

การตรวจจับจุดเชื่อมต่อปลอมบนเครือข่ายไร้สายโดยใช้การวิเคราะห์ค่า

RTT ร่วมกับอัลกอริทึม K-means

Rogue Access Point Detection on Wireless Networks Using RTT Analysis and K-means Algorithm

ภูธเนศ เมฆพยอม

บัณฑิตศึกษา สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์และเทคโนโลยี มหาวิทยาลัยเทคโนโลยีมหานคร

E-mail: phuthanet@mut.ac.th

และ ญัฐพงษ์ จันทร์แดง

สาขาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์และเทคโนโลยี มหาวิทยาลัยเทคโนโลยีมหานคร

E-mail: jnattapo@mut.ac.th

Manuscript Received January 31, 2026

Revised March 12, 2026

Accepted April 8, 2026

บทคัดย่อ

ในปัจจุบัน ท่ามกลางการเติบโตอย่างก้าวกระโดดของเทคโนโลยีเครือข่ายไร้สาย (WLAN) ที่อำนวยความสะดวกในชีวิตประจำวัน ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์กลับทวีความรุนแรงขึ้นเป็นเงาตามตัว โดยเฉพาะภัยคุกคามจากการสร้างจุดเชื่อมต่อปลอม หรือ แม่ข่ายปลอม (Rogue Access Point - RAP) บนมาตรฐาน IEEE 802.11 ช่องโหว่นี้เปิดโอกาสให้ผู้โจมตี (Attacker) สามารถดำเนินการโจมตีแบบ (Man in the Middle - MitM) เพื่อดักจับและโจรกรรมข้อมูลสำคัญของใช้งาน งานวิจัยฉบับนี้จึงมุ่งเน้นการศึกษาผลกระทบของการโจมตีดังกล่าวอย่างเป็นระบบ ผ่านกระบวนการทดสอบ และวิเคราะห์ข้อมูลทางสถิติ โดยนำอัลกอริทึม K-means มาประยุกต์ใช้ในการจำแนกความแตกต่างระหว่างจุดเชื่อมต่อจริงและจุดเชื่อมต่อที่เป็นภัยได้ถึง 99.7% ด้วยข้อมูลการทดสอบจากสภาพแวดล้อมจริง พร้อมทั้งนำเสนอแนวทางปฏิบัติเพื่อยกระดับมาตรการรักษาความปลอดภัยเครือข่าย ทั้งในระดับผู้ใช้งานทั่วไปและระดับองค์กรให้มีประสิทธิภาพยิ่งขึ้น

คำสำคัญ: สถานีแม่ข่ายปลอม, ภัยคุกคาม, แม่ข่ายปลอม, การโจมตีแบบคนกลาง, เครือข่ายท้องถิ่นไร้สาย, เครือข่ายไร้สาย

ABSTRACT

While the rapid expansion of WLAN technology facilitates daily life, it has simultaneously increased cybersecurity risks, particularly from Rogue Access Points (RAP) using the IEEE 802.11 standard. This vulnerability exposes users to Man-in-the-Middle (MitM) attacks and data theft. This research investigates these threats using experimental and statistical methods. Utilizing the K-means algorithm on real-world data, the proposed model identifies malicious access points with 99.7% accuracy. Finally, the study offers actionable guidelines to strengthen network security for both individuals and organizations.

Keywords: Rogue Access Points, Man in the Middle, WLAN, WIFI

1. บทนำ

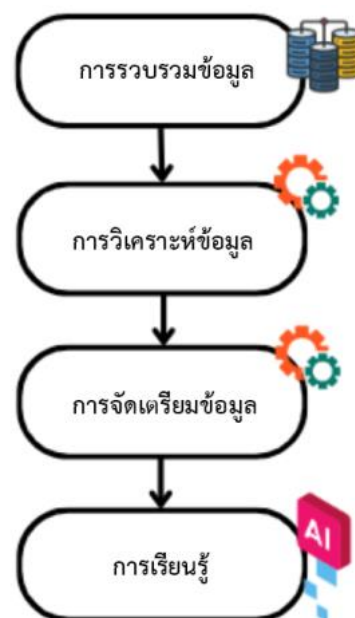
ในยุคเทคโนโลยีเครือข่ายไร้สาย (Wireless LAN) ตามมาตรฐาน IEEE 802.11 ได้กลายเป็นโครงสร้างพื้นฐานที่สำคัญอย่างยิ่งสำหรับการติดต่อสื่อสารและการเข้าถึงอินเทอร์เน็ต ทั้งในภาคธุรกิจและภาคครัวเรือน เนื่องจากความสามารถในการอำนวยความสะดวกและความยืดหยุ่นในการใช้งาน อย่างไรก็ตาม ความนิยมที่แพร่หลายนี้ได้นำมาซึ่งความเสี่ยงด้านความปลอดภัยทางไซเบอร์ที่ทวีความรุนแรงขึ้น รายงานจากหน่วยงานระดับชาติ เช่น FBI, CISA และ DoD ได้แจ้งเตือนถึงภัยคุกคามต่อโครงสร้างพื้นฐานทางเครือข่ายอย่างต่อเนื่อง โดยเฉพาะการใช้งานในพื้นที่สาธารณะที่มักขาดมาตรการป้องกันที่รัดกุม [1], [2] โดยเฉพาะอย่างยิ่งในการให้บริการ Wi-Fi ฟรี ซึ่งมักขาดมาตรการป้องกันที่เพียงพอ [3], [4], [5]

แม้ว่าจะมีความพยายามในการยกระดับมาตรฐานความปลอดภัยด้วยการใช้โปรโตคอลการเข้ารหัสที่ทันสมัย เช่น WPA2 และ WPA3 แต่ระบบเหล่านี้ยังคงถูกค้นพบช่องโหว่ที่สำคัญอย่างต่อเนื่อง อาทิ การโจมตีแบบ การโจมตีการติดตั้งคีย์ใหม่ (Key Reinstallation Attacks - KRACK) ที่สามารถบังคับให้เกิดการใช้รหัสซ้ำใน WPA2 [6] ช่องโหว่ Dragonblood ที่พบในกระบวนการ SAE Handshake ของ WPA3 [7] รวมถึงความเปราะบางต่อการโจมตีแบบ Brute Force ผ่านพีแอร์ WPS [8] ช่องโหว่เหล่านี้เป็นช่องทางให้ผู้โจมตี (Attacker) สามารถเจาะระบบเพื่อดักฟังหรือแทรกแซงการสื่อสารได้ หนึ่งในภัยคุกคามที่ฉวยโอกาสจากช่องโหว่เหล่านี้ได้รุนแรงที่สุดคือ จุดเชื่อมต่อปลอม ในรูปแบบการโจมตีแฝดชั่วร้าย (Evil Twin Attack) [9], [10] ซึ่งผู้โจมตีจะสร้างจุดเชื่อมต่อที่ปลอมแปลงชื่อเครือข่าย SSID ให้เหมือนกับของจริง [11] กลไกสำคัญที่ช่วยให้การโจมตีนี้ประสบความสำเร็จคือการใช้เทคนิค การโจมตีแบบถอดถอนการตรวจสอบสิทธิ์ (Deauthentication Attack) เพื่อส่งชุดคำสั่งตัดการเชื่อมต่อไปยังอุปกรณ์ของเหยื่อ บังคับให้หลุดจากเครือข่ายหลักและพยายามเชื่อมต่อใหม่ ซึ่งจากการสำรวจพบว่าเครือข่าย Wi-Fi จำนวนมากยังขาดมาตรการป้องกันการโจมตีรูปแบบนี้ [12] เมื่อเหยื่อเชื่อมต่อโดยรู้เท่าไม่ถึงการณ์เชื่อมต่อกับสถานีปลอม จะเปิดโอกาสให้ผู้โจมตีสามารถดำเนินการแบบคนกลาง (Man in the Middle - MitM) เพื่อดักจับข้อมูลสำคัญหรือติดตั้งมัลแวร์ได้ทันที [13], [3], [14] งานวิจัยในอดีตได้พยายามนำเสนอวิธีการตรวจจับโดยใช้คุณลักษณะทางกายภาพและสถิติของเครือข่าย เช่น การวิเคราะห์เวลาในการ

เดินทางของแพ็กเก็ต (Round Trip Time - RTT) และความแรงของสัญญาณ RSSI [15], [16] นอกจากนี้ ในปัจจุบันยังมีการนำเทคนิคการเรียนรู้ของเครื่อง Machine Learning มาประยุกต์ใช้เพื่อเพิ่มความแม่นยำ [17] อย่างไรก็ตาม ประสิทธิภาพของอัลกอริทึมเหล่านี้ขึ้นอยู่กับคุณภาพของข้อมูลเป็นสำคัญ บทความนี้จึงให้ความสำคัญกับขั้นตอนการเตรียมข้อมูล (Data Preprocessing) และการทำความสะอาดข้อมูล (Data Cleaning) โดยอาศัยหลักการวิเคราะห์ข้อมูล (Exploratory Data Analysis - EDA) เพื่อกำจัดข้อมูลขยะและค่าผิดปกติ Outliers ตามหลักการทางสถิติ [18], [19] ก่อนนำไปประมวลผล

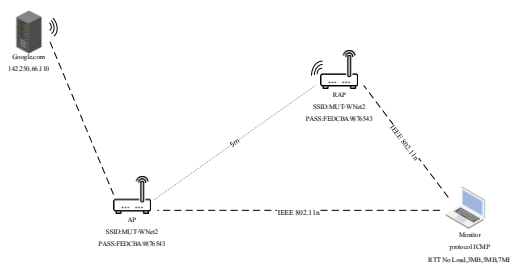
ดังนั้น บทความนี้จึงมีวัตถุประสงค์เพื่อวิเคราะห์ผลกระทบของภัยคุกคามจาก แม้อย่างปลอมบนเครือข่ายไร้สายอย่างเป็นระบบ โดยมุ่งเน้นการประยุกต์ใช้ อัลกอริทึม K-means Clustering ซึ่งเป็นเทคนิคการเรียนรู้แบบไม่มีผู้สอน Unsupervised Learning มาใช้ร่วมกับข้อมูลที่ผ่านการคัดกรองแล้ว เพื่อจำแนกกลุ่มของสถานีแม้อย่างผิดปกติออกจากสถานีที่เป็นภัยคุกคาม ผลลัพธ์จากการศึกษานี้จะนำไปสู่การเสนอแนวทางปฏิบัติในการเพิ่มความปลอดภัยสำหรับเครือข่ายระดับบุคคลและองค์กร

2. การออกแบบข้อมูล



รูปที่ 1 Flowchart ขั้นตอนการวิจัย

รูปที่ 1 กระบวนการทั้งหมดถูกออกแบบให้ทำงานตามลำดับ เพื่อให้ได้ผลการตรวจจับที่มีความถูกต้องและสามารถประเมินผลได้ด้วยตัวชี้วัดมาตรฐานทางสถิติ เช่น Accuracy และ F1 Score เพื่อลดความเสี่ยงจากการโจรกรรมข้อมูลและการเข้าถึงโดยไม่ได้รับอนุญาต [5] การใช้ Round Trip Time ในการตรวจจับโดยตรง จะช่วยยืนยันว่า Round Trip Time เป็นค่าที่เหมาะสมในการวัด โดยทำการจำลองสภาพแวดล้อมขึ้นมา เพื่อใช้ในการทดสอบ โดยจะมี Access Point ที่เป็นแม่ข่ายจริง มีการใช้งานปกติและ ทำการจำลอง แม่ข่ายปลอมขึ้นมาภายในระบบ โดย กำหนด SSID Password และ ช่องสัญญาณ ให้เหมือนกับ Access Point ตัวจริง ในการทดสอบได้ใช้สถานที่ ณ มหาวิทยาลัยเทคโนโลยีมหานคร อาคาร MIIX ห้อง MIIX301 และ ห้อง MIIX401 ในการทดสอบทั้ง 2 แบบ

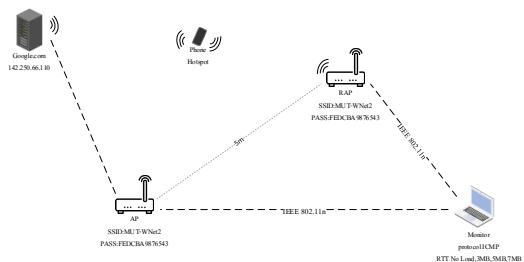


รูปที่ 2 แบบการจำลองระบบเครือข่ายแบบที่ 1

จากรูปที่ 2 การทดสอบดำเนินการโดยการวัดและบันทึกค่าเวลาในการเดินทางของแพ็กเก็ต Round Trip Time ระหว่างจุดเชื่อมต่อ Access Point และเซิร์ฟเวอร์ปลายทาง Google.com บนเครือข่ายย่านความถี่ 2.4 GHz โดยกำหนด (ซึ่งใช้อุปกรณ์ LINKSYS WAP300N) แม่ข่ายปลอมในระยะทาง 5 เมตร เงื่อนไขของปริมาณข้อมูลจราจร Traffic Load [11] ออกเป็น 4 ระดับ ได้แก่ สภาวะปกติ No Load, 3 MB, 5 MB และ 7 MB ตามแนวทางของ [4] ซึ่งในแต่ละระดับปริมาณการจราจรข้อมูลจะทำการเก็บตัวอย่างข้อมูลซ้ำ จำนวน 200 ครั้ง และ 500 ครั้ง เพื่อให้ได้ค่า Round Trip Time ที่นำไปวิเคราะห์ผลได้

จากรูปที่ 3 การทดสอบดำเนินการโดยการวัดและบันทึกค่าเวลาในการเดินทางของแพ็กเก็ต Round Trip Time ระหว่างจุดเชื่อมต่อไร้สาย Access Point และเซิร์ฟเวอร์ปลายทาง Google.com

เช่นกัน โดยกำหนดให้ใช้อุปกรณ์สมาร์ทโฟนทำหน้าที่เป็นเกตเวย์เชื่อมต่ออินเทอร์เน็ต (Mobile Hotspot Gateway) เพื่อทดสอบสมรรถนะบนเครือข่ายย่านความถี่ 2.4 GHz ภายใต้สถานการณ์ที่มีจุดเชื่อมต่อปลอมแปลง แม่ข่ายปลอม (LINKSYS WAP300N) ถูกติดตั้งในระยะทาง 5 เมตร การทดสอบกำหนดเงื่อนไขปริมาณการจราจรข้อมูล (Traffic Load) ออกเป็น 4 ระดับ ได้แก่ สภาวะปกติ No Load, 3 MB, 5 MB และ 7 MB ตามแนวทางของงานวิจัยอ้างอิง [6] ซึ่งในแต่ละระดับปริมาณการจราจรข้อมูล จะทำการเก็บตัวอย่างข้อมูลซ้ำจำนวน 200 และ 500 ครั้ง เพื่อนำค่า Round Trip Time ที่ได้ไปวิเคราะห์ผลทางสถิติ โดยการทดสอบจะเป็นระบบปิด แบบไม่มีอุปกรณ์ และ แบบมีอุปกรณ์ 14 ตัว ได้แก่ โทรศัพท์เคลื่อนที่ 5 เครื่อง สมาร์ททีวี 1 เครื่อง กล้องวงจรปิด 3 อุปกรณ์ อุปกรณ์ IOT 4 อุปกรณ์ และ NAS เพิ่มให้เห็นผลที่ชัดเจนยิ่งขึ้น จึงทำการทดสอบกับสถานที่จริง ที่ไม่สามารถควบคุมอุปกรณ์



รูปที่ 3 แบบการจำลองระบบเครือข่ายแบบที่ 2

การศึกษานี้ได้กำหนดรูปแบบจำลองระบบเครือข่ายเพื่อเก็บรวบรวมข้อมูลค่าเวลาในการเดินทางของแพ็กเก็ต Round Trip Time ออกเป็น 2 กรณีศึกษา เพื่อเปรียบเทียบพฤติกรรมของค่า Round Trip Time ภายใต้สภาพแวดล้อมที่แตกต่างกัน รวมถึงสถานที่จริง การทดสอบทั้งสองรูปแบบดำเนินการบนเครือข่ายไร้สายย่าน 2.4 GHz โดยมีการจำลองการโจมตีแบบแม่ข่ายปลอม และกำหนดเงื่อนไขปริมาณการจราจรข้อมูล (Traffic Load) 4 ระดับ คือ No Load, 3 MB, 5 MB และ 7 MB [6] โดยในแต่ละเงื่อนไขจะทำการบันทึกค่า Round Trip Time จำนวน 200 และ 500 ตัวอย่าง เพื่อนำไปวิเคราะห์ K-means Clustering โดยใช้ Algorithm 1 ในการเก็บข้อมูล

Algorithm 1 Record Data

```

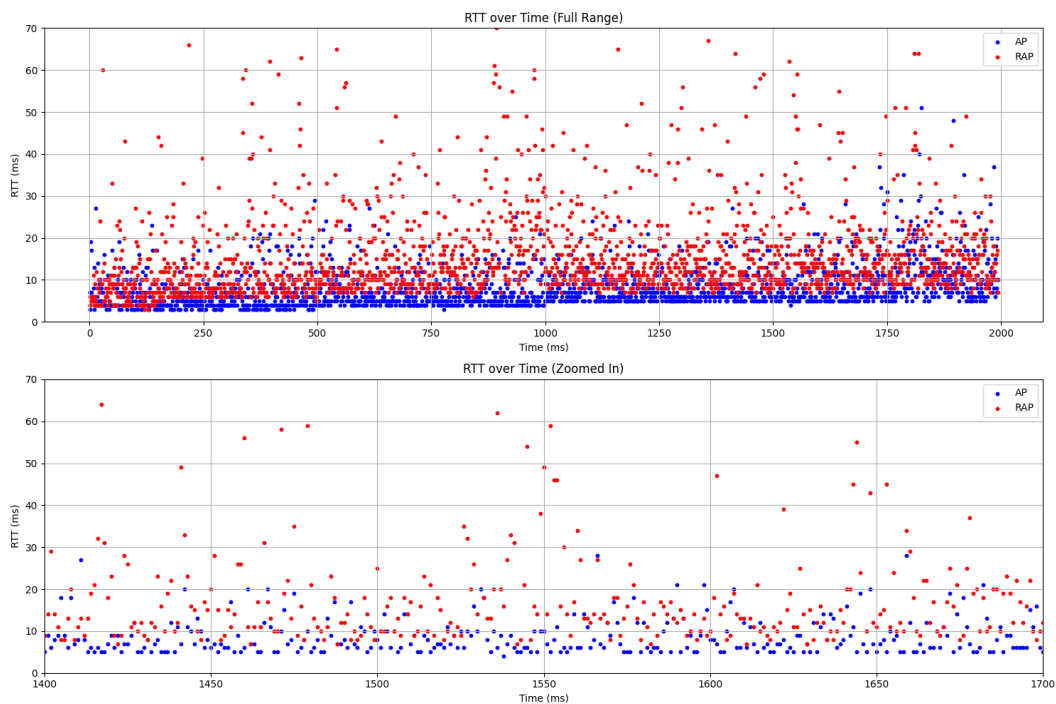
1: Target  $T = \text{"Ping.pe"}$ , Count  $N = 500$ 
2: Loads  $L = \{(\text{"NoLoad"}, 0), (\text{"3MB"}, 3072), (\text{"5MB"}, 5120), (\text{"7MB"}, 7168)\}$ 
3: Initialize Queue  $Q$ , CSV File  $F$ 
4: For each  $(\text{label}, \text{size}) \in L$ :
5:   Repeat  $N$  times: Enqueue( $(\text{label}, \text{size})$ ,  $Q$ )
6: While  $Q$  is not empty:
7:    $(\text{label}, \text{size}) = \text{Dequeue}(Q)$ 
8:   If  $\text{size} > 0$ :
9:      $\text{Cmd} = \text{"ping-l" + size + "-n1"} + T$ 
10:   Else:
11:      $\text{Cmd} = \text{"ping -n 1"} + T$ 
12:    $\text{Response} = \text{Execute}(\text{Cmd})$ 
13:   If  $\text{Response}$  matches Pattern:
14:      $(IP, \text{Bytes}, \text{Time}, \text{TTL}) = \text{Extract}(\text{Response})$ 
15:     Write  $(\text{label}, IP, \text{Bytes}, \text{Time}, \text{TTL})$  to  $F$ 

```

ในการศึกษานี้ ผู้วิจัยได้มุ่งเน้นการพัฒนาเครื่องมือในรูปแบบ Automated Script เพื่อเพิ่มประสิทธิภาพในการเก็บรวบรวมข้อมูล โดยมีเป้าหมายหลักคือการวัดและบันทึกค่าเวลาในการเดินทางไป-

กลับของข้อมูล (Round Trip Time - RTT) ซึ่งเป็นดัชนีชี้วัดความเร็วและความหน่วงของระบบเครือข่าย กระบวนการทำงานของสคริปต์นี้อาศัยกลไกของ (Internet Control Message Protocol - ICMP) ผ่านการเรียกใช้คำสั่ง Ping บนระบบปฏิบัติการไปยังเป้าหมายปลายทางที่กำหนดไว้ คือ Google.com เพื่อให้การวิเคราะห์ผลการทดลองครอบคลุมในทุกมิติ ผู้วิจัยจึงได้กำหนดตัวแปรสำหรับการทดสอบแบ่งออกเป็น 2 ส่วนหลัก ได้แก่ ตัวแปรด้านขนาดของแพ็กเก็ต L ซึ่งครอบคลุมตั้งแต่ระดับ No Load (ขนาดเริ่มต้น) ไปจนถึงการจำลองภาระงานขนาดใหญ่ที่ 3 MB, 5 MB และ 7 MB และตัวแปรด้านจำนวนครั้งในการบันทึกข้อมูล (counts) ซึ่งกำหนดไว้ที่ 200 และ 500 ครั้ง ต่อหนึ่งขนาดข้อมูล การจำลองสถานการณ์ด้วยความหลากหลายของตัวแปรเหล่านี้ จะช่วยให้ผลลัพธ์ที่ได้จากการ Ping สะท้อนถึงประสิทธิภาพที่แท้จริงของเครือข่ายภายใต้สภาวะต่าง ๆ ได้อย่างสมบูรณ์

3. การจัดการข้อมูล



รูปที่ 4 กราฟสัญญาณ Round Trip Time ข้อมูล AP และ RAP

รูปที่ 4 กราฟดังกล่าวแสดงการเปรียบเทียบลักษณะการเปลี่ยนแปลงของสัญญาณ AP และ RAP โดยใช้สีแดงและสีน้ำเงินเป็นตัวแทนตามลำดับ ซึ่งข้อมูลที่นำมาแสดงได้ผ่านการจัดเรียงตามลำดับเวลาแล้ว ผลที่ได้ช่วยให้เห็นแนวโน้มการกระจายตัวของค่า Round Trip Time ในแต่ละช่วงเวลา โดยในรูปที่ 4 ช่วงที่ 2 ด้านล่าง ได้มีการปรับมุมมองของกราฟเพื่อนำรายละเอียดของช่วงเวลาที่มีสัญญาณมีความผันผวนสูง ทั้งนี้แกน X ใช้ Round Trip Time ส่วนแกน Y แสดงระดับของค่า Round Trip Time ที่เปลี่ยนแปลงไปตามช่วงเวลา เพื่อให้เห็นภาพรวมความสามารถของอัลกอริทึม K-means ในการแยกแยะระหว่างสถานีแม่ข่ายปกติ (Normal AP) และสถานีแม่ข่ายปลอม (Rogue Access Point) การศึกษาได้นำผลลัพธ์การจัดกลุ่มมาตรวจสอบความถูกต้องเทียบกับข้อมูลจริง (Ground Truth) โดยใช้เครื่องมือวัดผลทางสถิติ การวิเคราะห์ความผิดพลาดด้วย ตารางแสดงผลการจำแนกข้อมูล (Confusion Matrix) จากการวิเคราะห์ผลการจำแนกข้อมูลด้วย (Confusion Matrix Heatmap) และ ผลการวัดประสิทธิภาพด้วย ดัชนีชี้วัด (Performance Metrics) เพื่อให้การประเมินผลมีความชัดเจนในเชิงปริมาณ การศึกษานี้ได้คำนวณค่าดัชนีชี้วัดประสิทธิภาพ 4 ด้าน ได้แก่ Accuracy, Precision, Recall และ F1-Score การใช้อัลกอริทึม K-means ร่วมกับการพิจารณาค่า Round Trip Time สามารถตรวจจับ แม่ข่ายปลอมได้อย่างมีประสิทธิภาพโดยเฉพาะอย่างยิ่งเมื่อพิจารณา F1-Score และ Accuracy ที่เพิ่มขึ้นตามปริมาณการจราจรข้อมูลของปริมาณการจราจรของข้อมูล (Traffic Load) ซึ่งสอดคล้องกับพฤติกรรมของการโจมตีแบบคนกลาง (Man in the Middle) ที่จะเกิดความล่าช้าสะสมเมื่อต้องประมวลผลข้อมูลจำนวนมาก

No.	Size	IP Address	Bytes	Time (ms)	TTL
10	No Load	104.26.9.179	32	18	56
11	No Load	104.26.9.179	32	36	56
511	3MB	104.26.9.179	3072	6	56
512	3MB	104.26.9.179	3072	6	56
1012	5MB	104.26.9.179	5120	7	56
1013	5MB	104.26.9.179	5120	7	56
1511	7MB	104.26.9.179	7168	28	56
1512	7MB	104.26.9.179	7168	11	56

รูปที่ 5 ตัวอย่างข้อมูลจาก Algorithm 1

รูปที่ 5 เนื่องจากข้อมูลค่าความหน่วงเวลา Round Trip Time ที่รวบรวมได้จากสภาพแวดล้อมเครือข่ายจริงมีความผันผวนของสัญญาณ Signal Fluctuation และความแปรปรวนสูง High Variance ซึ่งอาจเกิดจากความหนาแน่นของการจราจรข้อมูลหรือสัญญาณรบกวนชั่วคราว ส่งผลให้ชุดข้อมูลดิบปรากฏค่าที่สูงกว่าปกติ Extreme Values หรือค่าผิดปกติ Outliers การวิเคราะห์ข้อมูล (Exploratory Data Analysis - EDA) ทำการตรวจสอบการกระจายตัวของข้อมูล (Data Distribution) ในแต่ละขนาดแฟ้มเกิดเพื่อระบุลักษณะความเบ้ (Skewness) และพฤติกรรมของกลุ่มข้อมูล การกำจัดค่าผิดปกติด้วยวิธี (Interquartile Range - IQR) ทางสถิติ (Interquartile Range) เพื่อคัดกรองข้อมูลที่เป็น ค่าผิดปกติ (Outliers) ออกจากชุดข้อมูล โดยกำหนดขอบเขตอยู่ช่วงที่ยอมรับได้ (Acceptable Range) หากอยู่ในช่วงข้อมูลที่อยู่นอกเหนือช่วงดังกล่าวถือเป็นสัญญาณรบกวนและถูกตัดออกจากการคำนวณค่าเฉลี่ย เพื่อให้ได้ตัวแทนข้อมูลที่มีประสิทธิภาพสูงสุด

จึงได้พัฒนา Algorithm 2 ขึ้นมาเพื่อเป็นตัวช่วยในการจำแนก ระหว่าง Access Point กับ แม่ข่ายปลอมโดยใช้ค่าน้อยเป็น $\min(\gamma)$ และค่ามากเป็น $\max(\gamma)$ กำหนด ซึ่งสะท้อนอัตราส่วนหน่วงสูงต่อหน่วงต่ำของโหนดนั้น ๆ เกณฑ์ตัดสิน θ ถูกเรียนรู้ล่วงหน้าจากข้อมูล AP ที่เชื่อถือได้แบบรวมหลายอุปกรณ์ แยกตามโหนด เพื่อให้ค่ามาตรฐานไม่ยึดติด AP ใดตัวเดียว เมื่อประเมินค่าจริงของโหนด i ให้เปรียบเทียบกับ p_i กับ Th ถ้ามากกว่าจัดเป็น RAP มิฉะนั้นเป็น AP ปกติ แนวคิดนี้ใช้ Round Trip Time ซึ่งเป็นเวลารอบแฟ้มเกิดในการสื่อสารเครือข่าย จึงจับพฤติกรรมผิดปกติที่เกิดจากการเพิ่มหน่วงและความไม่เสถียรของ RAP ได้ โดยยังสอดคล้องกับแนวทางเฝ้าระวัง AP ในการรักษาความปลอดภัย WLAN

ขั้นตอนวิธีที่นำเสนอ Algorithm 2 Rogue AP Detection ถูกพัฒนาขึ้นเพื่อจำแนกความแตกต่างระหว่างจุดเชื่อมต่อปกติ (Normal Access Point - AP) และจุดเชื่อมต่อปลอม (Rogue Access Point - RAP) โดยอาศัยการวิเคราะห์ค่าเวลารอบในการรับส่งข้อมูล (Round Trip Time - RTT) ซึ่งสะท้อนถึงเสถียรภาพของเครือข่าย โดยกระบวนการทำงานแบ่งออกเป็น 2 ขั้นตอนหลักดังนี้

Algorithm 2 Rogue AP Detection

```

1: For each load  $k \in \{No\ Load, 3MB, 5MB, 7MB, All\}$ :
2:    $T\_temp = EmptyList$ 
3:   For each file  $d\_train \in D\_AP$  (Training Set):
4:      $RTT = Extract(d\_train, k)$ 
5:      $RTT' = \{x \in RTT \mid Q1 - 1.5IQR \leq x \leq Q3 + 1.5IQR\}$ 
6:      $\gamma = KMeans(RTT')$ ,  $\theta = \max(\gamma) / \min(\gamma)$ 
7:     Append  $\theta$  to  $T\_temp$ 
8:    $Threshold\_k = Average(T\_temp)$ 
9: For each file  $d \in D\_Test$ :
10:  For each load  $i \in \{No\ Load, 3MB, 5MB, 7MB, All\}$ :
11:    If  $TrueLabel(d) == "RAP"$ :
12:       $RTT\_i' = RTT\_i$ 
13:    Else:
14:       $RTT\_i' = \{x \in RTT\_i \mid Q1 - 1.5IQR \leq x \leq Q3 + 1.5 * IQR\}$ 
15:      If  $Count(RTT\_i') \geq 2$ :
16:         $\gamma = KMeans(RTT\_i')$ ,  $\rho_i = \max(\gamma) / \min(\gamma)$ 
17:        If  $i == All$ :  $Th = Threshold\_All$ 
18:        Else:  $Th = Threshold\_i$ 
19:        If  $\rho_i > Th$ :
20:           $Detection \leftarrow "Rogue\ AP"$ 
21:        Else:
22:           $Detection \leftarrow "Normal\ AP"$ 

```

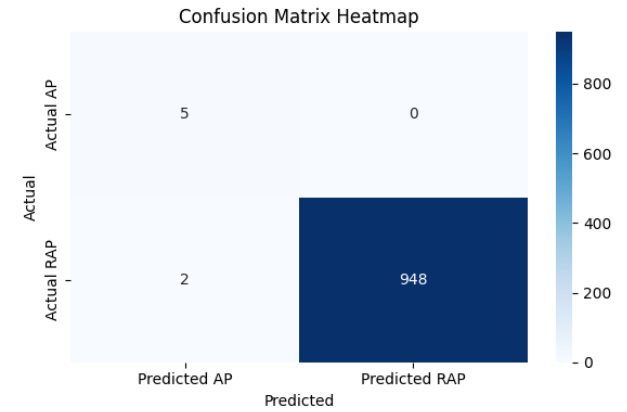
3.1 ขั้นตอนการเรียนรู้และกำหนดค่าเกณฑ์ (Training and Threshold Determination)

ในขั้นตอนแรก ระบบจะทำการประมวลผลชุดข้อมูลฝึกสอน D_AP จากอุปกรณ์ที่เชื่อถือได้ เพื่อหาค่าเกณฑ์มาตรฐาน $Threshold$ โดยจำแนกตามปริมาณปริมาณการจราจรข้อมูลที่บันทึกข้อมูลในแต่ละปริมาณการจราจรข้อมูล $load\ i \in \{No\ Load, 3MB, 5MB, 7MB, All\}$ กระบวนการเริ่มจากการดึงค่า RTT และทำการจัดข้อมูลที่มีความผิดปกติ Outlier ออกด้วยวิธีการ Interquartile Range (IQR) โดยพิจารณาเฉพาะข้อมูลที่อยู่ในช่วง $Q1 - 1.5IQR \leq x \leq Q3 + 1.5IQR$ เพื่อให้ได้ข้อมูลที่เป็นตัวแทนของเครือข่ายปกติอย่างแท้จริง จากนั้น ข้อมูลที่ผ่านการคัดกรองจะถูกนำมาจัดกลุ่มด้วยวิธี K-Means Clustering เพื่อหาค่าศูนย์กลางของกลุ่มข้อมูล γ และคำนวณหาค่าสัดส่วน θ ระหว่างค่าหน่วยเวลาสูงสุดและต่ำสุด ตามสมการ $\theta = \max(\gamma) / \min(\gamma)$ ค่าเฉลี่ยของ θ ที่ได้จากการวนซ้ำจะถูกกำหนดให้เป็นค่าเกณฑ์ตัดสิน $Threshold_k$ สำหรับแต่ละระดับ

3.2 ขั้นตอนการตรวจสอบและจำแนกประเภท (Detection Phase)

ในขั้นตอนการทดสอบกับชุดข้อมูลทดสอบ D_Test ระบบจะทำการคำนวณค่าสัดส่วนลักษณะเด่น ρ_i ของข้อมูลที่เข้ามา โดยมีการจัดการข้อมูลเบื้องต้น (Preprocessing) ที่แตกต่างกันตามสมมติฐานของประเภทอุปกรณ์ หากข้อมูลมีแนวโน้มเป็น RAP ระบบจะนำค่า RTT ทั้งหมดมาประมวลผลโดยไม่ตัดค่าผิดปกติทิ้งเพื่อรักษาคุณลักษณะความไม่เสถียรของเครือข่ายไว้ แต่หากเป็นกรณีปกติ จะใช้วิธีการกรองด้วย IQR เช่นเดียวกับขั้นตอนการเรียนรู้ เมื่อได้ชุดข้อมูล RTT สำหรับการตรวจสอบแล้ว ระบบจะดำเนินการผ่านกระบวนการ K-Means เพื่อคำนวณค่า $\rho_i = \max(\gamma) / \min(\gamma)$ และนำไปเปรียบเทียบกับค่าเกณฑ์มาตรฐาน (Th) ที่สอดคล้องกับระดับปริมาณการจราจรข้อมูลนั้นๆ โดยมีเงื่อนไขการตัดสินใจคือ หากค่า ρ_i มีค่ามากกว่า Th ระบบจะระบุอุปกรณ์ดังกล่าวเป็น "Rogue AP" แต่หากมีค่าน้อยกว่าหรือเท่ากับ จะระบุว่าเป็น "Normal AP"

4. สรุปผลการทดลอง



รูปที่ 6 Confusion Matrix Heatmap MIIIX301 Signal AP 1

จากรูปที่ 6 จากการทดสอบได้ใช้สถานที่ ณ มหาวิทยาลัยเทคโนโลยีมหานคร อาคาร MIIIX ห้อง MIIIX301 โดยใช้ Algorithm 2

ตารางที่ 1 ค่าความถูกต้องของการจำแนกห้อง MIIX301

Signal AP	Accuracy	Precision	Recall	F1 Score
1	0.997	0.99	0.997	0.998
2	0.732	0.99	0.731	0.844
3	0.99	0.99	0.99	0.992
4	0.99	0.99	0.99	0.992
5	0.992	0.99	0.992	0.993

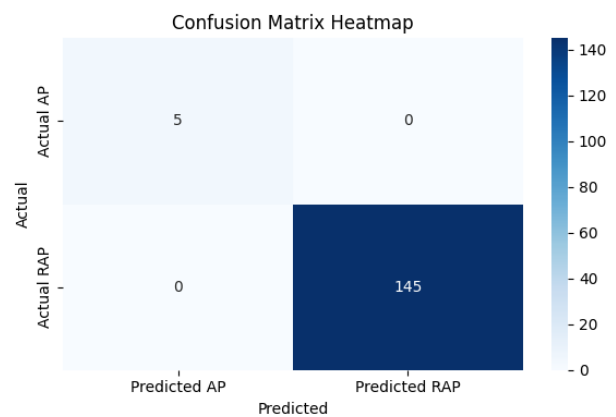
จากตารางที่ 1 จากการวิเคราะห์ประสิทธิภาพการจำแนกประเภทสัญญาณภายในห้อง MIIX301 ดังแสดงใน ตารางที่ 1 พบว่า โมเดลที่นำเสนอซึ่งใช้อัลกอริทึม K-means ร่วมกับการกำหนดพารามิเตอร์ของสัญญาณ (Signal Parameters) มีประสิทธิภาพในการทำงานที่โดดเด่นและมีความเสถียรสูงในสภาพแวดล้อมส่วนใหญ่ โดยเฉพาะอย่างยิ่งในจุดทดสอบ Signal AP 1, 3, 4 และ 5 ซึ่งให้ค่าความแม่นยำรวม (Accuracy) เฉลี่ยอยู่ในช่วง 0.990 ถึง 0.997 และมีค่า F1-Score สูงกว่า 0.99 ในทุกกรณี ผลลัพธ์นี้บ่งชี้ถึงขีดความสามารถของอัลกอริทึมในการแยกแยะคุณลักษณะระหว่างจุดเชื่อมต่อปกติ (Normal APs) และจุดเชื่อมต่อที่แปลกปลอม (Rogue APs) ได้อย่างชัดเจนและแม่นยำ

อย่างไรก็ตาม เมื่อพิจารณาผลลัพธ์ของ Signal AP 2 พบประเด็นที่น่าสนใจเกี่ยวกับพฤติกรรมการตัดสินใจของโมเดล กล่าวคือ แม้ค่าความแม่นยำ (Precision) จะยังคงอยู่ในระดับสูงมาก (0.99) ซึ่งหมายความว่าเมื่อโมเดลทำนายว่าเป็น RAPS จะมีความถูกต้อง แต่ค่าความถูกต้องรวม (Accuracy) และค่าความรำลึก (Recall) กลับลดลงเหลือเพียงประมาณ 0.732 และ 0.731 ตามลำดับ

จากรูปที่ 7 แสดงจากการทดสอบได้ใช้สถานที่ ณ มหาวิทยาลัยเทคโนโลยีมหานคร อาคาร MIIX ห้อง MIIX401 โดยใช้ Algorithm 2

จากตารางที่ 2 ผลการทดสอบของห้อง MIIX401 ซึ่งแสดงค่า Accuracy 0.99 และค่า Precision, Recall, F1 Score เป็น 1 ในทุกจุดทดสอบ แสดงให้เห็นว่าตัวรับสัญญาณ Wireless Network

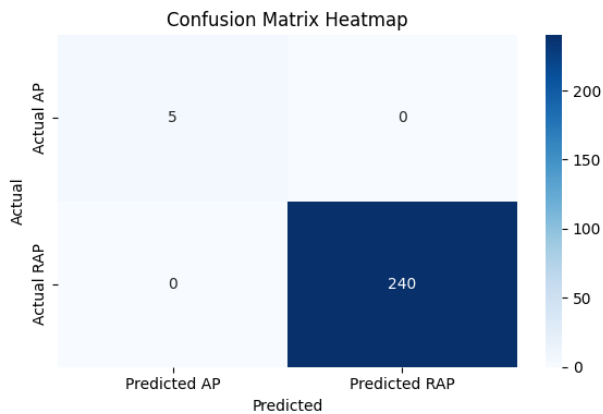
Adapter หรือหน่วยประมวลผลของห้อง MIIX401 มีประสิทธิภาพในการจัดการกับสัญญาณรบกวน Noise Resistance ได้ดีเยี่ยม ทำให้ข้อมูลที่ส่งเข้าสู่โมเดล K-means มีคุณภาพสูง ผลลัพธ์จึงออกมาถูกต้องแม่นยำ ผลการทดสอบบนอุปกรณ์ห้อง MIIX401 แสดงให้เห็นถึงประสิทธิภาพที่เหนือกว่าอย่างมีนัยสำคัญ โดยระบบสามารถทำค่า Precision, Recall และ ในทุกจุดทดสอบ AP 1-5 สิ่งนี้บ่งชี้ว่าอุปกรณ์ห้อง MIIX401 สามารถเอาชนะข้อจำกัดด้านสภาพแวดล้อมสัญญาณที่พบในรุ่นก่อนหน้าได้ โดยสามารถตรวจจับ แม้ขั้วปลอม โดยปราศจากการแจ้งเตือนที่ผิดพลาด False Alarms ซึ่งยืนยันถึงความเหมาะสมที่สุดในการนำไปใช้งานจริงเพื่อรักษาความปลอดภัยเครือข่าย WLAN



รูปที่ 7 Confusion Matrix Heatmap MIIX401 Signal AP 1

ตารางที่ 2 ค่าความถูกต้องของการจำแนกห้อง MIIX401

Signal AP	Accuracy	Precision	Recall	F1 Score
1	0.99	0.99	0.99	0.99
2	0.99	0.99	0.99	0.99
3	0.99	0.99	0.99	0.99
4	0.99	0.99	0.99	0.99
5	0.99	0.99	0.99	0.99



รูปที่ 8 Confusion Matrix Heatmap 200 Record Signal AP 3

จากรูปที่ 8 แสดงผลลัพธ์ของการทดสอบในโหมด WISP ที่จำนวน 200 Records ณ จุดรับสัญญาณ Signal AP 3 ซึ่งเป็นจุดที่โมเดลทำประสิทธิภาพได้ดีที่สุด ใช้เวลา 58 วินาทีโดยเฉลี่ย ต่อ 1 Record

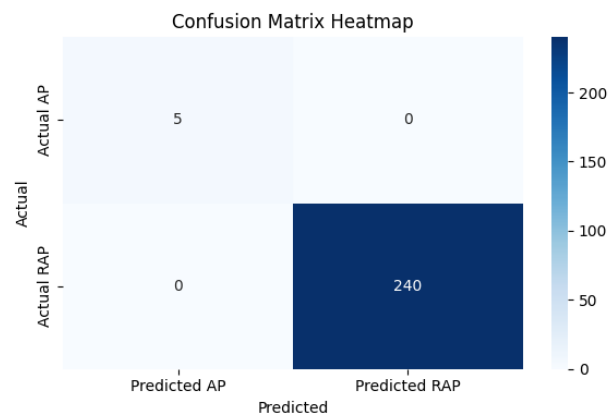
ตารางที่ 3 ค่าความถูกต้อง WISP Mode 200 Record

Signal AP	Accuracy	Precision	Recall	F1 Score
1	0.93	0.99	0.92	0.96
2	0.83	0.99	0.82	0.91
3	0.99	0.99	0.99	0.99
4	0.99	0.99	0.99	0.99
5	0.79	0.99	0.79	0.88

จากตารางที่ 3 ทดสอบเพื่อประเมินประสิทธิภาพของระบบตรวจจับการบุกรุกในโหมด WISP โดยใช้ชุดข้อมูลจำนวน 200 รายการ ณ จุดรับสัญญาณ Signal AP ที่แตกต่างกัน 5 จุด ดังแสดงในตารางที่ 3 พบว่าประสิทธิภาพของโมเดลมีความแปรผันตามตำแหน่งของจุดรับสัญญาณอย่างชัดเจน โดยเฉพาะที่จุด Signal AP 3 และ 4 ซึ่งให้ผลลัพธ์ที่ดีที่สุดในทุกจุดทดสอบ ซึ่งบ่งชี้ว่าโมเดลมีความน่าเชื่อถือสูงมากในการทำนายผลเชิงบวก โดยปราศจากความผิดพลาดในลักษณะ False Positive หรือการ

แจ้งเตือนเท็จเลย

ในทางกลับกัน ค่า Accuracy และ Recall ที่ลดลงอย่างมีนัยสำคัญ ณ จุด Signal AP 2 (0.82) และ AP 5 (0.79) สะท้อนให้เห็นข้อจำกัดของระบบในโหมด WISP ที่เกิดจากภาวะ False Negative ซึ่งมีสาเหตุหลักมาจากปัจจัยทางกายภาพ เช่น ระยะทางและสิ่งกีดขวางที่ก่อให้เกิดการลดทอนสัญญาณ (Signal Attenuation) ปัจจัยเหล่านี้ส่งผลกระทบต่อความชัดเจนของค่า RTT ทำให้ในสถานะที่มีสัญญาณรบกวนหรือ Jitter ค่า RTT ของ Rogue AP จะถูกลดทอนความผิดปกติจนมีลักษณะใกล้เคียงกับ AP ทั่วไป ส่งผลให้โมเดล K-means ซึ่งมีกลไกการตัดสินใจแบบ Conservative เพื่อลดความเสี่ยง เลือกที่จะจัดกลุ่มข้อมูลที่คลุมเครือดังกล่าวให้เป็นสถานะ 'ปกติ' จึงเป็นสาเหตุให้ค่า Recall ลดต่ำลงในที่สุด



รูปที่ 9 Confusion Matrix Heatmap 500 Record Signal AP 1

จากรูปที่ 9 แสดงผลลัพธ์การประเมินประสิทธิภาพผ่าน Confusion Matrix Heatmap ในโหมดการทำงาน WISP โดยใช้ชุดข้อมูลจำนวน 500 Records ณ จุดรับสัญญาณ Signal AP 1 ซึ่งเป็นจุดยุทธศาสตร์ที่โมเดลแสดงประสิทธิภาพได้สูงสุด ผลการทดสอบชี้ให้เห็นว่าโมเดลมีความแม่นยำ โดยสามารถจำแนก แม้ช่ายปลอม (Rogue Access Point - RAP) ได้ถูกต้องทั้งหมดจำนวน 240 ครั้ง (True Positive) และจำแนก Access Point ปกติได้ถูกต้องจำนวน 5 ครั้ง (True Negative) โดยปราศจากความผิดพลาด (Zero False Predictions) ทั้งในส่วน of False Positive และ False Negative นอกจากนี้ ในด้านประสิทธิภาพเชิงเวลา ระบบใช้เวลาในการ

ประมวลผลเฉลี่ยเพียง 2.14 นาทีต่อ 1 Record ซึ่งแสดงให้เห็นถึงความรวดเร็วและความน่าเชื่อถือในการตรวจจับภัยคุกคามจริง

ตารางที่ 4 ค่าความถูกต้อง WISP Mode 500 Record

Signal AP	Accuracy	Precision	Recall	F1 Score
1	0.99	0.99	0.99	0.99
2	0.72	0.99	0.72	0.83
3	0.88	0.99	0.88	0.94
4	0.71	0.99	0.7	0.83
5	0.99	0.99	0.99	0.99

จากตารางที่ 4 การทดสอบประสิทธิภาพของระบบในโหมด WISP ด้วยชุดข้อมูลจำนวน 500 Records โดยทำการทดสอบ ณ จุดรับสัญญาณ Signal AP 5 จุด และใช้เวลาประมวลผลเฉลี่ย 2.14 นาทีต่อ 1 Record ผลลัพธ์ที่ได้จาก รูปที่ 9 และ ตารางที่ 4 สำหรับ 500 Records การเพิ่มจำนวนข้อมูลเป็น 500 Records ส่งผลให้ค่าเฉลี่ยความถูกต้องในบางจุดลดลง เช่น AP 4 ลดลงจาก 0.99 เหลือ 0.71 ซึ่งอาจบ่งชี้ว่าเมื่อปริมาณ Traffic หนาแน่นขึ้น หรือระยะเวลาเก็บข้อมูลนานขึ้น สภาพแวดล้อมทางเครือข่าย ณ จุดนั้น ๆ อาจมีสัญญาณรบกวนที่ส่งผลกระทบต่อการตรวจจับข้อมูลมากขึ้น ในโหมด WISP ที่จำนวน 500 Records ระบบยังคงรักษาจุดเด่นเรื่องความแม่นยำ Precision ได้อย่างสมบูรณ์แบบ แต่มีความไวต่อสภาพแวดล้อมในแต่ละจุดรับสัญญาณสูงขึ้น การเลือกจุดติดตั้ง Placement ที่เหมาะสม เช่น AP 1 หรือ AP 5 จึงเป็นปัจจัยสำคัญที่สุดในการคงประสิทธิภาพของระบบในโหมดนี้ จากการทดสอบทั้ง 4 แบบผลการทดสอบในสภาพแวดล้อม การทดสอบในสภาพแวดล้อมดำเนินการ ณ อาคาร MIIX ห้อง MIIX401 และ MIIX301 เพื่อเปรียบเทียบประสิทธิภาพของอัลกอริทึม K-means ในการจำแนก แม้อาจปลอมภายใต้ปัจจัยแวดล้อมที่แตกต่างกัน

ชุดข้อมูล 200 Records Short-term Analysis ใช้เวลาเก็บข้อมูลเฉลี่ย 58 วินาทีต่อการทดสอบ ผลลัพธ์แสดงให้เห็นว่าจุดรับสัญญาณ Signal AP 3 และ 4 ให้ประสิทธิภาพดีที่สุด Accuracy 0.99 ในขณะที่ Signal AP 5 มีประสิทธิภาพต่ำที่สุด Accuracy 0.79 ซึ่งสะท้อนให้เห็นว่าในระยะเวลาสั้น โมเดลสามารถจับ

Pattern ของ RTT ได้ดี แต่ยังคงมีความเปราะบางต่อความอ่อนไหวต่อตำแหน่งการติดตั้ง (Placement Sensitivity)

ชุดข้อมูล 500 Records Long-term Analysis เมื่อเพิ่มจำนวนข้อมูลและใช้เวลาเก็บข้อมูลเป็นเฉลี่ย 2.14 นาที พบความเปลี่ยนแปลงของประสิทธิภาพอย่างมีนัยสำคัญ จุดที่เคยทำงานได้ดีในชุดข้อมูลก่อนหน้านี้อย่าง Signal AP 4 กลับมีค่า Accuracy ลดลงเหลือ 0.71 ในขณะที่ Signal AP 1 และ 5 กลับมีประสิทธิภาพสูงขึ้นเป็น 0.99 ปรากฏการณ์นี้บ่งชี้ว่าการเพิ่มระยะเวลาในการตรวจจับสัญญาณ อาจเป็นการเพิ่มโอกาสในการรับสัญญาณรบกวนที่แปรผันตามเวลา Time-variant Noise เข้ามาในระบบ ส่งผลให้ความแม่นยำในบางจุดลดลงเนื่องจากความผันผวนของค่า RTT ในทุกการทดสอบ ค่า Precision มีค่าเป็น 1.0 หรือเกือบ 1.0 เสมอ แสดงให้เห็นว่าจุดเด่นของอัลกอริทึมที่นำเสนอคือความน่าเชื่อถือ ความผันผวนของค่า Accuracy ที่เกิดขึ้นในห้อง MIIX301 AP 2 และ WISP Mode เกิดจากการลดลงของค่า Recall เป็นหลัก ซึ่งมีสาเหตุจากปัจจัยทางกายภาพ เช่น สัญญาณรบกวน Noise และสิ่งกีดขวางที่ทำให้ค่า RTT ของอุปกรณ์ Rogue AP มีความใกล้เคียงกับ AP ปกติในบางจังหวะ ทำให้โมเดลไม่สามารถตรวจจับได้ครบถ้วน

งานวิจัยนี้ได้นำเสนอวิธีการตรวจจับ แม้อาจปลอมโดยใช้ค่า RTT ร่วมกับอัลกอริทึม K-means ผลการทดสอบยืนยันว่าวิธีดังกล่าวมีประสิทธิภาพสูงในการแยกแยะภัยคุกคาม โดยเฉพาะในสภาพแวดล้อมที่มีการควบคุมในห้อง MIIX401 ซึ่งสามารถทำความถูกต้องได้ถึง 99.7% สำหรับการใช้งานจริงในสภาพแวดล้อมเปิด WISP Mode ระบบยังคงรักษามาตรฐานความแม่นยำ Precision ได้อย่างสมบูรณ์แบบ แต่อาจมีข้อจำกัดด้านความครอบคลุม Recall ในบางจุดติดตั้งที่มีสัญญาณรบกวนสูง การนำระบบไปประยุกต์ใช้จึงควรคำนึงถึงการสำรวจจุดติดตั้ง Site Survey ที่เหมาะสม เพื่อลดผลกระทบจากความแปรปรวนของสัญญาณและเพิ่มประสิทธิภาพในการตรวจจับให้สูงสุด สำหรับพื้นที่ที่มีอุปกรณ์หนาแน่นหรือมีสัญญาณรบกวนสูง ควรใช้อุปกรณ์รับสัญญาณที่มีคุณภาพสูง High-performance Wireless Adapter เหมือนกรณีการทดสอบในห้อง MIIX401 ที่สามารถจัดการกับ Noise ได้ดี จะช่วยให้ผลการตรวจจับแม่นยำขึ้นอย่างมีนัยสำคัญ หรือหากพบว่าการใช้งานอินเทอร์เน็ตมีความหน่วงผิดปกติ Lag หรือช้าลงอย่างไม่มีสาเหตุ โดยเฉพาะเมื่อมีการโหลดข้อมูลจำนวนมาก ให้พึงระวังว่าอาจกำลังเชื่อมต่ออยู่กับแม้อาจปลอมแม้ว่าชื่อ WiFi จะถูกต้องก็ตาม

เอกสารอ้างอิง

- [1] U.S. Department of Defense; FBI; NSA; CISA, "Russian Cyber Actors Use Compromised Routers to Facilitate Cyber Operations," Joint Cybersecurity Advisory, Feb. 27, 2024. [Online]. Available: <https://media.defense.gov/2024/Feb/27/200340753>. [Accessed: Sep. 21, 2025].
- [2] Cybersecurity and Infrastructure Security Agency (CISA), "CISA, NSA, FBI and International Partners Publish Guide: Protecting Communications Infrastructure," News Release, Dec. 3, 2024. [Online]. Available: <https://www.cisa.gov/news-events/news/cisa-nsa-fbi-and-international-partners-publish-guide-protecting-communications-infrastructure>. [Accessed: Sep. 21, 2025].
- [3] K. C. Patel and A. Patel, "Rogue Access Point: The WLAN Threat," in Proc. 2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 2023, pp. 1-6. doi: 10.1109/ICCCIS56430.2023.10037591.
- [4] T. Ueda, A. Saif, S. Miyata, M. Nakahara, and A. Kubota, "A Client-Side Evil-Twin Attack Detection System with Threshold Considering Traffic Load," in Proc. 2023 IEEE 13th International Conference on Consumer Electronics - Berlin (ICCE-Berlin), 2023, pp. 1-5. doi: 10.1109/ICCE-BERLIN58801.2023.10375616.
- [5] K. Murugesan, K. K. Thangadurai, and V. N. Muralidhara, "PoEx: Proof of Existence for Evil Twin Attack Prevention in Wi-Fi Personal Networks," in Proc. 2021 8th International Conference on Future Internet of Things and Cloud (FiCloud), 2021, pp. 1-7. doi: 10.1109/FiCloud49777.2021.00021.
- [6] M. Vanhoef and F. Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2," in Proc. 2017 ACM SIGSAC Conf. on Computer and Communications Security (CCS), 2017, pp. 1313-1328. doi: 10.1145/3133956.3134027.
- [7] M. Vanhoef and E. Ronen, "Dragonblood: A Security Analysis of WPA3's SAE Handshake," 2019. [Online]. Available: <https://wpa3.mathyvanhoef.com>. [Accessed: Sep. 21, 2025].
- [8] CERT Coordination Center (US-CERT), "WiFi Protected Setup (WPS) PIN brute force vulnerability," Vulnerability Note VU#723755, Dec. 27, 2011. [Online]. Available: <https://www.kb.cert.org/vuls/id/723755>. [Accessed: Sep. 21, 2025].
- [9] L. M. Zahavi, "A Technical Survey on Approaches for Detecting Rogue Access Points," Digital Commons Montclair, 2023. [Online]. Available: <https://digitalcommons.montclair.edu/etd/1326/>. [Accessed: Sep. 01, 2024].
- [10] ResearchGate, "Research on evil-twin, captive-portal attacks and mitigation (e.g., EvilScout, statistical detection)," n.d. [Online]. Available: <https://www.researchgate.net>. [Accessed: Sep. 21, 2025].
- [11] "What is Rogue Access Point? Protecting Against Cyber Infiltrators," ReasonLabs Cyberpedia. [Online]. Available: <https://cyberpedia.reasonlabs.com/EN/rogue%20access%20point%20detection.html>. [Accessed: Sep. 01, 2024].
- [12] Help Net Security, "94% of Wi-Fi networks lack protection against deauthentication attacks," Mar. 14, 2025. [Online]. Available: <https://www.helpnetsecurity.com/2025/03/14/wi-fi-networks-deauthentication-attacks/>. [Accessed: Sep. 21, 2025].
- [13] E. B. Blancaflor, F. D. C. Magno, C. I. S. Monteloyola, and L. A. T. Ogaya, "The Elusive Enigma: Unraveling Rogue Wi-Fi's Chessboard of Deception with Man in the Middle Mastery and Rogue Access Point Intrigue," in Proc. III International Conference on Electrical, Computer and Energy Technologies (ICECET), 2023, pp. 1-8. doi: 10.1109/ICECET2023.2023.1234567.
- [14] "Wi-Fi Experiment at RSAC 2017 Reveals Shocking Stats," Help Net Security, Feb. 24, 2017. [Online]. Available: <https://www.helpnetsecurity.com/2017/02/24/wifi-experiment-rsac-2017/>. [Accessed: Sep. 01, 2024].
- [15] R. Maayah, A. Abadleh, and E. Al-Subehat, "Analysis of RSS Patterns to Detect Rogue Access Points," in Proc. 2022 International Conference on Emerging Trends in Computing and Engineering Applications (ETCEA), 2022, pp. 1-5. doi: 10.1109/ETCEA57049.2022.10009667.
- [16] S. Kitisriworapan, A. Jansang, and A. Phonphoem, "Client-side rogue access-point detection using a simple walking strategy and round-trip time analysis," EURASIP Journal on Wireless Communications and Networking, vol. 2020, no. 1, pp. 1-24, 2020. doi: 10.1186/s13638-020-01745-4.
- [17] Z. Yang, Q. Lu, H. Zhang, F. Chen, and H. Xian, "Eliminating Rogue Access Point Attacks in IoT: A Deep Learning Approach With Physical-Layer Feature Purification and Device Identification," IEEE Internet of Things Journal, vol. 11, no. 8, pp. 14886-14899, 2024. doi: 10.1109/JIOT.2023.3345378.
- [18] M. Souppaya and K. Scarfone, "Guidelines for Securing Wireless Local Area Networks (WLANs)," NIST SP 800-153, Feb. 2012. doi: 10.6028/NIST.SP.800-153. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf>. [Accessed: Sep. 21, 2025].
- [19] J. W. Tukey, Exploratory Data Analysis. Addison-Wesley, 1977. [Online]. Available: NIST/SEMATECH e-Handbook of Statistical Methods: Data Cleaning & Exploratory Data Analysis, National Institute of Standards and Technology.



ภุณศ เมฆพยอม จบการศึกษา วิศวกรรมศาสตรบัณฑิต(วิศวกรรมคอมพิวเตอร์) ปัจจุบันศึกษา วิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมไฟฟ้าสาขาย่อยคอมพิวเตอร์) มหาวิทยาลัยเทคโนโลยีมหานคร ปัจจุบันเป็นอาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์และปัญญาประดิษฐ์ สถาบันนวัตกรรมมหานครโดยดำรงตำแหน่งเป็นผู้ช่วยรองอธิการบดีฝ่ายสถาบันนวัตกรรมมหานครฝ่ายกิจกรรมนักศึกษาและประชาสัมพันธ์



ผู้ช่วยศาสตราจารย์ ดร.ณัฐพงษ์ จันทรแดง จบการศึกษาวิศวกรรมศาสตรบัณฑิต(วิศวกรรมคอมพิวเตอร์) วิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมไฟฟ้าสาขาย่อยคอมพิวเตอร์) และ วิศวกรรมศาสตรดุษฎีบัณฑิต (วิศวกรรมไฟฟ้าสาขาย่อยคอมพิวเตอร์) มหาวิทยาลัยเทคโนโลยีมหานคร ปัจจุบันเป็นอาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์และปัญญาประดิษฐ์สถาบันนวัตกรรมมหานครโดยดำรงตำแหน่งเป็นหัวหน้าภาควิชา มีหัวข้องานวิจัยที่สนใจได้แก่การประมวลผลสัญญาณและภาพดิจิทัล (Signal and Image Processing) การรู้จำแบบ (Pattern Recognition) การรู้จำภาพ (Image Recognition) และ ปัญญาประดิษฐ์ (Artificial Intelligence)