On The Security Performance of Physical-Layer Network Coding

Kejie Lu[1], Shengli Fu[2], Yi Qian[3], and Tao Zhang[4]
[1] University of Puerto Rico at Mayagüez, Mayagüez, PR 00681
[2] University of North Texas, Denton, TX 76207
[3] National Institute of Standards and Technology, Gaithersburg, MD 20899
[4] New York Institute of Technology, Old Westbury, NY 11568

***Abstract*—Physical-layer network coding (PLNC) is a novel wireless communication technology, in which multiple transmitters can send signals on the same channel to the same receiver at the same time. Our previous studies have revealed that PLNC can substantially improve the throughput performance of the whole network. In this paper, we address the security performance of PLNC. In particular, we investigate the symbol error performance of a potential eavesdropper in the PLNC system. Extensive simulation studies show that PLNC can provide security means against passive eavesdroppers.**

I. Introduction

In the past decade, wireless communications and wireless networking have been developed and deployed significantly. In the foreseeable future, such a trend will continue and our society will steadily moving towards the ubiquitous computing age, in which wireless communication systems are essential and indispensable. Despite the promising features of wireless communications, there are still a number of challenges in the system design.

Amongst these challenges, the security, in particular the confidentiality, is one of the major difficult issue. This is mainly because of the broadcasting nature of wireless communications, which implies that a passive eavesdropper can overhear the transmission.

In addition to potential external eavesdropper, the confidentiality of wireless transmission may also be compromised due to the multi-hop transmission in multihop wireless networking technologies, such as *wireless mesh networks* [1]. For instance, in a WiMAX mesh network, service providers may choose to utilize the so-called *customer premise equipment* (CPE) owned by a customer to reduce the deployment cost of its network. However, such a low-cost solution may lead to the usage of un-trusted node in a multihop communication system.

In short, we note that the confidentiality concern is still a major challenge in wireless communication systems. And this is certainly not a new topic to the security community. Traditionally, a number of pioneer work [2]–[6] have been presented to address such an issue. For instance, in [2], Shannon defined *perfect secrecy* as the scenario that the eavesdropper cannot decode any meaningful information. Since such a scenario can be rather difficult to obtain, Wyner provided an alternative in [3], in which he defined the secrecy rate as the rate at which the eavesdropper's equivocation rate is no larger than the information rate of the legitimate receiver. According to [3], a positive secrecy rate can be obtained if the eavesdropper receives a degraded version of the signals received by the legitimate receiver, for discrete memoryless channel. In other words, the noise level at the eavesdropper is larger than that of the legitimate receiver. Wyner's model was later extended in [4]–[6].

Note that in most existing studies, there is a fundamental assumption for wireless communication that a receiver can only receive the signal from a single transmitter on a particular radio channel at a certain time. More signals from other transmitter will be considered as interference. This assumption, however, is no longer valid in *physical-layer network coding* (PLNC) system [7]. In PLNC system, a receiver can receive more than one signals from different transmitters on the same radio channel at the same time.

Our previous study have revealed the potential improvement of PLNC in terms of the throughput capacity [8]. In this paper, we address the security performance of PLNC. In particular, we investigate the symbol error performance of a potential eavesdropper in the PLNC system. Specifically, we consider two general cases: 1) the eavesdropper is an external node in the multihop wireless path; and 2) the eavesdropper is one of the intermediate node. Extensive simulation studies show that PLNC can provide security means against passive eavesdroppers.

The rest of this paper is organized as the follows. In Section II, we present the wireless communication system model with physical layer network coding. In Section III and Section IV, we elaborate on the symbol error performance of an external eavesdropper and an internal eavesdropper, respectively. In these two sections, extensive simulation experiments are conducted. We then conclude the paper in Section V.

II. Physical-Layer Network Coding

In this section, we first introduce the background of physical-layer network coding. We then describe the basic system model for the PLNC, the forwarding method, and the scheduling scheme.

A. background

In the past few years, network coding [9] has attracted significant attention in the research community because it has the potential to substantially improve the throughput performance of communication networks. In general, a node (switch and router) in current communication networks shall forward an incoming data unit, such as a packet or a time slot of data, to a certain output link at a later time, without changing the content. Such an operation can be considered as a simple "copy" function. By comparison, if network coding is used, then the output of the node can be expressed as a function that takes more than one previously received data units as the inputs.

In general, network coding can be applied to both wired and wireless networks. Particularly, in wired networks, most existing work have been focused on the multicast scenario [10]. In wireless networks, on the other hand, unicast traffic can also exploit the benefits of network due to the broadcast nature of wireless communication. In the literature, a number of studies have been developed to address the theoretical issues [8], [10]–[12] and practical implementations [13].

While the original design of network coding was implemented in or above the data link layer, the information can also be manipulated directly on the physical layer, which is natural in wireless communication systems because signals can be added in the time domain at the receiver. Such a concept is known as *physical-layer network coding* (PLNC) [7]. In PLNC, the intermediate nodes in a multi-hop path can receive combined signals from different source nodes at the same time over the same radio channel.

In traditional systems, if there are more than one signal arrives on the same channel at the receiver, all of them are interweaved and interfere with others. For PLNC systems, such a scenario is acceptable because the relay nodes is interested only in the summation, instead of individual signals. As shown in [14], the capacity is doubled in a simple three-node wireless communication system with symmetric 2-way traffic. In our previous study, we have conducted theoretical analysis to investigate the throughput capacity of random wireless networks [8].

B. The Basic System Model

In this paper, we consider the same system model as that in [7], [15], in which a three-node network is discussed to demonstrate the throughput improvement over other schemes. As shown in Fig. 1, nodes A will send information x_1 to node B, and B send x_2 to A. Both transmission will be relayed by node R. This is an typical scenario in WLAN, where relay R is the access point (AP) and A and B are the nodes of a basic service set (BSS).

The traditional relay schemes may take four steps to finish the information exchange:

1) $A \mapsto R : x_1$;
2) $R \mapsto B : x_1$;
3) $B \mapsto R : x_2$;
4) $R \mapsto A : x_2$;

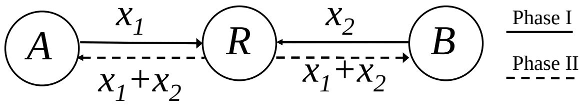


Fig. 1. System Model

For the same transmission requirement, the network coding relay may take three steps. Let the information symbols x_m be from some finite field with size M.

1) $A \mapsto R : x_1$;
2) $B \mapsto R : x_2$;
3) $R \mapsto \{A, B\} : x_R = x_1 \bigoplus x_2$;

where $\bigoplus$ denotes the summation in modulo to M. When $M = 2$, $\bigoplus$ is equivalent to the XOR operation for the bit level information. Since node A has the *a priori* information of x_1, A can decode x_2 through the modulo operation $x_2 = x_R \bigoplus x_1$. Similarly, B can extract x_1 through $x_1 = x_R \bigoplus x_2$. The network coding scheme not only reduce one time slot for the information exchange, but also fully exploit the broadcast benefits of wireless channel, which is always ignored in previous designs.

Further improvement is achieved through physical layer network coding, as shown in [7], [14], [15], where the information can be exchanged within two steps:

1) $A \mapsto R : x_1$, $B \mapsto R : x_2$;
2) $R \mapsto \{A, B\} : x_R = x_1 + x_2$;

where A and B will transmit their information simultaneously to the relay R at the first time slot. The relay node will broadcast the summation of x_1 and x_2 to both A and B.

C. The Forwarding Method

To facilitate PLNC, two major forwarding methods have been proposed. The first approach is known as *amplify-and-forward* (AF), in which the relay node will simply amplify what have been received in the first phase. For the simple three-node model we have illustrated above, we know that the received signal in the first time slot at the relay node R can be represented by:

$$(h_{AR} \times x_1) + (h_{BR} \times x_2) + N_R, \tag{1}$$

where h_{IJ} stands for the fading coefficient for the channel from I to J, and N_R represents the Gaussian noise at node R. According to [14], in the next time slot, relay node R will broadcast the received signal to both A and B. Therefore, node A will receive

$$(h_{RA} \times h_{BR} \times x_1) + (h_{RA} \times h_{AR} \times x_2) + (h_{RA} \times N_R) + N_A. \tag{2}$$

From Eq. (2) we can observe that, if node A can decode x_2 if it has the channel coefficients h_{AR}, h_{BR}, and h_{RA}. Similarly, node B can also decode message x_1 with certain channel coefficients.

Although the AF scheme provide a solution for PLNC, our previous investigation shows that it is not a good application for wireless communications with more than two hops. Therefore, in this paper, we consider the second forwarding

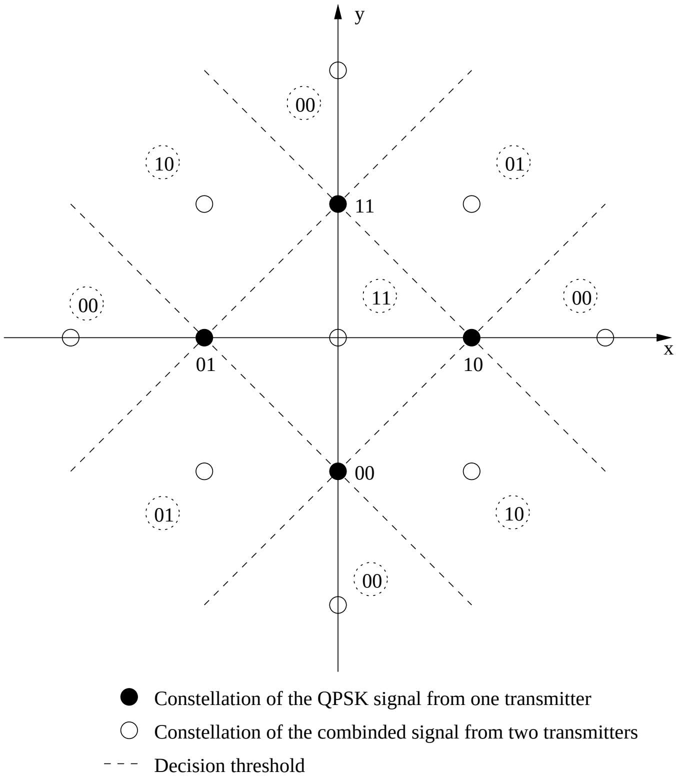

y
00
10
01
11
11
00
00
x
01
10
00
01
10
00
Constellation of the QPSK signal from one transmitter
Constellation of the combinded signal from two transmitters
Decision threshold

Fig. 2. Received constellation at relay node for QPSK.

scheme, namely, *decode-and-forward* (DF). In DF, the relay node will try to decode the received signal in such a way that it can transmit signals with the same modulation scheme in the second phase.

For the DF scheme, an example of the received signal at relay node is shown in Fig. 2 where both A and B transmit QPSK symbols to relay. While there are four constellation points for QPSK (solid circles), we can observe that there are a total of nine (9) nodes for the constellations of the combined signals (empty circles). Nevertheless, each of the nine nodes can be assigned by two bits (indicating with circles with dash lines). Consequently, each node in the system can use QPSK to transmit signals.

D. The Scheduling Scheme

With the DF scheme described above, we can use a simple scheduling scheme for the system if both node A and node B have infinite number of messages to send. To facilitate the discussion, we consider that the time has been partitioned into equal-length slots. In addition, we let $x_1(i)$ and $x_2(i)$ denote the i-th message from A to B and from B to A, respectively. Consequently, we can express the transmitted signals by using $x_1(i)$ and $x_2(i)$. The scheduling policy can then be described as below.

1) In the first time slot, nodes A and B send messages $x_1(1)$ and $x_2(1)$ to node R.
2) In the $(2k)$-th time slot ($k \geq 1$), node R send message $x_1(k)$+$x_2(k)$ to nodes A and B.

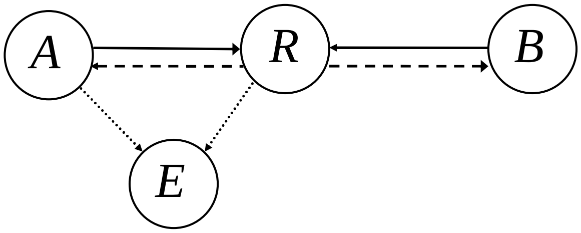


Fig. 3. System Model with external eavesdropper.

3) In the $(2k+1)$-th time slot ($k \geq 1$), nodes A and B send messages $x_1(k+1)+x_2(k)$ and $x_2(k+1)+x_1(k)$ to node R.
   In this manner, the relay node R will receive
   $$x_1(k+1) + x_2(k) + x_2(k+1) + x_1(k)$$
   in time slot $2k+1$. Note that node R has $x_1(k)$+$x_2(k)$, it can decode $x_1(k+1)$+$x_2(k+1)$.

From the description above, we can see that an external eavesdropper is able to decode transmitted messages between node A and node B if and only if it starts eavesdropping from the first time slot. In many cases, this makes the overhearing difficult. Nevertheless, we will study this worst case in the next section, in which the eavsdropper starts overhearing from the first time slot.

III. Symbol Error Performance of an External Eavesdropper

In this section, we consider the symbol error performance of an external eavesdropper. Without losing generality, we consider that an eavesdropper, denoted as node E, is located to the left of the relay node R, as shown in Fig. 3.

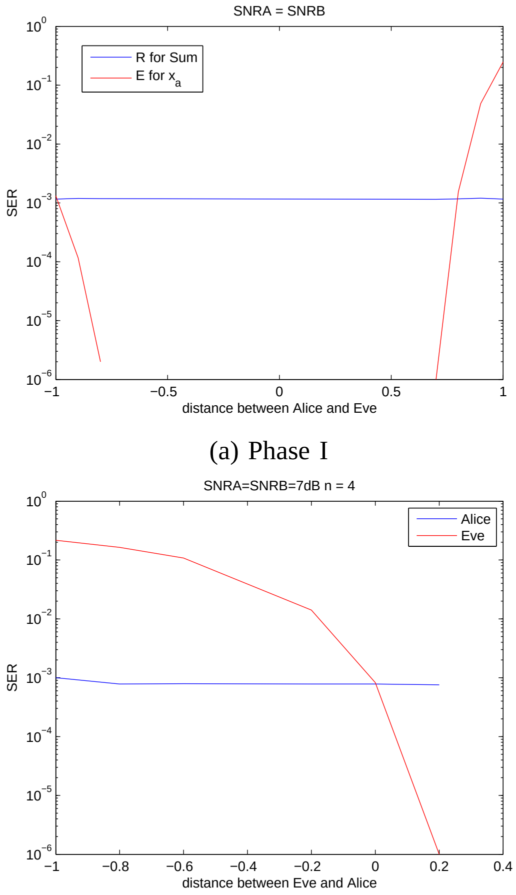
Clearly, Fig. 3 is a special case of the secrecy systems [2]. In this paper, we follow the main idea of [3]. Particularly, in our case, we are interested in the situation that the message rate at node E is the same as the message rate at node A (for decoding $x_2(i)$) and at node R (for decoding $x_1(i) + x_2(i)$). In the rest of this section, we elaborate on the symbol error performance of node A, R, and node E.

To simplify the discussion, we assume that node A, B, and R are on a straight line. Moreover, the distance between nodes A and R is the same as the distance between nodes B and R. We also assume that the signal propagation is governed by the large-scale propagation effects with the well-known log-distance path loss model [16]:

$$\overline{PL}(dB) = \overline{PL}(d_0) + 10nlog(\frac{d}{d_0}) \tag{3}$$

where n is the path loss exponent, d_0 is the close-in reference distance, and d is the distance between transmitter and receiver.

In Fig. 4, we first choose BPSK as the modulation scheme for nodes A, B and R. We consider Gaussian white noise and we let the noise level at every node be identical. In Fig. 4 (a), we compare the symbol error ratio (SER) performance in



(a) Phase I

(b) Phase II

Fig. 4. Symbol error performance for an external eavesdropper ($n = 4$).

phase I, and let the SNR at the relay node be 7dB. In this manner, the SER for decoding the summation of the two incoming signals is about 10^{-3}, which is represented by the blue line in Fig. 4 (a).

To evaluate the SER performance of node E, we assume a simple scenario, in which node E is also located on the straight line that links nodes A, B, and R. In this way, let node A be located at the origin and node R be located at 1 unit length. Now consider the coordinate of node E as the parameter, we show the SER performance for decoding signals from node A in Fig. 4 (a) (represented by the red line). We can clearly observe that, the SER will increase with the increase of the distance between nodes A and E. Particularly, if node E is located at -1, then the SER performance of E is slightly better than the SER performance of node R.

However, given the same distance to node A, if node E is between nodes A and R, the situation is completely different. Specifically, we observe that the SER performance of node E at location 1 is much worse than that of the relay node. The main reason for this phenomenon is that the signals from node B become strong interference to node E, since it is rather close to node R. We can further observe that these two curves has an intersection point and the corresponding coordinate is about 0.8. This implies that the region that the eavesdropper can have a better SER performance than the receiver is about $[-1, +0.8]$, which is smaller than the region without using PLNC, and the latter can be directly estimated as $[-1, +1]$.

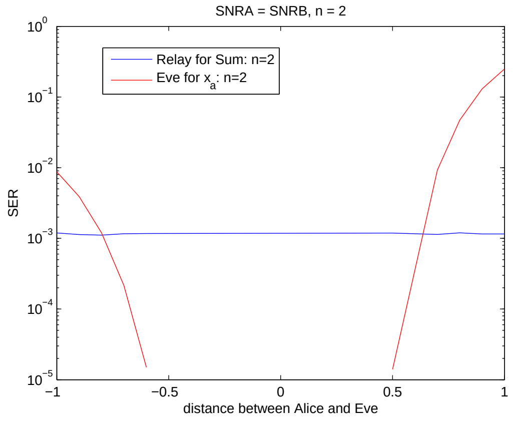


Fig. 5. Symbol error performance for an external eavesdropper ($n = 2$).

In Fig. 4 (b), we investigate the SER performance in the second phase. In particular, we compare the decoding of the signals from node R at nodes A and E. Note that node A will need the coded signal $x_1(1) + x_2(1)$ so that it can decode message $x_2(1)$; and node E also needs to get $x_2(1)$ because node A will send $x_1(2) + x_2(1)$ in the next slot according to our scheduling method proposed in the last section.

From Fig. 4 (b) we can observe that the SER performance of node A is a little lower than 10^{-3}. On the other hand, performance of node E is about the same if it is at the origin, and the SER increases with the decreases of the coordinate, since the distance between nodes E and node R increases. Clearly, the eavesdropping region in the second phase is about [0, +2]. Taking the intersection of the region of phase I and phase II, we can get the eavesdropping region for PLNC in this experiment as [0, +0.8], which is smaller than $[-1, +1]$, which is the region without using PLNC.

In our previous experiment, we have assumed that the path loss exponent be 4. In Fig. 5, we investigate another scenario in which the path loss exponent is 2, which is the value for the classic free-space path loss model [16]. In this figure, only the SER performance in the first phase is shown because the figure for phase II is almost the same as that in Fig. 4 (b). From this figure we observe an interesting phenomenon that the intersection points of the two SER performance is much closer to the origin. In particular, we note that the coordinates for the two intersection points are about -0.8 and $+0.6$. In other word, the effective eavesdropping region is now $[-0.8, +0.6]$ in the first phase. Compared to the previous experiment, we observe that interference to node E is much larger because the path loss exponent is now 2. Consequently, the SER performance of the eavesdropping node is further degraded, which implies a better privacy to the transmission from node A.

Finally, Fig. 6 compares the SER performance, in the first

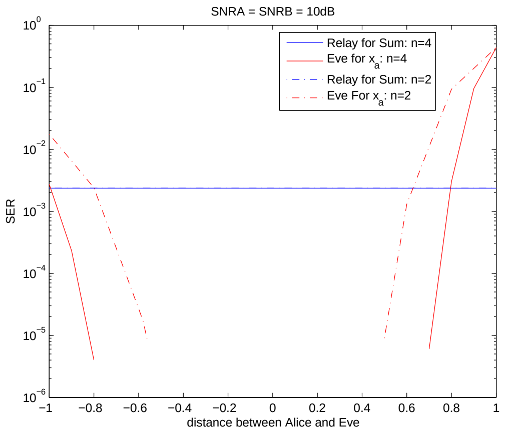


Fig. 6. Symbol error performance for an external eavesdropper with QPSK.

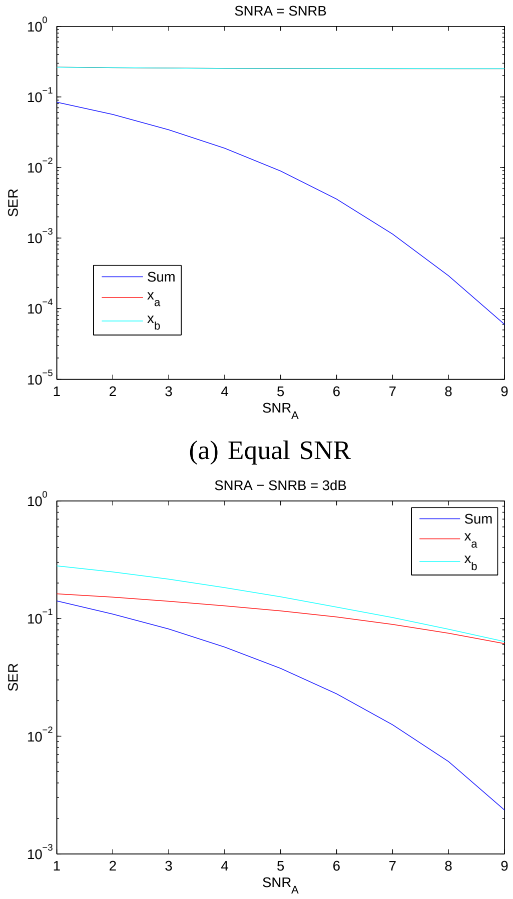
phase, of the relay node R and that of the eavesdropping node E, when QPSK is used as the modulation method. Here we choose the SNR at R for the signal from A and B be 10dB, which leads to approximately 2×10^{-3} SER for the summation of $x_1 + x_2$. In Fig. 6, the results for $n = 2$ and $n = 4$ are put together so we can compare their behavior. Clearly, we observe similar phenomenon that appears in the previous experiments, in which BPSK is the modulation scheme.

IV. Symbol Error Performance of an Internal Eavesdropper

In the previous section, we have discussed the SER performance of an external eavesdropper. In this section, we investigate another common scenario, in which the relay node itself is the eavesdropper. Traditionally, if an intermediate node is compromised, then the messages forwarded by the compromised node are no longer secure, and thus the confidentiality of the the transmission is breached in the physical layer. However, this situation is no longer true in the PLNC scenario, because the relay node is only responsible for decode and forward the summation of two incoming signals. In other words, we expect that the PLNC system shall provide strong confidentiality against the eavesdropping at the relay node.

Fig. 7 illustrates the SER performance of decoding the summation of the incoming signal (i.e., $x_1 + x_2$) and the individual signals (i.e., x_1 and x_2). In Fig. 7, we assume that the two incoming signals have the same power level. Here we use BPSK as the modulation scheme for signals at nodes A and B. We can observe that, while the SER performance of the combination improves with the increase of the SNR level, the SER performance for decoding individual messages x_1 and x_2 remain constant at about 25%. This result shows that the message can be securely transmitted through an compromised node is the two incoming signals have the same power level at the receiver, which is an excellent feature.

In Fig. 7 (b), we consider a slightly different scenario, in which the signal power levels from the two source node have 3dB difference. We first observe that, in such a case, the SER performance of decoding the summation is degraded compared to the equal power case above. For instance, in the previous case, the SER is 10^{-3} and the SNR is about 7dB. For the latter case, however, to obtain the same SER may need the higher SNR be about 10dB. Nevertheless, we can still observe that the SER performance of decoding individual message remain much worse than that of decoding the summation, even though the performance for decoding individual messages can improve with the increase of SNR. Particularly, we observe that when the higher SNR is 9dB, the SER difference is more than one order of magnitude.



(a) Equal SNR

(b) SNRA is 3dB higher than SNRB

Fig. 7. Symbol error performance for an internal eavesdropper.

From the results above, we can conclude that the PLNC scheme can significantly improve the confidentiality against an internal eavesdropper.

V. Conclusions

In this paper, we address the security issue in physical-layer network coding (PLNC). Specifically, we have investigated the symbol error performance of a potential eavesdropper in the PLNC system. Two general cases have been investigated. In the first case, we studied the symbol error performance of an external eavesdropper. Simulation results demonstrate that the PLNC can improve the security by limiting the area, in which eavesdropping may be able to decode the transmitted signals. In the second case, we considered the scenario that an intermediate relay node is compromised and acting as an eavesdropper. Results show that it is rather difficult for the relay node to decode individual message because the PLNC system tries to send different signals to the same relay node over the same channel, at the same time. In summary, extensive simulation studies show that PLNC can provide security means against passive eavesdroppers.

REFERENCES

[1] Kejie Lu, Yi Qian, and Hsiao-Hwa Chen, “A Secure and Service-Oriented Network Control Framework for WiMAX Networks,” IEEE Communications Magazine, Vol. 45, No. 5, pp. 124–130, May 2007.

[2] C. E. Shannon, “Communication Theory of Secrecy Systems,” *Bell Syst. Tech. J.*, vol. 28, pp. 656-715, Oct. 1949.

[3] A. Wyner, “The Wire-Tap Channel,” *Bell Syst. Tech. J.*, vol. 54, pp. 1355–387, Oct. 1975.

[4] I. Csiszar and J. Korner, “Broadcast Channels with Confidential Messages,” *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[5] 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.

[6] L. Ozarow and A. D. Wyner, “Wire-Tap Channel II,” *Bell Syst. Tech. J.*l, vol. 63, no. 10, pp. 2135–2157, Dec. 1984.

[7] S. Zhang and S. C. Liew, and P. P. Lam, “Physical-layer Network Coding,” in *Proc. MobiCom’06,*, pp. 358–365, ACM, 2006.

[8] Kejie Lu, Shengli Fu, and Yi Qian, “Capacity of Random Wireless Networks: Impact of Physical-Layer Network Coding,” in *Proc. IEEE ICC 2008*, Beijing, China, May 2008.

[9] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, “Network Information Flow,” *IEEE Transaction on Information Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.

[10] D. S. Lun, N. Ratnakar, M. Medard, R. Koetter, D. R. Karger, T. Ho, E. Ahmed, and F. Zhao, “Minimum-cost Multicast over Coded Packet Networks,” *IEEE Transaction on Information Theory*, vol. 52, no. 6, pp. 2608–2623, Jun. 2006.

[11] R. Dougherty, C.Freiling, and K. Zeger, “Unachievablility of Network Coding Capacity,” *IEEE Trans. on Information Theory*, vol. 52, no. 6, pp. 2365–2372, June 2006.

[12] A. Ramamoorthy, J. Shi, and R. Wesel, “On the Capacity of Network Coding for Random Networks,” *IEEE Trans. on Information Theory*, vol. 51, no. 8, pp. 2878–2885, Aug. 2005.

[13] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, “XORs in the Air: Practical Wireless Network Coding,” *IEEE/ACM Trans. Networking*, vol. 16, no. 3, pp. 497–510, June 2008.

[14] S. Katti and D. Katabi, “Embracing Wireless Interference: Analog Network Coding,” in *Proc. Applications, Technologies, Architectures, and Protocols for Computer Communications, 2007*, pp. 397–408, 2007.

[15] P. Popovski and H. Yomo, “Wireless Network Coding by Amplify-and-Forward for Bi-directional Traffic Flows,” *IEEE Comm. Lett.*, vol. 11, no. 1, pp. 16–18, Jan. 2007.

[16] T. S. Rappaport, *Wireless Communications: Principles and Practice*, the second edition, Prentice Hall, 2002.