ใบรับรองวิทยานิพนธ์

บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์

วิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมคอมพิวเตอร์)

ปริญญา

วิศวกรรมคอมพิวเตอร์	วิศวกรรมคอมพิวเตอร์
สาขา	**ภาควิชา**

เรื่อง การตรวจจับโปรแกรมแชร์ไฟล์แบบเพียร์ทูเพียร์ของเครือข่ายไร้สายแบบ IEEE802.11

P2P File Sharing Detection on IEEE802.11

นามผู้วิจัย ว่าที่ร้อยตรีณรงค์ ภูมิสุข

ได้พิจารณาเห็นชอบโดย

อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก .....

(รองศาสตราจารย์อนันต์ ผลเพิ่ม, Ph.D.)

อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม .....

(ผู้ช่วยศาตราจารย์ชัยพร ใจแก้ว, Ph.D.)

หัวหน้าภาควิชา .....

(ผู้ช่วยศาสตราจารย์เขมะฑัต วิภาตะวนิช, Ph.D.)

บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์รับรองแล้ว

.....

(รองศาสตราจารย์กัญจนา ธีระกุล, D.Agr.)

คณบดีบัณฑิตวิทยาลัย

วันที่ ..... **เดือน** ..... **พ.ศ.** .....

วิทยานิพนธ์

เรื่อง

การตรวจจับโปรแกรมแชร์ไฟล์แบบเพียร์ทูเพียร์ของ เครือข่ายไร้สายแบบ IEEE802.11

P2P File Sharing Detection on IEEE802.11

โดย

ว่าที่ร้อยตรีณรงค์ ภูมิสุข

เสนอ

บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์

เพื่อความสมบูรณ์แห่งปริญญาวิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมคอมพิวเตอร์)

พ.ศ. 2553

ว่าที่ร้อยตรีณรงค์ ภูมิสุข 2553: การตรวจจับโปรแกรมแชร์ไฟล์แบบเพียร์ทูเพียร์ของเครือข่ายไร้สายแบบ IEEE802.11 ปริญญาวิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมคอมพิวเตอร์) สาขาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก: รองศาสตราจารย์อนันต์ ผลเพิ่ม, Ph.D. 85 หน้า

บิตทอร์เรนต์เป็นโพรโทคอลการแบ่งปันไฟล์แบบเพียร์ทูเพียร์ที่มีความสามารถในการกระจายไฟล์ได้รวดเร็ว และใช้ทรัพยากรแบนด์วิทด์ของเครือข่ายได้อย่างเต็มประสิทธิภาพจึงเป็นที่นิยมอย่างแพร่หลายในปัจจุบัน แต่ผลกระทบอันเนื่องมาจากการใช้งานแบนด์วิทด์ที่เต็มประสิทธิภาพตลอดเวลาของบิตทอร์เรนต์ ทำให้โปรแกรมที่ใช้งานเครือข่ายอื่น ๆ ถูกโปรแกรมบิตทอร์เรนต์แย่งชิงแบนด์วิทด์ โดยเฉพาะเมื่อใช้งานโปรแกรมบิตทอร์เรนต์บนเครือข่ายไร้สายที่มีทรัพยากรแบนด์วิทด์จำกัดอยู่แล้ว เมื่อมีผู้ใช้งานบิตทอร์เรนต์บนเครือข่ายไร้สายแม้เพียงคนเดียวก็จะทำให้เกิดสภาวะขาดแคลนแบนด์วิทด์ที่ร้ายแรง แก่ผู้ใช้งานโปรแกรมอรรถประโยชน์อื่น ๆ บนเครือข่ายไร้สาย

งานวิจัยนี้ได้นำเสนอวิธีการตรวจจับการใช้งานบิตทอร์เรนต์บนเครือข่ายไร้สาย โดยอาศัยเพียงแค่ข้อมูลเครือข่ายของเฟรมข้อมูลบนชั้นแม็ค ซึ่งได้จากการศึกษาการกระจายตัวของขนาดเฟรมข้อมูลของโพรโทคอลบิตทอร์เรนต์ที่เกิดจากพฤติกรรมการส่งข้อมูลเพื่อติดต่อประสานจังหวะกันระหว่างเพียร์ โดยได้ออกแบบกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์ให้มีขั้นตอนการทำงานได้แก่ การสุ่มดักจับเฟรมข้อมูล การกรองเฟรมข้อมูล และการตัดสินการเป็นบิตทอร์เรนต์ นอกจากนี้ยังได้ทำการหาค่าช่วงเวลาเริ่มต้นและระยะเวลาที่เหมาะสมในการสุ่มดักจับข้อมูลที่ทำให้กลไกการตรวจจับมีความถูกต้องในการทำงานมากที่สุด

จากผลการทดสอบแสดงให้เห็นว่ากลไกตรวจจับบิตทอร์เรนต์บนเครือข่ายไร้สายให้ความถูกต้องในการตรวจจับสูงถึง 90% ประกอบการออกแบบอัลกอริทึมที่มีน้ำหนักเบา จึงทำให้กลไกง่ายต่อการพัฒนาและมีความต้องการใช้ทรัพยากรการประมวลผลน้อยมาก สามารถทำงานได้ในแบบเวลาจริง อีกทั้งยังสามารถตรวจจับบิตทอร์เรนต์ได้แม้มีการเข้ารหัสข้อมูล

_____ / / /

ลายมือชื่อนิสิต ลายมือชื่ออาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

Acting Sub Lieutenant Narong Phoomsuk 2010: P2P File Sharing Detection on IEEE802.11. Master of Engineering (Computer Engineering), Major Field: Computer Engineering, Department of Computer Engineering. Thesis Advisor: Associate Professor Anan Phonphoem, Ph.D. 85 pages.

BitTorrent is one of the most popular peer-to-peer file sharing protocols due to its efficiency and ease of use. The protocol separates a file into small pieces. One a piece of file has been completely downloaded, the particular piece becomes a new seed for further downloading. Therefore, more participants mean less downloading time. By its greedy characteristics and popularity, BitTorrent can consume all network resources in no time causes a starvation problem to other applications even in the high speed LAN. The problem becomes more severe in the limited bandwidth environment such as wireless LAN.

In the paper, a new approach to identify BitTorrent protocol in wireless LAN environment has been proposed. The mechanism is a light-weight detection protocol, based on the size of data link frames, which is small enough to be implemented on an access point. The method can be divided into 3 phases: Sampling, Filtering and Decision. Furthermore, this paper provides the experimental setup for finding the suitable sampling starting time and the optimal sampling time interval used for highest accuracy rate of new detection mechanism.

The experimental results show that the mechanism can detect BitTorrent in real-time mode with high accuracy rate. With a light-weight design based only on the data link frame size monitoring can cause the ease of implement with low computation power. The mechanism is also able to detect the encrypted transmission.

_____ _____ ___ / ___ / ___

Student's signature Thesis Advisor's signature

กิตติกรรมประกาศ

ข้าพเจ้าขอขอบพระคุณรองศาสตราจารย์ ดร. อนันต์ ผลเพิ่ม ประธานกรรมการที่ปรึกษาที่ได้ปลูกฝังระเบียบวิธีวิจัยเพื่อให้ข้าพเจ้าได้คิดอย่างเป็นระบบและมีแบบแผนที่ดี รวมไปถึงได้ให้คำปรึกษาในหลาย ๆ เรื่อง ไม่ว่าจะเป็นเรื่องการเรียน การทำงาน หรือแม้กระทั่งเรื่องครอบครัว ขอขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร. ชัยพร ใจแก้ว และ อาจารย์อภิรักษ์ จันทร์สร้าง ที่ช่วยให้คำแนะนำ และให้มุมมองที่แตกต่างในการวิจัย รวมไปถึงช่วยเหลือทางด้านเทคนิคการจัดการกับข้อมูลการทดลอง อีกทั้งยังให้คำถามที่เป็นประโยชน์ต่อการปรับปรุงวิทยานิพนธ์ฉบับนี้

ขอขอบคุณ คุณนันท์นภัส เบญจมาศ และคุณบัณฑิต มนัสเกษมศักดิ์ ที่ได้ให้คำปรึกษาการทำวิจัยมาโดยตลอด ทั้งยังคอยชี้แนะแนวทางที่ถูกต้องในการทำวิจัย และขอบคุณสมาชิกห้องปฏิบัติการวิจัยเครือข่ายไร้สาย (IWING) และเพื่อน พี่น้องสมาชิกห้องปฏิบัติการอื่น ๆ ทั้งปริญญาโท และปริญญาเอก ทุกท่าน ที่มิได้เอ่ยนาม ณ ที่นี้ ที่ให้คำปรึกษา ชี้แนะแนวทาง ทั้งยังคอยให้คำแนะนำดี ๆ เพื่อช่วยในการตัดสินใจในสถานการณ์ต่าง ๆ ของข้าพเจ้าให้เป็นไปในทางที่ถูกต้องและเหมาะสม

ขอบคุณเจ้าหน้าที่ธุรการโครงการปริญญาโทที่ช่วยเหลือในด้านการประสานงานต่าง ๆ ให้งานสำเร็จลุล่วงไปด้วยดี และขอบคุณพี่น้องและเพื่อน ๆ ทุกท่าน ที่ทำให้ที่คอยให้กำลังใจ และช่วยสร้างแรงบันดาลใจ ทำให้ข้าพเจ้าเกิดความมุ่งมั่นทำงานจนทำให้วิทยานิพนธ์ฉบับนี้สำเร็จลงได้

ขอขอบคุณศูนย์ไทยกริดแห่งชาติ (TNGC) ที่ได้ให้ความอนุเคราะห์วัสดุ-อุปกรณ์ต่าง ๆ ตลอดจนสถานที่ที่ใช้ในการทำวิจัย พร้อมทั้งขอขอบคุณ คุณนวพล นาราษฎร์ ที่ช่วยเหลือในการทำวิทยานิพนธ์ ทั้งทางตรงและทางอ้อม

ขอขอบพระคุณ บิดา นายชาญ ภูมิสุข ที่ได้สนับสนุนทุนทรัพย์ในการศึกษา และความพยายาม อดทนรอจนถึงวันที่ลูกได้เล่าเรียนสำเร็จปริญญาโท คุณงามความดีหรือประโยชน์อันใดที่เกิดจากวิทยานิพนธ์ฉบับนี้ ข้าพเจ้าขออุทิศให้บิดา มารดา บุพการี คณาจารย์และผู้มีพระคุณทุกท่าน

ณรงค์ ภูมิสุข

เมษายน 2553

สารบัญ

สารบัญตาราง

สารบัญภาพ

สารบัญภาพ (ต่อ)

สารบัญภาพ (ต่อ)

คำอธิบายสัญลักษณ์และคำย่อ

AP	=	Access Point
AR	=	Accuracy Rate
ACK	=	Acknowledgement
ATIM	=	Announcement Traffic Indication Map
BER	=	Bit Error Rate
BSSID	=	Basic Service Set ID
CDF	=	Cumulative Distribution Function
CF	=	Contention Free
CSMA/CA	=	Carrier Sense Multiple Access with Collision Avoidance
CRC	=	Cyclic Redundancy Check
CTS	=	Clear-to-Send
DA	=	Destination Address
FCS	=	Frame Check Sequence
FTP	=	File Transfer Protocol
FP	=	False Positive
FPR	=	False Positive Rate
HTTP	=	Hypertext Transfer Protocol
HTTPS	=	Hypertext Transfer Protocol Secure
IEEE	=	Institute of Electrical Electronics Engineers
IP	=	Internet Protocol
MAC	=	Media Access Control
MPDU	=	MAC Protocol Data Units
MSDU	=	MAC Service Data Unit
MTU	=	Maximum Transmission Unit
NAV	=	Network Allocation Vector
OSI	=	Open System Interconnection
PLCP	=	Physical Layer Convergence Procedure
PS	=	Power Save

คำอธิบายสัญลักษณ์และคำย่อ (ต่อ)

PSH	=	Push
P2P	=	Peer-to-Peer
RA	=	Receiver Address
RTS	=	Request-to-Send
SA	=	Source Address
SIFS	=	Short Interframe Space
TCP	=	Transmission Control Protocol
TP	=	True Positive
TPR	=	True Positive Rate
UDP	=	User Datagram Protocol
URL	=	Universal Resource Locator
WEP	=	Wired Equivalent Privacy
WLAN	=	Wireless Local Area Network

การตรวจจับโปรแกรมแชร์ไฟล์แบบเพียร์ทูเพียร์ของเครือข่ายไร้สายแบบ IEEE802.11

P2P File Sharing Detection on IEEE802.11

คำนำ

โพรโทคอลการส่งผ่านข้อมูลแบบเพียร์ทูเพียร์ เป็นโพรโทคอลสำหรับการแลกเปลี่ยนข้อมูลระหว่างเครือข่ายคอมพิวเตอร์ที่ใช้สถาปัตยกรรมการประมวลผลแบบกระจาย (Distributed System) มีการทำงานในลักษณะแยกศูนย์กลาง (Decentralized) จุดเด่นของระบบนี้คือมีการแบ่งปันทรัพยากรต่าง ๆ อาทิเช่น แบนด์วิดท์ (Bandwidth) ส่วนเก็บข้อมูล (Storage) และรอบในการประมวลผล (CPU Cycle) เป็นต้น ไฟล์ที่ต้องการดาวน์โหลดในระบบเพียร์ทูเพียร์จะไม่ได้อยู่ที่เครื่องใดเครื่องหนึ่งเหมือนอย่างสถาปัตยกรรมไคลเอนต์-เซิร์ฟเวอร์ (Client-Server) โดยไฟล์จะกระจายตัวไปยังเครื่องคอมพิวเตอร์หรือเพียร์ (Peer) อื่น ๆ ในระบบ จึงสามารถดาวน์โหลดไฟล์ได้จากหลากหลายต้นทางในเวลาเดียวกัน ซึ่งทำให้ความเร็วในการดาวน์โหลดไฟล์มีสูงมาก การส่งผ่านข้อมูลในลักษณะของเพียร์ทูเพียร์เช่นนี้จึงได้รับความนิยมอย่างมากและยาวนาน

โพรโทคอลบิตทอร์เรนต์ (BitTorrent Protocol) เป็นโพรโทคอลเพียร์ทูเพียร์แบบผสม (Hybrid Peer-to-Peer) ใช้เทคนิคในการตัดแบ่งข้อมูลเป็นชิ้นส่วนเล็ก ๆ ในการรับ-ส่งข้อมูล จึงทำให้บิตทำให้ข้อมูลสามารถกระจายไปยังเครื่องอื่น ๆ ได้อย่างรวดเร็ว ยิ่งมีจำนวนเครื่องที่ร่วมทำการแลกเปลี่ยนข้อมูลมากเท่าไร ก็ยิ่งส่งผลให้ประสิทธิภาพในการแลกเปลี่ยนข้อมูลโดยรวมของข้อมูลที่ต้องการแลกเปลี่ยนเพิ่มขึ้นเท่านั้น และด้วยการออกแบบให้ระบบมีความทนทานต่อความล้มเหลว บิตทอร์เรนต์จึงกำหนดให้มีเครื่องศูนย์กลางทำหน้าที่เก็บข้อมูลเฉพาะดัชนีของชิ้นส่วนไฟล์และรายชื่อเพียร์ที่เก็บชิ้นส่วนไฟล์เท่านั้น ทำให้ถึงแม้จะเกิดเหตุการณ์ที่เครื่องศูนย์กลางไม่สามารถให้บริการได้ แต่การดาวน์โหลดระหว่างเพียร์ก็ยังสามารถดำเนินการต่อไปได้อย่างปกติ และผลจากการที่เครื่องศูนย์กลางไม่จำเป็นต้องมีทรัพยากรในปริมาณมาก จึงทำให้ไม่เกิดข้อจำกัดในการปรับเปลี่ยนขนาดของระบบ (Scalability) ด้วยจุดเด่นในด้านต่าง ๆ เหล่านี้ จึงทำให้การใช้งานโพรโทคอลบิตทอร์เรนต์ในการแบ่งปันไฟล์ได้รับความนิยมอย่างแพร่หลายในปัจจุบันนี้ โพรโทคอลบิตทอร์เรนต์สามารถรับและส่งข้อมูลได้ในคราวเดียวกัน ทำให้ใช้ทรัพยากรเครือข่ายได้อย่างมีประสิทธิภาพมาก ประกอบกับมีการตัดแบ่งข้อมูลออกเป็นชิ้นเล็ก ๆ ทำให้มีโอกาสในการแย่งใช้ทรัพยากรในการแลกเปลี่ยนข้อมูลมากกว่าแอพพลิเคชั่นอื่น ๆ ซึ่งทำให้

โพรโทคอลบิตทอร์เรนต์ใช้ทรัพยากรเครือข่ายได้อย่างเต็มประสิทธิภาพตลอดเวลา โดยเฉพาะอย่างยิ่งบนเครือข่ายไร้สาย ที่มีทรัพยากรเครือข่ายน้อยอยู่แล้ว หากมีเครื่องเพียงแค่เครื่องเดียวที่มีการเปิดโปรแกรมบิตทอร์เรนต์โดยไม่ได้จำกัดการใช้งานแบนด์วิทด์อยู่ในเครือข่าย ก็จะทำให้เครื่องลูกข่ายอื่น ๆ ในเครือข่ายไร้สายได้รับผลกระทบในการใช้ทรัพยากรเครือข่ายไร้สายอย่างรุนแรง

การที่จะควบคุมผลกระทบที่เกิดจากการใช้งานโปรแกรมบิตทอร์เรนต์ที่อยู่ในเครือข่ายไร้สาย จำเป็นจะต้องมีกระบวนการตรวจจับการใช้งานโปรแกรมบิตทอร์เรนต์ที่ใช้ได้ผลอย่างมีประสิทธิภาพบนเครือข่ายไร้สาย ซึ่งแนวทางในปัจจุบัน ส่วนใหญ่ถูกพัฒนาให้ใช้ได้ประสิทธิภาพดีบนเครือข่ายใช้สาย โดยแนวทางการออกแบบกลไกการตรวจจับที่ผ่านมาสามารถแบ่งได้เป็น 3 กลุ่มใหญ่ ได้แก่แนวทางการตรวจจับโดยอาศัยหมายเลขพอร์ต ซึ่งพัฒนาได้ง่าย แต่มีข้อจำกัดในการตรวจจับเนื่องจากบิตทอร์เรนต์สามารถปรับเปลี่ยนการทำงานโดยใช้พอร์ตที่หลากหลาย (Arbitrary port) หรือแม้กระทั่งใช้พอร์ตที่เป็นที่รู้จักโดยทั่วไป (Well-known port) ที่ไม่ใช่เป็นพอร์ตปริยายของบิตทอร์เรนต์ได้ แนวทางต่อมาเป็นแนวทางในการตรวจหาสัญลักษณ์ที่อยู่ในแพ็กเกตของบิตทอร์เรนต์ ซึ่งมีข้อจำกัดในการตรวจจับหากมีการเข้ารหัสข้อมูล และการดูข้อมูลแพ็กเกตโดยไม่ได้รับอนุญาตยังเป็นข้อจำกัดทางกฎหมายในบางประเทศ อีกแนวทางหนึ่งคือการตรวจจับพฤติกรรมการทำงานของบิตทอร์เรนต์ ซึ่งที่ผ่านมาใช้การออกแบบกลไกการตรวจจับพฤติกรรมของบิตทอร์เรนต์บนเครือข่ายใช้สาย จะอาศัยข้อมูลในชั้นขนส่ง ซึ่งต้องทำการพัฒนาบนอุปกรณ์ที่มีทรัพยากรมาก

งานวิจัยนี้นำเสนอแนวทางการตรวจจับการใช้งานโปรแกรมบิตทอร์เรนต์บนเครือข่ายไร้สาย โดยอาศัยเพียงแค่ข้อมูลจากเฟรมข้อมูลของเครือข่ายไร้สาย (WLAN data frame) ซึ่งอยู่ในชั้นแม็ค (MAC Layer) ที่ถูกสร้างโดยโพรโทคอลบิตทอร์เรนต์เพื่อการควบคุมและประสานจังหวะการทำงานระหว่างเพียร์อันเป็นเอกลักษณ์ของโพรโทคอลบิตทอร์เรนต์เป็นตัวบ่งบอกถึงการมีอยู่ของกระแสข้อมูลของบิตทอร์เรนต์ ทำให้สามารถตรวจจับบิตทอร์เรนต์ได้แม้มีการเข้ารหัสข้อมูล และการออกแบบกลไกที่เรียบง่าย ไม่ซับซ้อน ทำให้ใช้ทรัพยากรพลังการประมวลผลต่ำ เหมาะสำหรับการนำไปพัฒนาบนอุปกรณ์ไร้สาย ที่มีทรัพยากรจำกัดอีกด้วย

วัตถุประสงค์

นำเสนอวิธีการในการตรวจจับโพรโทคอลบิตทอร์เรนต์ โดยอาศัยข้อมูล ที่ชั้นแม็ค ที่ใช้ได้ผลอย่างมีประสิทธิภาพบนเครือข่ายไร้สาย

การตรวจเอกสาร

ใจความสำคัญของบทนี้จะกล่าวถึงทฤษฎีและความรู้พื้นฐานที่เกี่ยวข้องกับงานวิจัย อันได้แก่ เพียร์ทูเพียร์ โพรโทคอลบิตทอร์เรนต์ และมาตรฐานเครือข่ายไร้สายแบบ IEEE802.11 และในหัวข้อสุดท้ายจะกล่าวถึงงานวิจัยที่เกี่ยวข้องกับการตรวจจับโพรโทคอลบิตทอร์เรนต์

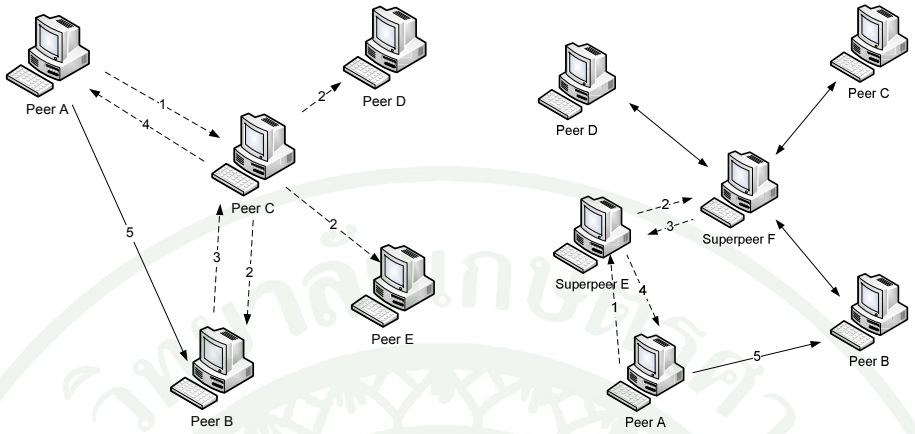
เพียร์ทูเพียร์

เพียร์ทูเพียร์ (P2P : Peer-to-Peer) (Pourebrahimi, 2005) เป็นสถาปัตยกรรมเครือข่ายของระบบประมวลผลแบบกระจายตัว (Distributed) มีการทำงานในลักษณะแยกศูนย์กลาง (Decentralized) มีคุณลักษณะในการแบ่งกันใช้งานทรัพยากร อาทิ รอบประมวลผลซีพียู (CPU Cycle) หน่วยความจำ แบนด์วิดท์ของเครือข่าย และส่วนเก็บข้อมูล (Storage) เป็นต้น โดยในแต่ละเพียร์ (Peer) ในระบบจะมีการเชื่อมต่อกันโดยตรง โดยทำหน้าที่เป็นทั้งผู้ให้บริการและผู้รับบริการในเวลาเดียวกัน ซึ่งสามารถจำแนกกลุ่มของการแยกศูนย์กลางได้เป็น 2 กลุ่มหลักได้แก่

1. เพียร์ทูเพียร์แยกศูนย์กลางโดยแท้จริง (Purely Decentralized)

แต่ละโหนด (Node)ในเครือข่ายเพียร์ทูเพียร์จะเรียกว่า Servant (Server+Client) (Pourebrahimi,2005) จะมีความสามารถในการทำงานเท่ากัน และทำหน้าที่เป็นผู้ให้บริการและผู้รับบริการในเวลาเดียวกัน ข้อดีของระบบนี้คือมีความสามารถในการปรับเปลี่ยนขนาดได้ง่าย (Scalability) กล่าวคือเมื่อต้องการจะเพิ่มปริมาณเพียร์ ก็สามารถเพิ่มเข้าสู่เครือข่ายได้ทันที ไม่จำเป็นต้องมีการปรับตั้งค่าที่ซับซ้อน และมีความทนทานต่อความล้มเหลว (Failure) ทั้งนี้เนื่องมาจากการทำงานที่เป็นอิสระไม่ขึ้นต่อกัน ดังนั้นหากเพียร์ใดไม่สามารถทำงานได้ เพียร์อื่น ๆ ก็ยังสามารถทำงานได้ แต่จุดอ่อนของเพียร์ทูเพียร์ชนิดนี้คือ จำเป็นจะต้องมีกระบวนการค้นหาเพียร์ (Discovery) ที่ต้องการติดต่อด้วย โดยจะต้องทำการส่งข้อมูลการร้องขอกระจายทุกทิศทาง (Flooding Request) เพื่อค้นหาว่าเพียร์ที่ต้องการจะติดต่อด้วยอยู่ที่ไหน เมื่อค้นพบเพียร์ที่ต้องการจะติดต่อด้วยแล้ว จึงค่อยทำการติดต่อโดยตรงกับเพียร์นั้นต่อไป ส่งผลให้เกิดการสิ้นเปลืองทรัพยากรคือแบนด์วิทด์ของเครือข่ายไปในการค้นหาเพียร์ในปริมาณมาก โดยโพรโทคอลเพียร์ทูเพียร์ที่จัดอยู่ในประเภทนี้ได้แก่ นูเทลล่า (Gnutella) (Kirk, 2003) ฟรีเนต (Freenet) (Clarke, 2009) คาซ่า (Kazaa) (Brilliant Digital Entertainment, 2010) คอร์ด (Chord) (Stoica *et. al.*, 2001) และ

แคน (CAN) (Ratanasami *et. al.*, 2001) รายละเอียดการติดต่อของเพียร์ แสดงดังภาพที่ 1 ก.



ก. Purely Decentralized ข. Purely Decentralized with Superpeer

ภาพที่ 1 ลักษณะโครงสร้างของเพียร์ทูเพียร์แยกศูนย์กลางโดยแท้จริงและขั้นตอนการค้นหาข้อมูล

ภาพที่ 1 ก. แสดงการทำงานระบบเพียร์ทูเพียร์แยกศูนย์กลางโดยแท้จริง โดยเริ่มจากเพียร์ A ต้องการจะติดต่อกับเพียร์ B แต่ไม่รู้ว่าเพียร์ B อยู่ที่ไหนจึงส่งคำร้องขอทุกทิศทางไปยังเพียร์ C ดังหมายเลข 1 เพียร์ C ก็จะทำหน้าที่ส่งคำร้องขอทุกทิศทางไปอีกทอดหนึ่งดังเช่นหมายเลข 2 เพียร์ B ซึ่งอยู่ใกล้เพียร์ C เมื่อได้รับคำร้องจากเพียร์ C จึงได้ส่งคำตอบรับหมายเลข 3 ไปยังเพียร์ C เมื่อเพียร์ C ได้รับการตอบรับจากเพียร์ B ก็จะทำการส่งต่อคำตอบรับหมายเลข 4 ของเพียร์ B ให้เพียร์ A เพียร์ A ก็จะทราบว่าที่อยู่ที่แน่นอนของเพียร์ B และสามารถส่งข้อมูลหมายเลข 5 เพื่อติดต่อโดยตรงกับเพียร์ B ต่อไป จะเห็นได้ว่าการใช้แบนด์วิทด์ในการส่งคำขอเพื่อค้นหาเพียร์ที่ต้องการติดต่อจะมีปริมาณมาก ซึ่งเป็นข้อเสียหลักของระบบเพียร์ทูเพียร์แยกศูนย์กลางโดยแท้จริง

อย่างไรก็ตามโพรโทคอลบางชนิดอย่างนูเทลล่า ได้แก้ปัญหาการสิ้นเปลืองทรัพยากรแบนด์วิทด์จากการที่แต่ละเพียร์จะต้องทำค้นหาเพียร์โดยการส่งคำร้องขอแบบกระจายทุกทิศทางนี้ด้วยการจัดลำดับชั้นของเพียร์ (Tier) คือแบ่งเพียร์เป็นกลุ่มย่อย ๆ และจัดให้มีหัวหน้ากลุ่ม เรียกว่า ซูเปอร์โหนด (Supernode) หรือ ซูเปอร์เพียร์ (Superpeer) คอยเป็นตัวจัดการค้นหาสมาชิกในกลุ่มและติดต่อผ่านสมาชิกของกลุ่มอื่นผ่านซูเปอร์เพียร์ด้วยกัน เพื่อลดปริมาณการใช้งานแบนด์วิทด์ของเครือข่ายโดยรวม ส่งผลให้ประสิทธิภาพโดยรวมของเครือข่ายดีขึ้น การติดต่อโดยใช้ซูเปอร์เพียร์ แสดงดังภาพที่ 1 ข.

ภาพที่ 1 ข. แสดงการทำงานระบบเพียร์ทูเพียร์แยกศูนย์กลางโดยแท้จริงที่มีซูเปอร์เพียร์ เริ่มจากเพียร์ A ต้องการจะติดต่อกับเพียร์ B ซึ่งอยู่คนละกลุ่มกัน เพียร์ A จะส่งคำร้องขอหมายเลข 1 ไปยังซูเปอร์เพียร์ E ที่เป็นหัวหน้ากลุ่ม จากนั้นซูเปอร์เพียร์ E จะทำการส่งต่อคำร้องขอของเพียร์ A หมายเลข 2 กระจายไปยังซูเปอร์เพียร์ด้วยกัน ซูเปอร์เพียร์หนึ่งที่ได้รับคำร้องขอคือ ซูเปอร์เพียร์ F ซึ่งมีเพียร์ B เป็นสมาชิกในกลุ่ม เมื่อซูเปอร์เพียร์ F รู้ว่าคำร้องขอที่ส่งมาเป็นของ เพียร์ B ก็ทำการส่งคำตอบรับกลับไปยังซูเปอร์เพียร์ E หมายเลข 3 ซึ่งแนบมากับที่อยู่ของเพียร์ B ด้วย เมื่อซูเปอร์เพียร์ E ได้รับคำตอบกลับพร้อมที่อยู่ของเพียร์ B แล้ว ก็จะส่งต่อข้อมูลหมายเลข 4 ไปบอกเพียร์ A เมื่อเพียร์ A ได้ที่อยู่ที่แท้จริงของเพียร์ B ก็จะสามารถส่งข้อมูลหมายเลข 5 เพื่อติดต่อกับเพียร์ B ต่อไป จะเห็นได้ว่าวิธีการนี้สามารถลดการใช้แบนด์วิดท์ในการส่งคำร้องขอกระจายทุกทิศทางไปได้มาก จึงช่วยบรรเทาปัญหาการใช้งานแบนด์วิดท์ได้ไม่เต็มประสิทธิภาพของระบบเพียร์ทูเพียร์แบบแยกศูนย์กลางได้มากในระดับหนึ่ง

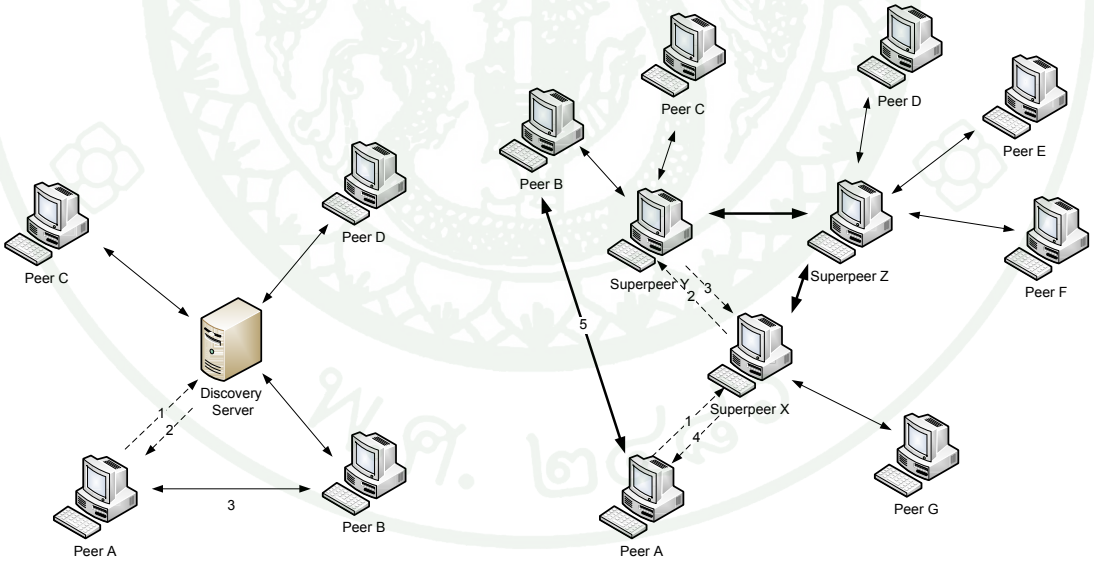
อุปสรรคอย่างหนึ่งของเพียร์ทูเพียร์แยกศูนย์กลางโดยแท้จริงคือ การที่ไม่มีศูนย์กลางทำให้ไม่สามารถมองภาพรวมของระบบได้ จึงเป็นการยากที่จะวิเคราะห์พฤติกรรมของเครือข่ายเพียร์ทูเพียร์ประเภทนี้

2. เพียร์ทูเพียร์แบบผสม (Hybrid Peer-to-Peer)

จะแตกต่างจากเพียร์ทูเพียร์แท้ตรงที่มีเครื่องแม่ข่ายศูนย์กลางในการติดต่อ เก็บรวบรวมข้อมูลทรัพยากรที่มีอยู่ เพียร์ที่ต้องการใช้ทรัพยากรจากเพียร์อื่น จะต้องติดต่อไปยังเครื่องแม่ข่ายเสียก่อน จากนั้นเครื่องแม่ข่ายก็จะส่งที่อยู่ของเพียร์ที่ต้องการติดต่อกลับมา เพียร์ที่ร้องขอจึงจะสามารถติดต่อกับเพียร์ที่ต้องการติดต่อโดยตรงได้ เพียร์ทูเพียร์แบบผสมแบ่งออกเป็นสองชนิดคือ ชนิดการทำดัชนีแบบรวมศูนย์ (Centralized indexing) และ ชนิดการทำดัชนีแบบแยกศูนย์กลาง (Decentralized indexing)

ในส่วนของชนิดการทำดัชนีแบบรวมศูนย์นั้น ดังแสดงในภาพที่ 2 ก. จะมีเครื่องแม่ข่ายศูนย์กลางทำหน้าที่ในการเก็บรักษาดัชนีของข้อมูลหรือไฟล์ ที่เพียร์กำลังแบ่งปันกันอยู่ โดยแต่ละเพียร์จำเป็นจะต้องรักษาการเชื่อมต่อกับเครื่องแม่ข่ายศูนย์กลางเอาไว้ โพรโทคอลที่มีการทำงานได้ลักษณะได้แก่ แนปสเตอร์ (Napster) (Fanning, 2001) ซึ่งมีข้อดีคือมีความรวดเร็วในการค้นหาข้อมูลของเพียร์ และสามารถรับประกันการค้นหาเพียร์ในแต่ละครั้งได้ แต่จุดด้อยของวิธีการนี้อยู่ที่ตัวเครื่องแม่ข่ายศูนย์กลางเอง ที่ถ้าหากล่มแล้วเพียร์อื่น ก็จะไม่สามารถใช้งานได้ อีกทั้งมีข้อจำกัดในการปรับเปลี่ยนขนาดของระบบเครือข่ายเนื่องจากมีข้อจำกัดในเรื่องขนาดของฐานข้อมูล

การทำดัชนีแบบแยกศูนย์กลาง แสดงในภาพที่ 2 ข.เครื่องแม่ข่ายศูนย์กลางจะทำการลงทะเบียนผู้ใช้ในระบบและอำนวยความสะดวกในกระบวนการค้นหาเพียร์ ระบบนี้จะมีซูเปอร์เพียร์ทำหน้าที่เก็บดัชนีกลางของกลุ่มย่อยของเพียร์ การติดต่อกับเพียร์ด้วยกันจะผ่านทางซูเปอร์เพียร์ แต่ไม่ส่งไปให้เพียร์อื่น ๆ โพรโทคอลที่มีลักษณะคล้ายรูปแบบนี้ได้แก่ คาซ่า และ มอร์เฟียส (Morpheus) เพียร์ใดเพียร์หนึ่งในกลุ่มจะถูกเลือกให้เป็นซูเปอร์เพียร์โดยอัตโนมัติ ถ้ามีพลังการประมวลผลและแบนวิดท์ที่เพียงพอ และเครื่องแม่ข่ายศูนย์กลางก็จะส่งรายชื่อของเพียร์ที่ประกอบด้วยซูเปอร์เพียร์มาให้เพื่อใช้ในการติดต่อไปยังซูเปอร์เพียร์อื่น ๆ ข้อดีของรูปแบบนี้เมื่อเทียบกับเพียร์ทูเพียร์แท้คือสามารถลดเวลาในการค้นหาเพียร์และก็ยังสามารถลดการติดต่อสื่อสารระหว่างเพียร์ด้วยกันเองส่งผลให้เครือข่ายได้รับแบนด์วิดท์เพิ่มขึ้น จุดเด่นเมื่อเปรียบเทียบกับการทำดัชนีแบบรวมศูนย์ก็คือลดภาระงานให้กับเครื่องแม่ข่ายศูนย์กลาง แต่ก็ต้องแลกมาซึ่งเวลาในการค้นหาเพียร์ที่เพิ่มขึ้น และข้อดีอีกจุดหนึ่งก็คือมีความทนทานต่อความล้มเหลวของระบบสูง เนื่องจากการที่ไม่มีเครื่องแม่ข่ายกลางเพียงจุดเดียว เมื่อเกิดปัญหาซูเปอร์เพียร์ตัวใดตัวหนึ่งล่ม เพียร์ที่เชื่อมต่อกับตัวที่ล่มก็จะไปเชื่อมต่อกับซูเปอร์เพียร์ตัวอื่น เครือข่ายก็จะทำงานต่อไปได้ และในกรณีที่เกิดซูเปอร์เพียร์ล่มพร้อมกันหลายตัว เพียร์ที่เหลืออยู่ก็จะกลายสภาพเป็นซูเปอร์เพียร์เสียเอง



ก. Hybrid peer-to-peer with centralized index ข. Hybrid peer-to-peer with decentralized index

ภาพที่ 2 ลักษณะโครงสร้างของเพียร์ทูเพียร์แบบผสม

ภาพที่ 2 ก. แสดงขั้นตอนการทำงานในระบบเพียร์ทูเพียร์แบบผสมที่มีการทำดัชนีแบบรวมศูนย์ เริ่มต้นทุกเพียร์ในระบบจะมีการติดต่อประสานงานกับเครื่องแม่ข่ายศูนย์กลางเป็นระยะ เมื่อ

เพียร์ A ต้องการจะติดต่อกับเพียร์ B จะส่งคำร้องขอหมายเลข 1 ไปยังเครื่องแม่ข่ายศูนย์กลาง ซึ่งมีฐานข้อมูลที่อยู่ของทุกเพียร์ในระบบ และยังมีดัชนีชี้นส่วนของไฟล์ที่แต่ละเพียร์ครอบครองอยู่ เมื่อแม่ข่ายได้รับคำร้องขอจากเพียร์ A ก็จะทำการส่งข้อมูลหมายเลข 2 ซึ่งบรรจุที่อยู่ของเพียร์ B ให้กับเพียร์ A เมื่อเพียร์ A ได้รับที่อยู่ของเพียร์ B แล้วก็จะสามารถส่งคำร้องขอการเชื่อมต่อหมายเลข 3 ไปยังเพียร์ B และสามารถติดต่อสื่อสารกันได้โดยตรง ถึงแม้ระบบนี้จะมีจุดเด่นในเรื่องการใช้แบนด์วิทด์ได้อย่างมีประสิทธิภาพ แต่ข้อเสียที่สำคัญคือมีความทนทานต่อความล้มเหลวต่ำ หากเครื่องแม่ข่ายศูนย์กลางล่ม เพียร์ทุกเพียร์ก็จะไม่สามารถติดต่อถึงกันได้ ทั้งระบบก็จะล่มตามไปด้วย

ภาพที่ 2 ข. แสดงขั้นตอนการทำงานในระบบเพียร์ทูเพียร์แบบผสมที่มีการทำดัชนีแบบแยกศูนย์กลาง โดยมีซูเปอร์เพียร์ทำหน้าที่แทนเครื่องแม่ข่ายศูนย์กลาง แต่จะเก็บที่อยู่เพียร์และดัชนีของชิ้นส่วนเฉพาะเพียร์ที่อยู่ในกลุ่มเท่านั้น เริ่มต้นทุกเพียร์ในแต่ละกลุ่มจะมีการติดต่อประสานงานกับเครื่องซูเปอร์เพียร์ของกลุ่มอยู่เป็นระยะ และในแต่ละซูเปอร์เพียร์ในระบบก็จะมีการติดต่อประสานงานกันอย่างเป็นระยะเช่นกัน เมื่อเพียร์ A ที่อยู่ในกลุ่มของซูเปอร์เพียร์ X ต้องการจะติดต่อกับเพียร์ B ก็จะส่งคำร้องขอหมายเลข 1 ไปยังซูเปอร์เพียร์ X ที่เป็นหัวหน้ากลุ่ม เมื่อซูเปอร์เพียร์ X ได้รับคำร้องขอจากเพียร์ A ก็จะส่งต่อคำร้องหมายเลข 2ไปยังซูเปอร์เพียร์ Y ซึ่งเป็นหัวหน้ากลุ่มของเพียร์ B เมื่อได้รับคำร้องขอซูเปอร์เพียร์ Y ก็จะทำการส่งที่อยู่หมายเลข 3 ของเพียร์ B กลับมาให้ซูเปอร์เพียร์ X หลังจากนั้นซูเปอร์เพียร์ X จะส่งข้อมูลที่อยู่ของเพียร์ B หมายเลข 4 ที่รับมาจากซูเปอร์เพียร์ Y ให้แก่เพียร์ A เมื่อเพียร์ A ได้รับข้อมูลที่อยู่ของเพียร์ B เรียบร้อยแล้วก็จะสามารถส่งข้อมูลติดต่อประสานงานหมายเลข 5 ไปยังเพียร์ B ได้โดยตรง ซึ่งถ้าหากในเวลาต่อมาซูเปอร์เพียร์ Y เกิดล่ม เพียร์ในกลุ่มของซูเปอร์เพียร์ Y ก็จะมาเข้าร่วมกลุ่มกับกลุ่มใกล้เคียงอย่างกลุ่มซูเปอร์เพียร์ X หรือ ซูเปอร์เพียร์ Z แทน แต่ถ้าเกิดในเวลาต่อมาซูเปอร์เพียร์ X และ Z เกิดล่มตามไปด้วย หนึ่งในเพียร์ที่อยู่ในกลุ่มก็จะถูกคัดเลือกให้ทำหน้าที่ซูเปอร์เพียร์แทน และสร้างกลุ่มขึ้นมาใหม่ จึงทำให้ระบบนี้ทนทานต่อความล้มเหลวมาก

โพรโทคอลบิตทอร์เรนต์

โพรโตคอลบิตทอร์เรนต์ (BitTorrent Protocol) (Cohen,2003) เป็นโพรโทคอลแบบเพียร์ทูเพียร์ที่พัฒนาโดย Bram Cohenในปี 2001 ออกแบบมาเพื่อใช้สำหรับการแลกเปลี่ยนไฟล์บนระบบเครือข่าย ไฟล์ต้นฉบับจะถูกตัดแบ่งเป็นชิ้นเล็ก ๆ (pieces) และกระจายไปยังเพียร์อื่น ๆ ที่ต้องการดาวน์โหลดไฟล์ต้นฉบับ ด้วยอัลกอริทึม Rarest First จะเลือกชิ้นส่วนให้แต่ละเพียร์ที่ต้องการ

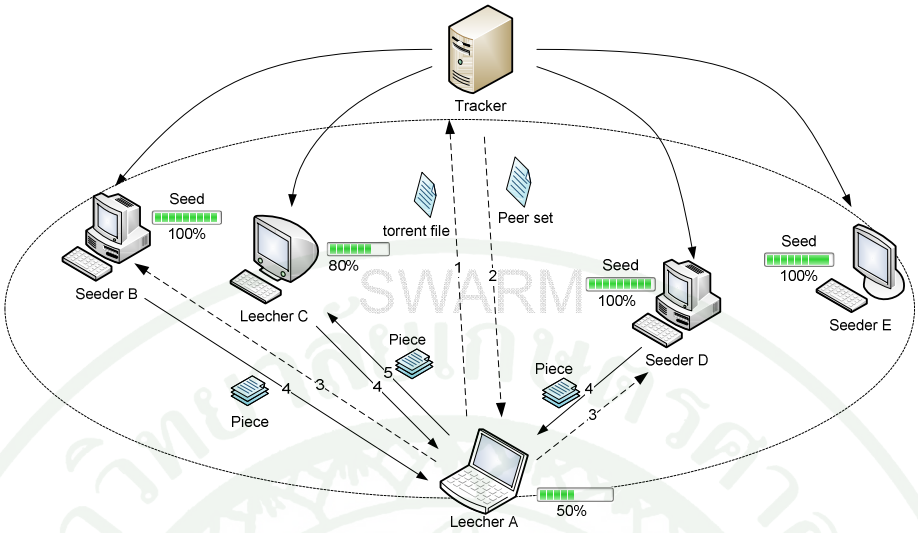
ดาวน์โหลดไฟล์มีชิ้นส่วนแตกต่างกันมากที่สุด และแก้ปัญหาชิ้นส่วนสุดท้าย (Last Piece Problem) (Cohen, 2003) โพรโทคอลบิตทอร์เรนต์ประกอบไปด้วยส่วนสำคัญหลัก ดังนี้

ไฟล์ทอร์เรนต์ (Torrent file) ไฟล์ที่มีนามสกุล .torrent ซึ่งเก็บข้อมูลเกี่ยวกับไฟล์ต้นฉบับ (เช่น ขนาดไฟล์, จำนวนชิ้นส่วน, ขนาดชิ้นส่วนเป็นต้น)

แทรกเกอร์ (Tracker) เป็นเครื่องแม่ข่ายที่คอยจัดการดูแลสถานะของเพียร์แต่ละตัวและส่งรายชื่อของเพียร์ให้กับเพียร์ที่ร้องขอ

เพียร์ (Peers) เป็นเครื่องต่าง ๆ ที่เชื่อมต่อกันเพื่อการดาวน์โหลดหรืออัพโหลดไฟล์ เรียกกลุ่มเพียร์ที่ทำการรับ-ส่งไฟล์ที่ใช้ไฟล์ทอร์เรนต์เดียวกันว่า สวอร์ม (Swarm) เพียร์ที่มีไฟล์ต้นฉบับทุกชิ้นจะเป็นผู้อัพโหลดไฟล์เรียกว่า ซีดเดอร์ (Seeder) เพียร์ที่มีไฟล์ต้นฉบับบางส่วนจะทำการดาวน์โหลดไฟล์จะเรียกว่า ลีชเชอร์ (Leecher) โดยโพรโทคอลบิตทอร์เรนต์ อาจกำหนดให้มีอย่างน้อย 1 ซีดเดอร์ ในสวอร์มเพื่อที่จะรับประกันว่า เพียร์ในสวอร์มจะสามารถดาวน์โหลดชิ้นส่วนของไฟล์ได้ครบทุกชิ้นและลีชเชอร์ยังสามารถอัพโหลดชิ้นส่วนที่ตัวเองมีให้กับเพียร์อื่น ในเวลาเดียวกันกับที่กำลังดาวน์โหลดชิ้นส่วนไฟล์ได้อีกด้วย

การใช้งานบิตทอร์เรนต์เริ่มต้นจะต้องได้มาซึ่งไฟล์ทอร์เรนต์ อาจดาวน์โหลดมาจากเว็บแทรกเกอร์ หรือจากวิธีการอื่น ๆ แล้วจึงเปิดใช้ด้วยโปรแกรมบิตทอร์เรนต์ไคลเอนต์ เช่น µTorrent (Strigeus, 2005) หรือ BitComet (BitComet Development Group, 2003) เป็นต้น จากนั้นบิตทอร์เรนต์ไคลเอนต์จะดึงข้อมูลยูอาร์แอล (URL) ของแทรกเกอร์ที่อยู่ในไฟล์ทอร์เรนต์ เพื่อจัดส่งข้อมูลในไฟล์ทอร์เรนต์ได้แก่ รหัสเพียร์ (Peer ID), ที่อยู่ไอพี (IP Address), หมายเลขพอร์ตที่เปิดรอ (Listening Port) รวมถึงค่าแฮช (Hash) ของไฟล์ทอร์เรนต์ไปยังแทรกเกอร์ผ่านโพรโทคอลทีซีพี (TCP) เมื่อแทรกเกอร์ได้ข้อมูลก็จะทำการสุ่มรายชื่อเพียร์ในสวอร์ม จำนวน 50 เพียร์ (โดยค่าปริยาย) ส่งมาให้บิตทอร์เรนต์ไคลเอนต์ บิตทอร์เรนต์ไคลเอนต์ก็จะใช้โพรโทคอลทีซีพีเปิดการเชื่อมต่อกับกลุ่มเพียร์ที่ได้รายชื่อมา เรียกกลุ่มเพียร์ที่มีการเชื่อมต่อกันเหล่านี้ว่าเพียร์เซต (Peer set)

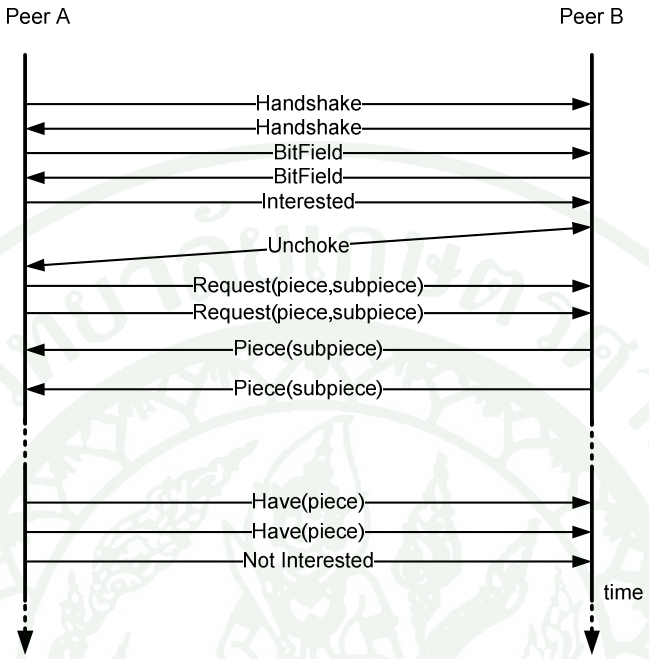


ภาพที่ 3 องค์ประกอบของบิตทอร์เรนต์และขั้นตอนการทำงาน

ภาพที่ 3 แสดงส่วนประกอบสำคัญต่าง ๆ ของบิตทอร์เรนต์ ได้แก่ ไฟล์ทอร์เรนต์, แทรกเกอร์, ซีดเดอร์, และลีชเชอร์ อีกทั้งยังแสดงขั้นตอนการทำงานของบิตทอร์เรนต์ เริ่มต้นเพียร์ A ซึ่งทำหน้าที่เป็นลีชเชอร์เปิดไฟล์ทอร์เรนต์ด้วยโปรแกรมบิตทอร์เรนต์ไคลเอนต์ โปรแกรมบิตทอร์เรนต์ก็จะส่งข้อมูลหมายเลข 1 ที่อยู่ในไฟล์ทอร์เรนต์ ไปยังที่อยู่แทรกเกอร์ที่ระบุไว้ในไฟล์เช่นกัน เมื่อแทรกเกอร์ได้รับข้อมูลก็จะเลือกเพียร์ที่อยู่ในสวอร์มมาทำเพียร์เซต ซึ่งในที่นี้เพียร์เซตจะประกอบด้วยซีดเดอร์ B, ลีชเชอร์ C, และซีดเดอร์ D จากนั้นแทรกเกอร์จะส่งข้อมูลเพียร์เซตหมายเลข 2 กลับมายังลีชเชอร์ A เมื่อลีชเชอร์ A ได้รับข้อมูลเพียร์เซตแล้วก็จะทำการส่งข้อมูลร้องขอหมายเลข 3 ไปยังเพียร์ที่มีรายชื่อในเพียร์เซต เมื่อเพียร์ต่าง ๆ ได้รับข้อมูลร้องขอก็จะส่งข้อมูลหมายเลข 4 ซึ่งเป็นชิ้นส่วนไฟล์ กลับคืนให้กับลีชเชอร์ A และในระหว่างการดาวน์โหลดหากลีชเชอร์ A มีชิ้นส่วนข้อมูลใดที่ลีชเชอร์ C ต้องการแล้ว ก็จะทำการส่งข้อมูลหมายเลข 5 ที่เป็นชิ้นส่วนไฟล์ไปให้กับลีชเชอร์ C ด้วย

เมื่อสร้างกลุ่มเพียร์เซตแล้วโพรโทคอลบิตทอร์เรนต์จะใช้ข้อความ (Message) ในการควบคุมและประสานจังหวะการทำงานของแต่ละเพียร์ให้ทำงานสอดคล้องกัน โดยเพียร์จะใช้ Handshake message ในการพิสูจน์ตัวตนของเพียร์อีกฝ่าย สมมติให้เพียร์ A ต้องการจะติดต่อกับเพียร์ B เพียร์ A ก็จะส่ง Handshake message ซึ่งประกอบด้วยค่ารหัสแทรกเกอร์ และค่าแฮชของไฟล์ ไปยังเพียร์ B ผ่านทางโพรโทคอลทีซีพี เมื่อเพียร์ B ได้รับ Handshake message แล้วก็จะตอบ

กลับด้วยการส่ง Handshake message คืนให้กับเพียร์ A จากนั้นเพียร์ A จะทำการตรวจสอบรหัสแทรกเกอร์และค่าแฮชไฟล์ว่าตรงกันหรือไม่ หากไม่ตรงกันก็จะตัดการเชื่อมต่อทันที



ภาพที่ 4 ขั้นตอนการติดต่อและรับ-ส่งไฟล์ระหว่างเพียร์ของโพรโทคอลบิตทอร์เรนต์

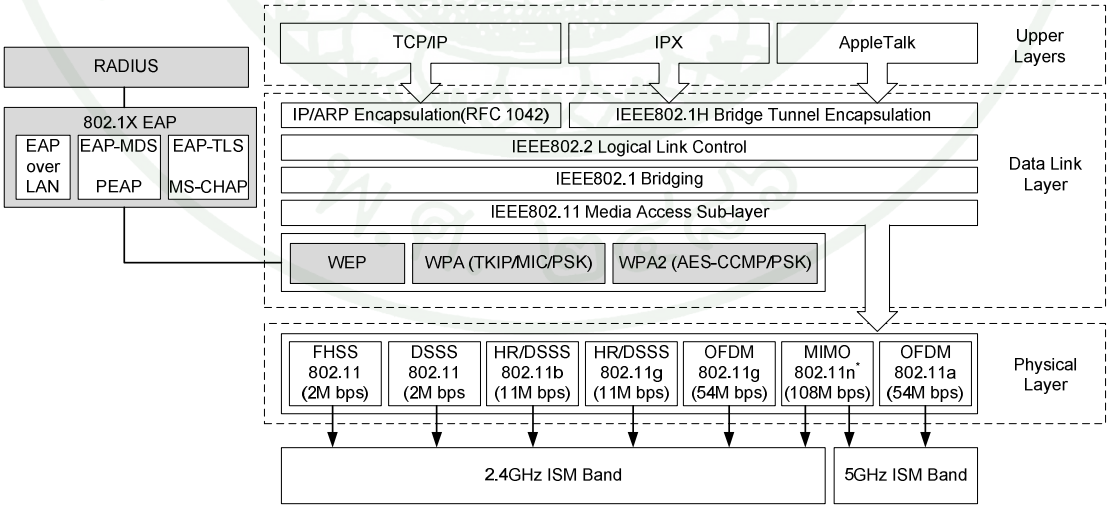
หลังจากผ่านกระบวนการ Handshake เรียบร้อยแล้ว เพียร์จะตั้งสถานะเริ่มต้นของอีกฝ่ายให้เป็นสถานะ not Interest และ Choke เช่น เพียร์ A ได้รับ Handshake จากเพียร์ B แล้วก็จะกำหนดค่าให้สถานะเริ่มต้นของเพียร์ B เป็น Not Interest หมายความว่า เพียร์ B ไม่ต้องการชิ้นส่วนจากเพียร์ A และ ค่าสถานะเริ่มต้นเป็น Choke หมายถึง เพียร์ A ไม่อนุญาตให้อัพโหลดข้อมูลไปยังเพียร์ B จากนั้นทั้งสองฝ่ายจะส่งข้อความ BitField ให้แก่กันและกัน และจะส่งครั้งเดียวเท่านั้น ซึ่งใน BitField จะประกอบด้วยดัชนีของชิ้นส่วนแต่ละชิ้นในไฟล์ที่ดาวน์โหลด BitField จึงมีขนาดไม่คงที่ และด้วยเหตุนี้ แต่ละเพียร์จึงสามารถรับรู้ว่าอีกฝ่ายมีชิ้นส่วนใดอยู่บ้าง เมื่อตรวจพบว่าอีกฝ่ายมีชิ้นส่วนที่ต้องการก็จะส่งข้อความ Interested ไปให้อีกฝ่าย เพียร์อีกฝ่ายจะรับรู้ว่าตนเองมีชิ้นส่วนที่อีกฝ่ายต้องการดาวน์โหลดเมื่อได้รับข้อความ Interested นี้เอง ถ้าเพียร์ที่เป็นเจ้าของชิ้นส่วนอนุญาตก็จะส่งข้อความ Unchoked กลับไป เมื่อเพียร์ผู้ร้องขอได้รับข้อความ Unchoked กลับมา ก็จะส่งข้อความ Request ไปยังเพียร์เจ้าของชิ้นส่วนเพื่อบ่งบอกว่าตนเองต้องการชิ้นส่วนใดและเริ่มจากตำแน่งที่เท่าใดของชิ้นส่วนนั้น โดยการตัดสินใจที่จะอนุญาตให้ดาวน์โหลดหรือไม่นั้นจะอาศัยขั้นตอนวิธีการเค้น (Choke Algorithm) เป็นตัวตัดสินใจ หลังจากการร้องขอชิ้นส่วนเรียบร้อยแล้วจึงเริ่มการส่งข้อมูลที่ละชิ้นส่วนย่อย (Sub-piece) และในระหว่างดาวน์โหลดชิ้นส่วน

เพียร์ที่ได้รับชิ้นส่วนแล้วจะส่งข้อความ Have ไปยังเพียร์อื่น ๆ ที่อยู่ในเพียร์เซต เพื่อแจ้งให้เพียร์อื่นทราบว่าตนเองได้มีชิ้นส่วนนี้ให้ดาวน์โหลดแล้ว และเมื่อดาวน์โหลดเสร็จก็จะส่งข้อความ Not Interested ออกไปเพื่อบ่งบอกว่าตนเองไม่ต้องการชิ้นส่วนใด ๆ แล้ว ขั้นตอนการติดต่อกันระหว่างเพียร์สามารถแสดงดังภาพที่ 4

ระหว่างการรับ-ส่งชิ้นส่วนของไฟล์ เพียร์จะทำการส่งข้อมูลต่าง ๆ ไปยังแทรกเกอร์ เช่น ค่าดาวน์โหลด ค่าอัพโหลด เป็นต้น และจะร้องขอรายชื่อเพียร์ชุดใหม่จากแทรกเกอร์ หากพบว่าจำนวนเพียร์เซตมีค่าต่ำกว่าค่าโดยปริยาย

มาตรฐานเครือข่ายไร้สายแบบ IEEE802.11

มาตรฐานเครือข่ายไร้สายแบบ IEEE802.11 (อนันต์, 2550) เป็นส่วนหนึ่งของมาตรฐาน IEEE802 ที่ประกาศใช้โดยสถาบันสำหรับวิศวกรรมไฟฟ้าและอิเล็กทรอนิกส์ (IEEE : Institute for Electrical and Electronic Engineers) ที่ถูกกำหนดรายละเอียดในการทำงานที่ชั้นกายภาพและชั้นแม็ค (MAC Layer) ของชั้นดาต้าลิงค์ (Data Link) และในชั้นกายภาพก็มีการกำหนดมาตรฐานการใช้งานสื่อแต่ละประเภทแยกย่อยลงไปอีก สามารถแสดงชั้นการทำงานของ IEEE802.11 เมื่อเทียบกับแบบจำลองโอเอสไอ (OSI Model) ได้ ดังภาพที่ 5

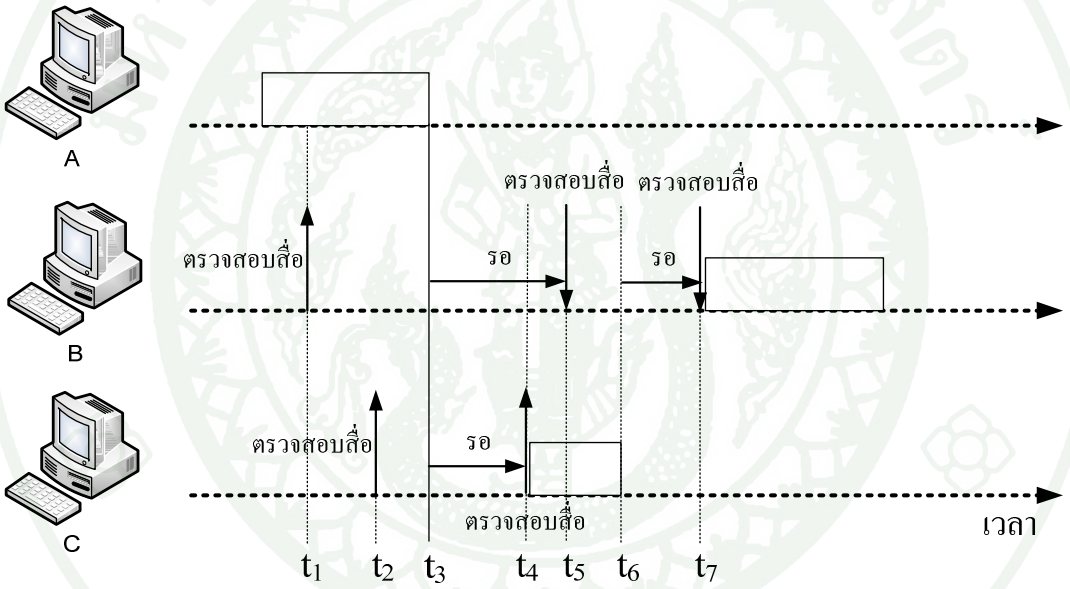


ภาพที่ 5 โพรโทคอลสแต็คของ IEEE802.11

ที่มา: http://www.javvin.com/pics/80211.gif (2010)

การเข้าใช้งานสื่อแบบซีเอสเอ็มเอ/ซีเอ

ด้วยคุณลักษณะเฉพาะของมาตรฐานเครือข่ายไร้สาย IEEE802.11 ที่ไม่มีคุณสมบัติการรับรู้เหมือนกันทุกโหนด (Single Experience) เหมือนกับเครือข่ายใช้สาย จึงจำเป็นที่มีกลไกการใช้งานสื่อแบบเฉพาะ ซึ่งตามมาตรฐาน IEEE802.11 ได้กำหนดให้ใช้กลไกการเข้าใช้งานสื่อแบบ ซีเอสเอ็มเอ/ซีเอ (CSMA/CA : Carrier Sense Multiple Access with Collision Avoidance) คือกำหนดให้มีการสุ่มเวลารอก่อนที่จะส่งข้อมูลหนึ่ง ๆ ออกไป หากครบเวลารอแล้ว ให้ทำการตรวจสอบสื่ออีกครั้ง ว่าสื่อมีอุปกรณ์อื่น ๆ ใช้งานอยู่อีกหรือไม่ หากไม่มีจึงจะสามารถส่งข้อมูลออกไปได้ ทั้งนี้เพื่อลดโอกาสการเกิดการชนกันของข้อมูลให้มากที่สุด



ภาพที่ 6 กลไกการเข้าใช้สื่อแบบซีเอสเอ็มเอ/ซีเอ

ในภาพที่ 6 เป็นการอธิบายกลไกการทำงานของซีเอสเอ็มเอ/ซีเอ เริ่มต้นด้วย สถานี A กำลังใช้งานสื่อเพื่อรับ-ส่งข้อมูลอยู่ ณ เวลา t_1 สถานี B ต้องการจะใช้สื่อจึงได้ทำการตรวจสอบสื่อว่าสื่อว่างหรือไม่ ซึ่งพบว่าสื่อไม่ว่าง สถานี B จึงต้องรอให้สถานี A ส่งข้อมูลเสร็จเสียก่อน ในระหว่างนั้น ณ เวลา t_2 สถานี C ก็ได้ทำการตรวจสอบสื่อ เพื่อเข้าใช้สื่อเช่นเดียวกัน แล้วก็พบว่าสื่อไม่ว่าง เนื่องจากสถานี A ใช้สื่ออยู่ จึงต้องรอจนกว่าสถานี A จะใช้สื่อเสร็จ ต่อมา ณ เวลา t_3 ที่สถานี A ใช้สื่อเสร็จเรียบร้อยแล้ว หาก สถานี B และ C เริ่มทำการส่งข้อมูลทันทีหลังจากสิ้นสุดการรอให้สถานี A ใช้สื่อเสร็จ ก็จะเกิดการชนกันของข้อมูลทันที กลไกซีเอสเอ็มเอ/ซีเอจึงกำหนดให้ทั้งสถานี B และ C ทำการสุ่มเวลารอใหม่อีกครั้ง ซึ่งสถานี C สุ่มได้เวลารอน้อยกว่า สถานี B ที่เวลา t_4 เมื่อ

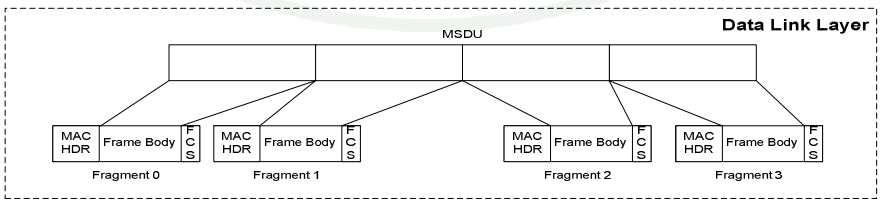
สถานี C สิ้นสุดระยะเวลาการรอจึงได้ทำการตรวจสอบสื่ออีกครั้งแล้วพบว่าสื่อว่าง จึงเริ่มทำการใช้สื่อ ต่อมา ณ เวลา t_5 สถานี B สิ้นสุดระยะเวลาการรอจึงได้ทำการตรวจสอบสื่อแล้วพบว่าสื่อไม่ว่าง ต้องรอจนกว่าสถานี C จะใช้งานเสร็จ ที่เวลา t_6 สถานี B ทราบว่าสถานี C ใช้งานสื่อเสร็จเรียบร้อยแล้วจึงสุ่มเวลาการรอใหม่ เมื่อสิ้นสุดระยะเวลาการรอ ที่เวลา t_7 สถานี B จึงทำการตรวจสอบสื่ออีกครั้งแล้วพบว่าสื่อว่าง จึงได้ทำการเข้าใช้สื่อในการรับ-ส่งข้อมูล

เฟรมของมาตรฐาน IEEE802.11

เฟรมของมาตรฐาน IEEE802.11 (Brenner,1997) ถูกออกแบบให้มีขนาดเล็ก ซึ่งแตกต่างจากเฟรมของเครือข่ายแบบมีสายที่สามารถมีขนาดใหญ่ได้ถึง 1516 ไบต์ ทั้งนี้เนื่องจากคุณลักษณะเฉพาะของเครือข่ายไร้สาย ที่ทำงานบนคลื่นความถี่จึงทำให้ความผิดพลาดทางบิต (BER : Bit Error Rate) มีอัตราที่สูง โอกาสที่ข้อมูลจะเสียหายเนื่องจากใช้เฟรมขนาดใหญ่จึงมีมาก ยิ่งไปกว่านี้หากข้อมูลที่ส่งไปเสียหายอาจอันเนื่องมาจากสัญญาณรบกวน หรือการชนกันของข้อมูล ก็ต้องทำการส่งข้อมูลใหม่ การออกแบบให้เฟรมมีขนาดเล็กจะสามารถสูญเสียค่าใช้จ่ายของการเสียแบนด์วิดท์เบื้องต้น (Overhead) ในปริมาณที่น้อย

อย่างไรก็ตามมาตรฐาน IEEE802.11 ได้กำหนดให้มีกลไกการแยกส่วนเฟรมและการรวมเฟรม (Fragmentation/Reassembly) ไว้ที่ชั้นแม็ค เพื่อให้รองรับกับการรับ-ส่งข้อมูลที่มีขนาดใหญ่ได้ถึง 1516 ไบต์ ที่ใช้งานบนเครือข่ายใช้สาย โดยกลไกนี้อาศัยอัลกอริทึม ส่งและรอ (Send-and-Wait) (Brenner, 1997) โดยกำหนดให้แต่ละสถานีที่กำลังส่งชิ้นส่วนเฟรมไปจะไม่ได้รับการอนุญาตให้ส่งชิ้นส่วนใหม่จนกว่าจะเข้าเงื่อนไขข้อใดข้อหนึ่งดังต่อไปนี้

1) จนกว่าจะได้รับ ACK ตอบกลับจาก ชิ้นส่วนนั้น
2) ตัดสินใจว่าชิ้นส่วนที่ทำการส่งไปใหม่นั้นไม่ได้รับและทำการโละข้อมูลทั้งเฟรมทิ้ง



ภาพที่ 7 MSDU และ MPDUs

ที่มา: http://www.sss-mag.com/pdf/802_11tut.pdf (2008)

ภาพที่ 7 เป็นการแสดงรายละเอียดของเฟรม (MSDU : MAC Service Data Unit) ที่ถูกตัดแบ่งเป็นชิ้นส่วนเฟรม (MPDUs : MAC Protocol Data Units)

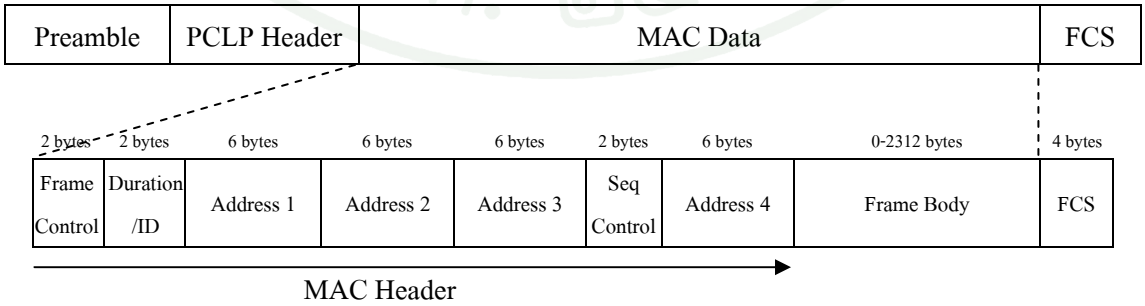
โครงสร้างเฟรม

มาตรฐาน IEEE802.11 ได้กำหนดเฟรมให้กับสถานีไร้สาย เพื่อใช้ในการติดต่อสื่อสาร ควบคุมและจัดการการใช้งานเครือข่ายไร้สายไว้หลายชนิดด้วยกัน เฟรมที่ใช้ในการติดต่อสื่อสารตามที่กำหนดไว้ในมาตรฐาน IEEE802.11 แบ่งออกเป็น 3 ประเภท ได้แก่ เฟรมการจัดการ (Management Frame) เฟรมควบคุม (Control Frame) และเฟรมข้อมูล (Data Frame) โดยทุก ๆ เฟรมของมาตรฐาน IEEE802.11 จะประกอบด้วยส่วนพรีเอมเบิ้ล (Preamble) ซึ่งใช้ในการประสานจังหวะ ถัดมาจะเป็นส่วนหัวพีแอลซีพี (PCLP Header) ที่ภายในเก็บข้อมูลทางตรรกะ (Logical) ที่ใช้เป็นตัวถอดรหัสเฟรมที่ชั้นกายภาพ และส่วนข้อมูลแม็ค (MAC Data) แสดงได้ดังภาพที่ 8

ภาพที่ 8 โครงสร้างเฟรม

ส่วนข้อมูลแม็ค

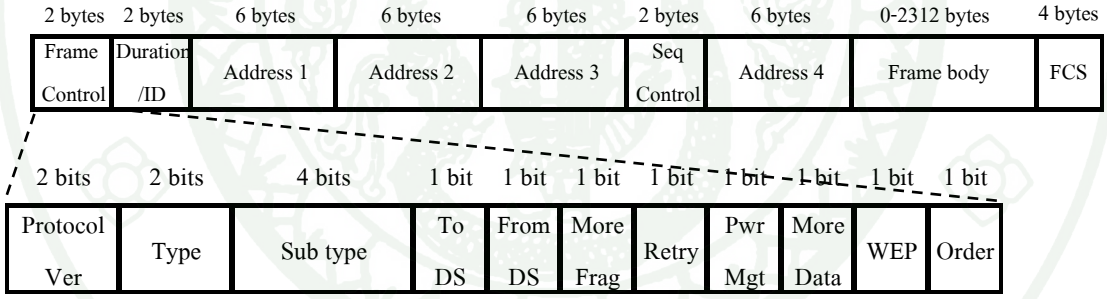
โครงสร้างของเฟรมที่นอกเหนือจากส่วนพรีเอ็มเบิ้ลและส่วนหัวพีแอลซีพี จะแยกเป็น 3 ส่วนได้แก่ ส่วนหัวแม็ค (MAC Header) ส่วนตัวเฟรม (Frame Body) และ ส่วนการตรวจสอบความผิดพลาดของเฟรม (FCS : Frame Check Sequence) ดังแสดงในภาพที่ 9



ภาพที่ 9 ส่วนข้อมูลแม็ค

จากภาพที่ 9 แสดงให้เห็นถึงรายละเอียดแต่ละไบต์ของเฟรม ซึ่ง 2 ไบต์แรกจะเป็นส่วนควบคุมเฟรม (Frame Control) ถัดมาอีก 2 ไบต์ จะเป็นส่วนช่วงเวลา (Duration) ซึ่งจะเก็บค่าระยะเวลาที่ใช้สำหรับการคำนวณเวลารอการส่งข้อมูล ถัดมาจะเป็นส่วนที่อยู่แม็ค (MAC Address) ขนาด 6 ไบต์ จำนวน 4 ชุด และ มีส่วนลำดับเฟรม (Sequence Control) จะบ่งบอกถึงลำดับของเฟรมรวมถึงหมายเลขชิ้นส่วนของเฟรมหากเฟรมมีการแยกส่วนกันส่ง

ในส่วนควบคุมเฟรมจะประกอบด้วย ค่าของรุ่นโพรโทคอล (Protocol Version) เป็น 2 บิตแรก ถัดมาเป็นส่วนประเภทเฟรมและประเภทเฟรมย่อย (Type และ SubType) ซึ่งบ่งบอกประเภทต่าง ๆ ของเฟรมมีขนาดรวม 6 บิต ส่วนถัดจากนี้จะมีขนาด 1 บิตจะเป็นประเภทของที่อยู่เฟรม (ToDS และ FromDS) ส่วนระบุสถานะการแบ่งชิ้นส่วนเฟรม (More Fragment) ส่วนระบุสถานะการส่งเฟรมซ้ำ (Retry) ส่วนระบุสถานะการประหยัดพลังงาน (Power Management) ส่วนระบุสถานะการมีเฟรมตามมาเพิ่มเติม (More Data) ส่วนระบุสถานะการเข้ารหัสข้อมูล (WEP : Wired Equivalent Privacy) และส่วนระบุลำดับเฟรม (Order) โครงสร้างของแต่ละส่วนสามารถแสดงได้ดังภาพที่ 10



ภาพที่ 10 ส่วนควบคุมเฟรม

ในส่วนของประเภทเฟรมและประเภทเฟรมย่อยที่มีขนาด 6 บิต สามารถแบ่งเป็นประเภทต่าง ๆ ตามตารางที่ 1

ตารางที่ 1 รายละเอียดประเภทเฟรมและประเภทเฟรมย่อย

ประเภทเฟรม	ประเภทเฟรมย่อย	รายละเอียด
00	0000	การร้องขอร่วมเครือข่าย (Associate Request)
00	0001	การตอบการร้องขอร่วมเครือข่าย (Associate Response)

ตารางที่ 1 (ต่อ)

ประเภทเฟรม	ประเภทเฟรมย่อย	รายละเอียด
00	0010	การร้องขอร่วมเครือข่ายใหม่ (Re-Associate Request)
00	0011	การตอบการร้องขอร่วมเครือข่ายใหม่ (Re-Associate Response)
00	0100	การร้องขอการตรวจสอบ (Probe Request)
00	0101	การตอบการร้องขอการตรวจสอบ (Probe Response)
00	1101-1111	จองเผื่ออนาคต (Reserved)
00	1000	บีคอน (Beacon)
00	1001	เอทิม (ATIM : Announcement Traffic Indication Map)
00	1010	การขอยกเลิกการร่วมเครือข่าย (Disassociation)
00	1011	การพิสูจน์ตัวจริง (Authentication)
00	1100	การขอยกเลิกการพิสูจน์ตัวจริง (Deauthentication)
00	1101-1111	จองเผื่ออนาคต (Reserved)
01	0000-1001	จองเผื่ออนาคต (Reserved)
01	1010	โพลประหยัดพลังงาน (Power-Save Poll)
01	1011	ร้องขอที่จะส่งข้อมูลอาร์ทีเอส (RTS :Request-to-Send)
01	1100	ตอบรับการร้องขอที่จะส่งข้อมูลซีทีเอส (CTS : Clear-to-Send)
01	1101	การตอบแอ็ค (ACK : Acknowledgement)
01	1110	การจบช่วงการแย่งเข้าใช้สื่อ (CF End : Contention Free End)
01	1111	การจบช่วงการแย่งเข้าใช้สื่อ + การตอบแอ็ค (CF End + CF-ACK)
10	0000	ข้อมูล
10	0001	ข้อมูล + CF-ACK
10	0010	ข้อมูล + CF-Poll
10	0011	ข้อมูล + CF-ACK + CF-Poll
10	0100	ไม่มีข้อมูล (Null)
10	0101	CF-ACK
10	0110	CF-Poll

ตารางที่ 1 (ต่อ)

ประเภทเฟรม	ประเภทเฟรมย่อย	รายละเอียด
10	0111	CF-ACK + CF-Poll
10	1000-1111	จองเผื่ออนาคต (Reserved)
11	0000-1111	จองเผื่ออนาคต (Reserved)

ในส่วนช่วงเวลา จะเก็บค่าของรหัสสถานี (Station ID) ในกรณีที่เป็นเฟรมข้อความของการประหยัดพลังงาน (PS-Poll : Power Save Poll) นอกนั้นจะใช้เก็บค่าของระยะเวลาการรอคอย

ในส่วนของที่อยู่ (Address) ที่มีอยู่ 4 ชุด ซึ่งค่าในแต่ละชุดจะขึ้นอยู่กับค่าของ ToDS และ FromDS ที่อยู่ในส่วนควบคุมเฟรมซึ่งมีรายละเอียดดังนี้

ที่อยู่ 1 จะเป็นค่าที่อยู่ของสถานีผู้รับเสมอ ถ้าค่า ToDS เป็น 1 จะเป็นค่าที่อยู่ของแอคเซสพ้อยท์ (AP : Access Point) ซึ่งเป็นชื่อของเครือข่าย (BSSID : Basic Service Set ID) ถ้าค่า ToDS เป็น 0 จะเป็นค่าที่อยู่ของสถานีผู้รับปลายทาง (DA : Destination Address) และเป็นค่าของที่อยู่แอคเซสพ้อยท์ผู้รับระหว่างทาง (RA : Receiver Address) ในกรณีที่ค่าของ ToDS และ FromDS เป็น 1

ที่อยู่ 2 จะเป็นค่าที่อยู่ของสถานีผู้ส่งเสมอ ถ้าค่า FromDS เป็น 1 จะเป็นค่าที่อยู่ของแอคเซสพ้อยท์ ถ้าค่า FromDS เป็น 0 จะเป็นค่าที่อยู่ของสถานีผู้รับต้นทาง (SA : Source Address) และจะเป็นค่าของที่อยู่แอคเซสพ้อยท์ผู้ส่งระหว่างทาง (TA : Transmitter Address) ในกรณีที่ค่าของ ToDS และ FromDS เป็น 1

ที่อยู่ 3 จะเป็นค่าของที่อยู่ในส่วนที่เหลือ กล่าวคือถ้าค่า FromDS เป็น 1 จะเป็นค่าที่อยู่ของสถานีผู้ส่งต้นทาง และถ้าค่า ToDS เป็น 1 จะเป็นค่าที่อยู่ผู้รับปลายทาง

ที่อยู่ 4 ใช้ในกรณีที่มีการใช้ระบบโครงสร้างการให้บริการแบบขยายผ่านเครือข่ายไร้สาย (Wireless Distribution System) ที่มีการรับ-ส่งข้อมูลของเฟรมจากแอคเซสพ้อยท์ตัวหนึ่งไปยังแอคเซสพ้อยท์อีกตัวหนึ่ง ซึ่งในกรณีค่าของทั้ง ToDS และ FromDS เป็น 1 ค่าที่อยู่ที่เก็บจะเป็นค่าที่อยู่ของผู้ส่งต้นทางที่แท้จริง

รายละเอียดการเก็บค่าที่อยู่ในที่อยู่ต่าง ๆ สามารถแสดงได้ดังตารางที่ 2

ตารางที่ 2 ส่วนประเภทของที่อยู่

ToDS	FromDS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

\ ส่วนลำดับเฟรมจะแสดงถึงลำดับของชิ้นส่วนของเฟรมที่ถูกแยกส่วนและเป็นตัวรู้จำการเกิดแพ็กเกตซ้ำซ้อน ซึ่งประกอบด้วย 2 ส่วนได้แก่ หมายเลขชิ้นส่วน (Fragment Number) และหมายเลขลำดับ (Sequence Number) ซึ่งทั้งสองตัวนี้จะเป็นตัวบ่งบอกปริมาณของชิ้นส่วนของเฟรม

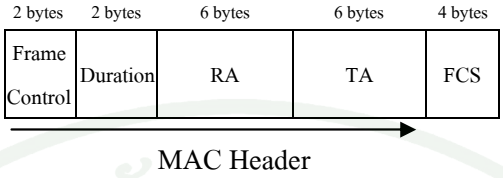
ในส่วนตรวจสอบความผิดพลาดของเฟรมซึ่งมีขนาด 32 บิต (4 ไบต์) จะใช้เป็นตัวตรวจสอบความผิดพลาดของแต่ละบิตในเฟรม โดยทั่วไปจะใช้การตรวจสอบแบบซีอาร์ซี (CRC : Cyclic Redundancy Check)

โครงสร้างเฟรมควบคุม

โครงสร้างเฟรมดังกล่าวในหัวข้อที่ผ่านมาพบในเฟรมประเภทเฟรมการจัดการและเฟรมข้อมูล และยังมีโครงสร้างเฟรมรูปแบบอื่น ๆ ที่น่าสนใจ ได้แก่ เฟรมควบคุมอาร์ทีเอส และเฟรมควบคุมซีทีเอส

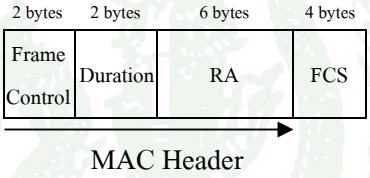
เฟรมอาร์ทีเอสและซีทีเอส ทำหน้าที่ในจัดการการจองเพื่อเข้าใช้สื่อ โดยโครงสร้างของเฟรมอาร์ทีเอสจะประกอบด้วยส่วนเฟรมควบคุมที่มีลักษณะเดียวกันกับเฟรมการจัดการและเฟรมข้อมูล ถัดมาจะเป็นส่วนของเวลารอซึ่งมีหน่วยเป็นไมโครวินาที (microseconds) โดยจะมีการคำนวณค่าของช่วงเวลารอสำหรับค่าเอ็นเอวี (NAV : Network Allocation Vector) ซึ่งได้จากการนำค่าของเวลาในการส่งเฟรมซีทีเอสมาบวกกับค่าเวลาของการส่งข้อมูลบวกกับค่าเวลาในการตอบแอ็คและบวกกับค่าของเวลาในการรอระหว่างเฟรม (SIFS : Short Interframe Space) อีก 3 ช่วง

ส่วนถัดมาจะเป็นค่าที่อยู่ของสถานีผู้รับปลาย ต่อจากนั้นจะเป็นส่วนค่าที่อยู่สถานีผู้รับต้นทาง สุดท้ายจะเป็นส่วนตรวจสอบความผิดพลาดของเฟรม โครงสร้างเฟรมอาร์ทีเอส แสดงดังภาพที่ 11



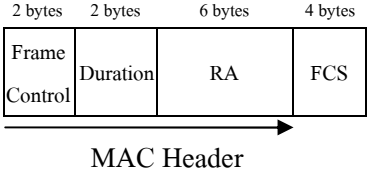
ภาพที่ 11 เฟรมอาร์ทีเอส

เฟรมซีทีเอสมีโครงสร้างเฟรมคล้ายกับอาร์ทีเอส ต่างกันตรงที่เฟรมซีทีเอสไม่มีส่วนเก็บค่าที่อยู่ของสถานีผู้ส่งต้นทาง และการคำนวณค่าของช่วงเวลารอสำหรับค่าเอ็นเอวีจะต่างกัน โดยจะคำนวณจากค่าเวลารอที่คำนวณได้สำหรับเฟรมอาร์ทีเอสหักลบด้วยค่าเวลาการส่งเฟรมซีทีเอสและหักลบด้วยค่าเวลาในการรอระหว่างเฟรม โครงสร้างของเฟรมซีทีเอสสามารถแสดงได้ดังภาพที่ 12



ภาพที่ 12 เฟรมซีทีเอส

เฟรมแอ็ค เป็นเฟรมที่ใช้ในการยืนยันการรับข้อมูล จะมีโครงสร้างเฟรมดังภาพที่ 13 ซึ่งโครงสร้างเฟรมจะเหมือนกับเฟรมซีทีเอสแต่จะตั้งค่าเวลาในการรอเป็น 0 ซึ่งหมายถึงการส่งข้อมูลเสร็จเรียบร้อยแล้วไม่จำเป็นต้องมีการรอหลังจากนี้ ค่าที่อยู่ของผู้รับจะทำการคัดลอกมาจากที่อยู่ 2 ของเฟรมก่อนหน้านี้



ภาพที่ 13 เฟรมแอ็ค

งานวิจัยที่เกี่ยวข้อง

จากการค้นคว้าข้อมูลที่ผ่านมาไม่พบว่ามีงานวิจัยใดที่มีการออกแบบกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์บนสภาพแวดล้อมของเครือข่ายไร้สาย แต่ในส่วนของการออกแบบกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์บนสภาพแวดล้อมเครือข่ายแบบใช้สายพบว่ามีหลากหลายงานวิจัย โดยสามารถจัดกลุ่มแนวทางการออกแบบกลไกได้ดังต่อไปนี้

1. แนวทางการตรวจสอบค่าพอร์ตโดยปริยายของโพรโทคอลบิตทอร์เรนต์ (Port base)

การตรวจสอบพอร์ตเป็นแนวทางพื้นฐานของการตรวจจับโปรแกรมทั่วไปที่ง่ายที่สุดโดย Sen and Wang (2004) ได้เสนอแนวทางการตรวจสอบหมายเลขพอร์ตโดยปริยายของโพรโทคอลบิตทอร์เรนต์ (6881-6889) (IANA, 2010) ซึ่งเป็นแนวทางที่ง่ายต่อการพัฒนา ใช้ทรัพยากรเครือข่ายน้อยแต่มีข้อจำกัด เนื่องจากโพรโทคอลบิตทอร์เรนต์ได้มีการพัฒนาให้สามารถใช้พอร์ตใด ๆ หรือแม้กระทั่งใช้พอร์ตที่รู้จักกันดี (Well-known Port) อย่างเช่นพอร์ต 80 ของโพรโทคอลเอชทีทีพี (HTTP) และพอร์ต 443 ของโพรโทคอลเอชทีทีพีเอส (HTTPS) เป็นต้น

อย่างไรก็ตาม Perényi *et. al.* (2006) ที่เสนอแนวทางการตรวจสอบจับแบบวิทยาการศึกษาสำนึก (Heuristics) ที่เน้นการตรวจสอบพฤติกรรมที่เกี่ยวกับการใช้พอร์ตในชั้นขนส่ง ก็ยังคงนำวิธีการตรวจสอบค่าพอร์ตปริยาย มาใช้ร่วมกับการตรวจจับแบบวิทยาการศึกษาสำนึกอยู่ เพื่อใช้เป็นการยืนยันว่าชุดที่อยู่ไอพีที่ทำการตรวจจับได้เกี่ยวพันกับพฤติกรรมการทำงานของโพรโทคอลบิตทอร์เรนต์ โดยได้ให้เหตุผลว่าผู้ใช้งานแบ่งปันไฟล์ด้วยโพรโทคอลบิตทอร์เรนต์ตามบ้านและที่พักอาศัยทั่วไป โดยส่วนใหญ่แล้วจะไม่ถูกจำกัดการใช้งานพอร์ต จึงยังคงมีการใช้พอร์ตปริยายที่โปรแกรมบิตทอร์เรนต์ไคลเอนต์กำหนดไว้เป็นจำนวนมาก

2. แนวทางการตรวจสอบสัญลักษณ์ข้อมูลที่เป็นเอกลักษณ์ของโพรโทคอลบิตทอร์เรนต์ (Signature base)

Moore and Papakiannaki (2005) ได้เสนอกลไกการตรวจจับบิตทอร์เรนต์ที่พัฒนาได้ง่ายไม่ซับซ้อน โดยทำการแกะข้อมูลจริง (payload) ในแพ็กเกตข้อมูลเพื่อตรวจหาข้อความ “0x13BitTorrent” ที่มีความยาว 19 ไบต์ ซึ่งเป็นตัวบ่งบอกถึงการมีอยู่ของโพรโทคอลบิตทอร์เรนต์ แต่จุดอ่อนของวิธีการนี้ก็คือการเข้าตรวจดูข้อมูลจริงของแพ็กเกตทุกแพ็กเกตจำเป็นจะต้องทรัพยากรการประมวลผลสูงมาก

Risso *et. al.* (2008) ได้เสนอแนวทางการแก้ไขปัญหาการใช้ทรัพยากรประมวลสูงในการตรวจสอบสัญลักษณ์ในทุกแพ็กเกต โดยพบว่าไม่ใช่ทุกแพ็กเกตที่มีจะสัญลักษณ์บ่งบอกว่าเป็นโพรโทคอลใดเสมอ จึงได้เสนอแนวทางการวิเคราะห์วาระ (Session) โดยสร้างตารางวาระ (Session Table) ที่เก็บข้อมูลแพ็กเกตที่มีสัญลักษณ์ และข้อมูลของกระแสข้อมูล (Flow) โดยมีความคาดหวังว่าจะสามารถใช้ตารางวาระลดปริมาณการดูแพ็กเกต ซึ่งสามารถดูแค่แพ็กเกตส่วนเริ่มของวาระได้ แต่ก็ต้องแลกมาด้วยความซับซ้อนในการพัฒนากลไก โดยจำเป็นต้องเพิ่มภาระการจัดการตารางวาระพร้อมกับการตรวจสอบแพ็กเกต

Chen *et. al.* (2008) ได้ออกแบบกรอบการทำงาน (Framework) สำหรับการตรวจจับแพ็กเกตโปรแกรมสื่อสารผ่านข้อความ (Instant Messaging) และโพรโทคอลเพียร์ทูเพียร์ ซึ่งในส่วนของการตรวจจับโพรโทคอลบิตทอร์เรนต์ Chen *et. al.* ได้ระบุว่าใช้การตรวจสอบความยาวของแพ็กเกตเป็นหลัก และเสริมด้วยการตรวจสอบบางฟิลด์ที่เป็นค่าคงที่ เช่น เมื่อพบว่าข้อมูลจริงมีขนาด 16 ไบต์ ใน 8 ไบต์แรกจะเป็นค่าคงที่ที่มีค่า 00 00 04 17 27 10 19 80 เสมอ

ถึงแม้ว่าการตรวจจับสัญลักษณ์จะพัฒนาได้ง่าย และมีหลายงานวิจัยที่ได้เสนอแนวทางการปรับปรุงกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์เพื่อลดการใช้ทรัพยากรในการประมวลผลแล้วก็ตาม แต่กระนั้นโพรโทคอลบิตทอร์เรนต์ ก็ได้พัฒนาการเข้ารหัสข้อมูลทำให้ไม่สามารถใช้วิธีค้นหาสัญลักษณ์ได้ อีกทั้งในบางประเทศการแกะแพ็กเกตอาจเป็นการละเมิดกฎหมายสิทธิส่วนบุคคลด้วย

3. แนวทางการตรวจจับพฤติกรรมที่เป็นเอกลักษณ์ของโพรโทคอลบิตทอร์เรนต์ (Behavior base)

งานวิจัยที่ใช้แนวทางการสังเกตพฤติกรรมการตรวจจับบิตทอร์เรนต์เริ่มมีมากขึ้น ซึ่งจุดเด่นของแนวทางนี้คือสามารถตรวจจับการมีอยู่ของโพรโทคอลบิตทอร์เรนต์ได้ไม่ว่าจะใช้พอร์ตใด ๆ อีกทั้งยังสามารถตรวจจับได้แม้โพรโทคอลจะมีการเข้ารหัสข้อมูลเอาไว้ งานวิจัยเหล่านี้ได้แก่ Sendil and Nagarajan (2009), Gebski *et. al.* (2006), Karagiannis *et. al.* (2005), Collins and Reiter (2006), Won *et. al.* (2006), Ngiwlai *et. al.* (2008), และ Constantinou and Mavrommatis (2006)

Won *et. al.* (2006) ได้นำเสนอแนวทางผสมผสาน โดยเสนอการให้มีการแบ่งการตรวจจับโพรโทคอลบิตทอร์เรนต์ เป็น 3 ขั้นตอน ได้แก่ ขั้นตอนการตรวจหาสัญลักษณ์ ขั้นตอนการดูพฤติกรรมของกระแสข้อมูลซึ่งประกอบด้วย หมายเลขโพรโทคอล, ที่อยู่ไอพีต้นทาง, ที่อยู่ไอพีปลายทาง, หมายเลขพอร์ตต้นทาง, และหมายเลขพอร์ตปลายทาง โดยสังเกตพฤติกรรมของกระแสข้อมูลที่เป็นแอพพลิเคชั่น ที่เกิดขึ้นในเวลาสั้น ๆ น้อยกว่า 1 นาทีทั้งในทิศทางการรับและส่งข้อมูล

รวมทั้งแพ็กเกตที่เกิดขึ้นในช่วงเวลาสั้น ๆ ที่มีการแบ่งกันใช้ที่อยู่ไอพี เป็นตัวบ่งบอกถึงพฤติกรรมการส่งข้อมูลของเพียร์ทูเพียร์

ทั้งนี้ทางคณะยังได้ศึกษาพฤติกรรมการส่งข้อมูลแพ็กเกตชนิดอื่น ๆ เช่นพฤติกรรมการส่งข้อมูลที่มีหลายวาระ ที่เกิดระหว่างที่อยู่ต้นทาง (Source IP Addess) สองไอพีเป็นตัวกรองแพ็กเกต ซึ่งพฤติกรรมเช่นนี้ มีลักษณะคล้าย ๆ กับพฤติกรรมของแพสสิฟเอฟทีพี (Passive FTP) เป็นต้น และในขั้นตอนสุดท้ายจะทำการตรวจสอบกับหมายเลขพอร์ตที่ใช้กันทั่วไป ซึ่งผู้เขียนคาดหวังว่าการใช้แนวทางการผสมผสานเช่นนี้จะสามารถลดทรัพยากรการประมวลที่ใช้เพียงแนวทางการตรวจหาสัญลักษณ์ที่ข้อมูลจริงเพียงอย่างเดียว

Sendil and Nagarajan (2009) ได้ศึกษาลักษณะกระแสข้อมูลที่ส่วนมากเป็นพฤติกรรมของโพรโทคอลเพียร์ทูเพียร์ ซึ่งพบว่าคู่ไอพีที่มีการใช้งานโพรโทคอลทีซีพี (TCP) และยูดีพี (UDP) พร้อมกัน จะน่าสงสัยว่าเป็นการทำงานของเพียร์ทูเพียร์ ลักษณะพฤติกรรมที่พบต่อมาก็คือ เพียร์ทูเพียร์ที่กำลังรับ-ส่งข้อมูลของไฟล์อยู่ จะมีการส่งชิ้นส่วนไฟล์ขนาดเล็กในปริมาณมากที่พอร์ตคงที่ค่าหนึ่ง

นอกจากนี้ทีมผู้วิจัยยังพบอีกว่า กระแสข้อมูลของเพียร์ทูเพียร์มักจะมีขนาดกระแสข้อมูลมากกว่า 2MB และการรับ-ส่งข้อมูลของกระแสข้อมูลจะกินระยะเวลามากกว่า 12 นาที ซึ่งเป็นผลมาจากการใช้งานของเพียร์ทูเพียร์ส่วนมากจะใช้สำหรับการรับ-ส่งข้อมูลขนาดใหญ่ เช่นเพลงหรือภาพยนตร์เป็นต้น ทางคณะวิจัยจึงได้ออกแบบกลไกการตรวจสอบพฤติกรรมการรับ-ส่งข้อมูลเพียร์ทูเพียร์โดยให้มีการตรวจสอบพฤติกรรมลักษณะดังกล่าวข้างต้น ร่วมกับการตรวจสอบค่าพอร์ตปริยายของเพียร์ทูเพียร์ และการตรวจสอบค่าพอร์ตที่เป็นที่รู้จักโดยทั่วไป

Karagiannis *et. al.* (2005) ได้ทำการสังเกตกระแสข้อมูลที่น่าจะเป็นพฤติกรรมของเพียร์ทูเพียร์ โดยได้เสนอแนวทางการพิจารณากระแสข้อมูลในหลายระดับ (Multi-Level) ซึ่งประกอบด้วยระดับทางสังคม (Social Level) ระดับหน้าที่การทำงาน (Functional Level) และระดับแอพพลิเคชั่น (Application Level) ซึ่งระบุว่าสามารถระบุแอพพลิชั่นที่ทำการตรวจจับโดยใช้กลไกนี้ได้ถึง 80% แต่ข้อเสียของวิธีการนี้คือ มีความยุ่งยากซับซ้อนในการนำไปพัฒนาเป็นอย่างมาก

Constantinou *et, al.* (2006) ได้ทำการสังเกตพฤติกรรมที่ชั้นขนส่งโดยสังเกตพฤติกรรมการส่งข้อมูลของโฮสต์ (Host) เช่น พฤติกรรมของโฮสต์ที่มีการบรอดคาสต์ (Broadcast) แพ็กเกตที่รับ-ส่งข้อมูลด้วยโพรโทคอลยูดีพีในปริมาณมาก ๆ ซึ่งมีความเป็นไปได้ว่าโฮสต์นี้อาจมีการส่งข้อมูลเพียร์ทูเพียร์อยู่ เนื่องจากโพรโทคอลเพียร์ทูเพียร์ต้องทำการส่งข้อมูลผ่านโพรโทคอลยูดีพี

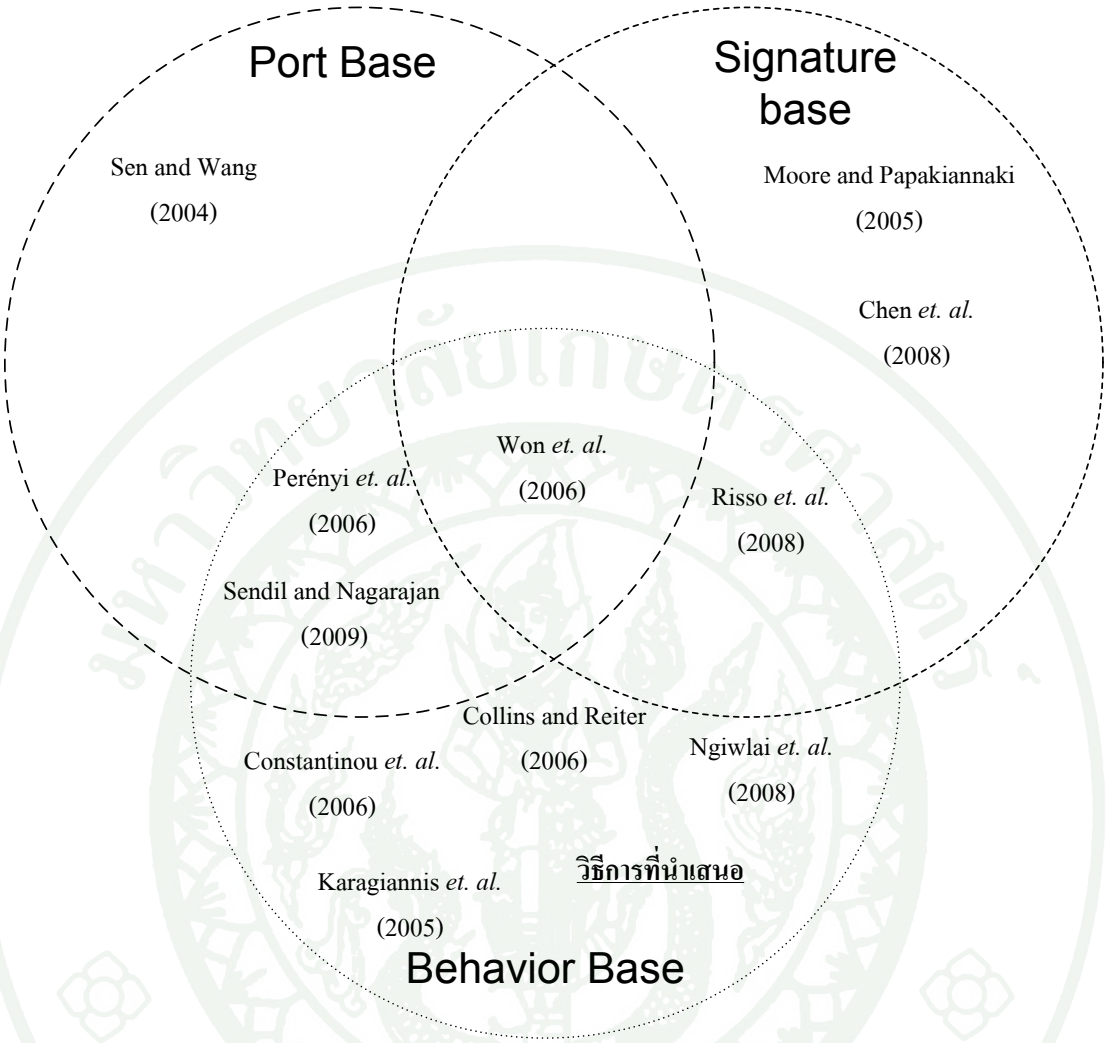
ไปเพื่อตรวจหาเพียร์ที่มีชิ้นส่วนข้อมูลอยู่

Collins and Reiter (2006) ได้ทำการสังเกตพฤติกรรมของโพรโทคอลบิตทอร์เรนต์ของกระแสข้อมูลและคู่ที่อยู่ไอพี โดยได้ทำการแบ่งกระแสข้อมูลออกเป็น 3 ชนิดได้แก่ กระแสข้อมูลสั้น (Short Flow) ประกอบด้วยแพ็กเกตไม่เกิน 3 แพ็กเกต, ข้อความ (Message) มีขนาดไม่เกิน 2 kB หรือมีแพ็กเกตไม่เกิน 4 แพ็กเกต, และข้อมูลไฟล์รับ-ส่ง (File Transfer) ที่มีขนาดเกิน 2 kB หรือมีแพ็กเกตมากกว่า 10 แพ็กเกตขึ้นไป ซึ่งพบว่าโพรโทคอลบิตทอร์เรนต์มีปริมาณของข้อความเป็นปริมาณมากถึง 84% เมื่อเทียบระหว่างปริมาณข้อความระหว่างโพรโทคอลบิตทอร์เรนต์กับปริมาณของโพรโทคอลเอชทีทีพี

Ngiwlai *et. al.* (2008) ได้นำเสนอแนวทางการตรวจจับโพรโทคอลบิตทอร์เรนต์โดยอาศัยพฤติกรรมการเค้น (Choke Algorithm) ซึ่งสามารถพัฒนาให้ตรวจจับโพรโทคอลบิตทอร์เรนต์ในเวลาจริงได้ แต่ก็ยังมีจุดอ่อนตรงที่สามารถทำงานได้กับบิตทอร์เรนต์ที่มีจำนวนเพียร์ที่ติดต่อกันมากกว่า 4 เพียร์ขึ้นไป แล้วแต่ละเพียร์จำเป็นต้องมีการรับ-ส่งข้อมูลในอัตราเร็วที่สม่ำเสมอ

งานวิจัยที่เป็นกลุ่มงานวิจัยที่ศึกษาพฤติกรรมของโพรโทคอลบิตทอร์เรนต์ที่ชั้นขนส่ง (Transport Layer) โดยดูปริมาณการส่งข้อมูลผ่านทางแพ็กเกตทีซีพีและยูดีพี ซึ่งจำเป็นต้องตรวจสอบข้อมูลในปริมาณมากก่อนจึงจะสามารถตัดสินใจในการตรวจจับบิตทอร์เรนต์ได้ และจำเป็นต้องใช้ทรัพยากรการประมวลผลสูง อีกทั้งยังมีข้อจำกัดที่ไม่สามารถนำไปพัฒนาให้ทำการตรวจจับในเวลาจริง (Real-time detection)

ลักษณะงานวิจัยที่ได้มีการแบ่งกลุ่มในข้างต้น มีลักษณะงานซ้อนทับกันในบางงานวิจัยซึ่งแสดงได้ดังภาพที่ 14



ภาพที่ 14 การจัดกลุ่มงานวิจัยที่ใช้แนวทางการศึกษาการใช้พอร์ต, แนวทางการสังเกตสัญลักษณ์, และแนวทางการสังเกตพฤติกรรมของโพรโทคอลเพียร์ทูเพียร์

ตารางที่ 3 จะเป็นการสรุปแนวทางงานวิจัยแต่ละกลุ่ม พร้อมทั้งแสดงการวิเคราะห์ถึงข้อดีและข้อเสียของแนวทางการวิจัยในแต่ละกลุ่ม พร้อมทั้งแสดงรายละเอียดของแนวทางที่นำเสนอในวิทยานิพนธ์ฉบับนี้

งานวิจัยที่กล่าวมาข้างต้นต่างก็มุ่งเน้นไปกับการออกแบบการตรวจจับโพรโทคอลบิตทอร์เรนต์ที่มีสภาพแวดล้อมที่เป็นเครือข่ายใช้สาย ซึ่งมีทรัพยากรมาก การที่จะนำวิธีการเหล่านี้ไปพัฒนาบนสภาพแวดล้อมเครือข่ายไร้สายจึง อาจไม่ให้ประสิทธิภาพได้เท่าที่ควร จึงจำเป็นต้องมีการออกแบบกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์ ที่ถูกออกแบบมาให้ทำงานบนเครือข่ายไร้สายที่มีทรัพยากรจำกัด ให้สามารถทำงานบนสภาพแวดล้อมไร้สายได้อย่างมีประสิทธิภาพ

ตารางที่ 3 งานวิจัยที่เกี่ยวข้องแบ่งตามกลุ่ม

กลุ่ม	ระดับชั้น	ข้อดี	ข้อเสีย	ทีมวิจัย
การตรวจสอบพอร์ต	ขนส่ง	-พัฒนาง่าย -ใช้ทรัพยากรน้อย	-ไม่สามารถใช้งานได้เมื่อมีการสุ่มพอร์ตหรือใช้พอร์ตที่รู้จักทั่วไป	Sen *et. al*. (04) Perényi *et. al*. (06) Sendil *et. al.* (09) Won *et. al.* (06)
การตรวจสอบสัญลักษณ์	แอพพลิเคชั่น	-พัฒนาง่าย	-ไม่สามารถตรวจจับเมื่อเข้ารหัส -ปัญหาด้านกฎหมาย -ใช้ทรัพยากรมาก	Moore *et. al.*(06) Chen *et. al.*(08) Risso *et. al.*(08) Won *et. al.*(06)
การสังเกตพฤติกรรม	ขนส่ง/เครือข่าย	-ตรวจจับได้แม้เข้ารหัส -ตรวจจับได้แม้ใช้พอร์ตใด ๆ	-พัฒนาค่อนข้างซับซ้อน -ใช้ทรัพยากรมาก	Won *et. al.* (06) Perényi *et. al.* (06) Sendil *et. al*. (09) Risso *et. al.*(08) Constantinou.*et.al.*(06) Collins *et. al.*(06) Karagiannis *et. al.*(05) Ngiwlai *et. al.* (08)
	แม็ค	**-ตรวจจับได้แม้เข้ารหัส -ตรวจจับได้แม้ใช้พอร์ตใด ๆ -พัฒนาง่าย -ใช้ทรัพยากรน้อย**	**-ออกแบบมาเพื่อใช้เฉพาะบนเครือข่ายไร้สาย**	**วิธีการที่นำเสนอ**

อุปกรณ์และวิธีการ

อุปกรณ์

1. ซอฟท์แวร์
    1. ระบบปฏิบัติการอูบันตูลินุกซ์ (Ubuntu) เวอร์ชั่น 8.04
    2. โปรแกรมไวร์ชาร์กเวอร์ชั่น 1.03 สำหรับลินุกซ์ (Wireshark 1.03 for Linux)
    3. ระบบจัดการฐานข้อมูลเอสคิวแอลเซิร์ฟเวอร์ 2008 (SQL Server 2008)
    4. ระบบปฏิบัติการวินโดวส์เอ็กซ์พีรุ่น 32 บิต (Windows XP 32 bit)
    5. โปรแกรมวิชวลสตูดิโอ 2008 (Visual Studio 2008)
    6. โปรแกรมไวร์ชาร์กเวอร์ชั่น 1.25 สำหรับวินโดวส์ (Wireshark 1.25 for Windows)
    7. โปรแกรมไฟล์ซิลล่าเอฟทีพีไคลเอนต์ เวอร์ชั่น 3.2.4.1 (Filezilla FTP Client 3.2.4.1)
    8. โปรแกรมไฟล์ซิลล่าเอฟทีพีเซิร์ฟเวอร์ เวอร์ชั่น 0.9.9 (Filezilla FTP Server 0.9.9)
    9. โปรแกรมอาปาเช่ เว็บเซิร์ฟเวอร์ เวอร์ชั่น 2.2.8 (Apache Web Server 2.2.8)
    10. โปรแกรมมิวทอร์เรนต์เวอร์ชั่น 1.6.1 (µTorrent 1.6.1)

2. ฮาร์ดแวร์
    1. เครื่องคอมพิวเตอร์ความเร็ว 2.0 GHz
    2. หน่วยความจำหลัก 2.9 GB
    3. ฮาร์ดดิสก์ความจุ 250 GB
    4. การ์ดเครือข่าย 10/100 Mpbs 1 ตัว
    5. อุปกรณ์ไวร์เลสเร้าทเตอร์ หรือ แอคเซสพ้อยท์ 1 ตัว

วิธีการ

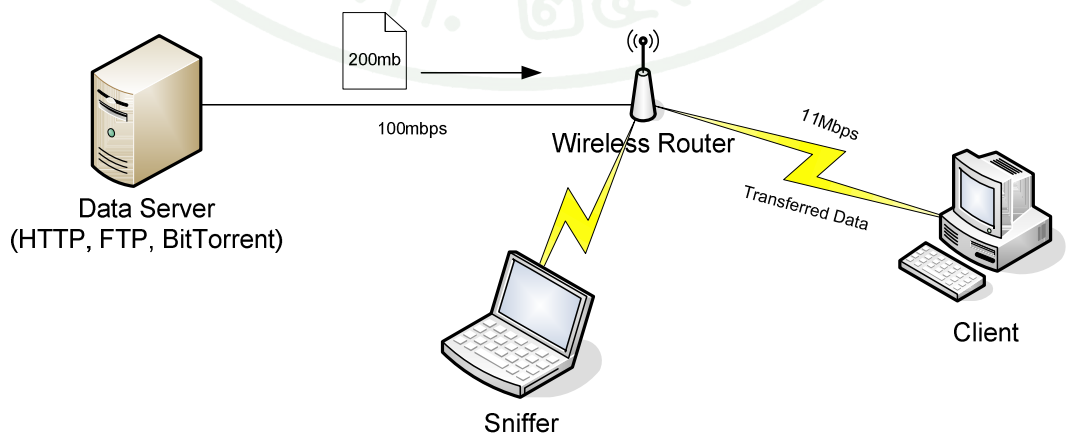
จากปัญหาการขาดแคลนกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์ที่มีประสิทธิภาพ เมื่อใช้งานบนสภาพแวดล้อมเครือข่ายไร้สาย งานวิจัยนี้จึงมีจุดมุ่งหมายเพื่อนำเสนอแนวทางตรวจจับโพรโทคอลบิตทอร์เรนต์ โดยอาศัยข้อมูลเฉพาะเท่าที่หาได้จากส่วนของเครือข่ายไร้สายเท่านั้น ซึ่งจำเป็นต้องใช้พลังในการประมวลผลต่ำ สามารถทำงานได้ในเวลาจริง และสามารถตรวจจับได้แม้ข้อมูลจะถูกเข้ารหัสมาก็ตาม

1. การตรวจจับโพรโทคอลบิตทอร์เรนต์บนสภาพแวดล้อมเครือข่ายไร้สาย

การที่จะออกแบบกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์ที่เหมาะสำหรับสภาพแวดล้อมบนเครือข่ายไร้สายนั้น จำเป็นจะต้องใช้ข้อมูลที่มีเฉพาะในเครือข่ายไร้สายเท่านั้น ซึ่งข้อมูลที่สามารถจะใช้งานได้ จะมีเพียงข้อมูลในชั้นแม็ค ซึ่งได้แก่ ข้อมูลที่อยู่ในเฟรมชนิดต่าง ๆ เท่านั้น และด้วยสภาพแวดล้อมไร้สายซึ่งมีทรัพยากรที่จำกัด จึงจำเป็นที่จะต้องออกแบบกลไกที่มีน้ำหนักเบา พัฒนาง่ายไม่ซับซ้อน ที่จะสามารถนำไปติดตั้งบนอุปกรณ์เครือข่ายไร้สายที่มีพลังการประมวลผลต่ำอย่างเช่นแอคเซสพ้อยท์ได้ ซึ่งด้วยข้อมูลที่มีให้ใช้อย่างจำกัดบนสภาพแวดล้อมเครือข่ายไร้สาย เราจึงมุ่งเน้นไปที่ความถี่ในการเกิดเฟรมข้อมูลในขนาดต่าง ๆ โดยมีสมมติฐานที่ว่าในกระแสข้อมูลของโพรโทคอลบิตทอร์เรนต์จะเกิดการกระจายตัวขนาดเฟรมข้อมูลขนาดต่าง ๆ ที่เกิดจากการรับ-ส่งข้อมูลเพื่อประสานจังหวะกันระหว่างเพียร์ในปริมาณที่มาก ซึ่งจะไม่พบในโพรโทคอลชนิดอื่น ในหัวข้อนี้จะกล่าวถึงการออกแบบการทดลองเพื่อทดสอบสมมติฐาน การออกแบบกลไกการตรวจจับบิตทอร์เรนต์ และการออกแบบการทดลองเพื่อวัดประสิทธิภาพของกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์บนเครือข่ายไร้สาย

1.1 ขั้นตอนการออกแบบการทดลองเพื่อทดสอบสมมติฐาน

จากสมมติฐานที่ว่าโพรโทคอลบิตทอร์เรนต์จะมีการกระจายตัวของขนาดเฟรมข้อมูลมากกว่าโพรโทคอลชนิดอื่น ๆ ณ ช่วงเวลาใด ๆ โดยการกระจายตัวของขนาดเฟรมข้อมูลอันเกิดจากการรับ-ส่งข้อมูลประสานจังหวะระหว่างเพียร์ด้วยกันนี้ สามารถใช้ในการระบุการมีอยู่ของโพรโทคอลบิตทอร์เรนต์ของคู่ที่อยู่แม็คของผู้ส่งต้นทางกับคู่ที่อยู่แม็คของผู้รับปลายทางนั้น ๆ ได้ จึงได้มีการออกแบบการทดลองที่เป็นสภาวะแวดล้อมควบคุมโดยมีรายละเอียดดังภาพที่ 15



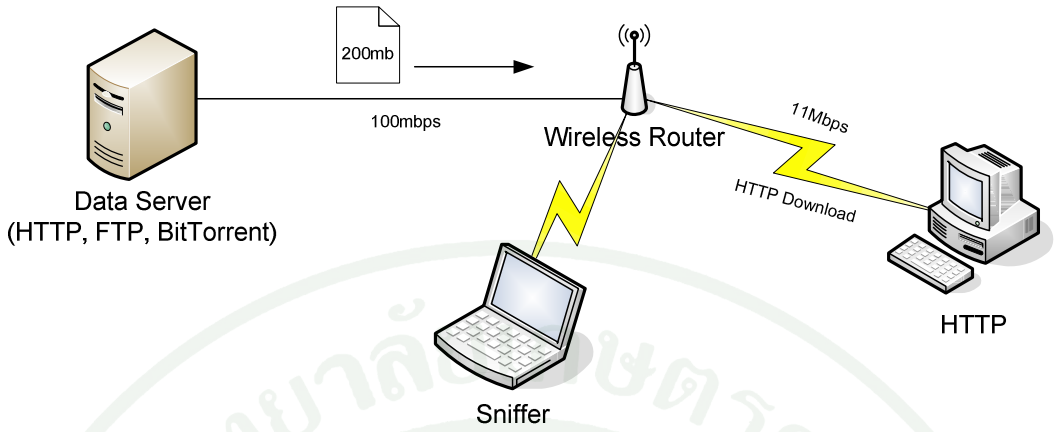
ภาพที่ 15 การทดลองเพื่อทดสอบสมมติฐาน

จากภาพที่ 15 เป็นการออกแบบการทดลองเพื่อทดสอบสมมติฐานโดยกำหนดให้มีเครื่องลูกข่ายหนึ่งเครื่องหรือหลายเครื่องทำการดาวน์โหลดไฟล์ที่มีขนาด 200 MB จากเครื่องแม่ข่าย โดยเครื่องลูกข่ายแต่ละเครื่องติดตั้งโพรโทคอลสำหรับใช้ดาวน์โหลดไฟล์ต่างชนิดกัน ทำการดาวน์โหลดไฟล์ ด้วยโพรโทคอลต่างชนิดกัน ผ่านทางเครือข่ายไร้สายที่ทำงานในโหมด 802.11b มีแบนด์วิทด์ 11mbps จากเครื่องแม่ข่ายที่เชื่อมต่อกับอุปกรณ์เร้าทเตอร์ไร้สาย ผ่านทางสายแลนโดยมีแบนด์วิทด์ 100mbps เลือกใช้โพรโทคอลในการทดลอง 3 โพรโทคอลได้แก่ เอชทีทีพี (HTTP), เอฟทีพี (FTP) และ บิตทอร์เรนต์ โดยควบคุมให้มีเฉพาะโพรโทคอลที่ทำการดาวน์โหลดไฟล์เชื่อมต่อกับเครือข่ายได้เท่านั้นเพื่อป้องกันข้อผิดพลาดอันเกิดจากโปรแกรมอื่นมีการใช้งานเครือข่ายอยู่ ทั้งนี้ การกำหนดขนาดไฟล์ให้มีขนาด 200MB เพื่อให้ไฟล์มีขนาดใหญ่เพียงพอที่จะสามารถเก็บข้อมูลช่วงระยะเวลาการดักจับได้นานเพียงพอ และขนาดไม่ใหญ่เกินไปทำให้บัฟเฟอร์ของโปรแกรมดักจับข้อมูลเต็มก่อนที่จะดาวน์โหลดไฟล์เสร็จสิ้น

ก่อนจะเริ่มต้นทำการทดลองทุกครั้ง จะต้องตรวจสอบสภาพแวดล้อมการใช้งานเครือข่ายไร้สาย โดยจะต้องมั่นใจว่าไม่มีอุปกรณ์ใด ๆ ที่มองไม่เห็นแอบลักลอบใช้เครือข่ายไร้สาย เพื่อป้องกันข้อผิดพลาดที่อาจเกิดขึ้นกับผลการทดลอง โดยจะใช้วิธีการใช้เครื่องดักจับข้อมูล (Sniffer) ทำการดักจับข้อมูลก่อนการทดลองทุกครั้ง ซึ่งข้อมูลที่ดักจับได้จะต้องมีเพียงแค่เฟรมบีคอน (Beacon Frame) เท่านั้นจึงจะถือได้ว่าไม่มีอุปกรณ์อื่นใดแอบลักลอบใช้งานเครือข่ายไร้สาย จากนั้นจึงเริ่มทำการทดลองโดยการให้เครื่องดักจับข้อมูลเริ่มทำการดักจับข้อมูล หลังจากนั้นจึงเริ่มดาวน์โหลดข้อมูลภายหลังจากเครื่องดักจับข้อมูลทำงานทันที กำหนดให้เก็บข้อมูลตั้งแต่เริ่มทำการดาวน์โหลดไปจนกระทั่งการดาวน์โหลดไฟล์เสร็จสิ้น ในกรณีที่การทดลองใดที่มีเครื่องลูกข่ายที่ดาวน์โหลดไฟล์มากกว่า 1 เครื่อง จะต้องรอให้ทุกไฟล์ในเครือข่ายทำการดาวน์โหลดเสร็จเรียบร้อยจึงจะหยุดการดักจับข้อมูล เสร็จแล้วจึงนำข้อมูลที่ดักจับได้มาวิเคราะห์การกระจายตัวของขนาดเฟรมข้อมูล รายละเอียดการทดลองแต่ละครั้ง สามารถแสดงได้ดังต่อไปนี้

การทดลองที่ 1 ดาวน์โหลดไฟล์ผ่านโพรโทคอล เอชทีทีพี

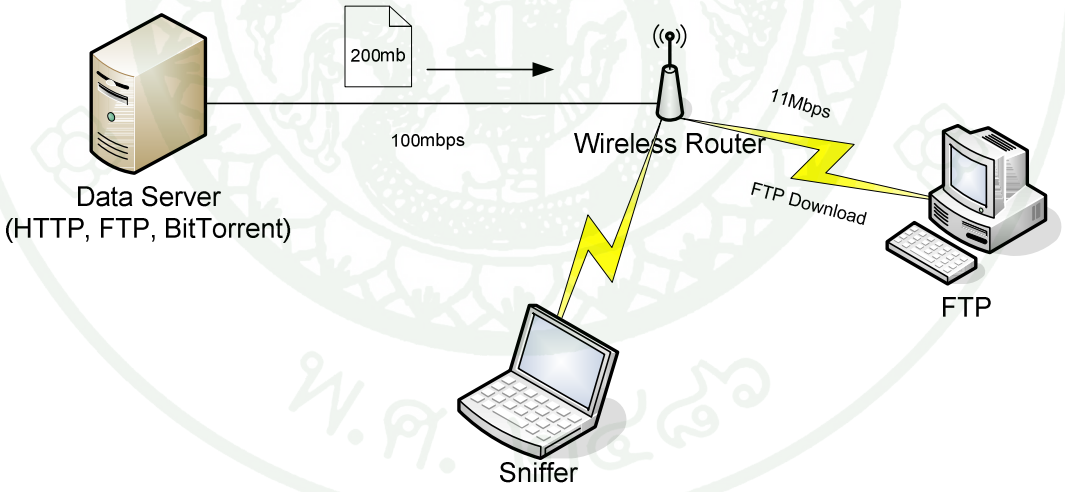
วัตถุประสงค์ เพื่อศึกษาการกระจายตัวของขนาดเฟรมข้อมูลเมื่อทำการดาวน์โหลดไฟล์ผ่านโพรโทคอลเอชทีทีพี บนเครือข่ายไร้สาย



ภาพที่ 16 การทดลองที่ 1 ดาวน์โหลดไฟล์ผ่านโพรโทคอล เอชทีทีพี

การทดลองที่ 2 ดาวน์โหลดไฟล์ผ่านโพรโทคอล เอฟทีพี

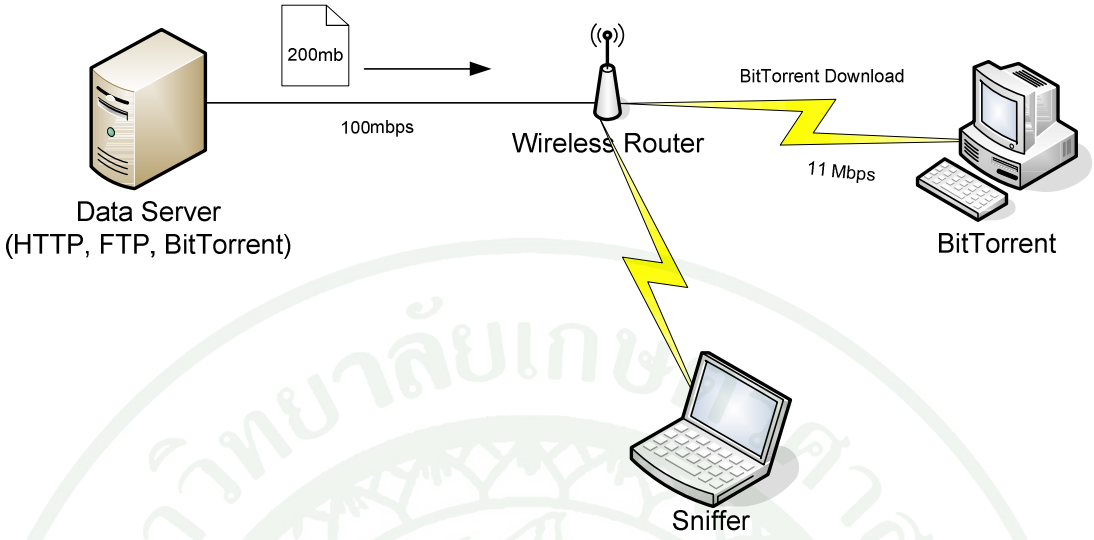
วัตถุประสงค์ เพื่อศึกษาการกระจายตัวของขนาดเฟรมข้อมูลเมื่อทำการดาวน์โหลดไฟล์ผ่านโพรโทคอลเอฟทีพี บนเครือข่ายไร้สาย



ภาพที่ 17 การทดลองที่ 2 ดาวน์โหลดไฟล์ผ่านโพรโทคอล เอฟทีพี

การทดลองที่ 3 ดาวน์โหลดไฟล์ผ่านโพรโทคอล บิตทอร์เรนต์

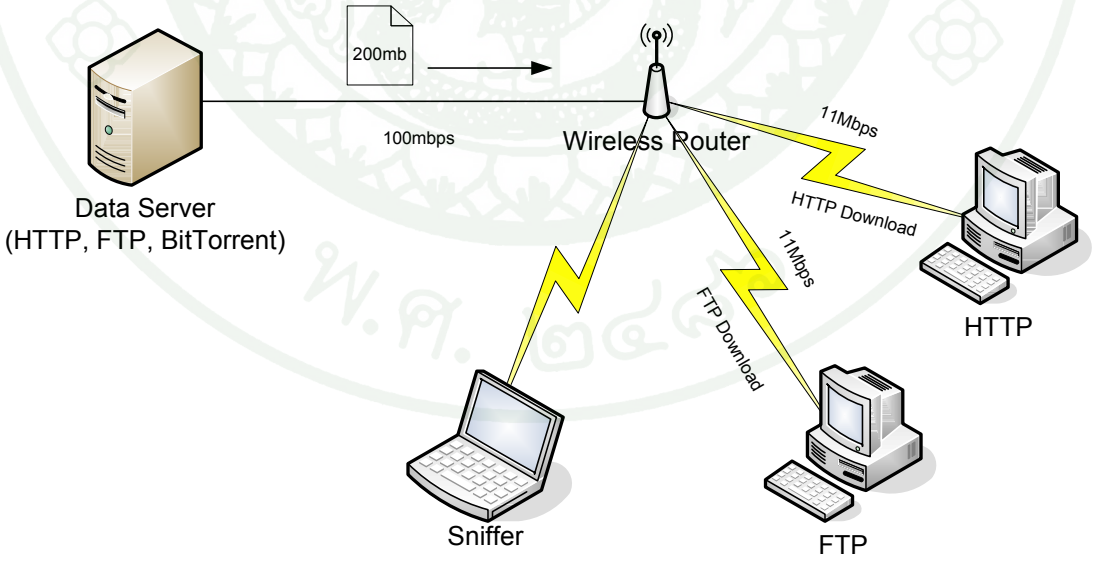
วัตถุประสงค์ เพื่อศึกษาการกระจายตัวของขนาดเฟรมข้อมูลเมื่อทำการดาวน์โหลดไฟล์ผ่านโพรโทคอลบิตทอร์เรนต์บนเครือข่ายไร้สาย



ภาพที่ 18 การทดลองที่ 3 ดาวน์โหลดไฟล์ผ่านโพรโทคอล บิตทอร์เรนต์

การทดลองที่ 4 ดาวน์โหลดไฟล์ผ่านโพรโทคอล เอชทีทีพีและเอฟทีพี

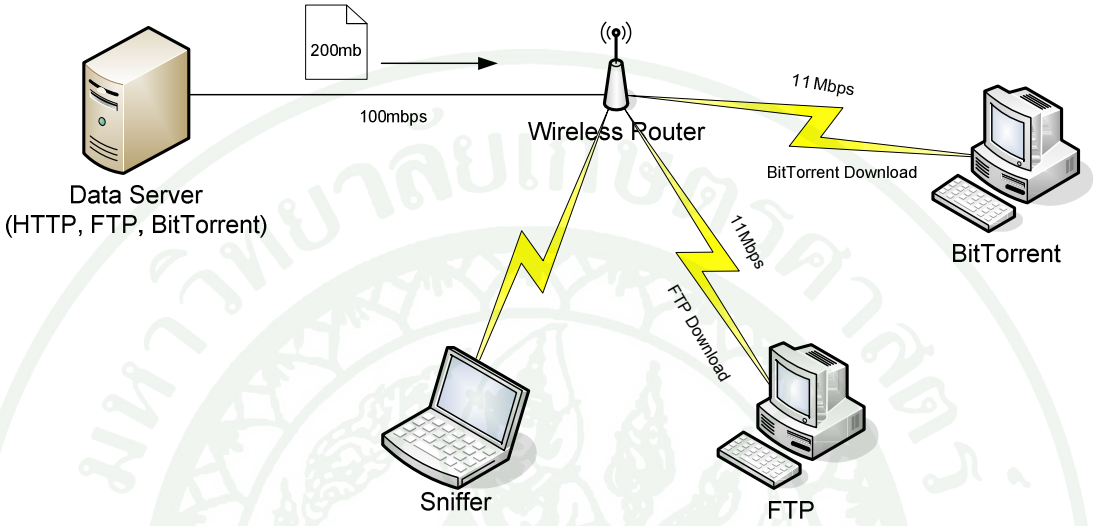
วัตถุประสงค์ เพื่อศึกษาการกระจายตัวของขนาดเฟรมข้อมูลเมื่อทำการดาวน์โหลดไฟล์ผ่านโพรโทคอลเอชทีทีพีและเอฟทีพี ที่มีการแข่งขันเข้าใช้สื่อบนเครือข่ายไร้สาย



ภาพที่ 19 การทดลองที่ 4 ดาวน์โหลดไฟล์ผ่านโพรโทคอล เอชทีทีพีและเอฟทีพี

การทดลองที่ 5 ดาวน์โหลดไฟล์ผ่านโพรโทคอล เอฟทีพีและบิตทอร์เรนต์

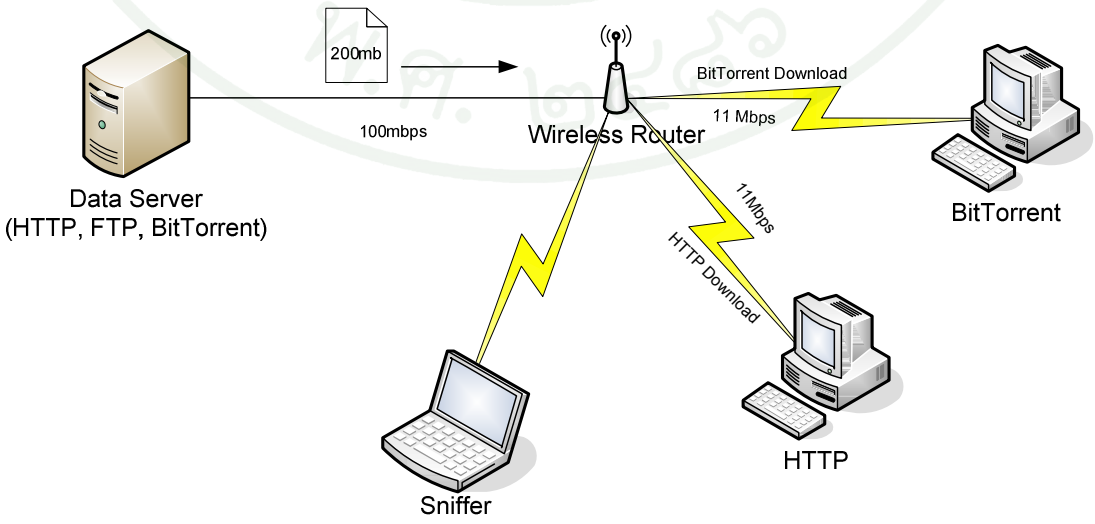
วัตถุประสงค์ เพื่อศึกษาการกระจายตัวของขนาดเฟรมข้อมูลเมื่อทำการดาวน์โหลดไฟล์ผ่านโพรโทคอลเอชทีทีพี เมื่อมีโพรโทคอลบิตทอร์เรนต์แข่งขันเข้าใช้สื่อบนเครือข่ายไร้สาย



ภาพที่ 20 การทดลองที่ 5 ดาวน์โหลดไฟล์ผ่านโพรโทคอล เอฟทีพีและบิตทอร์เรนต์

การทดลองที่ 6 ดาวน์โหลดไฟล์ผ่านโพรโทคอล เอชทีทีพีและบิตทอร์เรนต์

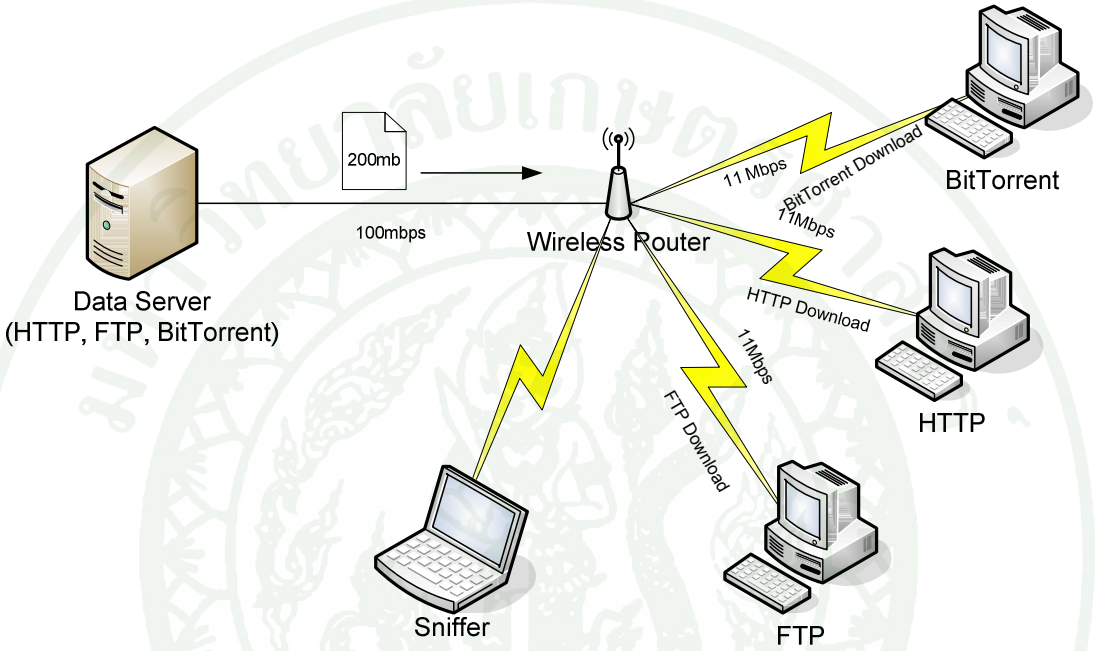
วัตถุประสงค์ เพื่อศึกษาการกระจายตัวของขนาดเฟรมข้อมูลเมื่อทำการดาวน์โหลดไฟล์ผ่านโพรโทคอลเอชทีทีพี เมื่อมีโพรโทคอลบิตทอร์เรนต์แข่งขันเข้าใช้สื่อบนเครือข่ายไร้สาย



ภาพที่ 21 การทดลองที่ 6 ดาวน์โหลดไฟล์ผ่านโพรโทคอล เอชทีทีพีและบิตทอร์เรนต์

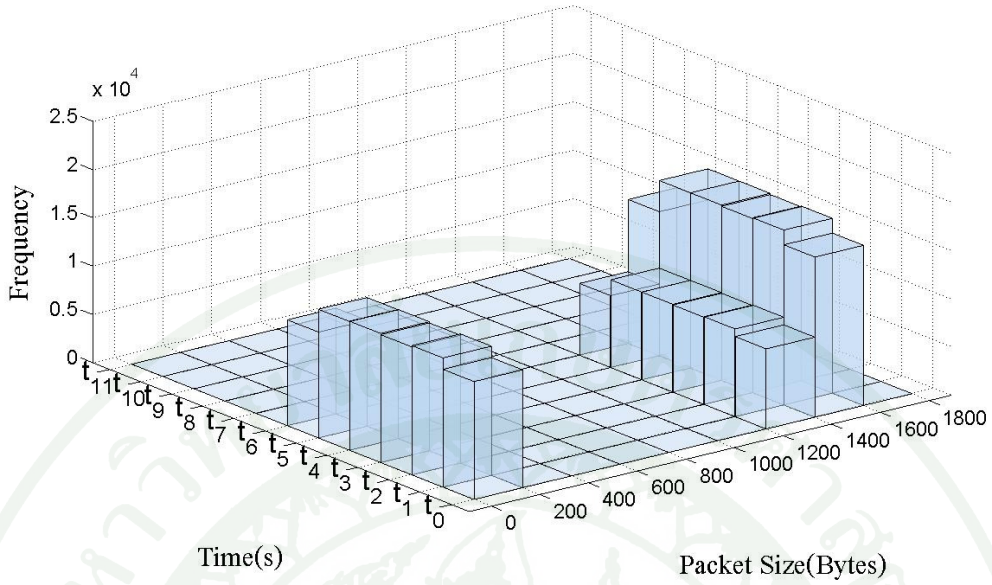
การทดลองที่ 7 ดาวน์โหลดไฟล์ผ่านโพรโทคอล เอชทีทีพี เอฟทีพีและบิตทอร์เรนต์

วัตถุประสงค์ เพื่อศึกษาการกระจายตัวของขนาดเฟรมข้อมูลเมื่อทำการดาวน์โหลดไฟล์ผ่านโพรโทคอลเอชทีทีพี เอฟทีพี และบิตทอร์เรนต์เมื่อมีการแข่งขันเข้าใช้สื่อบนเครือข่ายไร้สาย

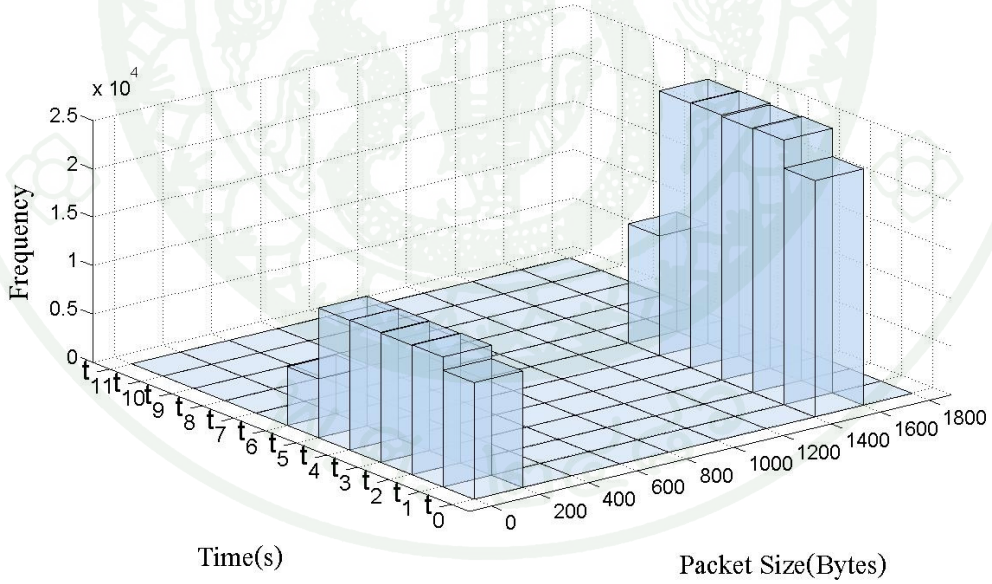


ภาพที่ 22 การทดลองที่ 7 ดาวน์โหลดไฟล์ผ่านโพรโทคอล เอชทีทีพี เอฟทีพีและบิตทอร์เรนต์

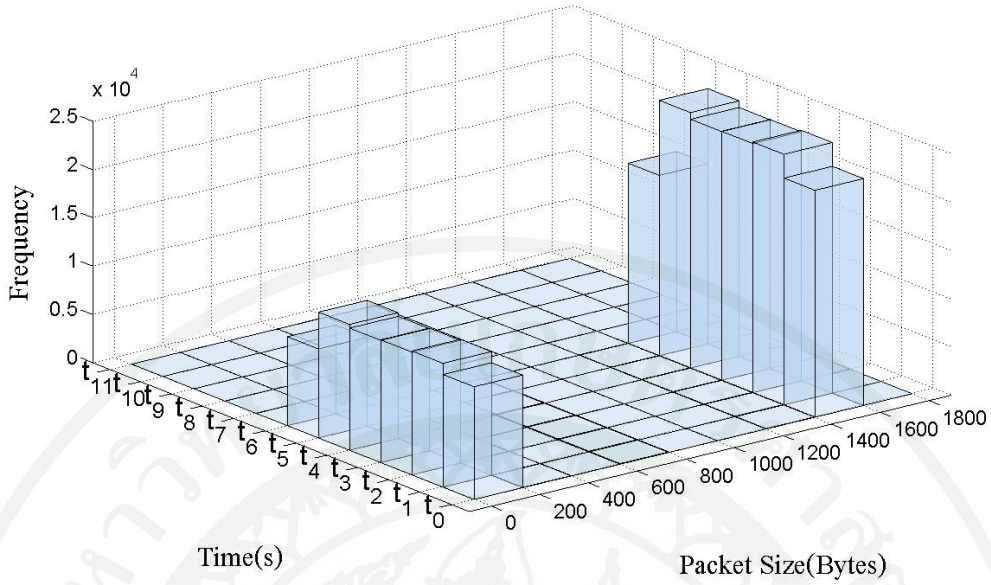
ซึ่งผลของการทดลองสมมติฐานของแต่ละการทดลองจะนำมาวิเคราะห์การกระจายตัวของขนาดเฟรมข้อมูล โดยนำข้อมูลในช่วง 600 วินาทีแรก มาแบ่งกลุ่มตามช่วงเวลา แต่ละช่วงห่างกัน 60 วินาที นำมาสร้างกราฟฮีสโตแกรมสามมิติ (Histogram 3D) เพื่อดูลักษณะการกระจายตัวของขนาดเฟรมข้อมูล โดยกำหนดให้แกน X เป็นช่วงของขนาดที่แต่ละช่วงมีความกว้าง 200 ไบต์ แกน Y เป็นช่วงของระยะเวลาที่แต่ละช่วงมีความกว้าง 60 วินาที และแกน Z เป็นความถี่ของขนาดเฟรมข้อมูลที่เกิดขึ้นในแต่ละช่วงเวลา ซึ่งผลการวิเคราะห์ข้อมูลการทดลอง นำมาสร้างกราฟได้ดังนี้



ภาพที่ 23 กราฟฮีสโตแกรมสามมิติ ของการทดลองที่ 1 (เอชทีทีพี)



ภาพที่ 24 กราฟฮีสโตแกรมสามมิติ ของการทดลองที่ 2 (เอฟทีพี)



ภาพที่ 25 กราฟฮีสโตแกรมสามมิติ ของการทดลองที่ 3 (บิตทอร์เรนต์)

ในส่วนของการทดลองที่มีเครื่องลูกข่ายดาวน์โหลดข้อมูลอยู่เครื่องเดียว วิธีการวิเคราะห์ข้อมูลจะทำโดยการจับคู่ที่อยู่แม็คระหว่างเครื่องแม่ข่ายกับเครื่องลูกข่าย แล้วกรองเฟรมให้เหลือเฉพาะเฟรมข้อมูล จากนั้นจึงทำการวิเคราะห์การกระจายตัวของขนาดเฟรมข้อมูลในแต่ละช่วงเวลา ซึ่งจากการผลการวิเคราะห์ข้อมูลโดยใช้กราฟฮีสโตแกรมสามมิติ ของการทดลองที่ 1-3 ดังแสดงได้จาก ภาพที่ 23-25 ตามลำดับ พบว่าขนาดเฟรมข้อมูลที่มีความถี่มากที่สุดจะอยู่ในช่วง 1400-1600 ไบต์ จะมีความถี่อยู่ที่ 15000-20000 เฟรมในหนึ่งช่วงเวลา รองลงมาจะเป็นขนาดเฟรมข้อมูลอยู่ในช่วง 0-200 ไบต์ จะพบความถี่ในแต่ละช่วงเวลาเกิดขึ้นประมาณ 5000-10000 เฟรม ซึ่งพบคุณลักษณะเช่นนี้เป็นไปในทางเดียวกันทั้ง 3 การทดลอง โดยขนาดเฟรมจะมีความถี่สูงตั้งแต่ช่วงเวลา t_0 - t_4 และจะเริ่มตกลงในช่วงเวลา t_5 ซึ่งวิเคราะห์ได้ว่าสาเหตุที่ความถี่ที่ช่วงเวลา t_5 ลดลงเนื่องมาจาก ได้ทำการดาวน์โหลดไฟล์เสร็จสิ้นในช่วงเวลา t_5 นั่นเอง

เมื่อทำการตรวจสอบในรายละเอียด พบว่าขนาดเฟรมที่มีความถี่สูงที่สุดในแต่ละช่วงเวลาคือ ขนาดเฟรม 1557 ไบต์ ซึ่งมีรายละเอียดเฟรมเป็นการส่งข้อมูลเต็ม MSDU เนื่องมาจากสภาพแวดล้อมเครือข่ายไร้สายที่ทำการทดลองเป็นสภาพแวดล้อมควบคุม จึงไม่มีการเข้าแข่งขันแย่งเข้าใช้สื่อ โพรโทคอลจึงสามารถดาวน์โหลดข้อมูลได้ในปริมาณที่สูงสุด รองลงมาคือขนาดเฟรม 97 ไบต์ ซึ่งรายละเอียดเฟรมเป็น แอ็คของชั้นขนส่ง ที่ส่งมาเพื่อยืนยันว่าได้รับข้อมูลที่ดาวน์โหลดเรียบร้อยแล้ว

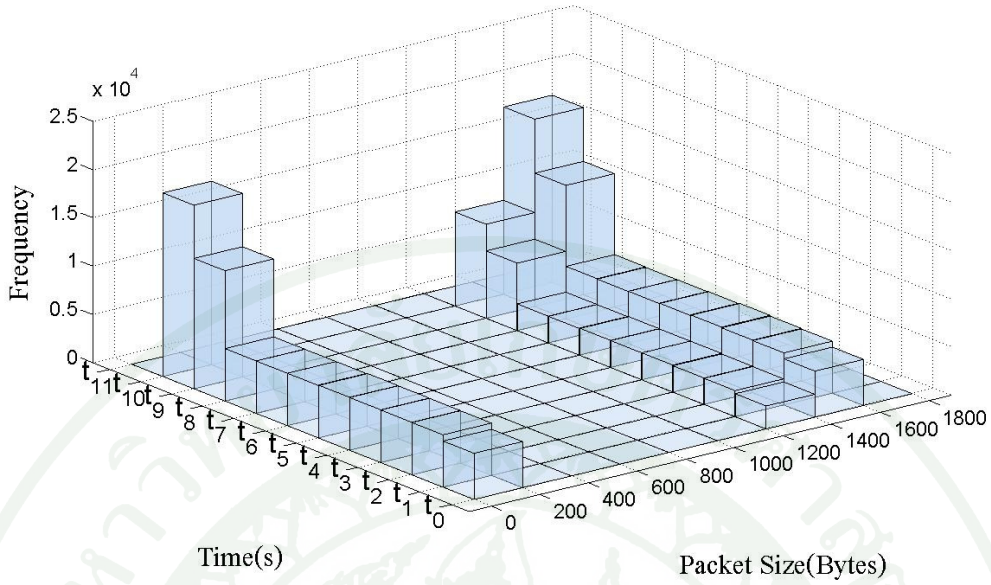
ในส่วนของผลการทดลองที่ 1 ที่ใช้โพรโทคอลเอชทีทีพีในการดาวน์โหลดไฟล์จะมีขนาดเฟรมข้อมูลที่มีปริมาณมากนอกเหนือจาก ขนาดเฟรม 1557 ไบต์ และ 97 ไบต์ นั่นคือขนาดเฟรมช่วง 1200-1400 ไบต์ โดยพบมีความถี่อยู่ที่ประมาณ 2000 เฟรมในแต่ละช่วงเวลา ซึ่งเมื่อตรวจสอบข้อมูลอย่างละเอียด พบว่าเป็นขนาดเฟรม 1273 ไบต์ ซึ่งรายละเอียดของเฟรมคือเฟรมข้อมูลขนาด 1176 ไบต์ ที่มาพร้อมกับพุช (PSH : Push) และแอ็คของชั้นขนส่ง ซึ่งเป็นการบังคับส่งข้อมูลของโปรแกรมเว็บเซิร์ฟเวอร์ (Wikipedia, n.d.) เพื่อให้การตอบสนองการทำงานของหน้าเว็บ (Web Page) รวดเร็วขึ้น จึงมักจะพบขนาดเฟรมชนิดนี้มีความถี่สูงได้ โดยเฉพาะกรณีการดาวน์โหลดไฟล์ผ่านโพรโทคอลเอชทีทีพี

อย่างไรก็ตามคุณลักษณะการกระจายตัวของขนาดเฟรมข้อมูลเช่นนี้ ยังไม่มีความแตกต่างอย่างมีนัยสำคัญ ที่จะสามารถใช้เป็นเครื่องมือในการตรวจจับโพรโทคอลบิตทอร์เรนต์ได้

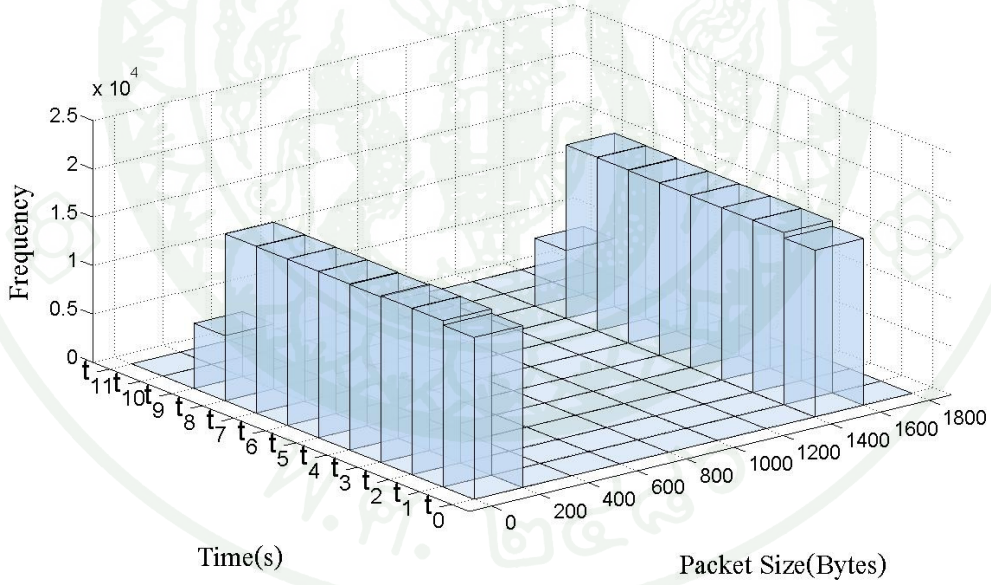
ในส่วนของการทดลองที่มีเครื่องลูกข่ายมากกว่าหนึ่งเครื่อง การวิเคราะห์ข้อมูลจะใช้การจับคู่ที่อยู่แม็คระหว่างเครื่องแม่ข่ายกับเครื่องลูกข่ายทีละคู่ แล้วจึงกรองเฟรมให้เหลือเฉพาะเฟรมข้อมูล และทำการวิเคราะห์การกระจายตัวของขนาดเฟรมข้อมูลในแต่ละช่วงเวลา ในแต่ละคู่แม็คเช่นเดียวกันกับในส่วนของการทดลองที่ใช้เครื่องลูกข่ายเครื่องเดียว ซึ่งจากการผลการวิเคราะห์ข้อมูลโดยใช้กราฟฮีสโตแกรมสามมิติ ของการทดลองที่ 4-7 พบว่าขนาดเฟรมข้อมูลที่มีความถี่มากที่สุดยังคงอยู่ในช่วง 1400-1600 ไบต์ และ 0-200 ไบต์ ในทุกการทดลอง และยังพบขนาดเฟรมที่อยู่ในช่วง 1200-1400 ไบต์ ที่มีความถี่ในแต่ละช่วงเวลาเกิดขึ้นประมาณ 2000-2500 เฟรม ในการทดลองที่มีเครื่องลูกข่ายเอชทีทีพีเช่นเดิม

จากการวิเคราะห์ข้อมูลทำให้พบว่ากราฟฮีสโตแกรมสามมิติสามารถบ่งบอกถึงความสามารถในการแย่งเข้าใช้สื่อของแต่ละโพรโทคอลได้ โดยโพรโทคอลที่สามารถแย่งเข้าใช้สื่อได้มากกว่าโพรโทคอลอื่นในช่วงเวลาใด ๆ จะมีความถี่ของขนาดเฟรมข้อมูลสูงกว่าอีกโพรโทคอลหนึ่งซึ่งแย่งใช้สื่อได้น้อยกว่า จะเห็นได้กราฟผลการทดลองที่ 4 ในช่วงแรกโพรโทคอลบิตทอร์-เรนต์จะมีความถี่ของขนาดเฟรมข้อมูลต่ำกว่าโพรโทคอลเอชทีทีพี ทั้งนี้สันนิษฐานว่าเนื่องมาจากกลไกการทำงานของบิตทอร์เรนต์ที่ต้องติดต่อประสานจังหวะกับเพียร์และแทรกเกอร์ก่อนจะเริ่มส่งข้อมูล แต่หลังจากที่ผ่านกระบวนการติดต่อระหว่างเพียร์เรียบร้อยแล้ว เมื่อเริ่มทำการส่งข้อมูลจริง ๆ โพรโทคอลบิตทอร์เรนต์ก็จะสามารถแย่งเข้าใช้สื่อได้มากกว่าโพรโทคอลเอชทีทีพี

ภาพที่ 26 – 29 จะแสดงกราฟฮีสโตแกรมสามมิติ ที่เป็นการวิเคราะห์ผลจากการทดลองที่มีเครื่องลูกข่ายมากกว่า 1 เครื่อง



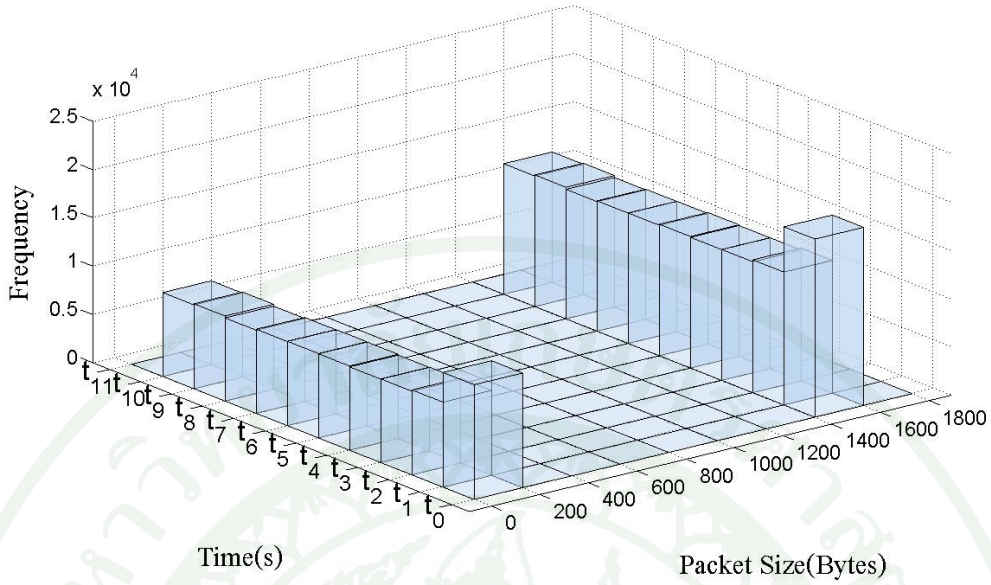
ก. เครื่องลูกข่ายเอชทีทีพี



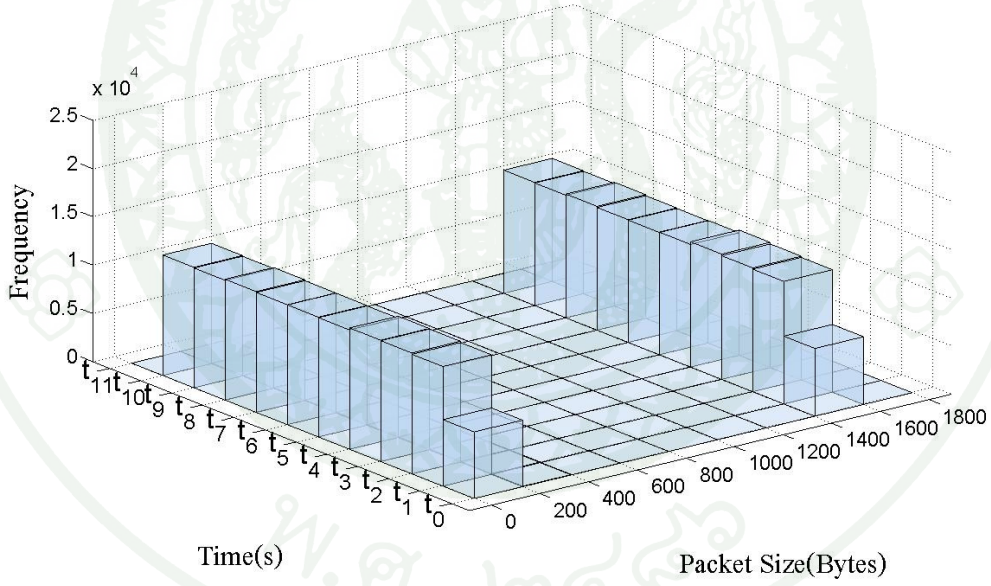
ข. เครื่องลูกข่ายเอฟทีพี

ภาพที่ 26 กราฟฮีสโตแกรมสามมิติ ของการทดลองที่ 4 (เอชทีทีพีและเอฟทีพี)

ในส่วนของการทดลองที่ 5 ที่มีการแย่งใช้สื่อระหว่างโพรโทคอลเอฟทีพีกับโพรโทคอลบิตทอร์เรนต์ ซึ่งในช่วงเวลาแรก โพรโทคอลบิตทอร์เรนต์สามารถแย่งใช้สื่อได้น้อยกว่าเอฟทีพีเช่นเคย ต่อมาเมื่อช่วงเวลา t_1 เป็นต้นมา โพรโทคอลบิตทอร์เรนต์สามารถแย่งใช้สื่อได้พอ ๆ กับโพรโทคอลเอฟทีพี โดยสังเกตได้จากปริมาณความถี่ของเฟรมข้อมูลในแต่ละช่วงเวลา



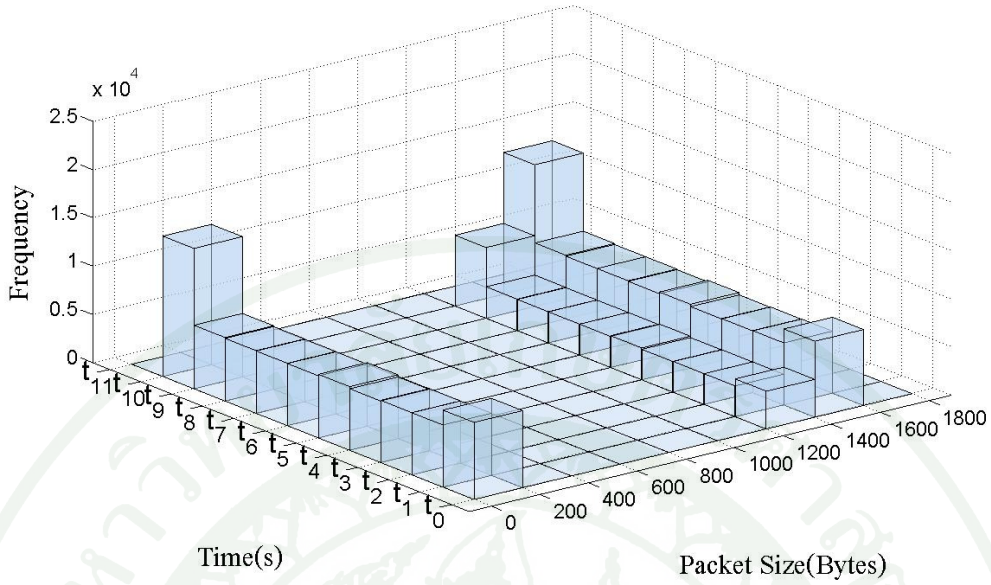
ก. เครื่องลูกข่ายเอฟทีพี



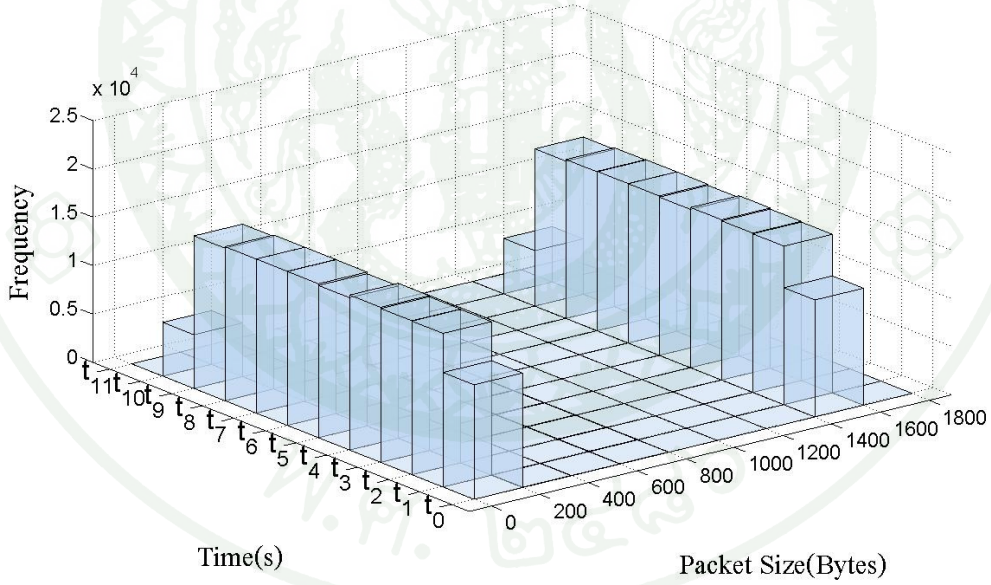
ข. เครื่องลูกข่ายบิตทอร์เรนต์

ภาพที่ 27 กราฟฮีสโตแกรมสามมิติ ของการทดลองที่ 5 (เอฟทีพีและบิตทอร์เรนต์)

กราฟการกระจายตัวของขนาดเฟรมข้อมูลของการทดลองดาวน์โหลดข้อมูลระหว่างโพรโทคอลเอฟทีพีกับโพรโทคอลเอชทีทีพีในการทดลองที่ 6 มีลักษณะคล้ายคลึงกับผลของการทดลองที่ 4 กล่าวคือโพรโทคอลเอฟทีพีมีการแย่งใช้สื่อได้มากกว่าเอชทีทีพี และขนาดเฟรมในช่วง 1200-1400 ไบต์ของโพรโทคอลเอชทีทีพีมีความถี่สูง

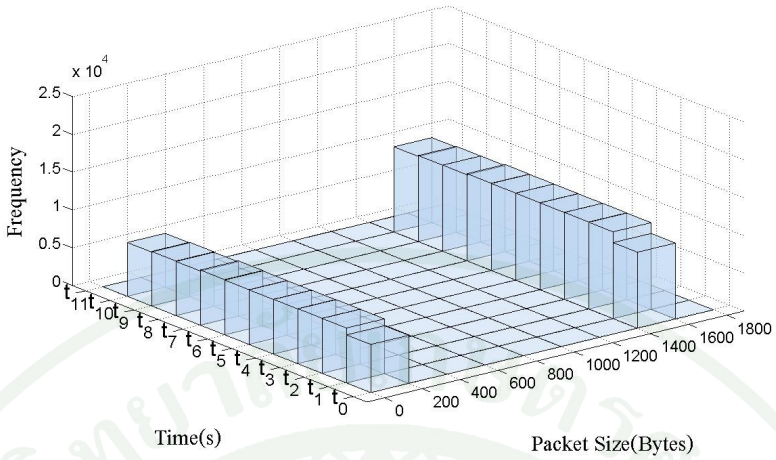


ก. เครื่องลูกข่ายเอชทีทีพี

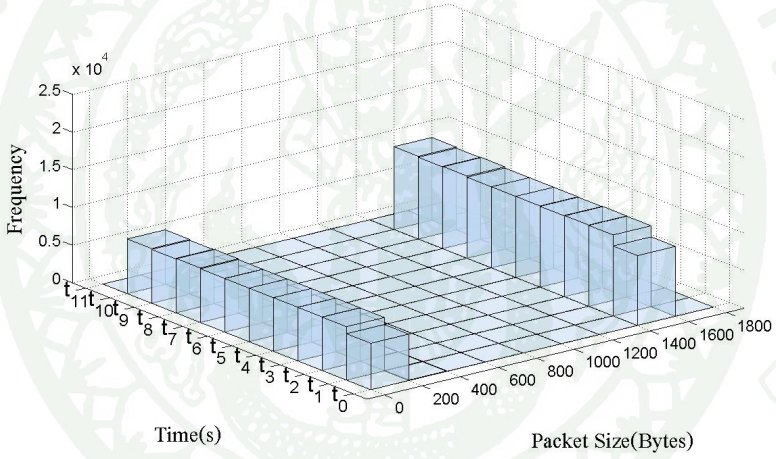


ข. เครื่องลูกข่ายบิตทอร์เรนต์

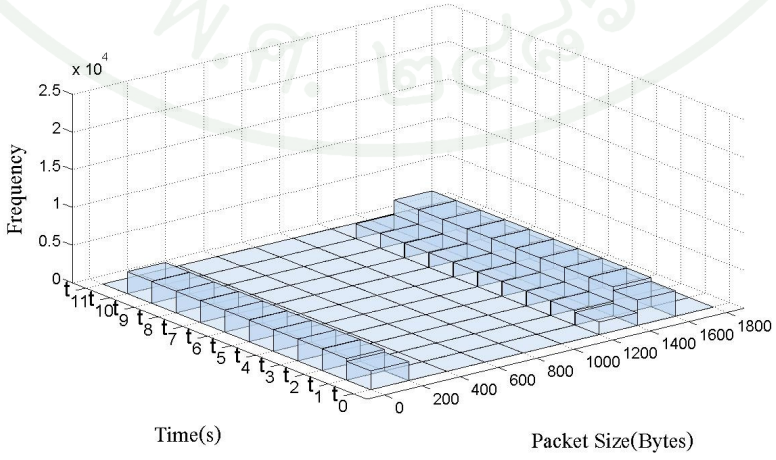
ภาพที่ 28 กราฟฮีสโตแกรมสามมิติ ของการทดลองที่ 6 (เอชทีทีพีและบิตทอร์เรนต์)



ก. เครื่องลูกข่ายเอฟทีพี



ข. เครื่องลูกข่ายบิตทอร์เรนต์



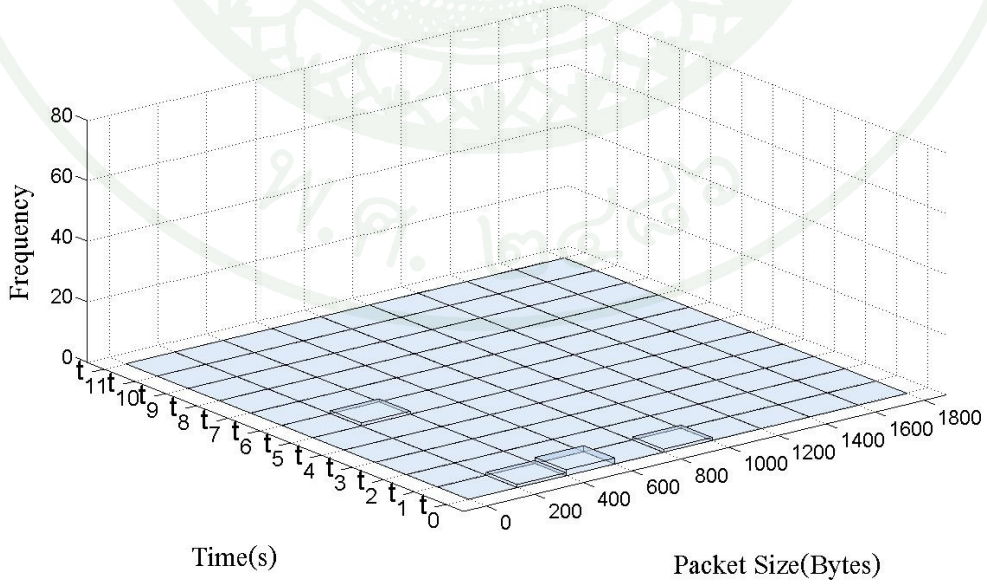
ค. เครื่องลูกข่ายเอชทีทีพี

ภาพที่ 29 กราฟฮีสโตแกรมสามมิติ ของการทดลองที่ 7 (รวมทุกโพรโทคอล)

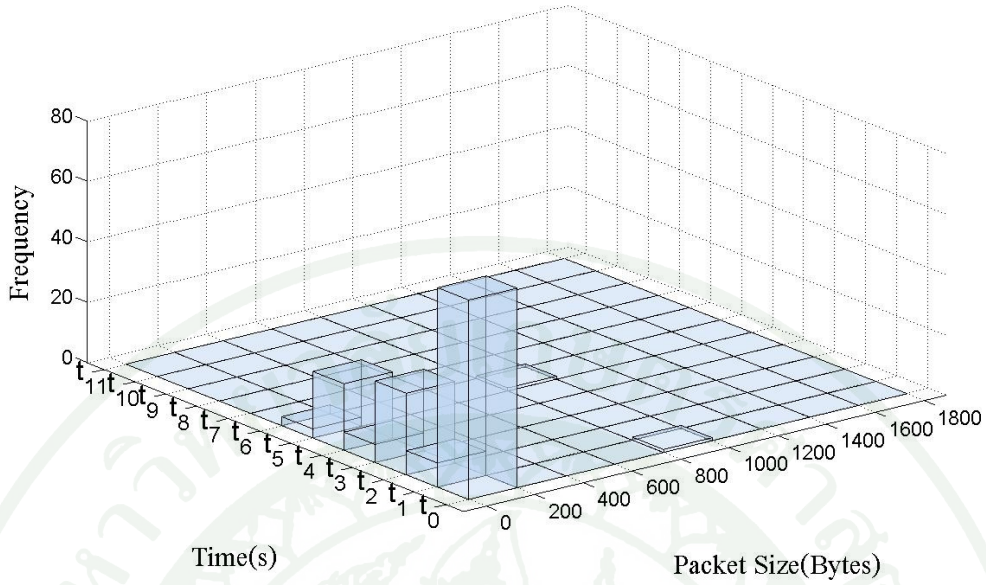
ผลจากการทดลองศึกษาการกระจายตัวของเฟรมข้อมูลจากทั้ง 7 การทดลอง พบว่าการกระจายตัวของขนาดเฟรมข้อมูลของโพรโทคอลแต่ละชนิดยังไม่มีความแตกต่างอย่างเป็นนัยสำคัญ และการกระจายตัวของขนาดเฟรมข้อมูลของโพรโทคอลบิตทอร์เรนต์ยังไม่เป็นเอกลักษณ์อย่างชัดเจน จึงยังไม่สามารถที่จะนำคุณลักษณะการกระจายตัวของขนาดเฟรมข้อมูลของโพรโทคอลมาใช้ในการออกแบบกลไกตรวจจับโพรโทคอลบิตทอร์เรนต์ได้

อย่างไรก็ตาม จากการสังเกตปริมาณความถี่ของขนาดเฟรมข้อมูลต่าง ๆ ที่ได้จากการทดลองซึ่งเฟรมที่มีปริมาณมากจะเป็นเฟรมข้อมูล ดังนั้นจึงน่าจะมีเฟรมที่มีปริมาณความถี่น้อย ที่เป็นเฟรมที่ใช้ในการติดต่อประสานจังหวะระหว่างเพียร์ที่เป็นคุณลักษณะเฉพาะที่มีเพียงในโพรโทคอลบิตทอร์เรนต์ซ่อนอยู่ ในแต่ละช่วงเวลา จึงได้เกิดข้อสมมติฐานที่ว่า ถ้าทำการกรองขนาดเฟรมข้อมูลที่มีความถี่ในปริมาณมากออกไป ก็จะสามารถเห็นคุณลักษณะการกระจายตัวของเฟรมข้อมูลที่เป็นเฟรมการติดต่อประสานจังหวะระหว่างเพียร์ ที่เป็นคุณลักษณะเฉพาะของโพรโทคอลบิตทอร์เรนต์ ซึ่งสามารถนำมาใช้ออกแบบกลไกตรวจจับโพรโทคอลบิตทอร์เรนต์ได้

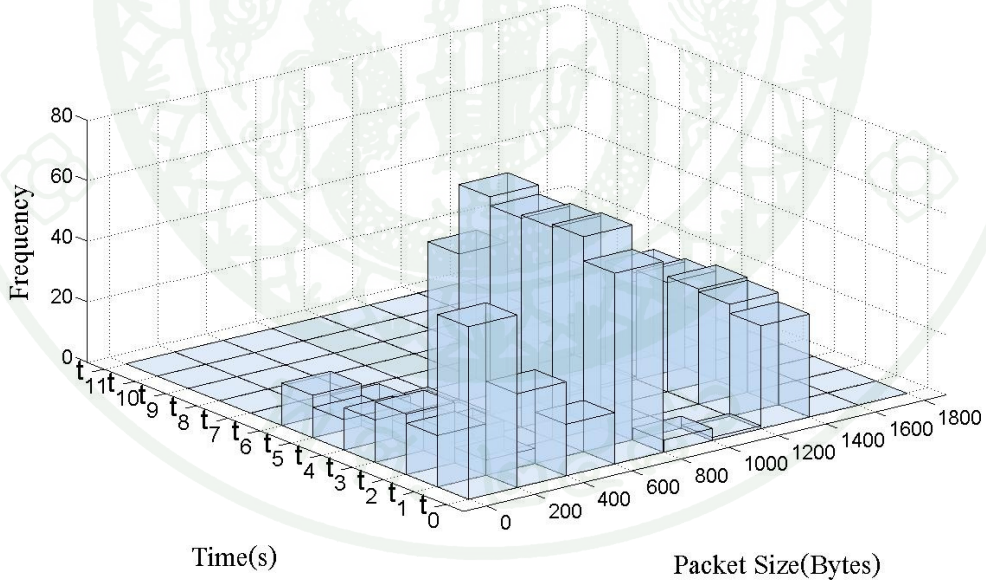
จากสมมติฐานนี้จึงได้ทำการวิเคราะห์ข้อมูลจากทั้ง 7 การทดลองใหม่ โดยทำการกรองขนาดเฟรมข้อมูลที่มีปริมาณมากออกเสียก่อน โดยขนาดเฟรมที่ทำการกรองออกได้แก่ ขนาดเฟรม 1557 ไบต์, 1273 ไบต์, และ 97 ไบต์ ซึ่งผลของการทดลองหลังจากที่กรองขนาดเฟรมที่มีปริมาณมากออกไปแล้วสามารถแสดงเป็นกราฟฮีสโตแกรมสามมิติดังนี้



ภาพที่ 30 กราฟฮีสโตแกรมสามมิติ ของการทดลองที่ 1 (เอชทีทีพี) หลังจากกรองเฟรม



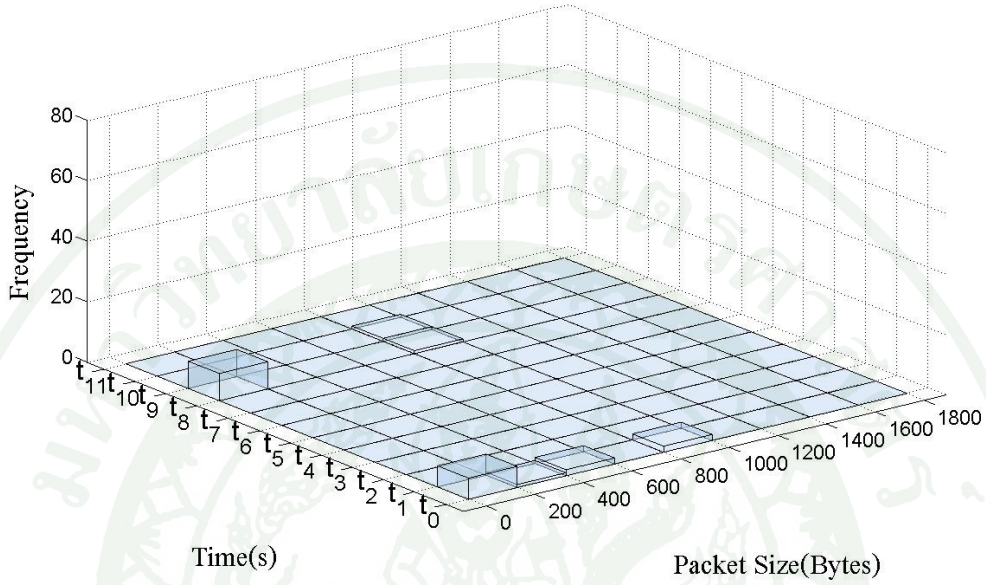
ภาพที่ 31 กราฟฮีสโตแกรมสามมิติ ของการทดลองที่ 2 (เอฟทีพี) หลังจากกรองเฟรม



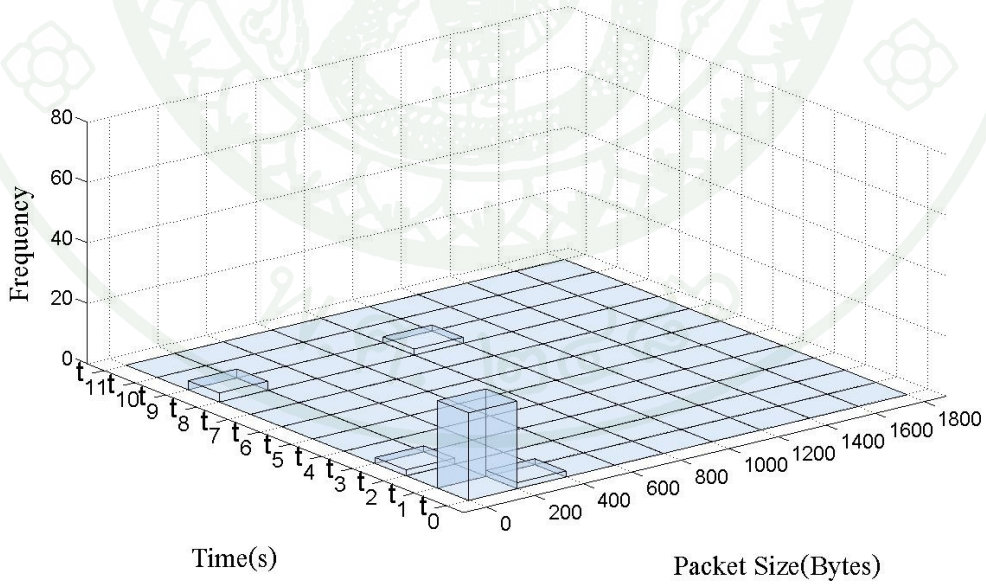
ภาพที่ 32 กราฟฮีสโตแกรมสามมิติ ของการทดลองที่ 3 (บิตทอร์เรนต์) หลังจากกรองเฟรม

ภาพที่ 30-32 เป็นกราฟฮิสโตแกรมสามมิติที่แสดงการกระจายตัวของขนาดเฟรมข้อมูล ที่สร้างจากผลการทดลองที่ 1-3 ตามลำดับ

ในส่วนของการทดลองที่มีเครื่องลูกข่าย 2 เครื่อง ผลการทดลองการกระจายตัวของขนาดเฟรมข้อมูลสามารถแสดงได้ดังภาพที่ 32-35 และภาพที่ 36 แสดงผลการทดลองที่มีเครื่องลูกข่าย 3 เครื่องด้วยกัน

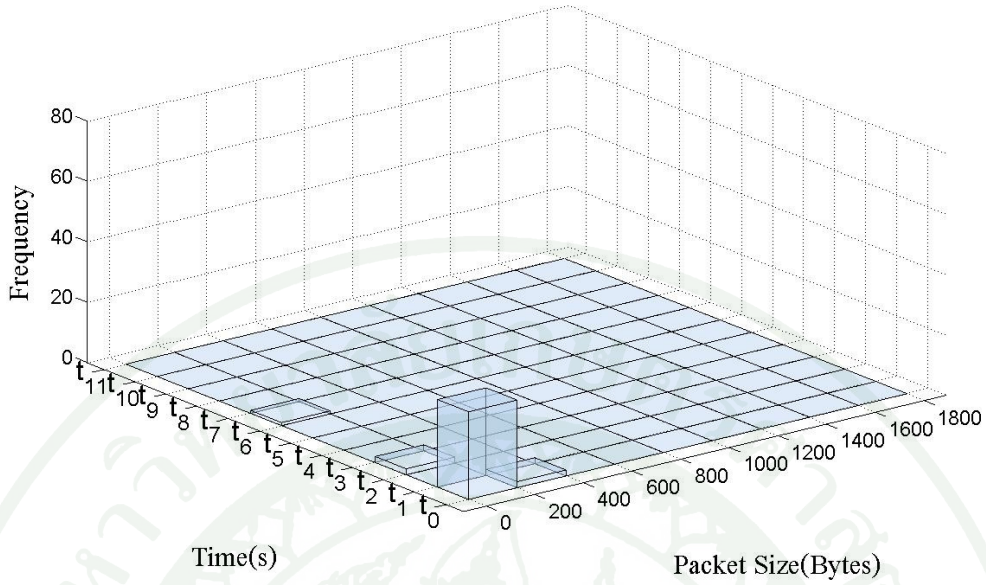


ก. เครื่องลูกข่ายเอชทีทีพี

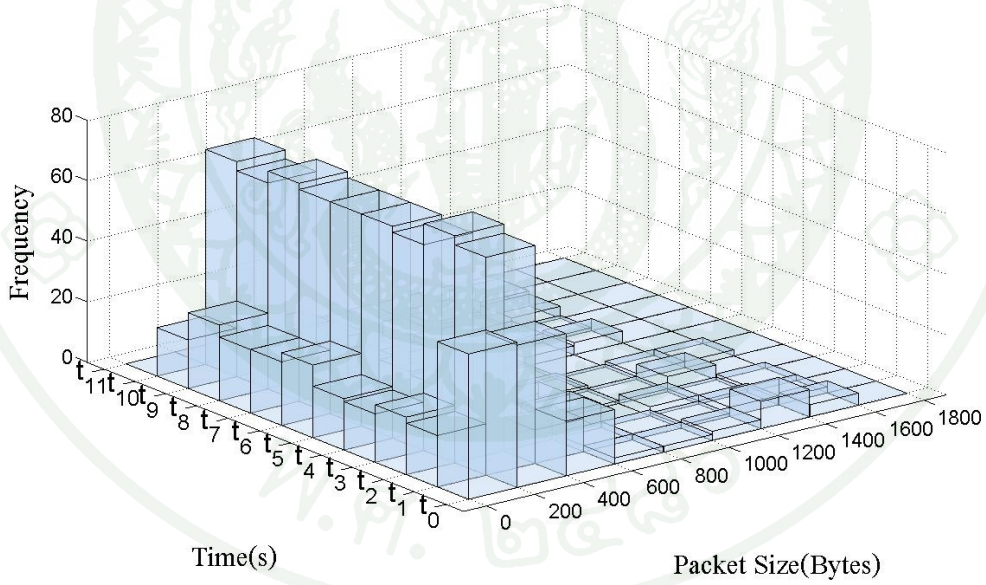


ข. เครื่องลูกข่ายเอฟทีพี

ภาพที่ 33 กราฟฮีสโตแกรมสามมิติ ของการทดลองที่ 4 (เอชทีทีพี และ เอฟทีพี) หลังจากกรองเฟรม

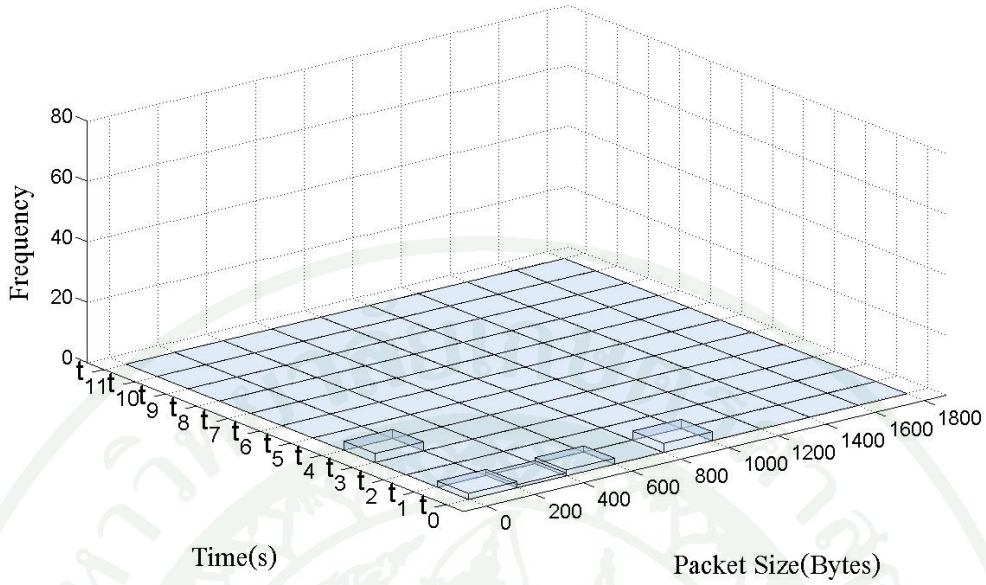


ก. เครื่องลูกข่ายเอฟทีพี

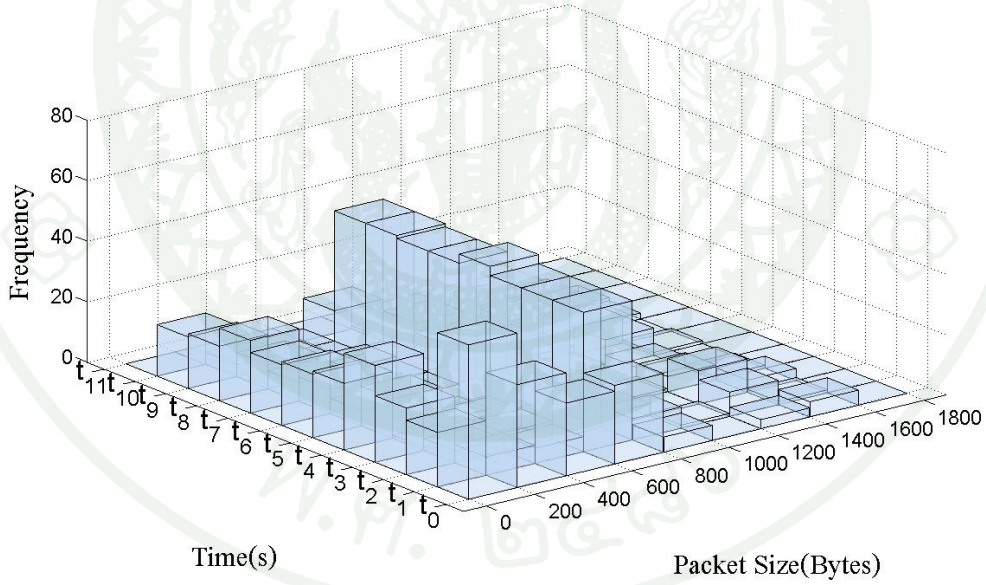


ข. เครื่องลูกข่ายบิตทอร์เรนต์

ภาพที่ 34 กราฟฮีสโตแกรมสามมิติ ของการทดลองที่ 5 (เอฟทีพี และ บิตทอร์เรนต์) หลังจากกรองเฟรม

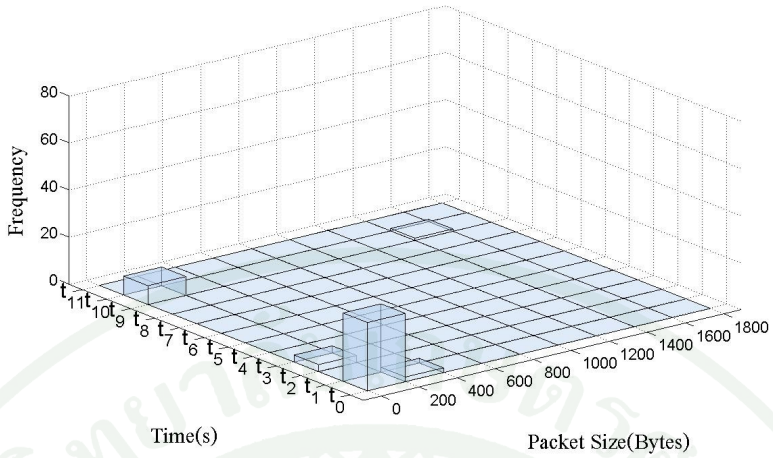


ก. เครื่องลูกข่ายเอชทีทีพี

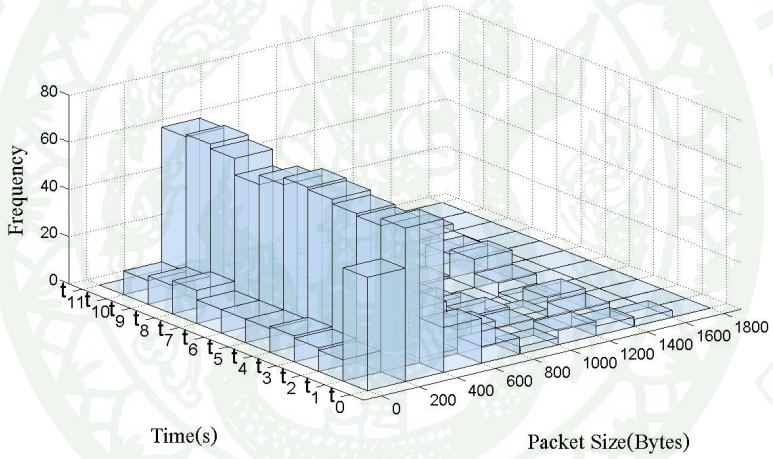


ข. เครื่องลูกข่ายบิตทอร์เรนต์

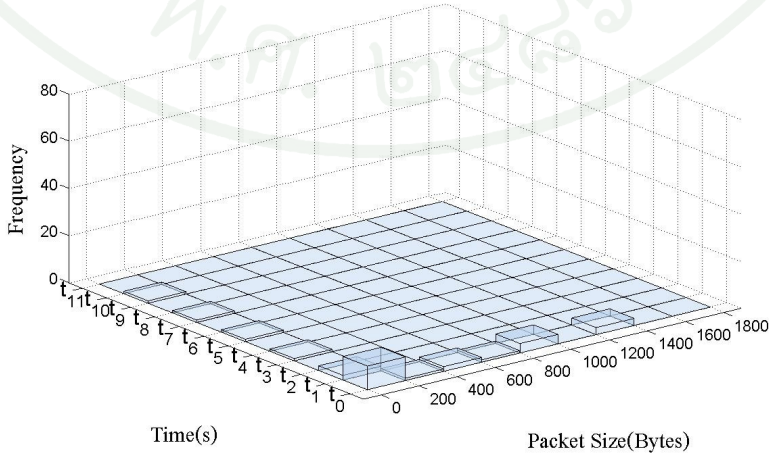
ภาพที่ 35 กราฟฮีสโตแกรมสามมิติ ของการทดลองที่ 6 (เอชทีทีพี และ บิตทอร์เรนต์) หลังจากกรองเฟรม



ก. เครื่องลูกข่ายเอฟทีพี



ข. เครื่องลูกข่ายบิตทอร์เรนต์



ค. เครื่องลูกข่ายเอชทีทีพี

ภาพที่ 36 กราฟฮีสโตแกรมสามมิติ ของการทดลองที่ 7 (รวมทุกโพรโทคอล) หลังจากกรองเฟรม

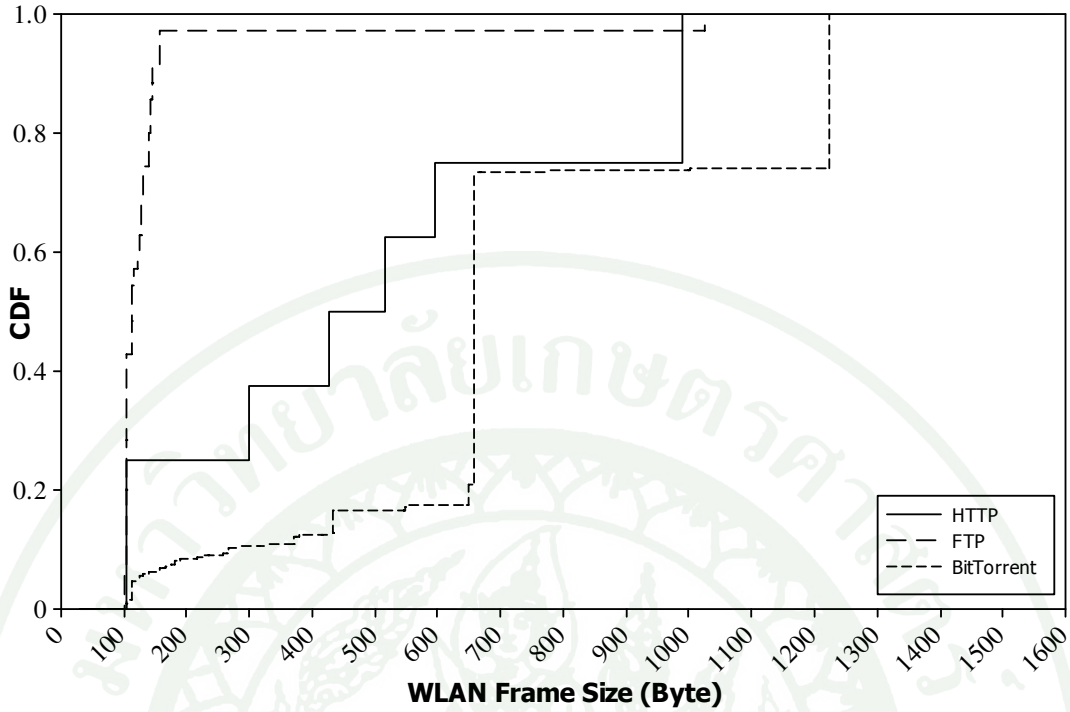
ในการวิเคราะห์ผลการทดลองที่ 1 หลังจากการกรองเฟรมที่มีปริมาณมากออกไป จากกราฟพบว่าขนาดเฟรมที่หลงเหลือจากการกรองมีเพียง 5 ขนาดเท่านั้น ซึ่งขนาดเฟรมเกือบทั้งหมดพบที่ช่วงเวลาแรกของการทดลองซึ่งสันนิษฐานได้ว่าเป็นเฟรมข้อมูลที่ใช้ในการติดต่อประสานจังหวะกันระหว่างเครื่องลูกข่ายกับเครื่องแม่ข่ายก่อนเริ่มส่งข้อมูล และขนาดเฟรมข้อมูลที่พบในช่วงเวลาสุดท้ายสามารถอธิบายได้ว่าเป็นการส่งข้อมูลเพื่อบ่งบอกว่าการดาวน์โหลดไฟล์เสร็จสิ้นแล้ว

สำหรับการดาวน์โหลดไฟล์ผ่านโพรโทคอลเอฟทีพีในการทดลองที่ 2 หลังจากการกรองขนาดเฟรมที่มีปริมาณมากออกไป กราฟแสดงให้เห็นว่า ณ ช่วงเวลาแรกขนาดเฟรมข้อมูลจะมีปริมาณมากที่สุดประมาณ 40-60 เฟรม ซึ่งสามารถอธิบายได้ว่าเป็นเฟรมที่ส่งข้อมูลคำสั่งเอฟทีพี (FTP Command) เพื่อติดต่อประสานจังหวะกันกับเครื่องแม่ข่ายก่อนจะเริ่มทำการส่งข้อมูล ในส่วนของช่วงเวลาอื่น ๆ จะพบขนาดเฟรมที่มีปริมาณประมาณ 20 เฟรม อยู่ในช่วงเวลา t_1-t_5 ซึ่งสันนิษฐานเป็นการพยายามเชื่อมต่อ (reconnect) ของโปรแกรมเอฟทีพีไคลเอนต์กับเครื่องแม่ข่ายซึ่งมีการตั้งเวลาตัดการเชื่อมต่อจากเครือข่าย (Disconnect Time) เอาไว้

การกระจายตัวของเฟรมข้อมูลในผลการทดลองที่ 3 ซึ่งทดลองกับโพรโทคอลบิตทอร์เรนต์ซึ่งหลังจากการกรองขนาดเฟรมที่มีปริมาณมากออกไปแล้ว กราฟฮีสโตแกรมสามมิติได้แสดงให้เห็นถึงคุณลักษณะการกระจายตัวอันเป็นเอกลักษณ์ของโพรโทคอลบิตทอร์เรนต์ กล่าวคือในแต่ละช่วงเวลาจะมีการกระจายตัวของขนาดเฟรมที่หลากหลายซึ่งสอดคล้องกับสมมติฐานที่ได้ตั้งเอาไว้ โดยช่วงขนาดเฟรมที่มีปริมาณมากที่สุดในแต่ละช่วงเวลาได้แก่ ขนาดเฟรมช่วง 600-800 ไบต์ โดยมีปริมาณเฟรมอยู่ในช่วง 40-60 เฟรม ในแต่ละช่วงเวลา ซึ่งอธิบายได้ว่า เฟรมเหล่านี้เกิดจากพฤติกรรมการส่งข้อมูลเพื่อติดต่อประสานจังหวะระหว่างเพียร์ที่เกิดขึ้นนอกเหนือจากการรับ-ส่งข้อมูล โดยเฟรมข้อมูลเหล่านี้จะค่อนข้างมีขนาดเล็กและมีปริมาณความถี่ที่เกิดขึ้นน้อยในแต่ละช่วงเวลา ซึ่งสอดคล้องกับสมมติฐานที่ตั้งไว้ข้างต้น

ในส่วนของการกระจายตัวของขนาดเฟรมข้อมูลในการทดลองที่ 4-7 ที่มีเครื่องลูกข่ายมากกว่า 1 เครื่อง เมื่อทำการจับคู่ที่อยู่แม็คระหว่างเครื่องลูกข่ายกับเครื่องแม่ข่าย แล้วนำข้อมูลการกระจายตัวของเฟรมมาสร้างกราฟ พบว่าเครื่องลูกข่ายที่ดาวน์โหลดไฟล์ผ่านโพรโทคอลแต่ละชนิดมีลักษณะการกระจายตัวของขนาดเฟรมข้อมูลเป็นไปในแนวทางเดียวกันกับการทดลองที่ 1-3

เราสามารถใช้กราฟซีดีเอฟ (CDF : Cumulative Distribution Function) เพื่อเปรียบเทียบการกระจายตัวของขนาดเฟรมข้อมูลในแต่ละโพรโทคอลโดยภาพที่ 37 เป็นการแสดงการกระจายตัวของขนาดเฟรม ในช่วงเวลา 360 วินาทีแรก ของการทดลองที่ 1-3



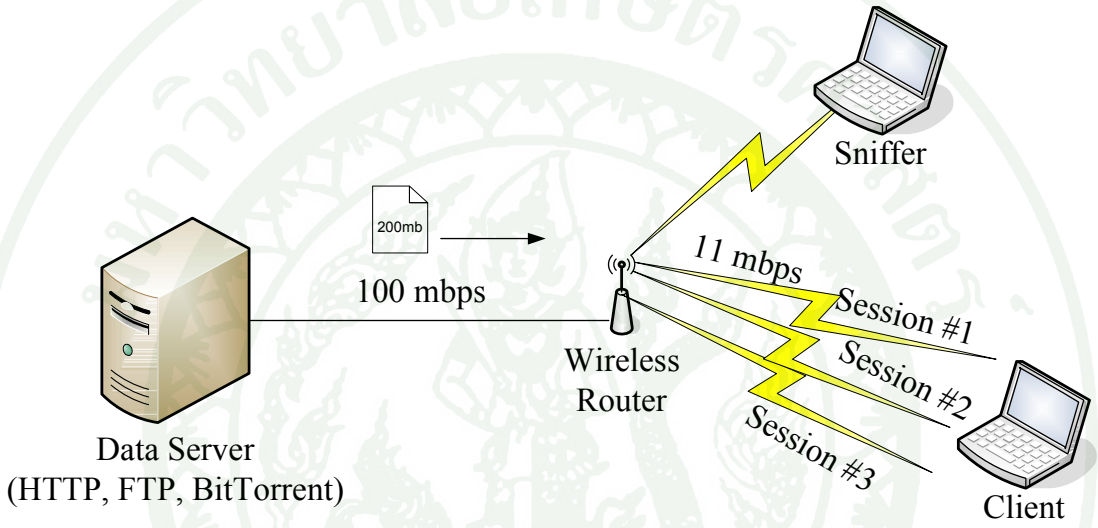
ภาพที่ 37 กราฟการกระจายตัวของขนาดเฟรมข้อมูลในแต่ละโพรโทคอลหลังจากกรองเฟรมแล้วของการทดลองที่ 1-3

จากภาพที่ 37 จะเห็นถึงความแตกต่างของการกระจายตัวของขนาดเฟรมข้อมูลของโพรโทคอลบิตทอร์เรนต์ ซึ่งมีความแตกต่างจากการกระจายตัวของโพรโทคอลอื่นอย่างมีนัยสำคัญ จากกราฟจะเห็นรอยหยักเป็นขั้นบันไดซึ่งก็คือขนาดของเฟรมข้อมูลที่แตกต่างกัน ดังจะเห็นได้ว่าโพรโทคอลบิตทอร์เรนต์มีปริมาณของขนาดเฟรมข้อมูลมากกว่าทั้งโพรโทคอลเอชทีทีพี และ เอฟทีพี ณ ช่วงเวลาใด ช่วงเวลาหนึ่ง ด้วยวิธีการจัดกลุ่มเฟรมข้อมูลตามขนาดเฟรมและทำการนับจำนวนขนาดของเฟรมข้อมูลที่พบ ณ ช่วงเวลาใดนี้ จึงน่าจะสามารถใช้ในการออกแบบกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์ โดยใช้เฉพาะข้อมูลบนชั้นแม็คที่มีเฉพาะในเครือข่ายไร้สายได้

อย่างไรก็ตาม ในการใช้งานจริงนั้น โอกาสที่ผู้ใช้งานจะทำการใช้งานเครือข่ายไร้สายเพียงแค่โพรโทคอลเดียวนั้นมีน้อยมาก ประกอบกับข้อจำกัดของการใช้ข้อมูลเฉพาะในชั้นแม็ค ที่ไม่สามารถแยกดูการติดต่อรับ-ส่งข้อมูลเฉพาะแอพพลิเคชั่นได้ จึงจำเป็นต้องมีการออกแบบการทดลองในกรณีที่มีการรับ-ส่งข้อมูลผ่านเครือข่ายไร้สายผสมกันหลายโพรโทคอล โดยได้กำหนดสมมติฐานไว้ว่า ถึงแม้การใช้ข้อมูลที่ชั้นแม็คเพียงอย่างเดียวจะไม่สามารถแยกโพรโทคอลบิตทอร์เรนต์ออกจากข้อมูลที่มีการผสมปนเปกันจากหลายโพรโทคอลที่กำลังใช้งานอยู่ได้ แต่ด้วยวิธีการกรองขนาดเฟรมข้อมูลที่ไม่ใช่เกิดจากพฤติกรรมการรับ-ส่งข้อมูลของโพรโทคอลบิตทอร์เรนต์ออกก็จะสามารถเห็นพฤติกรรมการกระจายตัวของขนาดเฟรมข้อมูลของโพรโทคอล

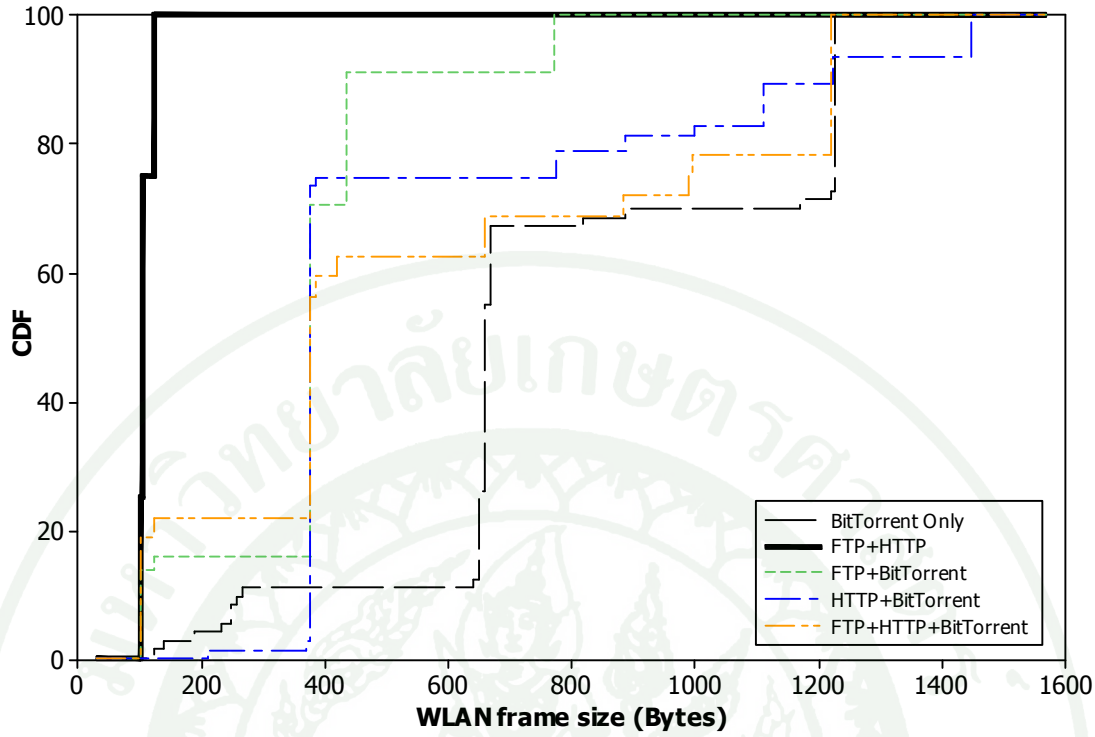
บิตทอร์เรนต์ชัดเจนขึ้น จนทำให้สามารถที่จะบ่งบอกถึงการมีอยู่ของโพรโทคอลบิตทอร์เรนต์ในข้อมูลซึ่งมีการผสมปนเปกันของโพรโทคอลหลายโพรโทคอลได้

การทดสอบสมมติฐานทำได้โดยการออกแบบการทดลองให้เครื่องลูกข่าย 1 เครื่องทำการดาวน์โหลดข้อมูลจากเครื่องแม่ข่ายผ่านโพรโทคอลต่างวาระกัน ในเครื่องเดียวกันดังจะแสดงได้ดังภาพที่ 38



ภาพที่ 38 การทดลองดาวน์โหลดไฟล์ด้วยโพรโทคอลต่างวาระกันบนเครื่องลูกข่ายเดียวกัน

วิธีทำการทดลองจะเหมือนกับการทดลองที่ใช้เครื่องลูกข่ายหลายเครื่องทุกประการยกเว้นเพียงจำนวนเครื่องลูกข่ายที่ใช้งานจะมีเพียงเครื่องเดียวเท่านั้น ซึ่งผลจากการทดลองการหาลักษณะการกระจายตัวของโพรโทคอลบิตทอร์เรนต์ในกรณีที่มีข้อมูลผสมกันหลายโพรโทคอลสามารถแสดงได้ดังนี้



ภาพที่ 39 กราฟซีดีเอฟการกระจายตัวของเฟรมข้อมูลที่มีโพรโทคอลบิตทอร์เรนต์ผสมอยู่ ณ วินาทีที่ 120-150 หลังจากการกรองเฟรมแล้ว

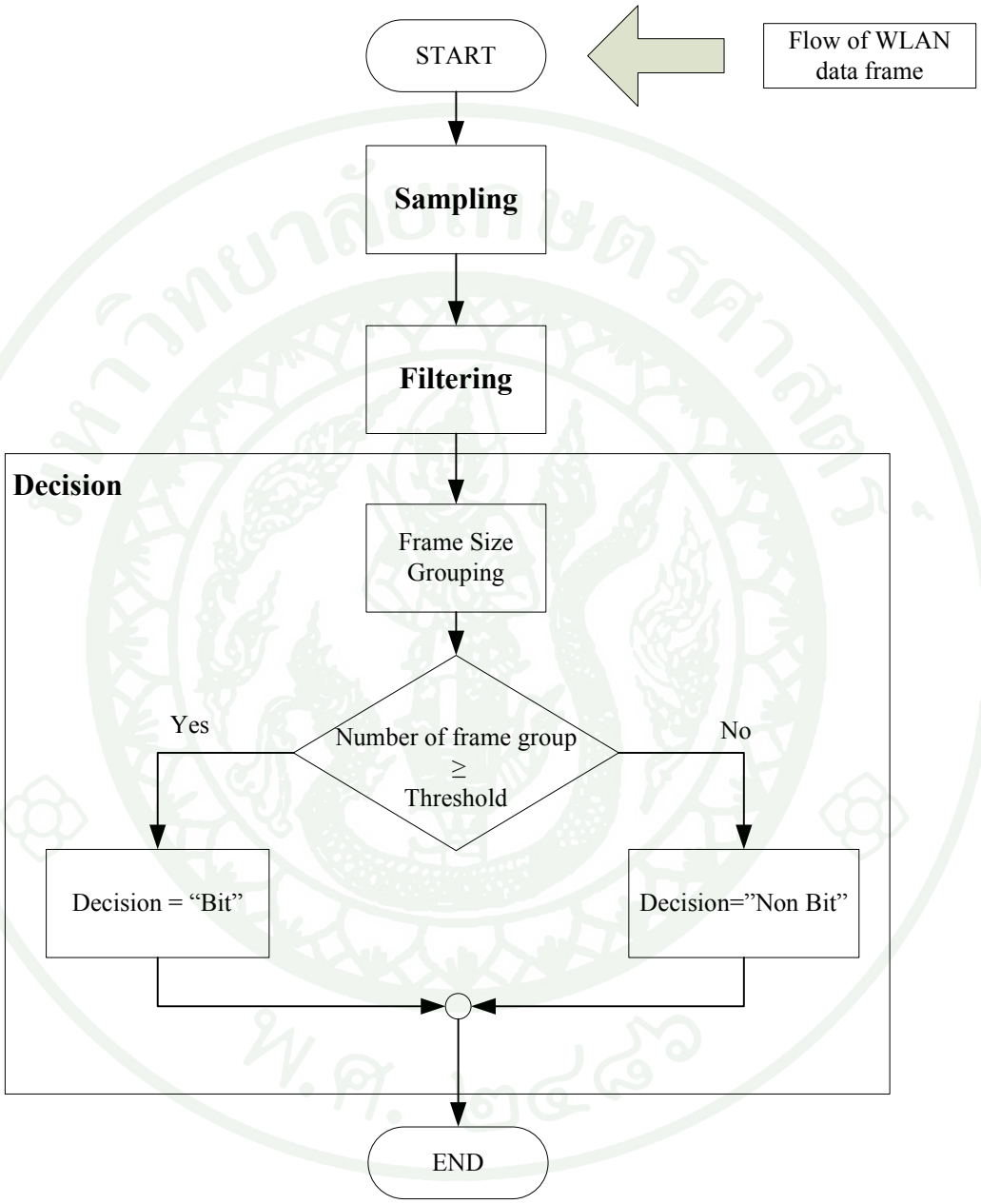
จากภาพที่ 39 เส้นทึบหนาแสดงให้เห็นถึงแนวโน้มการกระจายตัวของข้อมูลที่ไม่มีโพรโทคอลบิตทอร์เรนต์ทำงานอยู่ โดยเป็นการกระจายตัวของการดาวน์โหลดไฟล์ผ่านข้อมูลผสมของโพรโทคอลเอฟทีพีและเอชทีทีพี ซึ่งแตกต่างจากเส้นประที่เป็นผลการทดลองการกระจายตัวของขนาดเฟรมข้อมูลที่มีโพรโทคอลบิตทอร์เรนต์ทำงานอยู่อย่างมีนัยสำคัญ

จากกราฟจะเห็นรอยหยักเป็นขั้นบันไดซึ่งก็คือขนาดของเฟรมข้อมูลที่แตกต่างกัน ซึ่งจะเห็นว่าข้อมูลที่มีส่วนผสมของโพรโทคอลบิตทอร์เรนต์มีปริมาณของขนาดเฟรมข้อมูลมากกว่าข้อมูลที่ไม่มีโพรโทคอลบิตทอร์เรนต์ผสมอยู่ ณ ช่วงเวลาใด ช่วงเวลาหนึ่ง ด้วยวิธีการนับจำนวนขนาดของเฟรมข้อมูลที่พบ ณ ช่วงเวลาใดนี้เอง จึงน่าจะสามารถใช้ในการออกแบบกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์ โดยใช้ข้อมูลที่มีเฉพาะในเครือข่ายไร้สายได้

1.2 ขั้นตอนการออกแบบการทดลองเพื่อทดสอบสมมติฐาน

การออกแบบกลไกการตรวจจับบิตทอร์เรนต์โดยอาศัยการนับจำนวนขนาดเฟรมข้อมูล จะประกอบด้วยขั้นตอน 3 ขั้นตอน ได้แก่ การสุ่มดักจับข้อมูลที่จะนำมาวิเคราะห์ (Sampling)

การกรองเฟรมข้อมูล (Filtering) และการตัดสินการเป็นบิตทอร์เรนต์ของข้อมูล (Decision) ซึ่งแต่ละกระบวนการ แสดงดังภาพที่ 16 และส่วนรายละเอียดการทำงานของกลไก แสดงดังอัลกอริทึม 1



ภาพที่ 40 แผนภูมิแสดงกลไกการตรวจจับบิตทอร์เรนต์

1.2.1 การสุ่มดักจับข้อมูล

การสุ่มดักจับข้อมูลถือเป็นหัวใจสำคัญของกลไกการตรวจจับบิตทอร์เรนต์โดยอาศัยการนับจำนวนขนาดเฟรมข้อมูล ทั้งนี้เนื่องจากข้อมูลที่ได้จากขั้นตอนนี้ถือเป็นข้อมูลนำเข้าของขั้นตอนอื่น หากข้อมูลที่สุ่มจับได้มาไม่ได้แสดงออกถึงลักษณะเฉพาะของพฤติกรรมการมีอยู่ของ

โพรโทคอลบิตทอร์เรนต์อย่างชัดเจน ขั้นตอนอื่น ๆ ที่ใช้ข้อมูลนำเข้านี้ก็จะทำงานผิดพลาดไปด้วย ส่งให้กลไกตรวจจับทำงานอย่างไม่มีประสิทธิภาพ

การที่จะสามารถสุ่มดักจับข้อมูลที่ทำให้กลไกตรวจจับมีประสิทธิภาพที่สูงสุดจำเป็นจะต้องเลือกช่วงเวลาในเริ่มการสุ่มดักจับข้อมูลที่เหมาะสม (Optimal Starting Time) และ ระยะเวลาที่ใช้ในการดักจับข้อมูลที่เหมาะสม (Optimal Time Interval) การออกแบบการทดลองเพื่อหาช่วงเวลาในการเริ่มสุ่มดักจับข้อมูลที่เหมาะสม และค่าระยะเวลาที่ใช้ในการดักจับข้อมูลที่เหมาะสมจะกล่าวไว้ในหัวข้อการออกแบบการทดลองเพื่อวัดประสิทธิภาพของกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์บนเครือข่ายไร้สาย

1.2.2 การกรองขนาดเฟรมข้อมูล

การกรองขนาดเฟรมข้อมูล ถือได้ว่าเป็นขั้นตอนที่สำคัญมากขั้นตอนหนึ่ง การกรองเฟรมข้อมูลที่ถูกต้องจะส่งผลให้การตัดสินข้อมูลว่าเป็นโพรโทคอลบิตทอร์เรนต์หรือไม่นั้น มีความถูกต้องแม่นยำสูง ในทางกลับกัน หากทำการกรองเฟรมข้อมูลที่เกิดจากพฤติกรรมการทำงานของโพรโทคอลบิตทอร์เรนต์ออก และเหลือไว้ที่เฟรมที่ไม่ใช่พฤติกรรมของบิตทอร์เรนต์ ก็จะทำให้ขั้นตอนการตัดสินการเป็นบิตทอร์เรนต์ของข้อมูลทำงานผิดพลาด

เงื่อนไขที่นำมาใช้ในการกรองเฟรมข้อมูลได้มาจากการสังเกตการทดลองสมมติฐานโดยกำหนดให้ขนาดเฟรมที่จำเป็นต้องกรองออก เป็นเฟรมที่มีปริมาณมาก ในช่วงเวลาที่กำหนด แต่ก็มีบางขนาดเฟรมซึ่งสามารถดูรายละเอียดเฟรมจากข้อมูลชั้นขนส่งว่าไม่เข้าข่ายเป็นเฟรมของโพรโทคอลบิตทอร์เรนต์ ได้แก่ เฟรมขนาด 109 ไบต์ ที่มีรายละเอียดเป็น TCP DUP ACK จะเข้าข่ายเฟรมที่ต้องกรอกออกด้วย รายละเอียดของขนาดเฟรมข้อมูลที่ได้ทำการกรองออกมีดังนี้

ตารางที่ 4 รายละเอียดของเฟรมที่ทำการกรองออกในกระบวนการกรองข้อมูล

ขนาดเฟรมข้อมูล (ไบต์)	รายละเอียด
1557	Data 1460 Byte (MAX MTU)
1273	Data 1176 Byte with [PSH,ACK] Flag
109	[TCP DUP ACK]
97	Acknowledgement

1.2.3 การตัดสินการเป็นบิตทอร์เรนต์ของข้อมูล

ขั้นตอนนี้เป็นขั้นตอนที่ให้ผลลัพธ์จากข้อมูลที่ได้มาจากการสุ่มดักจับว่า เป็นพฤติกรรมการมีอยู่ของโพรโทคอลบิตทอร์เรนต์หรือไม่ โดยอาศัยการนับจำนวนของขนาดเฟรมข้อมูลที่หลงเหลือจากขั้นตอนการกรอง หากขนาดเฟรมข้อมูลมีจำนวนมากจนถึงค่าตัดสิน (Threshold) ก็จะให้ผลลัพธ์ว่าชุดข้อมูลที่ได้สุ่มดักจับมานี้มีพฤติกรรมของโพรโทคอลบิตทอร์เรนต์แสดงอยู่ การกำหนดค่าตัดสินที่เหมาะสมจะส่งผลโดยตรงต่อประสิทธิภาพของกลไกการตรวจจับบิตทอร์เรนต์ ซึ่งค่าตัดสินนี้จะใช้เป็นเครื่องมือในการหาค่าช่วงเวลาเริ่มต้นที่เหมาะสมในการดักจับข้อมูลและระยะเวลาการดักจับข้อมูลที่เหมาะสมต่อไป

อัลกอริทึมที่ 1 แสดงการขั้นตอนการทำงานของกลไกตรวจจับโพรโทคอล บิตทอร์เรนต์ เริ่มต้นโดยการเก็บเฟรมข้อมูลจากคู่ที่อยู่แม็คซึ่งเป็นผู้รับปลายทางและผู้ส่งต้นทาง โดยการกำหนดค่า ช่วงระยะเวลาในการเก็บข้อมูลไว้ในตัวแปร opt_ti โดยมีโพรซีเยอร์ Collect_Data() ทำหน้าที่เก็บรวบรวมข้อมูลตามช่วงระยะเวลาที่กำหนด เฟรมข้อมูลแต่ละเฟรมจะถูกเก็บไว้ในตัวแปรอาร์เรย์ Fr[] จากนั้นจะทำการตรวจสอบข้อมูลของประเภทเฟรมว่าเป็นประเภทเฟรมข้อมูลหรือไม่ โดยสามารถอ่านค่าได้จากพารามิเตอร์ frametype หากพบว่าเป็นเฟรมข้อมูลก็จะเรียกใช้ฟังก์ชัน IsFilterSize() เพื่อตรวจสอบขนาดของเฟรมข้อมูลว่าเป็นขนาดที่ต้องกรองออกหรือไม่ หากไม่ใช่ขนาดที่ต้องกรองออกก็จะเรียกใช้ฟังก์ชัน IsDuplicateSize() เพื่อตรวจสอบว่าเป็นขนาดเฟรมที่ยังไม่เคยเก็บมาก่อนหรือไม่ ถ้าพบว่าเป็นขนาดเฟรมใหม่ ก็จะทำกับเพิ่มค่าให้กับตัวแปร count ขึ้นอีก 1 จากนั้นจึงเพิ่มค่าให้ตัวแปร j อีก 1 เพื่อเก็บข้อมูลของเฟรมถัดไปจนกว่าจะครบช่วงระยะเวลาการดักจับข้อมูลโพรซีเยอร์นี้จะทำการคืนค่าของ count ซึ่งเป็นค่าของขนาดเฟรมที่นับได้

ส่วนโพรซีเยอร์ Decision() จะเป็นนำค่า ที่ได้คืนมาจากโพรซีเยอร์ Collect_Data() มาเปรียบเทียบกับค่าของตัวแปร threshold หากค่าที่ได้คืนมาจากโพรซีเยอร์ Collect_Data() มีค่ามากกว่าหรือเท่ากับค่า threshold ก็จะคืนค่า “Bit” แต่ถ้าหากมีค่าน้อยกว่าค่า Threshold ก็จะคืนค่า “Non Bit”

อัลกอริทึมที่ 1 ขั้นตอนการทำงานของกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์

```
Algorithm 1. DetectBitTorrent
1:      procedure Collect_Data(opt_ti)
2:        FrameBank Fr[] , int j=0, int count=0
3:        while i from 0 to opt_ti
4:          Fr[j] ⟵ wlan frame dumped from couple Addr.
5:          if Fr[j].frametype= “data”
6:            if not IsFilterSize(Fr[j].framesize)
7:              if not IsDuplicateSize(Fr[j].framesize)
8:                count++ ,
9:              endif
10:           endif
11:         Endif
12:         j++
13:       end while
14:     return count

15:     procedure Decision(opt_threshold)
16:       opt_ti ⟵ optimal time interval
17:       if Collect_Data(opt_ti) ≥ threshold
18:         return true
19:       else
20:         return  false
```

2. เครื่องมือชี้วัดประสิทธิภาพ

งานวิจัยนี้ใช้เกณฑ์วัดคอนฟิวชั่น (Confusion Matrix) (Fomby, n.d.) เป็นตัววัดประสิทธิภาพ โดยใช้ค่าอัตราความถูกต้อง (AR : Accuracy Rate) ค่าผลบวกแท้ (TP : True Positive) และค่าผลบวกลวง (FP : False Positve) ซึ่งเป็นค่าชี้วัดกลางที่สามารถนำไปเปรียบเทียบกับกลไกการตรวจจับอื่น ๆ ได้ง่ายตามที่ได้มีการแนะนำของ Sagarelli (2007)

รายละเอียดของเกณฑ์วัดคอนฟิวชั่นแสดงได้ดังภาพที่ 41

		Prediction	
		Negative	Positive
Actual	Negative	TN	TP
	Positive	FN	FP

ภาพที่ 41 เกณฑ์วัดคอนฟิวชั่น

เมื่อกำหนดให้

TP คือความสามารถในการตรวจจับโพรโทคอลบิตทอร์เรนต์ที่ถูกต้อง โดยที่เหตุการณ์นั้นมีการทำงานของโพรโทคอลบิตทอร์เรนต์อยู่

FN คือความผิดพลาดของกลไกที่ไม่ตรวจจับโพรโทคอลบิตทอร์เรนต์ ทั้ง ๆ ที่ในเหตุการณ์นั้นมีการทำงานของโพรโทคอลบิตทอร์เรนต์อยู่

FP คือความผิดพลาดของกลไกที่ตรวจจับโพรโทรคอลบิตทอร์เรนต์ ที่ตรวจจับเหตุการณ์ที่ไม่มีการทำงานของโพรโทรคอลของบิตทอร์เรนต์ แต่กลับตรวจพบว่าเป็นโพรโทคอลบิตทอร์เรนต์

TN คือความสามารถในการเพิกเฉยต่อข้อมูลที่ไม่ใช่เป็นโพรโทคอลบิตทอร์เรนต์ในเหตุการณ์ที่ไม่มีโพรโทคอลบิตทอร์เรนต์ทำงานอยู่

AR ใช้ในการวัดความถูกต้องของการตรวจจับของกลไก โดยหาได้จากสมการ (1)

$$AR = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

TPR (True Positive Rate) หรือ รีคอล (Recall) ใช้ในการตรวจสอบความแม่นยำในการตรวจจับของกลไก หาได้จากสมการ (2)

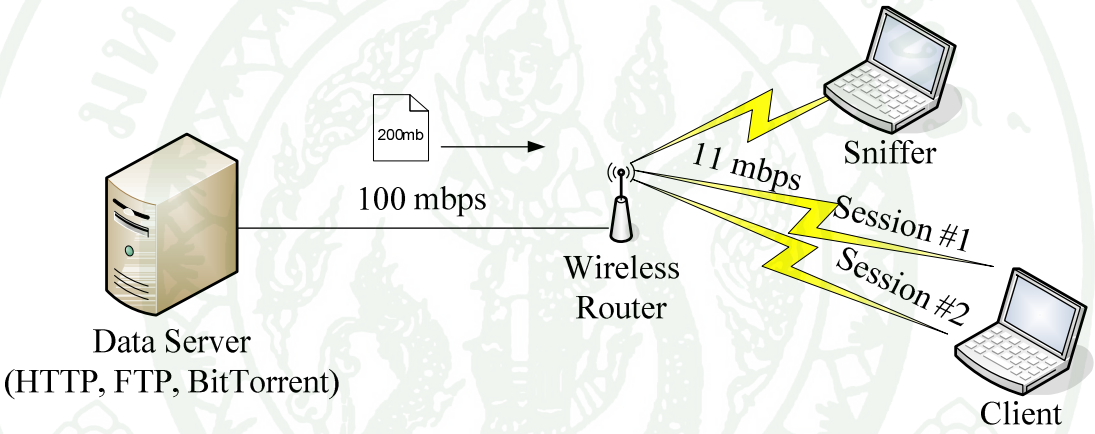
$$TPR = \frac{TP}{TP + FN} \tag{2}$$

FPR (False Positive Rate) แสดงถึงอัตราความผิดพลาดของกลไกที่ตรวจจับข้อมูลที่ไม่เป็นบิตทอร์เรนต์ว่าเป็นบิตทอร์เรนต์ หาได้จากสมการ (3)

$$FPR = \frac{FP}{FP + TN} \tag{3}$$

ผลและวิจารณ์

วิทยานิพนธ์นี้ได้ออกแบบการทดลองเพื่อหาค่าที่เหมาะสมที่นำมาใช้ในกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์ที่ออกแบบสำหรับสภาพแวดล้อมบนเครือข่ายไร้สายที่ทำให้กลไกมีประสิทธิภาพการตรวจจับสูงสุด โดยชุดข้อมูลที่ใช้ในการทดลองเป็นชุดข้อมูลที่สร้างขึ้นเอง และทำการทดลองภายใต้สภาพแวดล้อมควบคุม ซึ่งค่าตัวแปรที่ต้องการหาได้แก่ ค่าช่วงเวลาเริ่มต้นของการสุ่มดักจับข้อมูล และค่าระยะเวลาการสุ่มดักจับข้อมูล โดยผลการทดลองจะแบ่งเป็นสามส่วน ได้แก่ การทดลองหาค่าช่วงเวลาเริ่มดักจับข้อมูลที่เหมาะสม การทดลองหาค่าระยะเวลาการดักจับข้อมูลที่เหมาะสม และการทดลองประสิทธิภาพของกลไกในสภาพแวดล้อมการใช้งานปกติ



ภาพที่ 42 สภาพแวดล้อมในการทดลองกรณีมีการดาวน์โหลด 2 วาระ

การทดลองที่ใช้ในการหาค่าช่วงเวลาเริ่มต้นของการดักจับข้อมูล และการหาค่าระยะเวลาในการสุ่มดักจับข้อมูลที่เหมาะสม กำหนดให้ใช้รูปแบบการทดลองในลักษณะเดียวกับการทดลองเพื่อทดสอบสมมติฐานในกรณีที่เครื่องลูกข่ายทำการดาวน์โหลดข้อมูลผ่านโพรโทคอลมากกว่า 1 วาระ หากแต่เพิ่มการทดลองดาวน์โหลดข้อมูลให้หลากหลายขึ้น ชุดข้อมูลที่นำมาใช้ในการทดลองเป็นชุดทดลองที่สร้างเอง โดยได้มาจากการจัดหมู่ (Combination) ของโพรโทคอลทั้ง 3 ชนิด ชนิดละ 2 วาระ ซึ่งเมื่อทำการจัดหมู่ จะได้เป็นเหตุการณ์ทดลอง (Scenario) ที่จะนำมาใช้ทำการทดลอง 26 กรณี แบ่งเป็นกรณีที่มีการดาวน์โหลดโพรโทคอลชนิดเดียวกัน 6 กรณี (3 กรณีเป็นการทดลองดาวน์โหลดข้อมูล 1 วาระ และ อีก 3 กรณี เป็นการดาวน์โหลดข้อมูล 2 วาระ) การดาวน์โหลดโดยการผสม 2 โพรโทคอล 12 กรณี และ การดาวน์โหลดที่เป็นการผสมกัน 3 โพรโทคอล 8 กรณี รายละเอียดของเหตุการณ์ทดลองที่ใช้ทดลอง แสดงดังตารางที่ 5

ตารางที่ 5 ชุดข้อมูลที่ใช้เป็นเหตุการณ์ทดลอง

ลำดับที่	เหตุการณ์ทดลอง
1	HTTP Only
2	FTP Only
3	BitTorrent Only
4	FTP+HTTP
5	FTP+BitTorrent
6	HTTP+BitTorrent
7	FTP+HTTP+BitTorrent
8	HTTP1+HTTP2
9	FTP1+FTP2
10	BitTorrent1+BitTorrent2
11	HTTP1+HTTP2+BitTorrent
12	HTTP1+HTTP2+FTP
13	HTTP1+HTTP2+FTP+BitTorrent
14	FTP1+FTP2+HTTP
15	FTP1+FTP2+BitTorrent
16	FTP1+FTP2+HTTP+BitTorrent
17	BitTorrent1+BitTorrent2+FTP
18	BitTorrent1+BitTorrent2+HTTP
19	BitTorrent1+BitTorrent2+HTTP+FTP
20	FTP1+FTP2+HTTP1+HTTP2
21	BitTorrent1+BitTorrent2+HTTP1+HTTP2
22	BitTorrent1+BitTorrent2+FTP1+FTP2
23	BitTorrent1+BitTorrent2+HTTP1+HTTP2+FTP
24	BitTorrent1+BitTorrent2+FTP1+FTP2+HTTP
25	FTP1+FTP2+HTTP1+HTTP2+BitTorrent
26	BitTorrent1+BitTorrent2+FTP1+FTP2+HTTP1+HTTP2

ในเหตุการณ์ทดลองที่มีโพรโทคอลดาวน์โหลดข้อมูลมากกว่า 1 ชนิด จะกำหนดให้แต่ละโพรโทคอลเริ่มต้นดาวน์โหลดในเวลาที่ใกล้เคียงกันมากที่สุด และเครื่องดักจับข้อมูลจะหยุดดักจับข้อมูลต่อเมื่อได้เสร็จสิ้นการดาวน์โหลดไฟล์ของทุกโพรโทคอลแล้ว

ทุกเหตุการณ์ทดลองจะถูกนำมาแยกกลุ่มเป็นสองกลุ่ม ได้แก่กลุ่มเหตุการณ์ที่มีการใช้งานโพรโทคอลบิตทอร์เรนต์ (BitTorrent Host) เพื่อใช้สำหรับการวัดค่าผลบวกแท้ และผลลบลวง ส่วนอีกกลุ่มหนึ่งเป็นกลุ่มเหตุการณ์ที่ไม่มีการใช้งานโพรโทคอลบิตทอร์เรนต์ (Non-BitTorrent Host) เพื่อใช้สำหรับการวัดค่าผลลบแท้ และผลบวกลวง ซึ่งแต่ละเหตุการณ์สามารถแบ่งกลุ่มได้ดังตารางที่ 6

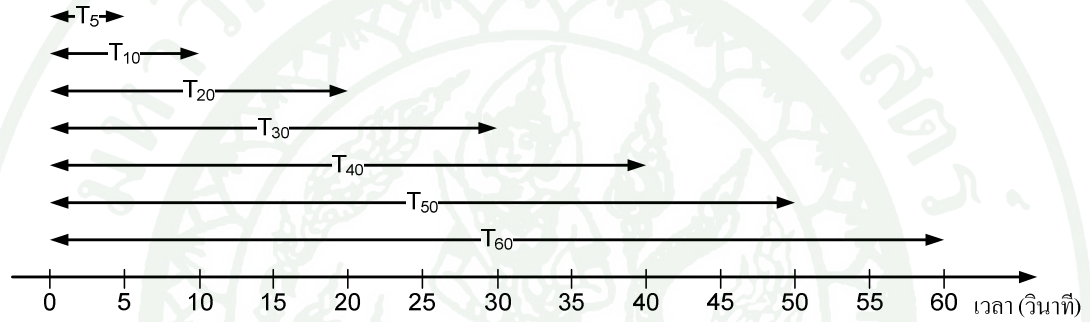
ตารางที่ 6 เหตุการณ์ทดลองแยกตามกลุ่มเหตุการณ์ที่ใช้ทดลองในสภาพแวดล้อมควบคุม

BitTorrent Host	Non-BitTorrent Host
BitTorrent Only	HTTP Only
FTP+BitTorrent	FTP Only
HTTP+BitTorrent	FTP+HTTP
FTP+HTTP+BitTorrent	HTTP1+HTTP2
BitTorrent1+BitTorrent2	FTP1+FTP2
HTTP1+HTTP2+BitTorrent	HTTP1+HTTP2+FTP
HTTP1+HTTP2+FTP+BitTorrent	FTP1+FTP2+HTTP
FTP1+FTP2+BitTorrent	FTP1+FTP2+HTTP1+HTTP2
FTP1+FTP2+HTTP+BitTorrent	
BitTorrent1+BitTorrent2+HTTP	
BitTorrent1+BitTorrent2+FTP	
BitTorrent1+BitTorrent2+HTTP+FTP	
BitTorrent1+BitTorrent2+HTTP1+HTTP2	
BitTorrent1+BitTorrent2+FTP1+FTP2	
BitTorrent1+BitTorrent2+HTTP1+HTTP2+FTP	
BitTorrent1+BitTorrent2+FTP1+FTP2+HTTP	
FTP1+FTP2+HTTP1+HTTP2+BitTorrent	
BitTorrent1+BitTorrent2+FTP1+FTP2+HTTP1+HTTP2	

ตารางที่ 7 สัดส่วนเหตุการณ์การทดลองที่ใช้ในสภาพแวดล้อมควบคุม

เหตุการณ์	จำนวน	%
เหตุการณ์ทั้งหมด	26	100
เหตุการณ์ที่มีบิตทอร์เรนต์	18	69.23
เหตุการณ์ที่ไม่มีบิตทอร์เรนต์	8	30.77

1. การทดลองหาค่าช่วงเวลาเริ่มดักจับข้อมูลที่เหมาะสม (The suitable sampling starting time)



ภาพที่ 43 ระยะเวลาการตรวจจับที่น่าสนใจที่ใช้ในการทดลอง

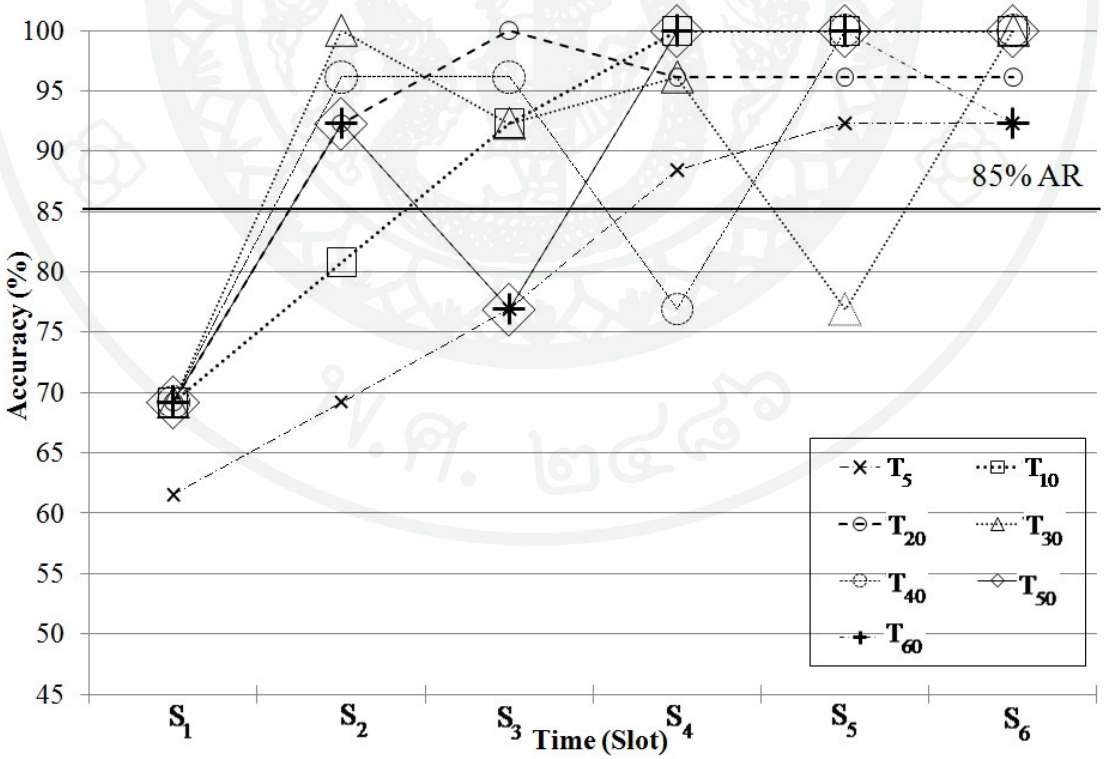
ในส่วนนี้ได้ทำการวัดประสิทธิภาพของกลไกที่ขึ้นอยู่กับ ค่าช่วงเวลาการเริ่มดักจับข้อมูล (S_t) และ ค่าระยะเวลาในการดักจับข้อมูล (T_i) โดย S_t ได้มาจากการแบ่งข้อมูลที่ได้มาจากการตรวจจับเป็น 6 ช่วง โดยสนใจระยะเวลาการตรวจจับ T_i สำหรับ i = 5, 10, 20, 30, 40, 50, และ 60 ตามลำดับ ดังแสดงในภาพที่ 43 โดยใช้การปรับค่าตัดสิน (threshold) เป็นเครื่องมือช่วยในการหาค่าที่เหมาะสม ในที่นี้คือได้ค่า AR สูงถึงค่าคาดหวัง โดยกำหนดให้ค่าคาดหวังอยู่ที่ 85% ผลการทดลองแสดงให้เห็นได้ดังนี้

ภาพที่ 44 เมื่อกำหนดให้ค่าคาดหวัง AR อยู่ที่ 85% ในกราฟ ค่า AR ของ 6 ช่วงเวลาแรกเมื่อกำหนดให้ ค่าตัดสินที่ 1 พบว่า สำหรับระยะเวลา T_5 ช่วง S_1 ได้ค่า AR = 61% แล้วก็มีแนวโน้มเพิ่มขึ้นเรื่อย ๆ จนถึงจุดอิ่มตัวที่ AR = 92% หลังจากนั้นระยะเวลาที่เหลือจะได้ค่า AR ที่ช่วง S_1 เท่ากับ 69% เท่ากันหมดทุกระยะ วิเคราะห์ได้ว่าที่เป็นเช่นนี้เนื่องมาจากในช่วง S_1 เป็นช่วงที่กำลังเริ่มต้นเตรียมการส่งข้อมูล (Initialize Time) ซึ่งจะพบการส่งข้อมูลเพื่อติดต่อประสานงานในแต่ละโพรโทคอล จึงก่อให้เกิดขนาดแพ็กเกตในปริมาณมากในช่วงเริ่มต้นนี้ ประกอบกับการใช้ค่าของค่าตัดสินที่ 1 มีความอ่อนไหวมาก คือเมื่อได้รับข้อมูลประเภทใดมาก็ตาม เพียง 1 แพ็กเกตก็สามารถทำให้กลไกตรวจจับว่าเป็นบิตทอร์เรนต์ ที่เป็นผลให้เกิดผลบวกลวงเป็นจำนวนมาก ค่า AR ของ T_{10}

จะมีแนวโน้มเพิ่มขึ้นเรื่อย ๆ และถึงจุดอิ่มตัวที่ 100% ตั้งแต่ช่วง S_4 เป็นต้นไป ที่ T_{20} ช่วง S_2-S_3 จะมีค่า AR สูงถึง 95% และจะตกลงมาเหลือประมาณ 75% ที่ช่วง S_4 จากนั้นก็มีค่า AR สูงขึ้น ถึง 100% ที่ S_5 เป็นต้นไปและอิ่มตัวอยู่ที่จุดนั้นไปจนถึง S_6

T_{30} หลังจากพ้น S_1 ก็จะมีค่า AR สูงถึง 100% ที่ S_2 จากนั้นค่า AR จะแกว่งขึ้นลงที่มากกว่า 90% จนมาตกเหลือ 75% ที่ S_4 และจะกลับไปขึ้นสูงถึง 100% ที่ S_5 เมื่อพิจารณาที่ T_{40} พบว่าหลังจากผ่าน S_1 ไปแล้ว ค่า AR ก็เพิ่มขึ้นจนถึง 100% ที่ S_3 และลดลงจนอิ่มตัวที่ประมาณ 96% ที่ S_4 เป็นต้นไป ในส่วนของ T_{50} เมื่อพ้น S_1 มาแล้ว ค่า AR จะแกว่งขึ้นลงอย่างแรง จาก 93% ที่ S_2 มาอยู่ที่ 77% ที่ S_3 แล้วถึงขึ้นไปอิ่มตัวที่ 100% ที่ S_4 ต่อไปจนถึง S_6 และ T_{60} จะได้ค่า AR เหมือนกับ T_5 ตั้งแต่ S_1-S_5 และตกลงมาเหลือ 92% ที่ S_6

เมื่อกำหนดค่าช่วงเวลาเริ่มต้นที่เหมาะสมคือช่วงที่ระยะเวลาทุกค่ามีค่า AR มากกว่าค่าคาดหวัง สำหรับ ค่าตัดสินที่ 1 นี้ช่วงเวลาที่เหมาะสมที่สุดได้แก่ ช่วง S_6 และช่วงที่ไม่เหมาะสมที่สุดได้แก่ S_1

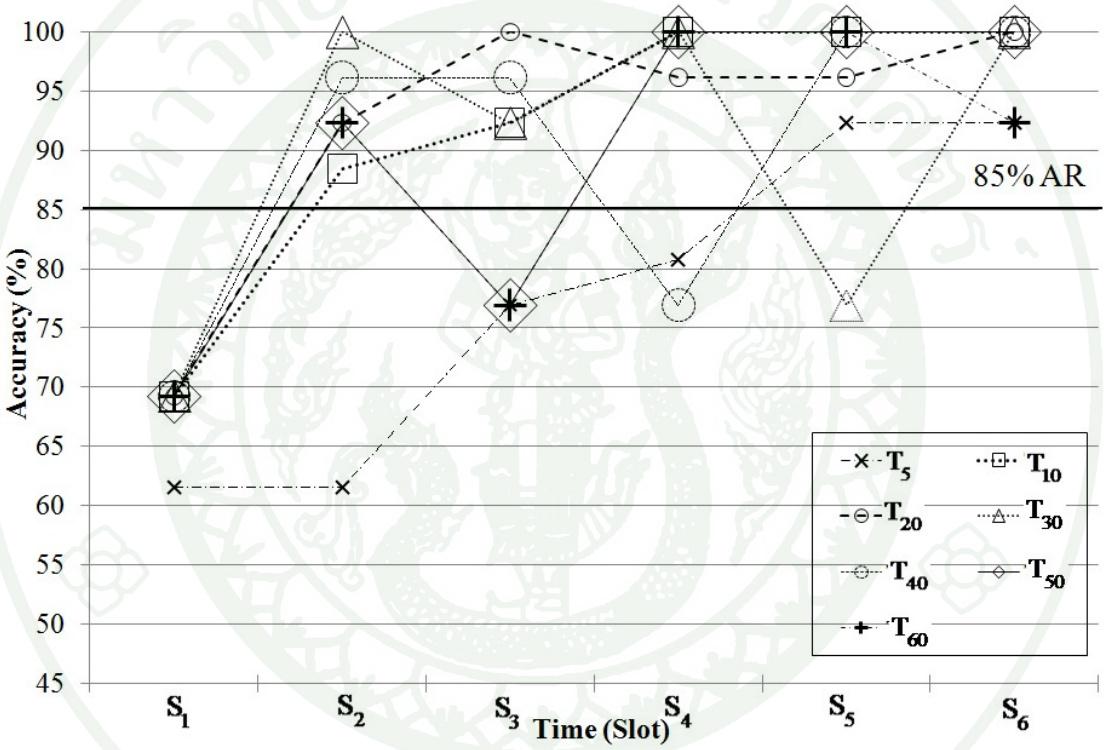


ภาพที่ 44 AR ของช่วงเวลาเริ่มส่งข้อมูลค่าต่าง ๆ ที่ ค่าตัดสินที่ 1

ภาพที่ 45 เป็นผลของการทดลองที่ใช้ค่าของ ค่าตัดสินที่ 2 ซึ่งพบว่า ค่า T_5 ยังคงมีลักษณะคล้ายผลการทดลองที่ใช้ค่าตัดสินที่ 1 คือที่ T_5 มีค่า AR 61% จากนั้นค่าก็จะสูงขึ้นเรื่อย ๆ จนอิ่มตัวที่

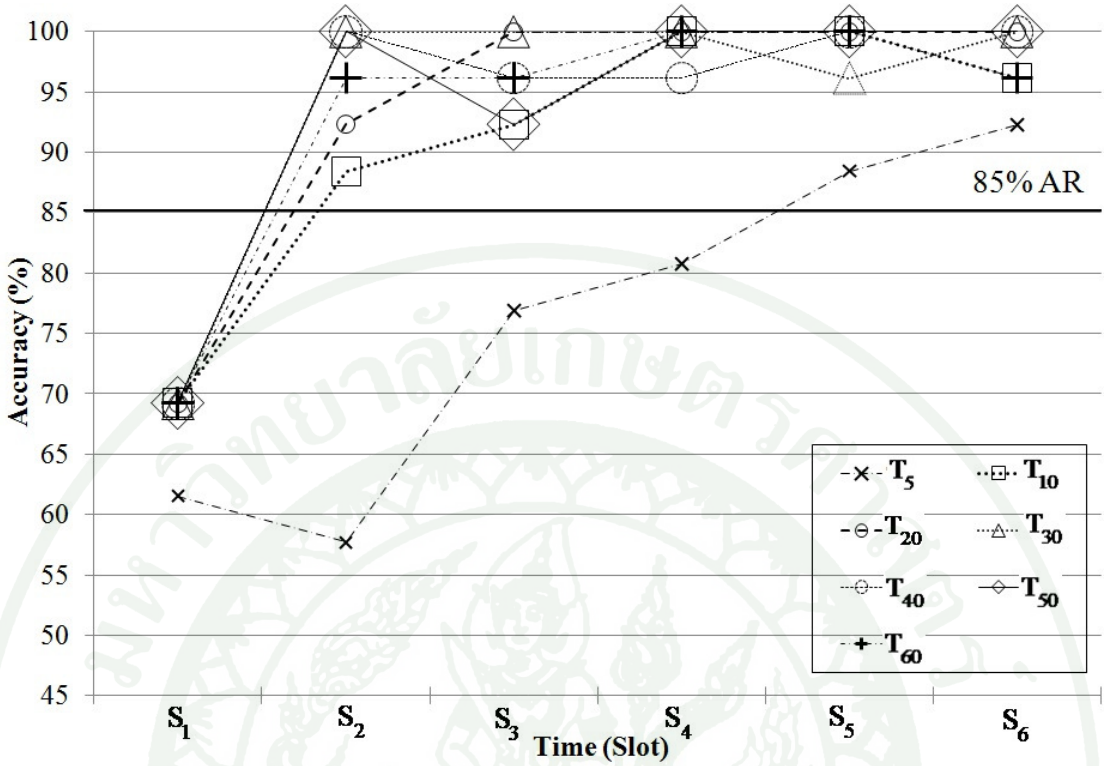
91% หากพิจารณาระยะเวลาอื่น ๆ ก็จะพบว่าที่ S_1 ยังคงมีค่า AR ต่ำกว่าค่าคาดหวังเช่นเดิม แต่พอถึงช่วง S_2 กลับพบว่า ค่า AR ของแต่ละระยะเวลาสูงกว่าค่าคาดหวังทุกตัวโดยมีค่าตั้งแต่ 88-100%

เมื่อพิจารณาช่วง S_3 พบว่าค่าระยะเวลาส่วนใหญ่ ไม่นับรวม T_5 ที่กล่าวไปก่อนหน้านี้แล้ว มีค่า AR สูงถึงค่าคาดหวังนอกจาก T_{50} และ T_{60} จากนั้น ช่วงเวลาถัดไปจะมีแนวโน้มของระยะเวลาที่มีค่า AR ไม่ถึงค่าคาดหวังน้อยลง จนทุกระยะเวลามีค่า AR สูงถึงค่าคาดหวังหมดที่ S_6 ซึ่งเป็นค่าที่เหมาะสมที่สุดเมื่อใช้ค่าตัดสินที่ 2

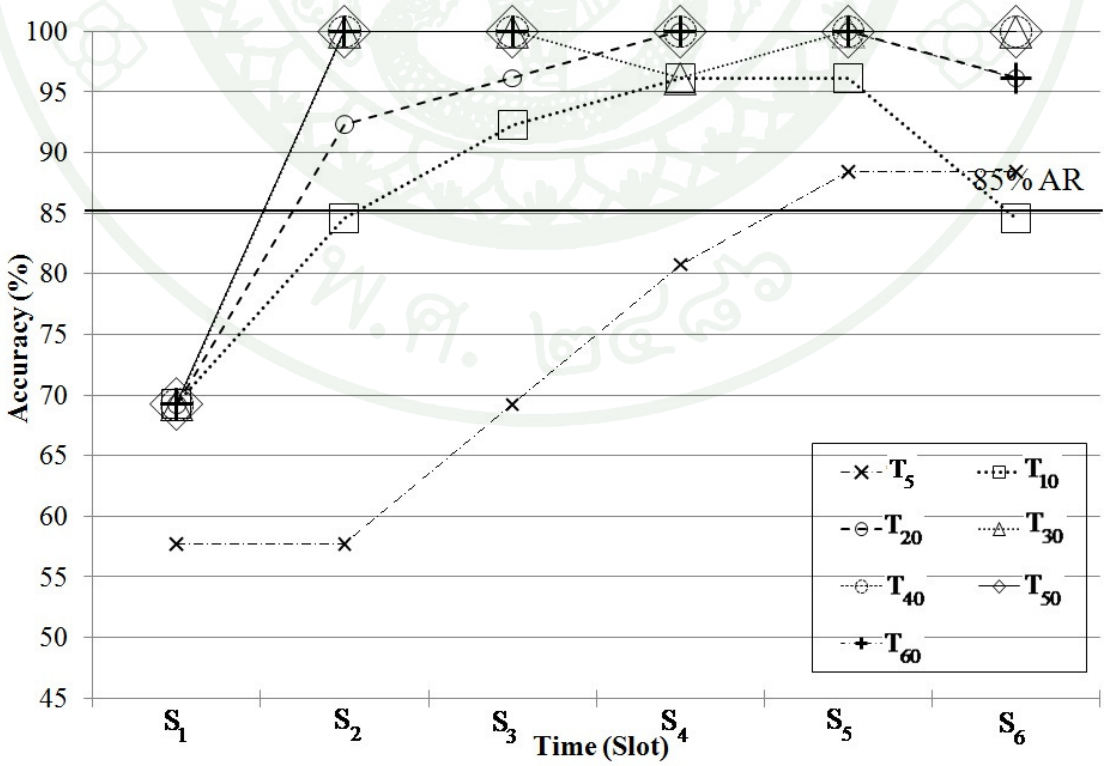


ภาพที่ 45 AR ของช่วงเวลาเริ่มส่งข้อมูลค่าต่าง ๆ เมื่อใช้ค่าตัดสินที่ 2

ในส่วนของการใช้ค่าตัดสินที่ 3 ยังพบว่าที่ช่วง S_1 ยังให้ค่า AR ต่ำกว่าค่าคาดหวังในทุกระยะเวลา เช่นกันกับ T_5 ที่ ได้ค่า AR ต่ำในช่วงแรก ๆ และมีแนวโน้มเพิ่มขึ้นเรื่อย ๆ ที่น่าสนใจคือทุกระยะเวลานอกจาก T_5 แล้วจะมีค่า AR พ้นค่าคาดหวังตั้งแต่ S_2 เป็นต้นไป ดังปรากฏให้เห็นได้ในภาพที่ 46 ซึ่งมีลักษณะเดียวกันกับกรณีทดลองใช้ค่าตัดสินที่ 4 ในภาพที่ 47

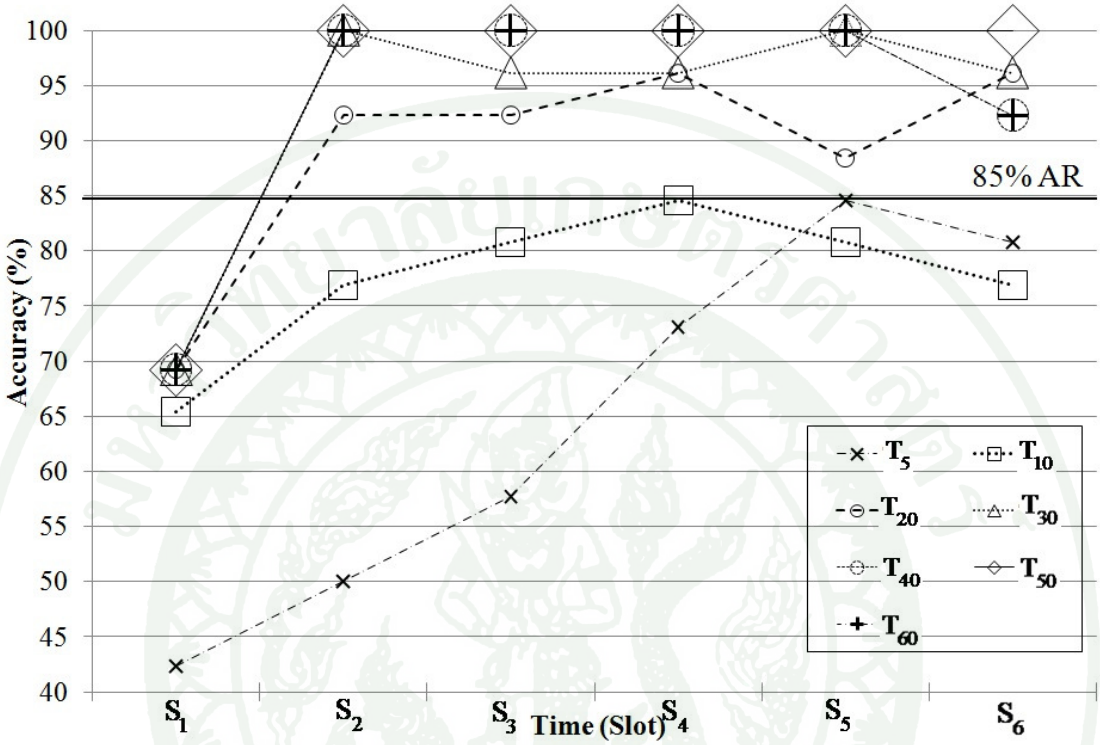


ภาพที่ 46 AR ของช่วงเวลาเริ่มส่งข้อมูลค่าต่าง ๆ เมื่อใช้ค่าตัดสินที่ 3



ภาพที่ 47 AR ของช่วงเวลาเริ่มส่งข้อมูลค่าต่าง ๆ เมื่อใช้ค่าตัดสินที่ 4

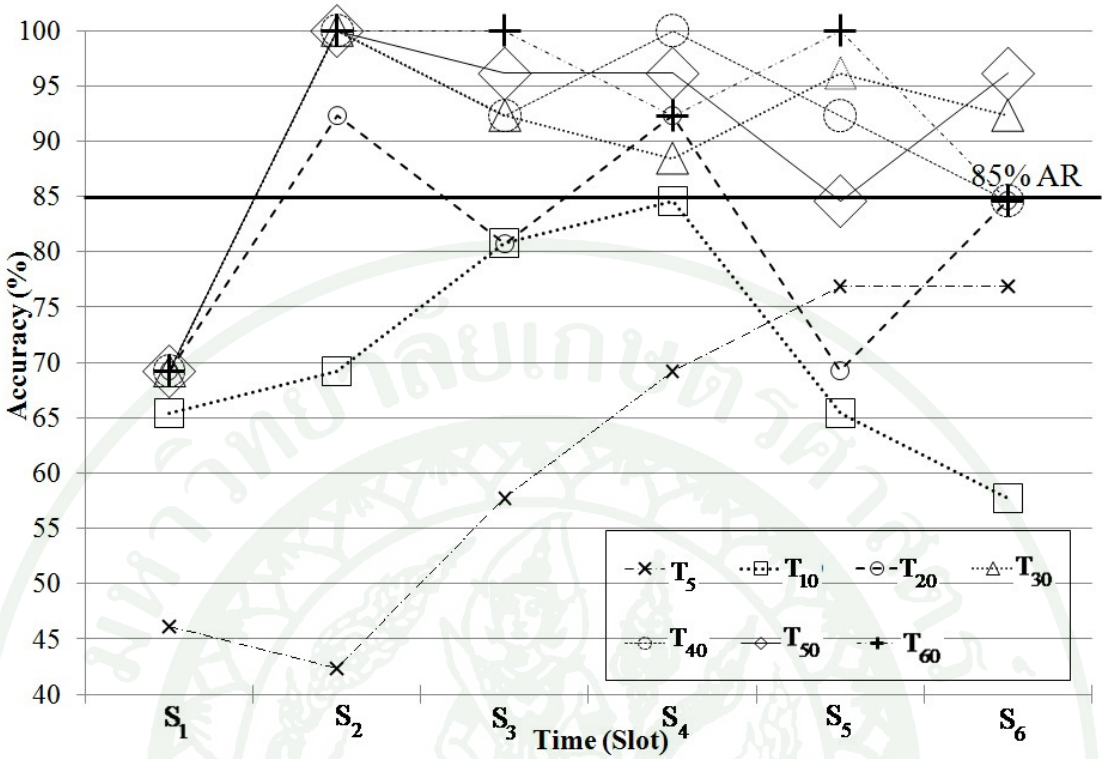
ภาพที่ 48 เป็นกราฟเมื่อใช้ค่าตัดสินที่ 5 ซึ่งมีลักษณะคล้ายกับกรณีใช้ ค่าตัดสินที่ 3 และ ค่าตัดสินที่ 4 แต่ต่างกันในส่วนของระยะเวลา T_{10} ที่ไม่มีช่วงเวลาใดให้ค่า AR ถึงค่าคาดหวังได้เลย



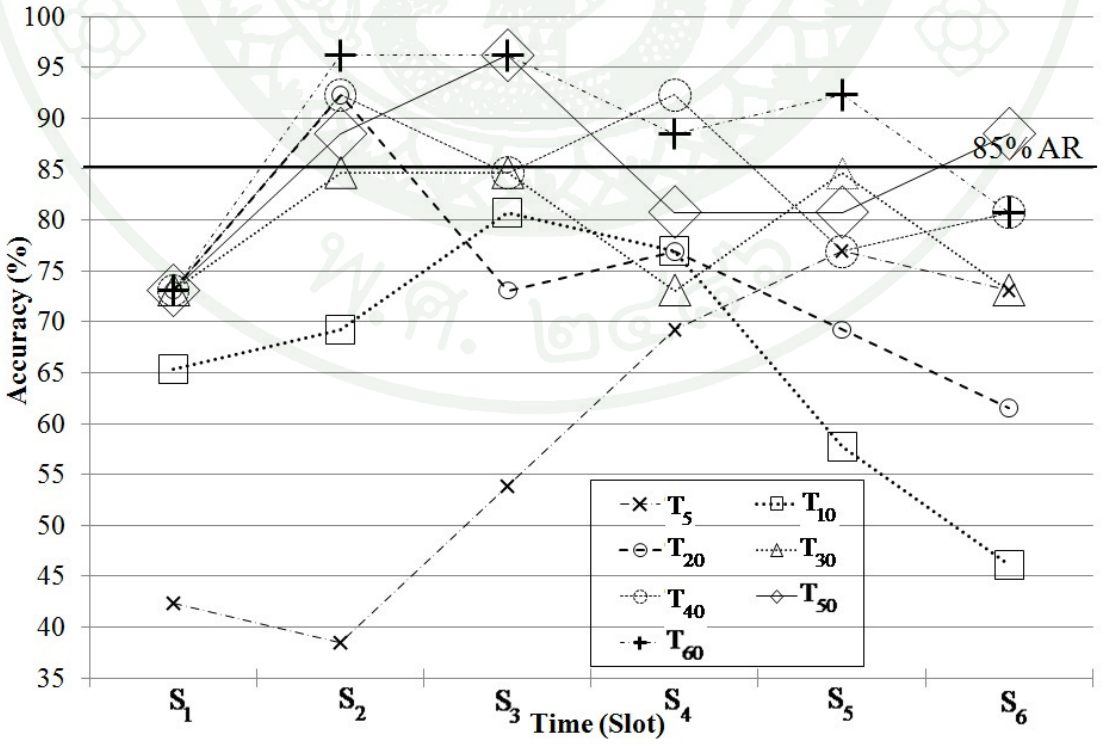
ภาพที่ 48 AR ของช่วงเวลาเริ่มส่งข้อมูลค่าต่าง ๆ ที่ ค่าตัดสินที่ 5

เมื่อใช้ค่าตัดสินที่ 6 เป็นต้นไป ถึง ค่าตัดสินที่ 10 ที่แสดงดังภาพที่ 49-53 ตามลำดับ พบว่าระยะเวลาที่มีค่า AR สูงถึงค่าคาดหวังมีแนวโน้มลดลงอย่างเห็นได้ชัด ซึ่งเป็นที่เข้าใจได้ว่า เกิดจากในแต่ละระยะเวลา ขนาดเฟรมที่หลงเหลือจากกระบวนการกรองเฟรมมีปริมาณน้อยกว่าค่าตัดสิน ทำให้คำตอบของกลไกตรวจจับที่มีลักษณะเป็นผลลบลวง คือมีโพรโทคอลบิตทอร์เรนต์ทำงานอยู่ในระยะเวลาที่สุ่มดักจับข้อมูลออกมา แต่ปรากฏว่าขนาดเฟรมที่เกิดจากโพรโทคอลบิตทอร์เรนต์มีปริมาณน้อยกว่าค่าตัดสิน ทำให้กลไกการตรวจจับตัดสินว่าไม่มีโพรโทคอลบิตทอร์เรนต์ทำงานอยู่นั่นเอง

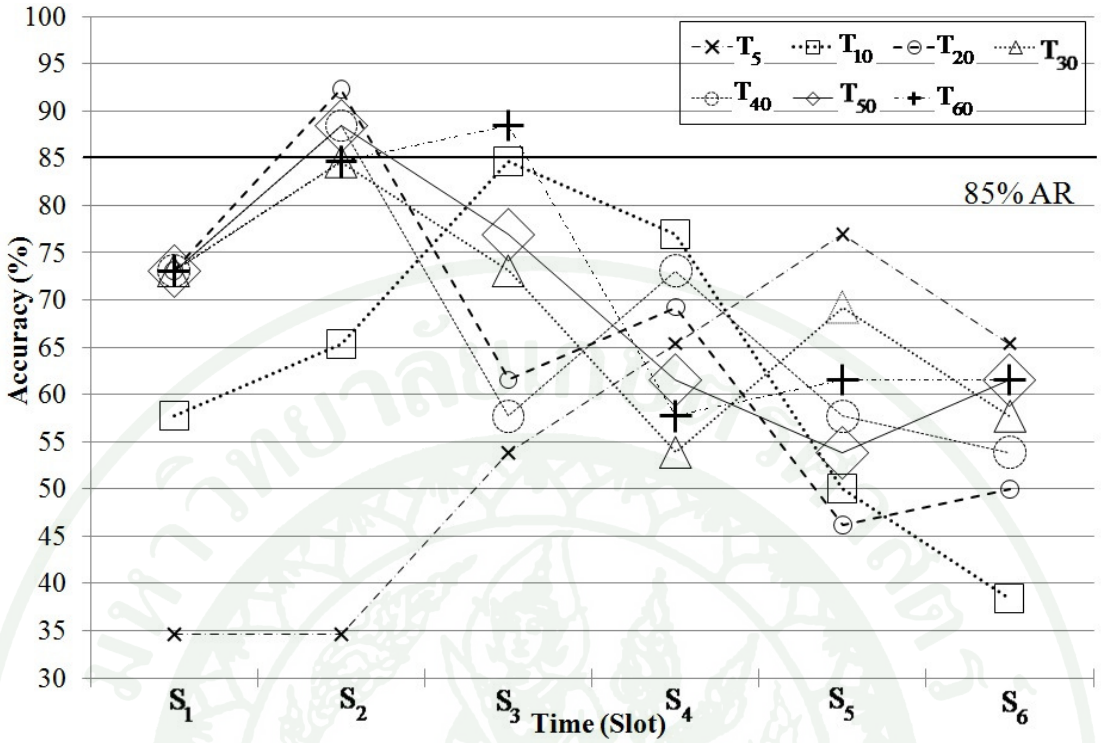
ในส่วนของระยะเวลา T_5 ที่มีแนวโน้มเป็นลักษณะเดียวกันทุก ๆ ค่าตัดสินนั้นสันนิษฐานว่าเป็นผลมาจากระยะเวลาในการดักจับข้อมูลเพียง 5 วินาทีน้อยเกินไป กลไกยังไม่สามารถรวบรวมข้อมูลได้เพียงพอ จึงส่งผลทำให้ความถูกต้องในการตัดสินมีน้อย



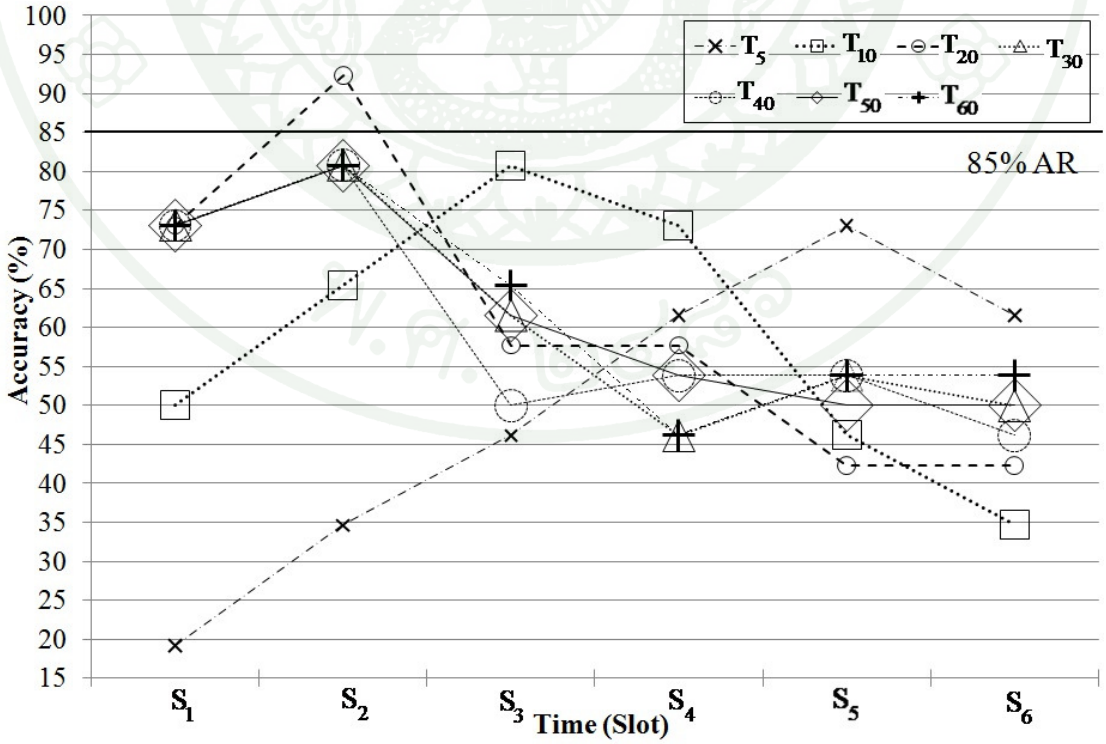
ภาพที่ 49 AR ของช่วงเวลาเริ่มส่งข้อมูลค่าต่าง ๆ ที่ ค่าตัดสินที่ 6



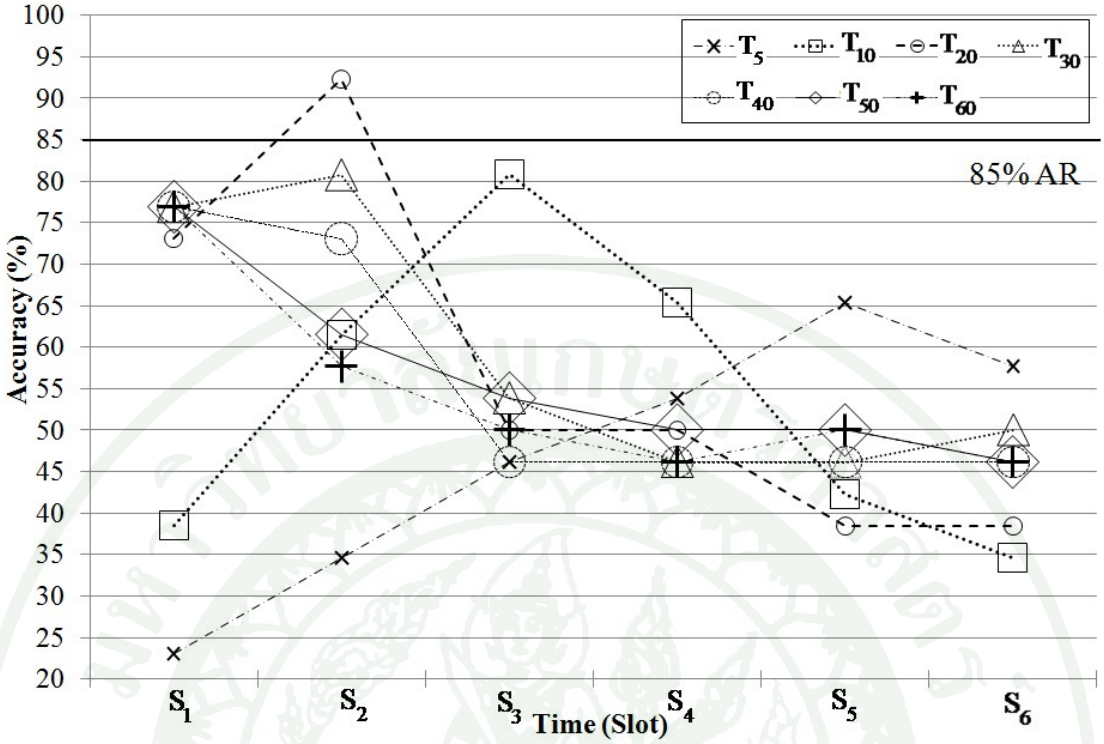
ภาพที่ 50 AR ของช่วงเวลาเริ่มส่งข้อมูลค่าต่าง ๆ ที่ ค่าตัดสินที่ 7



ภาพที่ 51 AR ของช่วงเวลาเริ่มส่งข้อมูลค่าต่าง ๆ ที่ ค่าตัดสินที่ 8



ภาพที่ 52 AR ของช่วงเวลาเริ่มส่งข้อมูลค่าต่าง ๆ ที่ ค่าตัดสินที่ 9



ภาพที่ 53 AR ของช่วงเวลาเริ่มส่งข้อมูลค่าต่าง ๆ ที่ ค่าตัดสินที่ 10

สรุปผลการทดลองในการทดลองนี้ จากการปรับค่าตัดสินพบว่าความถูกต้องของกลไกจะเปลี่ยนแปลงไป หากกำหนดให้ค่าคาดหวัง AR อยู่ที่ 85% เมื่อใช้ ค่าตัดสินที่ 1 และ 2 จะสรุปได้ว่าค่าช่วงเวลาที่เหมาะสมในการเริ่มดักจับข้อมูลคือช่วงเวลา S_6 และ เมื่อใช้ค่าตัดสินตั้งแต่ 3 ถึง 5 ค่าช่วงเวลาเริ่มต้นที่เหมาะสมคือตั้งแต่ช่วง S_2 เป็นต้นไป ในส่วนค่าตัดสินตั้งแต่ 6 เป็นต้นไป ไม่มีช่วงเวลาการเริ่มดักจับข้อมูลที่เหมาะสม และในช่วงเวลา S_1 ไม่เหมาะสมในการดักจับข้อมูลเป็นอย่างยิ่ง

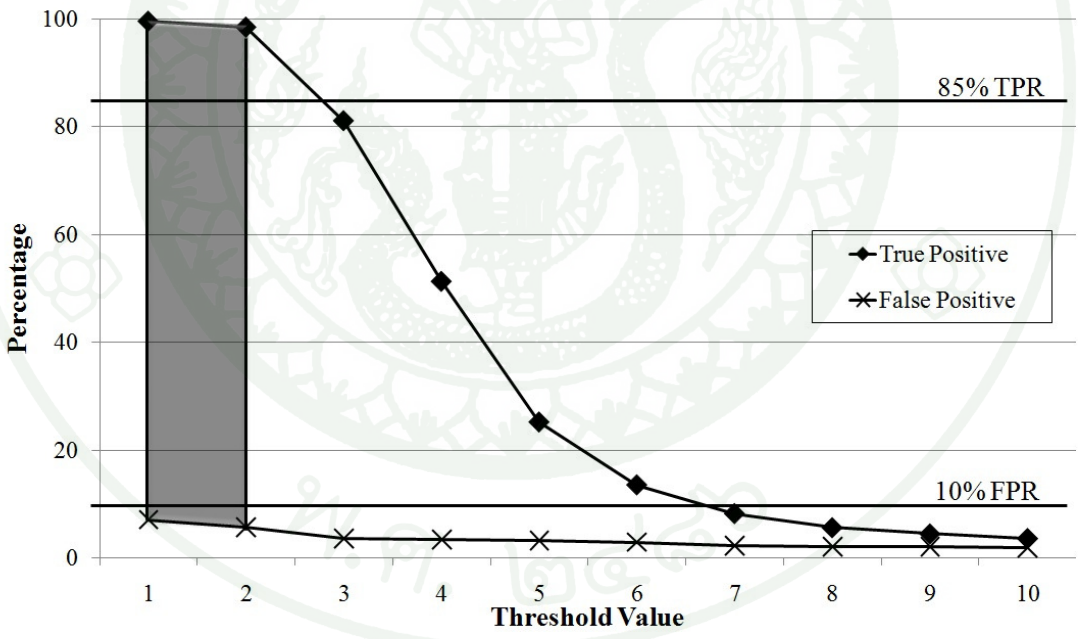
จากผลการทดลองสรุปได้ว่าค่าตัดสินที่ควรใช้งานคือค่า 3 และ 4 โดยกำหนดระยะเวลาที่เหมาะสมคือ T_{10} ถึง T_{60} เมื่อใช้ช่วงเวลาเริ่มต้นตรวจสอบตั้งแต่ S_2 ขึ้นไป และค่าตัดสินที่ 5 เมื่อกำหนดให้ระยะเวลาที่เหมาะสมตั้งแต่ T_{20} ถึง T_{60} เมื่อใช้ช่วงเวลาเริ่มต้นตรวจสอบข้อมูลตั้งแต่ช่วงเวลา S_2 เป็นต้นไป

2. การทดลองหาค่าระยะเวลาดักจับข้อมูลที่เหมาะสม (The suitable sampling interval time)

การทดลองนี้ใช้ข้อมูลจากสภาพแวดล้อมควบคุมชุดเดียวกันกับการทดลองหาช่วงเวลาเริ่มต้นที่เหมาะสมในการดักจับข้อมูล เนื่องจากระยะเวลาการดักจับข้อมูลมีผลต่อการตัดสินใจของ

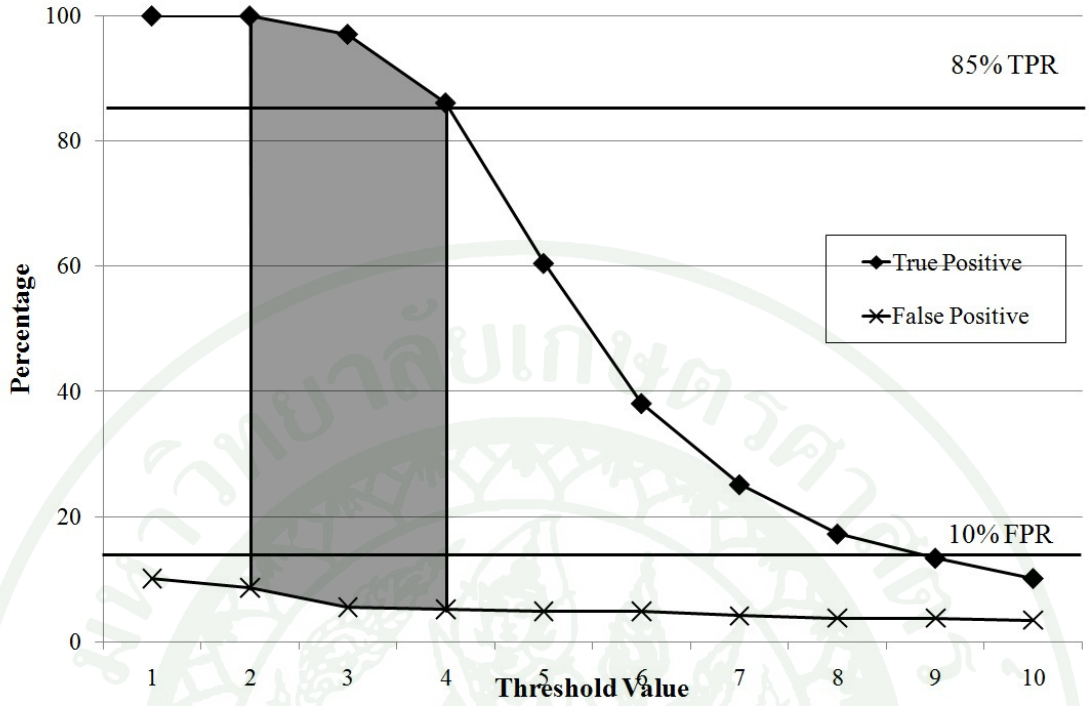
กลไกการตรวจจับที่ออกแบบเพื่อใช้สำหรับสภาพแวดล้อมเครือข่ายไร้สายอย่างมาก การกำหนดระยะเวลาในการดักจับข้อมูลสั้นเกินไป จะส่งผลให้การเก็บรวบรวมข้อมูลทำได้น้อยและทำให้ข้อมูลที่เก็บได้น้อยกว่าค่าตัดสินอยู่เสมอ ซึ่งจะเป็นผลให้ปริมาณของผลลบลวงสูงขึ้นมาก แต่อีกนัยหนึ่ง หากกำหนดให้ระยะเวลาการดักจับข้อมูลยาวนานจนเกินไป ก็จะทำให้ความรวดเร็วของกลไกการตรวจสอบโพรโทคอลบิตทอร์เรนต์ลดลง ซ้ำยังอาจทำให้ผลบวกลวงเพิ่มขึ้น

วัตถุประสงค์ของการทดลองนี้มุ่งหวังจะหาระยะเวลาในการดักจับข้อมูลที่เหมาะสมของกลไกที่นำเสนอ ที่ให้ค่าผลบวกแท้สูง คือเมื่อตรวจจับโพรโทคอลที่เป็นบิตทอร์เรนต์ก็สามารถตัดสินได้ถูกต้องว่า โพรโทคอลที่กำลังตรวจจับอยู่นี้เป็นบิตทอร์เรนต์ และให้ค่าผลบวกลวงต่ำ คือเกิดการตัดสินว่าพบบิตทอร์เรนต์ทั้ง ๆ ที่ข้อมูลที่กำลังตรวจสอบอยู่ไม่ใช่โพรโทคอลบิตทอร์เรนต์ การหาระยะเวลาดักจับข้อมูลที่เหมาะสม โดยใช้การปรับค่าตัดสิน เมื่อกำหนดให้ค่าคาดหวังคือ TPR มากกว่าหรือเท่ากับ 85% และ FPR น้อยกว่าหรือเท่ากับ 10% ได้ผลการทดลองดังนี้

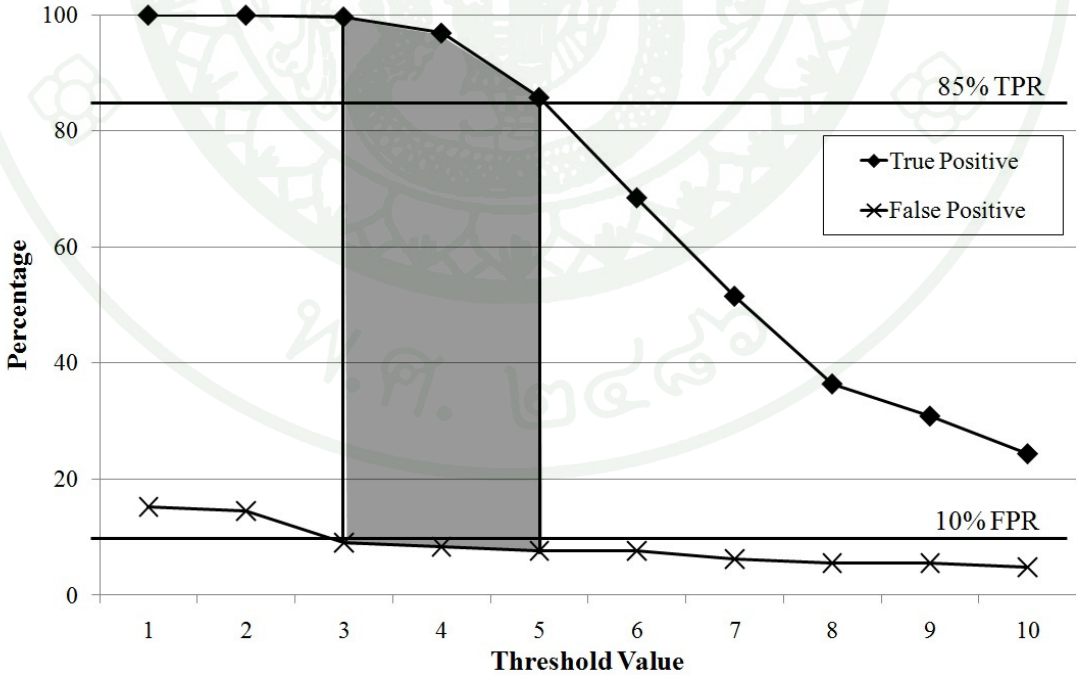


ภาพที่ 54 TPR และ FPR ของค่าระยะเวลาตรวจจับ 5 วินาที

ภาพที่ 54 แสดงกราฟผลการทดลองเมื่อใช้ระยะเวลาการตรวจจับที่ 5 วินาที ส่วนภาพที่ 55-56 แสดงกราฟผลการทดลองเมื่อใช้ระยะเวลาการตรวจจับที่ 10 และ 20 วินาทีตามลำดับ



ภาพที่ 55 TPR และ FPR ของค่าระยะเวลาตรวจจับที่ 10 วินาที



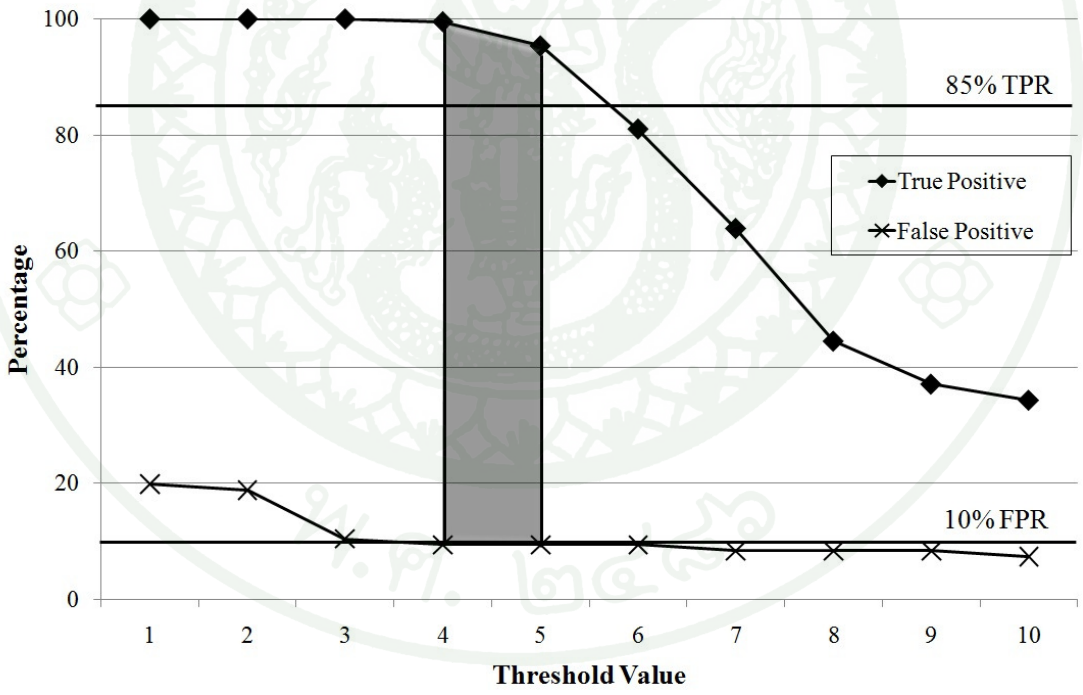
ภาพที่ 56 TPR และ FPR ของค่าระยะเวลาตรวจจับที่ 20 วินาที

จากภาพที่ 54 เมื่อกำหนดให้ระยะเวลาในการดักจับข้อมูลที่ 5 วินาที พบว่า ค่าตัดสินที่ 1, 2, และ 3 เท่านั้นที่ให้ค่า TPR สูงถึงค่าคาดหวัง และในส่วนของค่า FPR พบว่าไม่มีค่าตัดสินใดที่ มี

ค่า FPR สูงเกินค่าคาดหวัง จึงสรุปข้อมูลจากกราฟได้ว่า ค่าระยะเวลาการดักจับข้อมูลที่เหมาะสมคือ 5 วินาที หากใช้ค่าตัดสินที่ 1 และ 2 เมื่อกำหนดให้ค่าคาดหวัง TPR ไม่ต่ำกว่า 85% และ FPR ไม่เกิน 10%

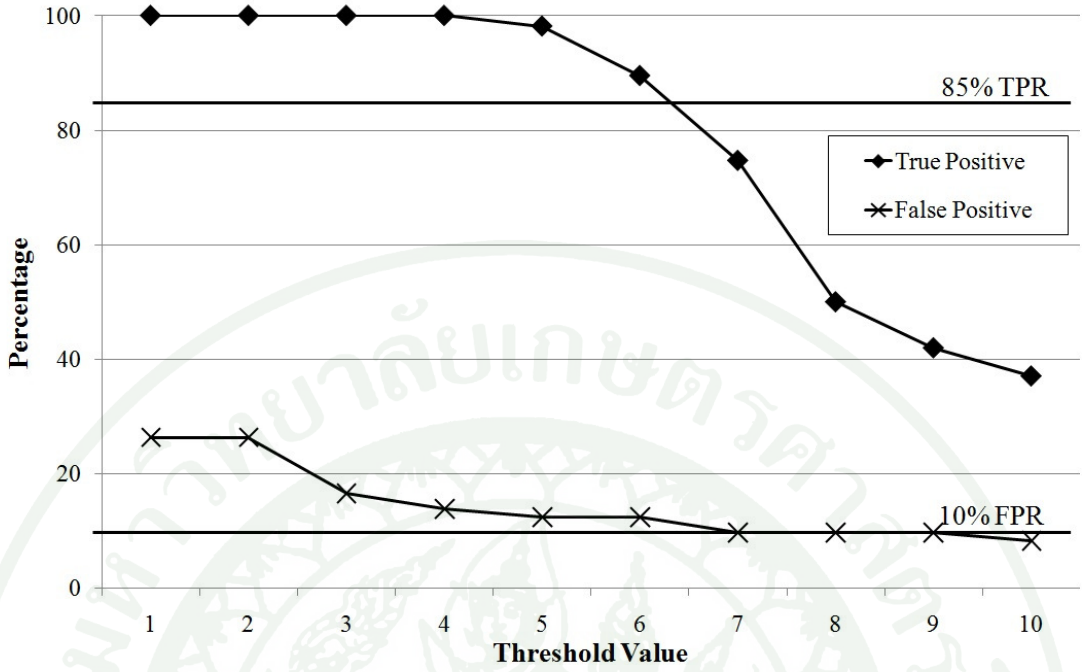
ภาพที่ 55 แสดงกราฟหากกำหนดระยะเวลาการดักจับข้อมูลที่ 10 วินาที ซึ่งเริ่มพบว่ามีค่า FPR ที่มีค่าสูงเกินค่าคาดหวังได้แก่ ค่าตัดสินที่ 1 และ 2 ตามลำดับ และพบค่า TPR ที่ต่ำกว่าค่าคาดหวังได้แก่ ตัดสินที่ 5 โดยค่าตัดสินที่ตรงตามเกณฑ์ของค่าคาดหวังได้แก่ ค่าตัดสินที่ 2, 3, และ 4

ภาพที่ 56 ก็ได้แสดงแนวโน้มการเพิ่มขึ้นของค่าตัดสินที่มีค่า TPR สูงเกินค่าคาดหวัง และค่า FPR ต่ำกว่าค่าคาดหวัง ที่ระยะเวลาการดักจับข้อมูลเป็น 20 วินาที โดยค่าตัดสินที่ตรงตามค่าคาดหวัง ได้แก่ ค่าตัดสินที่ 3, 4, และ 5

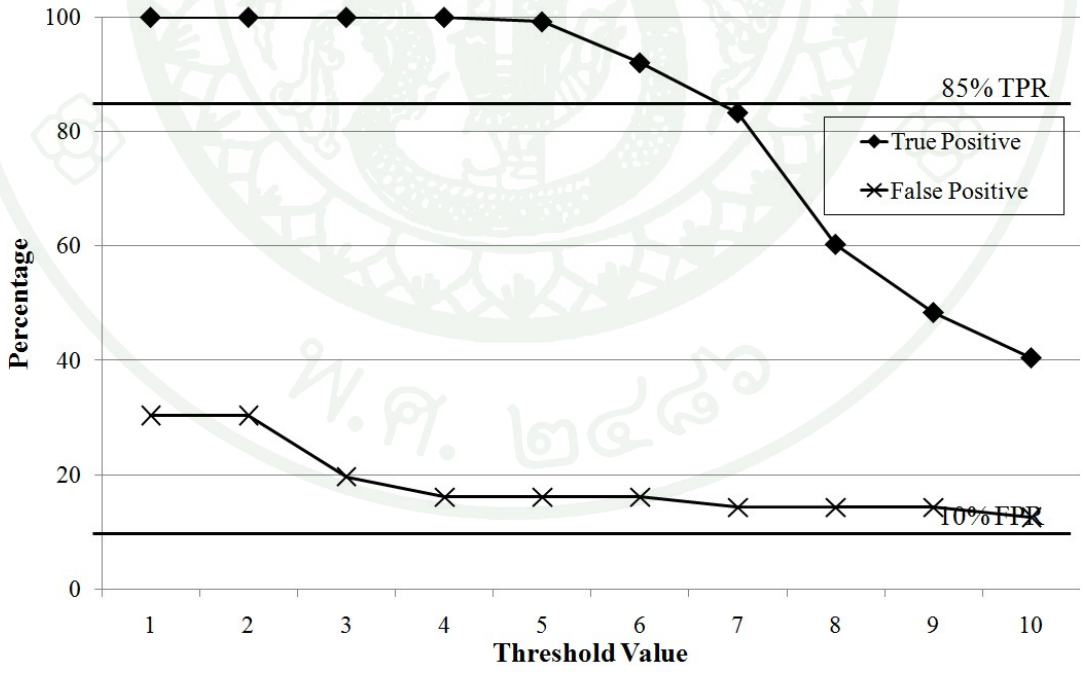


ภาพที่ 57 TPR และ FPR ของค่าระยะเวลาตรวจจับที่ 30 วินาที

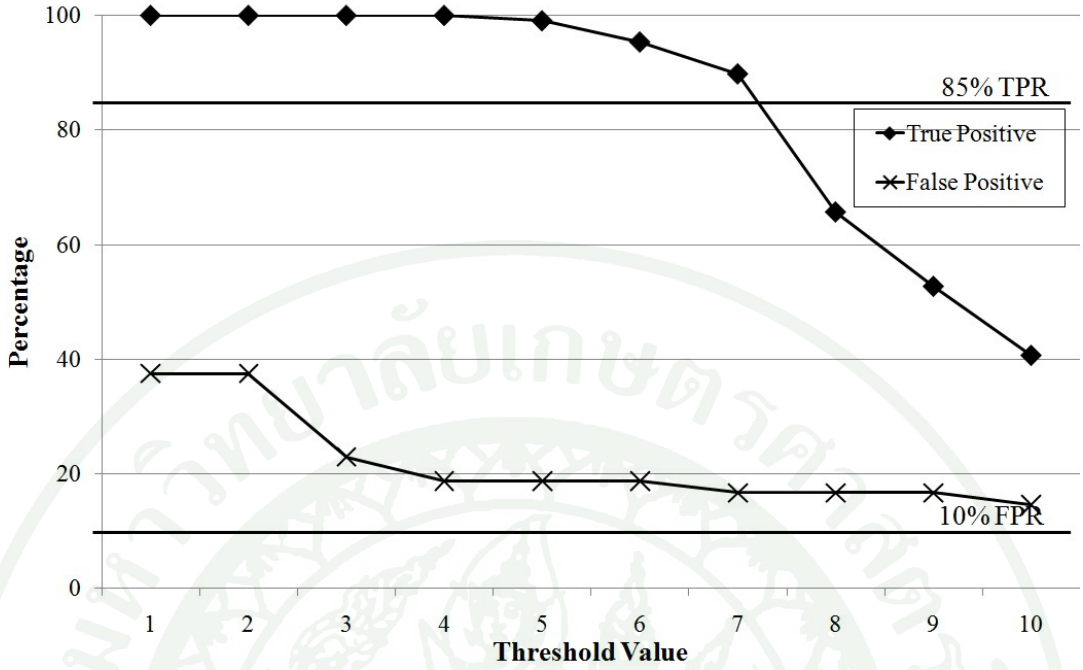
ภาพที่ 57 แสดงผลจากการทดลองเมื่อกำหนดระยะเวลาในการดักจับข้อมูลเป็น 30 วินาที ค่าตัดสินที่ตรงตามเงื่อนไขมี 2 ค่าได้แก่ ค่าตัดสินที่ 4 และ 5



ภาพที่ 58 TPR และ FPR ของค่าระยะเวลาตรวจจับที่ 40 วินาที



ภาพที่ 59 TPR และ FPR ของค่าระยะเวลาตรวจจับที่ 50 วินาที



ภาพที่ 60 TPR และ FPR ของค่าระยะเวลาตรวจจับที่ 60 วินาที

ภาพที่ 58, 59, และ 60 แสดงกราฟผลการทดลองเมื่อกำหนดระยะเวลาการดักจับข้อมูลที่ 40, 50, และ 60 ตามลำดับซึ่งจากกราฟแสดงให้เห็นว่า ไม่มีค่าตัดสินที่ตรงตามค่าคาดหวัง

สรุปผลการทดลองจากการกำหนดค่าระยะเวลาดักจับข้อมูลค่าต่าง ๆ ชี้ให้เห็นว่า ค่า TPR และ FPR มีแนวโน้มเพิ่มขึ้น โดยแปรผันตรงตามระยะเวลาการดักจับข้อมูล โดยที่ระยะเวลาการดักจับข้อมูลที่เหมาะสม ไม่ควรจะเกิน 30 วินาที เมื่อกำหนดให้ระยะเวลาดักจับข้อมูลที่เหมาะสมจะต้องตรงตามเงื่อนไขค่าคาดหวัง ที่ TPR $\geq$85% และ FPR$\leq$10% ค่าระยะเวลาดักจับข้อมูลที่เหมาะสมกับค่าตัดสินในแต่ละค่าสามารถดูได้จากช่องตารางเส้นขอบหนาในตารางที่ 8

อย่างไรก็ตามจากผลการทดลองจะพบว่าค่าระยะเวลาการดักจับข้อมูลที่เหมาะสมยังมีปริมาณมากอยู่ เพื่อที่จะหาค่าระยะเวลาการรอที่เหมาะสมยิ่งขึ้นไปอีก จึงได้กำหนดค่าคาดหวังให้สูงขึ้นไปอีก โดยกำหนดให้ระยะเวลาการดักจับข้อมูลที่เหมาะสมจะต้องมีค่าคาดหวัง TPR $\geq$90% และ FPR$\leq$6% ซึ่งระยะเวลาการดักจับข้อมูลที่ตรงตามค่าคาดหวังใหม่สามารถแสดงในช่องตารางเส้นขอบหนาในตารางที่ 9

ตารางที่ 8 ระยะเวลาการดักจับข้อมูลที่เหมาะสม เมื่อกำหนดค่าคาดหวัง TPR ≥85% และFPR≤10%

	T_5		T_{10}		T_{20}		T_{30}		T_{40}		T_{50}		T_{60}	
	TP	FP	TP	FP	TP	FP	TP	FP	TP	FP	TP	FP	TP	FP
Th 1	**99.5**	**7.12**	100	10.1	100	15.3	100	19.8	100	26.4	100	30.4	100	37.5
Th 2	**98.5**	**5.73**	**100**	**8.68**	100	14.6	100	18.8	100	26.4	100	30.4	100	37.5
Th 3	81.1	3.65	**97.07**	**5.56**	**99.7**	**9.03**	100	10.4	100	16.7	100	19.6	100	22.9
Th 4	51.3	3.47	**86.11**	**5.21**	**96.9**	**8.33**	**99.5**	**9.38**	100	13.9	100	16.1	100	18.8
Th 5	25.2	3.3	60.49	4.86	**85.8**	**7.64**	**95.4**	**9.38**	98.2	12.5	99.2	16.1	99.1	18.8
Th 6	13.6	2.95	38.12	4.86	68.5	7.64	81	9.38	89.5	12.5	92.1	16.1	95.4	18.8
Th 7	8.26	2.26	25.15	4.17	51.5	6.25	63.9	8.33	74.7	9.72	83.3	14.3	89.8	16.7
Th 8	5.63	2.08	17.29	3.82	36.4	5.56	44.5	8.33	50	9.72	60.3	14.3	65.7	16.7
Th 9	4.48	2.08	13.43	3.82	30.9	5.56	37	8.33	42	9.72	48.4	14.3	52.8	16.7
Th 10	3.63	1.91	10.19	3.47	24.4	4.86	34.3	7.29	37	8.33	40.5	12.5	40.7	14.6

ตารางที่ 9 ระยะเวลาการดักจับข้อมูลที่เหมาะสม เมื่อกำหนดค่าคาดหวัง TPR ≥90% และ FPR≤6%

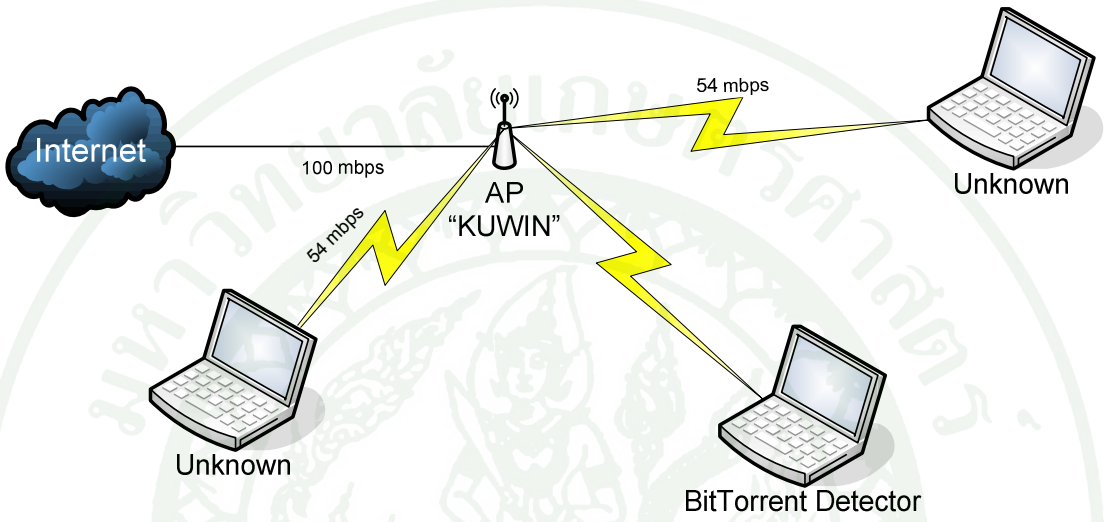
	T_5		T_{10}		T_{20}		T_{30}		T_{40}		T_{50}		T_{60}	
	TP	FP	TP	FP	TP	FP	TP	FP	TP	FP	TP	FP	TP	FP
Th 1	99.5	7.12	100	10.1	100	15.3	100	19.8	100	26.4	100	30.4	100	37.5
Th 2	**98.5**	**5.73**	100	8.68	100	14.6	100	18.8	100	26.4	100	30.4	100	37.5
Th 3	81.1	3.65	**97.07**	**5.56**	99.7	9.03	100	10.4	100	16.7	100	19.6	100	22.9
Th 4	51.3	3.47	86.11	5.21	96.9	8.33	99.5	9.38	100	13.9	100	16.1	100	18.8
Th 5	25.2	3.3	60.49	4.86	85.8	7.64	95.4	9.38	98.2	12.5	99.2	16.1	99.1	18.8
Th 6	13.6	2.95	38.12	4.86	68.5	7.64	81	9.38	89.5	12.5	92.1	16.1	95.4	18.8
Th 7	8.26	2.26	25.15	4.17	51.5	6.25	63.9	8.33	74.7	9.72	83.3	14.3	89.8	16.7
Th 8	5.63	2.08	17.29	3.82	36.4	5.56	44.5	8.33	50	9.72	60.3	14.3	65.7	16.7
Th 9	4.48	2.08	13.43	3.82	30.9	5.56	37	8.33	42	9.72	48.4	14.3	52.8	16.7
Th 10	3.63	1.91	10.19	3.47	24.4	4.86	34.3	7.29	37	8.33	40.5	12.5	40.7	14.6

จากผลการทดลองสรุปได้ว่าค่าระยะเวลาการดักจับข้อมูล ที่ควรใช้งานคือ 5 วินาที โดยใช้ค่าตัดสินที่ 2 และ ค่าระยะเวลาการดับจับข้อมูลที่ 10 วินาที โดยใช้ค่าตัดสินที่ 3 เมื่อต้องการผลบวกแท้มากกว่าหรือเท่ากับ 90% และผลบวกลวงน้อยกว่าหรือเท่ากับ 6%

3. การออกแบบการทดลองเพื่อวัดประสิทธิภาพของกลไกการตรวจจับพฤติกรรมของโพรโทคอลบิตทอร์เรนต์บนเครือข่ายไร้สายในสภาพแวดล้อมการใช้งานปกติ

วัตถุประสงค์ของการออกแบบการทดลองนี้ เพื่อทดสอบกลไกการตรวจจับที่ได้ออกแบบว่าสามารถใช้งานได้จริงและมีประสิทธิภาพหรือไม่ โดยทำการดักจับข้อมูลเครือข่ายไร้สายของ

มหาวิทยาลัยเกษตรศาสตร์ หรือ KUWIN (Kasetsart University, n.d.) ณ ภาควิชาวิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์ บางเขน ในช่วงเวลา 9.00 น., 13.00 น., และ 17.00 น. เพื่อนำมาใช้เป็นข้อมูลในการทดลอง โดยในแต่ละช่วงเวลาได้ทำการทดลองดักจับข้อมูล 5 ครั้ง รายละเอียดของการทดลองสามารถแสดงได้ดังภาพที่ 61



ภาพที่ 61 สภาพแวดล้อมในการทดลองดักจับข้อมูลบนเครือข่ายไร้สายที่ใช้งานปกติ

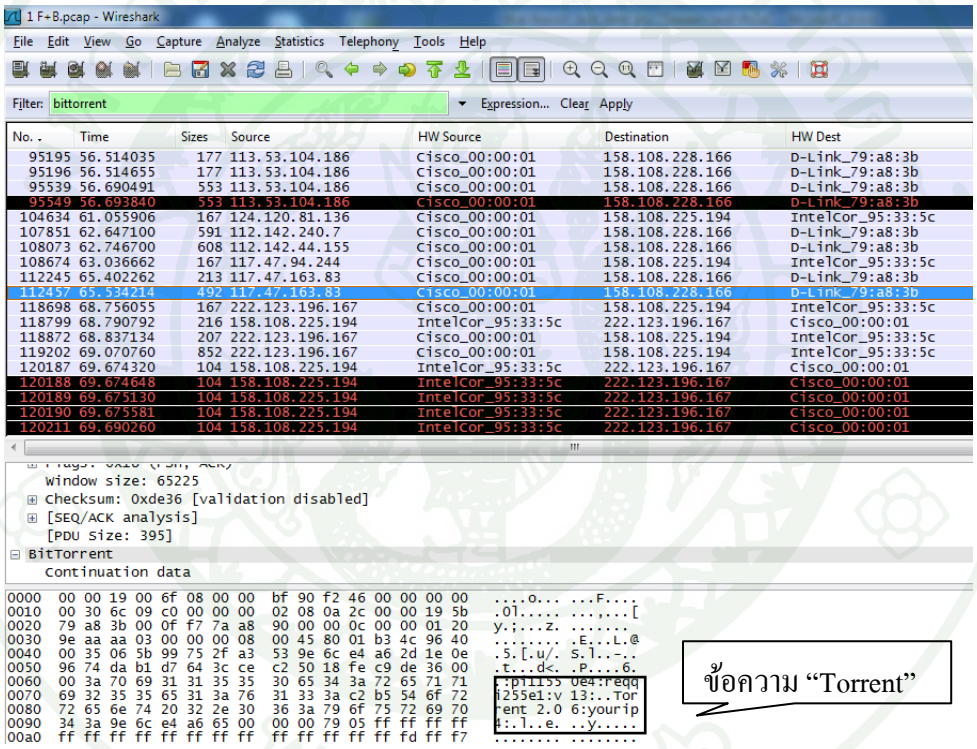
การทดลองกระทำโดยการตรวจสอบปริมาณของเครื่องลูกข่ายที่ตรวจจับสัญญาณได้ในขณะนั้น จากนั้นจึงทำการดักจับข้อมูลที่รับ-ส่งกันระหว่างคู่ที่อยู่แม็คต้นทางและที่อยู่แม็คปลายทาง ซึ่งหลังจากการดักจับข้อมูลทำให้ทราบว่า เมื่อเครื่องลูกข่ายทำการติดต่อกับเครื่องที่อยู่นอกเครือข่าย KUWIN จะพบว่าคู่ที่อยู่แม็คที่เครื่องลูกข่ายติดต่อด้วยมีค่า "00:00:0c:00:00:01" ซึ่งทราบในเวลาต่อมาว่าเป็นที่อยู่แม็คของเครื่องเกทเวย์ (Gateway) ของมหาวิทยาลัยเกษตรศาสตร์ แต่อย่างไรก็ตาม มีบางไอพีที่อยู่ในวงเครือข่ายของมหาวิทยาลัยเกษตรศาสตร์ แต่มีค่าที่อยู่แม็คเหมือนกับเกทเวย์ด้วย จึงอาจเกิดข้อผิดพลาดที่ต้องการตรวจสอบเครื่องลูกข่ายเฉพาะที่รับ-ส่งข้อมูลกับเครือข่ายภายนอกมหาวิทยาลัยได้ รายละเอียดไอพีที่มีค่าแม็คค่าเดียวกับเกทเวย์สามารถแสดงดังตารางที่ 10

ตารางที่ 10 ที่อยู่ไอพีที่มีค่าที่อยู่แม็คเหมือนกับเกทเวย์ที่พบในช่วงเวลาต่าง ๆ

ที่อยู่ไอพี	ช่วงเวลาที่พบ
158.108.171.3	9.00
158.108.244.25	9.00
158.108.8.156	9.00

ข้อมูลที่ได้จากการดักจับบนเครือข่ายไร้สายที่ใช้งานปกติ จะต้องทำการแบ่งกลุ่มข้อมูลเช่นเดียวกับข้อมูลที่ได้จากการทดลองในสภาพแวดล้อมควบคุม การแบ่งกลุ่มข้อมูลที่ได้จากการดักจับข้อมูลบนเครือข่ายไร้สายที่ใช้งานปกติ ทำได้โดยใช้วิธีการตรวจสอบด้วยโปรแกรมไวร์ชาร์ก (Wireshark, 1998) ซึ่งมีความสามารถในการตรวจจับโพรโทคอลบิตทอร์เรนต์โดยใช้วิธีการตรวจสอบสัญลักษณ์ประกอบกับการดูกระแสข้อมูล

ภาพที่ 62 แสดงถึงการตรวจจับเฟรมข้อมูลที่มีสัญลักษณ์บิตทอร์เรนต์ ซึ่งสัญลักษณ์ที่พบคือ ข้อความ “Torrent”



ภาพที่ 62 การตรวจหาสัญลักษณ์ของโพรโทคอลบิตทอร์เรนต์โดยใช้โปรแกรมไวร์ชาร์ก

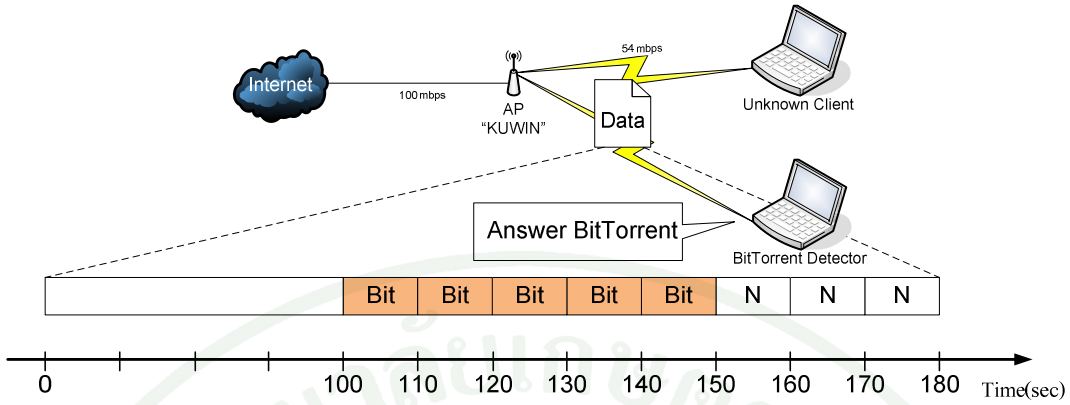
เมื่อใช้โปรแกรมไวร์ชาร์กเป็นเครื่องมือในการแบ่งกลุ่มของเครื่องลูกข่ายที่ดักจับสัญญาณได้เรียบร้อยแล้ว จึงได้ทำการแบ่งกลุ่มเป็นสองกลุ่มเช่นเดียวกับการทดลองในสภาพแวดล้อมควบคุมซึ่งได้แก่ กลุ่มเครื่องที่เป็นบิตทอร์เรนต์ที่ได้จากการตรวจสอบของโปรแกรมไวร์ชาร์ก และกลุ่มที่ไม่พบลักษณะของบิตทอร์เรนต์ ซึ่งโปรแกรมไวร์ชาร์กไม่ได้ระบุว่าเป็นลักษณะการทำงานของโพรโทคอลบิตทอร์เรนต์ โดยสามารถแสดงรายละเอียดของเครื่องลูกข่าย ที่ทำการดักจับข้อมูลได้ในเวลา ต่าง ๆ ได้ดังตารางดังต่อไปนี้

ตารางที่ 11 รายละเอียดของจำนวนเครื่องลูกข่ายที่พบในการดักจับข้อมูลที่มีการใช้งานเครือข่ายไร้สายปกติ

เวลา	ครั้งที่	เครื่องที่เป็นบิตทอร์เรนต์		เครื่องที่ไม่เป็นบิตทอร์เรนต์		รวม
		จำนวน	ร้อยละ	จำนวน	ร้อยละ	
9.00	1	2	33.33	4	66.67	6
	2	2	40	3	60	5
	3	2	40	3	60	5
	4	2	40	3	60	5
	5	2	28.57	5	61.43	7
13.00	1	2	16.67	10	16.67	12
	2	2	16.67	10	16.67	12
	3	1	8.33	11	8.33	12
	4	1	8.33	11	8.33	12
	5	1	6.67	14	6.67	15
17.00	1	3	13.64	19	86.36	22
	2	2	18.19	9	81.81	11
	3	2	16.67	10	83.33	12
	4	2	13.33	13	86.66	15
	5	2	16.67	10	83.33	12

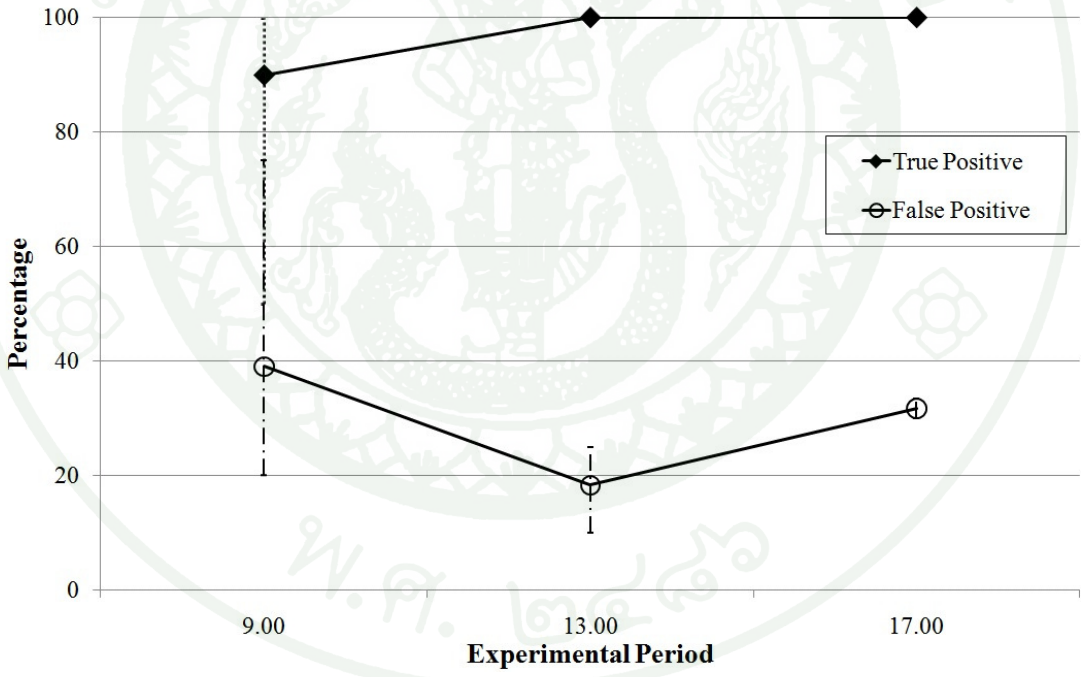
การทดลองวัดประสิทธิภาพของกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์บนเครือข่ายไร้สายที่ใช้งานปกตินี้จะใช้ค่าระยะเวลาดักจับข้อมูลที่เหมาะสมที่มีค่าผลบวกลวงน้อยที่สุด ซึ่งในที่นี้ค่าในการทดลองที่ใช้คือค่าตัดสินที่ 3 และระยะเวลาดักจับข้อมูลที่ 10 วินาที

การทดลองจะเริ่มโดยการเริ่มดักจับข้อมูลเป็นเวลา 180 วินาที หลังจากนั้นจึงทำการแบ่งข้อมูลเป็นช่วงละ 10 วินาทีตามค่าระยะเวลาดักจับที่เหมาะสม และจะทำการวิเคราะห์ข้อมูลตั้งแต่วินาทีที่ 100-180 ทั้งนี้ อ้างอิงตามค่าช่วงการเริ่มดักจับข้อมูลที่เหมาะสมคือหลังจากการเริ่มทำงานของบิตทอร์เรนต์ 20 วินาทีเป็นต้นไป โดยกลไกจะต้องตรวจสอบข้อมูล 8 ช่วงเวลา หากกลไกตัดสินว่าข้อมูลเป็นบิตทอร์เรนต์ 5 ใน 8 ช่วงเวลา ให้ถือว่าข้อมูลชุดนั้น เป็นบิตทอร์เรนต์ ภาพที่ 63 ได้แสดงถึงวิธีในการทดลองตรวจจับข้อมูล



ภาพที่ 63 การทดลองดักจับข้อมูลบนสภาพแวดล้อมปกติ

ผลการทดลองในส่วนของ TPR และ FPR เฉลี่ยในแต่ละช่วงเวลา แสดงได้ดังต่อไปนี้



ภาพที่ 64 กราฟผลการทดลองกลไกตรวจจับโพรโทคอลบิตทอร์เรนต์ในการใช้งานเครือข่ายปกติ

ภาพที่ 64 แสดงผลการทดลองกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์สภาพแวดล้อมไร้สายที่ใช้งานจริง โดยทำการทดลองเวลา 9.00, 13.00, และ 17.00 ทุกช่วงเวลาในการทดลองจะเป็นตัวแทนของความคับคั่งของการแย่งใช้สื่อ กล่าวคือ ที่เวลา 9.00 การใช้งานเครือข่ายไร้สาย ณ จุดที่ทำการทดลองมีปริมาณน้อย คือมีปริมาณเครื่องลูกข่ายที่ใช้เครือข่ายไร้สายอยู่ที่ประมาณ 6-7 เครื่อง ส่วนเวลา 13.00 แทนการใช้งานเครือข่ายในปริมาณปานกลาง คือประมาณ 10 เครื่อง

และช่วงเวลา 17.00 แทนการใช้งานเครือข่ายในปริมาณคับคั่ง คือประมาณ 20-25 เครื่องซึ่งแต่ละเวลาในการทำการทดลองจะทำการทดลอง 5 ครั้ง

ผลการทดลองพบว่า ค่า TPR ในทุกช่วงเวลาที่ทำการทดลองอยู่ที่ประมาณเฉลี่ย 90-100% ซึ่งค่านี้ได้สะท้อนถึงค่าผลลบลวงที่มีประสิทธิภาพ กล่าวคือถ้ากลไกการตรวจจับโพรโทคอลนี้ระบุว่าข้อมูลของเครื่องลูกข่ายที่กำลังตรวจสอบอยู่ไม่ได้มีการทำงานของโพรโทคอลบิตทอร์เรนต์ เราก็สามารถมั่นใจได้ 90%-100% ว่า เครื่องที่กำลังตรวจสอบอยู่นี้ ไม่ได้มีการทำงานของบิตทอร์เรนต์แน่นอน

จุดที่น่าสังเกตคือปริมาณเครื่องที่ทำการใช้โพรโทคอลบิตทอร์เรนต์มีน้อย อาจเกิดจากที่มหาวิทยาลัยเกษตรศาสตร์ ได้ทำการบีบแบนด์วิทด์เครื่องที่ใช้บิตทอร์เรนต์ และอาจประกอบกับช่วงเวลาที่ทำการทดลองเป็นช่วงปิดเทอม จึงมีปริมาณเครื่องลูกข่ายไร้สายใช้งานของโพรโทคอลบิตทอร์เรนต์น้อยกว่าช่วงเปิดเทอม

ในส่วนของค่า FPR นั้น มีค่าต่างกันในแต่ละช่วงเวลา ได้แก่ ช่วงเวลา 9.00 จะมีค่า FPR เฉลี่ยอยู่ที่เกือบ 40% ซึ่งอาจเกิดจากปริมาณเครื่องที่น้อย หากเกิดการตัดสินผิด แม้เพียงปริมาณน้อยก็อาจจะเป็นจะก่อให้เกิดสัดส่วนร้อยละในปริมาณมากได้ ส่วนช่วงเวลา 13.00 พบว่าค่า FPR เฉลี่ยอยู่ที่ประมาณ 20% และเวลา 17.00 ที่มีปริมาณเครื่องลูกข่ายใช้งานมาก แต่ก็ยังมีค่า FPR เฉลี่ยอยู่ที่ประมาณ 30% ซึ่งเมื่อตรวจสอบข้อมูลอย่างละเอียดพบว่าข้อมูลของเครื่องลูกข่ายที่ตรวจจับผิดพลาด มีลักษณะคล้ายคลึงกับข้อมูลที่จับได้ของโพรโทคอลบิตทอร์เรนต์มาก ซึ่งอาจจะเป็นผลมาจาก ขั้นตอนการกรองเฟรมของกลไกที่ใช้กฎการกรองที่ไม่ครอบคลุมเพียงพอ จึงทำให้มีพฤติกรรมของข้อมูลที่มีลักษณะคล้ายบิตทอร์เรนต์ ถูกกลไกตัดสินว่าเป็นโพรโทคอลบิตทอร์เรนต์ ทั้งนี้ ค่าความผิดพลาดที่สูงเช่นนี้ เป็นการเทียบกลไกการตรวจจับกับโปรแกรมไวร์ชาร์กเท่านั้น กล่าวคือ แม้ตัวโปรแกรมไวร์ชาร์กจะมีอัตราการตรวจจับบิตทอร์เรนต์ความถูกต้องสูง แต่ก็ยังมีโอกาสที่โปรแกรมไวร์ชาร์กจะตรวจจับผิดพลาดอยู่ จึงควรใช้วิธีการเปรียบเทียบกับชุดข้อมูลที่รู้แน่นอนว่ามีโพรโทคอลบิตทอร์เรนต์ทำงานอยู่จริง เพื่อให้ผลการทดลองมีความถูกต้องสูงที่สุด

สรุปและข้อเสนอแนะ

สรุป

โพรโทคอลบิตทอร์เรนต์เป็นโพรโทคอลแบ่งปันไฟล์แบบเพียร์ทูเพียร์ที่มีความสามารถในการใช้งานทรัพยากรแบนด์วิดท์ได้เต็มประสิทธิภาพตลอดเวลา ด้วยเทคนิคการแบ่งไฟล์ออกเป็นชิ้นส่วนเล็ก ๆ กระจายไปยังเพียร์ต่าง ๆ ได้อย่างรวดเร็ว และเมื่อเพียร์มีปริมาณมากขึ้น การบริโภคทรัพยากรแบนด์วิดท์ในเครือข่ายก็จะมากขึ้นอย่างทวีคูณ โดยเฉพาะอย่างยิ่งบนเครือข่ายไร้สาย ที่มีทรัพยากรแบนด์วิดท์จำกัดอยู่แล้ว หากมีเครื่องลูกข่ายเครื่องใดเครื่องหนึ่งบนเครือข่ายไร้สายเปิดใช้งานโพรโทคอลบิตทอร์เรนต์อยู่ ก็จะทำให้เครื่องลูกข่ายไร้สายอื่น ๆ ที่กำลังใช้งานโพรโทคอลอื่น ๆ บนเครือข่ายไร้สายเกิดภาวะขาดแคลนแบนด์วิดท์บนเครือข่ายไร้สายอย่างรุนแรงและรวดเร็ว ฉะนั้นจึงจำเป็นต้องมีการควบคุมและกำหนดการใช้งานโพรโทคอลบิตทอร์เรนต์บนเครือข่ายไร้สาย แต่ก่อนที่จะทำการควบคุมและกำหนดการใช้งานโพรโทคอลบิตทอร์เรนต์บนเครือข่ายไร้สายได้นั้นจำเป็นจะต้องมีกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์บนสภาพแวดล้อมเครือข่ายไร้สายเสียก่อน

แนวทางการตรวจจับโพรโทคอลบิตทอร์เรนต์ในปัจจุบันอาศัยข้อมูลบนเครือข่ายใช้สายในการออกแบบกลไกการตรวจจับ ดังนั้นกลไกที่ออกแบบจะต้องนำไปพัฒนาบนอุปกรณ์ที่อยู่บนเครือข่ายใช้สาย และลักษณะการทำงานจะเป็นแบบการตรวจจับรวมศูนย์แบบจุดเดียว โดยอุปกรณ์ที่จะติดตั้งกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์นี้ จะต้องมีทรัพยากรในการประมวลผลสูงมาก ทั้งนี้เนื่องมาจากจะต้องตรวจจับและวิเคราะห์ข้อมูลเครือข่ายทั้งบนระบบเครือข่ายใช้สายและระบบเครือข่ายไร้สาย ส่งผลให้อุปกรณ์ที่ติดตั้งมีราคาแพง อีกทั้งการติดตั้งอุปกรณ์ตรวจจับในลักษณะแบบรวมศูนย์เพียงจุดเดียวก็ยังเสี่ยงกับภาวะระบบตรวจจับล้มเหลว อันเนื่องมาจากอุปกรณ์ตรวจจับล่มได้

วิทยานิพนธ์นี้ได้มุ่งหวังที่จะออกแบบกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์ที่ทำงานบนเครือข่ายไร้สาย โดยทำการตรวจจับที่จุดแรกในการรับ-ส่งข้อมูลของเครือข่ายไร้สายซึ่งได้แก่ แอคเซสพ้อยท์ ซึ่งการที่จะใช้การตรวจจับในลักษณะเช่นนี้ได้จำเป็นจะต้องมีการออกแบบกลไกตรวจจับโพรโทคอลที่ออกแบบมาเพื่อใช้สำหรับสภาพแวดล้อมที่เป็นเครือข่ายไร้สายโดยเฉพาะ กล่าวคือจะต้องออกแบบกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์โดยใช้เพียงข้อมูลที่สามารถหาได้เฉพาะในเครือข่ายไร้สายเท่านั้น

วิทยานิพนธ์นี้ได้นำเสนอกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์บนสภาพแวดล้อมที่เป็นเครือข่ายไร้สาย โดยอาศัยข้อมูลเพียงแค่ขนาดเฟรมข้อมูลที่ชั้นแม็คของเครือข่ายไร้สาย ซึ่งง่ายต่อการพัฒนา บริโภคทรัพยากรน้อย ทำให้สามารถนำไปติดตั้งบนอุปกรณ์เครือข่ายไร้สายที่มีทรัพยากรจำกัดอย่างเช่นแอคเซสพ้อยท์ได้ ซึ่งกลไกแบ่งได้เป็น 3 ขั้นตอนได้แก่ การสุ่มดักจับข้อมูล การกรองเฟรม และการตัดสินการเป็นโพรโทคอลบิตทอร์เรนต์

ผลของการทดลองบนสภาพแวดล้อมควบคุมพบว่า กลไกสามารถตรวจจับได้ในเวลาจริง สามารถดักจับแม้มีการเข้ารหัสข้อมูล โดยที่ผลการทดลองเพื่อหาค่าช่วงเวลาเริ่มดักจับข้อมูลที่เหมาะสมพบว่า อยู่ที่ 20 วินาที หลังการเริ่มส่งข้อมูล สำหรับระยะเวลาการดักจับข้อมูลที่ 10 วินาที และใช้กับค่าตัดสินการเป็นบิตทอร์เรนต์ที่ 3 และ 4 หากใช้ระยะเวลาในการดักจับข้อมูลที่ 20 วินาทีเป็นต้นไป และค่าตัดสินในการเป็นบิตทอร์เรนต์ที่ 5 ช่วงเวลาเริ่มดักจับข้อมูลที่เหมาะสมจะเป็น 40 วินาทีเป็นต้นไป หลังจากเริ่มมีการส่งข้อมูลบิตทอร์เรนต์ ในส่วนของค่าระยะเวลาการดักจับข้อมูลที่เหมาะสมเมื่อกำหนดค่าคาดหวัง ที่ TPR 90% และ FPR 6% ได้แก่ ระยะเวลา 5 วินาที เมื่อกำหนดค่าตัดสินที่ 2 และระยะเวลา 10 วินาทีเมื่อกำหนดค่าตัดสินที่ 3 และเมื่อทำการทดสอบกลไกการตรวจจับโพรโทคอลบิตทอร์เรนต์ในสภาพแวดล้อมการใช้งานเครือข่ายไร้สายปกติ พบว่ากลไกสามารถให้ค่าความถูกต้องในการตรวจสอบ TPR 90%-100% โดยเฉลี่ย และมีความผิดพลาดในการตรวจสอบประมาณ 20% โดยเฉลี่ย เมื่อเทียบกับการตรวจจับด้วยโปรแกรมไวร์ชาร์ก

ข้อเสนอแนะ

การใช้การนับจำนวนขนาดเฟรมข้อมูล ยังมีความทนทานต่อการถูกทำลายน้อยมาก เพื่อเพิ่มความทนทานให้กับกลไกควรจะมี กลไกการให้น้ำหนัก การตัดสินด้วยการนับจำนวนขนาดเฟรมข้อมูล อีกทั้งการทดลองเพื่อให้ได้มาซึ่งขนาดของเฟรมที่ต้องกรอง ที่มีความละเอียดในการกรองสูงจะช่วยให้ประสิทธิภาพการทำงานของกลไกสูงขึ้น และการทดสอบในสภาพแวดล้อมที่เป็นสภาพการใช้งานปกติมีความจำเป็นมาก และเนื่องจากลักษณะพฤติกรรมการรับ-ส่งข้อมูลบนเครือข่ายไร้สายในสภาพแวดล้อมการใช้งานปกติของแต่ละสถานที่อาจมีพฤติกรรมที่แตกต่างกัน จึงควรจะต้องมีการออกแบบกลไกการเรียนรู้พฤติกรรมการรับ-ส่งข้อมูลของแต่ละสภาพแวดล้อมเสียก่อน จากนั้นจึงปรับค่าตัดสินให้เหมาะสมกับสภาพแวดล้อมนั้น ๆ ก่อนที่จะนำกลไกไปใช้งาน การเพิ่มเติมการพัฒนากลไกลงบนอุปกรณ์เครือข่ายไร้สายอย่างเช่น แอคเซสพ้อยท์ จะช่วยให้รู้ถึงการบริโภคทรัพยากรของกลไกเมื่อใช้งานกับอุปกรณ์ที่มีทรัพยากรจำกัดได้ชัดเจนยิ่งขึ้น และการทดสอบประสิทธิภาพระหว่างการตรวจจับแบบกระจายจุดและการตรวจจับแบบรวมศูนย์ดั้งเดิมของระบบว่า ทั้งสองแนวทางให้ประสิทธิภาพโดยรวมของระบบว่าเป็นอย่างไร

เอกสารและสิ่งอ้างอิง

อนันต์ ผลเพิ่ม. 2550. **แลนไร้สาย**. บริษัทซีเอ็ดยูเคชั่นจำกัด (มหาชน), กรุงเทพฯ.

BitComet Development Group. 2003**. BitComet - A free C++ BitTorrent/HTTP/FTP Download Client.** Available Source: http://www.bitcomet.com/, May 1, 2007.

BitTorrent Organization. 2008. **The BitTorrent Protocol Specification.** Available Source: http://bittorrent.org/beps/bep_0003.html, April 13, 2009.

Brenner, P. 1997. **A Technical Tutorial on the IEEE802.11 Protocol.** Available Source: http://www.sss-mag.com/pdf/802_11tut.pdf, August 20, 2009.

Brilliant Digital Entertainment Group. 2008. **Kazaa – Free Music.** Available Source: http://www.kazaa.com/, April 19, 2010.

Chen, Z., A. Delis, P. Wei. 2008. Identification and Management of Sessions Generated by Instant Messaging and Peer-to-Peer Systems. *In* **International Journal of Cooperative Information Systems**. 17 (1): 1-52.

Clarke, I. 2009. **The Freenet Project.** Available Source: http://freenetproject.org/, April 19, 2010.

Cohen, B. 2003. Incentive build robustness in bittorrent, pp. 1-5. *In* **Workshop on Economics of Peer-to-Peer System**. 5-6 June 2003, California, USA.

Collins, M.P. and M.K. Reiter. 2006. Finding Peer-to-Peer File-Sharing Using Coarse Network Behaviors, pp. 1-17. *In* **11th European Symposium on Research in Computer Security.** 18-20 September 2006, Hamburg, Germany.

Constantinou, F. and P. Mavrommatis. 2006. Identifying Known and Unknown Peer-to-Peer Traffic, pp. 93-102. *In* **Proceedings of the Fifth IEEE International Symposium on Network Computing and Applications.** 24-26 July 2006, Massachusetts, USA.

Fanning, S. 2001. **Napster is Music at Internet Speed**. Available Source: http://web.archive.org/web/20000229130418/http://www.napster.com/index.html, April 19, 2010.

Fomby, T.B. n.d. **Confusion Matrix.** Available Source: http://faculty.smu.edu/tfomby/eco5385/lecture/Confusion%20Matrix.pdf, May 1, 2007.

IANA. 2010. **Port Numbers.** Available Source: http://www.iana.org/assignments/port-numbers, April 1, 2010.

John, W. and S. Tafvelin. 2008. Heuristics to classify internet backbone traffic based on connection patterns, pp. 1–5. *In* **International Conference on Information Networking**. 23-25 January 2008, Busan, Korea.

Karagiannis T., K. Papagiannaki and M. Faloutsos. 2005. BLINC: Multilevel Traffic Classification in the Dark. *In* **ACM SIGCOMM Computer Communication Review**. 35 (4): 229-240.

Kasetsart University. n.d. **KUWIN.** Available Source: http://kuwin.ku.ac.th/, April 1, 2010

Kirk, P. 2003. **Gnutella – A Protocol for a Revolution.** Available Source: http://rfc-gnutella.sourceforge.net/, April 19, 2010.

Moore, A.W. and K. Papagiannaki. 2005. Toward the Accurate Identification of Network Applications, pp. 41-54. *In* **Proceedings of 6th International Workshop on Passive and Active Network Measurement.** 31 March – 1 April 2005, Boston, MA, USA.

Ngiwlay W., C. Intanagonwiwat and Y. Teng-amnuay. 2008. Bittorrent Peer Identification based on Behaviors of a Choke Algorithm, pp. 65-74. *In* **Proceedings of the 4th Asian Conference on Internet Engineering**. 18-20 November 2008, Bangkok, Thailand.

Perényi, M., T.D. Dang, A. Gefferth, S. Molnár. 2006. Identification and Analysis of Peer-to-Peer Traffic. *In* **Journal of Communications**. 1 (7): 36-46.

Phoomsuk, N. and A. Phonphoem. 2010. A Light-Weight BitTorrent Detection Mechanism for Wireless LAN Environment, pp. 151-156. *In* **Proceedings of 7th International Joint Conference on Computer Science and Software Engineering**. 12-14 May 2010, Bangkok, Thailand.

Pourebrahimi, B., K.L.M. Bertels and S. Vassiliadis. 2005. A Survey of Peer-to-Peer Networks, pp. 1-7. **Proceedings of the 16th Annual Workshop on Circuits, Systems and Signal Processing**. 17-18 Nov. 2005, Veldhoven, Netherlands.

Ratnasamy, S., P. Francis, M. Handley, R. Karp and S. Shenker. 2001. A Scalable Content-Addressable Network, pp. 161-172. *In* **Proceedings of ACM SIGCOMM**. 27-31 August 2001, California, USA.

Risso, F., M. Baldi, O. Morandi, A. Baldini and P. Monclus. 2008. Lightweight, Payload-Based Traffic Classification:An Experinmental Evaluation, pp. 5869-5875. *In* **Proceeding of IEEE Conference of Communications**. 19-23 May 2008, Beijing, China.

Salgarelli, L., F. Gringoli and T. Karagiannis. 2007. Comparing traffic classifiers. *In* **ACM SIGCOMM Computer Communication Review**. 37 (3): 65-68.

Sen, S. and J. Wang. 2004. Analyzing Peer-To-Peer Traffic across Large Networks. *In* **IEEE/ACM Transactions on Networking**. 12 (2): 219-232.

Sendil, S., and N. Nagarajan. 2009. An Optimized Method for Analyzing the Peer to Peer Traffic. *In* **European Journal of Scientific Research**. 34 (4): 535-541.

Stoica, I., R. Morris, D. Karger, F. Kaashoek, and H. Balakrishnan. 2001. **The Chord/DHash Project.** Available Source: http://pdos.csail.mit.edu/chord/, April 19, 2010.

Strigeusian, L. 2005. **µTorrent – a (very) tiny BitTorrent.** Available Source: http://www.utorrent.com/, May 1, 2007.

The Wireshark team. 1998. **Wireshark.** Available Source: http://www.wireshark.org/, May 10, 2007.

Wikipedia. n.d. **Transmission Control Protocol.** Available Source: http://en.wikipedia.org/wiki/Transmission_Control_Protocol, April 19, 2010.

Won, Y.J., P. Byung-Chul, J. Hong-Taek, K. Myung-Sup and J.W. Hong. 2006. A Hybrid Approach for Accurate Application Traffic Identification, pp. 1-8. *In* **Proceedings of the 4th IEEE/IFIP Workshop on End-to-End Monitoring Techniques and Services**. 3 April 2006, Vancouver, Canada.

ประวัติการศึกษา และการทำงาน

ชื่อ –นามสกุล	ว่าที่ร้อยตรีณรงค์ ภูมิสุข
วัน เดือน ปี ที่เกิด	13 เมษายน 2524
สถานที่เกิด	กรุงเทพมหานคร
ประวัติการศึกษา	สาขาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์ วิทยาเขตศรีราชา
ตำแหน่งหน้าที่การงานปัจจุบัน	เจ้าหน้าที่ดูแลศูนย์ข้อมูล
สถานที่ทำงานปัจจุบัน	ศูนย์ไทยกริดแห่งชาติ
ผลงานดีเด่นและรางวัลทางวิชาการ	
ทุนการศึกษาที่ได้รับ	