Scheme of Rogue AP detection in managed WLAN based on AP's location

Kwontaek Lim, Jiawei Shao, Jonghoon Lee, Souhwan Jung
(*School of Electronic Engineering, Soongsil University, Seoul 156-743, Korea*)

Abstract: A scheme of rogue access point(Rogue AP) detection based on AP's localization is proposed. Global position system(GPS) information and received signal strength(RSS) information are used to get the location of AP in a smartphone, which is compared with the database located in a remote server. The proposed scheme can detect not only fake access point (Fake AP) but also Evil Twin AP. It can be a user-oriented solution to detecting Rogue AP threats, and users can use it flexibly.

Key words: rogue access point(Rogue AP); wireless local area network(WLAN) security; Evil Twin attacks

CLD number: TP926 **Document code**: A
Article ID: 1674-8042(2012)04-0370-04 **doi**: 10.3969/j.issn.1674-8042.2012.04.014

Wireless local area network(WLAN) have been the outcome resulting from the combination of computer and wireless communication technologies since 1990s, which provides flexibility and mobility for communications. As the effective way to access Internet, it has been widely used in many areas. However, due to the particularity of the wireless network, information is transmitted on the air, and it is easy for the attacker to monitor or destroy packets. The wireless security seems to be remarkable. For most companies, WLAN is usually located behind the firewall. So once hackers break the firewall, they can use it as the springboard to attack the internal network. At the same time, IEEE802.11, the market leading role, has potential safety hazard, which makes situation of WLAN security be even worse.

There are many kinds of WLAN threats, such as man-in-middle, session Hijacking, denial of service (DoS) and so on. Most of them are operated on the condition of Rogue APs. And many real cases show that Rogue AP is one of the most challenging security issues in WLAN. Nowadays, there have been many solutions to detecting Rogue APs, which can be regarded as the administrator-oriented or user-oriented. The most common administrator-oriented solution is wireless intrusion petection system (WIPS), which uses sensors to monitor the radio spectrum on the air and then compares some characteristics to decide Rogue APs. It is usually be used in big companies because of high cost. Furthermore, the existing user-oriented solutions which use round trip time(RTT) or watermarked packet only can detect Evil Twin. In this paper we propose a novel user-oriented scheme using AP's localization to detect Rogue APs in public areas. Our solution mainly works on Managed WLAN. It can not only detect Evil Twin, but also detect Fake AP.

The rest of the paper is organized as follows: Section 2 describes related work to detect Rogue APs. Section 3 gives the proposed scheme. Finally, section 4 concludes the paper and describes future work.

1 Related work

Recently, there have been many researches on Rogue AP detection methods, most of which can be divided into administrator-oriented or user-oriented solutions.

1.1 Administrator-oriented detection

Administrator-oriented solutions need a centralized system to collect, detect and manage information, such as WIPS/WIDS (wireless instrusion detection system) solution.

WIPS is widely used in many enterprises, which uses sniffers to monitor the radio spectrum on the air and then compare some characteristic to decide Rogue APs. Recently there are many sniffers available, such as AirDefence, AirMagnet and Airwave, but they are very expensive. To improve the expens-

* **Received data**: 2012-08-15
Foundation item: The KCC(Korea Communications Commission), Korea, under the R&D program supervised by the KCA(Korea Communications Agency) (KCA-2012-08-911-05-001)
Corresponding author: Souhwan Jung (souhwanj@ssu.ac.kr)

ive deployment of sensors, Branch J W et al.[1] and AirWave's wireless management suite[2] provided solutions which employed the existing wireless devices on the network (the APs) to sniff the areas within their ranges. However, Bahl P et al.[3] showed that the method could not completely sniff the entire network space with the existing APs and other wireless devices. There may be Rogue APs in a dead angle, where they can not be found.

Yeo J et al.[4] improved the performance of wireless monitoring by merging packet captures from multiple network sniffers and carefully selecting sniffer placement.

For the characteristics to distinguish Rogue APs from legitimate ones, WEI Wei et al.[5] proposed a method by examining the arrival time of consecutive acknowledgement(ACK) pairs in transmission control protocol(TCP) traffics. They built a classifier based on a sequential hypothesis test for the automated online detection of remote access points (RAPs). However, the use of ACK pairs limits this technique to TCP traffic.

Jana S et al[6] obtained time stamps from the 802.11 beacon frames and used the clock skew variation between nodes to identify RAPs. They assumed that the RAP was connected directly to the wired network. So they calculated every AP's clock skews by collecting their beacons and probe messages. If any AP's clock skew was different from the existing clock skews in the database, the AP was then identified as a Rogue AP.

There are also some researches using AP localization to detect Rogue APs. Spencer J et al.[7] presented a framework by identifying potential threats in this way. The specific goal was to apply an artificial neural network (ANN) to monitoring wireless radio signals in order to detect location trend. The typical wireless network users would use their devices in a predictable pattern of locations. It would be possible to map the physical locations of users and train an intelligent system with the existing location patterns. By developing the established usage information, it would then be possible for the intelligent system to pinpoint anomalies in wireless locations.

Laurendeau C et al.[8] provided a mechanism to probabilistically delimit the location of a wireless network malicious insider to a candidate area. A large scale path loss model was used to construct a probable distance difference range between a rogue transmitter and a pair of trusted receivers. Hyperbolas were constructed at the minimum and maximum bounds of this range to delineate the position of a rogue with a given confidence level.

1.2 Administrator-oriented detection

User-oriented solutions allow the user to independently determine whether an AP is a Rogue AP without assistance from the WLAN administrator. It can be implemented on wireless devices, such as laptops, mobiles and pads.

Some authors in Refs.[9] and [10] utilize round trip time of TCP traffic to detect Rogue APs. If the node is connected through the Rogue AP, it will take two wireless hops to reach the wired-network, instead of one. The added delay will be visible in the round-trip time. However, the round-trip time is changed with the network type, speed and congestion level.

SONG Yi-ming et al.[11] also exploited the communication structure and property of Evil Twin attacks. In the Evil Twin AP scenario, the victim client communicates with a remote server through an Evil Twin AP and a normal AP. Obviously, compared with the normal AP scenario, the Evil Twin AP scenario has one more wireless hop. This can be seen by using the inter-packet arrival time(IAT).

Monica D et al.[12] proposed a solution which was different from previous work, which did not depend on timings to detect a multi-hop setting in Evil Twin attack. In this solution, the user sends a watermarked packet to the echo server, and then listens to different channels. If an Evil Twin attack is being launched, the watermark will necessarily appear on the wireless link between the Evil Twin and the legitimate APs. As we discussed before, the existing user-oriented solutions can not detect Rogue APs directly connected to the wired network.

2 Problem statement

Our solution can detect Rogue APs against managed WLAN in public areas. In this paper we take "T wifi zone" as an example, which is managed by SK Telecom in Korea. There are two kinds of Rogue APs against managed WLAN: Fake AP and Evil Twin AP.

2.1 Fake AP

A Fake AP is a Rogue AP that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been made to attract users of managed WLAN to connect it in order to get users information. Fake APs of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install an inexpensive wireless router that can potentially allow unauthorized parties access to a secure network. Recently, most companies use WIPS to detect this Fake AP, and we will not discuss it in our following solution.

Fig. 1 shows the Fake AP of the second kind,

which directly connects to a wired-network. It usually uses a fake service set identifier(SSID) to pretend a legitimate AP and thus allure users to connect it. Sometimes media access control(MAC) spoofing is optional.

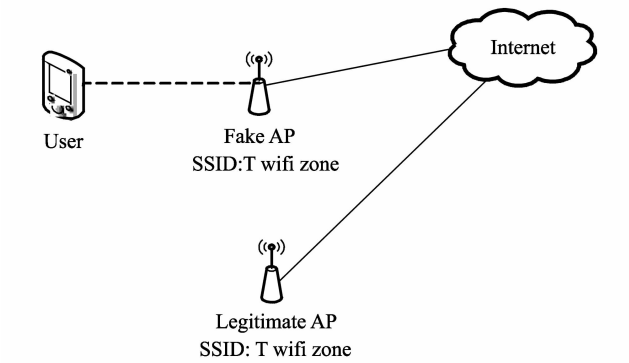

Fig. 1 A fake AP attack scenario

2.2 Evil Twin AP

Evil Twin AP is a term for a Rogue AP that appears to be a legitimate one offered on the premises, but actually has been set up by a hacker to eavesdrop on wireless communications among Internet surfers[13].

Evil Twin AP attack is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. Wireless devices link to the Internet via "hotspots" – nearby connection points that they lock on to, but these hotspots can act like an open door to thieves. Anyone with suitable equipment can locate a hotspot and take its place, substituting their own "Evil Twin AP". This type of Evil Twin AP attack may be used by a hacker to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there[14].

In Fig. 2, the first access point is an Evil Twin AP, which poses as 'T wifi zone', and connects to the legitimate AP.

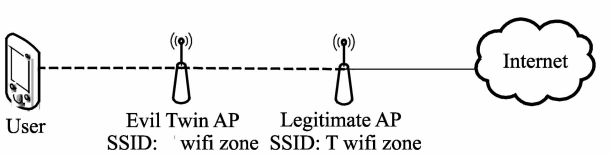

Fig. 2 An evil twin AP attack scenario

3 Proposed scheme

The framework of our proposed scheme includes two parts: user side and remote server. Users and the remote server communicate with each other by 3G network. User side agent is composed of Scanning, Localization, Comparison and Detection. Function of each component is as follows:

Scanning: Getting all the available WLANs in the sit and gathering the WLAN information such as basic SSID(BSSID), SSID, channel, received signal strength(RSS) and GPS information on current location of the user.

Localization: Getting targeted AP' location. We use the method in Ref. [15] to get the location of AP. In Ref. [15], authors combined GPS with RSS to localize access points in a smartphone, and the experiment shows that this method could get correct location information even under complex radio environment.

Comparison: Comparing APs' location information with same SSID. If all the APs' locations are different or there are no APs with the same SSID, it will send the location information of AP to remote server by 3G network, it will go to Detection.

Detection: Determining whether the AP is a fake one by receiving information, and noticing the user.

Remote server side has a database which stored the locations of legitimate APs. When it receives the information from user side, it will compare it with database and return the comparing results to user side. The component of the proposed scheme is shown in Fig. 3.

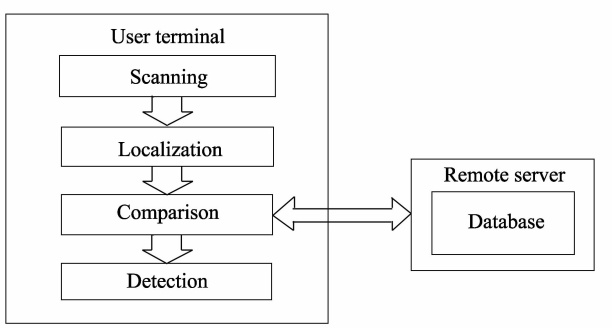

Fig. 3 Architecture of proposed framework

In our scheme we just need to add, delete or modify information in database when the legitimate APs' locations are changed. So we do not need a special administrator to operate it every day. Users can use our scheme anywhere when he wants to connect an AP. Now we will explain the flow of the proposed scheme in detail. The flow chart is illustrated in Fig. 4.

1) When the proposed detection method is used, it will firstly scan the WLANs available in the area.

2) If more than two"T wifi zones" exist, users will store the AP information.

3) Get the information of all "T wifi zone": BSSID, SSID, channel, RSS information. Addit-

ionally, get the GPS information on current location of the user.

4) Send the information to the remote server by 3G network after remote server calculates the AP location using method in Ref.[15].

5) The remote server compares it with database, and if the location information is the same as that in database, it is a legitimate AP. Otherwise it is a Rogue AP. The results will be shown to the user.

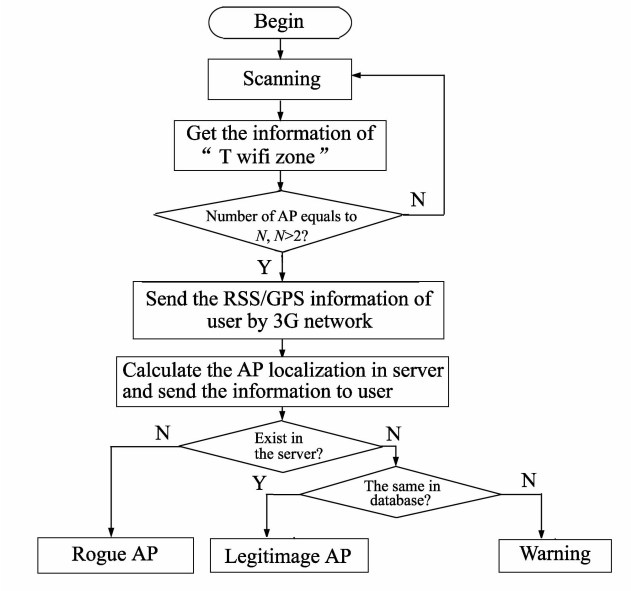

Fig.4 Proposed framework workflow

4 Conclusion

In this paper we have presented a novel Rogue AP detection scheme. It is a user-oriented solution, which can protect users against Evil Twin attacks as well as Fake AP attacks. It mainly works on detecting Rogue APs against the managed WLAN in public areas. The proposed framework performs by using previous methods to get APs' location and compare it with database managed by communications. It does not need to make any change of the existing hardware.

References

[1] Branch J W, Petroni N L Jr, Van Doorn L, et al. Autonomic 802.11 wireless LAN security auditing. IEEE Security & Privacy, 2004, 2(3): 56-65.

[2] AirWave. AirWave wireless management suite. ArubaNetworks, 2006.

[3] Bahl P, Chandra R, Padhye J, et al. Enhancing the security of corporate Wi-Fi networks using DAIR. Proc. of the 4th International Conference on Mobile Systems, Applications and Services (MobiSys 06), ACM Press, Uppsala, Sweden, 2006: 1-14.

[4] Yeo J, Youssef M, Agrawala A. A framework for wireless LAN monitoring and its applications. Proc. of 2004 ACM workshop on Wireless security(WiSe'04), Philadephia, USA, 2004: 70-79.

[5] WEI Wei, Suh K, WANG Bing, et al. Passive online detection of 802.11 traffic using sequential hypothesis testing with TCP ACK-pairs. IEEE Trans. on Mobile Computing, 2009, 8(3): 398-412.

[6] Jana S, Kasera S. On fast and accurate detection of unauthorized wireless access points using clock skews. IEEE Trans. on Mobile Computing, 2010, 9(3): 449-462.

[7] Spencer J. Use of an artificial neural network to detect anomalies in wireless device location for the purpose of intrusion detection. Proc. of the IEEE SoutheastCon, 2005: 686-691.

[8] Laurendeau C, Barbeau M. Hyperbolic location estimation of malicious nodes in mobile WiFi/802.11 networks. Proc. of the 2nd IEEE LCN Workshop on User Mobility and Vehicular Networks (ON-MOVE), 2008:600-607.

[9] Mano C D, Blaich A, Liao Q, et al. RIPPS: rogue identifying packet payload slicer detecting unauthorized wireless hosts through network traffic conditioning. ACM Trans. on Information and Syustem Security, 2008, 11(2): 1-23.

[10] HAN Hao, SHENG Bo, Tan C C, et al. A timing-based scheme for rogue AP detection. IEEE Trans. on Parallel and Distributed Systemas, 2011, 22(11): 1912-1925.

[11] SONG Yi-min, YANG Chao, GU Guo-fei. Who is peeping at your passwords at Starbucks? —To catch an evil twin access point. Proc. of IEEE/IFIP DSN 2010, Chicago, USA, 2010: 323-332.

[12] Monica D, Ribeiro C. WiFiHop-mitigating the Evil Twin attack through multi-hop detection. Proc. of the 16th European Conference on Research in Computer Security (ESORICS 2011), Leuven, Belgium, 201:21-39.

[13] Smith A D. Strange Wi-Fi spots may harbor hackers: ID thieves may lurk behind a hot spot with a friendly name. [2012-08-6-28]. http://www.m2mevolution.com/news/2007/05/09/2597106.htm.

[14] Wolfe D. Security watch. American Banker, 2007, 172(31): 7.

[15] Chun S M, Lee S M, Nah J W, et al. Localization of Wi-Fi access point using smartphone's GPS information. Proc. of IEEE Conference on Mobile and Wireless Networking (iCOST), 2011:121-126.