The Secrecy Capacity of Block Fading Multiuser Wireless Networks

Arsenia Chorti[†,*], Katerina Papadaki[‡], Panagiotis Tsakalides[*], H. Vincent Poor[†]

[†]Department of Electrical Engineering, EQUAD, 19 Olden Street, Princeton University, Princeton, New Jersey 08544, USA
[‡]Department of Management, London School of Economics and Political Science, Houghton Street, London WC2A 2AE
[*]Institute of Computer Science, Foundation for Research and Technology Hellas, Vassilika Vouton, GR-700 13, Crete, Greece
{achorti, poor}@princeton.edu, k.p.papadaki@lse.ac.uk, {achorti, ptsakalides}@ics.forth.gr

***Abstract*—The resilience of block fading wireless orthogonal frequency division multiple access (OFDMA) networks to passive eavesdroppers is investigated. The network secrecy capacity is evaluated in scenarios involving a base station and several terminals, some of which constitute passive eavesdroppers. Assuming a block fading Rayleigh channel, the probability of a secrecy outage during a transmission frame is evaluated with respect to a target secrecy rate τ in the following cases: (i) in the absence of any cooperation between the network nodes, and, (ii) when the full multi-user diversity is exploited both by the legitimate users as well as by the eavesdroppers. Remarkably, it is demonstrated that in a network of as few as 12 legitimate users and a single eavesdropper it is possible to transmit 1 bit/sec/Hz with a probability of secrecy outage less than 1%. Furthermore, the delay constrained secrecy capacity of this network is evaluated when the full channel state information (CSI) is available both at the base station and at all receiving nodes. A secure waterfilling scheme is discussed, satisfying a short-term power constraint.**

***Index Terms*—OFDMA networks, probability of secrecy outage, block fading Gaussian channel, delay constrained secrecy capacity, secure waterfilling**

I. Introduction

Security in the exchange of information in terms of data confidentiality in the presence of adversaries has commonly been treated as an inherently applied subject, despite the theoretical formulation of perfect secrecy early on [1]. Nevertheless, despite the incontestable success and importance of common cryptographic measures, the foreseen increasing deployment of wireless networks introduces new challenges. In more detail, in future communication networks the following matters need to be addressed:

- the generation, the management and the storage of secret keys need to be re-examined in large-scale, dynamic and decentralized networks (e.g. the Cloud),
- simple devices, such as sensors, cannot handle the overheads associated with public key encryption schemes,
- both symmetric and public key encryption approaches assume ideal transmission and reception and do not take into account the characteristics of the communication medium; specifically for wireless applications, there exists an experimentally established fundamental trade-off between common encryption techniques and throughput [2], [3].

In order to address these important issues in wireless communication networks, physical layer (information theoretic) approaches on security have been gaining renewed interest.

The breakthrough concept of physical layer security (PLS) [4] is to exploit the characteristics of the transmission medium such as fading or noise to achieve secrecy in wireless transmissions. PLS was pioneered by Wyner, who introduced the wiretap channel and established the possibility of creating perfectly secure communication links without relying on private (secret) keys [5]. Wyner showed that when an eavesdropper's channel is a degraded version of the main source-destination channel, the source and the destination can exchange information reliably (with asymptotically zero error rates) and with perfect secrecy (with asymptotically zero rate of information leakage). A rate at which information can be transmitted secretly from the source to its intended destination is termed an achievable secrecy rate, and the maximal achievable secrecy rate is termed the secrecy capacity (SC).

In [6], the SC of the scalar Gaussian wiretap channel was analyzed. In [7] Wyner's approach was generalized to the transmission of confidential messages over broadcast channels. Recently, there have been considerable efforts devoted to generalizing this result to the wireless fading channel and to multi-user scenarios [8], [9], [10], [11], [12].

In the present work we investigate block fading wireless orthogonal frequency division multiple access (OFDMA) networks with secrecy and delay constraints. Our study extends the results of [13] to networks with secrecy restrictions by providing closed form expressions for the probability of a secrecy outage with and without cooperation between the network nodes. Furthermore, we investigate the OFDMA network delay constrained secrecy capacity, assuming that the channel state information (CSI) over one frame of M-block channel realizations is available at the transmitter and at all the receiving nodes. Under this assumption, we derive the optimal secure waterfilling power allocation that maximizes the multi-user network secrecy capacity.

II. Problem Formulation

A multi-user setting is assumed in which each of M orthogonal OFDMA subchannels is allocated to one of K legitimate users according to a maximum signal to noise ratio (max-SNR) criterion; each of the OFDMA subchannels is allocated to the legitimate user with the largest SNR in the specific subchannel. All communications take place in the presence of E eavesdroppers that intercept the M OFDMA subchannels. To each legitimate user $k \in \{1, \ldots, K\}$, the base

978-1-4799-1089-2/13/$31.00 ©2013 IEEE

station wishes to broadcast corresponding secret messages by employing PLS techniques. Accordingly, a stochastic encoder is used that maps the confidential messages of user k to codewords of length $n^{(k)} = M^{(k)}N$. A codeword intended for the k-th user spans $M^{(k)}$ blocks of N symbols that undergo the same Rayleigh fading, i.e., each of the $M^{(k)}$ block fading realizations remain constant over N channel uses. Our investigations focus on block-fading Gaussian (BF-Gaussian) channels under delay and power constraints assuming that all available OFDMA subchannels are allocated, i.e., $\sum_{k=1}^{K} M^{(k)} = M$.

The group of $M^{(k)}$ transmission blocks is referred to as the k-th user transmission frame. For random coding arguments to hold, we assume for simplicity that $M^{(k)}$ is strictly finite (in essence corresponding to a finite depth interleaver) and let $N \to \infty$ so that $n^{(k)} \to \infty$. A similar line of work has been employed in [13]. An alternative line of work was suggested in [14] by jointly employing queues of secret keys allowing for the avoidance of secrecy outage events; however this option is not considered at present. The case of $M^{(k)} \to \infty$ corresponding to the ergodic case has been investigated in [8] and [9]. Finally, the finite MN codelength regime remains to be investigated; a viable framework can be provided by exploiting the results in [15].

III. System Model

We assume a Rayleigh BF-Gaussian channel and denote by $h_k^{(m)}$, $k \in \{1, \ldots, K\}$, $m \in \{1, \ldots, M\}$ the channel coefficients for the set of legitimate users and by $\tilde{h}_j^{(m)}$, $j \in \{1, \ldots, E\}$, $m \in \{1, \ldots, M\}$ the channel coefficients for the set of eavesdroppers. The channel coefficients are assumed to be i.i.d., following a zero-mean unit variance complex Gaussian distribution. Thus, all channel gains $g_k^{(m)} = |h_k^{(m)}|^2$ and $\tilde{g}_j^{(m)} = |\tilde{h}_j^{(m)}|^2$ are random variables drawn from an exponential distribution with underlying probability density function (pdf)

$$f(x) = e^{-x} \tag{1}$$

and a corresponding cumulative distribution function (cdf)

$$F(x) = 1 - e^{-x}. \tag{2}$$

The m-th OFDMA subchannel is allocated to the legitimate user with the highest channel gain α_m; the respective user is denoted by the index k_m^*, i.e.,

$$k_m^* = \arg \max_{k \in \{1, \ldots, K\}} g_k^{(m)}, \tag{3}$$

$$\alpha_m = g_{k_m^*}^{(m)}, \text{ for } m \in \{1, \ldots, M\}. \tag{4}$$

The random variable α_m corresponds to the K-th order statistic in a set of K channel gain realizations and its pdf is given by

$$f_K^{(K)}(x) = KF(x)^{K-1} f(x). \tag{5}$$

By analogy, we designate the index j_m^* to the eavesdropper with the highest channel gain β_m in the m-th OFDMA subchannel, i.e.,

$$j_m^* = \arg \max_{j \in \{1, \ldots, E\}} \tilde{g}_j^{(m)}, \tag{6}$$

$$\beta_m = \tilde{g}_{j_m^*}^{(m)}, \text{ for } m \in \{1, \ldots, M\}. \tag{7}$$

The random variable β_m corresponds to the E-th order statistic of E channel gain realizations, with pdf given by,

$$f_E^{(E)}(x) = EF(x)^{E-1} f(x). \tag{8}$$

During each transmission interval, the base station broadcasts codeword vectors $\mathbf{x}_\alpha \in \mathbb{R}^{MN}$. Correspondingly, we denote by $\mathbf{y}_\alpha^{(k)}$ the observation vector at the k-th legitimate user and by $\mathbf{y}_\beta^{(j)}$ the observation vector at the j-th eavesdropper. Furthermore, we denote by $\mathbf{u}^{(k)} \in \mathbb{R}^{MN}$ and by $\mathbf{w}^{(j)} \in \mathbb{R}^{MN}$ complex Gaussian circularly symmetric noise vectors with zero mean and unit variance, i.e.,

$$\mathbf{y}_\alpha^{(k)} = \mathbf{H}_\alpha^{(k)} \mathbf{x}_\alpha + \mathbf{u}^{(k)}, \tag{9}$$

$$\mathbf{y}_\beta^{(j)} = \mathbf{H}_\beta^{(j)} \mathbf{x}_\alpha + \mathbf{w}^{(j)}, \tag{10}$$

with

$$\begin{aligned}
\mathbf{H}_\alpha^{(k)} &= \operatorname{diag}\left(\mathbf{h}_k^{(1)}, \mathbf{h}_k^{(2)}, \ldots, \mathbf{h}_k^{(M)}\right), && (11)\\
\mathbf{H}_\beta^{(j)} &= \operatorname{diag}\left(\tilde{\mathbf{h}}_j^{(1)}, \tilde{\mathbf{h}}_j^{(2)}, \ldots, \tilde{\mathbf{h}}_j^{(M)}\right), && (12)\\
\mathbf{h}_k^{(m)} &= h_k^{(m)} \mathbf{I}_N, m \in \{1, \ldots, M\} && (13)\\
\tilde{\mathbf{h}}_j^{(m)} &= \tilde{h}_j^{(m)} \mathbf{I}_N, m \in \{1, \ldots, M\}, && (14)\\
\mathbf{u}^{(k)} &\sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N), && (15)\\
\mathbf{w}^{(j)} &\sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N), && (16)
\end{aligned}$$

with $\mathbf{I}_N$ denoting the $N \times N$ identity matrix.

IV. Probability of a Secrecy Outage in the High SNR Regime

Extending the results of [13] to networks with secrecy constraints, we define the secrecy capacity density (i.e., the instantaneous secrecy capacity) as the difference of the information density that is achievable at the set of legitimate users and the information density that is achievable at the set of eavesdropper on each of the OFDMA subchannels. The achievable information density depends on the degree of cooperation amongst the nodes in the two sets, as described in the following.

Definition: In the absence of cooperation, the secrecy capacity density (*non-cooperative instantaneous secrecy capacity*) of the M-block BF-Gaussian channel for a vector of input powers $\gamma = (\gamma_1, \ldots, \gamma_M)$ is given by

$$C_s^{(nc)}(\gamma) \doteq \frac{1}{M} \sum_{m=1}^{M} \left[\log \frac{1 + \alpha_m \gamma_m}{1 + \beta_m \gamma_m}\right]^+. \tag{17}$$

On the other hand, assuming the full diversity is exploited by the employment of an MRC receiver by the sets of legitimate users and eavesdroppers, the secrecy capacity density (*cooperative instantaneous secrecy capacity*) is given by

$$C_s^{(co)}(\gamma) \doteq \frac{1}{M} \sum_{m=1}^{M} \left[\log \frac{1 + \sum_{k=1}^{K} g_k^{(m)} \gamma_m}{1 + \sum_{j=1}^{E} \tilde{g}_j^{(m)} \gamma_m}\right]^+. \tag{18}$$

In the high SNR regime, i.e., for $\gamma_m \to \infty$ for $m = 1, \ldots, M$, the above expressions reach their maximum values, expressed respectively as

$$\hat{C}_s^{(nc)} = \frac{1}{M}\sum_{m=1}^{M}\left[\log\frac{\alpha_m}{\beta_m}\right]^+, \tag{19}$$

$$\hat{C}_s^{(co)} = \frac{1}{M}\sum_{m=1}^{M}\left[\log\frac{\sum_{k=1}^{K} g_k^{(m)}}{\sum_{j=1}^{E}\tilde{g}_j^{(m)}}\right]^+. \tag{20}$$

Based on the above, we can obtain asymptotic results for the probability of a secrecy outage in the high SNR regime. We investigate (i) the case in which there is no cooperation between any of the network nodes and (ii) the case in which the set of legitimate users and the set of eavesdroppers respectively form virtual multiple input multiple output (MIMO) networks. We note that in the absence of cooperation, the pdfs of α_m and β_m are given in (5) and (8) respectively. On the other hand, when the full multi-user diversity is exploited, the pdfs of the random variables at the output of the MRC combiners can be expressed as [16]

$$f^{(K)}(x) = \frac{Kx^{K-1}e^{-x}}{(K-1)!}, \tag{21}$$

$$f^{(E)}(x) = \frac{Ex^{E-1}e^{-x}}{(E-1)!} \tag{22}$$

for the sets of legitimate users and eavesdroppers, respectively.

The probability of a secrecy outage in a transmission frame w.r.t. to a target transmission rate τ in the non-cooperative case can be expressed as

$$\begin{aligned} P_{out}^{(nc)}(K,E,\tau) &= Pr(\hat{C}_s^{(nc)} < \tau) \\ &= 1 - \int_0^{\infty} K(1-e^{-x})^{K-1}e^{-x} \\ &\quad \int_0^{x2^{-\tau}} E(1-e^{-y})^{E-1}e^{-y}\mathrm{d}y\mathrm{d}x \\ &= K\Gamma(K)\sum_{n=1}^{E}(-1)^{n+1}\binom{E}{n}\frac{\Gamma(n2^{-\tau}+1)}{\Gamma(K+n2^{-\tau}+1)}. \end{aligned} \tag{23}$$

The secrecy outage probability in the cooperative case (virtual MIMO) can on the other hand be expressed as

$$\begin{aligned} P_{out}^{(co)}(K,E,\tau) &= Pr(\hat{C}_s^{(co)} < \tau) \\ &= 1 - \int_0^{\infty}\frac{Kx^{K-1}e^{-x}}{(K-1)!}\int_0^{x2^{-\tau}}\frac{Ey^{E-1}e^{-y}}{(E-1)!}\mathrm{d}y\mathrm{d}x \\ &= 1 - \frac{\sum_{n=0}^{K-1}\binom{K+E-1}{n}2^{n\tau}}{(1+2^{\tau})^{K+E-1}}. \end{aligned} \tag{24}$$

We compare the secrecy outage probabilities w.r.t. a target rate $\tau = 1$ bit/sec/Hz in Figs. 1 and 2. The effect of cooperation proves a decisive factor towards obtaining a region in which a secrecy outage occurs with very high probability and a region in which the secrecy outage probability is negligible; exploiting the full multi-user diversity the network exhibits a phase transition property in terms of secrecy.

Furthermore, in Fig. 3 we plot the minimum required number of legitimate users K versus the number of eavesdroppers E that is required in order to ensure the perfectly secret transmission of 1 bit/sec/Hz with a 99% certainty, i.e., for $P_{out}^{(co)}(K,E,1) < 0.01$. Notably, in the presence of a single eavesdropper ($E = 1$), this can be achieved with the full cooperation of as few as $K = 12$ legitimate users.

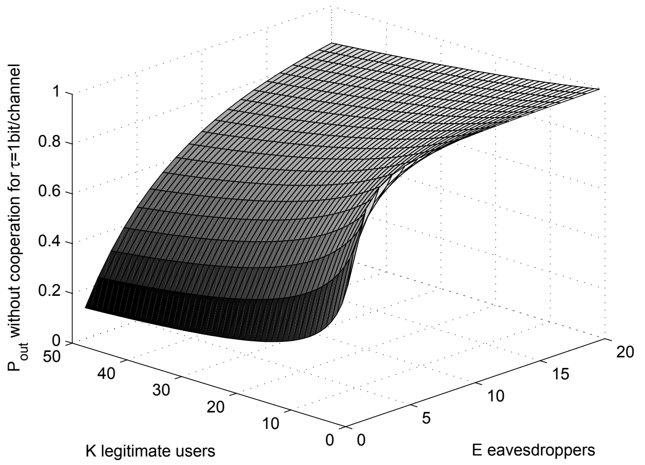

Fig. 1. Probability of a secrecy outage in the non-cooperative case for $\tau = 1$ bit/sec/Hz.

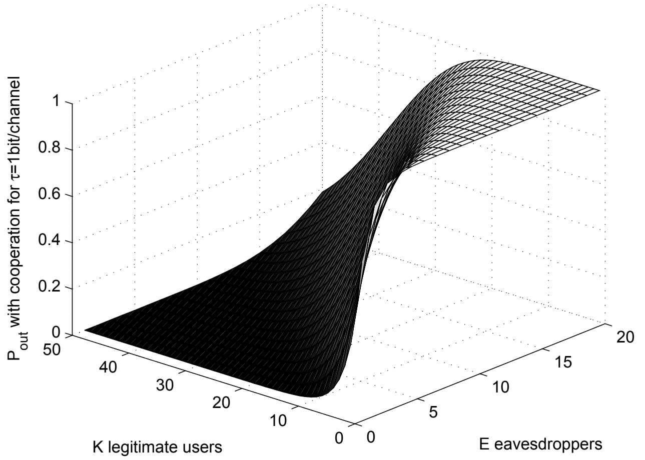

Fig. 2. Probability of a secrecy outage in the cooperative case for $\tau = 1$ bit/sec/Hz.

V. Block Fading Secrecy Capacity Density with Short-term Power Constraints

In the following we examine the BF-Gaussian secrecy capacity density in the non-cooperative and in the cooperative case with a short-term power constraint.

A. Secure Waterfilling in the Non-cooperative Case

Without loss of generality, we assume that the pairs of channel gains (α_m, β_m) have already been permuted so that the differences

$$\delta_m = \frac{1}{\beta_m} - \frac{1}{\alpha_m} \tag{25}$$

appear in non-increasing order.

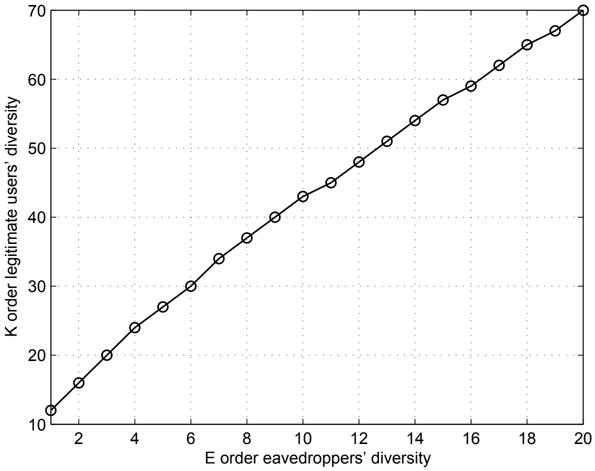

Fig. 3. Minimum number of legitimate users required to transmit 1 bit/sec/Hz with $P_{out}^{(co)} < 0.01$ as a function of the number of eavesdroppers.

Proposition 1: The power allocation $\gamma^* = (\gamma_1^*, \ldots, \gamma_M^*)$ that maximizes the secrecy capacity density of the non-cooperative M BF-Gaussian OFDMA network expressed as in (17) under a short-term power constraint in the form

$$\frac{1}{M}\sum_{m=1}^{M} \gamma_m^* \leq \mathcal{P}, \tag{26}$$

is the waterfilling solution

$$\gamma_m^*\left(\frac{1}{\lambda}\right) = \begin{cases} \frac{1}{2}\left[\sqrt{\delta_m^2 + \frac{4}{\lambda}\delta_m} - \left(\frac{2}{\alpha_m} + \delta_m\right)\right], & m \in \mathbb{Q} \\ 0, & \text{otherwise} \end{cases} \tag{27}$$

where $\mathbb{Q} = \{i : \frac{1}{\lambda} \geq \frac{1}{\alpha_i - \beta_i}\}$.

The functions $\gamma_m^*(\frac{1}{\lambda})$ are monotonically increasing and continuous in $\frac{1}{\lambda}$. As a result, there exists a unique integer μ in $\{1, \ldots, M\}$ such that $\frac{1}{\lambda} \geq \frac{1}{\alpha_m - \beta_m}$ for $m \leq \mu$ and $\frac{1}{\lambda} < \frac{1}{\alpha_m - \beta_m}$ for $m > \mu$. The waterlevel $\frac{1}{\lambda}$ can be derived by sequentially pouring water to the functions $\gamma_m^*(\frac{1}{\lambda})$ until the power constraint is met with equality, i.e.,

$$\sum_{m=1}^{\mu} \gamma_m^*\left(\frac{1}{\lambda}\right) = M\mathcal{P}. \tag{28}$$

B. Secure Waterfilling in the Cooperative Case

Similarly to the non-cooperative case, we assume that the pairs of MRC channel gains $(\sum_{k=1}^{K} g_k^{(m)}, \sum_{j=1}^{E} \tilde{g}_j^{(m)})$ have already been permuted so that the differences

$$\Delta_m = \frac{1}{\sum_{j=1}^{E} \tilde{g}_j^{(m)}} - \frac{1}{\sum_{k=1}^{K} g_k^{(m)}} \tag{29}$$

appear in non-increasing order.

Proposition 2: The power allocation $\hat{\gamma}^* = (\hat{\gamma}_1^*, \ldots, \hat{\gamma}_M^*)$ that maximizes the secrecy capacity density of the cooperative M BF-Gaussian OFDMA network expressed as in (18) under a short-term power constraint in the form

$$\frac{1}{M}\sum_{m=1}^{M} \hat{\gamma}_m^* \leq \mathcal{P}, \tag{30}$$

is the waterfilling solution

$$\hat{\gamma}_m^*\left(\frac{1}{\hat{\lambda}}\right) = \begin{cases} c_m, & m \in \hat{\mathbb{Q}} \\ 0, & \text{otherwise} \end{cases} \tag{31}$$

where $c_m = \frac{1}{2}\Big[\sqrt{\Delta_m^2 + \frac{4}{\hat{\lambda}}\Delta_m} - \Big(\frac{2}{\sum_{k=1}^{K} g_k^{(m)}} + \Delta_m\Big)\Big]$ and $\hat{\mathbb{Q}} = \Big\{i : \frac{1}{\hat{\lambda}} \geq \frac{1}{\sum_{k=1}^{K} g_k^{(m)} - \sum_{j=1}^{E} \tilde{g}_j^{(m)}}\Big\}$.

The functions $\hat{\gamma}_m^*(\frac{1}{\hat{\lambda}})$ are monotonically increasing and continuous in $\frac{1}{\hat{\lambda}}$. As a result, there exists a unique integer $\hat{\mu}$ in $\{1, \ldots, M\}$ such that $\frac{1}{\hat{\lambda}} \geq \frac{1}{\sum_{k=1}^{K} g_k^{(m)} - \sum_{j=1}^{E} \tilde{g}_j^{(m)}}$ for $m \leq \hat{\mu}$ and $\frac{1}{\hat{\lambda}} < \sum_{k=1}^{K} g_k^{(m)} - \sum_{j=1}^{E} \tilde{g}_j^{(m)}$ for $m > \hat{\mu}$. The waterlevel $\frac{1}{\hat{\lambda}}$ can be derived by sequentially pouring water to the functions $\hat{\gamma}_m^*(\frac{1}{\hat{\lambda}})$ until the power constraint is met with equality.

VI. Conclusions

In this paper, we have presented novel closed form expressions for the probability of a secrecy outage in M-BF Gaussian OFDMA networks in the non-cooperative and in the cooperative cases. Remarkably, it has been demonstrated that in a fully cooperative network in which the legitimate users and the eavesdroppers form virtual MIMOs it is possible to identify a simple criterion regarding the number of legitimate users as a function of the number of eavesdroppers in order to ensure the transmission of secret messages with a very high probability. As an example, in a fully cooperative network of 12 legitimate users in the presence of a single eavesdropper it is possible to transmit 1 bit/sec/Hz with perfect secrecy in 99% of the transmission frames. Furthermore, we have outlined the secure waterfilling approaches that correspond to non-cooperative and fully cooperative networks with short-term power constraints.

VII. Acknowledgements

This work was funded by the IOF "APLOE" (PIOF-GA-2010-274723) grant within the 7th Framework Program of the European Community.

References

[1] C. Shannon, "A mathematical theory of cryptography," *Bell System Technical J.*, vol. 28, p. 656715, Oct. 1949.

[2] E. Barka and M. Boulmalf, "Impact of encryption on the throughput of infrastructure WLAN IEEE 802.11g," in *Proc. of the IEEE Wireless Communications and Networking Conference*, Hong Kong, 11-15 Mar. 2007, pp. 2691 – 2697.

[3] S. Siwamogsatham, K. Hiranpruek, C. Luangingkasut, and S. Srilasak, "Revisiting the impact of encryption on performance of the IEEE 802.11 WLAN," in *Proc. 5th Int. Conf. on E. Eng./Electronics, Comp., Tel. and Inf. Techn.*, vol. 1, Krabi, Thailand, 14-17 May 2008, pp. 381 – 384.

[4] Y. Liang, H. V. Poor, and S. Shamai, *Information Theoretic Security*. Hanover, MA: Now Publishers, 2009.

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1385–1357, Oct. 1975.

[6] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wire-tap channel,” *IEEE Trans. Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[7] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” *IEEE Trans. Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

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

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

[10] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Information Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[11] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, “Physical layer security in wireless networks with passive and active eavesdroppers,” in *Proc. IEEE Global Communications Conf. (GLOBECOM)*, Anaheim, CA, Dec. 2012.

[12] ——, “On the resilience of wireless multiuser networks to passive and active eavesdroppers,” *IEEE J. Selected Areas in Communications*, vol. 31, no. 9, p. 1850, Sep. 2013.

[13] G. Caire, G. Taricco, and E. Biglieri, “Optimum power control over fading channels,” *IEEE Trans. Information Theory*, vol. 45, no. 5, pp. 1468–1489, Jul. 1999.

[14] O. Gungor, J. Tan, C. E. Koksal, H. El-Gamal, and N. B. Shroff, “Secrecy outage capacity of fading channels,” Dec. 2011, arXiv:1112.2791v1 [cs.IT].

[15] Y. Polyanskiy, H. V. Poor, and S. Verdú, “Channel coding rate in the finite blocklength regime,” *IEEE Trans. Information Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

[16] H.-C. Yang and M.-S. Alouini, *Diversity, Adaptation and Sceduling in MIMO and OFDM Systems*. Cambridge, UK: Cambridge University Press, 2011.