โครงงานเลขที่ วศ.คพ. P810-2/2565

เรื่อง

การคุ้มครองความเป็นส่วนตัวของไอโอทีจากผู้สังเกตการณ์เครือข่ายแบบพาสซีฟ

โดย

นายไตรภพ ศรีมณี 620610788

นายวราดร ศิริพันธุ์ 620612163

โครงงานนี้
เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตร์บัณฑิต
ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเชียงใหม่
ปีการศึกษา 2565

PROJECT No. CPE S810-1/65

IoT Privacy Protection against Passive Network Observer

Traiphob Srimanee 620610788

Waradorn Siripunt 620612163

A Project Submitted in Partial Fulfillment of Requirements

for the Degree of Bachelor of Engineering

Department of Computer Engineering

Faculty of Engineering

Chiang Mai University

2022

หัวข้อโครงงาน : การคุ้มครองความเป็นส่วนตัวของไอโอทีจากผู้สังเกตการณ์เครือข่ายแบบพาสซีฟ
: IoT Privacy Protection against Passive Network Observer
โดย : นายไตรภพ ศรีมณี รหัส 620610788
นายวราดร ศิริพันธุ์ รหัส 620612163
ภาควิชา : วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษา : ผศ.ดร.กำพล วรดิษฐ์
ปริญญา : วิศวกรรมศาสตร์บัณฑิต
สาขา : วิศวกรรมคอมพิวเตอร์
ปีการศึกษา : 2565

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเชียงใหม่ ได้อนุมัติให้โครงงานนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตร์บัณฑิต (สาขาวิศวกรรมคอมพิวเตอร์)

..... หัวหน้าภาควิชาวิศวกรรมคอมพิวเตอร์
(รศ.ดร. สันติ พิทักษ์กิจนุกูร)

คณะกรรมการสอบโครงงาน

..... ประธานกรรมการ
(ผศ.ดร.กำพล วรดิษฐ์)

..... กรรมการ
(อ.ดร.ณัฐนันท์ พรหมสุข)

..... กรรมการ
(ผศ.ดร.ยุทธพงษ์ สมจิต)

หัวข้อโครงงาน	: การคุ้มครองความเป็นส่วนตัวของไอโอทีจากผู้สังเกตการณ์เครือข่ายแบบพาสซีฟ
	: IoT Privacy Protection against Passive Network Observer
โดย	: นายไตรภพ ศรีมณี รหัส 620610788
	นายวราดร ศิริพันธุ์ รหัส 620612163
ภาควิชา	: วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษา	: ผศ.ดร.กำพล วรดิษฐ์
ปริญญา	: วิศวกรรมศาสตร์บัณฑิต
สาขา	: วิศวกรรมคอมพิวเตอร์
ปีการศึกษา	: 2565

บทคัดย่อ

โครงการนี้มุ่งเน้นในการพัฒนาระบบที่ช่วยป้องกันความเป็นส่วนตัวของผู้ใช้อุปกรณ์ไอโอที โดยการใช้ Raspberry Pi ในการบันทึกข้อมูลและส่งข้อมูลไปยังเซิร์ฟเวอร์ที่มีการอำพรางข้อมูลด้วย Better Efficiency Traffic Padding (BeTP) และการคัดกรองข้อมูลทราฟฟิกจริง โดยโปรแกรมที่พัฒนาขึ้นจะมีสองส่วน คือ ส่วนภายใน (Internal Module) และส่วนภายนอก (External Module) เพื่อเพิ่มความปลอดภัยในการใช้งาน โดยมีผลกระทบทั้งด้านสังคม สุขภาพ ความปลอดภัย กฎหมาย และวัฒนธรรม โดยผู้ใช้งานจะได้รับความสะดวกสบายในการใช้งานอุปกรณ์ไอโอทีอย่างปลอดภัยและเป็นส่วนตัว โครงการนี้เป็นการนำเสนอแนวคิดใหม่ๆในการป้องกันความเป็นส่วนตัวของผู้ใช้งานอุปกรณ์ไอโอที และอาจเป็นแนวทางในการพัฒนาระบบความปลอดภัยสำหรับอุปกรณ์ไอโอทีในอนาคต

Project Title	: IoT Privacy Protection against Passive Network Observer
Name	: Traiphob Srimanee 620610788
	Warardorn Siripunt 620612163
Project Title	: IoT Privacy Protection against Passive Network Observer
Department	: Computer Engineering
Project Advisor	: Asst. Prof. Kampol Woradit, Ph.D.
Degree	: Bachelor of Engineering
Academic Year	: 2022

ABSTRACT

This project aims to develop a system that helps protect the privacy of users of IoT devices. The system uses a Raspberry Pi to record and send data to a server that applies Better Efficiency Traffic Padding (BeTP) to obfuscate the data during transit, as well as filter out any fake traffic. The program is divided into two modules: the Internal Module and External Module, which increase security when using the IoT device.

The impact of this project is wide-ranging, affecting social, health, legal, and cultural aspects. Users will benefit from the convenience of using their IoT device with privacy and security assured. This project represents a new approach to protecting user privacy on IoT devices and may serve as a blueprint for future security systems for IoT devices.

This project represents a significant step towards the development of secure and private IoT devices, and it is hoped that it will inspire further research and development in this area.

กิตติกรรมประกาศ

โครงการพัฒนาโปรแกรมเพื่องานการพัฒนาด้านวิทยาศาสตร์และเทคโนโลยี “การคุ้มครองความเป็นส่วนตัวของไอโอทีจากผู้สังเกตการณ์เครือข่ายแบบพาสซีฟ” โครงงานเลขที่ วศ.คพ. P810-2/2565 จะไม่สามารถประสบความสำเร็จได้โดยที่ไม่ได้รับความกรุณาจากอาจารย์ที่ปรึกษาโครงการ ผศ.ดร.กำพล วรดิษฐ์ พร้อมทั้ง ผศ.ดร.ยุทธพงษ์ สมจิต และ อ.ดร.ณัฐนันท์ พรหมสุข ผู้ที่มีประสบกรณ์และความรู้ในการดูแลและสนับสนุนโครงการ ขอขอบคุณสำหรับคำแนะนำ ความรู้ และความช่วยเหลือ ที่จำเป็นต่อการดำเนินโครงการ

ขอขอบคุณภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเชียงใหม่ ที่มอบโอกาสให้ใช้สถานที่ในการทำงานให้กับผู้พัฒนา พร้อมทั้งทุนสนับสนุน

ท้ายที่สุด ขอขอบคุณเพื่อน/เพื่อนร่วมงานทุกคน สำหรับความช่วยเหลือ ความร่วมมือ ร่วมแรงร่วมใจ ความเสียสละ ความอดทนที่มีให้กัน และกันโดยเสมอมา

นายไตรภพ ศรีมณี คณะผู้พัฒนา

นายวราดร ศิริพันธุ์ คณะผู้พัฒนา

19 มีนาคม 2566

สารบัญ

บทที่ 1
บทนำ

1.1 ที่มาของโครงงาน

สืบเนื่องจากอุปกรณ์ Internet of Things หรือ IoT มีการใช้งานแพร่หลายมากในปัจจุบัน สามารถใช้ประโยชน์และเพิ่มความสะดวกสบายในครัวเรือนและภาคอุตสาหกรรม ในขณะเดียวกันอุปกรณ์เหล่านี้ยังมีจุดอ่อนที่ทำให้สามารถเข้าถึงข้อมูลส่วนตัวรวมไปถึงพฤติกรรมของผู้ใช้ผ่านการดักจับการรับส่งข้อมูลของอุปกรณ์ไอโอทีเช่นอุปกรณ์ตรวจจับการนอนที่สามารถอนุมานได้ว่าผู้ใช้ทำอะไรอยู่เช่น นอน ตื่น หรือ ตื่นมาทำกิจกรรมชั่วคราวเป็นต้น โดยการอำพรางแบบวิธีเดิม เช่น Firewall, VPN หรือ Independent Traffic Padding ยังคงมีปัญหาเนื่องจาก อุปกรณ์ไอโอทีส่วนใหญ่ติดต่อกับเซิร์ฟเวอร์เดียวหรือจำนวนน้อยมา กเมื่อเทียบกับเครือข่ายอื่นๆที่มีหลายเซิร์ฟเวอร์รองรับ ทำให้ผู้สังเกตการณ์รวมถึงผู้ให้บริการอินเตอร์เน็ตสามารถทราบถึงชนิดอุปกรณ์และทราฟฟิกที่ผ่านไปมาในเครือข่าย นำพาไปสู่การอนุมานกิจกรรมที่แท้จริงอย่างสังเขปของผู้ใช้เป้าหมายดังที่กล่าวมาข้างต้น ส่งผลให้ผู้ใช้ไม่ได้รับความเป็นส่วนตัวหรือเป็นช่องทางที่ก่อให้เกิดอาชญากรรมได้ โดยโครงงานนี้มุ่งเน้นที่จะปรับปรุงจุดอ่อนของวิธีการอำพรางทราฟฟิกแบบเดิม โดยจะหาทางลดอัตราการเดาทราฟฟิคจริงถูกให้น้อยลงมากที่สุด ด้วยวิธีการลดการใช้แบนด์วิดท์ในเครือข่ายน้อยที่สุดด้วย

1.2 วัตถุประสงค์ของโครงงาน

1. เพื่อเสริมสร้างความเป็นส่วนตัวและความไว้วางใจจากผู้ใช้ในอุปกรณ์ไอโอที
2. เพื่อทำให้บุคคลที่สามไม่สามารถอนุมานพฤติกรรมผู้ใช้ได้จากการรับส่งข้อมูลในเครือข่าย
3. เพื่อส่งเสริมการพัฒนาและค้นคว้าระบบการป้องกันจากการถูกตรวจจับจากผู้ดักจับสัญญาณของแพ็กเก็ตไอโอที

1.3 เป้าหมาย และขอบเขตโครงการ

เป้าหมายของโครงการนี้คือการพัฒนาแอปพลิเคชัน POC (Proof of Concept) ที่มีวัตถุประสงค์เพื่อสร้างโมเดลการป้องกันการดักจับข้อมูล (Data Exfiltration Prevention) ในระบบไอโอที โดยให้แน่ใจว่าผู้โจมตีจะไม่สามารถเข้าถึงเนื้อหาของแพคเก็ต แต่สามารถสังเกตเห็นปริมาณการส่งข้อมูลเท่านั้น การสื่อสารในระบบนี้ถูกสมมติว่าเป็น HTTPS และสามารถปกปิดการส่งข้อมูลของผู้ใช้ไอโอที ทั้งนี้เพื่อป้องกันการละเมิดความเป็นส่วนตัวของผู้ใช้งาน

1.4 ขอบเขตโครงการ:

1. พัฒนาแอปพลิเคชัน POC สำหรับป้องกันการดักจับข้อมูลในระบบไอโอที
2. การสื่อสารระหว่างอุปกรณ์ไอโอทีและเซิร์ฟเวอร์ IoT service server จะต้องเป็น HTTPS

3. สามารถปกปิดการส่งข้อมูลของผู้ใช้ไอโอที โดยมีการคัดกรองและถอดรหัสทราฟฟิกอำพรางที่ปลายทางของเซิร์ฟเวอร์ดีเอ็นเอส
4. การป้องกันจะเน้นไปที่การซ่อนปริมาณการส่งข้อมูลและป้องกันการเข้าถึงเนื้อหาของแพค-เก็ต
5. ประเมินผลและวิเคราะห์ประสิทธิภาพของแอปพลิเคชัน POC ในการป้องกันการดักจับข้อมูล

1.4.1 ขอบเขตด้านฮาร์ดแวร์

1. อุปกรณ์ไอโอทีสามารถเชื่อมต่อเครือข่ายได้ทั้งเครือข่ายไร้สายหรือใช้สาย
2. เซิร์ฟเวอร์ตรวจสอบจะมีตัวถอดรหัสและคัดกรองทราฟฟิกอำพรางออกจากทราฟฟิกจริง
3. แบนด์วิดท์สำหรับสื่อสารระหว่างอุปกรณ์ไอโอทีและเซิร์ฟเวอร์

1.4.2 ขอบเขตด้านซอฟต์แวร์

1. การเก็บทราฟฟิกระหว่างอุปกรณ์ไอโอทีกับเซิร์ฟเวอร์จะถูกเก็บไว้บน IoT traffic database
2. การอำพรางทราฟฟิกของไอโอทีจะจัดการบนเราเตอร์เฉพาะของไอโอทีด้วยโปรแกรมเฉพาะ
3. มีโปรแกรมการถอดรหัสและคัดกรองทราฟฟิกที่อำพรางจากทราฟฟิกจริง ทำให้เซิร์ฟเวอร์ IoT service server สามารถรับและประมวลผลข้อมูลที่ถูกต้องได้

1.5 ประโยชน์ที่ได้รับ

อุปกรณ์ไอโอทีในปัจจุบันติดต่อรับส่งข้อมูลต่างๆผ่านเซิร์ฟเวอร์ผู้ให้บริการอุปกรณ์จำนวนน้อยมาก จึงทำให้ผู้สังเกตการณ์สามารถอนุมานพฤติกรรมผู้ใช้ในเวลาต่างๆจากข้อมูลทราฟฟิกที่เข้าออกได้ ดังนั้น โครงการนี้จึงต้องการพัฒนาการรักษาความเป็นส่วนตัวของผู้ใช้อุปกรณ์ดังกล่าว โดยลดอัตราการคาดเดาจากผู้สังเกตการณ์ให้น้อยที่สุด เพื่อให้ผู้ใช้สามารถรักษาความเป็นส่วนตัว ปกป้องข้อมูลที่สำคัญได้มากขึ้น เมื่อผู้สังเกตการณ์ไม่สามารถอนุมานพฤติกรรมของอุปกรณ์เป้าหมายได้อย่างแม่นยำจะสามารถลดการเกิดอาชญากรรมที่อาจเกิดขึ้นในอนาคตได้

1.6 เทคโนโลยี และเครื่องมือที่ใช้

1.6.1 เทคโนโลยีด้านฮาร์ดแวร์

อุปกรณ์ Raspberry Pi 3 Model B: คอมพิวเตอร์บอร์ดขนาดเล็กใช้สำหรับการพัฒนา และทดสอบ

1. อุปกรณ์เซนเซอร์ไอโอที เซ็นเซอร์สวิตช์ไฟ
2. อุปกรณ์เซนเซอร์ไอโอที เซ็นเซอร์ตรวจจับการเคลื่อนไหว

3. อุปกรณ์เซนเซอร์ไอโอที ตัววัดอุณหภูมิ
4. เซิร์ฟเวอร์ตรวจสอบ: ใช้สำหรับตรวจสอบคีย์สำหรับการถอดรหัสและคัดกรองทราฟฟิก
5. เซิร์ฟเวอร์ผู้ให้บริการของอุปกรณ์ไอโอที: ใช้สำหรับจัดการข้อมูลและบริการต่าง ๆ ของอุปกรณ์ไอโอที

1.6.2 เทคโนโลยีด้านซอฟต์แวร์

1. Python: ภาษาหลักที่ใช้ในโครงการ สำหรับอำพรางทราฟฟิก จัดเก็บ และคัดกรองทราฟฟิกของไอโอที
2. JSON (JavaScript Object Notation): รูปแบบข้อมูลที่ใช้ในการแลกเปลี่ยนข้อมูลระหว่างเว็บไซต์
3. Visual Studio Code: เป็นโปรแกรมแก้ไข และพัฒนาโค้ด
4. Google Colab: เครื่องมือที่ให้บริการบนเว็บบราวเซอร์ และเป็นเหมือนโปรแกรม Jupyter Notebook ที่มีความสามารถในการแบ่งปันโค้ดได้ง่าย และสะดวก
5. RestfulAPI: เทคโนโลยีในการสร้าง API (Application Programming Interface) สำหรับการสื่อสารระหว่างแอปพลิเคชันหรือระบบ
6. Wireshark: ใช้ในการตรวจสอบแพ็กเก็ต และจับแพ็กเก็ตข้อมูลที่ถูกส่งผ่านเครือข่าย (Traffic) ของเครือข่ายไอโอที และแสดงผลลัพธ์

1.7 แผนการดำเนินงาน

ขั้นตอนการดำเนินงาน	2565							2566		
	มิถุนายน	กรกฎาคม	สิงหาคม	กันยายน	ตุลาคม	พฤศจิกายน	ธันวาคม	มกราคม	กุมภาพันธ์	มีนาคม
ศึกษางานวิจัย Stochastic Traffic Padding										
ทดลองการอำพรางด้วยStochastic Traffic Padding										
ศึกษาการส่งแพ็กเก็ตแบบมี Label (Key)										
ออกแบบระบบ										
พัฒนาโปรแกรมอำพรางทราฟฟิก										
ทดสอบระบบ										
ประเมินและตรวจสอบปัญหาที่พบ										
เขียนรายงานสรุปผลการทำงาน										

1.8 บทบาทและความรับผิดชอบ

การค้นคว้าวิธีการอำพราง ระบบ และทฤษฎีต่างๆ เช่น การใช้ Better Efficient Traffic Padding, Stochastic Traffic Padding, Network Security, Network Model, ศาสตร์ที่เกี่ยวข้องกับ Network Traffic โดยทั้งหมดผู้จัดทำจะรับผิดชอบร่วมกัน

1.9 ผลกระทบทางด้านสังคม สุขภาพ ความปลอดภัย กฎหมาย และวัฒนธรรม

วิธีการป้องกันความเป็นส่วนตัวส่งผลให้ลดอาชญากรรมอย่างมีนัยยะสำคัญเนื่องจากผู้สังเกตการณ์ไม่สามารถอนุมานพฤติกรรมผู้ใช้ได้ถูกต้อง และการโจรกรรมข้อมูลสำคัญที่อาจเกิดขึ้น ส่วนการเข้าถึงข้อมูลหรือทราฟฟิกจริง มีเฉพาะเพียงผู้ใช้และผู้ให้บริการไอโอทีเมื่อมีการขอหรือเข้าถึงข้อมูล จะต้องได้รับการอนุญาตจากผู้ให้บริการและผู้ใช้อุปกรณ์ เพื่อป้องกันการนำไปใช้ในทางที่ผิด และป้องกันความเป็นส่วนตัวของผู้ใช้

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

การจัดทำโครงการนี้เป็นการศึกษาค้นคว้าทฤษฎีที่เกี่ยวข้องของโครงการที่เคยมีผู้นำเสนอไว้แล้วซึ่งโครงการนี้ได้นำมาพัฒนาต่อยอด ซึ่งการพัฒนาต่อยอดนี้จะแบ่งโครงสร้างการทำงาน และสมมติฐานของการป้องกันความเป็นส่วนตัวของผู้ใช้อุปกรณ์ไอโอทีโดยมีสองส่วนคือ ส่วนของมอดูลภายใน (Internal Module) หรือใกล้ผู้ใช้ และส่วนของมอดูลภายนอก (External Module) หรือไกลผู้ใช้

2.1 การบันทึกทราฟฟิกเก่าของอุปกรณ์ไอโอที

การบันทึกทราฟฟิกเก่าของอุปกรณ์ไอโอทีนั้นจะใช้คำสั่งสคริปต์ที่เขียนด้วยภาษา Python ให้บันทึกข้อมูลแพ็กเก็ตทั้งหมดลงบนหน่วยความจำบนราสเบอร์รี่พายจัดเก็บข้อมูลแพ็กเก็ตในรูปแบบ JSON และบันทึกลงไฟล์ตั้งค่าราสเบอร์รี่พายให้เรียกใช้สคริปต์ Python นี้อัตโนมัติเมื่อเริ่มต้นระบบ

การอำพรางทราฟฟิกช่วงมอดูลภายใน จะใช้การอำพราง Better Efficiency Traffic Padding (BeTP) จะใช้งานในช่วงระหว่างอุปกรณ์ไอโอทีกับเซิร์ฟเวอร์ตรวจสอบ เนื่องจากเป็นช่วงเครือข่ายที่ไม่จำเป็นต้องลดแบนด์วิดท์ และข้อมูลทราฟฟิกมีขนาดเล็กมาก ส่วนการคัดกรองและถอดรหัสจะทำบนตัวอุปกรณ์เซิร์ฟเวอร์ตรวจสอบ

2.2 การคัดกรองทราฟฟิกจริงออกจากทราฟฟิกปลอม

เซิร์ฟเวอร์ตรวจสอบจะต้องเก็บคีย์ที่ใช้ในการเข้ารหัสและถอดรหัสข้อมูลในฐานข้อมูล เมื่อรับแพ็กเก็ตจากราสเบอร์รี่พาย, เซิร์ฟเวอร์ตรวจสอบจะตรวจสอบคีย์ที่ถูกใส่ไว้ในเพย์โหลดของแพ็กเก็ต หากคีย์ในเพย์โหลดตรงกับคีย์ที่เก็บไว้ในฐานข้อมูล, เซิร์ฟเวอร์ตรวจสอบจะถือว่าเป็นทราฟฟิกจริง แล้วทำการถอดรหัสข้อมูลด้วยคีย์นั้น แต่หากคีย์ในเพย์โหลดไม่ตรงกับคีย์ที่เก็บไว้ในฐานข้อมูล, เซิร์ฟเวอร์ตรวจสอบจะถือว่าเป็นทราฟฟิกปลอม แล้วทำการทิ้งแพ็กเก็ตนั้น เมื่อถอดรหัสข้อมูลที่ถือว่าเป็นทราฟฟิกจริงเสร็จสิ้น เซิร์ฟเวอร์ตรวจสอบจะส่งข้อมูลต่อไปยังเซิร์ฟเวอร์ผู้ให้บริการของอุปกรณ์ไอโอที

โดยการดำเนินการตามขั้นตอนนี้ จะช่วยป้องกันการส่งข้อมูลที่ไม่ได้รับอนุญาต และทำให้เซิร์ฟเวอร์ตรวจสอบสามารถคัดกรองทราฟฟิกจริงออกจากทราฟฟิกปลอม

2.3 เซิร์ฟเวอร์ให้บริการไอโอที

มีหน้าที่บริการและประมวลผลข้อมูลที่ได้รับมาจากอุปกรณ์ไอโอที เพื่อส่งข้อมูลกลับไปยังอุปกรณ์ไอโอที เซิร์ฟเวอร์ให้บริการไอโอทีจะได้รับต้นทางโดยการส่งจากเซิร์ฟเวอร์จะมีการอำพรางด้วย Better Efficiency Traffic Padding กระบวนการจะเกิดขึ้นที่เซิร์ฟเวอร์ตรวจสอบโดยจะดึงข้อมูลเก่าในเซิร์ฟเวอร์ได้

โดยตรงและสร้างชุดบิตคัดกรองใหม่เหมือนกับเราท์เตอร์ไอโอทีส่วนการคัดกรองทราฟฟิกก็จะทำในส่วนนี้เช่นกัน โดยเซิร์ฟเวอร์จะดูแลโดยผู้ให้บริการของอุปกรณ์ไอโอที

2.4 ราสเบอร์รี่พาย

ราสเบอร์รี่พาย หรือ Raspberry Pi เป็นคอมพิวเตอร์บอร์ดขนาดเล็กที่มีความสามารถในการทำงานเหมือนกับคอมพิวเตอร์ทั่วไป มีการออกแบบมาเพื่อใช้งานในการเรียนรู้เกี่ยวกับการเขียนโปรแกรม การควบคุมอุปกรณ์และการใช้งานระบบปฏิบัติการลินุกซ์ รวมถึงการนำไปใช้งานในการสร้างโปรเจกต์ต่าง ๆ ราคาถูกและมีขนาดเล็กทำให้เหมาะสำหรับผู้ที่ต้องการทดลองสร้างโปรเจกต์แบบขนาดเล็ก หรือต้องการคอมพิวเตอร์บอร์ดในการใช้งานเบื้องต้น ใช้งานได้หลากหลายทั้งในส่วนของการเรียนรู้ การเล่นเกม และการทำงานทั่วไป [9]

2.5 ฟังก์ชันแฮช

ฟังก์ชันแฮช คือวิธีการอย่างหนึ่งซึ่งทำให้ข้อมูลส่วนหนึ่งหรือทั้งหมด ให้กลายเป็นจำนวนเล็กๆ อันหนึ่งอย่างมีปฏิสัมพันธ์ ซึ่งจำนวนดังกล่าวเปรียบได้ว่าเป็น "ลายนิ้วมือ" ของข้อมูล ขั้นตอนวิธีของฟังก์ชันแฮชส่วนใหญ่จะเป็นการแบ่งย่อยข้อมูลและการผสมข้อมูลย่อยทั้งหมดเข้าด้วยกันเพื่อให้ได้ผลลัพธ์สุดท้าย ผลลัพธ์ดังกล่าวอาจเรียกว่า ผลบวกแฮช (hash sum) ค่าแฮช (hash value) รหัสแฮช (hash code) หรือเรียกว่า แฮช (hash) เฉยๆ ก็ได้ บ่อยครั้งที่การเอ่ยถึงแฮชจะหมายถึงฟังก์ชันแฮชโดยปริยาย ปกติแล้วฟังก์ชันแฮชจะทำงานผ่านดัชนีที่เก็บไว้ในตารางแฮชที่อยู่ในหน่วยความจำหรือแฟ้มข้อมูลชั่วคราว [11]

2.6 การเข้ารหัสแบบเอ็มดี 5

MD5 ย่อมาจาก Message-Digest algorithm 5 คือ รูปแบบการเข้ารหัสแบบ Hash (Cryptographic hash) ชนิดหนึ่ง คือ การแปลงรูปแบบของข้อมูลที่รับเข้ามาไม่ว่าขนาดเท่าใดก็ตาม ให้อยู่ในอีกรูปแบบหนึ่งที่มีขนาดคงที่ เพราะฉะนั้น จะไม่สามารถเรียกดูข้อมูลต้นฉบับได้ (Decrypt) ทำได้เพียงตรวจสอบว่าข้อมูลที่ให้มาแต่ละครั้งเหมือนกันหรือไม่ ความปลอดภัยจึงค่อนข้างสูง ในที่นี้ MD5 เป็นการเข้ารหัสแบบ 128-bit ให้ค่าเป็นตัวเลขฐาน 16 (0123456789abcd) ขนาด 32 ตัวอักษร แต่ก็มีบางประเภทที่ให้ค่าเป็น binary และ base64 [10]

2.7 Hyper Text Transfer Protocol: HTTP และ Hypertext Transfer Protocol: HTTPS

โปรโตคอล หรือ รูปแบบการสื่อสารบนระบบเครือข่าย Internet เพื่อการแลกเปลี่ยนข้อมูล ถ่ายโอนไฟล์ในรูปแบบ Multimedia เช่น ข้อความ ภาพกราฟิก เสียง วิดีโอ และไฟล์มัลติมีเดียอื่น ๆ ซึ่งทำงานอยู่ใน

ระดับ Application Layer บนโปรโตคอล TCP/IP ใช้ URL เพื่อระบุ Server ปลายทางในการดึงและแลกเปลี่ยนข้อมูลซึ่งมีโครงสร้างเป็นตัวอักษรและตัวเลข (text) ใช้สำหรับเป็น link เชื่อมระหว่าง ข้อมูล Text อื่นๆ ในรูปแบบ Plain text เป็นข้อความธรรมดาไม่มีการเข้ารหัส โดยสรุปรูปแบบดังนี้

1. เป็นโปรโตคอลหลักที่ใช้ในการแลกเปลี่ยนข้อมูล (HTML) กันระหว่าง Web Server และ Web Client (Browser)
2. ใช้ URL (Uniform Resource Locator) ในการเข้าถึงเว็บไซต์ (Web Site) ซึ่งจะขึ้นต้นด้วย http:// ตามด้วยชื่อของเว็บไซต์
3. ส่งข้อมูลเป็นแบบ Plain text หรือ Clear text คือ เป็นข้อความที่ไม่มีการเข้ารหัสข้อมูลในระหว่างการส่ง (None-Encryption) ทำให้สามารถถูกดักจับและอ่านข้อมูลได้ง่าย จึงไม่ปลอดภัย

HTTPS คือ โปรโตคอล หรือ รูปแบบการสื่อสารบนระบบเครือข่าย Internet ต่างกับ http คือการเพิ่ม S หรือ Secure คือมีการใช้ SSL (secure socket layer) และ TLS (transport layer security) ในการเข้ารหัสข้อมูลระหว่างการส่ง ช่วยรักษาความสมบูรณ์ถูกต้องของข้อมูลผู้ใช้และเก็บข้อมูลไว้เป็นความลับระหว่างคอมพิวเตอร์ของผู้ใช้กับเว็บไซต์ โดยมีความปลอดภัยและเป็นส่วนตัวระหว่างใช้งาน HTTPS หรือ HTTP + SSL จุดที่สำคัญคือมีส่วน Authentication เป็นการตรวจสอบเพื่อระบุตัวตน ในการเข้าสู่ Website ก่อนแลกเปลี่ยนข้อมูลโดยตรงกับทาง Web Server เป็นโปรโตคอลที่เข้ารหัสในการสื่อสาร โดยใช้ Asymmetric Algorithm เพื่อไม่ให้เกิดการโจรกรรมข้อมูลระหว่างกลางหรือ man-in-the-middle attacks มากกว่านั้นยังสามารถเข้ารหัสทั้ง 2 ทาง ระหว่าง Web Client – Web Server เพื่อป้องกันการปลอมแปลงข้อมูล และยังมั่นใจได้ว่าระหว่างการแลกเปลี่ยนข้อมูลจะไม่ถูกแกะ หรือ ปลอมแปลง เหมาะสำหรับธุรกิจที่มีข้อมูลเป็นความลับ เช่น ธนาคาร เป็นต้น [12]

2.8 ดีเอ็นเอส

ดีเอ็นเอส หมายถึง เครื่องบริการชื่อโดเมน มีชื่อภาษาอังกฤษว่า Domain Name System เป็นระบบชื่อโดเมนซึ่งเป็นระบบการแปลงชื่อโดเมนของเว็บไซต์เป็นที่อยู่โปรโตคอลอินเทอร์เน็ต ที่เครื่องคอมพิวเตอร์สามารถเข้าถึงได้ ระบบ ดีเอ็นเอส ทำหน้าที่เป็นตัวกลางในการแปลงชื่อโดเมนเป็นที่อยู่โปรโตคอลอินเทอร์เน็ตและส่งต่อข้อมูลระหว่างเครื่องคอมพิวเตอร์ได้อย่างรวดเร็ว ซึ่งทำให้ผู้ใช้งานสามารถเข้าถึงเว็บไซต์ได้ง่ายและสะดวกมากยิ่งขึ้นโดยไม่จำเป็นต้องจำหน้าที่อยู่โปรโตคอลอินเทอร์เน็ตของเว็บไซต์ที่ต้องการเข้าใช้งาน ระบบดีเอ็นเอส มีความสำคัญอย่างมากในการทำงานของอินเทอร์เน็ต และใช้งานโดยแทบทุกครั้งที่มีการเชื่อมต่อเครือข่ายอินเทอร์เน็ต โดยระบบดีเอ็นเอส จะมีโครงสร้างเป็นต้นไม้ที่แต่ละระดับจะมีโดเมนต่อไปยังระดับต่อไป โดยการแปลงชื่อโดเมนในดีเอ็นเอส จะใช้การค้นหาแบบฟังก์ชันที่เรียกตัวเอง (recursive) โดยระบบจะ

สืบทอดการค้นหาข้อมูลไปจนกระทั่งเจอข้อมูลที่ต้องการ และส่งคำตอบกลับมายังเครื่องคอมพิวเตอร์ผู้ใช้งาน [6]

2.9 เว็บเซิร์ฟเวอร์

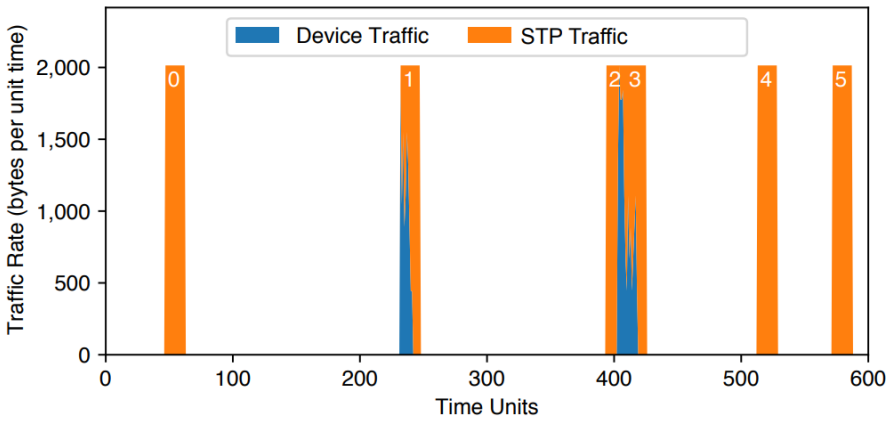
เว็บเซิร์ฟเวอร์ คือซอฟต์แวร์และฮาร์ดแวร์ของคอมพิวเตอร์ที่สามารถรับคำขอผ่านทาง HTTP ซึ่งเป็นโพรโทคอลเครือข่ายที่สร้างขึ้นเพื่อเผยแพร่เนื้อหาของเว็บ หรือผ่านทาง HTTPS ซึ่งเป็นรูปแบบที่ปลอดภัยขึ้น ตัวผู้ใช้งาน (user agent) ซึ่งอาจคือเว็บเบราว์เซอร์ หรือ เว็บครอว์เลอร์ จะเริ่มต้นการสื่อสารโดยการส่งคำขอรีซอร์สเฉพาะชุดหนึ่งผ่านทาง HTTP และเว็บเซิร์ฟเวอร์จะตอบกลับด้วยเนื้อหาของรีซอร์สนั้น หรือด้วยข้อความแอร์เรอร์ นอกจากนี้ เว็บเซิร์ฟเวอร์ยังสามารถรับและเก็บรีซอร์สที่ถูกส่งมาโดยตัวผู้ใช้งานหากมีการติดตั้งให้ทำเช่นนั้น เว็บเซิร์ฟเวอร์อาจเป็นได้ตั้งแต่คอมพิวเตอร์เครื่องเดียวหรือระบบเอ็มเบ็ด เช่น เราเทอร์, พรินเทอร์, เว็บแคม ที่มีการติดตั้งระบบให้ทำงานเป็นเว็บเซิร์ฟเวอร์ ในขณะที่เว็บไซต์ที่มีการเข้าชม (traffic) สูง โดยทั่วไปจะรันเว็บเซิร์ฟเวอร์ผ่านชุดคอมพิวเตอร์จำนวนมาก (fleets of computers) ที่ออกแบบมาโดยเฉพาะ [13]

2.10 โปรโตคอลอินเทอร์เน็ต

โปรโตคอลอินเทอร์เน็ต หรือ IP ย่อมาจาก Internet Protocol เป็นระบบเครือข่ายคอมพิวเตอร์ที่ใช้สำหรับการรับส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ต โดยโปรโตคอลอินเทอร์เน็ตจะใช้หมายเลขเพื่อระบุตัวตนของเครื่องคอมพิวเตอร์แต่ละเครื่องในเครือข่ายอินเทอร์เน็ต [14]

2.11 Stochastic Traffic Padding (STP)

เป็นอัลกอริทึมอย่างหนึ่ง ที่ใช้เพื่อการอำพรางรูปแบบของทราฟฟิกของกิจกรรมผู้ใช้อุปกรณ์ไอโอที ซึ่งมีอยู่สองวิธีการที่นำมาใช้ร่วมกัน คือการยิงทราฟฟิกอำพราง เพื่อปิดบังทับข้อมูลที่เกิดขึ้นหรือมีการสร้างข้อมูลเทียมขึ้นมาเพื่อให้ผู้ที่สังเกตการณ์ข้อมูลไม่สามารถที่จะอนุมานได้ว่าเกิดกิจกรรมขึ้นอยู่จริงๆหรือไม่ วิธีที่สองที่นำมาผนวกคือ เมื่อไม่มีทราฟฟิกเกิดขึ้นเป็นระยะเวลาหนึ่ง ก็จะทำการยิงทราฟฟิกปลอมเพื่อไม่ให้ผู้สังเกตุการณ์สามารถคาดเดาช่วงเวลาที่มีใช้งานอุปกรณ์ไอโอทีได้อย่างแน่ชัดโดย อัลกอริทึมนี้จะสามารถลดความมั่นใจของผู้สังเกตการณ์ลงได้ ทั้งนี้เอสทีพี ไม่ได้ทำให้เกิดค่าเวลาแฝงที่เพิ่มขึ้นแต่อย่างใด แล้วยังสามารถที่จะลดทอนความมั่นใจของผู้สังเกตการณ์ลงกับค่าใช้จ่ายของแบนด์วิดท์ [1]



รูปที่ 2.1 ภาพจำลองการอำพรางทราฟฟิกในระบบ [1]

จากรูปข้างต้นแผนภูมิกราฟแท่งข้างต้นคือตัวอย่างของการใช้อัลกอริทึมเอสทีพี ที่ใช้กับอุปกรณ์เต้ารับอัจฉริยะ หากดูจากแผนภูมิจะพบว่าช่วงวินาทีที่สองร้อยสามสิบและวินาทีที่สี่ร้อยนั้นมีทราฟฟิกเกิดขึ้นแต่ได้ถูกอำพราง รวมถึงช่วงเวลาอื่นๆที่ไม่มีทราฟฟิกเกิดขึ้นจริงด้วย ทำให้ผู้สังเกตุการณ์ไม่สามารถแยกแยะได้ว่าช่วงเวลาใดที่เกิดการรับส่งข้อมูลอุปกรณ์จริงกับผู้ใช้อุปกรณ์

2.12 ความมั่นใจของผู้สังเกตุการณ์

ความมั่นใจของผู้สังเกตุการณ์ หรือ Adversary Confidence เป็นวิธีการวัดความปลอดภัยของระบบโดยวัดความสามารถในการป้องกันการละเมิดความเป็นส่วนตัวของผู้ใช้งานโดยผู้สังเกตจะพยายามสอดแนมดูและเข้าถึงข้อมูลของผู้ใช้งาน

ความมั่นใจของผู้สังเกตุการณ์ สามารถใช้วัดความปลอดภัยของระบบ โดยตัวเลขที่น้อยกว่าจะแสดงให้เห็นถึงประสิทธิภาพที่ดีกว่าในการป้องกันการละเมิดความเป็นส่วนตัวของผู้ใช้งาน นั่นหมายความว่าเมื่อผู้ทดสอบพยายามสอดแนมและพยายามเข้าถึงข้อมูลของผู้ใช้งานแต่ไม่สามารถอนุมานได้อย่างถูกต้องได้ [1]

2.13 การใช้แบนด์วิดท์

การใช้แบนด์วิดท์เคือสัดส่วนของการส่งข้อมูลบนเครือข่ายระหว่างการป้องกันและไม่ป้องกัน โดยปกติแล้วการป้องกันอาจต้องเพิ่มการส่งข้อมูลเพิ่มเติมที่จะใช้ในการตรวจสอบและตรวจพบการละเมิดความปลอดภัยของเครือข่าย ซึ่งส่งผลให้การส่งข้อมูลบนเครือข่ายเพิ่มขึ้น การเพิ่มการส่งข้อมูลเพิ่มเติมนี้เป็นที่รู้จักกันว่า "Bandwidth Overhead"

Bandwidth Overhead ที่ต่ำกว่าจะถือว่าดีกว่า เนื่องจากมันจะไม่เพิ่มการส่งข้อมูลบนเครือข่ายเพิ่มขึ้นมากนัก ซึ่งสามารถช่วยประหยัดทรัพยากรเครือข่ายและลดความล่าช้าในการสื่อสารได้ ดังนั้น เมื่อออกแบบระบบป้องกันความปลอดภัยของเครือข่าย จะต้องมีการคำนึงถึง "Bandwidth Overhead" เพื่อให้ระบบทำงานได้มีประสิทธิภาพและไม่ส่งผลต่อการใช้ทรัพยากรของเครือข่ายในที่สุด [1]

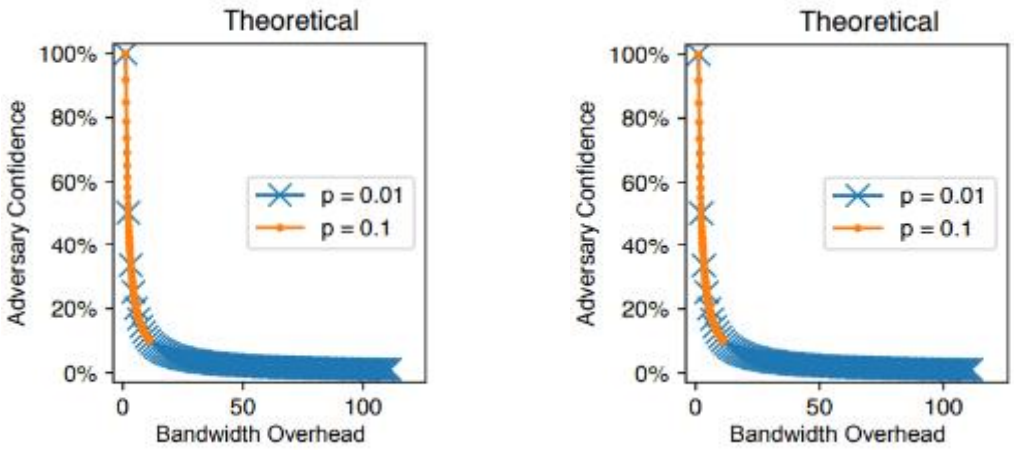
2.14 การแลกเปลี่ยนความมั่นใจของผู้สังเกตุการณ์ต่อแบนด์วิดท์

การปรับแต่งการป้องกันความปลอดภัยของเครือข่ายจะมีผลต่อค่า "Adversary Confidence" และ "Bandwidth Overhead" ซึ่งมีความสัมพันธ์กันดังนี้

ค่า adversary confidence สูง แต่ bandwidth overhead ต่ำ

เมื่อมีการปรับแต่งการป้องกันความปลอดภัยของเครือข่ายให้มีประสิทธิภาพสูง อาจทำให้ค่า adversary confidence สูงขึ้น ซึ่งแสดงถึงความมั่นใจในการป้องกันความเป็นส่วนตัวของผู้ใช้งาน แต่อาจทำให้การส่งข้อมูลบนเครือข่ายเพิ่มขึ้น นั่นคือค่า bandwidth overhead จะต่ำลง

ค่า adversary confidence ต่ำ แต่ bandwidth overhead ต่ำ: การปรับแต่งการป้องกันความปลอดภัยของเครือข่ายให้มีความเหมาะสม อาจทำให้ค่า adversary confidence ต่ำลง นั่นคือมีโอกาสที่มีผู้ประสงค์ร้ายสามารถดูข้อมูลของผู้ใช้งานได้ง่ายขึ้น แต่การส่งข้อมูลบนเครือข่ายจะลดลง ซึ่งหมายความว่าค่า bandwidth overhead จะต่ำลงเช่นกัน ดังนั้น ในการออกแบบระบบป้องกันความปลอดภัยของเครือข่ายจะต้องคำนึงถึงค่า adversary confidence และ bandwidth overhead ให้สมดุลกัน เพื่อให้ระบบทำงานได้มีประสิทธิภาพและไม่ส่งผลต่อการใช้ทรัพยากรของเครือข่ายในที่สุด [1]



รูปที่ 2.2 ความสัมพันธ์ระหว่างความมั่นใจของผู้สังเกตการณ์ และค่า bandwidth overhead [1]

2.15 ความแตกต่างระหว่างอุปกรณ์เครือข่าย และไอโอที

อุปกรณ์เครือข่าย เป็นอุปกรณ์ที่สามารถเชื่อมต่อหรือเข้าถึงอินเทอร์เน็ตโดยที่สามารถเข้าถึงทรัพยากรต่างๆได้ เช่น คอมพิวเตอร์ โทรศัพท์มือถือ เป็นต้น ส่วนไอโอทีเป็นอุปกรณ์ต่างๆที่ใช้ในชีวิตประจำวัน ที่มีตัวประมวลผล และรับส่งข้อมูลผ่านทางเครือข่ายอินเทอร์เน็ต เช่น หลอดไฟ กล้องวงปิด, อุปกรณ์ช่วยเหลือ เป็นต้น [6]

2.16 การจำแนกอุปกรณ์แต่ละตัวในเครือข่ายด้วยชื่อโดเมน (Domain name)

การจำแนกอุปกรณ์ต่างๆในเครือข่ายจะจำแนกด้วย ชื่อโดเมน ปลายทางที่มีการร้องขอจากอุปกรณ์ต่างๆ สังเกตได้จากจำนวนปลายทางที่อุปกรณ์ได้ส่งคำขอ (request) ไปหาเซิร์ฟเวอร์ ส่วนมากอุปกรณ์ไอโอทีจะส่งคำขอไปให้ผู้บริการข้อมูลของอุปกรณ์นั้น ๆ เพียง 1 – 2 จุดหมาย ส่วนอุปกรณ์เน็ตเวิร์คทั่วไปจะมีคำขอไปหาเซิร์ฟเวอร์เป็นจำนวนมากกว่า 2 จุดหมาย [6]

2.17 การแจกแจงเอกรูป (Uniform Distribution)

การแจกแจงเอกรูป เป็นการแจกแจงความน่าจะเป็นที่ผลลัพธ์ออกมาเท่ากัน เนื่องจาก probability density function ของการกระจายนี้มีความคงที่ระหว่างค่าต่ำสุดและค่าสูงสุดของการกระจายสามารถเขียนสูตรได้ดังนี้ [15]

$$p(x) = \frac{1}{n}$$

เมื่อ n จำนวนตัวอย่างทั้งหมดในการสุ่ม

จากการทดลองพบว่าเมื่อใช้การกระจายแบบเอกรูปนั้น เมื่อมีการใช้กับการส่งแพ็กเก็ตปลอมออกไปผลลัพธ์ที่ได้อยู่ในรูปแบบที่ตายตัว ทำให้ผู้สังเกตการณ์สามารถอนุมานได้ว่าแพ็กเก็ตที่อยู่ในทราฟฟิกนั้นเป็นของปลอม จึงทำให้การตัดสินการส่งแพ็กเก็ตปลอมด้วยการแจกแจงรูปแบบนี้ยังไม่สามารถป้องกันได้อย่างมีประสิทธิภาพ

2.18 การแจกแจงแบบเอ็กซ์โพเนนเชียล (Exponential Distribution)

การแจกแจงแบบเอ็กซ์โพเนนเชียล (Exponential Distribution) เป็นการแจกแจงความน่าจะเป็นต่อเนื่องที่ใช้อธิบายเวลาที่ใช้ในระหว่างเหตุการณ์ต่อเนื่องของระบบควบคุมคิวหรือความถี่ในการเกิดเหตุการณ์ใหม่ [16]

$$f(x) = \lambda e^{-\lambda x},\ x \geq 0$$

จากนั้น กำหนดให้ q เป็นความน่าจะเป็นในการส่งแพ็กเก็ตปลอมเข้าสู่เครือข่ายอินเตอร์เน็ตโดยการกระจายแบบเอ็กซโพเนนเชียล จะได้ว่า

$$q = P_x(x = X)$$

เมื่อให้ μ มีค่าเท่ากับ $\frac{1}{15}$ และ เมื่อมีการส่งทั้งหมด 100 แพ็กเก็ต

$$P_x(x = 100) = \frac{1}{15} e^{-\frac{1}{15}x} dx = 8.4842 \times 10^{-5}$$

แสดงว่าอัตราความน่าจะเป็นในการทำนายแพ็กเก็ตปลอมในการส่งทั้งหมดจะเท่ากับร้อยละ 8.4842×10^{-5}

2.19 การแจกแจงแบบปัวส์ซอง (Poisson Distribution)

การแจกแจงแบบปัวส์ซอง เป็นการแจกแจงในรูปแบบไม่ต่อเนื่องหรือดีสครีต และใช้กับเหตุการณ์ที่เกิดขึ้นได้ยาก (rare events) หรือเหตุการณ์ที่ไม่ได้เกิดขึ้นในเวลาอันสั้น โดยพารามิเตอร์เวลาเฉลี่ยจะมีค่าเท่ากับ lambda สามารถเขียนสูตรได้ดังนี้ [17]

$$p_x(x) = \frac{\lambda^x e^{-\lambda}}{x!} \text{ เมื่อ } \mathbf{x} \{0, 1, 2, 3, \ldots\}$$

จากนั้น กำหนดให้ **q** เป็นความน่าจะเป็นในการส่งแพ็กเก็ตปลอมเข้าสู่เครือข่ายอินเตอร์เน็ตโดยการกระจายแบบปัวส์ซอง จะได้ว่า

$$q = \frac{\mu^x e^{-\mu}}{x!}$$

μ คือ ค่าเฉลี่ยความน่าจะเป็นในการส่งแพ็กเก็ตปลอมเข้าสู่ระบบเครือข่ายอินเทอร์เน็ต

x คือ จำนวนแพ็กเก็ตทั้งหมดที่ตัดสินใจส่งไปในเครือข่าย

หากเปรียบเทียบผลลัพธ์ที่ได้จากการกระจายระหว่างเอ็กซโพเน็นเชียล และปัวส์ซองจะได้ว่าปัวส์ซองนั้นจะให้ค่าความน่าจะเป็นในการจัดส่งแพ็กเก็ตปลอมเข้าสู่เครือข่ายได้น้อยกว่า ส่งผลให้ผู้สังเกตการณ์ไม่สามารถทำนายการส่งแพ็กเก็ตปลอมและอนุมานการทำงานขอแพ็กเก็ตปลอมที่ส่งในเครือข่างอินเทอร์เน็ต

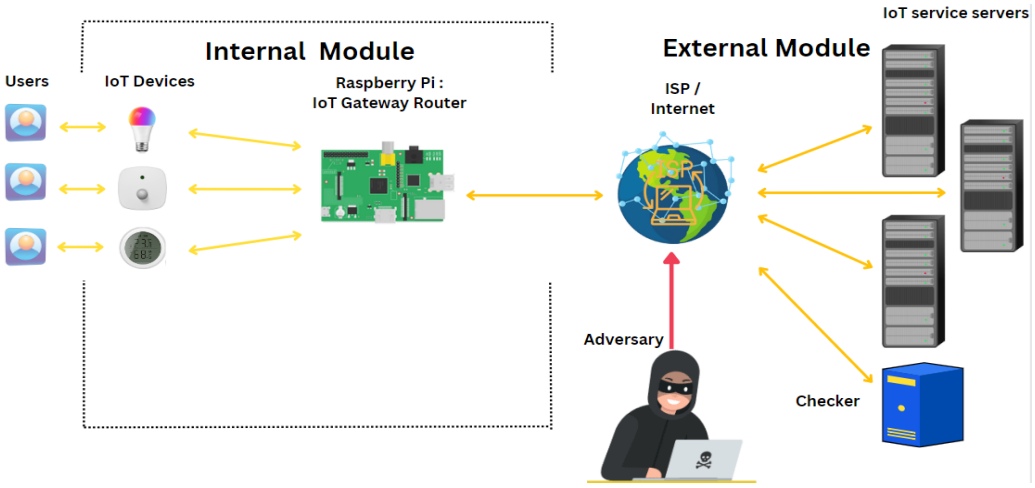
2.20 โปรแกรม Wireshark

โปรแกรม Wireshark มีความสามารถในการจับและวิเคราะห์ข้อมูลแพ็กเก็ตที่ส่งผ่านเครือข่าย เริ่มต้นจับข้อมูลเครือข่ายโดยเลือกอินเตอร์เฟซเครือข่ายที่ต้องการวิเคราะห์ [7]

บทที่ 3
วิธีการดำเนินการ

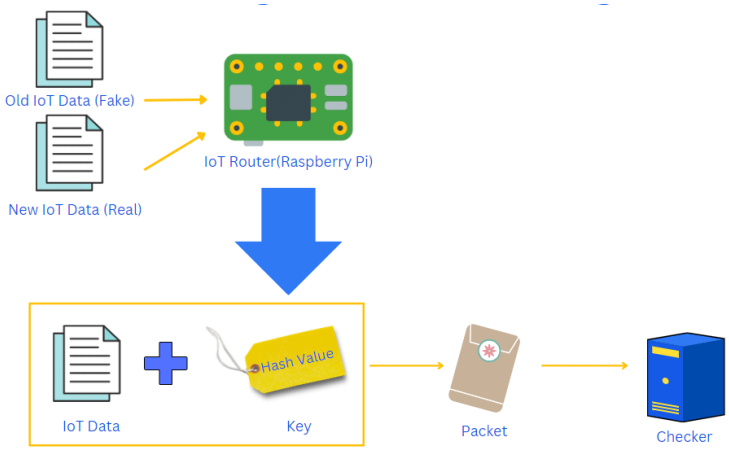
ในบทนี้จะกล่าวถึงหลักการ และการออกแบบระบบที่ใช้งาน การอำพรางทราฟฟิกช่วงนี้โดยจะใช้ Better Efficiency Traffic Padding ในการเรียกข้อมูลทราฟฟิกเก่ามาส่งอำพรางในช่วงที่อุปกรณ์เหล่านั้นไม่มีการรับส่งข้อมูลที่สำคัญ และข้อมูลเก่าที่ส่งไปนั้นจะมีชุดบิตที่บ่งบอกว่าเป็นแพ็กเก็ตที่ส่งไปเป็นข้อมูลจริงหรือข้อมูลปลอมที่ไว้หลอกอำพรางผู้สังเกตการณ์และผู้ให้บริการอินเทอร์เน็ต

3.1 โครงสร้างของระบบ



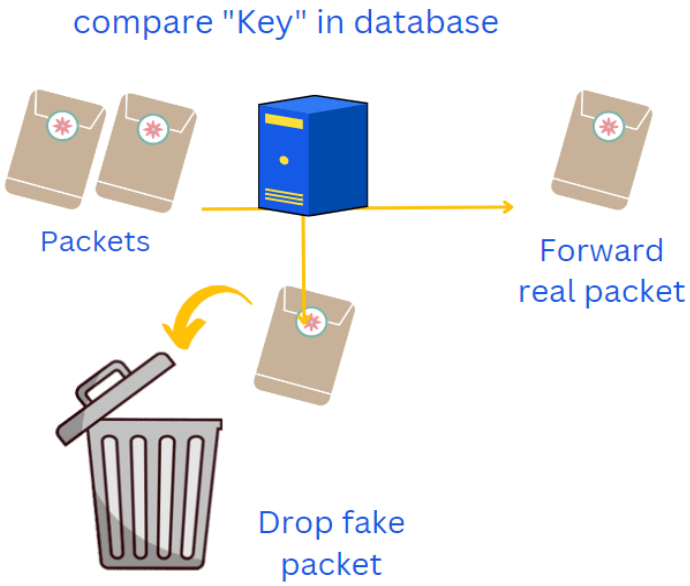
รูปที่ 3.1 แผนภาพสายงานของระบบ

3.2 มอดูลภายใน



รูปที่ 3.2 ส่วนประกอบต่าง ๆ ของส่วนมอดูลภายใน

3.3 มอดูลภายนอก



รูปที่ 3.3 ส่วนประกอบต่าง ๆ ของส่วนมอดูลภายนอก

3.4 การอนุมานทราฟิกของผู้บุกรุก

ผู้สังเกตการณ์จะอนุมานพฤติกรรมของผู้ใช้อุปกรณ์ไอโอที ได้จากการรับส่งข้อมูลต่างๆ ณ ช่วงเวลาหนึ่งและจำแนกอุปกรณ์จาก ชื่อโดเมน หรือ ที่อยู่โดเมน ปลายทางว่าเป็นอุปกรณ์อะไร เช่น อุปกรณ์ตรวจจับการนอน หลอดไฟที่บันทึกการเปิด-ปิดเวลา เป็นต้น ตัวอย่างการอนุมานพฤติกรรมของผู้ใช้เป้าหมาย ได้แก่ การสังเกตการเปิด-ปิดหลอดไฟจะมีช่วงเวลาหนึ่งที่ไม่มีการรับส่งข้อมูลจากหลอดไฟ ทำให้ผู้สังเกตการณ์คิดว่า ณ เวลานั้นไม่มีผู้ใช้อยู่ในบ้านหรือบริเวณนั้นเป็นเวลานานๆ ทำให้เปิดโอกาสที่จะก่ออาชญากรรมต่างๆในอนาคต

3.5 BeTP

เป็นอัลกอริทึมที่ประยุกต์มาจากอัลกอริทึม Stochastic Traffic Padding (STP) โดยการสุ่มส่งแพ็กเก็ตปลอมเข้าเครือข่ายอินเทอร์เน็ตซึ่งขึ้นอยู่กับเวลาด้วยฟังก์ชันชี้กำลัง เพื่อให้ผู้สังเกตการณ์ไม่สามารถคาดเดากิจกรรมของอุปกรณ์ไอโอทีที่ส่งแพ็กเก็ตไปยังเซิร์ฟเวอร์ ทำให้ผู้ใช้อุปกรณ์ไอโอทีมีความเป็นส่วนตัว และปลอดภัยมากขึ้น เช่น ในเวลาที่ไม่มีการใช้งานของอุปกรณ์ไอโอที ทำให้สามารถอนุมานได้ว่าผู้ใช้นั้นไม่อยู่บ้านหรือกำลังนอนหลับ ซึ่งอัลกอริทึมจะนำแพ็กเก็ตเก่าส่งสุ่มเข้าไปยังเซิร์ฟเวอร์จากนั้นให้เซิร์ฟเวอร์ตรวจสอบที่ทำหน้าที่ตรวจสอบรหัสของแต่ละแพ็กเก็ตที่ส่งเข้ามาจาก เราต์เตอร์ต้นทางแล้วเทียบกับรหัสที่จัดเก็บบนฐานข้อมูล ก่อนที่จะส่งไปให้เซิร์ฟเวอร์ผู้ให้บริการ

3.6 การสร้างคีย์สำหรับคัดกรองแพ็กเก็ตในเครือข่ายของเซิรฟเวอร์ตรวจสอบ

การสร้างคีย์ตรวจสอบโดยนำเลขชุดที่กำหนดไว้ไปเข้ารหัสด้วยอัลกอริทึมเข้ารหัสเอ็มดีห้า (MD5)

3.7 การตัดสินใจในการส่งแพ็กเก็ตปลอม และจริงในระบบเครือข่าย

การตัดสินใจขอระบบในการสุ่มจะใช้ การกระจายแบบเอ็กซ์โพเนนเชียล (Exponential Distribution Function) เพื่อสุ่มเวลาในการส่งแพ็กเก็ตถัดไป โดยจะสุ่มข้อมูลจากข้อมูลเก่าของอุปกรณ์ไอโอทีที่เก็บไว้ และใส่คีย์ไว้ในแพ็กเก็ตที่จะถูกส่ง เมื่อเซิร์ฟเวอร์ตรวจสอบได้รับแพ็กเก็ตจะทำการตรวจสอบคีย์ที่ระบบมี เพื่อเทียบว่าเป็นแพ็กเก็ตจริงหรือปลอม ทำให้เซิร์ฟเวอร์ตรวจสอบสามาถทราบข้อมูลจริงจากผู้ใช้ และแพ็กเก็ตปลอมจะถูกปัดตก เซิร์ฟเวอร์ตรวจสอบจะบันทึกข้อมูลของแพ็กเก็ตจริงที่ได้รับไว้ และเซิร์ฟเวอร์ตรวจสอบจะทำการส่งข้อมูลต่อไปยังเซิร์ฟเวอร์ไอโอที

3.8 กลุ่มผู้ใช้โปรแกรม

โปรแกรมที่พัฒนาขึ้นนี้เหมาะสำหรับผู้ที่ต้องการความเป็นส่วนตัวของข้อมูล สามารถใช้ได้กับผู้ใช้งานที่มีพื้นฐานด้านเทคโนโลยีและการเขียนโปรแกรมด้วยภาษา Python และมีความรู้ความเข้าใจเกี่ยวกับการควบคุมความเป็นส่วนตัวของข้อมูล ดังนั้นกลุ่มผู้ใช้โปรแกรมจะเป็นบุคคลที่ต้องการความเป็นส่วนตัวของข้อมูลของอุปกรณ์ไอโอทีและมีความเข้าใจเกี่ยวกับเทคโนโลยีและการเขียนโปรแกรมด้วยภาษา Python ในระดับพื้นฐาน

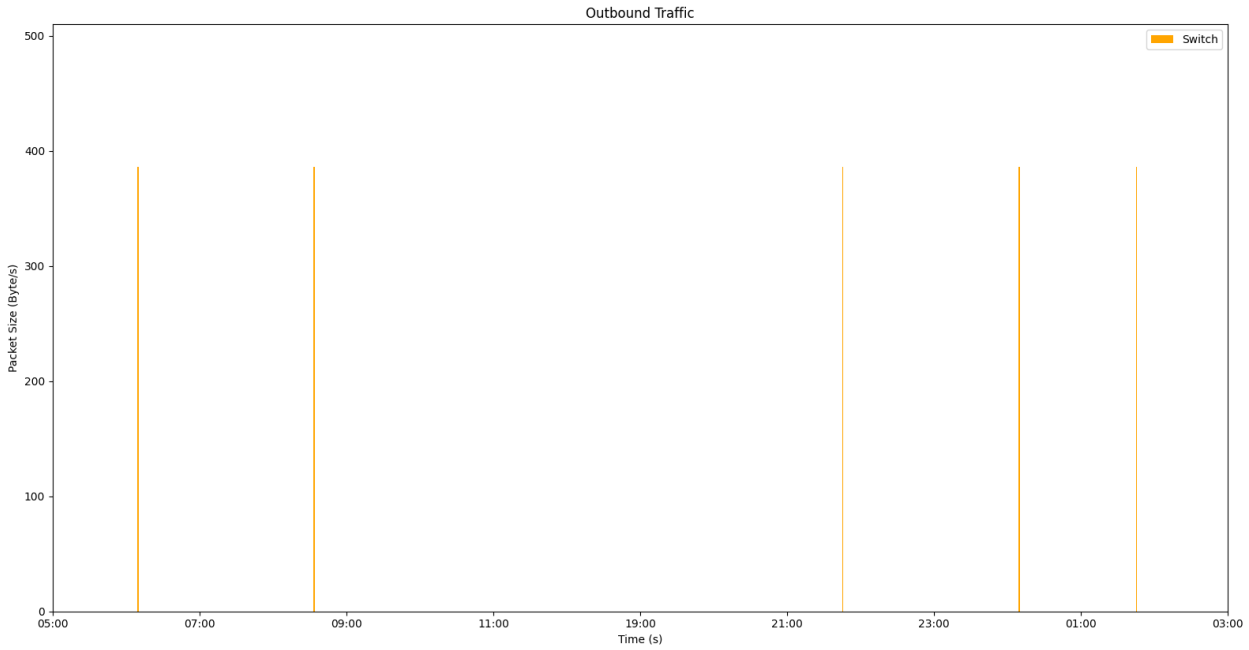
3.12 การใช้โปรแกรม Wireshark ในการอ่านผลลัพธ์

จับข้อมูลเครือข่ายโดยเลือกอินเตอร์เฟซเครือข่ายที่ต้องการวิเคราะห์หลังจากที่ได้จับข้อมูลเครือข่ายเป็นระยะเวลาที่เพียงพอ ให้หยุดการจับข้อมูล ส่งออกการวิเคราะห์แพ็กเก็ตเป็น CSV จะได้ไฟล์ที่มีข้อมูลจากการวิเคราะห์เครือข่ายโดยใช้ Wireshark ซึ่งสามารถนำไปวิเคราะห์และใช้อ่านผลลัพธ์ต่อไป

บทที่ 4
การทดลอง และผลลัพธ์

เนื้อหาในบทนี้จะเกี่ยวกับการในการทดสอบการทำงานของระบบการสุ่มส่งแพ็กเก็ตปลอมเข้าเครือข่ายอินเทอร์เน็ตซึ่งขึ้นอยู่กับเวลาด้วยฟังก์ชันชี้กำลัง เพื่อให้ผู้สังเกตการณ์ไม่สามารถคาดเดากิจกรรมของอุปกรณ์ไอโอทีที่ส่งแพ็กเก็ตไปยังเซิร์ฟเวอร์ ทำให้ผู้ใช้อุปกรณ์ไอโอทีมีความเป็นส่วนตัว และปลอดภัยมากขึ้น เช่น ในเวลาที่ไม่มีการใช้งานของอุปกรณ์ไอโอที ทำให้สามารถอนุมานได้ว่าผู้ใช้นั้นไม่อยู่บ้านหรือกำลังนอนหลับ ซึ่งอัลกอริทึมจะนำแพ็กเก็ตเก่าส่งสุ่มเข้าไปยังเซิร์ฟเวอร์จากนั้นให้เซิร์ฟเวอร์ตรวจสอบที่ทำหน้าที่ตรวจสอบรหัสของแต่ละแพ็กเก็ตที่ส่งเข้ามาจาก เราต์เตอร์ต้นทางแล้วเทียบกับรหัสที่จัดเก็บบนฐานข้อมูลก่อนที่จะส่งไปให้เซิร์ฟเวอร์ผู้ให้บริการ

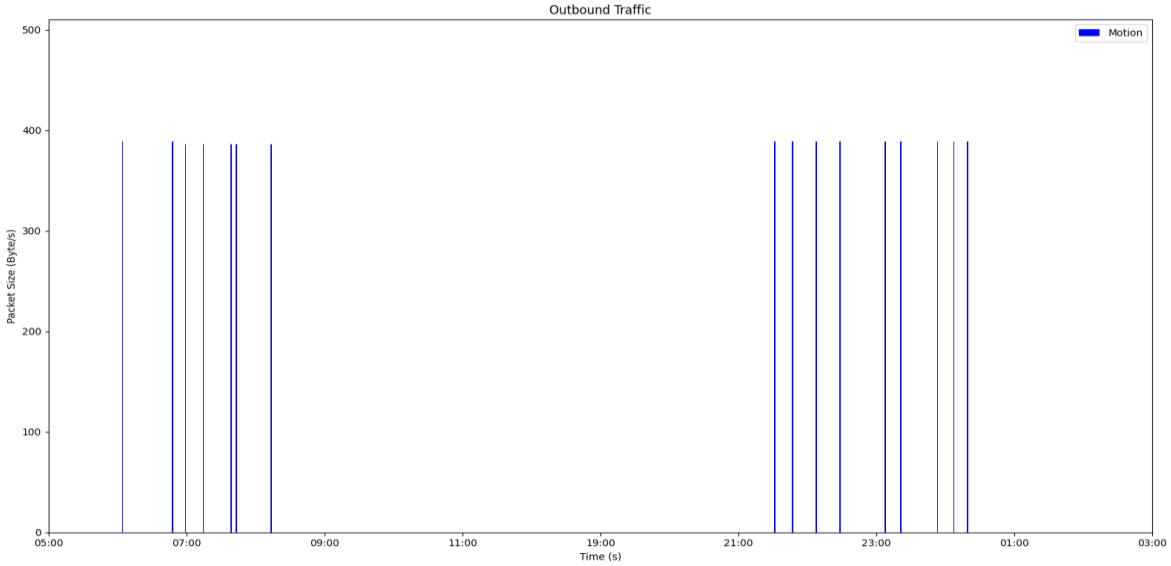
4.1 ปริมาณทราฟิกการใช้สวิตช์หลอดไฟฟ้าอัจฉริยะ



รูปที่ 4.1 แสดงปริมาณทราฟิกการใช้สวิตช์หลอดไฟฟ้าอัจฉริยะใน 1 วัน

จากกราฟแรกแสดงถึงการใช้หลอดไฟเปิดปิดของผู้ใช้ใน 1 วันผู้สังเกตการณ์สามารถเดาได้ว่าเวลานอนกับเวลาออกบ้านว่าช่วงไหนบ้าง เช่น เกิดการส่งแพ็กเก็ตของหลอดไฟในเวลา 6 โมงเช้า และ 8 โมงครึ่ง สามารถเดาได้ว่าผู้ใช้กำลังอยู่บ้านตื่นนอนจนถึงเวลาปิดไฟถึงจะออกจากบ้านทำให้สามารถทราบได้ว่าผู้ใช้กลับบ้าน และเข้านอนในช่วงเวลาไหนบ้าง และช่วงไหนผู้ใช้ไม่ได้รู้ตัวหรือไม่อยู่บ้านทำให้สามารถก่อโจรกรรมในอนาคตได้

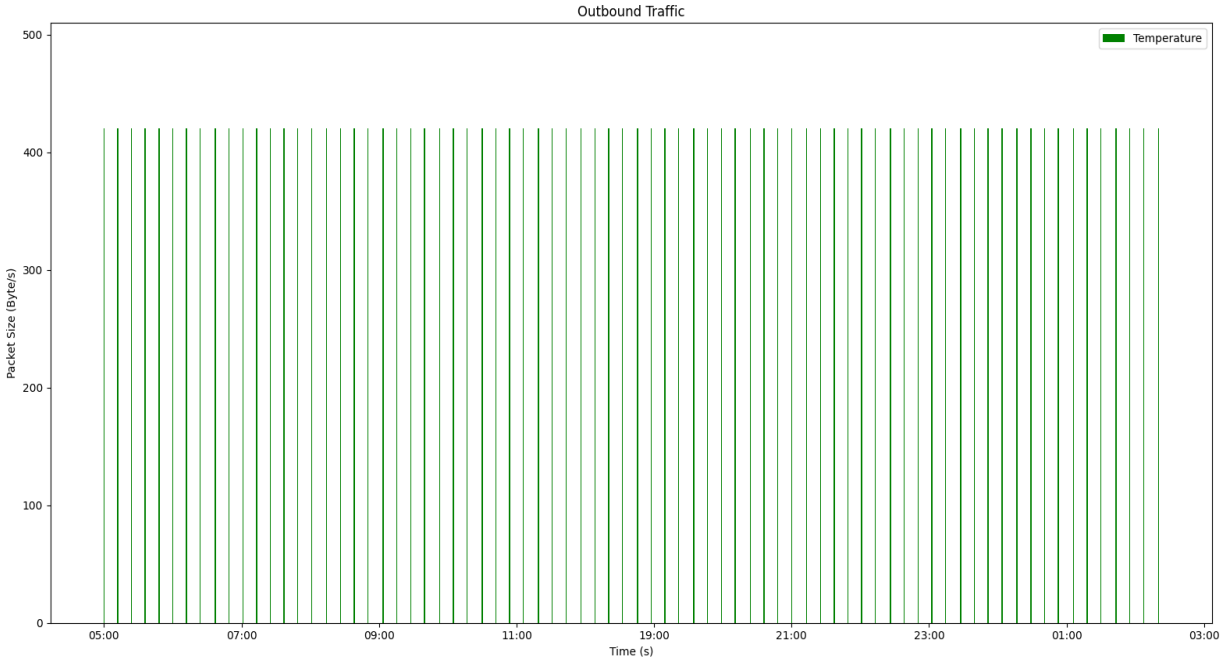
4.2 ปริมาณทราฟฟิกของการตรวจจับการเคลื่อนไหวของบุคคล



รูปที่ 4.2 แสดงปริมาณทราฟฟิกของการตรวจจับการเคลื่อนไหวของบุคคลใน 1 วัน

จากกราฟข้างต้นจะแสดงให้เห็นว่ามีการใช้งานของอุปกรณ์ตรวจจับการเคลื่อนไหวของบุคคลอยู่ทั้งหมดเป็นจำนวน 16 ครั้งภายในหนึ่งวัน มีการใช้งานให้ช่วงเช้าจำนวน 7 ครั้ง และช่วงเวลาเย็นถึงกลางคืนเป็นจำนวน 9 ครั้ง พบว่าในช่วงเวลากลางวันนั้นไม่มีการใช้งานของอุปกรณ์ตรวจจับการเคลื่อนไหวเลย เมื่อผู้สังเกตการณ์มาเห็นสามารถที่จะอนุมานได้ว่าผู้ใช้งานจะไม่อยู่บ้าน

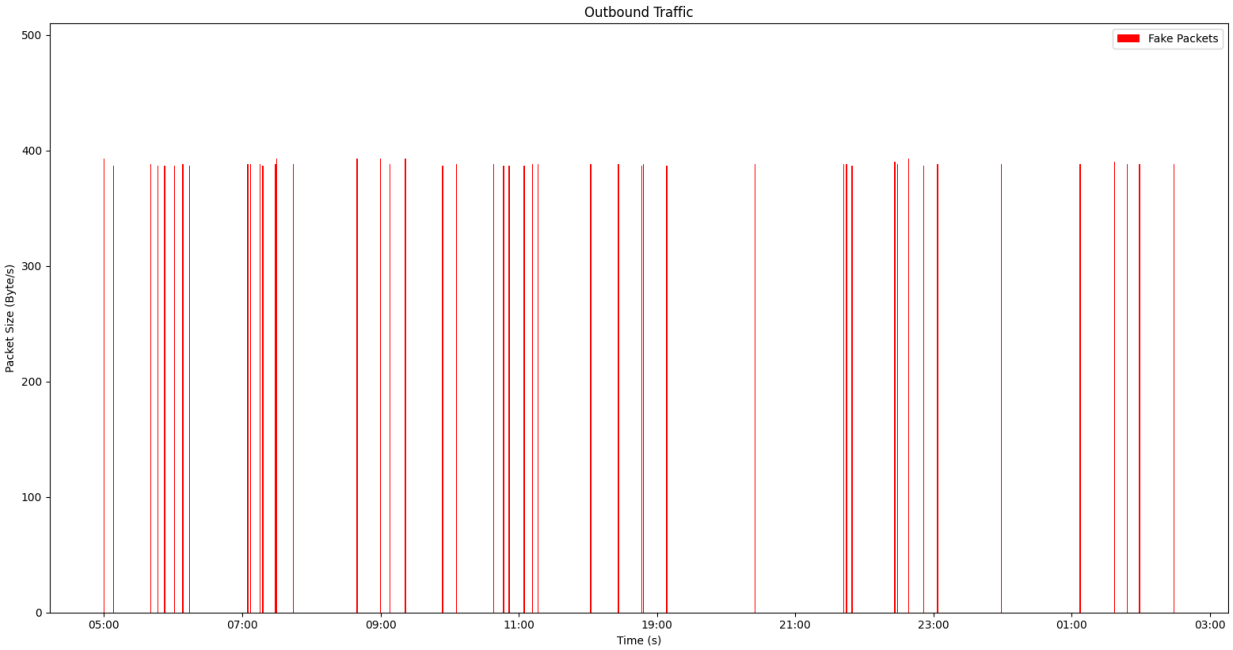
4.3 ปริมาณทราฟฟิกจากเครื่องวัดอุณหภูมิอัจฉริยะ



รูปที่ 4.3 แสดงปริมาณทราฟฟิกจากเครื่องวัดอุณหภูมิอัจฉริยะใน 1 วัน

จากกราฟข้างต้นจะแสดงให้เห็นว่า มีการใช้งานของเครื่องวัดอุณหภูมิตลอดทั้งวันมีเพราะอุปกรณ์ไอโอทีชนิดนี้จะมีการดึงข้อมูล (fetch) ตลอดช่วงระยะเวลาหนึ่ง ทำให้เมื่อผู้สังเกตการณ์เห็นสามารถที่จะมองรูปแบบของปริมาณทราฟฟิกออกแล้วทำการกรองทราฟฟิกออก

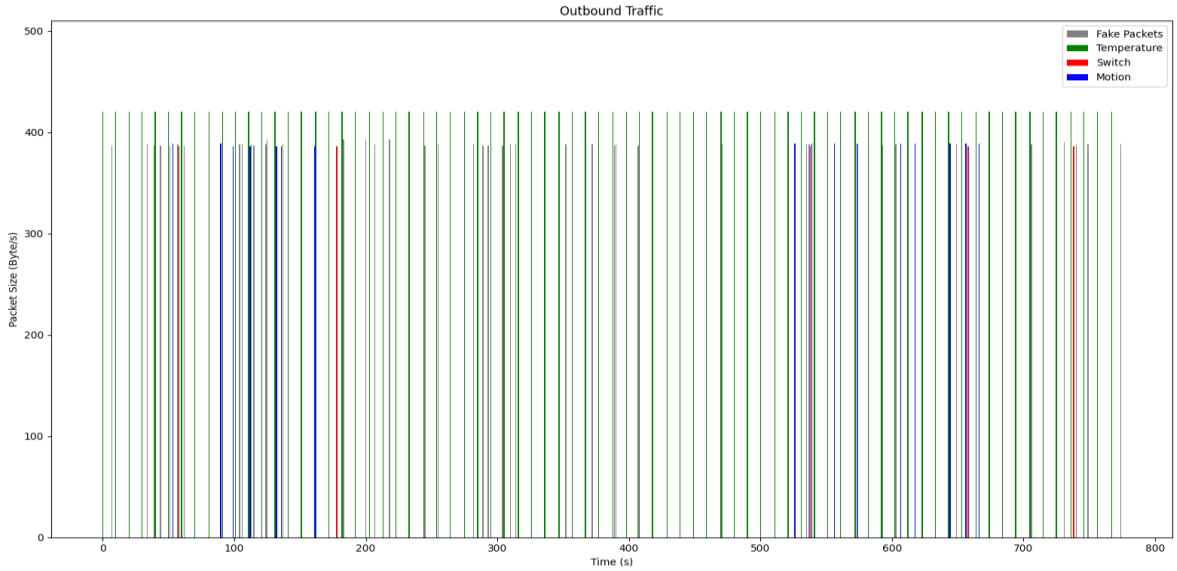
4.4 การส่งแพ็กเก็ตปลอมจากเราต์เตอร์ผู้ใช้



รูปที่ 4.4 แสดงการส่งแพ็กเก็ตปลอมจากเราต์เตอร์ผู้ใช้ในหนึ่งวัน

จากกราฟการส่งแพ็กเก็ตปลอมเป็นการส่งแพ็กเก็ตปลอมเข้าสู่เครือข่ายอินเทอร์เน็ต ผู้สังเกตการณ์เห็นแล้วจะอนุมานพฤติกรรมยากขึ้น เนื่องจากผู้สังเกตการณ์อาจเข้าใจว่ามีผู้ใช้กำลังทำอะไรบางอย่างอยู่ในบ้านโดยที่จริงแล้วผู้ใช้ไม่ได้อยู่บ้านจริง ผู้สังเกตการณ์อาจจะอนุมานคลาดเคลื่อนได้ หากเป็นผู้ประสงค์ร้ายที่จะก่ออาชญากรรมต่อผู้ใช้ลดความอยากก่อเหตุเหล่านั้นได้ การส่งแพ็กเก็ตปลอมจะไม่สามารถคาดเดารูปแบบการส่งได้อีกด้วย เนื่องจากความน่าจะเป็นที่ใช้การกระจายแบบปัวส์ซองที่ทำให้รูปแบบการส่งไม่มีความต่อเนื่องกัน

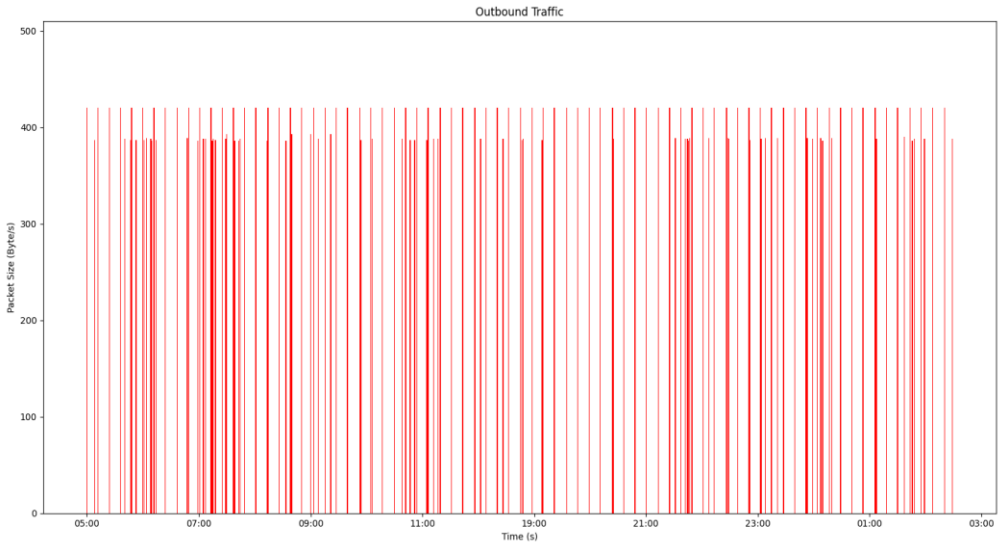
4.5 ทราฟฟิกต่าง ๆ ขอไอโอทีของผู้ใช้ที่แยกจากอุกปกรณ์ต้นทาง



รูปที่ 4.5 แสดงทราฟฟิกรวมของไอโอทีของผู้ใช้ที่แยกจากอุกปกรณ์ต้นทาง

กราฟการแสดงรูปทราฟฟิกไอโอทีทั้งหมดที่มีการแยกสีตามแหล่งต้นกำเนิดของอุปกรณ์ แสดงถึงในช่วงที่ไม่มีการใช้งานอุปกรณ์จะมีการส่งแพ็กเก็ตปลอมเข้าไปในเครือข่ายไป โดยส่วนใหญ่แพ็กเก็ตปลอมจะส่งในช่วงที่ไม่มีการใช้อุปกรณ์ และมีการส่งในช่วงในช่วงที่มีการใช้ด้วยเนื่องจากถ้าหากมีการส่งแพ็กเก็ตปลอมในช่วงที่ไม่มีการใช้งานอุปกรณ์ อาจทำให้ผู้สังเกตการณ์สามารถอนุมานรูปแบบการส่งแพ็กเก็ตปลอมได้ ส่งผลให้การป้องกันนั้นอาจถูกลดประสิทธิภาพลง และไม่สามารถป้องกันได้ในที่สุด จึงต้องส่งมีการแพ็กเก็ตปลอมทุก ๆ ช่วงเวลาทั้งเมื่อมีการใช้ และไม่มีการใช้อุปกรณ์ไอโอที

4.6 ทราฟฟิกของไอโอทีของผู้ใช้ที่แยกจากอุกปกรณ์ต้นทางจากมุมมองจากผู้สังเกตการณ์



รูปที่ 4.6 แสดงทราฟฟิกของไอโอทีของผู้ใช้ที่แยกจากอุกปกรณ์ต้นทางจากมุมมองจากผู้สังเกตการณ์

การแสดงภาพข้างต้นเป็นการแสดงถึงความสำคัญของการรักษาความเป็นส่วนตัวของผู้ใช้งานอุปกรณ์ไอโอที แม้ว่าผู้ใช้งานอาจไม่ได้อยู่หรือไม่ได้ใช้งานอุปกรณ์ไอโอทีอยู่เสมอไปก็ตาม การรักษาความเป็นส่วนตัวนั้นเป็นสิ่งสำคัญที่จะช่วยให้ผู้สังเกตการณ์ไม่สามารถทราบหรือคาดเดาได้แม่นยำว่าผู้ใช้งานกำลังใช้งานอุปกรณ์ไอโอทีอยู่หรือไม่

บทที่ 5
บทสรุป และข้อเสนอแนะ

5.1 สรุปผล

โครงการนี้เป็นการพัฒนาการป้องกันจากการถูกสังเกตการณ์และอนุมานพฤติกรรมของผู้ใช้จากอุปกรณ์ IoT ซึ่งมาจากวิทยานิพนธ์ที่มีอยู่เดิมแล้วนำมาพัฒนาเพื่อให้สามารถใช้ได้จริงมากขึ้น เนื่องจากอุปกรณ์เหล่านั้นจะติดต่อกับเซิร์ฟเวอร์ผู้ให้บริการเพียงที่เดียวหรือน้อยที่ และดีเอ็นเอสของเซิร์ฟเวอร์สามารถอนุมานได้ระดับหนึ่งได้ว่าเป็นอุปกรณ์ตัวใด ส่งผลให้ผู้สังเกตการณ์สามารถอนุมานต่ออีกได้ว่าผู้ใช้มีพฤติกรรมอย่างไรในบ้าน เช่น ออกไปทำงาน นอนหลับ อยู่บ้าน ฯลฯ โดยผู้สังเกตการณ์อาจเป็นได้ทั้งผู้ดักจับข้อมูลจนถึงผู้ให้บริการทางอินเทอร์เน็ต โดยคนเหล่านั้นจะสามารถทราบได้ว่าผู้ใช้มีพฤติกรรมอย่างไร เพื่อนำไปใช้ในทางที่ผิด เช่น การซื้อขายข้อมูล การโฆษณาแฝง การโจรกรรมในบ้านของผู้ใช้ เป็นต้น โดยการทดลองการป้องกันความเป็นส่วนตัวด้วยการสร้างแบบจำลองระบบการป้องกันบนอุปกรณ์ราสเบอร์รี่พาย และข้อมูลของอุปกรณ์ไอโอที จะถูกสร้างเลียนแบบจากข้อมูลจริงที่ปล่อยออกมาจากอุปกรณ์ IoT ส่วนการสังเกตทราฟฟิกจะใช้ Wireshark และเก็บข้อมูลการสังเกตที่ได้มาพล็อตกราฟทราฟฟิกเพื่อตรวจสอบการทดลองส่งแพ็กเก็ตปลอมและทดลองอนุมานพฤติกรรมของผู้ใช้

จากการทดลอง เมื่อมีการตรวจจับทราฟฟิกของอุปกรณ์ไอโอทีจาก Wireshark นั้นลดความสามารถของการอนุมานพฤติกรรมของผู้ใช้ได้อย่างเห็นได้ชัด เมื่อพล็อตกราฟทราฟฟิกออกมาจะเห็นได้ว่าทราฟฟิกที่เข้าสู่เครือข่ายดูเหมือนมีการใช้งานอุปกรณ์ตลอดเวลาในบ้านจนทำให้ผู้สังเกตการณ์อนุมานคลาดเคลื่อน

5.2 ปัญหาที่พบและแนวทางการแก้ไขปัญหา

ปัญหาที่พบในการทำโครงการมีดังนี้

การทดลองการส่งและสังเกตการณ์ทราฟฟิกของอุปกรณ์ไอโอทีจะต้องทดลองในเครือข่ายอินเทอร์เน็ตระบบปิด กล่าวคือ จะต้องไม่มีทราฟฟิกอื่นๆที่ถูกตรวจจับในการทดลอง เช่น เว็บไซต์อื่น ๆ ข้อมูลแชทสนทนา หรือ การส่งแจ้งเตือน เป็นต้น อุปกรณ์ไอโอทีต้องเชื่อมต่อกับเราต์เตอร์ราสเบอร์รี่พายเท่านั้น เนื่องจากทราฟฟิกที่ได้จากการสังเกตจะคลาดเคลื่อนและตรวจสอบการส่งแพ็กเก็ตปลอมเข้าสู่เครือข่ายได้หรือไม่

การวัดผลของค่าความสามารถในความมั่นใจของผู้สังเกตุการณ์และ bandwidth overhead โดยใช้สูตรที่กล่าวมานั้นใช้เวลาทำความเข้าใจเป็นเวลานาน จึงทำให้การกำหนดความน่าจะเป็นในสูตร ต้องทดลองใช้การกระจายต่างๆและทดลองวาดกราฟแล้วนำมาตรวจสอบผลลัพธ์ที่ได้ โดยคัดเลือกจากการกระจายที่ไม่ดูตายตัวและต่อเนื่องกัน โดยอาจารย์ที่ปรึกษาในโครงการนี้ได้แนะนำให้ใช้การกระจายแบบปัวส์ซอง เมื่อ

นำไปใช้นั้นได้ผลลัพธ์ค่าความน่าจะเป็นได้ดีกว่าการกระจายแบบอื่นๆเพราะความน่าจะเป็นที่ได้มีค่าน้อยกว่า แสดงว่าอัตราการทำนายได้ถูกจะลดน้อยลงเช่นกัน

5.3 ข้อเสนอแนะและแนวทาการพัฒนาต่อ

1. การกระจายของความน่าจะเป็นแนะนำให้ใช้การกระจายแบบปัวส์ซอง
2. การทดลองทราฟฟิกจะต้องลองกับอุปกรณ์ IoT ของจริงเพื่องประสิทธิภาพของผลลัพธ์ที่ดีกว่า
3. ค่าความน่าจะเป็นของผู้ใช้และทราฟฟิกจริงอาจมีการใช้ค่าความน่าจะเป็นที่ต่างกัน เนื่องจากการตัดสินใจและการเกิดเหตุการณ์ต่างๆนั้นมีอิสระต่อกัน

บรรณานุกรม

[1] Apthorpe, N., Huang, D. Y., Reisman, D., Narayanan, A., & Feamster, N. (2018). Keeping the smart home private with smart (er) iot traffic shaping. arXiv preprint arXiv:1812.00955.

[2] Liu, X., Zeng, Q., Du, X., Valluru, S. L., Fu, C., Fu, X., & Luo, B. (2021, October). Sniffmislead: Non-intrusive privacy protection against wireless packet sniffers in smart homes. In 24th international symposium on research in attacks, intrusions and defenses (pp. 33-47).

[3] Liu, X., Qiang, Z., Du, X., Valluru, S. L., Fu, C., Fu, X., & Luo, B.(2021). SniffMislead: Non-Instructive Privacy Protectionagainst Wireless Packet Sniffers in Smart Homes.

[4] Trimananda, R.,Varmaken, J., Markopoulou & Demsky, B. (2020). Packet-Level Signature for Smart Home Devices.

[5] Acar, A., Fereidooni, H., Abera, T., Sikder, A. K., Miettinen, M., Aksu, H., Conti, M., Sadeghi, A. R. & Uluagac, S. (2020). Peek-a-Boo: I see your smart home activities, even encrypted!.

[6] What is a DNS query? สืบค้นเมื่อวันที่ 5 ตุลาคม จาก https://www.cloudns.net/wiki/article/254/

[7] WiresharkforBeginners: A Visual Approach วันที่ 30 ตุลาคม จาก https://medium.com/@mackenziepech/wireshark-for-beginners-ba3c0771d01c

[8] Export Specified Packets from Wireshark วันที่ 30 ตุลาคม จาก https://www.wireshark.org/docs/wsug_html_chunked/ChIOExportSection.html

[9] ทำความรู้จัก Raspberry Pi วันที่ 30 ตุลาคม จาก http://www2.crma.ac.th/itd/Know/RBPI/index.asp

[10] เอ็มดี5. (2021, ตุลาคม 10). วิกิพีเดีย สารานุกรมเสรี. สืบค้นเมื่อ 02:45, ตุลาคม 10, 2021 จาก th.wikipedia.org/w/index.php?title=เอ็มดี5&oldid=9686943

[11] ฟังก์ชันแฮช. (2018, มีนาคม 5). วิกิพีเดีย สารานุกรมเสรี. สืบค้นเมื่อ 15:15, มีนาคม 5, 2018 จาก th.wikipedia.org/w/index.php?title=ฟังก์ชันแฮช&oldid=7491912

[12] Thailand, S. (2020, October 12). HTTP และ HTTPS คืออะไร และ แตกต่างกันอย่างไร - Seo Thailand. Seo Thailand. https://www.seothailand.in.th/http-and-https/

[13] เว็บเซิร์ฟเวอร์. (2021, พฤศจิกายน 18). วิกิพีเดีย สารานุกรมเสรี. สืบค้นเมื่อ 20:25, พฤศจิกายน 18, 2021 จาก th.wikipedia.org/w/index.php?title=เว็บเซิร์ฟเวอร์&oldid=9759750

[14] Wikipedia contributors. (2023, March 2). IP address. In Wikipedia, The Free Encyclopedia. Retrieved 15:41, April 5, 2023, from https://en.wikipedia.org/w/index.php?title=IP_address&oldid=1142467190

[15] Wikipedia contributors. (2023, March 13). Continuous uniform distribution. In Wikipedia, The Free Encyclopedia. Retrieved 15:51, April 5, 2023, from https://en.wikipedia.org/w/index.php?title=Continuous_uniform_distribution&oldid=1144473074

[16] Wikipedia contributors. (2023, March 28). Exponential distribution. In Wikipedia, The Free Encyclopedia. Retrieved 15:52, April 5, 2023, from https://en.wikipedia.org/w/index.php?title=Exponential_distribution&oldid=1147097347

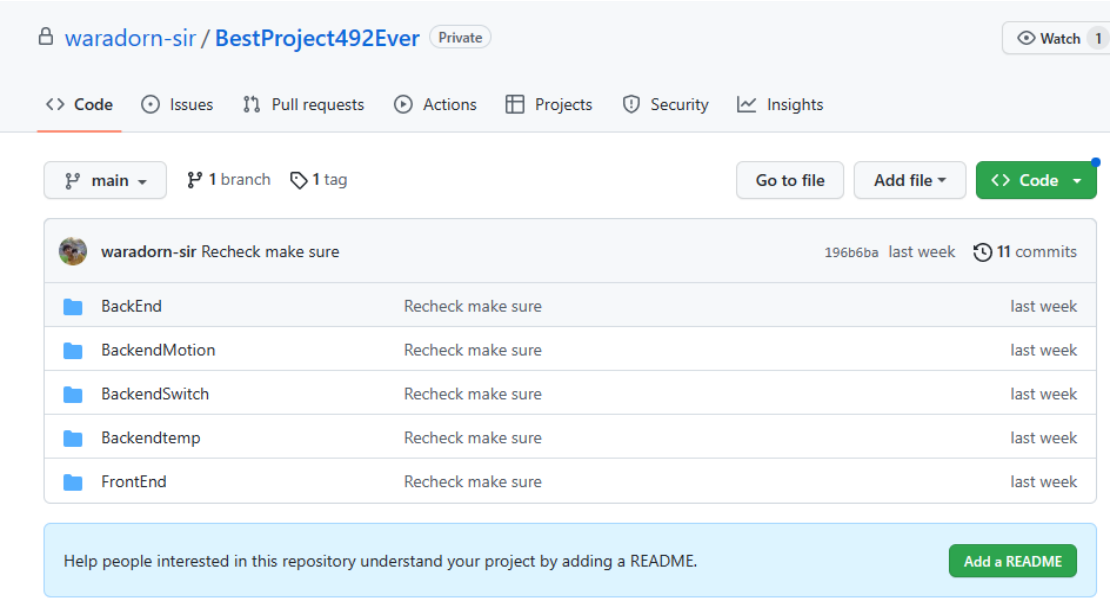
[17] Wikipedia contributors. (2023, March 28). Poisson distribution. In Wikipedia, The Free Encyclopedia. Retrieved 15:52, April 5, 2023, from https://en.wikipedia.org/w/index.php?title=Poisson_distribution&oldid=1147031355

ภาคผนวก

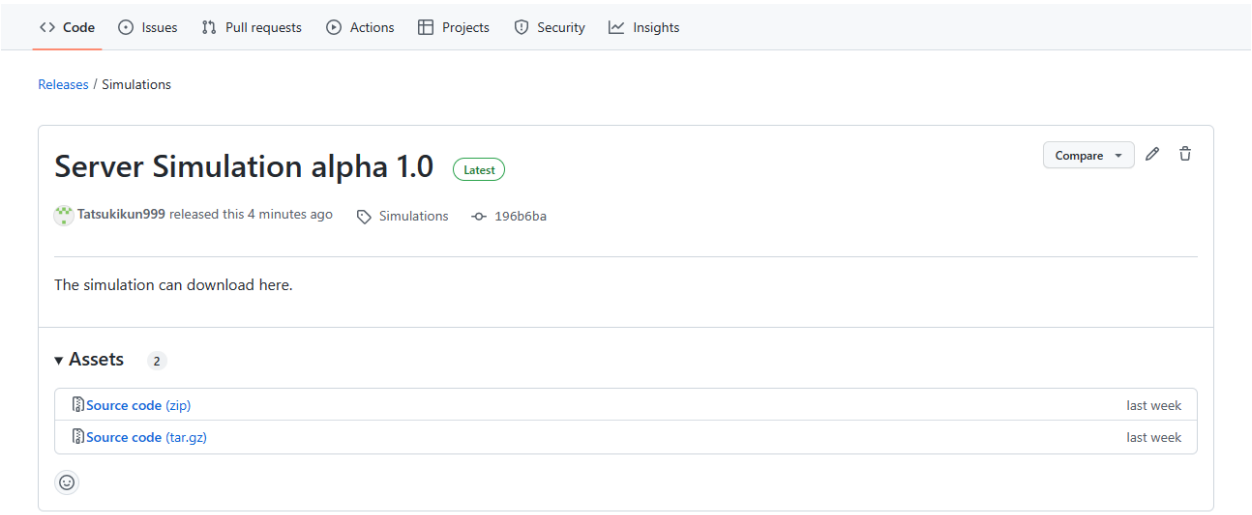
คู่มือการใช้งาน

สามารถอ่านจาก README หากติดปัญหา README.md

1. เข้าไปที่เว็บไซต์ github.com หรือ https://cmu.to/4lKlQ



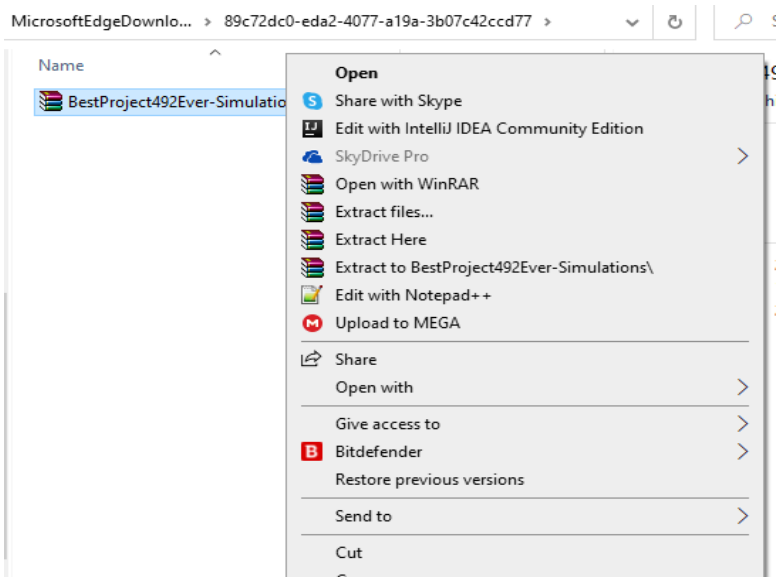
2. ไปที่ Server Simulation alpha 1.0



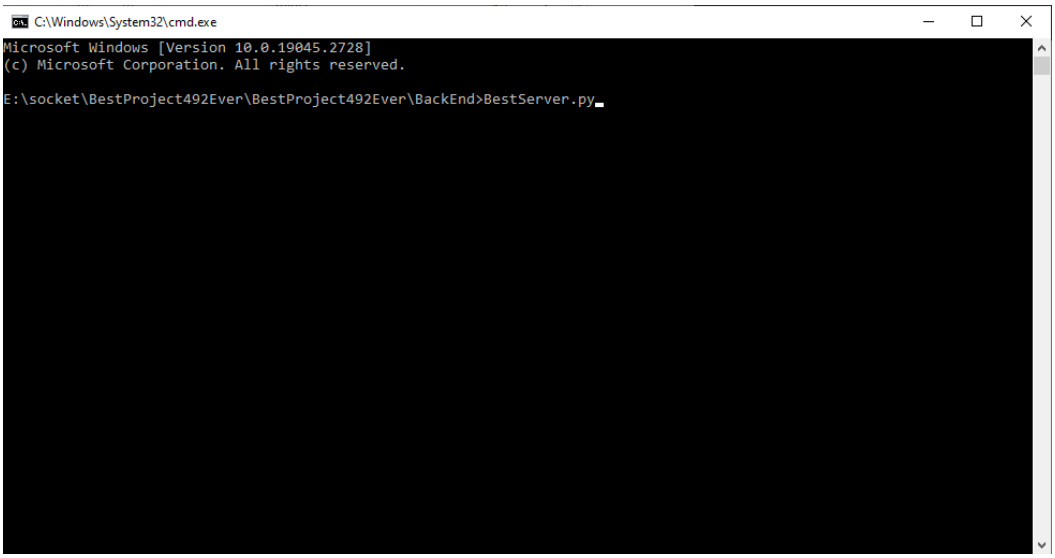
3. ดาวน์โหลดไฟล์ zip ของ source code

4. คลิกขวาเพื่อแตกไฟล์

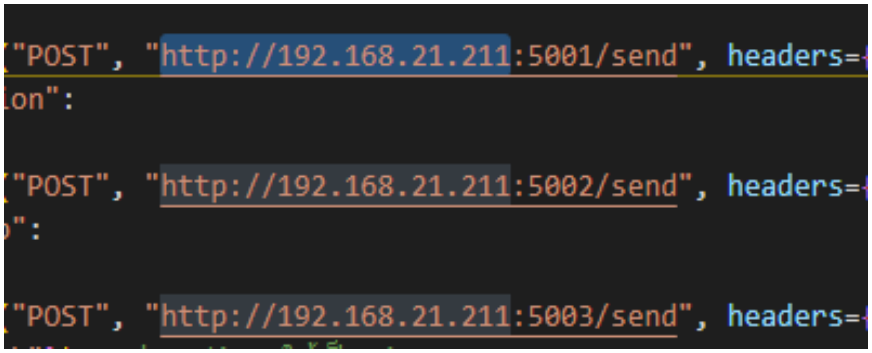
(คลิกขวาที่ไฟล์ > Extract Here หรือ Extract File... ในกรณีที่ประสงค์แตกไฟล์ในโฟลเดอร์ที่ต้องการ)



5. รันเซิร์ฟเวอร์แต่ละตัวโดยการผ่าน Terminal เข้า directory ของแต่ละไฟล์ โดยใช้คำสั่ง python ตามด้วยชื่อไฟล์เพื่อรัน



6. แก้เลข IP ทุกครั้งที่มีการเปลี่ยนการเชื่อมต่อเน็ตเวิร์ค



ประวัติผู้จัดทำ

ชื่อ-นามสกุล : ไตรภพ ศรีมณี

ระดับการศึกษา : ปริญญาตรี สาขาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเชียงใหม่

E-mail : traiphob.srimanee@gmail.com

การฝึกงาน : Like Me Co., Ltd.

กิจกรรมที่เคยแข่งขัน :

1. National Software Contest 2023 (ผ่านรอบคัดเลือก)

มีความสนใจ :

1. Socket network programming,
2. Network engineering

ประวัติผู้จัดทำ

ชื่อ-นามสกุล : นาย วราดร ศิริพันธุ์

ระดับการศึกษา : ปริญญาตรี สาขาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเชียงใหม่

E-mail : waradorn.sir@gmail.com

การฝึกงาน : Toyota Tsusho Systems (Thailand) co. ltd

กิจกรรมที่เคยแข่งขัน :

1. National Software Contest 2023 (ผ่านรอบคัดเลือก)
2. THAILAND CYBER TOP TALENT 2022 SENIOR (ผ่านรอบคัดเลือก)

มีความสนใจ : ความมั่นคงปลอดภัยทางไซเบอร์ และการศึกษาต่อศึกษาต่อปริญญาโท สาขาความปลอดภัยทางไซเบอร์