IJCSE International Journal of Computer Science and Engineering Open Access
Survey Paper Volume-4, Issue-4 E-ISSN: 2347-2693

A Survey on Wireless Malevolent Access Point Detection Methods for WLAN

Punam Rajput[1*] and Prasad Kulkarni[2]

[1*,2]*Department of Computer Science and Engineering,* University Aurangabad, Maharashtra, India.

www.ijcseonline.org

Received: Mar/25/2016 Revised: Apr/04/2016 Accepted: Apr/17/2016 Published: Apr/30/2016

***Abstract*— In Current Trends many public places like bus stations, restaurant, malls etc. provides Wi-Fi connectivity to the users with free of cost. These public places having a device like wireless access point through which they provide service to the end users. . It is designed to utilize the existing wireless LAN infrastructure. These rogue access points (APs) expose the enterprise network to a barrage of security vulnerabilities in that they are typically connected to a network port behind the firewall. The growing acceptance of wireless local area network causes a risk of wireless security attacks. The attacker creates a malevolent access point to attract the users and perform attacks on user devices through WLAN. Malevolent access point is one of the serious threats in wireless local area network. We Study in this paper survey on recent different fake access point detection methods and identified their advantages and disadvantages.**

Index Term—FAP, WLAN , MITMA, Evil Twin Attatck.

I. INTRODUCTION

Wireless Local Area Network technology has major use in many fields and anywhere, easy access. The use of public Wi-Fi has reached at a level that is difficult to avoid. If the malevolent access point is undetected then it is an open door for an attacker to get sensitive information. Attackers take the advantage of undetected rogue access points to get a free internet, confidential information.

This paper focuses on important security issues of wireless network which is called as Malevolent Access point. This rest paper of the paper organized as follows. Section II describes back-ground details of access point. Describes literature survey about malevolent access point detection algorithms. Section III describes solution Pro-posed system presented, and hypothesis in section IV. Section V describes the methodology. Section VI discusses the results. We have concluded in section VIII. In Section IX scope for further research.

II. RELATED WORKS

The threat of Malevolent Access Point has attracted both industrial and academic researchers to work on this problem. There are some methods which focused on this problem.

Chao Yang and his colleagues have used Statistical technique based on TCP packets to compute their IAT to detect Malevolent Access Point. if client is connected to remote server through Malevolent Access Point and a normal Access Point that is two hop wireless channel, so this gives the idea to detect Fake attacks by separating one-hop and two-hop wireless channels from the user to the remote server. In this they have used two algorithms, first is Trained Mean Matching, in this they are using training technique to detect Fake attack. The second algorithm is Hop Differentiating Technique; it is a non-training-based detection algorithm in Which they are using particular theoretical value for the threshold to detect Fake attack. They have tested this method under different RSSI levels for the accuracy of the detection of Malevolent Access Point.

Table 1
Comparison of various Papers

Paper Topic	Author Name	Year of Publics	Weakness	Algo.
Who Is Peeping at Your Passwords at Starbucks? - To Catch an Evil Twin Access Point	Yimin Song, Chao Yang, and Guofei Gu	2010 IEEE	wireless infrastructures (e.g., 3G or WiMax)	Trained Mean Matching (TMM) and Hop Differentiating Technique (HDT).
Active User-side Evil Twin Access Point Detection Using Statistical Techniques	Chao Yang, Yimin Song, and Guofei Gu, *Member, IEEE*	2011 IEEE	Distance, Packet, Hop	Trained Mean Matching (TMM) and Hop Differentiating Technique (HDT).
A Novel Approach for Rogue Access Point Detection on	Somayeh Nikbakhsh, Azizah Bt Abdul Manaf, Mazdak	2012 IEEE	Only Client Side	Wireless IDS

Corresponding Author: *Punam Rajput,* poorajput29@rediffmail.com

the Client-Side	Zamani, Maziar Janbeglou			
Online Detection of Fake Access Points using Received Signal Strengths	Taebeom Kim, Haemin Park, Hyunchul Jung, and Heejo Lee	2012 IEEE	Distance	Classification of received signal strength
Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN Based on Agents Terminology and Skew Intervals: A Proposal	Mr. Ahmed Ayad Abdalhameed,	April 2013	A Proposal	clock skews
Investigation: Elimination of Fake Access Points from WLAN Using Skew Intervals	Mr. Ahmed Ayad Abdalhameed,	May 2013	Time & Cost	Skews Intervals
Wireless LAN Intrusion Prevention System (WLIPS) for Evil Twin Access Points	Sachin R. Sonawane	June 2013	Centerlise System	Jpcap
Elimination of Rogue access point in Wireless Network	Mr. Sandip Thite,	Dec 2013	Distances	RSS
Wireless LAN Intrusion Detection and Prevention System for Malicious Access Point	Prof. Sandip Patil	March 2015	SSID ,IP, MAC ID, etc	Authentication and De-Authentication rules

III. PROBLEM STATEMENT AND OBJECTIVES

Wireless Local Area Network

Wireless Local Area Networks are now days are the easiest solution for the interconnection of various mobile devices like Tablets, Mobile Phones, PDAs, etc.
The unauthorized access point is divided into two categories-

1. Rogue Access point – the term rouge AP has been used in more than one context in wireless security literature. It is installed or set by not only by the outside attacker but also authorized user on the network to take a more advantages of the network.

2. Malevolent Access point – It is set or installed by an outside attacker without knowing to an authorized user of the net-work. It is set up by a malevolent attacker for the purpose of malevolent behavior such as falsification, eavesdropping, steals the information.

IV. HYPOTHESIS

The applied results of Fake access points are present on both wired and wireless side of the network. The most of the research work carried out is based on data source from audit Trails, system calls and network traffic. Working on this problem of malevolent detection in different directions in two parts. First parts is of Industry solutions focusing on wireless only, Second parts is of academic researchers focused on wired side.

V. METHODOLOGY

Malevolent access point detection is a challenging task. Current algorithm are available for man in the middle attack and malevolent attack. Currently available techniques will not work for every scenario. Some techniques only used for detection, no prevention policy present with these techniques. We proposed a novel approach which considers Mac address, SSID and signal strength of the access point for deciding current access point is Malevolent access point or not. In this technique initially we need to filter 802.11 packets. For that we must capture the packets during wireless traffic analysis. We can use Air cracking i.e. freely available software tool. It is used to analyze the wireless traffic and to capture a packet. By using that we can filter all the wireless network packets and capture beacon and management frame. If packet subtype is 0 then it contains management frame and if it is 8 then it contains a beacon frame. There is some AP who blocks beacon frame so that here we consider both beacon and management frame.

The Successful wireless-side methods use sensors in the entire network to collect physical-layer and link-layer information to help detect and locate Fake access point in a distributed architecture. Though largely used across many enterprises WLAN, such sensors based sniffing method is costly.

VI. RESULT & DISCUSSION

Most existing commercial products take the first approach they either manually scan the RF waves using sniffers (e.g., Air cracking, Air Magnet, Nets tumbler) or automate the process using sensors. Automatic scanning using sensors is less time consuming than manual scanning and provides a continuous vigilance to malevolent access point. However, it may require a large number of sensors for good coverage, which leads to a high deployment cost. Furthermore, since it depends on signatures of APs (e.g., Internet Protocol, MAC address, SSID, etc.), it becomes ineffective when a Malevolent access point spoofs signatures. Three recent research efforts also use RF sensing to detect malevolent access point. In, wireless clients are instrumented to collect information about nearby APs and send the information to a centralized server for malevolent access point detection. This approach is not resilient to spoofing. Secondly, it assumes that malevolent access points use standard beacon messages in IEEE 802.11 and respond to probes from the clients, which may not hold in practice. Last, all unknown APs (including those in the vicinity networks) are flagged as malevolent access point, which may lead to a large number of false positives. The main idea of is to enable dense RF monitoring through wireless devices attached to desktop machines. This study improves upon by providing more accurate and comprehensive malevolent access point detection. However, it relies on proper operation of a large number of wireless devices, which can be difficult to manage. In contrast, our approach only requires a single monitoring point, and is easy to manage and maintain.

VII. RECOMMENDATIONS AND SUGGESTIONS

The Malevolent access point detection system has been a major research area because of increased use of wireless network. In this paper we proposed a novel approach for detection of malevolent access point.

VIII. CONCLUSION

In this Paper we Surveyed different recent malevolent detection methods or solutions presented by researchers. We have given disadvantages of particular solution, depth of accuracy of various solutions, Factors affecting the detection of such methods...etc. So, as the era of Wireless Environment is growing faster, we need more general solution against one of the serious threat of fake attack.

IX. SCOPE FOR FURTHER RESEARCH

Our current approach detects Malevolent Access Points using fake Broadcast packets. In case of network partitioning our approach will be able to detect Malevolent Access Points in any network.

ACKNOWLEDGMENT

I would like to take this opportunity to specially thank Computer Department, AEC, Beed, for vesting trust in me.

REFERENCES/BIBLIOGRAPHY

[1] W.wei,S.Jaiswal,J.Kurose and D.Towsley,Identifying 802.11 traffic from passive measurments using iterative Bayesian inference in Proc. IEEE INFOCOM **06,2006**.

[2] L.Watkins,R.Beyah, and C. Corbett, Apassive apporach to rogue access point detection,in Proc. IEEE INFOCOM **06,2006.**

[3] Active User-side Evil Twin Access Point Detection Using Statistical Techniques Chao Yang, Yimin Song, and Guofei Gu, Member, IEEE.

[4] Roth, V., Polak, W., Rieffel, E. Turner, T.,"Simple and effective defense against Evil Twin Access Points", WiSec'08, March **31–** April **2, 2008,** Virginia,USA**, 2008.**

[5] S. B. Patil, S. M. Deshmukh, Dr. Preeti Patil and Nitin Chavan, "Intrusion Detection Probability Identification in Homogeneous System of Wireless Sensor Network", International Journal of Computer Engineering & Technology (IJCET), Volume **3,** Issue **2, 2012,** pp**. 12 - 18,** ISSN Print**:** 0976 – 6367**,** ISSN Online**:** 0976 – 6375.

[6] Ajay M. Patel, Dr. A. R. Patel and Ms. Hiral R. Patel, "A Comparative Analysis of Data Mining Tools for Performance Mapping of WLAN Data", International Journal of Computer Engineering & Technology (IJCET), Volume **4,** Issue **2, 2013**, pp. **241 - 251,** ISSN Print**:** 0976 – 6367, ISSN Online**:** 0976 – 6375**.**

[7] Sandip Patil and Vanjale S.B,"Wireless LAN Intrusion Detection and Prevention System for Malicious Access Point ", Proceedings of the 9th INDIACom; INDIACom-**2015**; IEEE Conference,**11-13th** March **,2015**

[8] Sandip Patil, Sandeep Vanjale, "Wireless LAN Intrusion Detection System (WLIDS) for Malicious Access Point:" Goa Conference IRAJ, and **13** July **2014.**

[9] Sandip Patil and Sandeep Vanjale, "A Survey on Malicious Access Point Detection Methods for Wireless Local Area Network", IJCSE (E-ISSN**:** 2347-2693) Vol**.2,** Issue **3,** March **2014.**

Authors Profile

Rajput Punam Udaysing, Student of M.E Computer, AEC, Beed, Maharashtra, India. Author is a student of M.E. Computer Science and Engineering of Aditya Engineering College, Beed under Dr Babasaheb Ambedkar University Aurangabad. She had completed graduation in bachelor of engineering in Computer Science Engineering from Dr Babasaheb Ambedkar University Aurangabad.

Prof. Prasad Ramkrishna Kulkarni Research Scholar, Aditya Engineering College, Beed. Under Dr Babasaheb Ambedkar University Aurangabad. Author is a Research Scholar of CSE Department of Aditya Engineering College, Beed under Dr Babasaheb Ambedkar University Aurangabad. He had completed M.Tech in bachelor of engineering in Computer Science Engineering from Sana Engineering College, Kodad, Dist Nalgonda,HYD. University:-Jntu. Hyderabad.

