3$ different channels at the same time for a varying number of frequency channels, N. These results are compared with a no jamming version of this setup.

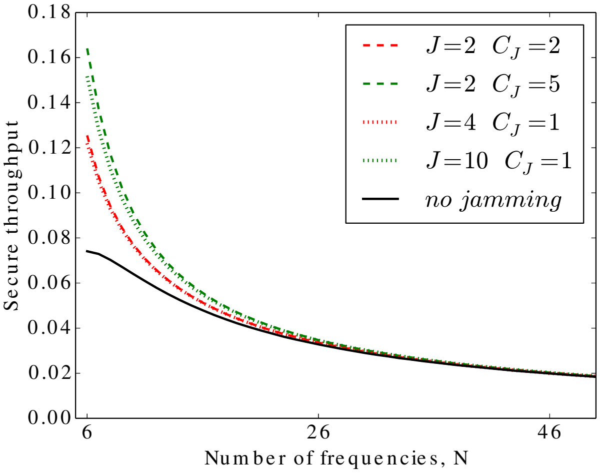

Fig. 4. Secure throughput in the presence of $E = 2$ broadband eavesdroppers listening to $C_E = 2$ different channels at the same time, $J = 4$ and $J = 10$ narrowband eavesdroppers as well as $J = 2$ broadband jammers securing $C_J = 2$, $C_J = 5$ different frequencies, for a varying number of frequency channels, N. These results are compared with a no jamming version of this setup.

In *Figure 4* we consider several jammer configurations to compare broadband jamming against narrowband jamming. We can again see that having jammers allows for a relevant gains in terms of secure throughput. We can also identify a slight increase in the secure throughput when using broadband jamming when compared with the equivalent narrowband version. For example, $J = 10$ jammers operating in $C_J = 1$

frequency leads to a somewhat lower secure throughput than $J = 2$ jammers operating in $C_J = 5$ frequencies, although the overall number of affected frequencies amounts to the same (10) in both cases. The same is noticeable for the cases $J = 4$, $C_J = 1$ and $J = 2$, $C_J = 2$. This happens because of the inherent characteristic of broadband jammers, as they do not repeat frequencies they operate on, allowing for a wider range of frequencies to be covered. This suggests that it is more advantageous to have fewer broadband jammers operating in a larger number of frequencies other than several narrowband jammers. This also reduces the burden of cooperation/synchronization that would be needed among narrowband jammers if, for example, we wanted to avoid jammers lying in the same frequency. Finally, *Figure 5* depicts the positive impact of jammers on the system in the presence of a larger number of eavesdroppers ($E = 20$). Even when presented with broadband adversaries, the negative effect of multiple eavesdroppers can be addressed by jammers by increasing the number of frequencies they operate on. In particular, note that 5 jammers alone operating in 3 frequencies each (dotted green line) are sufficient to ensure reasonable levels of secure throughput against 20 eavesdroppers.

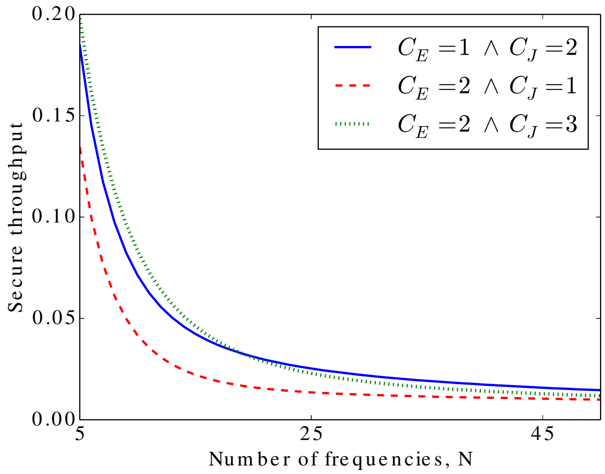

Fig. 5. Secure throughput in the presence of $E = 20$ eavesdroppers and $J = 5$ jammers for different setups (mix of broadband and narrowband devices), for a varying number of frequency channels, N.

V. Conclusion

We characterized the secure throughput (probability of secure communication) of a wireless system operating under Uncoordinated Frequency Hopping, a frequency hopping scheme in which devices hop uniformly at random between a set of frequencies. We considered the impact of broadband eavesdropper adversaries that are capable of overhearing information in multiple frequencies at a time, and broadband friendly jammers that are available to combat those eavesdroppers by causing them interference. We have seen that, like in the narrowband scenario, it is possible to adapt the number of hopping frequencies to maximize the secure throughput and reduce the probability of eavesdropping. We also unveil the positive effect of friendly jammers on the secure throughput, in particular of broadband jammers that are capable of providing reasonable levels of secure throughput against a much larger number of eavesdroppers in the system. The availability of broadband friendly jammers brings the additional benefit of allowing jammers to reduce the number of overlapping frequencies that may already be protected by other jammers, without the need for cooperation/synchronization between jammers. Future directions of this work include evaluating the effect of devices hopping at different rates, as well as incorporating an analytic model featuring the degradation of legitimate communication by jammers.

Acknowledgment

This work was partially funded by the iCIS project under grant CENTRO-07-ST24-FEDER-002003, and the project PEst-OE/EEI/LA0008/2013 (WINCE - Wireless Interference and Coding for Secrecy) funded by the Fundação para a Ciência e Tecnologia (Portuguese Foundation for Science and Technology) and conducted at Instituto de Telecomunicações, Portugal.

References

[1] P. Tague, M. Li, and R. Poovendran, “Mitigation of control channel jamming under node capture attacks,” *IEEE Transactions on Mobile Computing*, vol. 8, no. 9, pp. 1221–1234, September 2009.

[2] C. Pöpper, M. Strasser, and S. Capkun, “Anti-jamming broadcast communication using uncoordinated spread spectrum techniques,” *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 5, pp. 703–715, June 2010.

[3] M. Strasser, C. Pöpper, S. Capkun, and M. Cagalj, “Jamming-resistant key establishment using uncoordinated frequency hopping,” in *IEEE Symposium on Security and Privacy*, 2008, pp. 64–78.

[4] 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.

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

[6] E. Tekin and A. Yener, “The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming,” *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[7] 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.

[8] A. Sheikholeslami, D. Goeckel, H. Pishro-Nik, and D. 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*. IEEE, 2012, pp. 1179–1187.

[9] J. P. Vilela and J. Barros, “Collision-free jamming for enhanced wireless secrecy,” in *IEEE International Workshop on Data Security and PrivAcy in wireless Networks (held jointly with IEEE WoWMoM)*, Madrid, Spain, June 2013.

[10] J. S. Sousa and J. P. Vilela, “A characterization of uncoordinated frequency hopping for wireless secrecy,” in *7th IFIP Wireless and Mobile Networking Conference*, Vilamoura, Portugal, May 2014.

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

[12] 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.

[13] F. Quitin, M. M. U. Rahman, R. Mudumbai, and U. Madhow, “A scalable architecture for distributed transmit beamforming with commodity radios: Design and proof of concept,” *IEEE Transactions on Wireless Communications*, vol. 12, no. 3, pp. 1418–1428, 2013.