AN INFORMATION THEORETIC FRAMEWORK FOR ENERGY EFFICIENT SECRECY

Cristina Comaniciu
ECE Department
Stevens Institute of Technology
Cristina.Comaniciu@stevens.edu

H. Vincent Poor
Department of Electrical Engineering
Princeton University
poor@princeton.edu

Ruolin Zhang
ECE Department
Stevens Institute of Technology
rzhang2@stevens.edu

ABSTRACT

Physical layer energy-secrecy tradeoffs for wireless networks are investigated from an information theoretic perspective. An application layer characterization of physical layer secrecy is introduced to quantify the partial secrecy that can be achieved on a wireless transmission. Best effort and guaranteed partial secrecy channel models are introduced and analyzed. It is shown that a range of energy-secrecy Pareto optimal operating points can be achieved with an appropriate allocation of power resources between private and non-private data sub-streams.

Index Terms— *physical layer security, application layer security, partial secrecy, wire-tap channel, energy efficiency*

1. INTRODUCTION

For many wireless networks applications, energy efficiency, transmission reliability, and security constitute key performance requirements. In the context of energy efficiency for individual devices in wireless sensor networks, energy efficient security solutions are of prime interest. One possible security solution for wireless ad hoc networks, for which key distribution for encryption algorithms may be difficult to implement in a distributed fashion, is physical layer security. Secrecy assurance comes as a natural property of the physical layer, and can be exploited at the expense of a lower transmission rate, and higher energy per bit expenditure.

While secrecy and energy efficiency of communication systems are traditionally analyzed independently, in this work we consider jointly the secrecy and energy efficiency requirements, and we propose an information theoretic framework to analyze the energy-security tradeoffs that can be achieved by physical layer enforced secrecy. We introduce the notion of partial secrecy, which applies when the equivocation rate is smaller than the transmission rate, and thus the eavesdropper may potentially successfully decode part of the transmitted message. For many practical applications, such as sensed measurements and image data, a certain percentage of loss will be sufficient to render the decoded data useless for the eavesdropper. To characterize the partial secrecy metric we look jointly at the physical layer secrecy and application layer secrecy requirements. At the physical layer, the equivocation rate characterizes the uncertainty remaining at the eavesdropper after receiving the signal corresponding to a given transmitted message. At the application layer, the utility of the collective information obtained from all the physical layer messages potentially successfully decoded by the eavesdropper is characterized, and the application layer secrecy would require a close to zero utility for the eavesdropper. The utility that an eavesdropper would obtain at the application level can be related to how accurately the eavesdropper can decode (represent) the application layer message (e.g. image), which from an information theoretic perspective can be characterized by the rate-distortion function. We introduce thus a new metric to measure partial secrecy at the application level, as the minimum distortion that can be guaranteed at the eavesdropper.

Our work builds on the rich literature on information theoretic secrecy, which provides capacity regions for various channel models. For the classic Gaussian wire-tap channel [1] the secrecy-capacity region was first derived in [2], while analysis for fading channels and multiple antennas can be found for example in [3,4].

An extension of the wire-tap channel in which a common message is also transmitted was first proposed in [5]. This channel, which is known as the Broadcast Channel with Confidential Messages (BCC), serves as a paradigm for the study of security in networks involving both multicast and unicast transmissions. The work in [5] characterized the capacity-equivocation region and the secrecy capacity region of the discrete memoryless BCC, while in [6-11] we find a more general channel model for the fading BCC.

Our work departs from previous approaches by incorporating energy constraints and the notion of partial secrecy, which suitably characterizes the application layer secrecy requirements for some applications for which perfect secrecy is not required. Our proposed framework leads to derivation of Pareto optimal energy-secrecy curves that will enable a system designer to understand how the transmission system can dynamically adjust to varied system conditions with a soft degradation of secrecy.

2. SYSTEM MODEL

We consider the problem of transmitting information from a source to a destination node, via a Gaussian channel with multiplicative fading gain coefficients, having some security protection requirements against eavesdropper nodes, and under energy constraints. For illustrative purposes we assume that the channel state information (CSI) is known at both transmitter and receivers.

As opposed to previous work that has considered perfect secrecy requirements for a typical wireless data transmission, in this work, we address a specific set of applications (e.g. multimedia) for which a certain percentage of loss will render the decoded file unusable for an eavesdropper. As a consequence, for these applications, a requirement of partial secrecy rather than perfect secrecy will be sufficient.

We conjecture that partial secrecy can be achieved at a reduced energy per bit cost, and thus for suitable applications the source may tradeoff energy expenditure for secrecy rate. We define as the secrecy capacity, the maximum rate at which the source message can be transmitted with perfect secrecy.

In general, the secrecy level of a source message at the eavesdropper can be characterized by the *equivocation rate* [14], which measures the quantity of information that the eavesdropper gets about the source message, given its observations.

Previous work on physical layer security has focused on characterizing the perfect secrecy capacity, which requires that the achieved equivocation rate at the eavesdropper is equal to the message source rate. In this work we address the partial secrecy scenario, in which the equivocation rate may be smaller than the source rate for the confidential message, and it is equal to a percentage of the message rate being sent.

We define the *partial secrecy metric at the application layer*, as the minimum distortion D_{min} for the transmitted message that can be guaranteed to be incurred at the eavesdropper node. The minimum distortion is tightly related to the rate required to accurately represent the information in the source message, and it is application specific, being characterized by the rate-distortion function [14].

Since the eavesdropper will potentially decode the transmission partially, the quality of its decoded messages can be characterized in the same way as we characterize lossy compression. According to Shannon's rate distortion theory [14], the secrecy rate can be associated with the minimum distortion that the eavesdropper will experience on this transmission:

$$D_{\min} = f(R_e) = f(R_t - R_S), \quad (1)$$

where f is a decreasing function, R_t is the total transmission rate for the source and R_S is the secrecy rate.

We assume that a maximum transmission power P can be used by the source node, which has limited battery energy, and as such we consider as a performance metric the energy consumed per bit.

Using standard information theoretic notation, R_t bits of information are encoded and transmitted by the source, and the capacity R_t is measured in bits per transmission.

The energy per bit metric can be readily computed if we assume that R_t bits per transmission are being sent by the source in a given time unit interval (T), with power P. (The actual transmission rate will be related to the system bandwidth, but this metric is beyond the scope of this discussion.)

Then, the consumed energy per bit is given as

$$E_b = \frac{PT}{R_t} = \frac{P}{R_t} \quad \text{(Joules/bit) (2)}$$

We note that a higher source transmission rate R_t can be achieved if no secrecy requirements are imposed, and that R_t decreases when secrecy is desired, due to coding requirements. Higher energy consumption is expected in order to guarantee a higher level of secrecy at the physical layer.

We achieve partial secrecy by relaxing the requirement that the entire data stream must not be decoded by the eavesdropper. We thus allow for a fraction of the data to be potentially decoded, and based on how this can be achieved, two different partial secrecy models are proposed: (i) best effort and (ii) guaranteed.

Best effort partial secrecy model. In this model, the entire stream of data is treated equally, and a certain level of coding provides an information theoretic guarantee for a secrecy rate that is smaller than the source rate. In this case, part of the source transmission may be occasionally successfully decoded by the eavesdropper.

Guaranteed partial secrecy model. From the rate-distortion theory point of view, for many sources, the message's distortion does not usually decrease linearly with the percentage of rate used to describe the message. As such, following a reverse approach as for the classic lossy compression algorithms, a portion of the rate R_S that causes a maximum distortion (among all other R_S rate messages) could potentially be identified and transmitted securely. In this model, the initial stream of data is split into a private and a non-private stream. The "most significant" data (i.e. the stream that impacts most the distortion) will constitute the private stream and the rest of the data will be sent on a common channel.

3. BEST EFFORT PARTIAL SECRECY CHANNEL

In this scenario, the source transmits the message using a rate R_0, and part of that rate (R_S) can be transmitted securely.

The channel model that captures this scenario is a particular case of a wire-tap fading channel for which only a partial secrecy condition is imposed: the achieved secrecy rate, $R_S < R_0$. The energy – secrecy tradeoff is characterized by the required energy per bit to achieve a certain secrecy rate, which in turn corresponds to a guaranteed minimum distortion rate for the eavesdropper. The equivalent partial secrecy fading wire-tap channel mathematical model description follows.

We consider a fading wire-tap channel as in [3,4,6], in which the legitimate receiver and the eavesdropper experience different noise powers, μ^2 and σ^2, respectively, and different fading gain coefficients h_1 and h_2 (we assume quasi-static fading channel), respectively. The assumption on different noise power levels is fairly reasonable for wireless networks, where interference from other nodes often is approximated as adding to the background noise power.

As we have previously discussed, the source will transmit messages from a message set $W_0 = \{1, 2, \ldots, 2^{nR_0}\}$.

A $(2^{nR_0}, n)$ code consists of the following elements:

- One message set W_0, with the messages W_0 uniformly distributed over W_0;
- One stochastic encoder at the source node that maps each message $w_0 \in W_0$ to a codeword x^n;
- One decoder at the receiver that maps the received vector y^n to an estimate of the message $\hat{w}_0 \in W_0$;
- One decoder at the eavesdropper that tries to map the received vector z^n to a message estimate $\hat{\hat{w}}_0 \in W_0$;

The achieved secrecy level of transmission at the eavesdropper is measured by the equivocation rate defined as $\frac{1}{n} H(W_0 \mid Z^n)$.(3)

Based on previous work [6] on the secrecy capacity region for the fading wire-tap channel, we can readily determine the capacity region for the best effort partial secrecy channel, by accounting for the partial secrecy constraint:

$$C_{pS}^{beff} = \left\{ \begin{array}{l} (R_0, R_s): \\ R_0 \le \frac{1}{2}\log\left(1 + \frac{P|h_1|^2}{\mu^2}\right) \\ R_S \le \left[\frac{1}{2}\log\left(1 + \frac{P|h_1|^2}{\mu^2}\right) - \frac{1}{2}\log\left(1 + \frac{P|h_2|^2}{\sigma^2}\right)\right] \end{array} \right\} \quad (4)$$

The energy-secrecy tradeoff can be explored based on (2) and (4), where $R_t = R_0$ in (2). The budget power P allocated for the transmission of the stream will influence the partial secrecy capacity and the energy-distortion tradeoff curves.

4. GUARANTEED PARTIAL SECRECY CHANNEL

For this scenario we consider that the initial stream of data can be split into a private and a common information stream, which can be modeled as a variation of a fading broadcast channel with confidential messages (fading BCC), but without imposing the condition that the common stream needs to be correctly decoded by the eavesdropper as in [6]. We again assume different noise power

levels and different constant fading gain coefficients for the intended receiver and the eavesdropper.

As we have previously discussed, the source splits the original messages into a regular part and a confidential part, and as such, we define two message sets for the source: $W_0 = \{1, 2, \ldots, 2^{nR_0}\}$, and $W_1 = \{1, 2, \ldots, 2^{nR_1}\}$, as the regular and confidential set.

A $(2^{nR_0}, 2^{nR_1}, n)$ code consists of the following elements:

- Two message sets W_0 and W_1, with the messages W_0 and W_1 uniformly distributed over W_0 and W_1, respectively;
- One stochastic encoder at the source node that maps each message pair $(w_0, w_1) \in (W_0$ and $W_1)$ to a codeword x^n;
- One decoder at the receiver that maps the received y^n vector to an estimate of the message pair $(\hat{w}_0, \hat{w}_1) \in (W_0$ and $W_1)$;
- One decoder at the eavesdropper that tries to map the received z^n vector to a message pair estimate $(\hat{\hat{w}}_0, \hat{\hat{w}}_1) \in (W_0$ and $W_1)$;

The secrecy level of the confidential message W_1 achieved at the eavesdropper is measured by the equivocation rate similar to (3).

The overall secrecy rate achieved at the eavesdropper can be bounded as

$$\frac{1}{n}H(W_1 \mid Z^n) + \frac{1}{n}H(W_0 \mid Z^n) \geq \frac{1}{n}H(W_1 \mid Z^n). \qquad (5)$$

The bound in (5) on the overall secrecy rate is determined based on the observation that the equivocation rate is always nonnegative. In what follows we will neglect the potential partial secrecy achieved by the NP (common) stream, and impose total secrecy to be achieved for the confidential message (Pr stream).

Following on the work on the secrecy capacity region for the fading BCC, under a total transmitted power constraint P and superposition encoding [6], and adjusting for our partial secrecy conditions, we show that the partial secrecy-capacity region for the guaranteed partial secrecy channel can be determined as

$$C_{pS}^{gBCC} = \bigcup_{\beta \in [0,1]} \left\{ \begin{array}{l} (R_0, R_S): \\ R_0 \leq \frac{1}{2}\log\left(1 + \frac{(1-\beta)P|h_1|^2}{\mu^2 + \beta P|h_1|^2}\right) \\ R_1 \leq \left[\frac{1}{2}\log\left(1 + \frac{\beta P|h_1|^2}{\mu^2}\right) - \frac{1}{2}\log\left(1 + \frac{\beta P|h_2|^2}{\sigma^2}\right)\right] \\ R_S \geq R_1 \end{array} \right\}, \qquad (6)$$

where $(1-\beta)$ is the fraction of the total power allocated to the common message, and β is the fraction of the power budget that is allocated to the confidential message.

We note that the condition on R_1 in (6) represents the worst case R_1 guarantee, for the case in which we assume that the eavesdropper is able to decode the common message and cancel the interference from the common message to try to decode the private message.

As in [6], given the power budget P, β can be optimized to achieve the secrecy-capacity boundary, under the observation that the secrecy-capacity region is convex:

$$\max_{\beta \in (0,1)} \{\gamma_0 R_0(\beta) + \gamma_1 R_1(\beta)\} \quad (7).$$

By taking the derivative and setting it to 0 we get the optimal power allocation between the common and the confidential streams:

$$\beta\left(\frac{\gamma_1}{\gamma_0}\right) = \min\left\{\left(\frac{\gamma_1}{\gamma_2}\left(\frac{\sigma^2}{P|h_2|^2} - \frac{\mu^2}{P|h_1|^2}\right) - \frac{\sigma^2}{P|h_2|^2}\right)^+, 1\right\}. \qquad (8)$$

We note that for $\beta \in (0,1)$, we have the condition

$$\frac{\sigma^2}{\sigma^2 - \mu^2|h_2|^2/|h_1|^2} \leq \frac{\gamma_1}{\gamma_2} \leq \left(1 + \frac{\sigma^2}{P|h_2|^2}\right)\frac{P|h_1|^2|h_2|^2}{\sigma^2|h_1|^2 - \mu^2|h_2|^2}.$$

The choice of the ratio γ_1/γ_0, characterizes the energy-secrecy tradeoff, by influencing both the achievable R_S, as well as the achievable R_t in (2), $R_t = R_0 + R_1$. The range of values for the ratio γ_1/γ_0, determines the Pareto optimal curve that characterizes the secrecy-energy tradeoffs, i.e., the collection of points that give the best secrecy-energy performance, and for which one performance metric cannot be improved without negatively impacting the other. In the next section, numerical results are provided to illustrate these tradeoffs.

5. NUMERICAL RESULTS

We consider a system corrupted by Gaussian noise with signal-to-noise ratios μ^2/σ^2 of 0.2, 0.4 and 0.7 ($\sigma^2=1$). For illustration purposes, we define here as a minimum guaranteed distortion metric (D_{min}) the percentage of the source rate that achieves secrecy, and thus will not be available at the eavesdropper: $D_{min} = R_s/R_t$.

Best Effort Partial Secrecy Channel: To illustrate the results for this scenario, a range of SNRs at the eavesdropper were considered, ranging from 0.5dB to 5dB.

Fig. 1 depicts the total transmission rate, the achieved secrecy rate, the achieved minimum distortion at the eavesdropper and the energy per bit for $\mu^2/\sigma^2 = 0.4$ and two different ratios for the link gains: $|h_1|^2/|h_2|^2=1$ (solid lines) and $|h_1|^2/|h_2|^2=2.5$ (dashed lines). Fig. 2 depicts the energy-distortion tradeoff curves.

We note that although the overall rate and the secrecy rate increase with the increased transmission power (for fixed levels of noise), the achieved distortion decreases, while the energy per bit increases. As a consequence, the best energy-secrecy tradeoffs are achieved at lower power transmissions, but at the expense of a lower overall transmission rate. We further note that the best effort scheme does not offer much control on the energy-secrecy tradeoffs that can be achieved. Reducing the power at the expense of rate is one way to improve the energy and secrecy. Furthermore, we note that the energy-secrecy performance curves are greatly improved with better link gains for the intended receiver, which suggests that intelligent scheduling of transmission when the link gains are better for the intended transmission can greatly improve performance. A better control on the energy-secrecy tradeoffs can be achieved by the guaranteed partial secrecy scheme.

The Guaranteed Partial Secrecy Channel. For this channel model, the energy-secrecy performance will depend on the selection of β, the fraction of power allocated to the private stream. We recall that β was optimized to determine the boundary of the capacity region as in (6). The selection of the γ_1/γ_0 ratio will influence the achieved energy per bit consumption as well as the achievable distortion rate. We can see in Figure 3 how the common rate, secrecy rate and the achievable distortion depend on this ratio. For very small values of γ_1/γ_0, the emphasis is put mostly on R_0, and consequently all of the rate is transmitted as a common message. At the other extreme, large values for γ_1/γ_0 lead to only transmitting securely, while moderate values yield a combination of common and private streams. Due to space limitations, we have selected $\mu^2/\sigma^2 = 0.4$ and $|h_1|^2/|h_2|^2=1$ to illustrate our results in Fig.3, noting that similar trends for the plots were obtained for different values of the noise and link gain ratios.

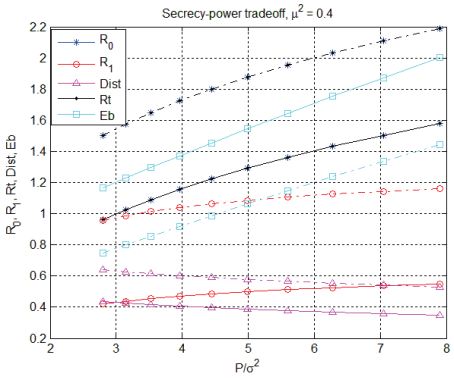

Fig.1. Best Effort Partial Secrecy $\mu^2/\sigma^2 = 0.4$; $|h_1|^2/|h_2|^2=1$ (solid line), $|h_1|^2/|h_2|^2=2.5$ (dashed line)

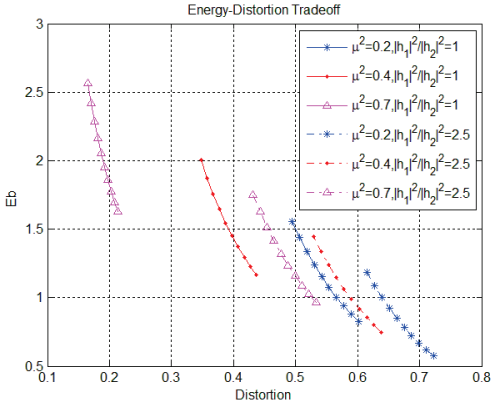

Fig.2. Energy-Distortion for Best Effort Partial Secrecy

In Fig. 4 we illustrate the energy-distortion tradeoffs for P/σ^2 = 3dB. We note that any distortion value can be obtained by appropriately allocating power between the private and non-private streams. Higher distortion levels come at the expense of a higher energy per bit requirement.

Finally, we illustrate via an image transmission example the impact of partial secrecy. While image transmission typically is not considered a secure transaction, a certain level of privacy can be achieved by enforcing a partial secrecy requirement.

We take as a transmission example the image Lena. The initial image is split into a private *(Pr)* and a common *(NP)* stream, according to the EZW compression algorithm [18]: the base image (low resolution) of rate cR_t is allocated to the common stream, while the difference image of rate R_t-cR_t = pR_t is allocated to the private stream (Fig. 5). The eavesdropper will be able to decode the common image, but not the private one, while the intended receiver will be able to decode both, and successfully reconstruct the initial image. The achieved distortion is equal to p. For the example in Figure 4, p = *0.6*. We can see that the eavesdropper will only be able to decode the common image (Fig. 5(a)) with a distortion of 0.6, which will result in sufficient level of privacy. Analyzing Fig. 4, we can see that by enforcing only a partial secrecy level, a significant energy-per-bit gain can be obtained, especially for more difficult transmission situations (eavesdropper channel noise close to the one of the intended receiver, and equal channel gains). For example, for μ^2/σ^2 = 0.7 we note about 36% energy savings for achieving 60% distortion (illustrated in Fig 5(a)) compared with the perfect secrecy case.

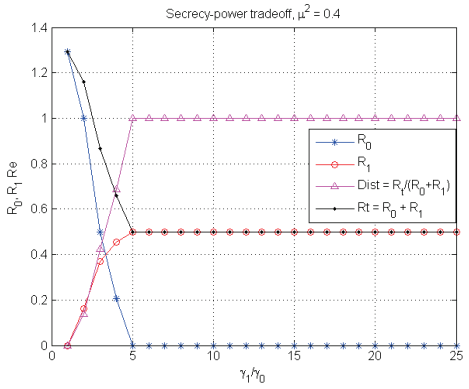

Fig.3. Performance metrics for Guaranteed Partial Secrecy

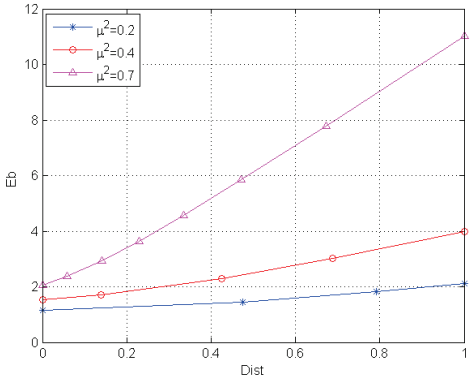

Fig.4. Energy-Distortion tradeoffs, P/σ^2 = 3 dB, $|h_1|^2/|h_2|^2=1$

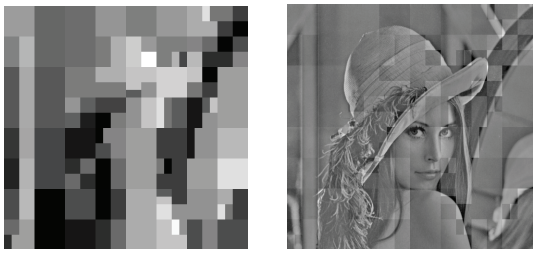

Fig.5. Lena image: (a) common image, (b) private image.

5. CONCLUSIONS

In this paper we have explored the energy-security tradeoffs for physical layer security in Gaussian wire-tap channels affected by multiplicative fading gains. Using an information theoretic framework, we have shown that security can be traded off for energy efficiency, and thus it allows for a graceful degradation of secrecy when energy resources are scarce. A new partial secrecy metric was defined as the minimum distortion rate that can be guaranteed at the eavesdropper.

We have shown that various Pareto optimal energy-secrecy operating points can be achieved by appropriately allocating the transmission power between private and non-private data sub-streams.

6. ACKNOWLEDGEMENT

This research was supported by the Office of Naval Research under grant number N00014-12-1-0767.

7. REFERENCES

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

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451-456, July 1978.

[3] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int'l Symp. Inform. Theory*, Adelaide, Australia, Sept. 2005, pp. 2152-2155.

[4] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int'l Symp. Inform. Theory,* Seattle, WA, USA, July 2006.

[5] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[6] Y. Liang, H. V. Poor and S. Shamai, "Secrecy capacity region of fading broadcast channels," in *Proc. IEEE Int'l Symp. Inform. Theory,* Nice, France, Jun. 2007, pp. 1291 – 1295.

[7] S. Shamai and A. Steiner, "A broadcast approach for a single-user slowly fading MIMO channel," *IEEE Trans. Inform. Theory*, vol. 49, no. 10, pp. 2617–2635, Oct. 2003.

[8] Y. Liang, L. Lai, H. V. Poor and S. Shamai, "The broadcast approach over fading Gaussian wiretap channels," in *Proc. IEEE Inform. Theory Workshop,* Taormina, Italy, Oct. 2009, pp. 1-5. [Also under review for the *IEEE Trans. Inform. Theory*]

[9] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inform. Theory*, 54(6), 2008, pp. 2470 – 2492.

[10] L. Li and A. J. Goldsmith, "Capacity and optimal resource allocation for fading broadcast channels-Part I: Ergodic capacity," *IEEE Trans. Inform. Theory*, vol. 47, no. 3, pp. 1083-1102, Mar. 2001.

[11] L. Li and A. J. Goldsmith, "Capacity and optimal resource allocation for fading broadcast channels-Part II: Outage capacity," *IEEE Trans. Inform. Theory*, vol. 47, no. 3, pp. 1103-1127, Mar. 2001.

[12] A. Jain, D. Gündüz, S. R. Kulkarni, H. V. Poor and S. Verdú, "Energy-distortion tradeoffs in Gaussian joint source-channel coding problems," *IEEE Trans. Inform. Theory.* vol. 58, no. 5, pp. 3153 - 3168, May 2012.

[13] D. N. C. Tse, "Optimal power allocation over parallel Gaussian broadcast channels," in *Proc. IEEE Int'l Symp. Inform. Theory*, Ulm, Germany, Jun. 1997, p. 27.

[14] T. M. Cover and J. A. Thomas, **Elements of Information Theory**, John Wiley and Sons, Inc.: New York, 1991.

[15] P. Cuff, "A framework for partial secrecy," in *Proc. IEEE Global Communications Conference*, Miami, FL, USA, Dec. 2010, pp. 1-5.

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

[17] R. Liu and W. Trappe, Eds., **Securing Wireless Communications at the Physical Layer**, Springer-Verlag, New York, 2010.

[18] J. M. Shapiro, "Embedded image coding using zerotrees of wavelet coefficients," *IEEE Trans. Signal Process* , vol. 41, no. 12, pp. 3445–3462, 1993.