IJERMS

International Journal of Engineering Researches and Management Studies

AN TRANSMISSION TO ENHANCE COOPERATIVE SECURITY IN WIRELESS SENSOR NETWORK

K. Ravi Kumar[*1] & R. Divya[2]
[*1]Asst.Professor, Dept. of Computer Science, Tamil University, Thanjavur-613010
[2]Research Scholar, Dept. of Computer Science, Tamil University, Thanjavur-613010

ABSTRACT

Wireless networking plays an extremely important role in civil and military applications. How ever security of information transfer via wireless networks remains a challenging issue. It is critical to ensure that confidential data are accessible only to the intended users rather than intruders. When Jamming and eaves dropping are two primary attacks at the physical layer of a wireless network. This article offers a tutorial on several prevalent methods to enhance security at the physical layer in wireless networks. We classify these methods based on their characteristic features into five categories, each of which is discussed in terms of two metrics. First, we compare their secret channel capacities, and then we show their computational complexities in exhaustive key search. Finally, we illustrate their security requirements via some examples with respect to these two metrics.

Keywords: Wireless sensor network , Mobility, Signal detection

1. INTRODUCTION

Wireless networks have become an indispensable part of our daily life, widely used in civilian and military applications. Security is aritical issue in wireless applications when peoplerely heavilyon wireless networks for transmission of important/private information ,such as credit card transactions or banking related data communications. Therefore, the ability to share secret information reliably in the presence of adversaries is extremely important .Adversaries may attempt to launch various attacks to gain unauthorized access to and modify the information, or even disrupt the information flows. Most commonly used security methods rely on cryptographic techniques employed at the upper layers of a wireless network. With regard to a symmetric cryptographic technique (as Depicted, such as the Data Encryption Standard (DES), a common private key is normally shared by two users. If these two users do not have this private key, a secure channel is required for the key exchange. Instead of using an additional channel, the physical layer methods can be employed here to distribute secret keys, to supply location privacy and to supplement upper-layer security algorithms. The application of physical layer security schemes and smore difficult for attackers to decipher trans- mitted information.

2. RELATED WORKS

Mobile wireless communication has experienced an unprecedented growth in data traffic in recent years, spurred by the popularity of various intelligent devices, the demand for exuberant multimedia content, and the rapid increase in the number of base stations (BSs). In particular, global mobile data traffic in 2013 was nearly 18 times the size of the entire glob-al Internet in 2000, and monthly global mobile data traffic by 2018 will surpass 15 Exabyte's. While the mature third generation network and the currently deploying fourth generation (4G) network may accommodate the data traffic surge for the next few years, they will not be able to support a very large number of devices with a huge network traffic demand in 2020 and beyond [2]. Against this backdrop, a number of disruptive trends and technologies shaping the fifth generation (5G) network are emerging worldwide through research and Methodology.

The authors in introduced an extra node as the relay node to improve the secrecy of the wireless transmission. Several relay strategies, such as amplify-and-forward (AF), decode- and-forward (DF) and noise forwarding (NF), were proposed and the corresponding achievable rate-equivocation regions were derived. It is shown that all these protocols have the ability to offer the secrecy rate gain. In the authors studied

The problem of relay placement from a secure connection perspective. Security enhancement can also be achieved via friendly jamming, which can reduce the leakage rate to the eavesdropper. The jamming signals can be sending from the source, the relay or the destination. Since the jamming signal would also interfere with legitimate nodes.

There should be a trade off of power allocation between the information signal and jamming signal. Power allocation for the source and relay nodes in cooperative jamming relay networks was studied, e.g.,

In this section, we introduce schemes that could be used to achieve physical layer security against different attacks. We can classify the existing physical layer security methods into five major categories: theoretical secure capacity, channel, coding, power, and signal detection approaches. In recent years, the fundamental issues of secure channel capacity have drawn much attention in the information theory community. Most of these works focused on the study of so-called Secrecy capacity, that is, the maximum rate achievable between the legitimate transmitter- receiver pair subject to the constraints on information attainable by the unauthorized receiver. In Wyner's original work, he showed for that discrete memory less channels the perfect secrecy capacity is actually the difference of the capacities for the two users. A similar result has been generalized to Gaussian channels by Leunget al.

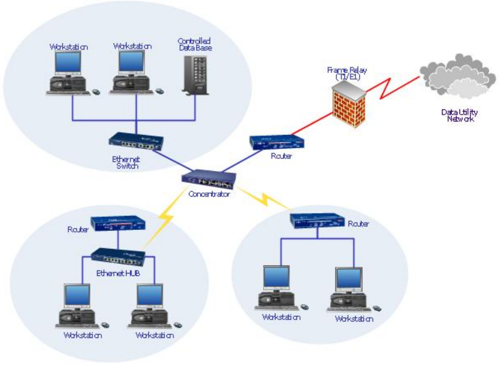

Fig of wireless networks in physical layer

The authors in extended their previous work by considering the presence of imperfect CSI. The important role of fading was characterized in terms of the average secure communication rates and outage probability. The authors in developed a secure communication protocol that adopts the following four-step procedure to ensure wireless information-theoretic security:

a. Common randomness via opportunistic transmission
b. Message reconciliation
c. Common key generation via privacy amplification
d. Message protection with a secret key

A set of security measures for assessing average secure key generation rates was established,
In a wireless network, secured services should satisfy certain requirements discussed below. The wireless communication medium is open to jamming (or interference) and eavesdropping Attacks from intruders. For transmission security (TRANSEC), a robustness function is widely used to encrypt data at the transmitter for different communication links, such as satellite links and mobile communication channels. TRANSEC usually provides a relatively weak capability of Combating attacks. The robustness functions may also include low probability of intercept (LPI),Low probability of detection (LPD), low probability of exploitation (LPE), and anti-jamming Protection.

3. PROPOSED METHOD

In this section, the security technology in PHY layer is analyzed and compared, and then some very innovative trends for future research are identified. As mentioned above, the secure techniques of PHY layer could effectively defend against the interference, jamming, and eavesdropping attack. In this section, we analyze, compare, and summarize the previous secure techniques of PHY layer in wireless networks, through the research of the factors affecting the technical characteristics, ability to defend against attacks, and complexity which is illustrated in Table 1, with (—) signifying no consideration or weakness.

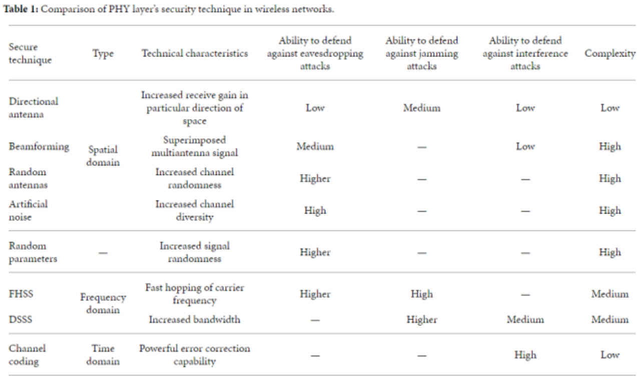

Table 1: Comparison of PHY layer's security technique in wireless networks.

Secure technique	Type	Technical characteristics	Ability to defend against eavesdropping attacks	Ability to defend against jamming attacks	Ability to defend against interference attacks	Complexity
Directional antenna	Spatial domain	Increased receive gain in particular direction of space	Low	Medium	Low	Low
Beamforming		Superimposed multiantenna signal	Medium	—	Low	High
Random antennas		Increased channel randomness	Higher	—	—	High
Artificial noise		Increased channel diversity	High	—	—	High
Random parameters	—	Increased signal randomness	Higher	—	—	High
FHSS	Frequency domain	Fast hopping of carrier frequency	Higher	High	—	Medium
DSSS		Increased bandwidth	—	Higher	Medium	Medium
Channel coding	Time domain	Powerful error correction capability	—	—	High	Low

From Table 1 secure techniques are divided into three categories: spatial domain-based, time domain-based, and frequency domain-based. Strictly speaking, random parametric technique does not act as defense against eavesdropping attacks from space but relies on randomization of weighting coefficients to achieve the eavesdropper's received signal randomization. However, because there are the same beam forming technology-based and many similarities of representation formula, we compare the random parameter with random antenna in Section 3.

Research field of physical security, especially in mobile devices, becomes increasingly widespread in recent years. Much effort has been (and is being) made worldwide for providing secrecy in the absence of complete or perfect channel knowledge of the parties. As shown in Table 1, we could claim that secure techniques defending against eavesdropping attacks have mainly three types:

i. Directional Transmission Technology (Beam forming and Directional Antenna).

It can only enhance the resilience of the eavesdropping attack to some extent but is not able to effectively eliminate the threat from eavesdropping attacks. However, with the development of antenna technology, defensive performance could gradually be improved.

ii. Random Parameters, Random Antennas, and FHSS.

Through randomization of weighting coefficients, channel parameters, and carrier frequency, an eavesdropper cannot effectively demodulate the correct information. These secure techniques have a high ability to resist eavesdropping.

iii. Artificial Noise.

It relies on adding artificial noise to increase channel diversity in the channel, make eavesdropping channel quality far worse than legitimate channel quality, impact eavesdropper's information demodulation.

4. SIMULATION AND PERFORMANCE ANALYSIS

We can use Wi-Fi technology contain personal computers, video-game consoles, smart phones, digital cameras, tablet computers, smart TVs, digital audio players with modern printers. Wi-Fi compatible devices be able to join to the Internet via a WLAN and a point. An access point (or hotspot) has a range of about 20 meters (66 feet) inside and a greater range outdoors. Hotspot coverage can be as small as a only room with walls that block radio waves, or as large as many square kilometres achieved by using multiple overlapping access points.

IEEE 802.11 wireless LANs use a media access control protocol called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). While the name is similar to Ethernet's Carrier Sense Multiple Access by Collision Detection (CSMA/CD), the operating concept is totally different. Wi-Fi systems are the half duplex joint media configurations, where all stations transmit and receive on the similar radio channel. The fundamental problem of a radio system is that a station cannot hear while it is sending, and hence it is not possible to detect a collision. Because of this, the developers of the 802.11 specifications came up with a collision avoidance mechanism called the Distributed Control Function (DCF).According to DCF, a Wi-Fi station will transmit only as the channel is clear. All transmissions are acknowledged, hence if a station do not receive an acknowledgement, it assumes a collision occurred and retries behind a random waiting interval. The incidence of collisions will increase because the traffic increases or in situations anywhere mobile stations cannot hear each other.

5. CONCLUSION

An article, issues in physical layer security for wireless networks have been discussed in a tutorial manner. Numerous existing physical layer security approaches contain introduced and compared in terms of their abilities to improve security in wireless transmissions. We have also exposed the effectiveness of several physical layer security schemes via illustrations. Two important metrics, secret channel capacity and computational complexity, contain used to compare the performance of different approaches. It should also be noted that due to hardware complexity, the low-cost performance of generally physical layer security schemes is still beyond the capability of current microelectronics technologies.

REFERENCES

1. *A. Khisti and G. W. Wornell, "safe Transmission by Multiple Antennas: The MIMOME Wiretap Channel,"2008, submitted to IEEE Trans. Info. Theory*
2. *Z. Li, W. Trappe, with R. Yates, "Private Communication via Multi-Antenna communication," Csonf. Info. Sci.with Sys., 2007, pp. 905–10.*
3. *W. Stallings, Cryptography and Network Security Principles with Practices , Prentice Hall PTR, 2006.*
4. *P. Parada and R. Blahut, "privacy Capacity of SIMO and Slow declining Channels," IEEE Int'l. Symp.Info. Theory, 2005, pp. 2152–55.*
5. *C. S. R. Murthy and B. S. Manoj, Ad Hoc Wireless Networks: Architectures with Protocols, Prentice Hall PTR,2004.*
6. *A. O. Hero, "safe Space-Time communiqué," IEEE Trans. Info. Theory, 2003, pp. 3235–49*