ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

A Review on Pilot Spoofing Attacks in Wireless Networks

Dr. Senthil Kumar M[1], Ms.Suganya S [2]

Associate Professor, Department of CSE, Valliammai Engineering College, Kancheepuram, Tamilnadu, India[1]

PG Scholar, Department of CSE, Valliammai Engineering College, Kancheepuram, Tamilnadu, India[2]

ABSTRACT: A pilot spoofing attack is one of the major threat in wireless networks .It is a spam that leads to steal information in an illegal manner . It also provides information about various categories of spoofing attacks such as IP spoofing, Email spoofing etc. This paper presents some of the detecting techniques and method to handle eavesdropping of information .The desideratum of this paper focuses on providing a Maximal secrecy rate of information in wireless network.

KEYWORDS: Pilot spoofing , Spam, Eavesdropping, Secrecy rate, IP Spoofing, Email Spoofing.

I.INTRODUCTION

Many people widely used wireless networks for various purposes .In this wireless environment establishing a secured communication is a tedious process. while during the transmission there might be a presence of intruder, if it so it is an unsecure. This paper mainly focuses on pilot spoofing attack and it measures .A pilot spoofing attack is a spam that unauthorized receiver can steal the information.Cryptographic methods to provide a secure environment encrypting a original information (plain text) and transmit in the form of cipher text to an authorized receiver where they can decrypt to get an original information[2].

Categories of spoofing attacks:-

There are various categories of spoofing attacks. They are

- IP Spoofing
- Email spoofing
- DNS server spoofing
- URL Spoofing
- Pilot spoofing

IP address Spoofing is an attacker sends IP packets from a false source address in order to disguise itself. ARP (Address Resolution Protocol) Spoofing is a malicious party sends spoofed ARP messages across a local area network in order to link the attacker MAC address with the IP address of the legitimate member of the network. DNS Server Spoofing is a malicious party modifies the DNS server in order to reroute a specific domain name to a different IP address. URL spoofing occurs when one website appears as if it is another.The URL that is displayed is not the real URL of the site, therefore the information is sent to a hidden web address.Pilot spoofing attack is one of the stealing of information during the transmission of information between the legitimate users.

DOI: 10.15680/IJIRCCE.2016. 0409085

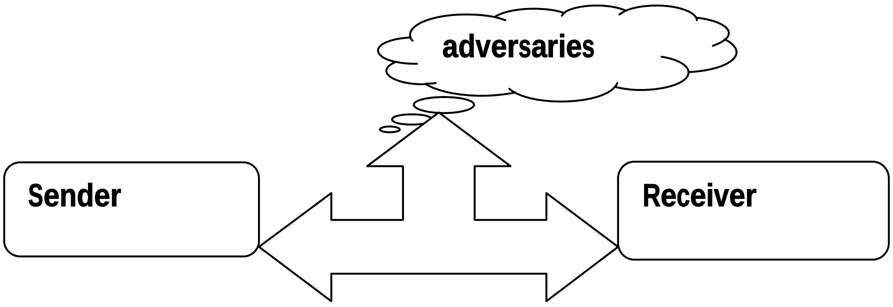

Fig-1

Fig-1 shows the basic representation of pilot spoofing attack during transmission of information.

II. LITERATURE SURVEY

This study mainly focuses on detecting techniques and methods to handle spoofing attack in an wireless network.

DETECTION MECHANISMS

Based on threshold value

Two way training detector is used to detect the attack. It is done based on the threshold value. If the presence of attack is confirmed then it can estimate the channels of both the legitimate and illegitimate users.It produces an approximate value with more accuracy compared to ERD(Energy Ratio Detector)[1].

Based on CSI.

In this paper detection of active eavesdropping is based on channel state information(CSI).It uses reverse training which means the transmitter design was already fixed based on the legitimate CSI simultaneously at the receiver end it tend to estimate at the transmitter side[4].

Based on PSK.

Detection of pilot spoofing attack is very tedious process .In this paper ,it proposes a detection from a known set of PSK(Phase Shift Keying) and also uses the scalar product between the received vectors to detect the intruder.

ERD

In this detection is made with the help of finding the signal strength received and transmitted at both terminals but it doesn`t care about the legitimate as well as illegitimate channels . It sets the ratio of received signal power levels both at transmitter and receiver to detect. It also shows the power imbalance between transmitter and receiver side when it is subjected to attack[12].

Based on RSS

RSS(Receive signal strength) is based on spatial correlation it does not include basic cryptographic methods rather it focuses signal energy received and transmitted. This method inherits signal strength from all connected wireless nodes to establish a secure communication.

METHODS TO HANDLE

Based on transmission

[9]While transmitting the signals it need to focuses on contamination so that we can send the signals in an orthogonal manner between the legitimate users.it will be hold good when the channel is free from other signals.

Beam forming

It uses MIMO technique(Multi-input-Multi-output).It gives a maximum positive secrecy rate in the legitimate as well as illegitimate channel. Maximizing the beam forming with the use of artificial noise. It leads to unavailable of eavesdropper in their respective channels[7] and[8].

Two way training based scheme

During the transmission of information the receiver is provided with the channel estimation and uses the downlink training . Here multiple antennas transmit signals to receiver[6]. It contains both link estimation so it can compare and provide difference on their estimations. It also send those estimated results back to the transmitter.

III.CONCLUSION

In this paper we have studied about pilot spoofing attack ,detecting the illegitimate channels and methods to provide a secure transmission . Information can be secured by transmitting those in an orthogonal manner mainly to avoid contamination of even legitimate signals. It can also overcome by usage of techniques such as MIMO , PSK predetermination while transmission, RSS(Received signal strength).During the implementation process some of the factors need to be considered in wireless environment are signal pattern , pre code design of transmitter.

IV.DISCUSSIONS

According to literature survey done , there are different ways for occurrence of spoofing attack and also they have main focuses on detecting the presence of adversaries as well as handling measures have mentioned .We need to concentrate much on providing secure transmission achieve maximal secrecy rate.

REFERENCES

[1] Qi Xiong, *Student Member, IEEE,* Ying-Chang Liang, *Fellow, IEEE,* Kwok Hung Li, *Senior Member, IEEE,*Yi Gong, *Senior Member, IEEE,* and Shiying Han, *Member, IEEE, Secure transmission against pilot spoofing attack:A Two way Training-based Scheme,* IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 5, MAY 2016.

[2] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 3rd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2003.

[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst.Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8,pp. 1355–1387, Oct. 1975.

[5] I. Csiszár and J. Korner, "Broadcast channels with confidential messages,"*IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[6] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[7] Q. Xiong, Y. Gong, Y.-C. Liang, and K. H. Li, "Achieving secrecy of MISO fading wiretap channels via jamming and precoding with imperfect channel state information," *IEEE Wireless Commun. Lett.*,vol. 3, no. 4, pp. 357–360, Aug. 2014.

[8] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[9] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[10] D. Kapetanovic, G. Zheng, K.-K. Wong, and B. Ottersten, "Detection of pilot contamination attack using random training and massive MIMO,"in *Proc. 24th PIMRC*, pp. 13–18,Sep. 2013,.

[11] J. Yang, S. Xie, X. Zhou, R. Yu, and Y. Zhang. (2014). "A semiblind twoway training method for discriminatory channel estimation in MIMO systems." [Online]. Available: http://arxiv.org/abs/1405.4626v1

[12] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems,"*IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932–940, May 2015.