Proactive Attack: A Strategy for Legitimate Eavesdropping

Hung Tran* and Hans-Jürgen Zepernick†
*Mälardalen University, Västerås, Sweden
†Blekinge Institute of Technology, Karlskrona, Sweden
Email: *tran.hung@mdh.se, †hans-jurgen.zepernick@bth.se

Abstract—**In this paper, we study a novel approach to eavesdrop the messages of suspicious users for a surveillance purpose. In particular, we consider a scenario in which the legitimate monitor can act as a jamming source and a decode-and-forward relay station that can force the suspicious users to reveal their exchanged messages. Accordingly, the power allocation policies for the jamming signal of the legitimate monitor subject to deterministic and non-deterministic interference channels are considered. On this basis, we derive a closed-form expression for the successful eavesdropping probability to evaluate the system performance. More importantly, our results reveal that the successful eavesdropping probability of the non-deterministic interference channel from the legitimate monitor to the suspicious receiver outperforms the one of the deterministic interference channel.**

Index Terms—**Physical Layer Security, Secrecy Capacity, Power Allocation, Cognitive Radio Networks, Spectrum Underlay Networks, Performance Analysis.**

I. INTRODUCTION

Recently, wireless security has received a lot of research attention. In particular, physical layer security has emerged as a promising approach to protect the communications confidentiality against eavesdroppers [1]–[3]. Accordingly, secrecy capacity has been proposed as a metric to quantify the security of a wireless system. This metric is based on the fact that if the main channel is better than the wiretap channel, the transmitter can exchange secure messages with the intended receiver at a non-zero secrecy rate [1]. In other words, the secrecy capacity is defined as the maximum achievable rate from the transmitter to the legitimate receiver minus the rate obtained by the eavesdropper listening over the wiretap channel [4]. As an extension of [1], the works in [5]–[10] have investigated the physical layer security for various wireless fading channels.

To reduce the information leakage due to an eavesdropper and to analyze the security performance of wireless systems, many works have studied the malicious active eavesdropping attacks in the wireless physical layer security literature [11]–[16]. It is noted that almost all existing works often consider the eavesdropping process as illegitimate attacks, and the eavesdropping process is prohibited from a national security point of view. Thus, there is not many research focusing on the improving the eavesdropping performance. However, in reality, the eavesdropping process is useful to discover the information exchange between suspicious users such as criminals and terrorists who may use smartphones for their communication. Hence, there are more and more demands for government agencies to control and legitimately eavesdrop suspicious wireless communications. In light of this notion, the most recent work reported by Jie Xu *et al.* [17], has presented a new approach to eavesdrop suspicious users over Rayleigh fading channels. Following this approach, the legitimate monitor (LM) sends jamming signals with optimized power control to moderate the suspicious communication. Accordingly, the LM can achieve the maximum average eavesdropping rate. However, Jie Xu *et al.* only consider the context of a single hop communication for the eavesdropping process. The impact of self-interference, deterministic, and non-deterministic interference channels from the LM to the suspicious receiver (SR) have not been studied.

Inspired by all of the above, in this paper, we analyze the performance of a legitimate eavesdropping model in which the power control of the LM is subject to deterministic and non-deterministic interference channels. Further, the LM can control the jamming signal to attack the suspicious user (SU) so that the LM and legitimate eaversdropper (LE) can improve the eavesdropping capability. Given these settings, main contributions of this paper are summerized as follows:

- Two power allocation policies with respect to the deterministic and non-deterministic interference channel for the jamming signal of the LM are obtained.
- A closed-form expression for successful eavesdropping probability is calculated to analyze the legitimate eavesdropping performance.
- Our numerical examples indicate that the non-deterministic interference channel between the legitimate monitor and suspicious receiver is an important factor to improve legitimate eavesdropping performance.

The remainder of this paper is organized as follows. In Section II, the system model, assumptions, and problem statement for the legitimate eavesdropping process are introduced. In Section III, the power allocation policies for the jamming signal of the LM are formulated. On this basis, a closed-form expression for the successful eavesdropping probability is derived. In Section IV, numerical results and discussions are provided. Finally, conclusions are given in Section V.

II. SYSTEM MODEL

In this section, the system model, channel assumptions, and problem formulation are provided.

A. System Model and Channel Assumptions

Let us consider the system model shown in Fig. 1 in which the LM tries to exploit the message exchange between the suspicious transmitter (ST) and SR. The eavesdropping message from the ST is then forwarded to the LE over a dedicated channel. In the considered context, the ST and SR may be devices of criminals or terrorists while the LM and LE may be drones, unmanned aerial vehicle (UAV), or smartphones which are equipped for soldiers in the battle field. We assume that the ST, SR, and LE have a single antenna, while the LM is a full-duplex device equipped with three antennas. The first antenna is used to send the jamming signal, the second antenna is used to eavesdrop the message from the ST, and the third antenna is used to broadcast the decoded message to the LE. The channel gains of the ST→SR, ST→LM, LM→LE links are denoted by h, g_1, and g_2, respectively. The channel gains of the LM→LM, LM→SR, and LM→LE interference links are denoted by f_0, f_1 and f_2, respectively.

We consider two cases of LM→SR interference links as follows:

- The channel gain f_1 of the LM→SR interference link is a deterministic variable and known at both the LM and SR.
- The channel gain f_1 of the LM→SR interference link is a non-deterministic variable, i.e, f_1 is an exponentially distributed random variable (RV) and LM and SR only know the channel mean gain of the LM→SR interference link.

Without loss of generality, we assume that the channel gains are exponentially distributed RVs which are constant during transmission of one message, but they may be independently changed thereafter. Accordingly, the probability density function (PDF) and cumulative distribution function (CDF) of channel gains are given, respectively, as follows:

$$f_X(x) = \frac{1}{\Omega_X}\exp\left(-\frac{x}{\Omega_X}\right), \tag{1}$$

$$F_X(x) = 1 - \exp\left(-\frac{x}{\Omega_X}\right), \tag{2}$$

where RV X refers to the channel gain, and $\Omega_X = \mathbf{E}[X]$ is the channel mean gain.

B. Problem Formulation

As modern wireless SU devices may be equipped with advanced techniques such as cognitive radios [18], they can adjust their transmit power according to the change of radio environment, e.g., interference and channel state information (CSI). In light of this, the LM can generate a reasonable jamming signal to the SR such that the ST must increase its transmit power to guarantee quality of service (QoS) for the SU communication. Accordingly, the LM can utilize this behavior to better overhear the message of the ST over the legitimate eavesdropping link ST→LM. If the LM can decode the ST message successfully, then the LM immediately forwards the decoded message to the LE.

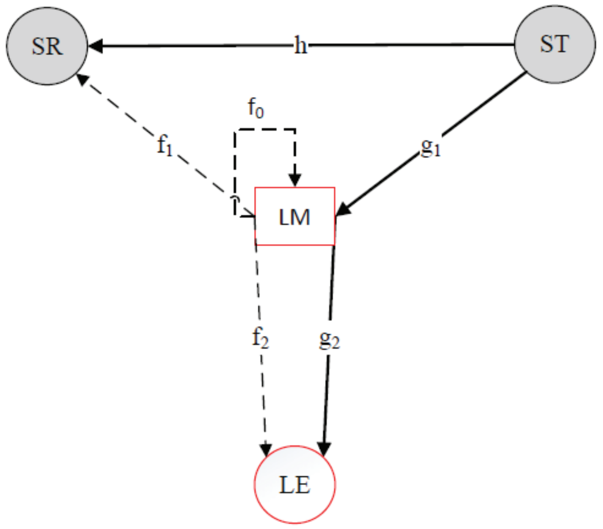

Fig. 1. A system model of attack to obtain information.

More specifically, the achievable rate of the ST→SR suspicious link under the effect of a jamming signal can be given by

$$R_{SR} = B\log_2\left(1 + \frac{P_{ST}h}{Q_J f_1 + N_0}\right), \tag{3}$$

where P_{ST} and Q_J are the transmit power of the ST and the power of the jamming signal generated by the LM, respectively. Further, symbols B and N_0 denote the system bandwidth and noise power, respectively. Here, the QoS for the SU communication can be expressed in terms of the outage probability constraint as follows:

$$\Pr\left\{R_{SR} \le r_0\right\} \le \epsilon_0, \tag{4}$$

where r_0 and ϵ_0 are outage target rate and outage probability constraint of the SR, respectively. Further, the transmit powers of the ST and LM are in practice subject to a maximum power constraint as follows:

$$0 \le P_{ST} \le P_{ST}^{\max}, \tag{5}$$

$$0 \le Q_J \le Q_J^{\max}. \tag{6}$$

For the legitimate eavesdropping process, the achievable data rate of the LM over the eavesdropping link ST→LM can be formulated as

$$R_{LM} = \log_2\left(1 + \frac{P_{ST}g_1}{\alpha Q_J f_0 + N_0}\right), \tag{7}$$

where f_0 is the self-interference channel gain of the LM. Symbol α is the interference cancellation efficiency coefficient of the LM, which depends on the interference cancellation technique of the LM, $0 \le \alpha \le 1$. If $\alpha = 0$, the LM can perfectly cancel the interference. On the other hand, if $\alpha = 1$, the LM cannot cancel any interference.

Whenever the LM decodes the eavesdropping message successfully, it forwards the decoded message to the LEs over a dedicated security channel. Here, the LE also suffers from interference due to the jamming signal of the LM, but this can be reduced by using advanced interference cancellation techniques. The achievable data rate of the LM→LE link can be expressed as

$$R_{LE} = B\log_2\left(1+\frac{P_{LM}g_2}{\beta Q_J f_2 + N_0}\right), \tag{8}$$

where $P_{LM} \in [0, P_{LM}^{\max}]$ is the transmit power of the LM used to forward the message to the LE, and $0 \le \beta \le 1$ is the interference cancellation efficiency coefficient.

The legitimate eavesdropping process is successful, only if the eavesdropping message is decoded successfully at the LE via the help of the LM. Here, the LM acts as a relay and active jamming station to help the eavesdropping process of the LE. Further, we define the successful legitimate eavesdropping probability to quantify the system performance as follows:

$$\mathcal{O}_{succ} = \Pr\left\{\frac{1}{2}\min\{R_{ST}, R_{LE}\} \ge r_1\right\} \tag{9}$$

where r_1 is the outage target rate of legitimate eavesdropping process.

III. PERFORMANCE ANALYSIS

In this section, we first derive the power allocation policies for the jamming signal, and then analyze the successful legitimate eavesdropping probability.

A. Power Allocation Policy for Jamming Signal

The power Q_J of the jamming signal is an active noise source to reduce the achievable data rate of the SR (see (3)). On the other hand, the ST must increase its transmit power P_{ST} to deal with the interference and then improve the performance. Thus, if the LM causes too much interference to the SR such that the ST cannot adjust its transmit power to satisfy its outage probability constraint, the SU will stop communicating and the legitimate eavesdropping process fails. To not cause severe interference to the SR, the LM needs to adjust the power of the jamming signal to satisfy the outage probability constraint given in (4), i.e,

$$\Pr\left\{\frac{P_0 h}{Q_0 f_1 + 1} \le \gamma_{th}\right\} = \epsilon_0, \tag{10}$$

where $\gamma_{th} = 2^{\frac{r_0}{B}} - 1$, $P_0 = \frac{P_{ST}}{N_0}$, and $Q_0 = \frac{Q_J}{N_0}$. Depending on the CSI of the LM→SR interference link, the power allocation for the jamming signal can be presented as follows.

1) Deterministic Interference Link from the LM to the SR: In this case, the SU knows exactly the CSI of both the LM→SR interference link and ST→SR communication link. As f_1 is deterministic, (10) can be rewritten as follows:

$$1 - \exp\left(-\frac{\gamma_{th}(Q_J f_1 + N_0)}{\Omega_h P_{ST}}\right) = \epsilon_0. \tag{11}$$

After some basic manipulations of (11), we obtain

$$Q_J = \underbrace{\frac{1}{f_1}\left[\frac{\Omega_h P_{ST}}{\gamma_{th}}\ln\frac{1}{1-\epsilon_0} - N_0\right]}_{Q_1}, \tag{12}$$

where Q_1 is the initial transmit power of the jamming signal for a given P_{ST}.

Whenever the ST can adjust its transmit power to adapt to the jamming signal and to guarantee its QoS, the LM can further increase Q_J. However, the LM must stop increasing transmit power of the jamming signal when the ST reaches the maximum value $P_{ST} = P_{ST}^{\max}$. Accordingly, the transmit power of the jamming signal should satisfy the following constraint:

$$Q_J \le \underbrace{\min\left\{\frac{1}{f_1}\left[\frac{\Omega_h P_{ST}^{\max}}{\gamma_{th}}\ln\frac{1}{1-\epsilon_0} - N_0\right], Q_J^{\max}\right\}}_{Q_2}. \tag{13}$$

In other words, the range for the transmit power of the jamming signal is given as follows:

$$Q_1 \le Q_J \le Q_2. \tag{14}$$

B. Non-deterministic Interference Link from LM→SR

Let us commence by considering the following property.

Property 1. *Let a and b be positive constants. Further, let X and Y be independent and exponentially distributed RVs with mean values Ω_X and Ω_Y, respectively. Then, the RV Z defined by*

$$Z = \frac{aX}{bY+1} \tag{15}$$

has the CDF given by

$$F_Z(z) = 1 - \frac{1}{\frac{b\Omega_Y}{a\Omega_X}+1}\exp\left(\frac{z}{a\Omega_X}\right). \tag{16}$$

Proof. See [19] or [20]. □

When the channel gain f_1 is an exponentially distributed RV with mean Ω_{f_1}, the outage probability constraint in (10) can be obtained by using (16) as

$$1 - \frac{1}{\frac{Q_0\Omega_{f_1}}{P_0\Omega_h}+1}\exp\left(-\frac{\gamma_{th}}{P_0\Omega_h}\right) = \epsilon_0, \tag{17}$$

After some mathematical manipulations, we obtain an expression for the power of the jamming signal as follows:

$$Q_J = \underbrace{\frac{P_{ST}\Omega_h}{\Omega_{f_1}}\left\{\frac{1}{1-\epsilon_0}\exp\left(-\frac{\gamma_{th}N_0}{P_{ST}\Omega_h}\right) - 1\right\}}_{Q_3}. \tag{18}$$

Although the ST can adapt its transmit power P_{ST} according to the channel conditions and interference, it cannot increase the power higher than the maximum value $P_{ST}^{\max}$. Further, the right hand side of (18) is a monotonically increasing function with respect to P_{ST}. Thus, the range for the Q_J is obtained as

$$Q_3 \le Q_J \le \min\left\{\frac{P_{ST}^{\max}\Omega_h}{\Omega_{f_1}}\Xi, Q_J^{\max}\right\}, \tag{19}$$

where Ξ is defined as

$$\Xi = \max\left\{\frac{1}{1-\epsilon_0}\exp\left(-\frac{\gamma_{th}N_0}{P_{ST}^{\max}\Omega_h}\right) - 1, 0\right\}. \tag{20}$$

C. Successful Legitimate Eavesdropping Probability

By substituting (7) and (8) into (9), we can rewrite the successful legitimate eavesdropping probability as follows:

$$\mathcal{O}_{succ} = \underbrace{\Pr\left\{\log_2\left(1+\frac{P_{ST}g_1}{\alpha Q_J f_0 + BN_0}\right) \geq \frac{2r_1}{B}\right\}}_{T_1} \quad (21)$$

$$\times \underbrace{\Pr\left\{\log_2\left(1+\frac{P_{LM}g_2}{\beta Q_J f_2 + BN_0}\right) \geq \frac{2r_1}{B}\right\}}_{T_2}, \quad (22)$$

where Q_J is the power of the jamming signal given in (19). With the help of (16), we obtain closed-form expressions of T_1 and T_2 as follows:

$$T_1 = \frac{P_{ST}\Omega_{g_1}}{\alpha Q_J \Omega_{f_0} + P_{ST}\Omega_{g_1}} \exp\left(-\frac{\theta_{th}BN_0}{P_{ST}\Omega_{g_1}}\right), \quad (23)$$

$$T_2 = \frac{P_{LM}\Omega_{g_2}}{\beta Q_J \Omega_{f_2} + P_{ST}\Omega_{g_2}} \exp\left(-\frac{\theta_{th}BN_0}{P_{ST}\Omega_{g_2}}\right), \quad (24)$$

where $\theta_{th} = 2^{\frac{2r_1}{B}} - 1$. Finally, substituting (23) and (24) into (21) yields a closed-form expression for the successful legitimate eavesdropping probability.

IV. Numerical Results

In this section, we provide numerical examples for the two power allocation policies of the jamming signal, and then examine the performance of the considered system. The following system parameters are used for both analysis and simulation:

- System bandwidth: $B = 5$ MHz.
- Outage target rates: $r_0 = r_1 = 64$ kbps.
- Outage probability constraint: $\epsilon_0 = 0.01$.
- Maximum transmit signal-to-noise ratio (SNR) of the ST: $\gamma_{ST}^{\max} = \frac{P_{ST}^{\max}}{N_0} = 5$ dB.
- Maximum transmit SNR of the jamming signal: $\gamma_J^{\max} = \frac{Q_J^{\max}}{N_0} = 10$ dB.
- Transmit SNR of the LM: $\gamma_{LM} = \frac{P_{LM}}{N_0} = 2$ dB.

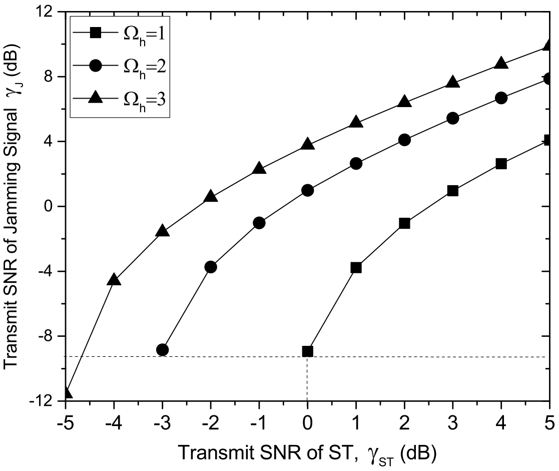

Fig. 2. Transmit SNR of the jamming signal with deterministic interference channel LM→SR $f_1 = 1$ and outage probability constraint $\epsilon_0 = 0.01$.

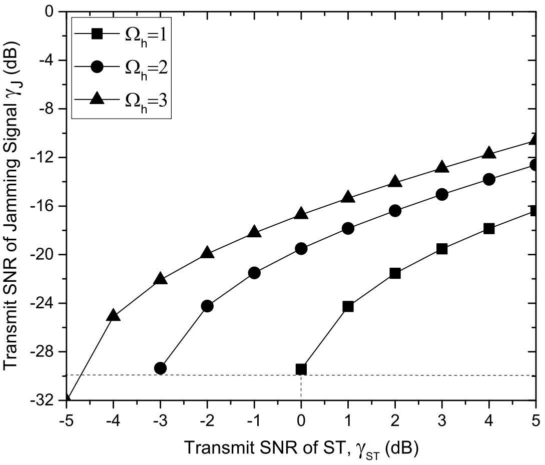

Fig. 3. Transmit SNR of the jamming signal with non-deterministic interference channel LM→SR $\Omega_{f_1} = 1$ and outage probability constraint $\epsilon_0 = 0.01$.

Figs. 2 and 3 show the relationship between the transmit SNR of the jamming signal $\gamma_J = \frac{Q_J}{N_0}$ of the LM and the transmit SNR $\gamma_{ST} = \frac{P_{ST}}{N_0}$ of the ST for deterministic and non-deterministic interference link, respectively. Clearly, to force the ST to increase its transmit SNR γ_{ST}, the LM must increase the transmit SNR γ_J of the jamming signal. However, for the same region of the ST transmit SNR $[0, 5]$ dB, the demand for the transmit SNR of the jamming signal for the deterministic interference link is always higher than the one of the non-deterministic interference link. To make this statement more clear, we observe the case $\Omega_h = 1$ in both Fig. 2 and 3. Clearly, the transmit SNR of the jamming signal must increase from -9 dB to 4 dB to keep the transmit SNR of the ST in the range of $[0, 5]$ dB (see Fig. 2). On the other hand, the transmit SNR of the jamming signal only needs to increase from -30 dB to -16 dB to keep the transmit SNR of the ST in the range of $[0, 5]$ dB (see Fig. 3). In other words, the LM only needs a low power level for the jamming signal when the ST does not know exactly the CSI of the LM→SR interference link.

Furthermore, the results shown in these figures reveal that when the channel mean gain of the SU increases, e.g. $\Omega_h = 1, 2, 3$, the LM needs more transmit SNR for the jamming signal to keep the transmit SNR of the ST at the same level, e.g., $\gamma_{ST} = 0$ dB. This can be explained by the fact that the SU only needs to use a small amount of power to maintain its QoS when the ST→SR link is in a good condition. Thus, the LM requires a high power level for the jamming signal to generate sufficient interference to the SR.

Fig. 4 shows the successful eavesdropping probability as a function of the ST transmit SNR. Clearly, we can see that the simulation matches very well with the analysis in all cases of channel mean gains from the ST→LM link and LM→SR link. Further, the successful eavesdropping probabilities for the deterministic and non-deterministic interference links are the same as the transmit SNR of the ST is below -1 dB, i.e,

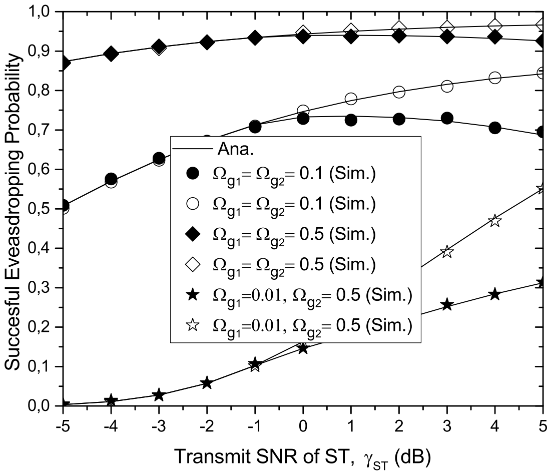

Fig. 4. Successful eavesdropping probability for the jamming signal versus the ST transmit SNR. The black markers show results for the deterministic interference link LM→SR, while the white markers express results for the non-deterministic interference link LM→SR.

$\gamma_{ST} \leq -1$ dB. However, in the high transmit SNR regime of the ST, i.e., $\gamma_{ST} \geq -1$ dB, the successful eavesdropping probability for the non-deterministic interference channel is better than the one of the deterministic interference channel. This can be explained by the fact that it is difficult for the SU to estimate the CSI for the non-deterministic interference channel. Hence, the ST needs to keep a high power level to maintain the QoS. In other words, the jamming signal of the LM forces the ST to increase its transmit power to enhance the performance of the SR. The LM utilizes the increasing transmit power of the ST to easily decode the eavesdropping messages. Further, we can also see that when the channel mean gain of the eavesdropping link ST→LM reduces from $\Omega_{g_1} = 0.5$ to $\Omega_{g_1} = 0.01$, the successful eavesdropping probability reduces significantly. Obviously, the eavesdropping process is seriously degraded if the ST→LM link is in bad condition.

V. Conclusions

In this paper, we have considered a new approach for a legitimate eavesdropping process by using a jamming signal. In particular, the LM can generate jamming signals to proactively attack the communication of the SU and then utilize an adjustment of the transmit power of the ST to enhance the legitimate eavesdropping performance. Power allocation policies for the jamming signal under deterministic and non-deterministic interference channel have been formulated. A performance analysis in terms of successful eavesdropping probability for the considered system model has been conducted. Our numerical examples indicate that when the channel between the LM and SR is non-deterministic, the demand for the power level of the jamming signal is smaller than in the case of deterministic interference link between the LM and SR. Further, the successful eavesdropping probability of the non-deterministic interference channel outperforms the one of the deterministic interference channel.

Acknowledgement

The research leading to these results has been performed in the SafeCOP-project, with funding from the European Commission and Vinnova under ECSEL Joint Undertaking grant agreement n0692529.

References

[1] A. D. Wayner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] C. Mitrpant, A. Vinck, and Y. Luo, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Transactions on Information Theory*, vol. 52, no. 5, pp. 2181–2190, May 2006.

[3] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[4] A. Fragkiadakis, E. Tragos, and I. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Communications Surveys Tutorials*, vol. 15, no. 1, pp. 428–445, First 2013.

[5] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *IEEE Proc. International Symposium on Information Theory*, Adelaide, Australia, Sep. 2005, pp. 2152–2155.

[6] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *IEEE Proc. International Symposium on Information Theory*, Seattle, U.S.A., July 2006, pp. 356–360.

[7] Y. Liang and H. Poor, "Generalized multiple access channels with confidential messages," in *Proc. IEEE International Symposium on Information Theory*, Seattle, U.S.A., Jul. 2006, pp. 952–956.

[8] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[9] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct 2008.

[10] I. Csiszar and P. Narayan, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2437–2452, June 2008.

[11] A. Mukherjee and A. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in *Proc. IEEE Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, U.S.A., Nov. 2011, pp. 265–269.

[12] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[13] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932–940, May 2015.

[14] G. Amariucai and S. Wei, "Half-duplex active eavesdropping in fast-fading channels: A block-markov wyner secrecy encoding scheme," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4660–4677, Jul. 2012.

[15] Y. Basciftci, O. Gungor, C. Koksal, and F. Ozguner, "On the secrecy capacity of block fading channels with a hybrid adversary," *IEEE Trans. Inf. Theory*, vol. 61, no. 3, pp. 1325–1343, Mar. 2015.

[16] A. Mukherjee and A. Swindlehurst, "Jamming games in the mimo wiretap channel with an active eavesdropper," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 82–91, Jan. 2013.

[17] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over rayleigh fading channels," *IEEE Commun. Lett.*, vol. PP, no. 99, pp. 1–5, Nov. 2015.

[18] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201 – 220, Feb. 2005.

[19] H. Tran, "Performance analysis of cognitive radio networks with interference constraints," Dissertation, Blekinge Institute of Technology, Karlskrona, Sweden, Mar. 2013.

[20] Y. Chen, H. Huang, and V. K. N. Lau, "Cooperative spectrum access for cognitive radio network employing rateless code," in *Proc. IEEE Int. Conf. on Commun.*, Beijing, China, May 2008, pp. 1–6.