การประชุมวิชาการทางวิศวกรรมไฟฟ้า ครั้งที่ 48
The 48th Electrical Engineering Conference (EECON-48)
วันที่ 19-21 พฤศจิกายน 2568 ณ โรงแรมฟูราม่า จังหวัดเชียงใหม่

# การวิเคราะห์ค่า Round Trip Time เพื่อการตรวจจับจุดเชื่อมต่อปลอมในเครือข่ายไร้สาย

# Round Trip Time Analysis for Detecting Rogue Access Points in Wireless Networks

**ภูธเนศ เมฆพยม ณัฐพงษ์ จันทร์แดง**
สาขาวิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีมหานคร phuthanet@mut.ac.th, jnattapo@mut.ac.th

## บทคัดย่อ

บทความนี้มุ่งเน้นการศึกษาวิธีการตรวจจับ และการป้องกันการโจมตีที่เกิดขึ้นจากสถานีแม่ข่ายปลอม โดยเฉพาะในเครือข่าย WLAN 802.11 ที่เสี่ยงต่อจุดเชื่อมต่อที่เป็นภัย Rogue Access Points โดยมีการจำลองการโจมตีแบบ Man in The Middle เพื่อวิเคราะห์ผลกระทบอย่างเป็นระบบ นอกจากนี้ ยังได้ใช้ข้อมูลที่ได้จากการทดลองมาผ่าน อัลกอริธึม K-means เพื่อจำแนกสถานีแม่ข่ายที่เป็นภัย บนความนี้ยังเสนอคำแนะนำในการเพิ่มความปลอดภัยสำหรับเครือข่าย ระดับบุคคล และองค์กร

**คำสำคัญ:** สถานีแม่ข่ายปลอม, ภัยคุกคาม, Rogue Access Points, Man in the Middle, WLAN, Wi-Fi

## Abstract

This article focuses on studying methods for detecting and preventing attacks originating from rogue access points, especially in WLAN 802.11 networks, which are vulnerable to malicious connection points. A Man-in-the-Middle attack simulation is used to systematically analyze the impact. Additionally, data obtained from experiments is processed through the K-means algorithm to classify malicious access points. Based on this, the article provides recommendations for enhancing security at both the individual and organizational network levels.

**Keywords:** Rogue Access Points, Man in the Middle, WLAN, Wi-Fi

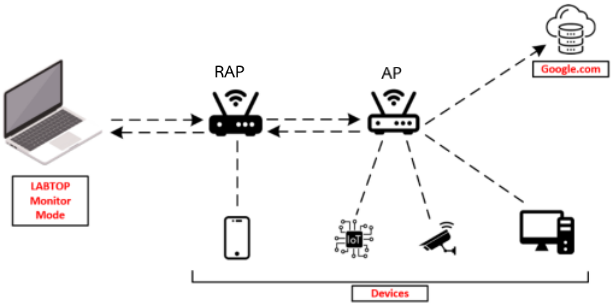
## บทนำ

ในช่วงไม่กี่ปีที่ผ่านมาระบบเครือข่ายไร้สาย ได้มีการเติบโตขึ้นอย่างรวดเร็ว และมีการใช้งานแพร่หลายเป็นอย่างมาก ทุกสถานที่ ที่สัญญาณเข้าถึงจะต้องมีเครือข่ายไร้สาย เกิดการเปลี่ยนแปลงเข้าสู่การทำงานระยะไกล และการเรียนออนไลน์ โดยเฉพาะช่วงการระบาดของไวรัสโคโรนา ทำให้เพิ่มการใช้งานเครือข่ายเหล่านี้มากยิ่งขึ้น และมันกลายเป็นสิ่งสำคัญที่ไม่สามารถขาดได้ไปแล้วในปัจจุบัน ซึ่งการใช้งานที่มากมายกลายเป็นปัญหาที่สำคัญอย่างยิ่ง ทางด้านความปลอดภัยของระบบเครือข่ายเหล่านี้ [3][4] มีผู้ประสงค์ร้ายเหล่านี้ที่เป็นภัยพยายามที่ใช้ช่องโหว่ของ ระบบที่ในการหลอกลวงเหยื่อ ด้วยวิธีต่างๆ ผ่านเครือข่ายไร้สาย โดยเฉพาะ การหลอกขโมยข้อมูลส่วนบุคคล[4][7] หรือเรียกว่า Man-in-the-Middle (MitM) [2][3][5][6]เป็นปัญหาด้านความปลอดภัยอย่างชัดเจน ผู้ประสงค์ร้ายเหล่านี้ใช้วิธีการตั้ง แม่ข่ายปลอม หรือ Rogue Access Points (RAP) ในการหลอกลวงให้เหยื่อเข้าไปใช้งาน ระบบเครือข่ายไร้สาย Wi-Fi เพื่อหลอกเอาข้อมูลส่วนบุคคลโดยอาศัย การตั้งแม่ข่ายฟรีตามสถานที่ต่างๆ ทำให้เหยื่อหลงกลและเชื่อมต่อกับเครือข่าย เช่น โรงแรมที่มี Wi-Fi ฟรี, ร้านกาแฟ,สถานที่สาธารณะ การเติบโตของจำนวน Access Point ทั่วโลกตั้งแต่ปี 2018 จนถึงปี 2023 คาดการณ์ว่ามีการตั้ง Wi-Fi สาธารณะทั่วโลกถึง ล้านจุดในปี 2022 ซึ่งเป็น สี่เท่าของจำนวนที่มีอยู่ในปี 2018 [1][2][3] ตัวเลขนี้แสดงให้เห็นถึง การเติบโตอย่างมีนัยสำคัญของการใช้งาน Access Point สาธารณะ

ในยุคดิจิทัลที่การใช้งานเครือข่ายแบบไร้สาย หรือ WLAN กำลังเติบโตอย่างรวดเร็ว ความปลอดภัยของเครือข่ายเหล่านี้ กลายเป็นปัญหาที่สำคัญยิ่ง การโจมตีโดยใช้ Rogue Access Point (RAP) ซึ่งเป็นการติดตั้งจุดเชื่อมต่อปลอมใน เครือข่ายเพื่อหลอกลวงผู้ใช้และขโมยข้อมูลส่วนตัวเป็นหนึ่ง ในภัยคุกคามที่ซับซ้อนและร้ายแรงที่สุดของเครือข่ายไร้สาย RAP สามารถใช้ในหลากหลายรูปแบบของการโจมตี RAPs ถือเป็นหนึ่งในภัยคุกคามที่ร้ายแรงที่สุดและซับซ้อนที่สุดต่อความปลอดภัยของเครือข่ายไร้สาย WLAN [1][2][7]

ความเสี่ยงเหล่านี้ได้กระตุ้นให้นักวิจัยและ ผู้เชี่ยวชาญในด้านความปลอดภัยพัฒนาวิธีการตรวจจับและ ป้องกันการโจมตีเหล่านี้อย่างต่อเนื่อง การตรวจจับ RAP ได้รับความสนใจอย่างมากในวงการวิจัย โดยวิธีการที่ถูกนำเสนอในบทความนี้ รวมถึงการวิเคราะห์ลักษณะสัญญาณ Round Trip Time (RTT) รวมถึงการใช้เทคโนโลยี Machine Learning ในการจำแนกและตรวจจับ RAP โดย เทคนิคที่ได้รับการศึกษาและพัฒนามีทั้ง K means Clustering เพื่อหาค่า Threshold และ ทำความสะอาดข้อมูลเพื่อเพิ่มความแม่นยำในการตรวจจับวัตถุประสงค์หลักของ บทความนี้คือการพัฒนาและประเมินประสิทธิภาพของ วิธีการตรวจจับ RAP ที่สามารถใช้งานได้จริงในสถานการณ์ เครือข่ายไร้สายที่มีความหลากหลายและซับซ้อน โดยเน้น การใช้เทคโนโลยี Machine Learning และการวิเคราะห์ สัญญาณเพื่อเพิ่มความปลอดภัยและลดความเสี่ยงจาก การโจมตีทางไซเบอร์ในเครือข่าย WLAN

โดยการจำลองสภาพแวดล้อมขึ้นมา เพื่อใช้ในการทดสอบ โดยมี Access Point ที่เป็นแม่ข่ายจริง มีการใช้งานปกติและ อุปกรณ์อื่นต่อพ่วงในเครือข่ายทั้งหมด 15 อุปกรณ์ ได้แก่ มือถือ 5 เครื่อง,สมาร์ตทีวี 1 เครื่อง ,กล่องวงจรปิด 3 อุปกรณ์,อุปกรณ์ IOT 4 อุปกรณ์ และ NAS ทำการจำลอง Rogue Access Point (RAP) แม่ข่ายปลอมขึ้นมา ในระบบ โดยกำหนด SSID และ Password ให้เหมือนกับ Access Point ตัวจริง




รูปที่ 1 แบบการจำลองระบบเครือข่าย

*ผู้ประพันธ์บรรณกิจ

## การออกแบบข้อมูล

ในการออกแบบการเก็บข้อมูลใช้คำสั่งที่ผู้ใช้สามารถเข้าถึงได้ง่ายและมีใช้งานทั่วไป ยังเป็นมาตฐานโดยอาศัย แพ็กเก็ต ICMP (Internet Control Message Protocol) โดยให้ทำการ Echo Request ไปยังโฮสต์ปลายทาง และรอรับแพ็กเก็ต ICMP Echo Reply กลับมา ด้วยคำสั่ง Ping ไปที่ Google โดยคำสั่งทั้งหมดทำงานบน Python Code ที่ได้ทำการสร้างไว้ Algorithm 1 สำหรับเก็บข้อมูลโดยเฉพาะ แบ่งเป็นการบันทึก แบบ No Load ทั้งหมด 500 Record, ข้อมูล 3MB ทั้งหมด 500 Record, ข้อมูล 5MB ทั้งหมด 500 Record, ข้อมูล 7MB ทั้งหมด 500 Record รวมเป็นข้อมูลทั้งหมด 2000 Record ข้อมูลทั้งหมดบันทึกในช่วงเวลาเร่งด่วน [8] ประมาณ (20:00 น.) ตามเวลาประเทศไทย การเก็บข้อมูลจะเก็บ สัญญาณ Access Point แม่ข่าย และ เก็บสัญญาณ Rogue Access Point แม่ข่ายปลอม รูปแบบข้อมูลทั้งสอง ที่ได้เป็นรูปแบบ ดังนี้

**Algorithm 1** Record Data

```
1: FUNCTION run_ping(sizes_mb, counts, target):
2:     /*GET file name from user*/
3:     /*CREATE CSV file and write header*/
4:     INIT empty queue
5:     FOR each size in sizes_mb:
6:         FOR i = 1 to counts[size]:
7:             /*ADD packet_size to queue*/
8:     WHILE queue not empty:
9:         /*GET packet_size from queue*/
10:        /*RUN ping with that size to target*/
11:        IF reply found:
12:            /*EXTRACT IP, bytes, time, TTL*/
13:            /*APPEND result to CSV*/
14: Return 0
```

ในช่วงเวลาที่มีการสื่อสารโปรแกรมจะทำการ เก็บเวลาไปกลับระหว่าง Access Point กับ Server ของ Google โดยรับข้อมูลเข้า เป็นจำนวน ขนาด sizes_mb (No Load, 3MB, 5MB, 7MB) [4], จำนวน Count 500 ครั้งต่อ Load และ Target จะเป็น Google.com และ Return ค่า RTT ออก โดยใช้ผ่านสัญญาณ คลื่นความถี่ 2.4 GHz (Frequency Band)

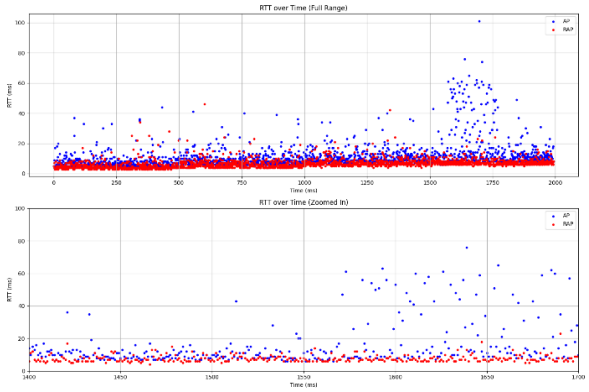
| | No. | Size | IP Address | Bytes | Time (ms) | TTL |
|---|---|---|---|---|---|---|
| 0 | 1 | No Load | 104.26.9.179 | 32 | 5 | 57 |
| 1 | 2 | No Load | 104.26.9.179 | 32 | 4 | 57 |
| 2 | 501 | 3MB | 104.26.9.179 | 3072 | 13 | 57 |
| 3 | 502 | 3MB | 104.26.9.179 | 3072 | 8 | 57 |
| 4 | 1001 | 5MB | 104.26.9.179 | 5120 | 8 | 57 |
| 5 | 1002 | 5MB | 104.26.9.179 | 5120 | 14 | 57 |
| 6 | 1501 | 7MB | 104.26.9.179 | 7168 | 8 | 57 |
| 7 | 1502 | 7MB | 104.26.9.179 | 7168 | 8 | 57 |

รูปที่ 2 ข้อมูลจากการบันทึก

จากรูปภาพที่ 2 เป็นข้อมูลที่ได้จากการบันทึกผลของ Algorithm 1 ซึ่งข้อมูลที่ได้มี ดังนี้ No ลำดับการบันทึกผล, Size ขนาดที่กำหนดในการ Ping แต่ละคำสั่ง, IP Address เป็นปลายทางที่ทำการส่งข้อมูลไป, Bytes เป็นขนาดที่ทำการส่งข้อมูลไปยังปลายทางในแต่ละครั้ง ขนาดเป็น Byte, Time เป็นเวลาที่ใช้ในการส่งข้อมูลไปกลับ, TTL (Time To Live) อายุข้อมูลของแพ็กเก็ตในเครือข่าย

## การจัดการข้อมูล

หลังจากได้ข้อมูลที่ผ่านการบันทึกด้วย Algorithm 1 มาได้รูปแบบข้อมูลดัง รูปที่ 3 ภาพที่ 1 จะต้องทำความสะอาดข้อมูลโดย การทำ EDA (Exploratory Data Analysis) ด้วย IQR Method คือการสำรวจและวิเคราะห์ข้อมูล พร้อมกับ ตัดค่า outliers โดยใช้เทคนิค IQR ซึ่งช่วยให้เราเข้าใจข้อมูลได้ดีขึ้น และลดผลกระทบของค่าที่ออกนอกช่วงมากเกินความจำเป็น




รูปที่ 3 สัญญาณ RTT ของ AP,RAP

จากกราฟสัญญาณ AP และ RAP โดยสีแดงเป็น AP และ สีน้ำเงินเป็น RAP ที่ยังไม่ผ่านการ EDA และ IQR Method จะสังเกตุเห็นว่า RTT ที่เป็น RAP รูปที่ 3 ภาพที่ 2 เป็นการขยายช่วงให้เห็นว่ามีการออกนอกช่วงอย่างชัดเจน โดยแกน X เป็น สัญญาณ RTT และ แกน Y เป็นเวลา

## การทดลอง

การทดลองนี้ ได้นำเสนอขั้นตอนการตรวจจับ Rogue Access Point โดยใช้ข้อมูล Round Trip Time ภายใต้โหลดต่าง ๆ เช่น No Load, 3MB, 5MB และ 7MB โดยมีเป้าหมายเพื่อแยกแยะ RAP ออกจาก AP ปกติ เพื่อให้สามารถวิเคราะห์ความผิดปกติของค่า RTT ได้อย่างแม่นยำ จึงมีการลบค่าผิดปกติ Outliers ออกจากข้อมูลด้วยวิธี IQR (Interquartile Range) จากนั้นจึงใช้ K-Means (k = 2) แบ่งข้อมูล RTT ออกเป็น 2 กลุ่ม หลังจากผ่านการ EDA แล้วทำการเก็บค่า Threshold ของ AP รวมถึง RAP เป็นแต่ละช่วง Load ข้อมูล จากนั้นจะทำการเทียบค่า Threshold แต่ละ Load ระหว่าง ค่าที่ได้จาก AP เทียบกับค่าสัญญาณ หากค่า Threshold ของสัญญาณใดๆ มีค่ามากกว่า ค่า Threshold ของ AP ถือว่าเป็น RAP และยังรวมถึงการตรวจสอบเทียบค่า ของสัญญาณทั้งช่วงด้วย โดยเป้าหมายหลักของการดำเนินการในครั้งนี้ คือการจำแนก RAP ออกจาก Access Point ที่เป็นของจริงได้อย่างมีประสิทธิภาพ โดยอาศัยลักษณะความผิดปกติที่อาจเกิดขึ้นในค่าของ RTT ซึ่งถูกนำมาวิเคราะห์อย่างละเอียด เพื่อให้การจำแนกสามารถทำได้แม่นยำและเชื่อถือได้สูงที่สุด การใช้ข้อมูล RTT ภายใต้โหลดต่างๆ ช่วยให้สามารถวิเคราะห์ และแยกแยะความผิดปกติ ที่เกิดขึ้นในช่วงสัญญาณเครือข่ายได้อย่างมีประสิทธิภาพ ทำให้สามารถจำแนก AP ปกติและ RAP ได้อย่างแม่นยำยิ่งขึ้น ข้อมูลที่ได้สามารถนำไปใช้เพื่อเสริมสร้างความปลอดภัยในระบบเครือข่ายไร้สาย โดยการตรวจจับ RAP ที่มีความปกติในค่าของ RTT

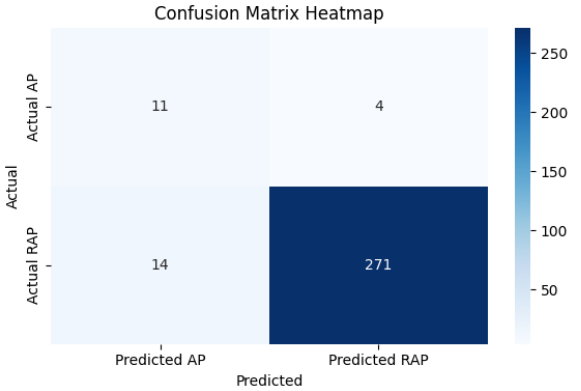
**Algorithm 2 Rogue AP Detection**

1: **For** each file d ∈ D:
2: **For** each load i ∈ {No Load, 3MB, 5MB, 7MB, All}:
3: $RTTi' = x \in RTTi \mid Q1 - 1.5 \cdot IQR \le x \le Q3 + 1.5 \cdot IQR$
4: $\gamma = KMeans(RTT\ i), \gamma\ max = max(\gamma), \gamma\ min = min(\gamma)$
5: $\rho i = \frac{\gamma\ \max}{\gamma\ \min}$
6: **If** i = All :
7: **If** $\rho i > \theta_{all}$ : /*Detection ⟵ "Detected Rogue AP"*/
8: **Else**: /*Detection ⟵ "No Rogue AP"*/
9: **Else**:
10: **If** $\rho i > \theta_i$ : /*Detection ⟵ "Detected Rogue AP"*/
11: **Else**: /*Detection ⟵ "No Rogue AP"*/

อัลกอริทึมนี้ใช้สำหรับตรวจจับ Rogue Access Point โดยอาศัยการวิเคราะห์ค่าระยะเวลาในการรับส่งข้อมูล RTT ภายใต้โหลดต่าง ๆ ที่กำหนดไว้ No Load, 3MB, 5MB, 7MB ทำการลบค่าผิดปกติ Outliers ของ RTT โดยใช้วิธี IQR (Interquartile Range) ในการวิเคราะห์ข้อมูลเวลาการตอบสนองของเครือข่าย หรือ RTT Round Trip Time การตรวจจับค่าผิดปกติถือเป็นขั้นตอนสำคัญเพื่อให้ผลวิเคราะห์มีความน่าเชื่อถือ โดยวิธีที่นิยมใช้คือการอ้างอิงค่าควอไทล์ ได้แก่ Q1 และ Q3 ซึ่งเป็นค่าทางสถิติที่ใช้แบ่งข้อมูลที่เรียงลำดับแล้วออกเป็นสี่ส่วนเท่า ๆ กัน Q1 แรกของข้อมูล ในขณะที่ ช่วงระหว่าง Q3 กับ Q1 เรียกว่า IQR ซึ่งสะท้อนถึงความกระจายของข้อมูลช่วงกลาง การใช้ค่า Q1, Q3 และ IQR ในการกรองค่าผิดปกติทำได้โดยกำหนดช่วงของค่าที่ยอมรับได้ให้อยู่ภายใน Q1 − 1.5 × IQR ถึง Q3 + 1.5 × IQR ค่าที่อยู่ภายในช่วงนี้จะถือว่าเป็นค่าปกติ ส่วนค่าที่อยู่นอกช่วงจะถือว่าเป็นค่าผิดปกติ Outlier และอาจถูกตัดออกจากการวิเคราะห์ ด้วยวิธีนี้ จะช่วยให้สามารถกรองข้อมูล RTT ที่เบี่ยงเบนมากเกินไปออกไปได้ ทำให้การวิเคราะห์ เช่น การตรวจจับแม่ข่ายปลอม Rogue Access Point มีความแม่นยำมากยิ่งขึ้น และนำค่าที่เหลือมาแบ่งกลุ่มด้วย K-Means (k = 2) คำนวณค่าอัตราส่วน $\rho i = \frac{\gamma\ \max}{\gamma\ \min}$ โดยที่ $\gamma\ \max$ และ $\gamma\ \min$ คือค่าเฉลี่ยของแต่ละกลุ่มที่ได้จาก K-Means จากนั้นเปรียบเทียบค่า $\rho i$ กับ threshold ถ้าเป็นกรณีโหลดทั้งหมด (All Load) เปรียบเทียบกับ $\theta_{all}$ ถ้าเป็นโหลดแบบเฉพาะเจาะจง (เช่น 3MB) เปรียบเทียบกับ $\theta_i$ หาก $\rho i$ มากกว่า threshold ที่กำหนด สรุปว่าเป็น Rogue AP หากไม่เกิน สรุปว่าเป็น AP ปกติ

## สรุปผลการทดลอง

การทดลองนี้มีเป้าหมายเพื่อตรวจจับ Rogue Access Point (RAP) หรือจุดเชื่อมต่อแม่ข่ายปลอมที่มีผู้ไม่หวังดี ใช้ช่องโหว่ของระบบในการหลอกลวงผู้ใช้งานที่เข้าสู่ระบบ โดยการวิเคราะห์ค่าความหน่วงเวลาเครือข่าย Round Trip Time (RTT) ที่ได้จากการ Ping ไปยังเซิร์ฟเวอร์ Google ภายใต้เงื่อนไขโหลดข้อมูลที่แตกต่างกัน (No Load, 3MB, 5MB และ 7MB) จากนั้นใช้การจัดกลุ่มด้วย K-Means Clustering เพื่อคำนวณค่าอัตราส่วนระหว่างกลุ่ม (ρ: rho) และทำการเปรียบเทียบด้วยค่าค่าเกณฑ์มาตรฐาน (θ: theta) เพื่อวินิจฉัยว่าเป็น AP หรือ RAP




รูปที่ 4 Confusion Matrix Heatmap ผลลัพธ์การพยากรณ์

จาก Confusion Matrix Heatmap ได้แสดงผลการประเมินประสิทธิภาพของโมเดลการตรวจจับ RAP โดยเทียบกับผลการทำนายกับข้อมูลจริง พบว่า โมเดลสามารถทำนาย RAP ได้ถูกต้องถึง 271 ครั้ง ทำนาย AP ถูกต้อง 11 ครั้ง ซึ่งแสดงให้เห็นว่าโมเดลมีความแม่นยำในการตรวจจับ RAP สูง แม้จะมีข้อผิดพลาดในการจำแนก AP เล็กน้อย แต่ในการทดลองนี้ได้พัฒนาเทคนิคการตรวจจับและการเก็บข้อมูล RAP จากนั้นทำการลบค่าผิดปกติด้วยวิธี IQR และใช้ K-Means Clustering (k=2) ในการจำแนกกลุ่มค่า RTT จากข้อมูล AP จริง หาก ρ สูงกว่า θ จะพิจารณาว่าเป็น RAP โดยการทดลองใช้ข้อมูลจาก AP จริง 3 สัญญาณ และ RAP จริง 50 สัญญาณ ให้ผลลัพธ์ความแม่นยำ (Accuracy) 94% และ F1 Score 96.79% แสดงให้เห็นว่าวิธีการนี้สามารถตรวจจับ RAP ได้อย่างแม่นยำ และมีประสิทธิภาพสูง เหมาะสำหรับประยุกต์ใช้ในระบบรักษาความปลอดภัยเครือข่ายไร้สายในสถานการณ์จริง

## เอกสารอ้างอิง

[1] R. Maayah, A. Abadleh and E. Al-Subehat, “Analysis of RSS Patterns to Detect Rogue Access Points,” *2022 International Conference on Emerging Trends in Computing and Engineering Applications (ETCEA)*, 2022, pp. 1–5. doi: 10.1109/ETCEA57049.2022.10009667.

[2] K. C. Patel and A. Patel, “Rogue Access Point: The WLAN Threat,” *2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, 2022, pp. 943–948. doi: 10.1109/ICCCIS56430.2022.10037591.

[3] 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,” *2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, 2023, pp. 1–6. doi: 10.1109/ICECET58911.2023.10389394.

[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,” *2023 IEEE Conference*, pp. 1–6. [Exact conference title not specified; assumed based on authors and context.]

[5] A. Yeboah-Ofori and A. Hawsh, "Evil Twin Attacks on Smart Home IoT Devices for Visually Impaired Users," *2023 IEEE International Smart Cities Conference (ISC2)*, 2023, pp. 1–6. doi: 10.1109/ISC257844.2023.10293225.

[6] S. Kitisriworapan, A. Jansang, and A. Phonphoem, "Client-Side Rogue Access-Point Detection Using a Simple Walking Strategy and Round-Trip Time Analysis," *Journal of Wireless Communications and Networking*, vol. 2020, no. 252, 2020. doi: 10.1186/s13638-020-01864-5.

[7] 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. 14886–14900, Apr. 2024. doi: 10.1109/JIOT.2023.3345378.

[8] J. Laorungruang, The Internet Using Behavior and Learning Achievement: A Case Study: Rajamangala University of Technology Phra Nakhon Students, M.S. thesis, Information Technology Policy and Management, College of Innovation, Thammasat University, 2018.

**ภูธเนศ เมฆพยม**
จบการศึกษา วิศวกรรมศาสตรบัณฑิต(วิศวกรรมคอมพิวเตอร์) ปัจจุบันศึกษา วิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมไฟฟ้าสาขาย่อยคอมพิวเตอร์) มหาวิทยาลัยเทคโนโลยีมหานคร ปัจจุบันเป็นอาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์และปัญญาประดิษฐ์ สถาบันนวัตกรรมมหานครโดยดำรงตำแหน่งเป็นผู้ช่วยรองอธิการบิดีฝ่ายสภาบันนวัตกรรมมหานครฝ่ายกิจกรรมนักศึกษาและประชาสัมพันธ์

**ผู้ช่วยศาตราจารย์ ดร.ณัฐพงษ์ จันทร์แดง**
จบการศึกษาวิศวกรรมศาสตรบัณฑิต(วิศวกรรมคอมพิวเตอร์) วิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมไฟฟ้าสาขาย่อยคอมพิวเตอร์) และวิศวกรรมศาสตรดุษฎีบัณฑิต (วิศวกรรมไฟฟ้าสาขาย่อยคอมพิวเตอร์) มหาวิทยาลัยเทคโนโลยีมหานคร ปัจจุบันเป็นอาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์และปัญญาประดิษฐ์สถาบันนวัตกรรมมหานครโดยดำรงตำแหน่งเป็นหัวหน้าภาควิชา มีหัวข้องานวิจัยที่สนใจได้แก่การประมวลผลสัญญาณและภาพดิจิทัล (Signal and Image Processing) การรู้จำแบบ (PatternRecognition) การรู้จำภาพ (Image Recognition) และปัญญาประดิษฐ์ (Artificial Intelligence)