A Characterization of Uncoordinated Frequency Hopping for Wireless Secrecy

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*—We characterize the secrecy level of communication under Uncoordinated Frequency Hopping, a spread spectrum scheme where a transmitter and a receiver randomly hop through a set of frequencies with the goal of deceiving an adversary. In our work, the goal of the legitimate parties is to land on a given frequency without the adversary eavesdroppers doing so, therefore being able to communicate securely in that period, that may be used for secret-key exchange. We also consider the effect on secrecy of the availability of friendly jammers that can be used to obstruct eavesdroppers by causing them interference. Our results show that tuning the number of frequencies and adding friendly jammers are effective countermeasures against eavesdroppers.**

I. Introduction

Wireless transmissions have always been particularly vulnerable to attacks of different nature: DoS (Denial of Service), eavesdropping, spoofing, and others which can directly interfere with the transmission of information between nodes. Spread spectrum (SS) techniques such as frequency-hopping SS and direct-sequence SS have helped improve the reliability of wireless communication by transmitting data over different frequencies or spreading patterns. These techniques are usually based on the exchange of a secret code among the intervenients that is used to make the transmission pattern (e.g. the frequency hopping sequence) unpredictable for illegitimate devices. The need for a pre-shared secret may not be adequate or even feasible, for example in spontaneous networks with unknown devices.

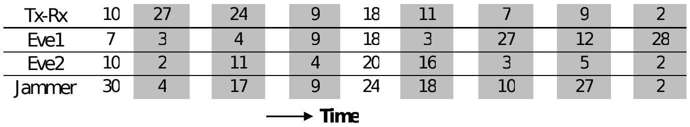
Uncoordinated Frequency Hopping (UFH) [1], [2] is a spread spectrum technique that addresses DoS jamming attacks without relying on a pre-shared secret. UFH operates in a similar way as coordinated frequency hopping, by transmitting information in different frequency channels through time, and constantly hopping between frequencies. However, in this scheme transmitter and receiver randomly hop through frequency channels without agreeing on a channel sequence beforehand. The operation of this scheme is based on the observation that, at some point in time, transmitter and receiver will land on the same frequency without an adversary jammer doing so, therefore being able to communicate reliably. Reliable communication comes at the cost of a high number of lost packets and repetitions, which significantly decreases the throughput performance of the system.

These periods of reliable communication can, however, be used to establish a shared secret that can subsequently be used as the basis for a regular coordinated frequency hopping scheme with higher performance levels.

Recent works on physical-layer security suggest that the physical characteristics of wireless channels may be used to enhance the secrecy level of these networks [3]. This propelled an interest on the use of jammers to secure wireless networks. In this case jammers are considered friendly [4] in the sense that they are willing to assist legitimate communication by causing interference to adversary eavesdroppers. The idea of interference for secrecy appeared in [5], whereby a transmitter with multiple antennas or, alternatively, a set of amplifying relays introduce noise in the system to overcome eavesdropper adversaries. 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. [4] and [7] present an analysis of the impact of jamming on the secrecy level of wireless networks, providing insight on the optimal configurations of jammers and proposing a scheme for selection of jammers in multi-terminal environments. Jammer selection schemes for inter-session interference have been recently proposed in [8], [9], whereby jammers can cause interference while sending their own traffic into the network.

In our present work, we perform an analysis of UFH as a defensive mechanism towards adversary eavesdroppers that aim to overhear as much information as possible. We characterize the inherent level of security that UFH provides against eavesdroppers by calculating its secure throughput, i.e. the probability that transmitter and receiver land on the same frequency without the eavesdroppers doing so. We then assess the effect on the secure throughput of adding friendly jammers whose goal is to cause interference to eavesdroppers without harming legitimate communication. For that, we consider the effect of varying parameters such as the number of jammers and adversary eavesdroppers, and the number of frequencies channels available.

The remainder of this article is organized as follows. Section II describes the system under consideration, including the attacker model and corresponding assumptions. In Section III we characterize the secrecy level of UFH with adversary eavesdroppers alone, while Section IV additionally considers the effect of friendly jammers on secure communication. Section V concludes the paper.



Tx-Rx	10	27	24	9	18	11	7	9	2
Eve1	7	3	4	9	18	3	27	12	28
Eve2	10	2	11	4	20	16	3	5	2
Jammer	30	4	17	9	24	18	10	27	2

Fig. 1. Example of secure communication under UFH. Numbers correspond to frequency channels, and only instances where communication occurs (Tx and Rx on the same channel) are depicted. Secure communication (shaded time-slots) happens when (1) eavesdroppers (Eve) lie on a different frequency than Tx and Rx, or (2) eavesdroppers lie on the frequency of Tx-Rx yet are obstructed by jammers on the same frequency.

II. System and Attacker Model

We consider a system where a transmitter Tx tries to communicate securely with a receiver Rx, while a set Π_e of adversary eavesdroppers ($K = |\Pi_\mathrm{e}|$) tries to overhear legitimate communication. These devices, which are assumed to be within communication range, follow the Uncoordinated Frequency Hopping (UFH) scheme, therefore hopping uniformly at random through a set of N frequency channels. In addition, a set $\Pi_\jmath$ of friendly jammers ($J = |\Pi_\jmath|$) hops uniformly at random between frequencies to assist legitimate communication by causing interference to potential eavesdroppers, if within the same frequency. All devices are equipped with a narrowband transceiver, and therefore send and receive signals on one frequency channel at a time.

Let $x \to y$ denote the event of *successful reception* by a device y of a message sent by x. Similarly, let $x \nrightarrow y$ denote the event of *unsuccessful reception*, i.e. the complementary event of $x \to y$. Successful communication happens when Tx and Rx land on the same frequency channel.

A. Assumptions

We assume that legitimate devices are synchronized and within communication range, i.e. Tx is able to transmit to Rx and jammers, eavesdroppers are able to overhear communication from Tx to Rx, and jammers are able to cause interference to potential eavesdroppers. With that, we abstract away from physical parameters such as transmission powers and distances between devices.

We consider that jammers coordinate with Tx and Rx to avoid harming legitimate communication, while causing interference to potential eavesdroppers. This may be achieved through different mechanisms, such as steered/sectorized [10] transmission towards regions of potential eavesdroppers via directional antennas, or distributed beamforming schemes that have been recently incorporated into regular wireless networks [11], therefore allowing jammers' signals to add up coherently at an intended receiver, while causing interference to potential eavesdroppers.

B. Attacker Model

We consider a passive eavesdropper adversary, who lies silently within communication range to overhear legitimate communication. The eavesdroppers have the same capabilities as Tx, Rx and jammers. In particular, eavesdroppers are equipped with the same type of transceivers as other devices, which allows all of them to hop between frequencies at a similar rate R. If, for instance, eavesdroppers could hop between frequencies much faster than the remaining devices, they would be able to detect legitimate communication on a given frequency and remain on that frequency until communication ends. However, the same kind of reasoning could be applied with respect to jammers, allowing them to hop between frequencies much faster and affect eavesdroppers more frequently, therefore improving the system's security level.

Under this model and as illustrated in *Figure 1*, we consider that secure communication happens when:

1) Tx and Rx land on the same frequency without any eavesdropper doing so;
2) Tx and Rx land on the same frequency as one or more eavesdroppers, but eavesdroppers are obstructed from overhearing legitimate communication through interference caused by jammers on the same frequency.

III. Secure Throughput

The secure throughput measures the transmission rate at which Tx can communicate with Rx without eavesdroppers being able to acquire any information.

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,

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

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

Proposition 1: The secure throughput for a setup with one Tx-Rx pair and K eavesdroppers hopping uniformly at random through N frequency channels is given by

$$\mathcal{T}_\mathrm{s} = \frac{N \times (N-1)^K}{N^{K+2}} \tag{1}$$

Proof: This results from counting the number of favorable cases and the number of possible cases: N is the number of favorable frequencies for the Tx-Rx pair, $(N-1)^K$ are the permutations with repetition of the $N-1$ remaining frequencies where the K eavesdroppers may land without being able to overhear communication, while N^{K+2} are the permutations with repetition of all N frequencies for all devices (K eavesdroppers, plus Tx and Rx). ■

A. Analysis

Figures 2 and 3 depict the behavior of the secure throughput with varying number of frequency channels N, for $K = 4$ and $K = 15$ eavesdroppers, respectively. Notice that the secure throughput assumes very low values, and those values decrease further with growing number of eavesdropper adversaries and number of frequencies. This happens because the secure throughput is a demanding security metric, in the sense that

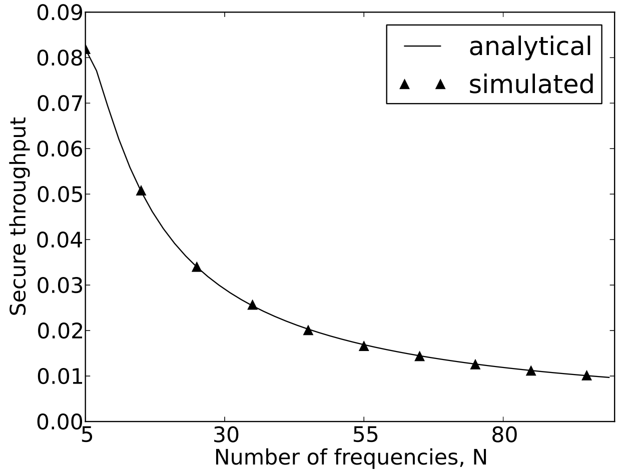


Fig. 2. Secure throughput in the presence of $K = 4$ eavesdroppers for varying number of frequencies, N. The analytical secure throughput is based on (1) and the simulated secure throughput is also presented for comparison.

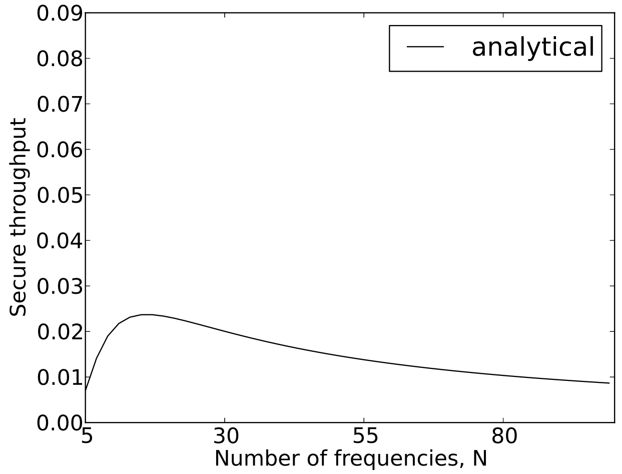


Fig. 3. Secure throughput in the presence of $K = 15$ eavesdroppers for varying number of frequencies, N.

one single eavesdropper being able to overhear communication deems that transmission insecure, even if other eavesdroppers are not able to do so. Increasing the number of frequencies diminishes the probability of legitimate communication, with corresponding impact on the secure throughput. However, the behavior in *Figure 3* suggests that for larger numbers of eavesdroppers one can adapt the number of frequencies to maximize the secure throughput as follows.

Proposition 2: The maximum secure throughput as function of the number of eavesdroppers K is given by

$$\max_{N \in \mathbb{N}} \mathcal{T}_{\mathrm{s}} = K + 1$$

Proof: For fixed but arbitrary K, let

$$f(n) = \frac{n \times (n-1)^K}{n^{K+2}}, n \in [1, +\infty]$$

be the continuous function equivalent to $\mathcal{T}_{\mathrm{s}}$ in (1).

Let $f^{'}(n)$ and $f^{''}(n)$ respectively represent the first and second order derivative of $f(n)$. Since the first derivative of $f(n)$ is

$$f^{'}(n) = \frac{(K-n+1) \times (n-1)^{K-1}}{n^{K+2}},$$

we get the following critical points where $f'(n) = 0$: $n = 1$ and $n = K + 1$, where $n = 1$ is discarded for being irrelevant from a practical standpoint.

By verifying the slope of the double derivative of $f(n)$,

$$f^{''}(n) = (K^2 + K \times (3-4n) + 2 \times (n-1)^2) \times (n-1)^{K-2} \times n^{-K-3}$$

we observe that for $K \in \mathbb{R}^+$, $f^{''}(K+1) < 0$, following that $K + 1$ is a local maximum.

Since the endpoint of $f(n)$ on the domain of n is $\lim_{n \to +\infty} \frac{(n-1)^K}{n^{K+1}} = 0$, the result follows. ■

IV. Secure Throughput with Jamming

We now consider a scenario where a set of J jammers are available to aid the Tx and Rx in securing communication by causing interference to eavesdroppers. These jammers may be devices specifically placed in the system with the purpose of helping legitimate devices to communicate securely, or devices that are silent due to some channel access mechanism to avoid collisions.

Proposition 3: The secure throughput for a setup with one Tx-Rx pair, K eavesdroppers and J jammers hopping uniformly at random through N frequency channels is given by

$$\mathcal{T}_{\mathrm{s}} = \frac{N \times (N-1)^K \times N^J + N \times (N^K - (N-1)^K) \times (N^J - (N-1)^J)}{N^{J+K+2}}$$

Proof: This results from counting the number of favorable and the number of possible cases as follows. We consider a transmission secure if

1) the Tx-Rx pair land on a given frequency without any eavesdropper doing so, or
2) the Tx-Rx pair land on a given frequency with one or more eavesdroppers, and one or more jammers are available at that frequency to cause interference to eavesdroppers.

Recall that we assume the use of techniques to mitigate the harmful effect of jammers over legitimate communication, as described in Section II-A.

$N \times (N-1)^K \times N^J$ represents the number of cases in which Tx and Rx land on one of the N frequencies, while all K eavesdroppers land on any of the remaining $N - 1$ frequencies and jammers land on any frequency N, therefore representing case 1) above.

$N \times (N^K - (N-1)^K) \times (N^J - (N-1)^J)$ represents the number of cases in which Tx and Rx land on one of the N frequencies, while at least one eavesdropper lands on that frequency, i.e. $N^K - (N-1)^K$ (the complementary of $(N-1)^K$). Similarly, $N^J - (N-1)^J$ corresponds to at least one jammer landing on that same frequency as Tx, Rx and eavesdropper(s).

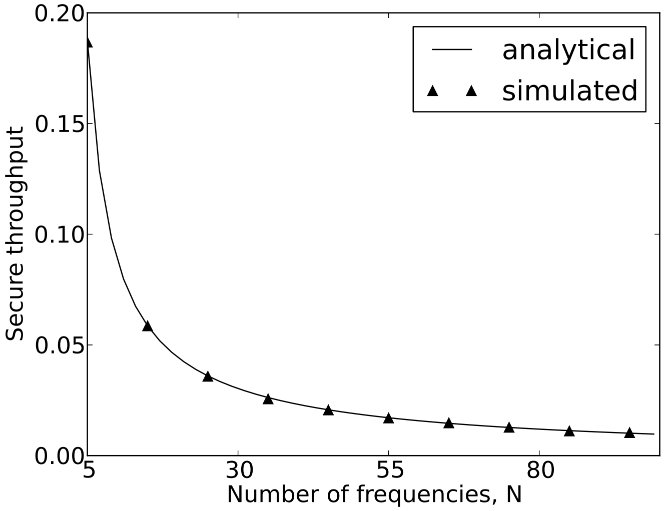


Fig. 4. Secure throughput in the presence of $K = 4$ eavesdroppers and $J = 5$ jammers for varying number of frequencies, N. The analytical secure throughput is based on Proposition 3, and the simulated secure throughput is presented for comparison.

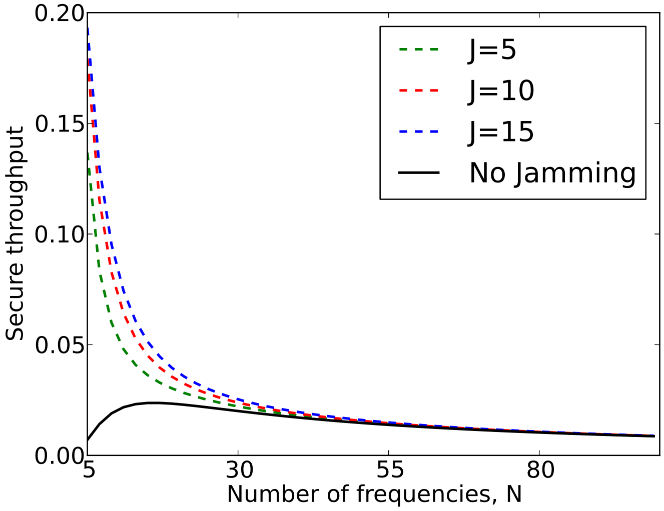


Fig. 5. Secure throughput in the presence of $K = 15$ eavesdroppers for $J = 5$, $J = 10$, $J = 15$ jammers and No Jamming, for varying number of frequencies, N.

Finally, N^{J+K+2} represents all possible cases for J jammers, K eavesdroppers, Tx and Rx hopping through N frequency channels. ■

A. Analysis

Figure 4 depicts the secure throughput with varying number of frequency channels N, for $K = 4$ eavesdroppers and $J = 5$ jammers. Notice that the secure throughput compares favorably with similar results without jamming in *Figure 2* due to the positive effect of friendly jammers on secure communication. *Figure 5* shows the secure throughput for larger number of eavesdroppers $K = 15$ and different numbers of jammers. In this case, even with larger number of eavesdroppers, the secure throughput does not suffer much when compared to *Figure 4* because of the positive effect of jammers on security. Moreover, the secure throughput in *Figure 5* compares favorably with the same setup but without jammers in *Figure 3*, specially for lower values of of number of frequencies, where the secure throughput is not dominated by the low probability of legitimate communication.

V. Conclusions

We characterize the secure throughput (i.e. probability of secure communication) of a wireless system operating under Uncoordinated Frequency Hopping (UFH). We show how to maximize the secure throughput by adapting the number of frequencies to the number of eavesdroppers in the system. We also unveil the positive effect on the secure throughput of friendly jammers that are available to assist legitimate communication by causing interference to eavesdroppers. Although UFH provides low values of secure throughput which would be unsuitable for regular communication, by maximizing the frequency of secure communication periods one could take advantage of those periods to exchange secret-keys that may be used to protect subsequent communication. Future directions of this work include expanding our system model to feature a degradation factor of legitimate communication by jammers, different hopping rates for the devices, and the development and implementation of these schemes in test-bed.

References

[1] 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.

[2] 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.

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

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

[6] 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.

[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] 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.

[11] 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.