# การพัฒนาระบบเครือข่ายไร้สายขององค์กร เพื่อการใช้งานอุปกรณ์ไอโอทีกรณีศึกษา ระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่

# Development of Wireless Systems of Organizations for using IoT Devices Case Study : Chiang Mai University's Wireless Network

สัจจะ ตันจันทร์พงศ์[1]

Sajja Tanchanpong[1]

Received: 17 January 2019

Revised: 11 March 2019

Accepted: 18 April 2019

## บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์ (1) เพื่อพัฒนาระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่ให้รองรับการใช้งานอุปกรณ์ไอโอที (2) เพื่อศึกษาเสถียรภาพของระบบเครือข่ายไร้สายที่ได้พัฒนาขึ้น (3) เพื่อศึกษาความพึงพอใจของผู้ดูแลระบบไอทีของหน่วยงานต่อระบบเครือข่ายไร้สายที่ได้พัฒนาขึ้น กลุ่มตัวอย่างที่ใช้ในการวิจัย ได้แก่ ผู้ดูแลระบบไอทีของหน่วยงานต่างๆ จำนวน 21 คน เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล ได้แก่ แบบสอบถาม วิเคราะห์ข้อมูลโดยใช้ความถี่ ร้อยละ ค่าเฉลี่ย และค่าส่วนเบี่ยง

[1] วิศวกร ฝ่ายระบบเครือข่ายคอมพิวเตอร์ สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่, โทรศัพท์ 053-941780, E-mail : sajja.t@cmu.ac.th

[1] Engineer, Computer Network Division, Information Technology Service Center, Chiang Mai University, Telephone : 053-941780, E-mail : sajja.t@cmu.ac.th

เบนมาตรฐาน ผลการวิจัย พบว่า (1) ระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่จะต้องสร้างชื่อบริการ SSID ขึ้นใหม่ โดยใช้การเข้ารหัสความปลอดภัยแบบ WPA2-PSK ควบคู่กับการตรวจสอบ MAC Address ของอุปกรณ์ไอโอที และพัฒนาโปรแกรมบริหารจัดการอุปกรณ์ไอโอที เพื่อให้ผู้ดูแลระบบสามารถเพิ่มลบอุปกรณ์ไอโอทีได้ด้วยตนเอง (2) เสถียรภาพของระบบเครือข่ายไร้สายที่ได้พัฒนาขึ้นอยู่ในเกณฑ์ดี (ค่าเฉลี่ยร้อยละ 98.87) (3) ความพึงพอใจของผู้ดูแลระบบไอทีของหน่วยงานต่อระบบเครือข่ายไร้สายที่ได้พัฒนาขึ้นโดยรวมอยู่ในระดับพอใจมาก (ค่าเฉลี่ย 4.52)

**คำสำคัญ:** ระบบเครือข่ายไร้สาย, จัมโบ้พลัส, อุปกรณ์ไอโอที

## Abstract

This research has the following objectives: (1) Develop Chiang Mai University's wireless system for use with IoT devices. (2) To study the stability of the developed wireless network (3) To study the satisfaction of IT system administrators towards the developed wireless system. A survey, in the form of a questionnaire, was taken to collect data from 21 IT managers from different departments. Statistics, consisting of frequency, percentages, frequency, percentages, mean, and standard deviation were used in data analysis. The result shows that (1) Chiang Mai University's wireless system can be configured to make a new service SSID and use WPA2-PSK security encryption together with MAC Address filtering to authenticate access. A software system has also been developed allowing IT administrators to maintain a list of IoT devices connected to the network.. Stability of developed wireless network was good. (average 98.87 percent) (3) The overall satisfaction of IT system administrators towards the developed wireless network were "very satisfied" (average 4.52).

**Keywords:** wireless network, JumboPlus, IoT device.

## บทนำ

ปัจจุบันมหาวิทยาลัยเชียงใหม่ได้ให้บริการระบบเครือข่ายไร้สายแก่นักศึกษา บุคลากร และหน่วยงานต่างๆ ให้สามารถเชื่อมต่อกับระบบเครือข่ายของมหาวิทยาลัยด้วยเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์ไร้สายด้วยมาตรฐาน IEEE 802.11b IEEE 802.11g และ IEEE 802.11n หรือที่รู้จักกันในชื่อ Wi-Fi ภายใต้ชื่อการให้บริการ (SSID) ว่า “@JumboPlus” โดยมีอุปกรณ์กระจายสัญญาณ (Access Point) ให้บริการทั่วพื้นที่มหาวิทยาลัยทั้งสิ้นกว่า 5,100 จุด เพื่อสนับสนุนงานทางด้านการเรียนการสอน การวิจัย และการบริหารจัดการทรัพยากรของมหาวิทยาลัย (สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่, 2561)

แม้ว่าจะมีจุดให้บริการระบบเครือข่ายไร้สายมากมายครอบคลุมทั่วพื้นที่ของมหาวิทยาลัย ซึ่งหน่วยงานต่างๆ สามารถใช้โน๊ตบุ๊ค แท็บเล็ต หรือสมาร์ทโฟนเชื่อมต่อระบบเครือข่ายไร้สายได้ แต่เนื่องจากระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่เป็นระบบเครือข่ายไร้สายแบบองค์กรที่มีอุปกรณ์ควบคุมจากส่วนกลาง ซึ่งมีความเข้มงวดในการรักษาความปลอดภัยที่สูง และอาศัยวิธีการเข้ารหัสรักษาความปลอดภัยข้อมูลที่มีความซับซ้อนแบบ WPA2-Enterprise จนทำให้อุปกรณ์ไอโอทีไม่สามารถเข้าใช้งานได้ ซึ่งสอดคล้องกับงานวิจัยที่พบว่าอุปกรณ์ไอโอทีโดยส่วนใหญ่จะเชื่อมต่อกับระบบเครือข่ายไร้สายแบบใช้งานภายในบ้านที่มีการเข้ารหัสไม่ซับซ้อน และอุปกรณ์ไอโอทีเหล่านี้มักจะไม่มีคีย์บอร์ดหรือหน้าจอทำให้การเชื่อมต่อกับระบบเครือข่ายที่เข้ารหัสความปลอดภัยเป็นเรื่องยุ่งยาก (Philip Lundrigan, Sneha Kumar Kasera, Neal Patwari, 2018)

ทั้งนี้อุปกรณ์ไอโอที (IoT) หรือที่รู้จักว่า “Internet of Things” เป็นเครือข่ายของสิ่งที่เป็นตัวตนจับต้องได้ (“things”) เช่น อุปกรณ์ตรวจวัด (Sensors device) อุปกรณ์ควบคุม (Control device) อุปกรณ์คอมพิวเตอร์ขนาดเล็ก โทรทัศน์อัจฉริยะ (Smart TV) เป็นต้น ปัจจุบันอุปกรณ์ไอโอทีเหล่านี้มีแนวโน้มได้รับความนิยมในการใช้งานเพิ่มมากขึ้นเรื่อยๆ เนื่องจากสามารถใช้งานได้หลากหลาย มีประสิทธิภาพในการทำงานสูง (พนิตา พงษ์ไพบูลย์, 2560) ซึ่งสามารถสร้างประโยชน์และช่วยสนับสนุนงานด้านต่างๆ ที่สำคัญของมหาวิทยาลัยได้เป็นอย่างดี

ซึ่งหากอุปกรณ์ไอโอทีไม่สามารถเชื่อมต่อกับระบบเครือข่ายไร้สายของมหาวิทยาลัยได้ ก็จะทำให้มหาวิทยาลัยสูญเสียโอกาสในการนำอุปกรณ์ไอโอทีเหล่านี้มาสนับสนุนการใช้งานในด้านต่าง ๆ ของมหาวิทยาลัย

ดังนั้นผู้วิจัยจึงจะทำการพัฒนาระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่ให้รองรับการใช้งานอุปกรณ์ไอโอที โดยจะกำหนดชื่อบริการ Service Set Identifier (SSID) ของระบบเครือข่ายไร้สายขึ้นมาใหม่ ว่า “@JumboPlusIoT” โดยมุ่งเน้นที่อุปกรณ์ไอโอทีที่ช่วยสนับสนุนงานทางด้านการเรียนการสอน การวิจัยและการบริหารจัดการทรัพยากรของมหาวิทยาลัยในหน่วยงานต่าง ๆ ซึ่งอุปกรณ์ไอโอทีทั้งหมดเหล่านี้ดูแลรับผิดชอบโดยผู้ดูแลระบบไอทีของหน่วยงานต่าง ๆ ผู้วิจัยจึงจะได้ทำการศึกษาความพึงพอใจของผู้ดูแลระบบไอทีของหน่วยงานต่อระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่สำหรับอุปกรณ์ไอโอทีที่ได้พัฒนาขึ้นด้วย เพื่อนำผลการศึกษาวิจัยมาใช้ปรับปรุงพัฒนาระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่ให้มีบริการที่ดียิ่งขึ้นต่อไป

## วัตถุประสงค์การวิจัย

1. เพื่อพัฒนาระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่ให้รองรับการใช้งานอุปกรณ์ไอโอที
2. เพื่อศึกษาเสถียรภาพของระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่สำหรับอุปกรณ์ไอโอทีที่ได้พัฒนาขึ้น
3. เพื่อศึกษาความพึงพอใจของผู้ดูแลระบบไอทีของหน่วยงานต่อระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่สำหรับอุปกรณ์ไอโอทีที่ได้พัฒนาขึ้น

## วิธีการศึกษา

**ประชากรและกลุ่มเป้าหมาย**

ระบบเครือข่ายไร้สายสำหรับอุปกรณ์ไอโอทีของมหาวิทยาลัยเชียงใหม่ที่ได้รับการพัฒนาขึ้น คาดว่าจะเปิดให้บริการแก่หน่วยงานต่าง ๆ ภายในมหาวิทยาลัย เพื่อให้สามารถนำอุปกรณ์ไอโอทีมาใช้สนับสนุนการเรียนการสอน การวิจัยและการบริหารจัดการมหาวิทยาลัยได้ ซึ่งผู้ดูแลระบบไอทีของหน่วยงานต่าง ๆ จะเป็นผู้ดูแลรับผิดชอบจัดการอุปกรณ์ไอโอทีทั้งหมดของหน่วยงาน โดยปัจจุบันมหาวิทยาลัยเชียงใหม่มีหน่วยงานต่าง ๆ ที่สำคัญ ประกอบด้วย 21 คณะ 3 วิทยาลัย

1 บัณฑิตวิทยาลัย 5 สถาบัน 6 สำนัก และ 1 สำนักงานมหาวิทยาลัย รวมทั้งสิ้น 37 หน่วยงาน ซึ่งมีผู้ดูแลระบบไอทีของหน่วยงาน จำนวน 50 คน (มหาวิทยาลัยเชียงใหม่, 2561)

โดยกลุ่มตัวอย่างที่ศึกษาในครั้งนี้ คือ หน่วยงานที่เข้าร่วมโครงการทดสอบการใช้งานระบบเครือข่ายไร้สายสำหรับอุปกรณ์ไอโอที ประกอบไปด้วย คณะทันตแพทยศาสตร์ คณะบริหารธุรกิจ คณะพยาบาลศาสตร์ คณะแพทยศาสตร์ คณะเภสัชศาสตร์ คณะรัฐศาสตร์และรัฐประศาสนศาสตร์ คณะวิทยาศาสตร์ คณะวิศวกรรมศาสตร์ คณะศึกษาศาสตร์ คณะสถาปัตยกรรมศาสตร์ คณะสังคมศาสตร์ บัณฑิตวิทยาลัย วิทยาลัยศิลปะ สื่อ และเทคโนโลยี สถาบันวิจัยวิทยาศาสตร์และเทคโนโลยี สำนักงานมหาวิทยาลัย สำนักหอสมุด และสำนักบริการเทคโนโลยีสารสนเทศรวมทั้งสิ้น 17 หน่วยงาน ซึ่งมีผู้ดูแลระบบไอทีของหน่วยงาน จำนวน 21 คน และทำการทดสอบเสถียรภาพของระบบด้วยอุปกรณ์ไอโอที จำนวน 17 รายการ ได้แก่ เครื่องพิมพ์ ไมโครคอนโทรล์เลอร์ ESP-8266 สมาร์ททีวี ตู้ควบคุมอุณหภูมิทางการแพทย์ เซนเซอร์วัดอุณหภูมิ แท็บเล็ต แอปเปิ้ลทีวี โน๊ตบุ๊ค โครมแคส สมาร์ทวอทซ์ กล้องแบบไอพี คอมพิวเตอร์ราสเบอรี่พาย และสมาร์ทโฟน

## เครื่องมือที่ใช้ในการวิจัย

การศึกษาเสถียรภาพของระบบด้วยอุปกรณ์ไอโอที จะใช้โปรแกรม EMCO Ping Monitor version 6.2.1 ทำการ Ping เป็นระยะๆ ซึ่งจะเป็นการส่งข้อมูล ICMP ประเภท echo request ไปยังอุปกรณ์ไอโอที และรอคอยการตอบรับเป็นข้อมูล echo response ซึ่งโปรแกรมจะบันทึกผลว่าการส่งข้อมูลให้อุปกรณ์ไอโอทีในแต่ละครั้งส่งข้อมูลสำเร็จหรือไม่ (EMCO Software, 2018) ซึ่งจะใช้เกณฑ์การประเมินเสถียรภาพโดยนับจากร้อยละของผลสำเร็จในการตอบกลับ การศึกษาความพึงพอใจของผู้ดูแลระบบไอทีของหน่วยงานจะใช้แบบสอบถาม จำนวน 5 ข้อ ได้แก่ ชื่อคณะหรือส่วนงาน ความพึงพอใจต่อโปรแกรมบริหารจัดการอุปกรณ์ไอโอที ความพึงพอใจต่อระบบเครือข่ายไร้สาย ปัญหาที่พบ และข้อเสนอแนะ โดยคำถามที่เป็นหัวข้อการประเมินความพึงพอใจ จะใช้เกณฑ์การประเมินความพึงพอใจ 5 ระดับ คือ พอใจมาก พอใจ เฉยๆ ไม่พอใจ และไม่พอใจมาก คำถามที่เป็นหัวข้อปัญหาที่

พบและข้อเสนอแนะ จะเป็นคำถามแบบปลายเปิด

## การเก็บรวบรวมข้อมูล

ประสานงานขอความร่วมมือกับผู้ดูแลระบบไอทีของหน่วยงานต่างๆ ให้เข้าร่วมโครงการและทดลองใช้งานระบบเครือข่ายไร้สายสำหรับอุปกรณ์ไอโอทีเป็นระยะเวลา 1 เดือน

คัดเลือกอุปกรณ์ไอโอทีจำนวน 17 รายการ มาทดสอบการเชื่อมต่อและวัดผลเสถียรภาพการใช้งานของอุปกรณ์ไอโอทีกับระบบเครือข่ายไร้สายด้วยวิธีการ Ping ทุกๆ 5 วินาที เป็นระยะเวลา 1 ชั่วโมง

จัดส่งแบบสอบถามให้แก่ผู้ดูแลระบบไอทีของหน่วยงานต่างๆ ที่ได้ทดลองใช้งาน จำนวน 21 คน เพื่อสอบถามความพึงพอใจต่อระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่สำหรับอุปกรณ์ไอโอทีที่ได้พัฒนาขึ้น และนำผลการประเมินความพึงพอใจไปวิเคราะห์ผลต่อไป

## การวิเคราะห์ข้อมูล

ในการวิเคราะห์ข้อมูลผู้วิจัยดำเนินการวิเคราะห์ข้อมูลดังนี้

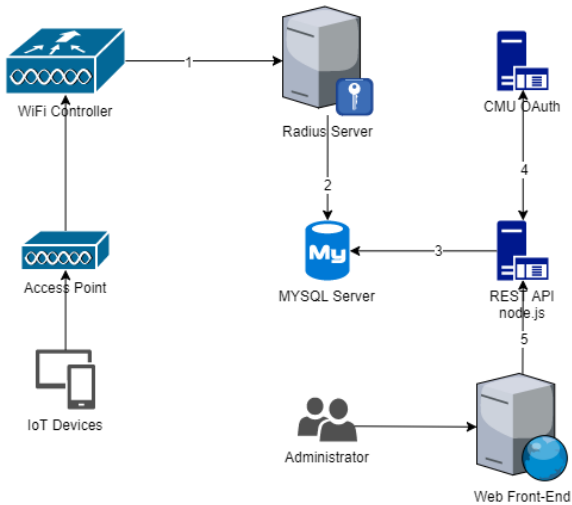
การวิเคราะห์เสถียรภาพของระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่สำหรับอุปกรณ์ไอโอที จะใช้สถิติวิเคราะห์พื้นฐาน ได้แก่ ความถี่ (Frequency) และร้อยละ (Percentage) ซึ่งร้อยละของผลสำเร็จในการตอบกลับจะถูกประเมินเป็นระดับ จำนวน 5 ระดับ คือ 100-99.99% =ดีเยี่ยม 99.98-99.00%=ดีมาก 98.99-95.00%=ดี 94.99-90.00%=พอใช้ 89.99-0%=ต้องปรับปรุง (Network Dynamics Pty Ltd., 2018)

การวิเคราะห์ประเมินความพึงพอใจของผู้ดูแลระบบไอทีของหน่วยงานต่อระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่สำหรับอุปกรณ์ไอโอที จะใช้สถิติวิเคราะห์พื้นฐาน ได้แก่ ค่าเฉลี่ย (Mean) ค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) และมาตราส่วนประมาณค่า (Rating Scale) จำนวน 5 ระดับ (บุญชม ศรีสะอาด, 2556: 82-83, 121)

## ผลการศึกษา

ผลการพัฒนาระบบเครือข่ายไร้สายของของมหาวิทยาลัยเชียงใหม่ เพื่อให้รองรับอุปกรณ์ไอโอทีได้ มหาวิทยาลัยเชียงใหม่ได้เพิ่มชื่อบริการ SSID ใหม่ว่า @JumboPlusIoT โดยมีการเข้ารหัสความปลอดภัยแบบ WPA2-PSK และการตรวจสอบตัวตนด้วยการระบุ MAC Address ของอุปกรณ์ไอโอที ซึ่งเป็นการรวมเอาวิธีการรักษาความปลอดภัยทั้งสองรูปแบบนี้มาประกอบใช้งานร่วมกัน พร้อมทั้งมีโปรแกรมบริหารจัดการอุปกรณ์ไอโอทีด้วย ซึ่งมีโครงสร้างการทำงานของระบบดังต่อไปนี้

ส่วนประกอบที่สำคัญของระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่สำหรับอุปกรณ์ไอโอที ประกอบด้วยอุปกรณ์ควบคุมระบบเครือข่ายไร้สาย (WiFi Controller) เครื่องคอมพิวเตอร์แม่ข่ายตรวจสอบพิสูจน์ตัวตน (Radius Server) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูลที่จัดเก็บ MAC Address (MySQL Server) ระบบยืนยันตัวตนแบบเปิดของมหาวิทยาลัยเชียงใหม่ (CMU OAuth) และโปรแกรมบริหารจัดการไอโอทีสำหรับผู้ดูแลระบบ (Web Front-End) ดังภาพประกอบ 1




**ภาพประกอบ 1** โครงสร้างการทำงานระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่สำหรับอุปกรณ์ไอโอที

หลักการที่สำคัญจะเริ่มจากการปรับแก้ไขอุปกรณ์ควบคุมระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่ (WiFi Controller) ให้ปล่อยชื่อบริการ SSID ชื่อว่า @JumboPlusIoT โดยกำหนดให้มีการเข้ารหัสความปลอดภัยแบบ WPA2-PSK และเปิดใช้การตรวจสอบตัวตนแบบ MAC Filtering ไปยังเครื่องคอมพิวเตอร์แม่ข่าย Radius Server ซึ่ง WiFi Controller จะทำการตรวจสอบหมายเลขประจำตัว MAC Address ของอุปกรณ์ไอโอที (IoT Devices) ที่จะมาเชื่อมต่อสัญญาณกับระบบเครือข่ายไร้สาย โดยจะอ้างอิงไปยังฐานข้อมูลของ MAC Address เป็นตัวตรวจสอบผ่าน RADIUS Protocol ซึ่งอุปกรณ์ WiFi Controller จะทำการแปลงค่า MAC Address เป็นตัวอักษรตัวพิมพ์เล็กทั้งหมด แล้วตัดอักขระพิเศษออกสร้างเป็น Datagram RADIUS Access-Request โดยใช้ MAC Address เป็นค่าในส่วนของข้อมูลชื่อผู้ใช้ Attribute User-Name และรหัสผ่านผู้ใช้ User-Password เช่น MAC Address 54-60-09-b9-6a-14 จะได้เป็น Access-Request { User-Name : 546009b96a14, User-Password : 546009b96a14 } ซึ่งถ้าตรวจสอบข้อมูล User-Name และ User-Password ถูกต้อง เครื่องคอมพิวเตอร์แม่ข่าย RADIUS Server ก็จะตอบอนุญาตให้เข้าใช้งาน Access-Accept กลับมายัง WiFi Controller ซึ่งอุปกรณ์ WiFi Controller ก็จะอนุญาตให้อุปกรณ์ไอโอทีเข้าร่วมเครือข่ายได้ แต่ถ้าตรวจสอบไม่เจอ User-Name หรือ User-Name และ User-Password ไม่ถูกต้อง เครื่องคอมพิวเตอร์แม่ข่าย RADIUS Server ก็จะตอบปฏิเสธไม่ให้เข้าใช้งาน Access-Reject กลับมา WiFi Controller ซึ่งอุปกรณ์ WiFi Controller ก็จะปฏิเสธอุปกรณ์ไอโอทีนั้นไม่ให้เข้าใช้งานเครือข่ายไร้สายต่อไป

การจัดการรายชื่ออุปกรณ์ไอโอทีที่จะอนุญาตให้เข้าใช้งานระบบเครือข่ายไร้สายนั้น จะถูกจัดเก็บเลขหมายเลขประจำตัวเครื่อง MAC Address ของอุปกรณ์ไอโอทีไว้บนฐานข้อมูล MySQL ที่ฐานข้อมูลกลาง ซึ่งเชื่อมต่อกับเครื่องคอมพิวเตอร์แม่ข่าย RADIUS Server โดยจะทำการพัฒนา Web Application เป็นโปรแกรมสำหรับบริหารจัดการรายชื่ออุปกรณ์ไอโอทีโดยผู้ดูแลระบบ (Admin User) ซึ่งสามารถทำการเพิ่มลบระเบียนบนฐานข้อมูลของอุปกรณ์ไอโอทีได้ โดยอาศัยการพัฒนา REST API ขึ้นมาด้วย node.js เพื่อใช้ในการเรียกการเพิ่ม และการลบ MAC Address บน

ฐานข้อมูล MYSQL โดยมี Url คือ https://mac-auth-reg-api.cmu.ac.th และมี Endpoint ชื่อ GET เพื่อใช้ในการเรียกข้อมูล POST เพื่อใช้ในการเพิ่มข้อมูล และ DELETE เพื่อใช้ในการลบข้อมูล

การพัฒนาระบบตรวจสอบและรักษาความปลอดภัยให้กับส่วนของการบริหารจัดการอุปกรณ์ไอโอที ผู้ดูแลระบบ (Admin User) ที่จะสามารถใช้งาน API ได้จะต้องได้รับสิทธิ์ก่อน โดยจะทำการเพิ่มบัญชี CMU IT Account ที่มีรูปแบบเป็น username@cmu.ac.th ของผู้ดูแลระบบเข้าไปในระบบก่อน จากนั้นผู้ดูแลระบบก็จะสามารถเข้าสู่ระบบด้วย CMU IT Account ผ่าน Protocol OAuth ของ CMU OAuth เพื่อขอโทเคนการอนุญาตให้เข้าถึง (Access Token) สำหรับการใช้งาน REST API โดยต้องแนบ Access Token ใน Authorization Header เป็นชนิด Bearer ทุกครั้งในการเรียกใช้งาน End point ทั้งนี้ในส่วนติดต่อกับผู้ใช้ (Front-end user interface) สำหรับใช้งาน REST API นั้น เพื่อให้ผู้ใช้งานไม่ต้องเขียนโปรแกรมในการติดต่อ API เอง ก็จะใช้ Web Application ที่พัฒนาขึ้นบนเว็บไซต์ https://mac-auth-reg.cmu.ac.th โดยผู้ดูแลระบบสามารถเข้าสู่ระบบ เพื่อเพิ่มลบรายชื่ออุปกรณ์ไอโอทีที่อยู่ในความดูแลของตนเองได้ทั้งหมด ผู้ดูแลระบบไอทีของหน่วยงานสามารถนำอุปกรณ์ไอโอทีมาเชื่อมต่อกับระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่ @JumboPlusIoT ได้ โดยการเพิ่มรายชื่ออุปกรณ์ไอโอทีนั้น ด้วยการระบุ MAC Address ของอุปกรณ์ไอโอทีลงในโปรแกรมบริหารจัดการอุปกรณ์ไอโอที และตั้งค่าของอุปกรณ์ไอโอทีให้เชื่อมต่อกับระบบเครือข่ายไร้สาย @Jumbo PlusIoT ด้วยการเข้ารหัสแบบ WPA2-PSK ตามรหัสผ่านที่มหาวิทยาลัยกำหนด จำนวน 8 ตัวอักษร ซึ่งอุปกรณ์ไอโอทีก็จะสามารถเชื่อมต่อและใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายไร้สายของมหาวิทยาลัยได้ทันที

ผลการศึกษาเสถียรภาพของระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่สำหรับอุปกรณ์ไอโอทีที่ได้พัฒนาขึ้น โดยการนำอุปกรณ์ไอโอทีมาทดสอบ จำนวน 17 รายการ ได้แก่ เครื่องพิมพ์ ไมโครคอนโทรล์เลอร์ ESP-8266 สมาร์ททีวี ตู้ควบคุมอุณหภูมิทางการแพทย์ เซนเซอร์วัดอุณหภูมิ แท็บเล็ต แอปเปิ้ลทีวี โน๊ตบุ๊ค โครมแคส สมาร์ทวอทซ์ กล้องแบบไอพี คอมพิวเตอร์ราสเบอรี่พาย และสมาร์ทโฟน พบว่า อุปกรณ์ไอโอทีทั้งหมดสามารถเชื่อมต่อเข้ากับระบบเครือข่ายไร้สาย @

JumboPlusIoT ได้ และเมื่อทดสอบเสถียรภาพการใช้งานของระบบ ด้วยการ Ping ไปยังอุปกรณ์ไอโอทีด้วยโปรแกรม EMCO Ping Monitor version 6.2.1 เป็นระยะๆ ทุกๆ 5 วินาที เป็นระยะเวลา 1 ชั่วโมง ได้ผลการการวิเคราะห์และข้อสรุปดังตารางที่ 1

**ตารางที่ 1** ผลการทดสอบเสถียรภาพของอุปกรณ์ไอโอทีกับระบบเครือข่ายไร้สาย @JumboPlusIoT

| ผลการทดสอบเสถียรภาพของระบบ | จำนวน (ครั้ง) | ร้อยละ | แปลผล |
|---|---|---|---|
| การตอบกลับของ Ping | 12,102 | 98.87 | ดี |
| การไม่ตอบกลับของ Ping | 138 | 1.13 | |

**หมายเหตุ:** 100-99.99%=ดีเยี่ยม 99.98-99.00%=ดีมาก 98.99-95.00%=ดี 94.99-90.00%=พอใช้ 89.99-0% ต้องปรับปรุง

จากตารางที่ 1 พบว่าอุปกรณ์ไอโอทีทั้งหมดสามารถเชื่อมต่อเข้ากับระบบเครือข่ายไร้สาย @JumboPlusIoT ได้อย่างมีเสถียรภาพ อยู่ในเกณฑ์ที่ดี โดยจะมีค่าการตอบกลับของคำสั่ง Ping ที่สำเร็จของอุปกรณ์ไอโอทีทั้งหมดอยู่ที่ 12,102 ครั้ง เป็นร้อยละ 98.87 และไม่ตอบกลับของคำสั่ง Ping มีผลรวมอยู่ที่ 138 ครั้ง เป็นร้อยละ 1.13

ผลการศึกษาความพึงพอใจของผู้ดูแลระบบไอทีของหน่วยงานต่อระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่สำหรับอุปกรณ์ไอโอทีที่ได้พัฒนาขึ้น ซึ่งหลังจากพัฒนาระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่ให้สามารถรองรับการเชื่อมต่ออุปกรณ์ไอโอทีได้แล้วนั้น ได้ทำการทดสอบระบบโดยผู้ดูแลระบบไอทีของหน่วยงานต่างๆ ภายในมหาวิทยาลัยเชียงใหม่ จำนวน 21 คน ทดลองใช้งานเป็นระยะเวลา 1 เดือน และภายหลังที่ครบกำหนดการทดลองใช้งานแล้ว ก็ได้จัดส่งแบบสอบถามให้แก่ผู้ดูแลระบบไอทีของหน่วยงานที่เข้าร่วมโครงการทดสอบทั้งหมด เพื่อประเมินความพึงพอใจต่อการใช้โปรแกรมบริหารจัดการอุปกรณ์ไอโอที และความพึงพอใจต่อการให้บริการระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่สำหรับอุปกรณ์ไอโอทีที่ได้พัฒนาขึ้น ซึ่งได้ผลการประเมินความพึงพอใจดังตารางต่อไปนี้

**ตารางที่ 2** แสดงค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และระดับความพึงพอใจต่อโปรแกรมบริหารจัดการ

| โปรแกรมบริหารจัดการอุปกรณ์ไอโอที | ค่าเฉลี่ย | ส่วนเบี่ยงเบนมาตรฐาน | แปลผล |
|---|---|---|---|
| ระบบตรงตามความต้องการของผู้ใช้งาน | 4.52 | 0.512 | พอใจมาก |
| ความสวยงามของการออกแบบหน้าจอ | 3.90 | 0.700 | พอใจ |
| การเพิ่มลบอุปกรณ์ไอโอทีทำได้สะดวก | 4.48 | 0.680 | พอใจ |
| การรักษาความปลอดภัยของระบบ | 4.48 | 0.680 | พอใจ |
| ความพึงพอใจต่อการใช้งานโดยรวม | 4.43 | 0.598 | พอใจ |

**หมายเหตุ:** 4.50-5.00=พอใจมาก 3.50-4.49=พอใจ 2.50-3.49=เฉยๆ 1.50-2.49=ไม่พอใจ 1.00-1.49=ไม่พอใจมาก

จากตารางที่ 2 พบว่าผู้ตอบแบบสอบถาม ซึ่งเป็นผู้ดูแลระบบไอทีของหน่วยงานต่างๆ จำนวนทั้งสิ้น 21 ราย ผู้ตอบแบบสอบถามมีความพึงพอใจต่อโปรแกรมบริหารจัดการอุปกรณ์ไอโอทีในด้านที่ระบบตรงตามความต้องการของผู้ใช้งานอยู่ในระดับพอใจมาก (ค่าเฉลี่ย 4.52) ความสวยงามของการออกแบบหน้าจออยู่ในระดับพอใจ (ค่าเฉลี่ย 3.90) การเพิ่มลบอุปกรณ์ไอโอทีทำได้สะดวกอยู่ในระดับพอใจ (ค่าเฉลี่ย 4.48) การรักษาความปลอดภัยของระบบอยู่ในระดับพอใจ (ค่าเฉลี่ย 4.48) และความพึงพอใจต่อการใช้งานโดยรวมอยู่ในระดับพอใจ (ค่าเฉลี่ย 4.43)

**ตารางที่ 3** แสดงค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และระดับความพึงพอใจต่อระบบเครือข่ายไร้สาย

| ระบบเครือข่ายไร้สาย @JumboPlusIoT | ค่าเฉลี่ย | ส่วนเบี่ยงเบนมาตรฐาน | แปลผล |
|---|---|---|---|
| ความครอบคลุมของพื้นที่ให้บริการ | 4.19 | 0.750 | พอใจ |
| ความสะดวกต่อการใช้งาน | 4.48 | 0.680 | พอใจ |
| ความเร็วของการเชื่อมต่ออินเทอร์เน็ต | 4.43 | 0.598 | พอใจ |
| เสถียรภาพของการใช้งาน | 4.14 | 0.910 | พอใจ |
| การรักษาความปลอดภัยของระบบ | 4.38 | 0.740 | พอใจ |
| ความพึงพอใจต่อการใช้งานโดยรวม | 4.52 | 0.512 | พอใจมาก |

**หมายเหตุ:** 4.50-5.00=พอใจมาก 3.50-4.49=พอใจ 2.50-3.49=เฉยๆ 1.50-2.49=ไม่พอใจ 1.00-1.49=ไม่พอใจมาก

จากตารางที่ 3 พบว่าผู้ตอบแบบสอบถาม ซึ่งเป็นผู้ดูแลระบบไอทีของหน่วยงานต่างๆ จำนวนทั้งสิ้น 21 ราย ผู้ตอบแบบสอบถามมีความพึงพอใจต่อการให้บริการระบบเครือข่ายไร้สาย @JumboPlusIoT ในด้านความครอบคลุมของพื้นที่ให้บริการอยู่ในระดับพอใจ (ค่าเฉลี่ย 4.19) ความสะดวกต่อการใช้งานอยู่ในระดับพอใจ (ค่าเฉลี่ย 4.48) ความเร็วของการเชื่อมต่ออินเทอร์เน็ตอยู่ในระดับพอใจ (ค่าเฉลี่ย 4.43) เสถียรภาพของการใช้งานอยู่ในระดับพอใจ (ค่าเฉลี่ย 4.14) การรักษาความปลอดภัยของระบบอยู่ในระดับพอใจ (ค่าเฉลี่ย 4.38) และความพึงพอใจต่อการใช้งานโดยรวมอยู่ในระดับพอใจมาก (ค่าเฉลี่ย 4.52)

## อภิปรายผล

การพัฒนาระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่ให้รองรับการใช้งานของอุปกรณ์ไอโอที ได้สร้างชื่อบริการ SSID ใหม่ว่า @JumboPlusIoT โดยมีการเข้ารหัสความปลอดภัยแบบ WPA2-PSK และการตรวจสอบตัวตนโดยใช้วิธีการระบุ MAC Address ของอุปกรณ์ไอโอที เป็นการรวมเอาวิธีการรักษาความปลอดภัยทั้งสองรูปแบบนี้มาประกอบใช้งานร่วมกัน พร้อมทั้งมีโปรแกรมบริหารจัดการอุปกรณ์ไอโอทีด้วย เป็นรูปแบบการใช้งานระบบเครือข่ายไร้สายขององค์กรแบบหนึ่งที่สามารถรองรับการใช้งานของอุปกรณ์ไอโอทีได้อย่างมีเสถียรภาพ ซึ่งสอดคล้องกับบทความ

แนะนำการเตรียมระบบเครือข่ายของมหาวิทยาลัยให้พร้อมสำหรับอุปกรณ์ไอโอที โดยแนะนำให้ใช้การตรวจสอบ MAC Address ร่วมกับ WPA2-PSK เช่นเดียวกัน (Joel Snyder, 2018)

การศึกษาเสถียรภาพของระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่สำหรับอุปกรณ์ไอโอทีที่ได้พัฒนาขึ้น เมื่อทดสอบการใช้งานกับอุปกรณ์ไอโอที จำนวนทั้งสิ้น 17 รายการ โดยเมื่อทดสอบด้วยวิธีการ Ping ทุกๆ 5 วินาที เป็นระยะเวลา 1 ชั่วโมง อุปกรณ์ไอโอทีทั้งหมดมีค่าเฉลี่ยการตอบสนองด้วยวิธีการ Ping อยู่ที่ร้อยละ 98.87 ไม่ตอบโดยเฉลี่ยร้อยละ 1.13 ซึ่งแสดงให้เห็นว่าอุปกรณ์ไอโอทีทั้งหมดสามารถเชื่อมต่อเข้ากับระบบเครือข่ายไร้สายสำหรับอุปกรณ์ไอโอทีได้อย่างมีเสถียรภาพอยู่ในเกณฑ์ที่ดี และมีความพร้อมในการเปิดให้บริการแก่หน่วยงานต่างๆ ภายในมหาวิทยาลัยเชียงใหม่อย่างเป็นทางการต่อไป

การศึกษาความพึงพอใจของผู้ดูแลระบบไอทีของหน่วยงานต่อระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่สำหรับอุปกรณ์ไอโอทีที่ได้พัฒนาขึ้น โดยเมื่อประเมินความพึงพอใจของผู้ดูแลระบบไอทีของหน่วยงานต่างๆ ที่ได้ทำการทดลองใช้งานระบบเป็นระยะเวลา 1 เดือน จำนวนทั้งสิ้น 21 คน พบว่า ความพึงพอใจต่อโปรแกรมบริหารจัดการอุปกรณ์ไอโอทีโดยรวมอยู่ในระดับพอใจ และความพึงพอใจต่อการให้บริการระบบเครือข่ายไร้สายโดยรวมอยู่ในระดับพอใจมาก ซึ่งจะเห็นว่าได้ว่าระบบเครือข่ายไร้สายใหม่นี้มีความพร้อมในการขยายผลการใช้งานไปยังผู้ดูแลระบบไอทีของหน่วยงานอื่นๆ ที่ยังไม่เคยได้ทดลองใช้ และสามารถเปิดให้บริการอย่างเป็นทางการต่อไป

## ข้อเสนอแนะ

### ข้อเสนอแนะในการนำผลการวิจัยไปใช้

ผลการวิจัยที่ได้จากการพัฒนาระบบเครือข่ายไร้สายของมหาวิทยาลัยเชียงใหม่สำหรับอุปกรณ์ไอโอทีที่ได้พัฒนาขึ้น ระบบเครือข่ายไร้สายดังกล่าวมีเสถียรภาพที่ดี และเป็นที่พึงพอใจของผู้ดูแลระบบไอทีของหน่วยงานต่างๆ ซึ่งมหาวิทยาลัยสามารถนำไปใช้งานได้จริงและเปิดให้บริการแก่หน่วยงานต่างๆ เพื่อจะได้นำอุปกรณ์ไอโอทีมาใช้สนับสนุนการเรียนการสอน การวิจัย และการบริหารจัดการทรัพยากรของมหาวิทยาลัยต่อไป

ข้อระมัดระวังของการใช้งานการเข้ารหัสแบบ WPA2-PSK ซึ่งเป็น Static Key และใช้รหัสแบบคงที่กับทุกอุปกรณ์ไอโอที อาจจะถูกสุ่มเดาด้วยโปรแกรมเจาะระบบได้โดยง่าย หรือ อาจมีเจ้าหน้าที่ดูแลระบบไอทีของหน่วยงานที่ทราบรหัสผ่าน นำรหัสผ่านดังกล่าวไปเปิดเผยต่อผู้ที่ไม่มีสิทธิ์ให้ทราบ จึงควรจำกัดกลุ่มผู้ใช้งานในวงแคบเฉพาะในกลุ่มของผู้ดูแลระบบไอทีของหน่วยงาน โดยไม่ควรเปิดเผยหรืออนุญาตให้กับผู้ใช้งานทั่วไป

ข้อระมัดระวังของการใช้ MAC Address Filter ซึ่งหากมีผู้ที่ทราบว่ามี MAC Address ใดที่สามารถเข้าใช้งานระบบเครือข่ายไร้สายได้ ก็อาจจะอาศัยโปรแกรมปลอมแปลงเป็น MAC Address ที่ได้รับสิทธิ์เข้าใช้งานได้ จึงควรจำกัดให้เฉพาะอุปกรณ์ไอโอทีเข้าใช้งานเท่านั้น โดยไม่อนุญาตให้นำโน๊ตบุ๊คหรือสมาร์ทโฟนมาใช้กับระบบเครือข่ายไร้สายของอุปกรณ์ไอโอทีนี้

**ข้อเสนอแนะในการทำวิจัยครั้งต่อไป**

ในการวิจัยครั้งต่อไปอาจพัฒนาให้โปรแกรมบริหารจัดการไอโอทีมีการแจ้งหมายเลขไอพี (IP) ของอุปกรณ์ไอโอทีให้ทราบในโปรแกรมด้วย ซึ่งจะช่วยให้การบริหารจัดการอุปกรณ์ไอโอทีของผู้ดูแลระบบทำได้ง่ายยิ่งขึ้น โดยอาจค้นหาจากอุปกรณ์ควบคุมระบบเครือข่ายไร้สาย ซึ่งจะมีข้อมูลทั้งหมดของอุปกรณ์ไอโอทีที่เชื่อมต่อกับระบบ หรือจากเครื่องคอมพิวเตอร์แม่ข่าย DHCP ซึ่งทำหน้าที่แจกหมายเลขไอพีให้แก่อุปกรณ์ไอโอทีที่เชื่อมต่อกับระบบ

จากข้อระมัดระวังของการใช้ MAC Address Filter เพื่อใช้เป็นข้อมูลในการกำหนดสิทธิ์เข้าใช้งานให้แก่อุปกรณ์ไอโอที ในการวิจัยครั้งต่อไป หากพัฒนาต่อยอดให้ระบบสามารถตรวจสอบข้อมูลชนิดอื่นๆ ของอุปกรณ์ไอโอทีก่อนการเข้าใช้งานได้ ก็จะช่วยเพิ่มความปลอดภัยให้กับระบบเครือข่ายไร้สายได้ดียิ่งขึ้น

## กิตติกรรมประกาศ

ผู้วิจัยขอขอบคุณสำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่ ภายใต้โครงการรับทุนอุดหนุนการวิจัยประจำปีงบประมาณ พ.ศ.2561 และทุกท่านที่มีส่วนเกี่ยวข้องที่ช่วยเหลือให้งานวิจัยฉบับนี้สำเร็จลุล่วงด้วยดี

## เอกสารอ้างอิง

บุญชม ศรีสะอาด (2556). *การวิจัยเบื้องต้น* พิมพ์ครั้งที่ 9. กรุงเทพฯ: สำนักพิมพ์สุวีริยาสาส์น.

พนิตา พงษ์ไพบูลย์ (2560). *คอลัมน์ทันกระแส IoT*. หนังสือพิมพ์โพสต์ทูเดย์ ฉบับวันที่ 5 มกราคม 2560.

มหาวิทยาลัยเชียงใหม่ (2561). *คณะและหน่วยงาน*. [ออนไลน์]. ได้จาก: https://www.cmu.ac.th [สืบค้นเมื่อ วันที่ 8 ธันวาคม 2561].

สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่. (2561). *เครือข่ายไร้สายมหาวิทยาลัยเชียงใหม่ Jumbo Ne*t. [ออนไลน์]. ได้จาก: https://jumbo.cmu.ac.th/ [สืบค้นเมื่อ วันที่ 17 เมษายน 2561].

EMCO Software (2018). *EMCO Ping Monitor version 6.2.1.* [Online]. Available from: https://emcosoftware.com/ping-monitor [accessed 8 December 2018].

Joel Snyder (2018). *Prep Your Campus Network for Internet of Things Devices.* [Online]. Available from: https://edtechmagazine.com/higher/article/2018/03/prep-your-campus-network-internet-things-devices [accessed 8 December 2018].

Network Dynamics Pty Ltd (2018). *Service Level Agreement (SLA)*. [Online]. Available from: https://networkdynamics.com.au/legals/sla/ [accessed 8 December 2018].

Philip Lundrigan, Sneha Kumar Kasera, Neal Patwari (2018). *STRAP: Secure TRansfer of Association Protocol.* School of Computing Department of Electrical and Computer Engineering University of Utah.