# การตรวจหาการบุกรุกเครือข่ายด้วยแผนภูมิควบคุมค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง

# Anomaly Detection with EWMA Control Chart


**ศิริพงา รัญเสวะ**

**Siriphanga Ransewa**


**วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญา**
**วิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์**
**มหาวิทยาลัยสงขลานครินทร์**

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science in Computer Science
Prince of Songkla University
2562

# การตรวจหาการบุกรุกเครือข่ายด้วยแผนภูมิควบคุมค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง

# Anomaly Detection with EWMA Control Chart

ศิริพงา รัญเสวะ

Siriphanga Ransewa

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญา
วิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์
มหาวิทยาลัยสงขลานครินทร์

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science in Computer Science
Prince of Songkla University
2562

**ชื่อวิทยานิพนธ์** การตรวจหาการบุกรุกเครือข่ายด้วยแผนภูมิควบคุมค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง

**ผู้เขียน** นางสาวศิริพงา รัญเสวะ

**สาขาวิชา** วิทยาการคอมพิวเตอร์

---

**อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก**

.....

(ผู้ช่วยศาสตราจารย์ ดร.นิษฐิดา เอลซ์)

**อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม**

.....

(รองศาสตราจารย์ ดร.สาธิต อินทจักร์)

**คณะกรรมการสอบ**

.....ประธานกรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.ชัชชัย คุณบัว)

.....กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.นิษฐิดา เอลซ์)

.....กรรมการ

(รองศาสตราจารย์ ดร.สาธิต อินทจักร์)

.....กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.สุภาภรณ์ กานต์สมเกียรติ)

บัณฑิตวิทยาลัย มหาวิทยาลัยสงขลานครินทร์ อนุมัติให้นับวิทยานิพนธ์ฉบับนี้ เป็นส่วนหนึ่งของการศึกษา ตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์

.....

(ศาสตราจารย์ ดร.ดำรงศักดิ์ ฟ้ารุ่งสาง)

คณบดีบัณฑิตวิทยาลัย

ขอรับรองว่า ผลงานวิจัยชิ้นนี้เป็นผลงานมาจากการศึกษาวิจัยของนักศึกษาเอง และขอขอบพระคุณผู้ที่มีส่วนเกี่ยวข้องทุกท่านไว้ ณ ที่นี้

ลงชื่อ.....
(ผู้ช่วยศาสตราจารย์ ดร.นิษฐิดา เอลซ์)
อาจารย์ที่ปรึกษาวิทยานิพนธ์

ลงชื่อ.....
(รองศาสตราจารย์ ดร.สาธิต อินทจักร์)
อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

ลงชื่อ.....
(นางสาวศิริพงา รัญเสวะ)
นักศึกษา

ข้าพเจ้าขอรับรองว่า ผลงานวิจัยนี้ไม่เคยเป็นส่วนหนึ่งในการอนุมัติปริญญาในระดับใดมาก่อนและไม่ได้ถูกใช้ในการยื่นขออนุมัติปริญญาในขณะนี้

ลงชื่อ.....

(นางสาวศิริพงา รัญเสวะ)

นักศึกษา

**ชื่อวิทยานิพนธ์** การตรวจหาการบุกรุกเครือข่ายด้วยแผนภูมิควบคุมค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง
**ผู้เขียน** นางสาวศิริพงา รัญเสวะ
**สาขาวิชา** วิทยาการคอมพิวเตอร์
**ปีการศึกษา** 2561

## บทคัดย่อ

อัตราการโจมตีทางเครือข่ายคอมพิวเตอร์ในปัจจุบัน เพิ่มขึ้นตามอัตราการขยายตัวของระบบเครือข่ายอินเทอร์เน็ต ประเภทของการโจมตีได้พัฒนาและเปลี่ยนแปลงไปจากเดิมมาก ทำให้การตรวจหาทำได้ยากกว่าการโจมตีในสมัยก่อน งานวิจัยชิ้นนี้ เสนอขั้นตอนวิธีในการตรวจหาความผิดปกติบนเครือข่ายคอมพิวเตอร์ในรูปแบบที่เรียกว่า Pulse wave Distributed Denial of Service (Pulse wave DDoS) โดยใช้ทฤษฎี encoding ข้อมูลด้วยชานนอนเอนโทรปี ค่าที่ได้จะถูกนำมาออกแบบแผนภูมิควบคุม โดยใช้แผนภูมิควบคุมค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง ซึ่งมีตัวแปรที่สำคัญที่เป็นตัวบ่งชี้การโจมตี และตัวแปรที่มีผลต่อสมรรถนะของตัวตรวจหาความผิดปกติสามตัวแปร ได้แก่ Threshold, Subgroup และ Group รูปแบบการโจมตีที่ได้ทดสอบแบ่งออกเป็นสองประเภทใหญ่ ๆ คือการโจมตีแบบกำหนดตำแหน่งและระยะเวลาของการเกิดการโจมตีเอง จำนวนสี่รูปแบบ และแบบสุ่มที่มีตำแหน่งและระยะเวลาของการโจมตี กำหนดด้วยค่าส่วนเบี่ยงเบนมาตรฐาน $(\sigma)$ สามค่าคือ $\sigma = \{5, 15, 30\}$ และใช้การสุ่มแบบยูนิฟอร์ม จากผลการทดลองได้แสดงให้เห็นว่า ขั้นตอนวิธีในการตรวจหาความผิดปกติที่ได้นำเสนอ สามารถตรวจหาความผิดปกติของการโจมตีแบบ Pulse wave DDoS ได้ ทั้งรูปแบบที่กำหนดเองและแบบสุ่ม

**Thesis Title** Anomaly Detection with EWMA Control Chart
**Author** Miss.Siriphanga Ransewa
**Major Program** Computer Science
**Academic Year** 2018

## ABSTRACT

Computer network attacks have been occurring more frequently with the growth of the internet. The types of attacks have evolved from those of the past, causing difficulties for network attack detection. This thesis proposes an algorithm for network anomaly detection of a Pulse wave Distributed Denial of service attack (Pulse wave DDoS) by applying Shannon entropy encoding to source port data. The encoding data are used to design a control chart which uses an exponentially weighted moving average. The capacity of our control chart depends on three parameters including group, subgroup, and threshold values. The testing data are categorized into two major patterns. The first patterns consist of four customized attack patterns. The second patterns were random attacks that varied both the position and interval of the attack times. The random patterns were generated by a uniform distribution determined by the standard deviation, $\sigma = \{5, 15, 30\}$. The experimental results show that our proposed algorithm is able to detect the anomaly attack of Pulse wave DDoS for both customized and random attack patterns.

# กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จได้ด้วยความช่วยเหลือและสนับสนุนจากบุคคลหลายฝ่าย ผู้วิจัยรู้สึกซาบซึ้งและขอกราบขอบพระคุณอย่างสูงมา ณ โอกาสนี้ คือ

ผู้ช่วยศาสตราจารย์ ดร.นิษฐิดา เอลซ์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่กรุณาให้ความรู้ คำปรึกษาแนะนำ และช่วยเหลือในการแก้ปัญหาต่าง ๆ ให้แก่ผู้วิจัยเสมอมา รวมถึงถ่ายทอดหลักการแนวคิดในการพัฒนาตัวเองและคุณธรรมสำหรับวิชาชีพแก่ผู้วิจัยมาโดยตลอด

รองศาสตราจารย์ ดร.สาธิต อินทจักร์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม ช่วยให้คำแนะนำและช่วยเหลือในการแก้ปัญหาให้แก่ผู้วิจัย พร้อมทั้งถ่ายทอดความรู้ในเรื่องต่าง ๆ อีกทั้งยังตรวจทานและแก้ไขวิทยานิพนธ์ให้แก่ผู้วิจัย

ผู้ช่วยศาสตราจารย์ นิธิ ทะนนท์ อาจารย์ประจำภาควิชาวิทยาการคอมพิวเตอร์ ที่ให้ข้อเสนอแนะในการทำวิทยานิพนธ์ และดูแลการทำวิทยานิพนธ์มาโดยตลอด

ผู้ช่วยศาสตราจารย์ ดร.ชัชชัย คุณบัว ประธานกรรมการสอบวิทยานิพนธ์ ที่กรุณาช่วยตรวจทานและแก้ไขวิทยานิพนธ์ให้มีความสมบูรณ์

ผู้ช่วยศาสตราจารย์ ดร.สุภาภรณ์ กานต์สมเกียรติ กรรมการสอบวิทยานิพนธ์ ที่ให้คำปรึกษา และกรุณาช่วยตรวจทานและแก้ไขวิทยานิพนธ์ให้มีความสมบูรณ์

อาจารย์ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยสงขลานครินทร์ทุกท่านที่ให้ความรู้ทางด้านวิชาการ ซึ่งสามารถนำความรู้นี้มาใช้ในการทำวิทยานิพนธ์

เจ้าหน้าที่ภาควิชาวิทยาการคอมพิวเตอร์ และเจ้าหน้าที่บัณฑิตวิทยาลัยทุกท่านที่ให้ความช่วยเหลือ และอำนวยความสะดวกเกี่ยวกับเอกสารต่าง ๆ

นายสกล จันทร์ขจร นักศึกษาภาควิชาวิทยาการคอมพิวเตอร์ ที่ให้คำแนะนำและดูแลการทำวิทยานิพนธ์มาโดยตลอด

เพื่อน ๆ พี่ ๆ และน้อง ๆ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ ที่ให้คำปรึกษา และช่วยเหลือในการทำวิทยานิพนธ์

คุณแม่วิชณี รัญเสวะ คุณพ่อไวกูล รัญเสวะ และสมาชิกในครอบครัวทุกคน ที่ให้การสนับสนุนคอยเป็นห่วงสุขภาพ รวมทั้งให้การสนับสนุนในการทำวิทยานิพนธ์แก่ผู้วิจัยมาโดยตลอด

ผู้วิจัยขอขอบพระคุณทุกท่านเป็นอย่างสูง ณ โอกาสนี้ด้วย

ศิริพงา รัญเสวะ

# สารบัญ

**หน้า**

# สารบัญ (ต่อ)

**หน้า**

# สารบัญ (ต่อ)

**หน้า**

# รายการตาราง

**ตาราง** **หน้า**

# รายการภาพประกอบ

**ภาพประกอบ** **หน้า**

# บทที่ 1

# บทนำ

## 1.1 ที่มาและความสำคัญของงานวิจัย

ปัจจุบันระบบเครือข่ายคอมพิวเตอร์ได้เข้ามามีบทบาทในชีวิตประจำวันเป็นอย่างมาก การขยายตัวอย่างรวดเร็วของเครือข่ายอินเทอร์เน็ต ทำให้ช่องทางในการติดต่อสื่อสารระหว่างเครือข่ายเพิ่มขึ้นไปด้วย ส่งผลให้ผู้ใช้สามารถติดต่อสื่อสารกันได้สะดวกขึ้น ในขณะเดียวกัน เมื่อระบบเครือข่ายคอมพิวเตอร์ขยายตัวเพิ่มขึ้น การโจมตีทางเครือข่ายคอมพิวเตอร์ก็เพิ่มขึ้นด้วย

ประเภทของการโจมตีระบบเครือข่ายคอมพิวเตอร์ที่สร้างความเสียหายให้แก่องค์กรเป็นอย่างมากและเป็นที่สนใจในงานวิจัยนี้ คือ การโจมตีโดยปฏิเสธการให้บริการ (Denial of Service: DoS) และการโจมตีโดยปฏิเสธการให้บริการแบบกระจาย (Distributed Denial of Service: DDoS) ที่มีจุดประสงค์เพื่อขัดขวางไม่ให้ใช้งานได้ตามปกติ ระบบที่เชื่อมต่อกับอินเทอร์เน็ตมักจะถูกโจมตีแบบ DoS/DDoS เนื่องจากอินเทอร์เน็ตประกอบไปด้วยทรัพยากรที่มีอยู่อย่างจำกัดและทำให้หมดไปหรือทำให้มีน้อยลงได้ เช่น แบนด์วิดธ์ (Bandwidth) พลังในการประมวลผล (Processing Power) และพื้นที่ที่จำกัดในการเก็บข้อมูล เป็นต้น (Handley et al., 2006) การโจมตีแบบ DoS/DDoS มีการเพิ่มขึ้นและมีการเปลี่ยนแปลงอยู่ตลอดเวลา (ENISA, 2017; Kaspersky, 2017) ในปัจจุบันรูปแบบของการโจมตีแบบ DoS/DDoS ได้เปลี่ยนแปลงไปจากเดิมมากและยากต่อการตรวจหา เรียกการโจมตีรูปแบบนี้ว่า Pulse wave DDoS (Imperva, 2017) ซึ่งคุณลักษณะที่เด่นชัดของการโจมตีประเภทนี้ คือมีการโจมตีในช่วงระยะเวลาสั้น ๆ เกิดขึ้นแบบซ้ำ ๆ สม่ำเสมอเพื่อหลีกเลี่ยงการตรวจหา แต่สามารถสร้างความเสียหายได้เช่นเดียวกับ DDoS โดยทั่วไป

แนวทางที่ใช้ในการตรวจหาความผิดปกติ มีด้วยกัน 2 แนวทาง คือ การตรวจหาความผิดปกติ (Anomaly Detection) และการตรวจหาการใช้ไปในทางมิชอบ (Misuse Detection) (Bace, 2000; Denning, 1986) โดย Anomaly Detection เป็นการตรวจหาการโจมตีที่ตั้งอยู่บนพื้นฐานการตรวจหาพฤติกรรมการใช้ทรัพยากรของระบบคอมพิวเตอร์ที่ผิดปกติไปจากการใช้งานทั่วไป แนวทางในการตรวจหาวิธีนี้ จะพยายามแยกพฤติกรรมการใช้อย่างปกติที่ยอมรับได้ออกมาและให้นิยามพฤติกรรมการใช้แบบอื่น ๆ เป็นการใช้ที่ผิดปกติที่เป็นการโจมตี ส่วน Misuse Detection จะตรวจหาโดยอาศัยคุณลักษณะหรือหารูปแบบการใช้งานเครือข่ายที่ได้กำหนดไว้แล้วว่าเป็นการโจมตีแล้วนำมาเปรียบเทียบหรือค้นหารูปแบบของเหตุการณ์ที่เกิดขึ้นในระบบ เพื่อระบุว่า

เป็นการโจมตีโดยตรง ดังนั้นวิธีการนี้จึงต้องอาศัยความรู้เกี่ยวกับการโจมตีและพฤติกรรมการใช้ที่ไม่เหมาะสมเป็นอย่างดี เพื่อที่สามารถกำหนดรูปแบบที่ใช้ในการค้นหาการโจมตีได้อย่างถูกต้องและครอบคลุมการโจมตี

ในงานวิจัยนี้ได้ประยุกต์แผนภูมิควบคุม ที่ใช้ในการตรวจหาผลิตภัณฑ์ที่มีความบกพร่องในกระบวนการผลิต เพื่อควบคุมคุณภาพให้อยู่ในเกณฑ์ที่ยอมรับได้ (Montgomery, 2009) แผนภูมิควบคุมเป็นเครื่องมือที่มีประสิทธิภาพในการตรวจหาข้อมูลที่อยู่นอกการควบคุม ทำให้สามารถตรวจหาสาเหตุของความผิดปกติ เพื่อจะได้ป้องกันและแก้ไขได้อย่างทันท่วงที การนำแผนภูมิควบคุมมาประยุกต์ เพื่อตรวจหาความผิดปกติในระบบเครือข่าย ที่มีการโจมตีแบบ Pulse wave DDoS โดยข้อมูลหรือสัญญาณการโจมตีจะถูก Encode ด้วยเอนโทรปี และใช้แผนภูมิควบคุมค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง (Montgomery, 2009) ในการตรวจหารูปแบบของการโจมตี

## 1.2 วัตถุประสงค์ของการวิจัย

เพื่อศึกษา ออกแบบ และพัฒนาขั้นตอนวิธีในการตรวจหาความผิดปกติ แบบ Pulse wave DDoS

## 1.3 ขอบเขตของการดำเนินการวิจัย

1. รูปแบบการโจมตีที่ใช้ในงานวิจัยนี้คือ การโจมตีแบบ Pulse wave DDoS โดยใช้ Source Port บนโพรโทคอล TCP และ UDP

2. รูปแบบของการโจมตีที่จำลองขึ้น มีทั้งแบบที่ผู้โจมตีกำหนดเป็นช่วง และการสุ่มแบบยูนิฟอร์ม

## 1.4 ขั้นตอนและระยะเวลาการดำเนินการ

### 1.4.1 ขั้นตอนการดำเนินการ

1. ศึกษางานวิจัยและเอกสารที่เกี่ยวข้อง
2. ศึกษาเทคโนโลยีและเครื่องมือสำหรับงานวิจัย
3. กำหนดขอบเขตของปัญหาในการทำวิจัย
4. วิเคราะห์และออกแบบกระบวนการ
5. พัฒนาและทดสอบประสิทธิภาพกระบวนการที่ได้ออกแบบไว้
6. เขียนบทความวิจัยและเผยแพร่
7. จัดทำเอกสารวิทยานิพนธ์

ตารางที่ 1-1 แผนการดำเนินการวิจัย

| ขั้นตอน | 2560 | | | | | 2561 | | | | | | | | | | | | 2562 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 8 | 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 1 |
| 1 | | | | | | | | | | | | | | | | | | |
| 2 | | | | | | | | | | | | | | | | | | |
| 3 | | | | | | | | | | | | | | | | | | |
| 4 | | | | | | | | | | | | | | | | | | |
| 5 | | | | | | | | | | | | | | | | | | |
| 6 | | | | | | | | | | | | | | | | | | |
| 7 | | | | | | | | | | | | | | | | | | |

**1.4.2 ระยะเวลาดำเนินการวิจัย**

สิงหาคม 2560 – มกราคม 2562

## 1.5 สถานที่และเครื่องมือที่ใช้ในการวิจัย

**1.5.1 สถานที่**

ห้องวิจัยกลุ่มคอมพิวเตอร์และเครือข่าย CS209 ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่

**1.5.2 เครื่องมือที่ใช้**

1) ด้านฮาร์ดแวร์

- เครื่องคอมพิวเตอร์ส่วนบุคคล CPU Intel Core I7 2.4 GHz Hard Disk 1TB Ram 8 GB จำนวน 1 เครื่อง
- เครื่องคอมพิวเตอร์ส่วนบุคคล CPU Intel Core I7 2.4 GHz Hard Disk 2TB Ram 8 GB จำนวน 2 เครื่อง

2) ด้านซอฟต์แวร์

- ระบบปฏิบัติการ Windows 7 64 bit
- ระบบปฏิบัติการ Ubuntu 16.14
- โปรแกรมประยุกต์ MATLAB 2010a

## 1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้ขั้นตอนวิธีในการตรวจหาความผิดปกติ แบบ Pulse wave DDoS

2. สามารถตรวจหาความผิดปกติ เพื่อจะได้ตรวจสอบและป้องกันแก้ไขได้อย่างทันท่วงที

# บทที่ 2

# ทฤษฎีที่เกี่ยวข้อง

## 2.1 บทนำ

เนื้อหาในบทนี้เป็นการกล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้อง โดยเนื้อหาส่วนแรกกล่าวถึง ภัยคุกคามและการบุกรุกทางคอมพิวเตอร์ การโจมตีโดยปฏิเสธการให้บริการ การโจมตีโดยปฏิเสธการให้บริการแบบกระจาย รวมไปถึงเรื่องของแนวทางในการตรวจหาความผิดปกติ ต่อมาเป็นการอธิบายเรื่องข้อมูลเครือข่ายคอมพิวเตอร์ ทั้งในเรื่องของโพรโทคอล และหมายเลขพอร์ต จากนั้นได้อธิบายถึงการ Encode ข้อมูลด้วยเอนโทรปี การสร้างแผนภูมิควบคุม และแผนภูมิควบคุมค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง และสุดท้ายเป็นการกล่าวถึงงานวิจัยที่เกี่ยวข้อง

## 2.2 ภัยคุกคามและการบุกรุก

### 2.2.1 ภัยคุกคาม (Threat)

ภัยคุกคาม คือ บุคคล สิ่งของ หรือเหตุการณ์ต่าง ๆ ที่เป็นสาเหตุของภัยอันตราย ที่เกิดขึ้นกับระบบคอมพิวเตอร์ในรูปแบบของการทำลายข้อมูล การเปิดเผยข้อมูล การแก้ไขข้อมูลรวมไปถึงการทำให้ระบบไม่สามารถให้บริการแก่ผู้ใช้ได้ โดยภัยคุกคามอาจเกิดขึ้นจากอุบัติเหตุ เช่น ไฟไหม้ น้ำท่วม ฯลฯ หรือเกิดจากเจตนาของบุคคลที่ประสงค์ร้ายต่อระบบ เช่นการพยายามที่จะผ่านกระบวนการรักษาความปลอดภัยของคอมพิวเตอร์ (GFI Software, 2010)

### 2.2.2 การบุกรุก (Intrusion)

การบุกรุก คือ การกระทำใด ๆ ที่ส่งผลต่อการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้ของทรัพยากรในระบบ หรือพยายามข้ามผ่านมาตรการรักษาความปลอดภัยของระบบคอมพิวเตอร์ เช่น พยายามใช้สิทธิ์นอกเหนือจากที่ได้รับ หรือพยายามใช้สิทธิ์นั้นในทางที่ผิด วิธีการบุกรุกแบ่งออกเป็น 2 แบบคือ การบุกรุกแบบ Active และการบุกรุกแบบ Passive (Kruegel et al., 2005; Mohan et al., 2015)

#### 2.2.2.1 การบุกรุกแบบ Active

เป็นการบุกรุกที่ทำให้เกิดการเปลี่ยนแปลงของข้อมูล หรือ การสร้างข้อมูลขึ้นมาใหม่โดยการปลอมแปลง เช่น การเปลี่ยนแปลงข้อมูลในไฟล์ ไม่ว่าจะเป็นการแก้ไข เพิ่มเติม หรือลบข้อมูล รวมถึงการทำให้ระบบไม่สามารถให้บริการแก่ผู้ใช้ได้ การโจมตีประเภทนี้สามารถตรวจจับได้ง่าย

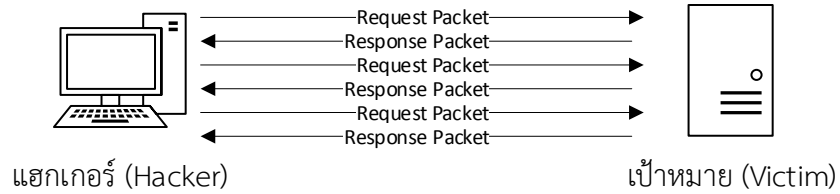
เนื่องจากมีร่องรอยการกระทำที่จัดว่าเป็นการบุกรุก ตัวอย่างประเภทของการโจมตีประเภทนี้ได้แก่ ไวรัส (Virus) ม้าโทรจัน (Trojan Horse) การโจมตีโดยปฏิเสธการให้บริการ (Denial of Service) เป็นต้น

**2.2.2.2 การบุกรุกแบบ Passive**

เป็นการบุกรุกที่ไม่ทำให้เกิดการเปลี่ยนแปลงของข้อมูล แต่เป็นการที่ผู้บุกรุกเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต เช่น การดักจับข้อมูลในสายสัญญาณ หรือเครือข่าย การบุกรุกประเภทนี้ตรวจจับได้ยาก เนื่องจากไม่ทิ้งร่องรอยการกระทำเอาไว้ แต่สามารถป้องกันได้ง่าย เช่น การ Encode ข้อมูลก่อนการรับส่ง เป็นต้น ตัวอย่างการโจมตีประเภทนี้ได้แก่ การดักจับข้อมูลต่าง ๆ ไม่ว่าจะเป็น Eavesdropping, Skimming, Sniffer หรือ Wiretap การปลอมตัว (IP Spoofing) หรือ การสแกนพอร์ต (Port Scanning) เป็นต้น

## 2.3 การโจมตีโดยปฏิเสธการให้บริการ (Denial of Service Attack)

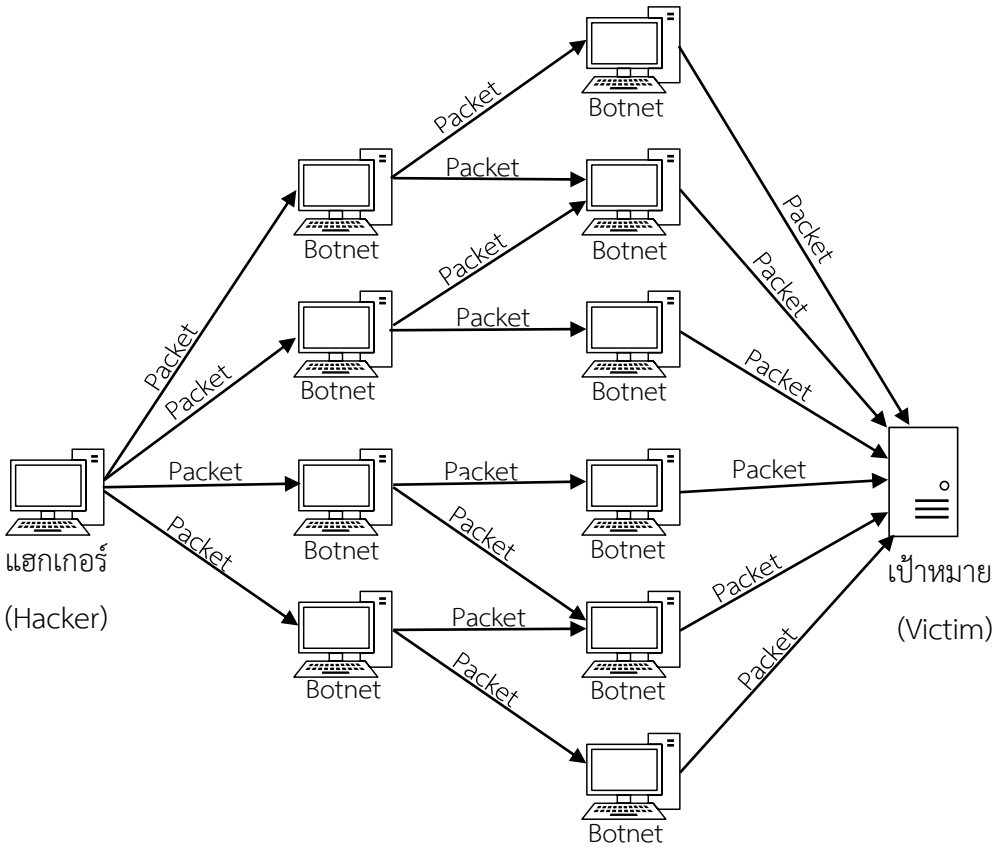
การโจมตีแบบ Denial of Service (DoS) โดยทั่วไปมีจุดประสงค์เพื่อขัดขวางไม่ให้ใช้งาน หรือทำให้เกิดความเสียหายต่อการใช้งานคอมพิวเตอร์ และทรัพยากรของระบบเครือข่าย ระบบที่เชื่อมต่อกับอินเทอร์เน็ตมักจะถูกโจมตีแบบ DoS เนื่องจากอินเทอร์เน็ตประกอบไปด้วยทรัพยากรที่มีอยู่อย่างจำกัด และสามารถถูกทำให้หมดไปได้ เช่น แบนด์วิดธ์ (Bandwidth) พลังในการประมวลผล (Processing Power) และพื้นที่ที่จำกัดของการเก็บข้อมูล โดยเป้าหมายในการโจมตีแบบ DoS ต้องการให้มีการใช้งานทรัพยากรที่มีอยู่จนถึงขั้นที่ทำให้ระบบมีปัญหาได้ (Handley et al., 2006) ประเภทของการโจมตีเพื่อขัดขวางและรบกวนการทำงานของเป้าหมายตามโพรโทคอลนั้นมีอยู่หลายรูปแบบ เช่น TCP Flood Attack (CERT, 1996-01), UDP Flood Attack (CERT, 1996-02), ICMP Flood Attack (CERT, 1999) เป็นต้น โดยวิธีการโจมตีนั้นผู้ไม่ประสงค์ดี หรือ แฮกเกอร์ (Hacker) จะส่งแพ็กเก็ตซึ่งเป็นหน่วยย่อยของข้อมูลเพื่อขอใช้บริการ (Request Packet) จำนวนมหาศาล ไปยังเป้าหมาย (Victim) เมื่อเป้าหมายได้รับแพ็กเก็ต ก็จะส่งแพ็กเก็ตตอบกลับ (Response Packet) จำนวนมาก ทำให้เครื่องเป้าหมายไม่สามารถให้บริการหรือใช้งานได้ ดังภาพประกอบที่ 2-1




ภาพประกอบที่ 2-1 การโจมตีแบบ DoS

## 2.4 การโจมตีโดยปฏิเสธการให้บริการแบบกระจาย (Distributed Denial of Service Attack)

การโจมตีแบบ Distributed Denial of Service Attack (DDoS) มีวัตถุประสงค์เพื่อขัดขวางการให้บริการเช่นเดียวกับการโจมตีแบบ DoS แต่แตกต่างกันตรงที่ เครื่องเป้าหมายจะมีแพ็กเก็ตที่ถูกส่งมาจากต้นทางหลายแหล่ง จึงเรียกการโจมตีแบบนี้ว่าการโจมตีแบบกระจาย (Distributed) ในขณะที่การโจมตีแบบ DoS แพ็กเก็ตจะถูกส่งมาจากต้นทางเพียงแหล่งเดียว (Aamir et al., 2013; DHS US-CERT, 2011) ตัวอย่างการโจมตีแบบ DDoS เช่น ผู้ไม่ประสงค์ดี หรือ แฮกเกอร์ จะทำการปล่อยไวรัส (Virus) หรือ โปรแกรมที่เป็นอันตราย เข้าไปควบคุมสั่งการเครื่องคอมพิวเตอร์ของเหยื่อเพื่อให้โจมตีเป้าหมายที่ต้องการโจมตีต่อไป เครื่องคอมพิวเตอร์ที่ถูกควบคุมเหล่านี้ เรียกว่า Botnet หรือ Zombie ส่งผลให้การโจมตีแบบ DDoS จะมีความรุนแรงมากกว่าแบบ DoS ผู้ไม่ประสงค์ดีจะทำการโจมตีสำเร็จได้อย่างรวดเร็วกว่าแบบ DoS ดังภาพประกอบที่ 2-2




ภาพประกอบที่ 2-2 การโจมตีแบบ DDoS

การโจมตีแบบ DoS/DDoS ในปัจจุบันมีแนวโน้มที่จะเพิ่มขึ้นเป็นอย่างมาก (ENISA, 2017; Kaspersky, 2017) เนื่องจากคอมพิวเตอร์เพียงเครื่องเดียวก็สามารถใช้เป็นเครื่องมือในการโจมตีได้ และโปรแกรมที่ใช้สำหรับโจมตี สามารถหาได้ทั่วไปบนอินเทอร์เน็ต

## 2.5 แนวทางในการตรวจหาความผิดปกติ

แนวทางในการตรวจหาความผิดปกติ เพื่อใช้ในการตรวจจับการโจมตีมี 2 แนวทาง คือ Anomaly Detection และ Misuse Detection (Bace, 2000; Denning, 1986; ปัทมา, 2555) โดย Anomaly Detection เป็นการตรวจหาการโจมตีที่ตั้งอยู่บนพื้นฐานการตรวจหาพฤติกรรมการใช้ทรัพยากรของระบบคอมพิวเตอร์ที่ผิดปกติไปจากการใช้งานปกติ แนวทางในการตรวจหาวิธีนี้ จะพยายามแยกพฤติกรรมการใช้อย่างปกติที่ยอมรับได้ออกมา และให้นิยามพฤติกรรมการใช้แบบอื่น ๆ เป็นการใช้ที่ผิดปกติที่เป็นการโจมตี

Misuse Detection จะตรวจหาการโจมตีโดยอาศัยคุณลักษณะหรือหารูปแบบการใช้งานเครือข่ายที่ได้กำหนดไว้แล้วว่าเป็นการโจมตี แล้วนำมาเปรียบเทียบหรือค้นหารูปแบบของเหตุการณ์ที่เกิดขึ้นในระบบ เพื่อระบุว่าเป็นการโจมตีโดยตรง ดังนั้นวิธีการนี้จึงต้องอาศัยความรู้เกี่ยวกับการโจมตีและพฤติกรรมที่ไม่เหมาะสมเป็นอย่างดี เพื่อที่สามารถกำหนดรูปแบบที่ใช้ในการค้นหาการโจมตีได้อย่างถูกต้อง และครอบคลุมการโจมตีได้ทั้งหมดที่รู้จัก สำหรับรายละเอียดของแนวทางการตรวจหาความผิดปกติทั้งสองแบบมีดังนี้

### 2.5.1 Anomaly Detection

การตรวจหาความผิดปกติด้วยแนวทาง Anomaly Detection ถือว่ากิจกรรมทั้งหมดเป็นกิจกรรมที่ปกติ ในการตรวจหาความผิดปกติจะต้องแยกกิจกรรมการทำงานปกติ ออกมา และให้กิจกรรมที่เหลือเป็นกิจกรรมที่ผิดปกติและถือว่าเป็นการโจมตี ตัวตรวจหาจะเก็บข้อมูลพฤติกรรมปกติของการใช้งานคอมพิวเตอร์ และมีเกณฑ์ในการชี้วัดต่าง ๆ เช่น ตัวชี้วัดทางสถิติ ตัวชี้วัดด้านความถี่ เป็นต้น หากมีเหตุการณ์ที่ต่างจากที่ระบุไว้ในระบบก็จะถือว่าเป็นเหตุการณ์ที่ผิดปกติ หรือมีเหตุการณ์ที่พยายามที่จะโจมตี การตรวจหาความผิดปกติด้วยแนวทางนี้ จะมีอัตราความผิดพลาดในการตรวจหาเชิงบวก (False Positive Rate) สูง ตัวอย่างเทคนิคที่ใช้สำหรับการตรวจจับการโจมตีตามแนวทางนี้ มีดังนี้

**2.5.1.1 Statistical Approach**

การใช้สถิติวิเคราะห์เพื่อตรวจหาความผิดปกตินั้น สามารถแบ่งได้เป็น 2 วิธีคือ การวิเคราะห์เชิงปริมาณ (Quantitative Analysis) และใช้การวัดทางสถิติ (Statistical Measure) ซึ่งจะใช้ความถี่ (Threshold Detection) เป็นเกณฑ์ในการแยกพฤติกรรม เทคนิคนี้จะใช้คุณสมบัติของผู้ใช้และพฤติกรรมของระบบ จะถูกอธิบายหรือแสดงในรูปแบบตัวเลข เช่น จำนวนไฟล์ที่มีการเข้าถึงในช่วงเวลาหนึ่ง จำนวนครั้งของการพยายามในการเข้าถึงข้อมูลที่ไม่สำเร็จ ปริมาณการใช้งานระบบ เป็นต้น ปัญหาที่สำคัญของวิธีการนี้คือ การกำหนดระดับค่าที่เหมาะสมในการตรวจหาของแต่ละเหตุการณ์ที่บ่งชี้ว่าเป็นพฤติกรรมที่ผิดปกติ (Patcha, 2007)

**2.2.5.1 Predictive Pattern Generation**

เป็นเทคนิคในการตรวจหาความผิดปกติที่ตั้งอยู่บนสมมุติฐานที่ว่า ลำดับของเหตุการณ์จะไม่กระจายแต่จะเป็นไปในรูปแบบที่สามารถทราบล่วงหน้าได้ ซึ่งจะให้ผลลัพธ์ในการตรวจจับการโจมตีที่ดีกว่า เพราะจะพิจารณาความสัมพันธ์และลำดับของเหตุการณ์ด้วย ดังนั้นในการตรวจจับวิธีนี้จึงเป็นวิธีที่จะพยายามทำนายเหตุการณ์ที่อาจเกิดขึ้นในอนาคตจากเหตุการณ์ที่เคยเกิดขึ้นมาแล้ว และสร้างเป็นกฎไว้ (Teng, 1990)

**2.5.1.3 Neural Network**

เป็นแนวทางในการตรวจหาความผิดปกติโดยใช้วิธีการเรียนรู้จากข้อมูลในอดีต โดยการใช้ Neural Network ซึ่ง Neural Network จะถูกฝึกให้เรียนรู้โดยข้อมูลในอดีต และต้องเป็นข้อมูลของเหตุการณ์ปกติ หลังจากนั้นระบบตรวจหาจะพยายามเปรียบเทียบข้อมูลการทำงานที่เกิดขึ้นจริง กับการทำงานที่เก็บไว้ใน Neural Network เพื่อตรวจหาความผิดปกติ ข้อดีของวิธีการนี้คือ ผลของการตรวจจับไม่ขึ้นกับการตั้งสมมติฐานทางสถิติ จึงใช้ได้ดีกับข้อมูลที่มีความซับซ้อน แต่อย่างไรก็ตาม แนวทางนี้มีปัญหาคือหากเลือกช่วงเวลาที่สั้นเกินไปในการเก็บข้อมูลเพื่อใช้สำหรับเรียนรู้ จะส่งผลให้ผลลัพธ์การทำงานไม่ดี เกิด False Positive Rate สูงและหากเลือกช่วงเวลาที่กว้างเกินไป ก็จะมีผลให้มีข้อมูลที่ไม่สัมพันธ์กัน อาจเกิด False Negative ได้เช่นกัน (Pradhan, 2012)

**2.5.2 Misuse Detection**

การตรวจหาความผิดปกติประเภทนี้ใช้วิธีการวิเคราะห์พฤติกรรมความผิดปกติ โดยจะทำการเปรียบเทียบพฤติกรรมของผู้ใช้ในขณะนั้น กับพฤติกรรมที่กำหนดไว้ หากพฤติกรรมการใช้งานผิดจากพฤติกรรมที่กำหนดไว้จะถือว่าเป็นความผิดปกติ หรือการโจมตี โดยทั่วไปแล้วหลักการ

ตรวจหาการโจมตี คือ ต้องมีรูปแบบที่กำหนดไว้เป็นต้นแบบในการเปรียบเทียบกับพฤติกรรมที่ตรวจหา วิธีการตรวจหาความผิดปกติประเภทนี้จะมีอัตราความผิดพลาดในการตรวจหาต่ำ แต่จะไม่สามารถตรวจจับการโจมตีที่เกิดขึ้นมาใหม่ได้ เนื่องจากการโจมตีที่เกิดขึ้นใหม่นั้นเป็นการโจมตีที่ไม่เคยเกิดขึ้นมาก่อน เครื่องมือในการสร้างตัวตรวจหาความผิดปกติรูปแบบนี้ ได้แก่ Expert System, Keystroke Monitoring, Model Based Intrusion Detection และ State Transition Analysis เป็นต้น

## 2.6 ข้อมูลเครือข่ายคอมพิวเตอร์

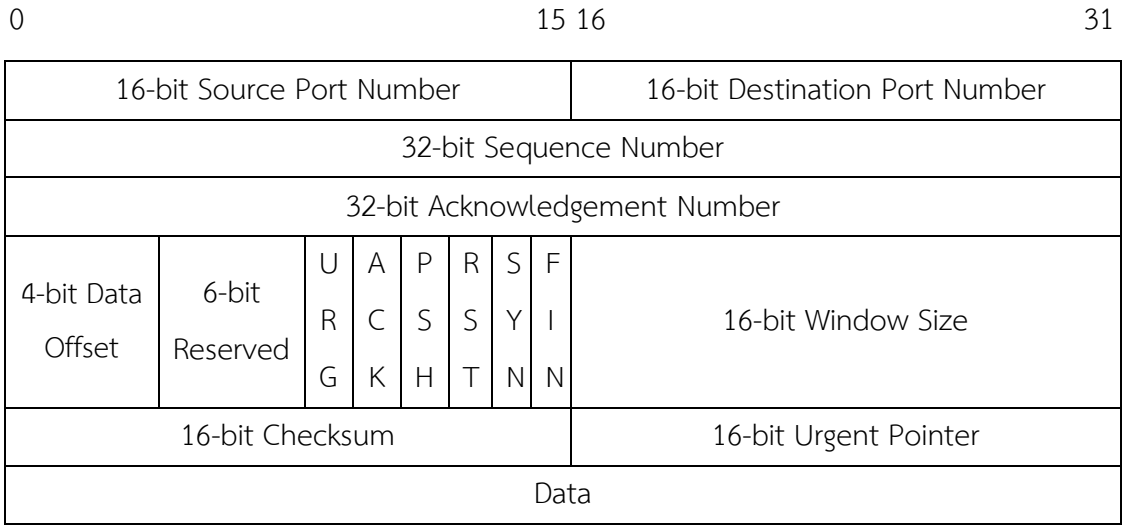
### 2.6.1 โพรโทคอล (Protocol)

โพรโทคอล เป็นข้อตกลงที่กำหนดเกี่ยวกับการสื่อสารระหว่างเครื่องคอมพิวเตอร์ต่าง ๆ ทั้งวิธีการรับ-ส่ง ตรวจสอบข้อผิดพลาด แสดงผลข้อมูลระหว่างเครื่อง หรือระหว่างเครือข่ายคอมพิวเตอร์ หากไม่มีโพรโทคอลการสื่อสารบนเครือข่ายจะไม่เกิดขึ้น (Bonaventure, 2018) ตัวอย่างโพรโทคอลในชั้นต่าง ๆ ดังตารางที่ 2-1

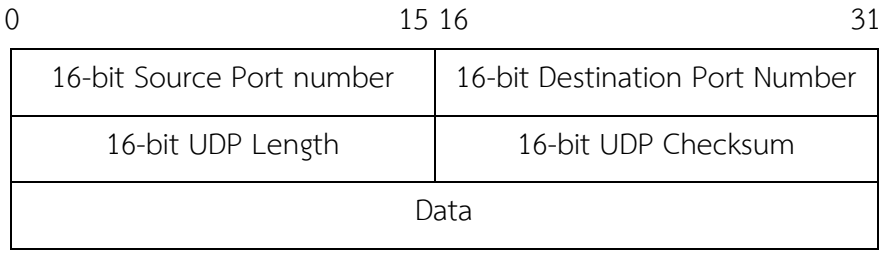
ตารางที่ 2-1 ตัวอย่างของโพรโทคอลในระบบอินเทอร์เน็ต

| ลำดับชั้น (Layer) | โพรโทคอล |
|---|---|
| Application layer | เช่น HTTP, FTP, DNS, SMTP เป็นต้น |
| Transport layer | เช่น TCP, UDP เป็นต้น |
| Internet layer | เช่น IP, ICMP เป็นต้น |
| Link layer | เช่น Ethernet เป็นต้น |

โพรโทคอลแต่ละ โพรโทคอลจะมี โครงสร้างของแพ็กเก็ตเฮดเดอร์ที่ไม่เหมือนกันตามประเภทของโพรโทคอลนั้น ๆ ตัวอย่างเช่น ใน RFC 793 (Postel, 1981) โพรโทคอล Transmission Control Protocol (TCP) และ ใน RFC 768 (Postel, 1980) โพรโทคอล User Datagram Protocol (UDP) เป็นโพรโทคอลพื้นฐานในการรับส่งข้อมูลทำงานอยู่ในระดับ Transport layer แพ็กเก็ตเฮดเดอร์ของโพรโทคอล TCP และ UDP แสดงดังภาพประกอบที่ 2-3




(ก) TCP Header




(ข) UDP Header

ภาพประกอบที่ 2-3 TCP และ UDP Header

**2.6.2 หมายเลขพอร์ต (Port Number)**

หมายเลขพอร์ต คือ ตัวเลข Integer ที่กำหนดให้กับแอปพลิเคชัน เพื่อให้สื่อสารกันได้ ในเฮดเดอร์ของโพรโทคอล TCP และ UDP จะมีการกำหนดหมายเลขพอร์ต เป็นเลขฐาน 2 ซึ่งจะได้ Source Port 16 บิต และพอร์ตปลายทางอีก 16 บิต (Kurose, 2003) ดังที่แสดงในภาพประกอบที่ 2-3 หมายเลขพอร์ตสามารถแทนด้วยตัวเลข Integer เริ่มตั้งแต่ 0 ถึง 65535 ใช้สำหรับระบุบริการ (Service) ที่ต้องการเรียกใช้ หมายเลขพอร์ตแต่ละหมายเลข สำหรับบริการใด ๆ ขึ้นอยู่กับระบบปฏิบัติการ (Operating System: OS) ที่ใช้ ไม่จำเป็นต้องเหมือนกัน จาก RFC 6335 หมายเลขพอร์ตแบ่งได้เป็น 3 ประเภท (Cotton, 2011) คือSystem Ports หรือ Well known Ports (หมายเลขพอร์ตที่กำหนดไว้โดย IANA ตั้งแต่พอร์ต 0 ถึง 1023), User Ports หรือ Registered Ports (พอร์ตหมายเลข 1024 ถึง 49151 และ Private Ports (พอร์ตหมายเลข 49152 ถึง 65535) ตัวอย่าง Well Known Ports ที่ใช้กันโดยทั่วไป แสดงดังตารางที่ 2-2 ดังนั้นในการแทน

ค่าหมายเลขพอร์ต จำนวนบิตสูงสุดที่ใช้แทนค่าข้อมูลหมายเลขพอร์ต 0-65535 คือจำนวน 16 บิต ผู้วิจัยได้ตั้งสมมติฐานว่า “จำนวนบิตที่ใช้แทนค่าจำนวนหมายเลขพอร์ตที่กำลังใช้งานในขณะที่เครือข่ายปกติ จะมีค่าน้อยกว่าจำนวนบิตของหมายเลขพอร์ตที่กำลังใช้งานในขณะที่เครือข่ายโดนโจมตี” จากสมมติฐานข้างต้นสามารถนำทฤษฎีสารสนเทศมาอธิบายได้ ซึ่งจะกล่าวในหัวข้อที่ 2.7

ตารางที่ 2-2 ตัวอย่าง Well Known Ports

| หมายเลขพอร์ต | โพรโทคอล |
|---|---|
| 20, 21 | File Transfer Protocol (FTP) |
| 22 | Secure Shell (SSH) |
| 23 | Telnet |
| 25 | Simple Mail Transfer Protocol (SMTP) |
| 53 | Domain Name System (DNS) |
| 80 | Hypertext Transfer Protocol (HTTP) |
| 110 | Post Office Protocol v3 (POP3) |
| 161, 162 | Simple Network Management Protocol (SNMP) |
| 443 | Secure Sockets Layer over HTTP (HTTPS) |

## 2.7 เอนโทรปี (Entropy)

ในทฤษฎีสารสนเทศ (Information Theory) Shannon ได้นำเสนอเอนโทรปี (Entropy) ว่าเอนโทรปีคือจำนวนบิต (bits) ที่น้อยที่สุดที่ใช้ในการแทนข้อมูลของตัวแปรสุ่ม

เอนโทรปีของตัวแปรสุ่ม $X$ กับ Probability Mass Function (PMF), $p(x)$, เมื่อ $p(x)$ คือ ค่าความน่าจะเป็นของ $x \in X$ นิยามได้ดังสมการที่ (2.1)

$$H(X) = -\sum p(x) log_2 p(x) \qquad (2.1)$$

หน่วยของเอนโทรปีคือ บิต ค่าเอนโทรปีจะสามารถวัดค่าเฉลี่ยของความไม่แน่นอนในตัวแปรสุ่มได้ ในการคำนวณหาค่าเอนโทรปีแสดงได้ดังตัวอย่าง

ตัวอย่างที่ 1 การหาค่าเอนโทรปีของตัวแปรสุ่มที่มีการแจกแจงแบบยูนิฟอร์ม

พิจารณาตัวแปรสุ่ม $X$ ที่มีการแจกแจงแบบยูนิฟอร์มจำนวน 32 ตัวอย่าง เพื่อจำแนกตัวอย่างแต่ละตัวจะต้อง Label ด้วยค่าที่แตกต่างกัน 32 ค่า ซึ่งสามารถแทนด้วยเลขฐานสองจำนวน 5 บิต โดยสามารถคำนวณค่าเอนโทรปีของตัวแปรสุ่ม $X$ ได้ดังนี้

$$\begin{aligned} H(X) &= -\sum_{i=1}^{32} p(i)\log_2 p(i) \\ &= -\sum_{i=1}^{32} \frac{1}{32}\log_2 \frac{1}{32} \\ &= \log_2 32 \\ &= 5\ bits \end{aligned}$$

ตัวอย่างที่ 2 การหาค่าเอนโทรปีของตัวแปรสุ่มที่ไม่ใช่การแจกแจงแบบยูนิฟอร์ม (ค่าของตัวแปรสุ่มแต่ละค่า เกิดขึ้นด้วยความน่าจะเป็นที่เท่ากัน)

ในการแข่งขันวิ่ง 100 เมตร มีผู้เข้าแข่งขันจำนวน 8 คน กำหนดให้ความน่าจะเป็นของการเข้าเส้นชัยเป็นอันดับ 1 ของผู้เข้าแข่งขันแต่ละคนคือ $(\frac{1}{2},\frac{1}{4},\frac{1}{8},\frac{1}{16},\frac{1}{64},\frac{1}{64},\frac{1}{64},\frac{1}{64})$ ค่าเอนโทรปีของการแข่งขันวิ่งครั้งนี้สามารถคำนวณได้ดังนี้

$$\begin{aligned} H(X) = &-\frac{1}{2}\log\frac{1}{2} -\frac{1}{4}\log\frac{1}{4} -\frac{1}{8}\log\frac{1}{8} -\frac{1}{16}\log\frac{1}{16} -\frac{1}{64}\log\frac{1}{64} -\frac{1}{64}\log\frac{1}{64} \\ &-\frac{1}{64}\log\frac{1}{64} -\frac{1}{64}\log\frac{1}{64} = 2\ bits \end{aligned}$$

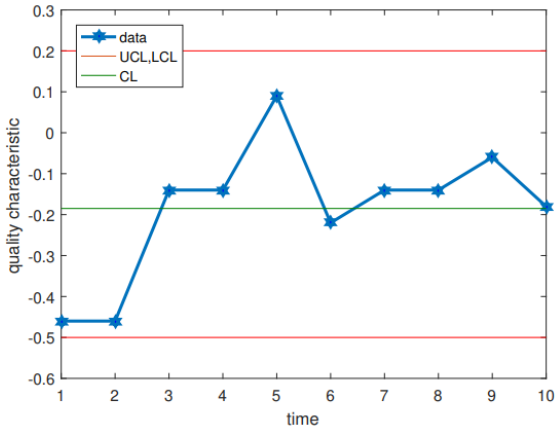
หากต้องการส่งข้อความไปยังสถานีโทรทัศน์เพื่อแจ้งผลการแข่งขันว่าผู้เข้าแข่งขันคนใดเป็นผู้ชนะ ซึ่งจำนวนบิตที่ใช้แทนผู้เข้าแข่งขัน 8 คนเท่ากับ 3 บิต อย่างไรก็ตาม ในกรณีนี้ความน่าจะเป็นในการชนะการแข่งขันของแต่ละรายไม่ได้มีการแจกแจงแบบยูนิฟอร์มจึงสามารถใช้จำนวนบิตที่น้อยกว่าปกติสำหรับผู้เข้าแข่งขันที่มีความน่าจะเป็นที่จะชนะการแข่งขันสูง และใช้จำนวนบิตที่มากขึ้นสำหรับผู้เข้าแข่งขันที่มีความน่าจะเป็นน้อย ซึ่งค่าเฉลี่ยของจำนวนบิตที่ใช้ในกรณีนี้จะเท่ากับค่าเอนโทรปีที่คำนวณได้

## 2.8 แผนภูมิควบคุม (Control Chart)

แผนภูมิควบคุม เป็นเครื่องมือสำหรับใช้ในการตรวจสอบความผิดพลาดในกระบวนการผลิตที่แสดงในรูปแบบกราฟ (Montgomery, 2009) กระบวนการผลิตมักมีโอกาสที่จะเกิดความผันแปร (Variation) อยู่เสมอ ซึ่งความผันแปรนี้จะเกิดขึ้นกับทุกกระบวนการโดยไม่สามารถหลีกเลี่ยงได้ จึงจำเป็นจะต้องมีตัวชี้วัดหรือตัวตรวจสอบความผิดปกติเหล่านี้ว่าเกินกว่าขีดจำกัดควบคุม (Control limit) ที่กำหนดไว้หรือไม่ แผนภูมิควบคุมประกอบด้วย

1. เส้นคุณภาพเฉลี่ย (Center Line: CL)
2. ขอบเขตบนของเส้นควบคุม (Upper Control Limit: UCL)
3. ขอบเขตล่างของเส้นควบคุม (Lower Control Limit: LCL)

ช่วงขอบเขต UCL และ LCL จะเป็นตัวกำหนดช่วงความเชื่อมั่นของความน่าจะเป็นที่จะตกอยู่ในช่วง 3 เท่าของส่วนเบี่ยงเบนมาตรฐาน หรือ 99.74% ดังแสดงในภาพประกอบที่ 2-4




ภาพประกอบที่ 2-4 แผนภูมิควบคุม

ในกรณีที่จุดสังเกตอยู่ในช่วงควบคุม (ระหว่างช่วงขอบเขต UCL และ LCL) แสดงว่ากระบวนการผลิตในช่วงเวลานั้นอยู่ในกระบวนการควบคุมทางสถิติ (In-control process) หากจุดสังเกตอยู่นอกช่วงการควบคุม แสดงว่ากระบวนการผลิตในช่วงเวลานั้นไม่อยู่ในกระบวนการควบคุมทางสถิติ (Out-of-control process) และจากภาพประกอบที่ 2-4 จะเห็นได้ว่ากระบวนการผลิตอยู่ในการควบคุมทางสถิติ

การเลือกช่วงความเชื่อมั่นที่ใช้ในการควบคุมการผลิตเป็นปัจจัยสำคัญที่ใช้ชี้วัดหรือตรวจสอบความผิดปกติ ถ้ากำหนดให้ $\theta$ เป็นค่าเฉลี่ยของประชากรที่ชิ้นงานอยู่ในการควบคุม และ $\hat{\theta}$ เป็นค่าเฉลี่ยของกลุ่มตัวอย่างที่ชิ้นงานอยู่ในการควบคุม ซึ่งเป็นค่าโดยประมาณของ $\theta$ เช่น $\theta$ เป็นค่า

เป้าหมายของน้ำหนักของชิ้นงานที่ทำการผลิต $\hat{\theta}$ จะเป็นค่าเฉลี่ยของน้ำหนักชิ้นงานที่ทำการผลิตได้จริง จากทฤษฎีการประมาณค่า ค่าคาดหวังของตัวอย่าง $E(\hat{\theta}) = \theta$ และค่าคาดหวังของส่วนเบี่ยงเบนมาตรฐานของตัวอย่าง $E(\sigma(\hat{\theta})) = \sigma(\theta)$

เส้นคุณภาพเฉลี่ย หรือ $CL$ เป็นค่าคาดหวังของข้อมูล สามารถคำนวณได้ดังสมการที่ (2.2)

$$CL = E(\hat{\theta}) \tag{2.2}$$

$$CL = \sum_{i=1}^{n} \bar{x}_i / n$$

โดยที่ $\bar{x}$ คือค่าเฉลี่ยของข้อมูล, $n$ คือจำนวนข้อมูลทั้งหมด

ขอบเขตบนของเส้นควบคุม: $UCL$ และ ขอบเขตล่างของเส้นควบคุม: $LCL$ คำนวณได้จากสมการที่ (2.3) และ (2.4) ตามลำดับ

$$UCL = E(\hat{\theta}) + L\sigma(\hat{\theta}) \tag{2.3}$$
$$UCL = CL + L\sigma_{\bar{x}}$$

$$LCL = E(\hat{\theta}) - L\sigma(\hat{\theta}) \tag{2.4}$$
$$LCL = CL - L\sigma_{\bar{x}}$$

โดย $L$ คือจำนวนเท่าของส่วนเบี่ยงเบนมาตรฐานของตัวอย่าง ซึ่งขอบเขตของการควบคุมจะมีจุดศูนย์กลางอยู่ที่ $CL$ การเลือกค่า $L$ จะขึ้นอยู่กับค่าความน่าจะเป็นที่ต้องการให้จุดสังเกตตกอยู่นอกช่วงการควบคุม โดยเรียกขอบเขตนี้ว่า “ขอบเขตความน่าจะเป็น (Probability Limits)” ตัวอย่างเช่นถ้าต้องการให้จุดสังเกตตกอยู่นอกช่วงการควบคุม 0.2% เมื่อเปิดตารางแจกแจงปกติมาตรฐาน ก็จะได้ค่า $L = 3.09$

ถ้ากำหนดให้ $L = 3$, $\sigma_{\bar{x}}$ คือส่วนเบี่ยงเบนมาตรฐานของค่าเฉลี่ยตัวอย่าง สามารถคำนวณได้ดังสมการ

$$\sigma_{\bar{x}} = \frac{\sigma}{\sqrt{n}} \tag{2.5}$$

เมื่อ $\sigma = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n-1}}$

แผนภูมิควบคุมเมื่อแบ่งตามชนิดของตัวแปรสุ่มแบ่งได้เป็น 2 ประเภทคือ แผนภูมิควบคุมวาริเอเบิล (Variable control chart) และ แผนภูมิควบคุมเชิงคุณภาพ (Attribute control chart)

## 2.9 แผนภูมิควบคุมค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง (The Exponentially Weighted Moving Average Control Chart: EWMA)

Roberts (1959) ได้เสนอแผนภูมิควบคุมค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง ซึ่งเป็นแผนภูมิควบคุมประเภทวาริเอเบิล (Montgomery, 2009) เหมาะสำหรับข้อมูลที่มีการเลื่อนของตัวแปรที่มีปริมาณน้อย ๆ (Small Shift) และ ข้อมูลอนุกรมเวลา (Time Series Data) แผนภูมิ EWMA นิยามได้ดังนี้

$$z_i = \lambda x_i + (1-\lambda) z_{i-1} \qquad (2.6)$$

เมื่อ $0 < \lambda \leq 1$ แทนค่าคงที่ และค่า หากแทนค่า $z_{i-1}$ ในสมการที่ (2.6) จะได้

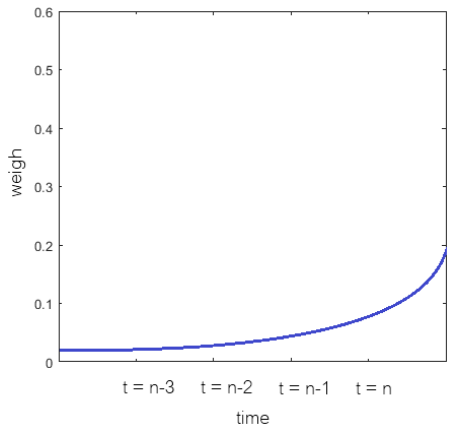
$$\begin{aligned} z_i &= \lambda x_i + (1-\lambda)[\lambda x_{i-1} + (1-\lambda) z_{i-2}] \\ &= \lambda x_i + \lambda(1-\lambda) x_{i-1} + (1-\lambda)^2 z_{i-2} \end{aligned}$$

ต่อมาเมื่อทำการแทนค่าตัวแปร $z_{i-j}$ ต่อไป สำหรับ $j = 2,3,\ldots,t$ จะได้

$$z_i = \lambda \sum_{j=0}^{i-1} (1-\lambda)^j x_{i-j} + (1-\lambda)^i z_o \qquad (2.7)$$

เมื่อกำหนดให้ตัวแปร $z_0$ เท่ากับค่าเฉลี่ยตัวอย่างกลุ่มแรก ดังนั้น $z_0 = \bar{x}$

จากนิยามในสมการ (2.7) ค่าถ่วงน้ำหนักของค่าเฉลี่ย $x_i$ ใน EWMA จะลดลงตามระยะห่างจาก $i$ ดังแสดงในภาพประกอบที่ 2-5




ภาพประกอบที่ 2-5 แผนภูมิควบคุมค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง

จากภาพประกอบที่ 2-5 เมื่อกำหนด $\lambda = 0.2$ หมายความว่า ค่าถ่วงน้ำหนักของค่าเฉลี่ย $x_i$ ณ เวลาที่ $t = n$ จะมีค่า 0.2 และค่าถ่วงน้ำหนักของค่าเฉลี่ย ณ เวลาที่ก่อนหน้า $t = n-1, n-2, n-3, \ldots$ มีค่าเท่ากับ 0.16, 0.128, 0.1024,... ตามลำดับ บางครั้ง EWMA ถูกเรียกว่า Geometric Moving Average (GMA) ค่าเฉลี่ย EWMA จึงเปรียบได้กับค่าเฉลี่ยถ่วงน้ำหนักของข้อมูลปัจจุบันและข้อมูลในอดีต

ในการสร้างแผนภูมิควบคุม สามารถใช้ค่า $UCL$ ที่คำนวณจาก EWMA ซึ่งสามารถหาได้จากสมการที่ (2.8)

$$UCL = CL + L\hat{\sigma}\sqrt{\frac{\lambda}{(2-\lambda)}} \tag{2.8}$$

ส่วนเบี่ยงเบนมาตรฐานของประชากร หรือ $\hat{\sigma}$ ซึ่งคำนวณได้จากสมการที่ (2.9) และสมการที่ (2.10)

$$E(s) = \left(\frac{2}{n-1}\right)^{\frac{1}{2}} \frac{\Gamma\left(\frac{n}{2}\right)}{\Gamma\left[\frac{(n-1)}{2}\right]}\sigma \tag{2.9}$$

จะได้

$$\hat{\sigma} = \frac{S}{C_4} \tag{2.10}$$

เมื่อ $S$ คือส่วนเบี่ยงเบนมาตรฐานของกลุ่มตัวอย่าง โดยค่าตัวแปร $C_4$ มีค่าเท่ากับ $\left(\frac{2}{n-1}\right)^{\frac{1}{2}} \frac{\Gamma\left(\frac{n}{2}\right)}{\Gamma\left[\frac{(n-1)}{2}\right]}$ โดยสามารถแสดงค่า $C_4$ สำหรับกลุ่มตัวอย่างขนาด 2 ถึง 25 ได้ดังตารางที่ 2-3

ตารางที่ 2-3 ค่า $C_4$ สำหรับกลุ่มตัวอย่างขนาด 2 ถึง 25

| ขนาดตัวอย่าง | $C_4$ | ขนาดตัวอย่าง | $C_4$ | ขนาดตัวอย่าง | $C_4$ |
|---|---|---|---|---|---|
| 2 | 0.7979 | 10 | 0.9727 | 18 | 0.9854 |
| 3 | 0.8862 | 11 | 0.9754 | 19 | 0.9862 |
| 4 | 0.9213 | 12 | 0.9776 | 20 | 0.9869 |
| 5 | 0.9400 | 13 | 0.9794 | 21 | 0.9876 |
| 6 | 0.9515 | 14 | 0.9810 | 22 | 0.9882 |
| 7 | 0.9594 | 15 | 0.9823 | 23 | 0.9887 |
| 8 | 0.9650 | 16 | 0.9835 | 24 | 0.9892 |
| 9 | 0.9693 | 17 | 0.9845 | 25 | 0.9896 |

## 2.10 งานวิจัยที่เกี่ยวข้อง

ในปี ค.ศ. 2008 Keunsoo Lee และคณะ ได้นำเสนอวิธีการตรวจหาความผิดปกติของการโจมตีแบบ DDoS โดยใช้วิธีการ Clustering โดยใช้พารามิเตอร์เก้าตัว ซึ่งห้าตัวจากเก้าตัว ได้แก่ Source IP, Destination IP, Source Port, Destination Port และ ชนิดของแพ็กเก็ต ถูก Encode โดยใช้แชนนอนเอนโทรปี ซึ่งสามารถตรวจหาความผิดปกติแบบ TCP SYN, UDP และ ICMP DDoS ได้

ในปี ค.ศ. 2008 Shui Yu และคณะ ได้นำเสนอวิธีการตรวจหาความผิดประเภท DDoS โดยได้นำทฤษฎีสารสนเทศ และเอนโทรปีมาใช้ โดยนับจำนวนแพ็กเก็ตที่มีปลายทางต่างกันเพื่อมาคำนวณเอนโทรปี หากค่าที่ได้น้อยกว่าค่า Threshold ที่กำหนด จะคำนวณอัตราเอนโทรปี หากค่าที่ได้ต่างกันน้อยกว่าค่า Threshold ที่กำหนด จะระบุว่าเป็นการโจมตี

ในปี ค.ศ. 2010 Suratose Tritilanunt และคณะ นำเสนอวิธีการตรวจหาความผิดปกติประเภท DoS และ DDoS โดยใช้แชนนอนเอนโทรปี Encode ปริมาณแพ็กเก็ตทั้งขาเข้า และขาออก โดยผลการทดลอง สามารถตรวจหาความผิดปกติแบบ ICMP flood ได้ร้อยละ 99.48 แบบ TCP SYN flood ได้ร้อยละ 99.40 และแบบ SMURF attacks ได้ร้อยละ 99.52

ในปี ค.ศ. 2013 Jaswinder Singh และคณะ เสนอวิธีการตรวจหาความผิดปกติแบบ DDoS โดยนำแชนนอนเอนโทรปีมาใช้ Encode source IP และ Encode ปริมาณแพ็กเก็ต จากนั้นระบุการโจมตีจากค่าของเอนโทรปี

ในปี ค.ศ. 2014 llija Basicevic และคณะ ได้นำเสนอวิธีการในการตรวจหาความผิดปกติโดยใช้เอนโทรปีของข้อมูลขาออก โดยเปรียบเทียบกับวิธี Cumulative Sum (CUSUM) ที่ใช้ EWMA ในการหาคำนวณเฉลี่ย โดยข้อมูลที่ใช้ในการ Encode เอนโทรปีนั้นได้แก่ จำนวนไบต์ จำนวนแพ็กเก็ต และจำนวนพอร์ตปลายทาง พบว่า ข้อมูลจำนวนพอร์ตปลายทางให้ผลการทดลองดีที่สุด การโจมตีที่ใช้ทดสอบคือ การโจมตีประเภท SYN Flood และ UDP DoS ในการใช้เอนโทรปีนั้น ให้ค่าอัตราความถูกต้องในการตรวจหาเชิงบวก (True Positive Rate: TPR) อยู่ที่ร้อยละ 90 และ อัตราความผิดพลาดในการตรวจหาเชิงบวก (False Positive Rate: FPR) อยู่ที่ร้อยละ 18 กับการโจมตีทั้งสองประเภท ส่วนการใช้ CUSUM-SYN นั้นพบว่า TPR เท่ากับร้อยละ 100 และ FPR เป็นร้อยละ 0 แต่ไม่สามารถตรวจหาการโจมตีประเภท UDP DoS ได้

ในปี ค.ศ. 2016 M. Ahmed และคณะ ได้รวบรวมวิธีการในการตรวจหาความผิดปกติบนเครือข่ายคอมพิวเตอร์ และได้แบ่งวิธีการเหล่านั้นออกเป็นสี่กลุ่มใหญ่ ได้แก่ Classification, Statistical, Clustering และ Information Theory ซึ่งในแต่ละวิธีการให้ผลดีกับประเภทของการโจมตีที่แตกต่างกัน เช่น Classification และ Clustering เหมาะกับการตรวจหา

โจมตีประเภท DoS แต่ไม่เหมาะกับการโจมตีประเภท Remote to Local (R2L) และ User to Root (U2R) เป็นต้น

ในปี ค.ศ. 2017 Ilya V. Chugunkov และคณะ ได้นำเสนอขั้นตอนวิธีในการป้องกันการโจมตีแบบ DDoS ประเภท Pulse wave โดยสังเกตจากการเพิ่มขึ้นของ IP Address ในช่วงเวลานั้น และใช้ Classifier ในการแยกเครื่องคอมพิวเตอร์ที่โจมตีไปอยู่ในกลุ่มเครือข่ายที่ถูกจำกัดแบนด์วิดธ์ เพื่อเป็นการลดภาระงานของเซิร์ฟเวอร์ และทำให้เครือข่ายโดยรวมสามารถใช้งานได้โดยปกติ

## 2.11 สรุป

ในบทนี้ได้นำเสนอทฤษฎี หลักการ ที่เกี่ยวข้องกับงานวิจัยนี้ ตลอดจนนำเสนอตัวอย่างงานวิจัยที่เกี่ยวข้องกับการตรวจหาความผิดปกติ โดยใช้การ Encode เอนโทรปี และการใช้แผนภูมิควบคุมต่าง ๆ ในบทถัดไปจะนำเสนอในส่วนของการออกแบบและพัฒนาขั้นตอนวิธีที่ใช้ในการตรวจหาความผิดปกติ ที่มีการโจมตีแบบ Pulse wave DDoS

# บทที่ 3

# การวิเคราะห์ออกแบบและพัฒนา

## 3.1 บทนำ

จากที่กล่าวไว้แล้วในบทที่ 1 ว่าการโจมตีทางเครือข่ายคอมพิวเตอร์ในปัจจุบัน มีการเปลี่ยนแปลงอยู่ตลอดเวลา และการโจมตีโดยปฏิเสธการให้บริการ เป็นการโจมตีที่สร้างความเสียหายเป็นอย่างมาก โดยเฉพาะการโจมตีแบบ DDoS การตรวจหาการโจมตีประเภทนี้ในปัจจุบันสามารถทำได้อย่างมีประสิทธิภาพ แต่วิธีการเหล่านั้นไม่ได้ครอบคลุมถึงการโจมตีแบบ Pulse wave DDoS ซึ่งเป็นการโจมตีที่ซับซ้อน และยากแก่การตรวจหากว่า DDoS เนื่องจากรูปแบบการโจมตีเป็นการโจมตีในช่วงระยะเวลาสั้น ๆ แต่สม่ำเสมอ เพียงพอที่จะทำให้เครือข่ายถูกปฏิเสธการให้บริการ

ดังนั้นผู้วิจัยได้วิเคราะห์และออกแบบขั้นตอนวิธีในการตรวจหาความผิดปกติของเครือข่ายคอมพิวเตอร์ ที่ถูกโจมตีด้วย Pulse wave DDoS โดยวิเคราะห์ข้อมูลเอนโทรปีของ Source Port และทำการสร้างกลไกในการตรวจหาที่พัฒนาขึ้นมาจากแผนภูมิควบคุมค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง และออกแบบกฎที่เป็นตัวบ่งชี้ความผิดปกติ

เนื้อหาในบทนี้จะกล่าวถึงการวิเคราะห์ข้อมูลเครือข่าย ประเภทของการโจมตีทางเครือข่าย รวมไปถึงทฤษฎีที่เกี่ยวข้อง ทั้งในเรื่องของเอนโทรปี และ แผนภูมิควบคุมที่นำมาออกแบบขั้นตอนวิธีในการตรวจหาความผิดปกติที่เกิดขึ้นบนเครือข่ายคอมพิวเตอร์ ซึ่งในส่วนแรกนั้นจะกล่าวถึง การโจมตีทางเครือข่ายคอมพิวเตอร์ ประเภท Pulse wave DDoS Attack เพื่อแสดงให้เห็นถึงรูปแบบสัญญาณของการโจมตีที่สนใจ ต่อมาจะอธิบายถึงแนวคิดในการสร้างขั้นตอนวิธีในการตรวจหาความผิดปกติ จากนั้นเป็นการอธิบายการออกแบบขั้นตอนวิธีในการตรวจหาความผิดปกติ และสุดท้ายเป็นการกำหนดเงื่อนไขในการเลือกค่าของตัวแปรที่เหมาะสมของขั้นตอนวิธีในการตรวจหาความผิดปกติ โดยมีรายละเอียดตามลำดับดังนี้

## 3.2 การโจมตีทางเครือข่ายคอมพิวเตอร์ประเภท Pulse wave DDoS

จากบทที่ 2 ได้อธิบายรูปแบบการโจมตีทางเครือข่ายคอมพิวเตอร์ประเภท DoS และ DDoS ซึ่งเป็นการโจมตีที่สร้างความเสียหายให้แก่องค์กรเป็นอย่างมาก แต่ในปัจจุบัน รูปแบบของการโจมตี ได้มีการเปลี่ยนแปลงไปมากและยากต่อการตรวจหา Imperva ให้คำนิยามรูปแบบการโจมตีนี้ว่า Pulse wave DDoS Attack

Pulse wave DDoS Attack เป็นการโจมตีที่มีเป้าหมายเพื่อขัดขวางการให้บริการแบบหนึ่ง แต่มีรูปแบบของการโจมตีที่เปลี่ยนไปจากเดิม ดังที่สรุปไว้ในตารางที่ 3-1 โดยสามารถระบุรูปแบบการโจมตีได้โดยมีคุณลักษณะสำคัญดังต่อไปนี้ (Imperva, 2017)

### 3.2.1 Immediacy

การโจมตีในรูปแบบ Pulse wave DDoS มีลักษณะแตกต่างจากการโจมตีแบบ DDoS ทั่วไป เมื่อพิจารณาจากกราฟการโจมตีในภาพประกอบที่ 3-1 จะเห็นได้ว่ากราฟของการโจมตีแบบ Pulse wave ไม่มีช่วง Ramp-up ที่สามารถพบได้ในการโจมตีแบบ DDoS โดยทั่วไป การเพิ่ม-ลดปริมาณของ Traffic เกิดขึ้นทันทีทันใด หลังจากที่เริ่มโจมตีอาจใช้เวลาเพียงไม่กี่วินาทีก็มีปริมาณถึงจุดสูงสุดแล้ว

### 3.2.2 Frequency

รูปแบบของการโจมตีจะเป็นแบบซ้ำ ๆ ซึ่งจะประกอบไปด้วย พัลส์ (Pulse) ตั้งแต่ 1 พัลส์ขึ้นไป ภายในช่วงระยะเวลาที่พิจารณา

### 3.2.3 Persistence

การโจมตีจะเกิดขึ้นเป็นช่วง ๆ แต่จะเกิดการโจมตีอยู่ตลอด อาจใช้เวลาเป็นชั่วโมง หลายชั่วโมง หรือ ยาวนานหลายวัน

### 3.2.4 Size

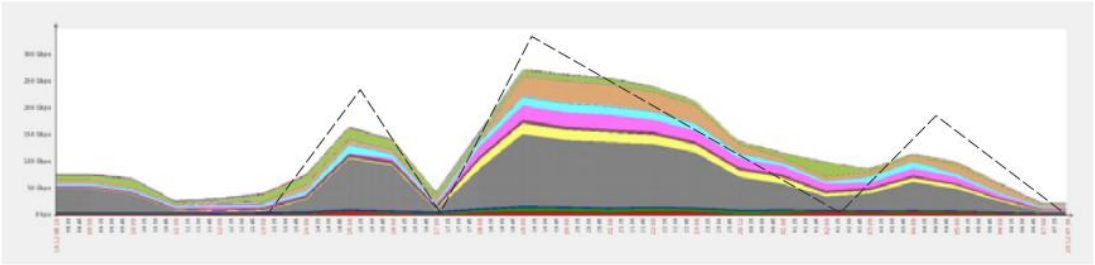
ในแต่ละพัลส์ จะมีปริมาณของการโจมตีเพียงพอจนทำให้เกิดความคับคั่งของเครือข่ายเป้าหมายได้

ตารางที่ 3-1 เปรียบเทียบคุณลักษณะระหว่าง Normal DDoS และ Pulse wave DDoS

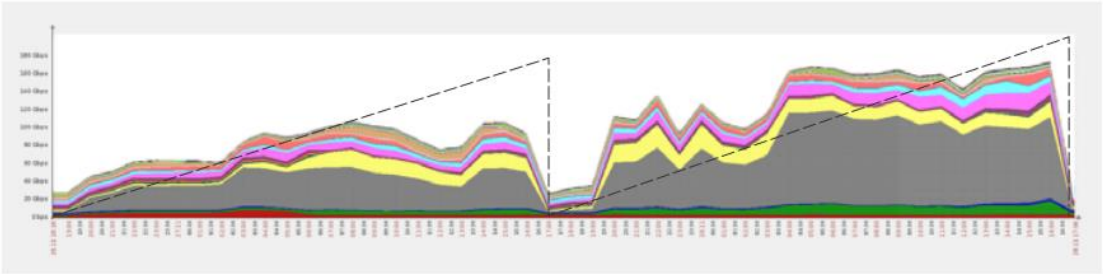
| **คุณลักษณะ** | **Normal DDoS** | **Pulse wave DDoS** |
|---|---|---|
| Immediacy | มี Ramp-up ในกราฟ | ไม่มี Ramp-up ในกราฟ |
| Frequency | เป็นการโจมตีแบบต่อเนื่อง | ในช่วงระยะเวลา 10 นาที มีพัลส์มากกว่า 1 พัลส์ขึ้นไป |
| Persistence | โจมตีต่อเนื่องจนกว่าเครือข่ายเป้าหมายไม่สามารถให้บริการได้ | เกิดขึ้นเป็นช่วง ๆ และเป็นระยะเวลานาน |
| Size | แพ็กเก็ตมีขนาดใหญ่ ทำให้เกิดความคับคั่งของเครือข่าย | ในแต่ละพัลส์ มีขนาดเพียงพอที่จะทำให้เกิดความคับคั่งของเครือข่าย |


ภาพประกอบที่ 3-1 แสดงกราฟการโจมตีแบบ Pulse wave DDoS Attack (Imperva, 2017)

ตัวอย่างรูปแบบการโจมตีแบบ DDoS โดยทั่วไป จะมีช่วง ramp-up คือรูปแบบของคลื่น จะติดกัน และค่อย ๆ สูงขึ้นจนถึงจุดสูงสุด หลังจากนั้นจะตามมาด้วยการลดลงอย่างช้า ๆ หรือลดลงอย่างรวดเร็วแบบต่อเนื่องกัน เมื่อทำซ้ำ ๆ รูปแบบมักจะคล้ายรูปสามเหลี่ยมหรือรูปฟันเลื่อยที่แสดงด้วยเส้นประ ดังภาพประกอบที่ 3-2 (ก) และ (ข)



(ก)



(ข)

ภาพประกอบที่ 3-2 (ก) แสดงกราฟการโจมตีแบบ DDoS ที่มีการลดลงแบบช้า ๆ (สามเหลี่ยม)
(ข) แสดงกราฟการโจมตีแบบ DDoS ที่มีการลดลงแบบทันทีทันใด (ฟันเลื่อย)
(Imperva, 2017)

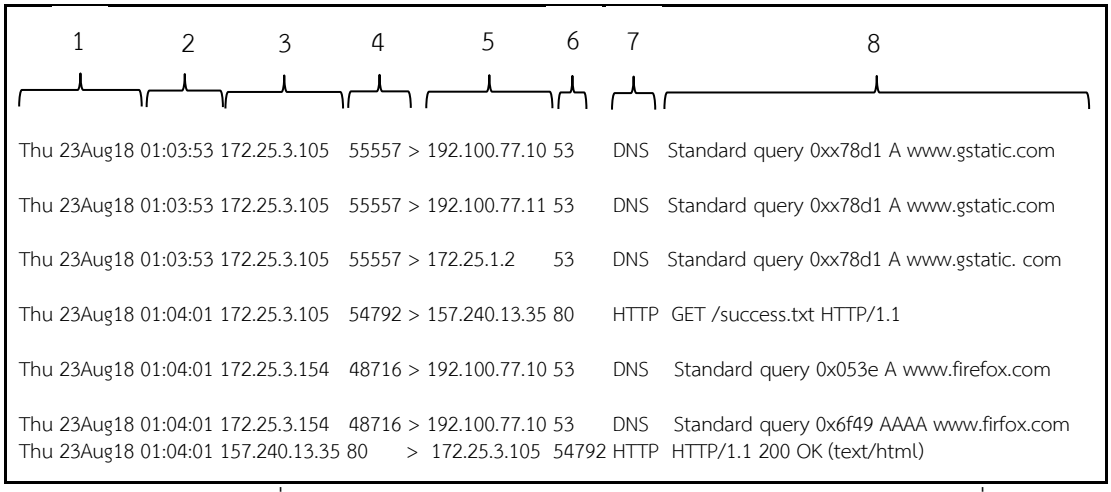
จากรูปแบบการโจมตีที่ได้ศึกษามาแล้วนั้น ผู้วิจัยจึงเลือกที่จะตรวจหาการโจมตีทางเครือข่ายคอมพิวเตอร์ประเภท Pulse wave DDoS และได้พัฒนาขั้นตอนวิธี ที่สามารถตรวจหาการโจมตีรูปแบบนี้ได้

## 3.3 แนวคิดในการสร้างขั้นตอนวิธีในการตรวจหาการโจมตี

### 3.3.1 รูปแบบที่บ่งบอกถึงการโจมตีทางเครือข่ายคอมพิวเตอร์

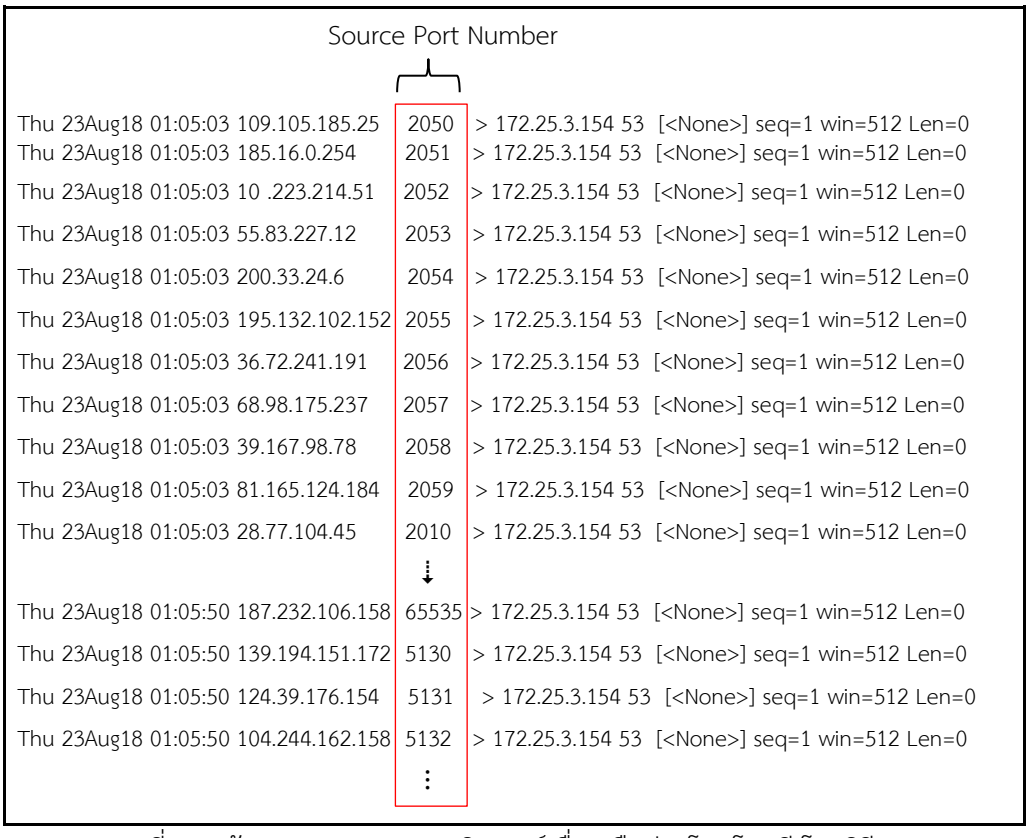
ข้อมูลที่ส่งหากันระหว่างเครื่องโดยทั่วไปแล้วจะอยู่ในรูปแบบของแพ็กเก็ตตามชนิดของโพรโทคอลต่าง ๆ แต่เพื่อให้ง่ายต่อการนำเสนอและทำความเข้าใจ ทางผู้วิจัยจึงได้นำเสนอข้อมูลจากล็อกไฟล์ (Logfile) ซึ่งแปลงข้อมูลเป็น ASCII แล้ว

ข้อมูลในล็อกไฟล์ที่เป็นการใช้งานเครือข่ายโดยทั่วไป จะมีข้อมูลต่าง ๆ ได้แก่ หมายเลข 1 แสดงข้อมูล Date หมายเลข 2 แสดงข้อมูล Time หมายเลข 3 แสดงข้อมูล Source IP Address หมายเลข 4 แสดงข้อมูล Source Port หมายเลข 5 แสดงข้อมูล Destination IP Address หมายเลข 6 แสดงข้อมูล Destination Port หมายเลข 7 แสดงข้อมูล Protocol และหมายเลข 8 แสดงข้อมูลรายละเอียดอื่น ๆ ดังตัวอย่างในภาพประกอบที่ 3-3




ภาพประกอบที่ 3-3 ข้อมูลจราจรทางคอมพิวเตอร์ของการใช้งานเครือข่ายโดยทั่วไป

เมื่อเครือข่ายโดนโจมตี การจราจรของข้อมูลในคอมพิวเตอร์จะมีลักษณะดังภาพประกอบที่ 3-4 ซึ่งเป็นการโจมตีประเภท Pulse wave DDoS Attack ไปยัง IP 172.25.3.154 ที่พอร์ต 53

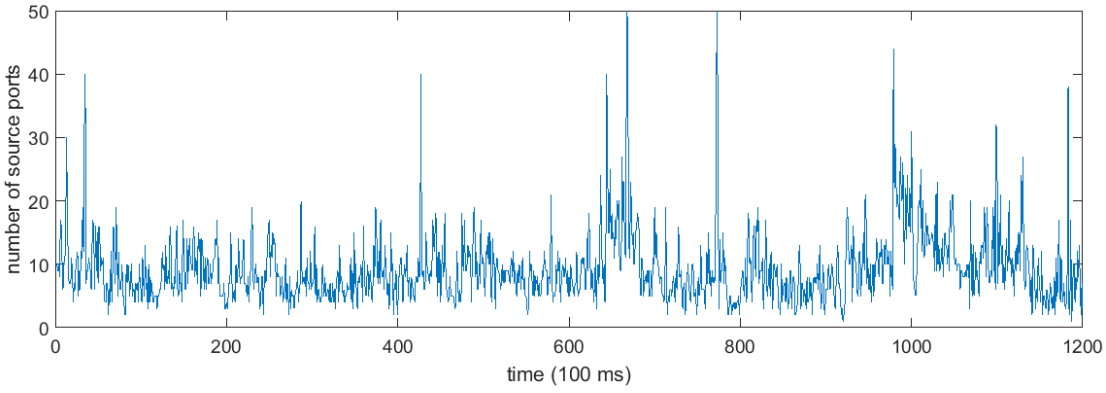



ภาพประกอบที่ 3-4 ข้อมูลจราจรทางคอมพิวเตอร์เมื่อเครือข่ายโดนโจมตี โดยวิธี Pulse wave DDoS Attack

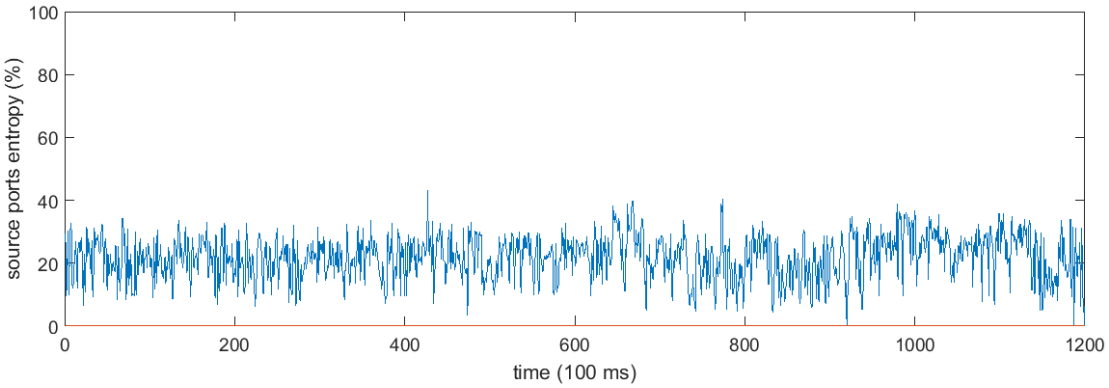
จากภาพประกอบที่ 3-4 เมื่อพิจารณาหมายเลข Source Port จะเห็นว่า หมายเลขพอร์ตมีการแจกแจงแบบยูนิฟอร์ม (Uniform Distribution) ในช่วง 0-65535 เมื่อเปรียบเทียบกับข้อมูลจราจรของการใช้งานเครือข่ายปกติพบว่า การแจกแจงของหมายเลข Source Port ที่มีการใช้งานปกติจะมีช่วงที่แคบกว่า จากรูปแบบการเกิดขึ้นของหมายเลข Source Port จึงได้ตั้งข้อสังเกตว่าน่าจะสามารถบอกถึงความผิดปกติที่เกิดขึ้นบนเครือข่ายคอมพิวเตอร์ได้ จึงได้นำข้อมูลนี้มา Encode ด้วยเอนโทรปี

### 3.3.2 เอนโทรปีของ Source Port (Source Port Entropy)

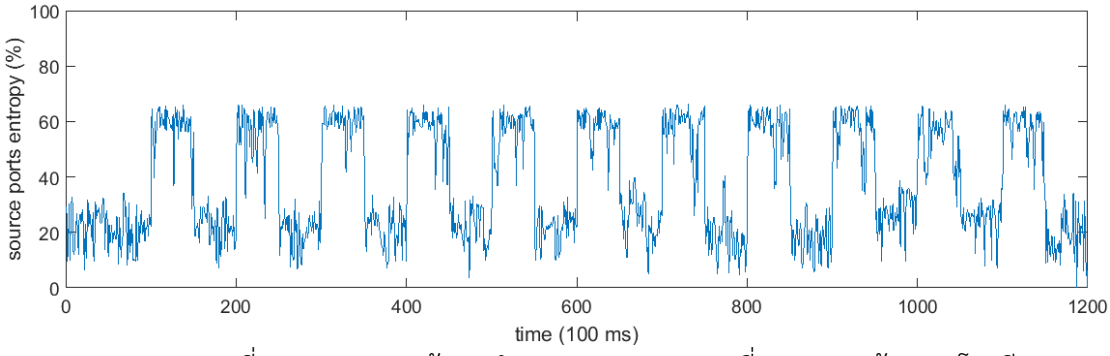
จากภาพประกอบที่ 3-5 แสดงจำนวน Source Port โดยแกนนอนแทนเวลาที่เก็บข้อมูลทุก 0.1 วินาที (s) ส่วนแกนตั้งแทนจำนวน Source Port ที่เกิดขึ้น ณ เวลาใด ๆ เมื่อกำหนดให้ $t$เป็นอะเรย์ (Array) ที่ใช้เก็บข้อมูล ตัวอย่างเช่น $t[200]$ แทนจำนวน Source Port ณ เวลาที่ $200 \times 100$ ms จากเวลาเริ่มต้น เมื่อนำข้อมูลชุดนี้ไป Encode ด้วยเอนโทรปี ก็จะได้รูปแบบของข้อมูล Source Port ดังที่แสดงในภาพประกอบที่ 3-6 จะเห็นว่าค่าเอนโทรปี จะมีการเปลี่ยนแปลงอยู่ในช่วงแคบ ๆ และหากจำลองการโจมตีแบบ Pulse wave DDoS โดยใช้ข้อมูลเดียวกัน เมื่อนำมาคำนวณค่าเอนโทรปีพบว่า ค่าเอนโทรปีของช่วงเวลาที่ถูกโจมตี มีค่าสูงขึ้นกว่าค่าที่มีการใช้งานเครือข่ายแบบปกติ ดังภาพประกอบที่ 3-7 จากรูปแบบของค่าเอนโทรปีของ Source Port ที่ปรากฏผู้วิจัยจึงมีแนวคิดที่จะพัฒนาขั้นตอนวิธี ในการตรวจหาความผิดปกติ ที่มีการโจมตีประเภท Pulse wave DDoS โดยใช้ข้อมูลเอนโทรปีของหมายเลข Source Port มาสร้างแผนภูมิควบคุม




ภาพประกอบที่ 3-5 กราฟของข้อมูลจำนวนของ Source Port ที่ยังไม่ Encode ด้วยเอนโทรปี




ภาพประกอบที่ 3-6 กราฟของข้อมูลจำนวน Source Port ที่ Encode ด้วยเอนโทรปี




ภาพประกอบที่ 3-7 กราฟของข้อมูลจำนวน Source Port ที่ Encode ด้วยเอนโทรปี เมื่อเครือข่ายถูกโจมตี

### 3.3.3 แผนภูมิควบคุม (Control Chart)

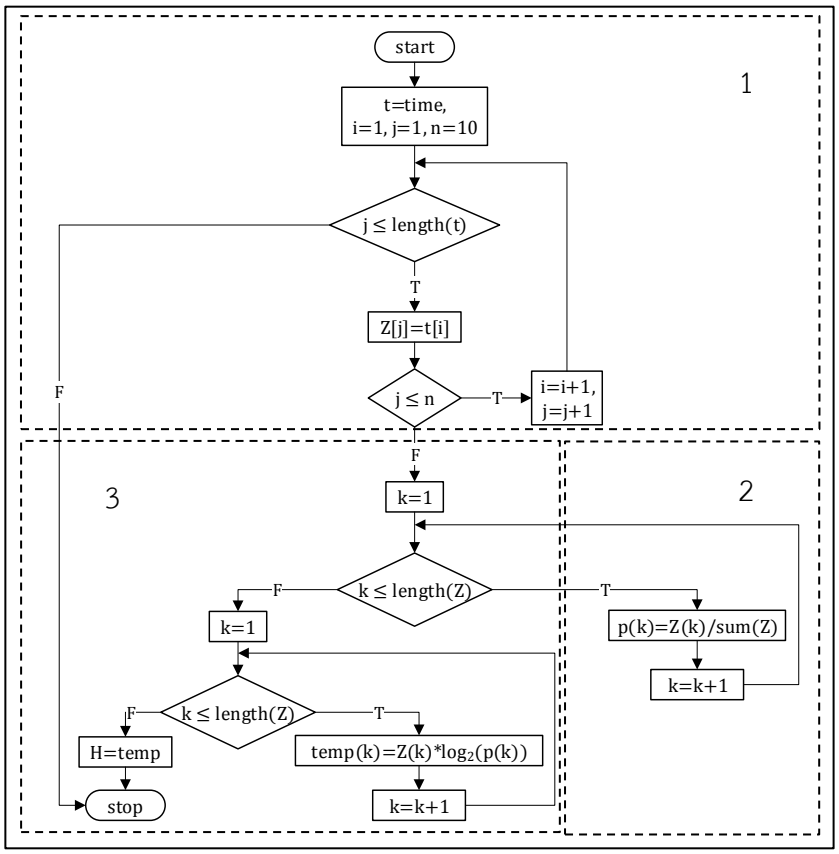
แผนภูมิควบคุมที่ได้กล่าวถึงไว้ในบทที่ 2 เป็นเครื่องมือที่มีประสิทธิภาพในการตรวจหาข้อมูลจากกระบวนการที่ตกอยู่นอกขอบเขตการควบคุม โดยประสิทธิภาพของแผนภูมิควบคุม จะขึ้นอยู่กับการออกแบบเส้นคุณภาพเฉลี่ย (Center Line: CL) ขอบเขตบนของเส้นควบคุม (Upper Control Limit: UCL) และ ขอบเขตล่างของเส้นควบคุม (Lower Control Limit: LCL) ที่เหมาะสมกับชุดข้อมูลนั้น ๆ

จากข้อมูลของ Source Port ที่มีการโจมตี จะเห็นว่าความถี่ของหมายเลข Source Port ที่ใช้งานจะสูงขึ้นดังนั้นจึงตั้งสมมุติฐานที่ใช้ในการตรวจหาการโจมตีไว้ว่า “ถ้าความถี่ของ Source Port มีการเปลี่ยนแปลงที่เพิ่มขึ้นอย่างผิดปกติ ก็จะจัดอยู่ในเหตุการณ์ต้องสงสัยว่าจะมีการโจมตี” จากสมมุติฐานจึงได้นำเสนอวิธีการกำหนดค่า CL และ UCL ที่เหมาะสม เพื่อตรวจหาความผิดปกติ เมื่อมีการโจมตีประเภท Pulse wave DDoS

## 3.4 ขั้นตอนวิธีในการตรวจหาความผิดปกติ

การตรวจหาข้อมูล Source Port ที่แสดงถึงสภาวะความผิดปกติ ประกอบด้วย 3 ขั้นตอน คือ ขั้นตอนที่ 1 การ Encode โดยการแปลงข้อมูล Source Port ด้วยเอนโทรปี ขั้นตอนที่ 2 การสร้างแผนภูมิควบคุมค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง และขั้นตอนที่ 3 การตรวจหารูปแบบของข้อมูลที่มีความผิดปกติ

### 3.4.1 การแปลงข้อมูล Source Port เป็นเอนโทรปี




ภาพประกอบที่ 3-8 แผนผังการทำงานของการแปลงข้อมูล Source Port เป็นเอนโทรปี

ในขั้นแรกเป็นขั้นตอนของการเตรียมข้อมูล โดยจะทำการแปลงข้อมูลเป็นค่าเอนโทรปี ซึ่งข้อมูลที่ใช้เป็นข้อมูลของจำนวนหมายเลข Source Port ที่ต่างกัน ณ เวลา $t_i$ ใด ๆ เมื่อตัวแปร $t$ คือเวลา $i$ คือลำดับของเวลาทุก 1 s โดยที่ค่า $i$ เพิ่มขึ้นทีละ 1 ($i = 1,2,3,\dots$) โดย $t_i$ จะถูกแบ่งออกเป็น $n$ ส่วน เมื่อ $n$ แทนกรอบของข้อมูล (Sampling Data) ที่นำมาใช้ในการคำนวณหาค่าเอนโทรปี และกำหนดให้ตัวแปร $z_j$ แทนจำนวนพอร์ตที่ใช้งานลำดับที่ $j$ ณ เวลา $\frac{t_i}{n}$ โดยที่ค่า $j$ มีค่าตั้งแต่ 1 จนถึง $n$ ($j = 1,2,3,\dots,n$) ซึ่งมีขั้นตอนวิธีการการแปลงแสดงไว้ดังภาพประกอบที่ 3-8 และมีตัวอย่างการคำนวณดังนี้

ตารางที่ 3-2 จำนวนพอร์ตที่ใช้งาน ณ เวลา $\mathrm{t_{i=1}}$ เมื่อกำหนดให้ $\mathrm{n} = 10$

| **เวลาที่ $t_{i=1}$** | $z_1$ | $z_2$ | $z_3$ | $z_4$ | $z_5$ | $z_6$ | $z_7$ | $z_8$ | $z_9$ | $z_{10}$ |
|---|---|---|---|---|---|---|---|---|---|---|
| Source Port ที่มีการใช้งาน | 53 | 20<br>21<br>22<br>53<br>67<br>68<br>445<br>563 | 80 | 0<br>22 | 21<br>22 | 53<br>80 | 53<br>80 | 445<br>600 | 0<br>21<br>22<br>53<br>445 | 1 |
| **รวม** | 1 | 8 | 1 | 2 | 2 | 2 | 2 | 2 | 5 | 1 |

จากตารางที่ 3-2 เมื่อมีข้อมูลของหมายเลขพอร์ตที่มีการใช้งาน ซึ่งแผนผังการทำงานในภาพประกอบที่ 3-8 แทนด้วยตัวแปร $Z$ จากตารางที่เวลา $t_{i=1}$ จะได้เซตของจำนวน Source Port $Z = \{z_1 = 1, z_2 = 8, z_3 = 2, z_4 = 2, z_5 = 2, z_6 = 2, z_7 = 2, z_8 = 2, z_9 = 5, z_{10} = 1\}$ จะเห็นว่า $z_j$ คือค่าความถี่สะสมของ Source Port ซึ่งมีการใช้งานพอร์ตรวมทั้งหมด 26 พอร์ต จากนั้นนำไปคำนวณค่าความน่าจะเป็น ของแต่ละ $z_j$ ดังส่วนที่ 2 ที่แสดงด้วยกรอบสี่เหลี่ยมเส้นประในภาพประกอบที่ 3-8 โดยใช้สมการ (3.1)

$$p(z_j) = \frac{z_j}{\sum z_j} \tag{3.1}$$

เมื่อ $p$ คือ ค่าความน่าจะเป็น จะได้

$$\begin{aligned} p(z_{j=1}) &= 1/26 = 0.0385 \\ p(z_{j=2}) &= 8/26 = 0.3077 \\ p(z_{j=3}) &= 2/26 = 0.0769 \\ &\vdots \\ p(z_{j=10}) &= 1/26 = 0.0385 \end{aligned}$$

จากนั้น ในกรอบสี่เหลี่ยมเส้นประของส่วนที่ 3 จากภาพประกอบที่ 3-8 ค่าคำนวณด้วยชานนอนเอนโทรปี (Shannon Entropy) สามารถกำหนดได้ดังสมการที่ (3.2)

$$H(Z) = -\sum_{j=1}^{n} p(z_j) log_2 \left(p(z_j)\right) \tag{3.2}$$

เมื่อ $H(Z)$ คือค่าเอนโทรปีของชุดของหมายเลขพอร์ตที่มีการใช้งาน ณ เวลา $t_{i=1}$

โดย
$$z_{j=1}log_2\left(p(z_{j=1})\right) = 0.0385 \times log_2(0.0385) = -0.1808$$
$$z_{j=2}log_2\left(p(z_{j=2})\right) = 0.3077 \times log_2(0.3077) = -0.5232$$
$$z_{j=3}log_2\left(p(z_{j=3})\right) = 0.0769 \times log_2(0.0769) = -0.2846$$
$$\vdots$$
$$z_{j=10}log_2\left(p(z_{j=10})\right) = 0.0385 \times log_2(0.0385) = -0.1808$$

จากผลลัพธ์ข้างต้น สามารถหาค่าเอนโทรปีของข้อมูล ณ เวลา $t_{i=1}$ จะได้

$$H(Z) = -\big((-0.1808) + (-0.5232) + (-0.2876) +, \dots, +(-0.1808)\big) = 2.9462$$

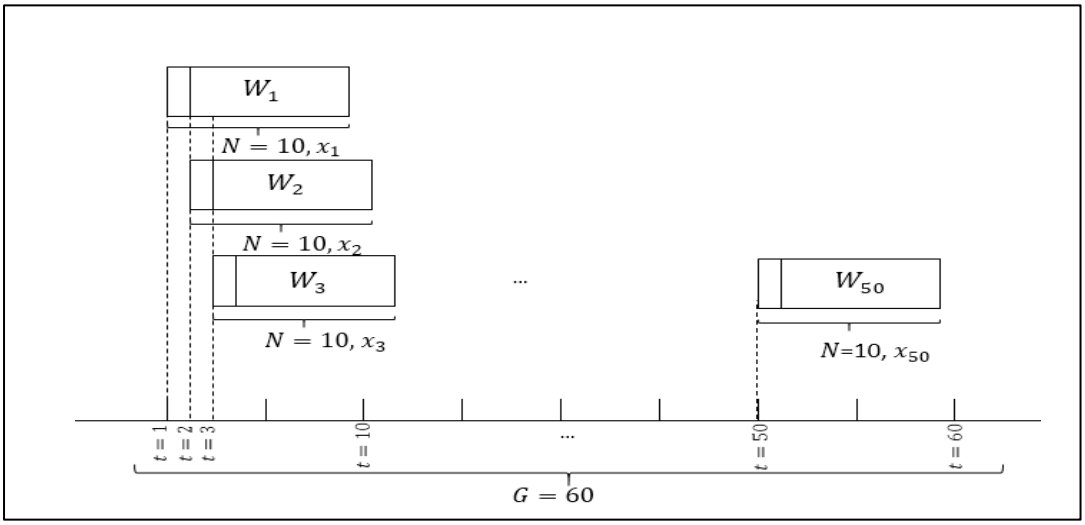
ดังนั้น ณ เวลา $t_{i=1}$ ค่าเอนโทรปี $H(Z)$ มีค่าเท่ากับ 2.9462 เพื่อนำไปออกแบบแผนภูมิควบคุม

### 3.4.2 การสร้างแผนภูมิควบคุมค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง

การออกแบบแผนภูมิควบคุมตามสมมุติฐานที่ใช้ในการตรวจหาความผิดปกติของจำนวน Source Port โดยใช้แผนภูมิ EWMA ซึ่งเป็นการคำนวณค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลังจากค่าเอนโทรปี จะต้องคำนวณ Control Line โดยใช้ข้อมูลแบ่งเป็นกลุ่ม (Groups) ที่มีจำนวน $G$ ตัว โดยกลุ่มนี้จะถูกแบ่งออกเป็นกลุ่มย่อย ๆ (Subgroup: $W$) ขนาด $N$ ตัว ณ เวลาที่ $t(i)$ ซึ่งกลุ่มย่อยดังกล่าวสามารถกำหนดได้ดังสมการ (3.3)

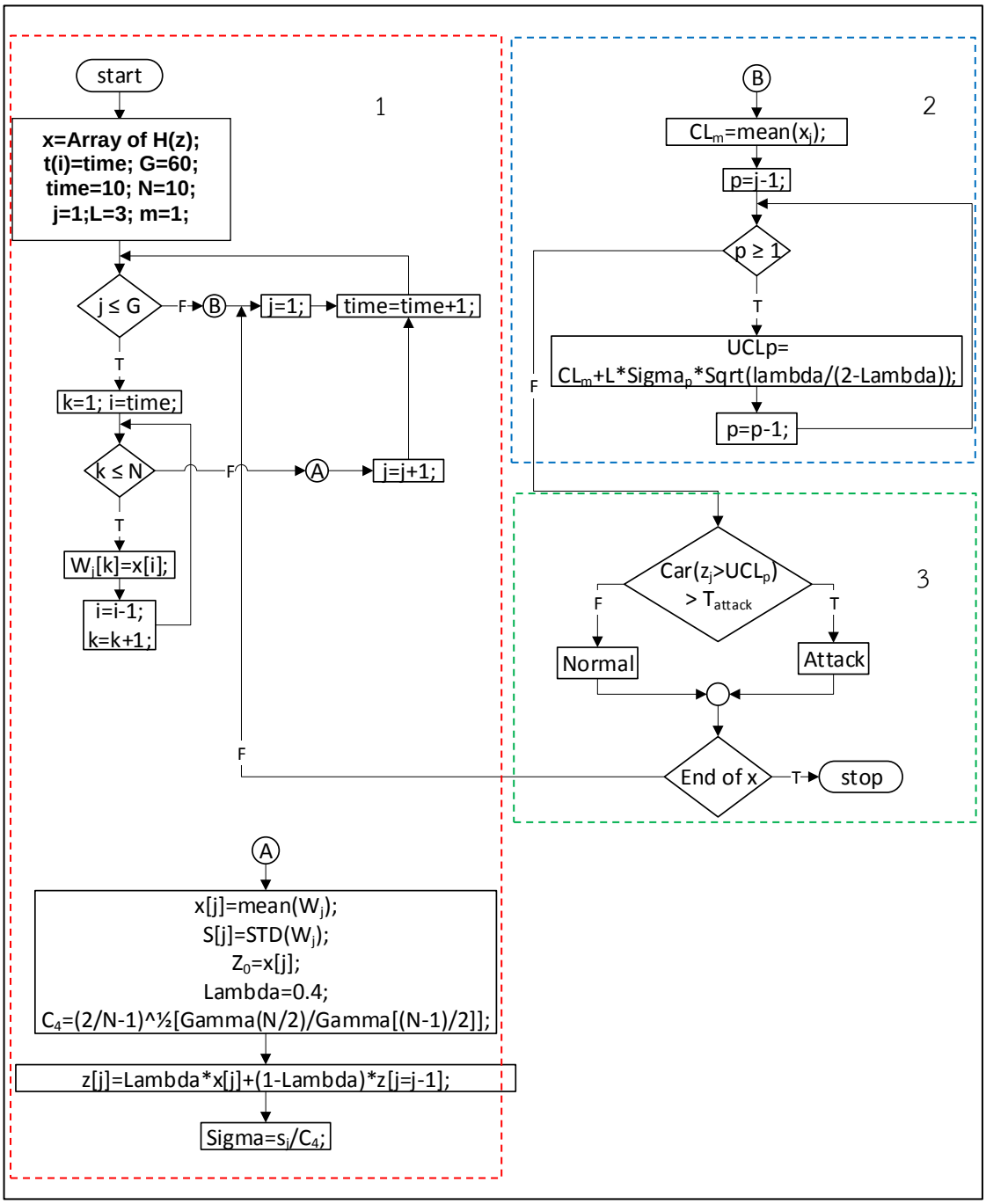
$$W_j = \{x_{t(i)} |\, t(i) = t(i-1), t(i-2), t(i-3), \dots, t(i-(N-1))\} \qquad (3.3)$$

สำหรับการกำหนดกลุ่มย่อย $W_j$ ได้แสดงไว้ในภาพประกอบที่ 3-9




ภาพประกอบที่ 3-9 แสดงการแบ่งกลุ่มเอนโทรปีออกเป็นกลุ่มย่อย (Subgroup)

สำหรับขั้นตอนการสร้างแผนภูมิ EWMA ได้แสดงไว้ในแผนผังการทำงานดังภาพประกอบที่ 3-10 ซึ่งในแผนผังการทำงาน ได้แบ่งออกเป็นขั้นตอนย่อย 3 ส่วนด้วยกัน โดยแต่ละส่วนจะใช้กรอบสี่เหลี่ยมที่เป็นเส้นประล้อมรอบ




ภาพประกอบที่ 3-10 แผนผังการทำงานของวิธีการที่นำเสนอ

ในกรอบเส้นประรูปสี่เหลี่ยมของภาพประกอบที่ 3-10 เป็นส่วนที่ 1 ที่ใช้คำนวณค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง ที่คำนวณด้วยสมการ

$$z_{ewma}[j] = \lambda x_j + (1-\lambda) z_{ewma}[j-1] \tag{3.4}$$

เมื่อ $0 < \lambda \leq 1$ และ $x_j$ คือ ค่าเฉลี่ยของสมาชิกในเซตย่อย $W_j$

จากตัวอย่างข้างต้น ที่ได้กำหนดขนาดตัวอย่างของกลุ่มย่อยไว้คือ $N = 10$ ก็จะได้กลุ่มย่อยแรกคือ

$$W_1 = \{2.9462, 0.9576, 1.5708, 3.0232, 0.9976, 2.3649, 3.2770, 3.0531, 1.2926, 1.1903\}$$

จากสมการที่ (3.4) ค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง $W_1$ คำนวณได้ดังนี้

$$\begin{aligned} z_{ewma}[1] &= \lambda x_{j=1} + (1-\lambda) z_{ewma}[1-1=0] \\ &= 0.4 \times 2.0673 + (1-0.4) \times 2.0673 \\ &= 2.0018 \end{aligned}$$

เมื่อค่าเริ่มต้น $z_{ewma}[0] = \mu_0$ และ $\lambda = 0.4$ และค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลังของ $W_2$ คำนวณได้ดังนี้

$$\begin{aligned} z_{ewma}[2] &= \lambda x_{j=2} + (1-\lambda) z_{ewma}[2-1=0] \\ &= 0.4 \times 2.0823 + (1-0.4) \times 2.0018 \\ &= 2.0340 \end{aligned}$$

ขั้นตอนต่อมาเป็นการประมาณค่าส่วนเบี่ยงเบนมาตรฐาน $\hat{\sigma}$ จากค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง สามารถคำนวณได้ดังสมการ (3.5)

$$\hat{\sigma} = \frac{S}{C_4} \tag{3.5}$$

โดยที่ $S$ คือ ส่วนเบี่ยงเบนมาตรฐานของเซตย่อย $W_j$ และ $C_4$ หาได้จากสมการ (3.6)

$$C_4 = \left(\frac{2}{N-1}\right)^{1/2} \frac{\Gamma(N/2)}{\Gamma[(N-1)/2]} \tag{3.6}$$

หรือสามารถดูได้จากตารางที่ 2-3 ที่ $N$ เท่ากับ 10 จะได้ $C_4$ เท่ากับ 0.9727 ดังนั้น เมื่อ $S$ เท่ากับ 0.9546 ก็จะได้ค่าประมาณของส่วนเบี่ยงเป็นมาตรฐาน $\hat{\sigma} = 0.9546/0.9727 = 0.9814$

จากส่วนที่ 2 ของภาพประกอบที่ 3-10 เป็นการคำนวณหา Center Line (CL) ได้โดยใช้สมการที่ (3.7)

$$CL = \sum_{j=1}^{G} x_j / G \tag{3.7}$$

เมื่อกำหนดค่า $G = 60$ จะคำนวณค่า $CL$ ได้ดังนี้

$$CL = \sum_{j=1}^{60} x_j / 60$$

$$CL = 2.18$$

จากนั้นจะนำค่า $CL$ ไปคำนวณหา Upper Control Limit (UCL) ซึ่งได้นิยามไว้ดังสมการที่ (3.8)

$$UCL = CL + L\hat{\sigma}\sqrt{\frac{\lambda}{(2-\lambda)}} \tag{3.8}$$

เมื่อ $L$ แทนสเกลของค่าส่วนเบี่ยงเบนมาตรฐานของค่าสถิติจากตัวอย่าง ในที่นี้ ได้กำหนดให้ $L = 3$ ซึ่งจะได้ช่วงความเชื่อมั่นจากค่าความน่าจะเป็นแบบสะสมเท่ากับ 0.9987 ที่ทำให้ความผิดพลาดประเภทที่หนึ่ง (Type I Error) เท่ากับ 0.0013

$$UCL = 2.18 + 3 \times 0.9814\sqrt{\frac{0.4}{(2-0.4)}}$$

$$UCL = 3.6521$$

ตัวอย่างเพิ่มเติมได้แสดงไว้ในตารางที่ 3-3

ตารางที่ 3-3 ข้อมูลการคำนวณ EWMA

| $W_j$ | $x_j$ | $z_{ewma}[j]$ | $S$ | $\hat{\sigma}$ | $UCL$ |
|---|---|---|---|---|---|
| $W_1$ | 2.0673 | 2.0018 | 0.9546 | 0.9814 | 3.6521 |
| $W_2$ | 2.0823 | 2.0340 | 0.9040 | 0.9294 | 3.5741 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| $W_{60}$ | 2.1352 | 1.9979 | 0.8484 | 0.8723 | 3.4885 |

### 3.4.3 การตรวจหาความผิดปกติ

ขั้นตอนสุดท้ายในขั้นตอนวิธีในการตรวจหาความผิดปกติ จากสมมุติฐานได้ออกแบบกฎการตรวจหาความผิดปกติไว้ในส่วนที่ 3 ของภาพประกอบที่ 3-10 ดังนี้

$$If\ Car\left(z_{ewma}\left[j\right] \geq\ UCL_j\right) > T_{attack}\ \ Then\ Attack\ is\ detected$$

เมื่อ ตัวแปร $Car$ คือ $Cardinality$ แทนจำนวนสมาชิกของเซตย่อย $W_j$ ที่สมาชิก $z_{ewma}\left[j\right] \geq UCL_j$ และตัวแปร $T_{attack}$ คือค่า Threshold ที่ใช้ตรวจหาความผิดปกติ

## 3.5 การเลือกค่าของตัวแปรที่เหมาะสมในขั้นตอนวิธีในการตรวจหาความผิดปกติ

จากขั้นตอนวิธีที่ได้นำเสนอในหัวข้อ 3.4 มีตัวแปรที่มีความสำคัญในการออกแบบและส่งผลต่อประสิทธิภาพของวิธีการที่ใช้ตรวจหาความผิดปกติ 3 ตัวแปร นั่นคือตัวแปร Threshold $(T_{attack})$ ตัวแปรขนาดกลุ่มย่อย $(N)$ และตัวแปร Group $(G)$ ซึ่งในการออกแบบแผนภูมิควบคุมจะต้องใช้ขนาดของกลุ่มและกลุ่มย่อยที่เหมาะสม เพื่อให้ได้แผนภูมิที่มีความไวในการหาได้อย่างถูกต้อง ส่วนเกณฑ์ที่ใช้เลือกตัวแปรที่เหมาะสมอีกตัวคือค่า Threshold ในกรณีที่เกิดเหตุการณ์ที่ไม่ปกติ (มีการโจมตีเกิดขึ้น) จะทำการพิจารณาจาก อัตราความผิดพลาดในการตรวจหาเชิงลบ หรือ False Negative Rate เป็นอันดับแรก ต่อมาจึงพิจารณา อัตราความผิดพลาดในการตรวจหาเชิงบวก หรือ False Positive Rate โดยที่ค่า False Positive Rate ในเหตุการณ์ปกติ (ไม่มีการโจมตีเกิดขึ้นเลย) ต้องมีค่าเป็นศูนย์หรือเข้าใกล้ศูนย์มากที่สุด ซึ่งผลการทดลองจะแสดงในบทที่ 4

## 3.6 สรุป

จากการศึกษา วิเคราะห์และออกแบบขั้นตอนวิธีในการตรวจหาความผิดปกติ พร้อมทั้งแสดงแนวคิดในการพัฒนาวิธีการตรวจหาความผิดปกติ ที่มีการโจมตีแบบ Pulse Wave DDoS ซึ่งประกอบไปด้วย 3 ขั้นตอน ได้แก่ ขั้นตอนที่ 1 การแปลงข้อมูล Source Port ด้วยเอนโทรปี ขั้นตอนที่ 2 การสร้างแผนภูมิควบคุมด้วยค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง และขั้นตอนที่ 3 การตรวจหาความผิดปกติ อีกทั้งได้อธิบายเงื่อนไขในการเลือกค่าของตัวแปรที่เหมาะสมของขั้นตอนวิธีในการตรวจหาความผิดปกติ ซึ่งจะแสดงในบทถัดไปที่จะกล่าวถึง ซึ่งเป็นส่วนของผลการทดลองในการตรวจหาความผิดปกติ โดยได้ทำการทดลองเปรียบเทียบค่าของตัวแปรต่าง ๆ

# บทที่ 4

# ผลการทดลองและวิจารณ์

## 4.1 บทนำ

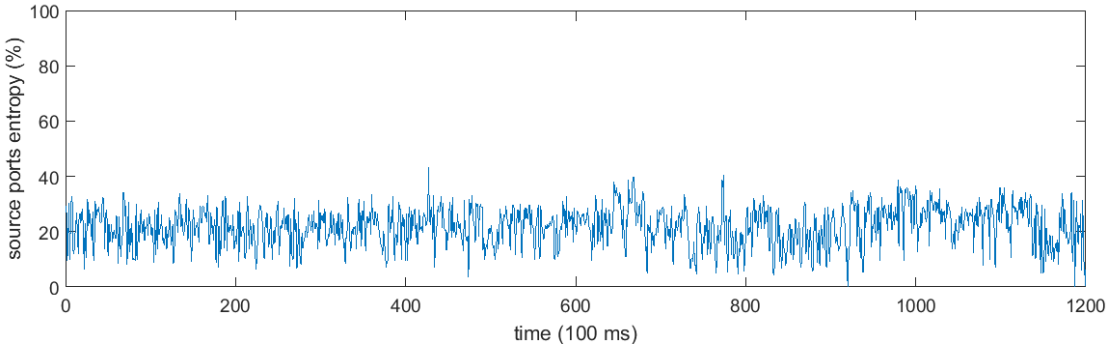
บทนี้จะกล่าวถึงการทดสอบและการประเมินประสิทธิภาพของขั้นตอนวิธีที่นำเสนอ ในส่วนแรกจะกล่าวถึง ชุดข้อมูลที่ใช้ในการทดสอบ ต่อมาได้กล่าวถึงวิธีการกำหนดค่าตัวแปรต่าง ๆ ของขั้นตอนวิธีที่นำเสนอ จากนั้นจะได้กล่าวถึงการวัดและการประเมินประสิทธิภาพ สุดท้ายเป็นผลการทดลอง โดยมีรายละเอียดตามลำดับดังที่จะได้นำเสนอ

## 4.2 ชุดข้อมูลที่ใช้ในการทดลอง

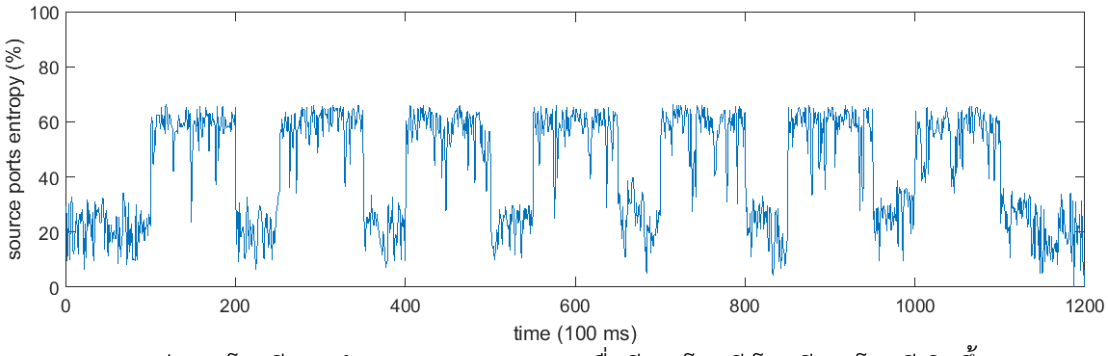
สำหรับการทดสอบขั้นตอนวิธีที่นำเสนอได้ใช้ข้อมูลเครือข่าย ของภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่ ซึ่งมีผู้ใช้งานเครือข่ายประมาณ 200 คน ประกอบด้วย อาจารย์ นักศึกษา และเจ้าหน้าที่ การเก็บข้อมูลจะเก็บข้อมูล Source Port ทุก 1 วินาที (s) ซึ่งในหนึ่งวินาทีจะถูกแบ่งออกเป็น 10 ส่วน (0.1 s หรือ100 ms) ตัวอย่างของข้อมูลในสภาวะปกติมีค่าความถี่ของ Source Port ปรากฏดังภาพประกอบที่ 4-1 ส่วนกรณีที่มีการโจมตีมีรูปแบบของค่าความถี่ปรากฏดังภาพประกอบที่ 4-2 ซึ่งวิธีการโจมตีที่ใช้คือ Pulse Wave DDoS Attack ที่มีการกำหนดรูปแบบความถี่ของข้อมูลการโจมตี 2 แบบ คือแบบกำหนดเอง ซึ่งมีการกำหนดช่วงเวลาที่ใช้ในการโจมตี จากภาพประกอบที่ 4-2 ก็คือตำแหน่งของการโจมตีที่ห่างกันด้วยสเกล (Scale) ที่ทำให้เกิดพัลส์คงที่ตามแกนนอน และระยะเวลาในการโจมตี (Duration) ที่เป็นความกว้างของพัลส์ประกอบด้วย 4 รูปแบบ ดังตารางที่ 4-1 ส่วนกราฟแสดงข้อมูลที่ใช้ในการทดลองเมื่อมีการโจมตีในรูปแบบต่าง ๆ ดังภาพประกอบที่ 4-2 (ก) - (ง) สำหรับรูปแบบความถี่ของการโจมตีแบบสุ่ม ตำแหน่งของการโจมตี กำหนดด้วยค่าส่วนเบี่ยงเบนมาตรฐาน $(\sigma)$ จำนวน 3 รูปแบบ คือ $\sigma = \{5, 15, 30\}$ ส่วนระยะเวลาในการโจมตี จะถูกสุ่มจากการแจกแจงแบบยูนิฟอร์ม ดังภาพประกอบที่ 4-3 (ก) - (ค)

ตารางที่ 4-1 รูปแบบที่ใช้ในการทดสอบขั้นตอนวิธี แบบกำหนดเอง

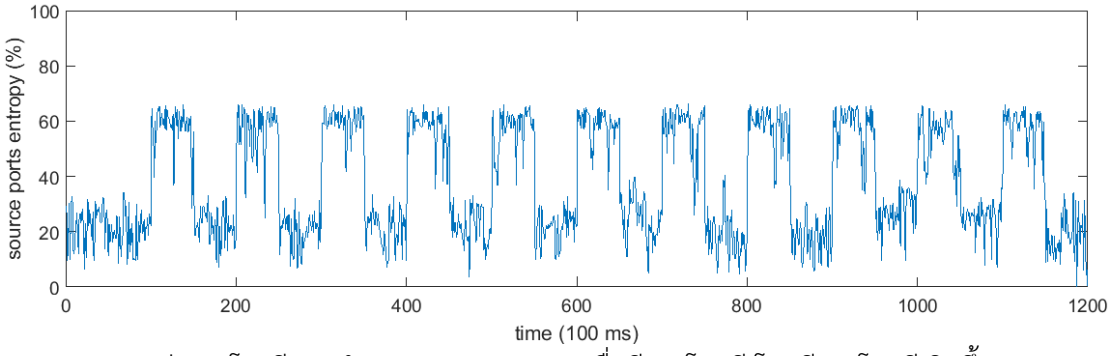
| **รูปแบบ** | **ตำแหน่งของการโจมตีที่ห่างกันด้วย Scale (100 ms)** | **ระยะเวลาการโจมตี (100 ms)/ครั้ง** |
|---|---|---|
| 1 | 150 | 100 |
| 2 | 100 | 50 |
| 3 | 50 | 25 |
| 4 | 50 | 15 |



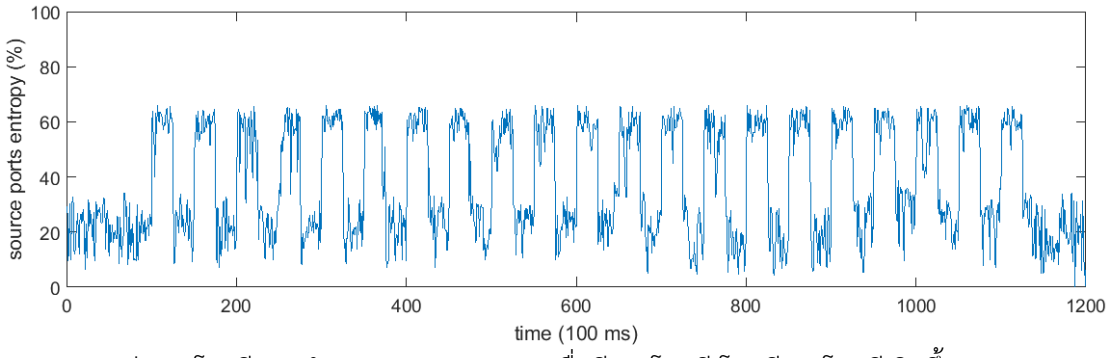

ภาพประกอบที่ 4-1 กราฟค่าเอนโทรปีของจำนวน Source Port เมื่อไม่มีการโจมตี



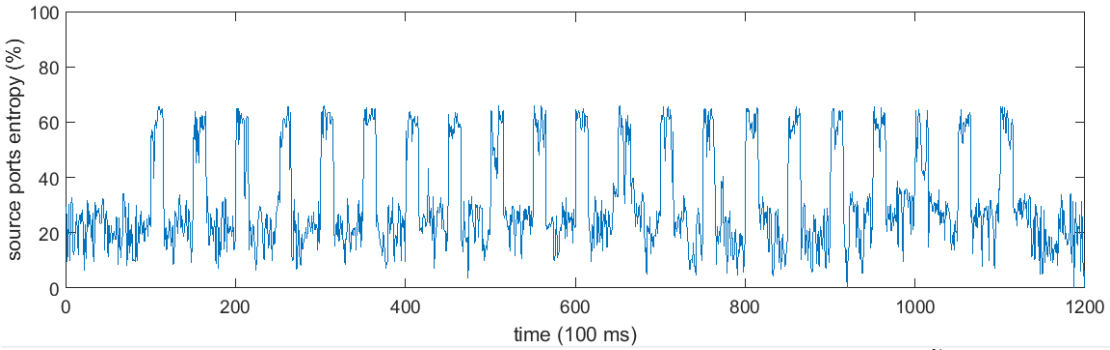

(ก) กราฟค่าเอนโทรปีของจำนวน Source Port เมื่อมีการโจมตี โดยมีการโจมตีเกิดขึ้นทุก ๆ 15000 ms และทุกครั้งที่โจมตีจะใช้เวลา 10000 ms




(ข) กราฟค่าเอนโทรปีของจำนวน Source Port เมื่อมีการโจมตี โดยมีการโจมตีเกิดขึ้นทุก ๆ 10000 ms และทุกครั้งที่โจมตีจะใช้เวลา 5000 ms

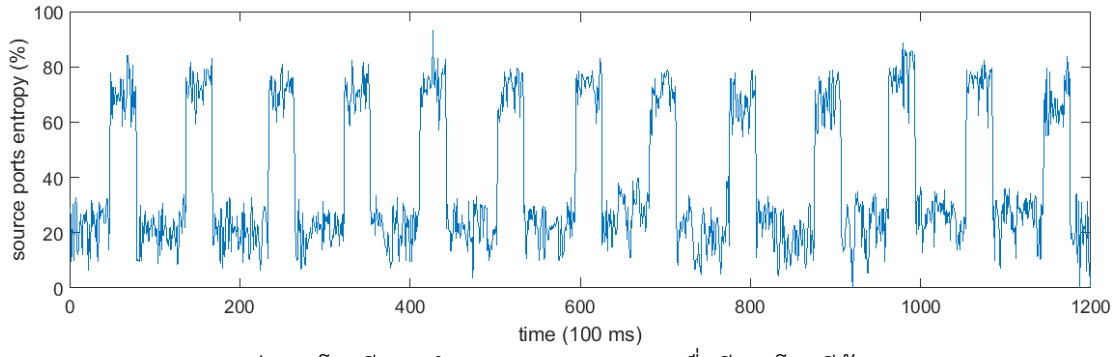



(ค) กราฟค่าเอนโทรปีของจำนวน Source Port เมื่อมีการโจมตี โดยมีการโจมตีเกิดขึ้นทุก ๆ 5000 msและทุกครั้งที่โจมตีจะใช้เวลา 2500 ms

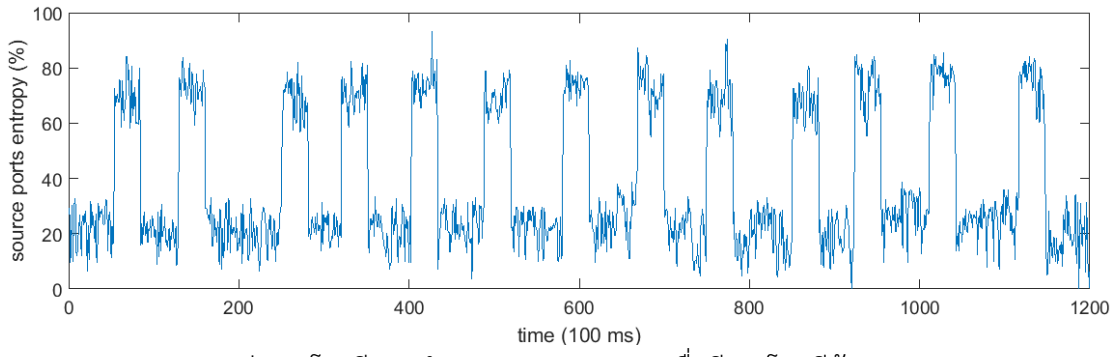



(ง) กราฟค่าเอนโทรปีของจำนวน Source Port เมื่อมีการโจมตี โดยมีการโจมตีเกิดขึ้นทุก ๆ 5000 msและทุกครั้งที่โจมตีจะใช้เวลา 1500 ms

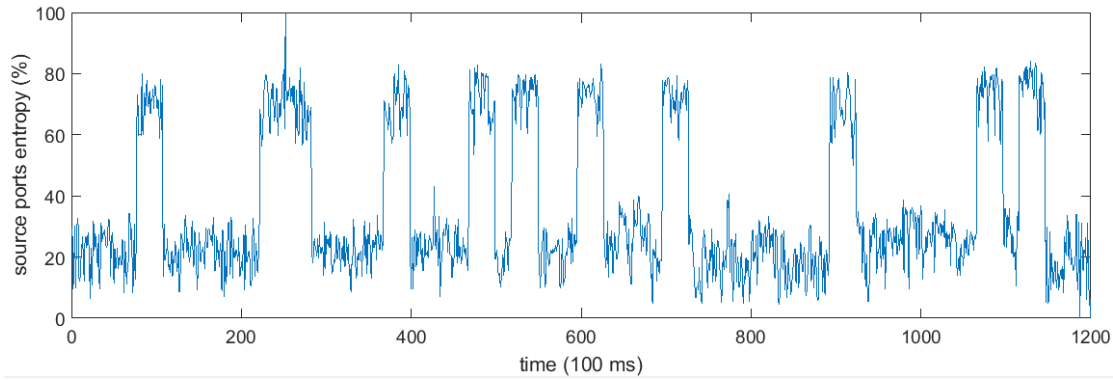
ภาพประกอบที่ 4-2 (ก)–(ง) รูปแบบการแจกแจงของความถี่ Source Port ที่มีการโจมตีแบบกำหนดเอง




(ก) กราฟค่าเอนโทรปีของจำนวน Source Port เมื่อมีการโจมตีด้วย $\sigma = 5$




(ข) กราฟค่าเอนโทรปีของจำนวน Source Port เมื่อมีการโจมตีด้วย $\sigma = 15$




(ค) กราฟค่าเอนโทรปีของจำนวน Source Port เมื่อมีการโจมตีด้วย $\sigma = 30$

ภาพประกอบที่ 4-3 (ก) - (ค) รูปแบบการโจมตีที่มีการสุ่มแบบยูนิฟอร์มด้วยค่าส่วนเบี่ยงเบนที่ต่างกัน

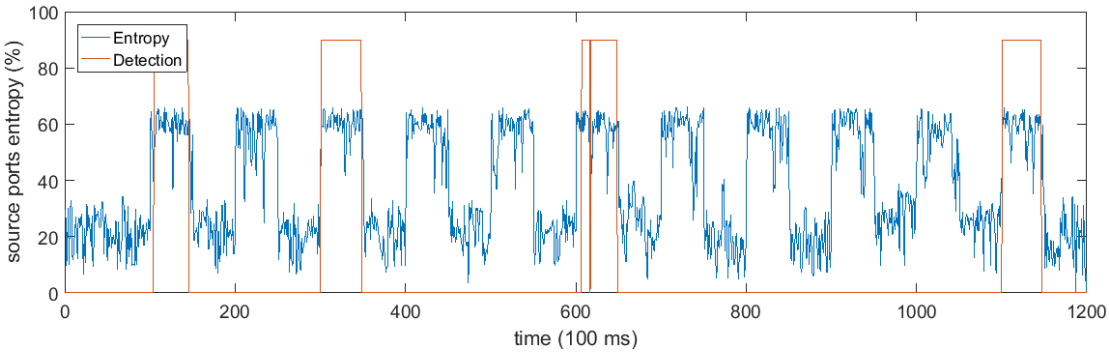
## 4.3 การกำหนดค่าตัวแปรต่าง ๆ ของวิธีที่นำเสนอ

จากขั้นตอนวิธีที่ได้นำเสนอในบทที่ 3 มีตัวแปรที่มีความสำคัญในการออกแบบวิธีการที่ใช้ตรวจหาความผิดปกติ นั่นคือ ตัวแปร Threshold $(T_{attack})$ ที่ใช้บ่งชี้ว่ามีการโจมตีหรือไม่ ส่วนตัวแปรขนาด Subgroup $(N)$ และตัวแปร Group $(G)$ จะบ่งบอกถึงสมรรถนะของตัวตรวจหาความผิดปกติ วิธีที่ใช้ในการกำหนดค่าตัวแปรต่าง ๆ เริ่มจากการหาช่วงที่เหมาะสมของ

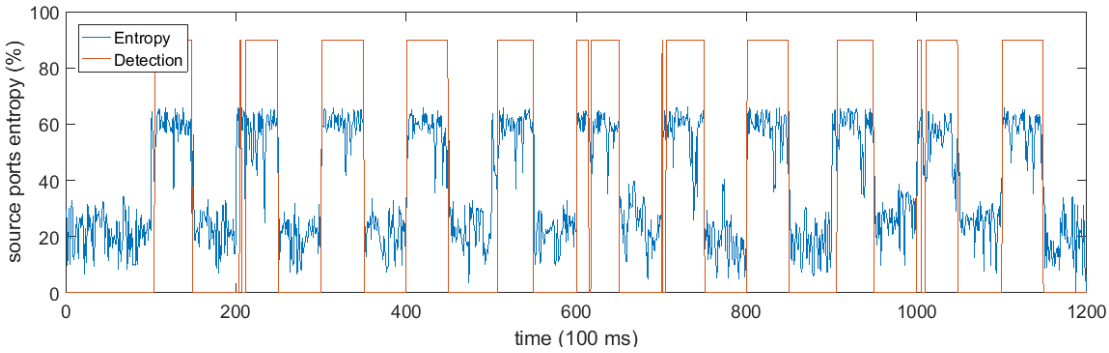
ค่าตัวแปร เมื่อได้ช่วงที่เหมาะสมแล้ว จึงจะพิจารณาเพิ่มความละเอียดค่าที่อยู่ในช่วงนั้นทีละ 1 ค่า เพื่อหาค่าที่เหมาะสมที่สุด ซึ่งการกำหนดค่าแต่ละตัวแปรมีรายละเอียดดังต่อไปนี้

### 4.3.1 ตัวแปร Threshold ($T_{attack}$)

ตัวแปร $T_{attack}$ คือค่า Threshold ที่ใช้ในการระบุความผิดปกติ เพื่อหาค่าที่เหมาะสมกับรูปแบบของความผิดปกติของข้อมูลที่มักจะมีรูปแบบต่าง ๆ กันดังที่ได้กล่าวมาแล้วในข้อ 4.1 ซึ่งค่าตัวแปร $T_{attack}$ ที่ใช้ในการทดสอบขั้นตอนวิธีที่นำเสนอ มีจำนวน 15 ค่า ได้แก่ 10, 15, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 35 และ 40




(ก) กำหนด $T_{attack} = 40$




(ข) กำหนด $T_{attack} = 24$

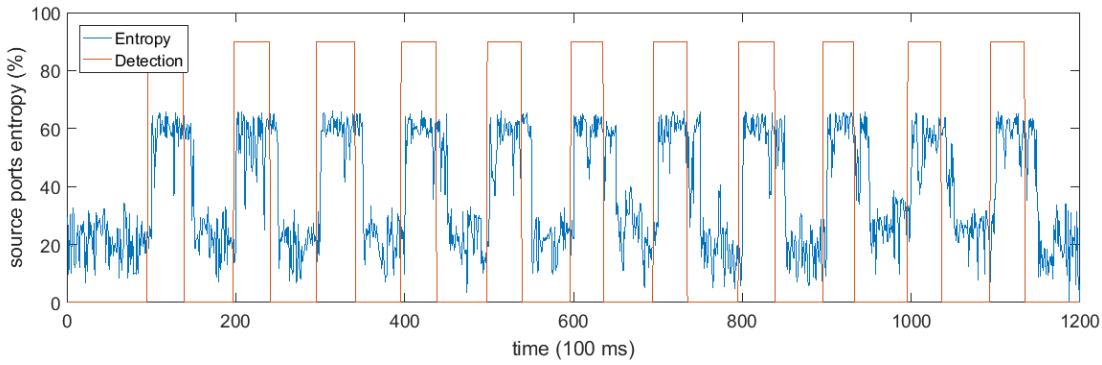
ภาพประกอบที่ 4-4 (ก) - (ข) กราฟผลลัพธ์จากการกำหนดค่า $T_{attack}$ ที่แตกต่างกัน

จากภาพประกอบที่ 4-4 (ก) และ (ข) เป็นกราฟแสดงจำนวน Source Port ที่มีการโจมตี เกิดพัลส์ขึ้นทุกตำแหน่งที่ห่างกัน 10000 ms และมีระยะเวลาการโจมตีครั้งละ 5000 ms เมื่อกำหนดตัวแปรขนาด Subgroup $N = 5$ และตัวแปร Group $G = 60$ การตรวจหาความผิดปกติด้วยขั้นตอนวิธีที่นำเสนอ ตัวแปร $T_{attack}$ ที่แตกต่างกัน ทำให้ความถูกต้องในการตรวจหาความผิดปกติแตกต่างกันด้วย จากรูป (ก) เมื่อกำหนด $T_{attack} = 40$ จะเห็นว่าตัวตรวจหา จับได้เพียง

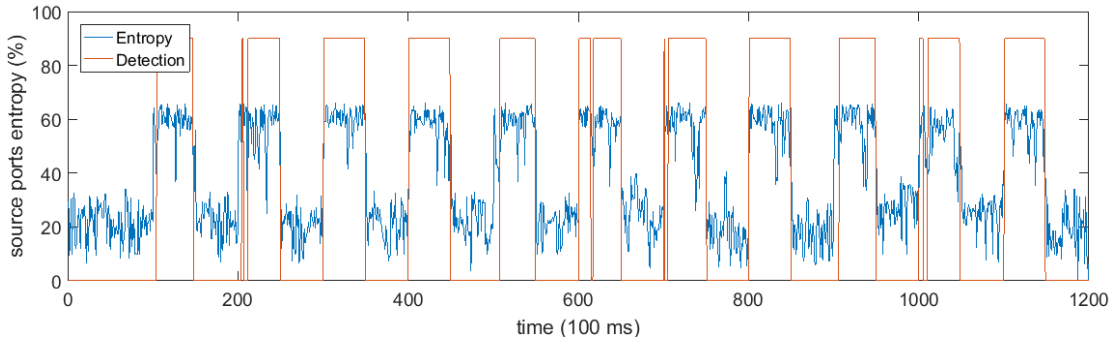
สี่พัลส์ ทั้งที่การโจมตีเกิดขึ้นทั้งหมดสิบเอ็ดพัลส์ ส่วนรูป (ข) เมื่อกำหนด $T_{attack} = 24$ จะเห็นว่าสามารถจับการโจมตีได้ทุกครั้ง

### 4.3.2 ตัวแปรขนาด Subgroup ($N$)

ตัวแปร $N$ ที่แทนขนาดของกลุ่มย่อย ซึ่งเป็นขนาดตัวอย่างที่ใช้ในการแบ่งกลุ่มของจำนวน Source Port ที่ได้ Encode ไว้ด้วยเอนโทรปี เพื่อใช้ในการคำนวณค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง ซึ่งค่าตัวแปร $N$ ที่ใช้ในการทดสอบขั้นตอนวิธีที่นำเสนอ มีจำนวน 14 ค่า ได้แก่ 2, 3, 4, 5, 6, 10, 11, 12, 13, 14, 15, 20, 25 และ 30 เมื่อกำหนดตัวแปร $T_{attack} = 24$ และตัวแปร Group $G = 60$




(ก) กำหนด $N = 30$




(ข) กำหนด $N = 5$

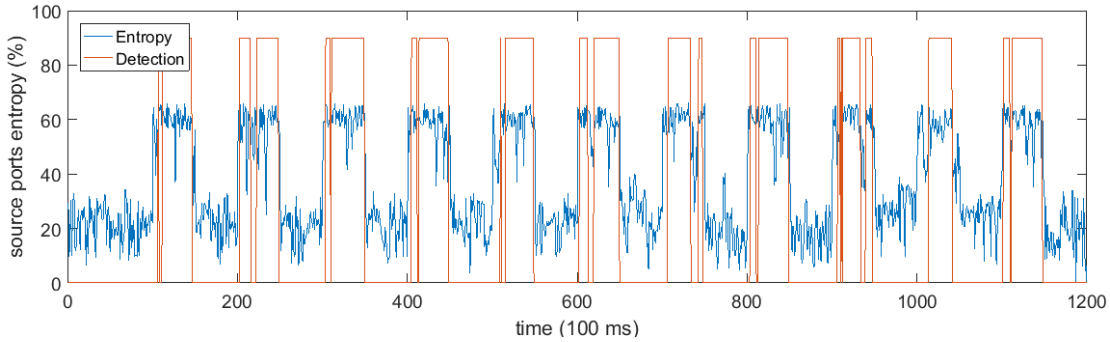
ภาพประกอบที่ 4-5 (ก) – (ข) กราฟผลลัพธ์จากการกำหนดค่า $N$ ที่แตกต่างกัน

จากภาพประกอบที่ 4-5 (ก) และ (ข) เป็นกราฟแสดงจำนวน Source Port ที่มีการโจมตีที่ทุกระยะห่างของตำแหน่งพัลส์เท่ากับ 10000 ms และมีความกว้างของพัลส์เป็นระยะเวลาการโจมตีครั้งละ 5000 ms เมื่อตรวจหาความผิดปกติด้วยขั้นตอนวิธีที่นำเสนอ ด้วยตัวแปร $N$ ที่แตกต่างกัน พบว่าขนาดของ $N$ มีผลต่อความถูกต้องแม่นยำของขั้นตอนวิธีในการตรวจหาความผิดปกติด้วย จากรูป (ก) เมื่อกำหนด $N = 30$ จะเห็นว่าในการตรวจหาแต่ละพัลส์ที่เกิดการโจมตี จับได้ไม่

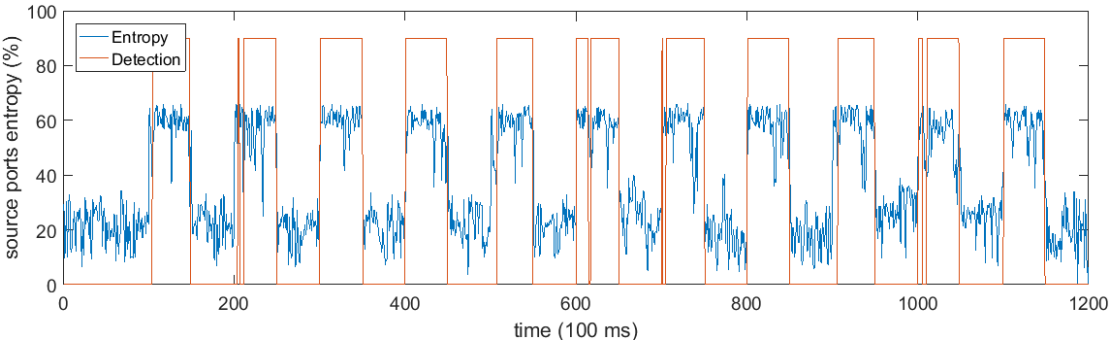
ครอบคลุมระยะเวลาในการโจมตีทั้งหมด ส่วนรูป (ข) เมื่อกำหนด $N = 5$ จะเห็นว่า สามารถตรวจหาการโจมตีได้แม่นยำกว่า

### 4.3.3 ตัวแปร Group ($G$)

ตัวแปร $G$ เป็นขนาดของกลุ่มตัวอย่างที่ใช้ในการพิจารณาจำนวนข้อมูลที่เหมาะสมในการคำนวณหา Control Line ในแต่ละครั้ง ซึ่งค่าตัวแปร $G$ ที่ใช้ในการทดสอบขั้นตอนวิธีที่นำเสนอ มีจำนวน 17 ค่า ได้แก่ 15, 30, 45, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 70, 90 และ 120 โดยที่มีการกำหนด $N$ และ $T_{attack}$ ไว้ที่ 5 และ 24 ตามลำดับ




(ก) กำหนด $G = 45$




(ข) กำหนด $G = 60$

ภาพประกอบที่ 4-6 (ก) – (ข) กราฟผลลัพธ์จากการกำหนดค่า $G$ ที่แตกต่างกัน

จากภาพประกอบที่ 4-6 (ก) และ (ข) เป็นกราฟแสดงจำนวน Source Port ที่มีการโจมตี เกิดขึ้นทุกช่วงระยะห่างของตำแหน่งพัลส์เท่ากับ 10000 ms และมีความกว้างของพัลส์เป็นระยะเวลาการโจมตีครั้งละ 5000 ms เมื่อตรวจหาความผิดปกติด้วยขั้นตอนวิธีที่นำเสนอ ด้วยตัวแปร $G$ ที่แตกต่างกันพบว่า ขนาดของ $G$ มีผลต่อความถูกต้องแม่นยำของขั้นตอนวิธีการตรวจหาความผิดปกติด้วยเช่นเดียวกัน จากรูป (ก) เมื่อกำหนด $G = 45$ จะเห็นว่าในการตรวจหาแต่ละพัลส์ที่มีการโจมตี ตัวตรวจหา จับได้ไม่ครอบคลุมระยะเวลาที่มีการโจมตีทั้งหมด ส่วนรูป (ข) เมื่อกำหนด $G = 60$ จะเห็นว่า สามารถตรวจหาได้ครอบคลุมแม่นยำกว่า

## 4.4 การวัดและการประเมินประสิทธิภาพ

การวัดความถูกต้องในการเลือกค่าของตัวแปรที่เหมาะสม (ตัวแปร Threshold: $T_{attack}$ ขนาดSubgroup: $N$ และ Group: $G$) กับการโจมตีที่ทำให้เกิดความผิดปกติในรูปแบบต่างๆ ที่ได้กล่าวมาแล้ว ดังตารางที่ 4-1 โดยเหตุการณ์ต่าง ๆ สามารถแบ่งออกเป็นกรณีด้วย Confusion matrix ที่แสดงในตารางที่ 4-2 ผู้วิจัยได้แบ่งการทดสอบออกเป็น 2 เหตุการณ์คือ เหตุการณ์ผิดปกติ (มีการโจมตี Pulse wave DDoS เกิดขึ้น) และเหตุการณ์ปกติ (ไม่มีการโจมตีเกิดขึ้นเลย) โดยเหตุการณ์ผิดปกติ (มีการโจมตี) จะแบ่งการทดสอบออกเป็น 2 ลักษณะ คือ ทดสอบอัตราความผิดพลาดในการตรวจหาเชิงบวก (False Positive Rate: FPR) คือ การที่เหตุการณ์ปกติ(ไม่มีการโจมตี) แต่ตัวตรวจหาระบุว่ามีการโจมตีเกิดขึ้น และ ทดสอบอัตราความผิดพลาดในการตรวจหาเชิงลบ (False Negative Rate: FNR) นั่นคือ การที่มีเหตุการณ์ผิดปกติ (มีการโจมตี) แต่ตัวตรวจหาไม่สามารถระบุความผิดปกติที่เกิดขึ้นได้ และสำหรับเหตุการณ์ปกติ (ไม่มีการโจมตี) จะทำการทดสอบเพียงกรณีเดียว คือ ทดสอบอัตราความผิดพลาดในการตรวจหาเชิงบวก (False Positive Rate: FPR) คือ การที่เหตุการณ์ปกติ(ไม่มีการโจมตี) แต่ตัวตรวจหาระบุว่ามีการโจมตีเกิดขึ้น ซึ่งในที่นี้ได้นำมาใช้ในการเลือกค่าของตัวแปรที่เหมาะสม โดยใช้ค่าความถูกต้อง (Accuracy: ACC) และมีวิธีการคำนวณดังนี้

ตารางที่ 4-2 Confusion matrix

| | | **True condition** | |
|---|---|---|---|
| | | Condition positive | Condition negative |
| **Predicted condition** | Predicted condition positive | $True\ positive$ $(TP)$ | $False\ positive$ $(FP)$ |
| | Predicted condition negative | $False\ negative$ $(FN)$ | $True\ negative$ $(TN)$ |
| | | $n_2$ | $n_1$ |

$$FPR = \frac{FP}{n_1} \tag{4.1}$$

$$FNR = \frac{FN}{n_2} \tag{4.2}$$

$$ACC = \frac{TP + TN}{n_1 + n_2} \tag{4.3}$$

โดยที่ $FP$ คือ จำนวนข้อมูลที่เป็นเหตุการณ์ปกติ แต่ถูกระบุว่าเป็นการโจมตี

$FN$ คือ จำนวนข้อมูลที่เป็นเหตุการณ์ผิดปกติ แต่ไม่สามารถระบุได้

$TP$ คือ จำนวนข้อมูลที่เป็นเหตุการณ์ปกติ และสามารถระบุได้ถูกต้อง

$TN$ คือ จำนวนข้อมูลที่เป็นเหตุการณ์ผิดปกติ และสามารถระบุได้ถูกต้อง

$n_1$ คือ จำนวนข้อมูลที่เป็นเหตุการณ์ปกติทั้งหมด

$n_2$ คือ จำนวนข้อมูลที่เป็นเหตุการณ์ผิดปกติทั้งหมด

## 4.5 ผลการทดลองและการเปรียบเทียบ

ผลการทดลองจะแบ่งตามชนิดของตัวแปร คือ ตัวแปร Threshold $(T_{attack})$ ตัวแปรขนาด Subgroup $(N)$ และตัวแปร Group $(G)$ ซึ่งแต่ละตัวแปรจะแบ่งผลการทดลองออกเป็น 2 กรณีนั่นคือ ค่าที่ตัดสินใจได้ (ใช้การเลือกค่าของตัวแปรที่เหมาะสมในขั้นตอนวิธีในการตรวจหาความผิดปกติ ที่กล่าวไว้แล้วในหัวข้อ 3.5) ตรงกับค่าความถูกต้อง (Accuracy: ACC) และ ค่าที่ตัดสินใจได้ ต่างกับค่าความถูกต้อง และผลการทดลองโดยทดลองกับข้อมูลแบบสุ่ม ดังตารางที่ 4-3 – 4-14 และภาพประกอบที่ 4-7 – 4-9 ในงานวิจัยชิ้นนี้ ได้นำเสนอกฎในการตัดสินใจเลือกค่าของตัวแปรต่าง ๆ สรุปเป็นข้อได้ดังนี้

1. เลือกค่าของตัวแปรที่ทำให้ FPR ของเหตุการณ์ปกติมีค่าเท่ากับ 0
2. จากเซตของคำตอบในข้อ 1 ตัวแปรที่ถูกเลือก คือตัวแปรที่ทำให้ FNR ของเหตุการณ์ผิดปกติ มีค่าน้อยที่สุด

### 4.5.1 ผลการทดลองตัวแปร Threshold

#### 4.5.1.1 ค่าที่ตัดสินใจได้ตรงกับค่าความถูกต้อง

ตารางที่ 4-3 การตัดสินใจเลือกค่า Threshold ที่เหมาะสมของความผิดปกติรูปแบบที่ 3

| Threshold | เหตุการณ์ผิดปกติ | | เหตุการณ์ปกติ | ACC |
|---|---|---|---|---|
| | FNR | FPR | FPR | |
| 10 | 0.1905 | 0.0178 | 0.0617 | 0.9067 |
| 15 | 0.1905 | 0.0059 | 0.0300 | 0.9133 |
| 20 | 0.1905 | 0.0030 | 0.0183 | 0.9150 |
| 21 | 0.1867 | 0.0015 | 0.0183 | 0.9175 |
| 22 | 0.1790 | 0.0015 | 0 | 0.9208 |
| 23 | 0.1714 | 0.0015 | 0 | 0.9242 |
| 24 | 0.1543 | 0.0015 | 0 | 0.9317 |
| 25 | 0.1295 | 0.0015 | 0 | 0.9425 |
| 26 | 0.1124 | 0 | 0 | 0.9508 |
| 27 | 0.1048 | 0 | 0 | 0.9542 |
| **28** | **0.0952** | **0** | **0** | **0.9583** |
| 29 | 0.1219 | 0 | 0 | 0.9467 |
| 30 | 0.6629 | 0 | 0 | 0.7100 |
| 35 | 1 | 0 | 0 | 0.5625 |
| 40 | 1 | 0 | 0 | 0.5625 |

จากตารางที่ 4-3 สำหรับรูปแบบของความผิดปกติรูปแบบที่ 3 นั่นคือมีการโจมตีเกิดขึ้นทุกช่วงระยะห่างของตำแหน่ง 5000 ms และมีระยะเวลาการโจมตีครั้งละ 2500 ms เมื่อกำหนดค่าตัวแปรขนาด Subgroup $N = 3$ และ ตัวแปร Group $G = 57$ จะเห็นว่า ค่า Threshold ที่เลือก และ ค่า Threshold ที่ตัดสินใจได้จากการคำนวณค่า ACC มีค่าเท่ากันคือ 28 โดยมีค่า FNR = 0.0952, FPR และ FPR เมื่อเหตุการณ์ปกติ = 0 และมีค่า ACC = 0.9583 ซึ่งเป็นค่าสูงสุด

ตารางที่ 4-4 การตัดสินใจเลือกค่า Threshold ที่เหมาะสมของความผิดปกติรูปแบบที่ 4

| Threshold | เหตุการณ์ผิดปกติ | | เหตุการณ์ปกติ | ACC |
|---|---|---|---|---|
| | FNR | FPR | FPR | |
| 10 | 0.1302 | 0.0271 | 0.0608 | 0.9458 |
| 15 | 0.1048 | 0.0316 | 0.0275 | 0.9492 |
| 20 | 0.0413 | 0.0158 | 0.0175 | 0.9775 |
| 21 | 0.0349 | 0.0158 | 0.0183 | 0.9792 |
| 22 | 0.0222 | 0.0147 | 0 | 0.9833 |
| **23** | **0.0127** | **0.0113** | **0** | **0.9883** |
| 24 | 0.1937 | 0.0068 | 0 | 0.9442 |
| 25 | 1 | 0 | 0 | 0.7375 |
| 26 | 1 | 0 | 0 | 0.7375 |
| 27 | 1 | 0 | 0 | 0.7375 |
| 28 | 1 | 0 | 0 | 0.7375 |
| 29 | 1 | 0 | 0 | 0.7375 |
| 30 | 1 | 0 | 0 | 0.7375 |
| 35 | 1 | 0 | 0 | 0.7375 |
| 40 | 1 | 0 | 0 | 0.7375 |

จากตารางที่ 4-4 สำหรับรูปแบบของความผิดปกติรูปแบบที่ 4 นั่นคือมีการโจมตีเกิดขึ้นทุกช่วงระยะห่างของตำแหน่ง 5000 ms และมีระยะเวลาการโจมตีครั้งละ 1500 ms เมื่อกำหนดค่าตัวแปรขนาด Subgroup $N = 3$ และ ตัวแปร Group $G = 60$ จะเห็นว่า ค่า Threshold ที่เลือก และ ค่า Threshold ที่ตัดสินใจได้จากการคำนวณค่า ACC มีค่าเท่ากันคือ 23 โดยมีค่า FNR = 0.0127, FPR = 0.0113 และ FPR เมื่อเหตุการณ์ปกติ = 0 และมีค่า ACC = 0.9883 ซึ่งเป็นค่าสูงสุด

#### 4.5.1.2 ค่าที่ตัดสินใจได้ต่างกับค่าความถูกต้อง

ตารางที่ 4-5 การตัดสินใจเลือกค่า Threshold ที่เหมาะสมของความผิดปกติรูปแบบที่ 1

| Threshold | เหตุการณ์ผิดปกติ | | เหตุการณ์ปกติ | ACC |
|---|---|---|---|---|
| | FNR | FPR | FPR | |
| 10 | 0.0986 | 0.0020 | 0.0808 | 0.9417 |
| 15 | 0.0986 | 0 | 0.1050 | 0.9425 |
| 20 | 0.0986 | 0 | 0.0967 | 0.9425 |
| 21 | 0.0986 | 0 | 0.1100 | 0.9425 |
| 22 | 0.0986 | 0 | 0.0958 | 0.9425 |
| 23 | 0.0986 | 0 | 0.0983 | 0.9425 |
| 24 | 0.0986 | 0 | 0.0975 | 0.9425 |
| 25 | 0.0986 | 0 | 0.1017 | 0.9425 |
| 26 | 0.0986 | 0 | 0.1083 | 0.9425 |
| 27 | 0.0986 | 0 | 0.1125 | 0.9425 |
| 28 | 0.0986 | 0 | 0.1117 | 0.9425 |
| 29 | 0.0986 | 0 | 0.1142 | 0.9425 |
| 30 | 0.0986 | 0 | 0.1092 | 0.9425 |
| **35** | **0.0986** | **0** | **0** | **0.9425** |
| 40 | 0.1000 | 0 | 0 | 0.9425 |

จากตารางที่ 4-5 สำหรับรูปแบบของความผิดปกติรูปแบบที่ 1 นั่นคือมีการโจมตีเกิดขึ้นทุกช่วงระยะห่างของตำแหน่ง 15000 ms และมีระยะเวลาการโจมตีครั้งละ 10000 ms เมื่อกำหนดค่าตัวแปรขนาด Subgroup $N = 13$ และ ตัวแปร Group $G = 120$ จะเห็นว่าค่า Threshold ที่เลือกคือ 35 ซึ่งมีค่า FNR = 0.0986, FPR และ FPR เมื่อเหตุการณ์ปกติ = 0 และมีค่า ACC = 0.9425 ส่วนค่า Threshold ที่ตัดสินใจได้จากการคำนวณค่า ACC อยู่ในช่วง 15 - 35 เนื่องจากค่า ACC มีค่ามากที่สุดเท่ากันนั่นคือ 0.9425

ตารางที่ 4-6 การตัดสินใจเลือกค่า Threshold ที่เหมาะสมของความผิดปกติรูปแบบที่ 2

| Threshold | เหตุการณ์ผิดปกติ | | เหตุการณ์ปกติ | ACC |
|---|---|---|---|---|
| | FNR | FPR | FPR | |
| 10 | 0.0891 | 0.0154 | 0.892 | 0.9508 |
| **15** | **0.0764** | **0.0046** | **0.0525** | **0.9625** |
| 20 | 0.0855 | 0 | 0.0192 | 0.9608 |
| 21 | 0.0855 | 0 | 0.0208 | 0.9608 |
| 22 | 0.0855 | 0 | 0.0208 | 0.9608 |
| 23 | 0.0873 | 0 | 0.0200 | 0.9600 |
| **24** | **0.0891** | **0** | **0** | **0.9592** |
| 25 | 0.0927 | 0 | 0 | 0.9575 |
| 26 | 0.0982 | 0 | 0 | 0.9550 |
| 27 | 0.1000 | 0 | 0 | 0.9542 |
| 28 | 0.1073 | 0 | 0 | 0.9508 |
| 29 | 0.1236 | 0 | 0 | 0.9433 |
| 30 | 0.1291 | 0 | 0 | 0.9408 |
| 35 | 0.2800 | 0 | 0 | 0.8717 |
| 40 | 0.6800 | 0 | 0 | 0.6883 |

จากตารางที่ 4-6 สำหรับรูปแบบของความผิดปกติรูปแบบที่ 2 นั่นคือมีการโจมตีเกิดขึ้นทุกช่วงระยะห่างของตำแหน่ง 10000 ms และมีระยะเวลาการโจมตีครั้งละ 5000 ms เมื่อกำหนดค่าตัวแปรขนาด Subgroup $N = 5$ และ ตัวแปร Group $G = 60$ จะเห็นว่า ค่า Threshold ที่เลือกคือ 24 ซึ่งมีค่า FNR = 0.0891, FPR และ FPR เมื่อเหตุการณ์ปกติ = 0 และมีค่า ACC = 0.9592 ส่วนค่า Threshold ที่ใช้เงื่อนไขตัดสินใจได้จากค่า ACC สูงสุดอยู่ที่ 15 นั่นคือค่า ACC มีค่ามากที่สุด = 0.9625 แต่จะมีค่า FNR = 0.0764, FPR = 0.0046 และค่า FPR เมื่อเหตุการณ์ปกติ = 0.0525 ดังนั้นจึงไม่เลือกค่า Threshold = 15

### 4.5.2 ผลการทดลองตัวแปร Subgroup

#### 4.5.2.1 ค่าที่ตัดสินใจได้ตรงกับค่าความถูกต้อง

ตารางที่ 4-7 การเลือกขนาดของ Subgroup ที่เหมาะสมของความผิดปกติรูปแบบที่ 1

| Subgroup | เหตุการณ์ผิดปกติ | | เหตุการณ์ปกติ | ACC |
|---|---|---|---|---|
| | FNR | FPR | FPR | |
| 2 | 0.3114 | 0.0020 | 0 | 0.8175 |
| 3 | 0.2829 | 0.0020 | 0 | 0.8342 |
| 4 | 0.2471 | 0.0020 | 0 | 0.8550 |
| 5 | 0.2243 | 0.0020 | 0 | 0.8683 |
| 6 | 0.2000 | 0.0020 | 0 | 0.8825 |
| 10 | 0.1286 | 0 | 0 | 0.9250 |
| 11 | 0.1100 | 0 | 0 | 0.9358 |
| 12 | 0.1029 | 0 | 0 | 0.9400 |
| **13** | **0.0986** | **0** | **0** | **0.9425** |
| 14 | 0.1071 | 0 | 0.0600 | 0.9375 |
| 15 | 0.1143 | 0.0020 | 0.0642 | 0.9325 |
| 20 | 0.1443 | 0.0120 | 0.0733 | 0.9108 |
| 25 | 0.1686 | 0.0260 | 0.1033 | 0.8908 |
| 30 | 0.2043 | 0.0400 | 0.1092 | 0.8642 |

จากตารางที่ 4-7 สำหรับรูปแบบของความผิดปกติรูปแบบที่ 1 นั่นคือมีการโจมตีเกิดขึ้นทุกช่วงระยะห่างของตำแหน่ง 15000 ms และมีระยะเวลาการโจมตีครั้งละ 10000 ms เมื่อกำหนดค่าตัวแปร Threshold $T_{attack} = 35$ และ ตัวแปร Group $G = 120$ จะเห็นว่าค่าขนาด Subgroup ที่เลือก และ ค่าขนาด Subgroup ที่ตัดสินใจได้จากการคำนวณค่า ACC มีค่าเท่ากันคือ 13 โดยมีค่า FNR = 0.0986, FPR และ FPR เมื่อเหตุการณ์ปกติเป็น 0 และมีค่า ACC = 0.9425 ซึ่งเป็นค่าสูงสุด

ตารางที่ 4-8 การเลือกขนาดของ Subgroup ที่เหมาะสมของความผิดปกติรูปแบบที่ 2

| Subgroup | เหตุการณ์ผิดปกติ | | เหตุการณ์ปกติ | ACC |
|---|---|---|---|---|
| | FNR | FPR | FPR | |
| 2 | 0.1745 | 0.0031 | 0 | 0.9183 |
| 3 | 0.1255 | 0 | 0 | 0.9425 |
| 4 | 0.1000 | 0 | 0 | 0.9542 |
| **5** | **0.0891** | **0** | **0** | **0.9592** |
| 6 | 0.1000 | 0.0015 | 0.0217 | 0.9533 |
| 10 | 0.0945 | 0.0046 | 0.0217 | 0.9542 |
| 11 | 0.1018 | 0 | 0.0208 | 0.9533 |
| 12 | 0.1036 | 0 | 0.0250 | 0.9525 |
| 13 | 0.1127 | 0 | 0.0242 | 0.9483 |
| 14 | 0.1164 | 0 | 0.0233 | 0.9467 |
| 15 | 0.1200 | 0.0138 | 0.0233 | 0.9375 |
| 20 | 0.1527 | 0.0308 | 0.0283 | 0.9133 |
| 25 | 0.2000 | 0.0615 | 0.0283 | 0.8750 |
| 30 | 0.2455 | 0.0862 | 0.0458 | 0.8408 |

จากตารางที่ 4-8 สำหรับรูปแบบของความผิดปกติรูปแบบที่ 2 นั่นคือมีการโจมตีเกิดขึ้นทุกช่วงระยะห่างของตำแหน่ง 10000 ms และมีระยะเวลาการโจมตีครั้งละ 5000 ms เมื่อกำหนดค่าตัวแปร Threshold $T_{attack} = 24$ และ ตัวแปร Group $G = 60$ จะเห็นว่าค่าขนาด Subgroup ที่เลือก และ ค่าขนาด Subgroup ที่ตัดสินใจได้จากการคำนวณค่า ACC มีค่าเท่ากันคือ 5 โดยมีค่า FNR = 0.0891, FPR และ FPR เมื่อเหตุการณ์ปกติ = 0 และมีค่า ACC = 0.9592 ซึ่งเป็นค่าสูงสุด

ตารางที่ 4-9 การเลือกขนาดของ Subgroup ที่เหมาะสมของความผิดปกติรูปแบบที่ 3

| Subgroup | เหตุการณ์ผิดปกติ | | เหตุการณ์ปกติ | ACC |
|---|---|---|---|---|
| | FNR | FPR | FPR | |
| 2 | 0.1429 | 0 | 0 | 0.9375 |
| **3** | **0.0952** | **0** | **0** | **0.9583** |
| 4 | 0.0971 | 0.0044 | 0 | 0.9550 |
| 5 | 0.1124 | 0.0104 | 0 | 0.9450 |
| 6 | 0.1371 | 0.0163 | 0 | 0.9308 |
| 10 | 0.4286 | 0.0341 | 0 | 0.7933 |
| 11 | 0.8419 | 0.0178 | 0 | 0.6217 |
| 12 | 0.6514 | 0.0296 | 0 | 0.6983 |
| 13 | 0.9390 | 0.0104 | 0 | 0.5833 |
| 14 | 0.9771 | 0.0059 | 0 | 0.5692 |
| 15 | 0.8990 | 0.0119 | 0.0242 | 0.6000 |
| 20 | 1 | 0 | 0.0267 | 0.5625 |
| 25 | 1 | 0 | 0.0258 | 0.5625 |
| 30 | 0.9714 | 0.0222 | 0.0242 | 0.5625 |

จากตารางที่ 4-9 สำหรับรูปแบบของความผิดปกติรูปแบบที่ 3 นั่นคือมีการโจมตีเกิดขึ้นทุกช่วงระยะห่างของตำแหน่ง 5000 ms และมีระยะเวลาการโจมตีครั้งละ 2500 ms เมื่อกำหนดค่าตัวแปร Threshold $T_{attack} = 28$ โดยกำหนดให้ตัวแปร Group $G = 57$ จะเห็นว่าค่าขนาด Subgroup ที่ถูกเลือก และ ค่าขนาด Subgroup ที่ตัดสินใจได้จากค่า ACC ที่มีค่าสูงสุดจะได้ค่าขนาดกลุ่มย่อยเท่ากันคือ 3 โดยมีค่า FNR = 0.0952, FPR และ FPR เมื่อเหตุการณ์ปกติ = 0 และมีค่า ACC = 0.9583 ซึ่งเป็นค่าสูงสุด

ตารางที่ 4-10 การเลือกขนาดของ Subgroup ที่เหมาะสมของความผิดปกติรูปแบบที่ 4

| Subgroup | เหตุการณ์ผิดปกติ | | เหตุการณ์ปกติ | ACC |
|---|---|---|---|---|
| | FNR | FPR | FPR | |
| 2 | 0.0698 | 0.0034 | 0 | 0.9792 |
| **3** | **0.0127** | **0.0113** | **0** | **0.9883** |
| 4 | 0.0476 | 0.0169 | 0 | 0.9750 |
| 5 | 0.0762 | 0.0226 | 0.0200 | 0.9633 |
| 6 | 0.0825 | 0.0554 | 0.0217 | 0.9375 |
| 10 | 0.2159 | 0.0723 | 0.0233 | 0.8900 |
| 11 | 0.3333 | 0.0689 | 0.0267 | 0.8617 |
| 12 | 0.2952 | 0.0847 | 0.0242 | 0.8600 |
| 13 | 0.3556 | 0.0904 | 0.0233 | 0.8400 |
| 14 | 0.3587 | 0.1085 | 0.0225 | 0.8258 |
| 15 | 0.3937 | 0.1130 | 0.0225 | 0.8133 |
| 20 | 0.5111 | 0.1819 | 0.0283 | 0.7317 |
| 25 | 0.6349 | 0.1944 | 0.0267 | 0.6900 |
| 30 | 0.8286 | 0.1740 | 0.0450 | 0.6542 |

จากตารางที่ 4-10 สำหรับรูปแบบของความผิดปกติรูปแบบที่ 4 นั่นคือมีการโจมตีเกิดขึ้นทุกช่วงระยะห่างของตำแหน่ง 5000 ms และมีระยะเวลาการโจมตีครั้งละ 1500 ms เมื่อกำหนดค่าตัวแปร Threshold $T_{attack} = 23$ และ ตัวแปร Group $G = 60$ จะเห็นว่าค่าขนาด Subgroup ที่เลือก และ ค่าขนาด Subgroup ที่ตัดสินใจได้จากค่า ACC ที่มีค่าสูงสุดจะได้ค่าขนาดกลุ่มย่อยเท่ากันคือ 3 โดยมีค่า FNR = 0.0127, FPR = 0.0113 และ FPR เมื่อเหตุการณ์ปกติ = 0 และมีค่า ACC = 0.9883 ซึ่งเป็นค่าสูงสุด

### 4.5.3 ผลการทดลองตัวแปร Group

#### 4.5.3.1 ค่าที่ตัดสินใจได้ตรงกับค่าความถูกต้อง

ตารางที่ 4-11 การเลือกขนาดของ Group ที่เหมาะสมของความผิดปกติรูปแบบที่ 1

| Group | เหตุการณ์ผิดปกติ | | เหตุการณ์ปกติ | ACC |
|---|---|---|---|---|
| | FNR | FPR | FPR | |
| 15 | 1 | 0 | 0 | 0.4167 |
| 30 | 1 | 0 | 0 | 0.4167 |
| 45 | 1 | 0 | 0 | 0.4167 |
| 55 | 0.3429 | 0 | 0 | 0.8000 |
| 56 | 0.3229 | 0 | 0 | 0.8117 |
| 57 | 0.3071 | 0 | 0 | 0.8208 |
| 58 | 0.2486 | 0.0040 | 0 | 0.8533 |
| 59 | 0.2357 | 0.0020 | 0 | 0.8617 |
| 60 | 0.2329 | 0.0020 | 0 | 0.8633 |
| 61 | 0.2257 | 0.0020 | 0 | 0.8675 |
| 62 | 0.2243 | 0.0020 | 0 | 0.8683 |
| 63 | 0.2229 | 0.0020 | 0 | 0.8692 |
| 64 | 0.2386 | 0.0020 | 0 | 0.8600 |
| 65 | 0.2471 | 0 | 0 | 0.8558 |
| 70 | 0.2429 | 0 | 0.0300 | 0.8583 |
| 90 | 0.2543 | 0 | 0.0308 | 0.8517 |
| **120** | **0.0986** | **0** | **0** | **0.9425** |

จากตารางที่ 4-11 สำหรับรูปแบบของความผิดปกติรูปแบบที่ 1 นั่นคือมีการโจมตีเกิดขึ้นทุกช่วงระยะห่างของตำแหน่ง 15000 ms และมีระยะเวลาการโจมตีครั้งละ 10000 ms เมื่อกำหนดค่าตัวแปร Threshold $T_{attack} = 35$ และ ตัวแปรขนาด Subgroup $N = 13$ จะเห็นว่าค่า Group ที่สอดคล้องกับค่า ACC สูงสุดคือ 120 โดยมีค่า FNR = 0.0986, FPR และ FPR เมื่อเหตุการณ์ปกติ = 0 และมีค่า ACC = 0.9425 ซึ่งเป็นค่าสูงสุด

ตารางที่ 4-12 การเลือกขนาดของ Group ที่เหมาะสมของความผิดปกติรูปแบบที่ 3

| Group | เหตุการณ์ผิดปกติ | | เหตุการณ์ปกติ | ACC |
|---|---|---|---|---|
| | FNR | FPR | FPR | |
| 15 | 1 | 0 | 0 | 0.5625 |
| 30 | 1 | 0 | 0 | 0.5625 |
| 45 | 1 | 0 | 0 | 0.5625 |
| 55 | 0.4590 | 0 | 0 | 0.7992 |
| 56 | 0.1200 | 0 | 0 | 0.9475 |
| **57** | **0.0952** | **0** | **0** | **0.9583** |
| 58 | 0.1086 | 0 | 0 | 0.9525 |
| 59 | 0.1010 | 0 | 0 | 0.9558 |
| 60 | 0.1124 | 0 | 0 | 0.9508 |
| 61 | 0.1238 | 0 | 0 | 0.9458 |
| 62 | 0.1410 | 0 | 0 | 0.9383 |
| 63 | 0.1429 | 0 | 0 | 0.9375 |
| 64 | 0.1410 | 0 | 0 | 0.9383 |
| 65 | 0.1429 | 0 | 0 | 0.9375 |
| 70 | 0.1429 | 0 | 0 | 0.9375 |
| 90 | 0.1352 | 0.0030 | 0 | 0.9392 |
| 120 | 0.1752 | 0.0030 | 0.0292 | 0.9217 |

จากตารางที่ 4-12 สำหรับรูปแบบของความผิดปกติรูปแบบที่ 3 นั่นคือมีการโจมตีเกิดขึ้นทุกช่วงระยะห่างของตำแหน่ง 5000 ms และมีระยะเวลาการโจมตีครั้งละ 2500 ms เมื่อกำหนดค่าตัวแปร Threshold $T_{attack} = 28$ และ ตัวแปรขนาด Subgroup $N = 3$ จะเห็นว่าค่า Group ที่สอดคล้องกับค่า ACC สูงสุดคือ 57 โดยมีค่า FNR = 0.0952, FPR และ FPR เมื่อเหตุการณ์ปกติ = 0 และมีค่า ACC = 0.9583 ซึ่งเป็นค่าสูงสุด

ตารางที่ 4-13 การเลือกขนาดของ Group ที่เหมาะสมของความผิดปกติรูปแบบที่ 4

| Group | เหตุการณ์ผิดปกติ | | เหตุการณ์ปกติ | ACC |
|---|---|---|---|---|
| | FNR | FPR | FPR | |
| 15 | 1 | 0 | 0 | 0.7375 |
| 30 | 1 | 0 | 0 | 0.7375 |
| 45 | 1 | 0 | 0 | 0.7375 |
| 55 | 1 | 0 | 0 | 0.7375 |
| 56 | 1 | 0 | 0 | 0.7375 |
| 57 | 1 | 0 | 0 | 0.7375 |
| 58 | 0.8254 | 0.0045 | 0 | 0.7800 |
| 59 | 0.1111 | 0.0090 | 0 | 0.9642 |
| **60** | **0.0127** | **0.0113** | **0** | **0.9883** |
| 61 | 0.0222 | 0.0113 | 0 | 0.9858 |
| 62 | 0.0317 | 0.0102 | 0 | 0.9842 |
| 63 | 0.0317 | 0.0090 | 0 | 0.9850 |
| 64 | 0.0286 | 0.0079 | 0 | 0.9867 |
| 65 | 0.0254 | 0.0079 | 0 | 0.9875 |
| 70 | 0.0254 | 0.0102 | 0.0200 | 0.9858 |
| 90 | 0.0190 | 0.0237 | 0.0417 | 0.9775 |
| 120 | 0.1143 | 0.0158 | 0.0308 | 0.9583 |

จากตารางที่ 4-13 สำหรับรูปแบบของความผิดปกติรูปแบบที่ 4 นั่นคือมีการโจมตีเกิดขึ้นทุกช่วงระยะห่างของตำแหน่ง 5000 ms และมีระยะเวลาการโจมตีครั้งละ 1500 ms เมื่อกำหนดค่าตัวแปร Threshold $T_{attack} = 23$ และ ตัวแปรขนาด Subgroup $N = 3$ จะเห็นว่าค่า Group ที่สอดคล้องกับค่า ACC มีค่าสูงสุดคือ 60 โดยมีค่า FNR = 0.0127, FPR = 0.0113 และ FPR เมื่อเหตุการณ์ปกติ = 0 และมีค่า ACC = 0.9883 ซึ่งเป็นค่าสูงสุด

#### 4.5.3.2 ค่าที่ตัดสินใจได้ต่างกับค่าความถูกต้อง

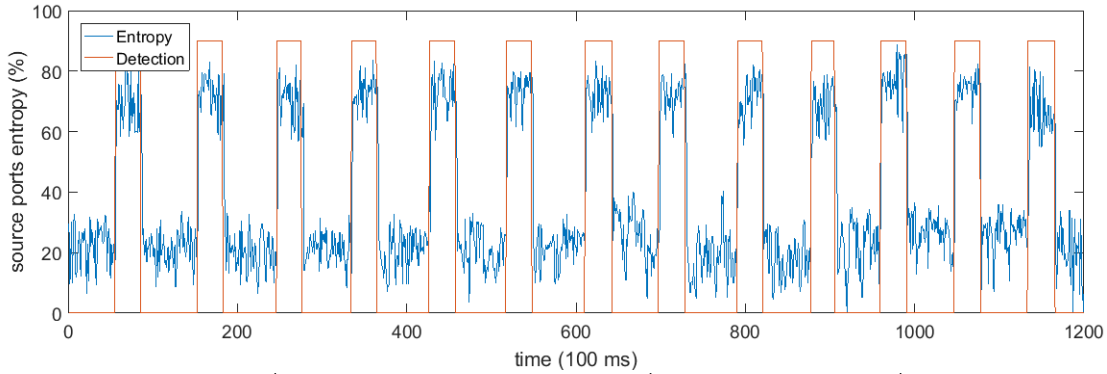
ตารางที่ 4-14 การเลือกค่า Group ที่เหมาะสมของความผิดปกติรูปแบบที่ 2

| Group | เหตุการณ์ผิดปกติ | | เหตุการณ์ปกติ | ACC |
|---|---|---|---|---|
| | FNR | FPR | FPR | |
| 15 | 1 | 0 | 0 | 0.5417 |
| 30 | 1 | 0 | 0 | 0.5417 |
| 45 | 0.2455 | 0 | 0 | 0.8875 |
| 55 | 0.1291 | 0 | 0 | 0.9408 |
| 56 | 0.1218 | 0 | 0 | 0.9442 |
| 57 | 0.1164 | 0 | 0 | 0.9467 |
| 58 | 0.1000 | 0 | 0 | 0.9542 |
| 59 | 0.0945 | 0 | 0 | 0.9567 |
| **60** | **0.0891** | **0** | **0** | **0.9592** |
| 61 | 0.0818 | 0 | 0.0217 | 0.9625 |
| 62 | 0.0800 | 0 | 0.0225 | 0.9633 |
| 63 | 0.0745 | 0.0015 | 0.0233 | 0.9650 |
| 64 | 0.0745 | 0.0015 | 0.0233 | 0.9650 |
| 65 | 0.0655 | 0.0015 | 0.0233 | 0.9692 |
| **70** | **0.0455** | **0.0031** | **0.0225** | **0.9775** |
| 90 | 0.1182 | 0 | 0.0500 | 0.9458 |
| 120 | 0.1509 | 0 | 0.0917 | 0.9308 |

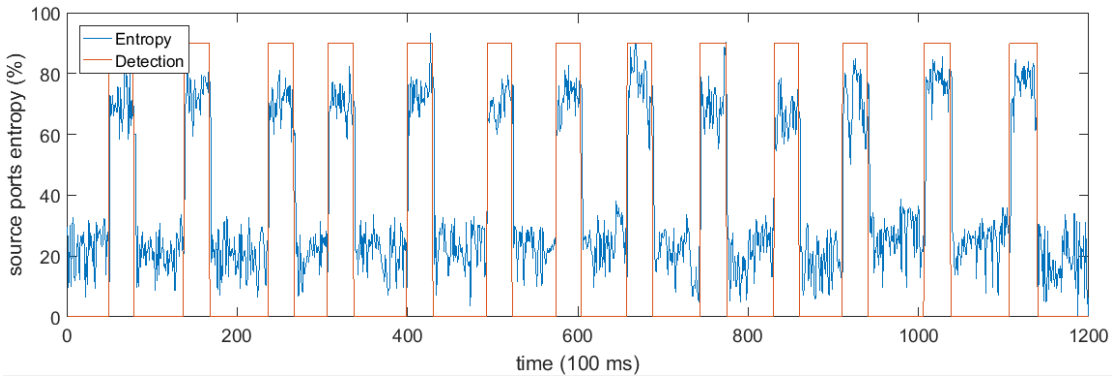
จากตารางที่ 4-14 สำหรับรูปแบบของความผิดปกติรูปแบบที่ 2 นั่นคือมีการโจมตีเกิดขึ้นทุกช่วงระยะห่างของตำแหน่ง 10000 ms และมีระยะเวลาการโจมตีครั้งละ 5000 ms เมื่อกำหนดค่าตัวแปร Threshold $T_{attack} = 24$ และ ตัวแปรขนาด Subgroup $N = 5$ จะเห็นว่าค่า Group ที่เลือกคือ 60 ซึ่งมีค่า FNR = 0.0891, FPR และ FPR เมื่อเหตุการณ์ปกติ = 0 และมีค่า ACC = 0.9592 ส่วนค่า Group ที่ตัดสินใจได้จากการคำนวณค่า ACC สูงสุดอยู่ที่ 70 เนื่องจากค่า ACC มีค่ามากที่สุด = 0.9775 แต่จะมีค่า FNR = 0.0455, FPR = 0.0031 และค่า FPR เมื่อเหตุการณ์ปกติ = 0.0225 ดังนั้นจึงไม่เลือก Group = 70

### 4.5.4 ผลการทดลองโดยทดลองกับข้อมูลแบบสุ่ม

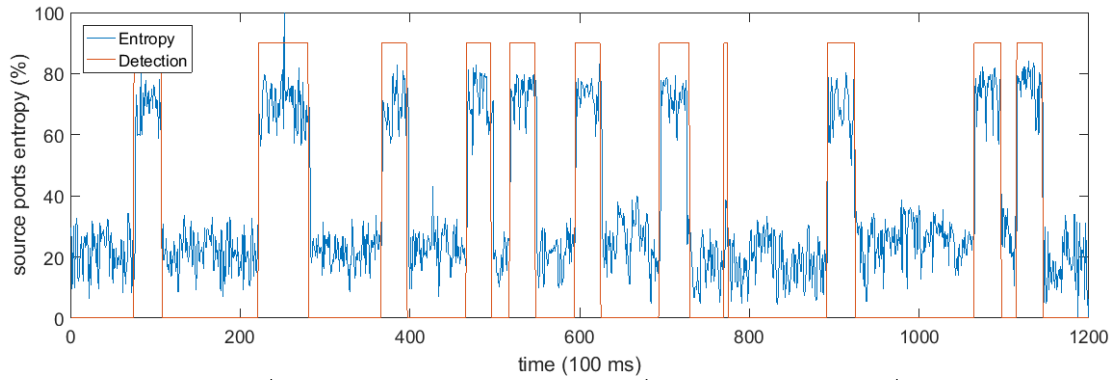
จากเงื่อนไขที่ใช้เลือกพารามิเตอร์ของแผนภูมิควบคุม ทำให้เราสามารถกำหนดค่าที่เหมาะสมสำหรับตรวจหาการโจมตี ซึ่งในหัวข้อนี้ได้ทดลองกับการโจมตีที่เกิดขึ้นแบบสุ่ม โดยที่การเกิดขึ้นของเหตุการณ์มีการแจกแจงยูนิฟอร์ม ที่มีค่าส่วนเบี่ยงเบนมาตรฐานตามที่กำหนดไว้ในหัวข้อที่ 4.2 ผลการทดลองของกรณีนี้ได้แสดงกราฟของการตรวจหาความผิดปกติ โดยใช้ขั้นตอนวิธีที่นำเสนอได้ดังภาพประกอบที่ 4-7 ถึง 4-9




ภาพประกอบที่ 4-7 การตรวจหาความผิดปกติ เมื่อมีการโจมตีแบบสุ่ม ที่ $\sigma = 5$




ภาพประกอบที่ 4-8 การตรวจหาความผิดปกติ เมื่อมีการโจมตีแบบสุ่ม ที่ $\sigma = 15$




ภาพประกอบที่ 4-9 การตรวจหาความผิดปกติ เมื่อมีการโจมตีแบบสุ่ม ที่ $\sigma = 30$

จากภาพประกอบที่ 4-7 – 4-9 เมื่อกำหนดค่าตัวแปร Threshold $T_{attack} = 24$ ตัวแปรขนาด Subgroup $N = 5$ และ ตัวแปร Group $G = 120$ พบว่าขั้นตอนวิธีในการตรวจหาความผิดปกติที่นำเสนอ สามารถตรวจหาความผิดปกติในรูปแบบสุ่ม ที่ $\sigma = 5, 15$ และ $30$ ได้ผลการทดสอบดังตารางที่ 4-15

ตารางที่ 4-15 ผลการทดลองกับข้อมูลแบบสุ่ม

| **รูปแบบ** | **FNR** | **FPR** | **FPR เมื่อเหตุการณ์ปกติ** | **ACC** |
|---|---|---|---|---|
| $\sigma = 5$ | 0.0569 | 0.0176 | 0.0917 | 0.9692 |
| $\sigma = 15$ | 0.0596 | 0.0151 | 0.0917 | 0.9700 |
| $\sigma = 30$ | 0.0175 | 0.0349 | 0.0917 | 0.9767 |

วิธีการที่นำเสนอสามารถตรวจหาการโจมตี Pulse wave DDoS แบบสุ่มได้เป็นส่วนใหญ่ ดังที่แสดงในภาพประกอบที่ 4-9 จะเห็นว่า ในแต่ละพัลส์มีตำแหน่งของการเกิดการโจมตี และระยะเวลาในการโจมตีแตกต่างกัน ซึ่งรูปแบบการโจมตีในลักษณะนี้ยากแก่การตรวจหา กว่าการโจมตีที่มีรูปแบบการเกิดที่แน่นอน ดังภาพประกอบที่ 4-2

## 4.6 สรุป

ในบทนี้ได้นำเสนอผลการทดลองของวิธีการตรวจหาความผิดปกติที่เกิดขึ้นในเครือข่ายคอมพิวเตอร์ จากการทดลองได้ทำการวัดและประเมินประสิทธิภาพ ของการเลือกค่าของตัวแปรที่มีความสำคัญในขั้นตอนวิธีที่เหมาะสม 3 ตัวแปร นั่นคือ ตัวแปรThreshold ขนาดSubgroup และ Group โดยใช้เงื่อนไขของการทดสอบอัตราความผิดพลาดในการตรวจหาเชิงบวก FPR และ การทดสอบอัตราความผิดพลาดในการตรวจหาเชิงลบ FNR โดยเปรียบเทียบกับการใช้ค่าความถูกต้อง ACC เมื่อทำการทดลองกับข้อมูลความผิดปกติรูปแบบต่าง ๆ ที่กำหนดเอง และความผิดปกติแบบสุ่ม จากผลการทดลองที่ได้นำเสนอไปแล้วนั้นสามารถสรุปได้ดังตารางที่ 4-16

ตารางที่ 4-16 สรุปผลการทดลอง

| รูปแบบ | Threshold | Subgroup | Group | FNR | FPR | FPR เมื่อเหตุการณ์ปกติ | ACC |
|---|---|---|---|---|---|---|---|
| 1 | 35 | 13 | 120 | 0.0986 | 0 | 0 | 0.9425 |
| 2 | 24 | 5 | 60 | 0.0891 | 0 | 0 | 0.9592 |
| 3 | 28 | 3 | 57 | 0.0952 | 0 | 0 | 0.9583 |
| 4 | 23 | 3 | 60 | 0.0127 | 0.0113 | 0 | 0.9883 |
| $\sigma = 5$ | 24 | 5 | 120 | 0.0569 | 0.0176 | 0.0917 | 0.9692 |
| $\sigma = 15$ | 24 | 5 | 120 | 0.0596 | 0.0151 | 0.0917 | 0.9700 |
| $\sigma = 30$ | 24 | 5 | 120 | 0.0175 | 0.0349 | 0.0917 | 0.9767 |

จากตารางที่ 4-16 เมื่อระบบถูกจำลองให้มีการโจมตีด้วย Pulse wave DDOS ที่ทำให้เกิดความผิดปกติสี่รูปแบบสามารถสรุปได้ดังนี้

รูปแบบที่ 1 ค่าของ Threshold ที่เหมาะสมอยู่ที่ 35 ส่วนค่าขนาด Subgroup ที่เหมาะสมอยู่ที่ 13 และค่าของ Group ที่เหมาะสมอยู่ที่ 120 ซึ่งทั้ง 3 ตัวแปรมีค่า FNR เท่ากับ 0.0986 มีค่า FPR และ FPR เมื่อเหตุการณ์ปกติ มีค่าเป็น 0 และมีค่า ACC เท่ากับ 0.9425

รูปแบบที่ 2 มีค่า Threshold ที่เหมาะสมอยู่ที่ 24 ส่วนค่าขนาด Subgroup ที่เหมาะสมเท่ากับ 5 และค่าของ Group ที่เหมาะสมอยู่ที่ 60 ซึ่งทั้ง 3 ตัวแปรมีค่า FNR เท่ากับ 0.0891 มีค่า FPR และ FPR เมื่อเหตุการณ์ปกติ มีค่าเป็น 0 และมีค่า ACC เท่ากับ 0.9592

รูปแบบที่ 3 มีค่า Threshold ที่เหมาะสมอยู่ที่ 28 ส่วนค่าขนาด Subgroup ที่เหมาะสมอยู่ที่ 3 และค่าของ Group ที่เหมาะสมอยู่ที่ 57 ซึ่งทั้ง 3 ตัวแปรมีค่า FNR เท่ากับ 0.0952 มีค่า FPR และ FPR เมื่อเหตุการณ์ปกติ มีค่าเป็น 0 และมีค่า ACC เท่ากับ 0.9583

รูปแบบที่ 4 มีค่า Threshold ที่เหมาะสมอยู่ที่ 23 ส่วนค่าขนาด Subgroup ที่เหมาะสมอยู่ที่ 3 และค่าของ Group ที่เหมาะสมอยู่ที่ 60 ซึ่งทั้ง 3 ตัวแปรมีค่า FNR เท่ากับ 0.0127 มีค่า FPR เท่ากับ 0.0113 และ FPR เมื่อเหตุการณ์ปกติ มีค่าเป็น 0 และมีค่า ACC เท่ากับ 0.9883

จากผลการทดลอง ขั้นตอนวิธีในการตรวจหาความผิดปกติทั้งแบบที่มีรูปแบบการโจมตีที่แน่นอน และสามารถตรวจหาความผิดปกติในรูปแบบสุ่มด้วยค่าส่วนเบี่ยงเบนมาตรฐานที่ $\sigma = \{5, 15, 30\}$ เมื่อการโจมตีแบบสุ่มทำให้เวลาที่เกิดเหตุการณ์อยู่ที่ตำแหน่งของเวลาการเกิดการโจมตีที่แตกต่างกัน และระยะเวลาในการโจมตีหรือความกว้างของพัลส์ที่แตกต่างกัน เมื่อกำหนด

ค่าตัวแปร Threshold $T_{attack} = 24$ ตัวแปรขนาด Subgroup $N = 5$ และ ตัวแปร Group $G = 120$ พบว่าแผนภูมิสามารถการตรวจหาความผิดปกติได้ดังนี้

รูปแบบสุ่มที่ $\sigma = 5$ มีค่า FNR เท่ากับ 0.0569 มีค่า FPR เท่ากับ 0.0176 มีค่า FPR เมื่อเหตุการณ์ปกติ เท่ากับ 0.0917 และมีค่า ACC เป็น 0.9692

รูปแบบสุ่มที่ $\sigma = 15$ มีค่า FNR เท่ากับ 0.0596 มีค่า FPR เท่ากับ 0.0151 มีค่า FPR เมื่อเหตุการณ์ปกติ เท่ากับ 0.0917 และมีค่า ACC เป็น 0.9700

รูปแบบสุ่มที่ $\sigma = 30$ มีค่า FNR เท่ากับ 0.0175 มีค่า FPR เท่ากับ 0.0349 มีค่า FPR เมื่อเหตุการณ์ปกติ เท่ากับ 0.0917 และมีค่า ACC เป็น 0.9767

# บทที่ 5

# สรุปปัญหาและข้อเสนอแนะ

## 5.1 บทนำ

สำหรับบทนี้ เป็นการสรุปผลงานวิจัย และกล่าวถึงปัญหาและอุปสรรคในงานวิจัย รวมถึงข้อเสนอแนะในการทำงานวิจัยดังนี้

## 5.2 สรุปผลการวิจัย

งานวิจัยนี้ได้นำเสนอขั้นตอนวิธีในการตรวจหาความผิดปกติ โดยมีการโจมตีแบบ Pulse wave DDoS ซึ่งเป็นการโจมตีแบบปฏิเสธการให้บริการประเภทหนึ่ง แต่มีรูปแบบของการเกิดการโจมตีแตกต่างไปจาก DDoS โดยทั่วไป ที่มีคุณลักษณะสำคัญคือ Immediacy จะเกิดการโจมตีอย่างรวดเร็ว กราฟของการโจมตีจะไม่มีช่วง Ramp-up Frequency รูปแบบของการโจมตีจะเป็นแบบซ้ำ ๆ ซึ่งจะประกอบไปด้วยพัลส์ ตั้งแต่ 1 พัลส์ขึ้นไป Persistence การโจมตีจะเกิดขึ้นเป็นช่วง แต่จะเกิดการโจมตีอยู่ตลอด อาจใช้เวลาเป็นชั่วโมง หลายชั่วโมง หรือ ยาวนานหลายวัน และ Size ในแต่ละพัลส์ จะมีขนาดของการโจมตีเพียงพอจนทำให้เกิดความคับคั่งของเครือข่ายเป้าหมายได้

ในการตรวจหาความผิดปกติที่มีการโจมตีแบบ Pulse wave DDoS ได้นำทฤษฎีการ Encode ข้อมูลโดยใช้เอนโทรปีของ Source Port เมื่อจำลองการโจมตีแบบ Pulse wave DDoS พบว่าเมื่อนำมาคำนวณค่าเอนโทรปี จะเห็นว่าค่าเอนโทรปีของช่วงเวลาที่ถูกโจมตีมีค่าสูงขึ้นมากกว่าค่าที่มีการใช้งานเครือข่ายแบบปกติ การตรวจหาความผิดปกติแบบ DDoS สามารถใช้ข้อมูลเอนโทรปีของ Source Port มาสร้างแผนภูมิควบคุม อย่างไรก็ตามประสิทธิภาพของแผนภูมิควบคุมขึ้นอยู่กับการออกแบบขอบเขตคุณภาพ ที่เหมาะสมกับระบบนั้น ๆ ในงานวิจัยชิ้นนี้ ได้นำเสนอวิธีการตรวจหาความผิดปกติแบบ Pulse wave DDoS โดยใช้ข้อมูลเอนโทรปีของ Source Port มาสร้างแผนภูมิควบคุมค่าเฉลี่ยเคลื่อนที่ของค่าถ่วงน้ำหนักเลขชี้กำลัง

จากขั้นตอนวิธีที่ได้นำเสนอ มีตัวแปรสำคัญในการออกแบบวิธีการที่ใช้ตรวจหาความผิดปกติ ประกอบด้วยตัวแปร Threshold $(T_{attack})$ ที่ใช้บ่งชี้ว่ามีการโจมตีหรือไม่ ตัวแปรขนาด Subgroup $(N)$ และตัวแปร Group $(G)$ ใช้บ่งบอกถึงสมรรถนะของตัวตรวจหาความผิดปกติ ในการหาค่าที่เหมาะสมของแต่ละตัวแปรได้พิจารณาจาก อัตราความผิดพลาดในการตรวจหาเชิงบวก อัตราความผิดพลาดในการตรวจหาเชิงลบ และ ค่าความถูกต้อง

จากผลการทดลอง วิธีการที่นำเสนอสามารถตรวจหาความผิดปกติได้ทั้งแบบที่มีรูปแบบการโจมตีที่แน่นอน และความผิดปกติในรูปแบบสุ่ม ด้วยค่าส่วนเบี่ยงเบนมาตรฐานที่ $\sigma = \{5, 15, 30\}$ ทำให้ตำแหน่งและระยะเวลาของการเกิดการโจมตีแตกต่างกัน

## 5.3 ปัญหาและอุปสรรคในการวิจัย

เนื่องจากในการวิจัยนี้ มีการใช้ทฤษฎีและความรู้ทางคณิตศาสตร์และสถิติเป็นส่วนใหญ่ ผู้วิจัยจึงต้องศึกษาความรู้และทฤษฎีต่าง ๆ เพื่อให้สามารถวิเคราะห์ และตีความหมายได้

## 5.4 ข้อเสนอแนะ

1. ตัวแปรต่าง ๆ ที่ใช้ในการทดลอง ควรออกแบบให้สามารถปรับค่าได้อัตโนมัติตามการแจกแจงของข้อมูล

2. เนื่องจากขนาดของเครือข่ายที่ใช้ในงานวิจัยมีขนาดเล็ก ในอนาคตควรมีการศึกษาและพัฒนาเพิ่มเติม สำหรับการใช้งานในเครือข่ายขนาดกลาง และขนาดใหญ่

# บรรณานุกรม

ปัทมา แสงหมี. 2555. สถาปัตยกรรมมาตรฐานโพรไฟล์สำหรับตรวจจับความผิดปกติ, วิทยานิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยสงขลานครินทร์.

Aamir M., and Zaidi M. A. 2013. A Survey on DDoS Attack and Defense Strategies: From Traditional Schemes to Current Techniques, Interdisciplinary Information Sciences, Vol.19, No.2, pp.173-200.

Bace R. G. 2000. Intrusion Detection. MacMillan Technical Publishing. USA

Basicevic I., Ocovaj S., and Popovic M. 2015. Evaluation of entropy-based detection of outbound denialof-service attacks in edge networks, Security and Communication Networks, pp.837844.

BITAG. 2013. Port Blocking. A Uniform Agreement Report, Broadband Internet Technical Advisory Group, Inc.

Bonaventure O. 2018. Computer Networking : Principles, Protocols and Practice, Saylor foundation. Available from http://inl.info.ucl.ac.be/cnp3.

CERT .1996. Advisory CA-1996-01, UDP Port Denial-ofService Attack. https://www-uxsup.csx.cam.ac.uk/pub/webmirrors/www.cert.org/advisories/CA-1996-01.html. (accessed 21/10/2018).

CERT. 1996. Advisory CA-1996-21, TCP SYN Flooding and IP Spoofing Attacks. https://www-xsup.csx.cam.ac.uk/pub/webmirrors/www.cert.org/advisories/CA-1996-21.html. (accessed 21/10/2018).

CERT. 1999. Advisory CA-1996-26, Denial-of-Service Attack via ping. https://www-uxsup.csx.cam.ac.uk/pub/webmirrors/www.cert.org/advisories/CA-1996-26.html. (accessed 21/10/2018).

Denning D. E. 1986. An intrusion-detection model, IEEE Transaction on Software Engineering, Vol.SE-13, No.2, February 1987, pp.222-232.

DHS US-CERT. 2011. Understanding DistributedDenial-of-Service Attacks. https://info.publicintelligence.net/DHSUnderstandingDDoS.pdf)

ENISA. 2017. ENISA Threat Landscape Report 2017. Technical Report, The European Union Agency forNetwork and Information Security.

GFI Software. 2010. Security threats: a guide for small and medium enterprises. White Paper, GFI Software.

Handley M., Rescorla E., and IAB. 2006. Internet Denial-of-Service Considerations. RFC 4732.

Imperva. 2017. Understanding Pulse Wave Attacks. White Paper, Imperva Incapsula.

Kaspersky. 2017. Threat Landscape for Industrial Automation Systems. Technical Report, Kaspersky Lab ICS CERT.

Kruegel C., Valeur F., and Vigna G. 2005. Intrusion Detection and Correlation Challenges and Solution, Springer. New York.

Lee K., Kim J., Kwon K.H., Han Y., and Kim S. 2008. DDoS Attack Detection Method Using Cluster Analysis. Expert Systems with Applications, Vol.34, No.3, pp.1659-1665.

Mohan V., Pawar., and Anuradha J. 2015. Network Security and Types of Attacks in Network. International Conference on Intelligent Computing, Communication & Convergence. pp.503-506.

Montgomery D. C. 2009. Introduction to Statistical Quality Control, 6th Edition. John Wiley & Sons, Inc. USA.

Patcha A., and Park J. M. 2007. An overview of anomaly detection techniques: Existing solutions and latest technological trends. The International Journal of Computer and Telecommunications Networking, pp.3448-3470.

Postel J. and ISI. 1980. User Datagram Protocol. RFC 768.

Postel J. and ISI. 1980. Transmission Control Protocol. RFC 793.

Pradhan M., Pradhan S. K., and Sahu S. K. 2012. Anomaly Detection using Artificial Neural Network. International Journal of Engineering Sciences & Emerging Technologies, Vol.2, pp.29-36.

Singh J., Sachdeva M. and Kumar M. 2013. Detection of DDoS Attacks Using Source IP Based Entropy. International Journal of Computer Science Engineering and Information Technology Research, Vol.3, Issue.1, Mar 2013, pp.201-210.

Teng H. S., Chen K., and Stephen C. 1990. Security Audit Trail Analysis Using Inductively Generated Predictive Rules. IEEE In Proceedings of the 6th Conference on Artificial Intelligence Applications, pp.24-29.

Thing V. L., Sloman M., and Dulay N. 2007. A Survey of Bots Used for Distributed Denial of Service Attacks. IFIP International Information Security Conference, Vol.232, pp.229-240.

Tritilanunt S., Sivakorn S., Juengjincharoen C. and Siripornpisan A. 2010. Entropy-based Input-Output Traffic Mode Detection Scheme for DoS/DDoS Attacks. International Symposium on Communications and Information Technologies, pp.804-809.

Yu S. and Zhou W. 2008. Entropy-Based Collaborative Detection of DDOS Attacks on Community Networks. 6th IEEE International Conference on Pervasive Computing and Communications, pp.566-571.

# ภาคผนวก

# ภาคผนวก ก.

## ผลงานตีพิมพ์

| | |
|---|---|
| เรื่อง | Anomaly detection using Source Port Data with Shannon Entropy and EWMA Control Chart |
| งานประชุมวิชาการ | 18th International Conference on Control, Automation and Systems (ICCAS 2018) |
| สถานที่ | YongPyong Resort, PyeongChang, GangWon, Korea |
| วันที่ | 17–20 October 2018 |

# ประวัติผู้เขียน

**ชื่อ สกุล** นางสาวศิริพงา รัญเสวะ

**รหัสประจำตัวนักศึกษา** 5710220099

**วุฒิการศึกษา**

| วุฒิ | ชื่อสถาบัน | ปีที่สำเร็จการศึกษา |
|---|---|---|
| วิทยาศาสตรบัณฑิต (วิทยาการคอมพิวเตอร์) | มหาวิทยาลัยสงขลานครินทร์ | 2556 |

**การตีพิมพ์เผยแพร่ผลงาน**

S. Ransewa, N. Elz, N. Thanon and S. Intajag. 2018. Anomaly detection using Source Port Data with Shannon Entropy and EWMA Control Chart, 18th International Conference on Control, Automation and Systems (ICCAS 2018), YongPyong Resort, PyeongChang, GangWon, Korea, pp.596-601