IJCSE International Journal of Computer Science and Engineering Open Access
Survey Paper Volume-2, Issue-3 E-ISSN: 2347-2693

A Survey on Malicious Access Point Detection Methods for Wireless Local Area Network

Sandip Patil[1*] and Sandeep Vanjale[2]

[1]*MTECH COMPUTER, BVDUCOE, Pune, Maharashtra, India, sandippatil82@gmail.com*
[2] Professor, PhD Student, BVDUCOE, Pune, Maharashtra, India, *sbvanjale@bvucoep.edu.in*

www.ijcaonline.org

Received: 5 March 2014 Revised: 14 March 2014 Accepted: 26 March 2014 Published: 30 March 2014

***Abstract*—** Wireless access points are today popularly used for the convenience of mobile users. The growing acceptance of wireless local area networks (WLAN) presented different risks of wireless security attacks. Now a day's in 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. The growing acceptance of wireless local area network causes a risk of wireless security attacks. The attacker creates a malicious access point to attract the users and perform attacks on user devices through WLAN. Malicious access point is one of the serious threats in wireless local area network. In this paper we have presented survey on recent different malicious access point detection solutions. We identified and compared their advantages and weaknesses.

***Index Term*—**RAP, WLAN , Man In Middle Attack, Wireless security, Malicious Attacker

I. INTRODUCTION

WLAN Security technology has major use in many fields. Wireless LAN has a wide range of applications due to its flexibility and easy access. The use of public Wi-Fi has reached at a level that is difficult to avoid. According to the poll conducted by Kaspersky's global face book pages 32 percent of the more than 1600 respondents said that they are using public Wi-Fi regardless of the security concerned. The Kaspersky study also discovered that about 70% of Tablet and 53% of the mobile phone users using free public Wi-Fi hotpots to go online. If the malicious 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 Malicious Access point. This rest paper of the paper organized as follows. Section II describes back-ground details of access point. Describes literature survey about malicious access point detection technique. 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 Malicious AP has attracted both industrial and academic researchers to work on this problem. There are some methods which focused on this problem.

Taebeom Kim and his colleagues used received signal strengths for detection of malicious access point, in this they measures correlated RSS sequences from nearby APs in order to determine whether the sequences are legitimate or fake or malicious. This method works in three phases. In phase one they are collecting RSS from nearby AP, In Second Phase they are doing normalization of collected RSSs, it estimates some missed RSSs, caused by some external factors and normalizes the estimated RSSs for generalization of a variety of wireless environments. In third phase they are determining which RSSs are highly correlated to others based on some empirical threshold value. They define that highly correlated RSS sequences as fake signals from a single device.

Chao Yang and his colleagues have used Statistical technique based on TCP packets to compute their IAT to detect Malicious AP. if client is connected to remote server through Malicious AP and a normal AP that is two hop wireless channel, so this gives the idea to detect Malicious 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 Malicious 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 Malicious attack. They have tested this method under different RSSI levels for the accuracy of the detection of Malicious AP.

Table 1
Comparison of various Papers

Paper Topic	Author Name	Year of Publics	Weak ness	Algo.
Who Is	Yimin	2010	wirele	Trained

Corresponding Author: *Sandip Patil, sandippatil82@gmail.com*

Peeping at Your Passwords at Starbucks? - To Catch an Evil Twin Access Point	Song, Chao Yang, and Guofei Gu	IEEE	ss infrastructures (e.g., 3G or WiMax)	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 the Client-Side	Somayeh Nikbakhsh, Azizah Bt Abdul Manaf, Mazdak Zamani, Maziar Janbeglou	2012 IEEE	Only Client Side	Wireless IDS
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)	Sachin R. Sonawane	June 2013	Centerlise System	Jpcap
for Evil Twin Access Points				
Elimination of Rogue access point in Wireless Network	Mr. Sandip Thite,	Dec 2013	Distances	RSS

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. As Wireless arena is growing rapidly users find it very convenient to use these devices to check mail, browse internet, etc. Such free services are available to the users through Wireless networks present at the public places like Coffee Shop, Airport, etc. Wireless networks further classify in two types: In the first the common network topology is that, where each node can reach to other node using radio relay systems having a big range. This topology doesn't use routing protocols. In Second network topology deploy radio relay systems as first one but each node in this has limited range so one node is using other node to reach another node which is beyond transmission range.

Wireless traffic encryption technique provides a security to wireless network using the wireless encryption protocol. Latest access points come with a built in wireless traffic encrypt ion technique. But the tools like Air cracking suite can be used by attacker to break the security of wireless network by monitoring wireless traffic.

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. Malicious Access point – It is set or installed by an outside attacker without knowing to an authorized user of the network. It is set up by a malicious attacker for the purpose of malicious behavior such as falsification, eavesdropping, steals the information.

IV. HYPOTHESIS

The effects of malicious 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 malicious 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

Malicious AP detection is a challenging task. Current techniques are available for man in the middle attack and malicious 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 malicious AP 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 Malicious AP in a distributed architecture. Though largely used across many enterprises WLAN, such sensors based sniffing method is costly.

VI. RESULT & DISCUSSION

Monitoring RF waves and IP traffic are two broad classes of approaches to detecting Malicious APs. Most existing commercial products take the first approach they either manually scan the RF waves using sniffers (e.g., Air Magnet, NetStumbler) or automate the process using sensors. Automatic scanning using sensors is less time consuming than manual scanning and provides a continuous vigilance to Malicious APs. 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., MAC address, SSID, etc.), it becomes ineffective when a Malicious AP spoofs signatures. Three recent research efforts also use RF sensing to detect Malicious APs. In, wireless clients are instrumented to collect information about nearby APs and send the information to a centralized server for Malicious AP detection. This approach is not resilient to spoofing. Secondly, it assumes that malicious 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 Malicious APs, 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 Malicious AP 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. The studies of detect Malicious APs by monitoring IP traffic.. The settings of their experiments are very restrictive. Furthermore, the visual inspection method cannot be carried out automatically. The technique in requires segmenting large packets into smaller ones, and hence is not a passive approach.

VII. RECOMMENDATIONS AND SUGGESTIONS

The malicious 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 malicious access point.

VIII. CONCLUSION

In this Paper we Surveyed different recent malicious detection methods or solutions presented by researchers. We have given weaknesses 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 malicious attack.

IX. SCOPE FOR FURTHER RESEARCH

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

ACKNOWLEDGMENT

I would like to take this opportunity to specially thanks Computer Department, B.V.U.C.O.E, Pune, for vesting trust in me.

REFERENCES

[1] Hao Han, Bo Sheng, Chiu C. Tan, Qun Li, Sanglu Lu, "A Timing-Based Scheme for Rogue AP Detection", 2011.

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

[3] 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.

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

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

[6] 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.

[7] 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.

[8] 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.

[9] Dipali D. Punwatkar and Kapil N. Hande, "A Review of Malicious Node Detection in Mobile Ad-hoc Networks", International Journal of Computer Sciences & Engineering (IJCSE), Volume 2, Issue 2, 2014, pp. 65-69, ISSN 2347-2693 (Online).

AUTHORS PROFILE

Sandip Vasantrao Patil, Student of M.Tech Computer, BVDUCOE, Pune, Maharashtra, India

Author is a student of M.Tech. Computer Science and Engineering of Bharati Vidyapeeth Deemed University,Pune. He had completed graduation in bachelor of engineering in Computer Science Engineering from Shivaji University,Kolhapur, Maharashtra, India in 2008.

Sandeep Vanjale Ph.D Student, BVDUCOE, Pune, Maharashtra, India

Author is a student of Phd. Computer Science and Engineering of Bharati Vidyapeeth Deemed University,Pune. He had completed graduation And M.Tech in bachelor of engineering in Computer Science Engineering..

