COOPERATIVE JAMMING METHOD USED FOR INCREASING SECRECY CAPACITY OF WIRELESS CHANNELS

Natasa Paunkoska, MSc
Faculty of Communication Networks and Security
UIST St. Paul the Apostle
Ohrid, Macedonia

Aneta Velkova, MSc
Faculty of Communication Networks and Security
UIST St. Paul the Apostle
Ohrid, Macedonia

Ninoslav Marina, PhD
Faculty of Communication Networks and Security
UIST St. Paul the Apostle
Ohrid, Macedonia

INTRODUCTION

Wireless networks, especially decentralized networks are use tremendously these days. Because of these properties and broadcast nature of the wireless medium they are very sensitive to passive and active attacks from unwanted parties. In 1975, Wyner defined the wiretap channel for establishing the possibility to create secure communication on the physical layer without use of cryptographic algorithms [1]. Since then many information theoretic results [2] based on this channel focus on the idea that there is much to be obtained from security coding at the physical layer. The aim of information-theoretic secrecy is to provide perfect secure communication between two legitimate communicating parties in presence of an eavesdropper.

Introducing additional node jammer or 'unfriendly nodes' as a cooperative method in the communication, that will perform intentional noise on the eavesdropper will help in increasing the achievable secrecy rates. There are many results about the transmission of confidential messages over wireless networks by using the multiple network configurations with friendly jammers. In [3], [4] it is concluded that cooperation can significantly improve information-theoretic secrecy in wireless networks, even though the results are tightly related to the entities position. The main emphasis is placed on finding the eavesdropper location, which may be placed anywhere in the wireless network, due to minimization of the vulnerability region.

Therefore, in this research work is consider establishment of positive secrecy capacity by investigated the cases with single jammer and single eavesdropper according to unknown location of the intruder.

SYSTEM MODEL AND PROBLEM FORMULATION

In this research work we consider the scenario depicted in Fig.1. Two-dimensional wireless network (square region ***R)*** with two communication nodes: legitimate transmitter (T) and legitimate receiver (R) with predefined positions, one friendly node (jammer J) that is also fixed point with coordinates (x_j, y_j) and one eavesdropper (**E**) that is uniformly distributed random point E_1, E_2,....E_n in the region ***R***. The eavesdropper does not transmit any signal, and tries to intercept the information that is transmitted between the pairs of legitimate nodes, hence reducing the secrecy capacity of the network.

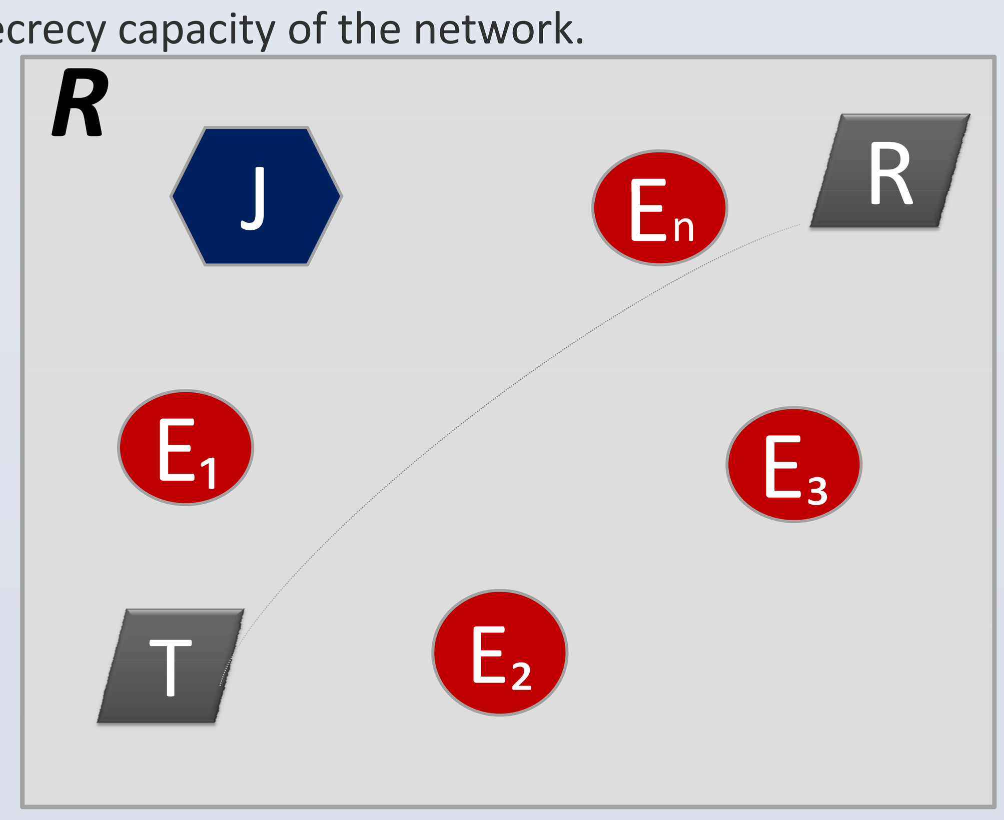

Fig.1 Secure communication in presence of eavesdropper, assisted by jammer

The idea is to be calculate the mean distance between a fixed point and a uniformly distributed random variable.

$$m(J) = E(dist(J,\mathbf{E}))$$

Without loss of generality can be assumed that the square has side 1. And d_{je} is the mean distances between the jammer and all uniformly distributed positions of the eavesdropper.

$$d_{je} = m(x_j, y_j) = \int_0^1 \int_0^1 \sqrt{(x-x_j)^2 + (y-y_j)^2}\,dxdy \qquad (1)$$

And d_{te} is the mean distances between the transmitter and all uniformly distributed positions of the eavesdropper.

$$d_{te} = m(x_t, y_t) = \int_0^1 \int_0^1 \sqrt{(x-x_t)^2 + (y-y_t)^2}\,dxdy \qquad (2)$$

Additional useful notations:

C_s	secrecy capacity between the transmitter and receiver
d_{tr}, d_{jr}	distance between transmitter and receiver, jammer and receiver
β	the path-loss coefficient, β = 3
$P_t = P_j = P$	transmitter power, jammer power
K(x)	$K(x) = 1/2\log_2(1+x)$
σ^2	variance for additive white Gaussian model, N(0,1)

SECRECY CAPACITY FOR COOPERATIVE JAMMUNG METHOD

Cooperating jamming method can increase the secrecy of the communication between T and R, and reduce the vulnerability region. In this technique, the jammer transmits a jamming signal that is independent of the source message with the goal to interfere with the eavesdropper's received signal. 'Unfriendly' nodes which are close to the eavesdropper, or closer to the eavesdropper than to the legitimate receiver, are likely to be useful jammers. The eavesdropper will be obstructed with interference, which mean it will become much weaker than the legitimate receiver for interrupting the legitimate communication.

The capacity between transmitter and receiver and transmitter and eavesdropper is calculated as:

$$C_{t,r} = K\left(\frac{d_{t,r}^{-\beta}}{\sigma^2 + Pd_{t,r}^{-\beta}}\right) \qquad C_{t,e} = K\left(\frac{d_{t,e}^{-\beta}}{\sigma^2 + Pd_{t,e}^{-\beta}}\right) \qquad (4)$$

The secrecy capacity between the legitimate transmitter and receiver is given as:

$$C_s = C_{t,r} - C_{t,e} \qquad (5)$$

From equitation (5) we can conclude that, if $d_{t,r} < d_{t,e}$ than the secrecy capacity is positive $C_s > 0$ and that we can expect secure communication between the both legitimate users in presence of intruder.

CONCLUSION

Cooperative jamming method can significantly increase the secrecy region in wireless networks, which is the region where eavesdroppers can be present and still information-theoretic secrecy is guaranteed.

Positions of cooperating jammers are quite important for the resulting secrecy region.

Using fixed position for the jammer and uniform distribution for the eavesdropper, positive secrecy capacity in the system model can be obtain in case when the distance between transmitter and receiver is smaller than the distance between transmitter and eavesdropper.

FUTURE WORK

- Choosing the best distribution for position of the jamming node.
- Introducing more than one jammer in the communication system.
- Involving more than one eavesdroppers with unknown locations.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel", Bell Syst. Tech. J., vol. 54, no. 8, pp. 2–10, October 1975

[2] C. Shannon, "Communication theory of secrecy systems", Bell System Technical Journal, 28(D):656–715, 1949.

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

[4] T. Draganov Stojanovski, N. Marina, "Secure Wireless Communications via Exhaustive Cooperative Jamming Against a Single Eavesdropper", 20th Telecommunications Forum TELFOR, Belgrade, November 2012.

[5] N. Shekutkovski, "Matematicka analiza 1", Prosvetno Delo, Skopje 2008.

CONTACT

Natasa Paunkoska
natasa.paunkoska@uist.edu.mk

Aneta Velkoska
aneta.velkoska@uist.edu.mk

Ninoslav Marina
rector@uist.edu.mk

University of Information Science and Technology "St. Paul the Apostle"
Partizanska B.B. Ohrid 6000 Republic of Macedonia Tel. +389 46 550003 Fax. +389 46 550004
www.uist.edu.mk