การพัฒนาการตรวจจับและสกัดกั้นแอพพลิเคชั่นบนระบบเครือข่าย
Development of Detective and Interception Application on Networks

วีระยุทธ คุณรัตนสิริ

สาขาวิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
weerayuth.k@rmutp.ac.th

บทคัดย่อ

ระบบสกัดกั้นข้อมูลบนระบบเครือข่าย มีชื่อเรียกอีกอย่างหนึ่งว่า ไฟร์วอลล์ ทำหน้าที่ควบคุมกฎในแลกเปลี่ยนข้อมูลบนระบบเครือข่าย ระบบเครือข่ายที่ไม่มีไฟร์วอลล์มีความเสี่ยงต่อการถูกคุกคาม งานวิจัยนี้นำเสนอการพัฒนาไฟร์วอลล์ เพื่อทำหน้าที่ตรวจจับแอพพลิเคชั่นเพียร์ทูเพียร์ ซึ่งเป็นแอพพลิเคชั่นที่มีการใช้งานแบนด์วิดท์เป็นจำนวนมาก ซึ่งระบบทำการตรวจจับและคัดแยกหมายเลขไอพีของผู้ใช้งานตามคลาสของแบนด์วิดท์ที่ได้จัดเตรียมไว้ การคัดแยกไอพีของผู้ใช้งานแอพพลิเคชั่นเพียร์ทูเพียร์ ทำให้ผู้ใช้งานแอพพลิเคชั่นอื่น ๆ สามารถใช้งานได้ปกติ ผลการทดลองพบว่าระบบสามารถสกัดกั้นแอพพลิเคชั่นที่ไม่ต้องการและจำกัดแบนด์วิดท์ที่เกิดจากการใช้งานเพียร์ทูเพียร์ได้

คำสำคัญ: ไฟร์วอลล์ การจำกัดข้อมูลจราจร ข้อมูลการจราจรของเพียร์ทูเพียร์

Abstract

Interception system on the network is known as a firewall. A firewall controls the rules on exchange of information on the network. The network system that do not have the firewall are vulnerable to threats. This paper presents the development of a firewall to detect the peer-to-peer application. The peer-to-peer(P2P) is an application that use a lot of bandwidth. This system detects and extracts the IP address of the user based on the class of bandwidth to be prepared. According to the extraction IP address of the peer-to-peer applications, the other applications can use the resource on the network system. The results showed that the system can block the application and limit the bandwidth that use the peer to peer applications.

Keyword: Firewall, Traffic shaper, Peer-to-peer traffic.

1. บทนำ

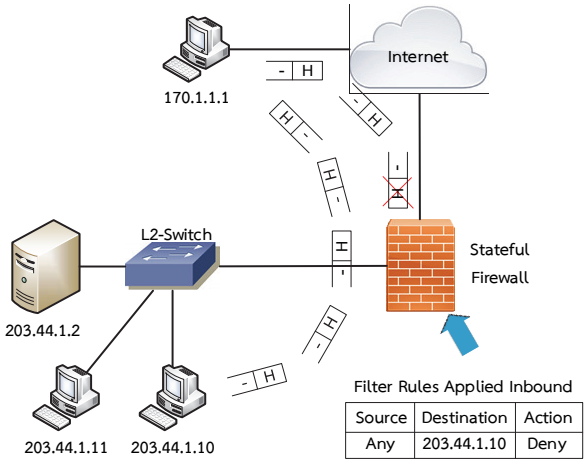
ไฟร์วอลล์เป็นระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ที่มีการใช้งานกันอย่างแพร่หลายในยุคเทคโนโลยีสารสนเทศในปัจจุบัน ซึ่งไฟร์วอลล์มีการใช้งานทั้งแบบที่เป็นฮาร์ดแวร์และแบบที่เป็นซอฟต์แวร์ โดยหน้าที่หลักของไฟร์วอลล์ทำหน้าที่การควบคุมเงื่อนไขของการสื่อสารแลกเปลี่ยนข้อมูล (Access Control) ระหว่างคอมพิวเตอร์ในระบบเครือข่ายที่เชื่อมต่อกัน โดยที่ไฟร์วอลล์สามารถกำหนดให้อุปกรณ์ชนิดใดสามารถทำการส่งข้อมูลไปยังอุปกรณ์ปลายทาง ด้วยการระบุบริการหรือช่องทาง (Port) ในปัจจุบันการใช้งานแบนด์วิดท์มีมากขึ้นเรื่อย ๆ ส่งผลให้การใช้งานแอพพลิเคชั่นในระบบเครือข่ายเกิดผลการล่าช้า ทำให้ต้องการระบบที่ใช้ในการปรับลดแบนด์วิดท์ที่อาจส่งผลกระทบกับแอพพลิเคชั่นอื่น ๆ ซึ่งการจำกัดข้อมูลจราจร (Traffic shaper) เป็นวิธีการหนึ่ง [1] โดยปัจจุบันแอพพลิเคชั่นมีการใช้งานแบนด์วิดท์มากเป็นอันดับต้น ๆ ได้แก่ การแชร์ไฟล์บนโปรโตคอลเพียร์ทูเพียร์ (Peer to Peer : P2P file sharing) หรือที่รู้จักกันว่า BitTorrent [2] โดยนักวิจัยชื่อ Jian Feng ได้ทำการวิจัยเรื่อง Research on the Technology of Peer- to- Peer Traffic Classification ซึ่งเป็นกล่าวถึงข้อดีและข้อเสียของการแยกแยะข้อมูลจราจรเพียร์ทูเพียร์ใน 3 วิธีได้แก่ Port-based, Payload-based และ Feature-based นอกจากนี้ Somnuk Puangpronpitag และคณะ [4] นำเสนอวิธีการแยกแยะข้อมูลจราจรเพียร์ทูเพียร์โดยใช้โปรโตคอลแบบลำดับชั้น ซึ่งผู้วิจัยใช้คำสั่ง iptable ร่วมกับคำสั่ง tc เพื่อแยกแยะข้อมูลจราจรประเภทเพียร์ทูเพียร์ 3 ชนิด ได้แก่ VoIP, Peer-to-Peer TV และ Bittorrent

งานวิจัยนี้นำเสนอระบบตรวจจับและสกัดกั้นแอพพลิเคชั่นบนระบบเครือข่าย โดยควบคุมแล้วสั่งงานผ่านเว็บอินเตอร์เฟสเพื่อทำให้ลดความยุ่งยากในการใช้งาน อันเกิดจากทักษะการใช้งานระบบปฏิบัติการ และโปรแกรมต่าง ๆ ในการสร้างความมั่นคงให้กับระบบเครือข่าย นอกจากนี้ระบบสามารถควบคุมการใช้แบนด์วิดท์บนระบบเครือข่ายของผู้ใช้งานแต่ละคนได้โดยผ่านทางหมายเลขไอพี

2. `ทฤษฎีที่เกี่ยวข้อง

2.1 ไฟร์วอลล์

ไฟร์วอลล์ เป็นเครื่องมือที่ใช้สำหรับควบคุมการแลกเปลี่ยนข้อมูลที่เกิดขึ้นในระบบเครือข่าย ซึ่งปัญหาการเข้าถึงข้อมูลผ่านระบบเครือข่าย หรือที่เรียกว่า ลอจิคัลแอคเซส (Logical Access) ที่สามารถเกิดขึ้นได้ง่ายกว่า การเข้าถึงทางกายภาพ เช่น การเข้าถึงตัวเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายในห้องศูนย์ข้อมูล เป็นต้น

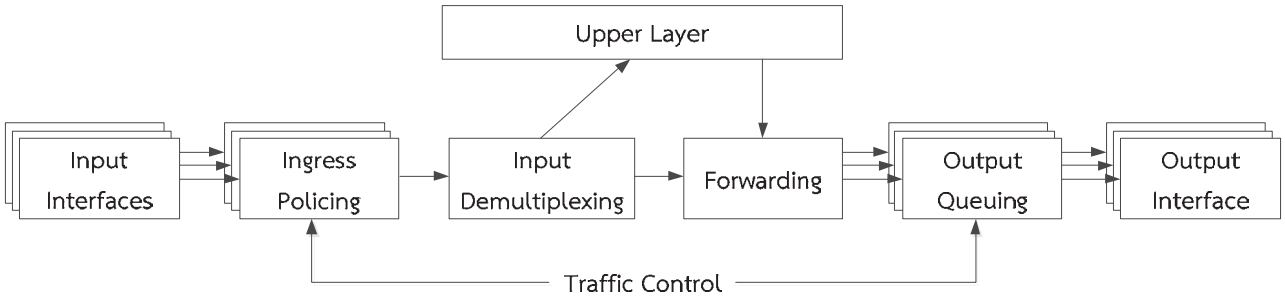


ภาพที่ 1 หลักการทำงานของสเตทฟูลไฟร์วอลล์

ภาพที่ 1 เป็นรูปแบบหนึ่งของไฟร์วอลล์ที่มีใช้งานในปัจจุบัน โดยสเตทฟูลไฟร์วอลล์สามารถที่จะวิเคราะห์ แพ็กเกจที่มีความต่อเนื่องของโปรโตคอลในเลเยอร์สูง ๆ ได้ เช่น TCP,FTP,HTTP หรือแม้กระทั่งแอพพลิเคชั่นเลเยอร์ ซึ่งจากภาพจะเห็นว่าข้อมูลของเครื่อง 203.44.1.10 ไม่ได้ถูกบล็อกในการส่งข้อมูลไปที่เครื่องปลายทาง 170.1.1.1 แต่กลับถูกบล็อกในการส่งข้อมูลขากลับที่ไฟร์วอลล์ อันเนื่องจากที่ไฟร์วอลล์ทำการกำหนดกฎ (Rules) ไว้ที่ข้อมูลขาเข้าไฟร์วอลล์นั่นเอง

2.2 การควบคุมข้อมูลจราจร (Traffic Control)

ในงานวิจัยนี้ทำการควบคุมข้อมูลจราจร โดยใช้คำสั่ง TC [5] ซึ่งเป็นคำสั่งที่จะทำการเปลี่ยนแปลงการทำงานภายในเคอร์เนล ในส่วนของการจัดส่งข้อมูลที่ออกจากคิวไปยังเครือข่าย แสดงดังภาพที่ 2 ซึ่งโดยปกติแล้วการ์ดเครือข่าย (Network Interface Card : NIC) จะมีคิวแบบ First-In-First-Out : FIFO ซึ่งเป็นคิวพื้นฐาน โดยหลักการทำงานของคิวแบบ



ภาพที่ 2 โครงสร้างของการจัดการข้อมูลจราจรในลินุกซ์

FIFO คือ เมื่อแพ็กเกจข้อมูลเข้ามาในคิว ข้อมูลจะถูกจัดส่งออกไปอย่างรวดเร็วตามลำดับการเข้าก่อน-ออกก่อน

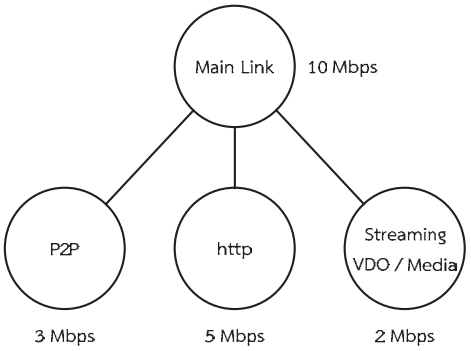
2.3 การจัดการคิวในลินุกซ์เพื่อส่งแพ็กเกจผ่านเครือข่าย

คิวและการจัดการคิวในลินุกซ์มีชื่อ เรียกว่า Queuing Disciplines หรือ qdisc โดยคิวที่ต่ออยู่กับการ์ดเครือข่ายเรียกว่า root qdisc โดยถ้าทำการเปลี่ยน root qdisc ให้เป็น qdisc ชนิดที่มีการแบ่งคลาสได้ (เรียก Classful qdisc) ซึ่งการแบ่งคลาสสามารถทำการ จำกัดความเร็วสูงสุดของแต่ละคลาส ควบคุมตามหมายเลขไอพีของเครื่องหรือซับเน็ต นอกจากนี้ยังสามารถควบคุมตามประเภทของบริการ (Services) ได้ ซึ่ง qdisc แบ่งออกเป็น 2 ประเภท ได้แก่ classless qdisc และ classful qdisc

- Classless qdisc เป็นคิวที่ไม่สามารถสร้างคลาสย่อยภายใต้ root qdisc ได้ ทำให้ไม่สามารถควบคุมแบนด์วิดท์ได้อย่างมีประสิทธิภาพ คิวประเภทนี้ได้แก่ pfifo_fast, TBF (Token Bucket Filter) และ SFQ (Stochastic Fairness Queuing) เป็นต้น
- Classful qdisc เป็นคิวที่สามารถสร้างคลาสย่อยเพื่อจัดประเภทแพ็กเกจและกำหนดความเร็วในการจัดส่งได้ ทำให้สามารถจัดการแบนด์วิดท์ที่มีความซับซ้อนได้อย่างมีประสิทธิภาพ ซึ่งคิวประเภทนี้ได้แก่ PRIO, CBQ (Classes Based Queue),HTB (Hierarchical Token bucket) เป็นต้น

2.4 โปรแกรม IPP2P

IPP2P เป็นโปรแกรมเสริมของแพ็กเกจ netfilter ที่สามารถแยกข้อมูลจราจรของ P2P ได้ โดย IPP2P เป็นเครื่องมือที่ใช้กรองแพ็กเกจที่ผ่านเข้ามา แต่จะไม่ได้ระงับการใช้งานของ P2P เพียงแต่จะทำการจำกัดปริมาณการใช้งานแบนด์วิดท์ที่เกิดจากการใช้งานโปรโตคอล P2P ตามที่กำหนด โดย IPP2P ได้รับ



ภาพที่ 3 โครงสร้างระบบการทำงานของ TC

การพัฒนาและทดสอบบนระบบปฏิบัติการลินุกซ์ ตระกูล SUSE แต่ก็สามารถทำงานบนลินุกซ์ตระกูลอื่น ๆ ได้ โดย IPP2P รองรับการทำงานในเคอร์เนลลินุกซ์ 2.4 ขึ้นไป

3. ขั้นตอนการดำเนินงาน

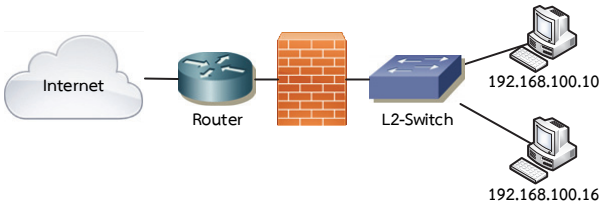
ในงานวิจัยนี้ ทำการทดสอบฟังก์ชั่นพื้นฐานทั่วไปของไฟร์วอลล์ เช่นการอนุญาตและไม่อนุญาติให้ใช้งานได้จากการระบุพอร์ตในการเชื่อมต่อ นอกจากนี้ยังทำการทดสอบการจำกัดความเร็วของข้อมูลการจราจรในแต่ละไอพีหรืออินเตอร์เฟสและส่วนสุดท้าย คือ การจำกัดการใช้งานแอพพลิเคชั่นเพียร์ทูเพียร์ โดยในขั้นตอนของการทดสอบระบบ P2P ผู้วิจัยเลือกใช้โปรแกรม P2P File Sharing ที่ได้รับความนิยมในปัจจุบันได้แก่

- Bittorrent
- eDonKey
- Kazaa
- Gnutella

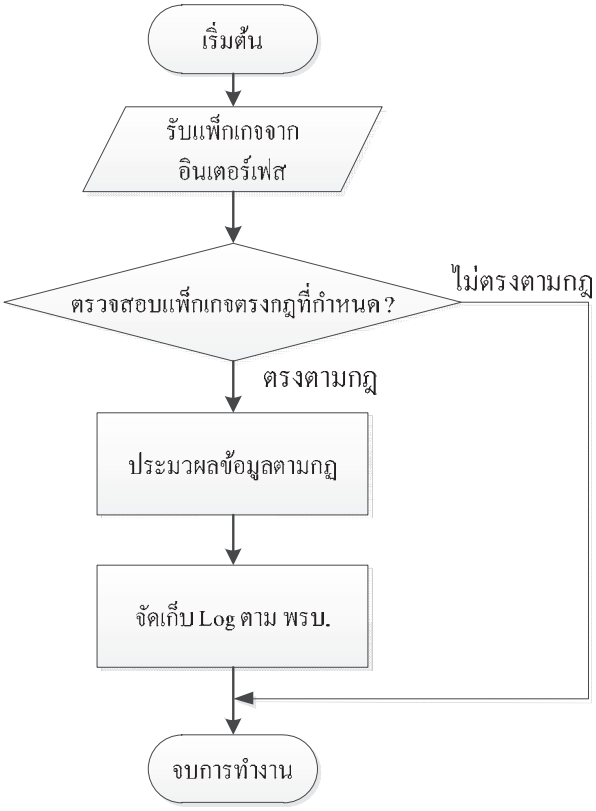
โดยมีแพ็กเกจเพื่อใช้ในการพัฒนาระบบสกัดกั้นข้อมูล ดังนี้

- Iptables ทำหน้าที่ควบคุมข้อมูลจราจร
- IPP2P ทำหน้าที่ตรวจจับข้อมูลชนิด P2P
- TC ทำหน้าที่ควบคุมแบนด์วิดท์

โครงสร้างการเชื่อมต่อ แสดงดังภาพที่ 4 ซึ่งประกอบด้วยเครื่องลูกข่ายจำนวน 2 เครื่อง เลเยอร์ 2 สวิตซ์ ไฟร์วอลล์ และเราเตอร์สำหรับใช้งานอินเตอร์เน็ต



ภาพที่ 4 โครงสร้างการเชื่อมต่ออุปกรณ์ต่าง ๆ

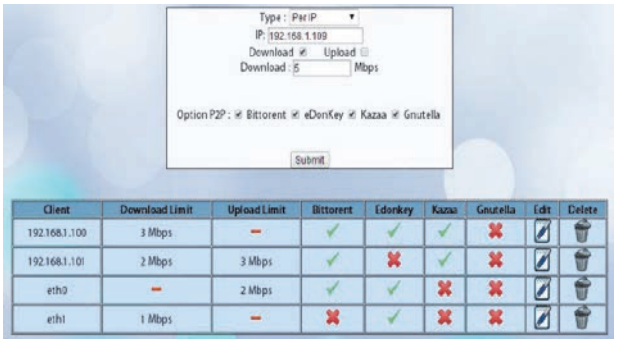


ภาพที่ 5 หลักการทำงานของระบบ

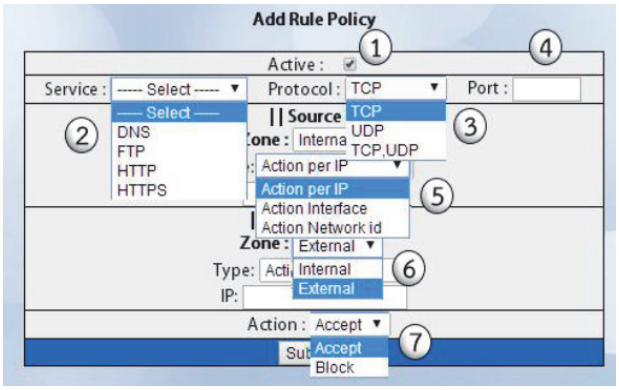
หลักการทำงานของระบบ มีขั้นตอน คือ เมื่อคอมพิวเตอร์แม่ข่ายได้รับแพ็กเกจที่ผ่านเข้ามาที่การ์ดเครือข่าย (Network Interface Card) ระบบจะนำแพ็กเกจเหล่านั้นมาตรวจสอบตามกฎที่ได้กำหนดไว้ ซึ่งหากตรงตามกฎที่กำหนดไว้ ระบบจะจัดการกับแพ็กเกจเหล่านั้นตามกฎที่กำหนดข้างต้น พร้อมกับทำการบันทึกข้อมูลจราจรตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งหลักการทำงานของระบบอธิบายดังภาพที่ 5

4. ผลการดำเนินการวิจัย

ภาพที่ 6 แสดงหน้าต่างการควบคุมและปรับแต่งปริมาณแบนด์วิดท์ของผู้ใช้งาน โดยผู้ดูแลระบบสามารถกำหนดหมายเลขไอพีที่ต้องการจำกัดแบนด์วิดท์ หรือสามารถระบุเป็นการ์ดเครือข่ายแทนได้ นอกจากนี้ระบบสามารถกำหนดแอพพลิเคชั่นของเพียร์ทูเพียร์ที่ผู้ใช้งานสามารถใช้งานได้หรือไม่ได้



ภาพที่ 6 หน้าต่างการสั่งงาน Traffic shaper



ภาพที่ 7 ตัวเลือกการเพิ่มกฎ Policy

จากภาพที่ 7 แสดงหน้าต่างการเพิ่มกฎ ซึ่งสามารถกำหนดตามแอพพลิเคชั่น/บริการที่ต้องการ โปรโตคอล และพอร์ตของเครื่องหรือหมายเลขไอพีที่ต้องการควบคุมว่าอนุญาต หรือไม่

อนุญาตตามกฎที่กำหนดมาข้างต้น นอกจากนี้ระบบยังสามารถจำกัดแบนด์วิดท์ที่ให้บริการของแอพพลิเคชั่นเพียร์-ทู-เพียร์ว่าต้องการจำกัดแบนด์วิดท์ต่อไอพี หรือจำกัดแบนด์วิดท์ของการใช้งานเพียร์ทูเพียร์ทั้งหมดโดยกำหนดที่อินเตอร์เฟสของไฟร์วอลล์แทน ซึ่งหน้าต่างการใช้งานแสดงดังภาพที่ 8

ภาพที่ 8 หน้าต่างการจำกัดข้อมูลจราจร

ตารางที่ 1 เป็นการเพิ่มกฎ (Rules) ในการจำกัดความเร็วในการรับส่งข้อมูลคอมพิวเตอร์ หรืออินเตอร์เฟส ดังตาราง โดยที่รายการที่ 1 เป็นการเพิ่มไอพีหมายเลข 192.168.100.10 โดยทำการจำกัดความเร็วในการดาวน์โหลด 0.5 Mbps และจำกัดความเป็นในการอัพโหลด 0.5 Mbps และจำกัดสิทธิ์การใช้งานเพียร์ทูเพียร์แอพพิลเคชั่น Kaza และ Gnutella แต่ยอมให้ใช้งาน Bitorrent และ Edonkey ได้

ตารางที่ 1 เพิ่มกฎการจำกัดข้อมูลจราจรผ่านเว็บไซต์

No.	Cilent	Traffic Limit		Option P2P			
		Down	Up	Bit	Edon	Kaz	Gnu
1	192.168.100.10	0.5	0.5	✓	✓	✗	✗
2	192.168.100.16	0.2	-	✗	✓	✓	✓
3	Eth0	-	0.1	✓	✗	✗	✗
4	Eth1	4	-	✓	✗	✗	✗
5	192.168.100.10	0.1	-	✓	✗	✗	✓

ตารางที่ 2 ผลการทดลองหลังจากเพิ่มกฎการจำกัดข้อมูลจราจร

Client	P2P Application	Traffic speed	
		Download	Upload
192.168.100.10	Bittorrent	10.8 kB/s	10.9 kB/s
	eDonKey	52.3 kB/s	-
	Kazaa	Unlimit	-
	Gnutella	13.8 kB/s	-
192.168.100.16	Bittorrent	451.4 kB/s	Unlimit
	eDonKey	20.6 kB/s	-
	Kazaa	10 kB/s	-
	Gnutella	21.3 kB/s	-

ในตารางที่ 2 แสดงผลลัพธ์ที่ได้จากการนำกฎที่ตั้งไว้จากตารางที่ 1 โดยคอมพิวเตอร์ที่มีหมายเลขไอพี 192.168.100.10 ซึ่งจากกฎในตารางที่ 1 กำหนดให้สามารถใช้งานได้เพียง Bittorrent และ eDonKey เท่านั้น แต่จากผลการทดสอบพบว่าที่แอพพลิเคชั่น Kazza ไม่มีการใช้งาน แต่ในแอพพลิเคชั่น Gnutella ยังสามารถใช้งานได้ ซึ่งจากการตรวจสอบพบว่าไอพี Gnutella ยังมีการเชื่อมต่อกับเครื่องภายนอกอยู่ ทำให้ไม่สามารถทำตามกฎที่กำหนดได้ ซึ่งผู้วิจัยได้แก้ไขปัญหาโดยการตัดการเชื่อมต่อของทุกไอพีก่อน เพื่อให้ทุกคอมพิวเตอร์ขาดการเชื่อมต่อจากภายนอก แล้วจึงทำการเปลี่ยนแปลงกฎตามที่ผู้ใช้กำหนด

ตารางที่ 3 ค่าความเร็วแบนด์วิดท์คลาดเคลื่อนหลังจากเพิ่มกฎการจำกัดข้อมูลจราจร

Client	P2P	Traffic speed	
		Download	Upload
192.168.100.10	Bittorrent	7.41 %	8.26 %
	eDonKey	4.4 %	-
	Kazaa	-	-
	Gnutella	27.54 %	-
192.168.100.16	Bittorrent	11.39 %	-
	eDonKey	2.91 %	-
	Kazaa	100 %	-
	Gnutella	6.1 %	-

ตารางที่ 3 แสดงค่าความคลาดเคลื่อนของการกำหนดกฎของผู้ใช้งานเปรียบเทียบกับแบนด์วิดท์จริงของระบบ โดยในการดาวน์โหลดข้อมูลผ่านแอพพิลเคชั่นเพียร์-ทู-เพียร์ก่อนที่ทำการเพิ่มกฎในการจำกัดข้อมูลจราจรความเร็วแบนด์วิดท์จะสามารถใช้งานได้ปกติ แต่เมื่อทำการเพิ่มกฎการจำกัดข้อมูลจราจรเข้าไปแอพพลิเคชั่นเพียร์-ทู-เพียร์ จะถูกทำการปรับแบนด์วิดท์ให้

ตรงตามกฎที่กำหนด แต่เมื่อมีการแก้ไขกฎเพิ่มเติมจากเดิม พบว่าแอพพลิเคชั่นเพียร์-ทู-เพียร์จะยังคงสามารถใช้งานที่แบนด์วิดท์ที่ความเร็วก่อนการแก้ไขกฎ ซึ่งถ้าผู้ใช้งานโหลดไฟล์ใหม่ หรือเปิดโปรแกรมใหม่ ก็จะถูกเข้าไปสู่กฎที่ได้ถูกแก้ไขทันที

5. สรุปผลการทดลอง

ระบบตรวจจับและสกัดกั้นแอพพลิเคชั่นบนระบบเครือข่ายสามารถสกัดกั้นบริการพื้นฐานบนระบบเครือข่ายได้โดยระบุหมายเลขไอพีของเครื่อง หรือกลุ่มของเครื่องที่ควบคุมตามซับเน็ท (sub-network) นอกจากนี้ยังจำกัดแบนด์วิดท์ของบริการเพียร์-ทู-เพียร์ (P2P) ของแต่ละไอพี หรือจำกัดแบนด์วิดท์ของทั้งหมดโดยการกำหนดที่อินเตอร์เฟสของไฟร์วอลล์ ซึ่งระบบสามารถปรับแบนด์วิดท์ทั้งค่าอัพโหลด (Upload) และดาวน์โหลด (Download) ตามความต้องการ นอกจากนี้ระบบสามารถรายงานปริมาณแบนด์วิดท์ที่ถูกใช้งานทั้งขาเข้าและขาออกของไฟร์วอลล์ พร้อมกันนี้ระบบรองรับการจัดเก็บข้อมูลจราจรตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งระบบที่ได้ทำการพัฒนานี้สามารถเพิ่มประสิทธิภาพโดยการปรับเปลี่ยนสเปคของเครื่องคอมพิวเตอร์ ซึ่งแตกต่างจากไฟร์วอลล์สำเร็จรูปที่ไม่สามารถปรับเปลี่ยนฮาร์ดแวร์ เช่น การเปลี่ยนการ์ดเครือข่ายจาก 1Gbps เป็นการ์ดแบบ 10Gbps เป็นต้น แต่ระบบนี้มีปัญหาของการควบคุมความเร็วของผู้ใช้งาน (Traffic Shaper) เมื่อมีการเปลี่ยนแปลงกฎที่ใช้ควบคุม ทำให้ผู้ใช้งานปัจจุบันจะได้รับการเปลี่ยนแปลงกฎในทันที ซึ่งแก้ไขได้โดยการสั่งให้โปรแกรมควบคุมความเร็วเริ่มทำงานใหม่

6.กิตติกรรมประกาศ

ขอขอบคุณคณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ที่ให้การสนับสนุนค่าใช้จ่ายในการนำเสนอบทความในครั้งนี้

7.เอกสารอ้างอิง

[1] S. M. Cherry, "Bandwidth shapers unclog busy networks," IEEE Spectrum, vol. 39, p. 61, 2002.

[2] สุรศักดิ์ สงวนพงษ์, "Linux Implementation of P2P Detection and Traffic Shaping", The Third Conference on Internet Technology (CIT2006), 11 มกราคม 2006, พะเยา

[3] Jian Feng, "Research on the Technology of Peer-to-Peer Traffic Classification," International Symposium on Computer, Communication, Control and Automation, p.491-494, 2010.

[4] S. Puangpronpitag, T. Chuachan, P. Pawara, "Classifying Peer-to-peer Traffic using Protocol Hierarchy," International Conference on Computer and Information Sciences (ICCOINS), 2014.

[5] Lucian Gheorghe, "Designing and Implementing Linux Firewalls with QoS using netfilter, iproute2, NAT and L7-filter," Packt Publishing, 2006.