A Scheme of Detection and Prevention Rogue AP using Comparison Security Condition of AP

Kangsuk Chae, Jiawei Shao, Souhwan Jung
School of Electronic Engineering
Soongsil University
Seoul, Korea
{chaekhan, shaojiawei, souhwanj}@ssu.ac.kr

Changmoon Han, Seongsoo Bae, Injang Jeong
Institute of Network Technology
SK Telecom
Seongnam, Korea
{cmhan, billy.bae, injang.jeong}@sk.com

Abstract—**Rogue Access Points (RAPs) cause serious security threats to wireless networks. To detect RAPs, we propose a novel user-oriented framework based on security condition. AP's security condition which includes cipher and authentication type has been specified by the vendors. So it is difficult to be faked when authentication type is specified as IEEE 802.1X by the vendors. Authorized APs' SSID and security level have stored in database, and by comparing this information we can determine whether an AP is a rogue one or not. Furthermore, we provide users with optional secure channel. The experimental results show that the proposed framework can work efficiently.**

Keywords-Rogue AP (RAP), WLAN Security, Wireless Intrusion Detection; Wireless Monitoring; Secure Wireless Channel

I. INTRODUCTION

As the development of mobile technologies, the demand for communication over Wireless LANs System (WLANs) has increased. More and more users start to use wireless devices to access the Internet. However, the popularity of wireless communication also provides new opportunities to attackers. Wireless transmission employs microwave to spread data over the air. So within the range of Access Point (AP), all wireless devices can receive the wireless signal. As the signal can't be directed to a specific receiver, it will be easy for cyber criminals to monitor network traffic, disrupt data flows and infiltrate networks. These risks make wireless security to be more important.

The most challenging security issues that should be considered are Rogue Access Points (RAPs). A RAP is typically referred to as an unauthorized device which connects to the corporate network in many literatures. In this paper we view RAPs as improperly configured, unauthorized, phishing and compromised APs, which were detailed described in [1]. A RAP can be detected on both the operator and user sides. Administrator-oriented solutions need centralized system that collects, detects and manages information, such as Wireless Intrusion Prevention System(WIPS). And these solutions can be classified into wireless-side and wired-side. On the wireless-side, solutions are proposed based on the intuitive idea of sniffing the RF spectrum to search unauthorized wireless traffic. And researchers developed wired-side techniques based on temporal traffic characteristics. But wireless-side solutions had deficiencies on cost and scalability. Meanwhile, wired-side solutions only can work on the assumption that a sample of wireless traffic is available for comparison. To mitigate these deficiencies some previous schemes have been done to combine wireless-side with wired-side. But these Administrator-oriented solutions only can be used in some areas with fixed users, such as companies, universities. Users who want to access to WiFi hotspots at airports or another public places can't be protected well against RAP. So user-oriented solutions are proposed to solve that problem.

User-oriented technique allows the user to independently determine whether an AP is a RAP or not without assistance from the WLAN operator. It can be implemented on wireless devices, such as laptops, mobiles and pads. So far, researches on it mainly detect two WiFi-hop, to identify RAPs. We propose a novel user-oriented framework for not only detection but also prevention. The proposed framework captures beacon messages to get some necessary information. If new AP's information is different with that in database, it can be a potential RAP. Furthermore, if new AP's security level is lower, the user can choose to use security channel. This proposed framework can avoid users connecting with RAP.

II. RELATED WORK

As discussed above, there are a variety of solutions existed for detecting Rogue Access Points, which can be classified into administrator-oriented and user-oriented. Administrator-oriented solutions need central server, while user-oriented solutions only work on the client side.

A. Administrator-oriented Solution

Administrator-oriented solution works on both wireless and wired side. It allows the Administrator to dynamically select detection algorithms and thus to maintain a detection baseline which can be readily extended when certain events occur.

1) Wireless-side Detection

The main wireless-side solution is to deploy sniffers throughout the network to gather information which can help detect RAPs. Nowadays, many wireless sniffers can be available, such as AirDefence [2], AirMagnet [3] and Airwave [4]. They use a combination of radio frequency sensors to scan the spectrum at 2.4 and 5GHz for unauthorized traffic.

This research was supported by the SK Telecom, Korea, under the R&D program.

Information gathered by sniffers is identifying characteristics including MAC addresses, vendor name, and SSID. Although they are widely used in many enterprises, it is expensive. The latest release, AirDefense 7.2 has a starting price of US $7, 995.

To improve the expensive deployment of sensors, [5] provided a solution by using inexpensive radio devices (such as USB wireless adapters). Furthermore, [6] and [7] proposed an agent based intrusion detection and response system for RAPs. In this system each agent is equipped with network cards to act as a sniffer, and return an information packet of new APs to the server. The server compares it to information of authorized APs which have been stored by hands to determine if it is a rogue AP. But the intrusion detection capabilities are stymied by MAC address spoofing.

[8] have shown that the clock skew of a device remains consistent over time but vary significantly across devices. So [9] explored the use of clock skew of a WLAN access point (AP) as a fingerprint to identify RAPs. They calculate every AP's clock skews by collecting their beacons and probe messages. If any AP's clock skew is different from existing clock skews in the database, the AP is then identified as a rogue AP. Although it is effective for detecting RAPs inserted by malicious outsiders, but can't be applied to detecting RAPs inserted by malicious insiders due to periodic clock synchronization among the nodes.

2) *Wired-side Detection*

All successful wireless traffic finally arrives at wired backbone. So centralized network administrator can manages and monitors WLAN at wired-side. The most common solution used in wired-side detection is using wireless traffic characteristics to distinguish wireless nodes. [10] present a RAP detection approach by analyzing traffic characteristics at the edge of a network. The link layer for wireless networks is not as reliable as Ethernet links due to variations in channel conditions. This causes a variation in wireless link capacity and introduces random delays.

[11] used spectral analysis to identify wireless traffic. The 802.11 PHY has multiple data transfer rate and each rate corresponds to a different PHY modulation scheme. It is the responsibility of the rate switching algorithm which have been specified by the vendor to select the proper rate (modulation scheme) per packet. As the rate changes during the frame transmission, noticeable and unique jumps in the Inter-packet Arrival Time(IAT) occur. We can artificially produce these variations and use them as a signature that's unique to wireless traffic.

[12] proposed a passive online RAP detection by examining the arrival time of consecutive ACK pairs in TCP traffics. They built a classifier based on a sequential hypothesis test and exploit fundamental properties of the 802.11 CSMA/CA MAC protocol and the half-duplex nature of wireless channels for automated online detection of RAPs. However, the use of ACK pairs limits this technique to TCP traffic.

[13] used the client-side bottleneck bandwidth as a distinguishing feature between wired and wireless hosts. The bottleneck bandwidth is computed using the packet-pair technique and the results are stabilized using the sliding window technique.

B. *User(Mobile)-oriented Solution*

Some authors in different research papers [14-16] utilizes round trip time of TCP traffic to detect rogue APs. If the node is connected through the RAP, it will take two wireless hops to reach the local DNS server, instead of one. The added delay will be visible in the round-trip time.

[17] exploit 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).

[18] proposed a solution which was different from previous work, it does 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.

[19] utilizes PLCP (Physical Layer Convergence Protocol) header of IEEE 802.11 frames to differentiate an attacker station from a genuine station. The modulation types and data rates in PLCP header depend on rate adaption algorithm used in the drivers of the wireless adaptors or access point and environments. Therefore, it is much harder to forge. However, because of limited data rates and modulation types in 802.11, it is possible that the data rate of attack station is the same with the data rate of the real station.

III. Proposed Framework

In this paper we propose a novel user-side solution, which based on security level to detect and prevent client against rogue AP. The authorized APs' SSID and security level have been inserted into database by hand.

The goals of the proposed framework as follows:

- Detect potential rogue AP from client side when access to WiFi hotspots.
- Notify users when security threats are detected.
- Support users with optional security association between mobile terminal and secure gateway to prevent against security threats.

A. *Basic Concept*

Our framework can detect potential RAP and provide users with protection. We get AP's information by analyzing beacon messages. And then compare these information with database to determine whether the AP is rogue one or not. If it is a rogue one, we will inform the user and support optional security channel.

B. *Architecture of Framework*

The proposed framework composes of User Terminal, Secure Gateway. The user terminal is equipped with some components which includes connection monitoring module (CMM), security check module (SCM), database (DB), threat alarm module (TAM), and security association module (SAM). Figure 1 shows the architecture of proposed framework.

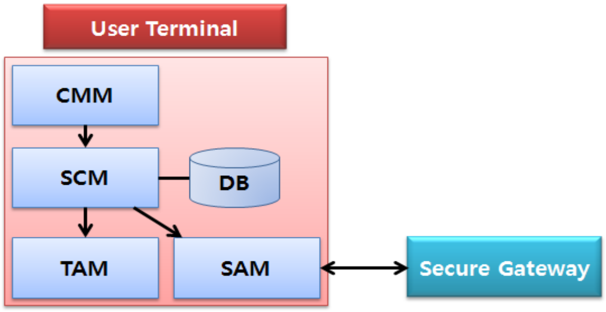


Figure 1. Architecture of proposed framework

Function of each components:

- CMM: Sniff and capture beacon messages to get SSID, cipher and authentication type from them.
- DB: Database saves the authorized APs' SSI security level information of previous connection. The security levels are defined in the Table1 and Table2.
- SCM: Compare the cipher and authentication type determined by CMM with DB. If the security level of this connection is lower than that with same SSID stored in DB, SCM will go to TAM.
- TAM: Inform the threats to the user.
- SAM: Associate secure channel with secure gateway (e.g. VPN server).

TABLE I. THE LEVEL OF CIPHER

Level	Cipher type
Level 1	CCMP
Level 2	TKIP
Level 3	WEP-104
Level 4	WEP-40
Level 5	No Cipher

Cipher types are based on IEEE Std 802.11i -2004 [20]

TABLE II. THE LEVEL OF AUTHENITCATION AND KEY MANAGEMENT

Level	Authentication type	Key management type
Level 1	IEEE 802.1X	RSNA key management
Level 2	PSK	RSNA key management using PSK
Level 3	No authentication	

Authentication and key management types are based on IEEE Std 802.11i -2004 [20]

C. *Operation of Framework*

In the proposed framework when a user wants to connect with an AP, CMM will get the SSID, cipher and authentication type of that AP. And then compares {SSID, cipher type, authentication type} with DB. If it isn't included in DB or not completely compared, it maybe a rogue AP. So the TAM will inform the user and ask whether he/she wants to connect with the secure GW or not. If the answer is OK he/she will associates secure channel with secure GW after this connection. And by answering NO, this connection will be prohibited.

However, in case, {SSID, cipher type, authentication type} is the same with the information in DB, SCM will check the security level defined in Table 1 and Table 2. If security level of this connection is low, TAM will inform the user. And then the user can choose to associates secure channel with secure GW after this connection or access to this AP directly. But if security level is high, this connection can be allowed. Figure 2 illustrates the flow of the proposed framework.

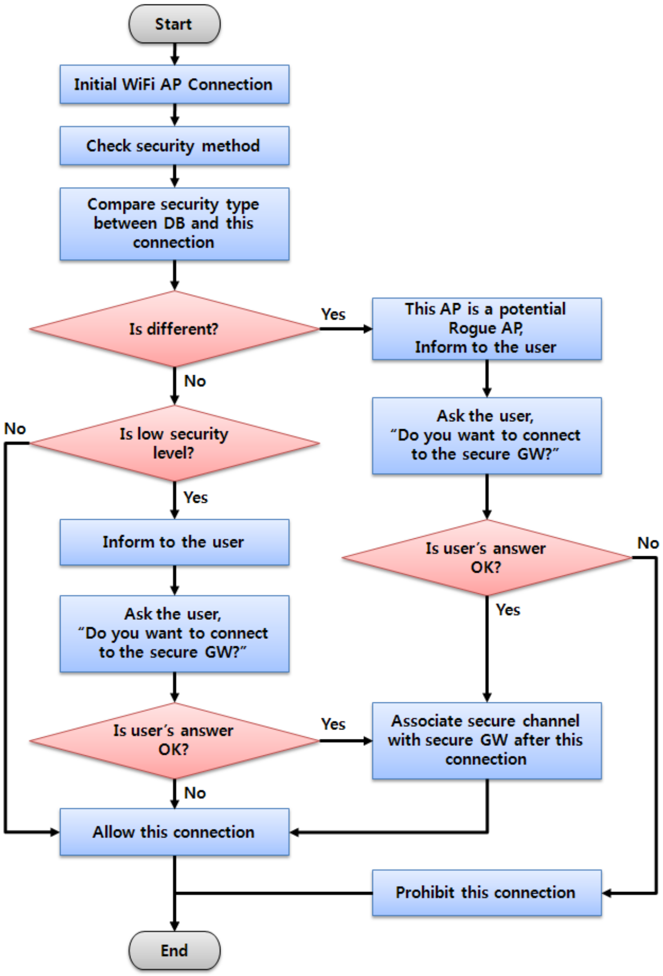

Start
Initial WiFi AP Connection
Check security method
Compare security type between DB and this connection
Is different?
Yes
This AP is a potential Rogue AP, Inform to the user
No
Ask the user, "Do you want to connect to the secure GW?"
No
Is low security level?
Yes
Inform to the user
Is user's answer OK?
No
Yes
Ask the user, "Do you want to connect to the secure GW?"
Is user's answer OK?
Yes
Associate secure channel with secure GW after this connection
No
Allow this connection
Prohibit this connection
End

Figure 2. Proposed framework workflow

IV. Experimental Analysis

For experiment, we set up two RAPs of SSUWLAN in our university and captured beacon messages from these APs. The beacon frame format is illustrated in Figure 3 which includes SSID and RSN of an AP [21]. The RSN information element contains authentication, pairwise cipher suite selectors, and a single group cipher suite selector. These sub-fields of RSN show the AP's cipher type, authentication and key management type.

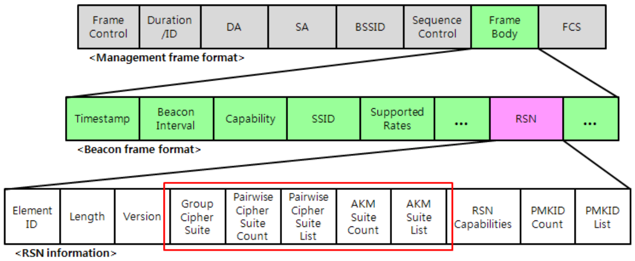
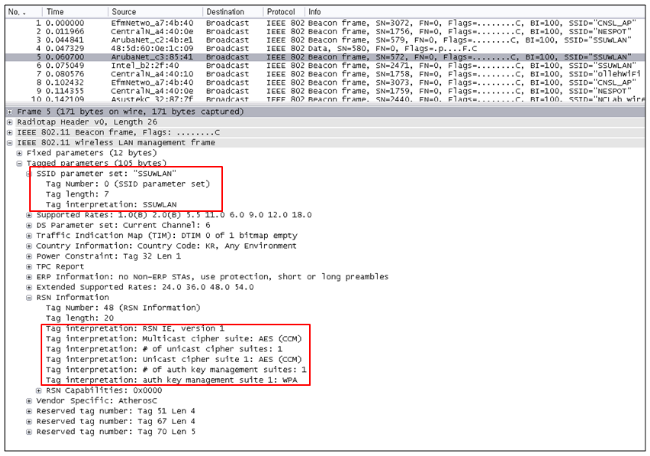


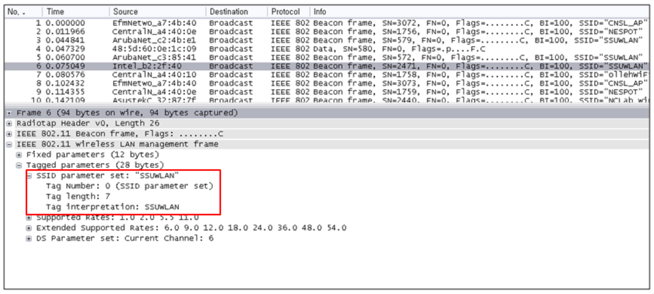
Figure 3. Beacon frame and RSN information [21]

In this experiment, the SSUWLAN AP's SSID, cipher type, authentication type have been stored in database. From captured beacon frame in Figure 4 we can see that this AP's SSID, cipher type and authentication type is {SSUWLAN, CCMP, WPA}. It is a legitimate one and its security level is high, so users can connect it directly. However, beacon frame in Figure 5 has the same SSID with legitimate AP and no RSN information. It is an open rogue AP. In other case, Figure 6 shows another rogue AP whose authentication type is PSK different with legitimate one. For these cases, our framework will ask the user if he/she wants to associate secure channel with secure GW after this connection.



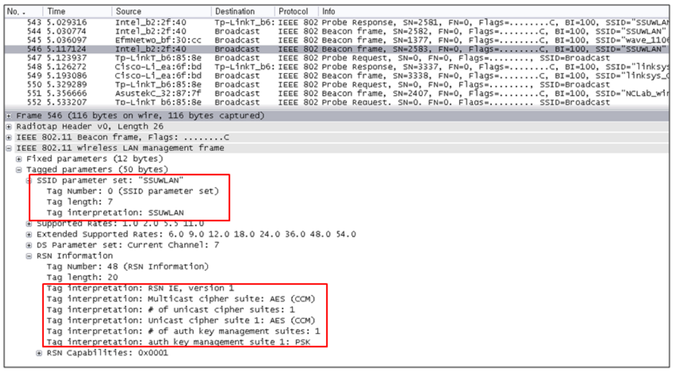
```
No. .   Time       Source              Destination   Protocol  Info
      1 0.000000   EfmNetwo_a7:4b:40   Broadcast     IEEE 802 Beacon frame, SN=3072, FN=0, Flags=........C, BI=100, SSID="CNSL_AP"
      2 0.011966   CentralN_a4:40:0e   Broadcast     IEEE 802 Beacon frame, SN=1756, FN=0, Flags=........C, BI=100, SSID="NESPOT"
      3 0.044841   ArubaNet_c2:4b:e1   Broadcast     IEEE 802 Beacon frame, SN=579, FN=0, Flags=........C, BI=100, SSID="SSUWLAN"
      4 0.047329   48:5d:60:0e:1c:09   Broadcast     IEEE 802 Data, SN=580, FN=0, Flags=.p....F.C
      5 0.060700   ArubaNet_c3:85:41   Broadcast     IEEE 802 Beacon frame, SN=572, FN=0, Flags=........C, BI=100, SSID="SSUWLAN"
      6 0.075049   Intel_b2:2f:40      Broadcast     IEEE 802 Beacon frame, SN=2471, FN=0, Flags=........C, BI=100, SSID="SSUWLAN"
      7 0.080576   CentralN_a4:40:10   Broadcast     IEEE 802 Beacon frame, SN=1758, FN=0, Flags=........C, BI=100, SSID="ollehWiFi
      8 0.102432   EfmNetwo_a7:4b:40   Broadcast     IEEE 802 Beacon frame, SN=3073, FN=0, Flags=........C, BI=100, SSID="CNSL_AP"
      9 0.114355   CentralN_a4:40:0e   Broadcast     IEEE 802 Beacon frame, SN=1759, FN=0, Flags=........C, BI=100, SSID="NESPOT"
     10 0.142109   AsustekC_32:87:7f   Broadcast     IEEE 802 Beacon frame, SN=2440, FN=0, Flags=........C, BI=100, SSID="NCLab_wire
⊞ Frame 5 (171 bytes on wire, 171 bytes captured)
⊞ Radiotap Header v0, Length 26
⊞ IEEE 802.11 Beacon frame, Flags: ........C
⊟ IEEE 802.11 wireless LAN management frame
  ⊞ Fixed parameters (12 bytes)
  ⊟ Tagged parameters (105 bytes)
    ⊟ SSID parameter set: "SSUWLAN"
        Tag Number: 0 (SSID parameter set)
        Tag length: 7
        Tag interpretation: SSUWLAN
    ⊞ Supported Rates: 1.0(B) 2.0(B) 5.5 11.0 6.0 9.0 12.0 18.0
    ⊞ DS Parameter set: Current Channel: 6
    ⊞ Traffic Indication Map (TIM): DTIM 0 of 1 bitmap empty
    ⊞ Country Information: Country Code: KR, Any Environment
    ⊞ Power Constraint: Tag 32 Len 1
    ⊞ TPC Report
    ⊞ ERP Information: no Non-ERP STAs, use protection, short or long preambles
    ⊞ Extended Supported Rates: 24.0 36.0 48.0 54.0
    ⊟ RSN Information
        Tag Number: 48 (RSN Information)
        Tag length: 20
        Tag interpretation: RSN IE, version 1
        Tag interpretation: Multicast cipher suite: AES (CCM)
        Tag interpretation: # of unicast cipher suites: 1
        Tag interpretation: Unicast cipher suite 1: AES (CCM)
        Tag interpretation: # of auth key management suites: 1
        Tag interpretation: auth key management suite 1: WPA
      ⊞ RSN Capabilities: 0x0000
    ⊞ Vendor Specific: AtherosC
    ⊞ Reserved tag number: Tag 51 Len 4
    ⊞ Reserved tag number: Tag 67 Len 4
    ⊞ Reserved tag number: Tag 70 Len 5
```

Figure 4. Beacon frame of legitimate AP



```
No. .   Time       Source              Destination   Protocol  Info
      1 0.000000   EfmNetwo_a7:4b:40   Broadcast     IEEE 802 Beacon frame, SN=3072, FN=0, Flags=........C, BI=100, SSID="CNSL_AP"
      2 0.011966   CentralN_a4:40:0e   Broadcast     IEEE 802 Beacon frame, SN=1756, FN=0, Flags=........C, BI=100, SSID="NESPOT"
      3 0.044841   ArubaNet_c2:4b:e1   Broadcast     IEEE 802 Beacon frame, SN=579, FN=0, Flags=........C, BI=100, SSID="SSUWLAN"
      4 0.047329   48:5d:60:0e:1c:09   Broadcast     IEEE 802 Data, SN=580, FN=0, Flags=.p....F.C
      5 0.060700   ArubaNet_c3:85:41   Broadcast     IEEE 802 Beacon frame, SN=572, FN=0, Flags=........C, BI=100, SSID="SSUWLAN"
      6 0.075049   Intel_b2:2f:40      Broadcast     IEEE 802 Beacon frame, SN=2471, FN=0, Flags=........C, BI=100, SSID="SSUWLAN"
      7 0.080576   CentralN_a4:40:10   Broadcast     IEEE 802 Beacon frame, SN=1758, FN=0, Flags=........C, BI=100, SSID="ollehWiF
      8 0.102432   EfmNetwo_a7:4b:40   Broadcast     IEEE 802 Beacon frame, SN=3073, FN=0, Flags=........C, BI=100, SSID="CNSL_AP"
      9 0.114355   CentralN_a4:40:0e   Broadcast     IEEE 802 Beacon frame, SN=1759, FN=0, Flags=........C, BI=100, SSID="NESPOT"
     10 0.142109   AsustekC_32:87:7f   Broadcast     IEEE 802 Beacon frame, SN=2440, FN=0, Flags=........C, BI=100, SSID="NCLab_wi
⊞ Frame 6 (94 bytes on wire, 94 bytes captured)
⊞ Radiotap Header v0, Length 26
⊞ IEEE 802.11 Beacon frame, Flags: ........C
⊟ IEEE 802.11 wireless LAN management frame
  ⊞ Fixed parameters (12 bytes)
  ⊟ Tagged parameters (28 bytes)
    ⊟ SSID parameter set: "SSUWLAN"
        Tag Number: 0 (SSID parameter set)
        Tag length: 7
        Tag interpretation: SSUWLAN
    ⊞ Supported Rates: 1.0 2.0 5.5 11.0
    ⊞ Extended Supported Rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
    ⊞ DS Parameter set: Current Channel: 6
```

Figure 5. Beacon frame of rogue AP case 1



```
No. .   Time       Source              Destination   Protocol  Info
    543 5.029316   Intel_b2:2f:40      Tp-LinkT_b6:  IEEE 802 Probe Response, SN=2581, FN=0, Flags=........C, BI=100, SSID="SSUWLAN
    544 5.030774   Intel_b2:2f:40      Broadcast     IEEE 802 Beacon frame, SN=2582, FN=0, Flags=........C, BI=100, SSID="SSUWLAN"
    545 5.036097   EfmNetwo_bf:30:cc   Broadcast     IEEE 802 Beacon frame, SN=1377, FN=0, Flags=........C, BI=100, SSID="wave_110
    546 5.117124   Intel_b2:2f:40      Broadcast     IEEE 802 Beacon frame, SN=2583, FN=0, Flags=........C, BI=100, SSID="SSUWLAN"
    547 5.123937   Tp-LinkT_b6:85:8e   Broadcast     IEEE 802 Probe Request, SN=0, FN=0, Flags=........, SSID=Broadcast
    548 5.126272   Cisco-Li_ea:6f:bd   Tp-LinkT_b6:  IEEE 802 Probe Response, SN=3337, FN=0, Flags=........C, BI=100, SSID="linksys
    549 5.193086   Cisco-Li_ea:6f:bd   Broadcast     IEEE 802 Beacon frame, SN=3338, FN=0, Flags=........C, BI=100, SSID="linksys_
    550 5.329289   Tp-LinkT_b6:85:8e   Broadcast     IEEE 802 Probe Request, SN=0, FN=0, Flags=........, SSID=Broadcast
    551 5.356666   AsustekC_32:87:7f   Broadcast     IEEE 802 Beacon frame, SN=2407, FN=0, Flags=........C, BI=100, SSID="NCLab_wir
    552 5.533207   Tp-LinkT_b6:85:8e   Broadcast     IEEE 802 Probe Request, SN=0, FN=0, Flags=........, SSID=Broadcast
⊞ Frame 546 (116 bytes on wire, 116 bytes captured)
⊞ Radiotap Header v0, Length 26
⊞ IEEE 802.11 Beacon frame, Flags: ........C
⊟ IEEE 802.11 wireless LAN management frame
  ⊞ Fixed parameters (12 bytes)
  ⊟ Tagged parameters (50 bytes)
    ⊟ SSID parameter set: "SSUWLAN"
        Tag Number: 0 (SSID parameter set)
        Tag length: 7
        Tag interpretation: SSUWLAN
    ⊞ Supported Rates: 1.0 2.0 5.5 11.0
    ⊞ Extended Supported Rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
    ⊞ DS Parameter set: Current Channel: 7
    ⊟ RSN Information
        Tag Number: 48 (RSN Information)
        Tag length: 20
        Tag interpretation: RSN IE, version 1
        Tag interpretation: Multicast cipher suite: AES (CCM)
        Tag interpretation: # of unicast cipher suites: 1
        Tag interpretation: Unicast cipher suite 1: AES (CCM)
        Tag interpretation: # of auth key management suites: 1
        Tag interpretation: auth key management suite 1: PSK
      ⊞ RSN Capabilities: 0x0001
```

Figure 6. Beacon frame of rogue AP case 2

V. Conclusion

In this paper we presented a novel RAP detection framework. It can protect user against evil twin attacks as well as SSID fake attacks. It is a user-oriented solution. So it can be used not only in companies, but also in public areas. The proposed framework performs by capturing beacon messages, getting {SSID, cipher type, authentication type} information, and comparing information with database. Our experiment showed that the proposed framework can work efficiently to protect users against RAPs.

Acknowledgment

This research was supported by the SK Telecom, Korea, under the R&D program.

References

[1] L. Ma, A. Y. Teymorian, X. Cheng, and M. Song "RAP: Protecting Commodity Wi-Fi Networks from Rogue Access Points," in Proc. QShine 2007, Vancouver, British Columbia, August 2007.

[2] "Tired of Rogues: Solutions for Detecting and Eliminating Rogue Wireless Networks," white paper, AirDefense, 2009.

[3] "Best Practices for Securing Your Wireless LAN," white paper, AirMagnet, 2004.

[4] "AirWave Wireless Management Suite," white paper, AirWave, 2006.

[5] P. Bahl, R. Chandra, J. Padhye, L. Ravindranath, M. Singh, A. Wolman, and B. Zill, "Enhancing the Security of Corporate Wi-Fi Networks Using DAIR," in Proc. MobiSys 2006, Uppsala, Sweden, June 2006.

[6] M. K. Chirumamilla, and B. Ramamurthy, "Agent Based Intrusion Detection and Response System for Wireless LANs," in Proc. IEEE ICC 2003, Anchorage Alaska, USA, May 2003.

[7] V.S.S. Sriram, G. Sahoo, and K.K. Agrawal, “Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN - A Multi-Agent Sourcing Methodology,” in Proc. IEEE IACC 2010, Patiala, India, February 2010.

[8] T. Kohno, A. Broido, and K. Claffy, “Remote Physical Device Fingerprinting,” IEEE Transactions on Dependable Secure Computing, Vol. 2, No. 2, pp. 93-108, 2005.

[9] 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, pp. 449-462, March 2010.

[10] S. Shetty, M. Song, and L. Ma, “Rogue Access Point Detection by Analyzing Network Traffic Characteristics,” in Proc. MILCOM 2007, Orlando, Florida, October 2007.

[11] C. Corbett, R. Beyah, and J. Copeland, “A Passive Approach to Wireless NIC Identification,” in Proc. IEEE ICC 2006, Istanbul, Turkey, June 2006.

[12] W. Wei, K. Suh, B. Wang, Y. Gu, J. Kurose, D. Towsley, and S. Jaiswal. “Passive Online Detection of 802.11 Traffic Using Sequential Hypothesis Testing with TCP ACK-Pairs,” IEEE Transactions on Mobile Computing, Vol. 8, No. 3, pp. 398-412, March 2009.

[13] K. F. Kaoa, I. E. Liaob, and Y. C. Lib, “Detecting Rogue Access Points Using Client-side Bottleneck Bandwidth Analysis,” Computers & Security, Vol. 28, No. 3-4, pp. 144–152, 2009.

[14] L. Watkins, R. Beyah, and C. Corbett, “A Passive Approach to Rogue Access Point Detection,” in Proc. IEEE GLOBECOM 2007, Washington, DC, USA, November 2007.

[15] C. D. Mano, A. Blaich, Q. Liao, Y. Jiang, D. A. Cieslak, D. Salyers, and A. Striegel, “RIPPS: Rogue Identifying Packet Payload Slicer Detecting Unauthorized Wireless Hosts Through Network Traffic Conditioning,” ACM Transactions on Information and Syustem Security, vol. 11, no. 2, May 2008.

[16] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, “A Timing-Based Scheme for Rogue AP Detection,” IEEE Transactions on Parallel and Distributed Systemas, Vol. 22, No. 11, pp. 1912-1925, November 2011.

[17] Y. Song, C. Yang, and G. Gu,” Who Is Peeping at Your Passwords at Starbucks? - To Catch an Evil Twin Access Point,” in Proc. IEEE/IFIP DSN 2010, Chicago, IL, USA, June-July 2010.

[18] D. Monica, and C. Ribeiro, “WiFiHop - Mitigating the Evil Twin Attack through Multi-hop Detection,” in Proc. ESORICS 2011, Leuven, Belgium, September 2011

[19] P. Chumchu, T. Saelim, C. Sriklauy, “A new MAC Address Spoofing Detection Algorithm using PLCP Header,” in Proc. ICOIN 2011, Kuala Lumpur, Malaysia, January 2011.

[20] IEEE Std 802.11i-2004, IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 6: Medium Access Control (MAC) Security Enhancements, July 2004.

[21] IEEE Std 802.11-2007, IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 2007.