Volume 6, Issue 7, July 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey on Detection of Fake Access Point in WLAN

Chhayadevi H. Khambalkar
Department of Computer Science & Engineering,
Bharati Vidyapeeth College of Engineering,
Shivaji University, Kolhapur, Maharashtra, India

Sandip V. Patil
Department of Information Technology,
Bharati Vidyapeeth Jawaharlal Nehru
Institute of Technology, Pune, MSBTE, Maharashtra, India

Abstract: Wireless LANs will greatly increase productivity and adaptability by providing anytime-anywhere access to business networks and systems. a similar properties that build WLANs thus convenient, however, can even leave them susceptible to misuse and attack by unauthorized or pretend devices. To safely tap the complete potential of WLANs, firms should take steps to search out and thrash these questionable Rogues. In this paper we are introducing the different research paper that we have studied during the analysis of this paper. Also this paper introduces the rogue access point detection, its challenges and solutions. There is an enormous risk for public Wi-Fi users being tricked into connecting to rogue access points. Rogue access point is one among the foremost serious threats in Wi-Fi, since it exposes an oversized variety of users to MITM and evil twin attack. Wireless access points (APs) are wide used for the convenience and productivity of Smartphone users. The growing popularity of wireless local area networks (WLANs) will increase the risk of wireless security attacks. A pretend AP will be set in any public areas so as to impersonate legitimate APs for substantiation.

Keywords: Wireless Security, Evil Twin Attack, Device Pairing, Rogue AP, Fake access point.

I. INTRODUCTION

Wireless LAN Security technology has wide range of use in many fields. Wireless LAN has a huge range of applications due to its tractability and easy contact. The use of public Wi-Fi has reached at that much level so it is difficult to avoid. According to the general study it is analyzed that about 70% of Tablet and 53% of the mobile phone users using free public Wi-Fi hotpots to go online. If the fake access point is undetected then it is an open door for an attacker to get sensitive information. Attackers take the advantage of undetected fake access points to get a free internet, confidential information. This paper focuses on important security issues of wireless network which is called as fake Access point.

II. LITERATURE SURVEY

In further studies, differentiating connection types is based on active measurements or certain assumptions about wireless links (such as very low bandwidth and high loss rates), which are not applicable to our scenario. Detection is difficult for users because the access point to which a user's device binds does not identify itself in a fashion that can be verified reliably by the user.

[1] "Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN - A Multi-Agent Sourcing Methodology", V. S. Shankar Sriram1, G. Sahoo, Krishna Kant Agrawal

It proposes a totally machine-driven idea (without any manual intervention) of detection and eliminating RAPs by applying the mobile Multi-Agents onto the network. We tend to are utilizing two completely different levels of mobile agents- Master and Slave Mobile Agents. For attaining the multi-agent sourcing methodology we extend the System design as mentioned. Firstly a master agent is generated on the DHCP-M server that is liable for control all the procedures of the authorization in Wireless Network. This Master Agent generates slave agents depends upon the quantity of active Access Points Connected to the Server at that moment of your time. These slave agents are then sent on the individual APs connected. Currently these slave agents are cloned on each Access Points are being sent to the each connect consumer system to the APs. Once the cloned salve agent at the consumer system detects any new Access purpose, it mechanically builds and sends data packet information of the Unauthorized AP to Clone Agent to the connected AP such as (SSID, MAC-Address, Vendors Name, and Channel Used). The Slave Agent at AP dispatches this data to its Master Agent on the Server. At the server the small print of the suspected AP is detected and matched therewith of the data kept into the repository regarding all the access points. If the data is matched and therefore the AP is found approved then a replacement slave agent is generated and send to it AP, rather if it's detected as a consumer MAC address, a disassociation frame is send to any or all APs to tell them to not connect with it, else if the main points doesn't match with the either of it then the MAC-Address of the AP is fetched from the data, the port at that the MAC-Address is connected is searched and so be blocked for any local area network traffic.

This multi agent based mostly design proved to not only establish however additionally eliminate the rogue access points fully. Our projected technique is extremely reliable and value effective, because it deals with multiple level of detection and doesn't need any specialised hardware device; implementation performed also supports our belief and results in a really effective methodology of complete removal of RAPs.

[2] "Rogue-Access-Point Detection Challenges, Solutions, and Future Directions" Raheem Beyah Georgia Tech, Aravind Venkataraman Cigital

RAPs are on around 20 % of all enterprise networks.1 Since APs have reached goods valuation, the appeal of deploying them in an unauthorized fashion has fully grown. Also, as a result of APs became significantly smaller, network administrators have difficulty visually detection them. This can be significantly true if an attacker uses a portable computer as an AP. unlike traditional attacks that initiate outside the network RAP insertion is most frequently because of within users. This apparently simple misfeasance will have important consequences because these rogue devices produce a back door to the network and threaten network security. This seemingly easy misfeasance will have important consequences; it creates a back door to the network, fully negating the numerous investments in securing the network. Many RAP detection approaches exist, however none are foolproof. Industry, government, and domain got to be aware of this drawback and promote progressive detection ways.

It creates a back door to the network, fully negating many investments in securing the network. Many RAP detection approaches exist, however none are foolproof. Industry, government, and domain have to be compelled to be aware of this drawback and promote progressive detection strategies.

[3] "A Novel Approach for Rogue Access Point Detection on the Client-Side", Somayeh Nikbakhsh, Azizah Bt Abdul Manaf, Mazdak Zamani, Maziar Janbeglou

There is an enormous risk for public Wi-Fi users being tricked into connecting to rogue access points. Rogue access purpose is especially serious threats in local area network, since it exposes a large range of users to MITM and evil twin attack. This paper planned a sensible technique that warns users to avoid connecting to the rogue access points. This technique compares the gateways and therefore the routes that a packet travels to work out whether or not an access purpose is legitimate or not. This technique will simply find Man-In-The-Middle and evil twin attack with none help from the local area network operator.

This paper is regarding about one among the security problems in wireless networks that are termed installation of unauthorized access purpose or rogue access purpose. Some researchers outline it as "wireless access point that's installed while not specific authorization from a local network management". The others define it as "Wi-Fi Access purpose that is setup by an attacker for the aim of sniffing wireless network traffic". During this paper we tend to use rogue access point we illustrate to the second definition.

The projected model may be a quite wireless Intrusion Detection System (Wireless IDS). The main approach during this work is utilizing consumer devices to perform scanning of rogue access point rather than Utilizing dedicated scanning devices. The second approach during this paper is to have one comprehensive resolution for all attainable rogue access points together with Man-In-The-Middle attacks and evil twin attacks. The projected methodology has the subsequent advantages compared to existing solution:

- Projected methodology will observe each MITM and evil twin attack.
- A user is often warned of a rogue access point to prevent being exposed to the attacker.

[4] "Online Detection of Fake Access Points Utilizing Received Signal Strengths", Taebeom Kim, Haemin Park, Hyunchul Jung, and Heejo Lee

This paper proposes a unique fake AP detection methodology to resolve the same issues within the client-side. The strategy leverages usual signal strengths (RSSs) and on-line detection algorithmic rule. Our methodology collects RSSs from close APs and normalizes them for correct measure. They calculate the similarity of normalized RSSs. If the resemblance between normalized RSSs is less than the fixed threshold value, it decides that the RSSs are generated from a pretend device. We will measure the optimum threshold value derived from the consecutive hypothesis testing. In experiment, once the fixed threshold value was two, actuality positive was over than 99 and therefore the false positive was less than 0.1% in 3 observations.

Our main contributions are as follows:

- To ensure the quality of a consumer, we tend to considered developing the pretend AP detection methodology on a restricted platform like a Smartphone.
- To ensure availableness to the client, our methodology discovers fake APs while not further observation devices or a network manager privilege in WLANs. Moreover, the method doesn't need modification of the AP device, and it will notice the fake APs even if their traffic is encrypted.
- For the light-weight methodology, we offer fixed threshold values for detecting the fake APs utilizing consecutive hypothesis testing to enable us to notice malicious APs while not learning tasks.

There are two constraints to the client-side methods: cumbersome processes and limited resources. Once the strategies plan to collect information, hard interval time incurs long processes to detect fake characteristics within the client-side. Moreover, the operational systems in smart phones offer restricted resources that may hardly be adopted within the client-side.

[5] "Active User-side Evil Twin Access Point Detection Utilizing Statistical Techniques", Chao Yang, Yimin Song, and Goofier Gu, Member, IEEE

It proposes to exploit fundamental communication structures and properties of evil twin attacks in wireless networks and to design new active, statistical and anomaly detection algorithms. Their preliminary evaluation in real-world widely deployed 802.11b and 802.11gwireless networks shows very promising results. It can identify evil twins with a very high detection rate while maintaining a very low false positive rate.

III. INTRODUCTION OF PROPOSED SYSTEM:

In short, our paper makes the following contributions:

- We propose a new light-weight user-side evil twin detection solution. Our technique doesn't have confidence “fingerprint” checking of suspect devices nor need a known approved AP/host list. Thus, this answer is especially attractive to traveling users.
- We propose to take advantage of the intrinsic communication structure and property of evil twin attacks. Moreover, we tend to propose two statistical anomaly detection algorithms for evil twin detection, TMM and HDT. Above all, our HDT improves TMM by removing the training requirement. HDT is proof against the setting modification like network saturation and RSSI fluctuation.
- We implement our techniques during a model system, ET-Sniffer (Evil Twin sniffer). We’ve got extensively evaluated ET-Sniffer in many real-world wireless networks, as well as each 802.11b and 802.11g. Our analysis results show that ET-Sniffer will discover an evil twin quickly and with high accuracy (a high detection rate and an occasional false positive rate).

We clearly declare that our designed ways cannot discover all kinds of man-in-the-middle attacks within the WLAN. In our preliminary work, our targeted drawback is evil twin AP detection, wherever the evil twin AP utilizes the conventional AP to connect to net. In fact, this drawback is so a very realistic threat featured by public WLANs provided at airports, hotels, libraries, or cafes, etc, as a result of it's simple for an attacker within the public space to induce free web access from public free Wi-Fi to launch such sorts of attacks.

[6] “An indirect Rogue Access point Detection System”, Qu, G. And Nefey M.M.(2010).RAPid. IEEE 978-1-4244-9328-9/10

Qu and Nefey gave new indirect Evil Twin access point detection system. They analyzed local round trip time (LRTT) information and designed a technique with many algorithms for locating wireless hosts effectively. Their work starts from passively scanning or observation network traffic to host discovery and detecting Client-side solution for Evil Twin access point. In this work, we tend to empirically analyzed intensive LRTT information and designed a light system - fast with many algorithms for effective wireless hosts detection. Ultimately, SYN, FIN, and ACK LRTTs will be compared against one another to find wireless hosts despite network speeds. The results show 1st time however merging 802.11n wireless technology will still be accurately separated from local area network hosts, while it continues to enhance.

In this work, we have a tendency to by trial and error analyzed intensive LRTT information and designed a light system - fast with many algorithms for effective wireless hosts detection. Ultimately, SYN, FIN, and ACK LRTTs will be compared against one another to find wireless hosts in spite of network speeds. The results show initial time however merging 802.11n wireless technology will still be accurately separated from local area network hosts, when it continues to boost.

[7] “Simple and effective defense against Evil Twin Access Points”. Roth V, Polak W, Rieffel E, and Turner T, (2008). WiSec’08, March 31–April 2, 2008, Alexandria, Virginia, USA.

Roth et al gave easy assurance mechanisms that facilitate the users or purchasers to observe an Evil Twin publicly web networks. This technique offers short authentication string protocols for commerce cryptographic keys. The little string proof is executed utilizing encryption the short strings as a sequence of colors, applied consecutive by the user’s device, and by the actual access purpose. The mechanism has negligible interface necessities and might be implemented cheaply on a good vary of mobile and wireless devices. We tend to design a proof of conception implementation and conducted a user study with it during a range of cafe’s in Palo Alto and metropolis.

Our aim was to design a mechanism to defeat evil twin attacks that would change a user to simply verify the reference to very little prior training or data. Following, the mechanism should be “psychologically acceptable”; in different words, it should be simple to understand and use by people that access the web from public locations. Similarly, we tend to needed to use a minimum of hardware so that our mechanism can be used even by little, cheap devices with restricted display capabilities.

IV. CONCLUSION

In this Paper we Surveyed different recent fake 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 time of Wireless Environment is growing faster, we need more general solution against one of the serious risk of fake access attack.

REFERENCES

[1] “Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN - A Multi-Agent Sourcing Methodology”, V. S. Shankar Sriram1, G. Sahoo, Krishna Kant Agrawal.

[2] “Rogue-Access-Point Detection Challenges, Solutions, and Future Directions” Raheem Beyah Georgia Tech, Aravind Venkataraman Cigital.

[3] "A Novel Approach for Rogue Access Point Detection on the Client-Side", Somayeh Nikbakhsh, Azizah Bt Abdul Manaf, Mazdak Zamani, Maziar Janbeglou.

[4] "Online Detection of Fake Access Points Utilizing Received Signal Strengths", Taebeom Kim, Haemin Park, Hyunchul Jung, and Heejo Lee.

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

[6] "An indirect Rogue Access point Detection System", Qu, G. And Nefey M.M.(2010).RAPid. IEEE 978-1-4244-9328-9/10.

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

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

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

[10] "Wireless LAN Intrusion Detection and Prevention System for Malicious Access Point",Sandip V Patil, March 2015.