# INCREASING INFORMATION SECRECY BY JAMMING WITH UNIFORMLY DISTRIBUTED EAVESDROPPERS

Aneta Velkoska PhD.[1], M.Sc. Natasha Paunkoska[2], Ninoslav Marina PhD.[1]
Faculty of Communication Networks and Security, University of Information Science and Technology, Ohrid[1]
Faculty of Information Systems, Visualization, Multimedia and Animation, University of Information Science and Technology, Ohrid[2]
aneta.velkoska@uist.edu.mk

***Abstract:*** *Transmission of confidential messages over wireless networks between a transmitter and a receiver in the presence of illegitimate receivers called eavesdroppers is an active area of research. Cooperation by jamming can improve information-theoretic secrecy in wireless networks. However, randomly chosen jammers can have a negative impact on the secrecy capacity. Our goal is to provide a closed form for positioning the friendly jammers in two-dimensional wireless network with uniformly distributed eavesdroppers while two legitimate partners are communicating.*

**Keywords**: INFORMATION-THEORETIC SECRECY, SECRECY CAPACITY, UNIFORMLY DISTRIBUTED EAVESDROPPERS, JAMMER

## *1. Introduction*

The issues of privacy and security in wireless communication networks have taken on an increasingly important role as these networks continue to flourish worldwide. Traditionally, security is viewed as an independent feature addressed above the physical layer and all widely used cryptographic protocols are designed and implemented assuming the physical layer has already been established and is error free.

In contrast with this framework, there exist both theoretical and practical contributions that support the potential of physical layer security ideas to significantly strengthen the security of digital communication systems. The basic principle of information-theoretic security — widely accepted as the strictest notion of security — calls for the combination of cryptographic schemes with channel coding techniques that exploit the randomness of the communication channels to guarantee that the sent messages cannot be decoded by a third party maliciously eavesdropping on the wireless medium (see Fig. 1).

A suitable metric to assess the secrecy level of a system is the secrecy capacity [1], i.e. the maximum transmission rate at which the source can communicate with the receiver without the eavesdropper being able to acquire any information.

Secrecy capacity can be increased in two ways: (a) by improving the signal-to-noise ratio (SNR) of the legitimate receiver (e.g. by shortening the distance to the transmitter) or (b) by reducing the SNR of the eavesdropper (e.g. by adding controlled interference). Interference then emerges as a valuable resource for wireless security. Friendly jammers, with different levels of channel state information, help the legitimate parties by causing interference to possible eavesdroppers.

Results shows that cooperation can significantly improve information - theoretic secrecy in wireless networks but the randomly chosen relay nodes can have a negative impact on the secrecy capacity. Finding the optimum positions for cooperating jammers which minimize the size of the vulnerability region in order to increase secrecy region is a challenging task. Therefore, our interest is solving this task in a 2D wireless network with two legitimate communication partners, uniformly distributed eavesdroppers and friendly jammers.

The paper is organized as follows. Section 2 presents related work and our goal. Section 3 describes our system model and problem formulation. In Section 4 we present the main result and investigate it in particular scenarios. Section 5 concludes the paper.

## *2. Related work*

Several interference generation schemes have been proposed to improve the secrecy rate of different types of wireless channels. A scheme for generation of artificial noise is proposed in [2] whereby a transmitter with multiple antennas or, alternatively, a set of amplifying relays introduces noise in the system that results in low outage probabilities of secrecy rate. In [3], a cooperative jamming scheme is proposed in which an otherwise disadvantaged user can help improve the secrecy rate by jamming a nearby eavesdropper. [4] 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 [5].

In [6], the secrecy level of two nodes communicating in the presence of eavesdroppers placed anywhere in a confined region is investigated. Friendly jammers, with different levels of channel state information, help the legitimate parties by causing interference to possible eavesdroppers. Results shows that jamming near the legitimate receiver leads to a small secrecy improvement and requires channel state information that may not always be available and multiple jammers are needed to achieve relevant secrecy gains throughout the entire confined region.

Secrecy of a cryptographic system is based on the secrecy of the secret key, and not on the secrecy of the cryptographic algorithm. Secret keys between communicating parties are exchanged in two ways: through physically secure channels e.g. a diplomatic suitcase or through public-key cryptographic protocols. The exchanged secret key is called master key, and is typically used to encrypt and exchange session keys, which are then used to encrypt the data flow between the two parties. In [7] and [8] is examined the possibility to use information-theoretic secrecy to exchange a master-key between the two communicating parties in a wireless network with multiple eavesdroppers via user cooperation. Secrecy capacity determines how quickly the master key will be exchanged between the two parties. Since the two communicating parties usually change the master key very rarely, it is sufficient to transmit it at even very small rates. Once the master key is exchanged, the legitimate parties can start communicating at maximum data rate since their communication channel is cryptographically protected achieving computational secrecy [9].

In order to tackle the unknown eavesdropper locations in [8] the pre-master key message is split into a large number B of data blocks. The two communicating nodes ensure that the entire pre-master key message is received correctly at the receiving node, which is required for the computation of the master key. Each data block is sent for a different network configuration of jammers. As the number of transmitted blocks grows, the eavesdropper is less able to intercept in a network configurations with large number of nodes. The secrecy level is observed in two-dimensional wireless network with two communication nodes: a transmitter at position (0, 0) and a receiver at position (1, 0), *N* friendly nodes (jammers), and a passive eavesdropper which does not transmit any signal, and tries to intercept the information that is transmitted between the pairs of legitimate nodes, hence reducing the secrecy capability of

the network. Its location is unknown to the two communicating nodes.

The following notation is used:

$X$ the transmitted signal from the transmitter,

$Y$ the received signal at the receiver,

$Z_e$ the received signal at the eavesdropper,

$J_k$ the received interfering signal from jammer k,

$V, V_e$ the additive noise at receiver and eavesdropper, which are independent zero mean Gaussian random variables with variance $\sigma^2$,

$[N]$ the set of all positive integers smaller than or equal to $N$,

$K(x)$ $K(x) = \frac{1}{2}\log_2(1+x)$,

$C_s$ secrecy capacity between the transmitter and the receiver,

$d_{j,i}$ the distance between nodes i and j,

$\beta$ the path-loss coefficient [10], $\beta = 3$ is used.

The additive white Gaussian model is considered. Then, the received signal at the receiver $r$ is

$$Y = d_{t,r}^{-\beta/2} X + \sum_{k\in[N]} d_{k,r}^{-\beta/2} J_k + V,$$

and the received signal at the eavesdropper $e$ equals

$$Z_e = d_{t,e}^{-\beta/2} X + \sum_{k\in[N]} d_{k,e}^{-\beta/2} J_k + V_e,$$

The instantaneous secrecy capacity [11] of the channel between the transmitter and the legitimate receiver is

$$C_s = \max\left(C_{t,r} - C_{t,e}, 0\right), \quad (1)$$

where the point to point capacity with jamming between transmitter $t$ and receiver $r$ or eavesdropper $e$, respectively is given by [8]:

$$C_{t,r} = K\left(\frac{P_t d_{t,r}^{-\beta}}{\sigma^2 + \sum_{j\in[N]} b_j P_j d_{j,r}^{-\beta}}\right),\ C_{t,e} = K\left(\frac{P_t d_{t,e}^{-\beta}}{\sigma^2 + \sum_{j\in[N]} b_j P_j d_{j,e}^{-\beta}}\right), \quad (2)$$

such that $b_j = 1$ if jammer $j$ is switched on, and $b_j = 0$ if jammer $j$ is switched off. Thus, each network configuration is defined by the array $[b_1, b_2, ..., b_N]$ and $P_t$ is the transmitter's power.

If the capacity of the communication channel between the transmitter and the eavesdropper $C_{t,e}$ is larger than the capacity of the channel between the two communicating nodes $C_{t,r}$ then $C_s = 0$, otherwise, $C_s > 0$. Geometrical area $R_s \subset R^2$ where an eavesdropper can be positioned and still $C_s > 0$ is called *secrecy region* and geometrical area $R_v \subset R^2$ where an eavesdropper can be positioned resulting in $C_s = 0$ is called *vulnerability region* [12].

Analysis shows that breaking the pre-master key message into data blocks, and using a different network configuration with cooperative jamming for each data block can significantly reduce the vulnerability region. But positions of cooperating jammers are quite important for the resulting secrecy region. Finding the optimum positions for cooperating jammers which minimize the size of the vulnerability region is still open question.

Therefore, our interest is solving this task in a 2D wireless network with two legitimate communication partners, uniformly distributed eavesdroppers and friendly jammers. Our work differs from previous in that we provide a closed form for positioning the jammers in a 2D region with uniformly distributed eavesdroppers. In particular we characterize the secrecy regions by expected positions of the jammers in a $[0,1]\times[0,1]$ region with uniformly distributed eavesdroppers.

## *3. System model and problem formulation*

We consider 2D wireless network with two communication nodes: a transmitter at position (0, 0) and a receiver at position $(r_1, r_2)$, $0 \le r_1, r_2 \le 1$, in presence of uniformly distributed passive eavesdroppers $Æ = \{ E_1, E_2, E_3, \dots \}$. Our goal is to find closed form for positioning the jammers $J(a, b)$ in a confined region $[0,1]\times[0,1]$ in order to characterize the secrecy regions in the system.

In the rest of the paper, we assume that the transmitter and all jammers have equal transmitting power $P_t = P_i = P$, $j \in [N]$. Since the function $K(x)$ is monotonically increasing, plugging equations (2) in (1), it follows that the secrecy capacity $C_s$ is positive if

$$\frac{d_{t,r}^{-\beta}}{\sigma^2 + \sum_{j\in[N]} b_j P d_{j,r}^{-\beta}} > \frac{d_{t,e}^{-\beta}}{\sigma^2 + \sum_{j\in[N]} b_j P d_{j,e}^{-\beta}}, \quad (3)$$

Since we want to characterize the secrecy regions in the system by the position of the jammers in a confined $[0,1]\times[0,1]$ region we assume that there is a single jammer. So, plugging $N = 1$, $j = 1$ in (3),

$$\frac{d_{t,r}^{-\beta}}{\sigma^2 + P d_{j,r}^{-\beta}} > \frac{d_{t,e}^{-\beta}}{\sigma^2 + P d_{j,e}^{-\beta}}, \quad (4)$$

In order to achieve information theoretic secrecy for the master key in the presence of eavesdroppers, it is sufficient that the signal quality at the eavesdropper is sufficiently degraded by the artificial noise generated by the jamming nodes for at least one configuration. In that case at least one data block out of B data blocks is not intercepted, and consequently the master key cannot be computed at the eavesdropper.

Since the position of the eavesdroppers is unknown, we assume that they are uniformly distributed over the region $[0,1]\times[0,1]$ and for the distances from the transmitter to the eavesdropper $d_{t,r}$ and from the jammer to the eavesdropper $d_{j,e}$ we consider their mean distances.

The mean distance of any fixed point $A(x_a, y_a)$ and some random nodes $Æ = \{ E_1, E_2, E_3, \dots \}$ uniformly distributed over region $[0,1]\times[0,1]$ is:

$$m(T, \mathsf{E}) = \int_0^1\int_0^1 \sqrt{(x-x_a)^2 + (y-y_a)^2}\, dxdy. \quad (5)$$

If we plugging $x_a = 0$, $y_a = 0$ in (5), the mean distance from the transmitter to the set of uniformly distributed eavesdroppers over the region $[0,1]\times[0,1]$ is:

$$d_{t,e} = m(T, \mathsf{E}) = \int_0^1\int_0^1 \sqrt{x^2 + y^2}\, dxdy = 0.7652. \quad (6)$$

## 4. Main result

**Theorem 1.** *The mean distance between a jammer J(a, b) and a set of uniformly distributed eavesdroppers over the region* $[0,1]\times[0,1]$ *is*

$$d_{j,e}=\frac{(1-a)^3}{12}\Omega_1\big((1-b,1-a);\ (b,1-a)\big)+$$
$$+\frac{(1-b)^3}{12}\Omega\big((a,1-b);\ (1-a,1-b)\big)+ \quad (7)$$
$$+\frac{a^3}{12}\Omega\big((1-b,\ a);\ (b,a)\big)+\frac{b^3}{12}\Omega\big((a,\ b);\ (1-a,\ b)\big),$$

*where*

$$\Omega_1\big((x,y);\ (z,w)\big)=\ln\big(\Phi(x,y)\Theta(z,w)\big)+\Psi(x,y)\Psi(z,w),$$
$$\Omega\big((x,y);\ (z,w)\big)=\ln\big(\Phi(x,y)\Phi(z,w)\big)+\Psi(x,y)\Psi(z,w),$$
$$\Theta(x,y)=\frac{b+1+x-y+\sqrt{x^2+y^2}}{b+1-x+y-\sqrt{x^2+y^2}},$$
$$\Phi(x,y)=\frac{x-y+\sqrt{x^2+y^2}}{x+y-\sqrt{x^2+y^2}},\Psi(x,y)=\frac{x}{y}\sqrt{1+\left(\frac{x}{y}\right)^2}.$$

*Proof.* Plugging $x_a = a$, $y_a = b$ in (5), where $a,b\in[0,1]$, the mean distance from the jammer to the set of uniformly distributed eavesdroppers over the region $[0,1]\times[0,1]$ is:

$$d_{j,e}=m(J,\mathsf{E})=\int_0^1\int_0^1\sqrt{(x-a)^2+(y-b)^2}\,dxdy\ . \quad (8)$$

This integral will require the following substitutions,

$$u = x-a \qquad v = y-b \qquad dxdy = dudv$$
$$x = 0 \Rightarrow u = -a, \qquad x = 1 \Rightarrow u = 1-a$$
$$y = 0 \Rightarrow v = -b, \qquad y = 1 \Rightarrow v = 1-b$$

Plugging these substitutions in (8),

$$d_{j,e}=m(J,\mathsf{E})=\int_{-a}^{1-a}\int_{-b}^{1-b}\sqrt{u^2+v^2}\,dudv. \quad (9)$$

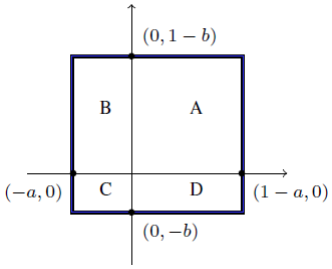


Fig. 1

This integral is considered in four regions (Fig. 1), A, B, C and D. In all these it requires the following trig substitutions,

$$u = p\cos\theta \quad v = \sin\theta \quad dudv = pdpd\theta$$

and results in equation (7). +

For particular position of the receiver ($r_1$, $r_2$) in the region $[0,1]\times[0,1]$ the secrecy regions where the jammer will degrade the signal quality at the eavesdropper by generating artificial noise can be obtained by plugging equation (7) in the inequality (4).

We will consider two different scenarios, first when the receiver is at position (0, 0.5) and second at position (0.5, 0.5).

**First scenario**, 2D wireless network with two communication nodes: a transmitter at position (0, 0) and a receiver at position (0, 0.5), in presence of uniformly distributed passive eavesdroppers Æ = { $E_1$, $E_2$, $E_3$, … }, (Fig. 2). We use that $P/\sigma^2=10$, where $\sigma^2$ is the noise power, and $\beta=3$.

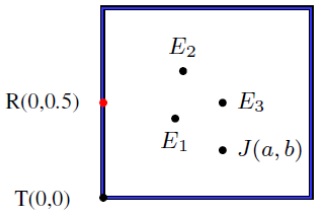


Fig. 2

Since the receiver is at position (0, 0.5),

$$d_{t,r}=0.5 \text{ and } d_{j,r}=\sqrt{a^2+(b-0.5)^2} \quad (10)$$

Plugging (6), (7) and (10) in (4) we obtain the secrecy regions presented in Fig.3. Positioning the jammer in the region $[0,1]\times[0,1]$ between the blue line (dot line) and the light blue line; between the green line and the orange line; between the red line and the closed curve in the middle, we will obtain positive secrecy capacity in the system.

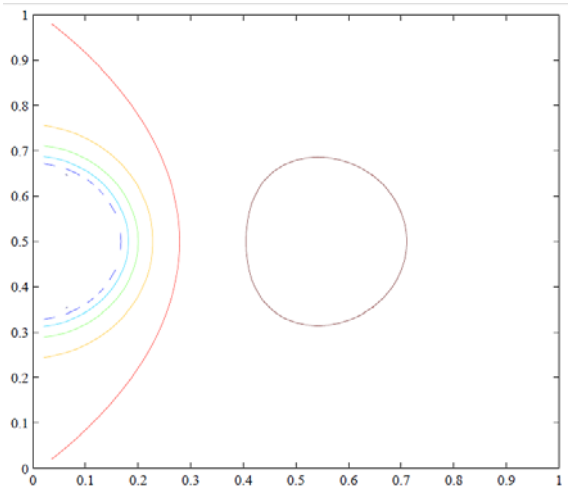


Fig. 3. Boundaries of secrecy in a confined region $[0,1]\times[0,1]$ with transmitter at (0, 0), receiver at (0, 0.5) and uniformly distributed eavesdroppers.

**Second scenario,** 2D wireless network with two communication nodes: a transmitter at position (0, 0) and a receiver at position (0.5; 0.5), in presence of uniformly distributed passive eavesdroppers Æ = { $E_1$, $E_2$, $E_3$, … }, (Fig. 4). We use that $P/\sigma^2=10$, where $\sigma^2$ is the noise power, and $\beta=3$.

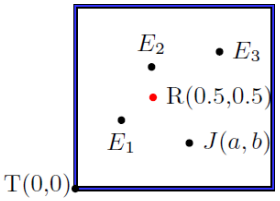


Fig. 4

Since the receiver is at position (0.5, 0.5),

$$d_{t,r} = 0.866 \text{ and } d_{j,r} = \sqrt{(a-0.5)^2 + (b-0.5)^2} \ . \quad (11)$$

Plugging (6), (7) and (11) in (4) we obtain the secrecy regions presented in Fig.5. Positioning the jammer in the region $[0,1]\times[0,1]$ between the dark blue line (dot line) and the blue line (dot line); between the light blue line and the green line; between the orange line and the red line, and outside the dark red line (the largest closed curve) we will obtain positive secrecy capacity in the system.

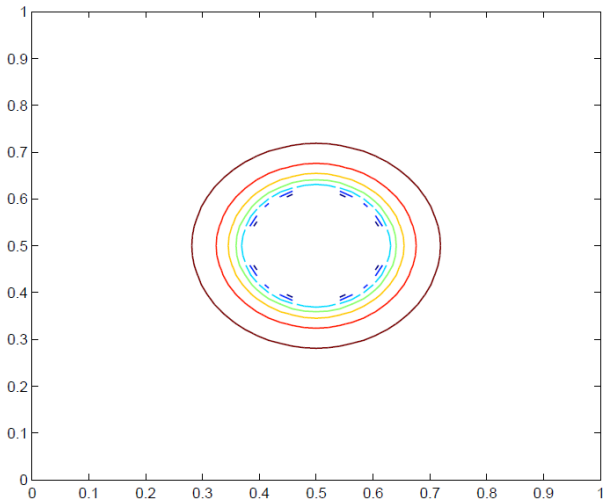


Fig. 5. Boundaries of secrecy in a confined region $[0,1]\times[0,1]$ with transmitter at (0, 0), receiver at (0.5, 0.5) and uniformly distributed eavesdroppers.

Notice, that in both scenarios the jamming near the legitimate receiver results with small secrecy regions, so once again we confirm that as the jammer is closer to the legitimate receiver the jamming leads to a small secrecy improvement.

## *5. Conclusion*

Positions of cooperating jammers are quite important for the resulting secrecy region. Finding the optimum positions for cooperating jammers which decrease the vulnerability region still is an open problem. In this paper we provide a closed form for positioning a single jammer in two dimensional wireless networks such the secrecy region is completely determined. With our model we confirm that the jamming near the legitimate receiver results with small secrecy regions. Our next challenge is to characterize the secrecy region in two and higher dimensional wireless network by obtaining a closed form for determining the positions of multiple cooperating jammers.

## *References:*

[1] Wyner, A. D.: The wire-tap channel. Bell System Technical Journal, vol. 54, pp. 1355–1387 (1975)

[2] Goel, S., Negi, R.: Guaranteeing secrecy using artificial noise. IEEE Transactions on Wireless Communications, vol. 7, no. 6, pp. 2180–2189 (2008)

[3] Tekin, E., Yener, A.: 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 (2008)

[4] Lai, L., Gamal, H. E.: The relay-eavesdropper channel: Cooperation for secrecy. IEEE Transactions on Information Theory, vol. 54, no. 9, pp. 4005–4019 (2008)

[5] Tang, X., Liu, R., Spasojevic, P., Poor, H. V.: Interference-assisted secret communication. In: IEEE Information Theory Workshop (ITW), Porto, Portugal, pp. 164168 (2008)

[6] Vilela, J. P., Bloch, M., Barros, J., McLaughlin, S. W.: Wireless Secrecy Regions with Friendly Jamming. In: IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, pp. 256–266 (2011)

[7] Marina, N., Stojanovski, T. D., Poor, H. V.: Increasing the Information-Theoretic Secrecy by Cooperative Relaying and Jamming. 50th Annual Allerton Conference on Communication, Control, and Computing (2012)

[8] Stojanovski, T. D., Marina, N.: Secure Wireless Communications via Exhaustive Cooperative Jamming Against a Single Eavesdropper. 20th Telecommunications Forum TELFOR, Belgrade, (2012)

[9] Shannon, C. E.: Communication theory of secrecy systems. In: Bell Systems Technical Journal, vol. 28, pp. 656-715 (1949)

[10] Rappaport, T. S.: Wireless Communications: Principles and Practice. Prentice Hall (1996)

[11] Leung-Yan-Cheong S., Hellman, M.: The Gaussian wire-tap channel. In: IEEE Transactions on Information Theory, vol. 24, no. 4, pp. 451–456 (1978)

[12] Marina, N., Bose, R., Hjrungnes, A.: Increasing the secrecy capacity by cooperation in wireless networks. In Proceedings of the IEEE Symposium on Personal and Indoor Mobile Radio Communications, pp. 19781982 (2009).