การตอบสนองการโจมตีแบบ DDoS ด้วยวิธีคงสภาพแบนด์วิดท์

DDoS Attack Response using Bandwidth Reservation

ประดิษฐ์ พิทักษ์เสถียรกุล[1*], ศิรปัฐช์ บุญครอง[2]

Pradit Pitaksathienkul[1*], Sirapat Boonkrong[2]

Received: 13 May 2016 ; Accepted: 23 September 2016

บทคัดย่อ

การโจมตีแบบกระจายเพื่อหยุดให้บริการ (DDoS) เป็นสาเหตุหนึ่งของเหตุการณ์ผิดปกติที่เกิดขึ้นในระบบเครือข่ายอินเทอร์เน็ต ซึ่งผลของการโจมตีเพื่อหยุดให้บริการนี้ ได้ก่อให้เกิดความเสียหายทางด้านเศรษฐกิจ ด้านสังคม และต่อผู้ใช้งาน โดยที่เครื่องที่ถูกโจมตีจะไม่สามารถให้บริการหรือประมวลผลใด ๆ ได้ งานวิจัยนี้จึงเสนอแนวทางในการตอบสนองการโจมตี เพื่อที่จะสามารถเป็นก้าวหนึ่งในการแก้ไขปัญหาจากการโจมตีนี้ ซึ่งจะใช้วิธีการอาศัยความร่วมมือของอุปกรณ์ในเครือข่าย โดยให้อุปกรณ์ในเครือข่ายจำกัดอัตราการส่งข้อมูลการโจมตีมายังเครื่องเป้าหมาย เพื่อให้เครื่องเป้าหมายสามารถรับส่งข้อมูลปกติต่อไปได้ จากผลการวิจัยนั้นปรากฏว่า แนวทางนี้สามารถคงสภาพการรับส่งข้อมูลปกติในเครื่องเป้าหมายจากการโจมตีประเภทนี้ได้

คำสำคัญ: การตอบสนองการโจมตี การคงสภาพแบนด์วิดท์

Abstract

Distributed Denial of Service (DDoS) is one of many threats that cause abnormality on the Internet. The attack can result in a lot of damage to the economy, society as well as to users in that the victim will not be able to provide services of process anything. This research, therefore, provides an approach to responsd to this type of attack, which will be a step towards a solution to the DDoS problem. The research proposes a method by using a cooperative between network devices that can be used in response to a DDoS attack. This response can maintain normal operation between legitimate devices. The result appears that this method can maintain bandwidth in trade for responding this type of attack.

Keywords: Attack Response, Bandwidth Reservation

บทนำ

การโจมตีแบบกระจายเพื่อหยุดให้บริการ (DDoS) เป็นการโจมตีที่สร้างปัญหาต่อประสิทธิภาพการใช้งานในระบบเครือข่าย ทำให้ผู้ใช้ไม่สามารถใช้งานระบบเครือข่ายได้ตามปกติ การโจมตี DDoS โดยอาศัยความจำกัดของทรัพยากร อย่างเช่น แบนด์วิดท์ (Bandwidth) หรือ หน่วยความจำ และ โดยอาศัยความเป็นระบบเปิดของระบบเครือข่าย จากการสำรวจข้อมูล พบว่าการโจมตีด้วยวิธีการส่งข้อมูลจำนวนมากมายังเครื่องเป้าหมายอย่างต่อเนื่อง ทำให้เครื่องเป้าหมายได้รับข้อมูลจำนวนมากอย่างรวดเร็วในระยะเวลาอันสั้น เป็นสาเหตุให้แบนด์วิดท์ของระบบเครือข่ายหมดไป เกิดปัญหาคอขวด และ เครื่องเป้าหมายไม่สามารถส่งข้อมูลปกติได้ต่อไป เครื่องโจมตีสามารถส่งข้อมูลจำนวนมาก ด้วยโพรโทคอล ICMP UDP หรือ TCP ก็ได้ ซึ่งเป็นการโจมตีที่สามารถกระทำได้โดยง่าย แต่ป้องกันได้ยาก[1]

จากปัญหาดังกล่าว ในงานวิจัยนี้ จึงนำเสนอวิธีคงสภาพแบนด์วิดท์ สำหรับตอบสนองการโจมตีแบบ DDoS คือ

---

[1] *นักศึกษาระดับปริญญาเอก,* [2]*รองศาสตราจารย์, คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ 10800*

[1] *Doctoral student,* [2]*Associate Professor, Department Of Information Technology, King Mongkut's University Of Technology North Bangkok 10800*

[*] *Corresponding author, Pradit Pitaksathienkul, Department Of Information Technology, King Mongkut's University Of Technology North Bangkok 10800, Thailand*

เมื่อเครื่องเป้าหมายตรวจพบการโจมตีเกิดขึ้น จะทำการส่งข้อมูลไปยังอุปกรณ์เครือข่ายที่อยู่ใกล้เคียง เพื่อจำกัดการส่งข้อมูลโจมตี ก่อนที่เครื่องเป้าหมายจะไม่สามารถส่งข้อมูลปกติออกไปได้ ซึ่งเป็นวิธีการที่ Ioannidis และ Bellovin[12] ได้นำเสนอ วิธีการนี้ ไม่ได้หยุดการโจมตี แต่ทำให้เครื่องเป้าหมายยังสามารถใช้งานเครื่อข่ายได้ตามปกติ เนื่องจากการหยุดการโจมตีที่เครื่องต้นทาง เป็นเรื่องที่ทำได้ยาก

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

1. การโจมตีด้วยการส่งข้อมูลจำนวนมาก

การโจมตีด้วยวิธีการนี้ อาจใช้วิธีการหลอกให้คอมพิวเตอร์ในระบบเครือข่าย (ที่อยู่ในลำดับเหนือเครื่องเป้าหมาย) ซึ่งมีอยู่จำนวนมาก ถูกติดตั้งโปรแกรมควบคุมด้วยวิธีการบางอย่างโดยผู้ใช้ไม่ทราบ เช่น โปรแกรมสคริปต์ บนเว็บเพจ เพื่อควบคุมให้คอมพิวเตอร์เหล่านั้น ให้ส่งข้อมูลแพ็กเก็ตโจมตีเมื่อถึงกำหนดเวลาที่ต้องการ คอมพิวเตอร์ที่ถูกควบคุมเหล่านี้ก็ทำการส่งข้อมูลแพ็กเก็ตโจมตีพร้อมๆกัน ไปยังเครื่องเป้าหมาย เพื่อทำให้แบนด์วิดท์ของระบบเครือข่ายหมดไป โดยทั่วไปการโจมตีด้วยวิธีการส่งข้อมูลจำนวนมาก จึงเป็นการโจมตีแบบ DDoS ดัง Figure 1

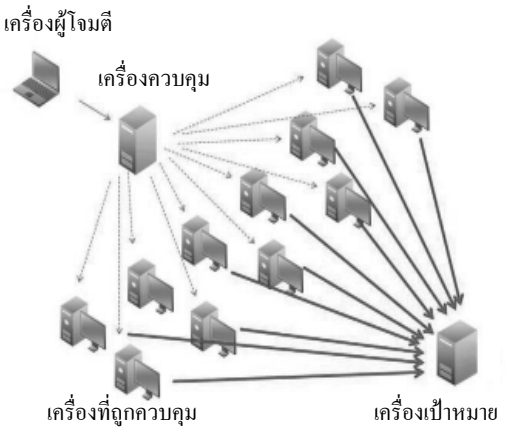


Figure 1 The DDoS attack by sending a large amount of data

2. การตอบสนองการโจมตี

การตอบสนองการโจมตี เป็นวิธีการที่เครื่องเป้าหมายกระทำต่อการโจมตีนั้น เพื่อรักษาสภาพการใช้งานให้คงอยู่ต่อไปได้ ซึ่งมีด้วยกัน 3 วิธี คือ

2.1 การตอบสนองการโจมตี โดยดำเนินการบนอุปกรณ์ที่อยู่ใกล้เครื่องโจมตี (Source based)

Mirkovic และคณะ[3] ทำการวิจัยโดยกำหนดการตอบสนองบนอุปกรณ์ Router ที่อยู่ติดกับเครื่องโจมตี พบว่า การตอบสนองโดยใช้อุปกรณ์ที่อยู่ใกล้เครื่องโจมตีมากที่สุด จะช่วยลดปริมาณข้อมูลโจมตีที่ถูกส่งมายังเครื่องเป้าหมายได้ เพราะยังไม่ถูกส่งมายังเครื่องเป้าหมาย ช่วยลดความเสี่ยงที่เครื่องเป้าหมายจะหยุดทำงาน แต่ปัญหาหลักคือ ในการโจมตีแบบกระจายนั้น ผู้โจมตีอาศัยเครื่องโจมตีจำนวนมาก การตอบสนองบนอุปกรณ์ที่อยู่ใกล้เครื่องโจมตี ไม่สามารถดำเนินการให้ครอบคลุมได้ และ ด้วยปริมาณข้อมูลที่อยู่ใกล้เครื่องโจมตีมีไม่มากพอ ทำให้ไม่สามารถแยกได้ว่า เป็นข้อมูลการโจมตีหรือ ข้อมูลปกติ

2.2 การตอบสนองการโจมตี โดยดำเนินการบนอุปกรณ์ที่อยู่ใกล้เครื่องที่ถูกโจมตี (Victim based) เช่น การตั้งข้อกำหนดบนอุปกรณ์ป้องกันการโจมตี เช่น Firewall โดยทำการจำกัดการเข้าถึงจากเครื่องโจมตี (Access List Control)[13] โดยการตรวจสอบว่า การโจมตีนั้น เกิดจากเครื่องโจมตีใดในเครือข่าย แล้วนำที่อยู่ของเครื่องโจมตี มาทำการกำหนดในรายการจำกัดการเข้าถึง เป็นวิธีที่ทำได้ง่ายและตอบสนองการโจมตีได้แม่นยำ เพราะดำเนินการใกล้กับเครื่องที่ถูกโจมตี แต่มีข้อจำกัดคือ อุปกรณ์ Firewall จะต้องมีขนาดใหญ่ เพื่อประมวลผลข้อมูลจราจรที่ไหลผ่านจำนวนมาก

จากวิธีการตอบสนองการโจมตีทั้ง 2 วิธี ดังกล่าวที่เป็นอุปกรณ์ระบบเดียวนั้น มีข้อจำกัดคือ การตอบสนองที่ไม่ครอบคลุม และ ต้องใช้อุปกรณ์ที่มีประสิทธิภาพสูง จึงมีวิธีการตอบสนอง โดยใช้ความร่วมมือกันของอุปกรณ์ในเครือข่าย เพื่อให้ได้การตอบสนองการโจมตีที่มีประสิทธิภาพ[14] ซึ่งทำการตรวจจับการโจมตีบนเครื่องเป้าหมาย เมื่อมีการโจมตีเกิดขึ้น

2.3 การตอบสนองการโจมตี แบบคงสภาพแบนด์วิดท์ Ioannidis และ Bellovin[12] ทำการวิจัยโดยใช้วิธี Pushback เมื่อตรวจพบการโจมตีเกิดขึ้น เครื่องเป้าหมายจะส่งข้อมูลสื่อสารไปยังอุปกรณ์ Router ที่อยู่ติดกัน เพื่อให้ทำการลดอัตราการส่งผ่านข้อมูล โดยปรับอัตราการเข้าออกของข้อมูลใน Queue ของอุปกรณ์ Router และทำเช่นนี้ย้อนกลับไปจนถึงเครื่องโจมตี วิธีการนี้มีข้อจำกัดคือ เป็นการเพิ่มภาระให้กับอุปกรณ์ Router ในการจัดการข้อมูลแพ็กเก็ตใน Queue

จากการศึกษาการตอบสนองการโจมตีที่กล่าวมาทั้ง 3 ประเภท พบว่า สิ่งที่ต้องการในการตอบสนองการโจมตีคือ การที่เครื่องเป้าหมายยังคงสามารถรับส่งข้อมูลปกติต่อไปได้ ขณะที่มีการโจมตีเกิดขึ้น ซึ่งในงานวิจัยนี้ เลือกใช้วิธีการตรวจจับการโจมตีบนเครื่องเป้าหมาย ตามงานวิจัยของ ประดิษฐ์ และ ศิรปัฐช์[7] ซึ่งสามารถคำนวณได้อย่างรวดเร็ว โดยพิจารณาอัตราการเปลี่ยนแปลงของการส่งข้อมูลแพ็กเก็ต

ปกติของเครื่องเป้าหมาย และ ใช้วิธีการตอบสนองการโจมตีโดยใช้ความร่วมมือกันของอุปกรณ์ในเครือข่าย เพื่อให้เครื่องเป้าหมายสามารถรับส่งข้อมูลปกติต่อไปได้

วิธีดำเนินการวิจัย

การตอบสนองการโจมตีแบบ DDoS ด้วยวิธีการอาศัยความร่วมมือของอุปกรณ์ในเครือข่าย จะกระทำภายหลังจากมีการตรวจจับการโจมตีเกิดขึ้น โดยจะทำการทดลองดังต่อไปนี้

การทดลองในงานวิจัยนี้ จะเป็นสร้างแบบจำลองเครือข่าย ด้วยโปรแกรม NS2 version 2.35 สร้างการโจมตีจากโหนดในระบบเครือข่าย จำนวน 100 โหนด ใช้เวลาในการทดลอง 80 วินาที เครื่องเป้าหมายทำการส่งข้อมูลปกติตั้งแต่วินาทีที่ 10 และ การโจมตีเกิดขึ้นตั้งแต่วินาทีที่ 30 ทำการวัดค่าทรูพุธ ที่เครื่องเป้าหมาย เพื่อคำนวณค่าเฉลี่ยของการส่งข้อมูลปกติ ก่อนเกิดการโจมตี และ คำนวณส่วนเบี่ยงเบนมาตรฐาน การทดลองนี้ใช้วิธีจำลองเครือข่ายแบบ transit-stub[10] ด้วย Waxman algorithm[11] เชื่อมต่อแต่ละโหนดเข้าด้วยกันเป็นการจำลองเครือข่ายที่ใกล้เคียงระบบเครือข่ายที่มีการใช้งานจริง ในแต่ละ link มีการรับส่งข้อมูลแบบ full duplex รองรับแบนด์วิดท์ที่ 1 Mbit/s มีการกำหนด queue ด้วยวิธีการ droptail โปรแกรมทำงานบนคอมพิวเตอร์ CPU Intel Core2 Duo 2.28 GHz ระบบปฏิบัติการ Ubuntu version 12.04 จำนวนโหนดที่ใช้ กำหนดไว้ใน Table 1

Table 1 Nodes using in Model

โหนดสำหรับการทดลอง	จำนวน
จำนวนโหนดทั้งหมด	200 โหนด
จำนวนโหนดที่ส่งแพ็กเก็ตโจมตี	100 โหนด
จำนวนโหนดเป้าหมาย	1 โหนด
จำนวนโหนดในเส้นทางปกติ	5 โหนด
จำนวน Router node	50 โหนด

ทำการทดลองรับส่งข้อมูล ตามภาพแบบจำลองที่ได้สร้างขึ้น ดัง Figure 2

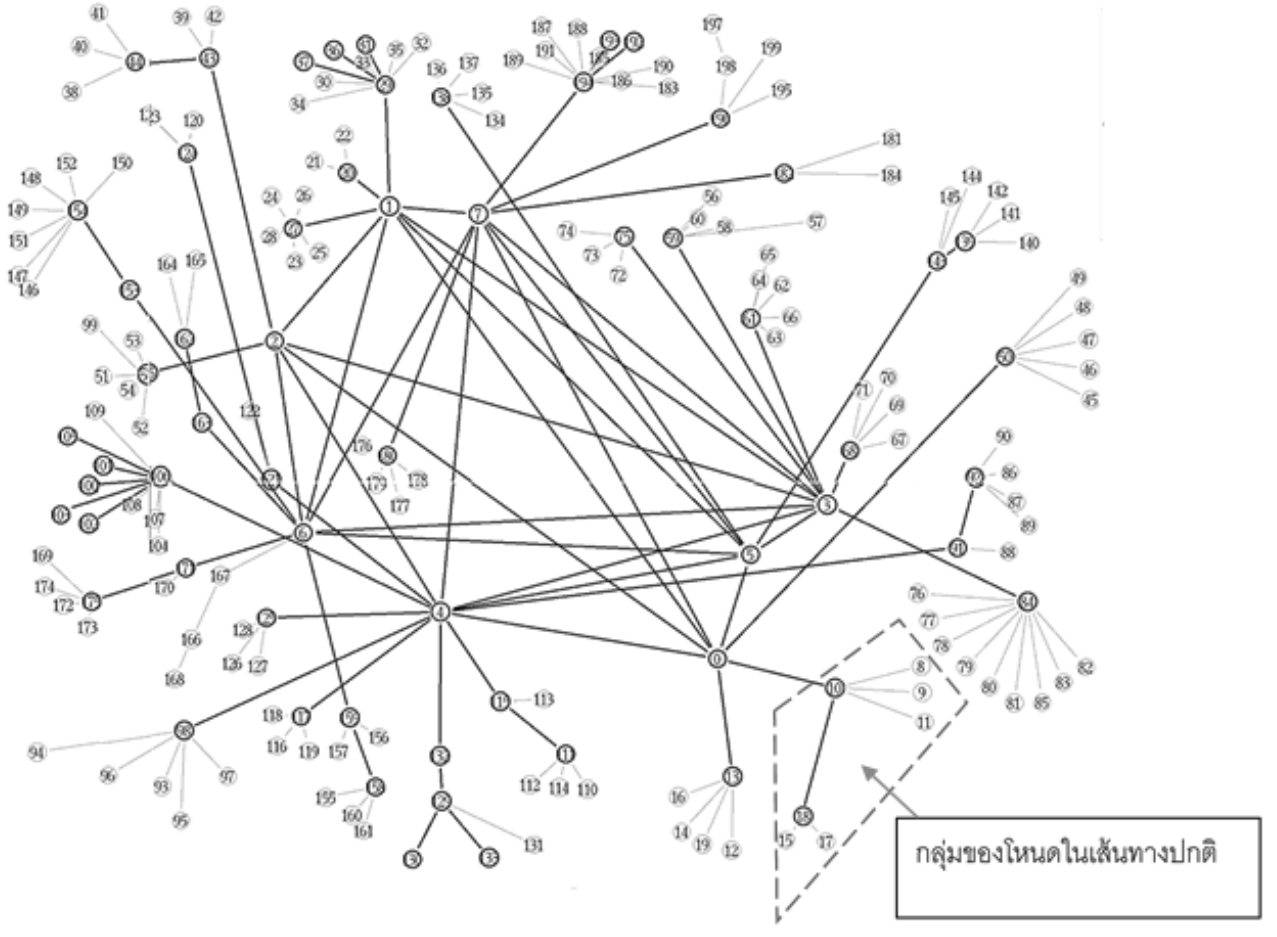


Figure 2 The model of the network used in this research

1. ออกแบบการทดลองขณะยังไม่มีการโจมตี

ขั้นตอนแรก ทำการกำหนดเครื่องที่เป็นเป้าหมายของการโจมตี ทำการส่งข้อมูลแพ็กเก็ตปกติจำนวน 1 โหนด มีการส่งข้อมูลแบบ udp และ tcp จากโหนดที่อยู่ข้างเคียงไปยังเครื่องอื่นในเครือข่าย ขนาดของแพ็กเก็ต เป็น 100 bytes ด้วยอัตราการส่งถ่ายข้อมูล 200,000 แพ็กเก็ต ต่อวินาที ตามลำดับ เริ่มจากวินาทีที่ 10 ถึงวินาทีที่ 80 ทำการจับเวลา ณ โหนดที่รับข้อมูล ทุก 0.5 วินาที เพื่อคำนวณแบนด์วิดท์

2. ออกแบบการทดลองขณะมีการโจมตี

ขั้นตอนที่สอง ที่เวลา 30 วินาที กำหนดให้เริ่มมีการโจมตี จากกลุ่มของโหนดที่วงกลมไว้ ใช้โหนดการโจมตีจำนวน 100 โหนด ซึ่งทำให้เครื่องเป้าหมายแทบจะไม่สามารถส่งข้อมูลปกติไปยังโหนดข้างเคียงได้ (เข้าใกล้ 0)

ในการโจมตีนั้น กำหนดให้แต่ละโหนดโจมตีมีการส่งข้อมูล ชนิด udp ด้วยขนาดของแพ็กเก็ต เป็น 100 bytes ด้วยอัตราการส่งถ่ายข้อมูล 50,0000 แพ็กเก็ตต่อวินาที ตามลำดับ

ทำการคำนวณค่าแบนด์วิดท์ ทั้งที่เป็นแบนด์วิดท์ของการส่งข้อมูลปกติ และ แบนด์วิดท์ของการส่งข้อมูลโจมตีที่เครื่องเป้าหมาย ขณะเกิดการโจมตี

3. ค่าเทรชโฮลด์ของการทดลอง

ขั้นตอนที่สาม ก่อนที่จะทำการโจมตี ทำการคำนวณค่าเฉลี่ยของการส่งข้อมูลแพ็กเก็ตปกติ และ ค่าส่วนเบี่ยงเบนมาตรฐาน การคำนวณหาค่าเทรชโฮลด์ ซึ่งเป็นค่าที่ใช้ตรวจสอบว่าเกิดการโจมตี โดยใช้ค่าเทรชโฮลด์ในการติดต่อสื่อสารกับอุปกรณ์เครือข่ายเพื่อจำกัดการส่งข้อมูลมายังเครื่องเป้าหมาย ก่อนที่เครื่องเป้าหมายจะไม่สามารถรับส่งข้อมูลต่อไปได้ ในการวิจัยนี้ ใช้ค่าเทรชโฮลด์จากการวิจัยของประดิษฐ์ และ ศิรปัฐช์[7]

4. ออกแบบการทำงานร่วมกันของอุปกรณ์ในเครือข่าย

เมื่อมีการโจมตีเกิดขึ้น เครื่องเป้าหมายจะทำการติดต่อกับอุปกรณ์ Router ที่อยู่ติดกัน เพื่อขอให้ลดการส่งข้อมูล เส้นทางการโจมตีแสดงด้วยเส้นทึบ ข้อมูลสื่อสารแสดงด้วยเส้นประ เมื่ออุปกรณ์ Router ได้รับการติดต่อ ก็จะทำการควบคุมแบนด์วิดท์ ด้วยค่าเทรชโฮลด์ที่ได้คำนวณไว้ ดัง Figure 3

เมื่ออุปกรณ์ Router ที่อยู่ติดกับเครื่องเป้าหมายทำการควบคุมแบนด์วิดท์ ก็จะส่งข้อมูลสื่อสารไปยังอุปกรณ์ Router ที่อยู่ถัดไป เพื่อขอให้ลดการส่งข้อมูลตามเส้นทางการโจมตี ขณะเดียวกัน อุปกรณ์ Router ที่อยู่ติดกับเครื่องเป้าหมาย จะกลับมาส่งข้อมูลด้วยอัตราปกติ เพื่อให้เครื่องเป้าหมายสามารถรับส่งข้อมูลปกติต่อไปได้ ดัง Figure 4

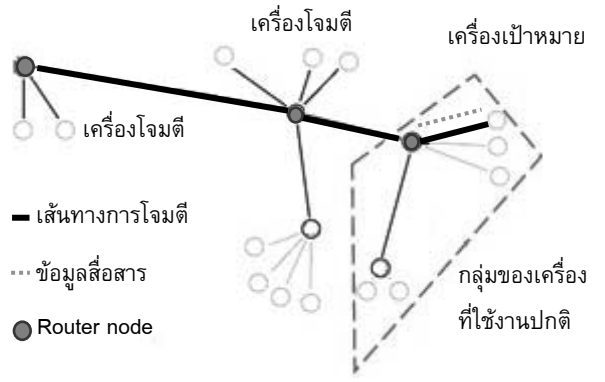


Figure 3 The victim sends information to the Router adjacent to reduce the data rate

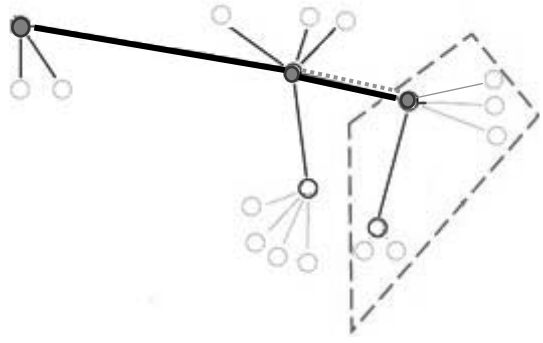


Figure 4 The Routers on the attack path contact between them to reduce the data rate

กระบวนการนี้ จะดำเนินไปจนกระทั่งถึงอุปกรณ์ Router ที่อยู่ติดกับเครื่องโจมตี ดัง Figure 5

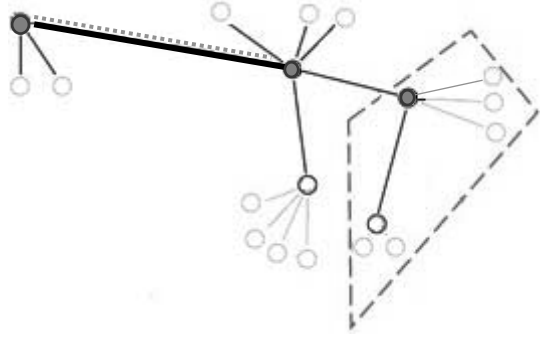


Figure 5 The process respond to an attack action until the equipment Router adjacent source attack

5. การหาเส้นทางย้อนกลับไปยังเครื่องโจมตี

ในการสร้างแบบจำลองระบบเครือข่ายนั้น โปรแกรม NS2 ได้จัดทำข้อมูลเส้นทางการเชื่อมต่อของแต่ละโหนด (Routing Table) สำหรับค้นหาเส้นทางการเชื่อมต่อกันระหว่าง

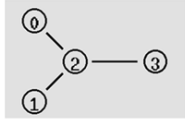
โหนดไว้ด้วย

ข้อมูล Routing Table จะถูกเก็บในรูปแบบ Adjacency Matrix ในอะเรย์ 2 มิติ มีขนาดเท่ากับ O (จำนวนโหนด^2) โดยเป็นข้อมูลเส้นทางการเชื่อมต่อของทุกโหนดในเครือข่าย ดัง Figure 6

	โหนดปลายทาง	โหนดปลายทาง	โหนดปลายทาง	...
โหนดต้นทาง	โหนดถัดไป	โหนดถัดไป	โหนดถัดไป	
โหนดต้นทาง	โหนดถัดไป	โหนดถัดไป	โหนดถัดไป	
โหนดต้นทาง	โหนดถัดไป	โหนดถัดไป	โหนดถัดไป	
...				

Figure 6 Attributes of Routing Table

ตัวอย่าง Routing Table ของแบบจำลอง ดัง Figure 7



คำสั่งสำหรับนำข้อมูล Routing Table ออกจากระบบ

```
$ns rtproto Static
$ns compute-routes
$ns get-routelogic
$ns dump-routelogic-nh
```

ผลลัพธ์ที่ได้เป็น Routing Table ของทั้งแบบจำลอง ในรูปแบบ Adjacency Matrix ของกราฟ

```
Routing table
Dumping Routing Table: Next Hop Information
     0    1    2    3
0    --   2    2    2
1    2    --   2    2
2    0    1    --   3
3    2    2    2    --
```

Figure 7 Example of Routing Table

ในแบบจำลองเครือข่ายที่สร้าง ใช้ OSPF Protocol ในการจัดทำข้อมูล Routing Table สำหรับแต่ละโหนด เพื่อใช้ในการหาเส้นทางสำหรับการส่งข้อมูลในเครือข่าย

ตัวอย่างคำสั่งในการทำ OSPF ใน NS2

```
Agent/rtProto/OSPF set helloInterval 1
Agent/rtProto/OSPF set routerDeadInterval 4
$ns rtproto OSPF
```

6. ออกแบบข้อมูลสื่อสาร

เป็นข้อมูลสื่อสารที่เครื่องเป้าหมายใช้ในการติดต่อกับ Router Node เพื่อร้องขอให้ทำการจำกัดข้อมูลที่ส่ง และเป็นข้อมูลสื่อสารระหว่าง Router Node ที่อยู่ในเส้นทางการโจมตี โดยส่งค่าเทรชโฮลด์ ที่คำนวณได้จากการตรวจจับการโจมตี ด้วยการสร้าง packet ในรูปแบบของ IP Datagram และเพื่อความปลอดภัยของการสื่อสาร จึงนำข้อมูลที่ส่ง ไปผ่าน Hash Function และ ทำการ Encryption ด้วย CESAR Cipher กำหนด key=3 ดัง Figure 8

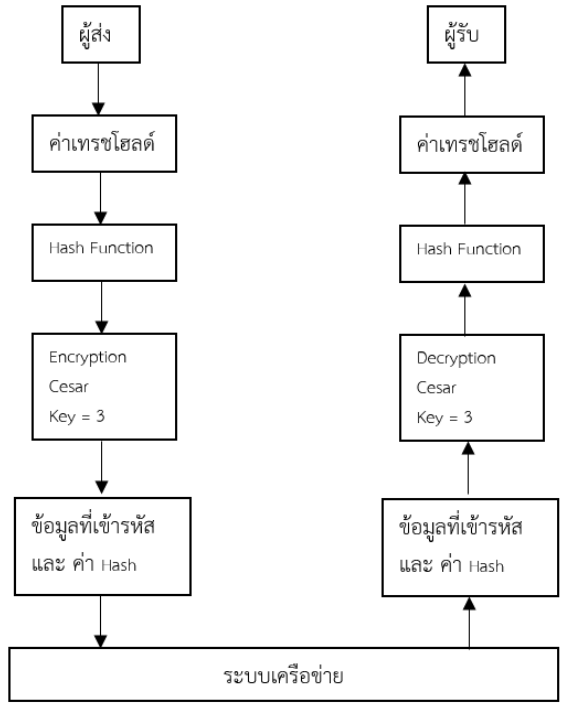


Figure 8 Step of Encryption and Decryption

เมื่อผู้รับได้รับข้อมูลสื่อสาร จะทำการถอดรหัสด้วย CESAR Cipher โดยใช้ key=3 จะได้ข้อมูลค่าเทรชโฮลด์ และค่า Hash ที่ถูกส่งมาด้วย

จากนั้นนำข้อมูลที่ผ่านการถอดรหัสแล้ว ไปคำนวณเพื่อหาค่า Hash แล้วนำค่า Hash ที่คำนวณได้ มาเปรียบเทียบกับ ค่า Hash ที่ถูกส่งมากับข้อมูล

หากค่า Hash มีค่าเท่ากัน แสดงว่า ข้อมูลสื่อสารนั้นถูกต้อง ไม่ได้ถูกแก้ไขระหว่างทาง

ผลการวิจัย

จากการออกแบบ แบบจำลองเครือข่าย เริ่มต้นจากการที่ยังไม่เกิดการโจมตี ทำการส่งข้อมูลแพ็กเก็ตโจมตีจากโหนดที่กำหนดให้ เมื่อเวลาวินาทีที่ 30 มายังเครื่องเป้าหมาย ทำการวัดปริมาณข้อมูลที่เครื่องเป้าหมาย เมื่อปริมาณข้อมูลแพ็กเก็ตโจมตีมากถึงระดับหนึ่ง จะทำให้ข้อมูลแพ็กเก็ตปกติของเครื่องเป้าหมาย สามารถส่งออกมาได้น้อยลง การตรวจจับการโจมตี กระทำที่เครื่องเป้าหมาย ดัง Figure 9

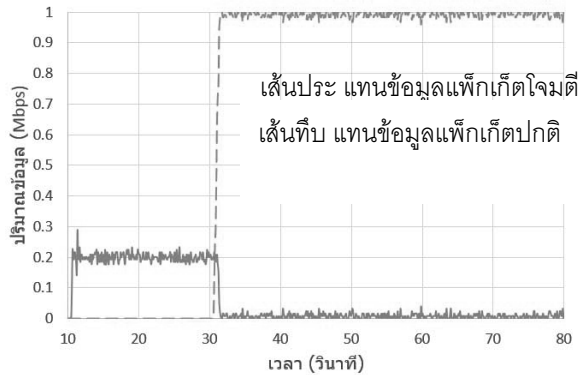


Figure 9 Characteristic of Attack and Normal packet before responding

ทำกระบวนการตอบสนองการโจมตี โดยเครื่องเป้าหมายติดต่อกับ Router node ที่อยู่ติดกับเครื่องเป้าหมาย เพื่อจำกัดแบนด์วิดท์ Router node ทำการติดต่อกับ Router node ที่อยู่ถัดขึ้นไป ทำการจำกัดแบนด์วิดท์ Router node ที่อยู่ติดกับเครื่องเป้าหมายปรับแบนด์วิดท์เป็นอัตราปกติ ทำให้เครื่องเป้าหมายสามารถรับส่งข้อมูลเป็นปกติได้กระทำย้อนไปตามเส้นทางโจมตี จนถึงเครื่องโจมตี ดัง Figure 10

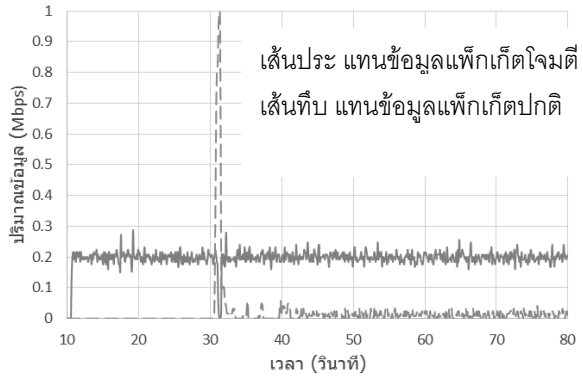


Figure 10 Characteristic of Attack and Normal packet after responding

ทำการเปรียบเทียบแบนด์วิดท์ของข้อมูลปกติ ขณะทำการตอบสนองการโจมตี ด้วยการคงสภาพแบนด์วิดท์ กับแบนด์วิดท์ของข้อมูลปกติก่อนการโจมตี และ ทำการเปรียบเทียบการแบนด์วิดท์ของข้อมูลปกติ ที่ไม่มีการตอบสนองการโจมตี

ผลลัพธ์ที่ได้ แสดงให้เห็นว่า การตอบสนองการโจมตีแบบคงสภาพแบนด์วิดท์ สามารถทำให้เครื่องเป้าหมาย ยังคงรักษาสภาพการรับส่งข้อมูลปกติได้ใกล้เคียงกับ แบนด์วิดท์ของข้อมูลปกติก่อนการโจมตี ดัง Figure 11

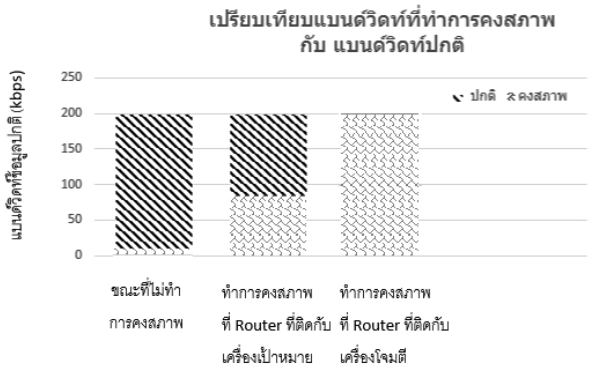


Figure 11 Efficiency of Responsding method compare with normal packet

สรุปผลการวิจัย

การตอบสนองการโจมตีแบบ DDoS ด้วยวิธีคงสภาพแบนด์วิดท์ เป็นส่วนหนึ่งในการทำให้ เครื่องเป้าหมายที่ถูกโจมตี ยังคงสามารถรับส่งข้อมูลปกติต่อไปได้ ในขณะที่มีการโจมตีเกิดขึ้น ซึ่งมีหลายแนวทาง เช่น การตอบสนองที่เครื่องผู้โจมตี การตอบสนองที่เครื่องเป้าหมาย และ การตอบสนองโดยอาศัยอุปกรณ์ในเครือข่าย วิธีการนี้ เป็นการสกัดกั้นข้อมูลโจมตีไม่ให้ส่งมาถึงยังเครื่องเป้าหมายได้ ผลปรากฏว่าสามารถทำให้เครื่องเป้าหมาย สามารถรับส่งข้อมูลปกติได้ 98% เปรียบเทียบกับข้อมูลปกติก่อนเกิดการโจมตี

การตอบสนองการโจมตีแบบ DDoS ด้วยวิธีคงสภาพแบนด์วิดท์ น่าจะเป็นแนวทางหนึ่งในการรักษาสภาพการใช้งานในเครือข่าย แต่ควรได้รับการศึกษาวิจัยในปัจจัยอื่นที่เกี่ยวข้องเพิ่มเติม

เอกสารอ้างอิง

1. Gupta D, Grover A, Bhandari. “Detection Techniques Against DDoS Attacks: A Comprehensive Review”. International Journal of Computer Applications; 2014. pp.49-57.
2. Kumar S, “A Pattern matching model for misuse instrusion detection”. In Proceeding of the 17th National Computer Security Conference,1994. pp. 11 – 21.
3. Mirkovic J, Reiher P, Prier G, “A Source Router Approach to DDoS Defense”. Usenix Security Symposium 2001 Work In Progress Session; 2001, pp. 1 – 16.
4. Blazek R B et al, “A Novel Approach to Detection of ‘Denial-of-Service’ Attacks via Adaptive Sequential

and Batch-Sequential Change-Point Detection Methods". In Proceeding of IEEE Workshop Information Assurance and Security; 2001, pp. 220 – 226

5. Fang-Yie L, I-Long L, "A DoS/DDoS Attacks Detecting System Using Chi-Square Statistic Approach". Systemics, Cybernetics&Informatics, Vol. 8 Issue 2, p41 – 51, 2010.
6. Mirkovic J, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms". ACM SIGCOMM Computer Communications Review, vol.34 no.2; 2004, pp. 39 – 53
7. ประดิษฐ์ พิทักษ์เสถียรกุล และ ศิรปัฐช์ บุญครอง, การตรวจจับการโจมตีแบบ DDoS ด้วยวิธีการกำหนดค่าเธรชโฮลด์. วารสารวิทยาศาสตร์และเทคโนโลยี ราชมงคลธัญบุรี 2559; 6[2]: หน้า 153-163.
9. J. Mirkovic, M. Robinson,P. Reiher, G. Oikonomou, "Distributed Defense Against DDoS Attacks", University of Delaware.2005; pp. 1 – 12,
10. Zegura E W, Calvert K L, Acharjee S B, "How to model an internetwork", INFOCOM '96.Fifteenth Annual Joint Conference of the IEEE Computer Societies. Networking the Next Generation. 1996. vol.2 , pp. 594 - 602.
11. Waxman, "Routing of multipoint connections", IEEE Journal on Selected Areas in Communications.1988. vol. 6, no. 9, pp.1617–1622.
12. Ioannidis J, Bellovin S.M. "Implementing Pushback: Router-Based Defense Against DDoS Attacks", In Proceeding of Internet Society Symposium on Network and Distributed System Security;2002. p.1-12.
13. Cisco. "Strategies to protect against distributed denial of service attacks.[online]. 2008; http://www.cisco.com/warp/public/707/newsflash.html
14. Mirkovic J, Robinson M, Reiher P, "Alliance Formation fro DDoS Defense", In Proceeding of NSPW'03 workshop on New security paradigms;2003. p. 11-18.