International Journal of Scientific and Technical Advancements
IJSTA
ISSN: 2454-1532

Detection and Mitigation of Rogue Access Point

Mehndi Samra[1], Mehak Mengi[2], Sparsh Sharma[3], Naveen Kumar Gondhi[4]
[1, 2, 3, 4]School of Computer Science Engineering, Shri Mata Vaishno University, Katra, India-180001
Email address:[1]mehndi.samra16@gmail.com, [2]mengimehak14@gmail.com, [3]sparsh_23june@yahoo.co.in, [4]naveen.gondhi@smvdu.ac.in

***Abstract*—**Wireless access points are popularly used nowadays for the ease of mobile users. The various risks associated with the wireless security attacks are presented due to growing acceptance of WLAN. Now a days Wi-Fi connectivity is provided to user at different public places and that to for free of cost. Every public place that provide Wi-Fi connectivity possesses a device like wireless access point through which the service is provided to the users. A rogue access point can be established by an attacker to lure the user and perform various attacks on the devices of a user through WLAN. Rogue Access Point is considered to be a serious threats in context to WLAN. In this paper we have presented survey on various rogue access point detection methods and their solutions. Identification of different rogue access point detection solutions along with the comparisons of their weakness and advantages are also discussed in this paper.

***Keywords*—**RAP; WLAN; MITM; anomaly detection system; honeypot; wireless security.

I. INTRODUCTION

As it is witnessed that WLAN Security technology has significant use in many fields. No doubt that there is a major weakness in wireless technology regarding the security, this is due to no control over the communication channel (the wireless medium). Wireless communication media is an open media where any user with a device that is fitted out with wireless interface can share and use the transmission medium with other users. A wide range of applications are carried out over WLAN, as it is easy to access and is flexible in nature. The extensive usage of public Wi-Fi has reached to such extend that is difficult to avoid. 32 percent of more than 1600 respondents use public Wi-Fi irrespective of concerned security, these statics have been provided by the poll that was conducted by Kaspersky's global face book page. Moreover, from the Kaspersky study it is discovered that about 72% of Tablet users and 56% of mobile phone users access free public Wi-Fi hotspots. Wi-Fi network is vulnerable to RAP (Rogue Access Point).

If the RAP is undetected then it will be like an open door for an attacker and an attacker can take advantage of undetected RAP to get sensitive information or to get a free internet, confidential information.

This paper presents an analysis of the most important and used security mechanisms that are implemented to overcome the security problem of wireless network which is Rogue Access point.

This paper focuses on important security issues of wireless network which is called as Rogue Access Point. The reminder of this paper is organized as follows: we describe the background details of access point along with the literature survey about rogue access point detection technique in section II. Section III explained the proposed system. Hypothesis are discussed in section IV. Section V comprises of Methodology. The results are discussed in section VI. Conclusion is presented in section VIII. The section IX comprises of scope for further research.

II. RELATED WORKS

Detecting a Rogue Access Point is a challenging problem as one has no cooperation from the RAP or offending system using the RAP. The threat of RAP has fascinated both industrial and academic researches to work on this problem. Taebeom Kim along with his colleagues used received signal strengths for detection of RAP. In this they measured the correlated RSS

Sequences from nearby APs so as to determine whether the sequences are legitimate or fake. This method works in three phases:

In the first phase there is collecting of all the RSS from nearby

APs, In second phase all these collected RSS are normalized and it estimates the missed RSSs, caused by some external factors and then estimated RSSs are normalizes for generalization of variety of wireless environment, In last phase it is determined which RSSs are highly correlated to other, which is based on some empirical threshold value. The highly correlated RSS sequences are considered as fake signals from single device [1].

Chao Yang along with his colleagues used a statistical techniques that was based on TCP packets to compute its TAT in order to detect Rogue Access Point. Wherever a client is connected to rogue access point and a normal access point that is two hop wireless channel, this in turn gives the idea to detect malicious attacks by just separating one-hop and two hop wireless channel, these channels are from user to remote server. The algorithms that are used are:

Trained Mean Matching, in which training techniques are used to identify the malicious attack and, Hop Differentiating Technique, in which non-training –based algorithm is followed, in this a particular threshold value is used in order to detect malicious attack. This method have been tested under different RSSI levels so as to get accurate result regarding the detection of Rogue Access Point [2].

The recent survey was done by Neha Agarwal and Shashikala Tapaswi, in which they detected the RAP using

Mehndi Samra, Mehak Mengi, Sparsh Sharma and Naveen Kumar Gondhi, "Detection and mitigation of rogue access point", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 195-198, 2015.

Shadow Honeynet. This detection of RAP using Shadow Honeynet comprises of three components:

Comparison of existing surveys.

PAPER TOPIC	AUTHOR NAME	WEAKNESS	ALGO.
Who is Peeping at your Passwords at Starbucks?- To Catch an Evil Twin Access Point	Yimini Song, Chao Yang, and Guofei	Wireless Infrastructures(e.g., 3G or WiMAX)	Trained Mean Matching (TMM) and Hop Differentiating Technique (HDT).
Active User-side Twin Access Point Detection Using Statistical Techniques [4]	Chao Yang, Yimini Song, and Guofei GU, Member, 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 Nikbakshi, Azizah Bt Abdul Manaf, Mazdak Zamani, Maziar Janbeglou	Only Client Side	Wireless IDS
Online Detection of Fake Access Points using Received Signal Strengths	Taebeom Kim, Haemin Park, Hyunchul Jung, and Heejo Lee	Distance	Classification of Received Signal Strength
Detecting and Eliminating Rogue Access Point in IEEE- 802.11 WLAN Based on Agents Terminolog y and Skew Intervals: A Proposal	Mr.Ahmed Ayad Abdalha meed	A Proposal	Clock skews
Investigation Elimination of Fake Access Points from WLAN Using Skew Intervals.	Mr.Ahmed Ayad Abdalha meed	Time and Cost	Skew Intervals
Wireless LAN Intrusion Prevention System (W LIPS) for Evil Twin Access Points	Sachin R.Sonawane	Centerlise System	Jpcap
Elimination of Rogue Access Point in Wireless Network	Mr. Sandip Thite	Distance	RSS
Wireless Rogue Access Point Detection Using Shadow Honeynet	Neha Agarwal, Shashikala Tapaswi	Connections are suspected by nature	Wireless IDS and Honeypot.

First component is Filtering engine, in which all the unauthorized traffic that is flowing towards the secure network is filtered. In this MAC spoofed APs are not detected, Second component is Anomaly detection sensors, in this analysis of characteristic of packets takes place, Third component is Shadow honeypot, in this the detectors are tuned towards the high sensitivity in order to increases false positive. The result of this stage is reflected back to low level stages in order to filter the harmful packets beforehand, if it is detected in future [3].

III. Problem Statement and Objectives Introduction

In this section, we state our RAP detection problem.

Wireless Local Area Network

WLANs are considered to be an easiest and best solution for interconnection of different mobile devices like Tablets, PDAs, Mobile Phones, etc. A drastic elevation in the growth of wireless arena has been witnessed and this is due to convenient usage of devices to check mails, browse internet and many more. These services are nowadays available to the end-users through

Wireless networks which is present at public places like at Airport, coffee shop, etc. Wireless networks are classified into two different types: The first type contains a common network topology in which each node can communicate with other node through radio relay systems that have big range. In this type of topology routing protocol is not used. While the second type contains radio relay system but in this each node has a limited range and so some other nodes are required as intermediator to reach to the node that is beyond the transmission range.

As far as the security of wireless network is concerned, wireless traffic encryption technique is used along with the wireless encryption protocols. Due to the rapid growth of wireless arena almost all the latest access point possesses the inbuilt wireless encryption technique. Wi-Fi network is vulnerable to RAP. Rogue Access Point is considered to be an unauthorized access point, the access point that is installed by the user without the knowledge of security administrator. RAP can be installed by the attacker that resides outside the organization or by authorized user. Rogue access point can categorized into four [5]:

- *Improperly Configured Access Point*: There can be minor or very little configuration mistakes which may lead to creation of rogue access point from the legitimate access point. The creation of such APs are mainly due to insufficient security knowledge with the network administrator, due to use of faulty AP' s driver or may be due to the reason that sometimes after the

Mehndi Samra, Mehak Mengi, Sparsh Sharma and Naveen Kumar Gondhi, "Detection and mitigation of rogue access point", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 195-198, 2015.

software updation, AP that was properly configured becomes vulnerable.

- *Unauthorized Access Point*: There are cases when an employee himself/herself install the AP in such a way that the network administrator is not aware of it. This is done in order to acquire flexibility, scalability and to sniff data and bandwidth.
- *Phishing Access Point*: If the unauthorized user installs an AP in order to obtain user's credentials like usernames and passwords by masquerading as an authorized user, this is termed to be as phishing access point.
- *Compromised Access Point*: In this the attackers are able to crack the key that is used in WEP and WPAPSK enabled network, this may lead to compromise. If an attacker finds out the key, then all the APs that are using same credentials are also compromised and this results into the Rogue Access Point.

The first three classes of RAP are easily detected but the last one class is most dangerous and difficult to detect.

IV. Hypothesis

The effect of rogue access point is witnessed on both wireless as well on wired network. The maximum research work that is carried out is grounded on data source that is received from the audit trails, network traffic and system calls. The problem of rogue access point detection is studied under two parts, first one focusses on wireless only through the industry solutions and the second one focusses on wired by the academic researchers.

V. Methodology

Detection of Rogue Access Point is a challenging task. The existing techniques were suitable for Man-In-The-Middle attack, Denial of Service attack and some malicious attacks but these current techniques will not fit into every scenario. We proposed a novel approach which includes the Mac address, SSID and signal strength of access point in order to decide whether the access point is rogue or not. In this technique initially we need to filter unauthorized access points and this is done by filtering component. At this stage MAC addresses of all the visible access point is matched against the list, which contains the list of MAC address of all the authorized access points. If there exist an access point whose MAC address doesn't match then that access point is considered to be rogue and is dropped. There can be a case where the MAC address is spoofed in order to get the MAC address of authorized access point, then the packet is passed to the anomaly detection sensors where different tools like Ettercap [6], Wireshark [7], Snort [8] and Anomaly detection heuristic payload sifting [9] are used in order to filter the unauthorized access point and detect different attacks. These attacks that can be detected are ARP spoofing, Man-in-the-middle attack, Denial-of-service (DOS) attack, Distributed denial of service (DDOS) attack and smurf like attacks. After the detection of attacks the packets are progressed to the shadow honeypot for validation. On the basis of the result obtained from anomaly detection and shadow honeypot a false negative and false positive rate is provided which in turn is passed back to filtering and detection stage for future detection of rogue access point [10].

VI. Result and Discussion

For the detection of Rogue Access Point the approach that is used is IP traffic. The traditional approach that was used for detection of RAP was either manually scanning of RF waves using sniffer, in which tools like NetStumbler and Air Magnet were used or by automatic scanning that uses sensors. Although the automatic scanning using sensor is less time consuming but it requires large number of sensors for good coverage and this leads to consumption of more cost and so is not cost efficient. As it depends on the AP's signature (e.g., SSID, MAC address, etc.) and if the signature is spoofed by the rogue AP then it results to be inefficient. In the last recent research which took place on 24 February 2015 used RF sensing to detect rogue access point. In this approach all the unauthorized access points with different MAC address, than that present in the list of authorized MAC address list are flagged as rogue, which in turn leads to large number of false positives. After the filtration stage detection techniques as anomaly detection sensors are used to detect the attacks present. The packets after the detection stage are passed to the shadow honeypot for validation. The result that is obtained from the last two stages that is from anomaly detection [11] and shadow honeypot decides whether the access point is rogue or not [12]. The result that is obtained from the shadow honeypot indicates the false positive and false negative rate, on the basis of which it is decided whether the access point is rogue or not. The result is then passed back to the filtering and detection stage for the future detection. The proposed approach improves the performance as the decline in the false positive rate takes place.

VII. Recommendations and Suggestions

Because of extensive usage of wireless in our day-to-day life, the system for detecting the rogue access point is considered to be a major area for research. In this paper we have proposed a novel approach for rogue access point detection.

VIII. Conclusion

In this paper, different recent surveys related to rogue access point detection method or solutions are presented. These surveys were presented by different researchers. We have specified the flaws of particular solution, depth of accuracy of various solutions, various factors that affect the detection of rogue access point. So, as the wireless arena is growing so fast, we need to come up with more feasible solution against one of the serious threat of malicious attacks.

References

[1] T. Kim, H. Park, H. Jung, H. Lee, "Online detection of fake access points using received signal strengths," 2012.

Mehndi Samra, Mehak Mengi, Sparsh Sharma and Naveen Kumar Gondhi, "Detection and mitigation of rogue access point", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 195-198, 2015.

[2] C. Yang, Y. Song, and G. GU, "Active User-side Evil Twin Access Point Detection Using Statistical Techniques,".
[3] N. Agrawal and S. Tapaswi, "Wireless rouge access point detection using shadow honeynet," Science + Business Media New York, Springer, 2015.
[4] V. Roth, W. Polak, E. Rieffel, and T. Turner, "Simple and effective defense against Evil Twin Access Points," WiSec'08, Virginia, USA, 2008.
[5] L. Ma, A. Y. Teymorian, and X. Cheng, "RAP: Protecting commodity Wi-Fi networks from rogue access points," *In The fourth international conference on heterogeneous networking for quality, reliability, security and robustness and workshops*, ACM, 2007.
[6] http://ettercap.github.io/ettercap/
[7] http://www.wireshark.org/
[8] http://www.snort.org/
[9] S. Singh, C. Estan, G. Varghese, and S. Savage, "Automated worm fingerprinting," *In Proceedings of the 6th Symposium on Operating Systems Design and Implementation (OSDI)*, 2004.
[10] J. Levine, R. LaBella, H. Owen, D. Contis, and B. Culve, "The use of honeynet to detect exploited systems across large enterprise networks," *In Proceedings IEEE Workshop on Information Assurance*, West Point, NY: United States Military Academy, 2003.

Mehndi Samra, Mehak Mengi, Sparsh Sharma and Naveen Kumar Gondhi, "Detection and mitigation of rogue access point", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 195-198, 2015.