Detection of Rogue Access Point Using Various Parameters

Sandeep Vanjale and P.B. Mane

Abstract The wireless local area network (WLAN) communication is a rapidly growing approach for data sharing. A wireless network provides network access to mobile devices. Benefits of WLAN are like flexibility, mobility, portability, imposes performance, and security requirements. Such communication brings new network security threats. Physical security of wireless networks is impossible because wireless network signals are unidirectional and can proceed out of intended coverage area. Intruder with an apt wireless receiver can snoop into the network still remaining virtually undetected. In a WLAN, the most important security apprehension is the presence of rogue access point (RAP). These RAPs can be definitely used by persons with inadequate security knowledge. Most of the security threats require an advanced technical knowledge or expensive intrusion devices. A RAP is a wireless AP, which is installed in a secure wireless network without network administrator permission. Such RAP allows intruder to do a man in the middle (MITM) attack. Existence of such RAP causes security threats in WLAN. The access point is very popular because of features like mobility, scalability, cost effectiveness, and ease of installation. Airtight report shows that lack of knowledge about secure wireless network causes number of security threats.

Keywords 802.11 · Rogue AP · Authorized AP · Network security

1 Introduction

The wireless local area network (WLAN) communication is a rapidly growing approach for data sharing. A wireless network provides network access to mobile devices. Benefits of WLAN are like flexibility, mobility, portability, imposes per-

Sandeep Vanjale (✉)
Department of Computer Engineering, BVDUCOE, Pune, India
e-mail: sbvanjale@bvucoep.edu.in

P.B. Mane
Department of Electronics Engineering, AISSMS, IOIT, Pune, India
e-mail: pbmane6829@rediffmail.com

S.C. Satapathy et al. (eds.), *Proceedings of the International Conference on Data Engineering and Communication Technology*, Advances in Intelligent Systems and Computing 468, DOI 10.1007/978-981-10-1675-2_69

formance, and security requirements. Such communication brings new network security threats. Physical security of wireless networks is impossible because wireless network signals are unidirectional and can proceed out of intended coverage area. Intruder with an apt wireless receiver can snoop into the network still remaining virtually undetected [1].

In a WLAN, the most important security apprehension is the presence of RAPs. These RAPs are which can be definitely used by persons with inadequate security knowledge. Most of the security threats require an advanced technical knowledge or expensive intrusion devices [2]. A RAP is a wireless AP, which is installed in a secure wireless network without network administrator permission. Such RAP allows intruder to do a man in the middle (MITM) attack. Existence of such RAP causes security threats in WLAN [3].

The access point is very popular because of features like mobility, scalability, cost effectiveness, and ease of installation. Airtight [4] report shows that lack of knowledge about secure wireless network causes number of security threats. On the basis of Gartner research, we can say that 20 % of WLAN worldwide have unapproved access points. Intruder can use an AP with a high broadcast power to cover-up as a authentic AP [5]. Mobile agents were used for RAP detection but it has the limitation that client permission is required to run code [6].

2 Related Works

i. Jana and Kasara proposed a server side solution using clock skews of access point in a wireless network. In this approach, clock skews are used as a fingerprint to detect RAP in a network. Clock skews are calculated using the time stamp values from the beacon frames. This approach cannot detect MAC spoofing and has a lack of accuracy and speed in the calculation of clock skews in TCP/ICMP [7].
ii. S. Nikbakhsh et al. proposed client side approach for the detection of MITM attack and Evil Twin attack performed by RAP. It checks routes and the gateways through which packet travels as well as easily can be implemented without modifying a network. It is easy to implement on mobile devices. But attacker can easily break the security by using sniffing programs [8].
iii. Chao Yang et al. proposed 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 802.11g wireless networks shows very promising results. It can identify evil twins with a very high detection rate while maintaining a very low false positive rate [9].
iv. Kim et al. proposed a client side approach using the concept of received signal strength (RSS) for RAP detection. In this method, highly correlated RSS sequences are collected in the wireless devices. After that the received signal is normalized and classified whether the collected signal is multiple or not. For

this, a sequential hypothesis technique is used. It is a lightweight solution to overcome the drawbacks of the client side approach. But in this technique, the distance between the client node and access points while calculating the signal strength was never considered. Distance affects the signal strength, hence reducing the effectiveness of this approach [10].

v. Han et al. proposed a timing-based scheme to detect RAP. It uses a client side approach, where the emphasis is on round trip time between the server and the user, to check whether the access point is authorized AP or not. The detection algorithm is effective and accurate, but only wireless traffic between AP and the station is considered to set the RAP. Large overhead due to the trade-off between the overhead and accuracy [11].
vi. Kao et al. proposed a client side RAP detection technique using bottleneck bandwidth analysis. It uses a passive packet analysis approach. It is based on bandwidth estimation using packet pair technology [12].

3 Limitations of Existing Methods

Following limitations were found in the existing methods by reviewing the above referred papers:

i. **Clock Skew Solution**: It is assumed that first, the authorized AP will be activated and then the malicious AP. But this assumption is weak, as one cannot control which AP will be activated first.
ii. **Inter Packet Arrival Time**: Can be used to detect RAPs, but it is not effective in case when Evil Twin is present [13].
iii. **Mobile Agent Code**: Mobile agent code is small, which is installed on a mobile device for the purpose of detecting RAP. But a mobile agent code cannot be installed without client permission, which results into a major drawback of this method [14, 15].
iv. **MAC Address & SSID**: SSID and MAC address is used to detect RAP. These properties can be spoofed by using many tools available on internet.
v. **RSS Level**: RSS of the access point is used by various methods to detect RAPs. But variations in RSS levels cause variation in results [16].
vi. **Wireless Traffic**: In wireless environment, network traffic can provide inaccurate results. Such inaccurate results create a suitable environment for RAP to perform attacks [17].
vii. **Workload of Access Point**: The effectiveness of detection of RAP is affected by the workload at the access point.

viii. **Server Side Approach**: The major drawback with the server side approach is that, if the central server is not available or compromised, then the system will not work properly. If client node is out of the reachability of a server then server cannot provide service to client. The server side approach is expensive, limited and cannot work for many real life scenarios [18].

Above vulnerabilities are observed in the existing methods, using which intruders perform various attacks on WLAN. These vulnerabilities can be eliminated by using multiple parameters for RAP detection.

4 Rogue Access Point Detection Parameters

4.1 SSID

SSID is a short form used for Service Set Identifier. SSID consist of 32 characters. In one network there can be multiple SSID's. There can be multiple access points having the same SSID in single network. Without SSID's it is difficult to communicate and interact with one another.

4.2 MAC Address

MAC address is a short form used for media access control. MAC address is used for communicated in between physical network segment and MAC address is assigned to network interfaces. It is a unique identifier.

4.3 RSSI

RSSI is known for received signal strength indicator. The quality of communication between the sensor unit and the access point is indicated by the RSSI value and it is expressed as decibels (dB). The RSSI values are always negative number because of low power levels and attenuation of free air. RSSI values can vary from 0 to −100. The value near to 0 signifies strong signal, whereas the value approaching −100 indicates weaker signal [19].

4.4 Channel and Frequency

Wireless channels are used to convey information signals from one network to another network. Channels can transmit the information signals from senders to receivers. The transmitting capacity of the channel is measured in bandwidth in Hz or its data rate in bits per second.

Wireless network consist of 13 channels which are unlicensed. Each channel has its own unique frequency from 2412 to 2484 MHz with difference of 5 MHz.

4.5 Authentication Type

User in any network wants security of its data being transferred from one source to destination. Transmission protocols and policies are known as authentication. Authentication types are given below:

4.5.1 WEP

WEP is a short from of wired equivalent policy. WEP is an older method of security used in case of older devices and it is easy to hack. So it is not used widely.

4.5.2 WPA

WPA is a term used in short form for Wi-Fi protected access. WPA provides guaranty to the user that only authorized people should have access to it. WPA is sub divided in two parts first one is WPA 1 and other is WPA 2.

4.5.3 WPA 2-PSK

PSK is term used for pre-shared key. This is the latest protocol used today for Wi-Fi security.

4.5.4 802.1X Authentication

It enhances security for 802.11 wireless network. It provides network access with validity [19].

4.6 Radio Type

IEEE has prepared different standards for wireless network with a suffix letter and it covers every standard including security aspects and quality service, e.g., 802.11a/b/g/n/ac.

5 System Architecture

In this system, Wi-Fi scanner scans all access points in the network. Access points in the network broadcast beacon frames after specific time. Capture beacon frame from each access point. From each beacon frame SSID, MAC address, Channel and frequency, RSSI of access point is extracted. This captured information is stored in whitelist.

Administrative login compares new AP parameter details with whitelist AP parameter values and sort authorized AP, unauthorized AP and Rogue AP in wireless network. Access point is scanned periodically and checks properties of access point from whitelist. We have used different parameters like SSID, MAC Address, Authentication type, Channel, Frequency, and Power (RSSI) for detection of RAP.

If SSID is same then check MAC address. If MAC address is also same then check authentication type. If authentication type is same then check channel & frequency of access point. If anyone parameter from all parameters is mismatch with whitelist content then declare that access point as rouge access point (Fig. 1).

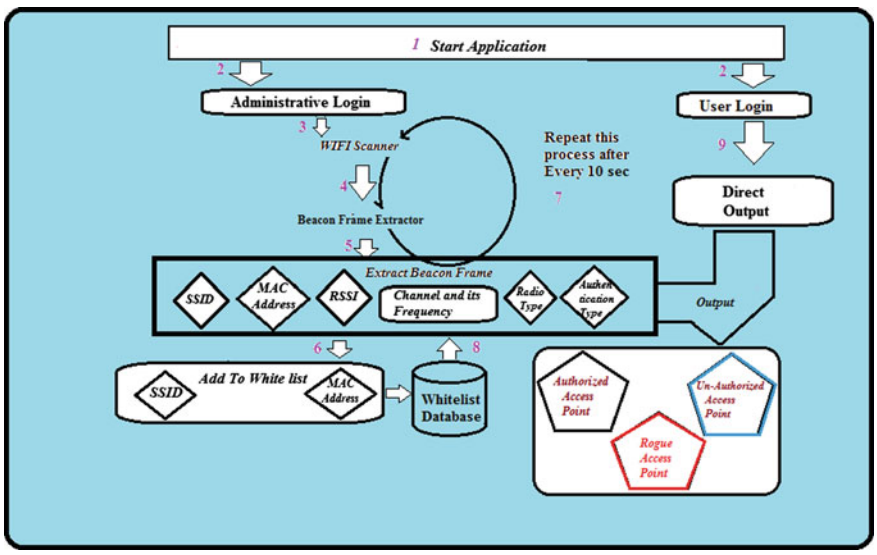

Fig. 1 Architecture of system

Table 1 List of all authorized and unauthorized access points present in network

Id	SSID	Authentication	MAC	RSSI	Channel	Frequency (MHz)	Radio_type	AP_type
1	Amit	Open	e8:de:27:50:45:d3	−30	6	2437	802.11n	Authorized
2	Paras123	WPA-Personal	5c:3c:27:o6:f6:67	−35	11	2462	802.11g	Unauthorized
3	Tataphtn3G	WPA-Personal	0a:1e:58:a0:c4:78	−26	6	2437	802.11n	Unauthorized
4	Sandeep123	WPA-Personal	5e:93:ac:b5:8f:44	−20	9	2452	802.11n	Authorized

Table 2 Rogue access point detection due to variation in RSSI

Id	SSID	Authentication	MAC	RSSI	Channel	Frequency (MHz)	Radio_type	AP_type
1	Amit	Open	e8:de:27:50:45:d3	−30	6	2437	802.11n	Authorized
2	Paras123	WPA-Personal	5c:3c:27:o6:f6:67	−35	11	2462	802.11g	Unauthorized
3	Amit	Open	e8:de:27:50:45:d3	−60	6	2437	802.11n	Rogue AP
4	Sandeep123	WPA-Personal	5e:93:ac:b5:8f:44	−20	9	2452	802.11n	Authorized

Table 3 Rogue access point detection using MAC address

Id	SSID	Authentication	MAC	RSSI	Channel	Frequency (MHz)	Radio_type	AP_type
1	Amit	Open	e8:de:27:50:45:d3	−30	6	2437	802.11n	Authorized
2	Paras123	WPA-Personal	5c:3c:27:o6:f6:67	−35	11	2462	802.11g	Unauthorized
3	Amit	Open	0a:1e:58:a0:c4:78	−40	6	2437	802.11n	Rogue AP
4	Sandeep123	WPA-Personal	5e:93:ac:b5:8f:44	−20	9	2452	802.11n	Authorized

Table 4 Rogue access point detection due to variation in RSSI

Id	SSID	Authentication	MAC	RSSI	Channel	Frequency (MHz)	Radio_type	AP_type
1	Amit	Open	e8:de:27:50:45:d3	−30	6	2437	802.11n	Authorized
2	Paras123	WPA-Personal	5c:3c:27:o6:f6:67	−35	11	2462	802.11g	Unauthorized
3	Amit	Open	e8:de:27:50:45:d3	−60	6	2437	802.11n	Rogue AP
4	Sandeep123	WPA-Personal	5e:93:ac:b5:8f:44	−20	9	2452	802.11n	Authorized

6 Results

Wi-Fi scanner captures the beacon frame. Following parameters values are extracted from the captured beacon frame (Table 1).

After giving authorization to access points, the result shows as they are authorized or unauthorized. If APs parameter value is changed by attacker then it becomes rogue access point (Tables 2, 3 and 4).

7 Conclusion

In this implemented solution, rogue access point is detected using various parameters. To detect RAP we have used various parameters like SSID, MAC address, RSSI value, channels and frequency, authentication, radio type, etc. It also detects MAC address and SSID spoofing attack with less false positive and false negative rates.

References

1. ia Sie Tung, Nurul Nadia Ahmad, Tan Kim Geok: Wireless LAN Security: Securing Your AP, IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.5B, May 2006.
2. Beyah, R.; Venkataraman, A.: Rogue-Access-Point Detection: Challenges, Solutions, and Future Directions, IEEE Security & Privacy, vol.9, no.5, pp. 56,61, Sept.-Oct. 2011.
3. Gaogang XIE, Tingting HE, Guangxing ZHANG: Rogue Access Point Detection Using Segmental TCP Jitter, WWW 2008, April 21–25, 2008, Beijing, China. ACM 978–1-60558-085-2/08/04.
4. www.airmagnet.com.
5. www.netstumbler.com.
6. M. Asaka, S. Okazawa, A. Taguchi, and S. Goto: A Method of Tracing Intruders by Use of Mobile Agents, San Jose, USA, June 2005.
7. S. Jana and S. Kasera: On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews, IEEE Transactions on Mobile Computing, vol. 9, no. 3, March 2010.
8. Nikbakhsh, Somayeh, Azizah Bt Abdul Manaf, Mazdak Zamani, and Maziar Janbeglou: A novel approach for rogue access point detection on the client-side. In Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on, pp. 684–687. IEEE, 2012.
9. Yang, Chao, Yimin Song, and Guofei Gu: Active user-side evil twin access point detection using statistical techniques. Information Forensics and Security, IEEE Transactions on 7, no. 5 (2012): 1638–1651.
10. Kim, Taebeom, Haemin Park, Hyunchul Jung, and Heejo Lee: Online Detection of Fake Access Points Using Received Signal Strengths. In Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th, pp. 1–5. IEEE, 2012.
11. Hao Han and Sanglu Lu: A Timing-Based Scheme for Rogue AP Detection, IEEE Transactions on Parallel and Distributed Systems, vol. 99, no. 1, pp. 5555. ISSN: 1045–9219, 04 Apr. 2011. IEEE computer Society Digital Library.

12. Kao, Kuo-Fong, I-En Liao, and Yueh-Chia Li.: Detecting rogue access points client-side bottleneck bandwidth analysis, computers & security 28, no. 3 (2009): 144–152.
13. Shafiullah Khan, Noor Mast and KokKeong Loo, Ayesha Salahuddin: Cloned AP Detection and Prevention Mechanism in IEEE 802.11 Wireless Mesh Networks, Journal of Information Assurance and Security 3 (2008) 257–262.
14. Kannadiga, Pradeep, and Mohammad Zulkernine, DIDMA: A distributed intrusion detection system using mobile agents. First ACIS International Workshop on Self-Assembling Wireless Networks. SNPD/SAWN 2005. Sixth International Conference on, pp. 238–245. IEEE, 2005.
15. G. Helmer, J. Wong, Y. Wang, V. Honavar, and Les Miller: Lightweight Agents for Intrusion Detection, Journal of Systems and Software, Elsevier, vol. 67, pp. 109–122, 2010.
16. Liran Ma, Amin Y. Teymorian, Xiuzhen Cheng, Min Song: RAP: Protecting Commodity Wi-Fi Networks from Rogue Access Points. Supported by National Science Foundation grant CCF-0627322.
17. Bo Yan, Guanling Chen, JieWang, Hongda Yin: Robust Access Point Detection Using Segmental TCP Jitter, WWW 2008 Published online 1 November 2008 ©Springer Science + Business Media, LLC 2008.
18. S. Srilasak, K. Wongthavarawat and A. Phonphoem: Integrated Wireless Rogue Access Point Detection and Counterattack System, International Conference on Information Security and Assurance, (2008).
19. Chougule, S. B. Vanjale et al.: Detection and Prevention of Rogue Access Point in the 802.11 Using Various Parameters, International Journal of Advanced Research in Computer Science and Software Engineering 5(5), May-2015, pp. 1723–1727.