Volume 5, Issue 9, September 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Detection of Fake Access Point in Wireless LAN Network

Sandeep[1], Rachna Rajput[2]

[1] Student, Department of Computer Engineering, GKU, Talwandi Sabo, India

[2] Assistant Professor, Department of Computer Engineering, GKU, Talwandi Sabo, India

Abstract: With the fast increase in demand of the wireless LAN system over the cable system, a lot of network security threats have come into light. One of leading threat among these is Rogue access point (RAP) which if not considered and detected, can leak important and confidential information of the user. Most dangerous attack with this rogue access point is session hijacking which consists of exploitation of web session. Due to which a lot of stress is given on the detection and prevention of these fake networks. In this paper, we propose a sensor node and heartbeat monitoring methodology for the detection as well as prevention of these fake access points. Sensor Node technology works to detect and eliminate fake access points to prevent session hijacking and heartbeat monitoring further works to detect MAC address spoofing of the legitimate access point. We implemented our methodology by simulating it in Matlab tool and validate our results regarding detection and prevention of fake access points.

Keywords: MAC, ESSID, LAN, SSL

I. INTRODUCTION

Nowadays wireless network with IEEE 802.11 standard has become need as well as demand of the cooperative world. The employees have to use the Internet and intranet in their daily routine work. In such situations network security has become the important issue for such large enterprisers as very important and confidential data can be accessed through air by malicious users. The vilest loophole in IEEE 802.11 wireless standard is the presence of the rogue access points which can be created even upon the secure networks by the illegitimate users present in the wireless network to conduct man in the middle attack [rogue]. These illegitimate users crack the vital information of the companies without knowing the network administrator of the organization. Employees also make it easy for them by switching off the main security settings of their computers. These unauthorized access points are created by illegitimate user like honey pot to attract the legitimate users of the organization. Users are lured by giving them the free high speed internet access. Because of these hazardous effects, it becomes very crucial to detect as well as stop these fake access points for maintaining the security of the data. In this paper, we propose a novel approach to detect RAP's by sensing the network using sensor nodes and heartbeat monitoring technique. The detection of fake access points is done to prevent session hijacking which reveals the confidential and sensitive information of the legitimate users. Due to most important method of session hijacking called man in the middle attack the communication between devices is sniffed and transmitted data is captured. To protect sensitive information of the user sensor nodes are deployed in the network to sense RAP's. These sensor nodes stores the MAC address of the authentic access point and when the user sends the probe request to a access point, sensor nodes senses that probe request and matches its ESSID with its own database. If it is not matched, it notifies the user about the present fake access point. But smart crackers sometimes spoof the MAC address of the legitimate access point. For these cases heartbeat monitoring technique is implemented in addition to sensor nodes which prevent the MAC address spoofing of the authentic access point. In the world, no two devices are alive with same MAC address. So in this technique, users ping the access point if it replies the users that means access point is alive, no MAC address spoofing is done, but if time expires this shows access point is down. In this way heartbeat monitoring technique works to detect rogue access point even if MAC address of legitimate access point is spoofed.

The paper has been organized as follows. Section II describes the current approaches that have been used to detect the rogue access points. In section III, the problem statement is defined and also our approach to solve this problem is given with full details. Simulation results are presented in section IV. Then the conclusion is given in section V.

II. LITERATURE REVIEW

Rouge access point is one of the leading security threats in current networked environment. Now- a-days connecting devices without the use of cable have increased everywhere. In [2] Ganesh B. Bandal et. Al proposed a rouge detection algorithm. The proposed system consist of 3 main components:1) Access Point: the access point can operate in two modes: a) Normal Mode is the mode that the access point performs as the regular access point and b)Sniffer Mode is the mode that the access point performs as the wireless sniffer collecting surround wireless data. 2) Switch: the switch is a part of counter attack mechanism. Switch can disable the port to which the rogue access point is attaching 3) Central System, Central System includes all intelligent functions such as the access point mode switching, sniffing data collection, rogue access point identification and localization and switch port blocking.

In [3] Mr. ahmed proposed a method for investigating elimination of fake access point using skew intervals. The proposed work has been presented in three modules: detecting access points, finding fake access point, blocking the fake access point. Clock skew has been used to overcome the limitation of existing methods in detecting MAC.

In [4] author has designed a verifier on the internal wired network to send test traffic towards wireless edge, and uses wireless sniffers to identify rouge APs that relay the test packets. To quickly sweep all possible rogue APs, the verifier uses a greedy algorithm to schedule the channels for the sniffers to listen to. To work with the encrypted AP traffic, the sniffers use a probabilistic algorithm that only relies on observed packet size.

In [6] Hemanshu kamboj represented a new hybrid technique for detection of fake access point. The proposed technique is based on number of beacon frames received in fixed time according to the climate conditions. In this technique threshold for the beacon frames have been fixed which will help in identifying the fake access point in which beacon will increase/decrease the threshold.

In [7] author proposed a method to detect the session hijacking attack. The proposed will detect the fake access point .The proposed scheme will be based on using wavelet based analysis of the received signal strength. In this technique they developed a model which describes the changes in the received signal strength of the access point. In this technique they used an optimal filter to analyze the received signal strength

In [8] , author proposed a novel approach to detect the fake access point. The proposed technique is based on the two approaches .One is received signal strength and other is online algorithm. We compare the signal strength of the access point with the legitimate access point, if the received signal strength is less than the threshold signal strength then access point is fake otherwise not.

In [9] The users on the network are increasing drastically from last few years. The wireless networks are used now a days and it is much vulnerable to security attacks. The honey pots are used to perform session hijacking attack. The honey pots are used to monitoring and surveillance and gathering information and understanding the properties of the network. In this paper authors showed a survey results .In this survey for the 4 months honey pots are deployed in the area and different attacks came from the different countries and perform different type of attacks on the network. All the attackers will try to hack the secure SSL server by gathering the information using honey pots

In [10] Raheem beyah et. Al proposed a temporal traffic characteristic based technique for rouge access point detection. The proposed method is independent of signal range of rouge AP's. This technique, when used in conjunction with an allowed AP policy or access list, can easily identify rogues. Proposed approach is very costly and challenging to be implemented on large scale.

III. PROPOSED APPROACH

Network based attacks are very common these days which can produce halting of services and stealing or misleading important information of network users. In this dissertation we have defined protection against rouge access point in wireless LAN network. Rough access point has become very famous security threat in the field of wireless LAN as it does not require any special technical knowledge. In this type of attack no intrusion device is needed. If this kind of threats are not detected and mitigated on time the disaster caused by them will not be cured. The proposed methodology provides a technique to resolve with rouge access point. Rough AP's are started by illegitimate users, to steal the credentials of the legitimate users. When the legitimate clients are connected to rough AP, all the traffic are start passing through the machine of the illegitimate user and it hijack the sessions and other information's of the legitimate users. In this problem, we work on to detect rough AP's so that legitimate users will not connect to rough AP to prevent session hijacking Deploying a infrastructure with finite number of legitimate users. The main objective of proposed approach is to Design a sensor based technique for detecting fake access point for session hijacking and Designing a Mitigation methodology to prevent from rough access point.

IV. SIMULATION RESULTS

In this section we are going to show the simulation results. Simulation for the proposed approach has been done using nam (Network Animator). The figure below gives formation of scenario.

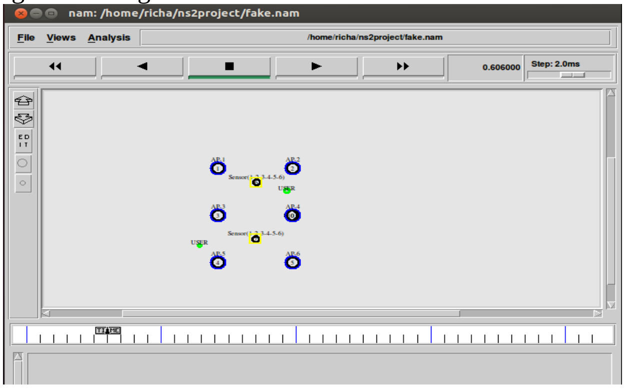

Figure 1: Formation of Proposed Scenario

Figure 2 shows the simulation of Fake access point in a network. From the figure you can see that user-PC had created a Fake access point and the whole data of user 2 is getting transmitted to user-PC by Fake Access point.

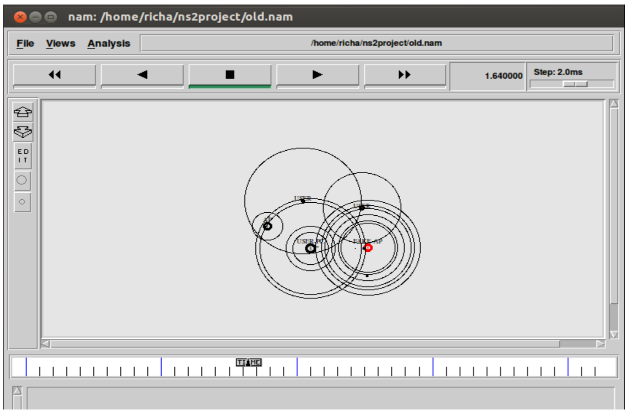
nam: /home/richa/ns2project/old.nam
File
Views
Analysis
/home/richa/ns2project/old.nam
1.640000
Step: 2.0ms
USER
USER
FAKE AP

Figure 5.5 gives the sharing of data among the users through access points in range.

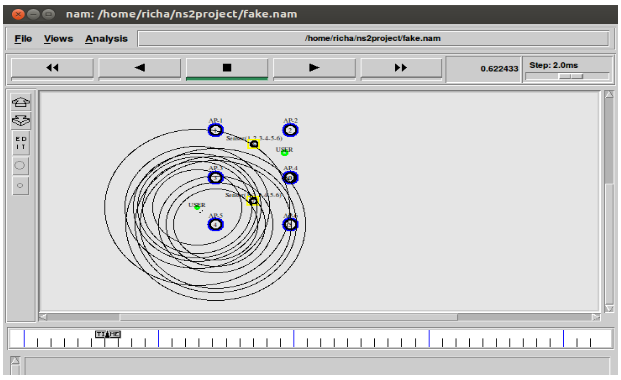

Figure 2: simulation of Fake access point

It can be viewed from the figure that connection authentication request had disconnected the fake access point from transferring the data through it.

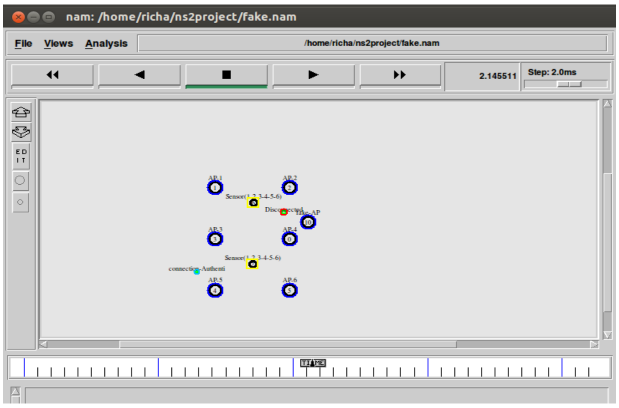

Figure 3: disconnection of fake access point

Figure 4 shows output of the algorithm in the form of graph. Graph is showing output for throughput as well as energy. Network throughput is the average rate of successful packet delivery over a communication channel.

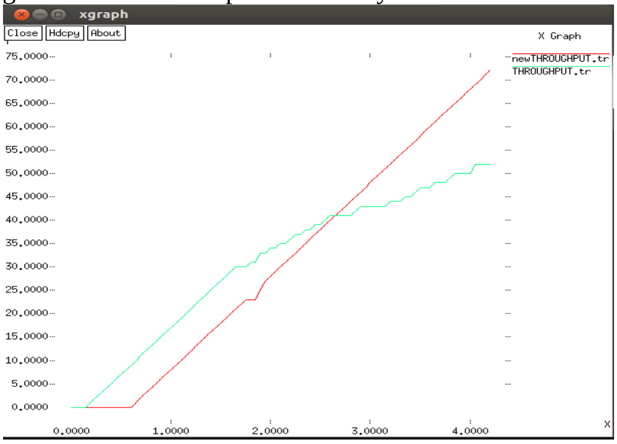

Figure 4: Graphical representation of throughput and energy

V. CONCLUSION AND FUTURE SCOPE

In our research work we have created a infrastructure based network. Here the routing information table has been used for the detection of unauthenticated fake access point. From the discussions in chapter 5 it has been concluded that rouge access point may lead to unusual loss of data of the user. By putting the proposed scenario to the old scenario the user can be saved from such loss of data. The transfer will be immediately disconnected as it starts using fake access point. So In proposed approach data can only travel through the access points having entry in routing table and a fake access point can’t be entered in the routing table. After analyzing the simulation results it could be said that proposed algorithm works efficiently over the previous approach. There is a minor packet loss in the proposed approach and throughput of proposed approach is much better in comparison with the existing one. So we can say this is a efficient method which could solve the problem of rouge access point.

Security is the most important concern in wireless networks. Further security can be improved by keeping the overheads simple.

REFERENCES

[1] Rogue Wireless Access Point Detection and Remediation

[2] Rogue Access Point Detection System in Wireless LAN

[3] Investigation: Elimination of Fake Access Points from WLAN Using Skew Intervals

[4] Detecting Protected Layer-3 Rogue APs, Department of Computer Science, University of Massachusetts Lowell

[5] “Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN - A Multi-Agent Sourcing Methodology and Skew Intervals: A Proposal”, International Journal of Engineering and Advanced Technology (IJEAT)ISSN: 2249 –8958,Volume-2, Issue-4, April 2013

[6] Hemanshu Kamboj,” Detection of Fake Access Point to Prevent Session Hijacking”, Vol. 1, Issue II, Mar. 2013, ISSN 2320-6802

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

[8] Online Detection of Fake Access Points using Received Signal Strengths” Taebeom Kim, Haemin Park, Hyunchul Jung, and Heejo Lee Div. of Computer and Communication Engineering Korea University Seoul, Korea

[9] ” Fast and accurate detection of fake points using non-crypto method in WLAN (2012)”, International Journal of Communications and Engineering Volume 05– No.5, Issue: 03 March 2012.

[10] RaheemBeyah,”Rogue Access Point Detection using Temporal Traffic Characteristics”, Communications Systems Center