International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

Wireless Physical Layer Security in Cognitive Radio

Manjunath S[1], Bhargava B R[2], Pradeep V S[3]

[1]*Assistant Professor, Dept. Of CSE, S J C Institute of Technology, Chickballapur, Karnataka, India*
[2]*Student, Dept. Of CSE, S J C Institute of Technology, Chickballapur, Karnataka, India*
[3]*Student, Dept. Of CSE, S J C Institute of Technology, Chickballapur, Karnataka, India*

Abstract - *One of the important trends which is supposed to have more attention in the system of cognitive radio is wireless security techniques. We proposed the security constraints on physical layer for cognitive radio networks. First, an overview on several existing security attacks to the physical layer in CRNs. Afterwards we discuss the related countermeasures on how to defend against these attacks. A new category of security issues and challenges have been introduced in the cognitive radio systems, and providing security techniques to realize good and reasonable protection must be one of the main researchers interest. The advance method will enable the many safety to make sure a strong and reliable communication within the existence of adversaries by providing adaptive certainty solutions within the communication systems by utilizing the physical layer certainty from different perspective.*

Key Words: Security Attacks In Wireless Network, Security Attacks In CRNs, Physical Layer Security, Wiretap Channel, Physical Layer Security Techniques

1. INTRODUCTION

Wireless networks are widely used in civilian and military applications. Transmission of important/private information has to be kept secret from non legitimate receivers. Security of information transfer via wireless networks remains a challenging issue because of the broadcast nature of the wireless channel. Adversaries may attempt to gain unauthorized access to and modify the information, or even disrupt the information flows. Thus, the issue of privacy and security is considered as a new QoS constraint in wireless network design [1,2]. Current security methods rely on cryptographic techniques like data encryption protocols, which are viewed as independent features addressed above the physical layer. Encryption is a technique for encoding the data, e.g., data encryption standard using private key shared by two users, such that it is not decode able by an unauthorized user [3]. Cryptographic methods assume high computational complexity that prevents the adversary to decode the message, and consider that an error-free physical layer link has been established. In addition, the transmission of an encrypted message (cipher text) is not perfectly secure, because the cipher text can still be decrypted by a malicious user with exhaustive key search [4]. To this end, there has been a considerable attention on studying the fundamental ability of the physical layer to secure wireless communications [1,2,5]. This emerging security technique is known as physical layer security, and covers varies secure methods using physical layer properties as already discussed

1.1 Security Attacks in Wireless Networks

The security attacks in wireless networks can be classified into two categories: passive and active [2,3]. In a passive attack, the attacker tries to listen, learn, and extract information from the ongoing communication without performing any interactions with legitimate users. The passive attackers monitor network traffic and wireless communication channels, and are in nature in the form of eavesdropping intrusion and traffic analysis. Eavesdropping attack refers to the scenario where an unintended receiver, known as an eavesdropper (EAV), intercepts a message. Traffic analysis is the ability of the unauthorized user to determine the location and identity of communicating users by intercepting and examining the transmitted messages, i.e., can observe the frequency and length of message being exchanged. On the other hand, in an active attack, an attacker attempts to modify the data information and performs active interactions with the legitimate system by sending some false data information. Examples of active attackers include denial of service (DoS) attacks, masquerade attacks, replay attacks, and information disclosure and message modification attacks.

A DoS attacker inhibits the usage of communication facilities. For example, an entity may suppress or suspend all messages directed to a particular destination. Also, a DoS attacker may disrupt the entire network, either by disabling the network or by overloading it with messages so as to degrade performance of the legitimate communication. Jamming is an example of a DoS attack at

the physical layer. An adversary can used RF jamming signals to disrupt the communications. In a masquerade attack, an intruder pretends to be a legitimate user to gain access to network applications or services illegally. A masquerade attacker tries to convince the sender that he/she is the authorized recipient of the message, and/or convince the receiver that he/she is the legitimate transmitter. The replay attack is a form of network attack in which a valid data transmission is maliciously repeated or delayed, i.e., an attacker injects malicious packets into the network to disrupt it. The message modification attack occurs when some portion of a legitimate message is altered or reordered to produce an unauthorized effect. An attacker make different packets by inserting improves into them, erasing information from them, reordering or delaying them.

1.2 Security Attacks in CRNs

As a wireless network, a CRN is also subject to security issues. Because of CR characteristics, CRNs face additional security challenges compared to traditional wireless networks. In this respect, different security threats and detection techniques in CRNs have been discussed in [2,6,7,8], and references therein. Here, we only present major attacks on the physical layer of CRNs, which include the primary user emulation (PUE) attack, spectrum sensing data falsification (SSDF) attack, jamming attack, and eavesdropping attack.

In the PUE attack, malicious users may masquerade as PUs by transmitting signals in the licensed band (not used by the PUs), so as to enforce SUs to vacate this band or to prevent other cognitive users to access that band. The purpose of PUE attacks can be of two types: greedy and malicious [7]. The greedy nodes, i.e., selfish PUE attacks, transmit fake incumbent signals to force SUs to vacate a specific band (spectrum hole) in order to occupy it. While, for a malicious PUE attack, the malicious attacker prevent the transmission of the SUs without using the spectrum band.

Another attack to cognitive radio networks is the objective function attack (OFA).This attack mainly targets on learning engine of cognitive radios. In cognitive radios, a cognitive engine has the ability to tune a lot of parameters to maximize its objective function [7]. These objective function stake high transmission data rate, low power consumption, low delay and high security level as variables. Among those variables of the objective function, high transmission rate and low delay are related to the channel, while low power consumption and high security level are directly determined by the inputs of the users. So for objective function attack, whenever the user wants to raise the security level, the malicious nodes may use some ways to increase the delay of the user. Thus, the user may connect high delay with high security level and not want to use high security level at all. Thus, it will become more susceptible to security attacks. It is necessary to remark that the OFA performance is related to what optimization method is used in the cognitive radio network [8]. Some cognitive radios do optimization instantly after getting the input of the environment. On the other hand, other cognitive radios observe the environment just once, then search for an optimized result, and the decision will not be changed by the input of the environment. In this case, the type of cognitive radio is not affected by OFAs. However, cognitive radio devices generally have high sensing ability and do optimization frequently. Therefore, a cognitive radio network is vulnerable to OFA attacks. In order to combat objective function attack, an easy suggestion has been made in. It is to define threshold values whenever the radio parameters need to be updated. If the detected parameters do not meet the predefined thresholds, the secondary user will not collect that information. Moreover, a good intrusion detection system can be used to strengthen the countermeasure. However, using an intrusion detection system is a general countermeasure that may not perform well in defending against objective function attack.

Learning attack (LA) is that the adversary provides false sensory input for learning radio in cognitive radios. If a learning radio learns some wrong ideas about the transmission schemes, it will be used all the way until it can learn the correct ideas. Generally, learning attack is combined with other types of attacks. For example, an attacker can conduct a PUE attack or an OFA attack whenever a cognitive radio tries to use the best transmission scheme [8]. Thus, the learning radio might decide that the best transmission scheme will not be optimal and it will take sub-optimal transmission schemes as the optimal transmission schemes, which leads to lower performances. Several methods are proposed so as to combat learning attack. First, the learning results must always be reevaluated over time. For example, the activities of the primary users in a cognitive radio network should be constantly recomputed so that the previously learned statistical process of activities of the primary users that may be incorrect will be abandoned. Second, there should be a truly controlled environment during the

learning phases, which means no malicious signals are present during the learning phase. Another principle would be that if the learned action breaks some basic theoretic results, then this action should not be used. Fourth, cognitive radios can make use of group learning instead of individual learning. Several secondary users can form a gaggle to find out the environment and therefore the attacker can't conduct learning attack so easily

The SSDF attack is related to cooperative spectrum sensing. A malicious user can initiate or report a false local sensing result on a specific band to its neighbors or to the fusion centre. The purpose of an SSDF attack is to confuse the SUs or the fusion centre for decision about the presence/absence of PUs. This may lead the SUs to vacate the spectrum band or to cause harmful interference to the PUs. Also, the goal of these attackers is to monopolize a specific band by forcing all other nodes to not use it. In the jamming attack, an attacker degrades the SNR below the required threshold by transmitting noise over the received channel. Jamming attacks can be classified as a single-channel jamming attack or multi-channel jamming attack [7,9]. In a single-channel jamming attack, the malicious user continuously transmits high power signals on one channel. In a multi-channel jamming attack, the attacker can jam multiple channels simultaneously by interfering signals on all channels at the same time or by switching from one channel to another according to the PUs activities.

In the eavesdropping attack, a malicious node listens to the transmission of the legitimate users and gets access to the content of exchanged data. This thesis focuses on the eavesdropping attacks since they are very difficult to detect, because they do not involve any alteration of the data.

2. Physical Layer Security

Fig-1 illustrates the general concept of physical layer security in a wireless network where the communication between legitimate transmitter (S) and legitimate receiver (D) is being eavesdropped by an unauthorized user known as an EAV. The communication channel between S and D is called the main channel, whereas the communication channel between S and EAV is referred to as the eavesdropper channel.

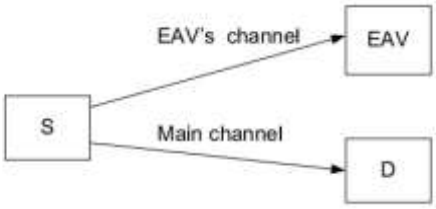

Fig-1: Example of an eavesdropping scenario in a wireless network.

In general, the signals received by D and EAV are different since nodes D and EAV may be located at different positions. The two channels through which signals pass have different fading and noise effects. With careful planning and execution, the integration of cryptographic and physical layer security techniques can provide a security solution that efficiently safeguards sensitive and confidential data for the wireless communication [5,10].

2.1 Wiretap Channel

The notion of wiretap channel was introduced by Wyner [11] under the assumption that the EAV channel or wiretap channel is a degraded version of the main channel. Wyner demonstrated that a positive information rate can be achieved with perfect secrecy if the EAV channel is noisier than the main channel. The idea [11] was to exploit the noise of the communication channel along with proper physical layer coding to ensure secure communication. A basic wiretap channel model is depicted in Fig-2.

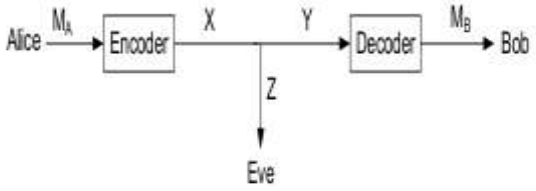

Fig-2: Wiretap channel model

Fig-2 where Alice sends a confidential message to Bob through a discrete memory less channel, while Eve eaves drops this message through another degraded version of discrete memory less channel. Alice encodes a message MA into a codeword X of length m, which is transmitted. The legitimate user receives the signal Y over the main channel, decodes it, and the message at Bob is MB. The signal received by Eve through the wiretap channel is denoted by Z.

The goal is to design a coding scheme, i.e., encoding algorithm and decoding algorithm that makes it possible to communicate both reliably and securely. In this structure, the performance of the coding scheme can be measured in terms of average error probability and equivocation rate [12,13]. The average error probability indicates the level of reliable communication between Alice and Bob. The equivocation rate at Eve measures the secrecy level of confidential message.

The works in [11] showed that a positive secrecy capacity can be achieved when the EAV channel is of lower quality than that of the main channel. However, various extensions of the wiretap channel to fading channels indicate that information theoretic security is achievable even when the EAV has a better average SNR than the legitimate receiver [12,13]. To further improve the physical layer security against eavesdropping attacks, distinct techniques such as thermal noise [8,9], interference [19,20], multiple antennas [1,4,9], cooperative relays [17,18], and selection diversity [16] have been used.

2.2 Physical Layer Security Techniques

In the following, we briefly discuss some examples of physical layer security approaches used to establish secure channel communication.

Coding and Signal Processing Techniques:

Channel codes are typically designed to make reliable secure communication by adding redundancy into transmitted data for allowing the receiver for error detection and correction, and adding randomness for keeping the EAV ignorant [7,12]. Some coding methods such as polar codes and low-density parity check (LDPC) codes can be used. However, coding techniques assume perfect random coding arguments. In addition, it is very difficult to design near-to-optimal codes for the wireless wiretap channel.

Secret Key Generation

The randomness of the wireless channel can be exploited for generating encryption keys [9,12]. Because of the rapid fluctuations of fading coefficients, the duration of every key can be short enough, so that the EAV can hardly detect it before a new one is generated and used. The key generation approach is based on the source and channel coding techniques to generate common secret keys between legitimate nodes.

Artificial Noise and Beam forming Techniques

A transmitter can artificially generate noisy versions of the signal to confuse the adversary user [14,15]. Artificial noise is generated by the usage of multiple antennas or the coordination of helping nodes. Moreover, the usage of transmit beam forming can improve wireless secure capacity and avoid physical jamming attempts [14]. However, artificial noise and beam forming approaches consume additional power resources for generating artificial noise and increase the computational complexity in performing beam former design.

Multiuser Diversity

In order to effectively defend against the eavesdropping attack, multiuser scheduling should be employed to minimize the EAV channel capacity at the same time maximizing the main channel capacity [4,16]. This requires the knowledge of CSI of both the main and wiretap links. If only main channel CSI is available at the transmitter, conventional MUD is applied where the wiretap channel information is not taken into account.

Cooperative Diversity

User cooperation has also great potential to enhance wireless security against eavesdropping attacks [17,18]. For example, a cooperative jamming technique is used in [18] where trusted relay nodes transmit a weighted jamming signal (independent of the source message) to the EAV with the purpose of degrading the EAV channel.

3. CONCLUSION

In this article, we investigated the safety issues associated with the physical layer in cognitive radio networks. First, we summarized the security attacks on the physical layer for cognitive radio networks and surveyed the existing countermeasures for those attacks. Different to existing wireless networks where interference is undesired, interference can be beneficial to improve the secure transmission when used to degrade the performance of the EAV channel. For instance, a device-to-device (D2D) communication has been introduced in to improve the security in cellular network where D2D generates interference to the EAV to reduce the achievable data rate of the EAV link.

REFERENCES

1. R. F. Schaefer and H. Boche, "Physical layer service integration in wireless networks: Signal processing challenges," IEEE Signal Processing Mag., vol. 31, no. 3, pp. 147–156, May 2014.
2. Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," IEEE Wireless Commun., vol. 18, no. 2, pp. 66–74, Apr. 2011.
3. W. Stallings, Cryptography and Network Security: Principles and Practice, 5th ed. Prentice Hall PTR, 2006.
4. Y. Zou, J. Zhu, X. Wang, and V. C. Leung, "Improving physical layer security in wireless communications using diversity techniques," IEEE Network, vol. 29, no. 1, pp. 42–48, Feb. 2015.
5. N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," IEEE Commun. Mag., vol. 53, no. 4, pp. 20–27, Apr. 2015.
6. A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. M. Leung, "A survey of security challenges in cognitive radio networks: Solutions and future research directions," Proc. IEEE, vol. 100, no. 12, pp. 3172–3186, Dec. 2012.
7. A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "Survey on security threats and detection techniques in cognitive radio networks," IEEE Commun. Surveys & Tutorials, vol. 15, no. 1, pp. 428–445, First Quarter 2013.
8. R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," IEEE Commun. Surveys & Tutorials, vol. 17, no. 2, pp. 1023–1043, Second Quarter 2015.
9. A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," IEEE Commun. Surveys & Tutorials, vol. 16, no. 3, pp. 66–74, Third Quarter 2014.
10. A. Yenner and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," IEEE Proc., vol. 103, no. 10, pp. 1814–1825, Oct. 2015.
11. A. Wyner, "The wire-tap channel," Bell. System Technical Journal, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.
12. M. Bloch, J. O. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
13. P. K. Gopola, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 10, pp. 4687– 4698, Oct. 2008.
14. S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
15. X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," IEEE Trans. Veh. Technol., vol. 59, no. 8, pp. 3831–3842, May 2010.
16. A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, "On the resilience of wireless multiuser networks to passive and active eaversdroppers," IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 1850–1863, Sep. 2013.
17. L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," IEEE Trans. Signal Processing, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
18. 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.
19. J. Yue, C. Ma, H. Yu, and W. Zhou, "Secrecy-based access control for device-to-device communication underlaying cellular networks," IEEE Commun. Lett., vol. 17, no. 11, pp. 2068–2071, Nov. 2013.
20. G. Zheng, I. Krikidis, C. Masouris, S. Timotheou, D.-A. Toumpakaris, and Z. Ding, "Rethinking the role of interference in wireless networks," IEEE Commun. Mag., vol. 52, no. 11, pp. 152–158, Nov. 2014.