IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 13, Issue 2 (Jul. - Aug. 2013), PP 66-73
www.iosrjournals.org

Detection of Session Hijacking and IP Spoofing Using Sensor Nodes and Cryptography

Abhishek Kumar Bharti [1], Manoj Chaudhary[2]
[1]*Research Scholar, Computer Science, YCoE , Punjabi University Patiala, Punjab, India*
[2]*Assistant Professor, Computer Science, YCoE , Punjabi University Patiala, Punjab, India*

Abstract: *Many web applications available today make use of some way of session to be able to communicate between the server and client. Unfortunately, it is possible for an attacker to exploit session in order to impersonate another user at a web application. The session hijacking is the most common type of attack in the infrastructure type of network. The confidentially is not providing under this attack to user information. Session hijacking attack is launched by making fake access point. If we detect the fake access point then we can stop session hijacking, and various techniques had been proposed. In this paper, we are giving a new mechanism to detect the fake access point with the use of sensor nodes in the network. In this mechanism we are also giving the protection against IP Spoofing by the use of public private key cryptography key exchange algorithm. We also discuss the results through simulations in Network Simulator 2.*

Keywords: *Session Hijacking, Fake Access Point, IP spoofing.*

I. Introduction

Wireless process control has been a popular topic recently in the field of industrial control. Compared to traditional wired process control systems, their wireless counterparts have the potential to save costs and make installation easier [12]. Wireless technologies range from complex systems, such as Wireless Local Area Networks (WLAN) and cell phones to simple devices such as wireless headphones, microphones, and other devices that do not process or store information. They also include infrared (IR) devices these use the direct line of sight between transmitter and receiver. As the wireless technology is growing very fast. So security in wireless networks have some additional challenges compared to wired networks. This is due to the fact that the traffic is transferred as radio waves in the air and anyone close enough with an antenna can receive them. There are various types of attacks are possible in wireless networks. The most common attacks are man-in-middle attack, denial-of-service attack.The man-in-the-middle (or middleperson) attack is one in which legitimate parties communicate via a hostile adversary but without their knowledge or consent. This attack can be devastatingly effective because the adversary enjoys complete control of the communication link and can inspect, inject, delay, delete, modify and re-order traffic to suit their purpose. It may be used, for example, to bypass weak authentication protocols, hijack legitimate sessions, perform active traffic analysis and deny service[14]. Session Hijacking is one of the popular attack in man-in-middle attack. In this paper we give a mechanism to prevent session hijacking attack. Its one of the favorite attack for the attackers because of the nature of the attack. A user who is trying to login or already logged in to a server , the attacker takes control over a session, basically hijacks the session from the user and continues the connection to the server pretending to be the user. Session hijacking have a great advantage to the attackers they don't have to waste hours and hours to crack the password , since the user has already been authenticated and in a active session it makes is so much easier to just listen to the traffic on the network without the knowledge of the user. There are three different types of session hijack attacks:

- Active Session Hijacking
- Passive Session Hijacking
- Hybrid Session Hijacking

Active Session Hijacking: The active attack is when the attacker hijacks a session on the network. The attacker will silence one of the machines, usually the client computer, and take over the clients' position in the communication exchange between the workstation and the server. And drop the connection between the user and the server. There are various methods for dropping the connection to the server, one of the most common is to send the huge amount of traffic, and this type of attack is known as Denial of Service. By doing this attacker has full control over the session and it communicate with the server pretending that it is the authenticated user fig1 shows how a typical session hijacking is conducted between a client and a server by an attacker. actual situation of the active session hijacking.

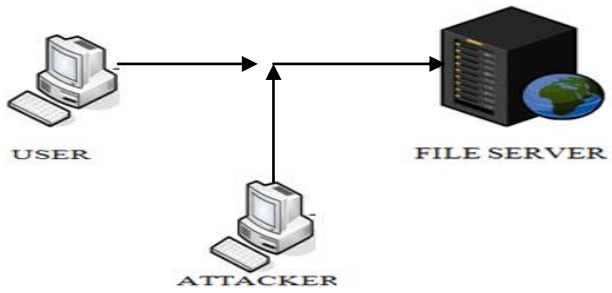


Figure 1: *Active Session Hijacking*

Passive Session Hijacking : Passive session hijack attacks are similar to the active attack, but rather than removing the user from the communication session, the attacker monitors the traffic between the workstation and server . In a passive session the attacker listens to all the data and captures them for future attacks, in most cases to perform any type of a hijacking attack it is important that the attacker starts off with passive mode. Figure 2 shows a typical passive hijacking.

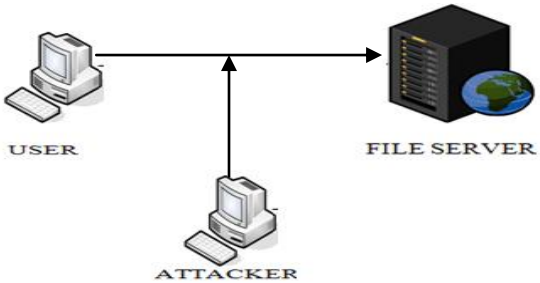


Figure 2: *Passive Session Hijacking*

Hybrid Session Hijacking: This attack is a combination of the active and passive attacks, which allow the attacker to listen to network traffic until something of interest is found. The attacker can then modify the attack by removing the workstation computer from the session, and assuming their identity.

In the infrastructure-based network, communication typically takes place only between the wireless nodes and the access point, but not directly between the wireless nodes. The access point does not just control medium access, but also acts as a bridge to other to wireless or wired networks. One of the ways in which a WLAN can be attacked is by introducing one or more unauthorized fake Access Points (APs) in the network. A fake AP can be set up by a malicious attacker. This fake AP is used to fool a wireless node in the WLAN into accessing the network through the fake AP instead of the authorized one. The fake AP can then launch a variety of attacks thereby comprising the security of the wireless communication. Setting up fake APs is not hard. And these Access points that are installed without proper authorization and verification that overall security policy is not obeyed by an AP is called rogue APs. These AP'S are installed and used by invalid users. Such APs are configured poorly, and it will used by an attackers.[11]

After the attacker set up a fake AP , it uses the packet sniffer software to sniff the packets . A (packet) sniffer is a program that intercepts and decodes network traffic broadcast through a medium. Sniffing is the act by a machine S of making copies of a network packet sent by machine A intended to be received by machine B. Sniffer is a program that is used for monitors and analyzes network traffic, detecting bottlenecks and problems. A network manager can keep traffic flowing efficiently by using this information. A sniffer can also be used legitimately or illegitimately to capture data being transmitted on a network. Network router reads every packet of data that passed from it, to determining whether it is delivered for a destination within the router's own network or whether it should be passed further along the Internet. A route that uses a sniffer it may be able to read the data in the packet as well as the source and destination addresses. In file sharing applications, sniffers are used on academic networks to prevent traffic bottlenecks. There are many techniques are given to detect fake access point like using clock skew [13].

In this paper a novel approach is given to detect the fake access point by the use of the sensor nodes. Even if we are using the sensor nodes to detect the fake access point if the attacker spoof the IP and MAC addresses of the client and pretend to be the valid authenticated user but it does not exist or may be that values belong to others. So in this novel approach a protection against the IP spoofing by public private key cryptographic key exchange algorithm.

II. Background And Related Work

Session hijacking is the stealing of the session of the user that is use to communicate with the server. In session hijacking 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 takes control over such a session, basically hijack the session from the user and continues the connection to the server pretending to be the user. And IP spoofing is the creation of IP packets using somebody else's IP source addresses. So in order to detect the session hijacking and IP spoofing various algorithms has been develop Extant defensive techniques and procedures are not completely effective against such attacks.

A. Technique for preventing Session Hijacking :

A.1 Rupinder Gill, and Smith, Jason and Clark, Andrew proposed an algorithm in 2006 that is based on IEEE 802.11 Network to detect the Session Hijacking distinct test scenarios. A correlation engine has also been introduced to maintain the false positives and false negatives at a manageable level. We also explore the process of selecting optimum thresholds for both detection techniques. This paper extends earlier work and explores usability, robustness and accuracy of these intrusion detection techniques by applying them to eight distinct test scenarios. A correlation engine has also been introduced to maintain the false positives and false negatives at a manageable level. We also explore the process of selecting optimum thresholds for both detection techniques. For the purposes of our experiments, Snort-Wireless open source wireless intrusion detection system was extended to implement these new techniques and the correlation engine. Absence of any false negatives and low number of false positives in all eight test scenarios successfully demonstrated the effectiveness of the correlation engine and the accuracy of the detection techniques[3].

A.2 Thawatchai Chomsiri in year 2008 made a comparative study between the security of Hotmail, Gmail and Yahoo Mail by Using Session Hijacking Hacking Test These three Web Mails were hacked by means of Session Hijacking. The researcher conducted this experiment on the LAN system and used information capturing technique to gain Cookies and Session ID inside Cookies. Then, Hijacking was conducted by using two Hijacking methods. The first method, which was common and easy to conduct, used only one Cookie. The second method, which was not very popular but offered high penetrating power, used all Cookies (Cookies cloned by SideJacking tools). The results show that the Web Mail with the highest security level is Yahoo Mail; the second one is Hotmail; and the Web Mail with the lowest security level is Gmail[1].

A.3 Bhavna C.K. Nathani Erwin Adi in year 2012 gives a procedure to identify the Website Vulnerability to Session Fixation Attacks Session fixation is a vulnerability of web applications where a malicious attacker gains full control of a victim's web account without having to use the victim's credentials such as username and password. The authors found that some 48% of Indonesian websites are vulnerable to such attacks because, contrary to best software engineering practices, many use default session management IDs generated by their development platforms. And tells that each website with a URL and/or cookie containing a string of characters that can represent a session ID was classified as vulnerable[4].

A.4 In year 2012 Srikanth Kamuni, S.ShreehaTejaswini, Bhaskar.J proposed a technique for detecting the session hijacking based on wavelet based real time session hijack detection based on Bluetooth signal analysis in which it tells A session hijacking is predominantly a man in the middle attack for wireless network where the attacker places itself in the route between the source and the destination node such that all the traffic is routed through the malicious node. A session hijacking is the result of accidental association attack or MAC spoofing attack. In this case the attacker places itself close to either the source or the destination or any other router node in such a way that it is considered as a legitimate router node. Therefore detection rate in most of the existing technique is low and unreliable. In this work we propose a real time mechanism for detecting the session hijacking attack by analyzing the signals received from the nodes through a monitoring station in the wavelet domain[2].

B. IP spoofing:

B.1 Al-Sammarraie Hosam ,Adli Mustafa and Shakeel Ahmad in year 2009 proposed an algorithm for IP spoofing over online environment IP and email spoofing gained much importance for security concerns due to the current changes in manipulating the system performance in different online environments. Intrusion Detection System (IDS) has been used to secure these environments for sharing their data over network and host based IDS approaches[5].

B.2 Vimal Upadhyay , Rajeev kumar proposed a technique to prevent IP spoofing using hashing encryption in year 2011 this paper gives a better technique for the protection against IP spoofing and this paper tells that the attack on any node or system can be done from any direction[7].

B.3 Noureldien A. Noureldien, Mashair O. Hussein in year 2012 proposed A method for Detecting and Preventing All Types of Spoofed Source IP Packets and SYN Flooding Packets at Source this method is

based on a network authentication server (AS), which performs an authentication process on SYN packets. The authentication process verifies the legitimacy of SYN packet's source IP address that initiate a connection request from a network subnet host to an external host. During the authentication process of SYN packets, AS identifies and blocks SYN packets with legal source IP address that chip in a TCP/SYN flooding attack. AS preserves network performance by exchanging authentication messages in plain text, and acts as a stateful inspection firewall and only SYN packets are subject for inspection. Our method which is capable to detect and prevent all types of spoofing packets including subnet spoofing contributes to standard ingress/egress methods in eliminating bogus traffic on the Internet[8].

B.4 In year 2012 an ant-based traceback is proposed to detect the IP spoofing. The proposed traceback approach uses flow level information to identify the spoofing request. To validate the detection method further, this paper considers the number of hop needs to reach the destination end. Using a mapping between IP addresses and their flow level with hop-counts, the server can distinguish spoofed IP packets from legitimate ones. The simulations results show that this approach discards almost 90% of spoofed IP request[9].

C. Fake access point:

C.1 Kiruthiga.S and Yuvarani.G in year 2012 proposed a technique for the fast and accurate detection of fake access point using non-cryptomethod in which they calculate the clock skew of an AP from the IEEE 802.11 Time Synchronization Function (TSF) time stamps sent out in the beacon/probe response frames. They uses two different methods for this purpose—one based on linear programming and the other based on least-square fit. They supplement these methods with a heuristic for differentiating original packets from those sent by the fake APs. They collect TSF time stamp data from several APs in three different residential settings. Using their measurement data as well as data obtained from a large Setting, they find that clock skews remain consistent over time for the same AP but vary significantly across APs..

C.2 Hemanshu Kamboj, Gurpreet Singh in year 2012 they also present the detection of fake access point using the sensors in the network but the use the beacon frames received in fix time . Fake access point is the honey. In the session hijacking attack we attract legitimate user to connect with the unencrypted access point .When the legitimate user connect with the access point, we hack the cookies, sessions of the legitimate user. In this paper, they are proposed a hybrid technique to detect fake access point. Their proposed technique is based on the number beacon frames received in fixed time according to the climate conditions[10].

To summarizing the background work and more work, technique and results we are presenting in table.

Author(s)	Year	Paper Name	Technique	Result
A. Session Hijacking				
Rupinder Gill, and Smith, Jason and Clark, Andrew[3]	2006	Experiences in Passively Detecting Session Hijacking Attacks in IEEE 802.11 Networks	Using sensor	Sensors cant do work in co-operation
Thawatchai Chomsiri[1]	2008	A Comparative Study of Security Level of Hotmail, Gmail and Yahoo Mail by Using Session Hijacking Hacking Test		Yahoo has maximum security and gmail has the lowest security
Bhavna C.K. Nathani Erwin Adi[4]	2012	Website Vulnerability to Session Fixation Attacks	Checks the url for checking the vnlnerability	
Srikanth Kamuni, S.ShreehaTejaswini, Bhaskar.J, Dr. G.Manjunath[2]	2012	Wavelet Based Real Time Session Hijack Detection Based On Bluetooth Signal Analysis	Monitering System using bluetooth	Efficiency increased to 90 % And its real implemented and can be applied to wifi and other networks.
B. IP spoofing				
Al-Sammarraie Hosam and Adli Mustafa[5]	2009	Exception Agent Detection System for IP Spoofing Over Online Environments	Create an intrusion detection system for ip spoofing	More efficient but costly.
Vimal Upadhyay , Rajeev kumar[7]	2011	Detection and preventing IP spoofing attack by Hashed Encryption	Hashing	Attacks in wireless node can be from any direction
Noureldien A. Noureldien, Mashair O. Hussein[8]	2012	Block Spoofed Packets at Source (BSPS): A method for Detecting and Preventing All Types of Spoofed Source IP Packets and SYN Flooding Packets at Source	Network authentication server	By network ad-ministrators and ISP's to alleviate bogus traffic in the Internet.

N.Arumugam, Dr.C.Venkatesh[9]	2012	A Dynamic Method to Detect IP Spoofing on Data Network Using Ant Algorithm	Ant-based traceback	Ensure good filtering of packets
Mrs. Mridu Sahu and Rainey C. Lal [6]	2012	Controlling IP spoofing through packet filtering	Packet filtering	Preventing spoofing through Packet filtering
C. Fake Access Point Detection Techniques				
Hemanshu Kamboj, Gurpreet Singh[10]	2012	Detection of Fake Access Point to Prevent Session Hijacking	Sensor nodes	Can detect the fake access point but not after IP spoofing
Kiruthiga.S and Yuvarani.G[11]	2012	Fast and Accurate Detection of Fake Access Points Using Non-crypto Method in WLAN	Clock Skew of Access Point	Can not find the MAC spoofing

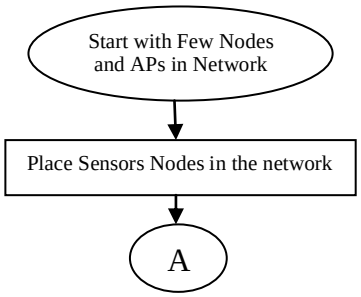
III. Problem Formulation

A typical session hijacking is a well-known man-in-the-middle attack in the world of network security and its one of the favorite attack for the attackers because of the nature of the attack. The session hijacking attack is generally implemented with the honey pot. The rogue access point acts like a honey pot. Like legitimate AP, fake AP broadcast the beacons signals. A user checks the beacon signals and make probe request to fake AP. Fake access point respond back with probe response. When client and access point are successfully mutually authenticated, connection between access point and client will be established. When client and access point are associated, client can able to access service provided by the access point. A problem arises when legitimate client connects to the fake access point. All the information send by the client can be spoofed by the attacker which operated the fake access point. This leads to the session hijacking. So there have to need some security mechanisms that detect the fake AP and prevent the session hijacking. If detect the fake AP then can prevent the session hijacking. Even if fake access point detection is possible then by IP spoofing the fake access point can't be detected so we need a mechanism that detect the fake access point as well as give the protection against IP spoofing.

IV. Proposed Technique

To prevent session hijacking, a novel technique is proposed under which, sensor nodes are placed in the network. Sensor nodes sense all the communication between AP and wireless devices i.e. probe request and probe responses. All sensor nodes stores all the information about AP in their database, such as MAC address, coverage area, attached devices, etc. When client wants to communicate with fake access point, client send probe request to access point and access point reply with probe response message. Sensor nodes sensing this communication and they check detail of AP in their database. If the detail of access point doesn't exist in the database of Sensor node, it sends an alarm message to the wireless device about fake AP. In this way a device is protected against fake AP.

In this technique the MAC address spoofing is possible so to prevent against the MAC spoofing new enhancement in the proposed mythology has been proposed. In this technique the public and private key cryptography is used to prevent MAC spoofing. At the start when the sensor nodes storing the knowledge about each node like MAC address, coverage area, attached devices, etc in the network at that time it assign a unique key to each access point in the network to prove its identity. And stores the unique key in their databases corresponding to each AP configuration that have saved. When a access point starts communication it send the unique key encrypt with the sensor node's public key to the sensor node. Sensor node decrypt with its private key and verifies from their database that the key is assign to this MAC address if yes positive acknowledgement will send to the access point if not matched it will send the alarm message to the wireless device about the fake access point. This message exchange is encrypted and decrypted which the asymmetric encryption algorithm. Below flowchart of the proposed technique is given



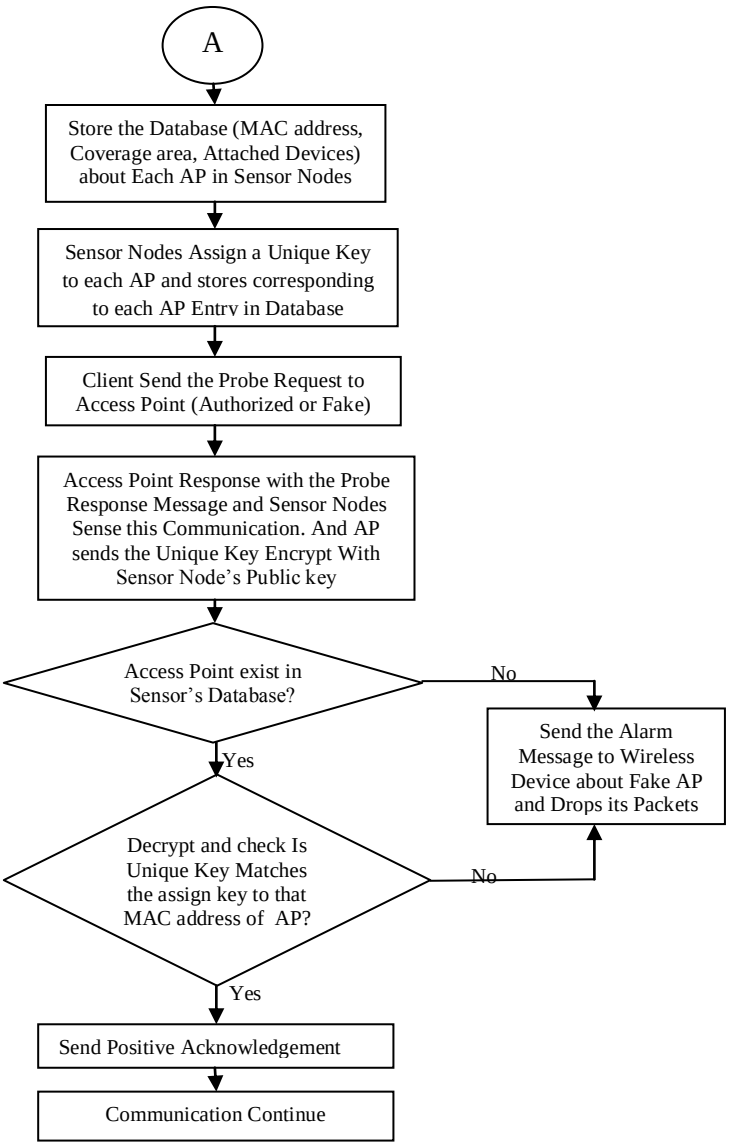


Figure 3: *Flow Chart of Proposed Technique*

V. Result

For the results we are trying to show the proposed technique to simulate through the Network Simulator 2. For this firstly make a network with few wireless nodes and access points. Fake access point is made and it start providing the services to the legitimate users figure 4 show this so that attacker can easily attack on the session of the user

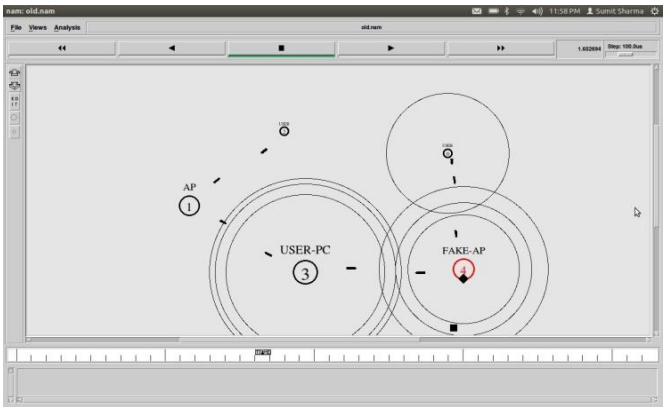


Figure 4: *User accessing the services using fake AP*

Now placing some sensor node in between the network , the sensor nodes store the information about the access points in its data base. The stored information contains the MAC addresses of the access points. The users are declared which wants to communicate with the access point. And sensor nodes also give the unique key to each AP and stores into the database corresponding to each AP. Figure 5 show this

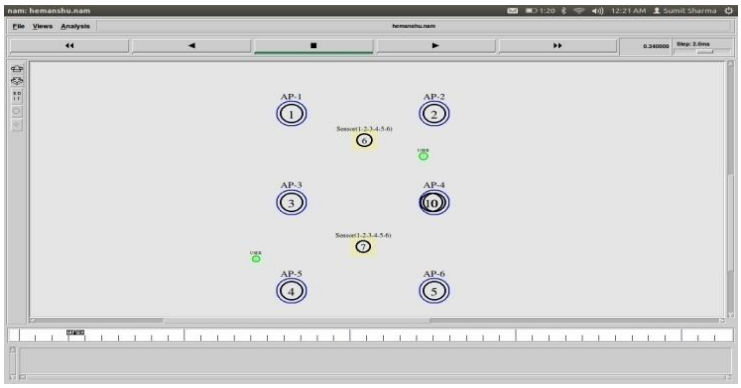


Figure 5 *Database maintain by sensor nodes and assign the unique key to each AP*

In figure 6, When the legitimate client send probe request message and access point reply with probe response message. It also send the unique key encrypt with the sensors public key that is near to it .The message exchange between client and access point is sensed by the sensor node. The sensor node decrypt the message that received from the Access Point. And verifies that it is same or different.

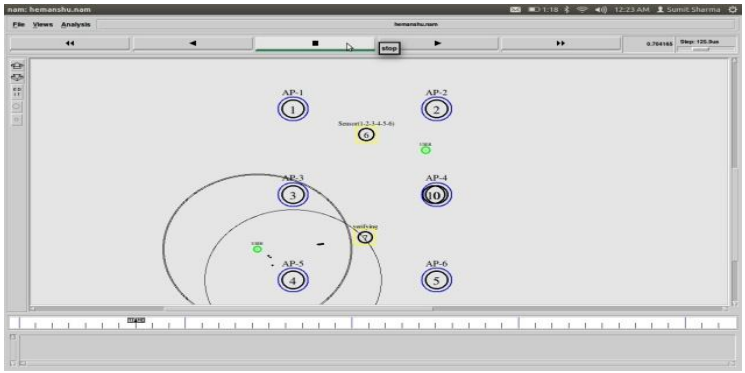


Figure 6: *Verifying the access point identity by sensor node*

If the sensor node sense the communication and verifies from the database if no entry then that access point is fake to whom the client wants the communication. It will generate the alert message for the client , but if there is an entry in the database it sends for the second step of verification for the IP spoofing it decrypt the message that came from that AP and verifies that the received unique key is same or different if it is same it do nothing and if different that access point is fake to whom the client wants the communication. It will generate the alert message for the client. Figure 7 show that access point is not in the database of the sensor so it will generate the alert message for the client and declare that access point is fake.

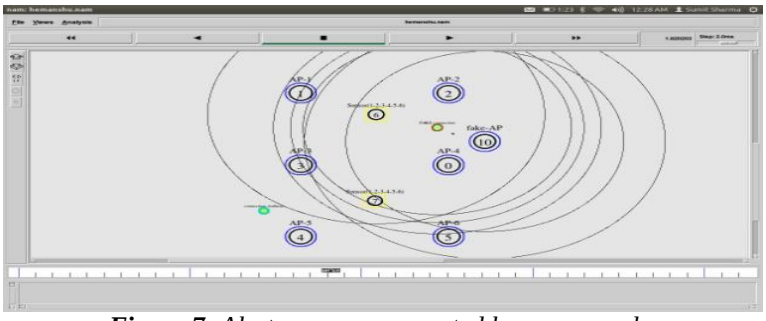


Figure 7: *Alert message generated by sensor node*

VI. Conclusion

This paper conclude that session hijacking is active type attack has very bad impact on the network .The fake access points will work like honey pot and used to gather network information. If the fake access points are detected which will work like a honey pot then session hijacking will be prevented .In this paper ,we propose sensor node based technique to prevent session hijacking by storing the information about the AP and this technique has vulnerability of MAC spoofing which is prevented through the use of public private key cryptography.

References

[1] Thawatchai Chomsiri "A Comparative Study of Security Level of Hotmail, Gmail and Yahoo Mail by Using Session Hijacking Hacking Test" in International Journal of Computer Science and Network Security, VOL.8 No.5, May 2008.

[2] Srikanth Kamuni, S.ShreehaTejaswini, Bhaskar.J "Wavelet Based Real Time Session Hijack Detection Based On Bluetooth Signal Analysis" in GJCAT, Vol 2 (2), 2012, 1210-1213 ISSN: 2249-1945.

[3] Rupinder Gill, and Smith, Jason and Clark, Andrew "Experiences in Passively Detecting Session Hijacking Attacks in IEEE 802.11 Networks" in: Proceedings of 4th Australasian Information Security Workshop (Network Security), 16-19 January 2006, Hobart, Tasmania.

[4] Bhavna C.K. Nathani Erwin Adi "Website Vulnerability to Session Fixation Attacks" Journal of Information Engineering and Applications ISSN 2224-5782 (print) ISSN 2225-0506 (online)Vol 2, No.7, 2012.

[5] Al-Sammarraie Hosam ,Adli Mustafa and Shakeel "Exception Agent Detection System for IP Spoofing Over Online Environments" International Journal of Computer Science and Information Security, Vol. 6, No. 1, 2009.

[6] Mrs. Mridu Sahu and Rainey C. Lal "Controlling IP spoofing through packet filtering" Int.J.Computer Techology & Applications,Vol 3 (1),155-159 ISSN:2229-6093.

[7] Vimal Upadhyay , Rajeev kumar "Detection and preventing IP spoofing attack by Hashed Encryption" International Journal of Enterprise Computing and Business Systems ISSN (Online) : 2230-8849 Vol. 1 Issue 2 July 2011.

[8] Noureldien A. Noureldien, Mashair O. Hussein "Block Spoofed Packets at Source (BSPS): A method for Detecting and Preventing All Types of Spoofed Source IP Packets and SYN Flooding Packets at Source: A Theoretical Framework" International Journal of Networks and Communications 2012, 2(3): 33-37 DOI: 10.5923/j.ijnc.20120203.03.

[9] N.Arumugam, Dr.C.Venkatesh "A Dynamic Method to Detect IP Spoofing on Data Network Using Ant Algorithm" IOSR Journal of Engineering (IOSRJEN) e-ISSN: 2250-3021, p-ISSN: 2278-8719, www.iosrjen.org Volume 2, Issue 10 (October 2012), PP 09-16.

[10] Hemanshu Kamboj, Gurpreet Singh " Detection of Fake Access Point to Prevent Session Hijacking" International Journal for Advance Research and Technology Vol. 1, Issue II, Mar. 2013 ISSN 2320-6802.

[11] Kiruthiga.S and Yuvarani.G "Fast and Accurate Detection of Fake Access Points Using Non-crypto Method in WLAN" International Journal of Communications and Engineering Volume 05– No.5, Issue: 03 March2012.

[12] Jianping Song, Song Han, Aloysius K. Mok, Deji Chen, Mike Lucas, Mark Nixon "WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control" IEEE Real-Time and Embedded Technology and Applications Symposium 1080-1812/08 2008 IEEE DOI 10.1109/RTAS.2008.15.

[13] Suman Jana and Sneha k. Kasera " On Fast and Accurate Detection of Unauthorized Wireless Access Point Using Clock Skews" IEEE TRANSACTION ON MOBILE COMPUTING , VOL. 9 NO. 3 MARCH 2010.

[14] Stephen Glass NICTA "Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks" 1550-445X/09 2009 IEEE DOI 10.1109/AINA.2009.131.