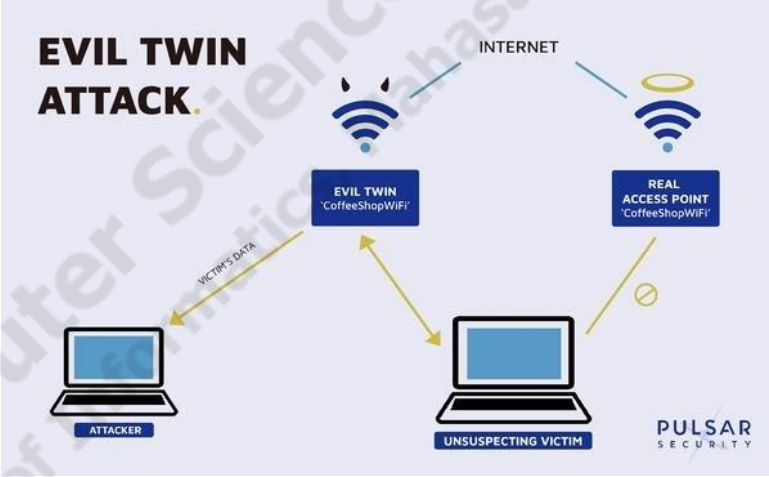
บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 Evil Twin Attack

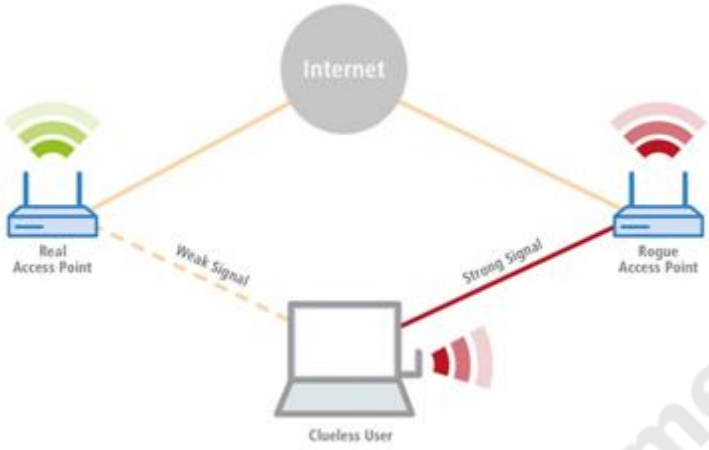
Evil Twin Attack [1] คือ การตั้งค่าหรือปลอมแปลงข้อมูลของ Access Point ให้เหมือนกับ Access Point ที่เป้าหมายต้องการเชื่อมต่อโดยจงใจให้มี ESSID (ชื่อของ WiFi ที่ระบุว่าเป็นของเราหรือสถานที่นั้นๆให้บริการ) เหมือนกันเช่น การตั้งชื่อ Airport_WiFi แล้วนำไปติดตั้งไว้ที่สนามบิน เพื่อให้เป้าหมายทำการเชื่อมต่อสัญญาณ WiFi ที่ถูกกระจายสัญญาณออกไปใหม่ หากเป้าหมายทำการเชื่อมต่อสัญญาณ WiFi ดังกล่าวโดยที่เป้าหมายไม่ทันสังเกตอาจทำให้ผู้ไม่ประสงค์ดีล้วงเอาข้อมูลไปได้โดยมีลำดับการทำงานดังภาพประกอบที่ 2.1 ภาพจำลองกระบวนการทำงานของ Evil Twin Attack



ภาพประกอบที่ 2.1 ภาพจำลองกระบวนการทำงานของ Evil Twin Attack

2.1.2 Rogue Access Point

Rogue Access Point [2] คือ Access Point ที่ไม่ได้รับอนุญาตให้ติดตั้งหรือเปิดใช้งานภายในองค์กร ซึ่งอาจรวมไปถึงการกระจายสัญญาณเครือข่ายไรสายของ Mobile Hotspot ด้วยเนื่องจากเป็นการกระจายสัญญาณโดยไม่ได้รับอนุญาตจากองค์กรซึ่งอาจทำให้เกิดการรบกวนการทำงานของเครือข่ายไร้สายหลักภายในองค์กรได้



ภาพประกอบที่ 2.2 จำลองกระบวนการทำงานของ Rouge Access Point

แต่อาจจะบอกไม่ได้ 100% ว่า Rogue Access Point นั้นจงใจที่จะทำขึ้นมาเพื่อสร้างความเสียหายแก่ผู้อื่นโดยการรบกวนการทำงานของเครือข่ายไร้สายหลักหรือไม่หรือเป็นเพียงเครือข่ายไร้สายที่ถูกเปิดใช้งานเพื่อความสะดวกของผู้ใช้งานเองเท่านั้น เช่น Hotspot WiFi จากมือถือ ที่บุคคลทั่วไปสามารถเปิดใช้งานได้

2.1.3 WiFi Phisher

WiFi Phisher [3] คือ เฟรมเวิร์กสำหรับสร้าง Rogue Access Point สำหรับเชื่อมต่อกับเป้าหมายที่ใช้การเชื่อมต่อไร้สาย เพื่อหลอกขโมย Passphrase หรือระบบที่พิสูจน์ตัวตนแบบ Captive Portal เพื่อขโมยข้อมูลล็อกอิน WiFi Phisher จะทำการ Disconnect ผู้ใช้ที่เชื่อมต่อกับ Access Point ปกติอยู่ด้วยการส่ง De-authentication packets ไปยัง Access Point และเครื่องผู้ใช้ จากนั้นก็จะดักข้อมูลของ Access Point แล้วปลอมตัวเป็น Access Point เครื่องนั้นๆ เมื่อเหยื่อพยายามที่จะเชื่อมต่อกับระบบเครือข่ายไร้สายใหม่อีกครั้ง ก็จะมาเชื่อมต่อที่ Access Point ปลอมเครื่องนี้แทน WiFi Phisher มีการติดตั้ง Web Server ขนาดเล็กไว้เพื่อใช้โต้ตอบการร้องขอ HTTP/HTTPS เมื่อไหร่ที่เป้าหมายเปิดเว็บไซต์เพื่อเล่นอินเทอร์เน็ต WiFi Phisher จะสร้างหน้าเว็บปลอมที่เหมือนจริงขึ้นมาเพื่อแอบถามข้อมูลล็อกอินและรหัสผ่าน เช่น ระบบพิสูจน์ตัวตน (Authentication) เมื่อผู้ใช้ใส่ชื่อผู้ใช้และรหัสผ่านลงไป แฮกเกอร์ก็จะได้ข้อมูลรหัสผ่านนั้นทันที

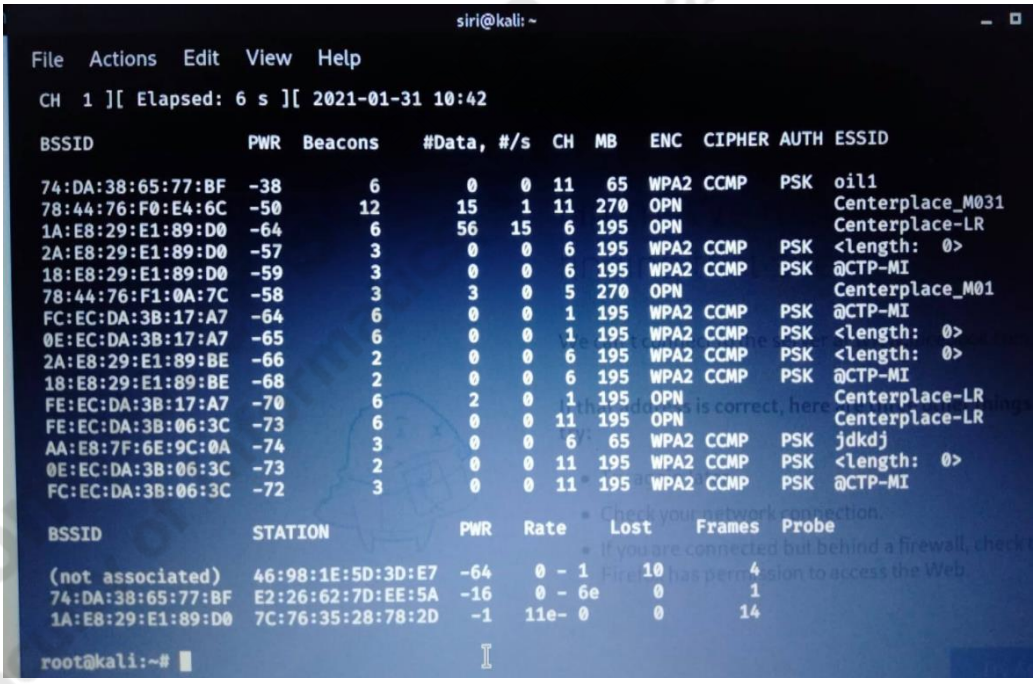
2.1.4 Air Crack

Air Crack [4] คือ เครื่องมือที่ใช้ในการดักจับและวิเคราะห์ข้อมูลของเครือข่าย Wireless LAN สามารถใช้ในการ Crack ข้อมูลที่เข้ารหัสทั้งในรูปแบบของ WEP WPA1 และ WPA2 และใน Monitor

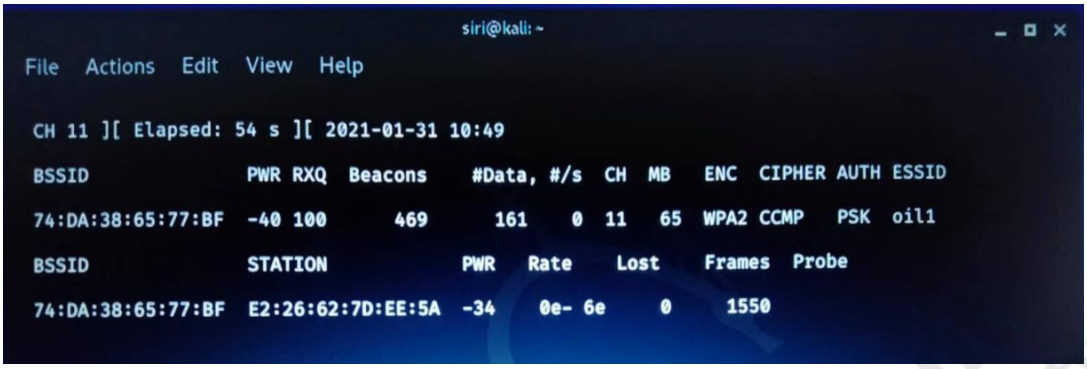
Mode สามารถใช้ในการตรวจจับและวิเคราะห์ข้อมูลต่างๆ ของ Wireless LAN รอบๆตัวได้ โดย Tool นี้มี Option หลากหลายมาก และหนึ่งใน Option ที่คนส่วนมากรู้จักและใช้งานบ่อยครั้ง คือ การทำ WPA hand-shake ซึ่งจะสามารถนำไฟล์ Pcap ที่ได้จากการดักจับข้อมูลนี้ไป Crack หา Password ได้

2.1.5 De-authentication Attack

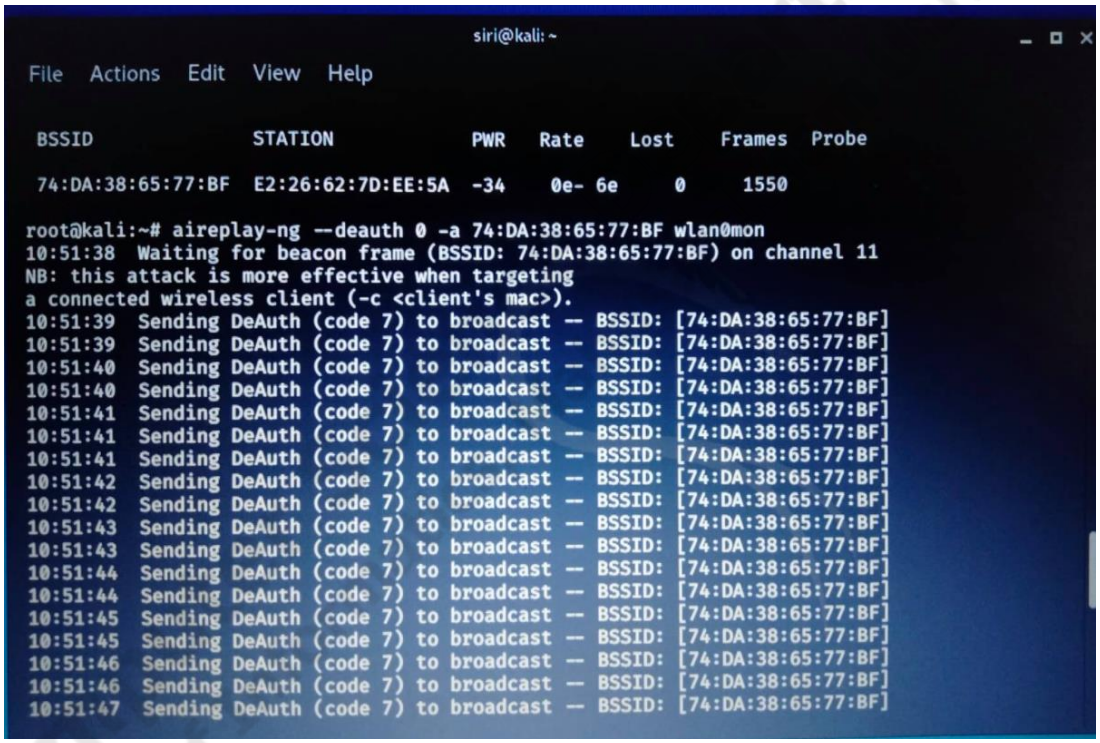
De-authentication Attack [5] คือการส่งเฟรม De-authentication packet ไปยังเครื่องที่กำลังเชื่อมต่อหรือติดต่อกับอุปกรณ์กระจายสัญญาณของเป้าหมาย เมื่อเครื่องเป้าหมายได้รับเฟรม De-authentication ซึ่งทำให้เครื่องที่ได้รับเฟรมดังกล่าวนั้นเข้าใจว่าได้รับการขอยกเลิกการเชื่อมต่อหรือการไม่สามารถให้บริการได้จากอุปกรณ์กระจายสัญญาณเป้าหมาย ซึ่งทำให้เครื่องที่เชื่อมต่ออยู่กับ Access Point นั้นไม่สามารถเชื่อมต่อได้ การส่งเฟรม De-authentication นั้นยังสามารถส่งไปยัง Access Point โดยตรงได้ ซึ่งจะทำให้เครื่องที่เชื่อมต่ออยู่กับ Access Point ดังกล่าวไม่สามารถเชื่อมต่อกับ Access Point ได้โดยมีตัวอย่างการใช้งานดังนี้



ภาพประกอบที่ 2.3 ภาพตัวอย่างการใช้ airodump-ng เพื่อสแกนหา Access Point บริเวณรอบๆ



ภาพประกอบที่ 2.4 ภาพตัวอย่างการใช้ airodump-ng และ เลือกเป้าหมาย



ภาพประกอบที่ 2.5 ภาพตัวอย่างการใช้ Deauthentication packet

2.1.6 WEP (Wireless Equivalent Privacy)

WEP [6] เป็นมาตรฐานความปลอดภัยของเครือข่ายไร้สายที่ถูกใช้งานอย่างเป็นทางการในปี ค.ศ 1999 ใช้อัลกอริทึมการเข้ารหัสตาม RC4 (Ron's Code 4) โดยปรับการเข้ารหัสจาก 40 ถึง 104 บิต เพื่อรองรับการพิสูจน์ตัวจริงขั้นพื้นฐาน แต่เนื่องจากเป็นการเข้ารหัสเพียง 40 บิต จึงทำให้เกิดช่องโหว่ในกลไกการพิสูจน์ตัวจริง จึงถูกแทนที่ด้วย WPA (WiFi Protected Access) ในปี ค.ศ 2003 และอย่างไรก็ตามถึงแม้ WPA จะได้รับการอัปเกรดให้มีความปลอดภัยสูงขึ้นแล้ว แต่สุดท้ายก็ยังมีช่องโหว่ในโพรโตคอล TKIP (Temporal Key Integrity Protocol) จึงทำให้ WPA ไม่ปลอดภัยอีกต่อไป

2.1.7 WPA2 (WiFi Protected Access 2)

WPA2 [7] ถูกใช้งานอย่างเป็นทางการในปี ค.ศ 2004 โดยใช้ AES (Advanced Encryption Standard เข้ามาช่วย และ มีการเข้ารหัส ที่แข็งแกร่งและยืดหยุ่นมากกว่า WPA สำหรับการพิสูจน์ความเป็นตัวจริง WPA และ WPA2 มีให้ใช้ 2 แบบ คือ ตัวเลือกโหมดส่วนตัว และ โหมดองค์กร

- โหมดส่วนตัวขึ้นอยู่กับคีย์ที่ใช้ร่วมกัน (ใครมีคีย์ก็เข้าได้) หลีกเลี่ยงการติดตั้งเซิร์ฟเวอร์การตรวจสอบสิทธิ์ ดังนั้นจึงใช้สำหรับ กรณี SOHO (Small Office Home Office)

- โหมดองค์กรขึ้นอยู่กับการใช้เซิร์ฟเวอร์การพิสูจน์ความเป็นตัวจริง เช่น RADIUS เพื่อเสนอการเข้าถึงควบคุม ดังนั้น ความมั่นคงปลอดภัยของ WLAN ยึดตาม WPA2 มาตั้งแต่ในเดือนตุลาคม ปี ค.ศ 2017 และต่อมา Mathy Vanhoef ได้พบโชว์ช่องโหว่ สำหรับทั้งโหมด SOHO (โหมดส่วนตัว) และองค์กร ช่องโหว่นี้ทำให้ผู้โจมตีสามารถเข้าถึงเครือข่ายไร้สายได้ เทคนิคการโจมตีนี้เรียกว่า KRACK (Key Reinstallation Attack) ซึ่งสามารถโจมตี WPA2 แม้ว่า WPA2 เปลี่ยนจาก WPATKIP มาเป็น AES-CCMP (CC Mode Protocol) และ การเข้ารหัส GCMP (Galois Counter Mode Protocol) แล้วก็ตาม ดังนั้นตั้งแต่ปี ค.ศ. 2017 WPA3 (WiFi Protected Access 3) ได้ถูกพัฒนาเพื่อแก้ไขช่องโหว่โดยได้เป็นมาตรฐานในปี ค.ศ. 2018 และ ได้มีการวางจำหน่ายในปี ค.ศ. 2020 โดย WPA3 ใช้ SAEH (Simultaneous Authentication of Equal Handshake) เพื่อแก้ไขปัญหาใน WPA2 แม้การพิสูจน์ตัวจริงจะถูกพัฒนาไปถึง WPA3 แล้วก็ตามแต่การโจมตีด้วยเทคนิค Evil Twin Attack ยังคงสามารถใช้โจมตีเครือข่ายไร้สายได้

2.1.8 Pyqt

Pyqt [8] ภาษาไพธอนสามารถสร้าง GUI ได้อย่างไม่ยากนัก มีมอดูลอยู่หลายตัวที่ใช้ทำแบบนี้ได้ เช่น Tkinter, Kivy, Wxpython เป็นต้น ในจำนวนนั้นตัวหนึ่งที่นิยมใช้กันอย่างกว้างขวางก็คือ Pyqt ซึ่งเป็นมอดูลสำหรับเขียนเฟรมเวิร์ก qt ด้วยภาษาไพธอน qt คือเฟรมเวิร์กสร้าง GUI ที่ได้รับความนิยมสูงและถูกใช้สร้างโปรแกรมต่างๆมามากมายแล้ว โดยเดิมมีพื้นฐานมาจากภาษา C++ แต่ก็ถูกพัฒนาขึ้นมาให้ใช้ในภาษาต่างๆเช่น Java, PHP, Python, Ruby, ฯลฯ ดังนั้นถ้าใช้ Pyqt เป็นแล้วหากจะเปลี่ยนไปเขียน GUI โดยใช้ qt ในภาษาอื่นก็ทำได้ไม่ยาก เพราะใช้พื้นฐานร่วมกัน qt นั้นได้ถูกพัฒนาขึ้นมาเรื่อยๆ ปัจจุบันเวอร์ชัน qt6 เพิ่งจะออกมา โดยมอดูลของ qt6 ในไพธอนนั้นมีชื่อว่า Pyqt6 แต่เนื่องจาก qt6 เพิ่งออกและยังมีข้อมูลน้อยอยู่ ในที่นี้จะยังคงสอน qt5 เป็นหลัก จนกว่า qt6 จะเริ่มอยู่ตัวและถูกใช้งานอย่างกว้างขวาง ถึงตอนนั้นก็อาจจะกลับมาแก้เนื้อหาทั้งหมดเป็น qt6 นอกจาก Pyqt แล้วก็ยังมี Pyside ที่เป็นมอดูลสำหรับใช้ qt ในไพธอนเช่นกัน ซึ่งแท้จริงแล้ว 2 ตัวนี้มีข้อแตกต่างกันตรงที่แค่ถูกพัฒนาขึ้นโดยคนละบริษัท และมีเงื่อนไขด้านลิขสิทธิ์การใช้งานแตกต่างกันเล็กน้อย และคำสั่งภายในนั้นมีความแตกต่างกันอยู่บ้างแต่โดยรวมแล้วส่วนใหญ่เหมือนกัน

โดยโครงงานปริญญานิพนธ์นี้ใช้ Pyqt ในการสร้างและออกแบบ GUI ในส่วนของระบบตรวจจับและตอบโต้การโจมตี โดยใช้ QT Designer ในการช่วยออกแบบ

2.2 งานวิจัยที่เกี่ยวข้อง

Sheikh Md. Rabiul Islam กล่าวไว้ในปี ค.ศ. 2013 [9] ว่า มาตรฐาน IEEE 802.11i แทนที่ Wired Equivalent Privacy (WEP) และคุณลักษณะด้านความปลอดภัยอื่น ๆ ของ IEEE ดั้งเดิมอย่างเป็นทางการ มาตรฐาน 802.11 มาตรฐานการควบคุมการเข้าถึงเครือข่ายที่ใช้พอร์ต IEEE 802.1x เป็นวิธีการเสริมสำหรับการตรวจสอบสิทธิ์ 802.11 ไร้สาย ลูกค้า โดยได้ทดลองใช้ซอฟต์แวร์ Aircrack-ng สำหรับแครคคีย์ที่ใช้พิสูจน์ตัวจริง ของ WPA (PSK) การทดสอบด้วยคีย์ ASCII แบบธรรมดาและ คีย์ Hexa-decimal ที่ซับซ้อนพบว่าสามารถถูกโจมตีได้หรือไม่

Jose-Ignacio Castillo-Velazquez และคณะ [10] ได้กล่าวไว้ ตั้งแต่ ปี ค.ศ. 2004 ว่ามันเป็นเรื่องปกติทั่วไป ที่จะใช้ WPA2 แทนที่ WPA ที่ถูกทำลายแล้วสำหรับความมั่นคงของเครือข่ายท้องถิ่นแบบไร้สาย (WLAN) WPA เข้ามาแทนที่ WEP ในปี ค.ศ. 2003 เนื่องจากโพรโทคอลรักษามั่นคงปลอดภัยแรกนั้นไม่ปลอดภัย และปัญหาด้านความมั่นคงของ WLAN คือ พบปัญหาของ WPA2 ในปี ค.ศ. 2017 แต่ยังไม่มี WPA3 ซึ่งกำลังอยู่ระหว่างการพัฒนา ดังนั้นในขณะนี้ ผู้คนจึงกำลังหาวิธีการด้านความมั่นคงให้กับ WLAN ของตัวเอง งานวิจัยนี้ เสนอข้อแนะนำในการปรับแต่งให้ระบบเข้มแข็ง (Hardening) ที่ได้รับการพิสูจน์แล้วว่า ได้ผลจริงจากการวิเคราะห์ในสถานการณ์ทดสอบ ผลลัพธ์ที่ได้แสดงให้เห็นว่า WLAN มีความมั่นคงมากขึ้นเมื่อทำการ Hardening

จะเห็นได้ว่าปัญหาด้านความปลอดถัยของ WLAN เป็นที่น่าสนใจในหลายงานวิจัยในโครงงานปริญญานิพนธ์นี้สนใจจะแก้ไขปัญหา การโจมตีด้วยเทคนิค Evil Twin Attack และ Rogue Access Point โดยมี Production ของเอกชนที่ได้พยายามแก้ไขปัญหาเดียวกันนี้ โดยจะได้กล่าวถึงต่อไป

Aruba Airwave Multivendor, On-premises Campus Network Management [11] เป็นซอฟต์แวร์ที่สามารถจัดการเครือข่ายที่มีสิทธิ์ใน ARUBA โดยสามารถตรวจสอบสถานะเครือข่ายไร้สายและ วิเคราะห์คุณภาพของสัญญาณ ตรวจหาตำแหน่งได้ และตรวจสอบ Rogue Access Point ในระยะโดยรอบได้

2.3 ตารางเปรียบเทียบระบบ

ตารางเปรียบเทียบฟังก์ชันของระบบ Aruba Airwave กับโครงงาน Detection and Response System Against The Evil Twin Attack

ตารางที่ 2.1 ตารางเปรียบเทียบฟังก์ชัน

Function	Detail	Aruba Airwave	Detection and Response System Against The Evil Twin Attack
Detect Rogue Access Point	ตรวจสอบ Access Point ที่ไม่ได้ลงทะเบียนไว้ได้ (Rogue Access Point)	✓	✓
Detect Evil Twin Attack	ตรวจสอบ Access Point ที่เป็นการโจมตีด้วยเทคนิค Evil Twin Attack		✓
Resolve Client Data of Access Point	กู้คืนข้อมูลของ Client ที่ล้มเหลวไปได้	✓	
REAL-TIME VISIBILITY AND CONTROL	แสดงผลและควบคุมการทำงานของ Access Point ได้แบบ Real-Time	✓	
Tracks Access Point Position	ตรวจสอบตำแหน่งที่ทำการติดตั้ง Access Point ได้	✓	✓
Response Evil Twin Attack	การตอบโต้การโจมตีด้วยเทคนิค Evil Twin Attack ได้		✓
Notification	แจ้งเตือนเมื่อมีปัญหา Evil Twin Attack ผ่านช่องทาง Line , E-mail ได้		✓