A Scrutiny about Physical Layer Security

[1]S. Suganya, [2]Dr. M. Senthil kumar

[1]PG Scholar, [2]Associate Professor
Department of computer science and Engineering,
Valliammai Engineering College

***Abstract*: In wireless environment, the communication across various users is established. To establish a secure transmission we need to track the entire process of layered approach. It is obvious that wireless environment uses a standard OSI model and protects the information in higher layer with the help of encryption techniques. Nowadays researchers focus on providing a security at various layers not alone in application itself. Hereby we tend to focus on physical layer security since many researchers had focused on transmission channel in theoretical setup. There are two types of threats in physical layers are jamming and eavesdropping. There are various detecting mechanisms such as two way training based detector, ERD etc to detect the presence of adversaries.**

***Keywords:* Two way training based detector, ERD, Jamming, Eavesdropping etc.**

Introduction

Wireless environment in which communication takes place in an faster rate and also plays a vital role to our day to day life[1]. It is widely used in numerous applications such as Banking etc. It is necessary that need to clearly understand about happenings/ functionalities of wireless communication process are represented in architecture(Fig-1). In this study we would like to discuss about various threats , techniques to provide security , transmission channel.

Based on transmission channel , the security system designed as follows

- Shannon's cipher channel
- Wyner's wiretap channel
- Gaussian wiretap channel
- Multi antenna wiretap channels
- Partial CSI
- Fading wiretap channel
- Broadcast channel
- Multiple Access channel
- Interference channel
- Relay channel

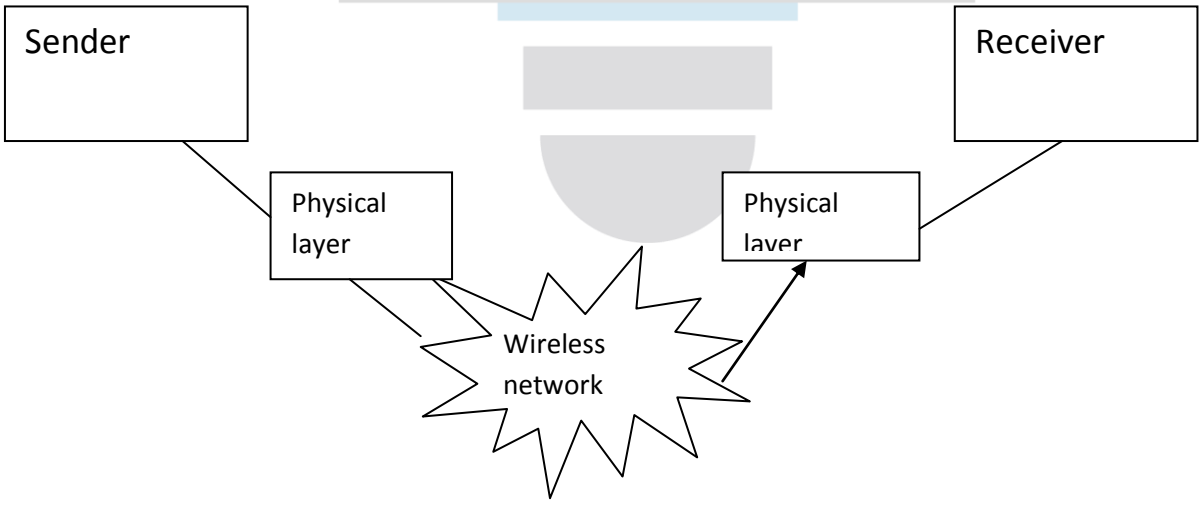

Fig-1 Overall Architecture of wireless communications

Shannon's cipher system

Shannon designed a secure transmission across sender and receiver without noise by proving a secret key K[3]. The key K is not known to adversary. It is important to know that message as well as secret key (K) are in binary numbers so that it provide much perfect secrecy known as one time pad approach.

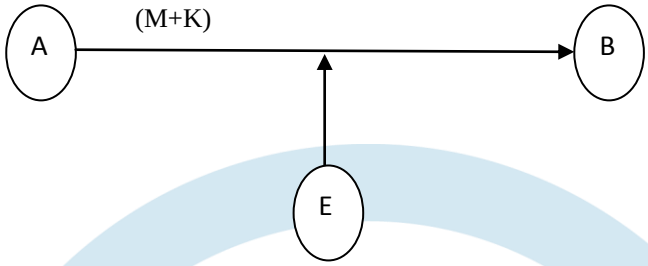

Fig -2 Representation of Shannon's cipher system

Wyner's wiretap channel

It is also similar to that of an Shannon's cipher model . The major differences is that there is a presence of noisy channel without a key across a legitimate users. Here there are secrecy criterion in terms of its secrecy. They are weak secrecy criterion and Strong secrecy criterion to mutual information[2].

Gaussian wiretap channel:

It is linear time invariant by adding a Gaussian white noise. It is given by the following equation[4].

$$Yb, i = HbXi + Nb, i$$

$$Ye, i = HeXi + Ne, i$$

Multi antenna wiretap channel:

It consists of multiple transmit as well as receiving antenna where the eavesdropper will be interpreted as an multiple single antenna[5].

Partial CSI:

There is a gain of all channels to the legitimate users this condition is called as perfect CSI.

Fading wiretap channel:

Multipath propagation as well as interferences leads to changing communication and conditions for mobile networks called as fading.

Broadcast channel:

Hereby the transmission process leads sending the information to more than one recipient.

Multiple Access Channel:

The recipients will be unique/ single but the message can be obtained from variety of sources.

Interference channel:

In this type of transmission medium there might be a presence of more number of transmitter as well as receiver pairs to establish communication.

Relay Channel:

Relay is to support the communication across transmitter and receiver. It increases the maximum transmission rate. It acts as confidential channel to send information against external adversaries.

THREATS IN PHYSICAL LAYER

There are two types of major threats in physical layer. They are

- Jamming and
- Eavesdropping

Jamming

It is the process of interrupting the transmission at the transmitter end in channel. Jammer will broadcast an interference signal on spectral band to interrupt the legitimate receiver reception. It is of two types . They are Active jammer and Reactive Jammer.

Active jammers

It is constantly sending the radio signals in channel to destroy the communication of legitimate users.

Reactive jammers

It will start its process only if transmission of signals takes place until it will be idle. Whenever if transmission starts it will tend to jamming the entire transmission channel to avoid a secure transmission.

Eavesdropping

During the transmission of information there might be a presence of adversaries across an legitimate users leads to eavesdropping. It is one of the major threat to the physical layer security. This threat was very curious and reflect much effect so the researchers have designed much more detecting mechanisms. Some of them are two way training based detector , Energy ratio based detector.

CONCLUSION

In this paper , we have provided of information regarding various factors physical layer security. It mainly includes the transmission channel (medium) where threats tends to occur. The major threats are also discussed. Further we can enhance it by searching more information built in security as well as various ways we can provide additional security .

REFERENCES

[1].Yi-sheng shiu and shih yu chang , Hsiao-chun wu , " Physical layer security in wireless Networks", IEEE wireless Communications, 2011.

[2].A.D. Wyner,"The Wiretap Channel", Bell System Tech. Vol. 54, 1975.

[3].Shannon CE *(1949) Communication theory of secrecy systems. Bell Syst Tech J 28:656–715.*

[4].Leung-Yan-Cheong SK, Hellman ME *(1978) The Gaussian wire-tap channel. IEEE Trans Inf Theory.*

[5]. Oggier F, Hassibi B*(2011) The secrecy capacity of the MIMO wiretap channel. IEEE Trans Inf Theory 57:4961–4972.*