Advanced Research in Electrical and Electronic Engineering
Print ISSN: 2349-5804; Online ISSN: 2349-5812 Volume 1, Number 3 (2014) pp. 66-70

http://www.krishisanskriti.org/areee.html

Cooperative Jamming for Physical Layer Security in Scalable Wireless Networks: A Review

Kaushal Kumar

Department of Electronics & Communication Engineering
National Institute of Technology, Kurukshetra, India

Abstract: **Cooperative jamming, a potential supplement can be used to improve physical layer based security by transmitting a weighted jamming signal to create interference at the eavesdropper. The secrecy rate is derived for cooperative jamming technique in terms of network throughput. We have analyzed the effect of Aloha protocol with cooperative jamming on the secrecy capacity of large scale network .To implement cooperative jamming with Aloha protocol a transmitter can be considered as a source or as a friendly jammer with the massage transmission probability *p*. We observed that an optimum level of security can be achieved for a specific value of jammer power using cooperative jamming and at the moderate value of massage transmission probability *p* using cooperative jamming with Aloha protocol.**

Keywords: **Jamming, Physical Layer, Scalable, Aloha protocol.**

1. INTRODUCTION

Confidentiality of data is a fundamental requirement for any wireless network due to significant growth in wireless applications in contemporary times. The performance of wireless communication has been degraded significantly due to open and shared medium and makes the system vulnerable to security threats. Earlier, complex cryptographic algorithms were used for security at higher network layers [1]. An information-theoretic approach at the physical layer can be used for secure communic-ation without using key encryption.Physical layer security exploits the channel state information(CSI) or characteristics of transmission medium to improve the intended receiver's channel quality. In the cooperative jamming scheme, when source transmits its message, the jammer interferes in order to confuse the eavesdropper. An artificial jamming signal that is independent of source, is transmitted to create interference at eavesdropper. In 1975, Wyner worked in the direction of physical layer security for single point-to-point communication. The most commonly used physical layer security schemes are decode-and- forward (DF), amplify-and-forward (AF) and cooperative jamming. However, the traditional physical layer based security can be compromised by channel conditions; if the main channel is worse than eavesdropper's channel , the secrecy capacity is typical zero as it cannot be negative [2- 3]. Csiszar and Korner generalized the transmission of confidential messages over broad- cast channels to the wireless channel and multi-user scenarios in [4-6]. Most of the studies on physical layer security deal with the network involving small number of nodes. Few studies has also been carried out for decentralized networks. The network connectivity [7-8] and coverage have been studied with physical layer constraints. These connectivity results do not concern with network throu -ghput . Secrecy capacity scaling laws have been analysed to provide some insight in to network throughput .

In this report, a different design objectives to implement cooperative scheme and cooperative jamming with Aloha protocol have been focused. In general cooperative scheme, interaction between the source , destination and eavesdropper in the presence of a friendly jammer having two antenna elements has been analysed to investigate the physical layer based security and the cooperative jamm- ing technique with Aloha protocol has been discussed to improve the secrecy capacity of large scale decentralized networks. An analytical formulation of secrecy capacity has been done with two antenna element jammer node for general cooperative jamming scheme. A matric termed as secrecy transm - ission capacity has been used to characterize the network throughput of large scale decentralized networks.The secrecy transmission capacity is the achievable rate of successful transmission of mess- ages per unit area for given constraints on the outage probability of the transmission between a legit- imate transmitter-receiver pair and the level of security.

Physical layer security is an emerging security area that explores possibilities of achieving perfect secrecy data transmission between the intended network nodes, while possible malicious nodes that eavesdrop the communication obtain zero information. The so-called secrecy capacity can be improved using friendly jammers that introduce extra interference to the eavesdroppers. Here, we investigate the interaction between the source that transmits the useful data and friendly jammers who assist the source by \masking" the eavesdropper. In order to obtain distributed solution, one

possibility is to introduce a game theoretic approach. The game is defined such that the source pays the jammers to interfere the eavesdropper, therefore, increasing the secrecy capacity. The friendly jammers charge the source with a certain price for the jamming and there is a tradeoff for the price. If the price is too low, the profit of the jammers is low and if the price is too high, the source would not buy the service" (jamming power) or would buy it from other jammers. To analyze the game outcome, we define and investigate a Stackelburg type of game and construct a distributed algorithm. Our analysis and results show the effectiveness of friendly jamming and the tradeoff for setting the price. The distributed game solution is shown to have similar performances to those of the centralized one.

2. SYSTEM MODEL

Consider a wireless network in which a source (S) that communicates with a destination (D) and a friendly jammer (J) who assist source for secure transmission by "masking" an eavesdropper (E). The eavesdropper is a passive malicious node tries to interpret source information without modifying it. Each node except friendly jammer is having a single omnidirectional antenna while jammer has two omnidirectional antenna element and half-duplexing constraint. In cooperative jamming scheme, we add a constraint to completely null out the jamming signal at the destination.

The distance between various pairs of nodes as source-destination, source-eavesdropper, jammer-destination and jammer-eavesdropper are dSD, dSE, dJD, dJE respectively. All the channels are assumed to undergo flat fading . Suppose

the so urce has a transmission power denoted by Ps and jammer power by PJ . We denote the source-destination channel by hSD , the source - eavesdropper channel by hSE, jammer- destination channel by hJD , the jammer-eavesdropper channel by hJE. We consider the distance–dependent term and path loss exponent (n) in the channel gain, along with small scale flat fading. Analytical formulation is given to explain how the secrecy rate varies with path loss exponent.

We can formulate the channel gains as the distance to the negative power of the path loss coefficient

$$h_{SD} = \frac{\alpha_{SD} \cdot e^{j\theta_{SD}}}{d_{SD}^{n/2}} \quad (1)$$

$$h_{SE} = \frac{\alpha_{SE} \cdot e^{j\theta_{SE}}}{d_{SE}^{n/2}} \quad (2)$$

$$h_{jD} = \begin{bmatrix} \frac{\alpha_1 \cdot e^{j\theta_1}}{d_{jD}^{n/2}} \\ \frac{\alpha_2 \cdot e^{j\theta_2}}{d_{jD}^{n/2}} \end{bmatrix} \quad (3)$$

$$h_{JE} = \begin{bmatrix} \frac{\beta_1 \cdot e^{j\phi_1}}{d_{jD}^{n/2}} \\ \frac{\beta_2 \cdot e^{j\phi_2}}{d_{jD}^{n/2}} \end{bmatrix} \quad (4)$$

Where $\alpha SD, \alpha SE$ are the fading amplitudes of source-destination channel & source-eavesdropper channel; $\theta SD, \theta SE$ are the phases of the source-destination channel & source-eaves dropper channel respectively; $\alpha 1, \alpha 2$ are the fading amplitudes in the jammer-destination channel; $\theta 1$, $\theta 2$ are the phase in the jammer-destination channel; $\beta 1, \beta 2$ are the fading amplitude in the jammer- eavesdropper channel respectively ; whereas $\phi 1, \phi 2$ are the phase in the jammer- eaves dropper channel respectively.

All channels are assumed to be additive white Gaussian noise with variance $\sigma 2$. If *S* denotes the signal power in Watts and N is the noise power in Watts. Then, normalized information rate *R*, in bits can be given by

$$R = \log_2(1 + \frac{S}{N}) \quad (5)$$

For the case of one eavesdropper, an achievable secrecy capacity from is

$$RS = \max\{0, Rd\text{-}Re\} \quad (6)$$

$$R = \log_2\left(1 + \frac{P_S |h_{SD}|^2}{\sigma^2}\right) - \log_2\left(1 + \frac{P_S |h_{SE}|^2}{\sigma^2 + P_S |w^f h_{jE}|^2}\right) \quad (7)$$

Where Rd is the achievable capacity of the source-destination link and Re is the achievable capacity of the source-eavesdropper link. The total transmit power of system is P0 = PJ + PS.

3. PROBLEM FORMULATION

To maximise the secrecy capacity under the consideration of total transmit power of the system const- raint and the jamming signal become null out at the destination the problem can be recast as from $\arg \max_w |w^f h_{JE}|^2$

$$\text{s.t. } w^f w \leq Pj \;\&\; PS \in [0, P0] \quad (8)$$

w is the weight vector of jamming signal. Substituting the values from (1) to (4), w can be expressed as follows [8].

$$w = \mu P_S \left(\frac{\alpha_1^2 \cdot e^{j2\theta_1} + \alpha_2^2 \cdot e^{j2\theta_2}}{d_{jD}^n} \right) \begin{bmatrix} \frac{\beta_1 \cdot e^{j\phi_1}}{d_{jB}^{n/2}} \\ \frac{\beta_2 \cdot e^{j\phi_2}}{d_{jB}^{n/2}} \end{bmatrix} - \mu c P_S \begin{bmatrix} \frac{\alpha_1 \cdot e^{j\theta_1}}{d_{jB}^{n/2}} \\ \frac{\alpha_2 \cdot e^{j\theta_2}}{d_{jB}^{n/2}} \end{bmatrix} \quad (9)$$

Where

$$\mu = \left[\left(\frac{\alpha_1^2 \cdot e^{j2\theta_1} + \alpha_2^2 \cdot e^{j2\theta_2}}{d_{jD}^n} \right)^2 \left(\frac{\beta_1^2 \cdot e^{j2\theta_1} + \beta_2^2 \cdot e^{j2\theta_2}}{d_{jD}^n} \right) - \left(\frac{\alpha_1^2 \cdot e^{j2\theta_1} + \alpha_2^2 \cdot e^{j2\theta_2}}{d_{jD}^n} \right) c^2 \right]^{-1/2} \quad (10)$$

And

$$c = \begin{bmatrix} \frac{\alpha_1^* \cdot e^{-j\theta_1}}{d_{jB}^{n/2}} & \frac{\alpha_2^* \cdot e^{-j\theta_2}}{d_{jB}^{n/2}} \end{bmatrix} \begin{bmatrix} \frac{\beta_1 \cdot e^{j\phi_1}}{d_{jB}^{n/2}} \\ \frac{\beta_2 \cdot e^{j\phi_2}}{d_{jB}^{n/2}} \end{bmatrix} \quad (11)$$

The secrecy rate for cooperative jamming scheme can be formulated as follows.

$$R_s(P_s) = \log_2 \frac{e_0 + e_1 P_s + e_1 P_s^2}{f_0 + f_1 P_s} \quad (12)$$

Where e_i and f_i are coefficients independent of P_s

4. COOPERATIVE JAMMING WITH ALOHA

A broadcast random network in which legitimate nodes and the eavesdroppers are distributed according to independent two - dimensional Poisson Point Processes (PPP) has been considered . The locations of all the source nodes are homogeneous with PPP density λ_t. The Aloha protocol has been employed which allow the source to actually transmit the massage signal with probability *p* in each time slot. Hence, location of the actual source in any time slot follow a homogeneous Poisson point processes with density $p\lambda_t$. The location of eavesdroppers also follow a homogeneous Poisson point processes with density λ_e. When the transmit power is allowed to vary, the power for message transmission is P_T and the power for jamming is PJ, which are the same for all sources.

4.1 SECRECY TRANSMISSION CAPACITY

According to Wyner's encoding scheme, the transmitter chooses two rates, namely, the rate of the transmitted code words R_t and the secrecy rate of the confidential messages R_s. The cost of secu- ring the messages against eavesdropping will be $R_e = R_t - R_s$. The perfect secrecy can be achieved when the mutual information between the confidential message and every eavesdropper's received signal approaches zero rate wise. The following outage events can result from any transmission .

Connection Outage (P_{co}): it is defined as the probability of massage cannot be decoded correctly by the intended receiver.

Secrecy Outage (P_{so}): it is defined as the probability of massage cannot be secured properly against eavesdropping.

5. SECRECY TRANSMISSION CAPACITY FORMULATION

In this section, the analytical formulation of secrecy transmission capacity for Rayleigh fading channels has been done. For a given connection outage constraint and a given secrecy outage constraint, the *secrecy transmission capacity* can be defined as the achievable rate of successful transmission of confidential messages per unit area. If connection outage probability is $P_{co} = \sigma$ and secrecy outage probability $P_{so} = \varepsilon$ then the secrecy transmission capacity can be defined as .

$$\tau = (1-\sigma)\lambda_t R_s \quad (13)$$

Where R_s is the average secrecy rate of confidential message between all source-receiver pair assuming all pairs having equal distance r. The secrecy rate R_s is a function of r, σ and ε.

The connection outage constraint σ has been used to find Rt and the secrecy outage constraint ε has been used to find Re. The threshold value of signal to interference ratio (SIR) for connection outage is given by

$$\beta_t = 2^{R_t} - 1 \quad (14)$$

Hence, the connection outage probability can be given as

$$P_{CO} = 1 - \exp\left[-\lambda_t \beta_t^{2/\alpha} \pi r^2 \Gamma\left(1 - \frac{2}{\alpha}\right) \Gamma\left(1 + \frac{2}{\alpha}\right) \right] \quad (15)$$

With the given connection outage constraint Pco = σ, the transmission rate Rt can be calculated from (14) and (15) as

$$R_t = \log_2 \left(1 + \frac{\ln\left(\frac{1}{1-\sigma}\right)}{\lambda_t \pi r^2 \Gamma\left(1 - \frac{2}{\alpha}\right) \Gamma\left(1 + \frac{2}{\alpha}\right)} \right)^{\alpha/2} \quad (16)$$

Similarly, the threshold value of signal to interference ratio (SIR) for secrecy outage is given by

$$\beta_e = 2^{R_e} - 1 \tag{17}$$

Hence, the secrecy outage probability can be given as

$$P_{SO} = \frac{\lambda_e}{\lambda_t \beta_t^{2/\alpha} \Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(1+\frac{2}{\alpha}\right)} \tag{18}$$

With the given secrecy outage constraint Pso = ε, the transmission rate Re can be calculated from (17) and (18) as

$$R_e = \log_2\left(1+\left[\frac{\lambda_t}{\lambda_e}\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(1+\frac{2}{\alpha}\right)\ln\left(\frac{1}{1-e}\right)\right]^{-\alpha/2}\right) \tag{19}$$

Hence, secrecy transmission capacity can be found using (13) as

$$\tau(r) = (R_t - R_e)(1-\sigma)\lambda_t$$

Which can also be formulated using (16) (19) and (20) as follows:

$$\tau = (1-\sigma)\lambda_t\left[\log_2\left(\frac{\left(1+\frac{\ln\left(\frac{1}{1-\sigma}\right)}{\lambda_t \pi r^2 \Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(1+\frac{2}{\alpha}\right)}\right)^{\alpha/2}}{1+\left[\frac{\lambda_t}{\lambda_e}\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(1+\frac{2}{\alpha}\right)\ln\left(\frac{1}{1-e}\right)\right]^{-\alpha/2}}\right)\right] \tag{20}$$

Where $v_1 = p + (1-p)\left(p_j/p_t\right)^{2/\alpha}$ (21)

And $v_2 = p - (1-p)\left(p_j/p_t\right)^{2/\alpha}$

In the case of fixed power transmission *i.e.* PJ = PT and in the high security system where ε→0; the optimal secrecy transmission capacity can be written as

$$\tau = (1-\sigma)p\,\lambda_t \frac{\alpha}{2\ln 2}\ln((1-p)k) \tag{22}$$

Where

$$k = \frac{\lambda_t}{\lambda_e}\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(1+\frac{2}{\alpha}\right)\ln\left(\frac{1}{1-\varepsilon}\right)\left[1+\left[\frac{\lambda_t}{\lambda_e}\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(1+\frac{2}{\alpha}\right)\ln\left(\frac{1}{1-e}\right)\right]^{-\alpha/2}\right]^{\frac{2}{\alpha}} \tag{23}$$

Hence, the optimal message transmission probability is [21]

$$\arg\max_p\ p\ln((1-p)k) \tag{24}$$

If the value of optimal message transmission probability is P_{opt} then

$$\frac{1}{1-P_{opt}} = W_0(\exp(1+\ln k)) \tag{25}$$

Where W0(.) is the real-valued principal branch of the Lambert W function.

6. SIMULATION RESULTS

Simulations were performed to evaluate the effect of cooperative jamming and cooperative jamming with Aloha protocol on the achievable secrecy capacity. To illustrate the effect of cooperative jamming scheme, a one-dimensional model in which a source, a destination , an eavesdropper and a friendly jammer are placed linearly for line-of-sight communi - cation between various nodes . The distance between source and destination is 100 m while the distance of eavesdropper and jammer from the source are 50 m & 25 m respectively. Noise level is $4*10^{-8}$. Firstly, the position of the source, destination, friendly jammer and eavesdropper were fixed. The source power is fixed at P_S= .02 Watt and the jammer power is varied up to .02 watt. The path loss exponent is n=3. Secrecy rate as a function of jammer power is shown in figure 1. From the obtained result, it is observed that on increasing the jammer power, secrecy rate first increases up to an optimal point, whose location depends upon the position of friendly jammer, then decreases.

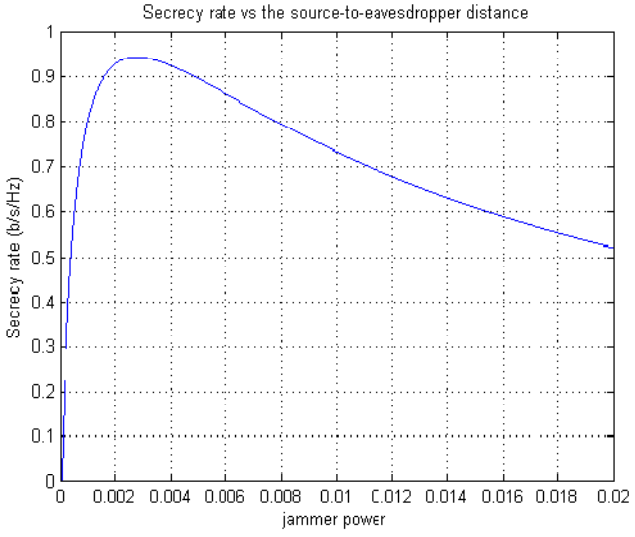

Figure 3: Secrecy rate versus power of friendly jammer

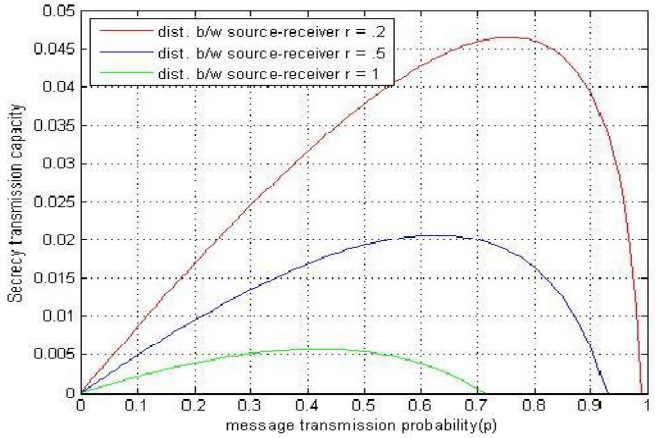

Figure 4: The secrecy transmission capacity τ versus the message transmission probability p with different values of distance between legitimate source and receiver 'r'

Figure 3 shows the variation of secrecy transmission capacity τ with the message transmission probability *p* for different values of distance between legitimate source and receiver node pair r. it has been observed that network throughput has been degraded when *p* is either very low or too high. Specially, for fixed power transmission (PJ =PT), the maximum secrecy transmission capacity is 0.046 achieved at p=0.76 (for r = .2), whereas the secrecy transmission capacity reduces to 0.03(i.e., a 34% reduction) if we reduce p to 0.38 (i.e. p is halved). Also, the secrecy transmission capacity has been degraded as distance between legitimate source and receiver increases.

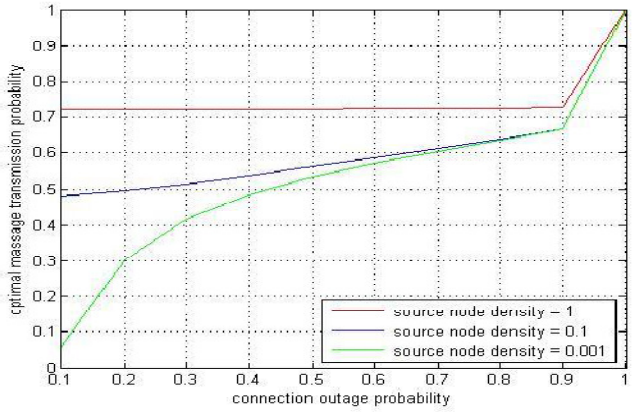

Figure 5: Optimal message transmission probability *p* with the secrecy outage probability ε for different values of PPP density of legitimate source nodes λt

7. CONCLUSION

Physical layer security technique based on cooperative jamming has been explored in the present work. Further, its implementation with Aloha protocol for decentralized wireless networks is performed. Simulation result for cooperative jamming scheme shows that high jammer power and proximity of eavesdropper to the legitimate source or receiver can be harmful for secure communication. Secrecy rate has been evaluated considering the path loss model using one antenna friendly jammer, by varying the position of eavesdropper and jammer power. For cooperative jamming with Aloha protocol, secrecy transmission capacity is maximum for moderate value of message transmission probability. From the obtained simulation results it is observed that a high level of secrecy capacity can be achieved with proper selection of design parameter for cooperative jamming with Aloha protocol. Hence, performance of the large scale networks in terms of secrecy can be improved using Aloha.

REFERENCES

[1] N. Sklavos and X. Zhang (Ed.), "Wireless Security and Cryptography: Specifications and Implementations. CRC Press, Boca Raton, FL, 07.

[2] A. D. Wyner, "The wire-tap channel, " Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, 1975.

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, " The Gaussian wiretap channel," IEEE Trans. Inf. Theory, vol. 24, pp. 451 - 456, Jul. 1978.

[4] Csiszár and J. Körner,"Broadcast channels with confidential message," IEEE Trans. Inf. Theory, vol. 24, pp. 339–348, May 1978.

[5] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4005 - 4019, Sept. 2008.

[6] Y. Liang, H. V. Poor and S. Shamai (Shitz), " Secure communication over fading channels", IEEE Trans. Information Theory, vol. 54, no. 6, pp. 2470-2492, Jun.08

[7] M. Haenggi, "The secrecy graph and some of its properties, " in Proc. IEEE Inter. Symp. Inf. Theory (ISIT), Toronto Canada, pp. 539–543, Jul. 2008.

[8] P. C. Pinto, J. Barros and M. Z. Win, " Secure communication in Stochastic wireless networks," *arXiv preprint arXiv:1001.3697*, Jan 2010.