การวิเคราะห์ประสิทธิภาพการโจมตีระบบโทรศัพท์ผ่านอินเทอร์เน็ตด้วยระบบตรวจจับการบุกรุก

An Analysis of Effectiveness of Internet Telephone System Attacks using Intrusion Detection Systems

ประสิทธิ์ สุภาสืบ* และ อรรถพล ป้อมสถิตย์

Prasit Supasueb* and Auttapon Pomsathit

วิทยาลัยนวัตกรรมดิจิทัลและเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต ปทุมธานี ประเทศไทย

College of Digital Innovation and Information Technology (DIIT), Rangsit University, Pathum Thani, Thailand

**Corresponding author, E-mail: prasit.s59@rsu.ac.th*

บทคัดย่อ

งานวิจัยนี้เป็นการนำเสนอการพัฒนาระบบตรวจจับการบุกรุกระบบโทรศัพท์ผ่านอินเทอร์เน็ตด้วยการโจมตีรูปแบบปฏิเสธการให้บริการ เนื่องจากองค์กรหรือหน่วยงานต่าง ๆ จำเป็นต้องมีเทคโนโลยีการรักษาความปลอดภัยสำหรับป้องกันภัยคุกคามเพื่อทำให้มีความสะดวกในการสื่อสาร เมื่อตรวจพบแพ็คเกจที่มีพฤติกรรมเสี่ยงต่อการโจมตีระบบโทรศัพท์ผ่านอินเทอร์เน็ต จะมีการแจ้งเตือนผ่านทางเว็บไซต์ โดยทำการทดลองการใช้ระบบตรวจจับการบุกรุกระบบโทรศัพท์ผ่านอินเทอร์เน็ต จากการทดลองพบว่าระบบสามารถตรวจจับการโจมตีระบบโทรศัพท์ผ่านอินเทอร์เน็ตจากการโจมตีแบบ Invite Flood, RTP Flood, UDP Flood และPing of Death ส่งผลกับทรัพยากรเครื่องได้แก่ CPU และแบนด์วิดท์ของเครือข่าย และการโจมตีแบบ RTP Flood ไม่ส่งผลกับทรัพยากรเครื่องเลย แต่ส่งผลโดยตรงกับโพรโทคอล SIP ที่ใช้ในการติดต่อสื่อสาร จากการทดลองทั้งหมด จะเห็นว่าการโจมตีจากภายในทั้งระบบเครือข่ายและระบบเครือข่ายไร้สาย ระบบสามารถตรวจจับได้จำนวนเหตุการณ์ที่เกิดขึ้นต่างกันเนื่องจากการโจมตี เป็นการส่งแพ็คเกจจำนวนมาก ๆ อย่างต่อเนื่องจึงเกิดการชนกันของข้อมูล (CSMA/CD) จากผลการทดลองจะเห็นว่าระบบเครือข่ายไร้สาย มีจำนวนเหตุการณ์ที่ต่างกันกับระบบเครือข่าย เนื่องจากระบบเครือข่ายไร้สายจะมีกระบวนการในการหลีกเลี่ยงเพื่อไม่ให้เกิดชนกันของข้อมูล (CSMA/CA) จึงทำให้จำนวนแพ็คเกจบางเหตุการณ์ไม่สามารถส่งผ่านระบบเครือข่ายไร้สายได้

คำสำคัญ: *ระบบตรวจจับการบุกรุก, Invite Flood, RTP Flood, UDP Flood, Ping of Death*

Abstract

This research presents the development of intrusion detection systems through the internet by Denial of Service (DoS) attack because organizations and agencies need to have security technology for threat protection in order to make communication more convenient. In this experiment test, Elastix was used to make phone calls over the internet, and Snort was used to detect the data of traffic in the network. When it detected packets that had a high risk of attack through Internet telephony, it would create an alert via the website. The test of intrusion detection systems was conducted through the internet. The results showed that Invite Flood, RTP Flood, UDP Flood and Ping of Death affected the machine resources including CPU and the bandwidth of network. The RTP Flood attack did not affect machine resources but directly affected SIP communications. All experiments showed that the attacks from within the wired and wireless network were detected with the different numbers of discovery due to the data collisions. The results showed that the wireless network had the different numbers of occurrences because wireless networks were based on the actions of avoiding data collisions, causing some packets not to be sent through the wireless network.

Keywords: *Intrusion Detection System, Invite Flood, RTP Flood, UDP Flood, Ping of Death*

1. บทนำ

เนื่องด้วยในปัจจุบันการขยายตัวของระบบเครือข่ายสัญญาณข้อมูลมีอัตราการเติบโตที่รวดเร็วกว่าการขยายตัวของเครือข่ายสัญญาณเสียงค่อนข้างมาก จึงทำให้มีการนำเทคโนโลยีที่สามารถนำสัญญาณเสียงเหล่านั้นมารวมอยู่บนระบบเครือข่ายของสัญญาณข้อมูล และมีการรับ-ส่งสัญญาณทั้งคู่ได้ในเวลาเดียวกันเพื่อเป็นการสะดวกและประหยัดค่าใช้จ่าย สำหรับการใช้งานเทคโนโลยีระบบโทรศัพท์ผ่านอินเทอร์เน็ตนั้น ทุกองค์กรสามารถนำเทคโนโลยีนี้มาประยุกต์ใช้งานได้ (Hanifan and Bandung, 2013) และภัยคุกคามทางด้านไซเบอร์ในปัจจุบัน ก็สามารถส่งผลกระทบต่อเทคโนโลยีระบบโทรศัพท์ผ่านอินเทอร์เน็ตได้ด้วยเช่นกัน

ดังนั้นประเทศไทยจึงมีความจำเป็นอย่างยิ่งที่จะต้องมีการบัญญัติกฎหมายที่เกี่ยวข้อง ในการเสริมสร้างความมั่นคงปลอดภัยด้านไซเบอร์และจัดตั้งคณะกรรมความมั่นคงปลอดภัยไซเบอร์แห่งชาติเพื่อให้ทันต่อการเติบโตของภัยคุกคามด้านไซเบอร์ 7 รูปแบบ 1.Malware 2.Phishing 3.SQL Injection Attack SQL 4.Cross-Site Scripting (XSS) 5.Denial of Service (DoS) 6.Session Hijacking and Man-in-the-Middle Attacks และ 7.Credential Reuse

จากรูปแบบการโจมตีที่มีความหลากหลายองค์กรและหน่วยงานต่าง ๆ จำเป็นต้องมีเทคโนโลยีการรักษาความปลอดภัยสำหรับป้องกันภัยคุกคามที่จะเกิดขึ้นในองค์กร (อรรถพล ป้อมสถิตย์, 2561) และในการใช้งานระบบโทรศัพท์ผ่านอินเทอร์เน็ต ขณะที่อินเทอร์เน็ตก็มีการพัฒนาไปอย่างรวดเร็วพร้อมทั้งมีการใช้งานกันอย่างแพร่หลาย เนื่องจากทำให้มีความสะดวกในการสื่อสารและสามารถที่จะแลกเปลี่ยนข้อมูลกันได้อย่างรวดเร็ว สิ่งที่ต้องคำนึงถึง

เป็นอย่างมากนั้นคือ ความปลอดภัยการพัฒนารูปแบบการบุกรุกได้เกิดขึ้นทุกวันโดยที่ผู้บุกรุกนั้นสามารถที่จะบุกรุกจากภายนอกหรือจะบุกรุกจากภายในของการใช้งานระบบโทรศัพท์ผ่านอินเทอร์เน็ต

ในงานวิจัยนี้ได้ใช้ระบบตรวจจับการบุกรุก (Intrusion Detection System: IDS) เป็นเครื่องมือที่ใช้ตรวจจับความพยายามบุกรุกระบบเครือข่าย โดยระบบจะแจ้งเตือนไปยังผู้ดูแลระบบเมื่อมีการบุกรุก หรือมีการพยายามที่จะบุกรุกเครือข่าย (อรรถพล ป้อมสถิตย์, 2559) ซึ่งระบบตรวจจับการบุกรุกระบบโทรศัพท์ผ่านอินเทอร์เน็ต จะมีการตอบสนองต่อการโจมตีในแบบการปฏิเสธการให้บริการ (Denial of Service: DoS) ของผู้บุกรุกตามข้อมูลของระบบตรวจจับการบุกรุกที่กำหนดไว้ และทำการแจ้งเตือนในรูปแบบสถิติในการโจมตี ผู้วิจัยจึงมีแนวคิดในการทำวิจัยการวิเคราะห์ประสิทธิภาพการโจมตีระบบโทรศัพท์ผ่านอินเทอร์เน็ตด้วยระบบตรวจจับการบุกรุก เพื่อเพิ่มประสิทธิภาพในการตรวจจับการบุกรุกระบบโทรศัพท์ผ่านอินเทอร์เน็ต และป้องกันการโจมตีจากผู้บุกรุกในการระงับ ชะลอ ขัดขวาง หรือรบกวนจนเครื่องแม่ข่ายไม่สามารถทำงานตามปกติได้ (อรรถพล ป้อมสถิตย์, และบุญเรือง เกิดอรุณเดช, 2562) โดยผลลัพธ์ที่ได้จากการวิจัยจะสามารถนำมาใช้ในการปรับปรุงและพัฒนาการดำเนินงานของผู้ดูแลระบบเครือข่ายของมหาวิทยาลัย หน่วยงาน ภาครัฐและภาคเอกชน เพื่อนำไปสู่ความมั่นคงของระบบคอมพิวเตอร์ตามวัตถุประสงค์ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี 2560

2. วัตถุประสงค์

1. เพื่อศึกษาและออกแบบระบบโทรศัพท์ผ่านอินเทอร์เน็ตด้วยโพรโตคอล SIP (Session Initiation Protocol)
2. เพื่อพัฒนาระบบตรวจจับการบุกรุกเพื่อป้องกันการโจมตีระบบโทรศัพท์ผ่านอินเทอร์เน็ตรูปแบบการปฏิเสธการให้บริการ (Denial of Service: DoS)
3. เพื่อวิเคราะห์ประสิทธิภาพระบบตรวจจับการบุกรุกกับระบบโทรศัพท์ผ่านอินเทอร์เน็ต

3. อุปกรณ์และวิธีการ / วิธีดำเนินการวิจัย

3.1 ซอฟต์แวร์ (Software)

3.1.1 ซอฟต์แวร์สำหรับระบบตรวจจับผู้บุกรุกเครือข่าย (IDS)

- Ubuntu 14.04 LTS Desktop
- Snort 2.9.7.3
- MySQL Server 5.6.25
- MySQL workbench 6.3
- Snort rules snapshot 2975
- php 5.6.11
- barnyard 2 2.1.13
- apache 2

3.1.2 ซอฟต์แวร์สำหรับ Sip Server

- Elastix 2.4

3.1.3 ซอฟต์แวร์สำหรับผู้บุกรุกเครือข่าย (Attacker)

- Kali Linux 64 bit

3.1.4 ซอฟต์แวร์สำหรับโทรศัพท์ผ่านเครือข่าย

- X-Lite 4.9

3.2 ฮาร์ดแวร์ (Hardware)

3.2.1 เครื่องคอมที่ทำหน้าที่เป็น IDS รายละเอียดคอมพิวเตอร์

- CPU Intel(R) Core(TM) i3-2120 CPU @ 3.30 GHz 3.30 GHz
- RAM 4 GB
- HDD SSD 60 GB
- Mainboard GIGABYTE GA-H61M-S2P
- VGA Radeon HD 5450

3.2.2 เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็น Sip Server A

- CPU Intel(R) Core(TM) i3-2120 CPU @ 3.30 GHz 3.30 GHz
- RAM 4 GB
- HDD SSD 60 GB
- Mainboard GIGABYTE GA-H61M-S2P
- VGA Radeon HD 5450

3.2.3 เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็น Sip Server B

- CPU Intel Pentium D 3.00 GHz
- RAM 1 GB
- HDD 80 GB
- Mainboard Acer E946GZ
- VGA Onboard
- ติดตั้ง Elastix 2.4

3.2.4 เครื่องคอมพิวเตอร์โน้ตบุ๊กที่ทำหน้าที่เป็น เครื่องโจมตี เครื่องติดตั้ง Softphone A และ B

- Dell Vostro 3400
- CPU Intel(R) Core(TM) i5 CPU M 460 @ 2.53GHz
- RAM 4 GB
- HDD 700 GB
- VGA Intel(R) HD Graphics

3.2.5 Router Cisco 2900 series จำนวน 2 ตัว

- ทำการ Config Router ให้สามารถหาเส้นทางติดต่อสื่อสารข้อมูลกันได้โดยใช้ความสามารถในโพรโทคอล RIP (Routing Information Protocol)

3.2.6 Switch Catalyst 2960 series จำนวน 3 ตัว

- ทำการ Config Switch ให้สามารถ mirror port

3.2.7 Wireless Router

- ทำการ Config Wireless Router ให้สามารถแจกจ่ายหมายเลขไอพีแบบอัตโนมัติโดยใช้ DHCP (Dynamic Host Configuration Protocol)

ในการทดสอบจะเปรียบเทียบการโจมตีระบบเครือข่าย และระบบเครือข่ายไร้สาย จากภายในและภายนอกด้วยการโจมตีรูปแบบปฏิเสธการให้บริการกับระบบโทรศัพท์ผ่านอินเทอร์เน็ตด้วยโพรโตคอล SIP (Session Initiation

Protocol) เพราะยากในการตรวจจับ และสร้างปัญหาในการให้บริการกับเครื่องแม่ข่ายที่ให้บริการต่าง ๆ ได้อย่างต่อเนื่องจนอาจทำให้เครื่องแม่ข่ายหยุดทำงานได้ (Zhenxin, Maochao, & Shouhuai, 2015) โดยมีรายละเอียดดังนี้

- โพรโทคอลที่ใช้ในการทดสอบ
    - TCP Protocol
    - UDP Protocol
    - ICMP Protocol
- การโจมตีโดยใช้โปรแกรม hping
    - การบุกรุกเครือข่าย Internal และ การบุกรุกเครือข่าย External
    - การโจมตีแบบเครือข่าย
    - การโจมตีแบบเครือข่ายไร้สาย

เพื่อที่จะวิเคราะห์ประสิทธิภาพการโจมตีระบบโทรศัพท์ผ่านอินเทอร์เน็ตด้วยระบบตรวจจับการบุกรุกจึงได้ทำการวิเคราะห์ประสิทธิภาพการโจมตีระบบโทรศัพท์ผ่านอินเทอร์เน็ตด้วยระบบตรวจจับการบุกรุกโดยแบ่งการทดสอบเป็น 4 รูปแบบ คือ

1. การโจมตีจากเครือข่ายภายใน (Internal) โดยการโจมตีผ่านระบบเครือข่าย ด้วยรูปแบบการโจมตีแบบ Denial of Service (DoS)

2. การโจมตีจากเครือข่ายภายใน (Internal) โดยการโจมตีผ่านระบบเครือข่ายไร้สาย ด้วยรูปแบบการโจมตีแบบ Denial of Service (DoS)

3. การโจมตีจากเครือข่ายภายนอก (External) โดยการโจมตีผ่านระบบเครือข่าย ด้วยรูปแบบการโจมตีแบบ Denial of Service (DoS)

4. การโจมตีจากเครือข่ายภายนอก (External) โดยการโจมตีผ่านระบบเครือข่ายไร้สาย ด้วยรูปแบบการโจมตีแบบ Denial of Service (DoS)

โดยการโจมตีแบบ Denial of Service (DoS) แบ่งรูปแบบการโจมตีออกเป็น 2 กลุ่ม คือ

- โจมตีแบบการบุกรุกระบบโทรศัพท์ผ่านอินเทอร์เน็ต แบ่งได้ดังนี้

    1. Invite Flood เป็นการปลอมแปลงข้อความส่งให้ SIP Server ในอัตราเร็วกว่าปกติส่งผลให้ SIP Server มีภาระการทำงานเพิ่มขึ้น จึงปฏิเสธการให้บริการ

    2. RTP Flood เป็นการส่งแพ็คเกจ UDP จำนวนมากเข้าไปที่ Port RTP ของ Softphone โดยจะต้องรู้ Port ของ Softphone ส่งผลให้ระบบเสียงของ Softphone มีปัญหา

- โจมตีแบบการบุกรุกระบบเครือข่ายทั่วไป แบ่งได้ดังนี้

    1. UDP Flood เป็นการส่งแพ็คเกจ UDP จำนวนมากเข้าไปที่ SIP Server ส่งผลให้ SIP Server มีภาระการทำงานเพิ่มขึ้น จึงปฏิเสธการบริการ

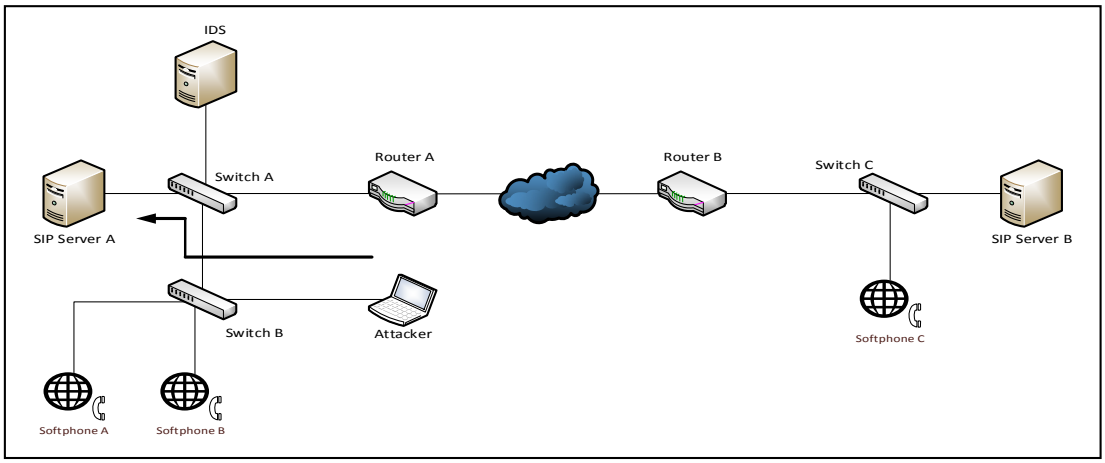
2. Ping of Death เป็นการส่งแพ็คเกจ ICMP จำนวนมากเข้าไปที่ SIP Server ส่งผลให้ SIP Server มีภาระการทำงานเพิ่มขึ้น จึงปฏิเสธการบริการ

5. โดยในการทดลอง ค่าในแกน x คือ จำนวนแพ็คเกจที่ตรวจจับได้ ค่าในแกน y คือ จำนวนครั้งที่ทดลอง และค่า % คือประสิทธิภาพการทำงานของ CPU , RAM และ Network ที่วัดได้จากการทดลอง

รูปแบบการโจมตีทั้ง 4 แบบจะโจมตีไปที่เครื่อง SIP Server ทั้งหมด 25 ครั้ง ครั้งละ 5 วินาทีโดยใช้ระบบตรวจจับการบุกรุก เพื่อเก็บข้อมูลการบุกรุกที่เกิดขึ้นในระบบเครือข่าย (LAN) และระบบเครือข่ายแบบไร้สาย (WLAN) โดยจะมีการโจมตีจากภายในและภายนอก แล้วนำผลการตรวจจับที่ได้มาทำการรวบรวมข้อมูลหาค่าเฉลี่ยและนำมาแสดงอยู่ในรูปของกราฟเพื่อให้ง่ายต่อการวิเคราะห์ข้อมูล ซึ่งผลการดำเนินการเป็นไปตามขั้นตอนดังนี้

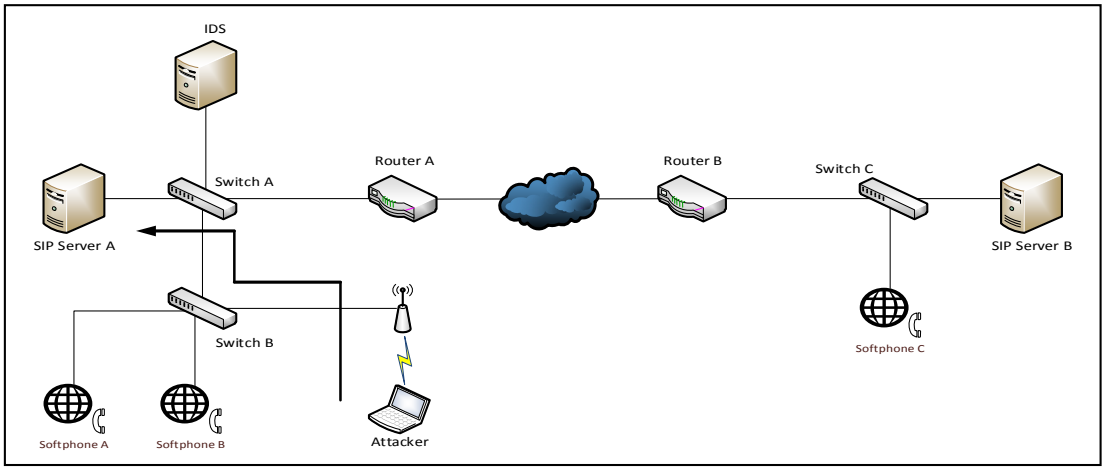
ผังเครือข่ายที่ใช้ในการทดลอง

ผังเครือข่ายแสดงการบุกรุกเครือข่ายจากภายใน โดยการโจมตีผ่านระบบเครือข่าย โดยใช้รูปแบบปฏิเสธการให้บริการ



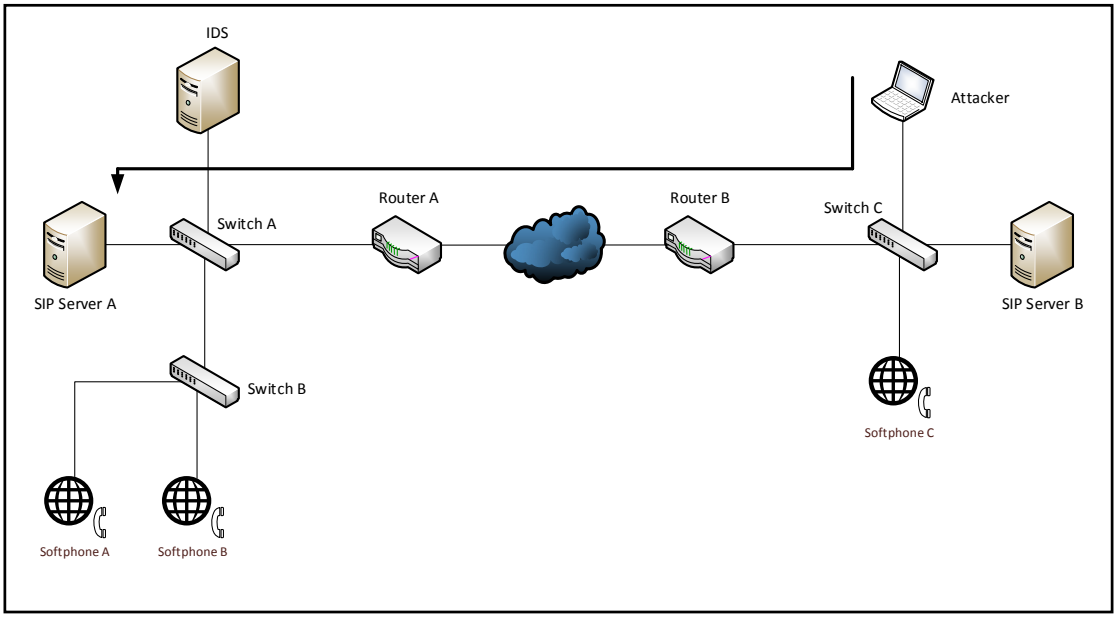
รูปที่ 1 แสดงผังเครือข่ายภายใน โดยการโจมตีผ่านระบบเครือข่าย

ผังเครือข่ายแสดงการบุกรุกเครือข่ายจากภายใน โดยการโจมตีผ่านระบบเครือข่ายไร้สาย โดยใช้รูปแบบปฏิเสธการให้บริการ



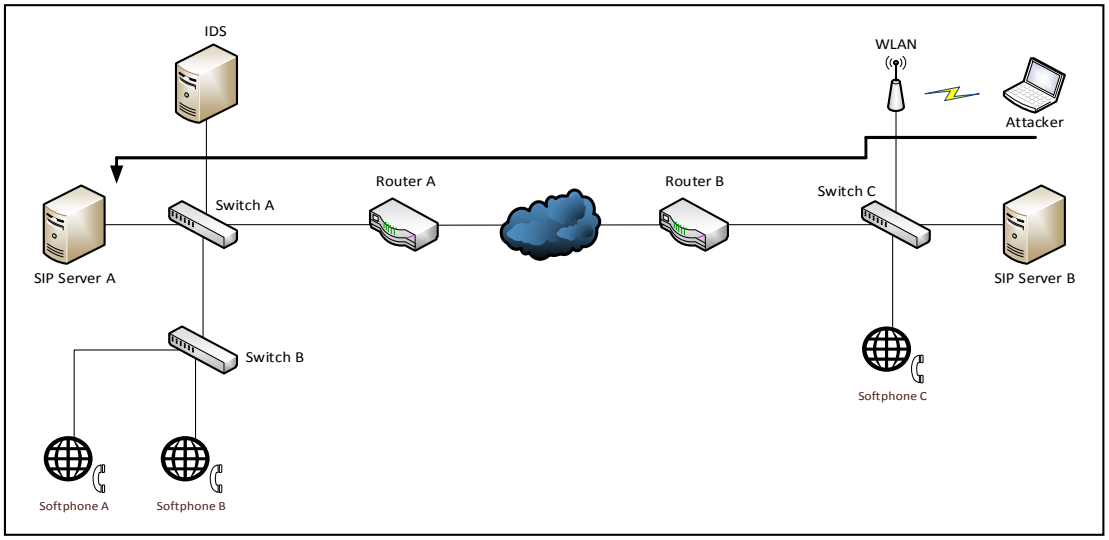
รูปที่ 2 แสดงผังเครือข่ายภายใน โดยการโจมตีผ่านระบบเครือข่ายไร้สาย

ผังเครือข่ายแสดงการบุกรุกเครือข่ายจากภายนอก โดยการโจมตีผ่านระบบเครือข่าย โดยใช้รูปแบบปฏิเสธการให้บริการ



รูปที่ 3 แสดงผังเครือข่ายภายนอก โดยการโจมตีผ่านระบบเครือข่าย

ผังเครือข่ายแสดงการบุกรุกเครือข่ายจากภายนอก โดยการโจมตีผ่านระบบเครือข่ายไร้สาย โดยใช้รูปแบบปฏิเสธการให้บริการ



รูปที่ 4 แสดงผังเครือข่ายภายนอก โดยการโจมตีผ่านระบบเครือข่ายไร้สาย

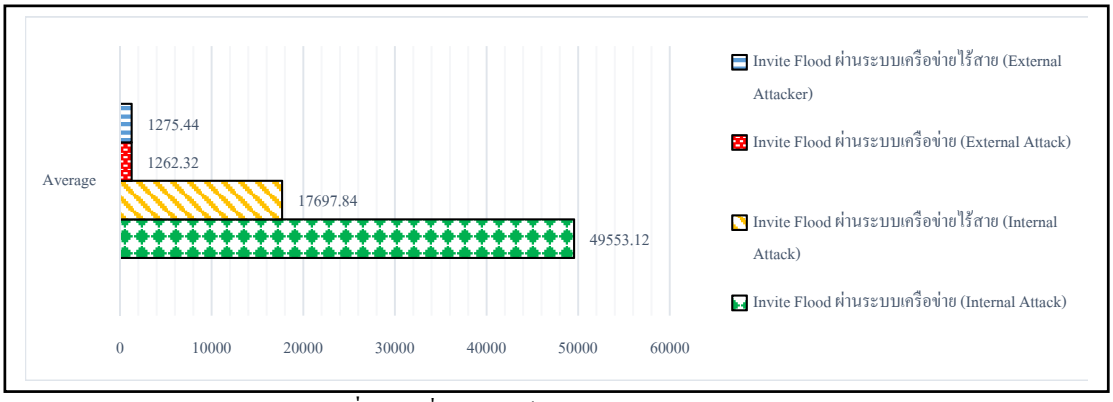
4. ผลการวิจัย

จากการที่ได้ตรวจสอบระบบตรวจจับการบุกรุกต่อระบบโทรศัพท์ผ่านอินเทอร์เน็ต โดยมีการทดลองโจมตี 4 รูปแบบคือ โจมตีแบบ Invite Flood, RTP Flood, UDP Flood และPing of Death (Albert Sagala, 2015) โดยแต่ละการโจมตีจะมี 2 ผลการทดลองคือ

1.ค่าเฉลี่ยจำนวนแพ็คเกจของการโจมตีของแต่ละรูปแบบซึ่งเป็นการเปรียบเทียบระหว่างการโจมตีผ่านระบบสาย และไร้สาย

2. การทำงาน CPU RAM และเครือข่ายของ SIP Server โดยเปลี่ยนแปลงรูปแบบการโจมตี แสดงรายละเอียดดังนี้

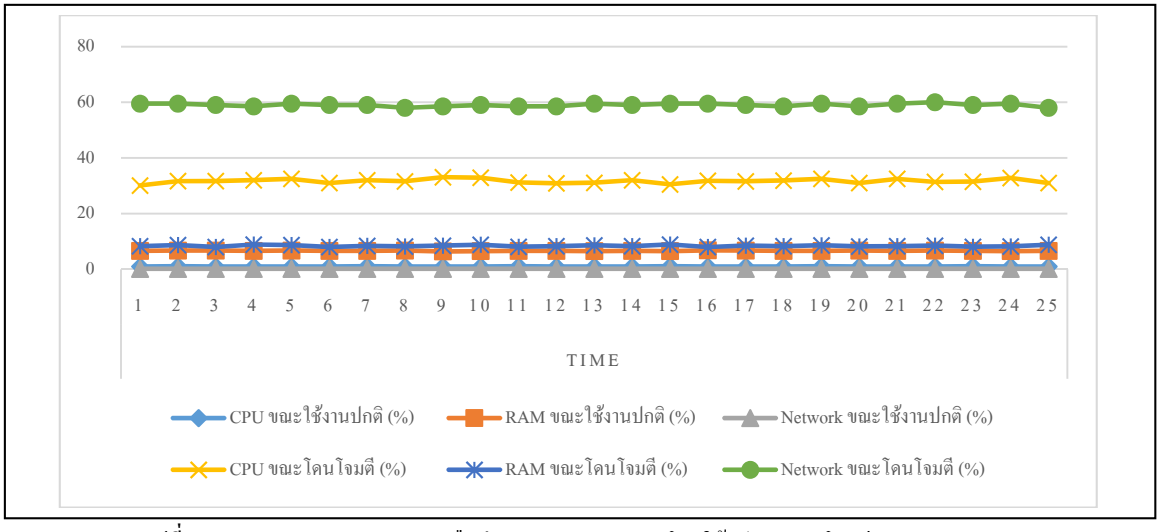
4.1 สรุปผลการโจมตีแบบ Invite Flood



รูปที่ 5 ค่าเฉลี่ยจำนวนแพ็คเกจของการโจมตีแบบ Invite Flood

จากรูปที่ 5 จะเห็นได้ว่าการบุกรุกจากเครือข่ายภายในผ่านระบบเครือข่ายในการทดลอง 25 ครั้ง มีค่าเฉลี่ยของการโจมตีแบบ Invite Flood มากที่สุดประมาณ 49553.12 แพ็กเกจ และการบุกรุกจากเครือข่ายภายนอกผ่านระบบเครือข่ายไร้สาย มีค่าเฉลี่ยของการโจมตีแบบ Invite Flood มากที่สุดประมาณ 1275.44 แพ็กเกจ

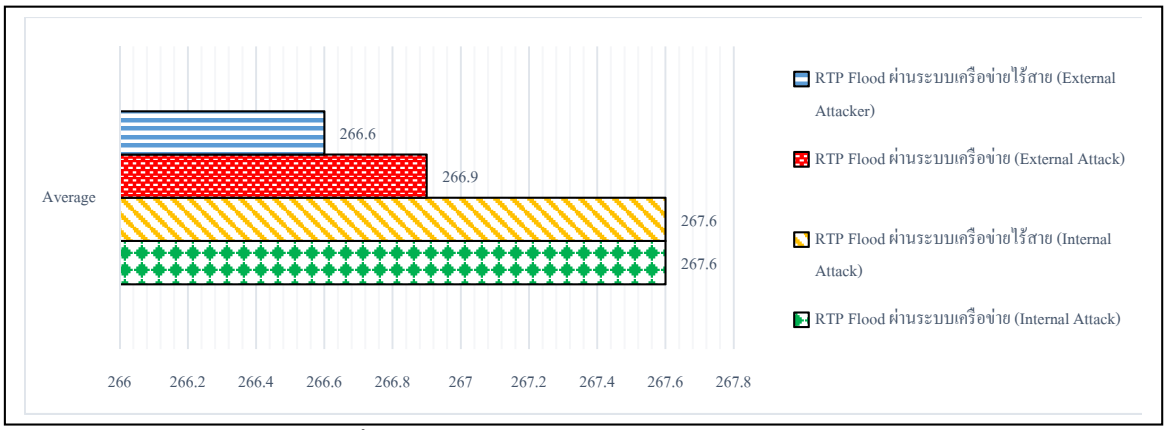
จากการโจมตีในรูปแบบของ Invite Flood จะเห็นได้ว่า การโจมตีที่ระบบสามารถตรวจจับได้มากที่สุดคือการโจมตีผ่านเครือข่ายจากภายในระบบเครือข่าย



รูปที่ 6 การทำงาน CPU RAM และเครือข่ายของ SIP Server A โดยใช้รูปแบบการโจมตีแบบ Invite Flood

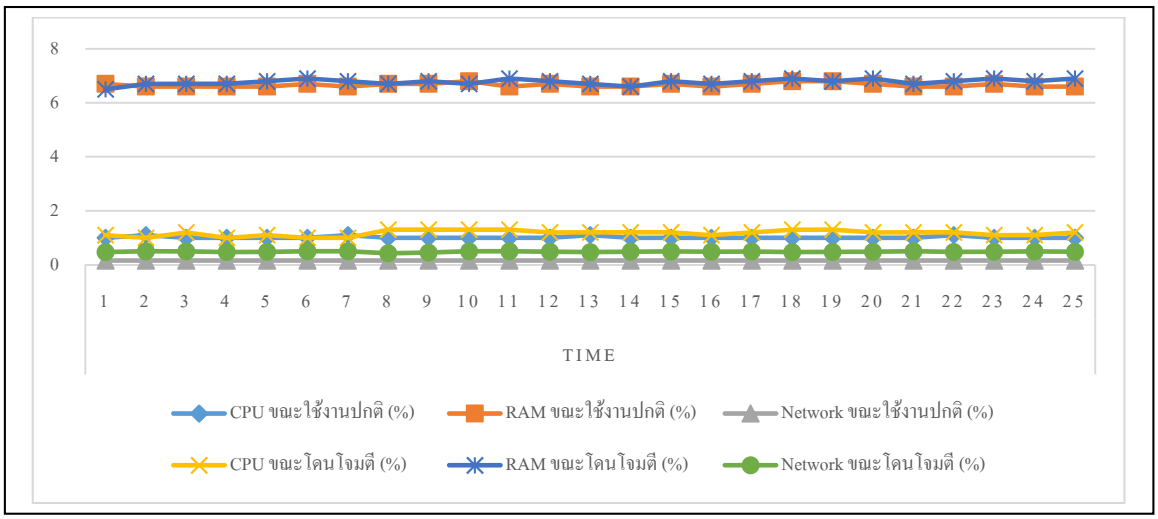
รูปที่ 6 แสดงให้เห็นว่าการโจมตีแบบ Invite Flood ทำให้ทรัพยากรของเครื่องที่ถูกโจมตีทำงานผิดปกติ เนื่องจากการโจมตีแบบ Invite Flood เป็นการส่ง Invite Message ในจำนวนมากส่งไปที่เครื่อง SIP Server โดยส่งผลให้ทรัพยากรเหล่านี้ ได้แก่ CPU และแบนด์วิดท์ของเครือข่ายเกิดการทำงานที่หนักผิดปกติ

4.2 สรุปผลการโจมตีแบบ RTP Flood



รูปที่ 7 ค่าเฉลี่ยจำนวนแพ็คเกจของการโจมตีแบบ RTP Flood

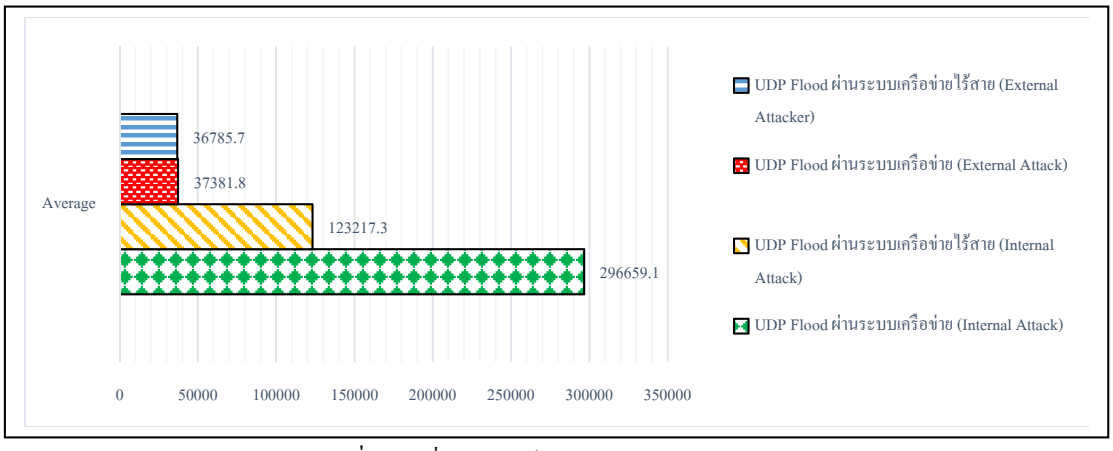
จากรูปที่ 7 จะเห็นได้ว่าบุกรุกจากเครือข่ายภายในผ่านระบบเครือข่ายในการทดลอง 25 ครั้ง มีค่าเฉลี่ยของการโจมตีแบบ RTP Flood มากที่สุดประมาณ 267.6 แพ็กเกจ และการบุกรุกจากเครือข่ายภายนอก ผ่านระบบเครือข่ายมีค่าเฉลี่ยของการโจมตีแบบ RTP Flood มากที่สุดประมาณ 266.9 แพ็กเกจ



รูปที่ 8 การทำงานของ CPU RAM และเครือข่ายของ SIP Server A โดยใช้รูปแบบการโจมตีแบบ RTP Flood

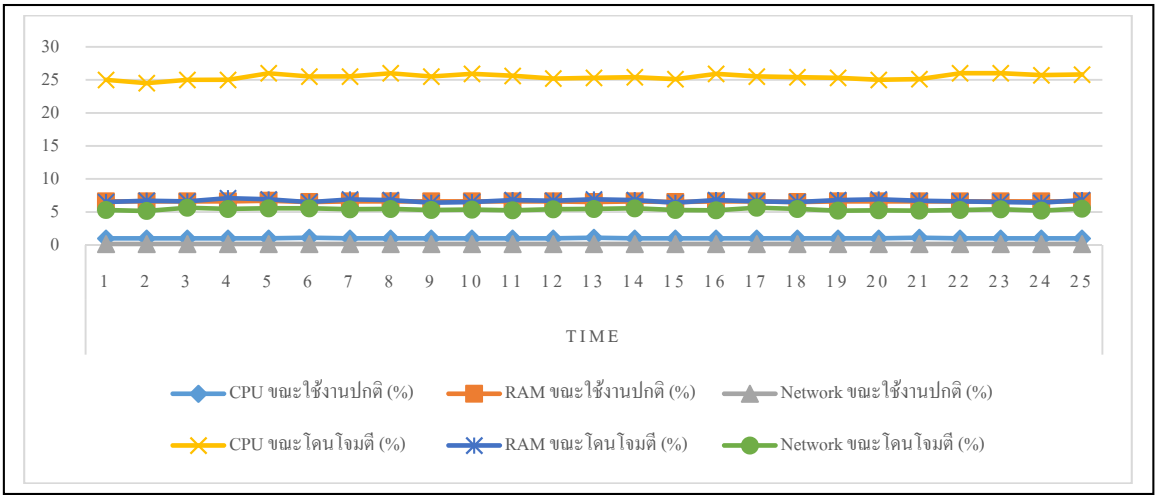
จากรูปที่ 8 เห็นว่าการโจมตีแบบ RTP Flood ไม่มีผลกับทรัพยากรของเครื่องที่ SIP Server จากที่ได้ทำการทดลอง การโจมตีแบบ RTP Flood เป็นการส่งแพ็กเกจ UDP ที่มีข้อมูลของ TCP ในจำนวนมาก (ซึ่งต้องรู้พอร์ต TCP ของ Client ที่กำลังติดต่อสื่อสาร) ไปยัง Client ที่มีการติดต่อสื่อสารส่งผลทำให้การติดต่อสื่อสารระหว่าง Client มีปัญหา

4.3 สรุปผลการโจมตีแบบ UDP Flood



รูปที่ 9 ค่าเฉลี่ยจำนวนแพ็คเกจของการโจมตีแบบ UDP Flood

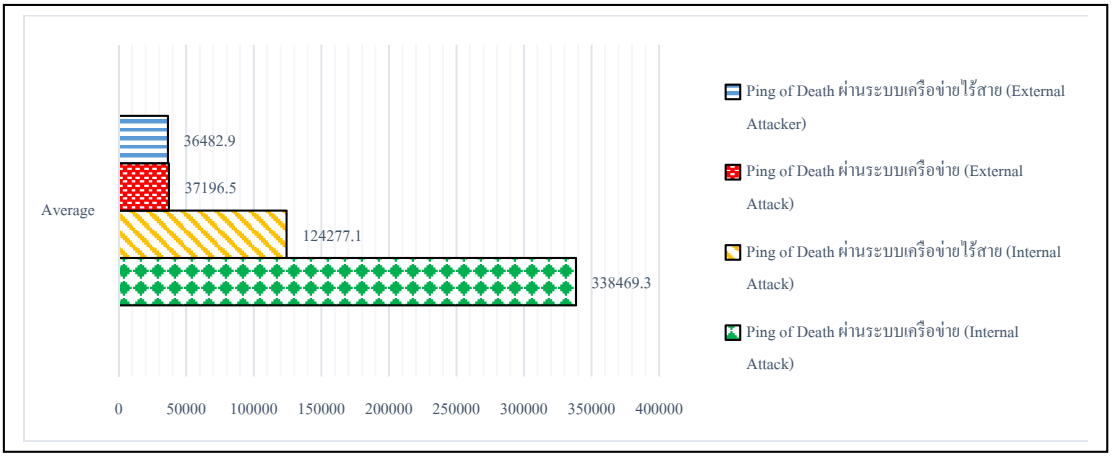
จากรูปที่ 9 เห็นได้ว่าการบุกรุกจากเครือข่ายภายในผ่านระบบเครือข่ายในการทดลอง 25 ครั้ง มีค่าเฉลี่ยของการโจมตีแบบ UDP Flood มากที่สุดประมาณ 296659.1 แพ็กเกจ และการบุกรุกจากเครือข่ายภายนอกผ่านระบบเครือข่าย มีค่าเฉลี่ยของการโจมตีแบบ UDP Flood มากที่สุดประมาณ 37381.8 แพ็กเกจ



รูปที่ 10 การทำงานของ CPU RAM และเครือข่ายของ SIP Server A โดยใช้รูปแบบการโจมตีแบบ UDP Flood

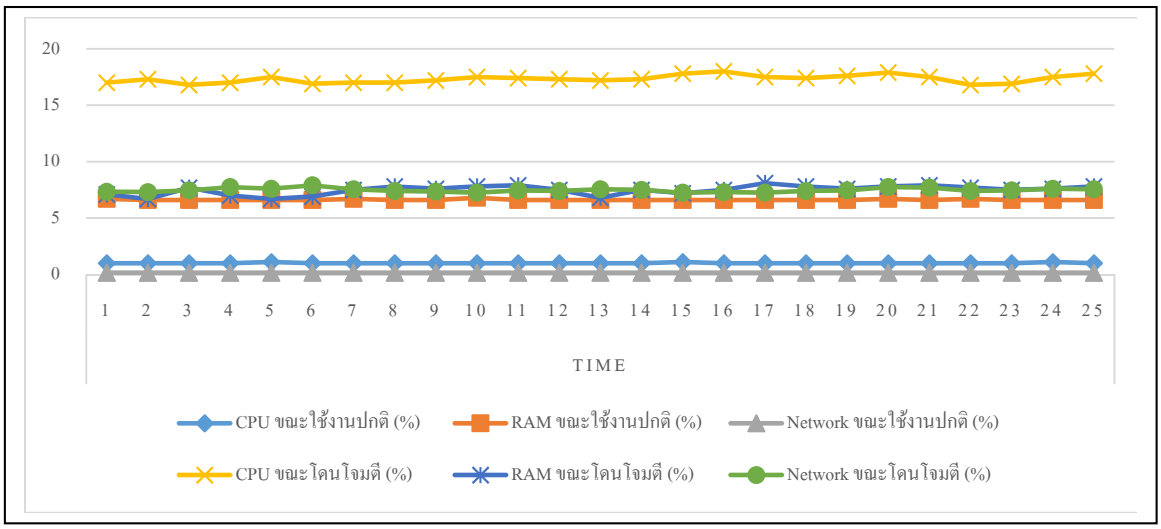
จากรูปที่ 10 แสดงให้เห็นว่าการโจมตีแบบ UDP Flood ทำให้ทรัพยากรของเครื่องที่ถูกโจมตีทำงานผิดปกติ การโจมตีแบบ UDP Flood เป็นการส่งแพ็กเกจ UDP จำนวนมากอย่างต่อเนื่องไปที่เครื่องเป้าหมายโดยส่งผลให้ทรัพยากรเหล่านี้ ได้แก่ CPU และแบนด์วิดท์ ของเครือข่าย เกิดการทำงานที่หนักผิดปกติ

4.4 สรุปผลการโจมตีแบบ Ping of Death



รูปที่ 11 กราฟแสดงผลรวมของ Ping of Death

จากรูปที่ 11 จะเห็นได้ว่าการบุกรุกจากเครือข่ายภายในในการทดลอง 25 ครั้ง ผ่านระบบเครือข่าย มีค่าเฉลี่ยของการโจมตีแบบ Ping of Death มากที่สุดประมาณ 338469.3 แพ็กเกจ และการบุกรุกจากเครือข่ายภายนอก ผ่านระบบเครือข่าย มีค่าเฉลี่ยของการโจมตีแบบ Ping of Death มากที่สุดประมาณ 37196.5 แพ็กเกจ



รูปที่ 12 การทำงานของ CPU RAM และเครือข่ายของ SIP Server A โดยใช้รูปแบบการโจมตีแบบ Ping of Death

รูปที่ 12 แสดงให้เห็นว่าการโจมตีแบบ Ping of Death ทำให้ทรัพยากรของเครื่องที่ถูกโจมตีทำงานผิดปกติ การโจมตีแบบ Ping of Death เป็นการส่งแพ็กเกจ Ping Request จำนวนมากอย่างต่อเนื่องไปที่เครื่องเป้าหมายโดยส่งผลให้ทรัพยากรเหล่านี้ ได้แก่ CPU และแบนด์วิดท์ของเครือข่าย เกิดการทำงานที่หนักผิดปกติ

5. การอภิปรายผล

จากผลการทดลองรูปที่ 5 7 9 และ 11 จะเห็นว่าการโจมตีจากภายในเครือข่ายทั้งการเชื่อมต่อแบบสายและไร้สายระบบตรวจจับการบุกรุกสามารถตรวจจับจำนวนการโจมตีได้มากกว่าการโจมตีจากภายนอกในทุกการทดลอง และการโจมตีแบบ UDP Flood และ Ping of Death สามารถตรวจจับการโจมตีได้มากกว่าการโจมตีแบบ Invite Flood และ RTP Flood เมื่อตรวจพบแพ็คเกจที่มีพฤติกรรมเสี่ยงต่อการโจมตีระบบโทรศัพท์ผ่านอินเทอร์เน็ต (Hanifan and Bandung, 2013) จะมีการแจ้งเตือนผ่านทางเว็บไซต์

จากผลการทดลองรูปที่ 6 8 10 และ 12 ผลกระทบของ CPU RAM และระบบเครือข่ายของระบบโทรศัพท์ผ่านอินเทอร์เน็ตด้วยโพรโตคอล SIP (Session Initiation Protocol) พบว่าระบบสามารถตรวจจับการโจมตีระบบโทรศัพท์ผ่านอินเทอร์เน็ตจากการโจมตีแบบ Invite Flood, RTP Flood, UDP Flood และPing of Death ส่งผลกับทรัพยากรเครื่อง ได้แก่ CPU และแบนด์วิดท์ของระบบเครือข่ายเฉลี่ยไม่เกิน 40 % และการโจมตีแบบ RTP Flood ส่งผลกับทรัพยากรของเครื่องน้อยมากเฉลี่ยไม่เกิน 5 % ทั้งนี้ RTP เป็นโปรโตคอลที่ใช้รูปแบบการทำงานของ UDP

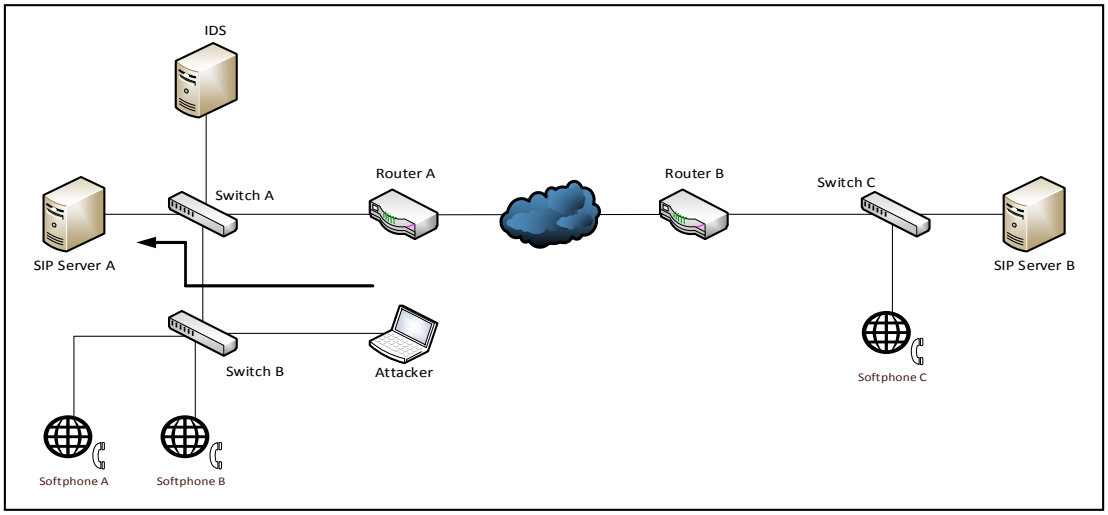
ซึ่งเป็นการส่งข้อมูลในทิศทางเดียว แบบเซิร์ฟเวอร์ไปยังไคลเอนต์ โดยจะไม่มีการตรวจสอบความถูกต้องของข้อมูล ดังนั้นจึงสามารถส่งข้อมูลได้อย่างรวดเร็ว ซึ่งได้ถูกนำมาใช้ในการส่งข้อมูลมัลติมีเดียซึ่งปัจจุบันมีการสื่อสารข้อมูลชนิดนี้จำนวนมาก

๖. บทสรุป

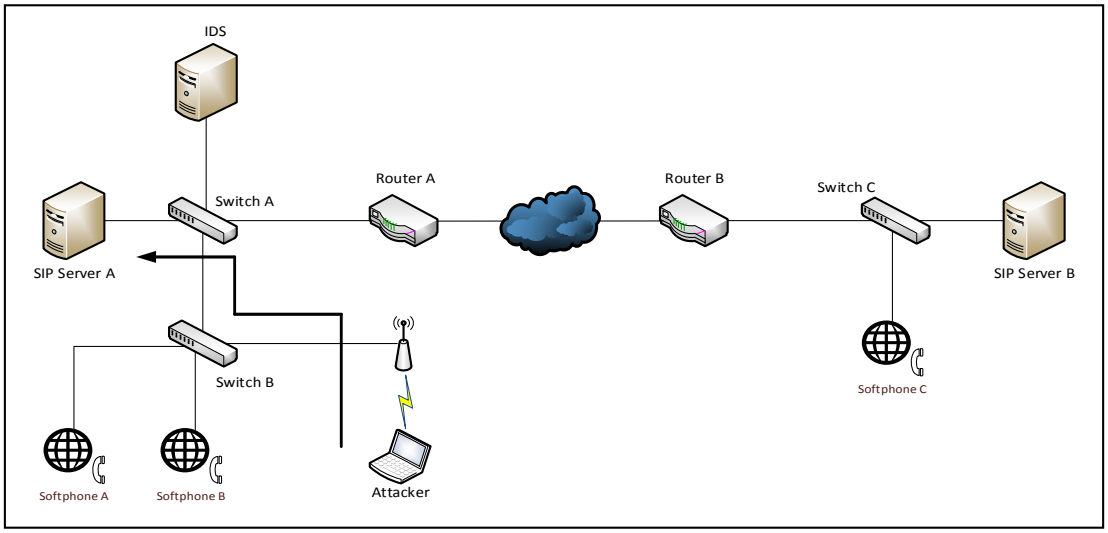
จากการทดสอบประสิทธิภาพของระบบตรวจจับการบุกรุกจะเห็นได้ว่า การตรวจจับการบุกรุกด้วยการโจมตีในรูปแบบปฏิเสธการให้บริการส่วนของเครือข่ายภายในผ่านระบบเครือข่าย และเครือข่ายภายในผ่านระบบเครือข่ายไร้สายกับระบบโทรศัพท์ผ่านอินเทอร์เน็ตด้วยโพรโตคอล SIP (Session Initiation Protocol) มีประสิทธิภาพในการตรวจจับการโจมตีแบบภายในมากกว่าการบุกรุกจากภายนอก จะเห็นว่าการโจมตีจากภายในทั้งระบบเครือข่ายและระบบเครือข่ายไร้สาย ระบบสามารถตรวจจับได้จำนวนเหตุการณ์ที่เกิดขึ้นต่างกันเนื่องจากการโจมตี เป็นการส่งแพ็คเกจจำนวนมาก ๆ อย่างต่อเนื่องจึงเกิดการชนกันของข้อมูล (CSMA/CD) จากผลการทดลองจะเห็นว่าระบบเครือข่ายไร้สาย มีจำนวนเหตุการณ์ที่ต่างกันกับระบบเครือข่าย เนื่องจากระบบเครือข่ายไร้สายจะมีกระบวนการในการหลีกเลี่ยงเพื่อไม่ให้เกิดชนกันของข้อมูล (CSMA/CA) จึงทำให้จำนวนแพ็คเกจบางเหตุการณ์ไม่สามารถส่งผ่านระบบเครือข่ายไร้สายได้ทำให้ผลการตรวจจับการบุกรุกผ่านเครือข่ายสายและไร้สายมีผลต่างกันเล็กน้อย

ส่วนการโจมตีรูปแบบปฏิเสธการให้บริการแบบ INVITE FLOOD ซึ่งเป็นการโจมตีโดยใช้เทคนิค SYN Flood ซึ่งอาศัยหลักการทำงานของ 3-Way Handshake ซึ่งมีการโจมตี INVITE FLOOD มีผลกระทบต่อ CPU และระบบเครือข่ายเฉลี่ยประมาณ 40% ซึ่งถือว่ามีผลกระทบต่อการทำงานของเครื่องแม่ข่าย SIP ซึ่งให้บริการระบบโทรศัพท์ผ่านอินเทอร์เน็ต และที่สำคัญไม่มีผลการทดลองในการโจมตีใดส่งผลกระทบต่อการทำงานของ RAM ผลที่ได้จากการทดสอบประสิทธิภาพระบบตรวจจับการบุกรุก จะสามารถนำไปประยุกต์ใช้สำหรับการวางระบบ เพื่อตรวจจับการบุกรุกจากผู้ไม่ประสงค์ดีโดยนำไปใช้ให้เหมาะสมกับระบบเครือข่ายและการให้บริการระบบโทรศัพท์ผ่านอินเทอร์เน็ตที่ต้องการ

ดังนั้นจากการวิเคราะห์ประสิทธิภาพการโจมตีระบบโทรศัพท์ผ่านอินเทอร์เน็ตด้วยระบบตรวจจับการบุกรุก จะเห็นได้ว่า การตรวจจับการบุกรุกในส่วนของเครือข่ายภายในผ่านระบบเครือข่าย และเครือข่ายภายในผ่านระบบเครือข่ายไร้สาย มีประสิทธิภาพในการตรวจจับมากกว่าการบุกรุกจากภายนอก ไม่ว่าจะเป็นการบุกรุกผ่านระบบเครือข่ายหรือ ระบบเครือข่ายไร้สาย



รูปที่ 13 แสดงผังการตรวจจับการโจมตีเครือข่าย ผ่านระบบเครือข่ายที่มีประสิทธิภาพในการตรวจจับมากที่สุด



รูปที่ 14 แสดงผังการตรวจจับการโจมตีเครือข่าย ผ่านระบบเครือข่ายไร้สายที่มีประสิทธิภาพในการตรวจจับมากที่สุด

ซึ่งผลที่ได้จากการทดสอบประสิทธิภาพระบบตรวจจับการบุกรุก จะสามารถนำไปประยุกต์ใช้สำหรับการวางระบบ เพื่อตรวจจับการบุกรุกจากผู้ไม่ประสงค์ดี โดยนำไปใช้ให้เหมาะสมกับระบบเครือข่ายของมหาวิทยาลัย หน่วยงาน ภาครัฐและภาคเอกชน เพื่อนำไปสู่ความมั่นคงของระบบคอมพิวเตอร์ตามวัตถุประสงค์ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี 2560

7. กิตติกรรมประกาศ

ผู้วิจัยขอขอบพระคุณ ผศ.ดร.เชฎฐเนติ ศรีสอ้าน คณบดี วิทยาลัยนวัตกรรมดิจิทัลและเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต ที่ให้การสนับสนุน และอำนวยความสะดวกในการจัดทำการวิจัย

8. เอกสารอ้างอิง

อรรถพล ป้อมสถิตย์. (2561). *Computer and Information Security Theory (พิมพ์ครั้งที่ 1)*. กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยราชภัฏสวนสุนันทา.

อรรถพล ป้อมสถิตย์, และบุญเรือง เกิดอรุณเดช. (2562). การเพิ่มสมรรถนะของระบบตรวจจับการบุกรุกด้วยฮันนี่พอทของระบบการส่งสัญญาณสื่อใหม่ ผ่านอินเทอร์เน็ต (Efficiency Increase of Intrusion Detection System with Honey Pot for Transmission New Media Broadcasting via Internet.). *สักทอง: วารสารวิทยาศาสตร์และเทคโนโลยี, 7*(1), 73-84.

อรรถพล ป้อมถิตย์. (2559). การเพิ่มประสิทธิภาพระบบตรวจจับการบุกรุกในการรักษาความมั่นคงทางไซเบอร์ด้วยฮันนี่พอท (Enhanced Efficiency of Intrusion Detection Systems with Honey Pot in Cyber Security.). *KKU Science journal, 44*(2), 384-397.

Sagala, A. (2015). Automatic SNORT IDS rule generation based on honeypot log. In *2015 7th International Conference on Information Technology and Electrical Engineering (ICITEE)* (pp. 576-580). IEEE.

Hanifan, Y., & Bandung. (2013). Designing VoIP security system for organizational network. International Conference on ICT for Smart Society (ICISS), 1-5

Zhenxin Z., Maochao X., & Shouhuai X. (2015) Characterizing Honeypot-Captured Cyber Attacks: Statistical Framework and Case Study. IEEE Transactions on Information Forensics and Security, 1775 – 1789