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 7, July 2016

A Study on Pilot Spoofing Attack Detection

Keerthy K Murali [1], Abhisha Devi C M [2]

M.Tech Student, Department of ECE., SNGCE, Kadayiruppu, Kolenchery, Kerala, India[1]

Assistant Professor, Department of ECE, SNGCE, Kadayiruppu, Kolenchery, Kerala, India[2]

ABSTRACT - The convenience of wireless network is very high. But we must realize the fact that they are very unsecure. For example wireless networks are susceptible to identity based attack such as spoofing attacks. Conventional cryptographic schemes are the techniques for the secure communication in the presence of third parties called adversaries but it require huge infrastructure and computational overhead. However, as the internet grew and computers became more advanced, high quality encryption techniques became well known around the globe. This paper describes survey on pilot spoofing attack detection in wireless networks. Spoofing attack is one kind of active eavesdropping conducted by a malicious user, in which one person or program can successfully falsify the data of another for illegitimate advantage. One of the best examples of spoofing attack is pilot spoofing attack. The pilot spoofing attack could also weaken the received signal strength at the legitimate receiver if the eavesdropper utilizes large enough power. Spoofing attack usually happened at network level. In which it might be based on physical layer properties comparing current CSI with previous CSI and using spatial information. Multiple antenna technologies are also used to achieve perfect secrecy rate in wireless network.

KEYWORDS: Wireless network security; Spoofing attack; Pilot spoofing attack; Attack detection;

I. INTRODUCTION

Network security mainly contains some policies and practices which are adopted to prevent and monitor unauthorized access, misuse, falsification, or denial of computer network and also network accessible resources. Users choose or are assigned an ID and password that allows them to access to information and programs within their authority. Network security covers a variety of computer networks which include both public and private that are used in everyday job, business transactions, government agencies and individuals.

Networks are subjected to attacks from malicious sources. Attacks can be mainly classified into two types, which are passive attacks and active attacks.

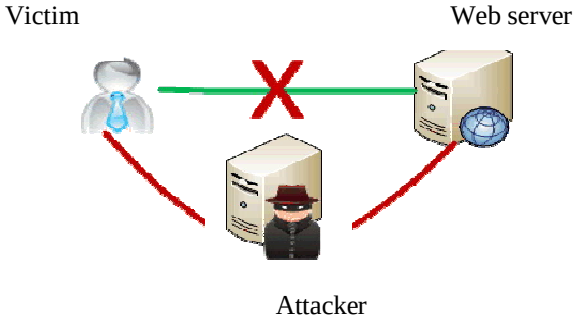

Fig.1.Man in the middle attack

When the intruder interrupts the data travelling the network called passive attack. If the intruder change or alter the data transmit through network called active attack. Idle scan and wiretapping are the examples of passive attack. The man in the middle attack shown in fig.1. (Attacker falsifies the data transmission between victim and web server) and cyber attack are examples of active attack. The original idea of spoofing attack is that the eavesdropper pretends to be

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 7, July 2016

the legitimate transmitter and sends the falsified information to the receiver. Conventional methods such as encryption method have been used to achieve such protection by using secrecy keys in transmission. However, computer became more widely available and due to the advances of computational capability of digital devices, the encryption methods face more and more challenges in secrecy key design and management. This paper mainly discuss about a survey on spoofing attack detection and localization based on physical properties and multiple antenna technologies. And also, we propose a scheme for both detecting spoofing attack and localizing adversaries.

II. RELATED WORKS

Mechanism based on cryptographic method

Conventionally, cryptographic authentication mechanism was used to detect spoofing attacks. [1] Mainly discuss about traditional approach of detecting spoofing attacks.

A. Working in secure and efficient key management (SEKM) framework

[1]In the case of unreliable wireless network, the main problems in mobile ad hoc network to providing infrastructure are mobility of host and lack of infrastructure, due to this fact, usually cryptographic mechanisms are used for secure communications in this type of networks. In fact, any cryptographic means is effective if its key management is strong. In this paper mainly discuss about a secure and efficient key management (SEKM) framework for mobile ad hoc networks. SEKM introduces a public key infrastructure (PKI) and applies a secret sharing scheme. It gives detailed information on the formation and maintenance of the server groups. In SEKM, through this method, each server group creates a view of the certificate authority (CA) also provides certificate update service for all nodes.

B. Working for Tesla certificate mechanism

[2]This paper shows the scalability problems for flat ad hoc networks. In this paper, the main task is to provide data and entity authentication for hierarchical ad hoc sensor networks. Sensor network mainly include three tiers of devices which are varying levels of computation and communication abilities. In the lowest tier consists of compute-constrained sensors that are unable to perform public key cryptography. This paper introduces a new type of certificate, which is named as TESLA certificate it can be used by low-powered nodes used to perform entity authentication. Our framework mainly authenticates incoming nodes, maintains trust relationships .When topology changes via an efficient handoff scheme, and provides data origin authentication for sensor data. Further, this type of framework assigns the authentication tasks to different nodes on their computational resources and resource-abundant access points which performs digital signatures and maintains most of the security parameters.

Mechanism based on using multiple antenna system

C. Guaranteeing secrecy using artificial noise

[3]This paper considered the main problem of secret communication in presence of a passive eavesdropper assuming a fading environment. The main assumption taken here that the channel gains of all the channels (thus, secrecy was not dependent on the secrecy of channel gains) is known by eavesdropper and they are also allowed to collude. Here also the paper showed how we can achieve secrecy, by adding artificially generated noise to the information signal. Here the artificial noise is generated by multiple antennas, so that only the eavesdropper's channel is degraded. Further, even if the transmitter has only a single antenna, relays can produces the artificial noise. A necessary condition for using the method of artificial noise is that the total number of transmit antennas must exceed the number of eavesdropper antennas.

Mechanism based on using physical properties

D. Pilot contamination for active eavesdropping

Recent studies on physical layer security assume that the availability of perfect channel state information (CSI) and study the importance of channel training needed for obtaining the CSI.[4] In this paper, mainly discuss how an active eavesdropper can attack the training phase in wireless communication which improve its eavesdropping performance. The main target of pilot contamination attack is at systems where the transmitter designs its precoder which is based on the estimates of the legitimate link's CSI and the estimation is carried out by having the receiver send pilot signals to facilitate the channel estimation at the transmitter, i.e., reverse training. During the reverse training phase, the active eavesdropper also sends the same pilot signals to falsify the transmitter about the correct channel to be estimated. So,

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 7, July 2016

the transmitter incorrectly designs the precoders[12] which will benefit the signal reception at the eavesdropper when data transmission occurs. The detection of the pilot contamination attack can be achieved by transmitting a sufficiently long pilot sequence in reverse training phase and analyzing the variance of the received signal at legitimate transmitter after normalizing it by the pilot sequence. If the variance is nearly in the range of receiver noise, it proves that the pilot contamination attack may have been conducted by eavesdropper.

E. The eavesdropping and jamming dilemma in multi- channel communications

[5]In this paper examined secret communication in multi- channel network from the adversary's perspective. Here Eavesdropper can undermine secret communication by either choosing to eavesdrop or jam, but Eve cant eavesdrop and jam at the same time .We have to focus on the problem how possibility to allocate jamming and transmission power by Evesdropper.Zero-sum game-theoretical approach is used. The main theory behind this is one participant's gain is equalized by other one's lose. In this work we focus on the problem how possibility to allocate jamming and transmission power by Eve and Alice has to be taken into account in the arrivals behaviour when Eve can also choose between jamming and eavesdropping mode. Channel secrecy capacity in terms of gain,

$$CS=\Sigma (\ln (1+h_iP_i/\sigma^2)-\ln (1+h_{Ei}P_i/\sigma^2_E) \quad ...(1)$$

Where, n is number of channels P =(P_1,...,P_n) with P_i is the power transmitted by Alice through channel i, h_i and h_{iE} are fading gains of main and eavesdropper's channels,σ2 and σ^2 E are background noise of main and eavesdropper's channels .

F. Channel-based spoofing detection in frequency-selective Rayleigh channels

[6]The main advantage of this technique is that which does not want priori knowledge of channel parameters and so it is more practical. In this paper introduces a generalized likelihood ratio test (GLRT) scheme. The spoofing detection is mainly based on false alarm rate and miss detection rate. The false alarm rate (or Type I error) is represented by α, which defined as the probability that the test defines Alice as the intruder Eve by mistake. The miss detection rate (or Type II error), represented by β, can be defined as., the probability that the test misses the detection of Eve.

G. Detection and Localization of Multiple Spoofing Attackers in Wireless Networks

[7]To propose to use received signal strength based spatial correlation, which can be a physical property depends on each wireless device that is hard to falsify and not reliant on cryptography on the basis for detecting spoofing attacks. This paper provided theoretical analysis of using the spatial correlation of RSS that is received signal strength inherited from wireless nodes for attack detection.

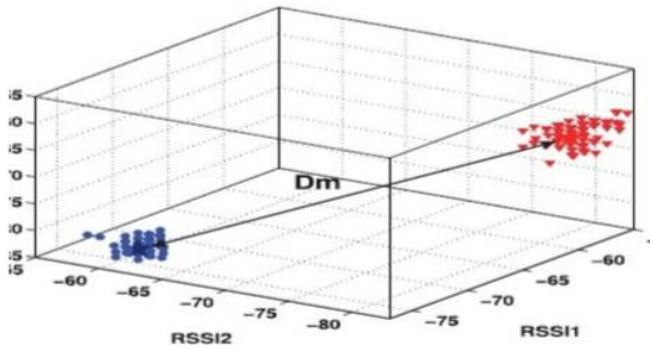

Fig.2 Illustration of RSS reading from two different locations

The fig2.shows the illustration of RSS reading from two different locations and D_m is the distance between two clusters RSS12 and RSS11 Also this paper derived the test statistic based on the cluster analysis of received signal strength readings. This approach can detect the presence of attacks and determine the number of adversaries, spoofing the same node identity, so that it can allocate or localize the number of attackers it may any number and eliminate can them. The number of Attacker determination is a particularly challenging problem ever faced. So here also developed SILENCE, a mechanism. This technique employs the minimum distance testing in addition to cluster analysis to arrive

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 7, July 2016

better accuracy in determining the number of attackers compared to other methods, which are Silhouette Plot and System Evolution, it use cluster analysis alone. Additionally, when the training data are available, here also introduces Support Vector Machines-based mechanism for improving the accurate number of attacker determination in the system.

H) Energy ratio based detection mechanism

[8]In this paper mainly motivated by the fact that the pilot spoofing attack can decrease the signal reception at the legitimate receiver, we propose the energy ratio detector (ERD) by exploring the variation of received signal power levels at the legitimate transmitter and the legitimate receiver. Our detection method mainly includes two phases: first, the legitimate receiver (Bob) sends the assigned pilot signal to the transmitter (Alice) through uplink channel, and transmitter Alice estimates the channel based on the signal samples; second, transmitter Alice calculates the received signal power, modulates it into a data signal and broadcasts it through downlink channel. Bob then demodulates the received data and calculates the power of the received signal. Bob then decides whether the system is under pilot spoofing attack or not by comparing the two power levels. Alice utilizes the same power to broadcast the data as that of Bob used for sending the pilot signal. This analysis shows that by setting the ratio of received signal power levels at the legitimate transmitter and the legitimate receiver as a test statistic[9][11], the detecting threshold[10] is derived without using the knowledge of the legitimate channel as well as the illegitimate channel CSI. The next step is to compare the test statistic with this threshold then assume whether there is present pilot spoofing attack or not.

III. CONCLUSION

In this letter we have done a study on spoofing attack detection in wireless network. Spoofing attack is one kind of active eavesdropping conducted by a malicious user, in which one person or program can successfully falsify the data of another for illegitimate advantage. We have studied all the references to develop a mechanism to detect and localize spoofing attackers in wireless network using energy ratio detection. Also studied a spoofing attack detection, attack detection technique and its classification, where it is used and today world as .much of data is send through wireless device it is very important to use this technique. Energy ratio based detection is very simple, precise and efficient in detecting attacker with more advanced characteristics.

REFERENCES

1 Wu, J. Wu, E. Fernandez, and S. Magliveras, ,"Secure and Efficient Key Management in Mobile Ad Hoc Networks",‖ Proc. IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS), 2005.
2. M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks",‖ Proc. ACM Workshop Wireless Security (WiSe), pp. 79-87, 2003.
3 S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise, IEEE Trans. Wireless Commun"., vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
4. 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.
5. A. Garnaev and W. Trappe, "The eavesdropping and jamming dilemma in multi-channel communications," in Proc. ICC, Jun. 2013, pp. 2160–2164
6. L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel- based spoofing detection in frequency-selective Rayleigh channels," IEEE Trans. Wireless Commun., vol. 8, no. 12, pp. 5948–5956, Dec. 2009.
7. J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 44–58, Jan. 2013.
8. Qi Xiong, Ying-Chang Liang,"An Energy-Ratio-Based Approach for Detecting Pilot Spoofing Attack in Multiple-Antenna Systems", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 5, May 2015
9. S. Kay, Fundamentals of Statistical Signal Processing, Volume II: Detection Theory. Englewood Cliffs, NJ, USA: Prentice-Hall, 1998.
10. D. V. Hinkley, "On the ratio of two correlated normal random variables," Biometrika, vol. 56, no. 3, pp. 635–639, Dec. 1969.
11. S. Kay, Fundamentals of Statistical Signal Processing, Volume I: Estimation Theory. Englewood Cliffs, NJ, USA: Prentice-Hall, 1998.
12. L. Xiao et al., "PHY-authentication protocol for spoofing detection in wireless networks," in Proc. GLOBECOM, Dec. 2010, pp. 1–6.

BIOGRAPHY

Ms.Keerthy K Murali [1] received her B.Tech Degree in Electronics and Communications Engineering from Mahatma Gandhi University, Kerala, India in 2014. She is currently studying her M.Tech Degree in Communication Engineering in Mahatma Gandhi University, Kottayam, Kerala, India. Her areas of interest include information forensics and security

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 7, July 2016

.**Ms.Abhisha Devi C M** [2] is an Engineering Graduate in Electronics and Communication Engineering from Calicut University. Did her masters M.Tech in NITK,Surathkal. At present she is associated with Electronics and Communication Department, SNGCE, Kolenchery. Her working areas include OFDM and Image processing.