Security in Wireless Networks

Analysis & Detection of Rogue Access Points and Evil Twin Attacks

Weeam Alshangiti Sumayyah Alahmadi

1. Introduction

Motivation

- As the popularity of wireless networks increases, the security threats increase.
  - **In 2015** → 50 millions AP worldwide →1 AP for every 150 user
  - **By 2018** → 340 million AP globally→1 AP for every 20 user
  - According to a study, 27% banked online in public wifi.
- The risk of interception is greater than with wired networks.
- Therefore, we need additional levels of security for our wireless network

Wireless Networks Background (Security Protocols)

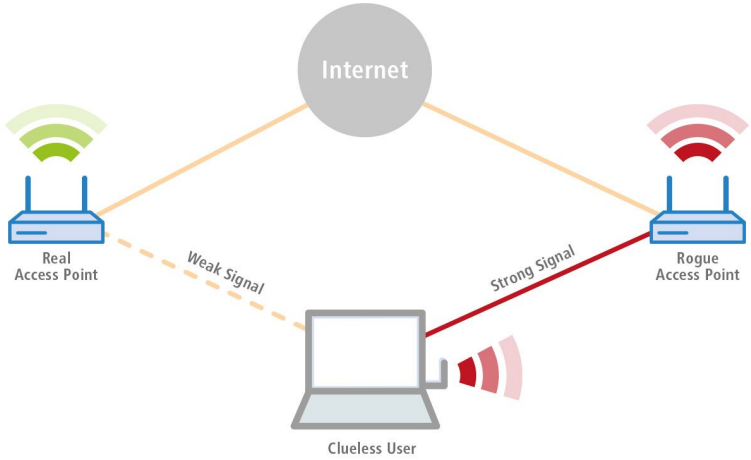
- **Wired Equivalent Privacy (WEP) -1999**
  - Rivest Cipher 4 (RC4) algorithm
- **Wi-Fi Protected Access (WPA) - 2003**
  - Introduced Temporal Key Integrity Protocol(TKIP)
  - Integrity check is implemented with message integrity code.
- **Wi-Fi Protected Access version II (WPA2) -2004**
  - Advanced Encryption Standard (AES) algorithm
  - An authentications server (802.1X)
  - robust protocol but it is still susceptible to ETA.

Most common Attacks in WLAN

- **Network Sniffing**
  - Capturing data as it is transmitted over a network
  - Passive and Active
- **Jamming or Denial of Service (DOS)**
  - Prevents legitimate users from accessing systems or network resources.
- **Unauthorized Access Points:**
  - Rogue Access Points
  - Evil Twin Attacks
  - Leads to Man-in-the-Middle Attacks

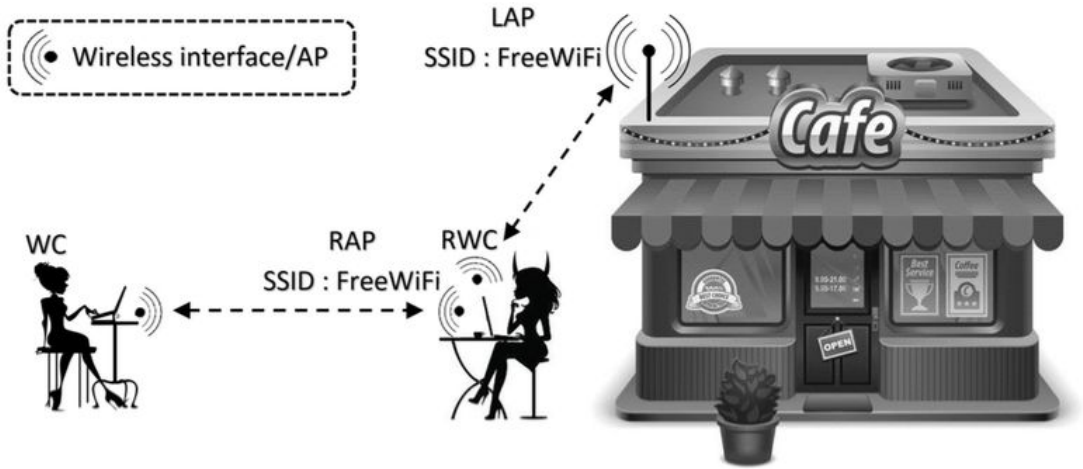
Rogue Access Point

- What is a rogue access point ?
- Why rogue access points are popular (20%)
- Firewall and WPA2 provide no protection against RAP

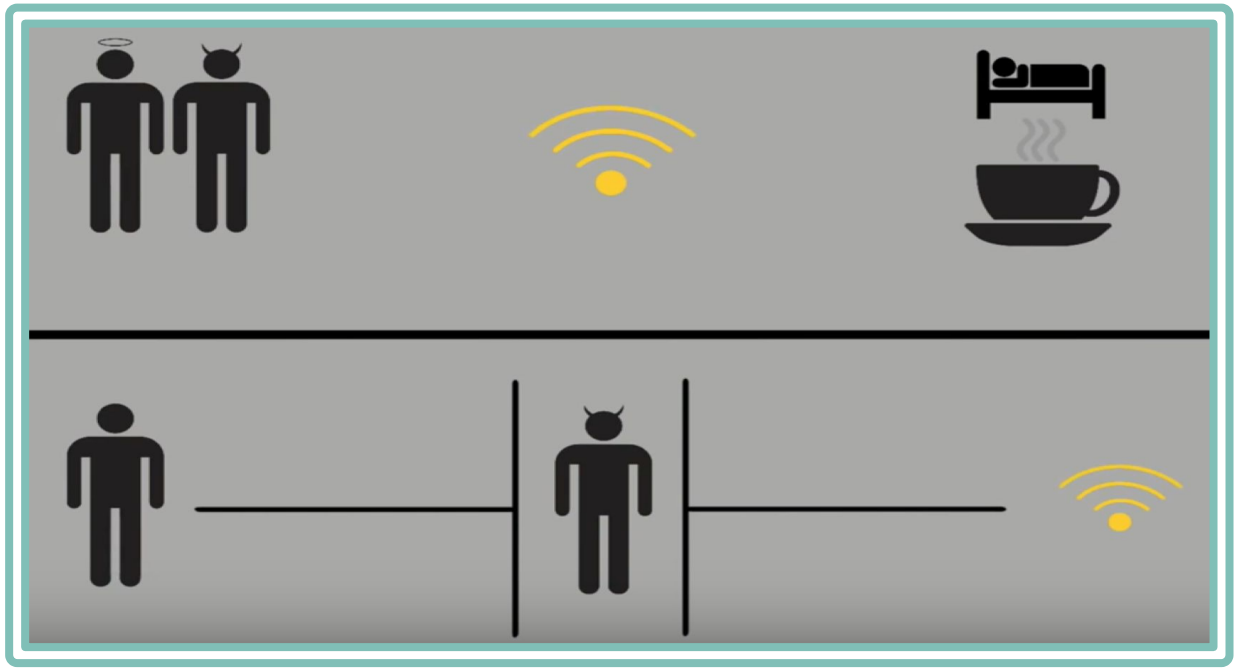


Evil Twin Attacks

- A copy of a legitimate Wi-Fi access point.
- It mimics a LAP in about every way including the SSID.
- High RSSI
- Cybercriminals intercept all traffic:
  - Steal account.
  - Redirect to malware sites
  - View file contents



Comparison Between Rogue Access Point and Evil Twin Attack



Similarities:

- Evil Twin may be considered as a type of Rogue AP.
- Both use AP for getting unauthorized access over a wireless network.
- The whole experience is transparent to the victim while the hacker is sniffing the network traffic.

Differences:

RAP	ETA
A physically plugged into the network	A software installed in a computer
Inside the wireless network	Usually outside the wireless network
Doesn't (and usually) have to be a copy of LAP	A copy of a legitimate AP
Redirecting traffic from the targeted machines to outside	Try to hook victims to connect to the fake network to steal information directly

2. Problem Definition

Detection and Protection against RAP and ETA

- Many solutions exist for each attack, but nothing for both
- One solution for detecting both attacks.
- Detections of the access point is protecting and defending against the attack.

3. Literature Review

A. Rogue Access Point

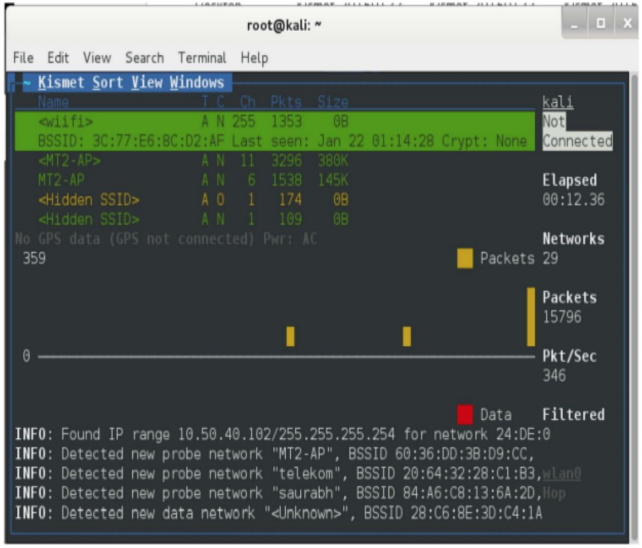
I. Detecting Rogue access point using Kismet

II. Rogue Access Point Detection Methods: Review

III. Rogue-Access-Point Detection Challenges, Solutions and Future Direction

Detecting Rogue access point using Kismet

- Kismet: wireless network detector, sniffer and Intrusion Detection System
- Kismet feature:
  Decode WEP Packet
  Support SSID decloaking



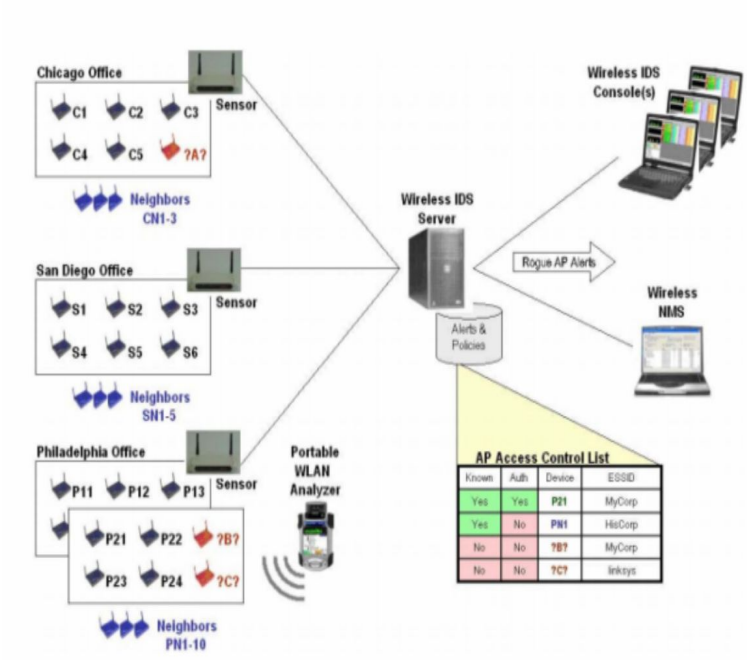
Kismet interface helps track rogue AP

Detecting Rogue access point using Kismet

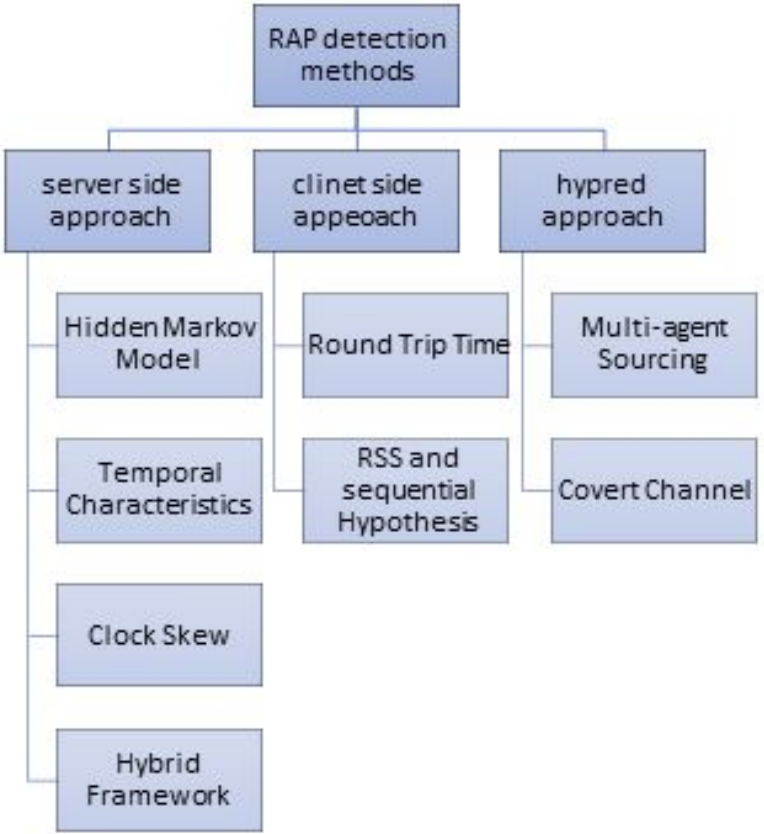
- Kismet methods:

Discover RAP existence and determine its location.

- Blocking RAP



Rogue Access Point Detection Methods: Review



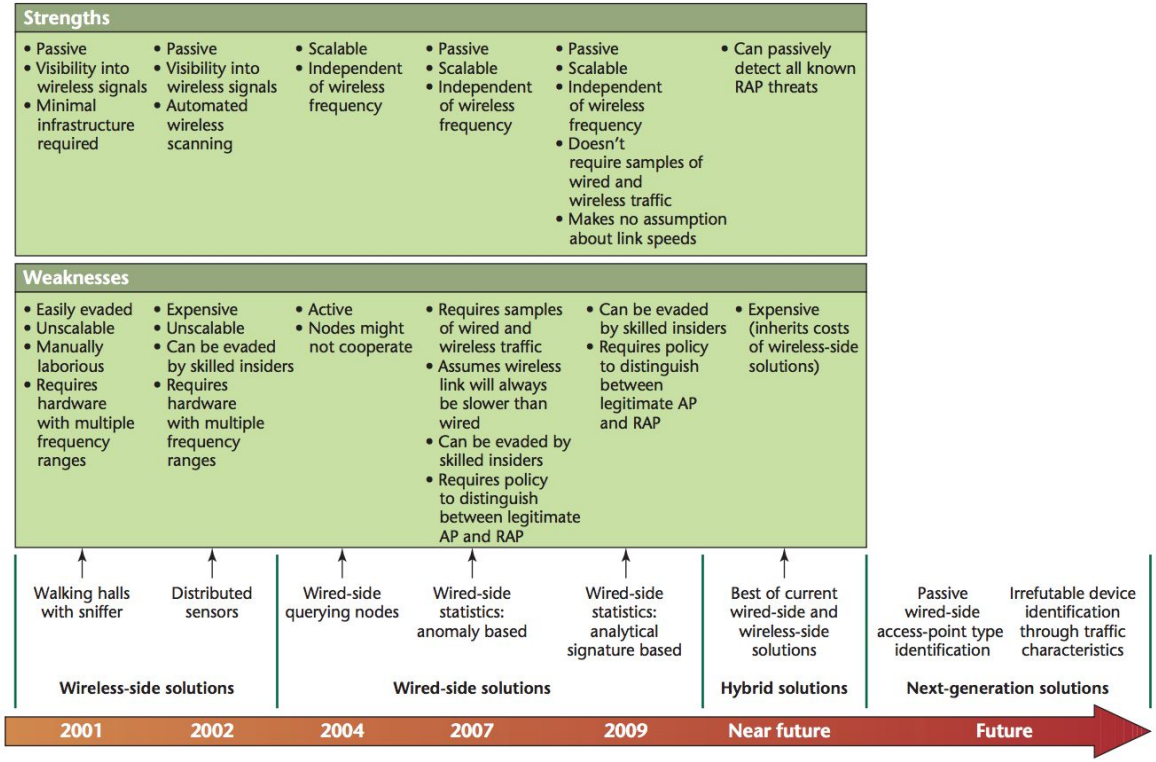
Rogue Access Point Detection Methods: Review

Methods → Parameters ↓	Round Trip Time	Temporal Characteristic -s	Covert channel	Hybrid framework	Hidden Markov Model	Received signal strength and Seq. Hypothesis	Multi-agent sourcing	Clock skew
Approach	Client side	Server side	Hybrid	Server side	Server Side	Client side	Hybrid	Server side
Type of RAP detection	Wireless	Wireless	Wired and Wireless	Wired and Wireless	Wired	Wired	Wired and Wireless	Wired
Other features	No assistance from WLAN operator	Independent of Wireless technology and effective for detecting RAPs inserted by malicious outsiders	Uses steganog-raphy	Cost-effective Used open source software for implementation	scalable and non-intrusive, requiring little deployment cost and effort	No assistance from WLAN operator	Independent of Wireless technology	

Rogue-Access-Point Detection Challenges, Solutions and Future Direction

- Detecting rogue AP:
  - Wireless side sniffing
  - Wired-side fingerprinting
  - Hybrid approach

Rogue-Access-Point Detection Challenges, Solutions and Future Direction



B. Evil Twin Attacks

I. User-Side Wi-Fi Evil Twin Attack Detection Using Random Wireless Channel Monitoring

- WC monitor the whole 11 Wi-Fi channels of 802.11 randomly.
- Mathematically modeled, prototyped and evaluated in real life environment
- Client side
- A detection rate approximates to 100%.

II. Security Analysis and Implementation of a Simple Method for Prevention and Detection against Evil Twin Attack in IEEE 802.11 Wireless LAN

- Requires minimal modifications.
- Assuming the client has been connected to the AP earlier.

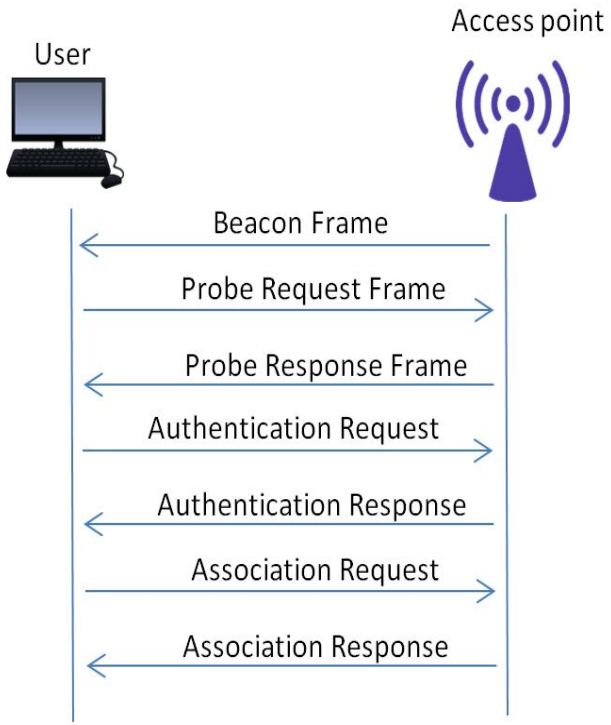
III. CETAD: Detecting Evil Twin Access Point Attacks in Wireless Hotspots

- Explores the similarities between LAPs and discrepancies between evil twin APs, and legitimate ones.
- It uses three statistics: similarity of ISP information, difference in RTT values, and standard deviation of RTT values.
- Installing an app at the client device - No changes in the APs.

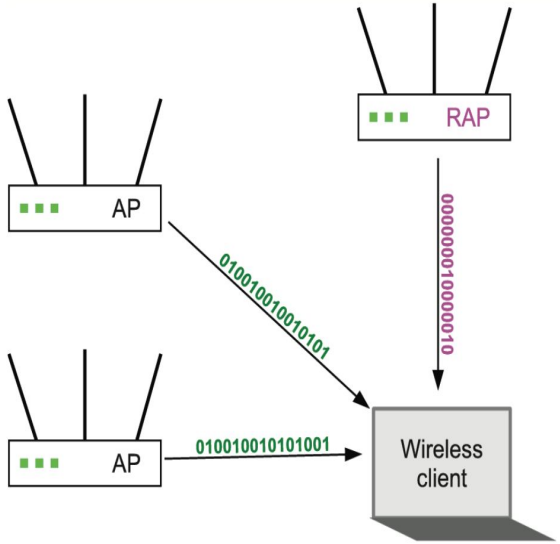
4. Proposed Approach

The Proposed Approach

- One solution for detecting both types of attacks, Rogue Access Point and Evil Twin attacks.
- Combine the Covert Channel method (Beacon Frame) with the Modification of the Operating System, Probe Response frame, and Access Point.



Covert Channel



- Hybrid approach (client-side and a server-side).
- Uses the Timestamp field in the beacon frame.
- AP send an authentication string to the client:
  - If the string matches, it connects to the AP
  - Otherwise, it disconnects.
- Two ways through which authentication string is passed to the client.
  - Transferring the first four bits each in a separate beacon frame (in sequence)
  - Using the difference between the intervals of a sequence of beacon frames

Modification of the Operating System, Probe Response frame, and Access Point.

1. Client's Operating System
   - Add **BSSID** and a **Count** to the list which stores SSID of previously connected APs.

2. Access Point
   - **SMC** table is maintained in the system.

TABLE I. TABLE MAINTAINED BY OS

SSID	BSSID	COUNT
CISL WI-FI	00-1A-5A-64-02-31	1
BEELINE_WI-FI	00-1B-6A-65-04-49	5
TP-LINK WI-FI	00-1C-7A-66-09-72	2

TABLE II. TABLE MAINTAINED BY AP

SMC

SSID	MAC	COUNT
DELL	00-17-AB-BE-28-1C	2
ACER	00-10-5A-44-12-B5	5
APPLE	00-17-AB-5A-6E-F5	1

3. Probe Response frame

- The probe response frames will contain a new information **'Count'**.

Order	Information
1	Beacon Interval
2	Time Stamp
3	SSID
4	Supported Rates
5	FH Parameter Set
6	DS Parameter Set
7	CF Parameter Set
8	Capability Information
9	IBSS Parameter Set
10	Count

Modified Probe Response Frame

Proposed Approach Details

- AP sends out its beacon frames (string in timestamp field).
- Client checks the timestamp field for a string match.
- Client sends a probe request.
- AP searches for the client's SSID, MAC and count.
- OS searches for AP's SSIDs, BSSID for the respective count value.
- If count values match, not ETA. If not, warning message is generated.
- Value of the Count is increased after sending and receiving the Association Response frame in both sides.

5. Approach Validation

Validation of the Proposed Approach

- Both methods proven to be efficient.
- No additional hardware nor software is required - minimal modifications ⇒ Straightforward and affordable.
- Client side - no need for network administration privileges.
- Doesn’t require scanning all AP in the area.
- Only employs unused bandwidth ⇒ doesn’t add any overhead.
- Hybrid approach

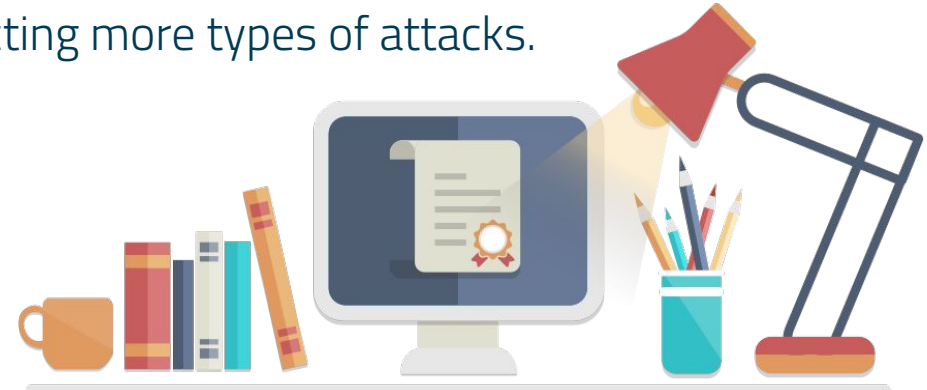
6. Limitations and Future Work

Limitations

- The need for more computational power.
- The need for more memory.

Future Work

- Different solutions can be combined.
- Other methods for detecting more types of attacks.



7. Conclusion

Conclusion

- Wireless network security background.
- Problem definition: One solution for detecting both types of attacks.
- We combined the Covert Channel method with the Modification of the Operating System, Probe Response frame, and Access Point method.
- Hybrid approach and Client side
- Different approaches and methods could be combined for better solutions

8. References

[1] Pacchiano, R. (2006, March 9). Track Down Rogue Wireless Access Points. Retrieved November 24, 2017, from http://www.wi-fiplanet.com/tutorials/article.php/3590551/Track-Down-Rogue-Wireless-Access-Points.htm

[2] Nakhila, O., & Zou, C. (2016). User-side Wi-Fi evil twin attack detection using random wireless channel monitoring. MILCOM 2016 - 2016 IEEE Military Communications Conference. doi:10.1109/milcom.2016.7795501

[3] Kumar, A., & Paul, P. (2016). Security analysis and implementation of a simple method for prevention and detection against Evil Twin attack in IEEE 802.11 wireless LAN. 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT). doi:10.1109/icctict.2016.7514574

[4] Mustafa, H., & Xu, W. (2014). CETAD: Detecting evil twin access point attacks in wireless hotspots. 2014 IEEE Conference on Communications and Network Security. doi:10.1109/cns.2014.6997491

[5] Sawicki, K., & Piotrowski, Z. (2012). The proposal of IEEE 802.11 network access point authentication mechanism using a covert channel. 2012 19th International Conference on Microwaves, Radar & Wireless Communications. doi:10.1109/mikon.2012.6233587

[6] Anmulwar, S., Srivastava, S., Mahajan, S. P., Gupta, A. K., & Kumar, V. (2014). Rogue access point detection methods: A review. International Conference on Information Communication and Embedded Systems (ICICES2014). doi:10.1109/icices.2014.7034106

[7] G, T., B, S. S., K, S. L., & Chandavarkar, B. R. (2015). Detecting Rogue Access Points using Kismet. 2015 International Conference on Communications and Signal Processing (ICCSP). doi:10.1109/iccsp.2015.7322813

[8] Beyah, R., & Venkataraman, A. (2011). Rogue-Access-Point Detection: Challenges, Solutions, and Future Directions. IEEE Security & Privacy Magazine,9(5), 56-61. doi:10.1109/msp.2011.75

[9] Patil, V., Thakur, P., & Deshmukh, S. (2012). Protecting Wi-Fi Networks from Rogue Access Points. Fourth International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom2012). doi:10.1049/cp.2012.2508

[10] Alotaibi, B., & Elleithy, K. (2016). Rogue Access Point Detection: Taxonomy, Challenges, and Future Directions. Wireless Personal Communications, 90(3), 1261-1290. doi:10.1007/s11277-016-3390-x

[11] Lu, Q., Qu, H., Zhuang, Y., Lin, X., Zhu, Y., & Liu, Y. (2017). A Passive Client-based Approach to Detect Evil Twin Attacks. 2017 IEEE Trustcom/BigDataSE/ICESS. doi:10.1109/trustcom/bigdatase/icess.2017.242

Questions