การต้านทานและการกู้คืนจากการโจมตี DDoS ของบอร์ด Raspberry Pi ที่ทำงานเป็น IoT ผ่านไวไฟ

RESISTANCE AND RECOVERY FROM DDOS ATTACK OF RASPBERRY PI BOARD BASED ON WIFI IOT SYSTEM

อินทัชพงค์ รัตนดิลก ณ ภูเก็ต[1]
ดร.ชัยพร เขมะภาตะพันธ์[2]

บทคัดย่อ

ปัจจุบันเทคโนโลยี IoT มีการนำมาประยุกต์ใช้ในหลายอุตสาหกรรม หรือภายในชีวิตประจำวันเช่น บ้านอัจฉริยะ (Smart Home) หากแต่เทคโนโลยีในด้านความมั่นคงปลอดภัยของเทคโนโลยี IoT ไม่ได้รับการพัฒนาให้มีประสิทธิภาพและไม่พร้อมรับมือกับการโจมตีทางไซเบอร์ในปัจจุบัน งานวิจัยนี้จึงเสนอการโจมตีทางไซเบอร์ในรูปแบบ DDoS ไปยังระบบ IoT แบบบ้านอัจฉริยะ (Smart Home) เพื่อแสดงให้เห็นถึงผลกระทบ ผลที่เกิดจากการโจมตี ขีดจำกัดของกำลังประมวลผลของอุปกรณ์ และความสามารถในการกู้คืนตนเองของอุปกรณ์ โดยเลือกใช้การโจมตีในรูปแบบ TCP SYN Flood, HTTP GET Flood, ICMP Flood และ UDP Flood Attack ซึ่งเป็นรูปแบบการโจมตีที่พบบ่อยและเป็นวิธีการโจมตีอันดับต้นๆที่มักถูกเลือกใช้ โดยได้แสดงถึงผลลัพธ์ของการโจมตีที่ส่งผลกระทบกับระบบ ทำให้ผู้ใช้งานไม่สามารถควบคุมหรือสั่งการอุปกรณ์ได้ในขณะที่เกิดการโจมตีแบบ TCP SYN Flood Attack ส่วนการโจมตีแบบ HTTP GET Flood Attack แสดงให้เห็นถึงขีดความสามารถในการประมวลผลของอุปกรณ์ การโจมตีแบบ ICMP Flood Attack และ UDP Flood Attack แสดงให้เห็นถึงประมาณการใช้งานเครือข่ายที่สูงขึ้น ทำให้การเรียกใช้บริการต่าง ๆ ผ่านเครือข่ายใช้เวลาสูงขึ้น

คำสำคัญ: การโจมตีทางไซเบอร์, Raspberry Pi, DDoS, TCP SYN Flood, HTTP GET Flood, ICMP Flood, UDP Flood

---

[1]นักศึกษาหลักสูตรวิศวกรรมศาสตร์มหาบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์

[2]อาจารย์ที่ปรึกษาสารนิพนธ์หลัก

ABSTRACT

Today, IoT technology is applied in many industries. Or within everyday life, such as a Smart Home. But the security technology of IoT technology has not been developed to be effective and is not ready to deal with today's cyberattacks. This research proposes cyberattacks in the form of DDoS on IoT Smart Home systems to demonstrate the impact. The consequences of the attack are device processing limit and the self-recovery capability of the device. It uses TCP SYN Flood, HTTP GET Flood, ICMP Flood, and UDP Flood Attack, which are the most common attack types and are often the top attack methods of choice. It shows the outcome of the attack that affected the system. As a result, users cannot control or operate a device during a TCP SYN Flood Attack. The HTTP GET Flood Attack demonstrates the processing capabilities of the device. The ICMP Flood Attack and UDP Flood Attack provide a more bandwidth usage of network. This makes running services over the network take longer.

Keywords: Cyber Attack, Raspberry Pi, DDoS, TCP SYN Flood, HTTP GET Flood, ICMP Flood, UDP Flood

บทนำ

ปัจจุบันเทคโนโลยี IoT ได้เข้ามามีส่วนช่วยพัฒนาการดำรงชีวิตของมนุษย์ในปัจจุบันให้สะดวกสบายขึ้น ช่วยลดขั้นตอนต่าง ๆ ในกระบวนการทำงาน ช่วยเพิ่มประสิทธิภาพของผลลัพธ์ หรือแม้กระทั่งช่วยเพิ่มความมั่นคงปลอดภัย การประยุกต์ใช้เทคโนโลยี IoT เกิดขึ้นทั้งในภาคอุตสาหกรรม หรือแม้กระทั่งภายในครัวเรือน ที่มีการนำเทคโนโลยีมาประยุกต์ใช้ให้เกิดเป็นบ้านอัจฉริยะ (Smart Home) เพื่อช่วยเพิ่มประสิทธิภาพภายในบ้าน และเสริมสร้างความสะดวกสบาย หรือความปลอดภัยให้แก่ผู้อยู่อาศัยและตัวเทคโนโลยี IoT เป็นองค์ความรู้ที่แพร่หลาย สามารถศึกษาหรือพัฒนาได้ด้วยตนเอง ทำให้การนำเทคโนโลยี IoT มาประยุกต์ใช้เพิ่มขึ้นแบบก้าวกระโดด

หากแต่ความสามารถด้านความมั่นคงปลอดภัยของตัวเทคโนโลยี IoT เองยังไม่ถูกสนใจหรือถูกพัฒนาให้เหมาะสมและครอบคลุมกับการใช้งานต่าง ๆ เท่าที่ควรทำให้เทคโนโลยี IoT อาจเป็นสาเหตุให้เกิดความเสียหาย หรือ อันตรายแก่ชีวิตและทรัพย์สิน ผ่านรูปแบบการโจมตีทางไซเบอร์ในรูปแบบต่าง ๆ เช่นการโจมตีแบบ DDoS และ DRDoS ที่เป็นที่นิยมและพบมากที่สุด โดยจุดอ่อนในเทคโนโลยี IoT ในปัจจุบันเกิดขึ้นในหลายส่วนเช่น Protocol, Sensors หรือแม้กระทั่งกำลังการประมวลผลของตัวอุปกรณ์ IoT ก็สามารถที่จะเป็นช่องโหว่ของการโจมตีได้

วัตถุประสงค์

เพื่อนำเสนอการโจมตีในรูปแบบ DDoS ไปยังระบบ IoT แบบ Smart Home ที่จำลองขึ้นโดยการใช้เทคนิคการโจมตีแบบ HTTP GET Flood Attack, TCP SYN Flood Attack, ICMP Flood Attack, UDP Flood Attack เพื่อศึกษาผลที่เกิดจากการโจมตี และเกิดระหว่างการโจมตี

1. ศึกษาปริมาณ Packet ที่ระบบสามารถตอบสนองได้
2. ศึกษาผลการทำงานของระบบ IoT ที่เกิดระหว่างการโจมตี
3. ศึกษาผลการทำงานของระบบ IoT ที่เกิดหลังการโจมตีสิ้นสุดลง
4. ศึกษาความสามารถในการกู้คืนตัวเอง (Resilience) ของระบบ IoT จำลอง

ขอบเขตของการวิจัย

1. ระบบ IoT ที่ใช้ทดสอบเป็นการจำลองระบบ IoT ในรูปแบบ Smart Home ที่สามารถสร้างและพัฒนาขึ้นได้ด้วยตนเอง
2. ระบบ IoT ที่จำลองขึ้นมาเพื่อใช้ในการทดสอบเป็นระบบปิดไม่มีการเชื่อมต่อกับ Internet ภายนอก
3. การเชื่อมต่อของเครือข่ายทั้งหมดในระบบ IoT ถูกนิยามความเร็วของการรับส่งข้อมูลเป็นแบบความเร็วสูงสุด

แนวคิดทฤษฎีและงานวิจัยที่เกี่ยวข้อง

1. ทฤษฎี IoT (Internet of Thing)

Internet of Things (IoT) หรือ อินเตอร์เน็ตสรรพสิ่ง เป็นแนวคิดที่เกี่ยวกับเครือข่ายวัตถุ อุปกรณ์ พาหนะ สิ่งปลูกสร้าง และสิ่งอื่นๆ ที่มีวงจรอิเล็กทรอนิกส์ ซอฟต์แวร์ เซนเซอร์ และการเชื่อมต่อกับเครือข่าย ซึ่งทำให้วัตถุเหล่านี้สามารถเก็บบันทึกและแลกเปลี่ยนข้อมูลได้ โดยโครงสร้างทางสถาปัตยกรรมของ IoT ประกอบด้วย 3 ระดับชั้น ชั้น Perception Layer เป็นชั้นที่เกี่ยวข้องกับอุปกรณ์ Sensors, อุปกรณ์ Actuatorsชั้น Network Layer เป็นชั้นที่เกี่ยวกับการรับส่งข้อมูลหรือการติดต่อสื่อสารผ่านเครือข่าย ชั้น Network Layer นี้ประกอบด้วย 2 ส่วนหลักคือ เทคโนโลยีที่เกี่ยวกับการสื่อสารและ Protocol

2. การโจมตีแบบ TCP SYN Flood Attack

SYN Flooding เป็นการโจมตีโดยการส่ง TCP Packet ไปยังเป้าหมายเหมือนขั้นตอนการเริ่มต้นร้องขอการเชื่อมต่อ (Negotiation) ตามรูปแบบการเชื่อมต่อแบบ TCP ปกติแต่เมื่อเครื่องเป้าหมายทำการตอบกลับด้วย SYN-ACK เครื่องที่ทำการโจมตีจะไม่ทำการส่งข้อมูลกลับไป ทำให้เครื่องเป้าหมายค้างอยู่ในสถานะ Half-Open ซึ่งหากมีการส่ง Packet ไปยังเครื่องเป้าหมายเป็นจำนวนมากจะทำให้เครื่องเป้าหมายให้บริการช้าลงหรือไม่สามารถให้บริการได้

3. การโจมตีแบบ HTTP GET Flood Attack

HTTP GET Flooding เป็นรูปแบบการโจมตีที่เกิดขึ้นในชั้น Application Layer โดยเครื่องที่โจมตีจะทำการส่ง GET Request ไปยังเครื่องเป้าหมาย เมื่อได้รับ Request เครื่องเป้าหมายจะเข้าสู่ขั้นตอน Resource Allocation เพื่อจองทรัพยากรสำหรับการประมวลผล แต่หากเครื่องเป้าหมายได้รับจำนวน Request จำนวนมากๆจะทำให้ทรัพยากรของเครื่องเป้าหมายในขั้นตอน Resource Allocation เต็มและทำให้เครื่องเป้าหมายไม่สามารถให้บริการได้

4. การโจมตีแบบ ICMP Flood Attack

ICMP Flooding เป็นรูปแบบการโจมตีที่ผู้โจมตีทำการส่ง ICMP Echo Request (Ping) จำนวนมากไปยังเครื่องเป้าหมาย ซึ่งในขั้นตอนการส่ง ICMP Echo Request แบบปกติไปยังเครื่องปลายทาง 1 ครั้งเครื่องต้นทางจะได้รับการตอบ ICMP Response กลับมา 1 ครั้งซึ่งหากการโจมตีไปยังเครื่องเป้าหมายในปริมาณมาก การโจมตีในรูปแบบนี้จะส่งผลให้ Traffic ของเครือข่ายเต็มและทำให้เครื่องอื่นๆภายในเครือข่ายไม่สามารถเข้าถึงเครื่องที่ถูกโจมตีได้

5. การโจมตีแบบ UDP Flood Attack

UDP Flooding เป็นรูปแบบการโจมตีที่ผู้โจมตีทำการส่ง IP Packet ที่มีส่วนประกอบของ User Datagram Protocol (UDP) ไปยังเครื่องเป้าหมายในลักษณะ Random Ports เมื่อเครื่องเป้าหมายได้รับ Packet เครื่องเป้าหมายจะทำการประมวลที่เกี่ยวกับ UDP ของผู้ใช้งานนั้น ซึ่งเมื่อไม่พบหรือไม่สามรถประมวลผลได้ เครื่องเป้าหมายจะตอบ Destination Unreachable Packet กลับไปยังเครื่องต้นทาง ซึ่งหากเครื่องเป้าหมายได้รับ Packet ที่ปริมาณที่มากจะส่งผลให้ Traffic ของเครือข่ายเต็มทำให้เครื่องอื่นๆภายในเครือข่ายไม่สามารถเข้าถึงเครื่องที่ถูกโจมตีได้

6. งานวิจัยเรื่อง A Survey: DDoS Attack on Internet of Things

เป็นงานวิจัยของ Krushang Sonar and Asst Prof. Hardik Upadhyay, Gujarat Technology University, India, International Journal of Engineering Research and Development, 2014 เป็นงานวิจัยที่ศึกษารูปแบบการโจมตีแบบ DDoS ทั้งหมดที่เป็นไปได้ ที่สามารถโจมตีระบบหรืออุปกรณ์ IoT ให้ไม่สามารถให้บริการ หรือตอบสนองต่อผู้ใช้งานได้ โดยผลจากการศึกษาของงานวิจัยชิ้นนี้ ได้แบ่งรูปแบบหรือเทคนิคการโจมตีตามลักษณะของ IoT Architecture

7. งานวิจัยเรื่อง Resistance of IoT Sensors against DDoS Attack in Smart Home Environment

เป็นงานวิจัยของ Ladislav Huraj, Marek Simon, Department of Applied Informatics, University of SS. Cyril and Methodius และ Tibor Horak, Institute of Applied Informatics, Automation and Mechatronics, Faculty of Materials Science and Technology, Trnava, Slovak University of Technology, Slovakia, Sensors MDPI, 2020 เป็นงานวิจัยที่ศึกษาการโจมตีแบบ DDoS ไปยังอุปกรณ์ Home Assistance ที่มีวางขายทั่วไปตามห้องตลาด ที่สามารถนำมาเชื่อมต่อกันเป็น Center Hub สำหรับควบคุมอุปกรณ์ IoT ต่าง ๆ ภายในบ้านได้ โดยงานวิจัยชิ้นนี้เลือกรูปแบบการโจมตี 2 แบบได้แก่ SYN Flood Attack และ HTTP GET Flood Attack โดยเลือกใช้อุปกรณ์ IoT คือ 1.Fibaro Home Center 2.Philip Hue Bridge 3.Amazon Echo Dot 4.Athom Homey 5.Google Home โดยผลการทดสอบแสดงให้เห็นว่าการโจมตีแบบ TCP SYN Flood ไม่ส่งผลกระทบต่อการทำงานของอุปกรณ์ Control Center แต่การโจมตีแบบ HTTP GET Flood ส่งผลต่อการควบคุม

อุปกรณ์ที่มีการประมวลผลแบบ Local Computing แต่อุปกรณ์ที่มีการประมวลผลแบบ Cloud Computing ไม่ได้รับผลกระทบดังกล่าว

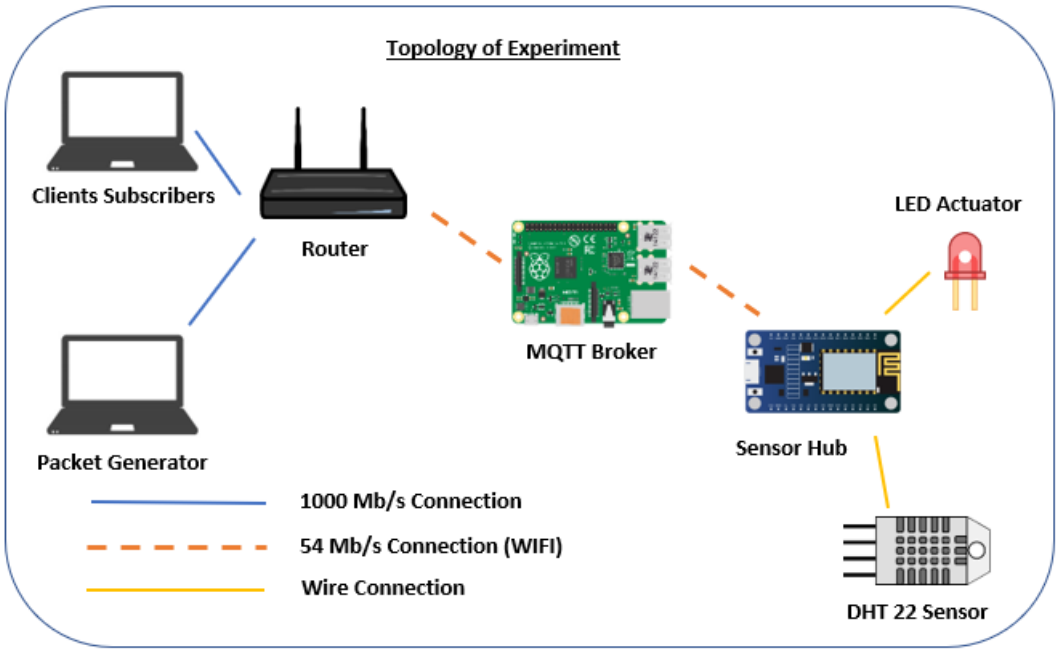
8. **งานวิจัยเรื่อง Vulnerability of Smart IoT-Based Automation and Control Devices to Cyber Attack**

เป็นงานวิจัยของ Tibor Horak, Marek Simon, Ladislav Huraj, and Roman Budjac, Institute of Applied Informatics, Automation and Mechatronics, Faculty of Materials Science and Technology, Trnava, Slovak University of Technology, Slovakia, Sensors MDPI, 2020 เป็นงานวิจัยที่ศึกษาและทดสอบการโจมตีในรูปแบบของ DDoS และ DRDoS ไปยังอุปกรณ์ Home Assistance ของผลิตภัณฑ์ Fibaro ที่เชื่อมต่อกับอุปกรณ์ IoT อย่าง Thermostat โดยการโจมตีแบบ DDoS ไปยัง port 80 และ 8000 ภายในระยะเวลา 60 นาทีแสดงให้เห็นว่าอุปกรณ์ IoT ถูกโจมตีและไม่สามารถให้บริการได้ตลอดระยะเวลาการโจมตี และการโจมตีแบบ HTTP GET Flood เป็นระยะเวลา 60 นาทีแสดงให้เห็นระยะเวลาการตอบสนองของอุปกรณ์สูงขึ้น และการโจมตีในรูปแบบ DRDoS ไปยังอุปกรณ์แบบ ICMP ECHO Flood เกิดสะท้อน Packet ไปยังอุปกรณ์ Thermostat ทำให้ไม่สามารถบันทึกค่าอุณหภูมิได้ตลอดระยะเวลาการโจมตี

ระเบียบวิธีวิจัย

งานวิจัยนี้ได้พัฒนาสร้างระบบจำลองการทดสอบออกมาในลักษณะ IoT แบบ Smart Home ที่ปัจจุบันมีการประยุกต์ใช้และสามารถสร้างขึ้นเอง ซึ่งมีการใช้งานที่แผร่หลายในปัจจุบัน เป็นรูปแบบหนึ่งของระบบ IoT ที่ไม่ขึ้นอยู่กับยี่ห้อของผลิตภัณฑ์ในท้องตลาด ภายในระบบจำลองใช้ Raspberry Pi Model B 8 GB ที่ติดตั้ง Raspbian OS เป็นระบบปฏิบัติการ พร้อมทั้งติดตั้ง Mosquitto Broker สำหรับรับส่งข้อมูลระหว่าง Publisher และ Subscriber ผ่าน MQTT Protocol พร้อมทั้งติดตั้ง FLASK ที่เป็น Web Framework ของ Python ที่รองรับ WSGI นอกจากนั้นยังติดตั้ง Paho-Mqtt Library ช่วยในการรับส่ง Message ระหว่าง Web และ MQTT Broker และติดตั้ง SocketIO Library ที่ช่วยทำให้ Web สามารถทำงานแบบ Asynchronous ส่วนในฝั่งของ Sensor Hub ใช้บอร์ด ESP 8266 ที่ติดตั้ง PubSubClient Library สำหรับรับส่ง Message กับ MQTT Broker ผ่าน MQTT Protocol และติดตั้ง DHT 22 Library เพื่อให้สามารถอ่านค่าอุณหภูมิและความชื้นจาก DHT 22 Sensor โดยมี LED Actuator และ DHT 22 Sensor เชื่อมต่อกับบอร์ด ESP 8266 ผ่าน GPIO Wire Connection และบอร์ด ESP 8266 เชื่อมต่อกับ MQTT Broker ผ่าน WIFI Connection การเชื่อมต่อ

ระหว่าง MQTT Broker และอุปกรณ์ High Speed Router เชื่อมต่อกันผ่าน WIFI Connection โดยการเชื่อมต่อแบบ WIFI Connection ทั้งหมดในระบบจำลองใช้ความเร็วที่ 54 Mb/s ส่วนของ Packet Generator หรืออุปกรณ์สร้างชุดการโจมตีใช้เครื่องคอมพิวเตอร์ที่ติดตั้ง Kali Linux เป็นระบบปฏิบัติการ และติดตั้ง HPing3 เป็นเครื่องสำหรับสร้างชุดการโจมตีในรูปแบบ TCP SYN Flood Attack, ICMP Flood Attack และ UDP Flood Attack พร้อมทั้งติดตั้ง WRK เป็นเครื่องมือสำหรับสร้างการโจมตีในรูปแบบ HTTP GET Flood Attack



รูปที่ 1 ภาพรวมของระบบ

แผนการโจมตี

ภายในงานวิจัยฉบับนี้ออกแบบแผนการโจมตีออกเป็น 2 ช่วง

1. ระหว่างการโจมตี
2. หลังการโจมตีสิ้นสุดลง

และมีลำดับของรูปแบบการโจมตีคือ

1. HTTP GET Flood Attack
2. TCP SYN Flood Attack

3. ICMP Flood Attack

4. UDP Flood Attack

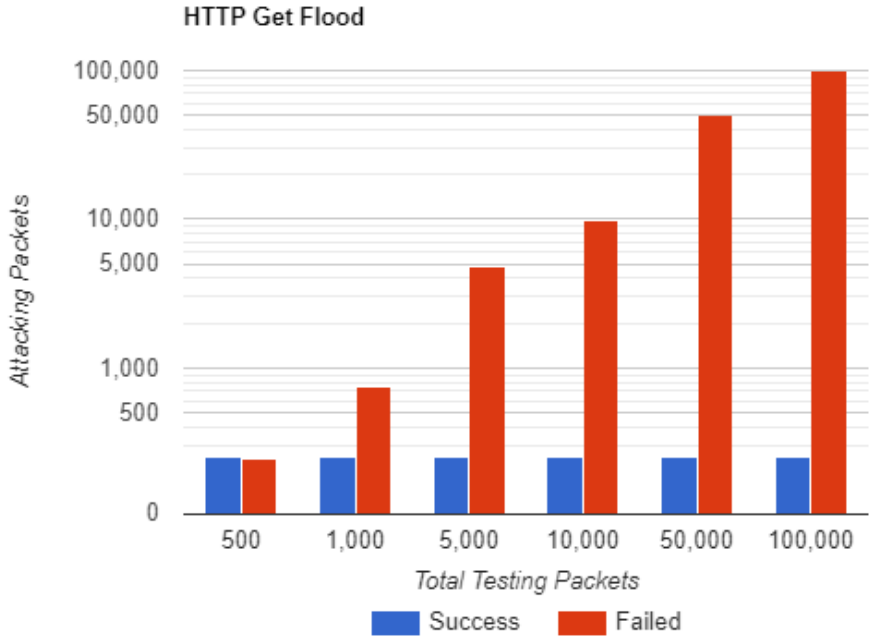
โดยใช้การโจมตีเป็นระยะเวลาต่อเนื่อง 1 นาทีสำหรับรูปแบบ HTTP GET Flood Attack และ10 นาที สำหรับการโจมตีแบบ TCP SYN Flood, ICMP Flood, UDP Flood Attack โดยทุก ๆ 1 นาทีจะทำการออกคำสั่งเพื่อสั่ง เปิดและปิด แอคชูเอเตอร์ LED, เรียกดูค่าอุณหภูมิและความชื้นผ่าน Web Application, ดูค่าอุณหภูมิความชื้นโดยตรงผ่าน Serial Monitor, ดูค่า Response Time ของ Web Application, ดูค่า CPU Usage ของ Raspberry Pi และดูค่า Memory ของ Raspberry Pi

หลังการโจมตีสิ้นสุดลงจะทำการออกคำสั่งทุก ๆ 1 นาทีเป็นระยะเวลา 5 นาทีเพื่อทดสอบความสามารถในการกู้คืนระบบ โดยการออกคำสั่งเปิดและปิด แอคชูเอเตอร์ LED, ดูค่าอุณหภูมิและความชื้นผ่าน Web Application, ดูค่าอุณหภูมิความชื้นโดยตรงผ่าน Serial Monitor, ดูค่า Response Time ของ Web Application, ดูค่า CPU Usage ของ Raspberry Pi และดูค่า Memory ของ Raspberry Pi

ผลการทดสอบ

HTTP GET Flood Attack

การโจมตีทั้ง 6 ครั้งแสดงให้เห็นว่า Raspberry Pi สามารถรับปริมาณ GET Requests ได้สูงสุดเฉลี่ยอยู่ที่ 173 Requests ต่อวินาที และปริมาณการใช้ CPU ของ Raspberry PI เพิ่มสูงขึ้นระหว่างที่เกิดการโจมตี การเข้าถึง Web Page ระหว่างการโจมตีเกือบทั้งหมดจะไม่สามารถเข้าถึงได้ หากครั้งไหนที่สามารถเข้าถึงได้จะมี Response Time ที่สูงจากปกติ การสั่งเปิดและปิดแอคชูเอเตอร์ LED ก็มี Response Time ที่สูงขึ้น การรับค่าอุณหภูมิและความชื้นจาก MQTT Broker มาแสดงบน Web Application ยังทำงานได้ การอ่านค่าอุณหภูมิและความชื้นของ DHT 22 ที่เชื่อมต่อกับบอร์ด ESP 8266 ยังทำงานได้ปกติ

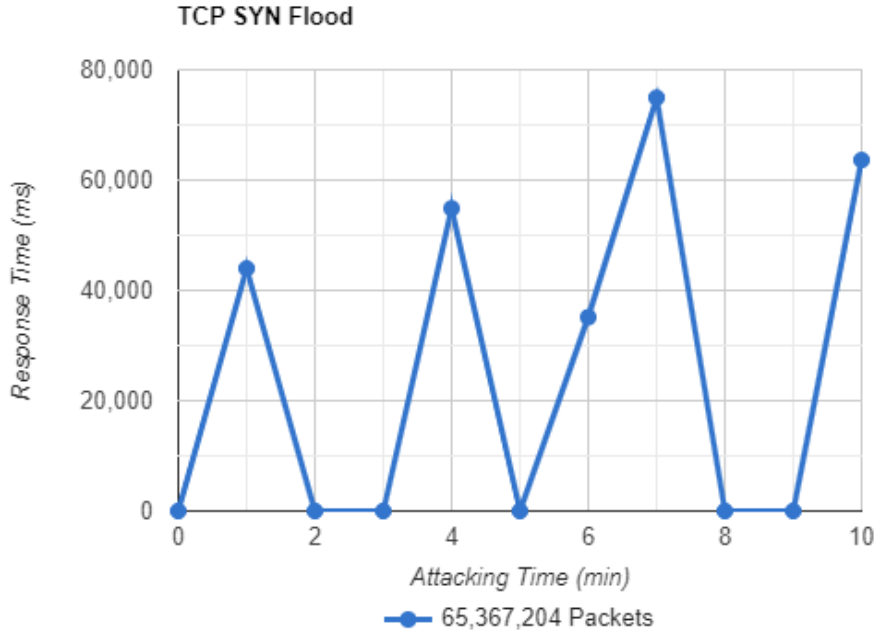


รูปที่ 2 กราฟแสดงปริมาณที่ Raspberry Pi สามารถประมวลผลได้และไม่ได้ เทียบกับปริมาณ Packet ทั้งที่โจมตี

TCP SYN Flood Attack

ทำการโจมตีเป็นระยะเวลา 10 นาที โดยสร้าง Packet ส่งไปโจมตีทั้งหมด 65,367,204 Packet โดยแต่ละ Packet มีขนาด 120 Bytes และ ปลอมหมายเลข IP Address ต้นทาง (Spoofing Source IP) ค่าเฉลี่ยการโจมตีอยู่ที่ 108,000 Packet ต่อ วินาที ระหว่างการโจมตีตลอด 10 นาที สามารถเรียก Web Application ได้เพียง 5 ครั้งจากทั้งหมด 10 ครั้ง การสั่งเปิดและปิดแอคชูเอเตอร์ LED มีเพียงครั้งเดียวที่สามารถสั่งเปิดได้โดยที่ไม่สามารถสั่งปิดได้ ครั้งอื่น ๆ ไม่สามารถสั่งเปิดและปิดแอคชูเอเตอร์ LED ได้ การแสดงค่าอุณหภูมิและความชื้นที่รับค่าจาก MQTT Broker บน Web Application สามารถทำได้เพียง 3 ครั้ง การทำงานของเซนเซอร์ DHT 22 ที่ไมโครคอนโทรลเลอร์ ESP 8266 ยังทำงานได้ปกติ

Raspberry Pi มีความสามารถในการกู้คืนตนเอง (Recovery) โดย Web Application กลับมาให้บริการได้หลังจากหยุดโจมตี 15-20วินาที แต่ไม่สามารถควบคุมสั่งการแอคชูเอเตอร์ LED ให้เปิดได้ ต้องทำการ Reboot ไมโครคอนโทรลเลอร์ ESP 8266

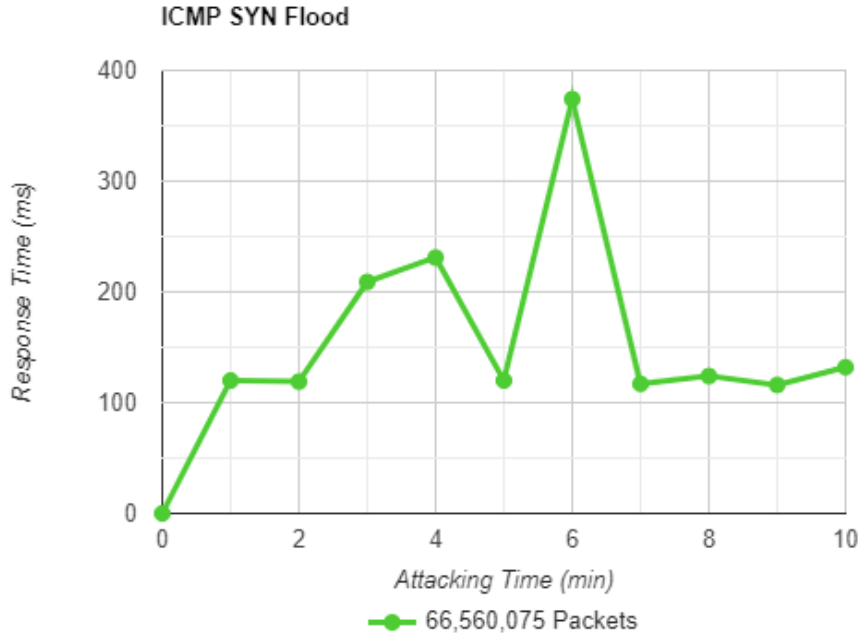


รูปที่ 3 กราฟแสดงระยะเวลาการตอบสนองของ Web Application เทียบต่อระยะเวลาการโจมตีแบบ TCP SYN Flood

ICMP Flood Attack

ทำการโจมตีเป็นระยะเวลา 10 นาทีโดยสร้าง Packet ไปโจมตีทั้งหมด 66,560,075 Packet โดยแต่ละ Packet มีขนาด 120 Bytes และปลอมหมายเลข IP Address ต้นทาง (Spoofing Source IP) ค่าเฉลี่ยการโจมตีอยู่ที่ 110,000 Packet ต่อ วินาที ระหว่างการโจมตีตลอดระยะเวลา 10 นาที การเข้าถึง Web Application สามารถทำได้ปกติ การสั่งการคำสั่งเปิดและปิดแอคชูเอเตอร์ LED สามารถทำได้ปกติ การรับค่าอุณหภูมิและความชื้นจาก MQTT Broker มาแสดงบน Web Application สามารถแสดงได้ปกติ เซนเซอร์ DHT22 ที่เชื่อมต่อกับไมโครคอนโทรลเลอร์ ESP 8266 สามารถทำงานได้ปกติ

Raspberry Pi มีความสามารถในการกู้คืนตนเอง (Recovery) ที่ค่า Resource ต่าง ๆ เช่น CPU และ Memory กลับมาทำงานปกติทันทีหลังการโจมตีสิ้นสุดลง

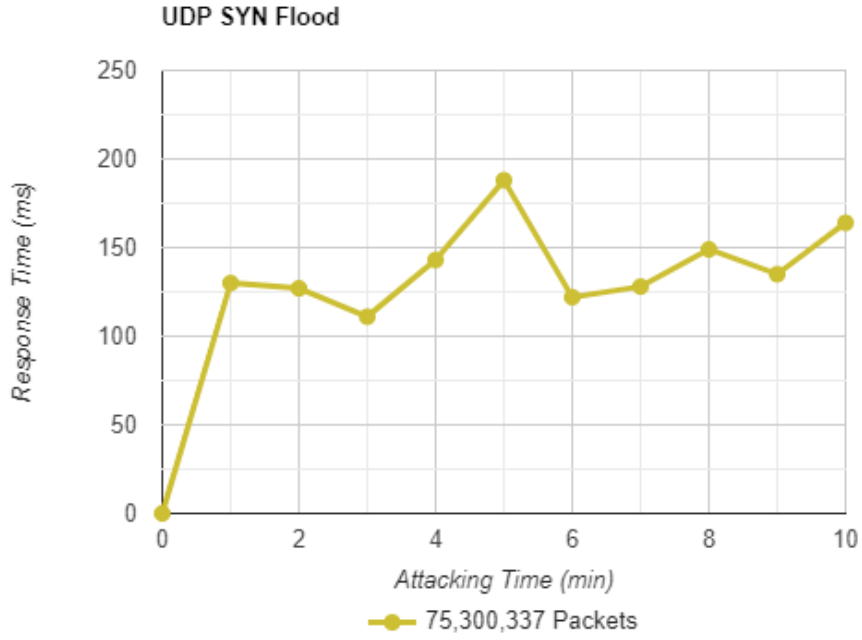


รูปที่ 4 กราฟแสดงระยะเวลาการตอบสนองของ Web Application เทียบต่อระยะเวลาการโจมตีแบบ ICMP SYN Flood

UDP Flood Attack

ทำการโจมตีเป็นระยะเวลา 10 นาทีโดยสร้าง Packet ไปโจมตีทั้งหมด 75,300,337 Packet โดยแต่ละ Packet มีขนาด 120 Bytes และ ปลอมหมายเลข IP Address ต้นทาง (Spoofing Source IP) ค่าเฉลี่ยการโจมตีอยู่ที่ 125,000 Packet ต่อ วินาที ระหว่างการโจมตีตลอดระยะเวลา 10 นาที การเข้าถึง Web Application สามารถทำได้ปกติ การสั่งการคำสั่งเปิดและปิดแอคชูเอเตอร์ LED สามารถทำได้ปกติ การรับค่าอุณหภูมิและความชื้นจาก MQTT Broker มาแสดงบน Web Application สามารถแสดงได้ปกติ เซนเซอร์ DHT22 ที่เชื่อมต่อกับไมโครคอนโทรลเลอร์ ESP 8266 สามารถทำงานได้ปกติ

Raspberry Pi มีความสามารถในการกู้คืนตนเอง (Recovery) ที่ค่า Resource ต่าง ๆ เช่น CPU และ Memory กลับมาทำงานปกติทันทีหลังการโจมตีสิ้นสุดลง



รูปที่ 5 กราฟแสดงระยะเวลาการตอบสนองของ Web Application เทียบต่อระยะเวลาการโจมตีแบบ UDP SYN Flood

สรุปผลการวิจัย

ระบบจำลองการทดสอบ IoT ในรูปแบบบ้านอัจฉริยะในงานวิจัยนี้แสดงให้เห็นถึงข้อจำกัดในด้านกำลังการประมวลของไมโครโพรเซสเซอร์ Raspberry Pi ที่นำมาประยุกต์ใช้ให้เป็นศูนย์ควบคุมกลาง (Control Center) และขีดจำกัดในด้านความมั่นคงปลอดภัย

HTTP GET Flood Attack

ไมโครโพรเซสเซอร์ Raspberry Pi มีข้อจำกัดด้านความสามารถประมวลผล GET Requests ได้เพียง 173 Requests ต่อวินาที และมีระยะเวลาการประมวลที่สูงขึ้น มีการใช้ปริมาณทรัพยากรในการประมวลที่สูงขึ้นแบบก้าวกระโดด มีอัตราการกู้คืนระบบด้วยตัวเองที่ใช้เวลาสูง

บทวิเคราะห์ HTTP GET Flood Attack

การโจมตีในรูปแบบ HTTP GET Flood Attack สามารถส่งผลกระทบกับการทำงานของระบบ IoT ได้อย่างชัดเจนหากปริมาณของ Packet GET Requests มีปริมาณที่สูงมากอาจทำให้ระบบ IoT ไม่สามารถให้บริการได้ ซึ่งจะส่งผลกระทบให้เกิดความเสียหายต่อผู้ใช้งาน โดย

แนวทางการป้องกันในการประยุกต์ใช้งานจริง หากเป็นระบบ IoT ที่ถูกใช้งานภายในองค์กรควรวางระบบ IoT ไว้ภายในเครือข่าย Intranet และมีใช้งาน Load Balance เพื่อช่วยจัดการกับปริมาณ Packet ที่มีจำนวนมาก หากเป็นการประยุกต์ใช้งานเองภายในครัวเรือน อาจเรียกใช้บริการ Commercial Cloud Services เพื่อให้มีทรัพยากรที่มากพอกับการจัดการปริมาณ Packet ที่มีจำนวนมาก

TCP SYN Flood Attack

ไมโครโพรเซสเซอร์ Raspberry Pi มีความสามารถให้บริการ Web Application ในขณะเกิดการโจมตีได้เพียง 50% และไม่มีความสามารถในการควบคุมการทำงาน หรือการรับค่าข้อมูลจากอุปกรณ์เซนเซอร์ ตลอดระยะเวลาการโจมตี มีการใช้ปริมาณทรัพยากรในการประมวลที่สูงขึ้นเป็นอย่างมากเมื่อเปรียบเทียบกับช่วงเวลาการทำงานแบบปกติ มีอัตราการกู้คืนระบบด้วยตัวเองที่ใช้เวลานาน และอาจจำเป็นต้องมีการ Reboot ตัวอุปกรณ์เพื่อให้เริ่มทำงานใหม่

บทวิเคราะห์ TCP SYN Flood Attack

การโจมตีในรูปแบบ TCP SYN Flood Attack สามารถส่งผลกระทบทำให้ระบบ IoT ไม่สามารถให้บริการได้อย่างชัดเจน รวมถึงไม่สามารถออกคำสั่งเพื่อควบคุมอุปกรณ์เซนเซอร์และแอคชูเอเคอร์ได้ ซึ่งเป็นผลกระทบที่ร้ายแรงต่อผู้ใช้งาน เพื่อให้ระบบ IoT สามารถรับมือหรือทนต่อการโจมตีในรูปแบบนี้ ต้องมีการประยุกต์นำ IPS (Intrusion Prevention System) เข้ามาใช้ร่วมกับระบบ IoT โดยออกแบบในลักษณะแยกกันเพื่อให้ IPS และ IoT มีทรัพยากรของตัวเองที่เพียงพอต่อการใช้งาน หรือเลือกใช้งาน Commercial Cloud Services เพื่อใช้บริการด้านความมั่นคงปลอดภัยจากผู้ให้บริการ

ICMP Flood Attack

ไมโครโพเซสเซอร์ Raspberry Pi มีความสามารถในการให้บริการ Web Application ที่ช้าลงกว่าช่วงเวลาปกติ และปริมารการใช้ CPU ของตัวอุปกรณ์มีแนวโน้มที่สูงขึ้นแต่ยังสามารถให้บริการการรับส่งข้อมูล หรือการควบคุมการสั่งการได้ มีอัตราการกู้คืนระบบด้วยตัวเองที่ค่อนข้างเร็ว

UDP Flood Attack

ไมโครโพเซสเซอร์ Raspberry Pi มีความสามารถในการให้บริการ Web Application ที่ช้าลงกว่าช่วงเวลาปกติ และปริมารการใช้ CPU ของตัวอุปกรณ์มีแนวโน้มที่สูงขึ้น แต่ยังสามารถให้บริการการรับส่งข้อมูล หรือการควบคุมการสั่งการได้ มีอัตราการกู้คืนระบบด้วยตัวเองที่ค่อนข้างเร็ว

บทวิเคราะห์ ICMP Flood Attack และ UDP Flood Attack

การโจมตีในรูปแบบทั้ง 2 นี้ไม่ค่อยส่งผลกระทบแบบเห็นได้ชัดกับการทำงานของระบบ IoT อาจเนื่องมาจาก ขนาดของ packet ที่ใช้ในการโจมตีของทั้ง 2 รูปแบบนี้มีขนาดเล็ก และระบบปฏิบัติการ Raspbian OS ของ Raspberry Pi มีการพัฒนาอย่างต่อเนื่องทำให้อาจมีการเตรียมการรองรับการใช้งาน Ping ที่มีประสิทธิภาพ และด้วยในปัจจุบันอุปกรณ์ที่เกี่ยวข้องกับเครือข่าย เช่น Routers มีปริมาณ Bandwidth ที่สูงมากหากภายในเครือข่ายมีอุปกรณ์ใช้งานที่ต่อพ่วงน้อย การโจมตีที่จะทำให้เกิด Overwhelming ใน Bandwidth ย่อมน้อยตามไปด้วย

สำหรับงานวิจัยต่อไปในอนาคต มีความเป็นไปได้ที่จะนำเอาความสามารถด้านความมั่นคงปลอดภัยเพิ่มเติม เช่น อุปกรณ์ IPS มาประยุกต์ร่วมใช้ภายในระบบ IoT แบบบ้านอัจฉริยะ (Smart Home) หรือการสร้างกฎของ Firewall ที่อุปกรณ์ไมโครโพรเซสเซอร์ Raspberry Pi เพื่อเพิ่มความมั่นคงปลอดภัยของระบบต่อไปได้

ข้อเสนอแนะ

ชุดคำสั่งที่ใช้สร้างการโจมตีในรูปแบบ HTTP GET Flood Attack, TCP SYN Flood Attack, ICMP Flood Attack และ UDP Flood Attack ภายในงานวิจัยนี้มีการกำหนดขนาดของ Packet ที่ 120 Byte เพื่อไม่ให้เกินกำลังการทำงานของอุปกรณ์ Packet Generator หากมีการปรับขนาดของ Packet ที่ใช้สำหรับการโจมตีให้มีขนาดที่ใหญ่ขึ้น อาจจะส่งผลกระทบที่รุนแรงกับระบบ IoT แบบบ้านอัจฉริยะ (Smart Home) ของงานวิจัยนี้ได้มากขึ้น

บรรณานุกรม

Da Yin. (2018). A DDoS Attack Detection and Mitigation with Software-Defined Internet of Things Framework College of Information Science and Engineering, Hunan Normal University, Changsha สืบค้นจาก IEEE. [4]

Hanan Mustapha. (2018). DDoS Attacks on the Internet of Things and their prevention methods School of Computing, Mathematics, & Digital Technology, Manchester Metropolitan University, UK ACM Digital Library. [5]

Krushang Sonar. (2014). A Survey: DDoS Attack on Internet of Things Gujarat Technology University, India, International Journal of Engineering Research and Development สืบค้นจาก Google Scholar. [1]

Ladislav Huraj. (2022). Resistance of IoT Sensors against DDoS Attack in Smart Home Environment Department of Applied Informatics, University of SS. Cyril and Methodius สืบค้นจาก Google Scholar. [2]

Tibor Horak. (2021). Vulnerability of Smart IoT-Based Automation and Control Devices to Cyber Attack Institute of Applied Informatics, Automation and Mechatronics, Faculty of Materials Science and Technology, Slovak University of Technology สืบค้นจาก Google Scholar. [3]