THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

A Novel Approach Towards illegitimate Access Point Discovery To Prevent Session Hijacking

Gurpreet Singh,
Department of Computer Science and Engineering
Cs.thapar.gurpreet@gmail.com

Dr.Sushil Garg
Department of Computer Science and Engineering
Sushilgarg70@gmail.com

***Abstract*: Wireless networks are highly imposed to threats rather than wired networks. There is always a possibility of attacks likesession hijacking, Man in the middle and so on. Honeypots are normally used to perform session highjack attack. In this attack, real users are attracted towards vulnerable access points and there is highjacked. In our work, a new approach is proposed based on sensor nodes to detect unreal access point which are applied in the network; these nodes have the responsibility of sensing the requests and response messages which are exchanged between APs and legitimate user. The ID of real access point is sensed and if it exists in the database, then network operation continues else sensor node generates alert.**

***Keywords*:** Session Highjacking, beacons, sensor, Access Point

I. INTRODUCTION

Wireless technologies these days enable all the devices to communicate with each other without the help of any physical medium like cabling. Due to their added flexibility and other characteristics like portability, scalability, improved bandwidth and low cost, there has been a tremendous increase in the deployment of WLANs. [1]. There are many advantages of these: Wireless system setup is troublefree and fast and there is less burden of wiring and cabling through floors and ceilings.It provides extensibility where wired ones can't reach. They offer more flexibility and reliability and adapt easily to changes. WLANs can be further classified into two main types.

Infrastructure Networks: In these type of networks, communication normally occurs between APs and the wireless nodes, but not directly. Static base stations are there and when the node goes beyond of the range of this base station; it enters in another one's range[2][3]. Infrastructure-based network consist of Cellular networks.[10]\

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

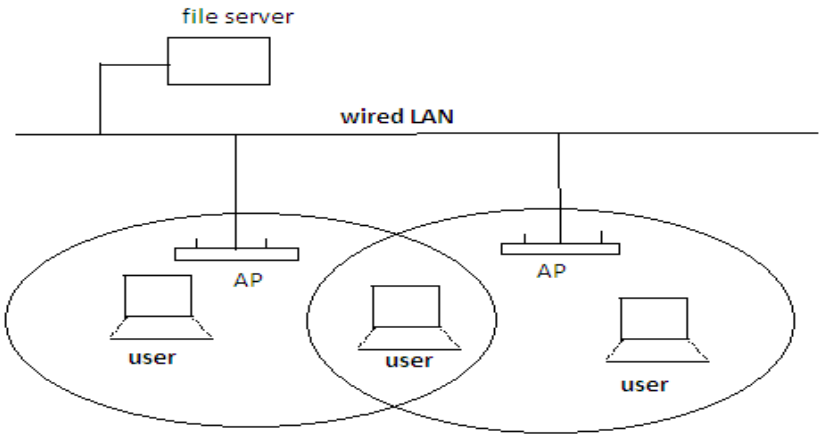

Figure1: Infrastructure Network[4]

Infrastructure less Networks: There is no need of any infrastructure for Ad-hoc wireless networks. Direct communication takes place between nodes so there is no requirement of access point controlling medium . There are no stationary routersand network's all nodes act as routers which means all nodes can move here and there and in an arbitrary manner, they can be connected. In the below figure, outer parts's nodesare out of each other's range. The node in the middle works as router and an ad hoc network has been formed by all nodes[10]

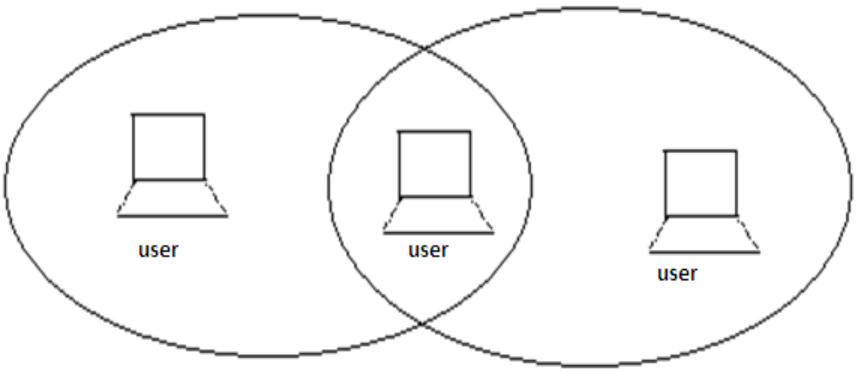

Figure2: An Infrastructure less Network[4]

Ad-hoc networks: Ad hoc networks are very flexible and they are not dependent on any pre-established infrastructure, which means they can be deployed anywhere and on any infrastructure. They are very useful in places with non-existing or damaged communication infrastructure and disaster recovery areas[10]. Main thing is Routing protocols which are used to forward the packets from one node to another. In mobile ad hoc network (MANET),devices cooperatively communicate with each other without any already established infrastructures like centralized access point. [9]

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

II. LITERATURE REVIEW

Security Concerns: Access Points have weaknesses and are easily captured by design mistakes and user interfaces like weak passwords[25]. Various attacks are possible due to these weaknesses.

Beacon Spoofing Attack:APs send notifications at regular intervals called as Beacons for synchronization [3]. Beacon frames are not protected and may be spoofed and masqueraded by the attacker. Figure below shows that the network can be flooded by the attacks froma large number of fake beacons along with legitimate beacons which leads to network congestion and performance deterioration [3]. The attack begins after spoofing the identity of legitimate AP. Then the attacker creates the virtual AP referred to as fake AP with same credentials as the original one. Then the interface of that soft AP comes into operation and starts producing large number of beacons along with the normal constant rate of the legitimate AP. This will flood the network and the client would be disconnected from the legitimate AP and then when it re associates it will be connected to the Fake AP[4][6]

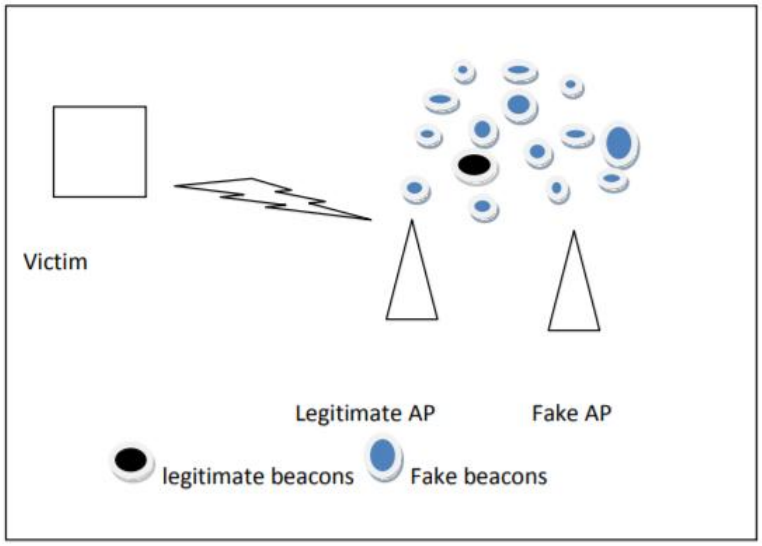

Figure3: Beacon Flood Attack

Sniffing: To monitor the health of a network, sniffing is used which helps in scanning for open access points which permits anyone to establish a connection and capture the passwords. Thus may serve as the way for detection of wireless threats but along with it this information gathering if done by the attacker is the cause of launch of a wide variety of attacks.Wireless networks are easier to sniff than wired ones.[5]

Wireless Spoofing: Wired and wireless networks both have well known techniques such as spoofing. An attacker can create frames by filling selected fields in them that has theaddress and id which imitates legitimate but actually it does not exist. [6]

Session Hijacking: A man-in-the-middle attack and favourite one for attackers. In this, authenticated user having valid session with the server is taken over by the attacker. An already authenticated user connected to a web server with valid session is taken over by

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

attacker by hijacking the session and makes the connection pretending to be legitimate. This has been very advantageous for attackers because they don't waste much time to crack a password and no need of dictionary attacks.[7][8]

III. PROPOSED METHODOLOGY

Two categories of attacks are there one are active and other are passive. And one of the active attack is called session hijacking which uses a technique called honey pot for attacks. The unreal access point becomes a honey pot. When any person connects to unreal AP, session hijacking attack can occur. If the fake APs are detected there is possibility to isolate session hijacking attack. In this work, novel technique is proposed to detect fake access point. First of all set up the network with wireless nodes, access points (AP). AP broadcast the beacon signals to show its presence to wireless nodes. A wireless node who wants to connect to AP, node make a probe request to AP, AP give reply back with probe response. There is possibility that attacker place fake AP in the network. Fake AP also broadcast the beacons signals, those wireless devices receive these signal they wants to attach this fake AP. Now a user is connected to the fake AP and the session between end user and server is hijacked. To overcome from this attack, a new methodology has been proposed in which network contains sensor nodes.These sensor nodes read all the com in the form of requests and replys.

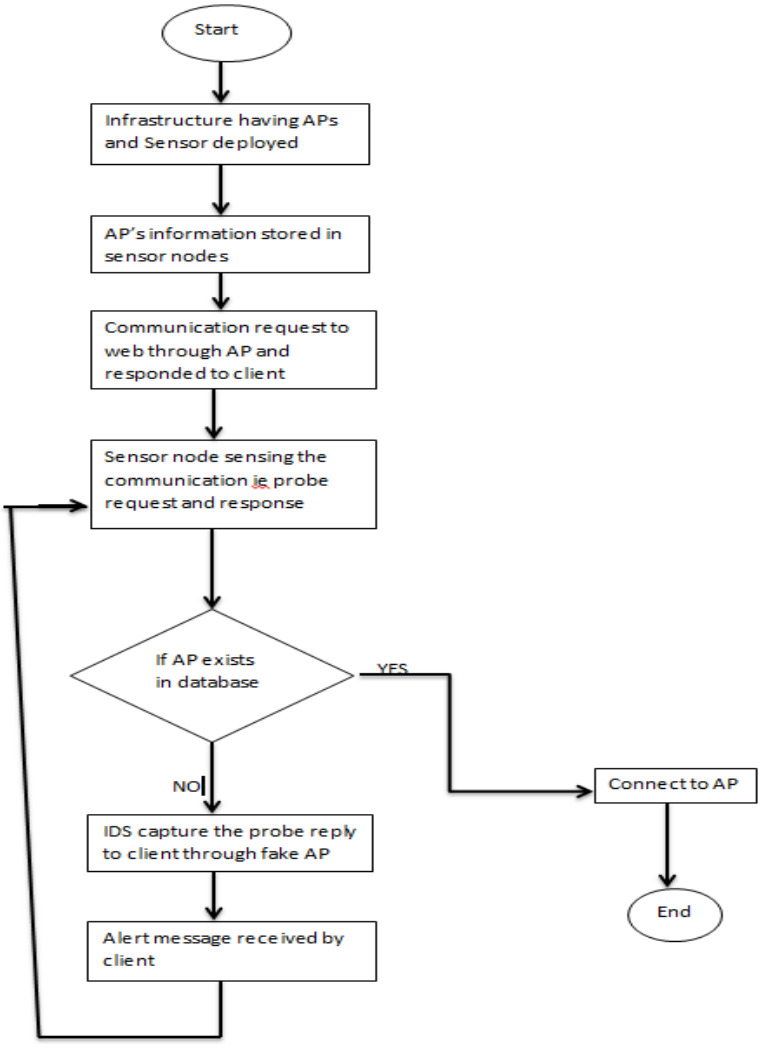

Figure4: Proposed Flowchart

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

IV. CONCLUSION

In this paper, we conclude that in wireless networks various typeof attacks are possible. The most common type of attacks which are possible is Man-in-Middle attack, Denial-of-service attack, Session Hijacking attack, Identity Spoofing attack. The session-hijacking attack can be easily implemented with honeypot. In this paper, through fake AP, session hijacking attacks is performed. The fake access point acts like honeypot. The fake access point is started by the legitimate users; no encryption technique is applied on access point so that maximum legitimate users can connect to fake access point. When any legitimate user connects to fake AP, its session will be hijacked by the other user who started the fake access point. To detect fake access point, novel technique is been proposed in this paper. The proposed technique is based on the sensor nodes. The sensor nodes are deployed in the network. In sensor node database identity information of the legitimate access points are stored. When any user try to connect with any access point, probe request and probe response message are sniffed by the sensor node. Sensor node verifies the properties of AP which is in sensed message, if it is successfully verified, normal operations on the network continues otherwise alert message is generated for the user which is connected to fake AP.

V. FUTURE SCOPE

The technique which is proposed in this paper for the detection of fake AP works well in all cases. The identity spoofing attack is possible in the proposed technique. Let suppose that if the fake access point spoofs the identity of legitimate access point, this technique fails. The second problem arise in novel approach is that, attacker can trigger security attack against the sensor nodes. To prevent identity spoofing attack many techniques have been studied. These techniques are like Access control list, Original identity hiding, MAC filtering and one way hash function. Every technique which is been discussed have certain disadvantages, like for implementing MAC filtering central controller is required , no central controller is present in our proposed technique. All the techniques which is been discussed for preventing identity spoofing will not be applied in our proposed technique. The efficient techniques are required for the proposed technique to prevent identity spoofing attack and attacks on sensor nodes.

VI. **R**EFERENCES

[1] Zhang, Ning and Lu, Shi, "Automatic detection of fake Wi-Fi access points", Technical Disclosure Commons, (February 28, 2019)
[2] Dondyk, E., Rivera, L., Zou, C.C.: Wi–Fi access denial of service attack to smartphone. Int. J. Secur. Netw. 8(3), 117–129 (2013).
[3] Chaudhary, A.; Kumar, A.; Tiwari, V.N., "A reliable solution against Packet dropping attack due to malicious nodes using fuzzy Logic in MANETs," Optimization, Reliabilty, and Information Technology (ICROIT), 2014 International Conference on , vol., no., pp.178,181, 6-8 Feb. 2014.
[4] Asier Martinez, UrkoZurutuza, Roberto Uribeetxeberria, Miguel Fernandez, Jesus lizarraga, Ainhoa Serna and Inaki Velez (2008).” Beacon frame Spoofing Attack Detection in IEEE 802.11 Networks”, In the proceedings of the third international conference on Availability, Reliability and Security (ARES08), pp 520-522, Barcelona, 4-7 th March.
[5] HosamRowaihy, SharanyaEswaran, Matthew Johnson, Dinesh Verma, AmotzBarNoy, Theodore Brown and Thomas La Porta, Pennsylvania State University; City University of New York; IBM T. J. Watson Research Center IEEE

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 9, NO. 4, APRIL 2010.

[6] KIRUTHIGA.S YUVARANI.G (2012) " 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

[7] MayankBansa[2012], Rajesh Gargi["A Study Comparison Between On-Demand Routing Protocols in MANET" International Journal Of Research In Computer engineering And Electronics. 1 Vol : 1 Issue :2

[8] SarojHirnwal, KirtiChauhan, Amit Gupta [2012] "Intrusion Detection Technique in Mobile Adhoc Network based on Quantitative Approach" International Journal of Computer Applications (0975 – 8887) Volume 37– No.8,

[9] Taebeom Kim, Haemin Park, Hyunchul Jung, and Heejo Lee (2012)"Online Detection of Fake Access Points using Received Signal Strengths" IEEE.

[10] Wei, T.-E., Mao, C.-H., Jeng, A.B., Lee, H.-M., Wang, H.-T., Wu, D.-J.: Android malware detection via latent network behavior analysis. In: The 2012 International Symposium on Advances in Trusted and Secure Information Systems (TSIS 2012), Liverpool, UK, pp. 1251–1258 (2012)

Copyright © 2019Authors