

Kennesaw State University
DigitalCommons@Kennesaw State University

KSU Proceedings on Cybersecurity Education,
Research and Practice

2018 KSU Conference on Cybersecurity Education,
Research and Practice

Oct 20th, 10:55 AM - 11:20 AM

Study of Physical Layer Security and Teaching Methods in Wireless Communications


Zhijian Xie

NC A&T State University, zxie@ncat.edu

Christopher Horne

NC A&T State University, ckhorne@ncat.edu

Follow this and additional works at: <https://digitalcommons.kennesaw.edu/ccerp>

 Part of the [Educational Methods Commons](#), [Electromagnetics and Photonics Commons](#), [Engineering Education Commons](#), [Information Security Commons](#), [Scholarship of Teaching and Learning Commons](#), [Special Education and Teaching Commons](#), [Systems and Communications Commons](#), and the [Technology and Innovation Commons](#)

Xie, Zhijian and Horne, Christopher, "Study of Physical Layer Security and Teaching Methods in Wireless Communications" (2018). *KSU Proceedings on Cybersecurity Education, Research and Practice*. 3. <https://digitalcommons.kennesaw.edu/ccerp/2018/education/3>

This Event is brought to you for free and open access by the Conferences, Workshops, and Lectures at DigitalCommons@Kennesaw State University. It has been accepted for inclusion in KSU Proceedings on Cybersecurity Education, Research and Practice by an authorized administrator of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

Abstract

In most wireless channels, the signals propagate in all directions. For the communication between Alice and Bob, an Eavesdropper can receive the signals from both Alice and Bob as far as the Eavesdropper is in the range determined by the transmitting power. Through phased array antenna with beam tracking circuits or cooperative iteration, the signals are confined near the straight line connecting the positions of Alice and Bob, so it will largely reduce the valid placement of an Eavesdropper. Sometimes, this reduction can be prohibitive for Eavesdropper to wiretap the channel since the reduced space can be readily protected. Two course modules have been developed for students to understand signal propagation in physical layer and how it is used to enhance channel security along with natural and man-made noise.

Location

KC 400

Disciplines

Educational Methods | Electromagnetics and Photonics | Engineering Education | Information Security | Scholarship of Teaching and Learning | Special Education and Teaching | Systems and Communications | Technology and Innovation

Study of Physical Layer Security and Teaching Methods in Wireless Communications

Xie and Horne: Study of Physical Layer Security and Teaching Methods in Wireless

Zhijian Xie, *Senior Member IEEE*, Christopher Horne, *Member IEEE*
North Carolina A&T State University, Greensboro, NC, USA
Email: zxie@ncat.edu, ckhorne@ncat.edu

I. INTRODUCTION

Wireless networks are increasingly used for a wide range of applications, including social networking, environmental monitoring, banking and other financial transactions. The benefits of mobile wireless communication freeing people from hard connections to a fixture are realized by having all signals fill up the space. The receiving devices are responsible to retrieve the information from the signals which are available to any devices in nearby space. Thus, security is an important issue in wireless communication system. Traditionally security is implemented at logical layers of communication networks, such as data encryption, which works well in most current situations with certain computation overhead [1-2]. The computation overhead is tolerable for most traditional system due to the advancement of computing power. However, in some emerging wireless networking architectures, issues of key management or computational limitation make the use of data encryption difficult or even non-realistic. Examples include ad hoc networks, sensor networks, radio-frequency identification (RFID), etc. [1,6]

To enhance security in traditional and emerging wireless networks, physical layer security has become a major research topic recently [3]. Leveraging the properties of wireless signal propagation, a properly designed system can inhibit the ability of potential eavesdroppers to gain information on confidential messages. The mechanism includes the exploration of noise, fading, interference and path diversity with multiple antennas.

Based on the physical layer security in wireless communications and related research, we developed two course modules to introduce the topics in these fields to undergraduate students. These two course modules are designed to teach students the nature of wireless signal propagation, communication secrecy, secrecy capacity, information entropy, spatial resolution, and cooperative protection. Two learning scenarios were developed based on previous studies [1,6,7]. Each course module has two parts: a) a lecture class with PowerPoint presentation on noise and fading in wireless channels and their security risks and b) a hands-on lab exercise using MATLAB to simulate a wireless communication channel with the presence of Eavesdroppers. Startup MATLAB codes were provided to students for each module.

This paper is organized as follows: Section II provides a background on the fundamental theory of wireless channel secrecy and secrecy capacity. Section III discusses Directional antenna beamforming and path diversity through a multiple

antenna array as well as use of relay nodes for cooperative protection. Section IV describes the teaching method used for the modules while Section V describes our teaching experience and student outcomes. Finally, Section VI summarizes lessons learned.

II. BACKGROUND

In most wireless channels, the wireless signal propagates in all directions. For the communication between Alice and Bob, an Eavesdropper can receive the signals from both Alice and Bob as far as the Eavesdropper is in the range defined by the transmitting power. The current security mechanism largely relies on cryptographic protocols, which is heavy-overhead and coordination intensive. Physical layer security is an on-going research area that make use of properties of the physical layer and seeks to achieve perfect secrecy in the wireless channel.

For example, through phased array antenna with beam tracking circuits, the signals are confined near the straight line connecting the positions of Alice and Bob. This will largely reduce the valid placement of an Eavesdropper. Sometimes, this reduction can be prohibitive for Eavesdropper to wiretap the channel since the reduced space can be readily protected. The learning objectives of these modules are that students will be able to understand signal propagation in physical layer and how channel security can be enhanced through properly designed system.

A. Communication Secrecy

Figure 1 shows Alice communicating with Bob while Eavesdropper (Eve) is in the range of the wireless signal propagation. The information from X to Y is represented as $I(X; Y)$, and the information from X to Z represented as $I(X; Z)$. The difference between the two information is defined as the secrecy capacity [4], $C = I(X; Y) - I(X; Z)$. Maximizing the secrecy capacity or implementing perfect secrecy is the goal of physical layer security. Channel noise plays an important role in physical layer security since the noise reduces channel information in different way for different channels. Proper noise level can increase the secrecy capacity. To understand the secrecy capacity, we need to understand what represents information.

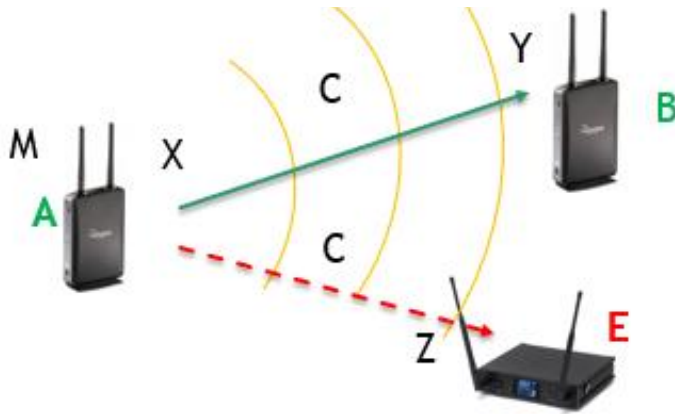


Fig. 1: Alice communicating with Bob, and Eavesdropper, Eve, is also listening.

B. Information Entropy

The basic information unit is true or false, which is corresponding the notion of bit, a unit used in computer technology taking two values, 0 or 1. The information size $H_0(A)$ of a set A as the number of bits that is necessary to encode all the elements in A . $H_0(A) = \log_2|A|$. Even though information size looks enough to represent the information, it does need to look more closely on information representation.

Compare two cases for information. They both contain N bits, each bit can be 0 or 1. In one case each bit takes equal chance to be 0 or 1. In the other case, each bit has more chance to be 1 than 0. Then in which case do the ten bits contain more information? This question has to be answered by information entropy. The information entropy is defined as the following:

$$H(A) = - \sum_{i=1}^n p_i \log_2 p_i \quad (1)$$

where p_i is the probability of the i^{th} state.

Based on the equation (1), the information entropy of the first case is greater than that of the second case. To understand this result, we can push the second case to an extreme, 100% chance to be 1, never be 0. It is easy to see this set does not contain any information. Correspondingly, the information entropy of the set becomes zero. Thus, information entropy is a good measurement for information.

Since the secrecy capacity is determined by information difference between the main channel and wiretap channel, maximize the difference is the target for physical layer security. The next two sub-sections describe two different approaches for this purpose.

III. SPATIAL DIFFERENTIATION

Adding noise to the original signal can maximize the secrecy capacity [4] as illustrated in Figure 2. However, the mechanism needs to have the guarantee that the main channel is better than wiretap channels. Spatial differentiation can be used to enhance the main channel and undermine the wire-tape channels [1,6,7].

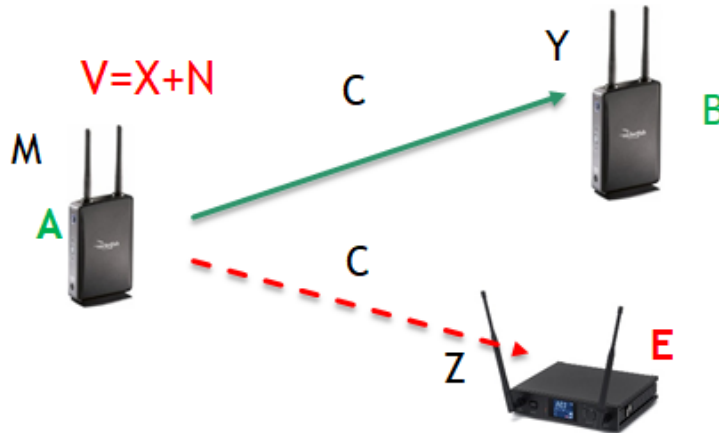


Fig. 2: Alice sends information to Bob with added noise to the information. Both B and E will receive reduced information, while the difference (secrecy capacity)

A. Beam Finding

When Alice communicates with Bob, it is possible for Alice to retrieve direction information of the signal sending from Bob using phased array antenna. Figure 3 depicts multiple wireless signals impinging on a phased array antenna each with their own electrical phase shift.

Once the phase differences retrieved from each path of antenna, Alice can generate certain phase different signal for transmitting, which will send signal to the direction of Bob.

In the hands-on laboratory setup, a startup MATLAB code is given for the bilateral communication of the main channel.

Step 1: User selects a position for Bob, then the code generates encoded signal based on predefined data string.

Step 2: With a certain noise level, the signal is received by each antenna of the phase antenna array. Based on the protocol of the known data, students extracted the phase shift information and deduced the angle of the incident wireless signal.

Step 3: With the information extracted in Step 2, students encoded the data sending to Bob with proper phase shift corresponding to the direction and sent the actual data to Bob through the phased array antenna.

Step 4: Bob received the data through regular antenna along with added noise. In this scheme, Bob uses a regular antenna to receive the signal. The signal then is decoded to retrieve the data and compared with the original data to calculate bit error rate (BER).

Step 5: Students then simulate the signal received by Eavesdropper at different directions. By comparing the bit error rate with Bob, the students can understand the secrecy capacity enhanced by beam finding techniques.

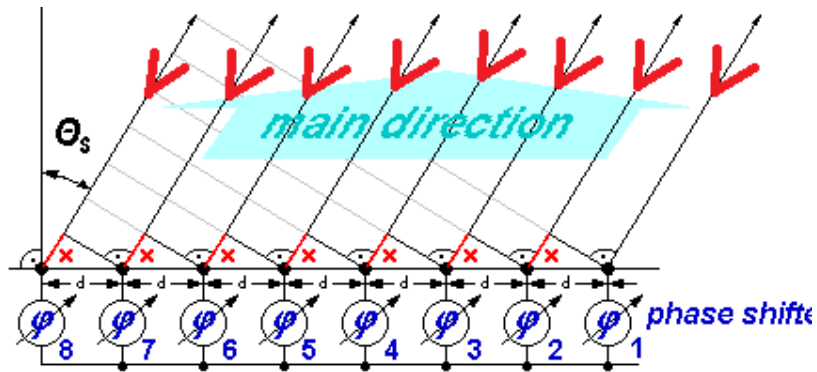


Fig. 3: Phase difference of incident signal on phased array antenna.

B. Cooperative Protection

While beam finding directs a signal to a certain direction, more sophisticated schemes can further enhance channel secrecy through cooperative protection. Cooperative protection covers a wide range of security methods. A multiple relay system shown in Figure 4 is elaborated to demonstrate strong protection against Eavesdroppers.

In the hands-on lab, a startup MATLAB code is given to emulate a relay system. Each relay has its own location, controllable phase delay and gain.

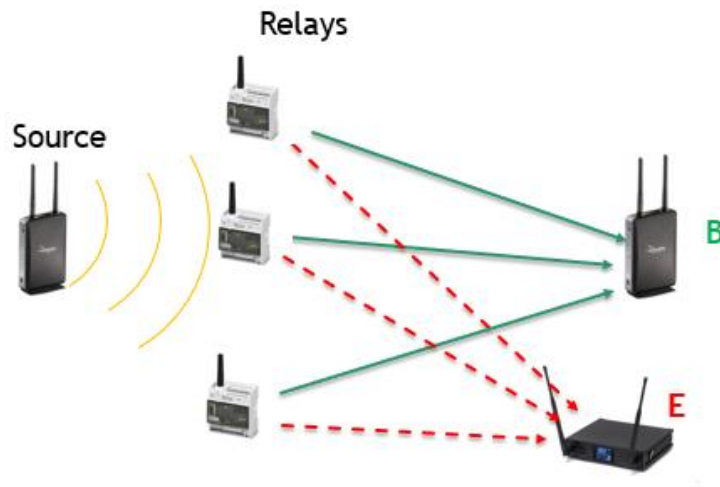


Fig. 4: Multiple relay system for cooperative protection against Eavesdropper.

Step 1: Setup locations for source relay and the receiver Bob. The MATLAB code generates channel properties for each relay.

Step 2: Cooperation between source and receiver could reach the optimal relay vector for the position of Bob through iteration. To save time, a given set of vectors based on relay channel properties is used for signal transmission. Noise is added to all signal path.

Step 4: Students decode the data received by Bob and compare it with the original data to compute the bit error rate.

Step 5: Students then simulate the signal received by Eavesdropper at different locations, including same directions from the source. By comparing the bit error rate with Bob, the students find the secrecy capacity enhanced by this scheme. The use of relay increases the spatial resolution for signal propagation.

IV. TEACHING METHOD

Two course modules were developed to teach students the topics on physical layer security in wireless communication. With both modules trying to enhance security, one module focuses on utilizing direction differentiation to increase secrecy capacity and the other module focuses on cooperative protection through feedback in a multiple-antenna system. The course module has the following learning objectives:

- A) Students will be able to describe what the physical layer security is.
- B) Students will be able to explain what the Eavesdropper is in wireless communication.

- C) Students will be able to expound what is considered as perfect secrecy.
- D) Students will be able to clarify secrecy capacity.
- E) Students will be able to quantify and qualify how noise in communication channel can be a resource for secrecy.
- F) Students will be able to quantify information entropy.
- G) Students will be able to explain how information is represented.
- H) Students will be able to simulate communication channel with phased array antenna using MATLAB.
- I) Students will be able to simulate cooperative protection using MATLAB.

Each of the two modules has two components: a) an instruction class with power point presentation, b) a hands-on lab exercise with lab manual and a MATLAB startup code. In the instruction class, the teacher utilized a PowerPoint presentation to explain the fundamental concepts of physical layer security in wireless communication system, related to the objectives described above. The class also prepares students for the hands-on lab exercise. The basic structure of the startup MATLAB code has been explained.

In the lab session of first module, students are asked to first determine the direction of the incident signal on a phased array antenna, then determine the phase delay in the transmit path of each antenna in the array, then send a series of data with certain noise to find the data bit error rate (BER). Finally, students are asked to demonstrate the BER of the Eavesdropper, which assume to have different direction from the intended communication partner.

On the second module, students were given a multiple relay system for wireless communication. Based on the feedback of the partner, the transmitter could get the optimized parameter for relays to create lowest BER near the partner. Students were asked to simulate the procedure and demodulate the signal to determine the BER for different locations. Students are asked to compare the difference of BER to different location and deduct the secrecy capacity.

V. TEACHING EXPERIENCE

Two course modules were taught in an undergraduate senior level course, Introduction to Wireless Communication, at North Carolina A&T State University in fall 2017. The Wireless Engineering Course teaches the fundamentals of designing and optimizing a wireless network through real-world examples in cellular, Wi-Fi, IOT design as well as interference mitigation techniques.

Ten (10) students were used for the learning study. Each course module consists of one 75 minute lecture and two lab sessions with detailed lab menus. The two modules were administered back to back. A pre-survey and a post-survey were conducted anonymously before and after the two modules. The survey results are presented in this session.

Ten students participated both pre and post surveys. Figure 5 shows the quantile plot comparison of students' self-rankings before and after the two modules for each of the nine objectives. In Figure 5 below, the X mark shows the average and the box shows the range of the middle half (from 25% to 75%). For all nine objectives, the students show good confidence of improvement after learning the modules.

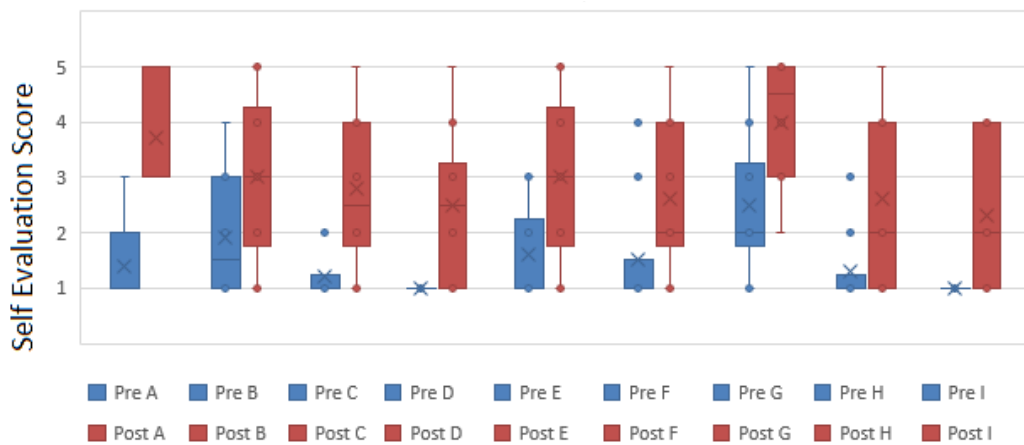


Fig. 5: Self ranking scores before and after learning modules on each learning objectives

The students learning the course modules have background in electrical engineering with little exposure to cyber space and cyber security issues in wireless channels. After finishing both modules, 50% of students agree and 10% of students strongly agree that learning objectives of these modules were met. 60% of students agree and 10% of student strongly agree the course module are useful in understanding cyber security concepts. 50% of students agree that the difficult level is appropriate and 40% of students enjoyed learning the modules. 50% of students agree that the lab time was worthwhile in understanding related concepts. However, these course modules alone are not enough to motivate students to pursue a career in cyber security due to the mismatch of the background

VI. CONCLUSION

This paper describes two course modules designed to expose students to the fundamental concepts on physical layer security of wireless communication, general vulnerabilities of wireless signal propagation, secrecy capacity and its enhancement

through different methods. Both modules consist of PowerPoint presentation, lab manual and hands-on lab MATLAB simulations. Students were taught ways of increasing the secrecy capacity through noise and signal gain through antenna beam finding.

Both course modules were taught in fall 2017. Our teaching experience and student observation demonstrated these course modules achieved their learning objectives especially the value of laboratory time to enhance learning of wireless communications risks such as cyber-attacks.

As a future work, a better introduction on MATLAB coding for students before the course modules will be prepared based on students' feedback, so students will be more interested in the learning the modules than struggling with coding issues. The Spring 2018 course will include a refined introduction to MATLAB coding for wireless communication channel simulation. The authors intention is also to pursue additional experiments in wireless internet security as part of a certificate program.

ACKNOWLEDGMENT

The authors would like to thank Dr. Xiaohong Yuan of N.C. A&T State University for her support of our research.

REFERENCES

- [1] Song, L., Zhang, Y., Zhou, X. (2014) "Physical Layer Security in Wireless Communication", CRC Press, ISBN: 978-1-4665-6700-9,
- [2] U. Maurer. (1993) "Secret key agreement by public discussion from common information", IEEE Trans. Inf. Theory, v.39, no.3 pp733-742
- [3] Cumanan, K., Xing, H., Xu, P. (2016) "Physical Layer Security Jamming: Theoretical Limits and Practical Designs in Wireless Networks". IEEE Access, Vol. 5, pp. 3603-3611.
- [4] C.E. Shannon (1948) "Communication theory of secrecy systems", Bell System Technical Journal, v.28, pp656-715.
- [5] Goel, S., Negi, R. (2008) "Guaranteeing secrecy using artificial noise", IEEE Trans. Wireless Communication, v.7, I.6, pp2180-2189
- [6] Gastpar, M., Gupta, P., Kramer, G. (2005) "Cooperative Strategies and Capacity Theorems for Relay Networks", IEEE Trans. Info. Theory, v.51, no.9, pp3037-3062
- [7] Mitran, P., Ochiai, H., Poor, H.V., Tarokh, V. (2005) "Collaborative beamforming for distributed wireless adhoc sensor networks", IEEE Trans. Signal Processing, v.53, I.11, pp4110-4124