DETECTION ANDPREVENTION OF FAKE ACCESS POINT USING SENSOR NODES

Hemashu Kamboj[1], Gurpreet Singh[2]

[1]Student, [2]Asst. Professor, Department of information technology, Lovely Professional University, Punjab, India
hemanshukamboj11@gmail.com, gurpreet.16523@lpu.co.in

Abstract

Networks are mainly of two types, wired and wireless. Now a days at most of the places people prefers wireless. The wireless network is much vulnerable to security attacks as compared to wired network. In wireless network there are various types of active and passive attacks are possible. The man-in-middle is one of the most common active attacks. The man-in-middle attack session hijacking attack can be performed generally using honey pot. In our work, the fake access point is the honey. In man-in-middle attack attacker attract legitimate user to connect with the unencrypted access point and that unencrypted access point is honey. When the legitimate user connect with the access point, attacker hack the cookies, sessions of the legitimate user. There are different types of detecting techniques are available and most of them are based on Beacon Frames. In this paper, a new technique is purposed in which sensor nodes are used in network and these sensors have storage of data about the access points that have use in the network. If any attacker try to perform an attack in the network by creating an fake access point, then sensor will sense and verifying attacker's fake access point by verifying MAC address of access point and after verifying report to legitimate user that you are connected with fake access point.

Keywords: *Honey Pot, Fake access Point, Attacks, Session, Hijacking, Cookies, Sensor.*

----------***----------

1. INTRODUCTION

The wireless networks can be broadly classified into two categories as Infrastructure and Infrastructure-less network. In Infrastructure type of network central controller is present, responsible for all data routing and controlling of the mobile devices.

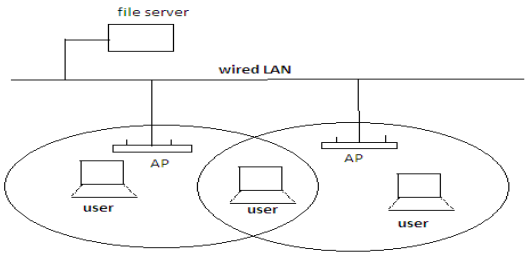

Figure 1: Infrastructure Network

In infrastructure-based networks, communication takes place only between the access point and the wireless node and not between the wireless nodes directly. The access point does not just control medium access but it also acts as a bridge to the wireless or wired networks. In the Infrastructure network the base stations are fixed and if the node goes out of the range of the base stations then it gets into the range of another station near to it. The Infrastructure-less network is the self configuring type of network in which no central controller is present.

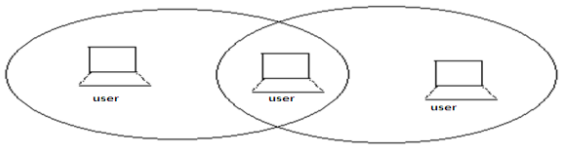

Figure 2: Infrastructure-less Network

Infrastructure less networks, do not have fixed routers all the nodes in the network act as routers. In both types of networks there are various types of attacks and these attacks are categorized into two categories the active and passive. The passive attacks does not effects the normal behavior of the network and simply sniffs the network. In active attacks, attacker affects the normal behavior of the network. Now a day's one of the popular and common active attack is man-in middle attack in which session is hijack. In this paper our work is to detect and prevent the session hijacking attack. The attack of session hijacking is generally performed with the help of fake access point.

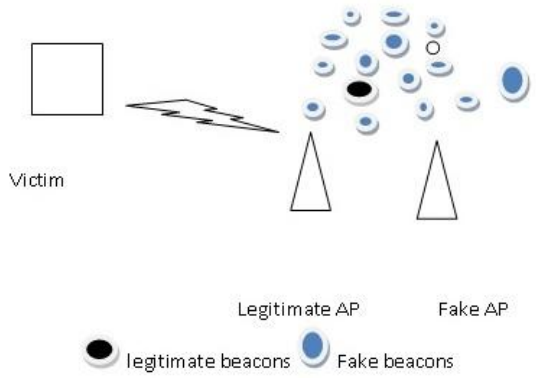

Figure 3: Beacon Flooding Attack

In session hijacking the attacker make an fake access point which act like honey pot and attacker not use any security and encryption on the honey pot so that letimate user attract towards it and attach with it. Both original and fake access points flood beacon frames to attract user.

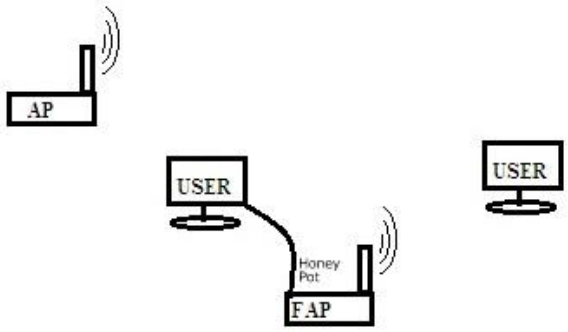

Figure 4: Honey Pot

If the legitimate user connects to the unencrypted fake access point and accesses the services of the access point, attacker can hijack the session of the users. A user who is already logged in(authenticated) to a web server and has a valid session existing between the user and the server, the attacker puts control over such a session and hijacks the session of the user and continues the connection . This is increasing day by day because in this attacker has a great advantage because there is no need to waste a lot ot time to crack passwords and to try to conduct a dictionary attack against the server. So in this type of attack attacker has easier to just listen to the traffic on the network and in this type of hacking user have very difficult make difference between fake access point and original. When attacker get the session of the legitimate user, attacker can access the services from the web server on the behalf of the legitimate user. In this paper a technique is purposed to detect and prevent the fake access point to prevent from session hijacking. In this technique fake access point detect and prevent with the help of sensor nodes.

In purposed technique the sensors are embedding network and stores the information to sensor of our network devices. After using sensors, attacker can make the fake access point in the network but can't hijack session. When a legitimate user attract towards fake access point and tries to connect with it, the sensor sense the legitimate user and after verifying that it going to connect with fake access point the sensor detect the fake access point and send message to legitimate that you are going to connect with fake network and after getting message, user will aware about network connection and then user try to connect with other access point. According to the size of network, the number of sensors are used and detection of fake access point is done by the sensor near to access point with which legitimate user try to connect.

2. PROBLEM FORMULATION

As there are various types of security attacks are possible in infrastructure type of network and if broadly classify these attacks then their are two categories the active attack and passive attack. In active attacks the most common type of attack is session hijacking and is done with the help of creating a fake access point. This type of attack also called man-in-middle attack. The session hijacking attack is implemented with honey pot and the honey pot is the fake access point. When the user connects to a fake access point the session of the user can be hijacking .There are some techniques which help in detecting the access point with which user is connect is original or fake but it not easy for all the users to use these techniques. So their is need of new technique which help users to detect the fake access point. If fake access point is detected then user can preventthesession hijacking by disconnecting with fake access point.

3. PURPOSED TECHNIQUE

Our new purposed technique is detection and prevention of fake access point with the help of sensor nodes. In other different techniques user has to do work to detect and prevent from attack but in our purposed technique network itself works to find the fake access point and user work is only to read message and prevent the fake access point by disconnecting with fake access point. If there is not any fake access point in the network then sensor simply verifying the connection and do not make any message for the user and network normally works.

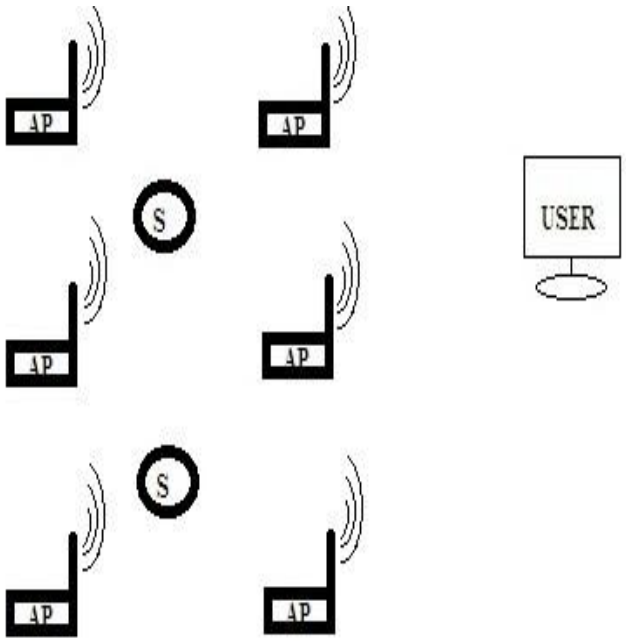

Figure 5: Network without Fake AP

If any user inside the network make a new access point in the same network then in this condition a access point will increase in number. If a new user tries to connect with that network then there are (n+1) numbers of access point.

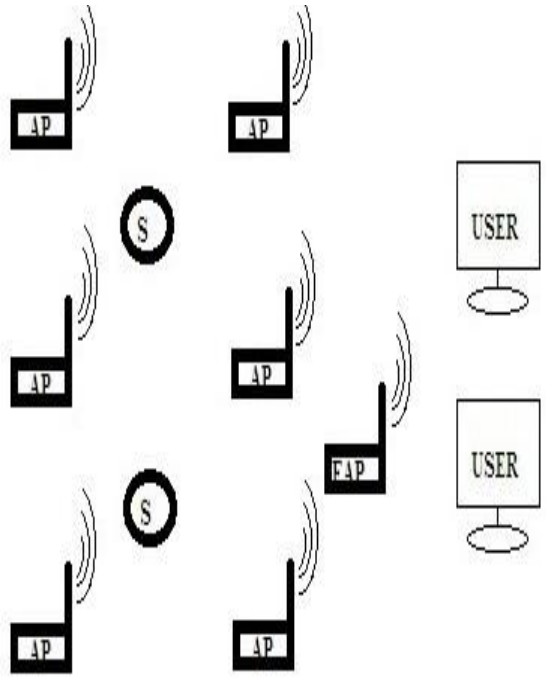

Figure 6: Network with Fake AP

The sensors present in the network verifying that the lefitimate user is connected with original access point present in the network or going to connect with the fake access point by verifying MAC address of access point with MAC address that present in MAC list in database. User sends probe request to access point access point responding. At that time while user and access point sending requests to each other, the sensor will sense their MAC addresses and then a connection is established between user and access point. For this scenario the sensors are implementing in the network in between the access points. The sensor near to the access point with which user tries to connect will sense and verifying that user connecting to original network or fake. After verifying, if sensor found that access point with which user connects is fake then it informs to the legitimate user. If user connects then sensor verifying the MAC address present in the access list, If a new user connects then again sensor check and results after verifying that the new MAC address is present with which user is going to connect and also check that how many user are already connected with that access point and after verification access point come to result that user is going continue with it or need to disconnect. The sensor work is only to inform to user and after that user has to disconnect to that access point.

Steps for proposed Methodology:
Step1: The infrastructure is deployed the finite numbers of legitimate Access points.
Step2: All sensor nodes have all the information about AP.
Step3: The mobile users can start accessing the Web services from the Access point.
Step4: It is assumed that in the network certain Fake access points can exits.
Step5: Fake access points are responsible for triggering the session hijacking attack.
Step6: The Purposed Technique is designed for detecting the fake access point.
Step7: In the network certain sensor nodes have been deployed for sensing the probe request and probe response messages.
Step8: Legitimate client send probe request to fake access point, fake access point reply with probe reply message.
Step9: The sensor nodes sense the communication.
Step10: If the details of the access point not found in the database of access point. The alert message is generated by sensor for legitimate client otherwise normal operations of the network continues

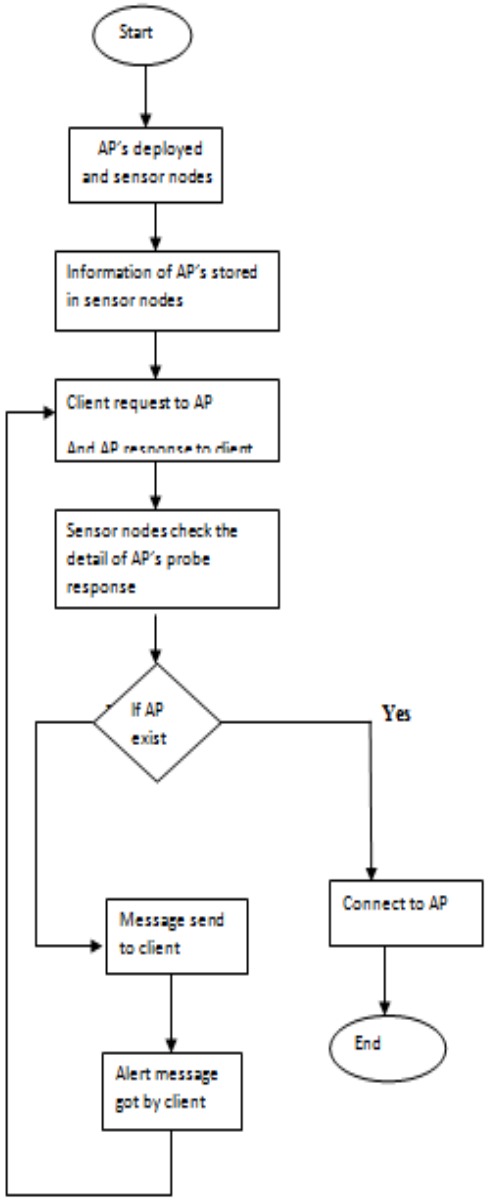

Figure 7: FLOWCHART

4. FUTUREWORK AND CONCLUSIONS

In this paper, conclude after studying the methods and procedure to create access point that it is very difficult to prevent from fake access point if they are created with the help of Backtrack 5 and with use of external wireless card as access point, so purposed technique give a new scenario that helpful in detecting fake access point. The fake access points will work like honey pot shown in Figure 4 and used to gather the network information and for fake access point, and a new user does not make itself any difference that which one original and fake. If legitimate users connect to that fake access point then all the information is hijack by the attackers. If the fake access points are detected then session hijacking can be prevented. So this technique will help in detecting fake access point with the help of implementing sensors in the network. In our future work, as in wireless technology everyday new technologies are introduced and technologies are not completely secured, as new technique comes the problems are comes and as problem solve the new problem arises, so in wireless technology there have don't 100% security, so this will going on continuously. In our work if attacker is able to spoof the MAC address then its not able to detect and controlling the spoofing with present techniques then in future there need a new technique for detecting and controlling on MAC spoofing and also the attacker may attack on sensor so have to secure the sensor using different techniques.

ACKNOWLEDGMENTS

I am very thankful to department of information technology (IT) of Lovely Professional University (LPU) Punjab India for providing the required facilities needed for the successful completion of this paper. I am also very thankful to those who have helped me directly or indirectly for accomplishment of this work.

REFERENCES

[1] A Mechanism for Detecting Session Hijacks in Wireless Networks, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 9, NO. 4, APRIL 2010.

[2] D. Liu, P. Ning, Establishing pair wise keys in distributed sensor networks, ACM Conference on Computer and Communications Security (CCS), October 2008, pp. 52–61.

[3]Monitoring unauthorized internet accesses through a 'honeypot' system ,INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS Int. J. Commun. Syst. 2011; 24:75–93.

[4] N. Sengottaiyan ,2009 "Modified Routing Algorithm for Reducing Congestion in Wireless Sensor Networks" Department of Computer Science and Engineering ,Nandha.

[5] Nick Nikiforakis1, Wannes Meert1, Yves Younan1, Martin Johns2, and Wouter Joosen11 IBBT-DistriNetKatholiekeUniversiteit Leuven, Celestijnenlaan 200A B3001, Leuven, Belgium.