INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 3 (2017) PAGES 2509 – 2516
RECEIVED : 25.05.2017 PUBLISHED : 19.06.2017
June 19, 2017

AN EFFICIENT APPROACH OF FUZZY GAME FRAMEWORK USING IN PHYSICAL LAYER SECURITY

[1]L.Gomathi M.E., [2]Mr.S.Sathish Kumar M.E., (Ph.D),

[1]Student, Embedded System Technology, Jayalakshmi Institute of Technology, Thoppur,

[2]Head of the Department, Department of Electronics and Communication Engineering, Jayalakshmi Institute of Technology, Thoppur.

ABSTRACT

Physical layer (PHY) security has turn into a promising area of examine recently. Wireless networks use unguided medium as communication channels, so gathering wireless data transmission is easier whilst compared to traditional cable systems. With the rise of new security challenges, many different solutions have been offered and are being developed. However, maintaining security in wireless networks still remains a challenge. Secure transmission techniques in these networks are discussed throughout this chapter. PHY security measures; the secrecy rate, the secrecy capacity and the outage secrecy rate are introduced. Security needs of wireless networks are discussed and the related common attack types are described. Main countermeasures that are proposed to prevent these attacks are also presented with both practical and theoretical perspectives.

1. INTRODUCTION

In order to highlight the effect of mobility in current security systems, the network model of the Open Systems Interconnect (OSI) reference model can be considered. This model, proposing a composition of seven layers; physical, data link, network, transport, presentation, session and application layers, distributes layers that network's are assumed to function independently from other layers. Using the OSI reference model can provide a formal definition and practical terms that affects information security on a layer-by-layer basis. Security can be seen as an aggregation of protection mechanisms of different layers.

A conceptual visualization of layered security solutions is shown in Figure 1. One should pass through the security layers in order to acquire private data. In such cases, physical layer (PHY) security becomes inevitably important, as it forms the first step of the security system.

PHY security has become popular with the arising of wireless technologies. Wireless medium is potentially unsafe as the communications signals are broadcasted into air and anyone in the antenna range can access the transmitted signals. In traditional wired technologies, the possibility of the transmit signals are gathered by an untrusted third party may not be a main trouble, as physical security is deployed by hiding cables in walls and cable endpoints locked up in server rooms or cabinets. If one use a special device to "line in" to sthetobe done link,. Hence, even a though physical it is not at t impossible, there is a certain difficulty for gathering the signals from a cable unless you have the endpoint.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 3 (2017) PAGES 2509 – 2516
RECEIVED : 25.05.2017 PUBLISHED : 19.06.2017
June 19, 2017

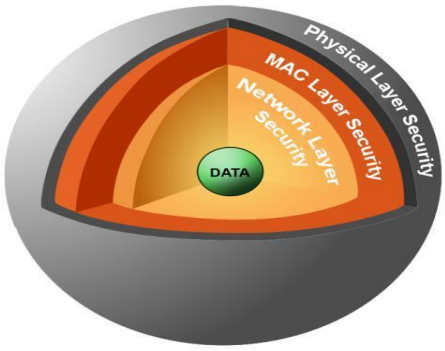

Figure 1. Layers of data

In this chapter, signaling based methods will be the main focus of the countermeasures. Beamforming and artificial noise techniques are proven to be effective countermeasures for privacy attacks and are therefore very important. *Beam forming* is a multi-antenna technique that enables the transmitter to focus signals spatially. *Artificial noise* (AN) is a recent concept that is utilized in PHY security methods, consisting of transmitting noise signals generated by the transmitter to non-legitimate users to degrade their signal reception quality. The AN studies in the literature usually follow isotropic. AN and smart AN approaches. Isotropic AN approach is based on broadcasting the generated noise without spatial selectivity (except for the legitimate user's),where as the smart direction.

2. RELATED WORK

Security is an important issue in wireless networks due to the open nature of wireless medium. Several studies have been conducted to improve security systems for wireless networks. As a consequence, there exist many solutions offered in different layers. In this section, a background on PHY security will be provided along with the related work. Eavesdropping attacks are unauthorized compromise of the data traffic between the between legitimate nodes.

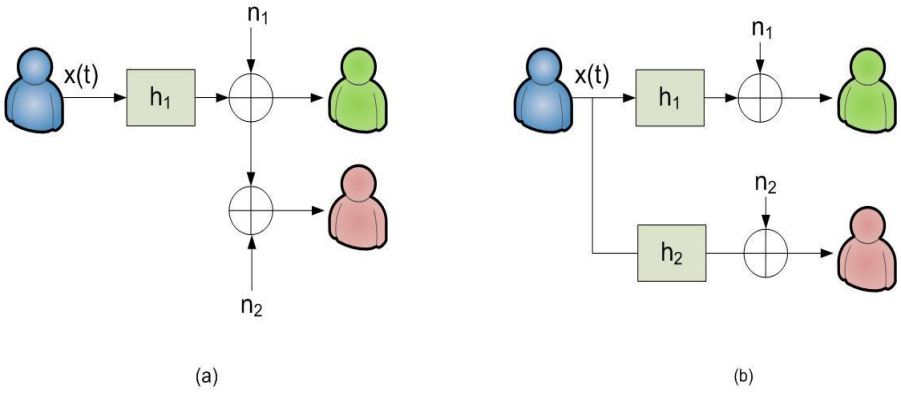

Figure 2. Channel model of a system with eavesdroppers, (a) Wiretap channel model of Wyner, (b) independent channel model.

Traffic analysis attacks are an example of eavesdropping-based attack type, where the content of the data is not compromised but the transmitter and receiver nodes are detected. In the pioneering work, the wiretap channel is introduced as seen in Fig 2(a) and it is showed that when an eavesdropper's channel channel, perfect secrecy, as defined can be achieved.The main reason was the requirement of the legitimate transmitter and receiver to have some advantage over the attacker in terms of channel quality, which cannot be guaranteed in a practical system. Moreover, almost at the same time, Diffie and Hellman published the basic principles of public-key cryptography, which was adopted by nearly all security systems. Physical-layer techniques were introduced to achieve secure communication, even if the channel is worse than the eavesdropper's channel artificial noise to confuse the eavesdropper. With two base stations connected by a high-capacity backbone, one base station can simultaneously transmit an interfering signal to secure the uplink communication for the other base station. In the scenario where the transmitter has a helping interferer or a relay node, the secrecy level can also be increased by having the interferer to send random noise signals independently at an appropriate rate. This scheme is referred to as cooperative jamming. When multiple cooperative nodes are available to help the transmitter, the optimal weights of the signal transmitted from cooperative nodes, which maximize an achievable secrecy rate, were derived for decode-and-forward protocols in and amplify-and-forward protocols in.

The second direction of using PHY attributes in encryption systems, which is referred to as PHY based key generation. This idea is based on channel reciprocity, which is the term for equality of transmitter to receiver and receiver to transmitter channel responses, in other words, uplink and downlink channels are the same. This specialty allows two communicating nodes to share a unique random data, as channel state information between two nodes cannot be gathered by any other nodes if it is not broadcasted. However, the slow changing environments may have limited source for key generation. Inevitably, generated key rate depends on the frequency of the changes in the channel.

3. EXISTING SYSTEM

To provide a security in physical layer for three-tier wireless sensor networks, a puzzle game framework is developed. The solution concept of Nash equilibrium is used in a prescriptive way, where the defender takes his part in the solution as an optimum defense against rational attackers. This study culminates in a strategy for handling distributed attacks from an unknown number of sources. In wireless sensor networks, the sinks collect the information from the remote sensor node with the help of accesses point. In practice, the small-size, low-cost and low-power sensors are randomly deployed to sense the data, which is sent back to the sinks by multi-hop transmissions. The proposed system focus on the secure transmission in two scenarios: i) the active sensors transmit their sensing data to the access points, and ii) the active access points forward the data to the sinks. Three-tier WSN where the geographically remote sensors transmit the sensed data to the sinks with the help of half-duplex decode-and-forward (DF) access points with no direct links between sensors and sinks.

Disadvantage

- Many applications do not require/need the data integrity, which is provided by physical layer model.

- In order to fast set up physical requires agreement between three-parties: users & service provider.

- Complex.

- This model is not adapted at all to telecommunication applications on computer.

4. PROPOSED SYSTEM

In this section we will first introduce the general signal and channel model of a wireless system in order to define performance metrics. The most basic wireless networks with eavesdropping can be simplified to have one transmitter node A, one legitimate receiver node B and an eavesdropper node E. Assume that all the nodes are equipped with single transmitting or receiving antenna for simplicity. Data bits are coded and modulated before transmission regarding to the selected modulation and coding scheme. Let s(k) be the data signal that A wants to send to B at time k and let x(k) represent the signal to be transmitted. For now, we assume A transmits only the data signal, without weighting or noise addition, so x(k) = s(k) is transmitted signal from A, as seen in Fig. 2(b). The received signals of A and E are given as rB(k) and rE(k) and they are defined as,

$$rB(k) = hAB(k)\, x(k) + nB(k) \quad (1)$$
$$rE(k) = hAE(k)\, x(k) + nE(k) \quad (2)$$

where nB(k) and nE(k) are the additive zero-mean Gaussian noise (AWGN) components and hAB(k) and hAE(k) are the channel coefficients of the channels between nodes A and B and nodes A and E, respectively. A very useful measure of the channel quality is the signal to interference and noise ratio (SINR). This ratio gives how strong the received data signal power compared to non-data signal power caused by channel noise and interference.

$$SINRB(k) = \frac{Psignal}{|hAB(k)|^2 / B^2\, \sigma} \quad (3)$$
$$SINRE(k) = \frac{Psignal}{|hAE(k)|^2 / E^2\, \sigma} \quad (4)$$

Where the average transmit signal power is defined as Psignal. Note that SINR is equal to signal to noise ratio (SNR) when the interference power is zero, however SINR definition is important for the security system models with interference, as given in the following sections.

Advantage

- It provides wide variety of choice.
- It does not depend or rely on a specific computer system.
- It interprets the product functionality at each-stage.
- It encrypts the data for security purpose.

- It is easy to add multiple-network models.
- PHY layer security is a reasonable next step towards thwarting wireless network intrusion.
- One approach is to leverage angle-of-arrival information to construct signatures that will uniquely identify associated clients.
- This is the principle behind Secure Array, which uses multiple antennas to construct such signatures.

5. SYSTEM MODULE

The main requirements of a wireless security network are the authentication, secrecy and data integrity along with robustness to physical attacks like jamming or natural effects like channel noise or interference. We give the detailed discussions of these requirements below.

Secrecy

Secrecy (data secrecy), in a communications system refers to the state that the information is obtainable solely by the legitimate receiver. This is a challenge that should be properly addressed especially for wireless communication systems. In wired communication networks, data secrecy is accepted to be guaranteed between two nodes, which means a cable is assumed to be secure and security is considered to be maintained on the network nodes on the way from sender to receiver. In another words, it is often accepted that if sender and receiver is directly connected by cable, then the data cannot be obtained by anyone else so secrecy is maintained on PHY. However, as mentioned, wireless medium has an open nature that makes it very hard to maintain secrecy. Any receiver in the coverage of sender antenna can capture the communication signals without being noticed. In wireless networks, non-legitimate receivers can execute such an attack, eliminating secrecy of data. In such case, maintaining physical security becomes very important.

Usually traffic analysis attack is performed where the encryption key cannot be gathered. Major countermeasures to eavesdropping and traffic analysis attacks are encryption, beamforming and artificial noise. These security techniques will be detailed review will be given in the following section.

Authentication

User authentication is a means of identifying the user and verifying that the user is allowed to access some restricted service. Proper authentication mechanisms can be considered as the base of the security expedients, because of their importance. If a non-legitimate user is able to get authenticated by the system, every restricted service and information can be easily accessed. Moreover, the risk of the information and/or the system to be altered is highly considerable, for example a wireless remote system can be severely damaged causing destructive incidents, depending on the application.

Data Integrity Awareness

In its broadest meaning, data integrity refers to the trustworthiness of information over its entire life

cycle. It is the representational faithfulness of information to the true state of the object that the information represents. Representational faithfulness has four essential attributes: completeness, currency/timeliness, accuracy/correctness and validity/authorization. Integrity is a critical requirement in wireless networks, because of the potential vulnerabilities originated from PHY. Major data integrity attacks are message modification and jamming attacks. Attacker can send forged control, management or data frames over wireless to mislead the recipient or facilitate another type of attack. Message modification is the general class of attack types that based on additions or deletions to actual data by malicious users. Jamming attacks are based on transmitting signals to depress or degrading the communication service performance.

Robustness

High degree of robustness against jamming and/or natural performance degrading effects such as noise or interference resulting from other wireless transmitters is one of the major design goals of wireless networks. The major attack type that a system should be robust against is denial of service attack type. A attack aims exhausting the availablecksmay focus on any resource of a system in order to degrade or cancel a service functionality.

Physical Layer Security Solutions

In this section, we will present solutions to deal with aforementioned system secrecy vulnerabilities and attack types. We categorize the solutions to achieve maximum secrecy as code based methods, signaling based methods and PHY-based encryption methods. Secrecy is the focus of PHY security in wireless networks, as it is the major vulnerability in wireless transmission. Code based and signaling based approaches exist for achieving maximum secrecy level and enhance robustness, which will be discussed in this section.

Signaling based methods

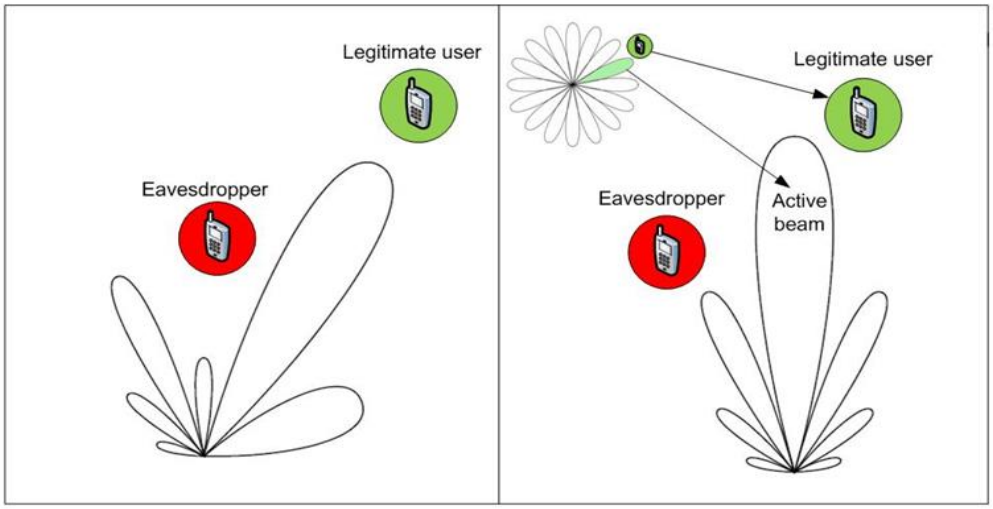

Figure 3. Beamforming, (a) adaptive beamforming , (b) switched beam system

Data protection can also be facilitated using signaling design approaches. The usual schemes in these approaches involve beam forming and the injection of artificial noise. From Table I, it can be seen that beam forming methods can be used to improve secrecy and can be used as a countermeasure to secrecy or authentication targeted attacks. These methods are detailed below. Solely beam forming type of optimization scenario is a basic beam forming weight adjustment case, in which signal beam is targeted to legitimate user and not sent to anywhere else. When this problem is formed to minimize total transmit power, it can be expressed as a convex optimization problem and can be solved easily with convex optimization methods.

CONCLUSION AND FUTURE RESEARCH DIRECTIONS

PHY security is a rather novel concept, implying that there are a lot of opportunities for researchers. Future research directions include new and more effective smart beam forming and techniques. Seeking of PHY countermeasures against specific attack types of wireless network is also a solid need of research. Practical implementation is also an open area of research for transferring PHY security techniques from theory into real world systems. In this chapter, the basic definitions and state of the art on the area of PHY security is introduced. Most common PHY attacks, such as eavesdropping, jamming, man in the middle, ID theft, are explained along with the security needs of wireless systems. The countermeasure techniques offered in PHY are categorized and detailed. As a result, the importance of PHY security systems are obvious, while more practical techniques should be pioneered for the networks.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankara subramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114, Aug 2002.

[2] A. D. Wyner, “The wire-tap channel,” Bell Syst. Technol. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] H. V. Poor, “Information and inference in the wireless physical layer,,” IEEE Wireless Commun., pp. 40–47, Feb. 2012.

[4] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, “Physical layer security in downlink multi-antenna cellular networks,” IEEE Trans. Commun., vol. 62, no. 6, pp. 2006–2021, Jun. 2014.

[5] H. Wang, X. Zhou, and M. C. Reed, “Physical layer security in cellular networks: A stochastic geometry approach,” IEEE Trans. Wireless Commun., vol. 12, no. 6, pp. 2776–2787, Jun. 2013.

[6] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, “Secure communication over MISO cognitive radio channels,” IEEE Trans. Wireless Commun., vol. 9, no. 4, pp. 1494–1502, 2010.

[7] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” IEEE Trans. Signal Process., vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[8] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical layer security in cooperative wireless networks," IEEE J. Sel. Areas Commun., vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[9] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in IEEE Global Tele commun. Conf. (GLOBECOM), 2008, pp. 1–5.

[10] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," IEEE Wireless Commun. Lett., vol. 3, no. 3, pp. 289–292, Jun. 2014.