International Journal of Computer Science and Engineering Communications,
Volume.5, Issue.4 (2017): Page.1641-1647
www.ijcsec.com

Secure Data Transmission against Pilot Spoofing using Cookie Management and MAC Address Validation

R.Sujatha[1], S.Brindha[2]
[1]*Research Scholar, Computer Applications, St.Peter's University, Chennai.*
[2]*Asst.Prof. Dept. of Computer Science & Applications, St.Peter's University, Chennai*
suji23@gmail.com

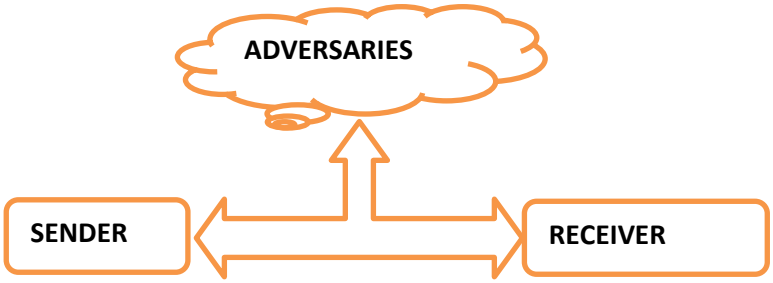
Abstract— *The pilot spoofing attack is one reasonably active eavesdropping activities conducted by a malicious user throughout the channel training phase. By transmission the identical pilot (training) signals as those of the legal users such an attack can able to manipulating the channel estimation outcome, which may result in a huge channel rate for the adversary but a small channel rate for the legitimate receiver. The proposed system has an intention for detecting the pilot spoofing attack and minimizing its damages, a tendency to style a two way training based scheme is introduced. An effective detector exploits the interfering element designed by the adversary, followed by a beam forming assisted data transmission. In addition to the solid detection performance, this scheme is also able to get the estimations of each legitimate channel. The cookies are analyzed and MAC address is generated. The encryption is achieved by using SHA-1 algorithm. A hash price is generated to the hacker using MD5 algorithm.*

Keywords— *spoofing attack, SHA-1, MD5, pilot spoofing, cookies.*

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are considered as one of the most significant technologies for the twenty first century advances in micro- electronic mechanical systems and wireless communication technologies, tiny, cheap, and smart sensors deployed in a physical area and networked through wireless links and the Internet provide plenty of opportunities for a plethora of civilian and military applications, for example, environmental monitoring, battle field surveillance, and industry process control. As against traditional wireless communication networks like cellular systems and mobile ad hoc networks, WSNs have unique characteristics, for example, denser level of node deployment, higher unreliability of sensor nodes, and huge power, calculation, and space constraints, which pose new challenges in the development and application of WSNs. As more and more wireless and sensor networks are deployed, the targets focus is on the malicious attack which increases. Due to openness of these systems, they are more liable to spoofing attack in which a malicious party impersonates another device or user on a network in order to launch against network hosts, steal data, spread malware or bypasses access control. Spoofing attacks are of serious risk as they can encourage an assortment of traffic injection attacks, for example, access point phishing. It is a prime concern to recognize the presence of spoofing and eliminate them from the network. The traditional approach to address spoofing attacks is to apply cryptographic authentication like a two way keying approach. URL spoofing happens when one website resembles another. The URL that is shown is not the genuine 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. The figure shows the basic representation of pilot spoofing attack during transmission of information.



II. RELATED WORK

Shyam Jadhav, Yogesh Katke, Vaibhav Joshi, Sagar Thore, has given a description on the openness nature of wireless system. In conventional security, cryptographic verification is utilized to confirm the nodes which are not desirable because of network overhead requirement. A unique data, that is a physical property connects with every node, which is difficult to distort, and it doesn't rely on upon cryptograph is utilized. This physical property can be utilized for recognizing spoofing attack exhibit in the system, deciding the quantity of assailant when various foes take on the appearance of an indistinguishable hub character from that of other nodes and limiting different attackers. Then the issue of deciding the number of attacker as multiclass recognition issue is formulated. Cluster-based systems are created to decide the number of attacker. Support Vector Machines (SVM) method used to improve the accuracy of determining the number of attackers. Additionally integrated detection and localization system are used to localize the positions of multiple attackers in the system. The eavesdropper and the corresponding optimal operation at the spoofing relay are obtained to find the maximum information leakage rate. Spoofing relay attack could entail new challenges from a physical-layer security point of view since it leads to significantly increase information leakage rate than conventional passive eavesdropping [1].

T C Deepthi and Jenelin S S explained about the concept of pilot spoofing attack that it is a eavesdropping conducted by malicious users while transmission takes place between a legitimate transmitter and receiver. Eavesdropper spoofing the legitimate transmitter on the estimation of Channel State Information (CSI) by sending the indistinguishable pilot signal as the real collector. In the pilot spoofing assault would decrease the strength of the received signal at the honest to goodness recipient when the spy uses sufficiently vast power. So, an Energy Ratio Detector (ERD) is used to help the legitimate users to identify and find such attacks. This Energy Ratio Detector identifies the presence of pilot spoofing attack by investigating the asymmetry of received signal power levels at the legitimate transmitter and recipient when there is an existing pilot spoofing attack. Also this identifier does not require changing the outline of current pilot flag and redesigning the procedure of current channel estimation handle. The ERD could shield the legitimate users from the pilot spoofing attack effectively [2].

Yong Zeng and Rui Zhang has presented the studies about new active eavesdropping technique via spoofing relay attack, which could be started by the eavesdropper to significantly enhance the information leakage rate from the source over conventional passive eavesdropping. Within this attack, the eavesdropper acting as a relay to spoof the origin to vary transmission rate in favor of its eavesdropping performance by enhancing or degrading the effective channel of the legitimate link.

Eavesdropper and the corresponding optimal operation at the spoofing relay are obtained to find the maximum information leakage rate. Spoofing relay attack imposes new challenges from a physical-layer security perspective since it leads to significant higher information leakage rate than conventional passive eavesdropping [3].

Keerthy K Murali, Abhisha Devi C M explained that the convenience of wireless network is very high. 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. A survey on pilot spoofing attack detection in wireless networks is described. 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 [4]. Dr. Senthil Kumar M, Ms.Suganya S has given a review on pilot spoofing in a wireless network that a pilot spoofing attack is one of the major threats 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. Some of the detecting techniques and method to handle eavesdropping of information are presented. The desideratum gives focus on providing a Maximal secrecy rate of information in wireless network [5].

III. IMPLEMENTATION

A new system model which will guarantee a system where the attacker couldn't hack the user's data is proposed. The techniques implemented in the system are too simple and strong for the user and hard for the hacker to break. A fundamentally modified pilot signal design and estimation process is identified. An efficient way of estimation of discriminatory channel is presented and is supposed to be secure from the pilot spoofing attack by randomly choosing the newly designed stochastic pilot signals.

Some of the huge issues are;

- Title Based Crawler to crawl all the URLs that match with the Title name;
- Implementing Scanning Method on URL's by using different types of Scan Engine like AVG, McAfee to detect the Phishing URLs.

ALGORITHMS USED STEPS INVOLVED IN MD5 ALGORITHM

- MD5 algorithm accepts the input message of arbitrary length and generates a 128-bit long hash value.
- MD5 hash algorithm includes of 5 steps as follows:

5. Append the Padding Bits. 2. Append the Length. 3. Initialize the MD Buffer. 4. Process the Message into 16-Word Blocks. 5. Output.

STEPS INVOLVED IN SHA1 ALGORITHM

The steps in SHA-1 algorithm are:

1. Append the Padding Bits.

- The message is "padded" with a 1 and as many 0's as required to bring the message length to 64 bits less than an even multiple of 512.

2. Append the Length.

- 64 bits are added towards the end of the padded message. These bits hold the binary format of 64 bits which indicates the length of the original message.

3. Prepare the Processing Functions.

- SHA1 requires 80 processing functions.

4. Prepare the Processing Constants.

- SHA1 requires 80 processing constant words.

5. Initialize the Buffers.

- SHA1 requires 160 bits or 5 buffers of words (32 bits).

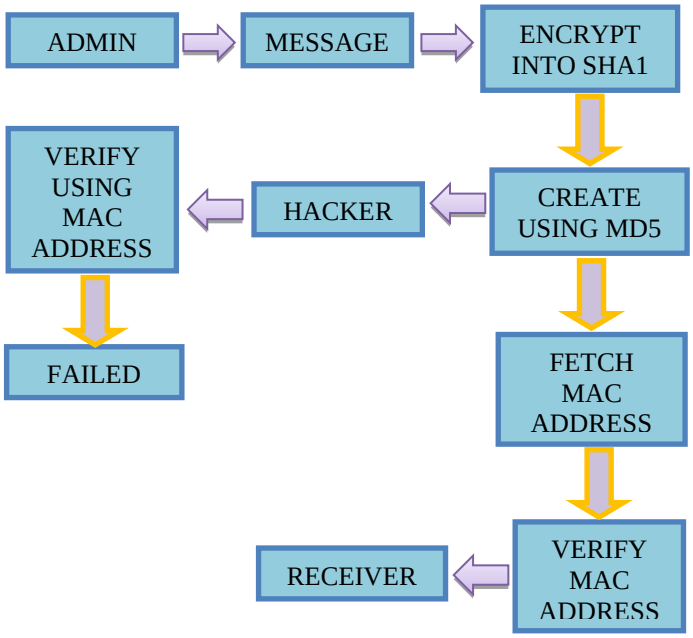
6. Processing Message in 512-bit blocks.

This is the important function of SHA1 algorithm which loops through the padded and appended message in 512-bit blocks.

7. Output:

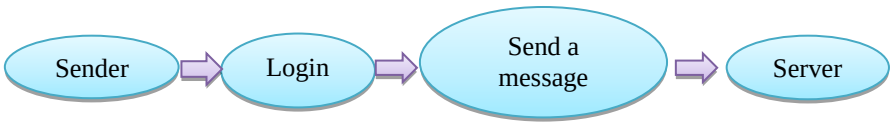
- Word buffers with the final message digest.

IV. SYSTEM ARCHITECTURE



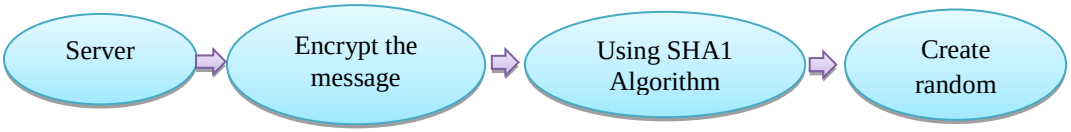
V. METHODOLOGIES COOKIE MANAGEMENT

- The attacker employs packet sniffing to study the network traffic between two parties in order to steal the session cookie.
- Many web sites use SSL encryption for login pages to prevent attackers from viewing the password, but encryption is not performed on the rest of the site once authenticated.
- This allows the attackers to study the network traffic in order to intercept all the data's that are submitted to the server or web pages viewed by the client.
- Since this data contains the session cookie, it permits him to impersonate the victim, even if the password itself is not compromised.
- Unsecured Wi-Fi hotspots are especially vulnerable, as anyone sharing the network will generally be able to study most of the web traffic between the access point and other nodes.



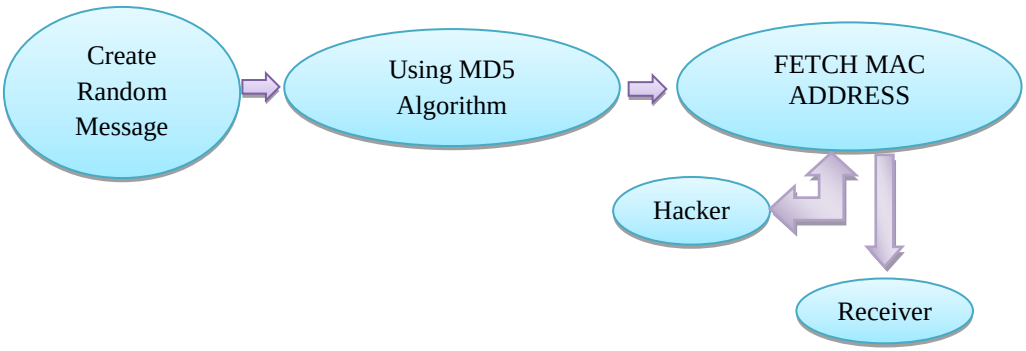
RANDOM ENCRYPTION

- A random encryption, or just cookie for short, is a token or short packet of data which is passed between the communicating systems, where the data is typically is not meaningful to the recipient system..
- The contents are opaque and are not interpreted until the recipient passes the cookie data back to the sender or to another program later.
- The cookie is most often used like a ticket for identifying a particular event or transaction.



MAC ADDRESS VALIDATION

- To prevent packet sniffing, a special technique is proposed under which, using random encryption to prevent this packet sniffing.
- Random encryption collects the MAC address of the machine and converts the MAC address into any encrypted format and enables session maintenance.

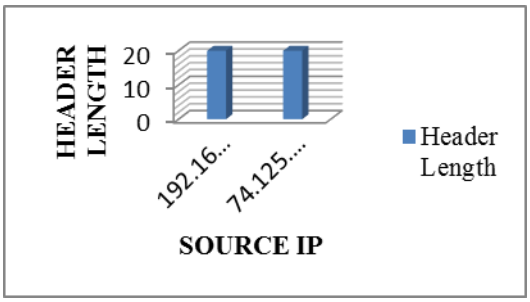


PERFORMANCE ANALYSIS

(i) Source IP vs. Header Length

A graph is plotted with source ip as x-axis and total length as y-axis. The header length is the same for both the source ip accessing the data.

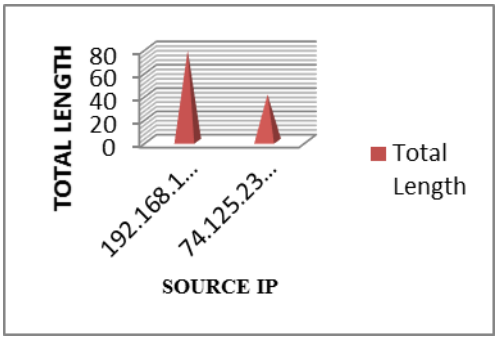
(ii)Source IP vs. Total Length



Source IP	Destination IP	Header Length	Date	Time
192.168.192.128	192.168.192.2	20	13-03-2017	10.59 am
74.125.236.220	192.168.192.128	20	13-03-2017	11.01 am

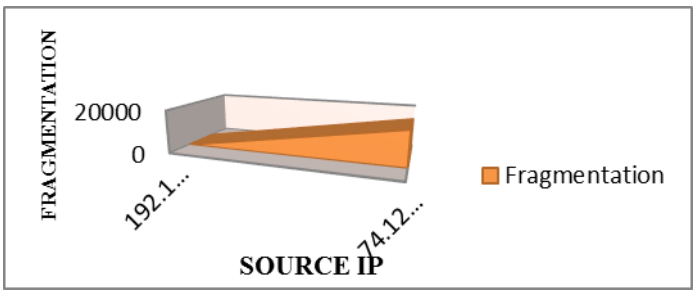
A graph is plotted with source ip as x-axis and total length as y-axis. The total length varies as the data is accessed from different source ip.

(iii) Source IP vs. Fragmentation



A graph is plotted with source ip as x-axis and fragmentation as y-axis. The fragmentation differs even when the both the flag=0.

Source IP	Destination IP	Total Length	Date	Time
192.168.192.128	192.168.192.2	78	13-03-2017	10.59a.m
74.125.236.220	192.168.192.128	40	13-03-2017	11.01a.m
Source IP	**Destination IP**	**Fragmentation**	**Date**	**Time**
192.168.192.128	192.168.192.2	0	13-03-2017	10.59a.m
74.125.236.220	192.168.192.128	16384	13-03-2017	11.01a.m



I. CONCLUSION

An active eavesdropping problem i.e., pilot spoofing attack is studied. A two-way training based scheme has been proposed to prevent from the pilot spoofing attack. An investigation is performed on the effectiveness of machine learning based phishing detection with known protected Websites. The effectiveness of each feature is studied and an optimal set of features are selected in the detector, in which a detection rate better than of 98%, with a false positive rate of 0.64% or below is achieved.

II. FUTURE SCOPE

In future, the emphasize must be given to improvise the standards in order to stop such attacks and make the channels safe and secure. The efficiency should be improved and time consumption for the URLs to be crawled will be reduced the technique can be used to make browser level plug-in for detecting phishing pages and auto blocking methods. In order to apply the prevention measure scheme to practical communication systems, the design of the proper reference signal patterns and the feedback procedure can be considered.

REFERENCES

[1]Shyam Jadhav, Yogesh Katke, Vaibhav Joshi, Sagar Thore , " Detection and Localization of Multiple Spoofing Attackers", in IJARCSSE, Vol. 4, Issue 10, October 2014

[2]T C Deepthi, Jenelin S S, "Detection and Localization of Pilot Spoofing Attacks in Wireless Communication Systems", in IJAREEIE, Vol. 5, Special Issue 2, March 2016.

[3]Yong Zeng, Rui Zhang,"Active eavesdropping via spoofing relay attack", in IEEE, May 2016.

[4]Keerthy K Murali , Abhisha Devi C M, "A Study on Pilot Spoofing Attack Detection", in IJIRCCE, Vol. 4, Issue 7, July 2016.

[5] Senthil Kumar M, Suganya S, "A Review on Pilot Spoofing Attacks in Wireless Networks", in Vol. 4, Issue 9, September 2016.

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

[7]S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jun. 2007, pp. 2466–2470.

[8]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.

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