การประเมินผลกระทบการโจมตีเครือข่ายไร้สายด้วยวิธี De-Authentication

อภิสิทธิ์ พลท่ากลาง

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม
วิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์
มหาวิทยาลัยธุรกิจบัณฑิตย์
พ.ศ. 2562

Impact Assessment of Wireless Network Attack using De-Authentication Method

Apisit Polthaklang

A Thematic Paper Submitted in Partial Fulfillment of the Requirements

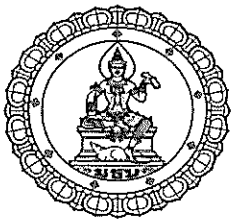
For the Degree of Master of Engineering

Department of Computer and Telecommunication Engineering

College of Innovative Technology And Engineering

Dhurakij Pundit University

2019



ใบรับรองสารนิพนธ์

วิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์

มหาวิทยาลัยธุรกิจบัณฑิตย์

ปริญญา วิศวกรรมศาสตรมหาบัณฑิต

หัวข้อสารนิพนธ์ การประเมินผลกระทบจากการโจมตีเครือข่ายไร้สายด้วยวิธี De-Authentication Attacks

เสนอโดย ร.ท.อภิสิทธิ์ พลท่ากลาง

สาขาวิชา วิศวกรรมคอมพิวเตอร์และโทรคมนาคม

อาจารย์ที่ปรึกษาสารนิพนธ์ อาจารย์ ดร.ชัยพร เขมะภาตะพันธ์

ได้พิจารณาเห็นชอบโดยคณะกรรมการสอบสารนิพนธ์แล้ว

.....ประธานกรรมการ

(อาจารย์ ดร.ประศาสน์ จันทราทิพย์)

.....กรรมการและอาจารย์ที่ปรึกษาสารนิพนธ์

(อาจารย์ ดร.ชัยพร เขมะภาตะพันธ์)

.....กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.มัชฌิกา อ่องแตง)

วิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์รับรองแล้ว

.....คณบดีวิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์

(ผู้ช่วยศาสตราจารย์ ดร.ณรงค์เดช กีรติพรานนท์)

วันที่ ...18.... เดือน ...สิงหาคม... พ.ศ. ...2562...

หัวข้อสารนิพนธ์	การประเมินผลกระทบการโจมตีเครือข่ายไร้สาย ด้วยวิธี De-Authentication
ชื่อผู้เขียน	อภิสิทธิ์ พลท่ากลาง
อาจารย์ที่ปรึกษา	อาจารย์ ดร.ชัยพร เขมะภาตะพันธ์
สาขาวิชา	วิศวกรรมคอมพิวเตอร์และโทรคมนาคม
ปีการศึกษา	2561

บทคัดย่อ

งานวิจัยนี้เป็นการประเมินผลกระทบที่เกิดขึ้นจากการโจมตีเครือข่ายไร้สายด้วยวิธี De-Authentication โดยจะทำการปลอมแปลงแมคแอดเดรสของอุปกรณ์กระจายสัญญาณเครื่องเป้าหมาย และดำเนินการโจมตีด้วยการส่งเฟรม Deauthentication ไปยังเครื่องคอมพิวเตอร์ที่กำลังเชื่อมต่อหรือติดต่อสื่อสารอยู่กับอุปกรณ์กระจายสัญญาณเป้าหมาย ซึ่งจะทำให้เครื่องคอมพิวเตอร์ที่ได้รับเฟรมดังกล่าวนั้น เกิดความเข้าใจว่าได้รับการขอยกเลิกการเชื่อมต่อการปฏิเสธหรือการไม่สามารถให้บริการได้จากอุปกรณ์กระจายสัญญาณไวไฟ โดยจะดำเนินการทดสอบการส่งสัญญาณการรบกวนหรือโจมตีในสภาวะที่มีความแตกต่างกัน จำนวน 4 รูปแบบการทดสอบ ประกอบด้วย การใช้งานในพื้นที่โล่งระดับสายตา ในพื้นที่ห้องทั่วไป ภายใต้การทำงานของมาตรฐาน IEEE 802.11g และ IEEE 802.11n

ผลการทดสอบ พบว่าผู้วิจัยสามารถดำเนินการรบกวนหรือโจมตีเครือข่ายไร้สายของทั้ง 4 รูปแบบการทดสอบได้จริง โดยค่าประสิทธิภาพของการโจมตีจะมีค่าลดลง เมื่อระยะของการทดสอบเพิ่มมากขึ้น ซึ่งทั้งสองมาตรฐาน IEEE 802.11g และ n มีผลที่ใกล้เคียงกัน และการโจมตีในพื้นที่โล่งแนวระดับสายตาสามารถดำเนินการได้ในระยะที่ไกลกว่าการโจมตีในพื้นที่ห้องทั่วไป ประมาณ 3.5 เท่า

Thematic Paper Title	Impact Assessment of Wireless Network Attack using De-Authentication Method
Author	Apisit Polthaklang
Thematic Advisor	Dr. Chaiyaporn Khemapatapan
Department	Computer and Telecommunication Engineering
Academic Year	2018

ABSTRACT

This research aims to assess the impact of wireless network attacking using de-authentication method. The attacking method is based on spoofing MAC address of target devices. Then, de-authentication frame with spoofed MAC address will be periodically sent to target devices. Consequently, devices received faked de-authentication frames from the connected wifi access point will terminate themselves from the current connections. Testing relies on 4 scenarios based on indoor/outdoor areas and IEEE 802.11g/n standards.

From the testing results, researcher can successfully attack all 4 wifi network scenarios. The success rate of attack decreases while the distance between attacker and wifi access point increases. Both IEEE 802.11g/n standards give the similar performances. Attacking on an outdoor area can archive more distance than indoor area about 3.5 times.

กิตติกรรมประกาศ

สารนิพนธ์นี้สำเร็จลุล่วงไปได้อย่างสมบูรณ์ โดยได้รับความอนุเคราะห์เป็นอย่างยิ่งจาก อาจารย์ ดร.ชัยพร เขมะภาตะพันธ์ อาจารย์ที่ปรึกษาสารนิพนธ์ที่ให้ข้อคิดเห็น คำแนะนำ คำปรึกษาที่เป็นประโยชน์ต่องานวิจัยและเอาใจใส่นักศึกษาเสมอมาตลอดจนแนะแนวทางในการแก้ไขปัญหาต่างๆ

ขอขอบคุณคณะอาจารย์ทุกท่าน เพื่อนร่วมรุ่น และเพื่อนร่วมงานที่คอยให้กำลังใจและเสนอแนะข้อมูลในการดำเนินงานสารนิพนธ์จนสำเร็จลุล่วงไปได้ด้วยดี

ขอขอบคุณมหาวิทยาลัยธุรกิจบัณฑิตย์

ท้ายสุดนี้ขอขอบคุณ พ่อ แม่ ภรรยา และบุตรธิดา ตลอดจนบุคคลในครอบครัวของผู้วิจัย ที่คอยให้กำลังใจและสนับสนุนผู้วิจัยในทุกๆ ด้าน ตลอดห้วงระยะเวลาการศึกษาจวบจนสำเร็จการศึกษา

อภิสิทธิ์ พลท่ากลาง

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญภาพ

ภาพที่ **หน้า**

สารบัญภาพ (ต่อ)

ภาพที่ **หน้า**

สารบัญภาพ (ต่อ)

ภาพที่ **หน้า**

บทที่ 1
บทนำ

1.1 หลักการและเหตุผล

ในปัจจุบันการใช้งานเครือข่ายไร้สาย Wireless หรือ wireless fidelity : Wi-Fi ได้รับความนิยมกันอย่างแพร่หลายเนื่องจากเครือข่ายแบบไร้สายไม้ได้มีการใช้สายสัญญาณในการเชื่อมต่อ แต่จะใช้คลื่นวิทยุเป็นช่องทางการสื่อสารแทนในการรับส่งข้อมูลระหว่างกันโดยผ่านอากาศเป็นตัวกลาง จึงทำให้เกิดความสะดวกในใช้งาน และที่สำคัญมีความง่ายในการติดตั้งใช้เวลาน้อย มีความเป็นระเบียบมากกว่าเครือข่ายแบบใช้สาย อย่างไรก็ตามเครือข่ายไร้สายยังมีข้อจำกัดในเรื่องของความปลอดภัยในหลายๆ ด้าน ซึ่งจากการที่เครือข่ายไร้สายใช้อากาศเป็นตัวกลางในการรับ – ส่งข้อมูล นั้น จึงไม่สามารถจำกัดขอบเขตด้านระยะทางของผู้รับและผู้ส่งได้อย่างชัดเจน ซึ่งอาจก่อให้เกิดปัญหาในด้านความมั่นคงปลอดภัยของเครือข่าย เช่น การโจมตีในรูปแบบต่างๆ การยืนยันตัวตน การจำกัดการใช้งานเครือข่ายโดยเฉพาะในเรื่องของการรักษาความลับ ซึ่งหากผู้ใดก็ตามที่อยู่ในระยะทางของการส่งสัญญาณก็จะสามารถเข้าถึงข้อมูลที่ทำการรับ-ส่งได้

การสื่อสารไร้สายโดยทั่วไปใช้มาตรฐาน IEEE 802.11 [1] ซึ่ง Institute of Electrical and Electronics Engineers : IEEE เป็นองค์กรที่กำหนดมาตรฐานการสื่อสารข้อมูลบนระบบเครือข่ายคอมพิวเตอร์ โดยได้กำหนดมาตรฐานสำหรับเครือข่าย Wireless LAN : WLAN ประกอบด้วยมาตรฐานย่อยต่างๆ เช่น a, b, g และ n รวมถึงอื่นๆ ซึ่งในแต่ละมาตรฐานย่อยนั้นจะมีการกำหนดคุณสมบัติต่างๆ สำหรับอุปกรณ์เครือข่ายแบบไร้สายที่แตกต่างกันออกไป เช่น ความเร็วในการรับ -ส่งข้อมูล การใช้งานคลื่นความถี่วิทยุในย่านความถี่สาธารณะ Industrial Scientific and Medical band : ISM Band นอกจากนี้ในมาตรฐาน IEEE 802.11 ยังกำหนดให้มีกลไกการเข้ารหัสข้อมูล (Encryption) และการตรวจสอบผู้ใช้ (Authentication) การเข้ารหัสเพื่อจำกัดการใช้งานข้อมูลให้อยู่ภายในกลุ่มที่รู้รหัสเท่านั้น อย่างไรก็ตาม เนื่องจากข้อมูลแพร่กระจายอยู่ในอากาศ และไม่จำกัดขอบเขตอยู่เพียงบริเวณเฉพาะหรือบริเวณแคบ ๆ เท่านั้น แต่สัญญาณของอุปกรณ์ไร้สายอาจแพร่ไปถึงบริเวณภายนอกขอบเขตความดูแล เนื่องจากข้อมูลทุกอย่างลอยอยู่บนอากาศ ซึ่งไม่สามารถมองเห็นและจับต้องไม่ได้ โดยปกติสถาปัตยกรรมของ IEEE 802.11 จะมีเฟรมการจัดการ เฟรมการ

ตรวจสอบสิทธิ์และเฟรมปฏิเสธการพิสูจน์ตัวตนซึ่งจะถูกส่งไปในอากาศแบบ Unencrypted ด้วยข้อความธรรมดาที่ไม่มีการเข้ารหัส ดังนั้นผู้ไม่หวังดีจึงสามารถดักจับรวมไปถึงปลอมแปลงเฟรมเหล่านี้ได้โดยวิธีการปลอมแปลงแมคแอดเดรส (MAC Address Spoofing) ของผู้ใช้งานหรือ AP ดังนั้นการรบกวนหรือการถูกโจมตีบนเครือข่ายไร้สาย 802.11a / b / g / n เช่นโจมตีแบบการปฏิเสธบริการ, Rogue AP, man-in-the-middle, การโจรกรรมข้อมูลประจำเครื่องใน Layer 2 และการโจรกรรมแบนด์วิดธ์ [2] จึงเป็นเรื่องที่พบเห็นได้บ่อย อีกทั้งในปัจจุบันความสามารถในการตรวจจับและรับมือเป็นไปได้ค่อนข้างยาก

จากสาเหตุดังที่กล่าวมาข้างต้น ผู้เขียนจึงมีแนวคิดที่จะศึกษาถึงขอบเขตความสามารถของการรบกวนหรือการโจมตีเครือข่ายไร้สายด้วยวิธี De-Authentication [3] โดยจะทำการปลอมแปลงแมคแอดเดรส (MAC Address Spoofing) ของอุปกรณ์กระจายสัญญาณ (Access Point : AP) เป้าหมาย และดำเนินการโจมตีด้วยการส่งเฟรม Deauthentication ไปยังเครื่องคอมพิวเตอร์ที่กำลังเชื่อมต่อหรือติดต่อสื่อสารอยู่กับอุปกรณ์กระจายสัญญาณเป้าหมาย ซึ่งจะทำให้เครื่องคอมพิวเตอร์ที่ได้รับเฟรม Deauthentication ดังกล่าวนั้น เกิดความเข้าใจว่าได้รับการขอยกเลิกการเชื่อมต่อการปฏิเสธหรือการ ไม่สามารถให้บริการได้ (Denial of Service : DoS) จากอุปกรณ์กระจายสัญญาณเป้าหมาย [4] ซึ่งการโจมตีด้วยวิธีนี้เป็นขั้นตอนหนึ่งที่สำคัญที่ Hacker สามารถนำไปใช้ในการแฮ็กพาสเวิร์ด หรือ Crack รหัสผ่านของเครือข่ายไร้สายต่อไปได้ จึงเป็นแรงจูงใจประการหนึ่งที่ทำให้ผู้วิจัยอยากศึกษาถึงผลกระทบที่เกิดขึ้นจากการถูกโจมตีรวมไปถึงการหาแนวทางป้องกันหรือตรวจจับรับมือจากการโจมตีด้วยวิธีดังกล่าวข้างต้น โดยจะดำเนินการทดสอบในพื้นที่จริงในระยะของการส่งสัญญาณการรบกวนหรือโจมตีที่มีความแตกต่างกัน ในสภาวะการใช้งานในพื้นที่โล่งระดับสายตา (Line-Of-Sight : LOS) และการใช้งานในพื้นที่ห้องทั่วไป ภายใต้การทำงานของมาตรฐาน IEEE 802.11g และ IEEE 802.11n ในย่านความถี่ 2.4 GHz ซึ่งผู้เขียนมีความมุ่งหวังเป็นอย่างยิ่งว่าผลที่ได้จากการทดสอบวิจัยจะเป็นประโยชน์ต่อผู้ที่เกี่ยวข้องและสนใจ โดยสามารถนำไปประยุกต์ใช้เป็นแนวทางในการออกแบบเครือข่ายแบบไร้สาย เพื่อให้เกิดความปลอดภัย และความน่าเชื่อถือ (Reliability) ในการใช้งานเครือข่ายไร้สาย และเป็นแนวทางในการตรวจจับหรือรับมือหากเกิดการรบกวนเครือข่ายไร้สายด้วยวิธีการดังกล่าว

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อศึกษาการรบกวนหรือโจมตีเครือข่ายไร้สายด้วยวิธี De-Authentication โดยการปลอมแปลงแมคแอดเดรส (MAC Address Spoofing) ของอุปกรณ์กระจายสัญญาณ Access Point และดำเนินการรบกวนหรือโจมตีด้วยการส่งเฟรม Deauthentication ไปยังผู้ใช้งาน Wireless Client

1.2.2 เพื่อศึกษาถึงขอบเขตของระยะทางที่สามารถรบกวนหรือโจมตีในสภาวะการใช้งาน ในพื้นที่โล่งระดับสายตาและการใช้งานในพื้นที่ห้องทั่วไป

1.3 สมมติฐานการวิจัย

เพื่อเป็นแนวทางในการวิจัย ผู้วิจัยได้ตั้งสมมติฐานของการวิจัยดังนี้

1.3.1 ผู้ทำการวิจัยสามารถรบกวนหรือโจมตีเครือข่ายไร้สายตามมาตรฐาน IEEE 802.11b/g/n โดยสามารถทำให้เครื่องคอมพิวเตอร์ที่กำลังเชื่อมต่ออยู่กับอุปกรณ์กระจายสัญญาณเครื่องเป้าหมายเกิดการยกเลิกการเชื่อมต่อการปฏิเสธหรือการไม่สามารถให้บริการได้

1.3.2 สามารถทราบและประเมินขอบเขตของระยะทางที่สามารถสร้างผลกระทบหรือสามารถรบกวนหรือโจมตีในสภาวะการใช้งานในพื้นที่โล่งระดับสายตา และการใช้งานในพื้นที่ห้องทั่วไป

1.4 ขอบเขตการวิจัย

ผู้วิจัยได้กำหนดขอบเขตของการวิจัยไว้ดังนี้

1.4.1 ศึกษาถึงวิธีการโจมตีเครือข่ายไร้สายด้วยวิธี De-Authentication โดยการปลอมแปลงแมคแอดเดรสของอุปกรณ์กระจายสัญญาณและดำเนินการโจมตีด้วยการส่ง Deauth Frame แบบ Broadcast ไปยังผู้ใช้งานเป้าหมาย Wireless Client

1.4.2 ดำเนินการรบกวนหรือโจมตีในสภาวะการใช้งานในพื้นที่โล่งระดับสายตาและการใช้งานในพื้นที่ห้องทั่วไป

1.4.3 ดำเนินการทดสอบภายใต้การทำงานของมาตรฐาน IEEE 802.11b/g/n ในย่านความถี่ 2.4 GHz. โดยใช้อุปกรณ์อุปกรณ์ Access Point ตราอักษร ZTE Model F668 Hardware Version v5.2 Software Version V5.2.10P3T7

1.4.5 ดำเนินการทดสอบภายใต้การกำหนดค่าระบบรักษาความปลอดภัยแบบ WEP WPA และ WPA2

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 สามารถเข้าใจถึงวิธีการโจมตีเครือข่ายไร้สายด้วยการปลอมแปลงแมคแอดเดรสของอุปกรณ์กระจายสัญญาณและการโจมตีด้วยการส่งแพ็คเกจ DeAuth ไปยังผู้ใช้งาน Wireless Client ที่ใช้ในการรบกวนหรือโจมตีเครือข่ายแบบไร้สาย

1.5.2 ผู้ที่สนใจสามารถนำผลที่ได้จากการทดสอบไปประยุกต์ใช้เป็นแนวทางในการออกแบบเครือข่ายไร้สาย เพื่อให้เกิดความปลอดภัย และมีความน่าเชื่อถือ (Reliability) ในการใช้งาน

1.5.4 เพื่อเป็นแนวทางในการตรวจจับและรับมือหากเกิดการโจมตีหรือบุกรุกเครือข่ายไร้สาย

บทที่ 2
แนวคิดทฤษฎีและงานวิจัยที่เกี่ยวข้อง

งานวิจัยนี้เป็นการศึกษาถึงขอบเขตความสามารถของการโจมตีเครือข่ายไร้สายด้วยวิธี De-Authentication [3] โดยจะทำการปลอมแปลงแมคแอดเดรส (MAC Address Spoofing) ของอุปกรณ์กระจายสัญญาณ (Access Point : AP) เป้าหมาย และดำเนินการโจมตีด้วยการส่งเฟรม Deauthentication ไปยังเครื่องคอมพิวเตอร์ที่กำลังเชื่อมต่อหรือติดต่อสื่อสารอยู่กับอุปกรณ์กระจายสัญญาณเป้าหมาย [4] ซึ่งประกอบด้วยข้อมูลทฤษฎีและงานวิจัยที่เกี่ยวข้องดังต่อไปนี้

2.1 ความเป็นมาของระบบเครือข่ายไร้สาย

2.2 มาตรฐานของเครือข่ายไร้สาย

2.3 เทคโนโลยีการส่งสัญญาณในเครือข่ายไร้สาย

2.4 โครงสร้างและรูปแบบการเชื่อมต่อ

2.5 พื้นที่ให้บริการเครือข่ายไร้สาย

2.6 ชื่อสำหรับให้บริการเครือข่ายไร้สาย

2.7 กลไกการสื่อสารข้อมูลของเครือข่ายไร้สาย

2.8 กลไกการรักษาความปลอดภัยในการตรวจสอบผู้ใช้ (Authentication)

2.9 เฟรมที่ใช้ในการจัดการ (Management Frame)

2.10 ช่องโหว่ ภัยคุมคาม และการโจมตี

2.11 ชนิดของการโจมตี (Type of Attacks)

2.12 กระบวนการโจมตีเครือข่ายไร้สายด้วยวิธี De-Authentication

2.13 งานวิจัยที่เกี่ยวข้อง

2.1 ความเป็นมาของระบบเครือข่ายไร้สาย (Wireless Network) [5]

เครือข่ายไร้สายได้รับการพัฒนาขึ้นมาใช้งานครั้งแรกเมื่อปี 1998 โดยใช้ความถี่ในย่าน 900 เมกกะเฮิรตซ์ แต่ความถี่ช่วงนี้ไม่สามารถใช้งานได้ในบางประเทศเนื่องจากเป็นย่านความถี่ที่ใช้กับโทรศัพท์มือถือ ต่อมาในปี 1992 หน่วยงาน IEEE (Institute of Electrical and Electronics Engineers) ได้ออกมากำหนดมาตรฐานของเครือข่ายไร้สายท้องถิ่น ได้แบ่งเป็น 3 กลุ่มได้แก่ กลุ่มที่ใช้ย่านความถี่ 2.4 GHz กลุ่มที่ใช้ความถี่ย่าน 5 GHz และกลุ่มที่ใช้ความถี่ย่านอินฟาเรด (Infrared) ตามลำดับ ซึ่งปัจจุบันย่านความถี่ที่เป็นที่นิยมใช้มากที่สุดคือ ย่านความถี่ 2.4 กิกะเฮิรตซ์ ส่วนอินฟาเรดนั้นไม่นิยมใช้เนื่องจากมีความเร็วในการส่งข้อมูลต่ำและแสงอินฟาเรดไม่สามารถเดินทางทะลุสิ่งกีดขวางได้เครือข่ายไร้สายเป็นระบบการสื่อสารข้อมูลที่มีความคล่องตัวมาก ซึ่งอาจจะนำมาใช้ทดแทนหรือต่อรวมกันกับระบบเครือข่ายใช้สายแบบดั้งเดิม โดยใช้การส่งคลื่นความถี่วิทยุในย่านวิทยุ RF และ คลื่นอินฟราเรด ในการรับและส่งข้อมูลระหว่างคอมพิวเตอร์แต่ละเครื่องผ่านอากาศโดยปราศจากความต้องการของการเดินสาย นอกจากนั้นระบบเครือข่ายไร้สายก็ยังมีคุณสมบัติครอบคลุมทุกอย่างคล้ายกับระบบเครือข่ายที่ใช้สาย ที่สำคัญก็คือการที่ไม่ต้องใช้สายนำสัญญาณทำให้สามารถเคลื่อนย้ายและทำให้การใช้งานทำได้สะดวก ไม่เหมือนระบบเครือข่ายแบบใช้สายที่ต้องใช้เวลาและการลงทุนในการปรับเปลี่ยนตำแหน่งการใช้งานเครื่องคอมพิวเตอร์

2.2 มาตรฐานเครือข่ายไร้สาย [6]

เครือข่ายไร้สายท้องถิ่นที่ใช้งานกันส่วนใหญ่ถูกพัฒนาขึ้นมาตามมาตรฐาน 802.11 โดยสาเหตุที่มาตรฐานนี้ถูกใช้งานมากและได้กลายเป็นอุปกรณ์ที่ใช้กันมาก เนื่องจากใช้คลื่นวิทยุที่มีกำลังสูงพอที่จะทะลุทะลวงสิ่งกีดขวางได้ดี สามารถมีรัศมีการใช้งานภายในอาคารได้ไกลถึงประมาณ 100 เมตร และในที่ไม่มีสิ่งกีดขวางได้ไกลถึงประมาณ 400 เมตร (ซึ่งนี่เป็นค่ามาตรฐานแต่การใช้งานในทางปฏิบัติอาจน้อยกว่านี้ถึงสามเท่า) และมีความเร็วในการทำงานสูงสุดถึง 11 – 300 เมกะบิตต่อวินาที นั่นก็เร็วพอที่จะนำมาใช้แทนระบบเครือข่ายแบบใช้สายได้ โดยมาตรฐานแต่ละมาตรฐานมีการโมดูเลตสัญญาณที่ต่างกัน และใช้ความถี่ต่างกัน จึงมีประสิทธิภาพที่ต่างกันด้วย

2.2.1 มาตรฐาน IEEE 802.11g เป็นมาตรฐานเครือข่ายไร้สายที่มีกลไกการส่งสัญญาณแบบ DSSS และ OFDM โดยรับส่งข้อมูลด้วยการใช้สัญญาณวิทยุความถี่ 2.4 GHz ด้วยความเร็วสูงสุดที่ 54 Mbps และมีความสามารถทำงานร่วมกับเครือข่ายไร้สายตามมาตรฐานIEEE 802.11b ได้โดยไม่ต้องปรับเปลี่ยนฮาร์ดแวร์ใหม่ใดๆ ทั้งสิ้น (Backward Compatibility)ซึ่งที่ความเร็วสื่อสาร 1, 2, 5.5 และ 11Mbps จะทำการส่งสัญญาณด้วยเทคนิค DSSS ส่วนความเร็ว 6, 9, 12, 18, 24, 36, 48, 54 Mbps ส่งสัญญาณด้วยการมัลติเพล็กซ์แบบ OFDM

2.2.2 มาตรฐาน IEEE 802.11nมาตรฐาน IEEE 802.11n เป็นเครือข่ายไวร์เลสที่ตามทฤษฎีแล้วจะให้ความเร็วสูงสุดถึง 600 Mbps ซึ่งตามมาตรฐานแล้วจะพบว่ามีความเร็วมากกว่ามาตรฐาน IEEE802.11g ถึง 12 เท่าโดยในมาตรฐาน IEEE 802.11n ได้เปลี่ยนวิธีการส่งสัญญาณวิทยุจากการใช้เสาเดียวทั้งการรับและการส่ง มาเป็นการใช้เสาหลายต้น หรือที่เรียกกันว่า MIMO (Multiple Input Multiple Output) ซึ่งช่วยทำให้รับส่ง สัญญาณด้วยความเร็วสูงมากขึ้น และทำให้มาตรฐาน IEEE 802.11n มีความเร็วเพิ่มขึ้น ดังนี้

2.2.2.1 การปรับลดค่า Guard interval (GI) ลงครึ่งหนึ่ง โดยค่า GI นี้คือระยะห่างระหว่างข้อมูลชุดหนึ่งๆ ที่ส่งออกไปในอากาศ ซึ่งจะช่วยป้องกันไม่ให้ข้อมูลเกิดการรบกวนระหว่างกัน โดยมาตรฐาน IEEE 802.11a/g มีค่า GI เท่ากับ 800 นาโนวินาที แต่มาตรฐาน IEEE 802.11n ได้ปรับลดค่า GI ลงเหลือครึ่งหนึ่ง คือ 400 นาโนวินาที

2.2.2.2 การใช้เทคนิค Spatial Multiplexing ในการทำงานของมาตรฐาน IEEE 802.11n จะใช้ช่องสัญญาณขนาด 20MHz และ 40MHz มีการใช้เทคนิค spatial multiplexing ทำให้สามารถใช้เสาหลายต้นในการส่งและรับข้อมูลขนานออกไปในช่องสัญญาณความถี่เดียวกัน ทำให้ไม่มีการกวนกันของสัญญาณ เมื่อจานวนชุดเสาอากาศคู่รับส่งเพิ่มขึ้น (Spatial stream) สามารถส่งข้อมูลได้เร็วขึ้น โดยมาตรฐานนี้กำหนดไว้สูงสุดที่ 4 Spatial stream มีความเร็ว stream ละ150 Mbps จึงทาให้มาตรฐาน 802.11n นี้มีความเร็วสูงสุดตามทฤษฎีที่ 600 Mbps

2.2.2.3 การเพิ่มจำนวนของคลื่นพาหะย่อย (Subcarrier) ในมาตรฐาน IEEE802.11n จะมีการเพิ่มคลื่นพาหะย่อย สาหรับส่งข้อมูลจากเดิม 48 ช่อง ไปเป็น 52 ช่อง บนช่องสัญญาณขนาด 20 MHz

2.2.2.4 การปรับปรุงส่วนการเข้ารหัสสาหรับป้องกันความผิดพลาดให้ทางานดีขึ้น กลไกนี้มีชื่อว่า FEC (Forward Error Correcting) ทางานโดยเพิ่มข้อมูลส่วนเกินสาหรับด้านรับเอาไว้ใช้ตรวจสอบและแก้ไขข้อผิดพลาด ตารางเปรียบเทียบคุณสมบัติของมาตรฐานเครือข่ายไร้สาย IEEE802.11g และ n มีความแตกต่างดังตารางที่ 2.1

ตารางที่ 2.1 การเปรียบเทียบเครือข่ายไร้สายมาตรฐาน IEEE 802.11g และ n [7]

มาตรฐานเครือข่ายไร้สาย	**802.11g**	**802.11n**
ความเร็วทางทฤษฎี	54Mbps	300Mbps
ความเร็วทางปฏิบัติ	18-27Mbps	100-150Mbps
ระดับความเร็ว	54Mbps,48Mbps,36Mbps,24 Mbps,12 Mbps,6 Mbps	300Mbps,270Mbps,240Mbps 180Mbps,120Mbps,90Mbps 60Mbps,30Mbps
คลื่นความถี่ที่ใช้	ISM Band2.4-2.4835GHz	ISM Band2.4-2.4835GHz UNII-1(5.150-5.250GHz) UNII-2(5.250-5.350GHz) UNII-3(5.725-5.825GHz)
โมดูเลตสัญญาณ	OFDM	MIMO
จำนวนช่องที่ไม่ทับซ้อน	3ช่อง(20MHz channel)	1 ช่องในย่าน 2.4GHz(40MHz channel) 3 ช่องในย่าน 2.4GHz(20MHz channel) 12 ช่องในย่าน 5GHz(40MHz channel) 24 ช่องในย่าน 5GHz(40MHz channel)

2.3 เทคโนโลยีการส่งสัญญาณในเครือข่ายไร้สาย [7]

เทคโนโลยีในการส่งสัญญาณมีอยู่ 2 ประเภท ได้แก่ ประเภทที่ใช้สัญญาณคลื่นความถี่วิทยุ และประเภทที่ใช้สัญญาณอินฟราเรดในการติดต่อรับส่งข้อมูล

2.3.1 ประเภทที่ใช้สัญญาณคลื่นความถี่วิทยุ

ระบบวิทยุแบบความถี่แคบ (Narrow Band Technology) เป็นการรับส่งความถี่ 902 เมกกะเฮิรตซ์ ถึง 928 เมกกะเฮิรตซ์, 2.14 เมกกะเฮิรตซ์ ถึง 2.484 เมกกะเฮิรตซ์และ 5.725 เมกกะเฮิรตซ์ ถึง 5.850 เมกกะเฮิรตซ์ สัญญาณจะมีกำลังต่ำ (โดยทั่วไปประมาณ 1 มิลลิวัตต์) และใช้ในการรับ-ส่งข้อมูลระหว่างต้นทางกับปลายทางเพียง 1 คู่เท่านั้น- ระบบเครือข่ายที่ไร้สายส่วนใหญ่มักนิยมใช้เทคนิค Spread Spectrum Technology ซึ่งใช้ความถี่ที่กว้างกว่าระบบวิทยุความถี่แคบ ซึ่ง Spread Spectrum คือ ช่วงความถี่ระหว่าง 902-928 เมกกะเฮิรตซ์ และ 2.4-2.484 กิกะกะเฮิรตซ์ โดยการส่งสัญญาณ

เทคนิค Spread Spectrum สามารถแบ่งได้เป็น 2 แบบคือ Direct Sequence และ Frequency-Hopping- Direct Sequence Spread Spectrum (DSSS) เป็นเทคนิคที่ยังใช้คลื่นพาหะที่ต้องระบุความถี่ที่ใช้ โดยสามารถส่งข้อมูลได้มากกว่าแบบ Narrow Band วิธีนี้เป็นวิธีที่เหมาะกับสภาพแวดล้อมที่มีการแทรกสอดรบกวนจากคลื่นวิทยุอื่น ๆ อย่างรุนแรง- Frequency Hopping Spread Spectrum (FHSS) การส่งสัญญาณรูปแบบนี้จะใช้ความถี่แคบพาหะเพียงความถี่เดียว (Narrow Band) โดยเน้นการนำไปใช้งาน ถ้าคำนึงถึงปัญหาทางด้านประสิทธิภาพและคลื่นรบกวนก็ควรใช้ วิธี DSSS ถ้าต้องการใช้ Adapter ไร้สายขนาดเล็กและราคาไม่แพงสำหรับเครื่อง Notebook หรือเครื่อง PDA ก็ควรเลือกแบบ FHSS- Orthogonal Frequency Division Multiplex (OFDM) เทคนิคนี้ถูกนำมาใช้เพื่อเพิ่มความเร็วในการส่งข้อมูลตามมาตรฐานใหม่ ๆ ของระบบเครือข่ายไร้สาย คือ IEEE 802.11a และ 802.11g การส่งสัญญาณคลื่นวิทยุแบบนี้เป็นการ Multiplex สัญญาณโดยช่องสัญญาณความถี่จะถูกแบ่งออกเป็นความถี่พาหะย่อย (subcarrier) หลาย ๆ ความถี่ โดยแต่ละความถี่พาหะย่อยจะตั้งฉากซึ่งกันและกัน ทำให้มันเป็นอิสระต่อกัน ความถี่ที่คลื่นพาหะที่ตั้งฉากกันนั้นทำให้ไม่มีปัญหาการซ้อนทับของสัญญาณที่อยู่ติดกัน

2.3.2 ใช้เทคโนโลยีอินฟาเรด (Infrared Technology)

ลำแสงอินฟราเรด (Infrared : IR) เป็นส่วนหนึ่งของสเปกตรัมแม่เหล็กไฟฟ้าอยู่ในย่านความถี่ของแสงที่อยู่ต่ำกว่าแสงสีแดงที่ตาของคนเราจะไม่สามารถมองเห็น ถูกนำมาใช้เพื่อการสื่อสารที่ใช้ในระยะใกล้ ได้แก่ อุปกรณ์ควบคุมแบบไร้สาย (Wireless Remote Control)ที่ควบคุมเครื่องรับโทรทัศน์ เครื่องเล่นวีดีโอ เครื่องคอมพิวเตอร์ Notebook คุณสมบัติเด่นของคลื่นอินฟราเรดและคลื่นสั้น คือ เดินทางเป็นแนวตรง ราคาถูก และง่ายต่อการผลิตใช้งาน แต่คลื่นประเภทนี้ไม่สามารถเดินทางผ่านวัตถุหรือสิ่งกีดขวางได้

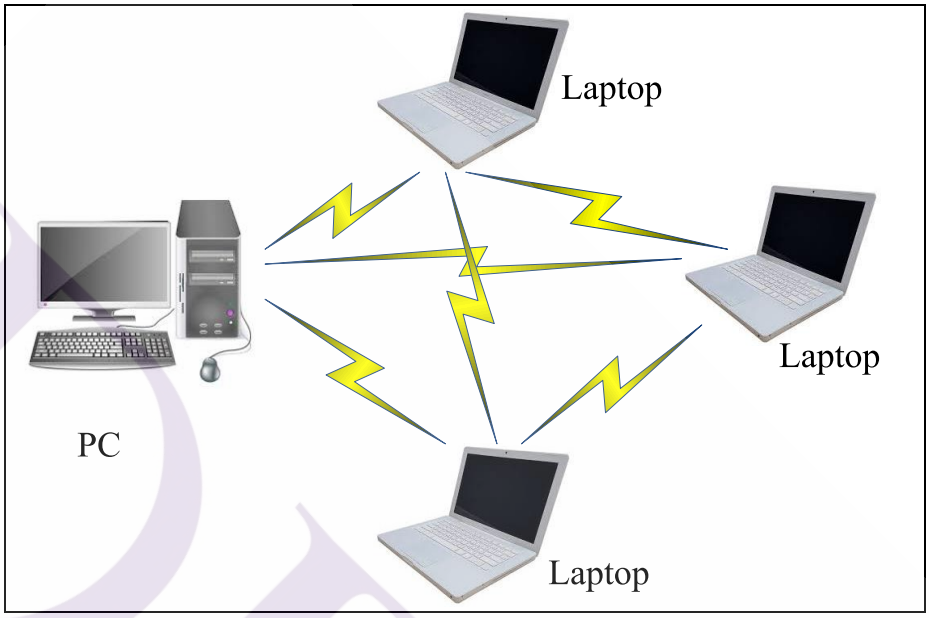
2.4 โครงสร้างและรูปแบบการเชื่อมต่อ [8]

รูปแบบการเชื่อมต่อของเครือข่ายไร้สายประกอบด้วยกัน 2 ส่วนหลักดังต่อไปนี้

2.4.1 การเชื่อมโยงระบบแบบ Ad-hoc หรือ Peer-to-Peer

เป็นรูปแบบที่เครื่องคอมพิวเตอร์ไร้สายต่างๆ เป็นอิสระต่อกัน ที่จะสื่อสารไปมาระหว่างกันโดยไม่ต้องพึ่งพาอาศัย Access Point ดังรูปที่ 2.1 เราเรียกรูปแบบการเชื่อมต่อนี้ว่าเครือข่าย Ad-hoc รูปแบบการเชื่อมต่อระบบเครือข่ายไร้สายแบบ ad hoc เป็นลักษณะการเชื่อมต่อแบบเครือข่ายโดยตรงระหว่างเครื่องคอมพิวเตอร์จำนวน 2 เครื่องหรือมากกว่านั้น เป็นการใช้งานร่วมกันของ Wireless Network Adapter โดยไม่ได้มีการเชื่อมต่อกับเครือข่ายแบบใช้สายเลย โดยที่เครื่องคอมพิวเตอร์แต่ละเครื่องจะมีความเท่าเทียมกัน สามารถทำงานของตนเองได้และขอใช้บริการจาก

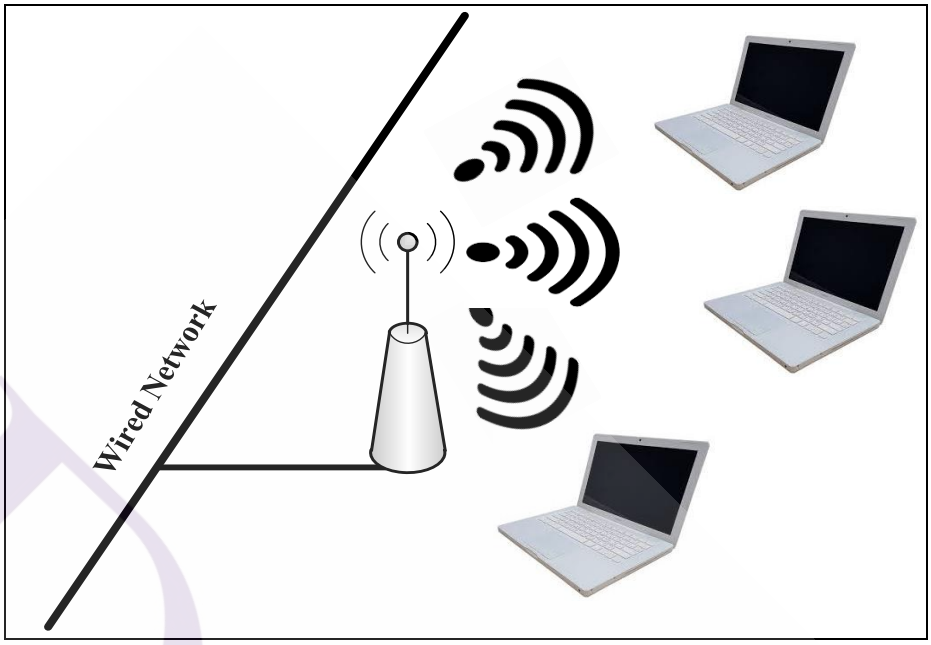
เครื่องอื่นได้ เหมาะสำหรับการนำมาใช้งานเพื่อจุดประสงค์ในด้านความรวดเร็วหรือติดตั้งได้โดยง่าย



ภาพที่ 2.1 ลักษณะการเชื่อมต่อแบบ Ad-hoc

2.4.2 การเชื่อมโยงระบบแบบ Infrastructure หรือ Client/Server

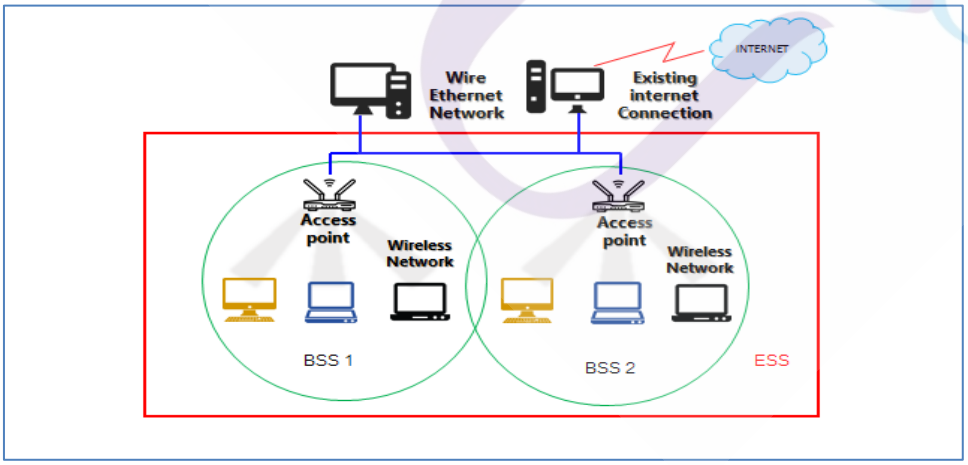
โครงสร้างการเชื่อมโยงแบบ Infrastructure ในรูปที่ 2.2 มีข้อพิเศษกว่าระบบAd-hoc ตรงที่มี Access Point เป็นศูนย์กลางการเชื่อมโยง และเป็นส่วนที่ช่วยเชื่อมโยงการติดต่อกันระหว่างคอมพิวเตอร์ไร้สายและอุปกรณ์ต่าง ๆ เพื่อเข้าสู่เครือข่ายหลัก (Ethernet Backbone) รวมถึงควบคุมการสื่อสารข้อมูลของอุปกรณ์ไร้สาย



ภาพที่ 2.2 ลักษณะการเชื่อมต่อแบบ Infrastructure

2.5 พื้นที่ให้บริการเครือข่ายไร้สาย [9]

ความเข้าใจเกี่ยวกับพื้นที่ให้บริการเครือข่ายไร้สาย (Basic Service Set) หรือ BSS คือการที่อุปกรณ์ทุกอุปกรณ์ ที่อยู่ภายในรัศมีของสัญญาณที่กำหนดให้ใช้ช่องสัญญาณที่เหมือนกันสำหรับทำการสื่อสาร โดยข้อมูลจะถูกแพร่กระจายถึงกันได้ ดังรูปที่ 2.3

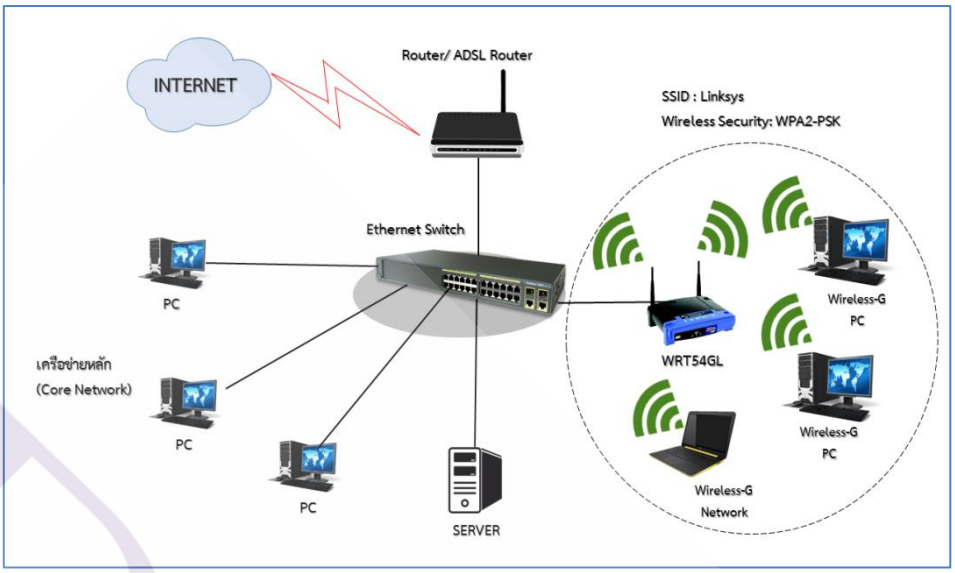


ภาพที่ 2.3 อธิบายพื้นที่ให้บริการ

จากรูปที่ 2.3 ขอบเขตพื้นที่ให้บริการหนึ่งพื้นที่เปรียบเสมือนหนึ่งกลุ่มพื้นที่ให้บริการ (Basic Service Set หรือ BSS) และการที่ไม่มี Access Point อยู่ตรงกลางจะเรียกว่า Ad-hocหากว่ามีหนึ่งพื้นที่ให้บริการแต่มี Access Point อยู่โดยไม่ทำการเชื่อมต่อกับเครือข่ายพื้นฐานที่มีสายก็จะถูกเรียกว่า พื้นที่บริการที่ไม่ขึ้นอยู่ใคร (Independent Basic Service Set) หรือหากมี Access Point และมีการเชื่อมต่อไปยังเครือข่ายพื้นฐานที่เป็นสายโดยใช้สายยูทีพีเราจะเรียกว่าเป็นแบบ Infrastructure ทันทีเครือข่ายแบบไร้สายที่ถูกออกแบบมาให้ผู้ที่ใช้งานสามารถเชื่อมโยงเครื่องคอมพิวเตอร์ไร้สายของตนเองเพื่อสื่อสารข้อมูลจากจุดใดๆ ได้อย่างอิสระภายในหนึ่งพื้นที่ให้บริการแต่เมื่อใดก็ตามที่ผู้ใช้งานเคลื่อนย้ายออกนอกพื้นที่ให้บริการ เครื่องคอมพิวเตอร์ไร้สายก็จะไม่สามารถทำการเชื่อมโยงเพื่อใช้งานเครือข่ายไร้สายได้ ดังนั้นมาตรฐาน IEEE 802.11 จึงมีโครงสร้างการเชื่อมโยงแบบหนึ่ง ซึ่งสามารถเพิ่มพื้นที่บริการให้ไกลออกไป โครงสร้างดังกล่าวนี้เรียกว่า พื้นที่บริการที่ถูกขยายออก (Extend Service Set หรือ ESS) ซึ่งภายในโครงสร้างเครือข่ายไร้สายแบบ ESS จะประกอบไปด้วย ระบบ Infrastructure หลายระบบรวมอยู่ด้วยกัน โดยแต่ละ Infrastructure จะถูกเชื่อมโยงกันผ่านเครือข่ายแบบมีสายดังรูปที่ 2.3 ซึ่งผู้ใช้งานสามารถที่จะเคลื่อนย้ายการทำงานจากจุดหนึ่งไปยังอีกจุดหนึ่งภายใน Infrastructure ทั้งสองพื้นที่

2.6 ชื่อสำหรับการให้บริการเครือข่ายไร้สาย [9]

ชื่อสำหรับการให้บริการเครือข่ายไร้สาย (Service Set Identifier) เป็นกลุ่มตัวอักษรที่มีขนาดความยาวไม่เกิน 32 ตัวอักษร ใช้เป็นชื่ออ้างอิงกลุ่มของการให้บริการ (Service Set) ของเครือข่ายไร้สาย ทุกอุปกรณ์ที่ต้องการสื่อสารข้อมูลกันระหว่างเครือข่ายไร้สายที่เป็นแบบการเชื่อมทั้งในแบบ Ad-hoc และ Infrastructure ที่ผ่าน Access Point ที่อยู่ในพื้นที่ให้บริการนั้น ๆ โดยจะต้องระบุ Service Set ID หรือ SSID ของตนเองให้เป็นชื่อเดียวกัน และหากไม่ทำการกำหนดให้เป็นชื่อเดียวกันอุปกรณ์นั้นก็จะไม่สามารถสื่อสารหรือเชื่อมโยงกันได้ดังรูปที่ 2.4



ภาพที่ 2.4 การกำหนด SSID ในพื้นที่ให้บริการ

จากรูปที่ 2.4 ในพื้นที่วงกลมที่เป็นเส้นปะ เป็นพื้นที่หนึ่งพื้นที่ให้บริการ (Service Set) ที่จะต้องมีการกำหนด SSID ให้เป็นชื่อเดียวกันมิเช่นนั้นก็จะไม่สื่อสารหรือทำการเชื่อมโยงกับอุปกรณ์ไร้สายภายในพื้นที่ให้บริการได้เลย

2.7 กลไกการสื่อสารข้อมูลของเครือข่ายไร้สาย [9]

บนเครือข่ายไร้สายประกอบไปด้วยอุปกรณ์ต่าง ๆ มากมาย เช่น Access Point ปริ๊นเตอร์ไร้สาย และเครื่องคอมพิวเตอร์เป็นต้น อุปกรณ์เหล่านี้สื่อสารข้อมูลถึงกันผ่านสื่อกลางที่เป็นอากาศ โดยอุปกรณ์ทุกชนิดมีสิทธิ์ครอบครองและเข้าใช้งานสื่อกลางสำหรับสื่อสารข้อมูลกันอย่างเท่าเทียมกัน หากไม่มีกลไกควบคุม และต่างคนต่างส่งข้อมูลโดยไม่มีการตรวจสอบก่อนว่าในเวลาขณะนั้นมีคนอื่นกำลังใช้สื่อกลางการส่งข้อมูลอยู่หรือไม่ ผลที่ตามมาก็คือ การสื่อสารบนระบบเครือข่ายไร้สายอาจล้มเหลว อันเนื่องมาจากเกิดการชนกันของข้อมูลในระหว่างการส่ง(Collision) มาตรฐาน 802.11 จึงได้มีการกำหนดกลไกขึ้นมาสำหรับควบคุม โดยหากเปรียบเทียบง่าย ๆ ก็คือสื่อกลางก็เป็น ถนนสาธารณะเป็นเส้นทางส่งข้อมูลจากต้นทางไปยังปลายทาง อุปกรณ์ไร้สายทุกอันมีสิทธิ์ใช้ถนนสาธารณะนี้ได้เท่าเทียมกันดังนั้นจึงได้มีการกำหนดข้อตกลงขึ้นมา โดยมาตรฐาน 802.11 ให้ใช้ CSMA/CA (Carrier Sense Multiple Access With Collision Avoidance) เป็นกลไกควบคุมการใช้งานสื่อกลางสำหรับสื่อสารข้อมูลของอุปกรณ์ไร้สายบนเครือข่ายไร้สาย และนี่ก็เป็นบทบาทหนึ่งของ MAC Layer ในมาตรฐานIEEE 802.11 คือการ

จัดสรรการเข้าใช้ช่องสัญญาณเพื่อใช้สื่อสารกัน ซึ่งแต่ละสถานีใน BSSหรือ IBSS จะต้องแบ่งกันใช้ช่องสัญญาณที่ถูกกำหนดมาสำหรับใช้งานร่วมกันอย่างเป็นธรรมซึ่งมาตรฐาน IEEE 802.11 ได้กำหนดให้ใช้กลไก CSMA/CA เพื่อจัดสรรการใช้ช่องสัญญาณร่วมกันดังนี้

- CSMA with Random Back-Off เป็นกลไกของ CSMA ที่เป็นวิธีการอย่างง่ายสำหรับจัดสรรการเข้าใช้ช่องสัญญาณของผู้ใช้แต่ละอุปกรณ์ไร้สายอย่างยุติธรรม กลไกนี้เป็นที่ยอมรับและนิยม ใช้กันอย่างแพร่หลาย เช่น ในมาตรฐาน IEEE 802.3 Ethernet LAN หลักการทำงานของกลไก CSMA คือ เมื่อสถานีหนึ่งต้องการเข้าใช้ช่องสัญญาณ สถานีดังกล่าวจะต้องตรวจสอบช่องสัญญาณก่อนว่ามีสถานีอื่นทำการรับส่งสัญญาณข้อมูลอยู่หรือไม่ และรอจนกว่าช่องสัญญาณจะว่าง เมื่อช่องสัญญาณว่างแล้วสถานีที่ต้องการเข้าใช้ช่องสัญญาณจะต้องรอต่อไปอีกระยะหนึ่ง (Random Back-Off) ซึ่งแต่ละสถานีได้กำหนดระยะเวลาในการรอดังกล่าวไว้แล้วด้วยการสุ่มค่าหลังจากเสร็จการใช้ช่องสัญญาณครั้งก่อน สถานีที่สุ่มได้ค่าระยะเวลาในการรอน้อยกว่าก็จะมีสิทธิในการเข้าใช้ช่องสัญญาณก่อน แต่อย่างไรก็ตามในบางกรณีกลไกดังกล่าวอาจจะกำหนดให้สถานีมากกว่าหนึ่งสถานีส่งข้อมูลในเวลาพร้อมๆ กันซึ่งจะทำให้เกิดการชนกันของสัญญาณได้ ซึ่งหากเกิดการชนกันของสัญญาณขึ้นจะต้องมีการส่งสัญญาณข้อมูลเดิมซ้ำอีกครั้งด้วยกลไกที่กล่าวมาแล้วข้างต้น

- CSMA/CA with Acknowledgement เป็นที่ควรสังเกตว่าเทคนิค CSMA/CD ไม่สามารถนำมาใช้กับเครือข่ายไร้สายได้ สาเหตุหลักๆ ก็คือการตรวจสอบการชนกันของสัญญาณในระหว่างที่ทำการส่งสัญญาณจะต้องใช้อุปกรณ์รับส่งคลื่นวิทยุที่เป็น Full Duplex (สามารถรับและส่งสัญญาณในเวลาเดียวกันได้) ซึ่งจะมีราคาแพงกว่าอุปกรณ์รับส่งคลื่นวิทยุที่ไม่สามารถรับและส่งสัญญาณ ในเวลาเดียวกัน นอกจากนี้แต่ละสถานีในพื้นที่ให้บริการ อาจไม่ได้ยินสัญญาณจากสถานีอื่นทุกสถานีหรือปัญหาที่เรียกว่า Hidden Node Problem ดังนั้นการตรวจสอบการชนกันของสัญญาณโดยตรงเป็นไปได้ยากหรือเป็นไปไม่ได้เลย มาตรฐาน IEEE 802.11 จึงได้กำหนดให้ใช้เทคนิค CSMA/CA with Acknowledgement สำหรับการจัดสรรการเข้าใช้ช่องสัญญาณของแต่ละสถานีเพื่อแก้ไขปัญหาเหล่านี้ ซึ่งการทำงานของกลไก CSMA/CA โดยหลักแล้วเป็นเช่นเดียวกับที่กล่าวไว้ในส่วนของ CSMA with Random Back-Off แต่จะมีรายละเอียดเพิ่มเติมเกี่ยวกับการหลีกเลี่ยงไม่ให้เกิดการชนกันของสัญญาณและเทคนิคสำหรับการตรวจสอบว่าเกิดการชนของสัญญาณหรือไม่ โดยสถานีผู้ส่งสัญญาณข้อมูลจะต้องรอรับAcknowledgement จากสถานีที่ส่งข้อมูลไปให้ หากไม่ได้รับ Acknowledgement กลับมาภายในเวลาที่กำหนดจะถือว่าเกิดการชนของสัญญาณขึ้น และต้องทำการส่งข้อมูลเดิมซ้ำอีกต่อไป

2.8 กลไกการรักษาความปลอดภัยในการตรวจสอบผู้ใช้ (Authentication) [9]

สำหรับเครือข่ายไร้สายมาตรฐาน IEEE 802.11 ผู้ใช้ที่เป็นเครื่องลูกข่ายจะมีสิทธิ์ในการรับส่งสัญญาณข้อมูลในเครือข่ายได้ก็ต่อเมื่อได้รับการตรวจสอบแล้วได้รับอนุญาต ซึ่งมาตรฐาน IEEE 802.11 ได้กำหนดให้มีกลไกสำหรับการตรวจสอบผู้ใช้ (Authentication) ใน 2 ลักษณะคือ Open System Authentication และ Shared Key Authentication ซึ่งเป็นดังต่อไปนี้

2.8.1 การพิสูจน์ตัวตนแบบระบบเปิด (Open System Authentication)

การตรวจสอบผู้ใช้ในลักษณะนี้เป็นทางเลือกแบบที่มีการตั้งค่ามาจากผู้ผลิต (default) ที่กำหนดไว้ในมาตรฐาน IEEE 802.11 ในการตรวจสอบแบบนี้จะไม่ตรวจสอบรหัสลับจากผู้ใช้ ซึ่งอาจกล่าวได้ว่าเป็นการอนุญาตให้ผู้ใช้ใดๆ ก็ได้สามารถเข้ามารับส่งสัญญาณในเครือข่ายนั่นเอง แต่อย่างไรก็ตามในการตรวจสอบแบบนี้อุปกรณ์ที่ทำหน้าที่เป็นสถานีแม่ข่ายไม่จำเป็นต้องอนุญาตให้สถานีผู้ใช้เข้ามาใช้เครือข่ายได้เสมอไป ในกรณีนี้บทบาทของ WEP จึงเหลือแต่เพียงการเข้ารหัสข้อมูลเท่านั้น กลไกการตรวจสอบแบบ open system authenticationมีขั้นตอนการทำงานดังต่อไปนี้

- สถานีที่ต้องการจะเข้ามาร่วมใช้เครือข่ายจะส่งข้อความซึ่งไม่ถูกเข้ารหัสเพื่อขอรับการตรวจสอบ (Authentication Request Frame) ไปยังอุปกรณ์ที่ทำหน้าที่เป็นสถานีแม่ข่าย โดยในข้อความดังกล่าวจะมีการแสดงความจำนงเพื่อรับการตรวจสอบแบบ open system

- อุปกรณ์ที่ทำหน้าที่เป็นสถานีแม่ข่ายโต้ตอบด้วยข้อความที่แสดงถึงการตอบรับหรือปฏิเสธ Request ดังกล่าว

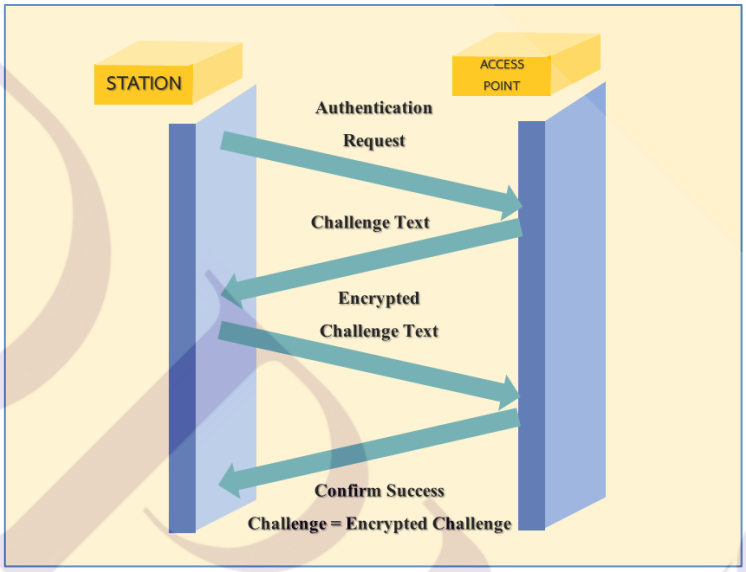
2.8.2 การพิสูจน์ตัวตนแบบใช้คีย์ร่วม (Shared Key Authentication)

การตรวจสอบผู้ใช้แบบ shared key authentication ในรูปที่ 2.5 จะอนุญาตให้สถานีผู้ใช้ซึ่งมีรหัสลับของเครือข่ายนี้เท่านั้น ที่สามารถเข้ามารับส่งสัญญาณกับอุปกรณ์ที่ทำหน้าที่เป็นสถานีแม่ข่ายได้ โดยมีการใช้เทคนิคการถามตอบที่ใช้กันทั่วไปผนวกกับการเข้ารหัสด้วย WEP เป็นกลไกสำหรับการตรวจสอบ ดังนั้นการตรวจสอบแบบนี้จะทำได้ก็ต่อเมื่อมีการEnable การเข้ารหัสด้วย WEP หรือ WPA เท่านั้น ส่วนกลไกการตรวจสอบดังกล่าวมีขั้นตอนการทำงานดังต่อไปนี้

- สถานีผู้ใช้ที่ต้องการจะเข้ามาร่วมใช้เครือข่ายจะส่งข้อความซึ่งไม่ถูกเข้ารหัสเพื่อขอรับการตรวจสอบ (Authentication Request Frame) ไปยังอุปกรณ์ที่ทำหน้าที่เป็นสถานีแม่ข่าย โดยในข้อความดังกล่าวจะมีการแสดงความจำนงเพื่อรับการตรวจสอบแบบ shared key

- หากสถานีแม่ข่ายต้องการตอบรับ Request ดังกล่าว จะมีการส่งข้อความที่แสดงถึงการตอบรับและคำถาม (challenge text) มายังเครื่องลูกข่าย ซึ่ง challenge textดังกล่าวมีขนาด 128 ไบต์ และถูกสุ่มขึ้นมา (โดยอาศัย PRNG) หากอุปกรณ์แม่ข่ายไม่ต้องการตอบรับ Request ดังกล่าว จะมีการส่งข้อความที่แสดงถึงการไม่ตอบรับ ซึ่งเป็นการสิ้นสุดของการตรวจสอบครั้งนี้

- หากมีการตอบรับจากสถานีแม่ข่าย สถานีผู้ใช้ที่ขอรับการตรวจสอบจะทำการเข้ารหัสข้อความคำถามที่ถูกส่งมาโดยใช้รหัสลับของเครือข่ายแล้วส่งกลับไปยังสถานีแม่ข่าย - สถานีแม่ข่ายจะทำการรถอดรหัสข้อความที่ตอบกลับมา โดยใช้รหัสลับของเครือข่าย หลังจากถอดรหัสแล้วหากข้อความที่ตอบกลับมาตรงกับข้อความคำถาม (challengetext) ที่ส่งไป สถานีแม่ข่ายจะส่งข้อความที่แสดงถึงการอนุญาตให้สถานีผู้ใช้นี้เข้าใช้เครือข่ายได้แต่หากข้อความที่ตอบกลับมาไม่ตรงกับข้อความคำถามสถานีแม่ข่ายจะโต้ตอบด้วยข้อความที่แสดงถึงการไม่อนุญาต



ภาพที่ 2.5 WEP Shared Key Authentication

2.9 เฟรมที่ใช้ในการจัดการ (Management Frame) [10]

ในมาตรฐาน IEEE 802.11 มีเฟรมหลายชนิดที่ใช้ในการสื่อสารกันระหว่างเครื่องลูกข่าย และ Access Point ให้สามารถสื่อสารกันได้ภายในระบบเครือข่ายไร้สาย ไม่ว่าจะเป็นเฟรมที่ใช้ในการจัดการ และควบคุมให้สามารถส่งข้อมูลถึงกัน และทุก ๆ เฟรมก็จะมีฟิลด์ที่ใช้ในการควบคุมเฟรมอีกทีหนึ่งด้วยไม่ว่าจะเป็นฟิลด์ที่ใช้บอกเวอร์ชัน ชนิดของเฟรม หรือแสดงสถานะต่าง ๆ เช่นมีการเข้ารหัสในการสื่อสารกันในแบบ WEP เป็นต้น แต่ส่วนที่สำคัญที่จะนำมาใช้ในการศึกษาในส่วนของการโจมตีเครือข่ายไร้สายท้องถิ่นก็คือเฟรมที่ใช้ในการจัดการซึ่งถือว่าเป็นช่องโหว่อีกอันหนึ่งที่จะใช้เป็นช่องทางในการโจมตีเครือข่ายไร้สายซึ่งเฟรมที่ใช้ในการจัดการที่สามารถใช้ในการโจมตีได้ก็คือ

- เฟรมที่ใช้ในการพิสูจน์ตัวตน (Authentication Frame) การพิสูจน์ตัวตนเริ่มต้นด้วยที่เครื่องลูกข่ายทำการส่งเฟรมที่ใช้ในการจัดการไปยัง Access Point ที่ต้องการจะติดต่อด้วย และ Access Point ก็จะส่งเฟรมตอบสนอง (Request) กับมายังเครื่องลูกข่ายที่ประกอบไปด้วยChallenge text ซึ่งแสดงการตอบรับและคำถาม มายังเครื่องลูกข่าย ต่อจากนั้นเครื่องลูกข่ายจะต้องทำการตอบกลับโดยการเข้ารหัสลับ Challenge text ด้วย เมื่อ Access Point รับเฟรมดังกล่าวจากเครื่องลูกข่ายแล้วก็จะมาทำการเปรียบเทียบว่าชนิดการเข้ารหัสใน Challenge text นั้นตรงกันหรือไม่ด้วยการทำการถอดรหัส ถ้าตรงกันถือว่าการพิสูจน์ตัวตนนั้นเสร็จสมบูรณ์

- เฟรมที่ใช้ปฏิเสธการพิสูจน์ตัวตน (Deauthentication Frame) โดยสถานีใด ๆ ในระบบเครือข่ายจะส่งเฟรมที่เป็นการปฏิเสธการพิสูจน์ตัวตน ออกไปยังสถานีอื่นที่ต้องการจะยกเลิกการติดต่อด้วย

- เฟรมที่ร้องขอการเชื่อมโยง (Association Request Frame) ในมาตรฐาน IEEE 802.11 การเชื่อมโยงจะหมายถึง การที่ Access Point ทำการจับจองทรัพยากรสำหรับใช้ในการติดต่อกับเครื่องลูกข่าย โดยกระบวนการจะเริ่มจากการที่เครื่องลูกข่ายจะเริ่มทำการส่งเฟรมที่ใช้ในการเริ่มต้นการเชื่อมโยงไปให้ Access Point โดยในเฟรมจะประกอบไปด้วยข้อมูลของWireless Network Adapter และก็ชื่อของเครือข่าย (SSID) ของเครือข่ายที่ต้องการจะทำการเชื่อมโยงด้วย และหลังจากที่รับเฟรมร้องขอจากเครื่องลูกข่ายแล้ว Access Point จะทำการพิจารณาการเชื่อมโยงกับเครื่องลูกข่ายนั้น ๆ และจะจับจองทรัพยากรให้กับเครื่องลูกข่าย และกำหนดหมายเลขการเชื่อมโยงให้กับเครื่องลูกข่ายด้วย

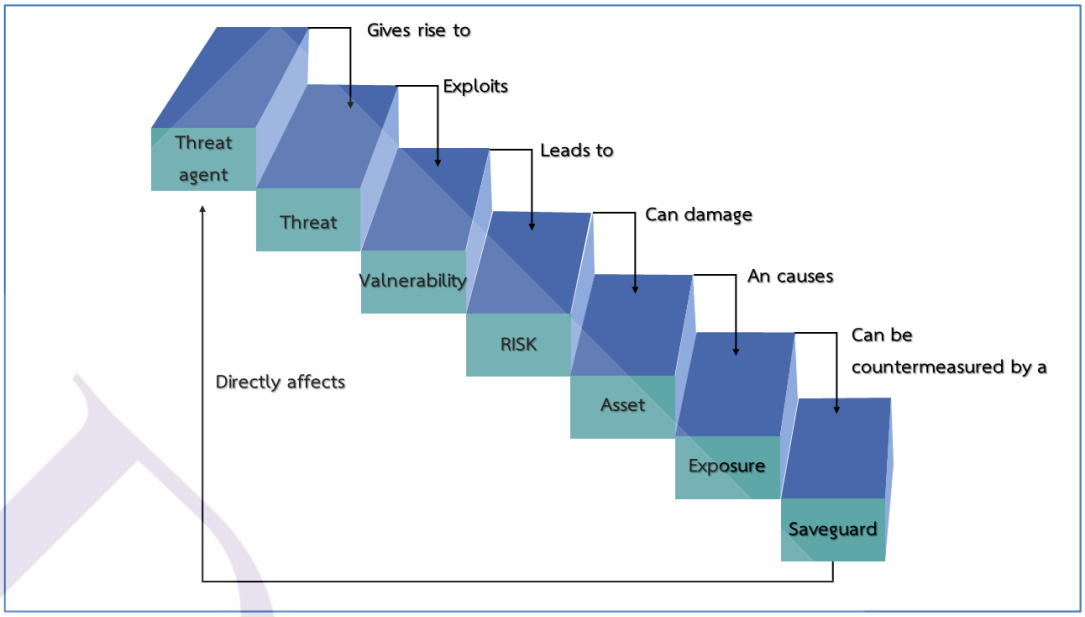
- เฟรมที่ตอบสนองการเชื่อมโยง (Association Response Frame) โดย Access Point จะตอบสนองการเชื่อมโยงด้วยการส่งเฟรมดังกล่าวนี้ที่ประกอบไปด้วยการยอม และไม่ยอมรับ โดยถ้า Access Point ยอมรับการเชื่อมโยงนี้ก็จะทำการส่งหมายเลขการเชื่อมโยง อัตราการส่งข้อมูล เป็นต้น ทำให้เครื่องลูกข่ายสามารถที่จะทำการเชื่อมโยงการสื่อสารภายในระบบเครือข่ายไร้สายด้วยกันได้- เฟรมที่ร้องขอการเชื่อมโยงใหม่ (Reassociation Request Frame) ถ้าเครื่องลูกข่ายเจอสัญญาณบีคอน (Beacon) ที่แข็งแรงกว่าเครื่องลูกข่ายจะทำการส่งเฟรมร้องขอการเชื่อมต่อใหม่ไปยัง Access Point อีกตัวหนึ่ง Access Point ตัวใหม่จะทำการส่งเฟรมที่หลงเหลือจากการส่งใน Access Point เดิมกลับมาให้เครื่องลูกข่าย

- เฟรมที่ตอบสนองการเชื่อมโยงใหม่ (Reassociation Response Frame) โดยเฟรมนี้จะใช้ในการตอบรับหรือปฏิเสธการเชื่อมไปยัง Access Point อีกตัวหนึ่งคล้ายกับกระบวนการในการเชื่อมโยง- เฟรมที่ใช้ปฏิเสธการเชื่อมโยง (Deassociation frame) โดยสถานีต่าง ๆ จะทำการส่งเฟรมดังกล่าวนี้เพื่อจะยกเลิกการเชื่อมโยงกับสถานีอื่น ๆ ที่ต้องการ

- เฟรมบีคอน (Beacon Frame) โดย Access Point จะทำการส่งเฟรมบีคอนออกไปเป็นระยะ ๆ (Periodic) เพื่อประกาศถึงข้อมูลเช่น เวลา (TimeStamp) SSID และอื่น ๆ ภายในขอบเขตของสัญญาณที่มีอยู่ โดยเครื่องลูกข่ายจะทำการส่งสัญญาณโพรบ (Probe) เพื่อหาว่ามีAccess Point ใดอยู่ภายในขอบเขตของตนบ้าง โดยพิจารณาจากสัญญาณบีคอนที่ตอบกลับมา

2.10 ช่องโหว่ ภัยคุมคาม และการโจมตี [9]

ช่องโหว่ (Vulnerability) ภัยคุกคาม (Threat) และการโจมตี (Attack) มีความสัมพันธ์ต่อกันอย่างมากกล่าวคือช่องโหว่ (Vulnerability) หมายถึง ความผิดพลาด จุดอ่อน หรือจุดบกพร่องของระบบระบบทุกระบบล้วนมีช่องโหว่ด้วยกันทั้งสิ้น ระบบที่ถูกอ้างว่ามีความปลอดภัยสูงเป็นระบบที่ได้ปิดช่องโหว่ที่เป็นที่รู้จัก (Known Vulnerabilities) ไว้แล้ว แต่ก็ยังมีช่องโหว่ที่ยังไม่ถูกค้นพบอีกเป็นจำนวนมาก เปรียบเสมือนกับบรรจุน้ำที่มีรอยแตกร้าวอยู่ด้านข้างถัง แต่ก็ยังสามารถบรรจุน้ำอยู่ได้ เมื่อใดก็ตามที่ไม่มีใครเอาของแข็งที่เป็นไม้หรือเหล็กมาทุบตรงรอยร้าวนั้น น้ำก็ยังไม่ทะลักออกมา เปรียบได้กับระบบที่ยังคงมีความปลอดภัยอยู่ ตราบใดที่ยังไม่มีใครค้นพบช่องโหว่ของระบบหรือรอยร้าวของถังน้ำนั้น ตัวอย่างของระบบคอมพิวเตอร์ที่มีช่องโหว่ได้แก่ ระบบคอมพิวเตอร์ที่ไม่ได้มีการติดตั้งซอฟต์แวร์ประเภทแอนตี้ไวรัส นั้นแน่นอนว่าระบบมีช่องโหว่ที่ไม่สามารถทำตรวจจับไวรัสคอมพิวเตอร์ เปรียบได้กับรอยแตกร้าวที่อยู่ข้างถังน้ำแต่ตราบใดก็ตามที่ยังไม่มีไวรัสคอมพิวเตอร์ที่แพร่กระจายตัวเองมายังระบบนี้ระบบก็ยังถือว่ามีความลอดภัยอยู่ สิ่งที่เป็นอันตรายต่อระบบคอมพิวเตอร์เรียกว่า ภัยคุกคาม (Threat) ที่เน้นว่าเป็นอันตรายต่อระบบนั้นหมายความว่า หากมีการกระทำการใดๆ ตามลักษณะของภัยคุกคามนั้น ระบบจะได้รับความเสียหาย แต่หากไม่มีการกระทำใดๆ ที่เกิดจากภัยคุกคามนั้นระบบก็ยังมีความปลอดภัย ดังนั้นภัยคุกคามนั้นก่อให้เกิดความเสี่ยง (Risk) ต่อการถูกโจมตี (Attack) นั่นเองเปรียบได้กับไวรัสคอมพิวเตอร์ ที่ถือได้ว่าเป็นภัยคุกคามต่อระบบที่ไม่มีซอฟต์แวร์แอนตีไวรัสแต่ไวรัสคอมพิวเตอร์ก็ยังถือว่าไม่เป็นอันตรายต่อระบบ ตราบใดที่มันยังไม่แพร่ตัวเองเข้าไปในระบบนั้นและทำให้ไฟล์ภายในระบบติดไวรัส ภัยคุกคามนั้นเปรียบภัยได้กับไม้หรือของแข็งที่เป็นเหล็กที่สามารถใช้ทุบถังน้ำตรงรอยร้าวข้างถัง ทำให้น้ำซึ่งเปรียบได้กับข้อมูลลับไหลออกจากถังน้ำ การกระทำอันเป็นผลมาจากภัยคุกคามเรียกว่า การโจมตี (Attack) การโจมตีส่งผลให้เกิดความเสียหายแก่ระบบ ผลจากการโจมตีมีความแตกต่างกันไปตามลักษณะของภัยคุกคามเช่น ไวรัสคอมพิวเตอร์สามารถทำลายไฟล์ระบบ (System file) ที่สำคัญ อาจฟอร์แมต (Format)ข้อมูลที่อยู่ภายในฮาร์ดไดรฟ์ (Hard drive) จนหมดหรือสามารถทำสำเนาตัวเองและย้ายตัวเองไปติดคอมพิวเตอร์เครื่องอื่นได้ดังภาพที่ 2.6 เป็นความสัมพันธ์ระหว่างส่วนประกอบทางด้านความปลอดภัยที่กล่าวมาข้างต้น



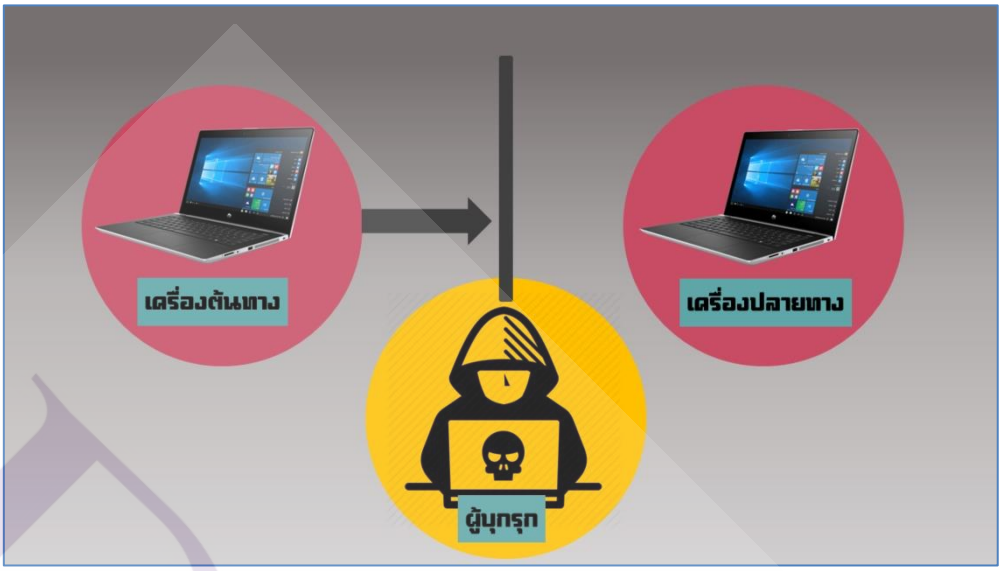
ภาพที่ 2.6 ความสัมพันธ์ระหว่างส่วนประกอบต่างๆ ทางด้านความปลอดภัย

2.11 ชนิดของการโจมตี (Type of Attacks) [9]

การโจมตี (Attack) เป็นการดำเนินการอันเป็นผลจากภัยคุกคามที่ส่งผลหลายๆ อย่างให้กับระบบคอมพิวเตอร์และเครือข่าย สามารถแบ่งกลุ่มของการโจมตีออกได้เป็น 4 ชนิด คือการขัดจังหวะ (Interruption), การดักฟัง (Interception) การแก้ไขเพิ่มเติม (Modification) และการปลอมตัวเป็นผู้อื่น (Fabrication)

2.11.1 การขัดจังหวะ (Interception)

การขัดจังหวะ (Interruption) เป็นการทำให้ผู้ใช้ที่ได้รับอนุญาตไม่สามารถเข้าถึงทรัพยากรภายในระบบได้ ไม่ว่าจะเป็นการโยกย้าย ทำลาย หรือซ่อนทรัพยากรไม่ให้สามารถใช้งานได้ การโจมตีชนิดนี้สามารถเกิดขึ้นได้หลายรูปแบบ แต่สามารถเรียกโดยรวมได้ว่าเป็นการโจมตีแบบ การปฏิเสธการให้บริการ (Denial of Services หรือ DoS) ไม่ว่าในเชิงกายภาพ เช่นการตัดสายเคเบิล การตัดระบบไฟ หรือสามารถทำได้โดยการส่งการร้องขอปริมาณมากๆ ไปยังเครื่องเป้าหมายเพื่อส่งผลให้เครื่องนั้นจะต้องทำการประมวลผลการร้องขอดังกล่าวจนไม่สามารถให้บริการกับผู้ใช้อื่นๆ ได้ การขัดจังหวะมีผลกระทบโดยตรงกับความพร้อมใช้ของข้อมูล(Data Availability) ทำให้ผู้ใช้ไม่สามารถเข้าถึงทรัพยากรภายในระบบได้ ตัวอย่างของการโจมตีชนิดนี้แสดงในภาพที่ 2.7



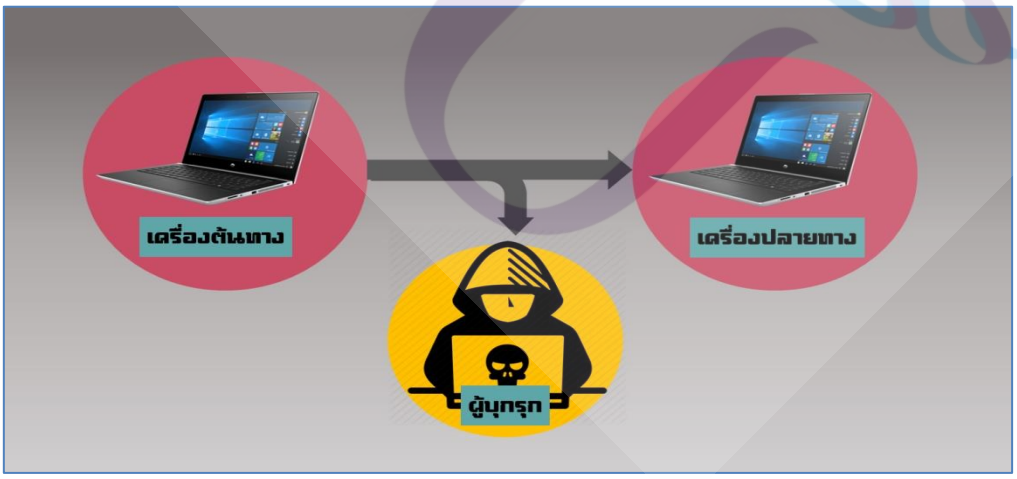
ภาพที่ 2.7 การโจมตีแบบขัดจังหวะ (Interruption)

ตัวอย่างหนึ่งของการโจมตีชนิดนี้ได้แก่ Ping of Death ซึ่งเป็นการโจมตีที่ผู้โจมตีส่งแพ็กเกจชนิด ICMP Echo Request ที่มีขนาดเกินกว่า 64 กิโลไบท์ ไปยังโฮสต์เป้าหมาย ระบบปฏิบัติการบางระบบไม่สามารถประมวลผลแพ็กเกจ ICMP Echo Request ที่มีขนาดใหญ่ผิดปกติได้ เป็นเหตุให้เครื่องนั้นค้างไปเลย ต้องทำการเปิดเครื่องใหม่ หากการโจมตีแบบนี้เกิดกับเซิร์ฟเวอร์จะทำให้ผู้ใช้อื่นๆไม่สามารถใช้บริการได้ หากเครื่องเป้าหมายสามารถจัดการกับแพ็กเกจ ICMP Echo Request ที่มีขนาดใหญ่ผิดปกติได้นั้น การโจมตียังสามารถทำได้โดยส่งแพ็กเกจ ICMP Echo Request ในปริมาณที่มากไปยังโฮสต์เป้าหมาย โดยที่โฮสต์ที่ทำการโจมตีนั้นใช้หมายเลขไอพีแอดเดรสต้นทางปลอม (Spoofed Source IP address) ทำให้โฮสต์เป้าหมายจะต้องประมวลผลโดยการส่งแพ็กเกจICMP Echo Reply กลับไปยังโฮสต์ที่ส่งICMP Echo Request มาแต่แพ็กเกจดังกล่าวไม่สามารถถูกส่งไปยังโฮสต์ต้นทางได้ เนื่องจากหมายเลขไอพีแอดเดรสต้นทางที่ระบุอยู่ในแพ็กเก็ตที่ส่งมานั้นไม่มีอยู่จริง ดังนั้นแพ็กเกจดังกล่าวก็จะวิ่งไปมาระหว่างเร้าเตอร์ภายในเครือข่ายนั้นจนกว่าค่า Time-to-live (TTL) จะลดลงเป็นศูนย์ เร้าเตอร์จึงจะดรอปแพ็กเกจนั้นทิ้งไป วิธีการนี้เรียกว่า Ping Flood คำว่า Floodหมายถึงการส่งข้อมูลปริมาณมากๆ ไปยังปลายทาง เปรียบเสมือนการปล่อยน้ำปริมาณมากๆให้ท่วมพื้นที่นั่นเอง เหตุการณ์ดังกล่าวใช้เวลานานพอสมควรในระหว่างที่แพ็กเกจนั้นยังไม่ถูกดรอป ปริมาณของทราฟฟิก (Traffic) ภายในเครือข่ายจะสูงขึ้นมาก ทำให้บริการต่างๆ ภายในเครือข่ายมีประสิทธิภาพลดลง การโจมตีประเภทนี้จะยิ่งได้ผลมากยิ่งขึ้นหากมีการใช้หลายๆเครื่องในการโจมตีโดยส่งแพ็กเกจปริมาณมหาศาลจากเครื่องนับพัน

เครื่องไปยังเครื่องเป้าหมายเครื่องเดียว วิธีการนี้เรียกว่า Distributed Denial-of-Services (หรือ DDoS) การที่ผู้บุกรุกสามารถกระทำอย่างนั้นได้ เป็นเพราะผู้บุกรุกสามารถเจาะเข้าไปยังเครื่องคอมพิวเตอร์คอมพิวเตอร์ที่ไม่มีระบบรักษาความปลอดภัยที่ไม่ดีและส่งโปรแกรมประเภทโทรจัน (Trojan)ฝังตัวลงไป โปรแกรมดังกล่าวเป็นโปรแกรมที่ใช้ควบคุมสั่งการจากระยะไกลให้โฮสต์ที่ถูกควบคุมทำสิ่งใดก็ได้ตามที่ต้องการ โดยที่เจ้าของเครื่องไม่รู้ตัว โฮสต์ที่ถูกควบคุมเรียกว่า ซอมบี้ (Zombie) หรือผีดิบ เปรียบเสมือนผีดิบที่ไม่มีความนึกคิด แต่ร่างกายถูกควบคุมโดยพ่อมด เมื่อถึงเวลาที่กำหนด ผู้บุกรุกจะสั่งการให้ซอมบี้นับพันส่งแพ็กเกจ ICMP Echo Request โดยมีปลอมแปลงหมายเลขไอพีแอดเดรสต้นทางไปยังโฮสต์เป้าหมาย เพื่อทำให้ปริมาณทราฟฟิกภายในเครือข่ายนั้นสูงขึ้นโดยฉับพลัน เป็นการปิดกั้นการให้บริการต่อผู้ใช้คนอื่น

2.11.2 การดักฟัง (Interception)

การดักฟัง (Interception หรือ Eavesdropping) เป็นการแฝงตัวเข้าไปอยู่ระหว่างการสื่อสารของคนอื่นและดักจับเอาข้อมูลที่มีการรับส่งกันออกมา โปรแกรมที่สามารถนำมาใช้เพื่อการดักจับข้อมูลมีมากมาย เช่น Ethereal, TCPdump, Snort เป็นต้น โดยมากแล้วข้อมูลที่ดักจับมา และสามารถนำไปใช้งานได้เลยมักเป็นข้อมูลที่เกี่ยวข้องกับบริการที่ส่งข้อมูลที่ไม่มีการเข้ารหัสลับ เช่น FTP, HTTP, SMTP หรือ Telnet เป็นต้น สำหรับข้อมูลที่ถูกเข้ารหัสลับมานั้น หลังจากที่ได้ข้อมูลนั้นมาแล้วผู้บุกรุกจะต้องพยายามถอดรหัสลับข้อมูลนั้นต่อไป ซึ่งก็ไม่ได้รับประกันว่าจะสามารถถอดรหัสลับข้อมูลดังกล่าวสำเร็จหรือไม่ และจะต้องใช้เวลานานเท่าใด ภาพที่ 2.8 แสดงขั้นตอนการดักฟัง



ภาพที่ 2.8 การโจมตีแบบดักฟัง (Interception)

แม้ว่าผู้ที่ดักฟังไม่สามารถถอดรหัสข้อมูลดังกล่าวได้ แต่อย่างน้อยผู้ดักฟังก็สามารถทำการโจมตีอีกชนิดหนึ่งที่เรียกว่า Replay Attack ได้ ซึ่งเป็นการโจมตีโดยการทำสำเนาข้อมูลที่มีการส่งไปมาระหว่างโฮสต์เป้าหมายและโฮสต์อื่นๆ เก็บเอาไว้ แล้วทำการส่งข้อมูลดังกล่าวไปยังโฮสต์เป้าหมายในภายหลังความเสียหายที่เกิดขึ้นจากการโจมตีประเภทนี้ คือ การรั่วไหลของข้อมูล การสูญเสียความเป็นส่วนตัว นอกจากนี้ข้อมูลที่รั่วไหลอาจยังสามารถนำไปใช้ในการโจมตีประเภทอื่นได้อีกเช่น หากสามารถดักจับข้อมูลที่เป็นยูสเซอร์เนมและพาสเวิร์ดของผู้ใช้รายหนึ่ง ก็สามารถปลอมตัวเป็นผู้ใช้รายนั้นในการเข้าถึงทรัพยากรภายในระบบนั้นได้ ซึ่งการตรวจจับการโจมตีประเภทนี้ทำได้ยากมาก เนื่องจากเป็นการโจมตีที่ไม่ได้มีการบุกรุกเข้าไปยังเป้าหมาย แต่เพียงแค่ดักจับเอาข้อมูลที่มีการส่งผ่านกันในเครือข่ายแล้วมาทำการวิเคราะห์หาความเป็นไปได้ที่จะเป็นข้อมูลที่เป็นความลับ ดังนั้นจึงเห็นได้ว่าการโจมตีประเภทนี้ถือเป็นจุดเริ่มต้นของการโจมตีอื่นๆ อีกมากมาย

2.11.3 การแก้ไขเพิ่มเติม (Modification)

การแก้ไขเพิ่มเติม (Modification) เป็นการแก้ไขข้อมูลที่มีการส่งผ่านเครือข่ายเพื่อให้ผู้รับข้อมูลนั้นได้ข้อมูลที่แตกต่างจากข้อมูลต้นฉบับ ภาพที่ 2.9 แสดงขั้นตอนการแก้ไขเพิ่มเติม

ภาพที่ 2.9 การโจมตีแบบแก้ไขเพิ่มเติม (Modification)

ในการโจมตีชนิดนี้นั้นเริ่มจากการดักฟัง (Interception) โดยที่เริ่มแรกผู้บุกรุกทำการดักฟังข้อมูลที่มีการส่งผ่านไปมาระหว่างผู้ส่งและผู้รับข้อมูล จากนั้นจึงนำข้อมูลนั้นมาแก้ไขและส่งกลับไปยังผู้รับข้อมูลทางช่องทางการสื่อสารเดิม ผู้ที่ได้รับข้อมูลนั้นก็จะคิดว่าเป็นข้อมูลที่มาจากผู้ส่ง แต่ความจริงแล้วข้อมูลได้ถูกแก้ไขให้มีความหมายเปลี่ยนแปลงไปการแก้ไขเพิ่มเติมข้อมูลส่งผลกระทบโดยตรงต่อความถูกต้องของข้อมูลภายในของระบบ เนื่องจากคุณสมบัตินี้เน้นว่าข้อมูลที่มีการส่งผ่านเครือข่ายหรือเก็บไว้ภายในเซิร์ฟเวอร์จะต้องไม่ถูกแก้ไขโดยที่ไม่สามารถตรวจจับได้

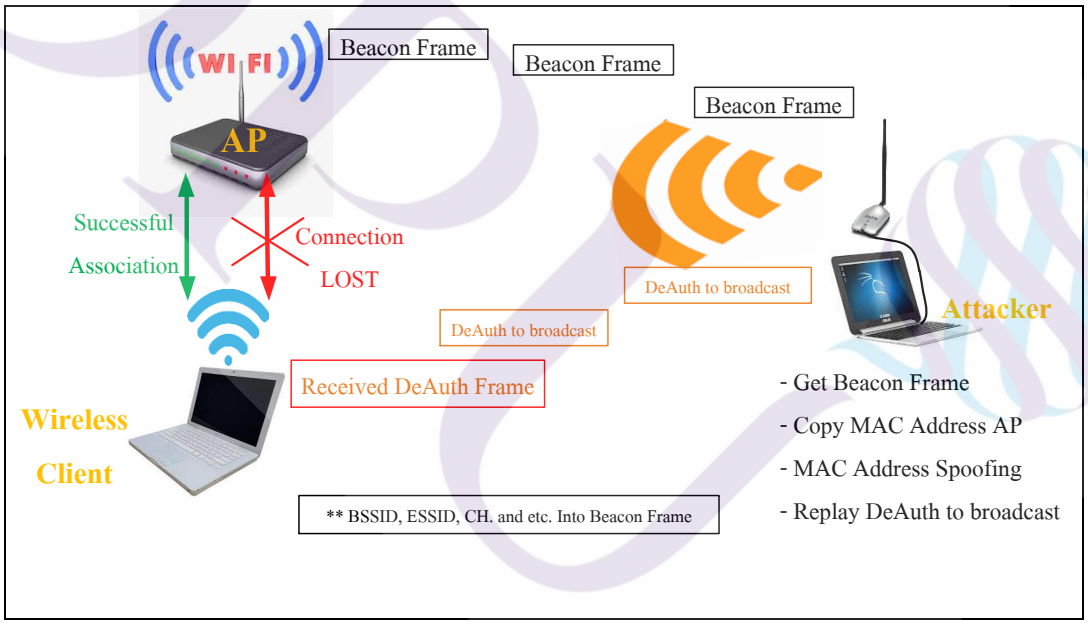
2.11.4 การปลอมตัวเป็นผู้อื่นการโจมตีชนิดนี้มีชื่อเรียกแตกต่างกันมากมาย เช่น Impersonation และ Masquerading แต่ทั้งหมดล้วนแล้วแต่หมายถึงการโจมตีที่เกิดจากการปลอมตัวเป็นผู้ใช้อื่นที่อยู่ในระบบ เพื่อหลอกผู้ใช้ที่เป็นเป้าหมายติดต่อด้วย ลักษณะของการโจมตีด้วยวิธีการนี้เป็นดังภาพที่ 2.10

ภาพที่ 2.10 การปลอมตัวเป็นผู้อื่น (Fabrication)

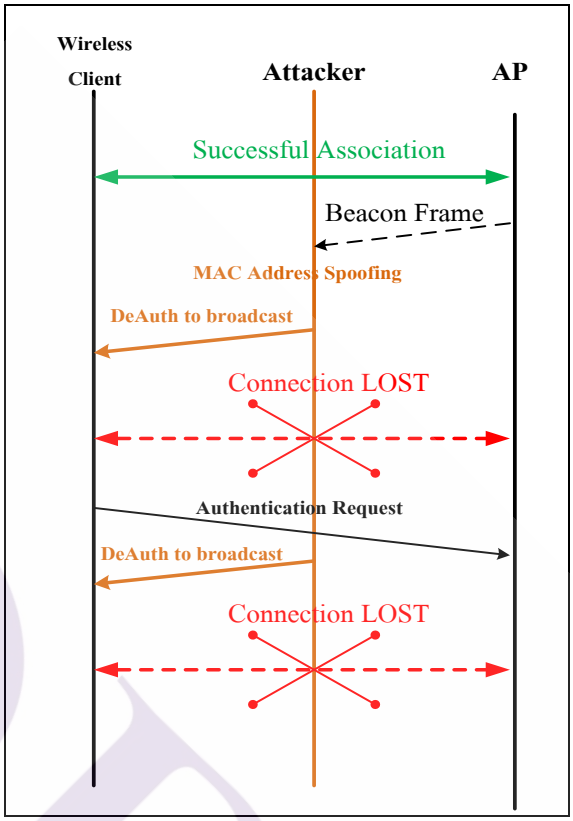
การโจมตีแบบนี้ส่งผลกระทบต่อคุณสมบัติที่เรียกว่า Authenticity หรือความเป็นตัวตนที่แท้จริง ดังนั้นจึงควรตรวจสอบตัวตนของผู้ใช้ก่อนที่จะทำการติดต่อด้วย โดยการยืนยันตัวตนดังกล่าวเรียกว่า Authentication

2.12 กระบวนการโจมตีเครือข่ายไร้สายด้วยวิธี De-Authentication [3]

การโจมตีเครือข่ายไร้สายด้วยวิธี De-Authentication เป็นอีกวิธีหนึ่งที่ Hacker นิยมใช้โจมตีเครือข่ายไร้สาย โดยจะทำการปลอมแปลงแมคแอดเดรส (MAC Address Spoofing) ของอุปกรณ์กระจายสัญญาณ (Access Point : AP) เป้าหมาย และดำเนินการโจมตีด้วยวิธีการส่งเฟรม Deauthentication ไปยังเครื่องคอมพิวเตอร์ที่กำลังเชื่อมต่อหรือติดต่อสื่อสารอยู่กับอุปกรณ์กระจายสัญญาณเป้าหมาย [4] ซึ่งผู้วิจัยได้ทำการศึกษาเพื่อที่จะดำเนินการทดสอบการรบกวนหรือการโจมตีเครือข่ายแบบไร้สายด้วยวิธีดังกล่าว โดยมีภาพรวมของกระบวนการแสดงในภาพที่ 2.11 และ ภาพที่ 2.12 ดังนี้



ภาพที่ 2.11 ภาพรวมของกระบวนการโจมตีเครือข่ายไร้สายด้วยวิธี De-Authentication



ภาพที่ 2.12 แสดงขั้นตอนของกระบวนการโจมตีเครือข่ายไร้สายด้วยวิธี De-Authentication

จากภาพที่ 2.11 จะแสดงให้เห็นถึงภาพรวมของกระบวนการโจมตี และในภาพที่ 2.12 แสดงถึงขั้นตอนของกระบวนการโจมตีเครือข่ายไร้สายด้วยวิธีการ ซึ่งมีรายละเอียดของแต่ละขั้นตอนในการทำงานดังนี้ [4]

- ขั้นตอนที่ 1 ก่อนที่จะดำเนินการโจมตีจะเห็นว่ามีการเชื่อมต่อสื่อสารกันโดยสมบูรณ์ Successful Association ระหว่างอุปกรณ์กระจายสัญญาณ AP กับผู้ใช้งาน Wireless Client ซึ่งในขณะเดียวกันนั้นอุปกรณ์กระจายสัญญาณ AP ก็จะมีการปล่อยสัญญาณเฟรมบีคอน (Beacon Frame) โดยจะทำการส่งออกไปเป็นระยะ ๆ (Periodic) เพื่อประกาศถึงข้อมูลต่าง ๆ เช่น เวลา (Time Stamp) SSID ESSID CH. รวมถึงอื่น ๆ ภายในขอบเขตของสัญญาณที่มีอยู่ โดยเครื่องลูกข่ายจะทำการส่งสัญญาณโพรบ (Probe) เพื่อหาว่ามี Access Point ใดอยู่ภายในขอบเขตของตนบ้าง โดยพิจารณาจากสัญญาณบีคอนที่ตอบกลับมา

- ขั้นตอนที่ 2 Attacker จะทำการตรวจค้นหา AP เป้าหมาย ที่ต้องการโจมตี โดยการดักจับข้อมูลเฟรมบีคอน (Beacon Frame) ของ AP เป้าหมายที่ทำการส่งสัญญาณออกไปเป็นระยะ ๆ

ในขั้นตอนนี้เองจะทำให้ Attacker ทราบถึงข้อมูลต่าง ๆ ที่สำคัญอันได้แก่ SSID ESSID CH รวมถึงอื่น ๆ ซึ่งสามารถนำไปใช้ในการโจมตีในขั้นตอนต่อไป

- ขั้นตอนที่ 3 เมื่อทราบข้อมูลที่ต้องการจากขั้นตอนที่ 2 แล้ว ในขั้นตอนนี้จะเป็นการคัดลอกและปลอมแปลงแมคแอดเดรส (MAC Address Spoofing) ของอุปกรณ์ AP เป้าหมาย จากนั้นดำเนินการรบกวนหรือโจมตีด้วยวิธีการส่งแพ็คเกจที่เรียกว่า DeAuth แบบ Broadcast กระจายไปยังผู้ใช้งาน Wireless Client ที่กำลังติดต่อสื่อสารอยู่กับ AP เป้าหมาย

- ขั้นตอนที่ 4 เมื่อผู้ใช้งาน Wireless Client ได้รับแพ็คเกจ DeAuth จากที่กล่าวมาในขั้นตอนที่ 3 แล้ว จึงเกิดความเข้าใจว่า AP เป้าหมาย เป็นผู้ส่งเฟรมที่ใช้ปฏิเสธการพิสูจน์ตัวตน (Deauthentication Frame) กล่าวคือสถานีใด ๆ ในระบบเครือข่ายจะส่งเฟรมที่เป็นการปฏิเสธการพิสูจน์ตัวตน ออกไปยังสถานีอื่นที่ต้องการจะยกเลิกการติดต่อด้วย ในจุดนี้เองจึงเป็นผลให้อุปกรณ์กระจายสัญญาณ AP เป้าหมายกับผู้ใช้งาน Wireless Client เกิดการยกเลิกหรือไม่สามารถติดต่อสื่อสารกันได้ Connection Lost ซึ่งจะเกิดขึ้นตลอดเวลาขณะทำการโจมตี จนกว่า Attacker จะยกเลิกการโจมตีด้วยการหยุดส่งแพ็คเกจ DeAuth ในขั้นตอนที่ 3 โดยจากนั้นจะเป็นร้องขอการเชื่อมต่อใช้งานใหม่อีกครั้งต่อไป

2.13 งานวิจัยที่เกี่ยวข้อง

2.13.1 [11] ชนัญญา สุวรรณศร และ นวพร วิสิฐพงศ์พันธ์ การวิเคราะห์หาจุดอ่อนและช่องโหว่ของเครือข่ายไร้สายมาตรฐาน 802.11n ได้ทำการโจมตี Access point แบบ DoS Attack เพื่อปฏิเสธการให้บริการจากการทดลองโดยการโจมตีแบบ DoS Attack ทั้ง 10 ครั้ง สามารถวิเคราะห์ผลได้ว่าเวลาที่ต้องใช้ในการโจมตีให้เครื่องลูกข่ายหลุดการเชื่อมในแต่ละมาตรฐาน 802.11b/g/n ใช้เวลาเท่ากันคือ 3 วินาทีโดยเฉลี่ย และเวลาในการกู้คืนระบบเพื่อเชื่อมต่อเครือข่ายที่ได้จากการทดลองทั้ง 10 ครั้ง สามารถวิเคราะห์ผลได้ว่าเครื่อง Access point สามารถกู้คืนระบบมาตรฐาน 802.11n เร็วที่สุดคือประมาณ 21 วินาทีโดยเฉลี่ยและเวลาที่ใช้ในการกู้คืนระบบมาตรฐาน 802.11b และ g นั้นไม่แตกต่างกันมากคือต้องใช้เวลา 26 และ 2 3 วินาทีตามลำดับ จากผลการทดลองแสดงให้เห็นว่าเครือข่ายไร้สายมาตรฐาน 802.11b/g/n มีฟังก์ชันระบบป้องกันการโจมตี DoS Attack ไม่แตกต่างกัน

2.13.2 งานวิจัยของ S. A. Nwabude [12] ได้นำเสนอวิธีการประเมินความเสี่ยง และมาตรการการป้องกันความปลอดภัย โดยรวบรวมจากงานวิจัยที่เป็นบทความตีพิมพ์เกี่ยวกับ การสื่อสารเครือข่ายไร้สายและความปลอดภัยเครือข่ายไร้สายครอบคลุมตั้งแต่ปี 2002 ถึง 2008 จากการศึกษาพบว่าเครือข่ายไร้สายมีการโจมตีที่แตกต่างกันเป็นทั้งแบบ Passive และ Active และมีระบบป้องกัน

ความปลอดภัยเครือข่ายไร้สายจะเริ่มตั้งแต่ WEP จนถึง WPA2 นำเสนอว่าวิธีการรักษาความปลอดภัยที่มีประสิทธิภาพสูงสุดคือ การผสมผสานเทคโนโลยีด้านความปลอดภัยเข้าด้วยกัน

2.13.3 เอกชัย ดวงแก้ว [13] ได้นำเสนอวิธีการทดสอบการถอดรหัสค่า WEP 64/128 bit key และ WPA/WPA2-PSK เพื่อประเมินจุดอ่อนและช่องโหว่ของระบบเครือข่ายไร้สายมาตรฐาน b/g และทดสอบกรณีศึกษาการขับรถตรวจสัญญาณ War Driving บริเวณถนนสีลม เพื่อวิเคราะห์ว่าแต่ละการติดตั้งทางกายภาพแต่ละแบบมีจุดอ่อนและช่องโหว่อย่างไร จากงานวิจัยดังกล่าวพบว่าการทดสอบการถอดรหัสค่า WPA/WPA2-PSK มีจุดอ่อนและช่องโหว่คือ หากสามารถทำการดักจับการทำ 4-Ways handshake ของขั้นตอนการขอเชื่อมต่อเครือข่ายได้และถ้ามีรายชื่อ password ที่ตรงกับค่า key ก็สามารถถอดรหัสค่า key ได้และจากการตรวจสัญญาณ War Driving บริเวณถนนสีลมนั้นพบว่ายังมีการใช้ค่าในการเข้ารหัสแบบ WEP อยู่มากถึง 45.36% และอีก25.46% นั้นไม่มีการเข้ารหัสใดๆ แต่ใช้วิธีป้องกันแบบอื่นๆเช่น MAC Address และ Disable SSID เป็นต้น

บทที่ 3
วิธีการดำเนินงาน

สารนิพนธ์นี้จัดทำขึ้นเพื่อศึกษาถึงขอบเขตความสามารถการรบกวนหรือการโจมตีเครือข่ายไร้สายด้วยวิธี De-Authentication [3] โดยจะทำการปลอมแปลงแมคแอดเดรส (MAC Address Spoofing) ของอุปกรณ์กระจายสัญญาณ (Access Point : AP) เป้าหมาย และดำเนินการโจมตีด้วยการส่งเฟรม Deauthentication ไปยังเครื่องคอมพิวเตอร์ที่กำลังเชื่อมต่อหรือติดต่อสื่อสารอยู่กับอุปกรณ์กระจายสัญญาณเป้าหมาย ซึ่งจะทำให้เครื่องคอมพิวเตอร์ที่ได้รับเฟรมดังกล่าวนั้นเกิดความเข้าใจว่าได้รับการขอยกเลิกการเชื่อมต่อการปฏิเสธหรือการไม่สามารถให้บริการได้ (Denial of Service : DoS) จากอุปกรณ์กระจายสัญญาณเป้าหมาย [4] โดยจะดำเนินการทดสอบโจมตีภายใต้การทำงานของมาตรฐาน IEEE 802.11g และ IEEE 802.11n ในสภาวะการใช้งานในพื้นที่โล่งระดับสายตา Line-of-sight : LOS และการใช้งานในพื้นที่ห้องทั่วไป มีวิธีการดำเนินงานดังนี้

3.1 วิธีการดำเนินการด้านฮาร์ดแวร์

3.2 วิธีการดำเนินการด้านซอฟแวร์

3.3 วิธีการออกแบบเลือกสถานที่ในทดสอบ

3.4 วิธีการและขั้นตอนการทดสอบ

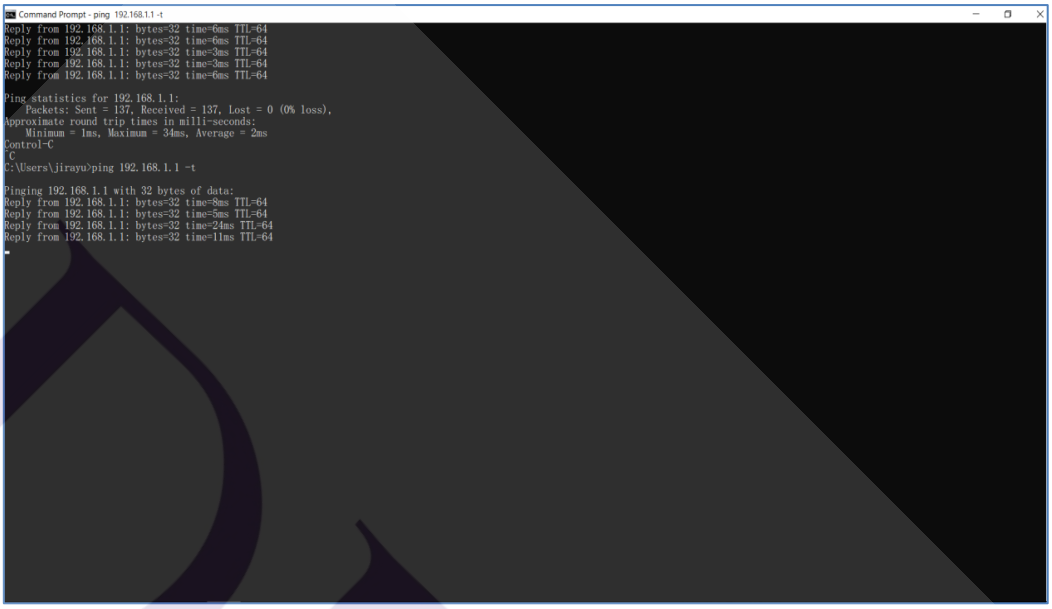
3.1 วิธีการดำเนินการด้านฮาร์ดแวร์

ในการทดสอบการรบกวนหรือการโจมตีเครือข่ายแบบไร้สายนี้ จะมีอุปกรณ์หลักที่ใช้ในการดำเนินการทดสอบ ได้แก่ เครื่องคอมพิวเตอร์โน้ตบุ๊ก จำนวน 2 เครื่อง อุปกรณ์ Wireless Lan Card จำนวน 1 ชุด อุปกรณ์กระจายสัญญาณ Access Point จำนวน 1 เครื่อง โดยมีวิธีการดำเนินการดังนี้

3.1.1 เครื่องคอมพิวเตอร์โน้ตบุ๊ก

เครื่องคอมพิวเตอร์โน้ตบุ๊ก จำนวน 2 เครื่อง ใช้สำหรับการทดสอบโดยเครื่องแรกกำหนดให้เป็น Attacker จะดำเนินการลงโปรแกรม Kali Linux ซึ่งจะขอแสดงวิธีการดำเนินการในหัวข้อถัดไป เพื่อทำงานร่วมกับอุปกรณ์ Wireless Lan Card ที่มีคุณสมบัติพิเศษในการทำงาน และเครื่องที่สองจะใช้สำหรับเชื่อมต่อเครือข่ายแบบไร้สายกับอุปกรณ์กระจายสัญญาณและเก็บผล

การสอบโดยการ Ping ซึ่งจะทำให้ทราบค่าประสิทธิภาพโดยรวมในการเชื่อมต่อได้ ดังแสดงในภาพที่ 3.1



ภาพที่ 3.1 แสดงหน้าจอการ Ping

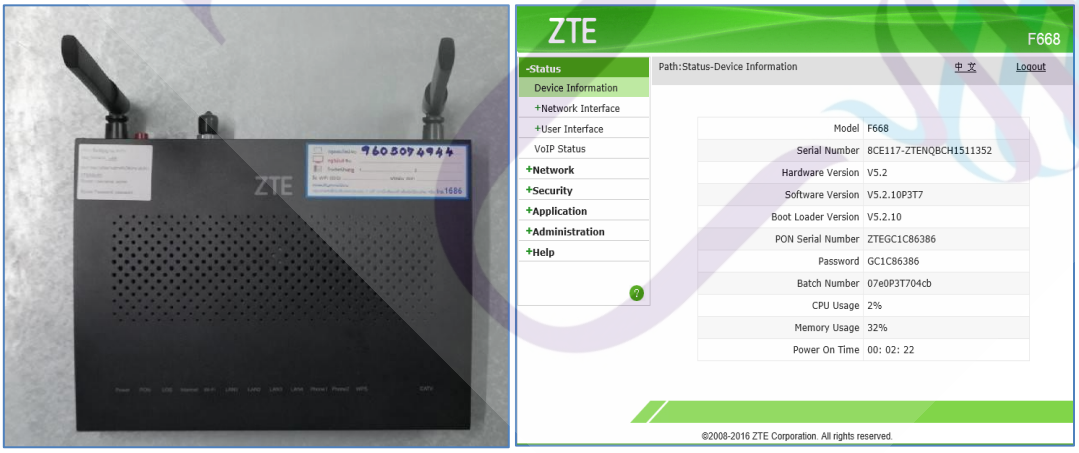
3.1.2 อุปกรณ์ Wireless Lan Card

สำหรับการวิจัยนี้การเลือกใช้อุปกรณ์ Wireless Lan Card ถือได้ว่ามีความสำคัญมาก เนื่องจากจะต้องเป็นอุปกรณ์ที่มีคุณสมบัติพิเศษกว่า Wireless Lan Card ที่ใช้ในงานโดยทั่วไป กล่าวคือจะต้องมีคุณสมบัติหลัก 3 ประการได้แก่ ความสามารถในการตรวจค้นหาอุปกรณ์ Access Point ที่กำลังใช้งานความสามารถในการปลอมแปลงแมคแอดเดรส (MAC Address Spoofing) และความสามารถในการส่งแพ็คเกจที่เรียกว่า Deauthentication ไปยังอุปกรณ์ไร้สายอื่นได้ โดยในงานวิจัยนี้ได้เลือกใช้อุปกรณ์ Wireless Lan Card ตราอักษร ALFA รุ่น AWUS036NH โดยมีคุณสมบัติตามที่กล่าวมาข้างต้นครบทุกประการ และสามารถใช้งานได้ในมาตรฐาน IEEE 802.11g/n มีกำลังออกอากาศ 2 วัตต์ ใช้สายอากาศชนิดรอบทิศทางเกณฑ์การขยายสัญญาณ 5 dBi ดังแสดงในภาพที่ 3.2

ภาพที่ 3.2 แสดงอุปกรณ์ Wireless Lan Card

3.1.3 อุปกรณ์กระจายสัญญาณ Access Point

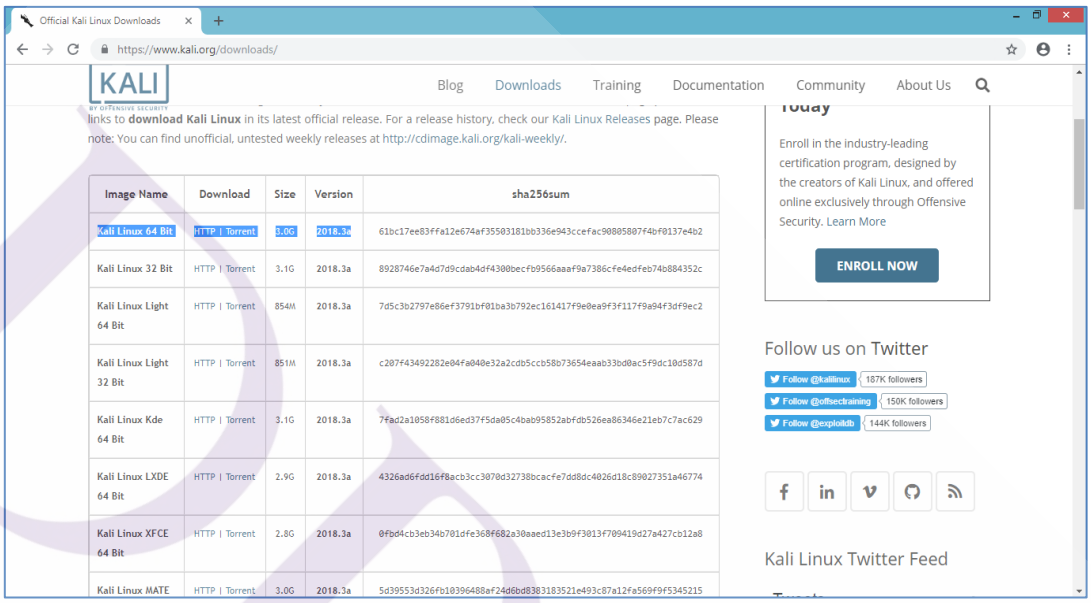
ในการเลือกอุปกรณ์กระจายสัญญาณ Access Point เพื่อที่จะทำการทดสอบสามารถเลือกใช้อุปกรณ์ที่มีขายตามท้องตลาดหรือที่มีการใช้งานทั่วไปไม่จำเป็นจะต้องเป็นยี่ห้อหรือรุ่นใดรุ่นหนึ่งเท่านั้น เพียงแต่สามารถรองรับการทำงานในย่านความถี่ 2.4 GHz ในมาตรฐาน IEEE 802.11g และ n โดยในงานวิจัยนี้ได้เลือกใช้อุปกรณ์ Access Point ตราอักษร ZTE Model F668 Hardware Version v5.2 Software Version V5.2.10P3T7 ดังแสดงในภาพที่ 3.3



ภาพที่ 3.3 แสดงรายละเอียดอุปกรณ์ Access Point

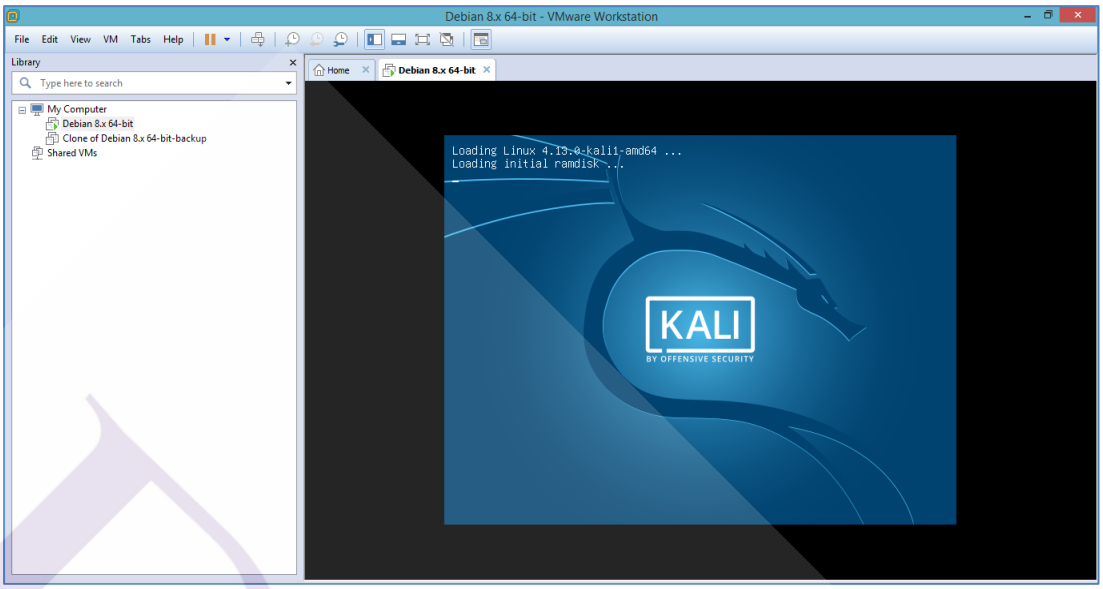
3.2 วิธีการดำเนินการด้านซอฟแวร์ [14]

ในการดำเนินการทดสอบส่งสัญญาณการรบกวนหรือโจมตีสำหรับงานวิจัยนี้ สิ่งที่ต้องการเตรียมอันดับแรกคือ Kali Linux ซึ่งสามารถจัดหาได้โดยการดาวน์โหลดจาก https://www.kali.org/downloads/ ดังแสดงในภาพที่ 3.4



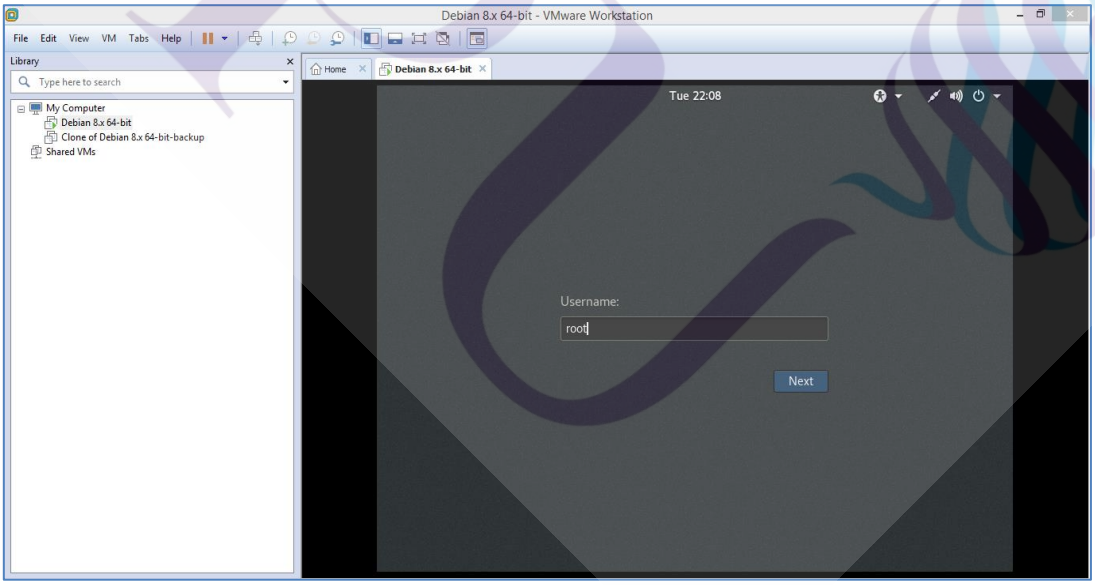
ภาพที่ 3.4 แสดงวิธีการดาวน์โหลด Kali Linux

เมื่อดาวน์โหลด Kali Linux เสร็จเรียบร้อยแล้วต่อไปเป็นการติดตั้งลงบนเครื่องคอมพิวเตอร์ที่เตรียมไว้สำหรับเป็นเครื่องในการ Attacker ซึ่งเมื่อติดตั้งแล้วเสร็จทำการเปิดโปรแกรมจะพบหน้าจอเริ่มต้นใช้งานดังแสดงในภาพที่ 3.5



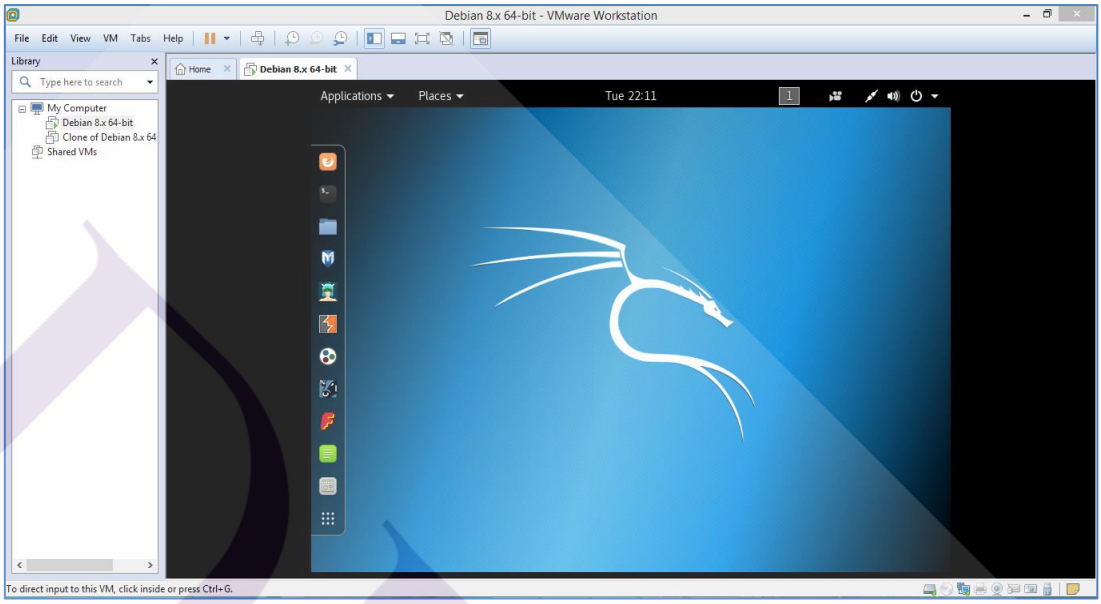
ภาพที่ 3.5 แสดงหน้าจอเริ่มต้นใช้งานของโปรแกรม Kali Linux

และเมื่อเปิดโปรแกรมขึ้นมาแล้วจะพบหน้าจอสำหรับกรอก Username และ Password เพื่อเข้าใช้งานดังแสดงในภาพที่ 3.6



ภาพที่ 3.6 แสดงหน้าจอสำหรับกรอก Username และ Password

เมื่อดำเนินการกรอก Username และ Password เสร็จเรียบร้อยแล้วก็จะพบหน้าจอแสดงถึงความสามารถพร้อมใช้งานของโปรแกรม Kali Linux ดังแสดงในภาพที่ 3.7



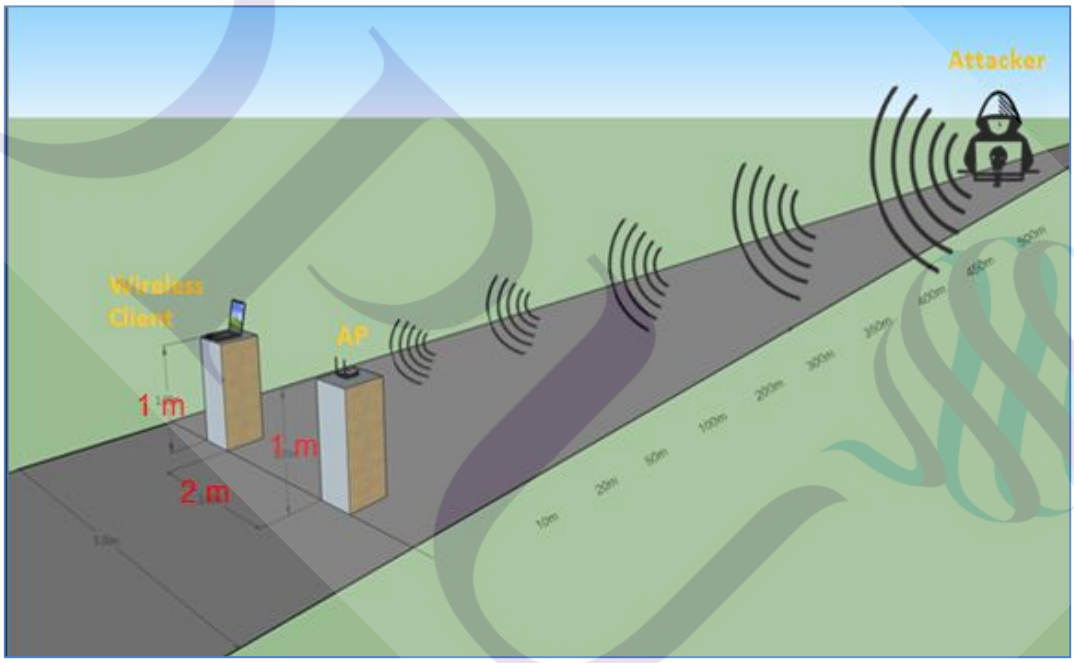
ภาพที่ 3.7 แสดงหน้าจอพร้อมใช้งานของโปรแกรม Kali Linux

3.3 วิธีการออกแบบเลือกสถานที่ในทดสอบ

ในการดำเนินการของงานวิจัยนี้จะเป็นการทดสอบการส่งสัญญาณเพื่อรบกวนหรือโจมตีในสองสภาพแวดล้อมการใช้งานโดยจะพิจารณาเลือกสถานที่ให้ใกล้เคียงกับการใช้งานจริงและมีพื้นที่ระยะทางที่เพียงพอสำหรับทดสอบ ซึ่งแบ่งเป็น 2 สภาวะการทำงานที่แตกต่างกัน ได้แก่ การทำงานบนพื้นที่โล่งแนวระดับสายตา Line-of-sight และการใช้งานในพื้นที่ห้องทั่วไป ภายใต้การทำงานของมาตรฐาน IEEE 802.11g และ IEEE 802.11n ในย่านความถี่ 2.4 GHz

3.3.1 การออกแบบเลือกสถานที่ในทดสอบการทำงานบนพื้นที่โล่งแนวระดับสายตา Line-of-sight ในการการออกแบบการทดสอบการทำงานบนพื้นที่โล่งแนวระดับสายตา Line-of-sight นั้นสิ่งแรกที่จะต้องคำนึงถึงคือการมีสถานที่โล่งและมีระยะทางที่ยาวมากเพียงพอไม่มีสิ่งบดบังในขณะทำการทดสอบ รวมไปถึงจะต้องมีสาธารณูปโภคไฟฟ้าเพื่อเป็นแหล่งจ่ายให้กับอุปกรณ์กระจายสัญญาณด้วย สำหรับงานวิจัยนี้ผู้วิจัยเองได้เลือกพื้นที่ในการทดสอบซึ่งเป็นถนนที่มีความยาวมากเพียงพอและดำเนินการทดสอบขณะไม่มีรถวิ่งสัญจร ซึ่งจะทำให้ได้ผลการทดสอบใกล้เคียงกับความเป็นจริงมากที่สุด ดังแสดงในภาพที่ 3.8

ภาพที่ 3.8 แสดงสถานที่ในทดสอบการทำงานบนพื้นที่โล่งแนวระดับสายตา



ภาพที่ 3.9 แสดงแบบจำลองการออกแบบบนพื้นที่โล่งแนวระดับสายตา

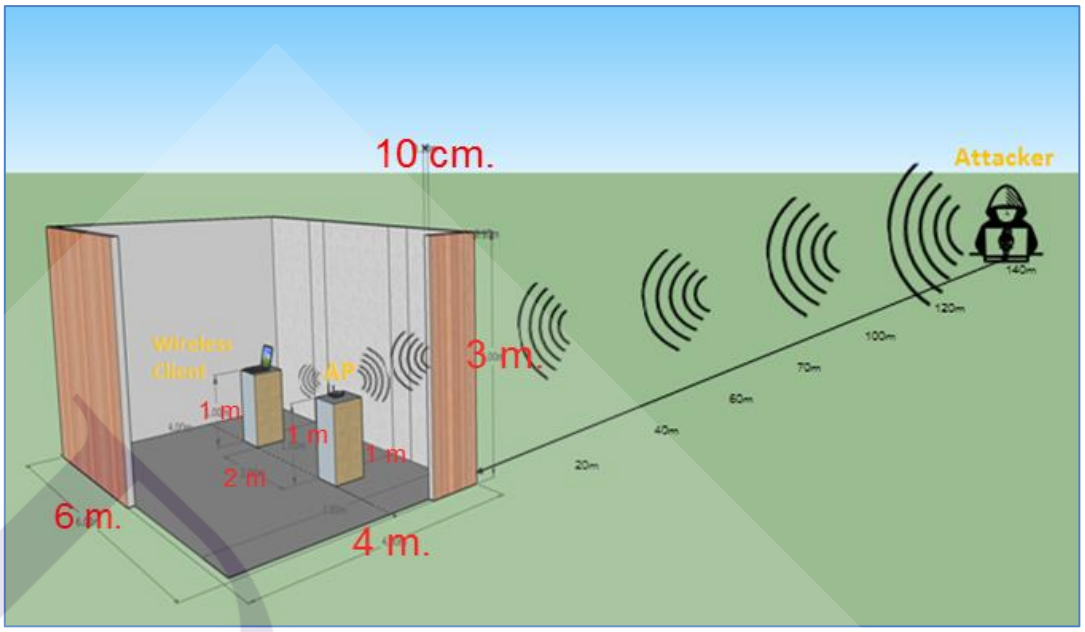
จากภาพที่ 3.9 จะแสดงให้เห็นแบบจำลองการออกแบบบนพื้นที่โล่งแนวระดับสายตา ซึ่งจะช่วยให้เข้าใจรูปแบบการทดสอบยิ่งขึ้น ซึ่งจะเห็นว่าผู้วิจัยได้ออกแบบในการวางอุปกรณ์กระจายสัญญาณ Access Point สูงจากพื้นประมาณ 1 เมตร และห่างจากเครื่องคอมพิวเตอร์สำหรับทำการเชื่อมต่อแบบไร้สายและเก็บผลการสอบโดยการ Ping ระยะห่าง 2 เมตร และเครื่อง

คอมพิวเตอร์ Attacker จะทำการทดสอบโดยเปลี่ยนและเพิ่มระยะทางให้ห่างจากอุปกรณ์กระจายสัญญาณกับเครื่องคอมพิวเตอร์ที่เชื่อมต่ออยู่ตามระยะที่กำหนด คือ 10 20 50 100 200 300 350 400 450 และ 500 เมตร ตามลำดับ

3.3.2 การออกแบบเลือกสถานที่ในทดสอบการใช้งานในพื้นที่ห้องทั่วไป

ในการการออกแบบการทดสอบการใช้งานในพื้นที่ห้องทั่วไป นั้น มีปัจจัยในการเลือกและต้องคำนึงถึงหลายด้าน เช่น จะต้องเป็นห้องที่มีขนาดเหมาะสมและเป็นขนาดมาตรฐานทั่วไป และภายนอกห้องจะต้องมีสถานที่โล่งและมีระยะทางที่ยาวมากเพียงพอไม่มีสิ่งบดบังเพื่อให้เครื่องคอมพิวเตอร์ที่กำหนดให้เป็น Attacker มีระยะทางในการเคลื่อนที่ โดยงานวิจัยนี้ได้เลือกพื้นที่ในการทดสอบเป็นห้องที่มีขนาดเหมาะสมมาตรฐานทั่วไป และมีถนนด้านข้างที่มีความยาวมากเพียงพอและดำเนินการทดสอบในขณะไม่มีรถวิ่งสัญจร ดังแสดงในภาพที่ 3.10 และ 3.11

ภาพที่ 3.10 แสดงสถานที่ในทดสอบการใช้งานในพื้นที่ห้องทั่วไป



ภาพที่ 3.11 แสดงแบบจำลองการออกแบบการใช้งานในพื้นที่ห้องทั่วไป

จากภาพที่ 3.11 เป็นภาพแสดงแบบจำลองการออกแบบการใช้งานในพื้นที่ห้องทั่วไป ซึ่งจะช่วยให้เข้าใจรูปแบบการทดสอบยิ่งขึ้น ในที่นี้ได้เลือกห้องที่มีขนาดความกว้าง 4 เมตร ยาว 6 เมตร สูง 3 เมตร และผนังห้องหนา 10 เซนติเมตร โดยการวางอุปกรณ์กระจายสัญญาณ Access Point สูงจากพื้นประมาณ 1 เมตร และห่างจากเครื่องคอมพิวเตอร์ที่ทำการเชื่อต่อแบบไร้สายสำหรับเก็บผลการสอบด้วยการ Ping และผนังห้อง ระยะห่าง 2 เมตร และเครื่องคอมพิวเตอร์ Attacker จะทำการทดสอบจากภายนอกห้องบนถนนโล้งโดยเปลี่ยนและเพิ่มระยะทางให้ห่างจากอุปกรณ์กระจายสัญญาณกับเครื่องคอมพิวเตอร์ที่กำลังเชื่อมต่ออยู่ตามระยะที่กำหนด คือ 20 40 60 80 100 120 และ 140 เมตร ตามลำดับ

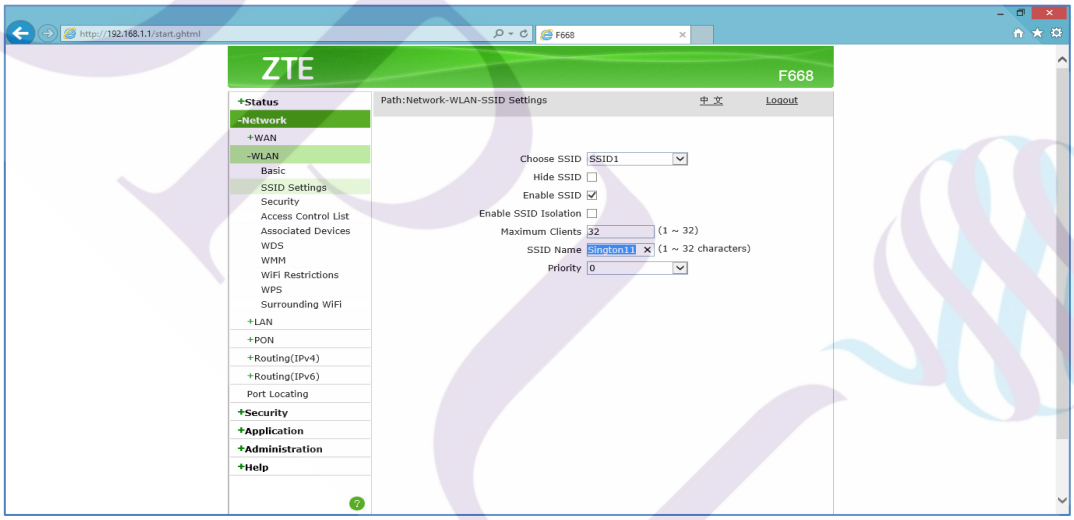
3.4 วิธีการและขั้นตอนการทดสอบ

งานวิจัยนี้เป็นวิเคราะห์และเปรียบเทียบประสิทธิภาพของการรบกวนหรือการโจมตีเครือข่ายไร้สาย ด้วยวิธี De-Authentication [3] โดยจะทำการปลอมแปลงแมคแอดเดรส (MAC Address Spoofing) ของอุปกรณ์กระจายสัญญาณ (Access Point : AP) เป้าหมาย และดำเนินการโจมตีด้วยการส่งเฟรม Deauthentication ไปยังเครื่องคอมพิวเตอร์ที่กำลังเชื่อมต่อหรือติดต่อสื่อสารอยู่กับอุปกรณ์กระจายสัญญาณเป้าหมาย ซึ่งจะทำให้เครื่องคอมพิวเตอร์ที่ได้รับเฟรม Deauthentication นั้น เกิดความเข้าใจว่าได้รับการขอยกเลิกการเชื่อมต่อการปฏิเสธหรือการไม่

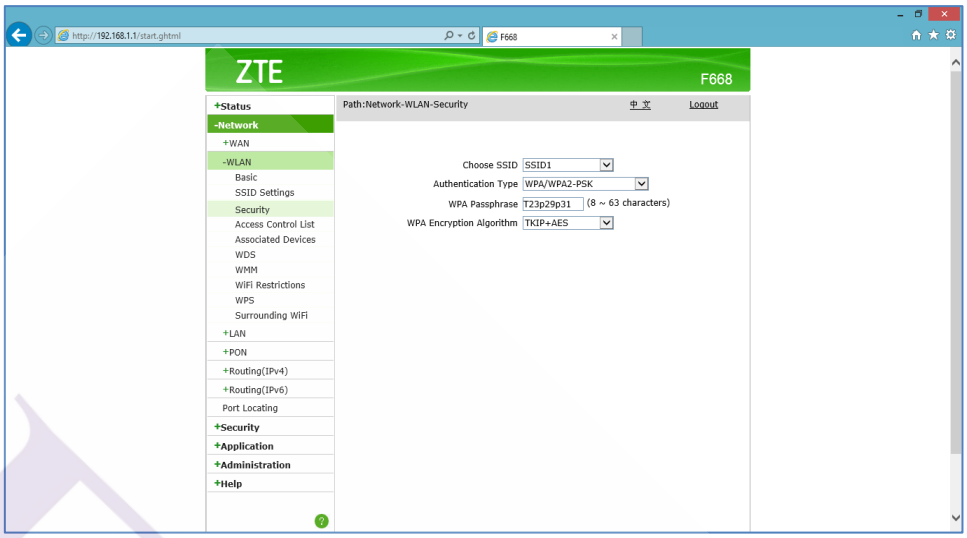
สามารถให้บริการได้ (Denial of Service : DoS) จากอุปกรณ์กระจายสัญญาณเป้าหมาย [4] โดยจะดำเนินการทดสอบ ในพื้นที่จริงในระยะของการส่งสัญญาณการรบกวนหรือโจมตีที่มีความแตกต่างกันในสภาวะการใช้งานในพื้นที่โล่งระดับสายตา และการใช้งานในพื้นที่ห้องทั่วไป ภายใต้การทำงานของมาตรฐาน IEEE 802.11g และ IEEE 802.11n ในย่านความถี่ 2.4 GHz ดังที่กล่าวมาแล้วในหัวข้อก่อนหน้า โดยมีวิธีการขั้นตอนในการดำเนินการหลักๆได้แก่ การ Setup และติดตั้งอุปกรณ์ตามจุดที่กำหนดการค้นหาอุปกรณ์กระจายสัญญาณเป้าหมาย การรบกวนหรือโจมตี โดยการส่งเฟรม Deauthentication และการเก็บผลการทดสอบโดยการ Ping ซึ่งในแต่ละขั้นตอนจะมีรายละเอียดปลีกย่อยอยู่มากพอสมควร ซึ่งผู้เขียนขออธิบายเพื่อเพิ่มความเข้าใจยิ่งขึ้นดังนี้

3.4.1 การ Setup และติดตั้งอุปกรณ์ตามจุดที่กำหนด

ก่อนเริ่มการทดสอบแต่ละรูปแบบหลังจากที่ได้กำหนดจุดในการติดตั้งดังที่ได้กล่าวมาแล้ว ในหัวข้อก่อนหน้า จะต้องดำเนินการติดตั้งอุปกรณ์ตามจุดที่กำหนดให้ถูกต้อง หลังจากนั้นจะเป็นการ Setup อุปกรณ์เพื่อทำการทดสอบในแต่ละรูปแบบโดยมีวิธีการดำเนินการดังนี้

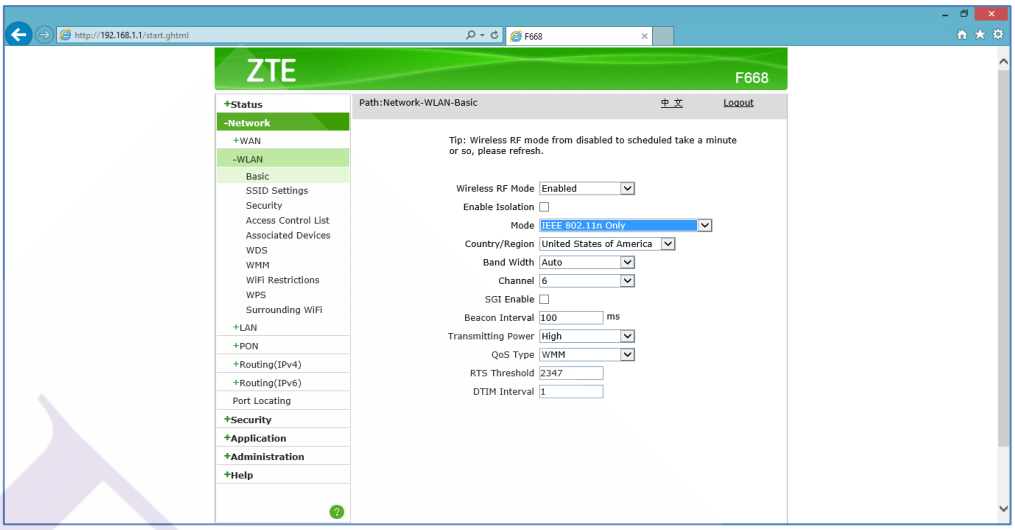


ภาพที่ 3.12 แสดงวิธีการตั้งชื่อสำหรับให้บริการ (SSID)

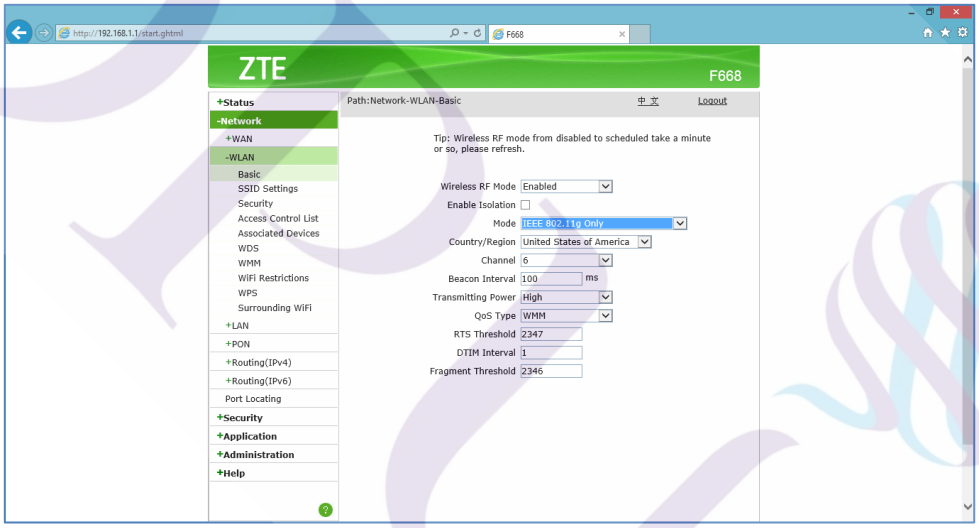


ภาพที่ 3.13 แสดงวิธีการตั้งรหัสผ่านสำหรับผู้เข้าใช้งาน

จากภาพที่ 3.12 จะแสดงให้เห็นถึงวิธีการตั้งชื่อสำหรับให้บริการ (SSID) และการกำหนดค่ารักษาความปลอดภัย ซึ่งจะเห็นว่าเป็นการตั้งค่าโดยการเข้าผ่านหน้าเว็บบราวเซอร์โดยผ่านไอพี แอดแดรส 192.168.1.1 ซึ่งเป็นหมายเลขไอพี แอดแดรสของเครื่องกระจายสัญญาณ และหลังจากใส่รหัสผ่านเสร็จเรียบร้อยแล้วจะเป็นการเข้าไปยังเมนู WLAN ตามด้วย SSID Settings และดำเนินการตั้งค่าในที่นี้ได้กำหนดให้ชื่อ Singtonl1 ทั้งนี้ในการดำเนินการทดสอบผู้วิจัยได้ทดลองปรับเปลี่ยนการกำหนดค่าระบบรักษาความปลอดภัยให้เป็นแบบ WEP WPA และ WPA2 ซึ่งผลที่ได้ปรากฏว่าทั้ง 3 รูปแบบ ได้รับผลกระทบเช่นเดียวกัน กล่าวคือ สามารถดำเนินการรบกวนหรือโจมตีได้ทั้ง 3 รูปแบบ จากนั้นเข้ามายังเมนู Security ดังภาพที่ 3.13 ซึ่งแสดงให้เห็นหน้าจอวิธีการตั้งรหัสผ่านสำหรับผู้เข้าใช้งานในที่นี้ได้กำหนดเป็น T23P29P31 เป็นอันเสร็จขั้นตอน



ภาพที่ 3.14 แสดงวิธีการตั้งค่าอุปกรณ์กระจายสัญญาณ IEEE 802.11n



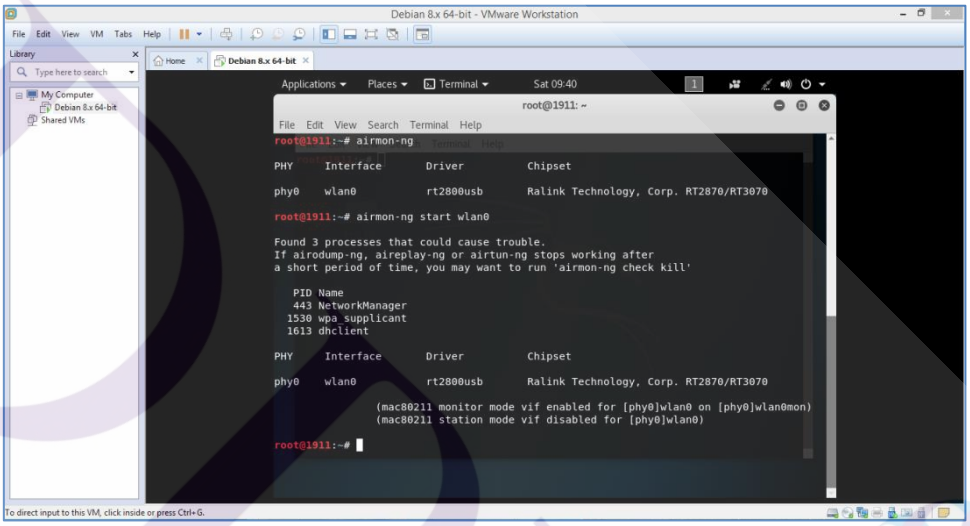
ภาพที่ 3.15 แสดงวิธีการตั้งค่าอุปกรณ์กระจายสัญญาณ IEEE 802.11g

จากภาพที่ 3.14 และ ภาพที่ 3.15 จะแสดงให้เห็นถึงวิธีการการตั้งค่าอุปกรณ์กระจายสัญญาณ IEEE 802.11g และ IEEE 802.11n ซึ่งจะเป็นการตั้งค่าโดยการเข้าผ่านหน้าเว็บบราวเซอร์ของเครื่องกระจายสัญญาณ และเข้าไปยังเมนู WLAN ตามด้วย Basic และเลือกหน้าต่าง Mode เป็น IEEE 802.11n หรือ IEEE 802.11g ให้สอดคล้องตรงกับการทดสอบในแต่ละรูปแบบ ทั้งนี้ในส่วน

ของการตั้งค่าช่องการใช้งานได้กำหนดให้เป็น Channel 6 เหมือนกันทุกครั้งเพื่อให้ได้ผลการทดสอบที่เที่ยงตรงที่สุด เป็นอันเสร็จขั้นตอนการตั้งค่าอุปกรณ์กระจายสัญญาณ

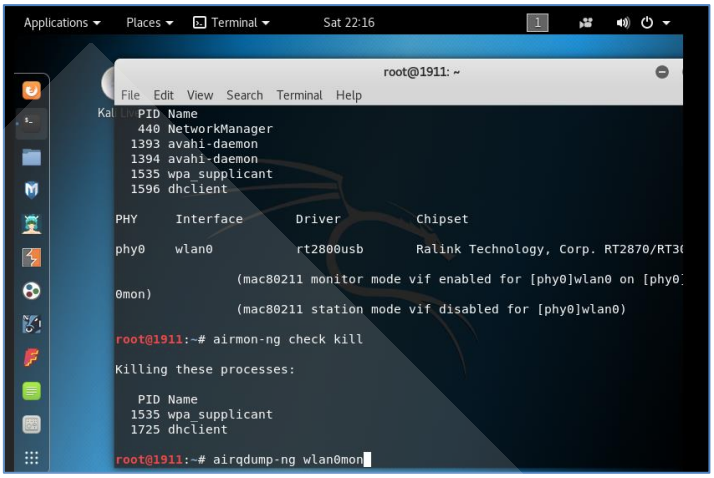
3.4.2 การค้นหาอุปกรณ์กระจายสัญญาณ

หลังจากที่ดำเนินการลงโปรแกรม Kali Linux และเชื่อมต่อสายกับอุปกรณ์ Wireless Lan Card ดังที่แสดงในหัวข้อที่ 3.1 และ 3.2 เสร็จเรียบร้อยแล้ว ในหัวข้อนี้จะขออธิบายวิธีการและขั้นตอนในการค้นหาอุปกรณ์กระจายสัญญาณดังนี้



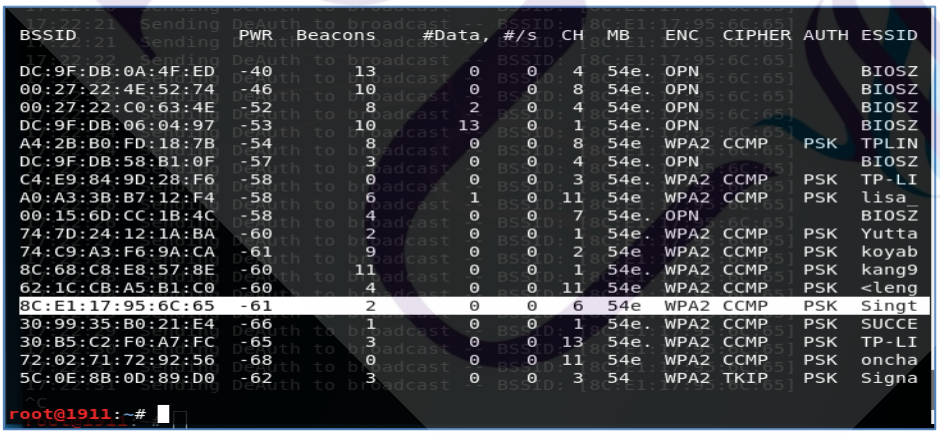
ภาพที่ 3.16 แสดงหน้าจอ Terminal พร้อมการตรวจสอบการเชื่อมต่ออุปกรณ์

หลังจากที่ดำเนินการตามขั้นตอนในหัวข้อที่ 3.1 และ 3.2 เสร็จเรียบร้อยแล้ว ตามภาพที่ 3.16 ในขั้นตอนนี้ให้เปิดหน้าจอ Terminal ของ Kali Linux ขึ้นมาซึ่งจะเห็นว่าเป็นหน้าจอสีดำสำหรับพิมพ์คำสั่งเพื่อสั่งงานตามที่ต้องการ ในที่นี้ใช้คำสั่งแรกคือ airmon-ng เพื่อตรวจสอบสถานะของการเชื่อมต่อ ซึ่งจะเห็นได้ว่าได้มีการเชื่อมต่อกับอุปกรณ์ Wireless Lan Card ที่ชื่อว่า WLAN0 เรียบร้อยแล้ว จากนั้นจะใช้คำสั่ง airmon-ng start wlan0 เพื่อเป็นการสั่งเริ่มต้นการใช้งานอุปกรณ์



ภาพที่ 3.17 แสดงการใช้คำสั่งการค้นหาอุปกรณ์กระจายสัญญาณ

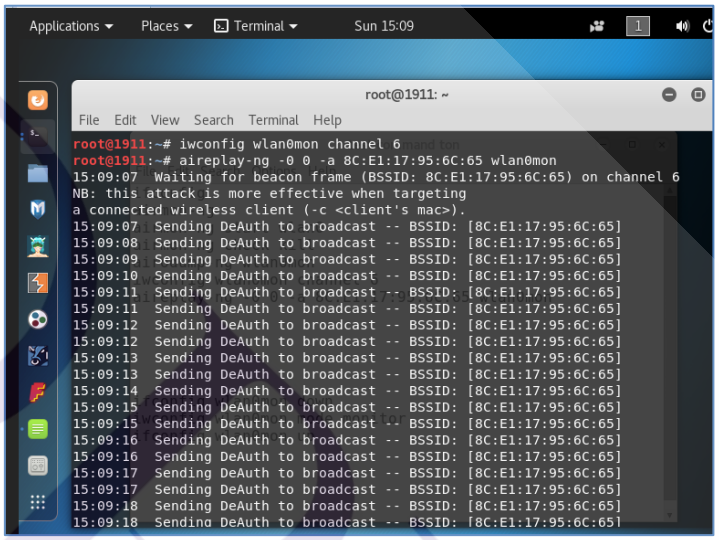
จากภาพที่ 3.17 เป็นการใช้คำสั่งต่อเนื่องมาจากภาพที่ 3.16 ในหน้าจอเดียวกัน ซึ่งจะใช้คำสั่ง airmon-ng check kill ซึ่งเป็นคำสั่งตามที่ระบบได้แจ้งเตือนเพื่อหยุดการทำงานของบางกระบวนการที่ไม่ต้องการและอาจทำให้เกิดความผิดพลาดในการทำงาน หลังจากนั้นจะใช้คำสั่ง airodump-ng wlan0mon เพื่อค้นหาอุปกรณ์กระจายสัญญาณที่ให้บริการอยู่โดยรอบเพื่อเลือกอุปกรณ์เป้าหมายที่ต้องการ



ภาพที่ 3.18 แสดงหน้าจอผลที่ได้จากการค้นหาอุปกรณ์

จากภาพที่ 3.18 จะเห็นว่าผลที่ได้จากการใช้คำสั่ง airodump-ng wlan0mon เพื่อค้นหาอุปกรณ์กระจายสัญญาณที่ให้บริการอยู่โดยรอบ จะทำให้ ทราบค่าที่มีความสำคัญหลายค่า โดยเฉพาะ BSSID หรือแมคแอดแดรส ระดับความแรงของสัญญาณ CH หรือช่องสัญญาณที่ให้บริการ และ ESSID คือชื่อสำหรับให้บริการ ซึ่งเป็นข้อมูลที่เป็นประโยชน์ต่อการนำไปใช้ในการรบกวนหรือโจมตีโดยการส่งเฟรม Deauthentication ในขั้นตอนต่อไป

3.4.3 การรบกวนหรือโจมตีโดยการเฟรม Deauthentication แบบ Broadcast



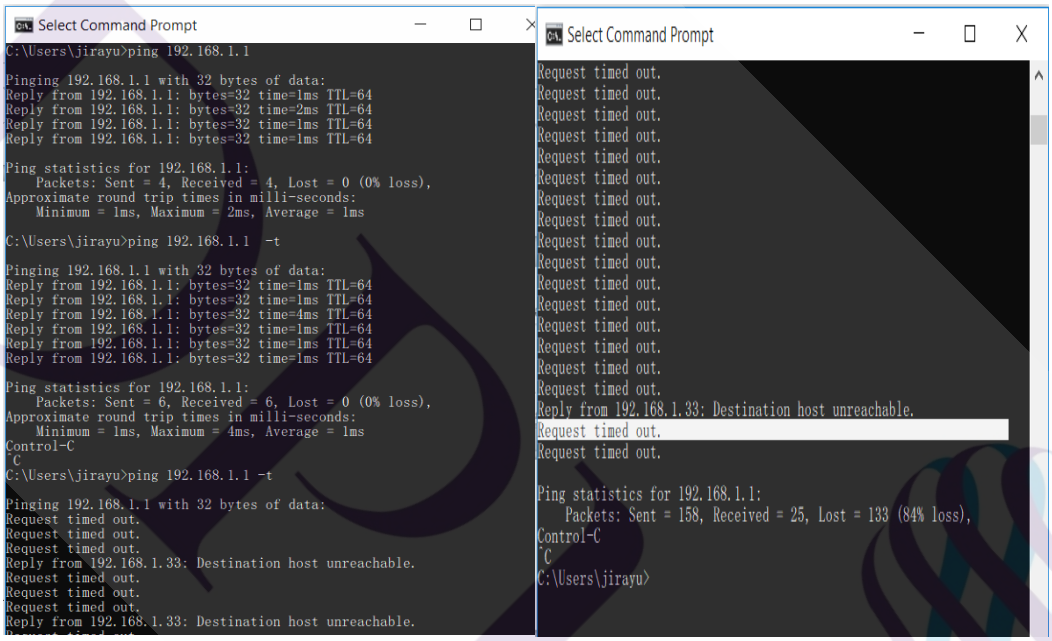
ภาพที่ 3.19 แสดงหน้าจอการส่งสัญญาณรบกวนหรือโจมตี

สำหรับขั้นตอนการรบกวนหรือโจมตีโดยการส่งเฟรม Deauthentication นั้น มีขั้นตอนหรือคำสั่งการทำงานอยู่ 2 คำสั่งย่อย ดังแสดงในรูปที่ 3.19 ได้แก่คำสั่ง iwconfig wlan0mon channel 6 ซึ่งเป็นคำสั่งในการควบคุมให้อุปกรณ์ Wireless Lan Card ส่งสัญญาณออกอากาศเฉพาะช่องสัญญาณที่กำหนด ในที่นี้จะเห็นว่าได้กำหนดให้เป็น CH 6 ซึ่งเป็นข้อมูลที่ได้มากจากขั้นตอนการค้นหาก่อนหน้า จากนั้นเป็นการใช้คำสั่ง aireplay-ng -0 0 –a 8C:E1:17:95:6C65 wlan0mon ซึ่งเป็นคำสั่งให้อุปกรณ์ Wireless Lan Card ส่งสัญญาณ Deauthentication Packet แบบ Broadcast ออกอากาศในช่องสัญญาณที่ 6 โดยปลอมแปลงตัวเองเป็นแมคแอดเดรส 8C:E1:17:95:6C65 ในการส่งสัญญาณ ซึ่งจะส่งผลให้เครื่องคอมพิวเตอร์ที่ได้รับแพ็คเกจที่เรียกว่า Deauthentication นั้นเกิดความเข้าใจว่าได้รับการปฏิเสธหรือการไม่สามารถให้บริการได้ Denial of Service จากอุปกรณ์กระจายสัญญาณเป้าหมาย โดยจะดำเนินการทดสอบในพื้นที่จริงในระยะของการส่งสัญญาณการรบกวนหรือโจมตีที่มีความแตกต่างกันตามที่ได้กำหนดไว้แล้วในหัวข้อที่ 3.3 ซึ่งจะดำเนินการการ

รบกวนหรือโจมตีพร้อมกับเก็บผลการทดสอบจำนวน 3 ครั้ง โดยแต่ละครั้งจะใช้เวลาประมาณ 10 นาที ตามลำดับ

3.4.4 การเก็บผลการทดสอบ

ในการเก็บผลการทดสอบนั้นจะใช้เครื่องคอมพิวเตอร์โน้ตบุ๊กที่สามารถเชื่อมต่อเครือข่ายแบบไร้สายกับอุปกรณ์กระจายสัญญาณภายใต้การทำงานของมาตรฐาน IEEE 802.11g และ IEEE 802.11n ในย่านความถี่ 2.4 GHz ได้ และทำการ Ping เพื่อเก็บผลสรุปซึ่งจะทำให้ทราบถึงค่าประสิทธิภาพในการเชื่อมต่อสัญญาณกับอุปกรณ์กระจายสัญญาณได้



ภาพที่ 3.20 แสดงหน้าจอผลการทดสอบ

จากภาพที่ 3.20 แสดงให้เห็นหน้าจอการเก็บผลการทดสอบด้วยการ ping ซึ่งจะทำให้ทราบค่าประสิทธิภาพโดยรวมของแต่ละวงรอบการทดสอบ อาทิ จำนวน packets Sent จำนวนแพ็คเกจที่ทำการ ping ทั้งหมด Received จำนวนแพ็คเกจ ที่สามารถรับได้ Lost คือจำนวนที่ไม่สามารถติดต่อสื่อสารหรือไม่สามารถรับแพ็คเกจได้ และ % loss จะเป็นค่าร้อยละของการสูญเสียหรือไม่สามารถติดต่อสื่อสารได้ โดยจะเก็บผลการทดสอบในแต่ละระยะทาง จำนวน 3 ครั้ง โดยแต่ละครั้งจะใช้เวลาประมาณ 10 นาที จากนั้นนำผลที่ได้แต่ละครั้งมาหาค่าเฉลี่ยและสรุปผลการดำเนินการต่อไป

บทที่ 4
ผลการทดลอง

ผลการทดสอบการรบกวนหรือการโจมตีเครือข่ายไร้สาย โดยวิธี De-Authentication [3] ซึ่งใช้เทคนิคการปลอมแปลงแมคแอดเดรสของอุปกรณ์กระจายสัญญาณเครื่องเป้าหมาย และดำเนินการรบกวนหรือโจมตีด้วยวิธีการส่งเฟรม Deauthentication ไปยังเครื่องคอมพิวเตอร์ที่กำลังติดต่อสื่อสารอยู่กับอุปกรณ์กระจายสัญญาณเครื่องเป้าหมายเครื่องนั้น ซึ่งจะส่งผลให้เครื่องคอมพิวเตอร์ที่ได้รับเฟรม Deauthentication นั้น เกิดความเข้าใจว่าได้รับการปฏิเสธหรือการไม่สามารถให้บริการได้ [4] โดยจะดำเนินการทดสอบในพื้นที่จริงในระยะของการส่งสัญญาณการรบกวนหรือโจมตีที่มีความแตกต่างกัน ในสภาวะการใช้งานในพื้นที่โล่งระดับสายตาและการใช้งานในพื้นที่ห้องทั่วไป ในย่านความถี่ 2.4 GHz ดังที่กล่าวไว้ตั้งแต่ต้นในหัวข้อก่อนหน้า ประกอบด้วยรูปแบบของมาตรฐานการใช้งานและสถานที่ที่มีความแตกต่างกัน โดยแบ่งเป็น 4 รูปแบบผลการทดสอบดังนี้

4.1 ผลการทดสอบในพื้นที่โล่งแนวระดับสายตา ภายใต้มาตรฐานการทำงาน IEEE 802.11n

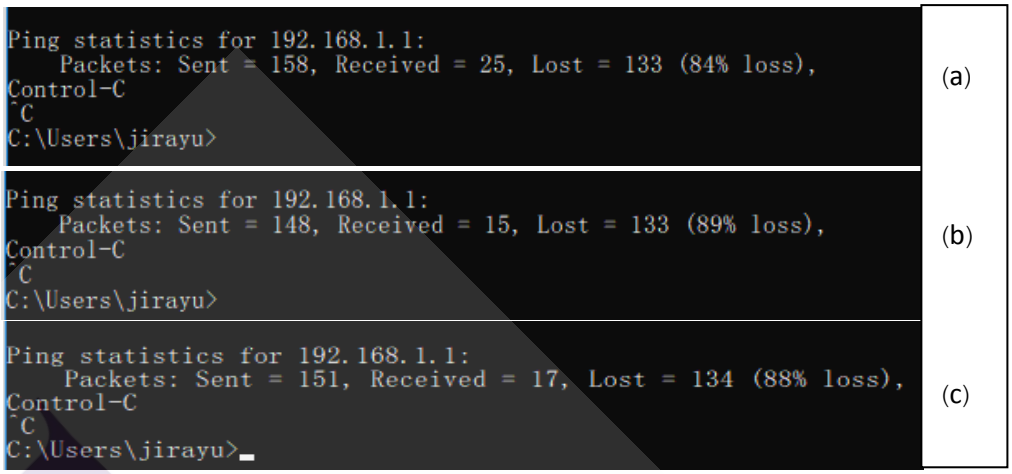
4.2 ผลการทดสอบในพื้นที่โล่งแนวระดับสายตา ภายใต้มาตรฐานการทำงาน IEEE 802.11g

4.3 ผลการทดสอบในพื้นที่ห้องทั่วไป ภายใต้มาตรฐานการทำงาน IEEE 802.11n

4.4 ผลการทดสอบในพื้นที่ห้องทั่วไป ภายใต้มาตรฐานการทำงาน IEEE 802.11g

4.1 ผลการทดสอบในพื้นที่โล่งแนวระดับสายตา ภายใต้มาตรฐานการทำงาน IEEE 802.11n

ในการดำเนินการทดสอบการรบกวนหรือการโจมตีเครือข่ายไร้สาย โดยวิธี De-Authentication ในพื้นที่โล่งแนวระดับสายตาภายใต้มาตรฐานการทำงาน IEEE 802.11n จากที่กล่าวมาแล้วในบทที่ 3 ซึ่งจะดำเนินการทดสอบจำนวน 3 ครั้ง ครั้งละประมาณ 10 นาที ในแต่ละระยะห่าง 10 20 50 100 200 300 350 400 450 และ 500 เมตร ตามลำดับระหว่างเครื่องที่กำหนดให้เป็น Attacker กับอุปกรณ์กระจายสัญญาณและเครื่องคอมพิวเตอร์ที่กำลังเชื่อมต่อแบบไร้สายสำหรับใช้ในการเก็บผลการทดสอบด้วยการ Ping ซึ่งจะทำให้ทราบค่า ประสิทธิภาพในการติดต่อสื่อสารหรือการเชื่อมต่อโดยรวมของระบบได้ ผู้วิจัยได้ดำเนินการทดสอบและรวบรวมผลการทดสอบในรูปแบบของรูปภาพ ตารางและกราฟสรุปผลซึ่งจำทำให้ง่ายต่อความเข้าใจยิ่งขึ้นดังนี้



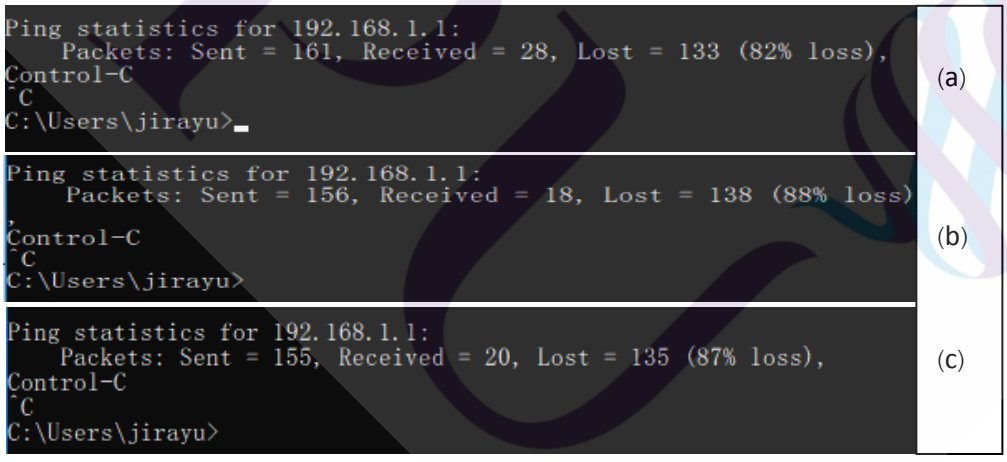
ภาพที่ 4.1 ผลการทดสอบ Outdoor ระยะ 10 เมตร ครั้งที่ 1-3 (IEEE 802.11n)

จากภาพที่ 4.1 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ 10 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 158, Received = 25, Lost = 133 และ 84% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 148, Received = 15, Lost = 133 และ 89% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 151, Received = 17, Lost = 134 และ 88% loss



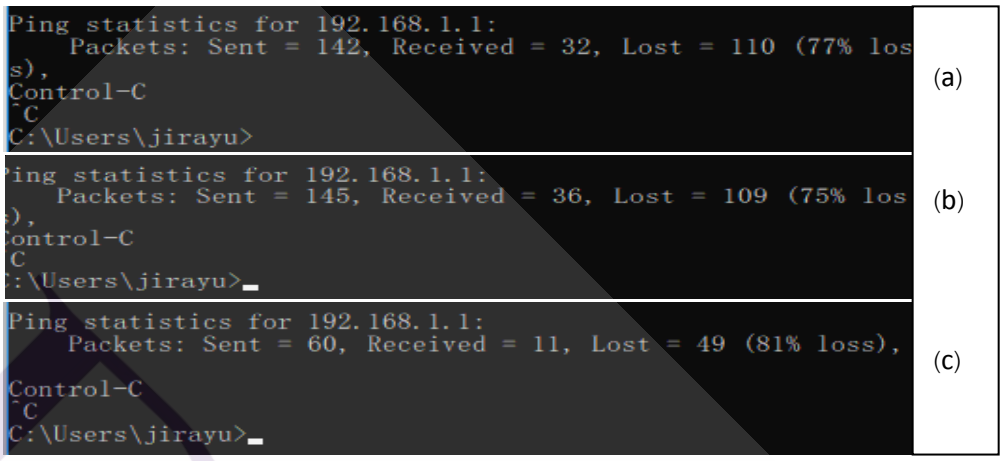
ภาพที่ 4.2 ผลการทดสอบ Outdoor ระยะ 20 เมตร ครั้งที่ 1-3 (IEEE 802.11n)

จากภาพที่ 4.2 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ 20 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 161, Received = 28, Lost = 133 และ 82% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 156, Received = 18, Lost = 138 และ 88% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 155, Received = 20, Lost = 135 และ 87% loss



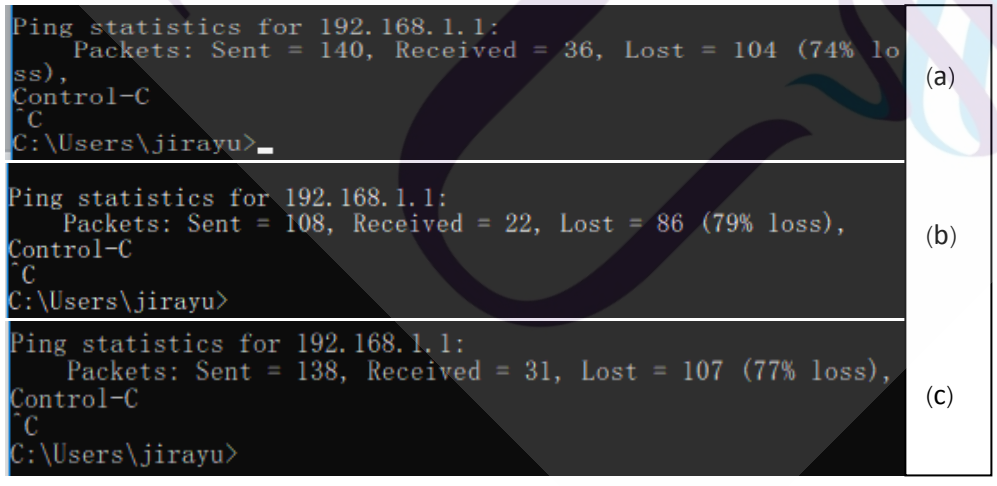
ภาพที่ 4.3 ผลการทดสอบ Outdoor ระยะ 50 เมตร ครั้งที่ 1-3 (IEEE 802.11n)

จากรูปที่ 4.3 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ 50 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 142, Received = 32, Lost = 110 และ 77% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 145, Received = 36, Lost = 109 และ 75% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 60, Received = 11, Lost = 49 และ 81% loss



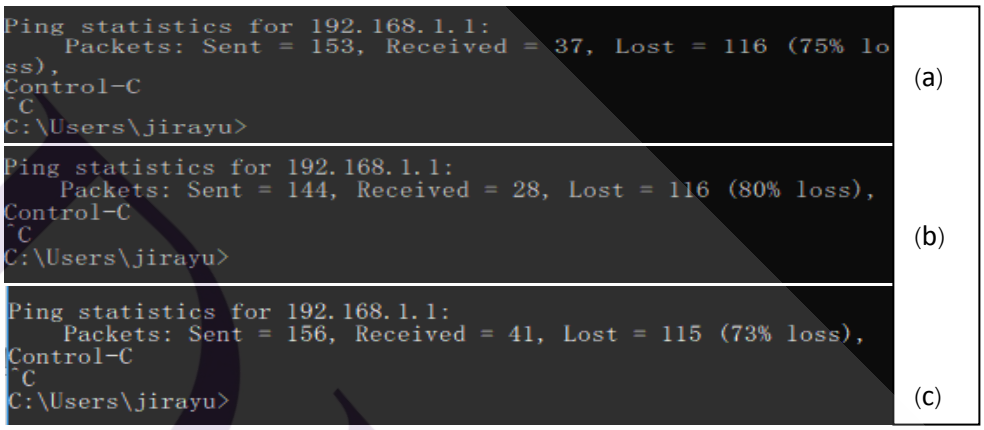
ภาพที่ 4.4 ผลการทดสอบ Outdoor ระยะ 100 เมตร ครั้งที่ 1-3 (IEEE 802.11n)

จากภาพที่ 4.4 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ100 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 140, Received = 36, Lost = 104 และ 74% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 108, Received = 22, Lost = 86 และ 79% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 138, Received = 31, Lost = 107 และ 77% loss



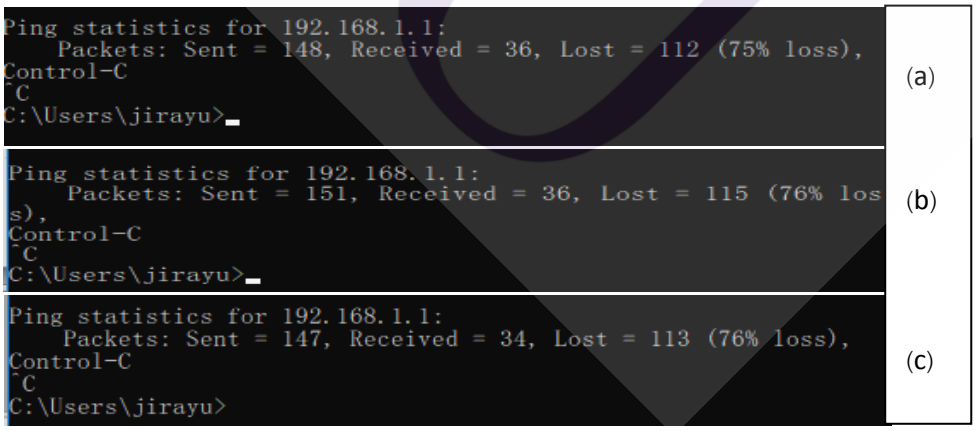
ภาพที่ 4.5 ผลการทดสอบ Outdoor ระยะ 200 เมตร ครั้งที่ 1-3 (IEEE 802.11n)

จากภาพที่ 4.5 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ200 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 153, Received = 37, Lost = 116 และ 75% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 144, Received = 28, Lost = 116 และ 80% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 156, Received = 41, Lost = 115 และ 73% loss



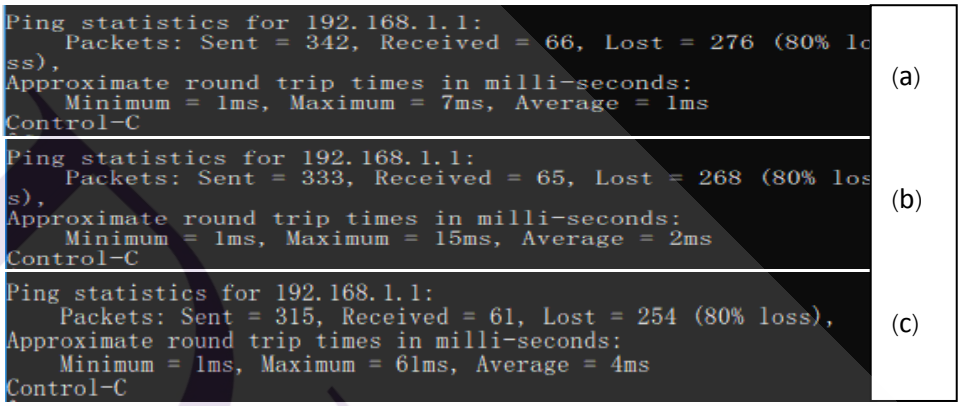
ภาพที่ 4.6 ผลการทดสอบ Outdoor ระยะ 300 เมตร ครั้งที่ 1-3 (IEEE 802.11n)

จากภาพที่ 4.6 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ300 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 148, Received = 36, Lost = 112 และ 75% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 151, Received = 36, Lost = 115 และ 76% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 147, Received = 34, Lost = 113 และ 76% loss



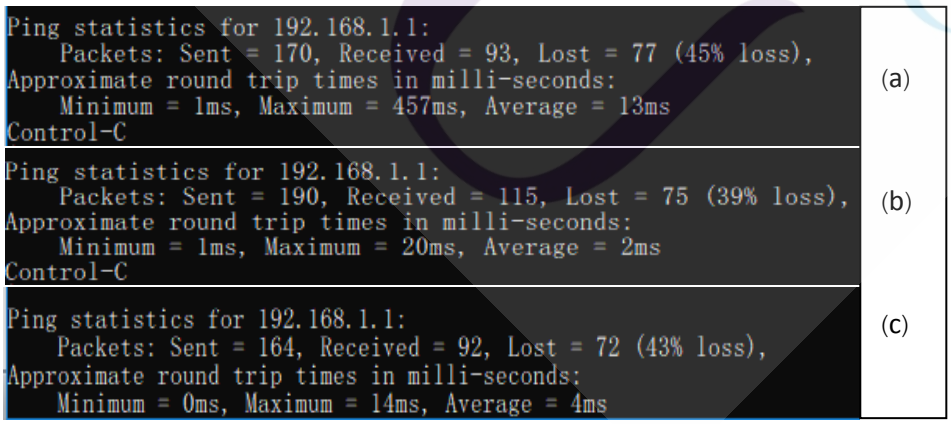
ภาพที่ 4.7 ผลการทดสอบ Outdoor ระยะ 350 เมตร ครั้งที่ 1-3 (IEEE 802.11n)

จากภาพที่ 4.7 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ350 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 342, Received = 66, Lost = 276 และ 80% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 333, Received = 65, Lost = 268 และ 80% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 315, Received = 61, Lost = 254 และ 80% loss



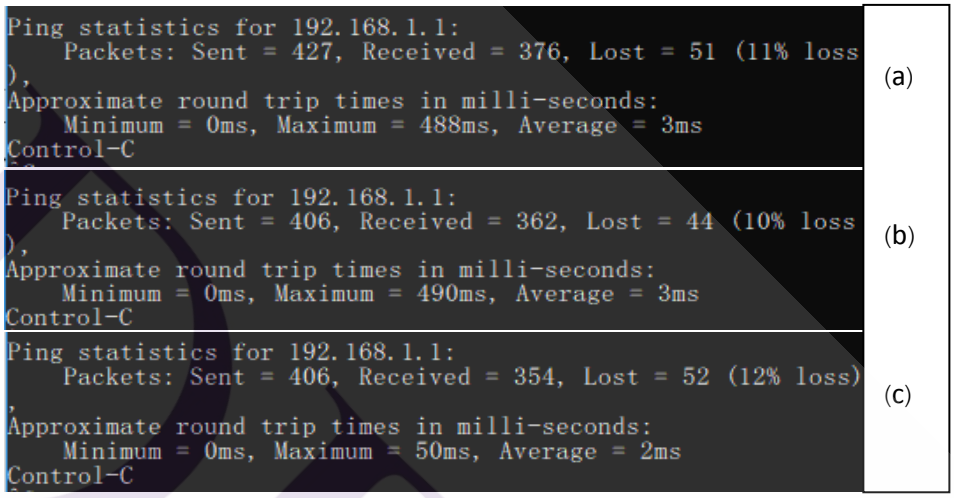
ภาพที่ 4.8 ผลการทดสอบ Outdoor ระยะ 400 เมตร ครั้งที่ 1-3 (IEEE 802.11n)

จากภาพที่ 4.8 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ400 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 170, Received = 93, Lost = 77 และ 45% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 190, Received = 115, Lost = 75 และ 39% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 164, Received = 92, Lost = 72 และ 43% loss



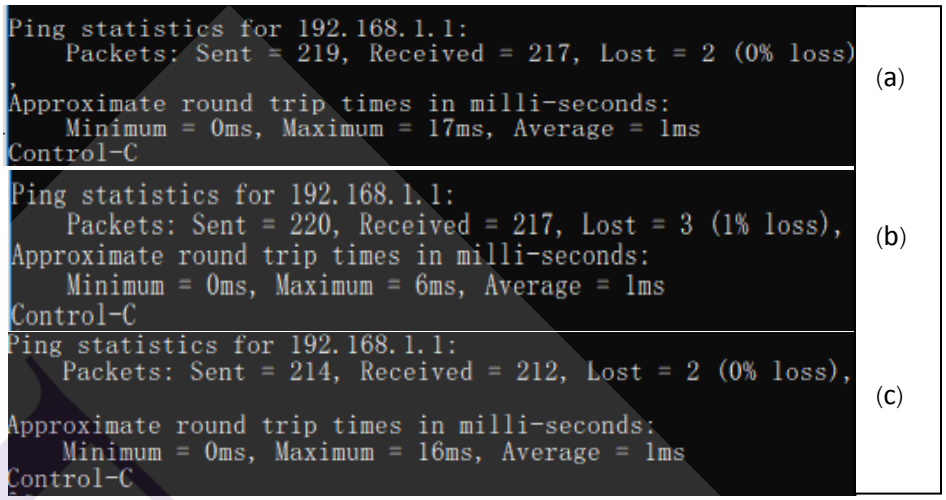
ภาพที่ 4.9 ผลการทดสอบ Outdoor ระยะ 450 เมตร ครั้งที่ 1-3 (IEEE 802.11n)

จากภาพที่ 4.9 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ450 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 427, Received = 376, Lost = 51 และ 11% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 406, Received = 362, Lost = 44 และ 10% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 406, Received = 354, Lost = 52 และ 12% loss

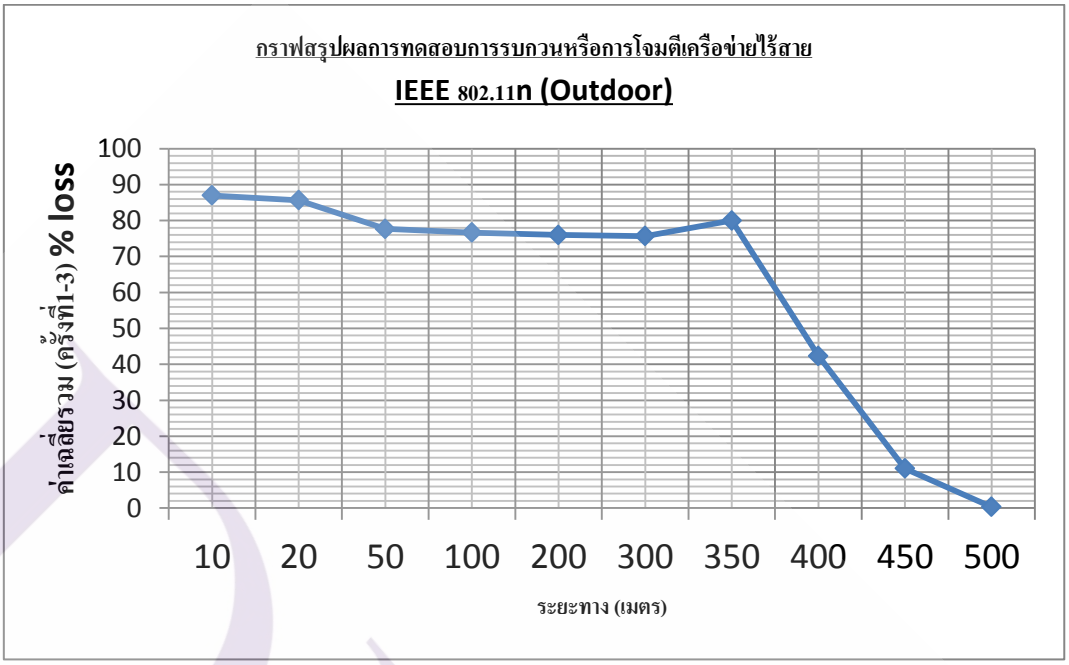


ภาพที่ 4.10 ผลการทดสอบ Outdoor ระยะ 500 เมตร ครั้งที่ 1-3 (IEEE 802.11n)

จากภาพที่ 4.10 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ 500 เมตร ดังนี้ ครั้งที่ 1 (a) มีจานวน Packets: Sent = 219, Received = 217, Lost = 2 และ 0% loss
ครั้งที่ 2 (b) มีจานวน Packets: Sent = 220, Received = 217, Lost = 3 และ 1% loss
ครั้งที่ 3 (c) มีจานวน Packets: Sent = 214, Received = 212, Lost = 2 และ 0% loss

ตารางที่ 4.1 สรุปผลการทดสอบในพื้นที่โล่งแนวระดับสายตา ภายใต้มาตรฐานการทำงาน IEEE 802.11n

ระยะทาง (เมตร)	ครั้งที่ 1	ครั้งที่ 2	ครั้งที่ 3	ค่าเฉลี่ยรวม (ครั้งที่1-3)
	% loss	% loss	% loss	% loss
10	84	89	88	87
20	82	88	87	85.66
50	77	75	81	77.66
100	74	79	77	76.66
200	75	80	73	76
300	75	76	76	75.66
350	80	80	80	80
400	45	39	43	42.33
450	11	10	12	11
500	0	1	0	0.33

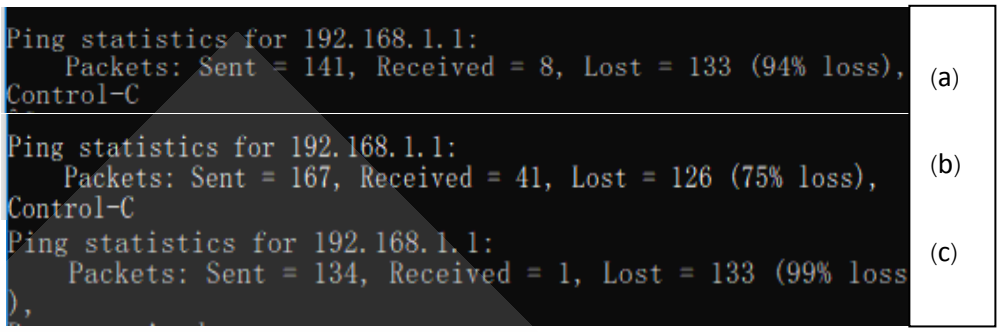


ภาพที่ 4.11 กราฟสรุปผลการทดสอบในพื้นที่โล่งแนวระดับสายตา (IEEE 802.11n)

จากตารางที่ 4.1 และรูปที่ 4.11 เป็นการแสดงผลสรุปการทดสอบในพื้นที่โล่งแนวระดับสายตา (IEEE 802.11n) ในรูปแบบของตารางและเส้นกราฟแสดงค่าเฉลี่ย % loss ในแต่ละระยะของการทดสอบ 10 20 50 100 200 300 350 400 450 และ 500 เมตร ตามลำดับ ซึ่งจะเห็นเมื่อระยะห่างในการทดสอบเพิ่มมากขึ้นจะส่งผลให้ประสิทธิภาพในการรบกวนหรือโจมตีเครือข่ายไร้สายโดยวิธีการ De-Authentication ลดลง และมีค่าเข้าใกล้ 0% loss ที่ระยะ 500 เมตร

4.2 ผลการทดสอบในพื้นที่โล่งแนวระดับสายตา ภายใต้มาตรฐานการทำงาน IEEE 802.11g

ในการดำเนินการทดสอบในพื้นที่โล่งแนวระดับสายตา ภายใต้มาตรฐานการทำงาน IEEE 802.11g นั้น จะดำเนินการในลักษณะเช่นเดียวกับการทดสอบ IEEE 802.11n ทุกด้าน โดยจะมีความแตกต่างกันเฉพาะการตั้งค่าอุปกรณ์กระจายสัญญาณให้เป็นโหมดการทำงาน ภายใต้มาตรฐานการทำงาน IEEE 802.11g เท่านั้น ซึ่งมีผลการทดสอบในรูปแบบของรูปภาพ ตารางและกราฟสรุปผลดังนี้



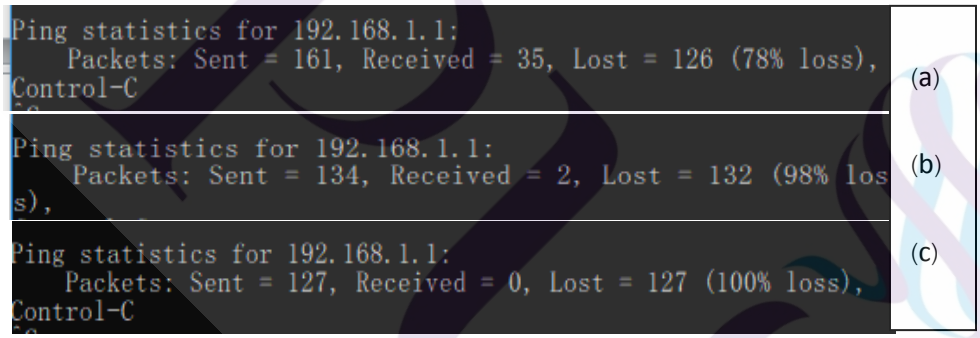
ภาพที่ 4.12 ผลการทดสอบ Outdoor ระยะ 10 เมตร ครั้งที่ 1-3 (IEEE 802.11g)

จากภาพที่ 4.12 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ 10 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 141, Received = 8, Lost = 133 และ 94% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 167, Received = 41, Lost = 126 และ 75% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 134, Received = 1, Lost = 133 และ 99% loss



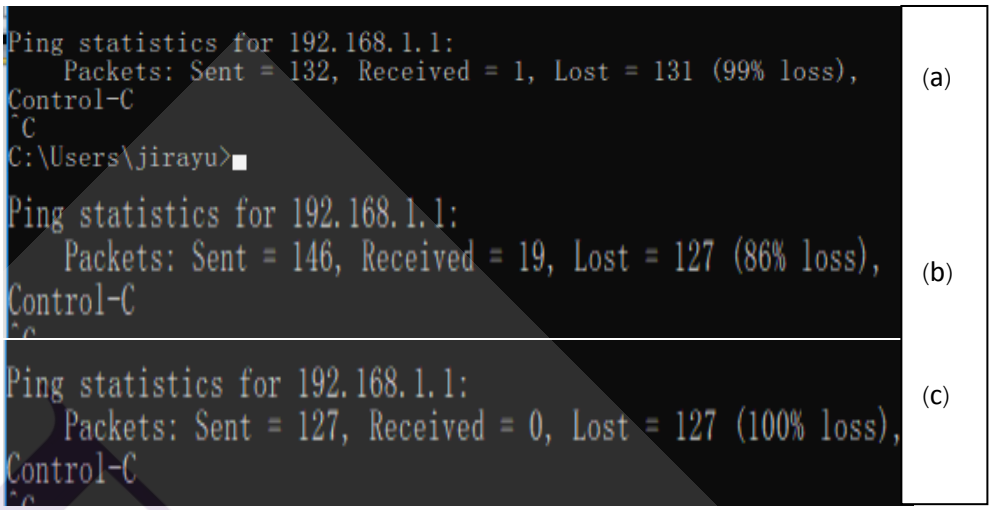
ภาพที่ 4.13 ผลการทดสอบ Outdoor ระยะ 20 เมตร ครั้งที่ 1-3 (IEEE 802.11g)

จากภาพที่ 4.13 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ 20 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 161, Received = 2, Lost = 126 และ 78% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 134, Received = 2, Lost = 132 และ 98% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 127, Received = 0, Lost = 127 และ 100% loss



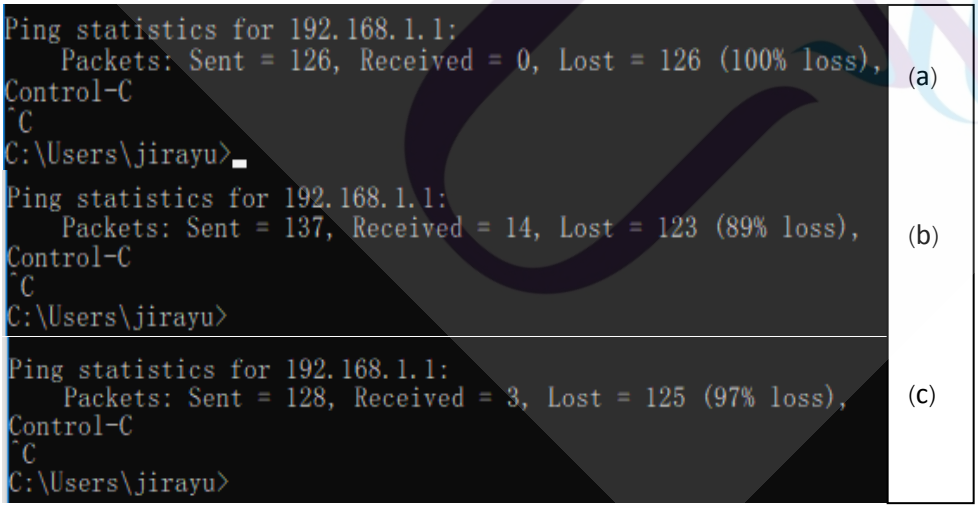
ภาพที่ 4.14 ผลการทดสอบ Outdoor ระยะ 50 เมตร ครั้งที่ 1-3 (IEEE 802.11g)

จากภาพที่ 4.14 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ 50 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 132, Received = 1, Lost = 131 และ 99% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 146, Received = 19, Lost = 127 และ 86% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 127, Received = 0, Lost = 127 และ 100% loss



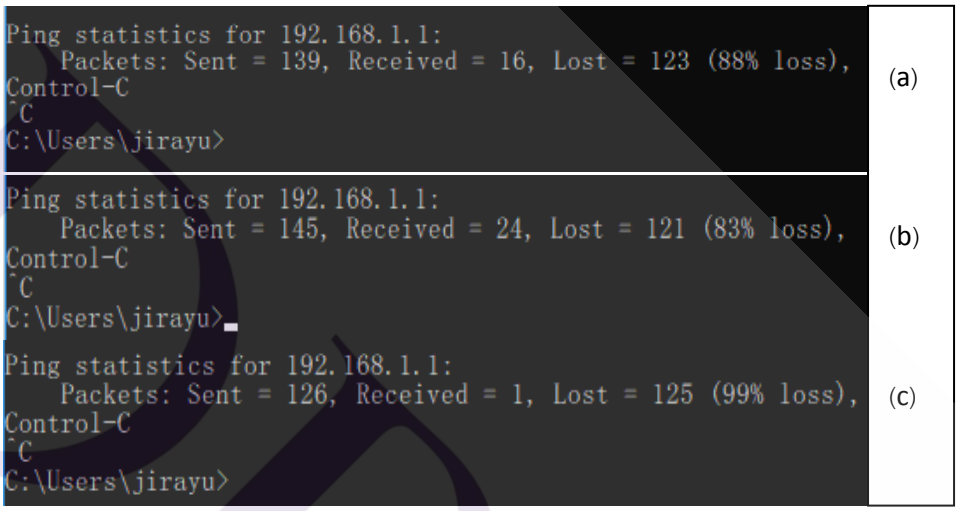
ภาพที่ 4.15 ผลการทดสอบ Outdoor ระยะ 100 เมตร ครั้งที่ 1-3 (IEEE 802.11g)

จากภาพที่ 4.15 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ 100 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 126, Received = 0, Lost = 126 และ 100% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 137, Received = 14, Lost = 123 และ 89% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 128, Received = 3, Lost = 125 และ 97% loss



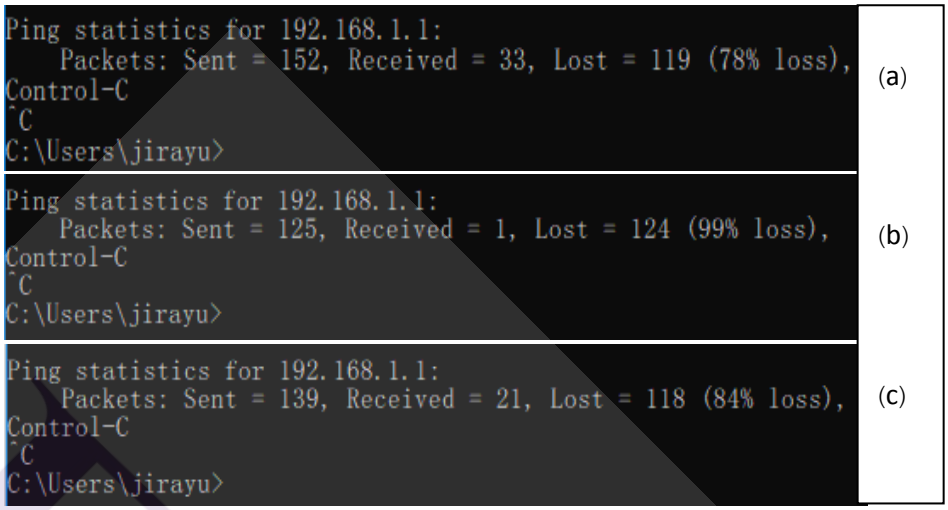
ภาพที่ 4.16 ผลการทดสอบ Outdoor ระยะ 200 เมตร ครั้งที่ 1-3 (IEEE 802.11g)

จากภาพที่ 4.16 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ 200 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 139, Received = 16, Lost = 123 และ 88% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 145, Received = 24, Lost = 121 และ 83% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 126, Received = 1, Lost = 125 และ 99% loss



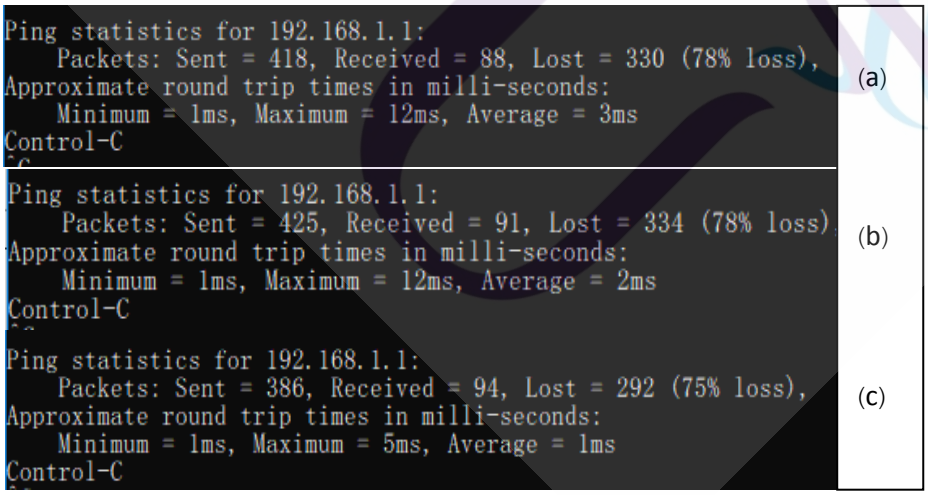
ภาพที่ 4.17 ผลการทดสอบ Outdoor ระยะ 300 เมตร ครั้งที่ 1-3 (IEEE 802.11g)

จากภาพที่ 4.17 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ 300 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 152, Received = 33, Lost = 119 และ 78% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 125, Received = 1, Lost = 124 และ 99% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 139, Received = 21, Lost = 118 และ 84% loss



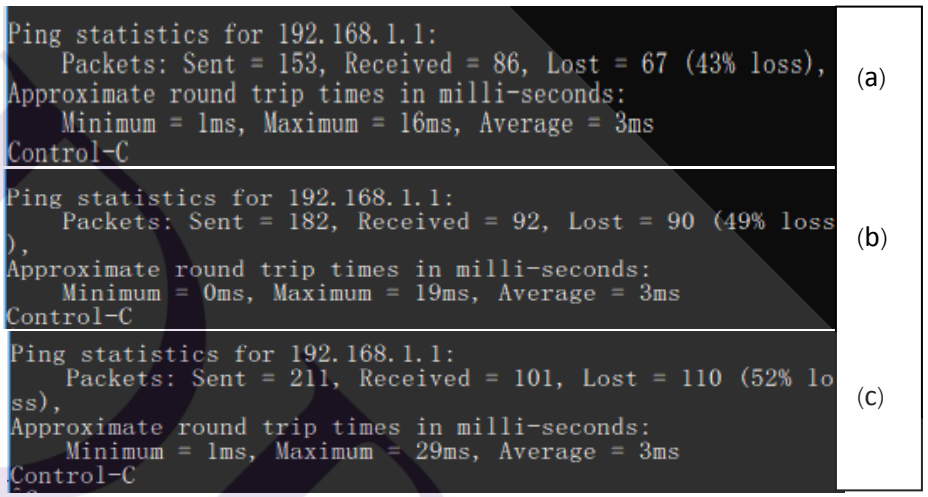
ภาพที่ 4.18 ผลการทดสอบ Outdoor ระยะ 350 เมตร ครั้งที่ 1-3 (IEEE 802.11g)

จากภาพที่ 4.18 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ 350 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 418, Received = 88, Lost = 330 และ 78% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 425, Received = 91, Lost = 334 และ 78% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 386, Received = 94, Lost = 292 และ 75% loss



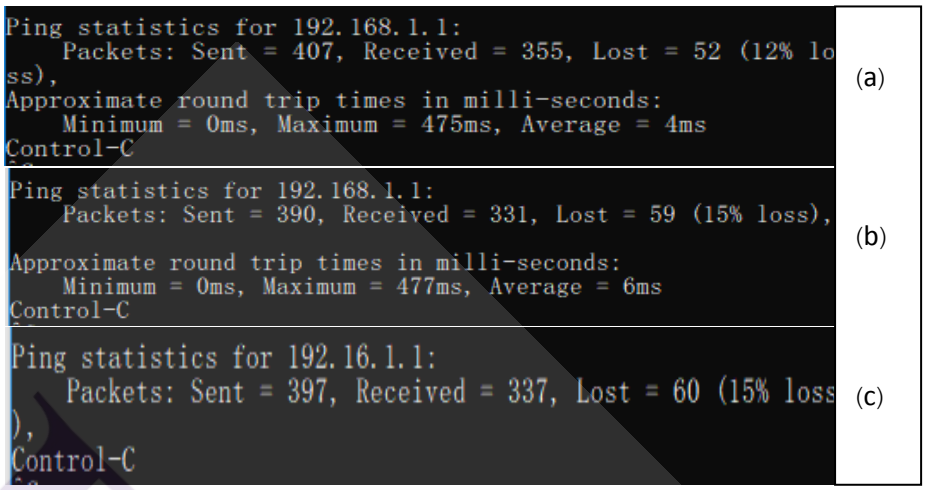
ภาพที่ 4.19 ผลการทดสอบ Outdoor ระยะ 400 เมตร ครั้งที่ 1-3 (IEEE 802.11g)

จากภาพที่ 4.19 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ 400 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 153, Received = 86, Lost = 67 และ 43% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 182, Received = 92, Lost = 90 และ 49% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 211, Received = 101, Lost = 110 และ 52% loss



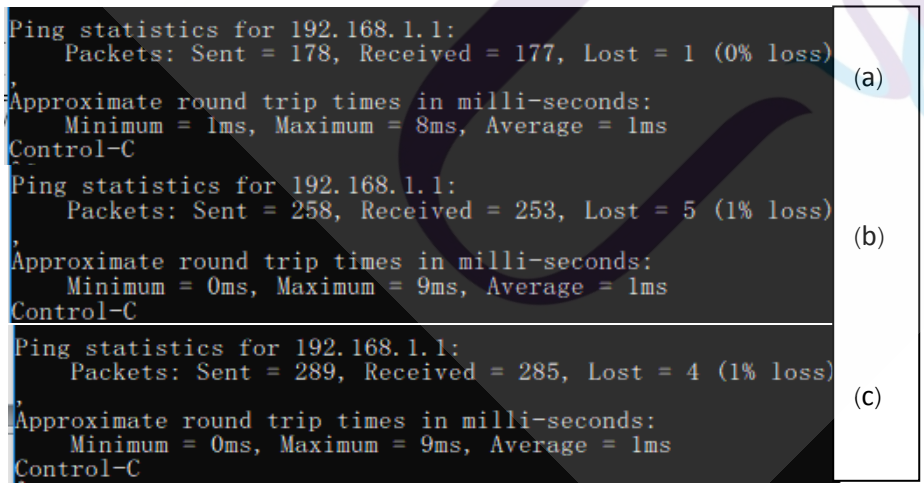
ภาพที่ 4.20 ผลการทดสอบ Outdoor ระยะ 450 เมตร ครั้งที่ 1-3 (IEEE 802.11g)

จากภาพที่ 4.20 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ 450 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 407, Received = 355, Lost = 52 และ 12% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 390, Received = 331, Lost = 59 และ 15% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 397, Received = 337, Lost = 60 และ 15% loss



ภาพที่ 4.21 ผลการทดสอบ Outdoor ระยะ 500 เมตร ครั้งที่ 1-3 (IEEE 802.11g)

จากภาพที่ 4.21 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่โล่งที่ระยะ 500 เมตร ดังนี้

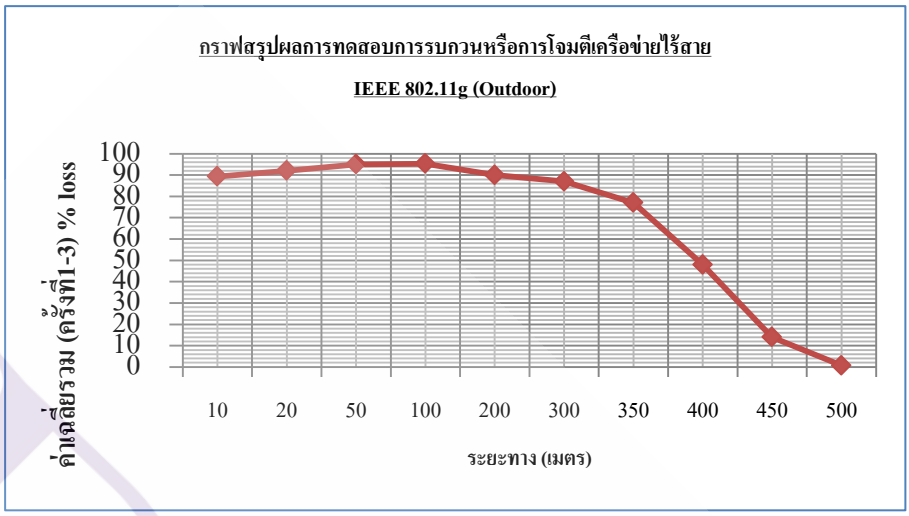
ครั้งที่ 1 (a) มีจานวน Packets: Sent = 178, Received = 177, Lost = 1 และ 0% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 258, Received = 253, Lost = 5 และ 1% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 289, Received = 285, Lost = 4 และ 1% Loss

ตารางที่ 4.2 สรุปผลการทดสอบในพื้นที่โล่งแนวระดับสายตา ภายใต้มาตรฐานการทำงาน IEEE 802.11g

ระยะทาง (เมตร)	ครั้งที่ 1	ครั้งที่ 2	ครั้งที่ 3	ค่าเฉลี่ยรวม (ครั้งที่1-3)
	% loss	% loss	% loss	% loss
10	94	75	99	89.33
20	78	98	100	92
50	99	86	100	95
100	100	89	97	95.33
200	88	83	99	90
300	78	99	84	87
350	78	78	75	77
400	43	49	52	48
450	12	15	15	14
500	0	1	1	0.66

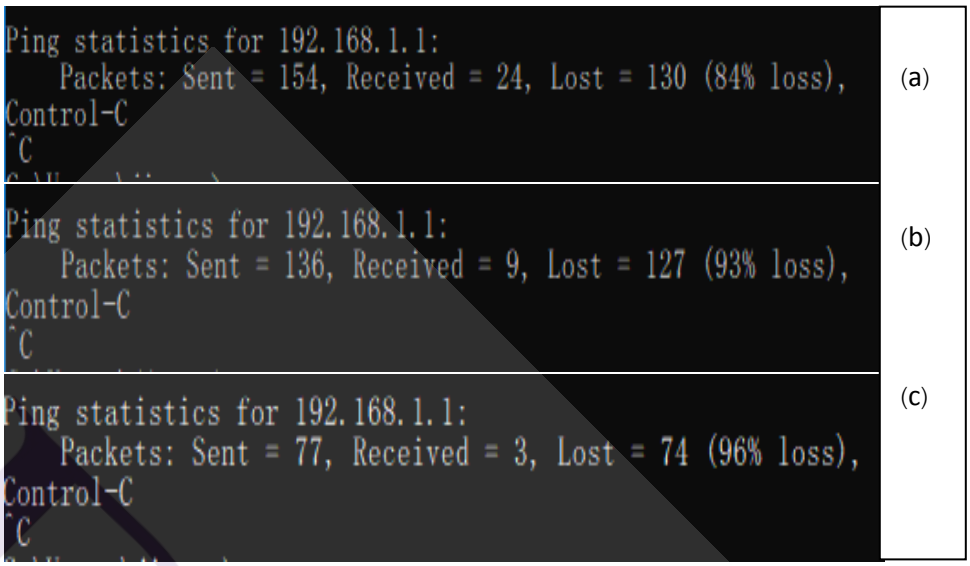


ภาพที่ 4.22 กราฟสรุปผลการทดสอบในพื้นที่โล่งแนวระดับสายตา (IEEE 802.11g)

จากตารางที่ 4.1 และรูปที่ 4.11 เป็นการแสดงผลสรุปการทดสอบในพื้นที่โล่งแนวระดับสายตา (IEEE 802.11g) ในรูปแบบของตารางและเส้นกราฟแสดงค่าเฉลี่ย % loss ในแต่ละระยะของการทดสอบ 10 20 50 100 200 300 350 400 450 และ 500 เมตร ซึ่งจะเห็นได้ว่าเมื่อระยะห่างในการทดสอบ เพิ่มมากขึ้นจะส่งผลให้ประสิทธิภาพในการรบกวนหรือโจมตีเครือข่ายไร้สาย โดยวิธีการ De-Authentication ลดลง และมีค่าเข้าใกล้ 0% loss ที่ระยะ 500 เมตร

4.3 ผลการทดสอบในพื้นที่ห้องทั่วไป ภายใต้มาตรฐานการทำงาน IEEE 802.11n

ในการดำเนินการทดสอบการรบกวนหรือการโจมตีเครือข่ายไร้สาย โดยวิธีการ De-Authentication ในพื้นที่ห้องทั่วไป ภายใต้มาตรฐานการทำงาน IEEE 802.11n จากที่กล่าวมาแล้วในบทที่ 3 ซึ่งจะดำเนินการทดสอบจำนวน 3 ครั้ง ครั้งละประมาณ 10 นาที ในแต่ละระยะห่าง 20 40 60 80 100 120 และ 140 เมตร ตามลำดับ ระหว่างเครื่องที่กำหนดให้เป็น Attacker ซึ่งอยู่ภายนอกห้องกับอุปกรณ์กระจายสัญญาณและเครื่องคอมพิวเตอร์ที่กำลังเชื่อมต่อแบบไร้สายซึ่งจะอยู่ภายในห้องสำหรับใช้ในการเก็บผลการทดสอบด้วยการ Ping ซึ่งจะทำให้ทราบค่า ประสิทธิภาพในการติดต่อสื่อสารหรือการเชื่อมต่อโดยรวมของระบบได้ ผู้วิจัยได้ดำเนินการทดสอบและรวบรวมผลการทดสอบในรูปแบบของรูปภาพ ตารางและกราฟสรุปผลซึ่งจะทำให้ง่ายต่อความเข้าใจยิ่งขึ้นดังนี้



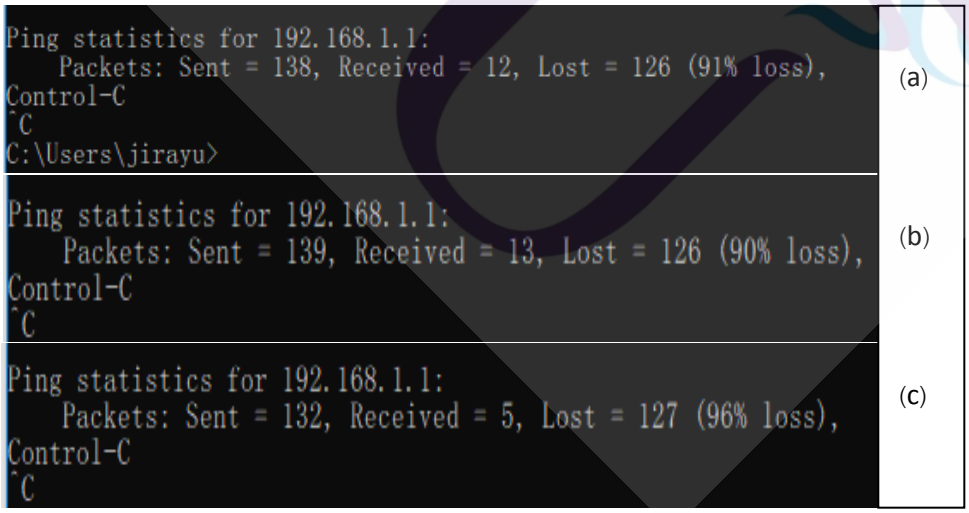
ภาพที่ 4.23 ผลการทดสอบ Indoor ระยะ 20 เมตร ครั้งที่ 1-3 (IEEE 802.11n)

จากภาพที่ 4.23 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่ห้องทั่วไป ระยะ 20 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 154, Received = 24, Lost = 130 และ 84% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 136, Received = 9, Lost = 127 และ 93% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 77, Received = 3, Lost = 74 และ 96% loss



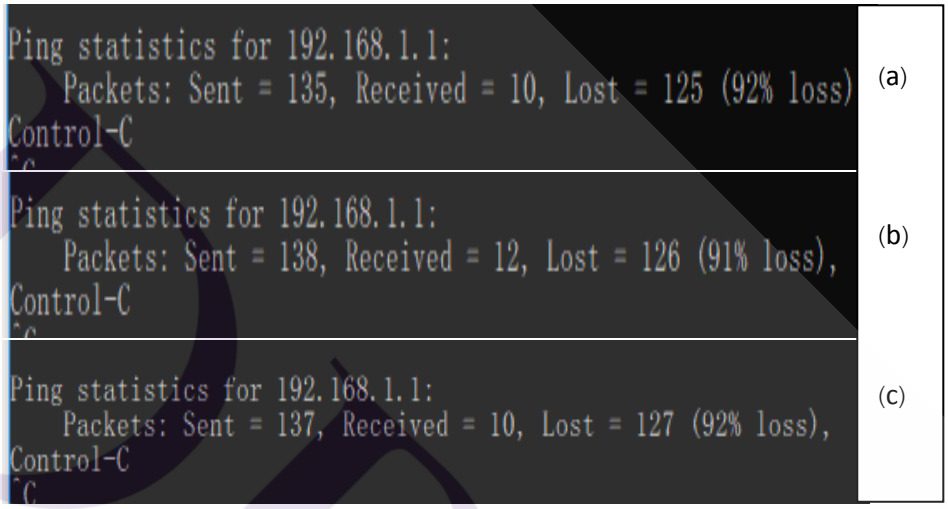
ภาพที่ 4.24 ผลการทดสอบ Indoor ระยะ 40 เมตร ครั้งที่ 1-3 (IEEE 802.11n)

จากภาพที่ 4.24 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่ห้องทั่วไป ระยะ 40 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 138, Received = 12, Lost = 126 และ 91% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 139, Received = 13, Lost = 126 และ 90% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 132, Received = 5, Lost = 127 และ 96% loss



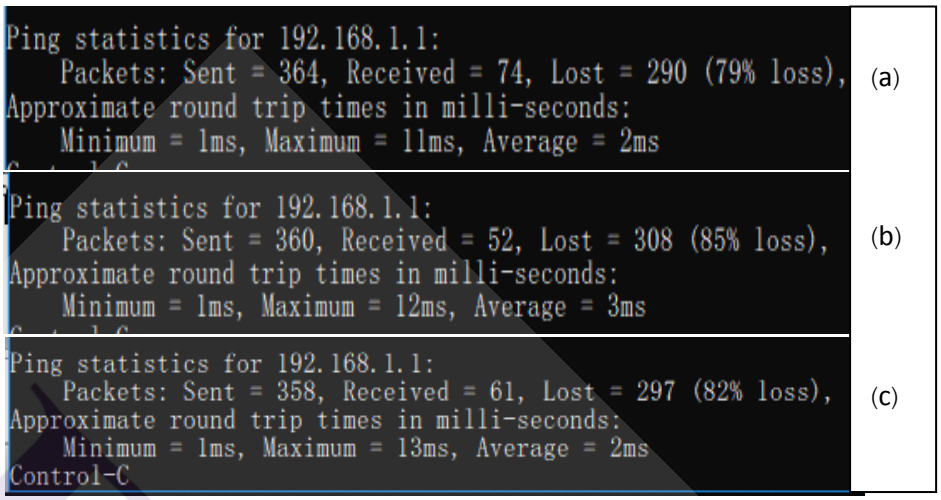
ภาพที่ 4.25 ผลการทดสอบ Indoor ระยะ 60 เมตร ครั้งที่ 1-3 (IEEE 802.11n)

จากภาพที่ 4.25 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่ห้องทั่วไป ระยะ 60 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 135, Received = 10, Lost = 125 และ 92% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 138, Received = 12, Lost = 126 และ 91% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 137, Received = 10, Lost = 127 และ 92% loss



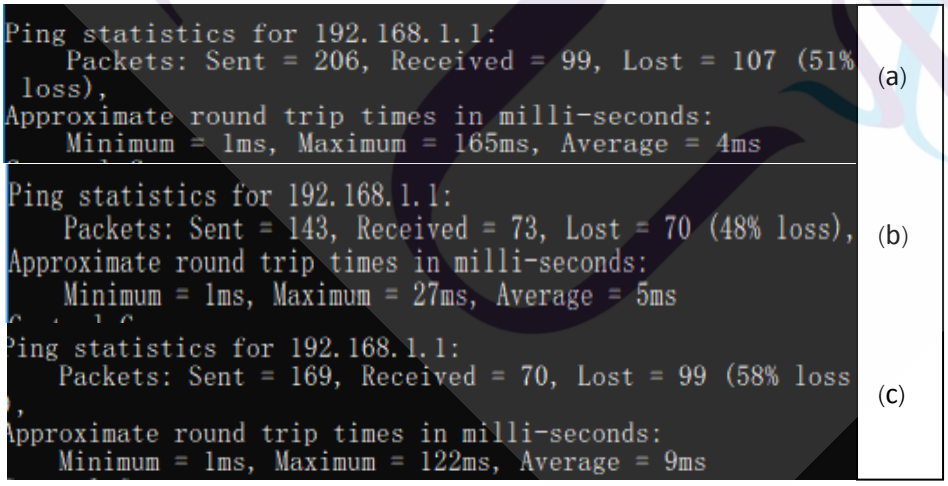
ภาพที่ 4.26 ผลการทดสอบ Indoor ระยะ 80 เมตร ครั้งที่ 1-3 (IEEE 802.11n)

จากภาพที่ 4.26 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่ห้องทั่วไป ระยะ 80 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 364, Received = 74, Lost = 290 และ 79% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 360, Received = 52, Lost = 308 และ 85% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 358, Received = 61, Lost = 297 และ 82% loss



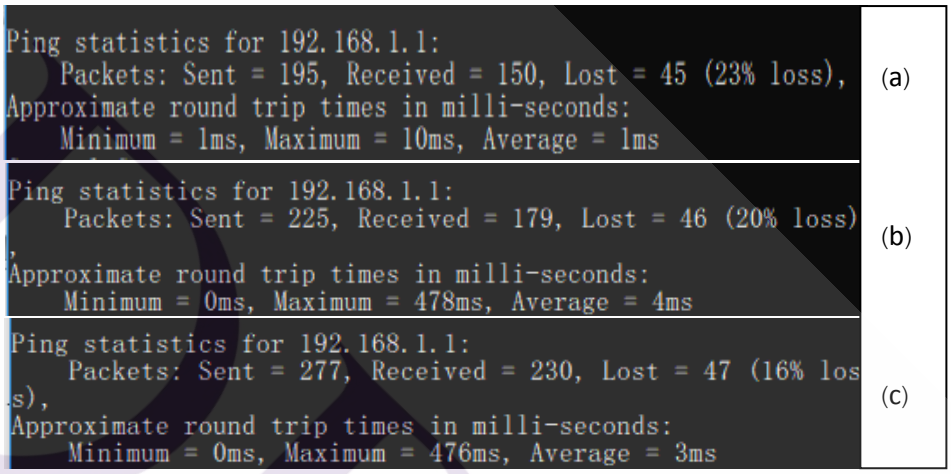
ภาพที่ 4.27 ผลการทดสอบ Indoor ระยะ 100 เมตร ครั้งที่ 1-3 (IEEE 802.11n)

จากภาพที่ 4.27 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่ห้องทั่วไป ระยะ 100 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 206, Received = 99, Lost = 107 และ 51% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 143, Received = 73, Los t= 70 และ 48% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 169, Received = 70, Lost = 99 และ 58% loss



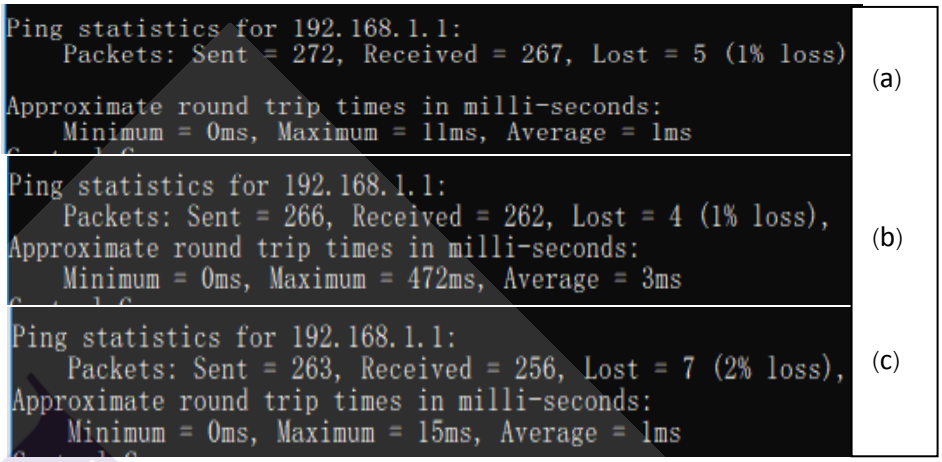
ภาพที่ 4.28 ผลการทดสอบ Indoor ระยะ 120 เมตร ครั้งที่ 1-3 (IEEE 802.11n)

จากภาพที่ 4.28 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่ห้องทั่วไป ระยะ 120 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 195, Received = 150, Lost = 45 และ 23% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 225, Received = 179, Lost = 46 และ 20% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 277, Received = 230, Lost = 47 และ 16% loss



ภาพที่ 4.29 ผลการทดสอบ Indoor ระยะ 140 เมตร ครั้งที่ 1-3 (IEEE 802.11n)

จากภาพที่ 4.29 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่ห้องทั่วไป ระยะ 140 เมตร ดังนี้

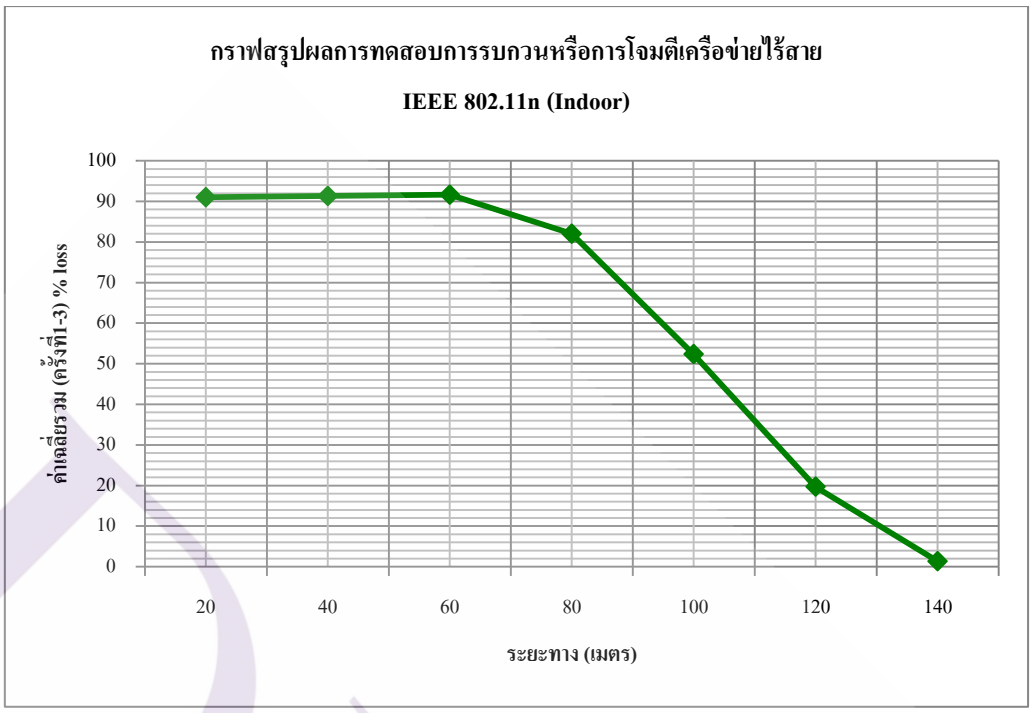
ครั้งที่ 1 (a) มีจานวน Packets: Sent = 272, Received = 267, Lost = 5 และ 1% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 266, Received = 262, Lost = 4 และ 1% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 263, Received = 256, Lost = 7 และ 2% loss

ตารางที่ 4.3 สรุปผลการทดสอบในพื้นที่ห้องทั่วไป ภายใต้มาตรฐานการทำงาน IEEE 802.11n

ระยะทาง (เมตร)	ครั้งที่ 1	ครั้งที่ 2	ครั้งที่ 3	ค่าเฉลี่ยรวม (ครั้งที่1-3)
	% loss	% loss	% loss	% loss
20	84	93	96	91
40	91	91	92	91.33
60	92	91	92	91.66
80	79	85	82	82
100	51	48	58	52.33
120	23	20	16	19.66
140	1	1	2	1.33

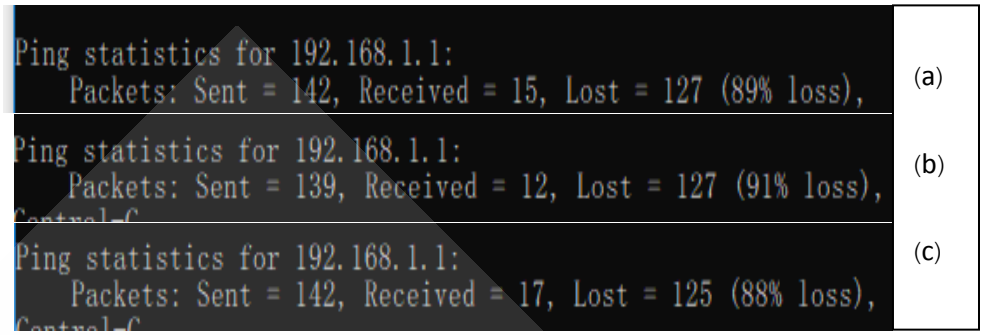


ภาพที่ 4.30 กราฟสรุปผลการทดสอบในพื้นที่ห้องทั่วไป (IEEE 802.11n)

จากตารางที่ 4.3 และรูปที่ 4.30 เป็นการแสดงผลสรุปการทดสอบในพื้นที่ห้องทั่วไป (IEEE 802.11n) ในรูปแบบของตารางและเส้นกราฟแสดงค่าเฉลี่ย % loss ในแต่ละระยะของการทดสอบ 20 40 60 80 100 120 และ 140 เมตร ตามลำดับ ซึ่งจะเห็นได้ว่า เมื่อระยะห่างในการทดสอบเพิ่มมากขึ้นจะทำให้ประสิทธิภาพในการรบกวนหรือโจมตีเครือข่ายไร้สาย โดยวิธีการ De-Authentication ลดลง และมีค่าเข้าใกล้ 0% loss ที่ระยะ 140 เมตร

4.4 ผลการทดสอบในพื้นที่ห้องทั่วไป ภายใต้มาตรฐานการทำงาน IEEE 802.11g

ในการดำเนินการทดสอบการรบกวนหรือการโจมตีเครือข่ายไร้สาย โดยวิธีการ De-Authentication ในพื้นที่ห้องทั่วไป ภายใต้มาตรฐานการทำงาน IEEE 802.11g นั้น จะดำเนินการในลักษณะเช่นเดียวกับการทดสอบ IEEE 802.11n ทุกด้าน โดยจะมีความแตกต่างกันเฉพาะการตั้งค่าอุปกรณ์กระจายสัญญาณให้เป็นโหมดการทำงาน ภายใต้มาตรฐานการทำงาน IEEE 802.11g เท่านั้น ซึ่งมีผลการทดสอบในรูปแบบของรูปภาพ ตารางและกราฟสรุปผลดังนี้



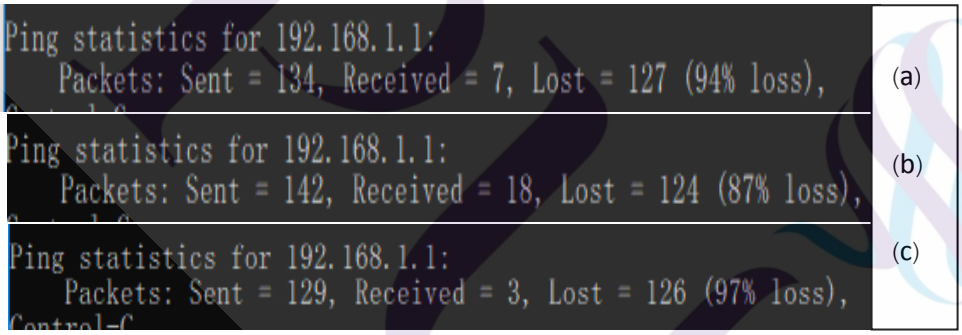
ภาพที่ 4.31 ผลการทดสอบ Indoor ระยะ 20 เมตร ครั้งที่ 1-3 (IEEE 802.11g)

จากภาพที่ 4.31 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่ห้องทั่วไป ระยะ 20 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 142, Received = 15, Lost = 127 และ 89% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 139, Received = 12, Lost = 127 และ 91% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 142, Received = 17, Lost = 125 และ 88% loss



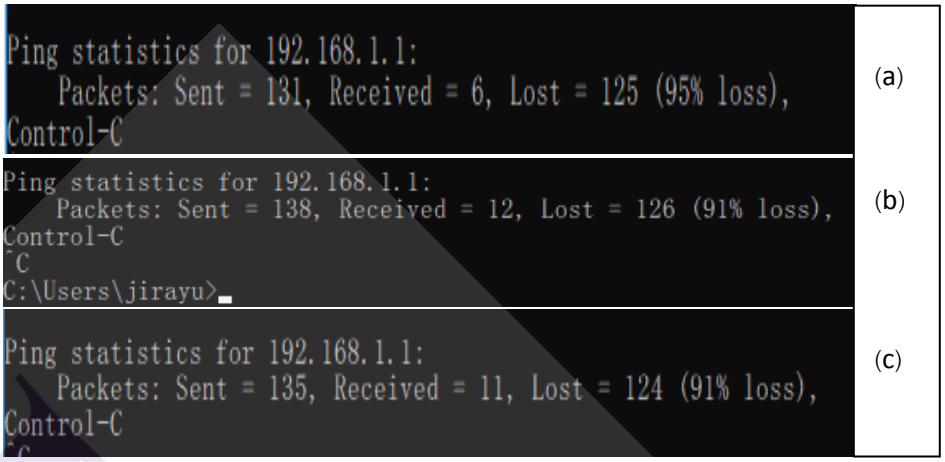
ภาพที่ 4.32 ผลการทดสอบ Indoor ระยะ 40 เมตร ครั้งที่ 1-3 (IEEE 802.11g)

จากภาพที่ 4.32 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่ห้องทั่วไป ระยะ 40 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 134, Received = 7, Lost = 127 และ 94% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 142, Received = 18, Lost = 124 และ 87% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 129, Received = 3, Lost = 126 และ 97% loss



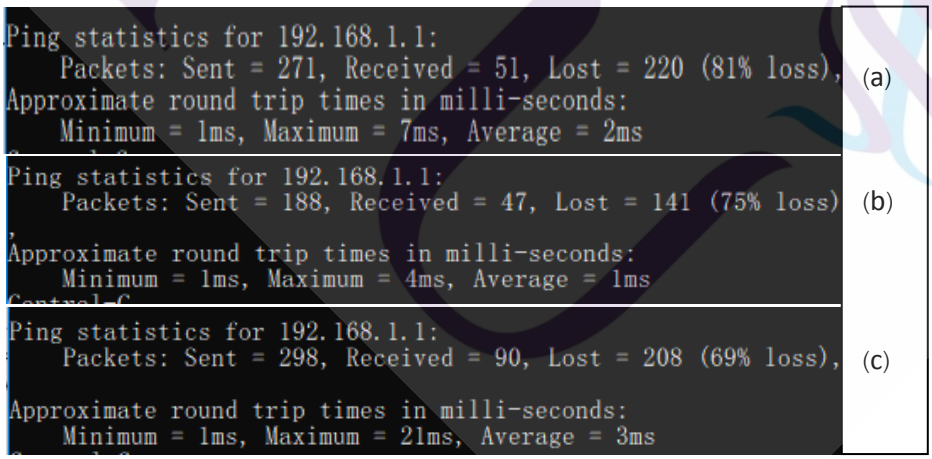
ภาพที่ 4.33 ผลการทดสอบ Indoor ระยะ 60 เมตร ครั้งที่ 1-3 (IEEE 802.11g)

จากภาพที่ 4.33 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่ห้องทั่วไป ระยะ 60 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 131, Received = 6, Lost = 125 และ 95% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 138, Received = 12, Lost = 126 และ 91% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 135, Received = 11, Lost = 124 และ 91% loss



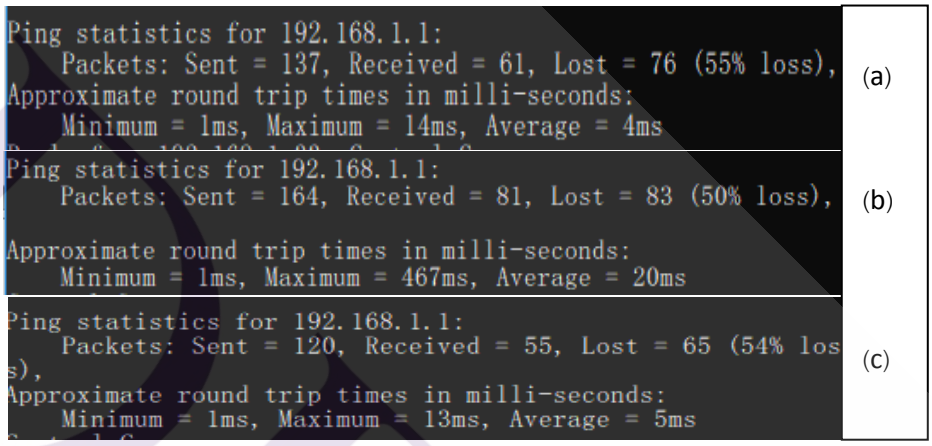
ภาพที่ 4.34 ผลการทดสอบ Indoor ระยะ 80 เมตร ครั้งที่ 1-3 (IEEE 802.11g)

จากภาพที่ 4.34 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่ห้องทั่วไป ระยะ 80 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 271, Received = 51, Lost = 220 และ 81% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 188, Received = 47, Lost = 141 และ 75% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 298, Received = 90, Lost = 208 และ 69% loss



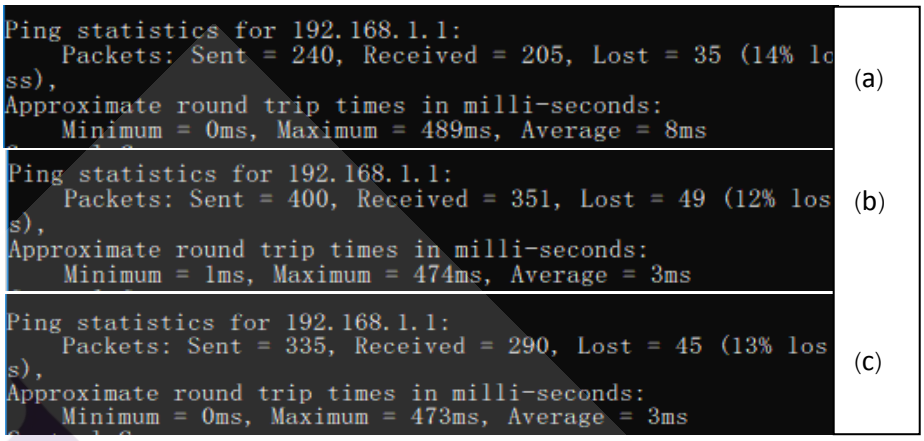
ภาพที่ 4.35 ผลการทดสอบ Indoor ระยะ 100 เมตร ครั้งที่ 1-3 (IEEE 802.11g)

จากภาพที่ 4.35 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่ห้องทั่วไป ระยะ 100 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 137, Received = 61, Lost = 76 และ 55% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 164, Received = 81, Lost = 83 และ 50% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 120, Received = 55, Lost = 65 และ 54% loss



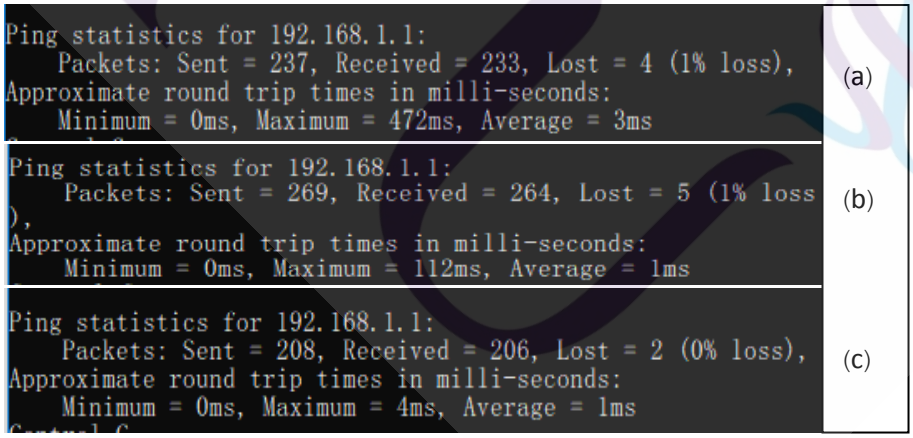
ภาพที่ 4.36 ผลการทดสอบ Indoor ระยะ 120 เมตร ครั้งที่ 1-3 (IEEE 802.11g)

จากภาพที่ 4.36 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่ห้องทั่วไป ระยะ 120 เมตร ดังนี้

ครั้งที่ 1 (a) มีจานวน Packets: Sent = 240, Received = 205, Lost = 35 และ 14% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 400, Received = 351, Lost = 49 และ 12% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 335, Received = 290, Lost = 45 และ 13% loss



ภาพที่ 4.37 ผลการทดสอบ Indoor ระยะ 140 เมตร ครั้งที่ 1-3 (IEEE 802.11g)

จากภาพที่ 4.37 จะแสดงให้เห็นถึงสถิติผลการทดสอบในพื้นที่ห้องทั่วไป ระยะ 140 เมตร ดังนี้

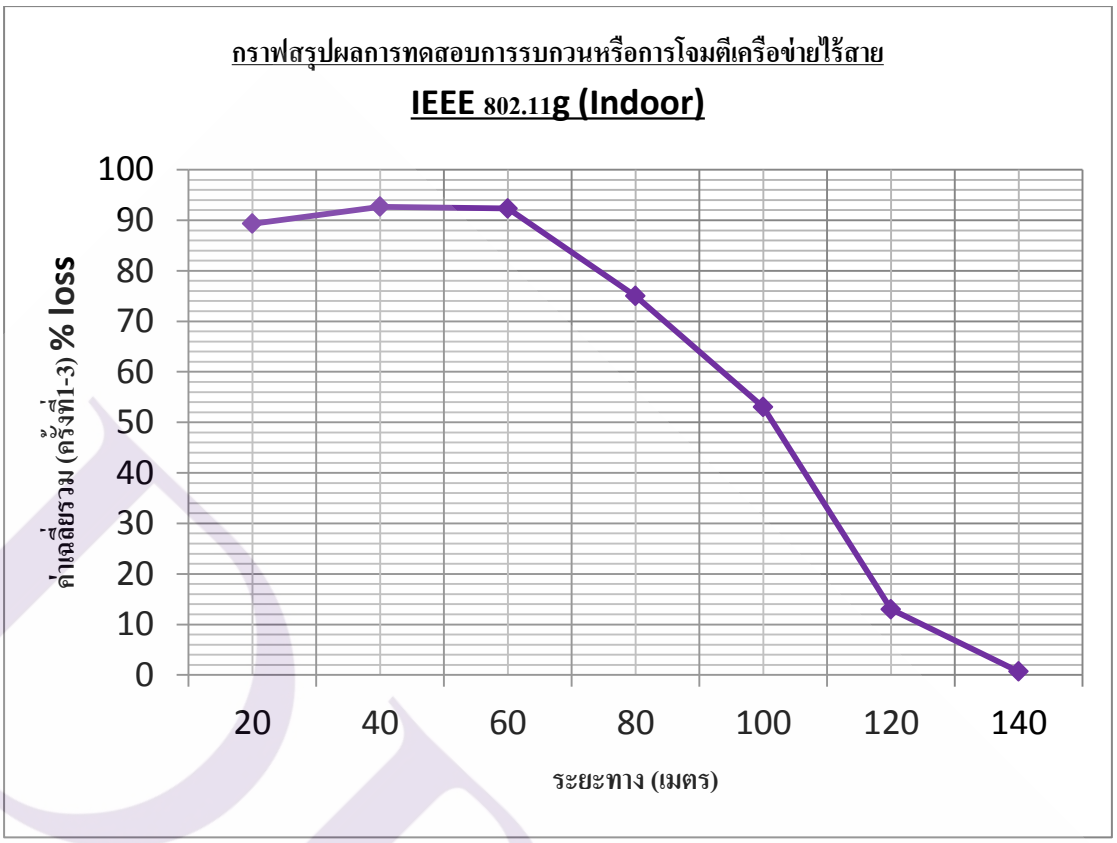
ครั้งที่ 1 (a) มีจานวน Packets: Sent = 237, Received = 233, Lost = 4 และ 1% loss

ครั้งที่ 2 (b) มีจานวน Packets: Sent = 269, Received = 264, Lost = 5 และ 1% loss

ครั้งที่ 3 (c) มีจานวน Packets: Sent = 208, Received = 206, Lost = 2 และ 0% loss

ตารางที่ 4.4 สรุปผลการทดสอบในพื้นที่ห้องทั่วไป ภายใต้มาตรฐานการทำงาน IEEE 802.11g

ระยะทาง (เมตร)	ครั้งที่ 1	ครั้งที่ 2	ครั้งที่ 3	ค่าเฉลี่ยรวม (ครั้งที่1-3)
	% loss	% loss	% loss	% loss
20	89	91	88	89.33
40	94	87	97	92.66
60	95	91	91	92.33
80	81	75	69	75
100	55	50	54	53
120	14	12	13	13
140	1	1	0	0.66



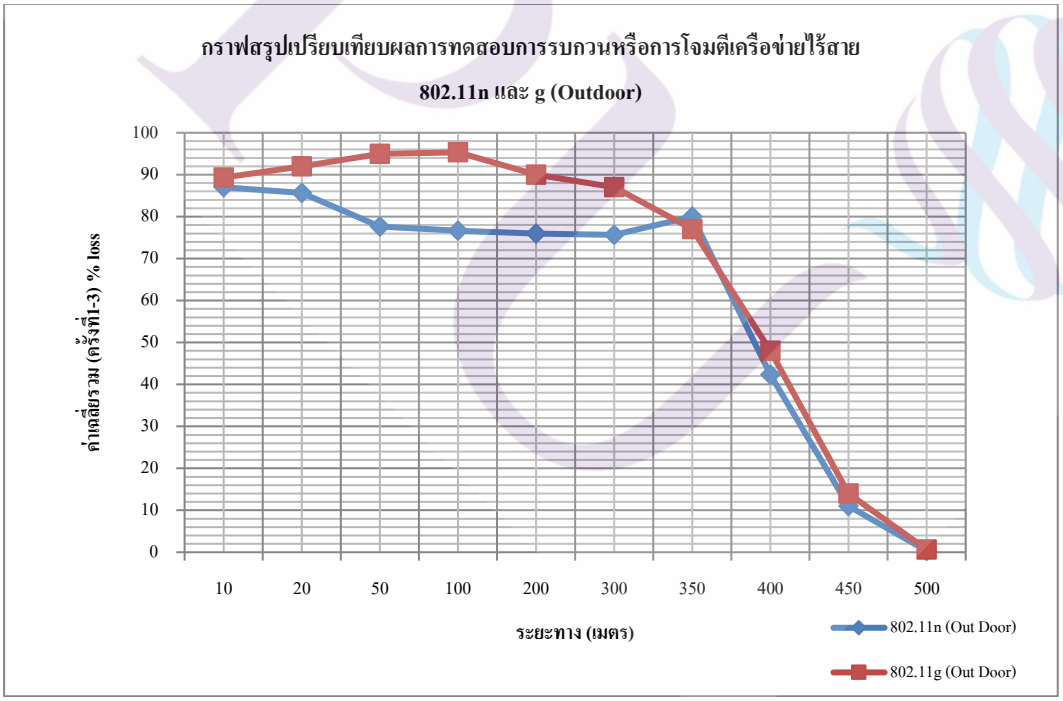
ภาพที่ 4.38 กราฟสรุปผลการทดสอบในพื้นที่ห้องทั่วไป (IEEE 802.11g)

จากตารางที่ 4.4 และรูปที่ 4.38 เป็นการแสดงผลสรุปการทดสอบในพื้นที่ห้องทั่วไป (IEEE 802.11g) ในรูปแบบของตารางและเส้นกราฟแสดงค่าเฉลี่ย % loss ในแต่ละระยะของการทดสอบ 20 40 60 80 100 120 และ 140 เมตร ตามลำดับ ซึ่งจะเห็นได้ว่า เมื่อเครื่องที่เป็น Attacker กับอุปกรณ์กระจายสัญญาณและเครื่องคอมพิวเตอร์ที่กำลังเชื่อมต่อแบบไร้สายอยู่ มีระยะห่างเพิ่มมากขึ้น จะทำให้ค่าประสิทธิภาพในการติดต่อสื่อสารหรือการเชื่อมต่อโดยรวมของระบบดีขึ้น ซึ่งตรงกันข้ามกับประสิทธิภาพในการรบกวนหรือโจมตีเครือข่ายไร้สาย โดยวิธีการ De-Authentication ลดลงและมีค่าเข้าใกล้ 0% loss ที่ระยะ 140 เมตร

บทที่ 5
บทสรุปและข้อเสนอแนะ

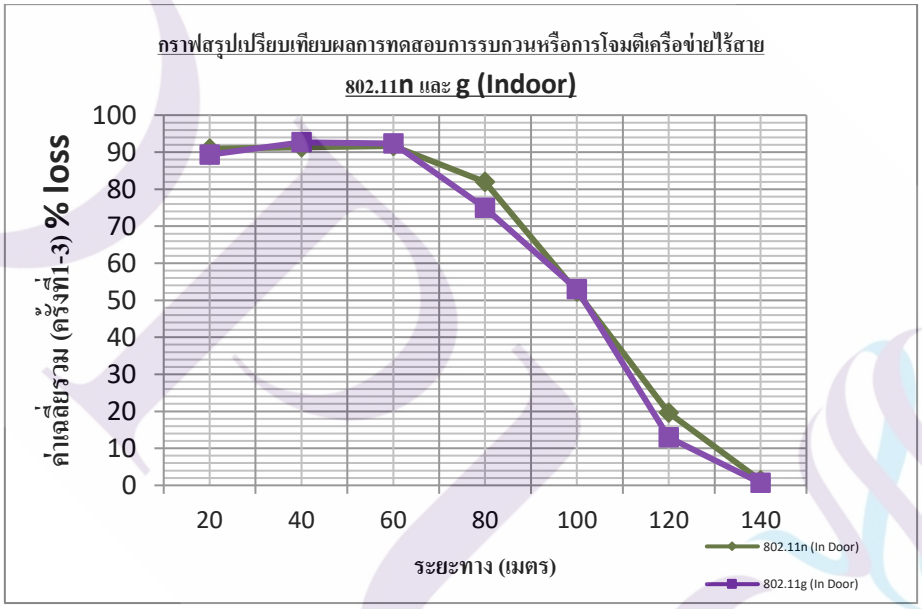
5.1 สรุปผลการวิจัย

จากการทดสอบการรบกวนหรือการโจมตีเครือข่ายไร้สาย ดังมีผลการทดสอบตามที่ได้แสดงในบทที่ 4 นั้น สรุปได้ว่าผู้วิจัยสามารถดำเนินการรบกวนหรือโจมตีเครือข่ายไร้สายของทั้ง 4 รูปแบบการทดสอบได้จริง และการทดสอบในพื้นที่โล่งแนวระดับสายตาจะสามารถรบกวนหรือการโจมตีได้ในระยะที่ไกลกว่าการทดสอบในพื้นที่ห้องทั่วไป ประมาณ 3.5 เท่า โดยประสิทธิภาพของการรบกวนหรือโจมตีจะลดลง เมื่อระยะของการทดสอบเพิ่มมากขึ้น ซึ่งจะแสดงการวิเคราะห์และสรุปผลในแต่ละรูปแบบการทดสอบพร้อมเปรียบเทียบผลการดำเนินการของทั้ง 4 รูปแบบการทดสอบ เพื่อให้ง่ายต่อการทำความเข้าใจดังนี้



ภาพที่ 5.1 กราฟสรุปเปรียบเทียบผลการทดสอบการรบกวนหรือการโจมตีเครือข่ายไร้สาย 802.11n และ g (Outdoor)

จากภาพที่ 5.1 เป็นกราฟที่แสดงสรุปเปรียบเทียบผลการทดสอบในพื้นที่โล่งแนวระดับสายตาภายใต้มาตรฐานการทำงาน IEEE 802.11n และ IEEE 802.11g สรุปได้ว่าสามารถดำเนินการรบกวนหรือโจมตีเครือข่ายไร้สายได้จริง โดยทั้งสองรูปแบบมีผลการทดสอบที่ใกล้เคียงกันและสามารถนำค่าเฉลี่ยของค่า % loss มาเปรียบเทียบได้ดังนี้ (IEEE 802.11n และ g) ที่ระยะของการทดสอบ 10-350 เมตร มีค่า = 79.80% loss และ 89.38% loss ที่ระยะ 400 เมตร = 42% loss และ 48% loss ที่ระยะ 450 เมตร = 11% loss และ 14% loss และที่ระยะ 500 เมตร = 0.33% loss และ 0.66% loss จากการเปรียบเทียบข้างต้นสามารถวิเคราะห์ได้ว่าค่าประสิทธิภาพของการรบกวนหรือโจมตีจากระยะเริ่มต้นไปถึงระยะประมาณ 350 เมตร จะได้ค่าเฉลี่ยที่ใกล้เคียงกัน และจะเริ่มลดลงอย่างเห็นได้ชัด เมื่อระยะของการทดสอบเพิ่มมากขึ้น จนมีค่าเข้าใกล้ 0% loss ที่ระยะ 500 เมตร เช่นเดียวกันทั้งสองมาตรฐาน



ภาพที่ 5.2 กราฟสรุปเปรียบเทียบผลการทดสอบการรบกวนหรือการโจมตีเครือข่ายไร้สาย 802.11n และ g (Indoor)

จากภาพที่ 5.2 เป็นกราฟที่แสดงสรุปเปรียบเทียบผลการทดสอบในพื้นที่ห้องทั่วไป ภายใต้มาตรฐานการทำงาน IEEE 802.11n และ IEEE 802.11g สรุปได้ว่าสามารถดำเนินการรบกวนหรือโจมตีเครือข่ายไร้สายได้จริงโดยทั้งสองรูปแบบมีผลการทดสอบที่ใกล้เคียงกันและสามารถนำค่าเฉลี่ยของค่า % loss มาเปรียบเทียบได้ดังนี้ (IEEE 802.11n และ g) ที่ระยะของการทดสอบ 20-80 เมตร = 88.99% loss และ 87.33% loss ที่ระยะ 100 เมตร = 52.33% loss และ 53% loss ที่ระยะ 120 เมตร = 19.66% loss และ 13% loss และที่ระยะ 140 เมตร = 1.33% loss และ 0.66% loss จากการเปรียบเทียบข้างต้นสามารถวิเคราะห์ได้ว่าค่าประสิทธิภาพของการรบกวนหรือโจมตีจากระยะเริ่มต้นไปถึงระยะประมาณ 80

เมตร จะได้ค่าเฉลี่ยที่ใกล้เคียงกัน และจะเริ่มลดลงอย่างเห็นได้ชัด เมื่อระยะของการทดสอบเพิ่มมากขึ้น จนมีค่าเข้าใกล้ 0% loss ที่ระยะ 140 เมตร เช่นเดียวกันทั้งสองมาตรฐาน

5.2 ข้อเสนอแนะ

5.2.1 เพื่อเป็นแนวทางในการตรวจจับและรับมือหากถูกรบกวนหรือการโจมตีเครือข่ายไร้สายด้วยวิธีการ De-Authentication สามารถนำเทคนิคการป้องกันความปลอดภัย เช่น IDS (Wireless Intrusion Detection System) IPS (Wireless Intrusion prevention system) Spectrum Analyzer เพื่อตรวจหา Rouge AP และการสังเกตบุคคลหรืออุปกรณ์ที่แปลกปลอม เช่นคอมพิวเตอร์หรือสายอากาศที่ไม่ทราบแหล่งที่มาอยู่ในพื้นที่หรือระยะดังที่กล่าวมาข้างต้นหรือไม่

5.2.2 เพื่อเป็นการป้องกันหรือลดโอกาสในการถูกรบกวนหรือการโจมตีเครือข่ายไร้สายด้วยวิธีการ De Authentication ผู้ดูแลระบบควรตั้งค่ากำลังส่งของอุปกรณ์กระจายสัญญาณ ให้พอเหมาะไม่แรงจนเกินไป ซึ่งจะทำให้ Attacker สามารถดักจับสัญญาณหรือโจมตีจากระยะไกลได้

5.2.3 เพื่อให้เกิดความปลอดภัย และมีความน่าเชื่อถือ (Reliability) ในการใช้งาน ควรเลือกพื้นที่ในการติดตั้งอุปกรณ์กระจายสัญญาณให้เหมาะสม เพื่อไม่ให้สัญญาณที่แพร่ออกอากาศไปยังนอกพื้นที่ที่ไม่ต้องการใช้งาน

5.2.4 เนื่องจากการโจมตีเครือข่ายไร้สายด้วยวิธีการ De Authentication ดังกล่าว เป็นการโจมตีในส่วนของเฟรมการจัดการบนมาตรฐาน 802.11g และ 802.11n ซึ่งเฟรมการจัดการนี้จะถูกส่งในรูปแบบข้อความธรรมดาที่ไม่ได้มีการเข้ารหัสและมีค่าคงที่เช่นเดิมทุกเฟรม จึงสามารถปลอมแปลงและถูกโจมตีได้ง่าย [15] ทั้งนี้ เมื่อวันที่ 30 กันยายน 2009 ได้ประกาศให้มีการใช้งานมาตรฐาน IEEE 802.11w ซึ่งสามารถป้องกันการโจมตีจากเฟรมการจัดการดังกล่าวได้ [16] โดยมีกลไกในการทำงานการตรวจจับการยกเลิกการตรวจสอบและการยกเลิกการเชื่อมโยง ด้วยการสร้างคีย์เพิ่มเติมเพื่อตรวจสอบความถูกต้องและมีการกำหนดลำดับหมายเลขในแต่ละเฟรม ซึ่งเป็นส่วนสำคัญในการเพิ่มรายละเอียดกระบวนการตรวจสอบการทำงานของระบบมากยิ่งขึ้น จึงทำให้สามารถป้องกันการโจมตีได้อย่างสมบูรณ์ ดังนั้น ในปัจจุบันจะพบว่าอุปกรณ์เครือข่ายไร้สายรุ่นใหม่ๆ เช่น 802.11ac และ 802.11.ad จะมีกลไกการทำงานของมาตรฐาน 802.11w รวมอยู่ด้วยแล้ว จึงสามารถป้องกันการโจมตีเครือข่ายไร้สายด้วยวิธีการ De Authentication หรือการโจมตีในส่วนของเฟรมการจัดการได้

บรรณานุกรม

บรรณานุกรม

ภาษาต่างประเทศ

Aireplay-ng, www.aircrack-ng.org/doku.php?id=aireplay-ng

Fakariah Hani Mohd Ali, Mohamad Yusof Darus,Norkhushaini Awang Faculty of Computer and Mathematical Sciences Universiti Teknologi MARA 40450 Shah Alam Selangor MALAYSIA Wireless Intruder Detection System (WIDS) in Detecting De-Authentication and Disassociation Attacks in IEEE 802.11

Genetic Programming Based WiFi Data Link Layer Attack Detection Patrick LaRoche, A. Nur Zincir-Heywood Faculty of Computer Science Dalhousie University Halifax, Nova Scotia B3H 1W5, Canada

IEEE-SA Standards Board. ANSI/IEEE Std 802.11, 1999 Edition (R2003). IEEE, New York, NY, USA, 1999.

K. Pawade “Advanced Security Measures in a Wireless LAN “International Journal of Emerging Research in Management &Technology, pp 18-24, 2013, ISSN: 2278-9359

Mac Layer Management frame Denial of Service Attacks Jaspreet Kaur Department of Information Technology Indira Gandhi Delhi Technical University for Women, Delhi, India 2016 International Conference on Micro-Electronics and Telecommunication Engineering

S. A. Nwabude .Wireless Local Area Network (WLAN):Security Risk Assessment and Countermeasures. Master's degree of Science in Electrical Engineering. Blekinge Institute of Technology ,2008.

T.D. Nguyen, H.M. Nguyen, B.N. Tran, V. Hai & M. Mittal, “A Lightweight Solution For Defending Against De-Authentication/Disassociation Attacks On 802.11 Networks”. In Proceeding 17th International Conference On Computer Communications And Networks (ICCCN ’08), pp. 1-6. Virgin Islands August 3 - 7, 2008

Weakness in 802.11w and an improved mechanism on protection of management frame Weijia Wang,Haihang Wang Department of Computer Science and Technology Tongji University,Shanghai 2018.

ภาษาต่างประเทศ (ต่อ)

Wireless Intruder Detection System (WIDS) in Detecting De-Authentication and Disassociation Attacks in IEEE 802.11Norzaidi Baharudin Faculty of Computer and athematical Sciences Universiti Teknologi MARA 40450 Shah Alam Selangor MALAYSIA

ภาษาไทย

ชนัญญา สุวรรณศร และ นวพร วิสิฐพงศ์พันธ์ การวิเคราะห์หาจุดอ่อนและช่องโหว่ของเครือข่ายไร้สายมาตรฐาน 802.11n ภาควิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ NCCIT2010-186

ดร.ศุภกร กังพิศการ, วิทยาการเข้ารหัสลับเพื่อความมั่นคงปลอดภัยของเครือข่าย

มหาวิทยาลัยศรีนครินวิโรฒ. มาตรฐาน IEEE 802.11 .เว็บไซต์ : http://wise.swu.ac.th/.ปีที่ : 2001 แหล่งที่มา : http://wise.swu.ac.th/Default.aspx?tabid=3440 , เข้าถึงเมื่อ 10 ตุลาคม 2561.

วิชาญ แปลกโฉมฉิน การศึกษาการโจมตีเครือข่ายท้องถิ่นไร้สาย สารนิพนธ์วิทยาศาสตร์มหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ บัณฑิตวิทยาลัยมหาวิทยาลัยเทคโนโลยีมหานคร ปีการศึกษา 2553

เอกชัย ดวงแก้ว. การตรวจสอบหาจุดอ่อนและช่องโหว่เครือข่ายไร้สายมาตรฐาน 802.11 b/g. สารนิพนธ์วิทยาศาสตร์มหาบัณฑิต.มหาวิทยาลัยเทคโนโลยีมหานคร, 2550

อำนาจ มีมงคล, ออกแบบและติดตั้ง Wireless LAN (2553)

ประวัติผู้เขียน

ชื่อ-นามสกุล	ร้อยโท อภิสิทธิ์ พลท่ากลาง
ประวัติการศึกษา	พ.ศ. 2547 ประกาศนียบัตรวิชาชีพ สาขาวิชาช่างอิเล็กทรอนิกส์ โรงเรียนช่างฝีมือทหาร พ.ศ. 2552 อุตสาหกรรมศาสตร์บัณฑิต สาขาวิชาเทคโนโลยีโทรคมนาคม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้า พระนครเหนือ
ตำแหน่งและสถานที่ทำงานปัจจุบัน	นายทหารสื่อสาร แผนกอำนวยการระบบควบคุมบังคับบัญชา กองการสื่อสาร สำนักแผนและอำนวยการสื่อสาร กรมการสื่อสารทหาร กองบัญชาการกองทัพไทย