การศึกษาเรื่องมัลติคาสต์ที่เชื่อถือได้บนการเชื่อมโยงผ่านดาวเทียมแบบทิศทางเดียว โดยใช้เทคนิคบรอดคาสต์ดิสค์ เอฟอีซี และการแลกเปลี่ยนแบบเพียร์ทูเพียร์

A Study on Reliable Multicast on Unidirectional Satellite Link Using Broadcast Disk, FEC and Peer-to-Peer Sharing Techniques

คำนำ

ในปัจจุบันอัตราความต้องการใช้งานระบบเครือข่ายคอมพิวเตอร์เพิ่มสูงขึ้นมาก รวมถึงมีการนำข้อมูลประเภทมัลติมีเดียเข้ามาใช้อย่างมากมาย ทำให้ข้อมูลที่รับ-ส่งเริ่มมีขนาดใหญ่เพิ่มขึ้นด้วย ปัญหาที่ตามมาคือเกิดความคับคั่งของข้อมูลบนระบบเครือข่าย เนื่องจากความจุของช่องสัญญาณมีปริมาณจำกัด วิธีการมัลติคาสต์ที่สามารถช่วยลดปัญหาความคับคั่งของข้อมูลบนระบบเครือข่ายคอมพิวเตอร์จึงถูกเสนอขึ้น การส่งข้อมูลแบบมัลติคาสต์เป็นการส่งข้อมูลจากผู้ส่งหนึ่งรายไปยังผู้รับหลายรายพร้อมกันด้วยการส่งข้อมูลเพียงชุดเดียว (RFC 1301, 1992) แอพพลิเคชั่นที่ใช้บริการมัลติคาสต์จะใช้บริการโปรโตคอลยูดีพี (User Defined Protocol : UDP) (RFC 768, 1980) ซึ่งเป็นบริการที่อยู่ในระดับชั้นทรานสปอร์ต (Transport Layer) ตามโครงสร้างมาตรฐานสากลของสถาปัตยกรรมระบบเครือข่ายโอเอสไอ (Open Systems Interconnection : OSI) (ISO 7498, 1994) โปรโตคอลยูดีพีให้บริการรับ-ส่งข้อมูลที่มีความน่าเชื่อถือไม่ถึงร้อยเปอร์เซ็นต์ ดังนั้นแอพพลิเคชั่นจึงต้องจัดการเรื่องความน่าเชื่อถือเองโดยมีการทำอยู่ในระดับชั้นแอพพลิเคชั่น (Application Layer) กลไกในการสร้างความน่าเชื่อถือที่นิยมและใช้กันอย่างแพร่หลายคือ การใช้ข้อความตอบการได้รับข้อมูลหรือ ACK (Acknowledgement) และข้อความปฏิเสธการได้รับข้อมูลหรือ NACK (Negative Acknowledgement) (RFC 793, 1981) โดยที่ผู้รับจะส่งข้อความดังกล่าวเพื่อแจ้งให้ผู้ส่งทราบว่าตนเองได้รับหรือไม่ได้รับแพ็กเก็ตใด ซึ่งมีผลให้ผู้ส่งส่งแพ็กเก็ตที่สูญหายให้แก่ผู้รับอีกครั้ง ปัจจัยสำคัญของวิธีการสร้างความน่าเชื่อถือคือ ระบบเครือข่ายที่ใช้ต้องสนับสนุนการสื่อสารแบบสองทิศทาง นั่นคือผู้รับต้องสามารถส่งสถานะการรับข้อมูลให้ผู้ส่งได้

ถึงแม้ระบบเครือข่ายเพื่อเชื่อมต่อเข้ากับอินเตอร์เน็ตในปัจจุบันมีการเชื่อมโยงกันอย่างกว้างขวาง แต่สำหรับประเทศที่กำลังพัฒนานั้นบางพื้นที่เป็นแหล่งทุรกันดาร หรือมีลักษณะเป็นเกาะ เช่น ประเทศฟิลิปปินส์ ประเทศอินโดนีเซีย เป็นต้น การลงทุนในการวางโครงสร้าง

สายสัญญาณระบบเครือข่ายภาคพื้นดินนั้นมีค่าใช้จ่ายสูงมาก ทำให้เกิดปัญหาความเหลื่อมล้ำด้านการรับข้อมูลข่าวสารกับประชาชนในเมืองใหญ่ อันเกิดจากการขาดแคลนโครงสร้างพื้นฐาน ทางเลือกหนึ่งที่ประเทศเหล่านั้นจะสามารถทำได้คือการใช้ระบบเครือข่ายดาวเทียมซึ่งมีต้นทุนต่ำกว่า ในกรณีการรับข้อมูลข่าวสารเพียงอย่างเดียว ผู้รับสามารถติดตั้งอุปกรณ์รับสัญญาณดาวเทียมเพื่อรับข้อมูลและไม่ต้องเสียค่าใช้จ่ายเพิ่มเติม เช่นเดียวกับการติดตั้งอุปกรณ์ดาวเทียมเพื่อรับสัญญาณโทรทัศน์ผ่านดาวเทียมซึ่งมีรูปแบบการสื่อสารแบบทิศทางเดียว ประเทศกำลังพัฒนาสามารถนำระบบเครือข่ายดาวเทียมมาประยุกต์ใช้เพื่อกระจายความเท่าเทียมในการเข้าถึงข้อมูลข่าวให้แก่ประชาชน การสร้างความน่าเชื่อถือสำหรับการสื่อสารแบบทิศทางเดียว ได้แก่ การส่งข้อมูลวนรอบซ้ำทั้งชุดหรือ Data Carousel ในกรณีที่เป็นการสื่อสารทิศทางเดียวผู้ส่งไม่สามารถทราบได้ว่ามีแพ็กเก็ตใดสูญหายบ้าง ผู้ส่งจึงต้องส่งข้อมูลซ้ำทั้งหมด โดยวนรอบส่งซ้ำไปเรื่อยๆ และคาดหวังว่าผู้รับจะได้รับแพ็กเก็ตทั้งหมด ผู้ส่งไม่สามารถทราบได้ว่าจะต้องส่งข้อมูลซ้ำเป็นจำนวนกี่รอบ จึงเป็นวิธีที่ใช้แบนวิดธ์มาก อีกกลไกหนึ่งที่ใช้ในการสร้างความน่าเชื่อถือคือ Forward Error Correcting (FEC) (Blahut, 1984) โดยใช้การเข้ารหัส (Encoding) และการถอดรหัส (Decoding) ข้อมูล ผู้ส่งจะส่งทั้งข้อมูลที่เป็นแพ็กเก็ตต้นฉบับ (Original Packet) และข้อมูลที่ได้จากการเข้ารหัสซึ่งเป็นแพ็กเก็ตพิเศษ (Redundant Packet) ไปให้ผู้รับ ถ้าผู้รับได้รับแพ็กเก็ตต้นฉบับไม่ครบ ผู้รับสามารถถอดรหัสแพ็กเก็ตพิเศษเพื่อใช้กู้คืนแพ็กเก็ตต้นฉบับที่หายไป อย่างไรก็ตามผู้รับจำเป็นต้องได้รับแพ็กเก็ตในจำนวนที่เพียงพอต่อจำนวนแพ็กเก็ตต้นฉบับที่สูญหาย จึงจะสามารถกู้แพ็กเก็ตต้นฉบับได้ครบถ้วน

โครงการระบบเครือข่ายดาวเทียม Asian Internet Interconnection Initiatives หรือ AI3 (AI3 Project, 2004) เป็นโครงการที่ได้รับทุนสนับสนุนจากรัฐบาลญี่ปุ่น โดยมีวัตถุประสงค์ในการพัฒนาระบบเครือข่ายดาวเทียมขึ้นเพื่อประโยชน์ด้านการศึกษาระหว่างสถาบันการศึกษา โดยใช้ในการส่งข้อมูลข่าวสาร เทปบันทึกการเรียนการสอน และการถ่ายทอดการเรียนการสอนแบบเรียลไทม์ เป็นต้น ระบบเครือข่ายดาวเทียมนี้มีการให้บริการทั้งช่องสัญญาณดาวเทียมแบบสองทิศทางและแบบทิศทางเดียว แต่เนื่องจากแอพพลิเคชั่นที่มีการใช้งานทั่วไปจะมีการใช้งานอยู่บนโปรโตคอลมาตรฐานซึ่งต้องอาศัยการเชื่อมต่อแบบสองทิศทางในการสร้างความน่าเชื่อถือ แต่ในการใช้งานผ่านช่องสัญญาณดาวเทียมแบบทิศทางเดียวไม่มีกลไกที่จะให้ผู้รับส่งสถานะการรับข้อมูลให้ผู้ส่งทราบได้ จึงทำให้การใช้งานบนช่องสัญญาณดาวเทียมแบบทิศทางเดียวยังไม่เกิดประสิทธิภาพสูงสุด

งานวิทยานิพนธ์ฉบับนี้นำเสนอวิธีการส่งข้อมูลแบบมัลติคาสต์ที่เชื่อถือได้บนระบบเครือข่ายดาวเทียมแบบทิศทางเดียว โดยศึกษาอัตราการสูญหายของแพ็กเก็ตที่เกิดขึ้นบนการสื่อสารผ่านระบบเครือข่ายดาวเทียม เพื่อนำมาใช้กำหนดอัตราการสูญหายบนเครือข่ายจำลอง ศึกษาผลความน่าเชื่อถือของข้อมูลจากรูปแบบการให้บริการข้อมูล ศึกษาประสิทธิภาพในการส่งข้อมูล เก็บสถิติของจำนวนรอบที่ต้องใช้เพื่อส่งข้อมูลซ้ำ ศึกษาอัตราการสูญหายที่มีผลต่อประสิทธิภาพจากการสร้างความน่าเชื่อถือด้วย FEC และเสนอการใช้วิธีแลกเปลี่ยนข้อมูลภายในกลุ่มผู้รับเพื่อเพิ่มประสิทธิภาพในการสร้างความน่าเชื่อถือ

วัตถุประสงค์ของการทำวิทยานิพนธ์

วิธีการมัลติคาสต์ถูกนำมาใช้ในการกระจายข้อมูลที่มีขนาดใหญ่ไปยังผู้รับหลายราย เนื่องจากเป็นวิธีการที่สามารถลดจำนวนข้อมูลบนระบบเครือข่าย ซึ่งถือเป็นการเพิ่มประสิทธิภาพให้กับระบบเครือข่ายให้สามารถรองรับความต้องการในปัจจุบันและในอนาคต ที่มีแนวโน้มการใช้งานและการส่งข้อมูลที่มีขนาดใหญ่สูงขึ้น การขยายระบบเครือข่ายให้รองรับกับความต้องการที่เพิ่มสูงขึ้นถือเป็นทางเลือกหนึ่งแต่ต้องใช้การลงทุนที่สูง แม้ว่าการมัลติคาสต์เป็นวิธีที่ถือได้ว่ามีการใช้แบนวิดธ์ต่ำ แต่พื้นฐานของการมัลติคาสต์นั้นเป็นการทำงานบนระบบการสื่อสารที่ไม่รับรองความถูกต้องของข้อมูล ซึ่งความถูกต้องของข้อมูลถือเป็นปัจจัยที่สำคัญปัจจัยหนึ่งของการสื่อสาร ดังนั้นจึงได้มีงานวิจัยต่างๆ พัฒนาวิธีการในการสร้างความน่าเชื่อถือสำหรับการสื่อสารแบบมัลติคาสต์

ปัญหาความเหลื่อมล้ำทางด้านการรับข้อมูลข่าวสารต่างๆ เกิดจากการขาดแคลนทรัพยากรและเทคโนโลยีเพื่อช่วยในการเชื่อมโยงการติดต่อสื่อสาร ซึ่งอาจเกิดจากสาเหตุของสภาพภูมิประเทศซึ่งเป็นพื้นที่ทุรกันดาร รวมถึงสาเหตุจากการขาดทุนทรัพย์ การใช้ดาวเทียมเป็นเครื่องมือในการเชื่อมโยงระบบเครือข่ายคอมพิวเตอร์เพื่อรับข้อมูลข่าวสารต่างๆ ผ่านช่องสัญญาณดาวเทียมถือเป็นวิธีการหนึ่งที่ทำให้ลดปัญหาด้านความเหลื่อมล้ำทางด้านข้อมูลข่าวสารต่างๆ เนื่องจากการเชื่อมโยงระบบเครือข่ายคอมพิวเตอร์ผ่านดาวเทียมเป็นวิธีการที่มีต้นทุนต่ำ หากผู้รับเพียงต้องการรับข้อมูลแต่ฝ่ายเดียว ดังนั้นการสร้างความน่าเชื่อถือในการสื่อสารข้อมูลแบบทิศทางเดียวจึงเป็นวิธีการหนึ่งที่ช่วยเสริมให้การลดปัญหาความเหลื่อมล้ำทางด้านการรับข้อมูลข่าวสารเป็นไปได้ดียิ่งขึ้น

โครงสร้างของระบบเครือข่าย AI3 เป็นเครือข่ายระบบดาวเทียมที่ประกอบด้วยช่องสัญญาณการสื่อสารแบบทิศทางเดียว และช่องสัญญาณสื่อสารแบบสองทิศทาง เครือข่าย AI3 ถูกพัฒนาขึ้นโดยมีวัตถุประสงค์เพื่อเป็นช่องทางในการกระจายข้อมูลด้านการศึกษา ซึ่งการสร้างความน่าเชื่อถือโดยทั่วไปจะทำงานโดยอาศัยช่องสัญญาณแบบ 2 ทิศทาง ดังนั้นการใช้งานที่ต้องการความน่าเชื่อถือจึงถูกนำไปใช้งานบนช่องสัญญาณดาวเทียมแบบ 2 ทิศทาง เพื่อให้การใช้งานช่องสัญญาณดาวเทียมแบบทิศทางเดียวเกิดประโยชน์และประสิทธิภาพสูงสุด ในงานวิทยานิพนธ์นี้จึงต้องการพัฒนาวิธีการสร้างความน่าเชื่อถือในการมัลติคาสต์แบบทิศทางเดียว เพื่อนำมาใช้งานช่องการสื่อสารดังกล่าว โดยในงานวิทยานิพนธ์นี้ได้ทดลองสร้างความน่าเชื่อถือด้วยวิธีการต่างๆ อันได้แก่ วิธีการสร้างความน่าเชื่อถือด้วย Data Carousel วิธีการสร้างความน่าเชื่อถือ

ด้วย FEC และวิธีการสร้างความน่าเชื่อถือด้วย Peer-to-Peer Sharing เพื่อเปรียบเทียบประสิทธิภาพ และหาวิธีการที่เหมาะสมกับประเภทความต้องการข้อมูลแต่ละแบบ อีกทั้งยังได้ทดลองผ่านเครือข่ายดาวเทียม AI3 และเครือข่ายจำลอง เพื่อให้ทราบถึงข้อจำกัดของวิธีแต่ละวิธี

การตรวจสอบเอกสาร

ความรู้พื้นฐาน

ดาวเทียมจะมีหน้าที่ทวนสัญญาณข้อมูลที่ได้รับจากสถานีส่งข้อมูลภาคพื้นดิน โดยกระจายสัญญาณข้อมูลกลับลงมายังพื้นดิน ระยะเวลาเดินทางของข้อมูลจากผู้ส่งไปยังผู้รับจะประกอบไปด้วย ระยะเวลาส่งขาขึ้นหมายถึง ระยะเวลาที่ข้อมูลเดินทางจากสถานีส่งบนพื้นโลกถึงดาวเทียม และระยะเวลาส่งขาลง หมายถึง ระยะเวลาที่ข้อมูลใช้ในการเดินทางจากดาวเทียมถึงสถานีรับบนพื้นโลก ระยะเวลาเดินทางของข้อมูลนี้จะขึ้นอยู่กับระยะห่างระหว่างดาวเทียมกับพื้นโลก ซึ่งระยะห่างของดาวเทียมนี้จะต่างกันออกไปขึ้นอยู่กับประเภทของดาวเทียม เช่น ดาวเทียมค้างฟ้า (Geostationary orbit) มีระยะห่างจากพื้นโลกประมาณ 36,000 กิโลเมตร ใช้ระยะเวลาในการสะท้อนข้อมูลประมาณ 558 มิลลิวินาที ดาวเทียมวงโคจรระดับต่ำ (Low earth orbit) มีระยะห่างจากพื้นโลกต่ำกว่า 2,000 กิโลเมตร และดาวเทียมที่มีวงโคจรระดับกลาง (Medium earth orbit) มีระยะห่างจากพื้นโลก ระหว่างดาวเทียมวงโคจรระดับต่ำ และดาวเทียมค้างฟ้า คือระหว่าง 2,000 ถึง 36,000 กิโลเมตร (Defense Space Technology Centre., 2006)

การมัลติคาสต์ข้อมูลบนระบบเครือข่ายจะมีการเรียกใช้บริการจากโปรโตคอลยูดีพีที่อยู่ในชั้นทรานสปอร์ต ซึ่งเป็นที่ทราบดีว่าโปรโตคอลยูดีพีเป็นโปรโตคอลที่ไม่มีกระบวนการสร้างความน่าเชื่อถือ แต่อย่างไรก็ตามความน่าเชื่อถือก็ยังคงเป็นสิ่งที่จำเป็นสำหรับการส่งข้อมูลในบางแอพพลิเคชั่น เช่น เว็บบราวต์เซอร์ ไฟล์เซิร์ฟเวอร์ รีโมทเซิร์ฟเวอร์ เป็นต้น ดังนั้นจึงได้มีการคิดค้นวิธีในการสร้างความน่าเชื่อถือให้กับการส่งข้อมูลแบบมัลติคาสต์ เช่น การส่งข้อมูลวนซ้ำ การทำ FEC การแลกข้อมูลในกลุ่มของผู้รับ เป็นต้น การกำหนดกลุ่มของผู้รับจะใช้โปรโตคอลไอพี ซึ่งหมายเลขกลุ่มของผู้รับจะเป็นหมายเลขไอพีแอดเดรสคลาส D (RFC 1112, 1989) ซึ่งมี 4 บิต แรกเป็น 1110 เมื่อผู้รับต้องการรับข้อมูล ผู้รับจะต้องแจ้งการเป็นสมาชิกกลุ่มมัลติคาสต์แก่เร้าท์เตอร์ในเครือข่ายของตนให้ทราบโดยใช้โปรโตคอลไอจีเอ็มพี (Fenner, 1997) หรือ Internet Group Management Protocol (IGMP) ผู้รับสามารถเป็นสมาชิกกลุ่มมัลติคาสต์ได้มากกว่า 1 กลุ่ม โปรโตคอลไอจีเอ็มพียังถูกใช้ในการตรวจสอบสถานะความเป็นสมาชิกกลุ่มมัลติคาสต์ระหว่างผู้รับและเร้าท์เตอร์

ความรู้พื้นฐานและทฤษฎีที่เกี่ยวข้องในวิทยานิพนธ์ฉบับนี้ ประกอบด้วย รูปแบบการบริการส่งข้อมูลกรณีมีข้อความร้องขอและกรณีไม่มีข้อความร้องขอ กลไกการสร้างความน่าเชื่อถือประเภทต่างๆ การควบคุมคุณภาพการให้บริการข้อมูลโดยวิธีบรอดคาสต์ดิสค์

1. การสื่อสารดาวเทียม

ตำแหน่งของดาวเทียมจากจุดคงที่บนพื้นโลกนั้นขึ้นอยู่กับวงโคจรของดาวเทียม เช่น ดาวเทียมที่มีวงโคจรต่ำจะทำให้ดาวเทียมหมุนรอบโลกด้วยความเร็วสูงมาก การรับ-ส่งสัญญาณจะทำได้ยากเพราะสถานีรับสัญญาณจะมีเวลาน้อยในการติดต่อสื่อสาร ก่อนที่ดาวเทียมจะลับขอบฟ้า ส่วนดาวเทียมที่โคจรที่ความสูง ประมาณ 36,000 กิโลเมตรจากพื้นโลกเหนือเส้นศูนย์สูตร จะมีระยะเวลาในการหมุนรอบโลกประมาณ 24 ชั่วโมงซึ่งเท่ากับเวลาที่โลกหมุนรอบตัวเอง หมายความว่าดาวเทียมจะเสมือนอยู่ในตำแหน่งที่คงที่ตลอดเวลาเมื่อสังเกตจากพื้นโลก จึงเรียกดาวเทียมที่โคจรในความสูงประมาณ 36,000 กิโลเมตรนี้ว่าดาวเทียมแบบประจำที่ (Geosynchronous satellite)

สมาพันธ์โทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ได้มีการประชุมตกลงในระดับนานาชาติว่าด้วยการใช้วงโคจรและคลื่นความถี่สำหรับดาวเทียม เพื่อให้การใช้งานไม่เกิดความทับซ้อนและรบกวนกัน ตารางที่ 1 แสดงคลื่นความถี่หลักที่ใช้ในทางพาณิชย์ ช่วงคลื่น C เป็นคลื่นความถี่แรกที่นำมาใช้ ประกอบด้วยคลื่นความถี่ 2 ช่วง ช่วงความถี่ต่ำถูกกำหนดเพื่อใช้สำหรับการส่งสัญญาณจากดาวเทียมลงมายังโลก (downlink) ช่วงคลื่นความถี่สูงถูกกำหนดเพื่อใช้สำหรับสถานีภาคพื้นดินในการส่งสัญญาณขึ้นไปยังดาวเทียม (uplink)ช่วงคลื่น C นี้มีความถี่ในช่วง 4 กิกะเฮิร์ต – 6 กิกะเฮิร์ต ซึ่งเป็นช่วงคลื่นเดียวกับที่ใช้ในการสื่อสารบนพื้นผิวโลก เป็นการสื่อสารด้วยสัญญาณไมโครเวฟที่ใช้ช่วงคลื่น 2 กิกะเฮิร์ต – 10 กิกะเฮิร์ต จึงทำให้การสื่อสารผ่านดาวเทียมในช่วงคลื่น C ไม่สามารถขยายการใช้งานได้อีก

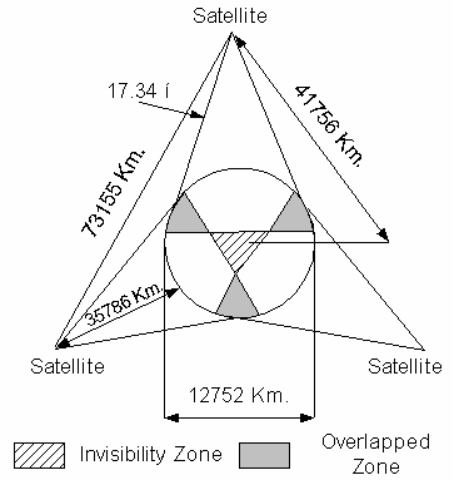
ตารางที่ 1 แสดงคลื่นความถี่หลักของดาวเทียมที่ใช้ในทางพาณิชย์

ช่วงความถี่	ความถี่	ขาลง (กิกะเฮิร์ต)	ขาขึ้น (กิกะเฮิร์ต)	ปัญหา
C	4/6	3.7-4.2	5.925-6.425	มีการใช้งานช่วงความถี่เดียวกันในภาคพื้นดิน
Ku	11/14	11.7-12.2	14.0-14.5	สัญญาณถูกรบกวนได้ง่ายโดยฝน
Ka	20/30	17.7-21.7	27.5-30.5	สัญญาณถูกรบกวนได้ง่ายโดยฝน

ที่มา: Tanenbaum (1996)

ช่วงความถี่ถัดมาคือช่วงคลื่น Ku การสื่อสารดาวเทียมสามารถใช้คลื่นช่วงนี้ได้ดีกว่าช่วงคลื่น C และเป็นช่วงคลื่นที่มีการใช้งานน้อย อย่างไรก็ตามข้อจำกัดใหม่ที่เกิดขึ้นคือ “ฝน” ช่วงคลื่น Ku และช่วงคลื่น Ka ที่ใช้ความถี่คลื่นสูงกว่า จะถูกรบกวนโดยฝนได้ง่าย แต่พายุฝนขนาดใหญ่ซึ่งจะรบกวนคลื่นสัญญาณให้หายไปทั้งหมดนั้นมักจะเกิดขึ้นในพื้นที่วงแคบ จึงสามารถหลีกเลี่ยงได้โดยการเพิ่มจำนวนสถานีรับสัญญาณภาคพื้นดินให้มากขึ้นและวางสถานีกระจายเป็นบริเวณกว้าง ซึ่งแม้ว่าจะสามารถลดปัญหาได้แต่ก็ทำให้มูลค่าโดยรวมของระบบสูงขึ้น

จากภาพที่ 1 แสดงระดับวงโคจรของดาวเทียมค้างฟ้า ซึ่งมีระยะห่างจากพื้นผิวโลก 35,786 กิโลเมตร และมีระยะห่างจากแกนโลก 41,756 กิโลเมตร และแสดงให้ถึงพื้นที่ที่สามารถครอบคลุมได้ด้วยดาวเทียมค้างฟ้าจำนวน 3 ดวง ซึ่งจะมีบางพื้นที่ถูกครอบคลุมด้วยดาวเทียมมากกว่า 1 ดวง และมีบางพื้นที่ที่ดาวเทียมทั้ง 3 ดวงไม่สามารถครอบคลุมถึงได้เนื่องจากถูกบังด้วยส่วนโค้งของพื้นผิวโลก (Invisibility Zone) แม้ว่าการส่งสัญญาณระหว่างดาวเทียมกับสถานีภาคพื้นดินมีความเร็วสูงถึง 300,000 กิโลเมตรต่อวินาที แต่ระยะทางทั้งขาขึ้นและขาลงประมาณ 72,000 กิโลเมตร ทำให้ต้องใช้เวลาในการส่งข้อมูลจากผู้ส่งไปยังผู้รับนานถึง 500-600 มิลลิวินาที (250-300 มิลลิวินาที สำหรับขาขึ้น และ 250-300 มิลลิวินาที สำหรับขาลง) โดยทั่วไปจะอ้างอิงระยะนี้โดยใช้ค่าประมาณ 558 มิลลิวินาที (279 มิลลิวินาที สำหรับขาขึ้น และ 279 มิลลิวินาที สำหรับขาลง) ซึ่งเป็นเวลาที่ข้อมูลใช้เดินทางเพียงทางเดียวจากผู้ส่งไปยังผู้รับ



ภาพที่ 1 ตำแหน่งการโคจรของดาวเทียมค้างฟ้า (Geosynchronous Satellite)
ที่มา: Defense Space Technology Centre (2006)

2. รูปแบบการบริการส่งข้อมูล

การส่งข้อมูลระหว่างผู้ส่งไปยังผู้รับสามารถแบ่งได้เป็น 3 ลักษณะ ได้แก่ แบบยูนิคาสต์ (Unicast)แบบมัลติคาสต์ (Multicast) และแบบบรอดคาสต์ (Broadcast) การส่งข้อมูลแบบยูนิคาสต์เป็นการส่งแบบหนึ่งต่อหนึ่ง คือในการสื่อสารครั้งหนึ่งๆ จะมีผู้ส่งเพียงหนึ่งรายและมีผู้รับเพียงหนึ่งราย ดังนั้นเมื่อมีผู้รับมากกว่าหนึ่งรายต้องการของรับข้อมูลชุดเดียวกัน จะเกิดจำนวนคู่สนทนาที่ต้องส่งแบบยูนิคาสต์ตามจำนวนผู้รับที่ต้องการรับข้อมูล

การติดต่อสื่อสารแบบมัลติคาสต์และบรอดคาสต์จะเป็นการติดต่อสื่อสารแบบหนึ่งต่อกลุ่ม หมายถึงในการสื่อสารครั้งหนึ่งๆ จะเป็นการส่งข้อมูลเพียงหนึ่งชุดจากผู้ส่งเพียงหนึ่งราย แต่สามารถมีผู้รับข้อมูลได้มากกว่าหนึ่งราย การติดต่อสื่อสารทั้งสองลักษณะนี้ต่างกันที่ การสื่อสารแบบมัลติคาสต์จะมีจุดประสงค์เพื่อส่งข้อมูลให้กลุ่มของผู้รับที่ต้องการรับข้อมูล โดยเจาะจงกลุ่มของผู้รับด้วยหมายเลขที่อยู่ที่เป็นไอพีแอดเดรสคลาส D โดยจะต้องไม่ใช้หมายเลขไอพีที่ถูกกำหนดเป็นมาตรฐานในการใช้งานซึ่งระบุไว้ใน RFC 1700 (1994) ส่วนการสื่อสารแบบบรอดคาสต์มีจุดประสงค์เพื่อส่งข้อมูลให้ทุกๆ สถานีที่มีการเชื่อมต่อในเครือข่ายเดียวกัน

การส่งข้อมูลจากผู้ส่งไปยังผู้รับสามารถเกิดขึ้นได้ 2 กรณี กรณีแรกเกิดจากการร้องขอข้อมูลจากฝ่ายผู้รับ ในกรณีนี้เมื่อผู้รับต้องการข้อมูลใดๆ จะส่งข้อความร้องขอข้อมูลที่ต้องการไปยัง

ผู้ส่ง เมื่อผู้ส่งได้รับข้อความร้องขอข้อมูล จึงส่งข้อมูลตามที่ผู้รับร้องขอ หากกรณีไม่พบข้อมูลที่ผู้รับร้องขอ ผู้ส่งจะส่งข้อความแจ้งให้ผู้รับทราบว่าไม่พบข้อมูลที่ร้องขอ กระบวนการจัดส่งข้อมูลรูปแบบนี้มีลักษณะคล้ายผู้รับดึงข้อมูลจากผู้ส่ง จึงเรียกรูปแบบนี้ว่า Pull model การจัดส่งข้อมูลจากผู้ส่งไปยังผู้รับอีกกรณีหนึ่ง สามารถทำได้โดยผู้ส่งส่งข้อมูลออกไปโดยไม่มีการร้องขอข้อมูลจากผู้รับ กรณีนี้ผู้รับจะต้องทราบว่าข้อมูลที่ต้องการจะถูกส่งมาเวลาใด วิธีการจัดส่งข้อมูลรูปแบบนี้มีลักษณะคล้ายการส่งสัญญาณโทรทัศน์ รูปแบบนี้เรียกว่า Push Model

2.1 Pull Model

การส่งข้อมูลด้วยรูปแบบนี้ผู้ส่งสามารถตรวจสอบผู้ร้องขอข้อมูลได้ว่าเป็นผู้ใด และยังสามารถตรวจสอบสิทธิ์ของผู้ร้องขอข้อมูลก่อนส่งข้อมูลได้ การให้บริการข้อมูลในรูปแบบนี้เป็นแบบยูนิคาสต์ซึ่งต้องอาศัยการสื่อสารแบบ 2 ทิศทางระหว่างผู้รับและผู้ส่ง สามารถพบได้ในการให้บริการ WWW การให้บริการ FTP เป็นต้น ข้อดีและข้อเสียของการให้บริการข้อมูลแบบ Pull Model แสดงดังตารางที่ 2

ตารางที่ 2 ข้อดีและข้อเสียของ Pull Model

ข้อดี	ข้อเสีย
• สามารถระบุผู้รับได้ • สามารถตรวจสอบสิทธิ์ของผู้ร้องขอ • ให้บริการข้อมูลได้ตรงตามที่ผู้รับต้องการและในเวลาที่ต้องการ	• ต้องการการสื่อสารแบบ 2 ทิศทาง • เป็นการให้บริการแบบหนึ่งต่อหนึ่ง

2.2 Push Model

การส่งข้อมูลด้วยรูปแบบนี้เหมาะกับการใช้งานในกรณีที่ผู้รับไม่สามารถส่งคำร้องขอข้อมูลไปยังผู้ส่งได้ การให้บริการมัลติคาสต์ข้อมูลเป็นการส่งข้อมูลในรูปแบบ Push Model เพื่อให้บริการส่งข้อมูลไปยังกลุ่มของผู้รับ เพื่อเป็นการลดปริมาณความคับคั่งของข้อมูลบนเครือข่าย เช่น การมัลติคาสต์ข้อมูลประเภทมัลติมีเดียเนื่องจากเป็นข้อมูลที่มีขนาดใหญ่ เป็นต้น เพื่อให้การบริการข้อมูลเป็นไปตามความต้องการของผู้รับ ผู้ส่งและผู้รับจำเป็นต้องมีการตกลงเรื่องข้อมูลที่

ผู้รับต้องการ รวมถึงเวลาที่ผู้ส่งส่งข้อมูลไว้ล่วงหน้า ข้อดีและข้อเสียของการให้บริการข้อมูลแบบ Push Model แสดงดังตารางที่ 3

ตารางที่ 3 ข้อดีและข้อเสียของ Push Model

ข้อดี	ข้อเสีย
• สามารถใช้ได้กับการสื่อสารแบบทิศทางเดียว (จากผู้ส่งไปยังผู้รับ) • เป็นการให้บริการแบบหนึ่งต่อกลุ่ม (ลดความคับคั่งของข้อมูลบนระบบเครือข่าย)	• ไม่สามารถระบุผู้รับได้ • ไม่สามารถตรวจสอบสิทธิ์ของผู้รับได้ (แต่สามารถเข้ารหัสเพื่อป้องกันข้อมูลได้) • ผู้รับต้องทราบเวลาที่ผู้ส่งจะจัดส่งข้อมูลที่ต้องการ เพื่อรอรับข้อมูล

3. กลไกการสร้างความน่าเชื่อถือ (Reliability Mechanism)

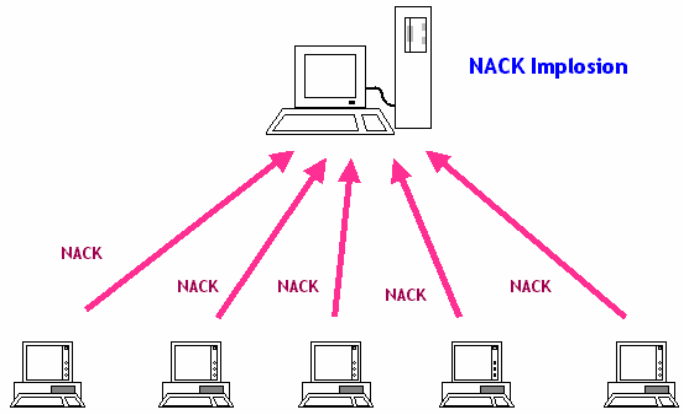
วัตถุประสงค์ในการสื่อสารบนระบบเครือข่ายคือ การส่งข้อมูลไปยังผู้รับ และทำให้ผู้รับสามารถรับข้อมูลได้ถูกต้องครบถ้วน แต่จากสาเหตุต่างๆ เช่น ความคับคั่งของข้อมูล การชนกันของข้อมูล ความเสียหายของสื่อ เป็นต้น ทำให้ผู้รับไม่ได้รับข้อมูลถูกต้องครบถ้วน ดังนั้นความน่าเชื่อถือในการสื่อสารข้อมูลจึงเป็นสิ่งสำคัญสำหรับบางแอพพลิเคชั่น กลไกพื้นฐานในการสร้างความน่าเชื่อถือสำหรับการสื่อสารบนระบบเครือข่ายที่อาศัยการสื่อสารแบบสองทิศทาง คือ การใช้ข้อความตอบกลับจากผู้รับ (Acknowledge: ACK หรือ Negative Acknowledge: NACK) โดยผู้รับจะส่งข้อความแจ้งสถานะการรับข้อมูลให้แก่ผู้ส่ง ส่วนวิธีการสร้างความน่าเชื่อถือที่ใช้การสื่อสารแบบทิศทางเดียว ได้แก่ การส่งข้อมูลวนซ้ำ หรือ Data Carousel เป็นวิธีการสร้างความน่าเชื่อถือโดยผู้ส่งจะส่งข้อมูลทั้งหมดซ้ำเป็นจำนวนหลายๆ รอบ และวิธีถัดมาเป็นการใช้วิธีการส่งแพ็กเก็ตพิเศษที่ได้จากการเข้ารหัสข้อมูล เพื่อให้ผู้รับถอดรหัสแพ็กเก็ตพิเศษเพื่อนำมาในการกู้คืนแพ็กเก็ตต้นฉบับที่สูญหาย วิธีนี้เรียกว่า Forward Error Correcting หรือ FEC

3.1 การใช้ข้อความตอบกลับ

การสร้างความน่าเชื่อถือด้วยการตอบกลับจากผู้รับเป็นกลไกแบบง่าย คือ เมื่อผู้รับได้รับแพ็กเก็ตจากผู้ส่งก็จะแจ้งกลับไปยังผู้ส่งว่าได้รับข้อมูลเรียบร้อยแล้วด้วย Acknowledge

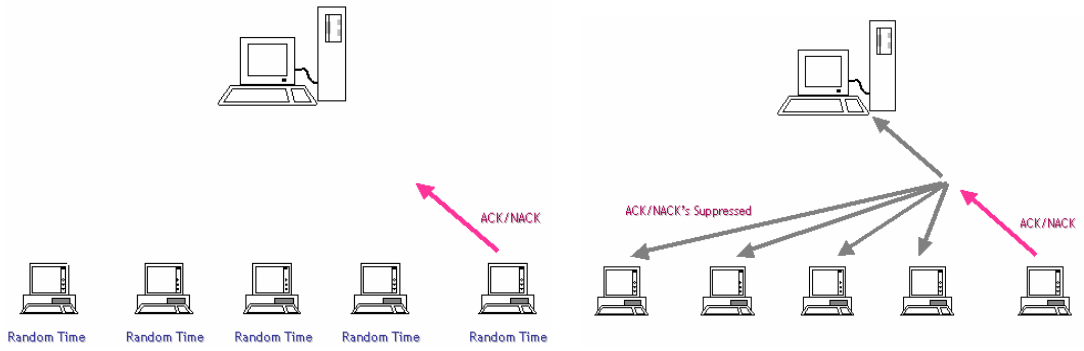
Packet (ACK) บางโปรโตคอลละเว้นการส่ง ACK เพื่อลดปริมาณข้อมูลบนเครือข่าย แต่หากว่าผู้รับเห็นว่าลำดับที่ของแพ็กเก็ตที่ได้รับมีการกระโดดข้าม แสดงให้เห็นว่าอาจมีแพ็กเก็ตสูญหาย ผู้รับจะคอยแพ็กเก็ตช่วงเวลาหนึ่งก่อนเพื่อให้แน่ใจว่าแพ็กเก็ต ได้สูญหายไปจริง แล้วจึงส่ง Negative Acknowledge Packet (NACK) ไปแจ้งให้ผู้ส่งส่งแพ็กเก็ตซ้ำ

การใช้กลไกสร้างความน่าเชื่อถือด้วย NACK นั้นอาจเกิดปัญหาที่เรียกว่า “NACK Implosion” ขึ้นได้ดังภาพที่ 2 โดยเมื่อทางฝ่ายผู้รับไม่สามารถรับแพ็กเก็ตได้ครบถ้วนหรือถูกต้องตามที่ต้องการ ผู้รับจะส่งข้อความที่เรียกว่า NACK เพื่อไปแจ้งฝ่ายผู้ส่งให้ส่งข้อมูลมาให้อีกครั้ง หากว่ามีผู้รับหลายรายที่ไม่ได้รับแพ็กเก็ตเดียวกัน จะทำให้มี NACK ถูกส่งไปแจ้งผู้ส่ง เพื่อร้องขอแพ็กเก็ตเดียวกันเป็นจำนวนมาก ทำให้เกิดปัญหาทางด้านผู้ส่งที่ต้องจัดการกับแพ็กเก็ตเดียวกันเป็นจำนวนมาก



ภาพที่ 2 การเกิดปัญหา NACK Implosion

Floyd *et al.* ,(1995) เสนอวิธีการปัญหาดังกล่าว ด้วยการลดปริมาณของ NACK ที่จะถูกส่งไปยังผู้ส่ง โดยการให้ผู้รับสุ่มเวลาเพื่อคอยก่อนที่จะส่ง NACK และการส่ง NACK จะเป็นการส่งไปยังผู้รับอื่นๆ ที่อยู่ในกลุ่มย่อยของตนด้วย เมื่อผู้รับรายอื่นๆ ได้รับ NACK ที่เป็นการร้องขอแพ็กเก็ตเดียวกับของตัวเอง ก็จะยกเลิกการส่ง NACK ของตัวเองทันที ซึ่งมีการทำงานดังภาพที่ 3(a) และ ภาพที่ 3(b)



(a) (b)

ภาพที่ 3 การแก้ปัญหา NACK Implosion

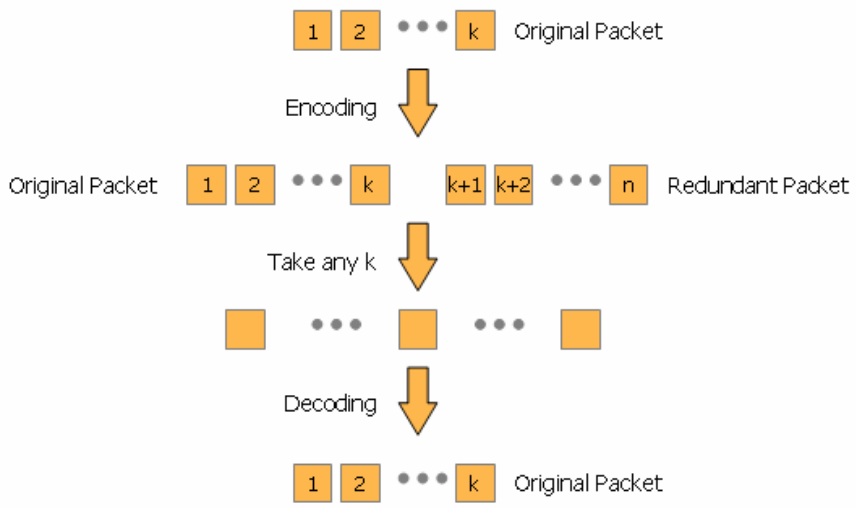
3.2 การส่งข้อมูลวนซ้ำ (Data Carousel)

ในกรณีที่เป็นการใช้ช่องทางการสื่อสารแบบทิศทางเดียว ผู้รับไม่สามารถส่งข้อความตอบกลับไปยังผู้ส่งได้ จึงไม่สามารถใช้กระบวนการสร้างความน่าเชื่อถือด้วยการส่ง ACK และ NACK ผู้ส่งส่งข้อมูลไปยังผู้รับแต่ฝ่ายเดียว โดยไม่สามารถทราบได้ว่าผู้รับไม่ได้รับแพ็กเก็ตใด และไม่สามารถทราบได้ว่าจะต้องส่งแพ็กเก็ตใดซ้ำให้แก่ผู้รับบ้าง ดังนั้นผู้ส่งจำเป็นต้องส่งแพ็กเก็ตซ้ำทุกแพ็กเก็ต ถึงแม้ว่าส่งข้อมูลซ้ำทุกแพ็กเก็ตครบแล้ว ผู้ส่งก็ยังไม่สามารถทราบได้ว่าผู้รับสามารถรับแพ็กเก็ตได้ครบทุกแพ็กเก็ตหรือไม่ ดังนั้นการสร้างความน่าเชื่อถือด้วยวิธีนี้จะต้องส่งแพ็กเก็ตซ้ำทุกแพ็กเก็ตเป็นจำนวนหลายๆ รอบ การส่งข้อมูลซ้ำๆ แบบนี้มีลักษณะเหมือนม้าหมุนที่หมุนวนไปเรื่อยๆ จึงเรียกว่า Data Carousel ข้อมูลจะหยุดส่งเมื่อได้ส่งข้อมูลครบตามจำนวนรอบหรือครบตามระยะเวลาที่ได้ถูกกำหนดไว้ล่วงหน้า

3.3 การทำ FEC

วิธีการ FEC สามารถแบ่งกระบวนการทำงานออกเป็นสองส่วนหลักๆ ด้วยกัน ได้แก่ กระบวนการเข้ารหัส (Encoding) และกระบวนการถอดรหัส (Decoding) กระบวนการ เข้ารหัสและถอดรหัส ถูกนำมาใช้ในการกู้คืนแพ็กเก็ตที่สูญหายในกรณีที่ผู้รับได้รับแพ็กเก็ตมาไม่ครบถ้วน โดยที่ทางฝ่ายผู้ส่งจะนำไฟล์ข้อมูลมาสร้างแพ็กเก็ตต้นฉบับ (Original Packet) จำนวน K แพ็กเก็ต จากนั้นจะนำแพ็กเก็ตต้นฉบับมาใช้ในการเข้ารหัสเพื่อสร้างแพ็กเก็ตพิเศษ (Redundant Packet) โดยจำนวนแพ็กเก็ตหลังการเข้ารหัสจะถูกกำหนดด้วยค่าตัวคูณที่เรียกว่า Stretch Factor ซึ่งมีค่ามากกว่า

1 นำมาคูณกับจำนวนแพ็กเก็ตต้นฉบับ จำนวนแพ็กเก็ตหลังการเข้ารหัสจะมีจำนวนเพิ่มขึ้นจาก k แพ็กเก็ต เป็น n แพ็กเก็ต โดยที่แพ็กเก็ตจำนวน k แพ็กเก็ตแรก ยังคงเป็นแพ็กเก็ตต้นฉบับ และตั้งแต่แพ็กเก็ตที่ k+1 ถึงแพ็กเก็ตที่ n จะเป็นแพ็กเก็ตพิเศษ ผู้ส่งจะส่งแพ็กเก็ตจำนวน n แพ็กเก็ต ให้แก่ผู้รับ เมื่อผู้รับรับแพ็กเก็ตและมีการสูญหายของบางแพ็กเก็ตเกิดขึ้น ผู้รับจะใช้แพ็กเก็ตต้นฉบับที่รับได้และมีความถูกต้องทั้งหมด ร่วมกับแพ็กเก็ตพิเศษที่ได้รับและมีความถูกต้องอีกจำนวนหนึ่ง เพื่อให้ได้เป็นจำนวนอย่างน้อย k แพ็กเก็ต ซึ่งเท่ากับจำนวนแพ็กเก็ตต้นฉบับ ผู้รับก็จะสามารถถอดรหัสแพ็กเก็ตพิเศษเพื่อกู้คืนแพ็กเก็ตต้นฉบับกลับมาได้ ซึ่งลำดับการทำงานแสดงดังภาพที่ 4



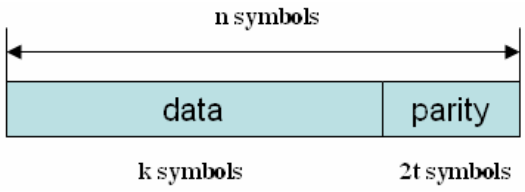
ภาพที่ 4 จำนวนแพ็กเก็ตในการเข้ารหัสและถอดรหัสข้อมูลของวิธีการ FEC
ที่มา: Byers *et al*., (1998)

การเข้ารหัสข้อมูลที่มีการนำมาใช้งานในปัจจุบันมีหลายแบบ ได้แก่ Turbo Codes (Berrou *et al*., 1996) การเข้ารหัสแบบนี้ได้ถูกนำมาใช้กับการอุปกรณ์รับและส่งสัญญาณดาวเทียมและอุปกรณ์ส่งคลื่นวิทยุต่างๆ (Orten *et al*., 2002) ซึ่งถือเป็นการทำงานใช้ระดับชั้นดาต้าลิ้งค์ (Data Link Layer) การเข้ารหัสแบบ Reed-Solomon มีการใช้งานในระดับดาต้าลิ้งค์เช่นกัน และยังถูกนำมาใช้งานในระดับชั้นแอพพลิเคชั่น (Application Layer) เพื่อเพิ่มประสิทธิภาพในการสร้างความน่าเชื่อถือ ซึ่งการเข้ารหัสด้วยวิธีนี้มีการพัฒนา 2 แบบ ได้แก่ การพัฒนาด้วย Vandermonde Matrices โดย Rizzo, (1997) และการพัฒนาด้วย Cauchy Matrices โดย Blomer *et al*., (1995) การเข้ารหัสแบบ Tornado Codes โดย Luby *et al*., (1997) เป็นวิธีการ FEC ที่ถูกนำมาใช้งานใน

ระดับชั้นแอพพลิเคชั่น มีประสิทธิภาพในด้านการประมวลผลที่เร็วกว่าวิธีการ FEC แบบ Reed-Solomon Codes

3.3.1 Reed-Solomon Codes (Blomer *et al*., 1995; Rizzo, 1997)

การเข้ารหัสข้อมูลแบบ Reed-Solomon Codes (RS) มีลักษณะเป็นรหัสวนที่ไม่เป็นไบนารี (Nonbinary Cyclic Codes) ซึ่งใช้ทฤษฎีพื้นฐานทางพีชคณิตและ Finite Field ที่เรียกว่า Galois Field (GF) โดยการเข้ารหัสจะกระทำบนข้อมูลไบนารีที่มีความยาว (Length) ของสัญลักษณ์ข้อมูล หรือที่เรียกว่า ซิมโบล (symbol) เท่ากับ L สัญลักษณ์การขยายฟิลด์จึงเป็น $GF(2^L)$ ดังนั้นจำนวนซิมโบลที่สามารถมีได้จะมีค่าเท่ากับ 2^L -1 ซิมโบล และมีรูปแบบการเข้ารหัสเป็น RS(n, k) ซึ่งแสดงดังภาพที่ 5 โดยที่ n เป็นจำนวนซิมโบลทั้งหมดหลังการเข้ารหัส k เป็นจำนวนซิมโบลต้นฉบับ และซิมโบลพิเศษ (parity) ที่ได้จากการเข้ารหัสจะมีค่าเท่ากับ 2t หรือเท่ากับ n-k รหัสแบบ Reed-Solomon Codes เป็นรหัสที่มีคุณสมบัติในการกู้คืนข้อมูลส่วนที่ผิดพลาด (Error) และสูญหาย (Erasure) ได้ โดยประสิทธิภาพในการกู้คืนซิมโบลส่วนที่ผิดพลาดจะมีค่าเท่ากับ t หมายความว่าจะสามารถกู้คืนซิมโบลต้นฉบับที่ถูกต้องได้ในกรณีที่มีการผิดพลาดของซิมโบลไม่เกิน t ซิมโบล จากจำนวน n ซิมโบล และประสิทธิภาพในการกู้คืนซิมโบลต้นฉบับที่สูญหายจะมีค่าเท่ากับ 2t ซึ่งหมายความว่าหากซิมโบลที่ได้รับทั้งหมดมีความถูกต้อง แต่เกิดการสูญหายของซิมโบลไม่เกินจำนวน 2t ซิมโบล จากจำนวน n ซิมโบล ก็จะสามารถกู้คืนซิมโบลต้นฉบับส่วนที่สูญหายกลับมาได้



ภาพที่ 5 การเข้ารหัสข้อมูลด้วย Reed-Solomon Codes

ตัวอย่างการเข้ารหัส Reed-Solomon Codes ด้วยสัญลักษณ์การขยายฟิลด์ $GF(2^8)$ จำนวนซิมโบลที่สามารถมีได้จะเท่ากับ 255 ซิมโบล ดังนั้นการเข้ารหัสด้วยโค้ด (code) มาตรฐาน RS(255, 223) หมายถึง มีซิมโบลต้นฉบับจำนวน 223 ซิมโบล และซิมโบลพิเศษ 32 ซิมโบล จำนวนซิมโบลทั้งหมดหลังการเข้ารหัสจะเท่ากับ 255 ซิมโบล ประสิทธิภาพในการกู้คืนซิมโบลที่

ผิดพลาด (Error) จะเท่ากับ 16 ซิมโบล และประสิทธิภาพในการกู้คืนซิมโบลที่สูญหาย (Erasure) จะเท่ากับ 32 ซิมโบล การเข้ารหัสด้วย Reed-Solomon Codes สามารถใช้โค้ดที่มีขนาดสั้นกว่าโค้ดมาตรฐานได้ เช่น RS(160, 128) ซึ่งหมายถึงมีซิมโบลต้นฉบับจำนวน 128 ซิมโบล และมีซิมโบลทั้งหมดหลังการเข้ารหัสเท่ากับ 160 ซิมโบล ขั้นตอนการเข้ารหัสจะทำการสร้างซิมโบลที่มีค่า 0 จำนวน 95 ซิมโบล เพื่อให้ได้จำนวนซิมโบลครบตามสัญลักษณ์การขยายฟิลด์ของ GF(2^8) แต่จะไม่ถูกส่งให้แก่ผู้รับ การใช้ขนาดโค้ดที่สั้นกว่าโค้ดมาตรฐานนี้เรียกว่า Shorten

มีงานวิจัยที่พัฒนาการเข้ารหัสข้อมูลแบบ RS ด้วยกัน 2 แนวทาง คือ การพัฒนาโดยใช้ Vandermonde Matrices (Rizzo, 1997) และการพัฒนาโดยใช้ Cauchy Matrices (Blomer *et al.*, 1995) เวลาที่ใช้ในการประมวลผลสำหรับการเข้ารหัสข้อมูลจะเป็นสัดส่วนกับจำนวนแพ็กเก็ตต้นฉบับ ซึ่งจะมีค่าเท่ากับ $k(1+l)P$ และเวลาที่ใช้ในการประมวลผลสำหรับการถอดรหัสข้อมูลจะเท่ากับ $k(1+x)P$ โดยที่ k เป็นจำนวนแพ็กเก็ตต้นฉบับ l เป็นจำนวนแพ็กเก็ตพิเศษที่ต้องการสร้าง x เป็นจำนวนแพ็กเก็ตต้นฉบับที่ผู้รับไม่ได้รับ และ P เป็นขนาดของแพ็กเก็ต ในการถอดรหัสแพ็กเก็ตเพื่อกู้คืนแพ็กเก็ตต้นฉบับ ผู้รับจะต้องได้รับแพ็กเก็ตต้นฉบับและแพ็กเก็ตพิเศษเป็นจำนวนรวมกันอย่างน้อยเท่ากับจำนวนแพ็กเก็ตต้นฉบับทั้งหมด (Blomer *et al.*, 1995)

เมทริกซ์แบบ Cauchy Matrices เป็นเมทริกซ์ที่มีขนาด $m * n$ ดังนั้นการพัฒนา FEC ด้วย Cauchy Matrices จะเปรียบแพ็กเก็ตต้นฉบับและแพ็กเก็ตพิเศษได้กับเซตของข้อมูลจำนวน 2 เซต ได้แก่ เซต $X = \{x_1, x_2, x_3, \ldots, x_m\}$ และเซต $Y = \{y_1, y_2, y_3, \ldots, y_n\}$ โดย X เป็นเซตของแพ็กเก็ตต้นฉบับ และ Y เป็นเซตของแพ็กเก็ตพิเศษ ข้อมูลทั้ง 2 เซต จะถูกนำมาจัดให้อยู่ในรูปของเมทริกซ์ดังภาพที่ 6 การสร้างแพ็กเก็ตพิเศษจะกระทำโดยใช้ Exclusive-Or ซึ่งสัญลักษณ์ + ที่ปรากฏในภาพที่ 6 เป็นสัญลัษณ์ของการทำ Exclusive-Or ระหว่างแพ็กเก็ตต้นฉบับและแพ็กเก็ตพิเศษ

$$\begin{bmatrix} \frac{1}{x_1+y_1} & \frac{1}{x_1+y_2} & \cdots & \frac{1}{x_1+y_n} \\ \frac{1}{x_2+y_1} & \frac{1}{x_2+y_2} & \cdots & \frac{1}{x_2+y_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{x_m+y_1} & \frac{1}{x_m+y_2} & \cdots & \frac{1}{x_m+y_n} \end{bmatrix}$$

ภาพที่ 6 ลักษณะของ Cauchy Matrices
ที่มา: Blomer *et al*., (1995)

ลักษณะของเมทริกซ์แบบ Vandermonde Matrices เป็นเมทริกซ์ขนาด n * n การพัฒนา FEC ด้วย Vandermonde Matrices จะเปรียบแพ็กเก็ตต้นฉบับและแพ็กเก็ตพิเศษได้กับเซตของจำนวน 1 เซต ตัวอย่างเช่น เซต $X = \{x_1, x_2, x_3, \ldots, x_n\}$ ข้อมูลในเซตจะถูกนำมาจัดให้อยู่ในรูปของเมทริกซ์ดังภาพที่ 7 หลังจากนั้นจะนำมาผ่านกระบวนการหาค่าดิเทอร์มินัลของแต่ละเมทริกซ์ และ Exclusive-Or เพื่อสร้างแพ็กเก็ตพิเศษ

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ 1 & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{bmatrix}$$

ภาพที่ 7 ลักษณะของ Vandermonde Matrices
ที่มา: Byer *et al*., (1997)

Byers *et al*., (1998) ได้วัดประสิทธิภาพเวลาที่ใช้ในการประมวลผลสำหรับการเข้ารหัสข้อมูลและการถอดรหัสข้อมูลของวิธีการ Forward Error Correcting (FEC) แบบ Reed-Solomon Codes ที่พัฒนาด้วย Vandermonde Matrices และ Cauchy Matrices โดยมีการทำงานบนเครื่อง Sun รุ่น Ultra SPARC1 หน่วยประมวลผลความเร็ว 167 เมกะเฮิร์ต หน่วยความจำหลักขนาด 64 เมกะไบต์ ระบบปฏิบัติการ Solaris 2.5.1 และกำหนดขนาดของแพ็กเก็ตเท่ากับ 1 กิโลไบต์ ผลการวัดประสิทธิภาพแสดงตามตารางที่ 4

ตารางที่ 4 เวลาที่ใช้ในการเข้ารหัสและถอดรหัสด้วย Reed-Solomon Codes: หน่วยเป็นวินาที

ขนาด	การเข้ารหัส		การถอดรหัส	
	Vandermonde	Cauchy	Vandermonde	Cauchy
250 กิโลไบต์	9	4.6	11	2.06
500 กิโลไบต์	39	19	32	8.4
1 เมกะไบต์	150	93	161	40.5
2 เมกะไบต์	623	442	1147	199
4 เมกะไบต์	ไม่มีผลทดลอง	1717	ไม่มีผลทดลอง	300
8 เมกะไบต์	ไม่มีผลทดลอง	6994	ไม่มีผลทดลอง	3166
16 เมกะไบต์	ไม่มีผลทดลอง	30802	ไม่มีผลทดลอง	13629

ที่มา: Byers *et al*., (1998)

จากตารางแสดงให้เห็นว่าเวลาที่ใช้ในการเข้ารหัสและถอดรหัสข้อมูล จากการพัฒนาด้วย Cauchy Matrices นั้นใช้เวลาในการประมวลผลน้อยกว่าการพัฒนาด้วย Vandermonde Matrices ประมาณหนึ่งเท่า และยังแสดงให้เห็นว่าการเข้ารหัสข้อมูลของทั้งสองวิธีการพัฒนา จะใช้เวลาเพิ่มขึ้นประมาณ 4 เท่า ของทุกๆ ขนาดข้อมูลต้นฉบับที่เพิ่มขึ้นสองเท่า Blomer *et al*., 1995 ได้เผยแพร่ชุดคำสั่งที่ใช้ในวิธีการ FEC แบบ Reed-Solomon Codes ที่พัฒนาด้วย Cauchy Matrices ในส่วนของเข้ารหัสข้อมูลจะประกอบไปด้วยขั้นตอนการสร้างแพ็กเก็ตต้นฉบับจากการอ่านข้อมูลจากไฟล์ข้อมูล และสร้างแพ็กเก็ตพิเศษจากแพ็กเก็ตต้นฉบับที่ได้เตรียมไว้ โดยมีชุดคำสั่งที่แสดงการเข้ารหัสข้อมูลเพื่อสร้างแพ็กเก็ตพิเศษดังภาพที่ 8

```
/* The variables that are defined prior to computing the redundant
   packets are:

MultField : The size of the multiplicative group of the finite
field.
ExptoFieldElt : A table that goes from the exponent of an element,
in terms of a previously chosen generator of the multiplicative
group, to its representation as a vector over GF(2).
FieldEltToExp : The table that goes from the vector representation
of an element to its exponent of the generator.
Bit : An arry of integers that is used to select individual bits: (A
& Bit[i]) is equal to 1 if the i-th Bit of A is 1, and o otherwise.
*/

/* The number of rows in Cauchy matirc is equal to the number of
redundant packets. */
For row = 0 to Rpacket-1

   /* The number of columns in Cauchy matrix is equal to the number
      of information packets. */
   For col = 0 to Mpackets-1

      /* exponent is the multiplicative exponent of the element of
         the Cauchy matrix we are currently looking at. XOR
         computes the coordinatewise exclusive-or of the bit
         representation of two integers. % is the remainder
         operator. */
      exponent = (MultField -
                  FieldEltToExp[row XOR col XOR Bit[Lfiled-1]]) %
                  MultField

      /* Each element of finite field is now represented as a
         Lfield by Lfield 0-1 matrix. */
      For row_bit = 0 to Lfield-1

         /* Check if the current bit of the matrix element is 1. */
         If (ExpToFieldElt[exponent+row_bit] & [Bit[col_bit])
            For segment = 0 to Nsegs-1

               /* (a^=b) is short of (a = a XOR b). */
               redundant_packets[row][segment+row_bit*Nsegs] ^=
               message[segment+col_bit*Nsegs+col*Lfield*Nsegs]
```

ภาพที่ 8 ขั้นตอนการเข้ารหัสข้อมูลแบบ Reed-Solomon Codes ด้วย Cauchy Matrices

ที่มา: Blomer *et al*., (1995)

การถอดรหัสข้อมูลทางด้านผู้รับจะประกอบด้วยขั้นตอนการตรวจสอบจำนวนแพ็กเก็ตต้นฉบับที่ไม่ได้รับเพื่อคำนวณหาจำนวนแพ็กเก็ตพิเศษที่ต้องใช้ในการถอดรหัสข้อมูล เมื่อแพ็กเก็ตที่ไม่ซ้ำกันมีจำนวนเพียงพอต่อการถอดรหัสข้อมูลจึงถอดรหัสข้อมูลเพื่อสร้างไฟล์ข้อมูล โดยมีชุดคำสั่งในการถอดรหัสข้อมูลแสดงดังภาพที่ 9

```
/* The variables FieldEltToExp, MulField and MultField are as
   described in the encoding algorithm.

The following variables are computed in the decoding routine before
the marix inversion step is called:

RowInd : An array that keeps track of the extra packets received:
RowInd[i] is the identifier of the i-th extra packet that was
received.
ColInd : An array that keeps track of the message packets received:
ColInd[i] is the identifier of the i-th message packet that was
received.
M : The submatrix of the original Cauchy matrix.
RecMsg : The array where the message is to be stored. The information
contained in the Message packets that were received has already been
copied to this array.
*/

For row = 0 to Rpackets -1
   For col = 0 to Mpackets -1

      /* != is the Not-Equal operator. */
      If (col != row)

         /* (a+=b) is short for (a = a+b) */
         C[row] += FieldEltToExp[RowInd[row] XOR RowInd[col]]
         D[col] += FieldEltToExp[ColInd[row] XOR ColInd[col]]

      E[row] += FieldEltToExp[RowInd[row] XOR ColInd[col] XOR
                Bit[Lfield-1]]
      F[col] += FieldEltToExp[RowInd[row] XOR ColInd[col] XOR
                Bit[Lfield-1]]

For row = 0 to Nextra-1
   For col = 0 to Nextra -1
      InvMat[row][col] = E[col] + F[row] - C[col] - D[row] -
                         FieldEltToExp[RowInd[col] XOR
                         ColInd[row] XOR Bit[Lfield-1]]
      If (InvMat[row][col] >= 0)
         InvMat[row][col] = InvMat[row][col] % MultField
      Else
         InvMat[row][col] = (MultField - ((-InvMat[row][col] %
                             MultField)) % MultField
```

ภาพที่ 9 ขั้นตอนการถอดรหัสข้อมูลแบบ Reed-Solomon Codes ด้วย Cauchy Matrices

ที่มา: Blomer *et al*., (1995)

```
For row = 0 to Rpackets -1
   For col = 0 to Mpackets -1

      /* If the message packet was received, then process it. */
      If (RecIndex[col] == 1)
         exponent = (Multfield - FieldEltToExp[RowInd[row] XOR
                     col XOR Bit[Lfield-1]]) % MultField
         For row_bit = 0 to Lfield-1
            For col_bit = 0 to Lfield-1
               If (ExpToFieldElt[exponent+row_bit] & Bit[col_bit])
                  For segment =0 to Nsegs-1
                     M[row_bit+row*[Lfield][segment] ^=
                     RecMsg[segment+col_bit*Nsegs+col*Lfield*Nsegs]

For row = 0 to Rpackets -1
   For col = 0 to Mpackets -1
      exponent = InvMat[row][col]

      For row_bit = 0 to Lfield-1
         For col_bit = 0 to Lfield-1
            If (ExpToFieldElt[exponent+row_bit] & Bit[col_bit])
               For segment = 0 to Nsegs-1
                  RecMsg[segment+row_bit*Nsegs+ColInd[row]
                  *Lfield*Nsegs] ^= M[col_bit+col*Lfield][segment]
```

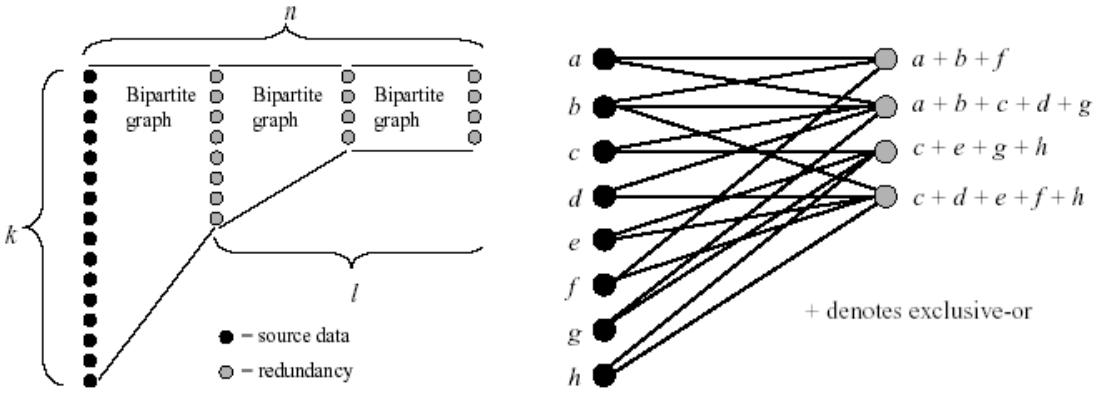
ภาพที่ 9 ต่อ

3.3.2 Tornado Codes (Luby *et al*., 1997)

การเข้ารหัสข้อมูลและการถอดรหัสข้อมูลของ Tornado Codes จะสร้างแพ็กเก็ตต้นฉบับและแพ็กเก็ตพิเศษให้อยู่ในรูปแบบของกราฟคู่ที่เรียกว่า Bipartite Graph โดยใช้วิธีการสุ่มแพ็กเก็ตมาผ่านกระบวนการ Exclusive-Or ซึ่งเป็นคำสั่งที่ใช้เวลาในการประมวลผลน้อย จึงทำให้ Tornado Codes เป็นอัลกอริทึม FEC ที่ใช้เวลาในการประมวลผลสำหรับการเข้ารหัสข้อมูลและการถอดรหัสข้อมูลน้อยกว่าการ FEC แบบ Reed-Solomon Codes ซึ่งมีลักษณะของกราฟตามภาพที่ 10

จากภาพที่ 10 สัญญลักษณ์ ● และ ◯ แสดงถึงโหนดซึ่งเป็นแพ็กเก็ตต้นฉบับและแพ็กเก็ตพิเศษ ตามลำดับ ในขั้นตอนการเข้ารหัสข้อมูลจะทำสุ่มแพ็กเก็ตต้นฉบับที่แสดงเป็นเส้นกราฟแนวตั้งด้านซ้ายมาผ่านกระบวนการ Exclusive-Or เพื่อสร้างแพ็กเก็ตพิเศษ โดยจะแสดงตามเส้นกราฟแนวตั้งเส้นถัดมา จากนั้นจะสุ่มแพ็กเก็ตพิเศษ และนำมาผ่านกระบวนการ Exlusive-Or อีกครั้ง เป็นการสร้างแพ็กเก็ตพิเศษแบบลำดับชั้น จำนวนแพ็กเก็ตพิเศษที่ได้จากการเข้ารหัสแต่ละรอบจะมีจำนวนน้อยกว่าหรือเท่ากับครึ่งหนึ่งของจำนวนแพ็กเก็ตที่นำมาใช้ในเข้ารหัสข้อมูล

เวลาที่ใช้ในการประมวลผลสำหรับการเข้ารหัสข้อมูลและการถอดรหัสข้อมูลจะเป็นสัดส่วนกับจำนวนของแพ็กเก็ตต้นฉบับ ซึ่งจะมีค่าเท่ากับ $(k+l)\ln(1/\varepsilon)P$ โดยที่ k เป็นจำนวนแพ็กเก็ตต้นฉบับ l เป็นจำนวนแพ็กเก็ตพิเศษที่ต้องการสร้าง P เป็นขนาดของแพ็กเก็ต และ ε คือค่า Reception overhead สำหรับการกู้คืนแพ็กเก็ตต้นบับที่สูญหายเพื่อสร้างไฟล์ข้อมูลต้นฉบับนั้นทางผู้รับจำเป็นต้องได้รับแพ็กเก็ตจำนวนที่มากเพียงพอ ผู้รับจะต้องได้รับแพ็กเก็ตจำนวนอย่างน้อยเท่ากับ $(1+\varepsilon)k$ โดยปกติค่า ε จะมีค่ามากกว่า 0



ภาพที่ 10 โครงสร้างการเข้ารหัสและถอดรหัสข้อมูลแบบ Tornado Codes
ที่มา: Luby *et al*., (1997)

Byers *et al*., (1998) ได้สรุปคุณสมบัติของวิธีการ FEC แบบ Tornado Codes และ Reed-Solomon Codes ตามตารางที่ 5 แสดงให้เห็นว่าเวลาที่ใช้ในการประมวลผลสำหรับการเข้ารหัสและถอดรหัสข้อมูลด้วยวิธีการ FEC แบบ Tornado Codes มีความเร็วสูงกว่าวิธีการ FEC แบบ Reed-Solomon Codes แต่มีจุดด้อยในด้านการถอดรหัสข้อมูลเนื่องจากผู้รับจำเป็นจะต้องรับข้อมูลได้อย่างน้อยเท่ากับจำนวนแพ็กเก็ตต้นฉบับบวกด้วยค่า Reception overhead หรือค่า ε

ตารางที่ 5 เปรียบเทียบคุณสมบัติของวิธีการ FEC แบบ Reed-Solomon codes และ Tornado Codes

	Reed-Solomon Codes	**Tornado Codes**
Packet Required	k	$(1+\varepsilon)k$
Encoding times	$k(1+l)P$	$(k+l)\ln(1/\varepsilon)P$
Decodeing times	$k(1+x)P$	$(k+l)\ln(1/\varepsilon)P$
Basic operation	Complex filed operation	Simple XOR

ที่มา: Byers *et al*., (1998)

Byers *et al*., (1998) ได้แสดงการเปรียบเทียบตัวอย่างเวลาที่ใช้ในการประมวลสำหรับการเข้ารหัสและการถอดรหัสข้อมูลของวิธีการ FEC แบบ Reed-Solomon Codes ที่พัฒนาด้วย Cauchy Matrices และวิธีการ FEC แบบ Tornado Codes โดยมีการทำงานบนเครื่อง Sun รุ่น Ultra SPARC1 หน่วยประมวลผลความเร็ว 167 เมกะเฮิร์ต หน่วยความจำหลักขนาด 64 เมกะไบต์ ระบบปฏิบัติการ Solaris 2.5.1 และกำหนดขนาดของแพ็กเก็ตเท่ากับ 1 กิโลไบต์ ซึ่งผลที่ได้แสดงตามตารางที่ 6 โดยจะเห็นว่าความแตกต่างด้านเวลาที่ใช้ในการประมวลผลสำหรับการเข้ารหัสข้อมูลและถอดรหัสข้อมูล จะสูงขึ้นเมื่อขนาดของไฟล์ข้อมูลมีขนาดสูงขึ้น

ตารางที่ 6 เปรียบเทียบเวลาที่ใช้ในการเข้ารหัสและถอดรหัสด้วย Reed-Solomon Codes (Cauchy Matrices) และ Tornado Codes : หน่วยเป็นวินาที

ขนาดไฟล์ข้อมูล	การเข้ารหัส		การถอดรหัส	
	RS-Cauchy	Tornado Codes	RS-Cauchy	Tornado Codes
250 กิโลไบต์	4.6	0.06	2.06	0.06
500 กิโลไบต์	19	0.12	8.4	0.09
1 เมกะไบต์	93	0.26	40.5	0.14
2 เมกะไบต์	442	0.53	199	0.19
4 เมกะไบต์	1717	1.06	300	0.40
8 เมกะไบต์	6994	2.13	3166	0.87
16 เมกะไบต์	30802	4.33	13629	1.75

ที่มา: Byers *et al*., (1998)

4. การควบคุณภาพการให้บริการ

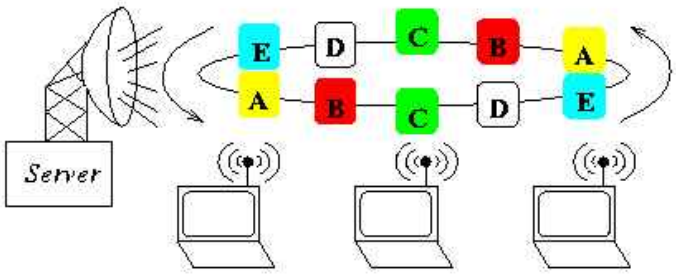
4.1 บรอดคาสต์ดิสค์ (Broadcast Disk)

ในการบริการส่งข้อมูลแบบไคลน์เอนท์-เซิร์ฟเวอร์โดยทั่วไปไคลน์เอนท์ซึ่งเป็นผู้รับข้อมูลจะส่งคำร้องขอข้อมูลไปยังเซิร์ฟเวอร์ซึ่งเป็นผู้ส่งข้อมูล ซึ่งการทำงานในลักษณะนี้จะเป็นการทำงานในรูปแบบของ Pull Model ผู้รับจำเป็นต้องมีความสามารถในการส่งข้อมูล จึงเป็นสิ่งที่ไม่สามารถเกิดขึ้นได้ในการทำงานบนช่องสัญญาณการสื่อสารแบบทิศทางเดียว Acharya *et al*. (1995) ได้เสนอวิธีการให้บริการข้อมูลที่มีลักษณะการสื่อสารแบบทิศทางเดียว เรียกว่า บรอดคาสต์ดิสค์ (Broadcast Disk) ซึ่งช่องทางการไหลของข้อมูลที่ถูกส่งไปยังผู้รับจะถูกเรียกว่า ดิสค์ (Disk) สิ่งที่แตกต่างกันระหว่างการส่งข้อมูลแบบบรอดคาสต์ดิสค์กับการส่งข้อมูลแบบบรอดคาสต์และแบบมัลติคาสต์ คือ การส่งข้อมูลแบบบรอดคาสต์ดิสค์จะมีการส่งข้อมูลมากกว่าหนึ่งดิสค์ ซึ่งสามารถกำหนดความเร็วในการส่งข้อมูลที่แตกต่างกันได้ในแต่ละดิสค์ เพื่อใช้ในการปรับความเร็วให้เหมาะสมกับความต้องการของข้อมูล หรือใช้ในการสร้างลำดับชั้นของความเร็วในการส่งข้อมูล

ที่เหมาะสมกับความสามารถในการรับข้อมูลของผู้รับซึ่งมีความสามารถในการรับข้อมูลที่มีความเร็วแตกต่างกัน

การส่งข้อมูลแบบบรอดคาสต์ดิสค์จะต้องกำหนดจำนวนของดิสค์และอัตราส่วนความเร็วในการส่งแพ็กเก็ตของไฟล์ข้อมูลที่อยู่ในแต่ละดิสค์ไว้ล่วงหน้า ผู้ส่งจะเตรียมไฟล์ข้อมูลที่ผู้รับต้องการ ซึ่งอาจได้จากการสอบถามผ่านช่องทางการสื่อสารอื่น เช่น โทรศัพท์ และจัดเก็บไว้ในดิสค์ที่มีอัตราความเร็วในการส่งข้อมูลเหมาะสมกับระดับความสำคัญของไฟล์ข้อมูลหรือจำนวนความต้องการของไฟล์ข้อมูลนั้นๆ ที่ได้รับมาจากการสอบถามดังกล่าว

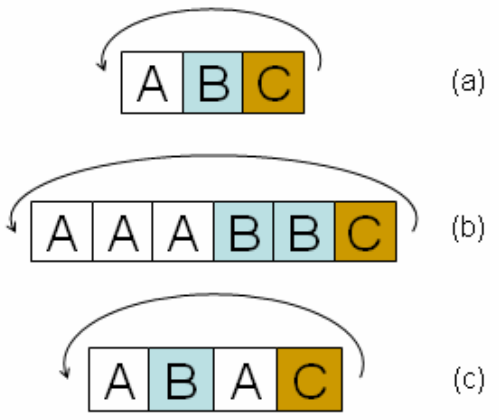
การทำงานของบรอดคาสต์ดิสค์ในรูปแบบ Flat ดังภาพที่ 11 แสดงถึงดิสค์ที่เก็บไฟล์ข้อมูลจำนวน 5 ดิสค์ ได้แก่ A B C D และ E การส่งข้อมูลจะเป็นการส่งแพ็กเก็ตของไฟล์ข้อมูลหนึ่งแพ็กเก็ต สลับกันไปในแต่ละดิสค์ และจะวนซ้ำเพื่อส่งแพ็กเก็ตในแต่ละดิสค์อย่างต่อเนื่อง การส่งข้อมูลในรูปแบบ Flat นี้ทุกดิสค์จะมีอัตราส่วนความเร็วในการส่งข้อมูลที่เท่ากัน ซึ่งแสดงให้เห็นว่าแต่ละไฟล์ข้อมูลมีความสำคัญเท่ากัน การส่งข้อมูลแบบบรอดคาสต์ดิสค์ในรูปแบบ Flat เป็นการดัดแปลงมาจากการส่งข้อมูลแบบวนซ้ำที่เสนอโดย Imielinski *et al.*, (1994) แต่อย่างไรก็ตามผู้ส่งสามารถกำหนดความเร็วในการส่งข้อมูลของแต่ละดิสค์ให้มีความเร็วแตกต่างกันได้ ดังนั้นจึงมีรูปแบบการส่งข้อมูลในรูปแบบอื่นเกิดขึ้นเรียกว่าแบบ Skewd และแบบ Multi-disk



ภาพที่ 11 ตัวอย่างการส่งข้อมูลแบบบรอดคาสต์ดิสค์ในรูปแบบ Flat
ที่มา: Achary *et al.*, (1995)

จากภาพ 12(a) เป็นตัวอย่างการส่งข้อมูลแบบ Flat ประกอบด้วยดิสค์ที่เก็บไฟล์ข้อมูลจำนวน 3 ดิสค์ ได้แก่ A B และ C ซึ่งมีลักษณะการส่งข้อมูลดังที่ได้กล่าวไว้ข้างต้น รูปแบบในภาพ 12(b) เรียกว่า Skewed เป็นการส่งแพ็กเก็ตของไฟล์ข้อมูลที่อยู่ในดิสค์ A B และ C ในสัดส่วนที่

แตกต่างกันโดยส่งแพ็กเก็ตของไฟล์ข้อมูลในดิสค์เดียวกันต่อเนื่องกัน สัดส่วนของจำนวนแพ็กเก็ตในแต่ละดิสค์ที่ส่งในหนึ่งช่วงเวลาเป็นการกำหนดอัตราความเร็วในการส่งและความสำคัญของไฟล์ข้อมูลที่อยู่ในแต่ละดิสค์ รูปแบบในภาพ 12(c) เรียกว่า Multi-disk เป็นการส่งแพ็กเก็ตของไฟล์ข้อมูลในดิสค์ A B และ C สลับกันและมีสัดส่วนที่แตกต่างกัน แต่ละไฟล์ข้อมูลจะมีช่วงเวลาที่แน่นอนในการส่งข้อมูล 1 แพ็กเก็ต จากที่กล่าวมารูปแบบการส่งข้อมูลที่สามารถปรับอัตราความเร็วในการส่งข้อมูลของแต่ละดิสค์ไม่เท่ากัน จะใช้ได้เพียง 2 รูปแบบ คือ Skewed และ Multi-disk ซึ่งการส่งข้อมูลแบบบรอดคาสต์ดิสค์ในรูปแบบ Skewed จะมีจุดด้อยในเรื่องของการคำนวณรอบระยะเวลา (periodic) การมาถึงของแพ็กเก็ตถัดไปสำหรับไฟล์ข้อมูลนั้น แต่ความสามารถนี้มีในรูปแบบ Multi-disk ซึ่งจะทำให้ผู้รับสามารถคำนวณเวลาในการรับแพ็กเก็ตถัดไปได้



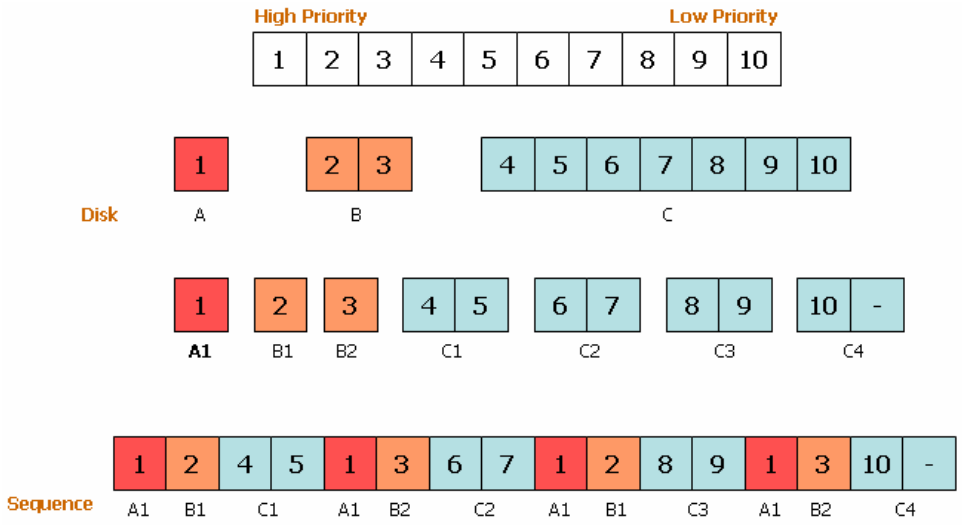
ภาพที่ 12 ตัวอย่างโครงสร้างการบรอดคาสต์ดิสค์
ที่มา: Achary *et al*., (1995)

Achary *et al*., (1995) ได้นำเสนอวิธีการสร้างตารางลำดับการส่งแพ็กเก็ตของไฟล์ข้อมูลด้วยวิธีการบรอดคาสต์ดิสค์ในรูปแบบ Multi-disk โดยอัลกอริทึมในการสร้างตารางลำดับการส่งไฟล์ข้อมูลมีขั้นตอนการทำงานดังนี้

1. จัดเรียงลำดับความสำคัญของไฟล์ข้อมูลจากมากไปหาน้อย
2. แบ่งกลุ่มไฟล์ข้อมูลออกเป็นดิสค์ โดยกำหนดเป็นช่วงของอัตราความสำคัญ
3. กำหนดอัตราความเร็วในการส่งข้อมูลแต่ละดิสค์ เช่น ดิสค์ที่หนึ่งมีความถี่ในการส่งข้อมูลเท่ากับ 4 ดิสค์ที่สองมีความถี่ในการส่งข้อมูลเท่ากับ 2 และดิสค์หนึ่งมีความถี่ในการส่งข้อมูลเท่ากับ 1 เป็นต้น

4. แบ่งไฟล์ข้อมูลในแต่ละดิสค์ออกเป็นกลุ่มย่อย

5. จัดลำดับการส่งแพ็กเก็ตของไฟล์ข้อมูลโดยใช้วิธีการเลือกไฟล์ข้อมูลครั้งละหนึ่งกลุ่มย่อยที่อยู่แต่ละดิสค์ โดยเริ่มจากดิสค์ที่หนึ่งจนถึงดิสค์สุดท้าย และวนกลับมาเลือกกลุ่มย่อยถัดไปในดิสค์ที่หนึ่งจนถึงดิสค์สุดท้าย เป็นเช่นนี้จนครบทุกกลุ่ม



ภาพที่ 13 ตัวอย่างการสร้างตารางการบรอดคาสต์ดิสค์ในรูปแบบ Multi-disk
ที่มา: Achary *et al*., (1995)

ภาพที่ 13 แสดงตัวอย่างการสร้างตารางการส่งไฟล์ข้อมูลแบบบรอดคาสต์ดิสค์ในรูปแบบ Multi-disk โดยไฟล์ข้อมูลจะถูกเรียงลำดับความสำคัญของข้อมูลจากมากไปน้อย และแบ่งกลุ่มของไฟล์ข้อมูลไว้บนดิสค์ทั้งหมด 3 ดิสค์ ได้แก่ A B และ Cโดยใช้การกำหนดช่วงของอัตราความสำคัญของไฟล์ข้อมูล จากนั้นแบ่งกลุ่มของไฟล์ข้อมูลในแต่ละดิสค์ออกเป็นกลุ่มย่อย จากภาพแสดงให้เห็นว่าไฟล์ข้อมูลที่อยู่ในดิสค์ A มีหนึ่งกลุ่ม คือไฟล์หมายเลข 1 ไฟล์ข้อมูลที่อยู่ในดิสค์ B ถูกแบ่งออกเป็นกลุ่มละหนึ่งไฟล์ คือ ไฟล์หมายเลข 2 และไฟล์หมายเลข 3 ในดิสค์ C ถูกแบ่งออกเป็นกลุ่มจำนวน 4 กลุ่ม แต่ละกลุ่มมีจำนวน 2 ไฟล์ คือ (4,5) (6,7) (7,8) (8,9) และ (10, -) ในกลุ่มสุดท้ายของดิสค์ C มีไฟล์ข้อมูลเพียง 1 ไฟล์ คือไฟล์ข้อมูลหมายเลข 10 ดังนั้นจึงสร้างช่องว่างที่ไม่มีการส่งไฟล์ข้อมูลใด Achary *et al*., (1995) เสนอให้ใช้ช่องว่างนี้ในการส่งข้อมูลเพื่อแจ้งข่าวสารต่างๆ และในขั้นตอนสุดท้ายจัดลำดับการส่งแพ็กเก็ตของไฟล์ข้อมูลโดยใช้วิธีการเลือกไฟล์จากกลุ่มย่อยทีละกลุ่มในแต่ละดิสค์สลับกันไปและวนซ้ำ

4.2 การควบคุมการไหลและความคับคั่งของข้อมูล (Flow and Congestion Control) (Jacobson, 1998)

การควบคุมการไหลของข้อมูลเป็นการควบคุมการส่งข้อมูลให้เกิดการใช้ประโยชน์จากเครือข่ายสูงสุด ส่วนด้านการควบคุมความคับคั่งของข้อมูลนั้นเป็นการควบคุมไม่ให้ข้อมูลถูกส่งออกไปยังเครือข่ายมากเกินแบนวิดธ์ที่เครือข่ายจะรับได้ วิธีที่เป็นที่นิยมในการควบคุมการไหลและความคับคั่งของข้อมูลนั้น ได้แก่ การควบคุมตามขนาดหน้าต่างรับข้อมูลของผู้รับ (Window-Based) (RFC 813, 1982) และการควบคุมตามอัตราความคับคั่งบนระบบเครือข่าย (Rate-Based) (Jain *et al*., 1987)

สำหรับวิธีการควบคุมการไหลและความคับคั่งของข้อมูลแบบ Window-Based นั้น ผู้รับจะประกาศขนาดหน้าต่างรับข้อมูลของตัวเองไปยังผู้ส่ง ขนาดหน้าต่างรับข้อมูลนี้เป็นตัวที่แสดงให้ทราบถึงขนาดของหน่วยความจำที่ใช้สำหรับจัดเก็บข้อมูลที่ผู้รับจะสามารถรับได้จากผู้ส่งในช่วงเวลาหนึ่ง โดยผู้รับจะส่งข้อมูลนี้ไปกับ ACK แพ็กเก็ต ส่วนวิธีการควบคุมการไหลและความคับคั่งของข้อมูลแบบ Rate-Based นั้นเป็นการปรับอัตราความเร็วในการส่งข้อมูลแพ็กเก็ต โดยผู้ส่งจะใช้วิธีการสำรวจความคับคั่งของเครือข่าย เพื่อใช้เป็นข้อมูลในการปรับอัตราความเร็ว

งานวิจัยที่เกี่ยวข้อง

มีงานวิจัยเกี่ยวกับการสร้างความน่าเชื่อถือในการมัลติคาสต์มากมายที่ถูกพัฒนา ซึ่งแต่ละงานวิจัยก็ใช้วิธีที่แตกต่างกันไป โดยสามารถแบ่งลักษณะการทำงานของงานวิจัยต่างๆ ได้ 3 กลุ่ม ซึ่งกลุ่มแรกจะเป็นการใช้กลไกการตอบกลับจากผู้รับด้วย ACK และ/หรือ NACK ในการสร้างความน่าเชื่อถือ กลุ่มที่สองสร้างความน่าเชื่อถือด้วยการใช้วิธีการ FEC และกลุ่มสุดท้าย เป็นการนำวิธีการของ 2 กลุ่มแรกมารวมกัน (Hybrid) ตัวอย่างงานวิจัยในการสร้างความน่าเชื่อถือได้แก่

John *et al*., (1996) เสนอ RMTP (Reliable Multicast Transport Protocol) มีการจัดการด้านความน่าเชื่อถือของข้อมูลสำหรับการบริการส่งข้อมูลแบบมัลติคาสต์ด้วยการใช้ข้อความตอบกลับจากผู้รับ โดยผู้ส่งจะเลือกส่งซ้ำเฉพาะแพ็กเก็ตที่เกิดการสูญหาย โปรโตคอลนี้มีแนวความคิดหลักคือการรวมกลุ่มของผู้รับที่อยู่ในพื้นที่เดียวกัน ดังนั้นจึงมีโครงสร้างเครือข่ายในกลุ่มผู้รับข้อมูลเป็นแบบลำดับชั้น (hierarchy) จะมีผู้รับพิเศษหนึ่งรายเป็นตัวแทนกลุ่มผู้รับเรียกว่า Designated Receiver (DR) ทำหน้าที่เป็นตัวแทนในการส่งข้อความตอบกลับการไม่ได้รับข้อมูลของผู้รับในกลุ่มตนเองไปยังผู้ส่ง เพื่อให้ผู้ส่งส่งข้อมูลที่สูญหายมาอีกครั้ง ข้อความตอบกลับการไม่ได้รับข้อมูลจะถูกส่งจากผู้รับที่ทำหน้าที่เป็น DR ของกลุ่ม ดังนั้นสำหรับหนึ่งแพ็กเก็ตจะมีเพียงหนึ่งข้อความตอบกลับจากผู้รับหนึ่งกลุ่ม ซึ่งวิธีการนี้เป็นการลดปัญหา NACK Implosion ที่จะเกิดขึ้นที่ด้านผู้ส่ง โปรโตคอลนี้ยังสนับสนุนการทำงานแบบลำดับชั้นมากกว่าหนึ่งลำดับชั้น โดยตัวแทนกลุ่มที่อยู่ในระดับสูงกว่าจะทำหน้าที่ติดต่อกับผู้ส่งแทนตัวแทนกลุ่มที่อยู่ในระดับล่างของกลุ่มตนเอง อีกทั้งยังสนับสนุนการร้องขอข้อมูลจากผู้รับในเวลาที่แตกต่างกัน อาจเกิดจากการเชื่อมต่อเน็ตเวิร์คของผู้รับในเวลาที่แตกต่างกัน โดยผู้รับที่เป็นตัวแทนกลุ่มจะใช้ข้อมูลที่อยู่ในแคชของตนส่งให้กับผู้รับใหม่ที่ร้องขอข้อมูล

Rizzo *et al*., (1997) เสนอ RMDP (Reliable Multicast data Distribution Protocol) เป็นการให้บริการส่งข้อมูลแบบมัลติคาสต์ที่ใช้ช่องสัญญาณการสื่อสารแบบ 2 ทิศทาง โดยมีกระบวนการสร้างความน่าเชื่อถือด้วยวิธีการ FEC แบบ Reed-Solomon Codes ที่พัฒนาด้วย Vandermonde Matrices และสนับสนุนการให้บริการส่งข้อมูลสำหรับกลุ่มของผู้รับที่มีความสามารถในการรับข้อมูลที่ความเร็วแตกต่างกัน โดยขั้นตอนพื้นฐานการทำงานของโปรโตคอลนี้จะเข้ารหัสแพ็กเก็ตต้นฉบับเพื่อให้ได้แพ็กเก็ตพิเศษ แพ็กเก็ตทั้งหมดจะถูกส่งเมื่อมีการร้องขอข้อมูลจากผู้รับ แพ็กเก็ตสามารถถูกส่งมากกว่าหนึ่งรอบเนื่องจากผู้รับบางรายที่มีความสามารถในการรับข้อมูลที่ความเร็ว

ต่ำมากจนทำให้ไม่สามารถรับแพ็กเก็ตได้มากเพียงพอจากการส่งข้อมูลเพียงหนึ่งรอบ วิธีการ FEC แบบ Reed-Solomon Codes ที่พัฒนาด้วย Vandermonde Matrices ไม่สามารถใช้งานได้กับข้อมูลที่มีขนาดใหญ่เกินไป เนื่องจากขนาดของข้อมูลต้นฉบับมีผลต่อความเร็วในการเข้ารหัสและถอดรหัสข้อมูล ดังนั้นจึงใช้วิธีแบ่งข้อมูลต้นฉบับออกเป็นส่วนย่อยเรียกว่า บล็อค (Block) และเข้ารหัสข้อมูลแต่ละบล็อค แพ็กเก็ตจากทุกบล็อคจะถูกส่งสลับกันโดยจะส่งแพ็กเก็ตต้นฉบับของแต่ละบล็อคจนครบและจึงส่งแพ็กเก็ตพิเศษ เมื่อข้อมูลถูกแบ่งออกเป็นบล็อคจึงเกิดข้อจำกัดขึ้นทางด้านผู้รับ เนื่องจากแพ็กเก็ตพิเศษของแต่ละบล็อคไม่สามารถใช้แทนกันได้ ซึ่งผู้รับจะต้องรับแพ็กเก็ตในแต่ละบล็อคให้ครบตามจำนวน k แพ็กเก็ต ซึ่งเป็นจำนวนแพ็กเก็ตต้นฉบับในแต่ละบล็อค Rizzo *et al*., (1997) ได้เสนอวิธีในการจัดการด้านการร้องขอข้อมูลอย่างง่ายในกรณีที่ผู้รับสามารถส่งข้อมูลไปยังผู้ส่งได้ โดยผู้รับจะส่งคำร้องขอข้อมูลโดยอาศัยการทำงานของโปรโตคอลไอจีเอ็มพีเป็นระยะ ซึ่งถือเป็นการแจ้งการเป็นสมาชิกในกลุ่มมัลติคาสต์ และผู้ส่งจะเริ่มส่งข้อมูลเมื่อตรวจสอบแล้วพบว่ามีสมาชิกในกลุ่มมัลติคาสต์รอรับข้อมูล และหยุดส่งเมื่อผู้ส่งตรวจสอบสถานะของผู้รับแล้วพบว่าไม่มีผู้รับรายใดรอรับข้อมูล แต่หากผู้ส่งหยุดส่งข้อมูลก่อนที่ผู้รับจะสามารถรับข้อมูลได้ครบ ผู้รับจะส่งคำร้องขอข้อมูลใหม่เพื่อให้ผู้ส่งส่งข้อมูลอีกครั้ง

Schooler *et al*. ,(1997) เสนอ Fcast (Filecasting) เป็นการให้บริการแบบมัลติคาสต์ที่ใช้ช่องสัญญาณการสื่อสารแบบ 2 ทิศทาง โดยมีการสร้างความน่าเชื่อถือด้วยวิธีการ FEC แบบ Reed-Solomon Codes ที่พัฒนาด้วย Vandermonde Matrices (Rizzo, 1997) และใช้วิธีการ Data Carousel โดยจะหยุดการส่งข้อมูลเมื่อตรวจสอบสถานะของผู้รับที่เป็นสมาชิกในกลุ่มมัลติคาสต์แล้วไม่พบว่ามีผู้รับรายใดรอรับข้อมูล ซึ่งการตรวจสอบนี้สามารถทำได้ด้วยโปรโตคอลไอจีเอ็มพี โดยผู้รับที่ต้องการรับข้อมูลจะส่งข้อความผ่านโปรโตคอลไอจีเอ็มพีเป็นระยะเพื่อแจ้งการเป็นสมาชิกกลุ่มมัลติคาสต์ และรอรับข้อมูลที่มัลติคาสต์ไอพีและพอร์ตที่ได้แจ้งการเป็นสมาชิกไว้ เนื่องจากวิธีการ FEC ที่ใช้เป็นแบบ Reed-Solomon Codes ซึ่งมีปัญหาด้านเวลาที่ใช้ในการประมวลผลสำหรับการเข้ารหัสและถอดรหัสข้อมูลกับข้อมูลที่มีขนาดใหญ่ จึงแก้ปัญหาด้วยการแบ่งข้อมูลออกเป็นส่วนเรียกว่า บล็อค (Block) สำหรับการส่งข้อมูลจะส่งแพ็กเก็ตของแต่ละบล็อคสลับกัน และในกรณีมีไฟล์ข้อมูลมากกว่าหนึ่งไฟล์จะส่งแพ็กเก็ตของแต่ละไฟล์ข้อมูลสลับกัน เมื่อแพ็กเก็ตต้นฉบับถูกส่งจนครบจากนั้นจึงส่งแพ็กเก็ตพิเศษ โดยโปรโตคอล Fcast มีการใช้เทคนิคมัลติเลเยอร์มัลติคาสต์ซึ่งมีลักษณะเช่นเดียวกับการทำบรอดคาสต์ดิสค์เพื่อกำหนดความเร็วในการส่งข้อมูลออกเป็นระดับต่างๆ ช่วยลดปัญหาคอขวดทางด้านผู้รับ ซึ่งมีสาเหตุมาจากความหลากหลายของชนิดของเครือข่ายทางด้านผู้รับ เช่น การเชื่อมต่อเครือข่ายด้วยโมเด็ม การเชื่อมต่อเครือข่ายแบบ

อีเทอร์เน็ต เป็นต้น โปรโตคอลนี้ใช้วิธีการแบ่งข้อมูลออกเป็นส่วนย่อยเพื่อช่วยเพิ่มประสิทธิภาพด้านเวลาที่ใช้ในการประมวลผลในการเข้ารหัสและถอดรหัสข้อมูล แต่กลับเป็นการลดประสิทธิภาพทางด้านผู้รับเช่นเดียวกับโปรโตคอล RMDP

Gemmell *et al*., (1997) เสนอ ECSRM (Erasure Correcting Scalable Reliable Multicast) เป็นการให้บริการข้อมูลแบบมัลติคาสต์ที่ใช้ช่องสัญญาณการสื่อสารแบบ 2 ทิศทาง ซึ่งเป็นงานที่พัฒนาต่อจาก SRM (Scalable Reliable Multicast) ที่นำเสนอโดย Floyd *et al*. ,(1995) พื้นฐานของ SRM มีการสร้างความน่าเชื่อถือด้วยการใช้ข้อความตอบกลับจากผู้รับ โดยทางด้านผู้รับจะส่ง NACK แพ็กเก็ตไปยังผู้ส่งเพื่อเป็นการบอกให้ผู้ส่งทราบว่าไม่ได้รับแพ็กเก็ตใด Gemmell *et al*., (1997) เสนอการพัฒนาต่อจาก SRM ด้วยการใช้ FEC แบบ Reed-Solomon Codes ที่พัฒนาด้วย Vandermonde Matrices (Rizzo, 1997) เข้ารหัสแพ็กเก็ตต้นฉบับ โดยแก้ปัญหาด้านเวลาที่ใช้ในการประมวลผลสำหรับการเข้ารหัสและถอดรหัสข้อมูลกับข้อมูลที่มีขนาดใหญ่โดยการแบ่งข้อมูลออกเป็นส่วน จากนั้นใช้แพ็กเก็ตที่ได้จากการเข้ารหัสข้อมูลส่งไปยังผู้รับแทนการส่งแพ็กเก็ตต้นฉบับที่สูญหายซ้ำ ซึ่งวิธีการนี้ทำให้ลดปริมาณการส่งแพ็กเก็ตซ้ำลงได้ เนื่องจากแพ็กเก็ตพิเศษหนึ่งแพ็กเก็ตสามารถนำมาถอดรหัสเพื่อใช้กู้คืนแพ็กเก็ตต้นฉบับใดๆ ได้หนึ่งแพ็กเก็ต Gemmell *et al*., (1997) ได้เสนอการปรับโครงสร้างของข้อความ NACK แพ็กเก็ตใหม่เนื่องจากการทำงานของ NACK แพ็กเก็ตใน SRM มีลักษณะเป็นแบบหนึ่งต่อหนึ่ง หมายถึง หนึ่งข้อความ NACK แพ็กเก็ตจะใช้สำหรับแจ้งให้ผู้ส่งส่งแพ็กเก็ตซ้ำหนึ่งแพ็กเก็ตซึ่งเป็นแพ็กเก็ตที่ผู้รับไม่ได้รับ Gemmell *et al*., (1997) ได้สังเกตว่าการสูญหายของแพ็กเก็ตที่เกิดขึ้นกับผู้รับแต่ละรายส่วนใหญ่จะไม่ซ้ำกัน ดังนั้นจึงเกิดการส่งข้อความ NACK เพื่อร้องขอแพ็กเก็ตซ้ำเป็นจำนวนมาก โครงสร้างของข้อความ NACK แพ็กเก็ตใน ECSRM จะบอกคู่ลำดับของหมายเลขบล็อคและจำนวนแพ็กเก็ตพิเศษที่ผู้รับต้องการ ตั้งแต่หมายเลขบล็อคแรกจนถึงหมายเลขบล็อคสุดท้าย ซึ่งทำให้จำนวน NACK แพ็กเก็ตที่ถูกส่งไปยังผู้ส่งมีจำนวนลดลง

Byers *et al*., (1998) เสนอ DF (Digital Fountain) เป็นการให้บริการแบบมัลติคาสต์ โดยมีกระบวนการสร้างความน่าเชื่อถือด้วยวิธีการ FEC แบบ Tornado Codes (Luby *et al*., 1997) ซึ่งเป็นวิธีการ FEC ที่มีประสิทธิภาพในการประมวลผลเพื่อเข้ารหัสและถอดรหัสข้อมูล และมีการจัดส่งข้อมูลแบบเลเยอร์มัลติคาสต์ (Layer Multicast) ซึ่งเป็นวิธีการที่สนับสนุนการส่งข้อมูลที่ความเร็วมากกว่าหนึ่งระดับเพื่อให้ผู้รับสามารถเลือกเป็นสมาชิกในระดับความเร็วที่เหมาะสมกับเครือข่ายของผู้รับ Byers *et al*., (1998) ได้ออกแบบให้ผู้รับสามารถรับข้อมูลในเลเยอร์มัลติคาสต์ล่างสุด

จนถึงเลเยอร์มัลติคาสต์ที่ผู้รับได้ลงทะเบียนเพื่อรับข้อมูล และแสดงตัวอย่างตารางการส่งข้อมูลแบบเลเยอร์มัลติคาสต์แบบ 4 เลเยอร์ ในตารางที่ 7 ซึ่งจะเริ่มจากเลเยอร์ที่ 0 ถึงเลเยอร์ที่ 3 โดยกำหนดให้แบนด์วิดธ์ในเลเยอร์ B_i มีขนาดเท่ากับ 2^{i-1} ในกรณีที่ i มีค่ามากกว่าหรือเท่ากับ 1 เมื่อ i เป็นหมายเลขของเลเยอร์ และแบนด์วิธด์มีค่าเท่ากับ 1 ในกรณีที่หมายเลขเลเยอร์มัลติคาสต์เป็น 0

ตารางที่ 7 ตารางการส่งแพ็กเก็ตสำหรับเลเยอร์มัลติคาสต์ 4 เลเยอร์

เลเยอร์	**แบนด์วิดธ์**	**การส่งแพ็กเก็ต**							
	ต่อรอบ	**รอบ 1**	**รอบ 2**	**รอบ 3**	**รอบ 4**	**รอบ 5**	**รอบ 6**	**รอบ 7**	**รอบ 8**
3	4	0-3	4-7	0-3	4-7	0-3	4-7	0-3	4-7
2	2	4-5	0-1	6-7	2-3	4-5	0-1	6-7	2-3
1	1	6	2	4	0	7	3	5	1
0	1	7	3	5	1	6	2	4	0

ที่มา : Byer et al., (1998)

เมื่อไฟล์ข้อมูลผ่านการเข้ารหัสข้อมูลเพื่อสร้างแพ็กเก็ตพิเศษแล้ว แพ็กเก็ตต้นฉบับและแพ็กเก็ตพิเศษจะถูกแบ่งของเป็นส่วนย่อยเรียกว่า บล็อค (Block) แต่ละส่วนย่อยจะมีจำนวนแพ็กเก็ตเท่ากับผลรวมแบนด์วิธด์จากทุกเลเยอร์ สำหรับการส่งข้อมูลแบบเลเยอร์มัลติคาสต์แบบ 4 เลเยอร์ ไฟล์ข้อมูลจะถูกส่งซ้ำเป็นจำนวน 8 รอบ แพ็กเก็ตในหนึ่งบล็อคจะถูกจัดลำดับจากแพ็กเก็ตลำดับที่ 0 ถึง B-1 โดยที่ B เท่ากับจำนวนแพ็กเก็ตในหนึ่งบล็อค การส่งข้อมูลในแต่ละรอบ แพ็กเก็ตในแต่ละบล็อคจะถูกส่งในเลเยอร์ที่กำหนดไว้ตามตารางที่ 7 Byers *et al*., (1998) กล่าวถึงวิธีของทางด้านผู้รับในการสร้างไฟล์ข้อมูลจากแพ็กเก็ตที่ได้รับไว้ 2 แนวทาง ได้แก่ ถอดรหัสข้อมูลเมื่อได้รับแพ็กเก็ตพิเศษแต่ละแพ็กเก็ตแบบเรียลไทม์ และการถอดรหัสข้อมูลเมื่อได้รับแพ็กเก็ตต้นฉบับและแพ็กเก็ตพิเศษในจำนวนที่เพียงพอ ซึ่ง Byers *et al*., (1998) เลือกใช้วิธีการที่สองเนื่องจากพบว่าเป็นวิธีที่ง่ายและมีประสิทธิภาพด้านความเร็วที่เพียงพอในการใช้งาน

Yoon *et al*. ,(1999) เสนอ ARM (Adaptive Reliable Multicast) เป็นการให้บริการข้อมูลแบบมัลติคาสต์ที่ใช้ช่องสัญญาณการสื่อสารแบบ 2 ทิศทาง ซึ่งมีกระบวนการสร้างความน่าเชื่อถือด้วยวิธีการ FEC แบบ Tornado Codes (Luby *et al*., 1997) การทำงานของ ARM ผู้ส่งจะสามารถ

ปรับจำนวนแพ็กเก็ตพิเศษที่จะส่งให้แก่ผู้รับตามจำนวนที่ผู้รับต้องการได้ โดยผู้ส่งจะส่งข้อความร้องขออัตราการสูญหายที่เกิดขึ้นกับไฟล์ข้อมูลที่ผู้ส่งได้จัดส่งเป็นระยะ ผู้รับจะคำนวณเพื่อประมาณค่าอัตราการสูญหายที่เกิดขึ้นกับไฟล์ข้อมูลที่ผู้ส่งร้องขอและส่งกลับไปยังผู้ส่ง ผู้ส่งจะใช้ข้อมูลที่ได้รับเพื่อคำนวณหาจำนวนแพ็กเก็ตพิเศษที่ต้องส่งไปให้ผู้รับใช้ในการถอดรหัสเพื่อกู้คืนแพ็กเก็ตต้นฉบับที่สูญหาย หากอัตราการสูญหายของข้อมูลที่ได้รับมีการเปลี่ยนแปลงจากที่ได้รับครั้งก่อนหน้าจะคำนวณใหม่อีกครั้งเพื่อหาจำนวนแพ็กเก็ตพิเศษที่ต้องส่งไปให้ผู้รับ ในกรณีที่ผู้ส่งส่งแพ็กเก็ตต้นฉบับและแพ็กเก็ตพิเศษจำนวนหนึ่งที่เกิดจากการคำนวณอัตราการสูญหายไปยังผู้รับครบแล้ว แต่ผู้รับยังไม่สามารถรับแพ็กเก็ตได้ครบ ซึ่งอาจเนื่องมาจากมีอัตราการสูญหายเพิ่มขึ้น ผู้รับจะส่งข้อความร้องขอข้อมูลเพิ่มโดยใช้ NACK แพ็กเก็ต Yoon *et al*., (1999) ได้สรุปข้อดีของ ARM ไว้ดังนี้

- สามารถหาจำนวนแพ็กเก็ตพิเศษที่ผู้รับต้องการใช้แม้ว่าการส่งแพ็กเก็ตต้นฉบับยังไม่เสร็จสิ้นลง ทำให้ไม่มีการรอข้อมูลหลังจากแพ็กเก็ตต้นฉบับถูกส่งครบ
- การส่งแพ็กเก็ตพิเศษที่ได้จากการเข้ารหัสข้อมูลไปยังผู้รับแทนการส่งแพ็กเก็ตซ้ำตามที่ผู้รับต้องการ เป็นการลดปริมาณข้อมูลที่ต้องใช้ในการส่งไปยังผู้รับเพื่อใช้แทนแพ็กเก็ตที่สูญหาย เนื่องจากแพ็กเก็ตพิเศษหนึ่งแพ็กเก็ตสามารถนำมาถอดรหัสเพื่อใช้กู้คืนแพ็กเก็ตต้นฉบับใดๆ ได้หนึ่งแพ็กเก็ต
- เป็นการลดปัญหา NACK Implosion ที่จะเกิดขึ้นทางด้านผู้ส่ง เนื่องจากการร้องขอแพ็กเก็ตสำหรับหนึ่งไฟล์ข้อมูลจะใช้ NACK แพ็กเก็ตเพียงหนึ่งแพ็กเก็ต เพราะเป็นเพียงการแจ้งจำนวนแพ็กเก็ตที่ต้องการ

Pokavanich *et al*., (2000) เสนอ Packet Delivery Scheduling for Reliable Multicasting Over Unidirectional Link เป็นการให้บริการข้อมูลแบบมัลติคาสต์โดยมีการสร้างความน่าเชื่อถือด้วยวิธีการ Data Carousel ซึ่งจำนวนรอบของการส่งข้อมูลซ้ำนี้เกิดจากการคำนวณโดยใช้ ขนาดของไฟล์ข้อมูล อัตราความเร็วในการส่งข้อมูล และช่วงระยะเวลาที่เรียกว่า Time Period ในกรณีที่จำนวนรอบในการส่งข้อมูลที่ได้จากการคำนวณมีค่าไม่ถึงหนึ่งรอบ ซึ่งอาจมีสาเหตุมาจาก ขนาดของข้อมูลที่มีขนาดใหญ่ หรือการกำหนดช่วงระยะเวลาที่สั้นจนเกินไป Pokavanich *et al*., (2000) ได้เสนอให้ส่งไฟล์ข้อมูลนั้นอย่างน้อยเป็นจำนวนหนึ่งรอบ และเสนอการใช้บรอดคาสต์ดิสค์ในการควบคุมอัตราความเร็วในการส่งข้อมูลของแต่ละกลุ่มข้อมูลที่เรียกว่า ดิสค์ (Disk) โดยจะมีการกำหนดระดับความสำคัญให้กับแต่ละดิสค์ ซึ่งแต่ละไฟล์ข้อมูลจะถูกคำนวณเพื่อหาระดับ

ความสำคัญโดยการใช้ ขนาดของไฟล์ข้อมูล อัตราความเร็วในการส่งข้อมูล ช่วงระยะเวลา และจำนวนการร้องขอไฟล์ข้อมูลนั้นๆ จากผู้รับ Pokavanich *et al*., (2000) แสดงตัวอย่างการคำนวณหาค่าระดับความสำคัญไว้ดังนี้

- อัตราความเร็วในการส่งข้อมูลบนเครือข่ายเท่ากับ 230,000 ไบต์ต่อวินาที
- ขนาดของไฟล์ข้อมูลเท่ากับ 2,000,000 ไบต์
- จำนวนความต้องการของผู้รับเท่ากับ 400 ราย
- ช่วงระยะเวลาในการส่งข้อมูลเท่ากับ 1 ชั่วโมง

จำนวนข้อมูลที่สามารถส่งได้ภายในช่วงเวลาที่กำหนดเท่ากับ 230000 * (1 * 60 * 60) ซึ่งเท่ากับ 8,280,000 ไบต์ และจำนวนข้อมูลรวมจากผู้รับทุกรายเท่ากับ 2000000 * 400 ซึ่งเท่ากับ 8,000,000 ไบต์ เมื่อหาอัตราส่วนของค่าทั้งสองจะได้ 8280000 / 8000000 ซึ่งเท่ากับ 1.035 และจะเรียกค่านี้ว่า ค่าระดับความสำคัญของไฟล์ข้อมูล โดยค่าระดับความสำคัญที่ได้มีค่าต่ำจะหมายถึงมีความสำคัญมาก

Tommasi *et al*., (2002) เสนอ SMDP (Satellite Multicast Distribution Protocol) เป็นการให้บริการข้อมูลแบบมัลติคาสต์ผ่านเครือข่ายดาวเทียมแบบทิศทางเดียว และใช้ช่องสัญญาณเครือข่ายภาคพื้นดินแบบสองทิศทางในการช่วยเพิ่มประสิทธิภาพการสร้างความน่าเชื่อถือ โดย SMDP จะใช้ FEC แบบ Reed-Solomon Codes ที่พัฒนาด้วย Vandermonde Matrices (Rizzo, 1997) และเนื่องจากปัญหาด้านการประมวลผลข้อมูลในการเข้ารหัสและถอดรหัสข้อมูลสำหรับข้อมูลที่มีขนาดใหญ่ จึงแบ่งไฟล์ข้อมูลออกเป็นส่วนเรียกว่า บล็อค (Block) ผู้ส่งจะส่งแพ็กเก็ตต้นฉบับและแพ็กเก็ตพิเศษผ่านเครือข่ายดาวเทียม ในกรณีที่ผู้รับสามารถรับแพ็กเก็ตในจำนวนที่เพียงพอ ผู้รับจะถอดรหัสแพ็กเก็ตพิเศษเพื่อกู้คืนแพ็กเก็ตต้นฉบับที่ไม่ได้รับและสร้างส่วนย่อยของไฟล์ข้อมูลนั้นๆ ในกรณีที่บางบล็อคผู้รับไม่สามารถรับแพ็กเก็ตได้เพียงพอ Tommasi *et al*., (2002) เสนอให้ผู้รับส่งคำร้องขอผ่าน NACK แพ็กเก็ต เพื่อร้องขอแพ็กเก็ตต้นฉบับที่สูญหายผ่านโปรโตคอลทีซีพีผ่านการเชื่อมโยงเครือข่ายภาคพื้นดิน กระบวนการก่อนเริ่มต้นส่งไฟล์ข้อมูลผู้ส่งจะส่งข้อความแบบมัลติคาสต์ผ่านเครือข่ายดาวเทียมเพื่อแจ้งให้แก่ผู้รับทุกรายทราบถึงไฟล์ข้อมูลที่จะส่งในลำดับถัดไป โดยข้อความนี้จะประกอบไปด้วยข้อมูลต่างๆ ของไฟล์ข้อมูล เช่น ชื่อหรือหมายเลขไฟล์ข้อมูล ขนาดของแพ็กเก็ต จำนวนบล็อค จำนวนแพ็กเก็ตในบล็อค เป็นต้น ข้อความแจ้งการส่งไฟล์ข้อมูลนี้จะถูกส่งซ้ำไปยังผู้รับ โดยจะมีหมายเลขของข้อความกำกับ ซึ่งหมายเลขนี้

จะลดลงครั้งละหนึ่ง การส่งข้อความนี้มีจุดประสงค์เพื่อให้ผู้รับสามารถรอรับข้อมูลที่ตนเองต้องการได้ทัน และทำให้ผู้รับสามารถพักการทำงานอื่นที่ไม่จำเป็นชั่วคราว เมื่อหมายเลขลำดับข้อความแจ้งการส่งข้อมูลลดลงเท่ากับศูนย์ ผู้ส่งจึงเริ่มส่งแพ็กเก็ตต้นฉบับและแพ็กเก็ตพิเศษผ่านเครือข่ายดาวเทียม หลังจากแพ็กเก็ตถูกส่งจนครบผู้ส่งจะรอรับข้อความการร้องของการส่งแพ็กเก็ตซ้ำจากผู้รับผ่านโปรโตคอลทีซีพี

Basu *et al*., (2003) เสนอ RMUS (A Reliable Multicast Protocol for Unidirectional Satellite Link) เป็นการให้บริการข้อมูลแบบมัลติคาสต์ผ่านช่องสัญญาณดาวเทียมแบบทิศทางเดียวและใช้เครือข่ายภาคพื้นดินแบบสองทิศทางในการสร้างความน่าเชื่อถือ ซึ่งมีวิธีการสร้างความน่าเชื่อถือโดยใช้กระบวนการตอบกลับจากผู้รับ ซึ่งผู้รับจะไม่ส่งข้อความแจ้งการไม่ได้รับแพ็กเก็ตในทันที ผู้รับจะเก็บรวบรวมข้อมูลแพ็กเก็ตที่สูญหาย และหลังจากที่การส่งข้อมูลเสร็จสิ้นลงผู้ส่งจะส่งแพ็กเก็ตร้องขอรายงานการสูญหายของแพ็กเก็ตจากผู้รับ และผู้รับจะอาศัยช่องทางการสื่อสารช่องทางอื่น เช่น เครือข่ายภาคพื้นดิน เป็นต้น ในการส่งรายงานนี้ให้แก่ผู้ส่ง ซึ่งทำให้ผู้ส่งสามารถสรุปผลการสูญหายของแพ็กเก็ตจากผู้รับทั้งหมดได้และส่งแพ็กเก็ตที่สูญหายซ้ำให้แก่ผู้รับผ่านช่องทางการสื่อสารแบบทิศทางเดียว การทำงานข้างต้นถือเป็นวิธีการควบคุมการผิดพลาดของข้อมูล Basu *et al*., (2003) ได้กล่าวว่าปัจจัยที่สำคัญของการสูญหายของข้อมูลคือความคับคั่งของข้อมูล ซึ่งมีสาเหตุมาจากข้อมูลที่ถูกส่งไปยังระบบเครือข่ายมีปริมาณมากเกินกว่าที่หน่วยความจำชั่วคราวของเร้าท์เตอร์บนเครือข่ายจะสามารถเก็บข้อมูลได้ จึงได้เสนอวิธีการควบคุมความคับคั่งของข้อมูลซึ่งมีพื้นฐานการทำงานมาจาก MBFC (Sano *et al*., 1998)

อุปกรณ์และวิธีการ

อุปกรณ์

1. คอมพิวเตอร์เซิร์ฟเวอร์ ส่วนที่ 1 จำนวน 1 ชุด

1.1 รุ่น HP Server Dual CPU Pentium III, 933 Mhz, หน่วยความจำ 512 เมกะไบต์

1.2 ระบบปฏิบัติการ Window 2000 Server

1.3 ซอฟต์แวร์ที่ใช้ในการจำลองระบบปฏิบัติการ FreeBSD Cygwin (Red Hat Inc., 2000)

1.4 ซอฟต์แวร์จำลองเครือข่าย Network Simulator (NS) เวอร์ชั่น allinone2.26 (Information Sciences Institute, 2004)

2 คอมพิวเตอร์ส่วนบุคคล ส่วนที่ 2 จำนวน 3 ชุด

2.1 คอมพิวเตอร์สำหรับทำหน้าที่ส่งข้อมูล และรับข้อมูล 2 ชุด

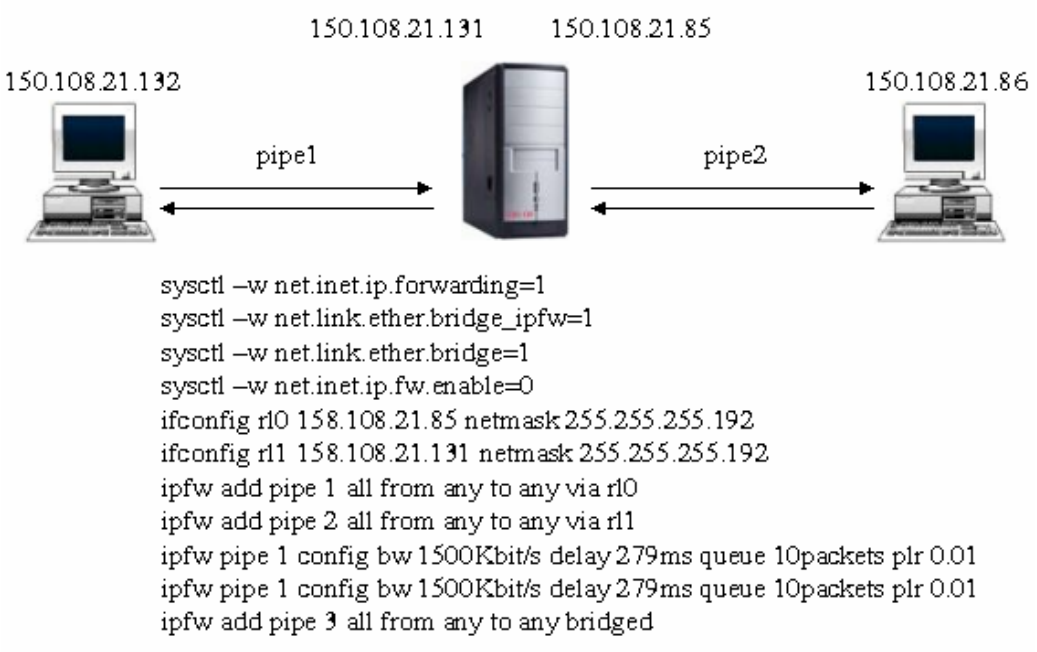
2.1.1 รุ่น Pentium III, 500 Mhz, หน่วยความจำ 128 เมกะไบต์

2.1.2 ซอฟต์แวร์ระบบปฏิบัติการ Linux เวอร์ชั่น Fedora Core 2 (Red Hat Inc., 2003)

2.2 คอมพิวเตอร์สำหรับทำหน้าที่เลียนแบบดาวเทียม 1 ชุด

2.2.1 รุ่น Pentium III, 500 Mhz, หน่วยความจำ 128 เมกะไบต์

2.2.2 ซอฟต์แวร์ที่ใช้ในการจำลองดาวเทียม Dummynet (Rizzo, 2004a)



ภาพที่ 14 โครงสร้างจำลองเครือข่ายดาวเทียมด้วยโปรแกรมจำลองเครือข่าย Dummynet

3 เครือข่ายดาวเทียมจากโครงการ Asian Internet Interconnection Initiatives: AI3

3.1 เครื่องคอมพิวเตอร์ที่ทำหน้าที่รับ-ส่งข้อมูล มหาวิทยาลัย KEIO

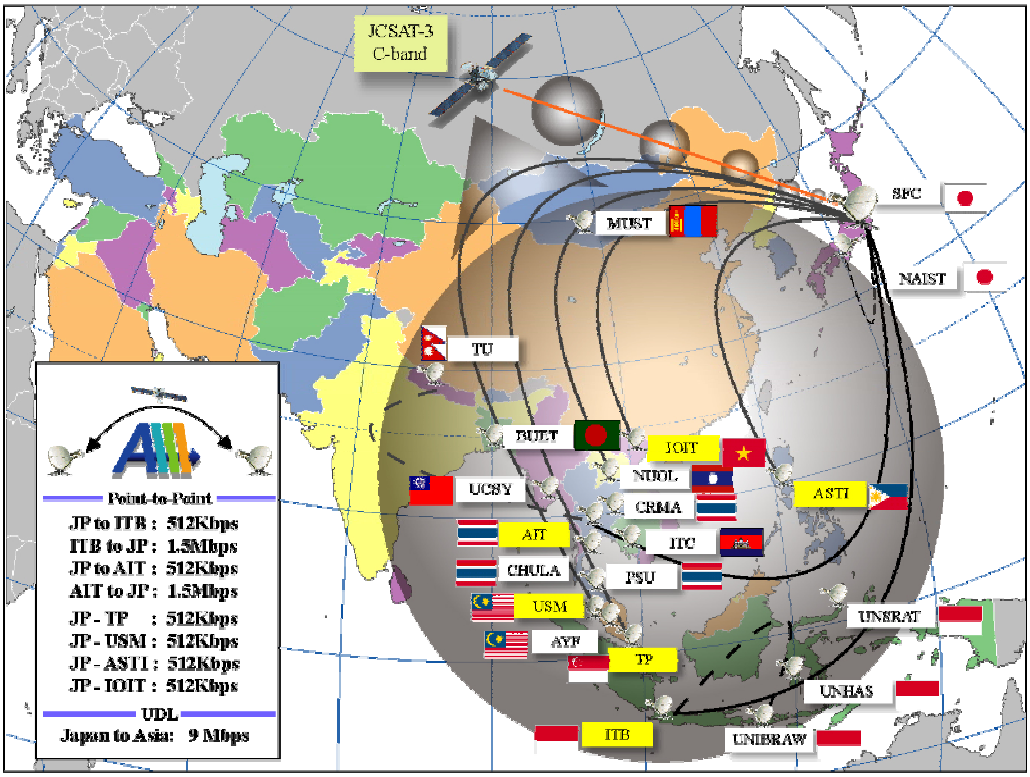
3.1.1 รุ่น Pentium III Xeon, 1.2 กิกะเฮิร์ต, หน่วยความจำ 256 เมกะไบต์

3.1.2 ระบบปฏิบัติการ FreeBSD 4.5

3.2 เครื่องคอมพิวเตอร์ที่ทำหน้าที่รับ-ส่งข้อมูล สถาบันเทคโนโลยีแห่งเอเชีย

3.2.1 รุ่น Celeron, 633 เมกะเฮิร์ต, หน่วยความจำ 128 เมกะไบต์

3.2.2 ระบบปฏิบัติการ Linux เวอร์ชั่น Fedora Core 2



ภาพที่ 15 โครงสร้างเครือข่ายดาวเทียมภายใต้โครงการ AI3
ที่มา: AI3 Project (2005)

ภาพที่ 15 แสดงเครือข่ายดาวเทียมของประเทศญี่ปุ่นภายใต้โครงการ “Asian Internet Interconnection Initiative (AIII หรือ AI3) ซึ่งมีวัตถุประสงค์เพื่อประโยชน์ทางการศึกษา เช่น กระจายการศึกษาในชั้นเรียนไปยังประเทศต่างๆ ในภูมิภาคเอเชีย เป็นต้น ซึ่งสถาบันเทคโนโลยีแห่งเอเชีย (Asian Institute of Technology: AIT) ได้ร่วมเป็นสมาชิกภายใต้โครงการ AI3

วิธีการ

เนื่องจากข้อจำกัดด้านอุปกรณ์ที่ใช้ในการทดลอง ดังนั้นการทดลองส่วนใหญ่ในงานวิทยานิพนธ์จะเป็นการส่งข้อมูลโดยมีผู้รับเพียงรายเดียว แต่อย่างไรก็ตามการทดลองทั้งหมดยังคงให้บริการแบบมัลติคาสต์ข้อมูล งานวิทยานิพนธ์นี้ประกอบด้วยการศึกษาการสูญหายของข้อมูลผ่านเครือข่ายดาวเทียม และการทดลองการสร้างความน่าเชื่อถือด้วยวิธีการต่างๆ บนเครือข่ายจำลอง NS-2 เครือข่ายจำลอง Dummynet และเครือข่ายดาวเทียม ซึ่งได้แบ่งการศึกษาออกเป็น 5 ส่วน ได้แก่

1. ศึกษาอัตราการสูญหายของข้อมูลผ่านเครือข่ายดาวเทียม
2. ศึกษาผลความน่าเชื่อถือของข้อมูลจากรูปแบบการบรอดคาสต์ดิสค์
3. ศึกษาประสิทธิภาพการสร้างความน่าเชื่อถือด้วยวิธีการบรอดคาสต์ดิสค์และ Data Carousel
4. ศึกษาประสิทธิภาพการสร้างความน่าเชื่อถือด้วยวิธีการบรอดคาสต์ดิสค์และ FEC (Reed-Solomon Codes พัฒนาด้วย Cauchy Matrices)
5. ศึกษาประสิทธิภาพการสร้างความน่าเชื่อถือด้วยวิธีการบรอดคาสต์ดิสค์และ Peer-to-Peer Sharing

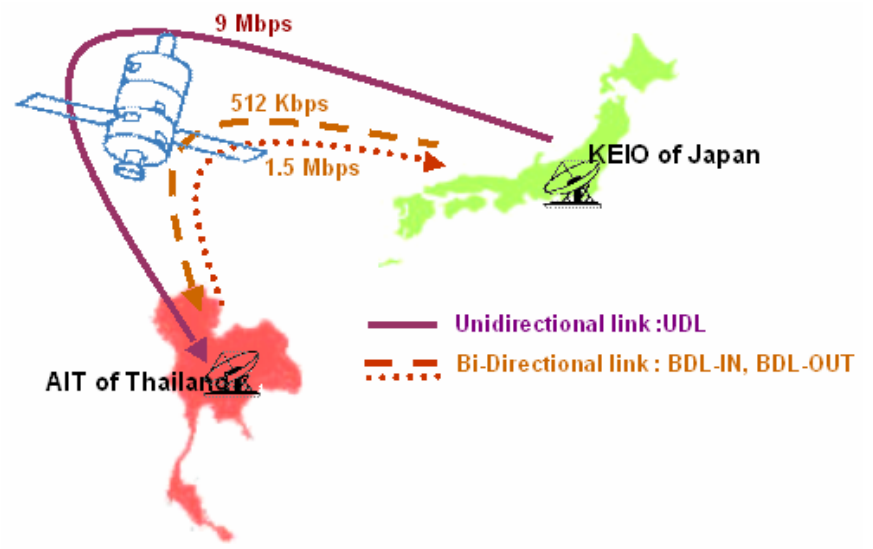
1. ศึกษาอัตราการสูญหายของข้อมูลผ่านเครือข่ายดาวเทียม

การศึกษาการสูญหายของข้อมูลในส่วนนี้ เป็นการศึกษาเพียงบางส่วนของเครือข่าย AI3 โดยเป็นการศึกษาระหว่างมหาวิทยาลัยเคโอะ (Keio) ประเทศญี่ปุ่น กับสถาบันเทคโนโลยีแห่งเอเชีย (AIT)ประเทศไทย ซึ่งมีการเชื่อมโยงเครือข่ายดังภาพที่ 16 ซึ่งช่องสัญญาณที่ใช้ในการศึกษามีคุณสมบัติดังนี้

1. ช่องสัญญาณแบบทิศทางเดียว (Unidirectional link: UDL) เป็นการส่งข้อมูลจากประเทศญี่ปุ่น มายังประเทศไทย มีขนาดช่องสัญญาณ 9 เมกะบิตต่อวินาที
2. ช่องสัญญาณแบบสองทิศทาง-กรณีเป็นฝ่ายรับข้อมูล (Bidirectional link-Incoming: BDL-IN) เป็นการส่งข้อมูลจากประเทศญี่ปุ่น มาประเทศไทย มีขนาดช่องสัญญาณ 512 กิโลบิตต่อวินาที

3. ช่องสัญญาณแบบสองทิศทาง-กรณีเป็นฝ่ายส่งข้อมูล (Bidirectional link-Outgoing: BDL-OUT) เป็นการส่งข้อมูลจากประเทศไทย ไปประเทศญี่ปุ่น มีขนาดช่องสัญญาณ 1.5 เมกะบิตต่อวินาที

ช่องสัญญาณทั้ง 3 นี้มีชนิดคลื่นการสื่อสารในช่วง C ซึ่งมีความคงทนต่อสภาพอากาศที่เปียกชื้น หรือมีฝน



ภาพที่ 16 ส่วนของเครือข่ายดาวเทียมภายใต้โครงการ AI3 ที่ใช้ในงานวิทยานิพนธ์

การศึกษาอัตราการสูญหายของข้อมูลของช่องสัญญาณทั้ง 3 ทำโดยส่งแพ็กเก็ตขนาดต่างๆ จำนวน 5 ขนาด ได้แก่ 128, 256, 512, 1024 และ 1500 ไบต์ และกำหนดความเร็วในการส่งแพ็กเก็ตไว้ที่ 1.5 เมกะบิตต่อวินาที จำกัดแพ็กเก็ตที่ส่งใน 1 ชั่วโมง เป็นจำนวน 10000 แพ็กเก็ต ส่งแพ็กเก็ตเป็นระยะเวลา 100 ชั่วโมง ภาพที่ 17 และ 18 แสดงลำดับการทำงานของชุดคำสั่งที่ใช้ในการศึกษาการสูญหายของแพ็กเก็ต บนช่องสัญญาณดาวเทียมทั้ง 3 ช่องสัญญาณ และเนื่องด้วยการเดินทางของข้อมูลในระบบเครือข่ายคอมพิวเตอร์จากปลายทางด้านผู้ส่งไปยังปลายทางด้านผู้รับนั้นสามารถมีเส้นทางการเดินทางได้มากกว่าหนึ่งเส้นทาง ดังนั้นถึงแม้แพ็กเก็ตที่ถูกส่งจากผู้ส่งไปยังผู้รับจะมีการส่งตามลำดับที่ถูกต้อง แต่ลำดับแพ็กเก็ตที่ไปถึงผู้รับสามารถสลับลำดับที่ได้ ข้อกำหนดในการศึกษาอัตราการสูญหายของข้อมูลครั้งนี้จะถือว่าหากแพ็กเก็ตที่ได้รับมีลำดับน้อยกว่าแพ็กเก็ตที่ได้รับล่าสุด จะไม่ถือว่าได้รับแพ็กเก็ตนั้น แต่อย่างไรก็ตามลักษณะการเชื่อมโยงเครือข่ายสำหรับผู้ส่งและผู้รับที่ใช้ในงานวิทยานิพนธ์นี้เป็นการเชื่อมโยงภายในเครือข่ายเดียวกับ

อุปกรณ์รับและส่งสัญญาณดาวเทียม ดังนั้นลำดับการมาถึงของแพ็กเก็ตทางด้านผู้รับจึงไม่เกิดการสลับลำดับกัน

```
Packet_Seq = 0
Packet_Size = 128 // up on each experiment

For Hours = 1 to 100
   For Packet_Count = 1 to 10000
      Packet_Seq = Packet_Seq + 1
      PACKET_SEND(Packet_Size, Packet_Seq)
      Sleep for send next packet
   Next Packet_Count

   Sleep for next hour
      Next Hours
```

ภาพที่ 17 ขั้นตอนการส่งข้อมูลเพื่อศึกษาอัตราการสูญหายของข้อมูลด้านผู้ส่ง

```
Current_Packet_Seq = 0

While (True)
   PACKET_RECEIVE(Packet_Size, Packet_Seq)

   If Packet_Seq > Current_Packet_Seq then
      Write log (Packet_Seq, 1)
   Else
      For I = Current_Packet_Seq to Packet_Seq
         Write log (I, 0)
      Next I
   End If

   Current_Packet_Seq = Packet_Seq
End Loop
```

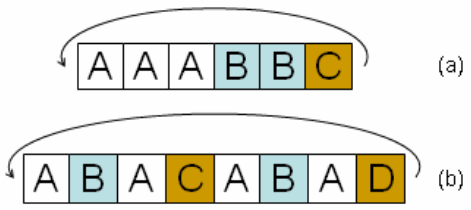
ภาพที่ 18 ขั้นตอนการรับข้อมูลเพื่อศึกษาอัตราการสูญหายของข้อมูลด้านผู้รับ

2. ศึกษาผลความน่าเชื่อถือของข้อมูลจากรูปแบบการบรอดคาสต์ดิสค์

การศึกษาการสร้างความน่าเชื่อถือในงานวิทยานิพนธ์นี้เป็นการให้บริการข้อมูลโดยใช้พื้นฐานของการบรอดคาสต์ดิสค์ โดยมีวัตถุประสงค์ในการนำบรอดคาสต์ดิสค์มาใช้ในการให้บริการข้อมูลคือ เพื่อให้บริการไฟล์ข้อมูลมากกว่า 1 ไฟล์ข้อมูล ในหนึ่งช่วงเวลา และใช้ความสามารถด้านการปรับอัตราส่วนความเร็วในการให้บริการส่งข้อมูลแต่ละดิสค์ ให้เหมาะสมกับ

ความต้องการของไฟล์ข้อมูลแต่ละกลุ่ม การบรอดคาสต์ดิสค์ที่มีความสามารถในการปรับอัตราส่วนความเร็วมี 2 รูปแบบ คือ Skewed และ Multi-disk

ข้อกำหนดในการศึกษาผลความน่าเชื่อถือของข้อมูลจากรูปแบบการบรอดคาสต์ดิสค์ 2 แบบ คือ Skewed และ Multi-disk ใช้วิธีการสร้างความน่าเชื่อถือด้วย Data Carousel โดยทดลองบนเครือข่าย NS-2 ซึ่งมีการจำลองผู้รับจำนวน 10 ราย และมีการกำหนดอัตราการสูญหายในการส่งข้อมูลตั้งแต่ 1% ถึง 16% ส่วนของการบรอดคาสต์ดิสค์แบบ Skewed กำหนดให้มีการส่งไฟล์ข้อมูลจำนวน 3 ไฟล์ ได้แก่ ไฟล์ข้อมูล A B และ C แต่ละไฟล์ข้อมูลมีขนาด 700 เมกะไบต์ ซึ่งมีลำดับการส่งข้อมูลดังภาพที่ 19(a) และในส่วนของการบรอดคาสต์ดิสค์แบบ Multi-disk กำหนดให้มีการส่งไฟล์ข้อมูลจำนวน 4 ไฟล์ ได้แก่ ไฟล์ข้อมูล A B C และ D แต่ละไฟล์ข้อมูลมีขนาด 700 เมกะไบต์ ซึ่งมีลำดับการส่งข้อมูลดังภาพที่ 19(b)



ภาพที่ 19 ลำดับการส่งแพ็กเก็ตในการศึกษาผลความน่าเชื่อถือของข้อมูล

ผลที่ได้จากการทดลองในส่วนนี้แสดงให้เห็นว่ารูปแบบของการบรอดคาสต์ดิสค์ทั้ง 2 แบบ ไม่มีผลต่อความน่าเชื่อถือของข้อมูล โดยจะได้แสดงรายละเอียดในบทถัดไป การสร้างความน่าเชื่อถือในส่วนถัดไปของงานวิทยานิพนธ์นี้เลือกการบรอดคาสต์ดิสค์แบบ Skewed เนื่องจากเป็นวิธีการง่ายต่อการพัฒนา

3. ศึกษาประสิทธิภาพการสร้างความน่าเชื่อถือด้วยวิธีการบรอดคาสต์ดิสค์และ Data Carousel

การสร้างความน่าเชื่อถือในการทดลองส่วนนี้ใช้กระบวนการที่เรียกว่า Data Carousel และใช้กระบวนการบรอดคาสต์ดิสค์เพื่อใช้ในการควบคุมคุณภาพการให้บริการส่งข้อมูล โดยทดลองบนระบบเครือข่ายต่างๆ ดังนี้

1. เครือข่ายดาวเทียม AI3 สำหรับช่องสัญญาณแบบทิศทางเดียว (UDL)
2. เครือข่ายจำลอง NS-2
3. เครือข่ายจำลอง Dummynet

3.1 การเตรียมข้อมูล

งานวิทยานิพนธ์นี้ได้ทดลองบนเครือข่าย 3 เครือข่ายดังกล่าวข้างต้น ในการทดลองผ่านเครือข่ายดาวเทียม และเครือข่ายจำลอง Dummynet นั้นจำเป็นต้องใช้ไฟล์ข้อมูลจริง ในงานวิทยานิพนธ์นี้จึงมีการสร้างไฟล์ข้อมูลขึ้นโดยมีลักษณะเป็นแอสกีไฟล์ ซึ่งประกอบด้วยตัวอักขระตัวเลข และอักขระพิเศษ ส่วนการทดลองบนเครือข่ายจำลอง NS-2 จะใช้การจำลองไฟล์ข้อมูล

ในหนึ่งชุดการทดลองจะส่งไฟล์ข้อมูล 9 ไฟล์ โดยจะเรียกว่า P1 ถึง P9 มีขนาด 1, 30, 20, 10, 5, 4, 3, 2 และ 1 เมกะไบต์ ตามลำดับ ในการทดลองสำหรับแต่ละเครือข่ายยังได้เปลี่ยนขนาดของไฟล์ข้อมูล P1 ทั้งหมด 7 ขนาด ได้แก่ 1, 5, 10, 50, 100, 500 และ 1000 เมกะไบต์ เพื่อทดสอบว่าขนาดของไฟล์ข้อมูลมีผลต่อประสิทธิภาพของวิธีการสร้างความน่าเชื่อถือหรือไม่

3.2 การกำหนดอัตราการสูญหายของข้อมูล

อัตราการสูญหายของข้อมูลถือเป็นปัจจัยที่สำคัญสำหรับประสิทธิภาพในการสร้างความน่าเชื่อถือ ดังนั้นสำหรับการทดลองบนเครือข่ายจำลอง Dummynet และเครือข่ายจำลอง NS-2 จึงต้องมีการกำหนดอัตราการสูญหาย และเพื่อเป็นการทดสอบว่าอัตราการสูญหายของข้อมูลมีผลต่อประสิทธิภาพของกระบวนสร้างความน่าเชื่อถือหรือไม่ ซึ่งอัตราการสูญหายที่ถูกกำหนดในการทดลองมี 3 อัตรา ได้แก่ 1%, 10% และ 25% ส่วนการทดลองผ่านเครือข่ายดาวเทียมนั้นไม่สามารถควบคุมอัตราการสูญหายได้จึงเป็นการทดลองที่ใช้อัตราการสูญหายที่เกิดขึ้นจริงในขณะทดลอง

3.3 การควบคุมคุณภาพด้วยบรอดคาสต์ดิสค์

งานวิทยานิพนธ์นี้มีการควบคุมคุณภาพการให้บริการด้วยวิธีการบรอดคาสต์ดิสค์รูปแบบ Skewed โดยมีการให้บริการส่งข้อมูลพร้อมกัน 3 ดิสค์ ในหนึ่งช่วงเวลา เพื่อสนับสนุนการส่งข้อมูลที่มีความสำคัญในระดับต่างๆ 3 ระดับ ได้แก่ ข้อมูลที่มีความสำคัญสูงที่ต้องการความ

รวดเร็วในการส่งข้อมูลมากที่สุด ข้อมูลที่มีความสำคัญระดับกลางที่ต้องการความรวดเร็วในการส่งข้อมูลรองลงมา และสุดท้ายข้อมูลที่มีความสำคัญระดับต่ำสุด คือต้องการความเร็วในการส่งข้อมูลน้อยที่สุด โดยมีอัตราส่วนความเร็วในการส่งข้อมูลของทั้ง 3 ดิสค์ เป็น 4:2:1 ซึ่งหมายความว่าจะส่งแพ็กเก็ตของไฟล์ข้อมูลที่อยู่ในดิสค์ที่หนึ่งจำนวน 4 แพ็กเก็ต ส่งแพ็กเก็ตของไฟล์ข้อมูลที่อยู่ในดิสค์ที่สองจำนวน 2 แพ็กเก็ต ส่งแพ็กเก็ตของไฟล์ข้อมูลที่อยู่ในดิสค์ที่สามจำนวน 1 แพ็กเก็ต และวนส่งแพ็กเก็ตซ้ำทุกกลุ่มไปเรื่อยๆ

3.4 การควบคุมการไหลของข้อมูล

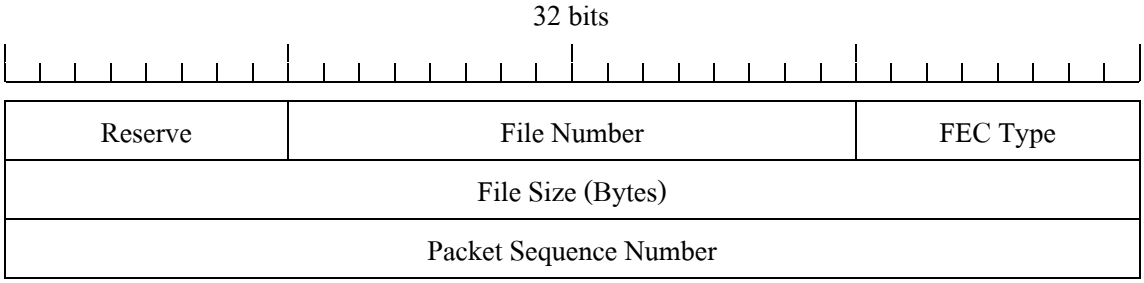
อัตราความเร็วของการส่งข้อมูลโดยรวมจะถูกกำหนดที่ 1.5 เมกะบิตต่อวินาที โดยจะมีการเว้นช่วงเวลาในการส่งแต่ละแพ็กเก็ตซึ่งเป็นการควบคุมการไหลของข้อมูลแบบ Rate-based โดยมีสูตรการคำนวณต่างๆ ดังตารางที่ 8

ตารางที่ 8 สูตรการคำนวณหาค่าต่างๆ ที่เกี่ยวกับการควบคุมการไหลของข้อมูล

ค่า	การคำนวณ
จำนวนไบต์ที่ถูกการส่งใน 1 วินาที	อัตราความเร็วรวม * 1024 * 1024 / 8
จำนวนแพ็กเก็ตต่อ 1 วินาที	จำนวนไบต์ที่ถูกส่งใน 1 วินาที / ขนาดแพ็กเก็ต
จำนวนไมโครวินาทีที่ใช้ต่อ 1 แพ็กเก็ต	1 / จำนวนแพ็กเก็ตต่อ 1 วินาที * 1000000
เวลาที่ใช้ในการหน่วงระหว่างแพ็กเก็ต	จำนวนไมโครวินาทีที่ใช้ต่อ 1 แพ็กเก็ต – (เวลาสิ้นสุดการส่งแพ็กเก็ต – เวลาเริ่มต้นการส่งแพ็กเก็ต)

3.5 โครงสร้างแพ็กเก็ต

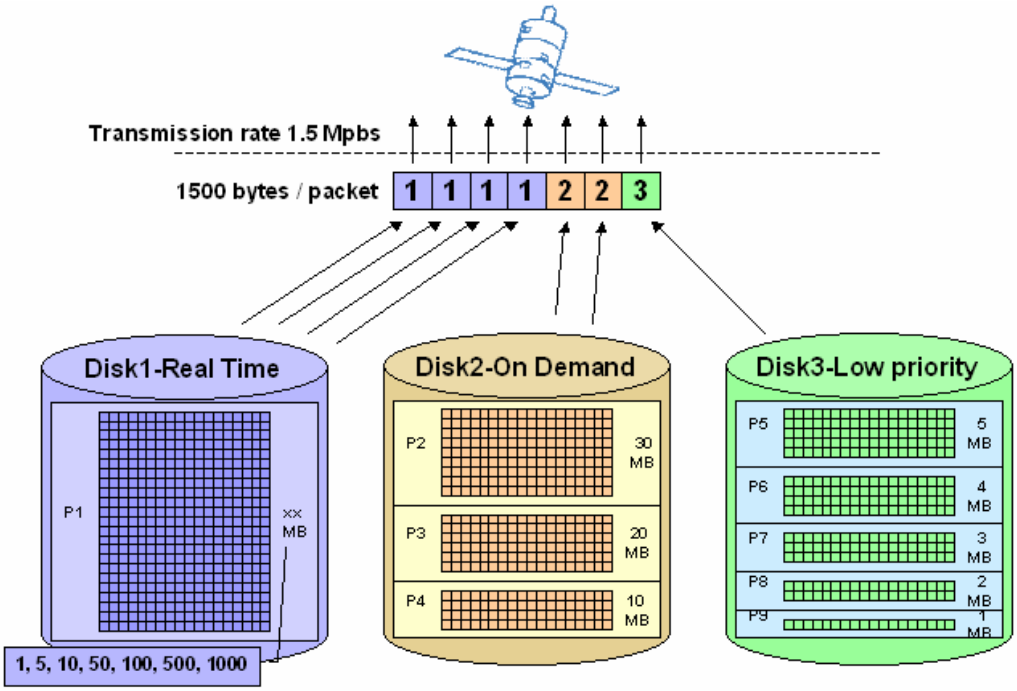
การสร้างความน่าเชื่อถือในการมัลติคาสต์ข้อมูลนี้จะกระทำที่ระดับชั้นแอพพลิเคชั่น ซึ่งไฟล์ข้อมูลจะต้องถูกแบ่งออกเป็นแพ็กเก็ตย่อยๆ ดังนั้นสิ่งที่จะทำให้ผู้รับทราบถึงลำดับที่ของแพ็กเก็ตและข้อมูลต่างๆ ของไฟล์ข้อมูลที่จะเป็นข้อมูลให้ผู้รับสามารถรวมแพ็กเก็ตกลับเป็นไฟล์ข้อมูลได้ จะถูกจัดเก็บไว้ในส่วนที่เรียกว่าเฮดเดอร์ซึ่งจะถูกส่งไปกับทุกแพ็กเก็ต ในงานวิทยานิพนธ์นี้ได้กำหนดให้เฮดเดอร์มีขนาด 12 ไบต์ ประกอบไปด้วยข้อมูลต่างๆ ดังภาพที่ 20



ภาพที่ 20 รูปแบบเฮดเดอร์ขนาด 12 ไบต์ ของแพ็กเก็ต

Reserve	สำรองไว้ใช้ภายหลัง (ในการทดลองนี้นำมาใช้บอกหมายเลขรอบที่ส่งไฟล์ข้อมูลนั้นๆ)
File Number	หมายเลขไฟล์ข้อมูลที่ส่ง
FEC Type	รูปแบบของวิธีการ FEC
File Size(Byte)	ขนาดของไฟล์ข้อมูล มีหน่วยเป็นไบต์
Sequence Number	หมายเลขลำดับของแพ็กเก็ต

เพื่อให้แต่ละแพ็กเก็ตเป็นอิสระต่อกัน ขนาดของแพ็กเก็ตที่ถูกส่งไปบนเครือข่ายจะต้องมีขนาดไม่เกิน 1500 ไบต์ เพื่อป้องกันการถูกแบ่งแพ็กเก็ตซึ่งเป็นข้อกำหนดของโปรโตคอลอีเทอร์เน็ต ขนาดของแพ็กเก็ต 1500 ไบต์ นั้นจะต้องประกอบด้วยส่วนหัวของชั้นแอพพลิเคชั่น ชั้นทรานสปอร์เตชั่น ชั้นเน็ตเวิร์ค ซึ่งมีขนาด 12, 8 และ 60 ไบต์ ตามลำดับ ดังนั้นขนาดของข้อมูลในแพ็กเก็ตจึงมีขนาด 1420 ไบต์ ซึ่งองค์ประกอบของการทดลองเพื่อศึกษาประสิทธิภาพในการสร้างความน่าเชื่อถือในส่วนนี้มีรายละเอียดดังภาพที่ 21



ภาพที่ 21 แสดงองค์ประกอบกระบวนการทดลองสร้างความน่าเชื่อถือ

3.6 การตรวจสอบความถูกต้องในการสร้างความน่าเชื่อถือ

เพื่อเป็นการตรวจสอบความถูกต้องของข้อมูล จากการสร้างความน่าเชื่อถือด้วยวิธีการต่างๆ ในการทดลองของงานวิทยานิพนธ์นี้ จึงได้ใช้กระบวนการเข้ารหัสเพื่อตรวจสอบข้อมูลด้วย MD5 กระบวนการตรวจสอบนี้ไม่ได้รวมอยู่ในกระบวนการสร้างความน่าเชื่อถือ โดยจะเป็นเพียงการกระทำเพื่อการตรวจสอบความถูกต้องของการสร้างความน่าเชื่อถือเท่านั้น

ภาพที่ 22 และ 23 แสดงชุดคำสั่งที่ใช้ในการทดลองสร้างความน่าเชื่อถือด้วย Data Carousel ในกรณีที่เป็นผู้ส่ง และเป็นผู้รับข้อมูลตามลำดับ

```
TimeSlot = {1, 1, 1, 1, 2, 2, 3}
Disk(1) = {P1}
Disk(2) = {P2, P3, P4}
Disk(3) = {P5, P6, P7, P8, P9}
Round(P1, P2, P3, …, P9) = 1
Sequence(P1, P2, P3, …, P9) = 0
FecType = 0

While (True)
   Data = READ_PACKET[Disk[TimeSlot]]

   If Data = Null Then
      Round[Disk[TimeSlot]] = Round[Disk[TimeSlot]] + 1
      Sequence[Disk[TimeSlot]] = 0
      Next Disk[TimeSlot]
   Else
      Program# = Disk(TimeSlot)
      Sequence(Program#) = Sequence[Program#] + 1
      PACKET_SEND(Round[Program#], Program#, FecType, Size[Program#],
                  Sequence[Program#], Data)
      Next TimeSlot
      Sleep for send next packet
   End

End Loop
```

ภาพที่ 22 ขั้นตอนการส่งข้อมูลเพื่อทดลองสร้างความน่าเชื่อถือด้วยบรอดคาสต์ดิสก์และ Data Carousel

```
TCurrent_Packet_Seq = 0

While (True)
   PACKET_RECEIVE(Round, Program#, FecType, Size, Packet_Seq, Data)
   Received = CHECK_SEQ(Program#, Packet_Seq)

   If Received = No Then
      Write Log (Program#, Packet_Seq)
      WRITE_FILE(Program#, Packet_Seq, Data)
   End If
   If  PROGRAM_COMPLETE[Program#] Then
      Write Log (Program#, Round)
   End If

End Loop
```

ภาพที่ 23 ขั้นตอนการรับข้อมูลเพื่อทดลองสร้างความน่าเชื่อถือด้วยบรอดคาสต์ดิสก์และ Data Carousel

4 ศึกษาประสิทธิภาพการสร้างความน่าเชื่อถือด้วยวิธีการบรอดคาสต์ดิสค์และ FEC (Reed-Solomon Codes พัฒนาด้วย Cauchy Matrices)

จากการทดลองสร้างความน่าเชื่อถือด้วย Data Carousel ที่จะแสดงในบทถัดไปนั้นแสดงให้เห็นว่าจะต้องใช้จำนวนรอบในการส่งข้อมูลไปยังผู้รับเป็นจำนวนหลายรอบ งานวิทยานิพนธ์นี้จึงต้องการทดสอบประสิทธิภาพในการสร้างความน่าเชื่อถือโดยวิธีการ FEC ซึ่งในการทดลองนี้เลือกใช้วิธีการ FEC แบบ Reed-Solomon Codes เนื่องจากเป็นวิธีการที่มีการเปิดเผยชุดคำสั่งในการทำงาน ทั้งการพัฒนาด้วย Cauchy Matrices (Luby, 2004) และการพัฒนาด้วย Vandermonde Matrices (Rizzo, 2004b) แต่เนื่องจากผลการวัดประสิทธิภาพเปรียบเทียบระหว่าง Cauchy Matrices และ Vandermonde Matrices (Luby, 2004) แสดงให้เห็นว่าการพัฒนาด้วย Cauchy Matrices มีประสิทธิภาพดีกว่าการพัฒนาด้วย Vandermonde Matrices ดังนั้นการทดลองนี้จึงเลือกใช้การพัฒนาด้วย Cauchy Matrices และการทดลองนี้ได้ทดลองบนเครือข่าย 2 เครือข่าย ได้แก่

1. เครือข่ายดาวเทียม AI3 สำหรับช่องสัญญาณแบบทิศทางเดียว (UDL)
2. เครือข่ายจำลอง Dummynet

รายละเอียดการทดลองของการทดลองในส่วนนี้สำหรับการกำหนดอัตราการสูญหาย การควบคุมการไหลของข้อมูล และการตรวจสอบความถูกต้องในการสร้างความน่าเชื่อถือ มีรายละเอียดเช่นเดียวกับการทดลองเพื่อศึกษาประสิทธิภาพการสร้างความน่าเชื่อถือด้วยวิธีการบรอดคาสต์ดิสค์และ Data Carousel ส่วนรายละเอียดการเตรียมข้อมูล และโครงสร้างแพ็กเก็ต มีความแตกต่างเพียงเล็กน้อยดังนี้

4.1 การเตรียมข้อมูล

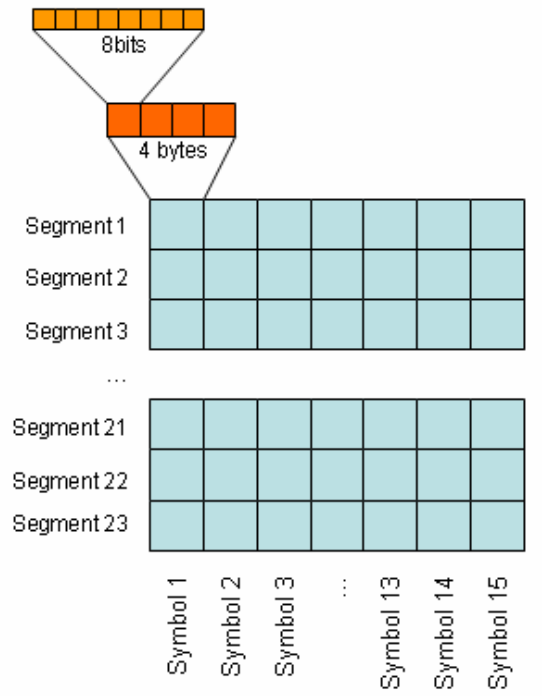
มีการเพิ่มกระบวนการเข้ารหัสข้อมูลเพื่อสร้างแพ็กเก็ตพิเศษไว้ล่วงหน้า เนื่องจากกระบวนการเข้ารหัสต้องใช้เวลามาก ไม่สามารถเข้ารหัสข้อมูลในเวลาที่ส่งข้อมูลได้ และด้วยข้อจำกัดในเรื่องเวลาที่ใช้ในการประมวลผลของการเข้ารหัสข้อมูล ซึ่งเวลาที่ใช้ในการเข้ารหัสข้อมูลจะมากขึ้นเป็น 4 เท่า สำหรับขนาดของข้อมูลที่เพิ่มขึ้นทุกๆ 2 เท่า งานวิทยานิพนธ์นี้จึงใช้วิธีการแบ่งข้อมูลเป็นส่วนย่อยที่เรียกว่า บล็อค (Block) หลังจากนั้นจึงเข้ารหัสข้อมูล และกำหนด

ค่าตัวคูณ (Stretch Factor) เท่ากับ 2 ซึ่งค่าตัวคูณนี้ใช้สำหรับการทดลองเพื่อศึกษาประสิทธิภาพของ FEC เท่านั้น

จากผลการศึกษาอัตราการสูญหายที่จะกล่าวถึงในบทถัดไป ได้พบลักษณะการสูญหายของข้อมูลจำนวนมากเป็นการสูญหายแบบต่อเนื่อง ซึ่งมีจำนวนแพ็กเก็ตที่สูญหายต่อเนื่องกันสูงสุดเป็นจำนวน 1419 แพ็กเก็ต ดังนั้นเพื่อเป็นการป้องกันการสูญหายแบบต่อเนื่องที่อาจเกิดขึ้นในแต่ละบล็อคจนทำให้ไม่สามารถกู้คืนข้อมูลต้นฉบับของบล็อคนั้นกลับมาได้ อันเนื่องมาจากการแบ่งส่วนข้อมูลให้มีขนาดเล็กเกินไปจนทำให้ผู้รับไม่สามารถรับข้อมูลได้เพียงพอที่จะถอดรหัสข้อมูลต้นฉบับกลับคืนมาได้ จึงกำหนดให้แต่ละบล็อคมีจำนวนแพ็กเก็ตต้นฉบับ 2000 แพ็กเก็ต และในบล็อคสุดท้ายให้มีจำนวนได้ต่ำสุด 1500 แพ็กเก็ต และสูงสุดได้ 3499 แพ็กเก็ต

การใช้ Reed-Solomon Codes ในงานวิทยานิพนธ์นี้จะใช้ซิมโบล (symbol) ที่มีความยาว (Length) เท่ากับ 15 ดังนั้นสัญลักษณ์ของการขยายฟิลด์จึงเป็น $GF(2^{15})$ ซึ่งทำให้สามารถมีจำนวนซิมโบลได้สูงถึง $2^{15} - 1$ ซิมโบล จากการกำหนดจำนวนแพ็กเก็ตในแต่ละบล็อคและค่าตัวคูณที่ได้กล่าวไว้ข้างต้น ถือเป็นการกำหนดโค้ด (code) ที่ใช้ในการเข้ารหัสข้อมูลเป็น RS(4000, 2000) สำหรับทุกบล็อคยกเว้นบล็อคสุดท้ายจะมีโค้ดที่ไม่คงที่ซึ่งขึ้นอยู่กับจำนวนแพ็กเก็ตในบล็อค

ข้อมูลในแต่ละแพ็กเก็ตจะถูกแบ่งออกเป็นซิมโบล โดยแต่ละซิมโบลจะมีขนาดเท่ากับ 32 บิต (4 ไบต์) และเนื่องจากต้องการให้ขนาดของแพ็กเก็ตมีขนาดใหญ่สุดที่ระบบอีเทอร์เน็ตจะสามารถรองรับได้ (1500 ไบต์) เพื่อเป็นการลดปริมาณของข้อมูลบนเครือข่ายซึ่งเกิดจากเฮดเดอร์ที่จะถูกใส่ให้กับทุกแพ็กเก็ต ดังนั้นในแต่ละแพ็กเก็ตจะมีการสร้างเป็นเซกเมนต์ (Segment) ซึ่งในแต่ละเซกเมนต์จะมีขนาดเท่ากับ 60 ไบต์ (15 ซิมโบล) โดยมีจำนวนเซกเมนต์ในแต่ละแพ็กเก็ตเท่ากับขนาดของแพ็กเก็ตสูงสุดในระบบอีเทอร์เน็ต (1500 ไบต์) ลบด้วยขนาดของแพ็กเก็ตเฮดเดอร์ที่อยู่ในชั้นแอพพลิเคชั่น (12 ไบต์) ชั่นทรานสปอร์ตเตชั่น (8 ไบต์) และชั้นเน็ตเวิร์ก (60 ไบต์) หารด้วยขนาดของเซกเมนต์ (60 ไบต์) ซึ่งมีค่าเท่ากับ (1500-12-8-60)/60 หรือ 23 เซกเมนต์ โดยภาพที่ 24 เป็นการแสดงลักษณะการแบ่งซิมโบลในแต่ละแพ็กเก็ต



ภาพที่ 24 การแบ่งซิมโบลในหนึ่งแพ็กเก็ต

4.2 โครงสร้างแพ็กเก็ต

เนื่องด้วยการนำวิธีการ FEC แบบ Reed-Solomon Codes ที่พัฒนาด้วย Cauchy Matrices ที่ได้มีการเผยแพร่โดย Luby, 2004 ซึ่งมีผลต่อการกำหนดขนาดของข้อมูลแต่ละแพ็กเก็ต ทำให้ไม่สามารถกำหนดขนาดของข้อมูลในแต่ละแพ็กเก็ตให้มีขนาดเดียวกับการทดลองเพื่อศึกษาประสิทธิภาพการสร้างความน่าเชื่อถือด้วยวิธีการบรอดคาสต์ดิสค์และ Data Carousal ซึ่งขนาดของข้อมูลแต่ละแพ็กเก็ตใหญ่สุดที่เป็นไปได้จึงมีขนาดเท่ากับ 1380 ไบต์

เพื่อเป็นการเพิ่มประสิทธิภาพความเร็วในการเข้ารหัสไฟล์ข้อมูล จึงได้แบ่งไฟล์ข้อมูลเป็นบล็อค ดังนั้นจึงจำเป็นต้องส่งหมายเลขลำดับบล็อคของไฟล์ข้อมูลไปยังผู้รับด้วย เพื่อให้ผู้รับสามารถรวบรวมข้อมูลในลำดับที่ถูกต้องได้ การทดลองในส่วนนี้จึงใช้ฟิลด์ Reserve ที่อยู่ในส่วนหัวของแพ็กเก็ตเพื่อบอกลำดับของส่วนย่อยของไฟล์ข้อมูล

5 ศึกษาประสิทธิภาพการสร้างความน่าเชื่อถือด้วยวิธีการบรอดคาสต์ดิสค์และ Peer-to-Peer Sharing

การให้บริการข้อมูลแบบกลุ่มเป็นจุดประสงค์ในการบริการข้อมูลสำหรับงานวิทยานิพนธ์นี้ แต่ในการทดลองเพื่อศึกษาประสิทธิภาพการสร้างความน่าเชื่อถือทั้ง 2 แบบที่ผ่านมา มุ่งเน้นวิธีการให้เกิดความน่าเชื่อถือกับผู้รับแต่ละราย โดยที่ผู้รับแต่ละรายมีอิสระต่อกัน ไม่จำเป็นต้องเป็นมีการเชื่อมโยงเครือข่ายถึงกัน ซึ่งสำหรับการทดลองในส่วนนี้เป็นการทดลองโดยตั้งอยู่บนสมมติฐานที่ว่า “ผู้รับมีการเชื่อมโยงเครือข่ายถึงกันเป็นกลุ่มๆ และผู้รับในแต่ละกลุ่มมีสิทธิร้องขอข้อมูลที่ตนไม่ได้รับจากสมาชิกในกลุ่มได้” ดังนั้นในการทดลองส่วนนี้จึงเป็นการสร้างความน่าเชื่อถือด้วยการแบ่งปันข้อมูลของตนกับผู้รับในกลุ่ม

เนื่องจากการทดลองสร้างความน่าเชื่อถือด้วยวิธีการ Peer-to-Peer Sharing จำเป็นต้องมีผู้รับมากกว่าหนึ่งรายแต่ข้อจำกัดในด้านทรัพยากร จึงทำให้ไม่สามารถทดลองผ่านเครือข่ายดาวเทียม และเครือข่ายจำลอง Dummynet ได้ ดังนั้นการทดลองในส่วนนี้จะทดลองบนเครือข่ายจำลอง NS-2 เพียงเครือข่ายเดียว และมีรายละเอียดสำหรับการกำหนดอัตราการสูญหาย การเตรียมข้อมูล การควบคุมการไหลของข้อมูล และโครงสร้างแพ็กเก็ตเช่นเดียวกับการทดลองสร้างความน่าเชื่อถือด้วยวิธีการบรอดคาสต์ดิสค์และ Data Carousel ที่ได้กล่าวข้างต้น

ผลการทดลองและวิจารณ์

จากผลการทดลองผ่านเครือข่ายดาวเทียม AI3 ที่แสดงในงานวิทยานิพนธ์นี้ อัตราการสูญหายที่แสดงในแต่ละการทดลองเป็นอัตราการสูญหายที่คำนวณจากการทำงานที่ชั้นแอพพลิเคชั่น ดังนั้นการสูญหายของข้อมูลที่เกิดขึ้นจึงเป็นการสูญหายที่เกิดขึ้นตลอดเส้นทางการเดินทางของข้อมูลจากผู้ส่งไปยังผู้รับไม่ใช่อัตราการสูญหายที่เกิดขึ้นเฉพาะบนช่องสัญญาณดาวเทียม เส้นทางที่ข้อมูลต้องผ่านจากผู้ส่งไปยังผู้รับประกอบด้วย ระบบเครือข่ายด้านผู้ส่ง อุปกรณ์เร้าท์เตอร์ด้านผู้ส่ง อุปกรณ์ส่งสัญญาณดาวเทียม อุปกรณ์รับสัญญาณดาวเทียม อุปกรณ์เร้าท์เตอร์ด้านผู้รับและระบบเครือข่ายด้านผู้รับ อีกทั้งในการทำงานของ อุปกรณ์รับและส่งสัญญาณดาวเทียมมีการทำงานเพื่อลดการสูญหายของข้อมูล (Orten *et al*., 2002) ซึ่งเป็นการทำงานในชั้นดาต้าลิ้งค์ อัตราการสูญหายที่คำนวณได้ในชั้นแอพพลิเคชั่นจึงอาจมีมากกว่า หรือน้อยกว่าการสูญหายที่เกิดขึ้นจริงบนช่องสัญญาณดาวเทียม

1. <u>ผลการศึกษาอัตราการสูญหายของข้อมูลผ่านเครือข่ายดาวเทียม</u>

จากการทดลองแสดงให้เห็นว่าขนาดแพ็กเก็ตที่แตกต่างกันทั้ง 5 ขนาด ไม่ส่งผลให้อัตราการสูญหายเพิ่มขึ้นและลดลง ซึ่งผลที่ได้เป็นในทิศทางเดียวกันทั้งหมดทั้ง 3 ช่องสัญญาณ ส่วนเมื่อเปรียบเทียบอัตราการสูญหายที่เกิดขึ้นระหว่างช่องสัญญาณทั้ง 3 แสดงให้เห็นว่าช่องสัญญาณแบบสองทิศทาง-กรณีเป็นฝ่ายรับข้อมูล (BDL-IN) มีอัตราการสูญหายต่ำสุดสำหรับทุกขนาดของแพ็กเก็ตเมื่อเทียบกับช่องสัญญาณอื่น ซึ่งสาเหตุที่น่าจะเป็นปัจจัยสำคัญต่อการทดลองครั้งนี้คือ อัตราการใช้งานปกติของทั้ง 3 ช่องสัญญาณ เนื่องจากช่องสัญญาณสองทิศทาง-กรณีเป็นฝ่ายรับข้อมูล (BDL-IN) มีการใช้งานในขณะทดลองน้อยที่สุด ช่องสัญญาณแบบสองทิศทาง-กรณีเป็นฝ่ายส่งข้อมูล (BDL-OUT) มีการใช้งานสูงเป็นอันดับถัดมา และช่องสัญญาณแบบทิศทางเดียว (UDL) มีการใช้งานสูงที่สุด ซึ่งมีรายละเอียดอัตราการสูญหายดังตารางที่ 9

ตารางที่ 9 อัตราการสูญหายของแพ็กเก็ตผ่านเครือข่ายดาวเทียม

รูปแบบการเชื่อมโยง	ขนาดแพ็กเก็ต (ไบต์)				
	128	**256**	**512**	**1024**	**1500**
UDL	0.7130	0.7959	0.7643	0.7643	1.4042
BDL-IN	0.1419	0.1640	0.0018	0.0024	0.0219
BDL-OUT	0.1538	0.2406	0.0930	0.1305	0.3957

อีกสิ่งหนึ่งที่พบจากการทดลองคือ รูปแบบของการสูญหายของข้อมูล ซึ่งมีการสูญหายของแพ็กเก็ตที่อยู่ติดกันเกิดขึ้นหลายครั้ง ซึ่งจะเรียกการสูญหายแบบนี้ว่าเป็นการสูญหายแบบต่อเนื่องหรือBurst Loss โดยจะถือว่าการสูญหายของแพ็กเก็ตที่อยู่ติดกันจำนวนตั้งแต่ 2 แพ็กเก็ต ขึ้นไปเป็นการสูญหายแบบต่อเนื่อง จำนวนแพ็กเก็ตที่สูญหายติดกันเป็นจำนวนมากที่สุด เกิดขึ้นกับการทดลองผ่านช่องสัญญาณแบบสองทิศทาง-กรณีเป็นฝ่ายรับข้อมูล (BDL-IN) คือ 1,419 แพ็กเก็ต และถัดมาเป็นช่องสัญญาณแบบสองทิศทาง-กรณีเป็นฝ่ายส่งข้อมูล (BDL-OUT) คือ 741 แพ็กเก็ต สุดท้ายช่องสัญญาณแบบทิศทางเดียว (UDL) มีจำนวนแพ็กเก็ตสูญหายติดกันเป็นจำนวนมากสุดที่ 20 แพ็กเก็ต ตารางที่ 10 เป็นการเปรียบเทียบจำนวนแพ็กเก็ตที่เกิดการสูญหายจากการสูญหายแบบต่อเนื่องต่อจำนวนแพ็กเก็ตที่เกิดการสูญหายทั้งหมด โดยช่องสัญญาณ UDL จะมีอัตราส่วนจำนวนแพ็กเก็ตที่สูญหายแบบต่อเนื่องต่ำสุด โดยมีค่าประมาณ 21% ถึง 39% ช่องสัญญาณ BDL-OUT มีอัตราส่วนจำนวนแพ็กเก็ตที่สูญหายแบบต่อเนื่องมากขึ้นเป็นลำดับถัดมา โดยมีค่าประมาณ 60% ถึง 84% สุดท้ายสำหรับช่องสัญญาณ BDL-IN มีอัตราส่วนจำนวนแพ็กเก็ตที่สูญหายแบบต่อเนื่องสูงสุดโดยมีค่าประมาณ 72% ถึง 100% อัตราส่วนจำนวนแพ็กเก็ตที่สูญหายแบบต่อเนื่องที่เกิดขึ้นกับการทดลองบนช่องสัญญาณ BDL-IN ที่ขนาดแพ็กเก็ตขนาด 128 ไบต์ มีอัตราสูงถึง 100% เนื่องจากมีการสูญหายเกิดขึ้นเพียง 1 ครั้ง และเป็นการสูญหายแบบต่อเนื่อง

คาดว่าผลอัตราส่วนจำนวนแพ็กเก็ตที่สูญหายแบบต่อเนื่องที่เกิดขึ้นนี้ ที่ช่องสัญญาณแบบ UDL มีอัตราส่วนจำนวนแพ็กเก็ตที่สูญหายแบบต่อเนื่องต่ำสุดน่าจะเป็นสาเหตุมาจากขนาดของช่องสัญญาณแบบ UDL มีขนาดแบนวิดธ์สูงกว่าช่องสัญญาณในแบบอื่นๆ ซึ่งช่องสัญญาณแบบ BDL-IN มีขนาดของช่องสัญญาณต่ำสุด โดยเมื่อมีความต้องการส่งข้อมูลเป็นจำนวนมากไปบนช่องสัญญาณการสื่อสารที่มีขนาดเล็ก จะทำให้อุปกรณ์เร้าท์เตอร์ไม่สามารถส่งข้อมูลออกไปยังช่องสัญญาณการสื่อสารได้ทันกับข้อมูลที่ได้รับจากผู้ส่ง ดังนั้นอุปกรณ์เร้าท์เตอร์จะเก็บข้อมูลที่

ได้รับไว้ในหน่วยความจำชั่วคราวเพื่อรอส่งออกไปยังช่องสัญญาณ และเมื่อหน่วยความจำชั่วคราวของอุปกรณ์เร้าท์เตอร์เต็ม ข้อมูลบางส่วนจึงต้องถูกทิ้งไปทำให้เกิดการสูญหายของข้อมูล

ตารางที่ 10 อัตราส่วนการสูญหายของแพ็กเก็ตแบบต่อเนื่อง ต่อการสูญหายของแพ็กเก็ตทั้งหมดผ่านเครือข่ายดาวเทียม

รูปแบบการเชื่อมโยง	**ขนาดแพ็กเก็ต (ไบต์)**				
	128	**256**	**512**	**1024**	**1500**
UDL	25.0771	27.1517	26.4035	21.3921	39.6382
BDL-IN	100.0000	99.9390	72.2222	91.6667	96.8037
BDL-OUT	64.4993	84.9127	60.4301	73.0268	71.3925

ตารางที่ 11 แสดงการเปรียบเทียบจำนวนครั้งที่เกิดการสูญหายแบบต่อเนื่องต่อจำนวนครั้งที่เกิดการสูญหายทั้งหมด ผลการทดลองของทั้ง 3 ช่องสัญญาณ จากการทดลองที่ขนาดแพ็กเก็ต 128 ไบต์ และ 256 ไบต์ มีอัตราส่วนจำนวนครั้งที่เกิดการสูญหายแบบต่อเนื่องมากและน้อยสลับกันไปมาระหว่างช่องสัญญาณที่ทดลองทั้ง 3 ช่องสัญญาณ แต่หากวิเคราะห์เพียงขนาดแพ็กเก็ต 512 ไบต์ 1024 ไบต์ และ 1500 ไบต์ แสดงให้เห็นว่าช่องสัญญาณแบบ UDL มีอัตราส่วนจำนวนครั้งในการสูญหายแบบต่อเนื่องต่ำสุดโดยมีค่าประมาณ 10% ถึง 20% ช่องสัญญาณแบบ BDL-OUT มีอัตราส่วนจำนวนครั้งที่เกิดการสูญหายแบบต่อเนื่องสูงขึ้นเป็นลำดับถัดมา โดยมีค่าประมาณ 14% ถึง 39% และช่องสัญญาณแบบ BDL-IN มีอัตราส่วนจำนวนครั้งที่เกิดการสูญหายแบบต่อเนื่องสูงสุด โดยมีค่าประมาณ 16% ถึง 100%

ตารางที่ 11 ความถี่ของจำนวนครั้งที่เกิดการสูญหายของแพ็กเก็ตแบบต่อเนื่อง ต่อจำนวนครั้งที่เกิดการสูญหายของแพ็กเก็ตทั้งหมดผ่านเครือข่ายดาวเทียม

รูปแบบการเชื่อมโยง	**ขนาดแพ็กเก็ต (ไบต์)**				
	128	**256**	**512**	**1024**	**1500**
UDL	12.8690	13.8612	13.5306	10.8605	20.1808
BDL-IN	100.0000	66.6667	16.6667	33.3333	65.0000
BDL-OUT	9.7521	10.1485	14.2191	27.5720	39.6267

จากผลการศึกษาอัตราการสูญหายของข้อมูลบนการสื่อสารผ่านช่องสัญญาณดาวเทียม แสดงให้เห็นว่าขนาดของแพ็กเก็ตไม่ส่งผลต่ออัตราการเกิดการสูญหายของข้อมูล ซึ่งปัจจัยที่มีผลกระทบต่ออัตราการสูญหายคือจำนวนการใช้งานที่เกิดขึ้นในขณะที่ทดลอง ส่วนปัจจัยด้านขนาดของช่องสัญญาณของเครือข่ายที่ใช้งานจะมีผลต่อรูปแบบการสูญหายของข้อมูลที่จะทำให้เกิดอัตราส่วนการสูญหายแบบต่อเนื่องสูงในกรณีที่ช่องสัญญาณเครือข่ายมีขนาดเล็ก

2. ผลการศึกษาผลความน่าเชื่อถือของข้อมูลจากรูปแบบการบรอดคาสต์ดิสค์

การศึกษาผลความน่าเชื่อถือของข้อมูลจากรูปแบบการบรอดคาสต์ดิสค์ ได้ศึกษาโดยกำหนดให้มีผู้รับจำนวน 10 ราย ดังนั้นผลการทดลองจากการบรอดคาสต์ดิสค์รูปแบบ Skewed ที่แสดงในตารางที่ 12 และผลการทดลองจากการบรอดคาสต์ดิสค์รูปแบบ Multi-disk ที่แสดงในตารางที่ 13 จึงเป็นจำนวนรอบสูงสุดที่ใช้ในการส่งไปยังผู้รับทั้ง 10 ราย

ตารางที่ 12 จำนวนรอบที่ใช้ในการส่งข้อมูลจากผลการศึกษาความน่าเชื่อถือด้วยการบรอดคาสต์ดิสค์แบบ Skewed

ไฟล์ข้อมูล	อัตราการสูญหาย (เปอร์เซ็นต์)															
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
A	4	5	6	7	6	6	7	7	8	8	9	9	8	9	10	9
B	4	5	6	5	6	6	8	7	8	8	9	8	11	9	12	10
C	4	4	5	5	5	5	6	6	6	6	6	7	7	7	7	7

ตารางที่ 13 จำนวนรอบที่ใช้ในการส่งข้อมูลจากผลการศึกษาความน่าเชื่อถือด้วยการบรอดคาสต์ดิสค์แบบ Multi-Disk

ไฟล์ข้อมูล	อัตราการสูญหาย (เปอร์เซ็นต์)															
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
A	4	5	6	6	7	6	8	7	7	8	8	8	9	9	10	9
B	6	6	6	6	6	6	7	7	7	8	9	9	8	10	10	9
C	4	4	5	5	5	5	6	6	6	6	7	7	7	7	8	8
D	4	4	5	5	5	5	6	6	6	6	7	7	7	7	7	8

ผลการทดลองเพื่อการศึกษาผลความน่าเชื่อถือจากการบรอดคาสต์ดิสค์แบบ Skewed และ Multi-disk แสดงให้เห็นว่ารูปแบบการบรอดคาสต์ดิสค์ทั้ง 2 แบบ ไม่มีผลต่อความน่าเชื่อถือของข้อมูล เนื่องจากความแตกต่างของการบรอดคาสต์ดิสค์ทั้ง 2 แบบ แตกต่างกันเพียงลำดับในการส่งแพ็กเก็ตของไฟล์ข้อมูล โดยที่ผู้รับทุกรายยังคงต้องได้รับทุกแพ็กเก็ตของไฟล์ข้อมูล สิ่งที่ได้จากการศึกษาบรอดคาสต์ดิสค์ทั้ง 2 รูปแบบ คือ จำนวนรอบที่ใช้ในการส่งข้อมูลมีแนวโน้มสูงขึ้นเมื่ออัตราการสูญหายของข้อมูลเพิ่มขึ้น โดยผลการทดลองจากการบรอดคาสต์ดิสค์แบบ Skewed ที่แสดงในตารางที่ 12 มีจำนวนรอบที่ใช้ในการส่งข้อมูลต่ำสุดคือ 4 รอบ และมีจำนวนรอบที่ใช้ในการส่งข้อมูลสูงสุดคือ 12 รอบ ผลการทดลองจากการบรอดคาสต์ดิสค์แบบ Multi-disk ที่แสดงในตารางที่ 13 มีจำนวนรอบที่ใช้ในการส่งข้อมูลต่ำสุดคือ 4 และจำนวนรอบที่ใช้ในการส่งข้อมูลสูงสุดคือ 10 รอบ

3. <u>ผลการศึกษาประสิทธิภาพการสร้างความน่าเชื่อถือด้วยวิธีการบรอดคาสต์ดิสค์และ Data Carousel</u>

ผลการศึกษาประสิทธิภาพการสร้างความน่าเชื่อถือในส่วนนี้ แสดงให้ทราบถึงจำนวนรอบสำหรับแต่ละไฟล์ข้อมูล (P1 ถึง P9) ที่ผู้ส่งต้องส่งไฟล์ข้อมูลไปยังผู้รับ ซึ่งไฟล์ข้อมูลทั้ง 9 ไฟล์ จะถูกแบ่งออกเป็น 3 ดิสค์ เพื่อให้บริการส่งข้อมูลที่มีความเร่งด่วนแตกต่างกัน โดยแพ็กเก็ตของไฟล์ข้อมูลทั้ง 3 ดิสค์ จะถูกสลับกันส่งออกไป ด้วยวิธีการของบรอดคาสต์ดิสต์ และเมื่อไฟล์ข้อมูลของแต่ละกลุ่มถูกส่งครบแล้วก็จะเริ่มส่งรอบถัดไป ซึ่งเป็นการสร้างความน่าเชื่อถือด้วยวิธีการ Data Carousel ผลการทดลองจะแสดงเป็น 3 ส่วน ตามประเภทของเครือข่ายที่ใช้ในการทดลอง อันได้แก่ เครือข่ายดาวเทียม AI3 สำหรับช่องสัญญาณแบบทิศทางเดียว เครือข่ายจำลอง NS-2 และเครือข่ายจำลอง Dummynet ซึ่งในแต่ละเครือข่ายได้ทดลองเครือข่ายละ 4 ครั้ง ดังนั้นในการแสดงผลการทดลองในแต่ละส่วนจึงเป็นการแสดงจำนวนรอบสูงสุดจากผลการทดลองทั้ง 4 ครั้ง

3.1 ผลการทดลองผ่านเครือข่ายดาวเทียม AI3 สำหรับช่องสัญญาณแบบทิศทางเดียว (UDL)

เนื่องจากการทดลองผ่านเครือข่ายดาวเทียมไม่สามารถกำหนดอัตราการสูญหายได้ ดังนั้นจำนวนรอบที่ใช้ในการส่งข้อมูลจึงขึ้นอยู่กับอัตราการสูญหายที่เกิดขึ้นจริงบนเครือข่าย ซึ่งอัตราการสูญหายเฉลี่ยที่เกิดขึ้นในการทดลองทั้ง 4 ครั้ง มีค่าตามลำดับดังนี้ 1.11, 0.38, 2.86 และ 0.01 ตามลำดับ อัตราการสูญหายที่เกิดขึ้นที่ทำให้แต่ละไฟล์ข้อมูลใช้จำนวนรอบในการส่งข้อมูลสูงสุด ในแต่ละการทดลองที่มีขนาดไฟล์ข้อมูล P1 แตกต่างกันไป ได้ผลตามตารางที่ 14

ตารางที่ 14 อัตราการสูญหายของแพ็กเก็ตในแต่ละไฟล์จากการส่งข้อมูลผ่านเครือข่ายดาวเทียม

ขนาดไฟล์ P1	ไฟล์ข้อมูล								
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**
1	2.59	0.72	2.46	3.14	0.71	1.91	0.48	0.58	0.27
5	0.31	10.03	5.00	24.40	0.51	1.96	46.68	3.23	0.89
10	4.01	2.73	3.95	4.11	3.21	2.37	4.52	3.26	1.72
50	5.12	5.92	5.01	5.46	7.81	4.10	7.76	5.79	4.44
100	0.98	1.24	0.90	0.58	1.40	1.03	1.20	0.68	0.88
500	0.19	0.11	0.28	0.07	0.14	0.00	0.05	0.00	0.00
1000	0.24	2.26	2.36	2.16	0.90	1.05	1.46	1.19	1.94

จากตารางที่ 14 ในการทดลองที่ขนาดของไฟล์ข้อมูล P1 มีขนาด 1 เมกะไบต์ มีอัตราการสูญหายต่ำสุดเท่ากับ 0.27% บนไฟล์ข้อมูล P9 และมีอัตราการสูญหายสูงสุดเท่ากับ 2.59% บนไฟล์ข้อมูล P1 ในการทดลองที่ขนาดของไฟล์ข้อมูล P1 มีขนาด 5 เมกะไบต์ มีอัตราการสูญหายต่ำสุดเท่ากับ 0.31% บนไฟล์ข้อมูล P1 และมีอัตราการสูญหายสูงสุดเท่ากับ 46.68% บนไฟล์ข้อมูล P7 ในการทดลองที่ขนาดของไฟล์ข้อมูล P1 มีขนาด 10 เมกะไบต์ มีอัตราการสูญหายต่ำสุดเท่ากับ 1.72% บนไฟล์ข้อมูล P9 และมีอัตราการสูญหายสูงสุดเท่ากับ 4.52% บนไฟล์ข้อมูล P7 ในการทดลองที่ขนาดของไฟล์ข้อมูล P1 มีขนาด 50 เมกะไบต์ มีอัตราการสูญหายต่ำสุดเท่ากับ 4.10% บนไฟล์ข้อมูล P6 และมีอัตราการสูญหายสูงสุดเท่ากับ 7.81% บนไฟล์ข้อมูล P5 ในการทดลองที่ขนาดของไฟล์ข้อมูล P1 มีขนาด 100 เมกะไบต์ มีอัตราการสูญหายต่ำสุดเท่ากับ 0.58% บนไฟล์ข้อมูล P4 และมีอัตราการสูญหายสูงสุดเท่ากับ 1.40% บนไฟล์ข้อมูล P5 ในการทดลองที่ขนาดของไฟล์ข้อมูล P1 มีขนาด 500 เมกะไบต์ มีอัตราการสูญหายต่ำสุดเท่ากับ 0% บนไฟล์ข้อมูล P6 P8 และ P9 และมีอัตราการสูญหายสูงสุดเท่ากับ 0.28% บนไฟล์ข้อมูล P3 สุดท้ายในการทดลองที่ขนาดของไฟล์ข้อมูล P1 มีขนาด 1000 เมกะไบต์ มีอัตราการสูญหายต่ำสุดเท่ากับ 0.90% บนไฟล์ข้อมูล P5 และมีอัตราการสูญหายสูงสุดเท่ากับ 2.36% บนไฟล์ข้อมูล P3

การสูญหายของข้อมูลแบบต่อเนื่องที่เกิดขึ้นเป็นจำนวนมากจากการส่งข้อมูลในรอบใดรอบหนึ่งก็จะทำให้มีอัตราการสูญหายโดยรวมที่เกิดขึ้นกับไฟล์ข้อมูลนั้นสูงเช่นกัน แต่แพ็กเก็ตเหล่านั้นอาจส่งถึงผู้รับได้ในการส่งรอบอื่น ทำให้อัตราการสูญหายของข้อมูลจะไม่มีผลโดยตรงต่อ

จำนวนรอบที่ใช้ในการส่งข้อมูล ดังนั้นอัตราการสูญหายที่แสดงในตารางที่ 14 จึงไม่ใช้อัตราการสูญหายสูงสุดที่เกิดขึ้นในแต่ละไฟล์ข้อมูล แต่เป็นเพียงอัตราการสูญหายที่เกิดขึ้นที่ทำให้เกิดการใช้จำนวนรอบสูงสุดในการส่งข้อมูล ส่วนอัตราการสูญหายของข้อมูลสูงสุดที่เกิดขึ้นในแต่ละไฟล์ข้อมูลจากการส่งข้อมูลผ่านเครือข่ายดาวเทียมแสดงในตารางที่ 15

ตารางที่ 15 อัตราการสูญหายของแพ็กเก็ตสูงสุดในแต่ละไฟล์จากการส่งข้อมูลผ่านเครือข่ายดาวเทียม

ขนาดไฟล์ P1	ไฟล์ข้อมูล								
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**
1	2.59	0.72	2.46	3.14	0.71	1.91	0.48	0.58	0.27
5	0.31	10.03	5.00	24.40	0.51	1.96	46.68	3.23	0.89
10	4.01	3.16	3.95	4.11	3.21	2.81	4.52	3.26	1.72
50	6.43	5.92	5.01	5.46	7.81	5.76	7.76	7.67	4.44
100	0.98	1.24	0.90	0.58	1.40	1.03	1.20	0.68	0.88
500	0.19	0.11	0.28	0.07	0.14	0.00	0.05	0.00	0.00
1000	0.52	2.26	2.36	2.16	0.90	1.05	1.46	1.19	1.94

จากตารางที่ 15 แสดงให้เห็นว่ามี 6 ไฟล์ ที่มีอัตราการสูญหายของข้อมูลสูงสุด แต่ไม่ได้ใช้จำนวนรอบในการส่งข้อมูลสูงกว่าการทดลองที่เกิดอัตราการสูญหายต่ำกว่า ผลการเปรียบเทียบนี้เป็นการเปรียบเทียบกันของการทดลองทั้งหมด 4 ครั้ง และเป็นการเปรียบเทียบกันระหว่างไฟล์ข้อมูลเดียวกัน และในการทดลองที่ขนาดไฟล์ข้อมูล P1 มีขนาดเดียวกัน

ตารางที่ 16 จำนวนรอบสูงสุดที่ใช้ในการส่งข้อมูลผ่านเครือข่ายดาวเทียม

ขนาดไฟล์ P1	ไฟล์ข้อมูล								
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**
1	2	3	3	3	2	2	2	2	2
5	2	3	3	5	3	3	3	3	2
10	4	4	4	4	4	4	3	2	2
50	5	4	3	5	3	3	3	3	3
100	3	3	2	3	3	3	2	2	2
500	3	2	2	2	2	1	2	1	1
1000	3	4	3	3	2	2	2	2	2

ตารางที่ 16 แสดงจำนวนรอบสูงสุดที่ใช้ในการส่งข้อมูลผ่านเครือข่ายดาวเทียมช่องสัญญาณแบบทิศทางเดียว โดยผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 2 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุดเท่ากับ 3 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 5 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 2 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 5 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 10 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 2 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 4 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 50 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 3 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 5 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 100 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 2 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุดเท่ากับ 3 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 500 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 1 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 3 รอบ และสุดท้ายผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1000 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 2 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุดเท่ากับ 4 รอบ

จากผลของจำนวนรอบที่ใช้ในการส่งข้อมูลสำหรับไฟล์ข้อมูล P1 ที่ขนาดของไฟล์ข้อมูลที่แตกต่างกันทั้ง 7 ขนาด แสดงให้เห็นว่าขนาดของไฟล์ข้อมูลที่ใหญ่ขึ้นไม่ได้ส่งผลให้ใช้จำนวนรอบในการส่งข้อมูลเพิ่มขึ้น และสรุปได้ว่าจากผลการทดลองทั้งหมดมีอัตราการสูญหาย

ต่ำสุด 0% ที่ไฟล์ข้อมูล P6 P8 และ P9 ในการทดลองที่ขนาดไฟล์ข้อมูล P1 เป็น 500 เมกะไบต์ และอัตราการสูญหายสูงสุด 46.68% ที่ไฟล์ข้อมูล P7 ในการทดลองที่มีขนาดของไฟล์ข้อมูล P1 เป็น 5 เมกะไบต์ เมื่อเปรียบเทียบถึงอัตราการสูญหายที่เกิดขึ้น กับจำนวนรอบที่ใช้ในการส่งข้อมูล ทำให้ทราบว่าอัตราการสูญหายของข้อมูลที่สูงขึ้นไม่ได้ส่งผลให้ต้องใช้จำนวนรอบในการส่งข้อมูลมากขึ้นเสมอไป ตัวอย่างเช่น ไฟล์ข้อมูล P7 ที่การทดลองที่ขนาดไฟล์ข้อมูล P1 เป็น 5 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลเพียง 3 รอบ และมีอัตราการสูญหายเกิดขึ้นสูงถึง 46.68% แต่สำหรับไฟล์ข้อมูล P1 ที่การทดลองที่ขนาดของไฟล์ข้อมูล P1 เป็น 50 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลถึง 5 รอบ แต่มีอัตราการสูญหายเพียง 5.12%

ผลการทดลองการสร้างความน่าเชื่อถือด้วย Data Carousel ผ่านเครือข่ายดาวเทียม AI3 ช่องสัญญาณแบบทิศทางเดียว แสดงให้เห็นว่าขนาดของไฟล์ข้อมูลไม่มีผลโดยตรงต่อจำนวนรอบที่ใช้ในการส่งข้อมูล ส่วนอัตราการสูญหายที่สูงขึ้นก็ไม่ส่งผลให้ต้องใช้จำนวนรอบที่สูงขึ้นเสมอไป จากผลการทดลองทั้งหมดในส่วนนี้สามารถสรุปได้ว่า จำนวนรอบที่ต้องใช้ในการส่งข้อมูลจะขึ้นอยู่กับการสูญหายของแพ็กเก็ต โดยถึงแม้ว่าอัตราการสูญหายของข้อมูลโดยรวมที่เกิดขึ้นกับไฟล์ข้อมูลหนึ่งๆ จะมีไม่มาก แต่หากการสูญหายของแพ็กเก็ตเกิดขึ้นกับแพ็กเก็ตเดิมที่เคยสูญหายจากการส่งในรอบก่อนหน้า ก็จะทำให้ยังคงต้องส่งแพ็กเก็ตซ้ำทั้งหมดในรอบถัดไป ซึ่งการสูญหายของแพ็กเก็ตนี้ไม่สามารถระบุได้ว่าจะเกิดขึ้นเมื่อใดทำให้ไม่สามารถป้องกันการเกิดการสูญหายของแพ็กเก็ตเดิมที่เคยสูญหายจากการส่งในรอบก่อนหน้านี้ได้

3.2 ผลการทดลองบนเครือข่ายจำลอง NS-2

ผลการทดลองบนเครือข่าย NS-2 แบ่งออกเป็น 3 ส่วน ตามอัตราการสูญหายที่ได้กำหนดไว้ ได้แก่ 1% 10% และ 25% ได้แสดงตามตารางที่ 17 18 และ 19

ตารางที่ 17 จำนวนรอบสูงสุดที่ใช้ในการส่งข้อมูลบนเครือข่ายจำลอง NS-2 ที่อัตราการสูญหาย 1%

ขนาด	ไฟล์ข้อมูล								
ไฟล์ P1	P1	P2	P3	P4	P5	P6	P7	P8	P9
1	2	3	3	3	3	3	3	3	2
5	3	3	3	3	3	3	3	3	3
10	2	3	3	3	3	2	3	2	3
50	3	3	3	2	3	3	2	3	2
100	4	3	3	3	3	2	2	2	3
500	3	3	3	2	3	3	3	2	2
1000	4	4	3	3	3	3	2	2	2

ในการทดลองที่อัตราการสูญหาย 1% ที่แสดงในตารางที่ 17 ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 2 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 3 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 5 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลเท่ากับ 3 รอบ ทุกไฟล์ข้อมูล ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 10 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 2 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 3 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 50 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 2 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 3 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 100 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 2 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 4 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 500 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 2 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 3 รอบ และสุดท้ายผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1000 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 2 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 4 รอบ และจากผลการทดลองที่อัตราการสูญหายที่ 1% นี้ แสดงให้เห็นว่าจำนวนรอบที่ใช้ในการส่งข้อมูลสำหรับไฟล์ข้อมูล P1 ทั้ง 7 ขนาด มีแนวโน้มสูงขึ้นแต่การเพิ่มขึ้นของจำนวนรอบที่ใช้ในการส่งข้อมูลนี้ไม่เป็นการเพิ่มขึ้นทุกครั้งที่ขนาดของไฟล์ข้อมูลเพิ่มขึ้น และยังคงมีบางไฟล์ข้อมูลที่มีขนาดใหญ่กว่าแต่ใช้จำนวนรอบน้อยกว่าไฟล์ข้อมูลที่มีขนาดเล็กกว่า

ตารางที่ 18 จำนวนรอบสูงสุดที่ใช้ในการส่งข้อมูลบนเครือข่ายจำลอง NS-2 ที่อัตราการสูญหาย 10%

ขนาดไฟล์ P1	ไฟล์ข้อมูล								
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**
1	4	6	6	5	5	5	5	5	4
5	5	5	7	5	5	5	5	4	4
10	5	5	5	5	5	5	5	4	4
50	6	6	5	6	4	4	5	4	4
100	6	5	5	5	5	5	4	5	4
500	6	6	5	5	5	4	5	4	4
1000	7	6	5	6	5	6	4	5	4

ในการทดลองที่อัตราการสูญหาย 10% ที่แสดงในตารางที่ 18 ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 4 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 6 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 5 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 4 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 7 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 10 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 4 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 5 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 50 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 4 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 6 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 100 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 4 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 6 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 500 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 4 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 6 รอบ และสุดท้ายผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1000 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 4 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 7 รอบ และจากผลการทดลองที่อัตราการสูญหาย 10% ผลจำนวนรอบที่ใช้ในการส่งข้อมูลสำหรับไฟล์ข้อมูล P1 ทั้ง 7 ขนาด แสดงให้เห็นว่าเมื่อไฟล์ข้อมูลใหญ่ขึ้นจะมีแนวโน้มในการใช้จำนวนรอบในการส่งข้อมูลสูงขึ้นเช่นกัน โดยถึงแม้การเพิ่มขึ้นของจำนวนรอบที่ใช้ในการส่งข้อมูลนี้จะไม่เพิ่มขึ้นทุกครั้งที่ขนาดของไฟล์ข้อมูลเพิ่มขึ้น แต่ผลการทดลองที่อัตราการสูญหาย 10% นี้แสดงให้เห็นชัดเจนกว่าผลการทดลองที่อัตราการสูญหาย 1% ว่าจำนวนรอบที่

ใช้ในการส่งข้อมูลมีแนวโน้มสูงขึ้นเมื่อขนาดของไฟล์ข้อมูลเพิ่มสูงขึ้น เพราะถึงแม้ผลจำนวนรอบที่ใช้ในการส่งข้อมูลที่อัตราการสูญหายที่ 10% นี้ จะไม่ใช้จำนวนรอบในการส่งข้อมูลเพิ่มขึ้นทุกครั้งที่ขนาดของไฟล์ข้อมูลเพิ่มสูงขึ้น แต่ก็ใช้จำนวนรอบในการส่งข้อมูลไม่น้อยกว่าจำนวนรอบในการส่งข้อมูลของไฟล์ข้อมูลที่มีขนาดเล็กกว่า ซึ่งผลการทดลองที่อัตราการสูญหาย 1% นั้นมีบางไฟล์ข้อมูลที่ใช้จำนวนรอบในการส่งข้อมูลน้อยกว่าไฟล์ข้อมูลที่มีขนาดเล็กกว่า

ตารางที่ 19 จำนวนรอบสูงสุดที่ใช้ในการส่งข้อมูลบนเครือข่ายจำลอง NS-2 ที่อัตราการสูญหาย 25%

ขนาดไฟล์ P1	**ไฟล์ข้อมูล**								
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**
1	6	9	14	7	8	8	8	8	6
5	7	10	9	8	8	8	7	7	5
10	8	12	10	7	10	7	7	7	7
50	9	9	8	8	7	9	6	7	7
100	10	11	10	10	9	6	7	7	6
500	10	9	8	8	8	7	7	7	8
1000	12	9	8	9	8	7	8	7	6

ในการทดลองที่อัตราการสูญหาย 25% ที่แสดงในตารางที่ 19 ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 6 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 14 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 5 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 5 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 10 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 10 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 7 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 12 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 50 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 7 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 9 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 100 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 6 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 11 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 500 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 7 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 10 รอบ และสุดท้ายผลการทดลองที่

ไฟล์ข้อมูล P1 มีขนาด 1000 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 6 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 12 รอบ และจากผลจากการทดลองที่อัตราการสูญหาย 25% นี้แสดงให้เห็นผลชัดเจนกว่าผลการทดลองจากอัตราการสูญหายที่ 1% และ 10% ในด้านของขนาดของไฟล์ข้อมูลที่มีผลต่อจำนวนรอบที่ใช้ในการส่งข้อมูล เนื่องจากจะเห็นได้ว่าจำนวนรอบที่ใช้ในการส่งข้อมูลสำหรับไฟล์ข้อมูล P1 ทั้ง 7 ขนาด ที่การเพิ่มขึ้นของจำนวนรอบที่ใช้ในการส่งข้อมูลเกือบทุกครั้งที่ขนาดของไฟล์ข้อมูลเพิ่มสูงขึ้น ซึ่งมีเพียงครั้งเดียวที่จำนวนรอบที่ใช้ในการส่งข้อมูลไม่เพิ่มขึ้นในขณะที่ขนาดของไฟล์ข้อมูลเพิ่มขึ้น คือผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 500 เมกะไบต์ แต่อย่างไรก็ตามจำนวนรอบสูงสุดที่ใช้ในการส่งข้อมูลจากผลการทดลองที่อัตราการสูญหาย 25% นี้คือ 14 รอบ ซึ่งเกิดที่ไฟล์ข้อมูล P3 ที่การทดลองที่ไฟล์ข้อมูล P1 ขนาด 1 เมกะไบต์ โดยไฟล์ข้อมูล P3 นี้มีขนาดของไฟล์ข้อมูลเพียง 20 เมกะไบต์ แสดงให้เห็นว่าไฟล์ข้อมูลที่มีขนาดเล็กกว่าอาจใช้จำนวนรอบในการส่งข้อมูลมากกว่าไฟล์ข้อมูลที่มีขนาดใหญ่กว่าได้ในกรณีที่มีอัตราการสูญหายใกล้เคียงกัน

จากผลการทดลองที่ใช้ อัตราการสูญหายที่แตกต่างกัน 3 อัตรา แสดงให้เห็นว่าขนาดของไฟล์ข้อมูลมีผลในการใช้จำนวนรอบในการส่งข้อมูลสูงขึ้น และเมื่ออัตราการสูญหายของข้อมูลสูงขึ้นจะต้องใช้จำนวนรอบที่มากขึ้นตามลำดับ แต่อย่างไรก็ตามขนาดของไฟล์ข้อมูลที่มีขนาดเล็กกว่าอาจใช้จำนวนรอบในการส่งข้อมูลสูงกว่าไฟล์ข้อมูลที่มีขนาดใหญ่กว่าได้เช่นกัน เนื่องจากไม่สามารถทราบล่วงหน้าถึงการสูญหายของแพ็กเก็ต จึงทำให้ไม่สามารถป้องกันไม่ให้แพ็กเก็ตที่เคยสูญหายในรอบก่อนหน้าสูญหายซ้ำอีกได้ ผลที่ได้จากการบนเครือข่ายจำลอง NS-2 ให้ผลสอดคล้องกับผลที่ได้จากการทดลองผ่านเครือข่ายดาวเทียม AI3 แม้ว่าอัตราการสูญหายที่เกิดขึ้นกับไฟล์ข้อมูลหนึ่งมีอัตราการสูญหายที่เกิดขึ้นต่ำกว่าอีกไฟล์ข้อมูลหนึ่ง แต่อาจต้องใช้จำนวนรอบในการส่งข้อมูลมากกว่าได้ เนื่องจากไม่สามารถควบคุมการสูญหายของแพ็กเก็ต และป้องกันการเกิดการสูญหายซ้ำที่แพ็กเก็ตเดิมที่เคยสูญหายได้

3.3 ผลการทดลองบนเครือข่ายจำลอง Dummynet

ผลการทดลองบนเครือข่าย Dummynet แบ่งออกเป็น 3 ส่วน ตามอัตราการสูญหายที่ได้กำหนดไว้ ได้แก่ 1% 10% และ 25% ได้แสดงตามตารางที่ 20 21 และ 22 ตามลำดับ

ตารางที่ 20 จำนวนรอบสูงสุดที่ใช้ในการส่งข้อมูลบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 1%

ขนาดไฟล์ P1	ไฟล์ข้อมูล								
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**
1	2	3	2	3	2	3	2	2	2
5	3	3	3	2	3	2	2	2	2
10	3	3	3	3	2	2	3	2	2
50	3	3	3	3	3	2	3	2	2
100	3	3	3	3	3	2	2	2	3
500	3	3	2	3	3	3	2	2	2
1000	4	3	2	3	2	3	2	2	2

ในการทดลองที่อัตราการสูญหาย 1% ที่แสดงในตารางที่ 20 ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1 5 10 50 100 และ 500 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 2 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 3 รอบ ส่วนผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1000 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 2 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 4 รอบ และจากผลการทดลองที่อัตราการสูญหาย 1% นี้แสดงให้เห็นว่าผลจำนวนรอบที่ใช้ในการส่งข้อมูลจากไฟล์ข้อมูล P1 ทั้ง 7 ขนาด มีแนวโน้มสูงขึ้น เมื่อขนาดของไฟล์ข้อมูลเพิ่มสูงขึ้น ถึงแม้การเพิ่มขึ้นของจำนวนรอบที่ใช้ในการส่งข้อมูลจะไม่ได้เพิ่มขึ้นทุกครั้งที่ขนาดของไฟล์ข้อมูลเพิ่มขึ้นก็ตาม เช่นกรณีไฟล์ข้อมูล P1 ในการทดลองที่ไฟล์ข้อมูลมีขนาด 5 10 50 100 และ 500 เมกะไบต์ ใช้จำนวนรอบในการส่งข้อมูลเท่ากันที่ 3 รอบ แต่อย่างไรก็ตามการเพิ่มขึ้นของจำนวนรอบที่ใช้ในการส่งข้อมูลสำหรับการทดลองที่อัตราการสูญหาย 1% บนเครือข่ายจำลอง Dummynet นี้ ให้ผลที่ชัดเจนกว่าผลการทดลองที่อัตราการสูญหาย 1% บนเครือข่ายจำลอง NS-2 เนื่องจากผลการทดลองที่อัตราการสูญหาย 1% บนเครือข่ายจำลอง NS-2 นั้น ไฟล์ข้อมูลที่มีขนาดใหญ่กว่า อาจใช้จำนวนรอบในการส่งข้อมูลน้อยกว่าไฟล์ข้อมูลที่มีขนาดเล็กกว่า แต่ผลการทดลองที่อัตราการสูญหาย 1% บนเครือข่ายจำลอง Dummynet ไม่มีผลเช่นนั้น

ตารางที่ 21 จำนวนรอบสูงสุดที่ใช้ในการส่งข้อมูลบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 10%

ขนาดไฟล์ P1	ไฟล์ข้อมูล								
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**
1	3	5	5	4	4	4	4	3	4
5	4	5	6	4	5	4	6	4	3
10	5	4	4	4	4	4	6	4	4
50	5	4	5	4	4	4	4	4	4
100	5	5	6	6	6	4	3	4	3
500	7	5	4	6	4	4	4	5	3
1000	7	6	4	5	5	5	3	4	4

ในการทดลองที่อัตราการสูญหาย 10% ที่แสดงในตารางที่ 21 ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 3 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 5 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 5 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 3 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 6 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 10 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 4 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 6 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 50 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 4 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 5 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 100 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 3 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 5 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 500 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 3 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 7 รอบ และสุดท้ายผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1000 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 3 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 7 รอบ และจากผลการทดลองที่อัตราการสูญหาย 10% จำนวนรอบที่ใช้ในการส่งข้อมูลจากไฟล์ข้อมูล P1 ทั้ง 7 ขนาด แสดงให้เห็นว่า เมื่อไฟล์ข้อมูลมีขนาดใหญ่ขึ้น แนวโน้มในการใช้จำนวนรอบในการส่งข้อมูลจะสูงขึ้น แต่การเพิ่มขึ้นของจำนวนรอบในการส่งข้อมูลจากผลการทดลองที่อัตราการสูญหาย 10% นี้ ไม่เพิ่มขึ้นทุกครั้งเมื่อขนาดของไฟล์ข้อมูลเพิ่มขึ้น

ตารางที่ 22 จำนวนรอบสูงสุดที่ใช้ในการส่งข้อมูลบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 25%

ขนาดไฟล์ P1	ไฟล์ข้อมูล								
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**
1	5	8	7	7	8	7	6	6	7
5	8	7	9	8	7	8	6	7	5
10	8	8	8	10	7	6	7	5	6
50	13	12	7	7	6	6	7	5	6
100	10	8	7	9	7	6	6	6	4
500	11	11	11	9	6	9	6	5	5
1000	10	8	7	8	7	7	8	6	6

ในการทดลองที่อัตราการสูญหาย 25% ที่แสดงในตารางที่ 22 ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 5 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุดเท่ากับ 8 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 5 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 5 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 9 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 10 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 5 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 10 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 50 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 5 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 13 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 100 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 4 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 10 รอบ ผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 500 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 5 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 11 รอบ และสุดท้ายผลการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1000 เมกะไบต์ มีการใช้จำนวนรอบในการส่งข้อมูลต่ำสุดเท่ากับ 6 รอบ และใช้จำนวนรอบในการส่งข้อมูลสูงสุด 10 รอบ และผลการทดลองที่อัตราการสูญหาย 25% จำนวนรอบที่ใช้ในการส่งข้อมูลสำหรับการทดลองนี้มีแนวโน้มเพิ่มขึ้นเมื่อไฟล์ข้อมูลมีขนาดใหญ่ขึ้นซึ่งสังเกตได้จากผลการทดลองของไฟล์ข้อมูล P1 ทั้ง 7 ขนาด เช่นกัน แต่การเพิ่มขึ้นของจำนวนรอบที่ใช้ในการส่งข้อมูลจากผลการการทดลองที่อัตราการสูญหาย 25% นี้ไม่เป็นการเพิ่มขึ้นทุกครั้ง

ที่ขนาดของไฟล์ข้อมูลเพิ่มขึ้น อีกทั้งยังมีบางไฟล์ข้อมูลที่มีขนาดของไฟล์ข้อมูลใหญ่กว่าแต่ใช้จำนวนรอบในการส่งข้อมูลน้อยกว่า

จากผลการทดลองทั้ง 3 อัตราการสูญหาย โดยจำนวนรอบที่ใช้ในการส่งข้อมูลสำหรับไฟล์ข้อมูล P1 ทั้ง 7 ขนาด แสดงให้เห็นว่าขนาดของไฟล์ข้อมูลที่มีขนาดใหญ่ขึ้นมีแนวโน้มในการใช้จำนวนรอบในการส่งข้อมูลสูงขึ้นแต่ไม่เป็นผลเสมอไป ส่วนอัตราการสูญหายที่เพิ่มขึ้นนั้นแสดงให้เห็นว่าจำนวนรอบที่ต้องใช้ในการส่งข้อมูลมีแนวโน้มสูงขึ้น แต่ก็ไม่ได้เป็นผลทุกครั้งไปเช่นกัน ซึ่งมีสาเหตุเนื่องมาจากการสูญหายของแพ็กเก็ตที่ไม่สามารถทราบได้ว่าจะเกิดขึ้นเมื่อใด ทำให้ไม่สามารถควบคุมการสูญหายของแพ็กเก็ตไม่ให้เกิดการสูญหายกับแพ็กเก็ตเดิมที่เคยสูญหายได้

ผลการทดลองจากทั้ง 3 เครือข่าย ได้แก่ ระบบเครือข่ายดาวเทียม AI3 สำหรับช่องสัญญาณดาวเทียมแบบทิศทางเดียว ระบบจำลองเครือข่าย NS-2 และระบบจำลองเครือข่าย Dummynet ได้แสดงให้เห็นว่าจำนวนรอบที่ใช้ในการส่งข้อมูลขึ้นอยู่กับการสูญหายของแพ็กเก็ต ซึ่งเนื่องมาจากการที่ไม่สามารถระบุ หรือทราบได้ว่าแพ็กเก็ตจะเกิดการสูญหายเมื่อใดหรือแพ็กเก็ตใด ทำให้ไม่สามารถควบคุมไม่ให้แพ็กเก็ตที่ส่งไปซ้ำในรอบถัดไปเกิดการสูญหายซ้ำได้ จึงทำให้ต้องส่งแพ็กเก็ตซ้ำเป็นจำนวนหลายๆ รอบ แต่อย่างไรก็ตามจากผลการทดลองที่ได้จากทั้ง 3 เครือข่าย ทำให้ทราบว่าขนาดของไฟล์ข้อมูลที่เพิ่มขึ้น มีผลทำให้จำนวนรอบที่ใช้ในการส่งข้อมูลมีแนวโน้มเพิ่มขึ้นถึงแม้จะไม่เป็นผลเสมอไป และอัตราการสูญหายที่เพิ่มขึ้นก็ส่งผลให้จำนวนรอบที่ใช้ในการส่งข้อมูลมีแนวโน้มเพิ่มขึ้นเช่นกัน ถึงแม้จะไม่เป็นผลเสมอไปก็ตาม แต่เมื่อทั้งขนาดของไฟล์ข้อมูลและอัตราการสูญหายเพิ่มขึ้น จำนวนรอบที่ต้องใช้ในการส่งข้อมูลจะมีแนวโน้มเพิ่มขึ้นเสมอ

4. <u>ผลการศึกษาประสิทธิภาพการสร้างความน่าเชื่อถือด้วยวิธีการบรอดคาสต์ดิสค์และ FEC (Reed-Solomon Codes พัฒนาด้วย Cauchy Matrices)</u>

จากการทดลองที่ผ่านมาพบว่าอัตราการสูญหายที่เกิดขึ้นทั้งหมด จะมีอัตราการสูญหายไม่เกินครึ่งหนึ่ง ซึ่งหมายถึงจำนวนข้อมูลทั้งหมด (ข้อมูลต้นฉบับที่ถูกส่งในรอบที่หนึ่ง และข้อมูลสำเนาที่ถูกส่งในรอบถัดๆ ไป) มีการสูญหายโดยรวมไม่เกินครึ่งหนึ่ง แต่จำนวนรอบที่ใช้ในการส่งไฟล์ข้อมูลส่วนใหญ่กลับต้องใช้มากกว่า 2 รอบ เนื่องจากแพ็กเก็ตในลำดับที่เดียวกันมีการสูญหายมากกว่า 2 รอบ และแพ็กเก็ตส่วนใหญ่ผู้รับสามารถรับได้มากกว่าหนึ่งครั้ง จะเห็นได้ว่าแพ็กเก็ตที่ส่งไปตั้งแต่รอบที่ 2 เป็นต้นไป เป็นได้ทั้งแพ็กเก็ตที่ผู้รับเคยได้รับ และเป็นแพ็กเก็ตที่ผู้รับยังไม่ได้

รับ หากเราสามารถทำให้แต่ละแพ็กเก็ตที่ส่งออกไปในรอบที่ 2 สามารถใช้กู้คืนแพ็กเก็ตในลำดับใดๆ ได้ที่ไม่ขึ้นกับลำดับแพ็กเก็ตในรอบแรก ก็จะทำให้ประสิทธิภาพในการส่งข้อมูลซ้ำในรอบที่ 2 มีประสิทธิภาพสูงขึ้น ซึ่งอาจทำให้ไม่จำเป็นต้องส่งข้อมูลมากกว่า 2 รอบ ในการเพิ่มประสิทธิภาพของข้อมูลส่วนที่ถูกส่งไปซ้ำนี้ ได้ถูกทดลองโดยการใช้วิธีการ FEC แบบ Reed-Solomon Codes ที่พัฒนาด้วย Cauchy Matrices โดยนำมาใช้ในการสร้างแพ็กเก็ตพิเศษ และส่งแพ็กเก็ตพิเศษเหล่านี้ไปยังผู้รับสำหรับใช้ในการถอดรหัสเพื่อกู้คืนแพ็กเก็ตต้นฉบับใดๆ ที่สูญหายการจากส่งในรอบแรก

ผลที่ได้จากการทดลองครั้งนี้แสดงให้เห็นว่าการนำวิธีการ FEC มาใช้ในการสร้างแพ็กเก็ตพิเศษ เพื่อใช้ในการส่งไปยังผู้รับแทนการส่งสำเนาแพ็กเก็ตต้นฉบับ สามารถทำให้ผู้รับรับแพ็กเก็ตพิเศษและนำมาถอดรหัสเพื่อกู้คืนแพ็กเก็ตต้นฉบับที่สูญหาย เพื่อสร้างไฟล์ข้อมูลต้นฉบับได้ด้วยการส่งแพ็กเก็ตต้นฉบับเพียงหนึ่งรอบ และส่งแพ็กเก็ตพิเศษอีกหนึ่งรอบ ซึ่งสามารถเปรียบเทียบได้เท่ากับการส่งข้อมูลจำนวน 2 รอบ ผลการทดลองนี้เป็นผลที่ได้จากการทดลองทั้งเครือข่ายดาวเทียม AI3 และเครือข่ายจำลอง Dummynet ที่อัตราการสูญหายของข้อมูล 1% 10% และ 25% ส่วนการทดลองบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหายของข้อมูล 50% นั้น มีเพียงบางไฟล์ข้อมูลที่ผู้รับสามารถรับแพ็กเก็ตได้เพียงพอสำหรับการสร้างไฟล์ข้อมูลต้นฉบับ ผลการทดลองเพื่อศึกษาประสิทธิภาพการสร้างความน่าเชื่อถือในส่วนนี้ได้แบ่งออกเป็น 2 ส่วน ตามประเภทของเครือข่ายที่ใช้ในการทดลอง ซึ่งได้แก่ เครือข่ายดาวเทียม AI3 และเครือข่ายจำลอง Dummynet

เนื่องด้วยข้อจำกัดทางด้านประสิทธิภาพในการเข้ารหัส และถอดรหัสข้อมูลของวิธีการ FEC แบบ Reed-Solomon Codes ที่พัฒนาด้วย Cauchy Matrices ซึ่งต้องใช้เวลามากขึ้นเป็น 4 เท่าสำหรับทุกๆ ขนาดของไฟล์ข้อมูลที่เพิ่มขึ้น 2 เท่า ทำให้การนำวิธีการเข้ารหัสเข้ามาเพื่อช่วยเพิ่มประสิทธิภาพในการสร้างความน่าเชื่อถือต้องใช้วิธีการแบ่งข้อมูลออกเป็นบล็อคให้มีขนาดที่เล็กก่อน เพื่อช่วยเพิ่มประสิทธิภาพด้านเวลาที่ใช้ในการเข้ารหัสและถอดรหัสข้อมูล และจากผลการทดลองทำให้พบข้อจำกัดที่เกิดจากการแบ่งข้อมูลออกเป็นส่วนๆ เพื่อเพิ่มประสิทธิภาพด้านเวลาที่ใช้ในการเข้ารหัสและถอดรหัสข้อมูล และเนื่องด้วยจำนวนรอบที่ใช้ในการส่งข้อมูลสำหรับทุกไฟล์ข้อมูลเป็นเพียงหนึ่งรอบสำหรับข้อมูลแพ็กเก็ตต้นฉบับ และอีกหนึ่งรอบสำหรับแพ็กเก็ตพิเศษ ผลการทดลองที่แสดงถัดไปนี้จึงเป็นแสดงเพียงอัตราการสูญหายที่เกิดขึ้นที่ได้จากการทดลอง

4.1 อัตราการสูญหายจากผลการทดลองผ่านเครือข่ายดาวเทียม AI3 สำหรับช่องสัญญาณแบบทิศทางเดียว (UDL)

การทดลองทั้งหมดในส่วนนี้การทดลองที่ไฟล์ข้อมูล P1 มีขนาด 5 เมกะไบต์ ไม่มีการเกิดการสูญหายขึ้นทั้ง 9 ไฟล์ข้อมูล จึงแสดงอัตราการสูญหายเป็น 0% ทั้งหมด ดังนั้นผลอัตราการสูญหายที่แสดงในตารางที่ 23 และ 24 สำหรับการทดลองในไฟล์ข้อมูล P1 มีขนาด 5 เมกะไบต์ จะแสดงเป็น 0% ทั้งหมด

ตารางที่ 23 อัตราการสูญหายจากบล็อคที่มีอัตราการสูญหายสูงสุดผ่านเครือข่ายดาวเทียม

ขนาด	**ไฟล์ข้อมูล**								
ไฟล์ P1	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**
1	0.26	0.15	0.21	0.08	0.20	0.08	0.00	0.03	0.00
5	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
10	0.56	3.18	0.73	0.30	2.19	2.15	2.00	0.30	0.39
50	5.25	5.20	4.60	9.01	4.89	4.28	4.21	4.38	4.93
100	2.75	1.40	0.00	0.00	0.03	1.05	0.00	0.03	0.00
500	4.68	1.18	0.55	0.30	1.06	0.10	0.24	0.03	0.00
1000	4.20	0.00	0.05	0.00	0.00	0.00	0.00	0.00	0.00

ตารางที่ 24 อัตราการสูญหายเฉลี่ยจากทุกบล็อคผ่านเครือข่ายดาวเทียม

ขนาดไฟล์ P1	ไฟล์ข้อมูล								
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**
1	0.26	0.07	0.08	0.06	0.18	0.05	0.00	0.03	0.00
5	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
10	0.41	1.35	0.22	0.11	1.33	1.78	2.00	0.30	0.39
50	4.62	4.62	4.34	5.32	4.54	4.18	4.21	4.38	4.93
100	0.41	0.33	0.00	0.00	0.03	0.69	0.00	0.03	0.00
500	0.51	0.29	0.16	0.18	0.59	0.03	0.24	0.03	0.00
1000	0.51	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00

ในตารางที่ 23 ซึ่งแสดงอัตราการสูญหายของข้อมูลจากบล็อคที่มีอัตราการสูญหายสูงสุด แสดงให้เห็นว่าไฟล์ข้อมูล P4 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 50 เมกะไบต์ เกิดอัตราการสูญหายสูงสุดเท่ากับ 9.01% ส่วนอัตราการสูญหายของข้อมูลเฉลี่ยจากทุกบล็อคของแต่ละไฟล์ข้อมูลได้แสดงในตารางที่ 24 โดยมีอัตราการสูญหายสูงสุดเท่ากับ 5.32% ที่ไฟล์ข้อมูล P4 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 50 เมกะไบต์ การทดลองที่ไฟล์ข้อมูล P1 มีขนาด 50 เมกะไบต์ มีอัตราการสูญหายเกิดขึ้นสูงสุด โดยมีอัตราการสูญหายเฉลี่ยทั้ง 9 ไฟล์ข้อมูลเท่ากับ 4.57% จากผลการทดลองแสดงให้เห็นว่ามีอัตราการสูญหายของข้อมูลค่อนข้างต่ำ จำนวนแพ็กเก็ตพิเศษที่ส่งไปเท่ากับจำนวนแพ็กเก็ตต้นฉบับนั้น สามารถใช้กู้คืนข้อมูลแพ็กเก็ตต้นฉบับในกรณีที่มีการสูญหายได้ถึงครึ่งหนึ่ง ดังนั้นเมื่อไฟล์ข้อมูลที่มีอัตราการสูญหายไม่มาก แพ็กเก็ตพิเศษที่ถูกส่งไปจึงถูกนำไปใช้งานเพียงจำนวนไม่มากเช่นกัน ดังนั้นหากเราทราบหรือประมาณค่าอัตราการสูญหายที่จะเกิดขึ้นได้ จะทำให้เราสามารถปรับอัตราส่วนจำนวนแพ็กเก็ตพิเศษให้พอดีกับความต้องการใช้งานได้ เพื่อเป็นการลดจำนวนข้อมูลที่ไม่จำเป็นบนระบบเครือข่าย

4.2 ผลการทดลองบนเครือข่ายจำลอง Dummynet

ผลการทดลองบนเครือข่ายจำลอง Dummynet จะถูกแบ่งออกเป็น 4 ส่วน ตามอัตราการสูญหายที่กำหนดไว้ 3 อัตรา ได้แก่ 1% 10% และ 25% ส่วนการทดลองพิเศษที่อัตราการสูญหาย

50% เป็นทดลองเพื่อแสดงให้เห็นถึงข้อจำกัดของการสร้างความน่าเชื่อถือด้วยการใช้ FEC ซึ่งจะแสดงเป็นส่วนสุดท้าย

ตารางที่ 25 อัตราการสูญหายจากบล็อคที่มีอัตราการสูญหายสูงสุดบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 1%

ขนาดไฟล์ P1	ไฟล์ข้อมูล								
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**
1	0.86	1.48	1.20	1.20	1.28	0.91	0.81	0.89	1.18
5	1.06	1.23	1.50	1.15	1.11	1.11	1.14	0.79	1.12
10	1.15	1.18	1.20	1.05	1.15	1.20	1.21	0.69	0.53
50	1.33	1.38	1.13	1.22	0.95	0.80	1.01	1.02	1.91
100	1.30	1.25	1.13	1.33	1.48	0.98	0.94	1.18	0.86
500	4.80	1.48	1.13	1.31	1.25	1.13	0.77	1.28	1.12
1000	1.40	1.43	1.29	0.98	1.19	1.13	0.72	1.12	0.72

ตารางที่ 26 อัตราการสูญหายเฉลี่ยจากทุกบล็อคบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 1%

ขนาดไฟล์ P1	ไฟล์ข้อมูล								
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**
1	0.86	1.00	0.99	1.11	1.14	0.90	0.81	0.89	1.18
5	1.05	1.01	1.04	1.01	0.91	0.90	1.14	0.79	1.12
10	1.02	0.95	0.97	0.89	0.92	1.05	1.21	0.69	0.53
50	1.04	1.00	0.91	1.11	0.91	0.79	1.01	1.02	1.91
100	0.99	1.02	0.97	1.07	1.38	0.97	0.94	1.18	0.86
500	1.03	1.04	0.98	1.05	1.11	1.04	0.77	1.28	1.12
1000	0.99	1.00	0.96	0.87	1.03	1.07	0.72	1.12	0.72

ในตารางที่ 25 ได้แสดงอัตราการสูญหายของข้อมูลจากบล็อคที่มีอัตราการสูญหายสูงสุด ผลจากการทดลองบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 1% โดยมีอัตราการสูญหายสูงสุดเท่ากับ 4.80% ที่ไฟล์ข้อมูล P1 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 500 เมกะไบต์ และมีอัตราการสูญหายต่ำสุดเท่ากับ 0.53% ที่ไฟล์ข้อมูล P9 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 10 เมกะไบต์ ส่วนอัตราการสูญหายของข้อมูลเฉลี่ยจากทุกบล็อคของแต่ละไฟล์ข้อมูลได้แสดงในตารางที่ 26 โดยมีอัตราการสูญหายสูงสุดเท่ากับ 1.38% ที่ไฟล์ข้อมูล P5 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 100 เมกะไบต์ และมีอัตราการสูญหายต่ำสุดเท่ากับ 0.53% ที่ไฟล์ข้อมูล P9 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 10 เมกะไบต์

จากการวิเคราะห์อัตราการสูญหายที่เกิดขึ้นในผลการทดลองที่อัตราการสูญหาย 1% นั้น มีบล็อคที่มีอัตราการสูญหายเกิดขึ้นสูงสุดถึง 4.80% ที่ไฟล์ข้อมูล P1 ในการทดลองที่ไฟล์ข้อมูล P1 ขนาด 500 เมกะไบต์ ตามที่แสดงในตารางที่ 25 ซึ่งในการทดลองนี้กำหนดอัตราการสูญหายเพียง 1% และผลของอัตราการสูญหายเฉลี่ยทั้ง 9 ไฟล์ข้อมูล เกิดขึ้นเท่ากับ 1.04% แสดงให้เห็นว่าการสุ่มการสูญหายของแพ็กเก็ตจากโปรแกรมจำลองเครือข่าย Dummynet ให้ผลคล้ายกับผลการทดลองผ่านเครือข่ายดาวเทียม AI3 ช่องสัญญาณแบบทิศทางเดียว คือ การสูญหายของแพ็กเก็ตอาจเกิดขึ้นมากในบล็อคใดบล็อคหนึ่งได้

ตารางที่ 27 อัตราการสูญหายจากบล็อคที่มีอัตราการสูญหายสูงสุดบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 10%

ขนาดไฟล์ P1	**ไฟล์ข้อมูล**								
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**
1	9.47	10.70	11.80	10.32	10.58	10.67	9.50	10.03	10.07
5	10.14	10.70	10.63	10.08	10.19	10.48	10.39	9.84	8.42
10	10.60	11.00	10.63	10.38	10.11	9.81	9.87	9.54	11.18
50	11.48	10.95	10.13	11.16	10.53	10.58	9.89	9.70	9.34
100	11.15	10.65	10.53	11.00	9.75	10.15	10.18	10.53	10.92
500	11.15	10.60	10.80	10.60	9.89	10.10	10.18	9.54	10.66
1000	11.15	10.75	11.00	11.10	10.47	10.10	9.74	10.16	12.63

ตารางที่ 28 อัตราการสูญหายเฉลี่ยจากทุกบล็อคบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 10%

ขนาดไฟล์ P1	ไฟล์ข้อมูล								
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**
1	9.47	9.91	10.15	9.83	10.29	10.38	9.50	10.03	10.07
5	10.05	10.00	10.09	9.84	9.72	9.79	10.39	9.84	8.42
10	10.06	10.09	10.16	9.99	9.63	9.65	9.87	9.54	11.18
50	10.00	10.08	9.69	10.61	10.13	9.64	9.89	9.70	9.34
100	9.99	9.99	10.00	10.19	9.75	9.93	10.18	10.53	10.92
500	9.95	10.07	10.21	10.11	9.88	9.77	10.18	9.54	10.66
1000	10.00	9.96	10.23	10.69	10.32	9.51	9.74	10.16	12.63

อัตราการสูญหายของข้อมูลจากบล็อคที่มีอัตราการสูญหายสูงสุด จากการทดลองบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 10% แสดงในตารางที่ 27 โดยมีอัตราการสูญหายสูงสุดเท่ากับ 12.63% ที่ไฟล์ข้อมูล P9 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1000 เมกะไบต์ และมีอัตราการสูญหายต่ำสุด 8.42% ที่ไฟล์ข้อมูล P9 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 5 เมกะไบต์ ส่วนอัตราการสูญหายของข้อมูลเฉลี่ยจากทุกบล็อคของแต่ละไฟล์ข้อมูลได้แสดงในตารางที่ 28 โดยมีอัตราการสูญหายสูงสุดเท่ากับ 12.63% ที่ไฟล์ข้อมูล P9 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1000 เมกะไบต์ และมีอัตราการสูญหายต่ำสุดเท่ากับ 8.42% ที่ไฟล์ข้อมูล P9 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 5 เมกะไบต์

ตารางที่ 29 อัตราการสูญหายจากบล็อคที่มีอัตราการสูญหายสูงสุดบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 25%

ขนาดไฟล์ P1	ไฟล์ข้อมูล								
	P1	P2	P3	P4	P5	P6	P7	P8	P9
1	23.82	25.70	26.15	25.58	25.68	25.33	24.89	23.19	25.07
5	24.56	25.68	25.95	26.00	25.70	25.63	25.37	24.80	24.01
10	27.17	25.65	26.33	26.08	24.88	25.40	25.33	25.26	26.12
50	25.58	25.55	26.43	26.27	25.61	26.39	24.63	24.64	25.33
100	26.50	26.13	25.70	26.43	25.83	25.98	24.74	24.61	24.41
500	27.10	25.88	26.65	26.02	25.63	25.03	24.25	24.57	24.01
1000	26.55	26.30	26.68	26.33	25.08	24.65	25.48	24.57	26.12

ตารางที่ 30 อัตราการสูญหายเฉลี่ยจากทุกบล็อคบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 25%

ขนาดไฟล์ P1	ไฟล์ข้อมูล								
	P1	P2	P3	P4	P5	P6	P7	P8	P9
1	23.82	24.66	24.76	25.02	25.63	24.69	24.89	23.19	25.07
5	24.49	24.95	25.18	25.56	25.55	25.46	25.37	24.80	24.01
10	24.96	24.72	25.16	25.25	24.57	24.85	25.33	25.26	26.12
50	24.82	24.91	24.89	25.39	25.36	25.12	24.63	24.64	25.33
100	25.04	24.87	24.85	25.50	25.39	25.28	24.74	24.61	24.41
500	25.04	24.98	25.16	25.52	25.53	24.34	24.25	24.57	24.01
1000	24.98	24.98	25.04	24.96	24.84	24.41	25.48	24.57	26.12

อัตราการสูญหายของข้อมูลจากบล็อคที่มีอัตราการสูญหายสูงสุด จากการทดลองบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 25% แสดงในตารางที่ 29 โดยมีอัตราการสูญหายสูงสุดเท่ากับ 27.17% ที่ไฟล์ข้อมูล P1 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 10 เมกะไบต์ และมีอัตราการสูญหายต่ำสุด 23.19% ที่ไฟล์ข้อมูล P8 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1 เมกะไบต์

ส่วนอัตราการสูญหายของข้อมูลเฉลี่ยจากทุกบล็อคของแต่ละไฟล์ข้อมูลได้แสดงในตารางที่ 30 โดยมีอัตราการสูญหายสูงสุดเท่ากับ 26.12% ซึ่งเกิดขึ้น 2 ครั้ง ที่ไฟล์ข้อมูล P9 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 10 เมกะไบต์ และไฟล์ข้อมูล P9 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1000 เมกะไบต์ และมีอัตราการสูญหายต่ำสุดเท่ากับ 23.19% ที่ไฟล์ข้อมูล P8 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1 เมกะไบต์

จากการทดลองผ่านเครือข่ายดาวเทียม AI3 ช่องสัญญาณดาวเทียมแบบทิศทางเดียว และเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 1% 10% และ 25% แสดงให้เห็นว่าการเกิดการสูญหายของแต่ละบล็อคสามารถมีการสูญหายในการอัตราที่ไม่เท่ากันได้ ซึ่งหมายความว่าอัตราการสูญหายเฉลี่ยของไฟล์ข้อมูลซึ่งเป็นอัตราการสูญหายเฉลี่ยจากทุกบล็อคของไฟล์ข้อมูล อาจมีค่าน้อยกว่าอัตราการสูญหายสำหรับบล็อคที่มีอัตราการสูญหายสูงสุดได้ ดังนั้นหากอัตราการสูญหายโดยรวมมีอัตราการสูญหายไม่เกิน 50% แต่มีบางบล็อคที่มีอัตราการสูญหายเกินกว่า 50% ก็จะทำให้ไม่สามารถกู้คืนข้อมูลได้ (ในกรณีที่ใช้ค่า Stretch Factor เท่ากับ 2 ในการเข้ารหัสข้อมูล) จึงได้ทดลองเพิ่มบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 50% ซึ่งได้ผลการทดลองดังนี้

ตารางที่ 31 อัตราการสูญหายจากบล็อคที่มีอัตราการสูญหายสูงสุดบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 50%

ขนาดไฟล์ P1	**ไฟล์ข้อมูล**								
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**
1	48.49	51.00	50.80	49.48	49.60	49.76	50.86	50.13	51.45
5	50.53	51.20	51.65	50.75	50.23	49.98	49.19	48.06	49.80
10	50.88	51.65	51.84	50.88	49.48	49.80	49.93	47.70	49.61
50	52.10	50.64	50.83	51.55	50.19	50.18	51.29	49.84	51.32
100	51.98	50.43	50.63	50.40	50.95	49.62	49.06	50.49	50.33
500	51.88	51.50	51.13	50.63	49.58	50.63	51.03	50.82	50.07
1000	52.05	51.18	51.33	51.31	50.28	51.08	52.06	50.33	51.97

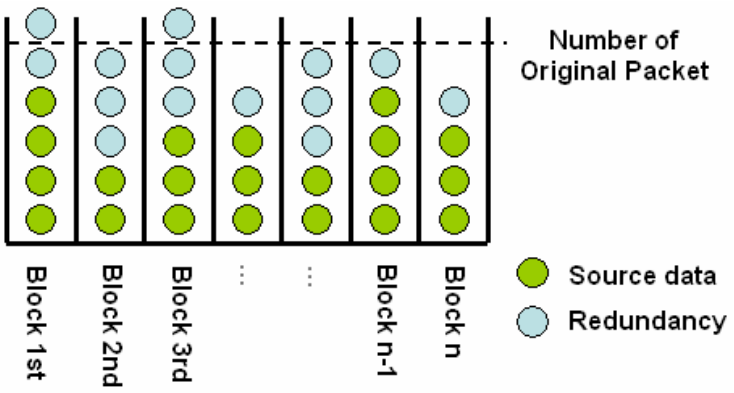
ตารางที่ 32 อัตราการสูญหายเฉลี่ยจากทุกบล็อคบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 50%

ขนาดไฟล์ P1	ไฟล์ข้อมูล								
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**
1	48.49	49.57	49.83	49.07	49.58	49.64	50.86	50.13	51.45
5	50.13	49.77	50.43	50.03	50.16	49.51	49.19	48.06	49.80
10	50.47	50.16	50.32	49.86	49.08	49.72	49.93	47.70	49.61
50	49.97	49.91	49.70	50.89	49.95	49.64	51.29	49.84	51.32
100	49.90	49.47	49.70	49.86	50.61	49.54	49.06	50.49	50.33
500	49.86	49.76	50.30	49.81	49.54	50.28	51.03	50.82	50.07
1000	49.72	49.77	49.70	50.30	50.28	50.71	52.06	50.33	51.97

อัตราการสูญหายจากบล็อคที่มีอัตราการสูญหายสูงสุดแสดงในตารางที่ 31 มีอัตราการสูญหายสูงสุดเท่ากับ 52.10% ที่ไฟล์ข้อมูล P1 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 50 เมกะไบต์ และมีอัตราการสูญหายต่ำสุดเท่ากับ 47.70% ที่ไฟล์ข้อมูล P8 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 10 เมกะไบต์ ส่วนอัตราการสูญหายของข้อมูลเฉลี่ยจากทุกบล็อคของแต่ละไฟล์ข้อมูลได้แสดงในตารางที่ 32 โดยมีอัตราการสูญหายสูงสุดเท่ากับ 52.06% ที่ไฟล์ข้อมูล P7 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 1000 เมกะไบต์ และมีอัตราการสูญหายต่ำสุดเท่ากับ 47.70% ที่ไฟล์ข้อมูล P8 ในการทดลองที่ไฟล์ข้อมูล P1 มีขนาด 10 เมกะไบต์

จากผลการทดลองแสดงให้เห็นว่าถึงแม้ไฟล์ข้อมูล P1 ที่การทดลองที่ไฟล์ข้อมูล P1 มีขนาด 50 เมกะไบต์ มีอัตราการสูญหาย เฉลี่ยของไฟล์ข้อมูลเพียง 49.97% แต่มีบล็อคข้อมูลหนึ่งที่มีอัตราการสูญหายสูงถึง 52.10% ก็ทำให้ผู้รับไม่สามารถกู้คืนข้อมูลกลับมาได้จากการส่งแพ็กเก็ตต้นฉบับเพียงหนึ่งรอบ และแพ็กเก็ตพิเศษอีกหนึ่งรอบ ซึ่งจะเห็นได้ว่าหากยังคงเข้ารหัสข้อมูลโดยไม่มีการแบ่งข้อมูลออกเป็นส่วนย่อย ผู้รับก็จะยังสามารถกู้คืนข้อมูลได้ เนื่องจากอัตราการสูญหายเฉลี่ยจากทุกบล็อคไม่เกิน 50% ดังนั้นการแบ่งข้อมูลออกเป็นส่วนย่อยก่อนแล้วจึงเข้ารหัสข้อมูลเป็นการเพิ่มประสิทธิภาพด้านเวลาที่ใช้ในการเข้ารหัสข้อมูล แต่กลับเป็นการลดทอนประสิทธิภาพของการถอดรหัสในกรณีที่มีอัตราการสูญหายมาก

ภาพที่ 25 แสดงตัวอย่างประสิทธิภาพของ FEC ที่ถูกลดทอนเมื่อแบ่งข้อมูลออกเป็นบล็อค ซึ่งจะเห็นว่าบล็อคที่ 1 และบล็อคที่ 3 รับแพ็กเก็ตได้มากกว่าที่ต้องการบล็อคละ 1 แพ็กเก็ต แต่ไม่สามารถนำแพ็กเก็ตไปใช้กับบล็อคที่มีจำนวนแพ็กเก็ตไม่เพียงพอได้ เนื่องจากการเข้ารหัสข้อมูลในแต่ละบล็อคมีความเป็นอิสระต่อกัน ดังนั้นไฟล์ข้อมูลตามตัวอย่างนี้จึงไม่สามารถสร้างกลับเป็นไฟล์ข้อมูลต้นฉบับได้



ภาพที่ 25 ประสิทธิภาพของวิธีการ FEC ที่ถูกลดทอนเมื่อแบ่งข้อมูลออกเป็นบล็อค
ที่มา: Byers *et al*., (1998)

5. ผลการศึกษาประสิทธิภาพการสร้างความน่าเชื่อถือด้วยวิธีการบรอดคาสต์ดิสค์และ Peer-to-Peer Sharing

การทดลองสุดท้ายนี้เป็นการสร้างความน่าเชื่อถือด้วยวิธีการแบ่งข้อมูลที่ตัวเองได้รับให้กับผู้รับภายในกลุ่มของตนเอง เป็นการหาจำนวนผู้รับภายในกลุ่มเพื่อแลกเปลี่ยนข้อมูลกัน จากการส่งข้อมูลเพียงหนึ่งรอบ โดยการทดลองในส่วนนี้จะทดลองบนเครือข่ายจำลอง NS-2 เท่านั้น เนื่องจากไม่สามารถจัดเตรียมทรัพยากรที่เพียงพอได้สำหรับเครือข่ายดาวเทียม AI3 และเครือข่ายจำลอง Dummynet และในการทดลองส่วนนี้ได้ทดลองทั้งหมด 4 ครั้ง ดังนั้นผลการทดลองที่แสดงจึงเป็นการหาจำนวนผู้รับจากการรับไฟล์ข้อมูลทั้ง 9 ไฟล์ข้อมูล (P1 ถึง P9) ภายในการส่งข้อมูลจากผู้ส่งเพียงหนึ่งรอบ และเนื่องจากเป็นผลลัพธ์จากการทดลองทั้งหมด 4 ครั้ง จึงแสดงเป็นจำนวนผู้รับสูงสุดที่เกิดขึ้นจากการทดลองทั้ง 4 ครั้ง

ตารางที่ 33 จำนวนผู้รับอย่างน้อยสำหรับการแลกเปลี่ยนข้อมูลในกลุ่มผู้รับบนเครือข่ายจำลอง NS-2

อัตราการสูญหาย	**ขนาดไฟล์ P1 (เมกะไบต์)**						
	1	**5**	**10**	**50**	**100**	**500**	**1000**
1%	3	3	4	4	3	3	5
10%	6	7	6	7	6	6	7
25%	9	9	10	10	11	11	11

จากตารางที่ 33 แสดงให้เห็นว่าเมื่ออัตราการสูญหายเพิ่มขึ้นจำนวนผู้รับภายในกลุ่มที่ใช้ในการแลกเปลี่ยนข้อมูลจะสูงขึ้นตาม ส่วนทางด้านขนาดของไฟล์ข้อมูลที่เพิ่มขึ้นนั้นสำหรับผลการทดลองที่ 1% และ 10% แสดงให้เห็นว่าขนาดของไฟล์ข้อมูลที่เพิ่มขึ้นไม่มีผลต่อจำนวนผู้รับที่ใช้ในการแลกเปลี่ยนข้อมูลภายในกลุ่มเนื่องจากบางไฟล์ข้อมูลที่มีขนาดใหญ่กว่าแต่มีการใช้จำนวนผู้รับในการแลกเปลี่ยนข้อมูลภายในกลุ่มจำนวนน้อยกว่า ส่วนผลการทดลองที่อัตราการสูญหาย 25% แสดงให้เห็นว่าขนาดของไฟล์ข้อมูลมีผลต่อจำนวนผู้รับที่ใช้ในการแลกเปลี่ยนข้อมูลภายในกลุ่มเนื่องจากเมื่อไฟล์ข้อมูลมีขนาดเพิ่มขึ้นจำนวนผู้รับภายในกลุ่มจะเพิ่มขึ้นเช่นกัน แม้จะไม่ได้เป็นการเพิ่มขึ้นทุกครั้งที่ขนาดของไฟล์ข้อมูลเพิ่มขึ้นก็ตาม ดังนั้นหากวิเคราะห์ผลการทดลองทั้ง 3 อัตราการสูญหาย จึงสามารถสรุปได้ว่าขนาดของไฟล์ข้อมูลจะไม่ส่งผลให้จำนวนผู้รับภายในกลุ่มที่ใช้ในการแลกเปลี่ยนข้อมูลเพิ่มขึ้นเสมอไป

จากผลการทดลองที่อัตราการสูญหายทั้ง 3 อัตรา เมื่อพิจารณาที่จำนวนผู้รับอย่างน้อยสำหรับการแลกเปลี่ยนข้อมูลภายในกลุ่ม ต่อขนาดของไฟล์ข้อมูลที่เพิ่มขึ้น แสดงให้เห็นว่าขนาดของไฟล์ข้อมูลมีขนาดแตกต่างกันอย่างมาก แต่จำนวนผู้รับอย่างน้อยสำหรับการแลกเปลี่ยนข้อมูลภายในกลุ่มมีจำนวนแตกต่างกันเพียง 1 ถึง 2 ราย ในแต่ละอัตราการสูญหาย ซึ่งสามารถสรุปได้ว่าการสร้างความน่าเชื่อถือด้วยวิธีการ Peer-to-Peer Sharing สามารถรองรับการให้บริการไฟล์ข้อมูลที่มีขนาดใหญ่เพิ่มขึ้นได้ โดยส่งผลให้จำนวนผู้รับอย่างน้อยที่ต้องการในการแลกเปลี่ยนข้อมูลภายในกลุ่มเพิ่มขึ้นเพียงเล็กน้อย

สรุปผลการวิจัย และข้อเสนอแนะ

จากการศึกษาวิธีการสร้างความน่าเชื่อถือสำหรับการมัลติคาสต์บนช่องสัญญาณเครือข่ายดาวเทียมแบบทิศทางเดียว เพื่อเป็นแนวทางในการพัฒนาการใช้งานช่องสัญญาณแบบทิศทางเดียวบนระบบเครือข่ายดาวเทียม AI3 ให้เกิดประโยชน์สูงขึ้น ผู้วิจัยสามารถสรุปผลการทดลอง และข้อเสนอแนะสำหรับเป็นแนวทางในการพัฒนาระบบขึ้นใช้งานผ่านเครือข่ายดาวเทียม AI3 ได้ดังนี้

สรุปผลการวิจัย

แม้ลักษณะการสูญหายของข้อมูลบนเครือข่ายจำลองจะไม่สามารถกำหนดให้มีลักษณะการสูญหายแบบต่อเนื่องได้เช่นเดียวกับที่เกิดขึ้นผ่านเครือข่ายดาวเทียม แต่ผลการทดลองทั้ง 3 เครือข่าย (เครือข่ายดาวเทียม AI3 ช่องสัญญาณแบบทิศทางเดียว เครือข่ายจำลอง NS-2 และเครือข่ายจำลอง Dummynet) สำหรับการทดลองเพื่อศึกษาประสิทธิภาพการสร้างความน่าเชื่อถือด้วยวิธีการบรอดคาสต์ดิสค์และ Data Carousel นั้นสามารถแสดงให้เห็นว่าอัตราการสูญหายที่เพิ่มขึ้นไม่ส่งผลให้ใช้จำนวนรอบในการส่งข้อมูลเพิ่มขึ้นเสมอไป ผลจากลักษณะการสูญหายของข้อมูลแบบต่อเนื่องบนเครือข่ายดาวเทียมแสดงให้เห็นอย่างชัดเจนในเรื่องนี้เนื่องจากการสูญหายของข้อมูลอาจเกิดขึ้นมากในรอบใดรอบหนึ่งจึงส่งผลให้อัตราการสูญหายโดยรวมที่เกิดขึ้นกับไฟล์ข้อมูลนั้นสูง ส่วนผลการทดลองบนเครือข่ายจำลองทั้ง NS-2 และ Dummynet ก็ส่งผลเช่นเดียวกันนี้แม้จะไม่เด่นชัดเช่นเดียวกับผลจากการทดลองผ่านเครือข่ายดาวเทียม และจากผลการทดลองผ่านเครือข่ายจำลองทั้ง 2 เครือข่าย ซึ่งสามารถควบคุมอัตราการสูญหายได้นั้น แสดงให้เห็นว่าเมื่ออัตราการสูญหายของข้อมูล และขนาดของไฟล์ข้อมูลสูงขึ้น จะส่งผลให้ใช้จำนวนรอบที่ใช้ในการส่งข้อมูลสูงขึ้น ซึ่งจำนวนรอบที่ใช้ในการส่งข้อมูลที่สูงขึ้นหมายถึง ต้องใช้เวลาที่ใช้ในการส่งข้อมูลนานขึ้น

เมื่อนำวิธีการ FEC ใช้ในการสร้างความน่าเชื่อถือสำหรับการสื่อสารดาวเทียมแบบทิศทางเดียว จากการทดลองทั้งเครือข่ายดาวเทียม AI3 ช่องสัญญาณแบบทิศทางเดียว และเครือข่ายจำลอง Dummynet แสดงให้เห็นว่าการกำหนดค่า Stretch Factor (ค่าที่ใช้กำหนดจำนวนแพ็กเก็ตหลังจากผ่านการเข้ารหัสข้อมูลต้นฉบับ) เท่ากับ 2 สามารถทำให้ผู้รับสามารถรับนำข้อมูลแพ็กเก็ตพิเศษ ไปถอดรหัสเพื่อกู้คืนข้อมูลแพ็กเก็ตต้นฉบับที่สูญหายได้ แต่จากการทดลองเพิ่มเติมบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 50% ทำให้ทราบว่าการแบ่งข้อมูลออกเป็นบล็อคเพื่อเพิ่ม

ประสิทธิภาพด้านความเร็วในการเข้ารหัสและถอดรหัสข้อมูล เป็นการลดทอนประสิทธิภาพของวิธีการ FEC เมื่อมีอัตราการสูญหายเฉลี่ยประมาณ 50% แต่ผลจากการศึกษาอัตราการสูญหายของข้อมูลผ่านเครือข่ายดาวเทียม และการทดลองสร้างความน่าเชื่อต่างๆ ผ่านเครือข่ายดาวเทียม ยังไม่พบการเกิดอัตราการสูญหายของข้อมูลเท่ากับหรือเกินกว่า 50% ซึ่งการทดลองทั้งหมดในส่วนนี้แสดงให้เห็นว่าหากอัตราการสูญหายที่เกิดขึ้นมีอัตราการสูญหายโดยรวมต่ำกว่า 50% ผู้รับสามารถกู้คืนข้อมูลจากการส่งข้อมูลเพียงหนึ่งรอบ (เท่ากับ 2 รอบเมื่อเทียบกับการสร้างความน่าเชื่อถือด้วย Data Carousel) แต่ข้อเสียคือผู้ส่งและผู้รับต้องมีขั้นตอนการเข้ารหัสและถอดรหัสข้อมูลเพิ่มขึ้นซึ่งเป็นขั้นตอนที่ต้องใช้การประมวลผลสูง

การนำวิธีการ Peer-to-Peer Sharing มาช่วยในการสร้างความน่าเชื่อถือในการสื่อสารแบบทิศทางเดียวเป็นอีกวิธีการหนึ่งที่ได้ทดลองแต่การทดลองนี้มีวัตถุประสงค์เพื่อหาจำนวนผู้รับภายในกลุ่มที่จะสามารถแลกเปลี่ยนข้อมูลที่ตนได้รับ เพื่อให้สามารถรับข้อมูลทั้งหมดได้ภายในการส่งข้อมูลเพียงหนึ่งรอบ ดังนั้นจึงหมายความว่าผลการทดลองนี้ตั้งอยู่บนสมมติฐานว่าทุกแพ็กเก็ตจะต้องถูกส่งถึงผู้รับรายใดรายหนึ่งในกลุ่มของผู้รับ แต่ในระบบการสื่อสารที่จริง แพ็กเก็ตทั้งหมดอาจไม่สามารถถูกรับได้จากการส่งข้อมูลเพียงรอบเดียว เนื่องจากการส่งข้อมูลผ่านดาวเทียมจะประกอบด้วยการส่งข้อมูลขาขึ้น (uplink) และการส่งข้อมูลขาลง (downlink) ดังนั้นหากแพ็กเก็ตสูญหายในขณะที่เป็นการส่งข้อมูลขาขึ้น ก็จะทำให้ไม่มีผู้รับรายใดสามารถรับแพ็กเก็ตนั้น (Awal *et al*., 2005) จากผลการศึกษาผลว่าการสร้างความน่าเชื่อถือด้วย Peer-to-Peer Sharing สามารถรองรับการให้บริการไฟล์ข้อมูลที่มีขนาดใหญ่เพิ่มขึ้นได้ โดยส่งผลให้จำนวนผู้รับอย่างน้อยในการแลกเปลี่ยนข้อมูลภายในกลุ่มผู้รับมีจำนวนเพิ่มขึ้นเพียงเล็กน้อย

ข้อเสนอแนะ

การสร้างความน่าเชื่อถือด้วยวิธีการ FEC นั้นหากสามารถนำวิธีการ FEC แบบ Tornado Codes มาใช้แทน Reed-Solomon Codes จะทำให้ไม่ต้องอาศัยวิธีการแบ่งข้อมูลออกเป็นบล็อคซึ่งเป็นวิธีการที่ลดทอนประสิทธิภาพของวิธีการ FEC อีกทั้ง Tornado Codes เป็นวิธีการที่มีประสิทธิภาพในด้านเวลาที่ใช้ในการประมวลผลเพื่อเข้ารหัสและถอดรหัสข้อมูล ในกรณีที่ใช้ Reed-Solomon Codes ควรแยกเครื่องที่ใช้ในการประมวลผลสำหรับการเข้ารหัสและถอดรหัสข้อมูลออกจากเครื่องที่ใช้ในการรับและส่งข้อมูล

การสร้างความน่าเชื่อถือบนการสื่อสารแบบทิศทางเดียวที่ได้ทำการศึกษาทั้ง 3 วิธี ได้แก่ Data Carousel FEC และ Peer-toPeer Sharing มีข้อดีและข้อด้อยที่แตกต่างกัน เพื่อให้เกิดประสิทธิภาพในการสร้างความน่าเชื่อถือบนการสื่อสารแบบทิศทางเดียวที่ดีขึ้น จึงควรนำทั้ง 3 วิธี มาทำงานร่วมกัน

เอกสารและสิ่งอ้างอิง

Achary, S., R. Alonso, M. Franklin and S. Zdonik. 1995. Broadcast Disks: Data Management for Asymmetric Communication Environment, pp. 199-210. **Proceedings of ACM SIGMOD Conference**.

AI3 Project. 2005. AI3 Network Topology. **About AI3 Project**. Available Source: http://www.ai3.net/, March, 2005.

Armstrong, S., A. Freier and K. Marzullo. 1992. Multicast Transport Protocol. **RFC 1301**. Available Source: http://www.ietf.org/rfc/rfc1301.html, March, 2004.

Awal, M. A., K. Kanchanasut and Y. Tsuchimoto. 2005. Multicast Packet Loss Measurement and Analysis over Unidirectional Satellite Network, pp. 254-268. **Asian Internet Engineering Conference (AINTEC)**. Springer-Verlag, Bangkok.

Basu, P. and K. Kanchanasut. 2003. A Reliable Multicast Protocol for Unidirectional Satellite Link, pp. 390-393. **Proceeding of the 2003 International Symposium on applications and the Internet**. Orlando, Florida, USA.

Berrou, C., A. Glavieux and P. Thitimajshima. 1996. Near Shannon Limit Error – Correcting Coding and Decoding: Turbo codes. **IEEE Transaction on Communications** 44 (10): 1064-1070.

Blahut, R. E. 1984. **Theory and Practice of Error control Codes**. Addison Wesley, MA.

Blomer, J., M. Kalfane, M. Karpinski, R. Karp, M. Luby and D. Zuckerman. 1995. An XOR-Based Erasure-Resilient Coding Scheme. **International Computer Science Institute Technical Report TR-95-048**. 19.

Byers, J., M. Luby and Mitzenmacher. 1998. A Digital Fountain Approach to Reliable Distribution of Bulk Data, pp. 56-67. **Proceedings of ACM SIGCOMM.** Vancouver, Cannada.

Clark, D. 1982. Window and Acknowlegement Strategy in TCP. **RFC 813**. Available Source: http://www.ietf.org/rfc/rfc0813.html, March, 2004.

Defense Space Technology Centre. 2006. **Satellite Communication System**. Available Source: http://www1.mod.go.th/opsd/dstcweb/ict/satellite.doc, Febuary, 2006.

Deering, S. 1989. Host extensions for IP multicasting. **RFC 1112**. Available Source: http://www.ietf.org/rfc/rfc1112.html, March, 2004.

Fenner, W. 1997. Internet Group Management Protocol version 2. **RFC 2236**. Available Source: http://www.ietf.org/rfc/rfc2236.html, March, 2004

Floyd, S., V. Jacobson, L. Ching-Gung, S. McCanne and L. Zhang. 1995. A Reliable Multicast Framework for Light-weight Sessions and Application Level Framing, pp. 342-354. **Proceedings of ACM SIGCOMM**.

Gemmell, J. 1997. Scalable Reliable Multicast Using Erasure-Correcting Re-sends. **Microsoft Research Technical Report MSR-TR-97-20**. 15.

Imielinski, T. and B. Badrinath. 1994. Mobile Wireless Computing: Challenges in Data Management. **Communications of the ACM** 37 (10): 19-28.

Information Sciences Institute. 2004. Network Simulator information and installation. **Network Simulator version all-in-one 2.26**. Available Source: http://www.isi.edu/nsnam/ns/, March, 2004.

International Organization for Standardization. 1994. Information Technology - Open Systems Interconnection - Basic Reference Model: The Basic Model. **ISO 7498 2nd ed**. Available Source: http://www.iso.org, March, 2004.

Jacobson, V. 1988. Congestion Avoidance and Control, pp. 314-329. **Proceedings of the ACM SIGCOMM Symposium on Communication Architectures and Protocols**.

Jain, R., K. Ramakrishnan and D.-M. Chiu. 1987. Congestion avoidance in computer networks with a connectionless network layer. **Digital Equipment Corporation Technical Report DEC-TR-506**. 21.

John C. Lin and S. Paul. 1996. RMTP: A Reliable Multicast Transport Protocol, pp. 1414-1424. **Proceedings of the IEEE INFOCOM**. San Francisco CA, United States of America.

Luby, M., M. Mitzenmacher, A. Shokrollahi, D. Spielman and V. Stermann. 1997. Practical Loss-Resilient Codes, pp. 150-159. **Proceedings of the 29th ACM Symposium on Theory of Computing**.

_____. 2004. Cauchy-based Reed-Solomon codes. **Reed Solomon Codes – Cauchy Matrices Source Code**. Available Souce: http://www.icsi.berkeley.edu/~luby/ cauchy.tar.uu, March, 2004.

Orten, P. and B. Rislow. 2002. **Theory and Practice of Error Control Coding for Satellite and Fixed Radio Systems**. Available Source: http://www.telenor.com/ telektronikk/ volumes/ pdf/1.2002/Page_078-091.pdf, March, 2004.

Postel, J. 1980. User Datagram Protocol. **RFC 768**. Available Source: http://www.ietf.org/rfc/ rfc0768.html, March, 2004.

_____. 1981a. Internet Protocol DARPA Internet Program Protocol Specification. **RFC 791**. Available Source: http://www.ietf.org/rfc/rfc0791.html, March, 2004.

_____. 1981b. Transmission Control Protocol Protocol DARPA Internet Program Protocol Specification. **RFC 793**. Available Source: http://www.ietf.org/rfc/rfc0793.txt, March, 2004.

Red Hat Inc. 2000. Cygwin information and installation. **Cygwin Version 2.340.2.5**. Available Source: http://www.cygwin.com/, March, 2004.

_____. 2003. Fedora information and installation. **Fedora Core 2**. Available Source: http://fedora.redhat.com/, March, 2004.

Rizzo L. 1997. Effective Erasure Codes for Reliable Computer Communication Protocols. **ACM Computer Communication Review** 27 (2): 24-36.

_____. 1998. Dummynet and Forward Error Correction. pp. 129-137. **Proceeding of FREENIX Annual Technical Conference**. New Orieans, LA.

_____. 2004a. Dummynet information and installation. **PicoBSD version 000608**. Available Source: http://info.iet.unipi.it/~luigi/ip_Dummynet/pico.000608.bin, March, 2004.

_____. 2004b. Software FEC in computer communication. **Reed Solomon Codes – Vandermonde Matrices Source Code**. Available Souce: http://info.iet.unipi.it/~luigi/vdm.tar.gz, March, 2004.

_____ and L. Vicisano. 1997. A Reliable Multicast data Distribution Protocol Based on Software FEC Techniques, pp. 116-127. **Proceedings of the Fourth IEEE Workshop on the Architecture and Implementation of High Performance Communication Systems**. Chalkidiki, Greece.

Reynolds, J. and J. Postel. 1994. Assigned Numbers. Network Working Group. **RFC 1700**. Available Source: http://www.ietf.org/rfc/rfc1700.html, March, 2004.

Sano, T., N. Yamanouchi, T. Shiroshita and O. Takahashi. 1998. Flow and Congestion Control for Bulk Reliable Multicast Protocols – towards coexistence with TCP. **Proceedings of IEEE INFOCOM**. San Francisco.

Schooler, E. and J.Gemmell. 1997. Using multicast FEC to solve the midnight madness problem. **Microsoft Research Technical Report MS-TR-97-25**. 17.

Tanenbaum, A. S. 1996. **Computer Networks**. 1st ed. Prentice-Hall, Inc.

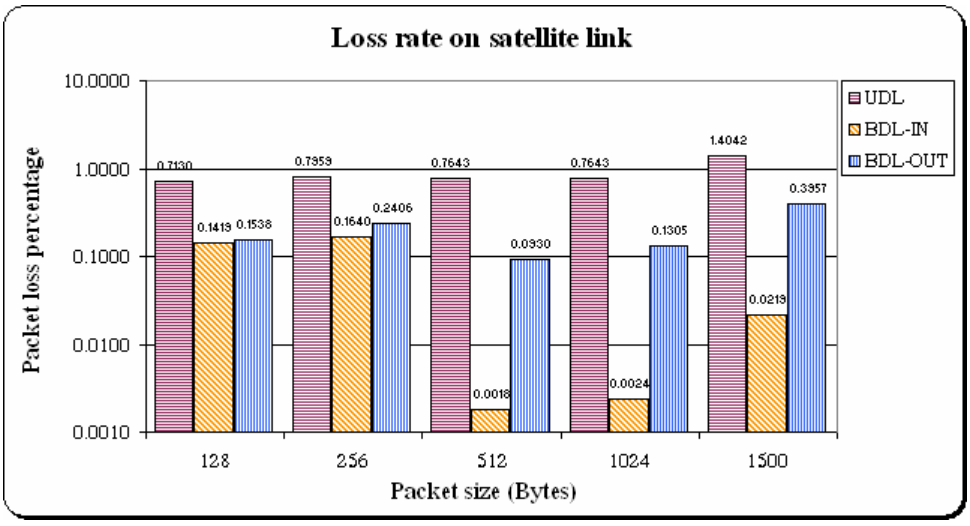
Tommasi, F., S. Molendini and A. Vilei. 2002. The Satellite Multicast Distribution Protocol (SMDP). **Proceedings of International Conference on Software, Telecommunications and Computer Networks IEEE SOFTCOM**. Split, Croatia.

Pokavanich, W. and K. Kanchanasut. 2000. **Packet Delivery Scheduling for Reliable Multicasting Over Unidirectional Link**. M.S. thesis. Asian Institute of Technology.

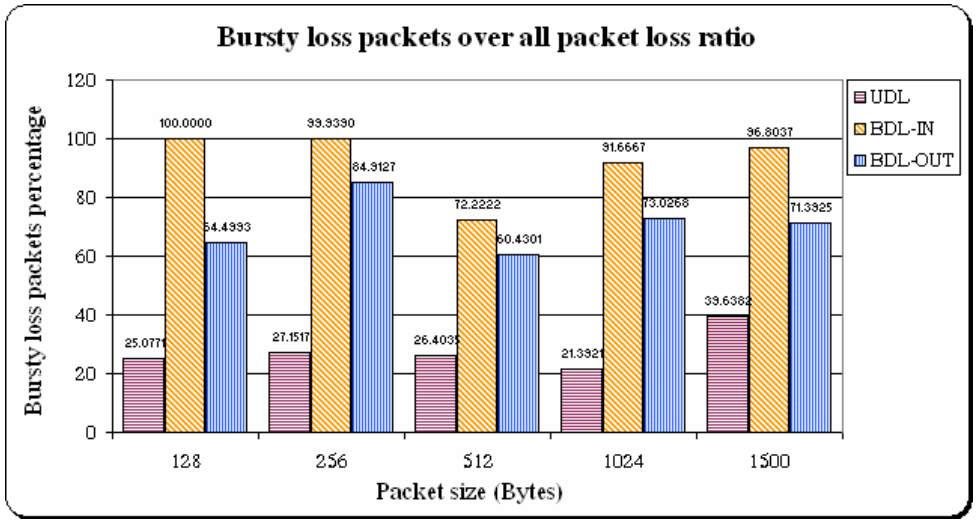
Yoon, J., A. Bestavros and I. Matta. 1999. Adaptive Reliable Multicast. **Boston University Technical Report BU-CS-1999-012**. 5.

ภาคผนวก

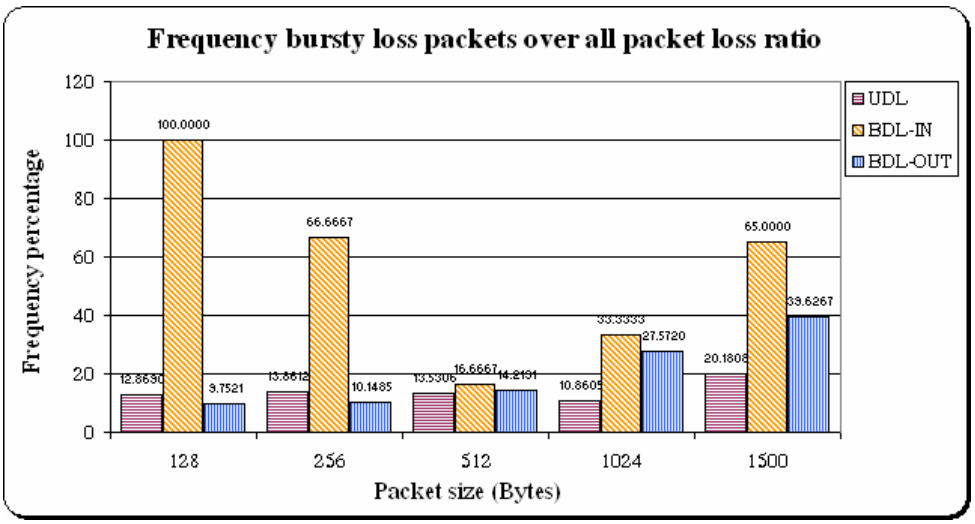
ผลการศึกษาศึกษาอัตราการสูญหายผ่านเครือข่ายดาวเทียม



ภาพผนวกที่ 1 อัตราการสูญหายของแพ็กเก็ตผ่านเครือข่ายดาวเทียม



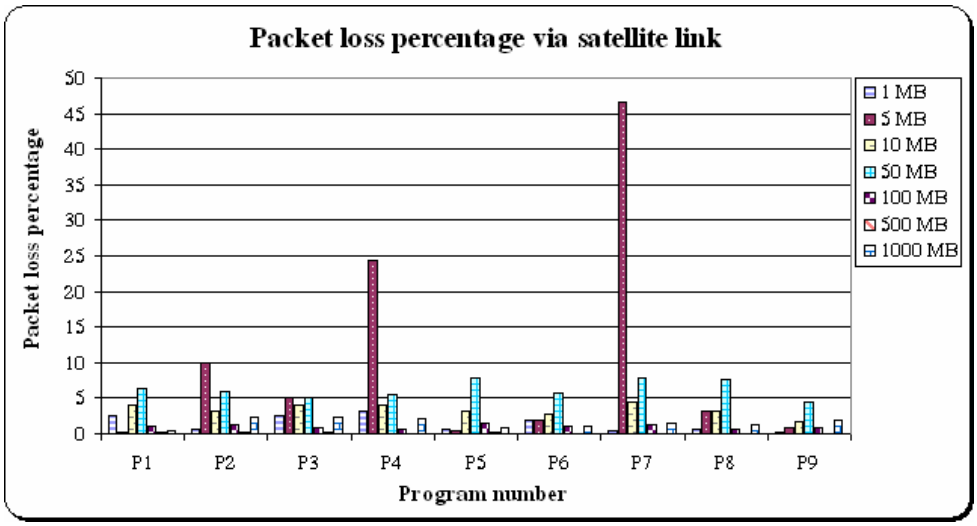
ภาพผนวกที่ 2 อัตราการส่วนการสูญหายของแพ็กเก็ตแบบต่อเนื่อง ต่อการสูญหายของแพ็กเก็ตทั้งหมดผ่านเครือข่ายดาวเทียม



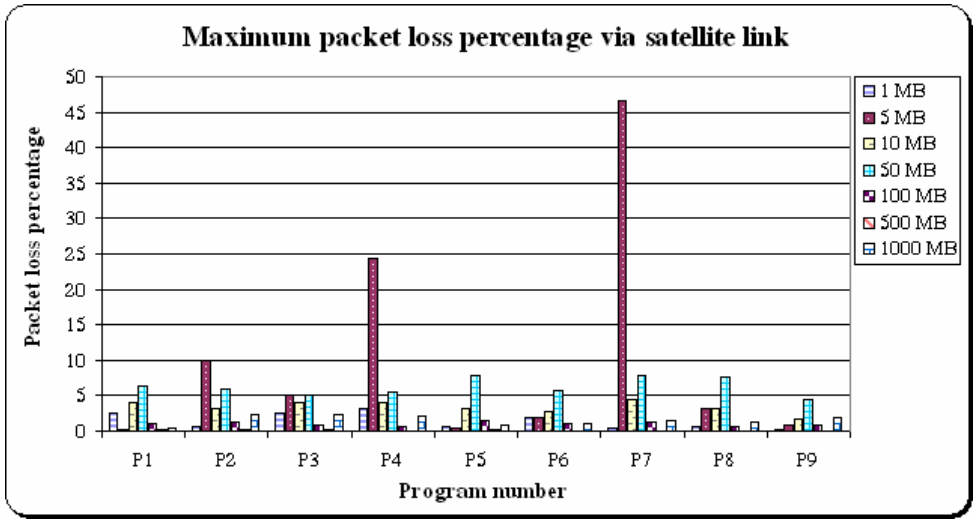
ภาพผนวกที่ 3 ความถี่ของจำนวนครั้งที่เกิดสูญหายของแพ็กเก็ตแบบต่อเนื่อง ต่อจำนวนครั้งที่เกิดการสูญหายของแพ็กเก็ตทั้งหมดผ่านเครือข่ายดาวเทียม

ผลการทดลองสร้างความน่าเชื่อถือด้วยวิธีการ Data Carousel

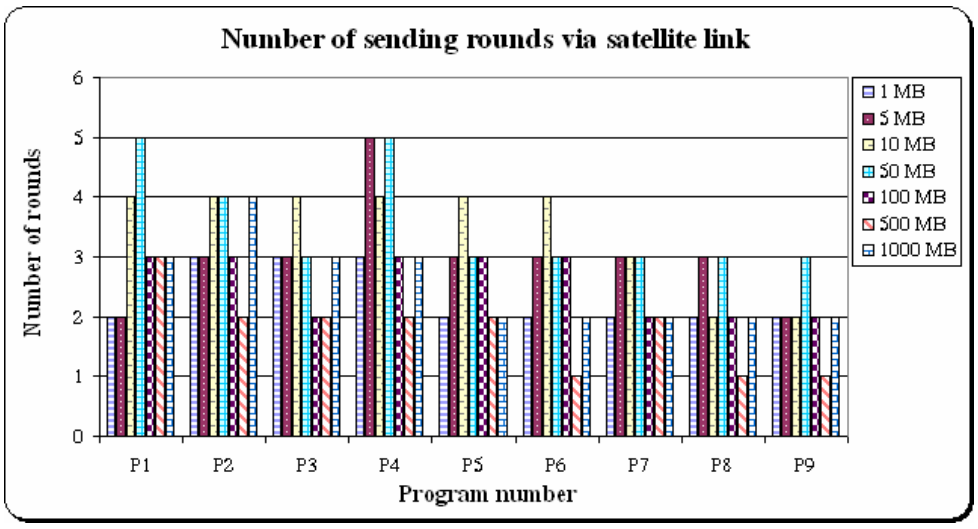
เครือข่ายดาวเทียม AI3



ภาพผนวกที่ 4 อัตราการสูญหายของแพ็กเก็ตในแต่ละไฟล์จากการส่งข้อมูลผ่านเครือข่ายดาวเทียม

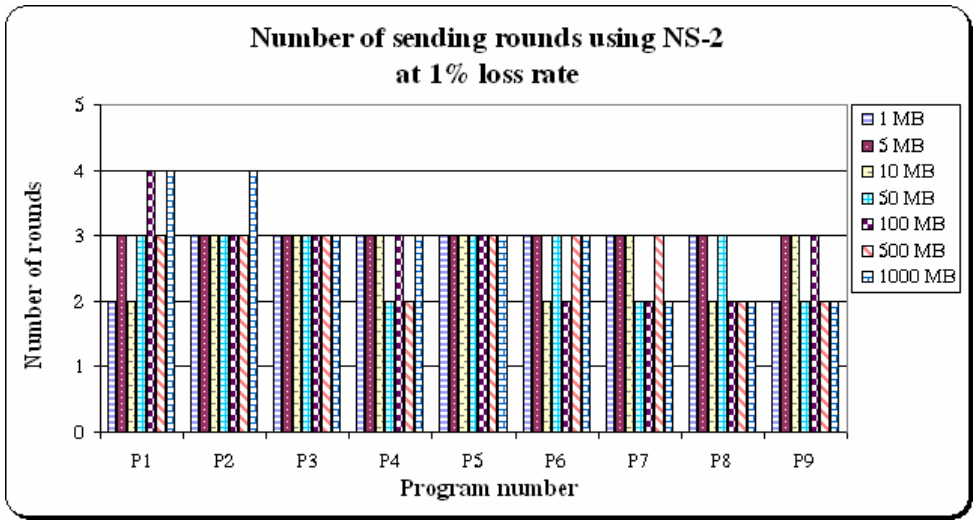


ภาพผนวกที่ 5 อัตราการสูญหายของแพ็กเก็ตสูงสุดในแต่ละไฟล์จากการส่งข้อมูลผ่านเครือข่ายดาวเทียม

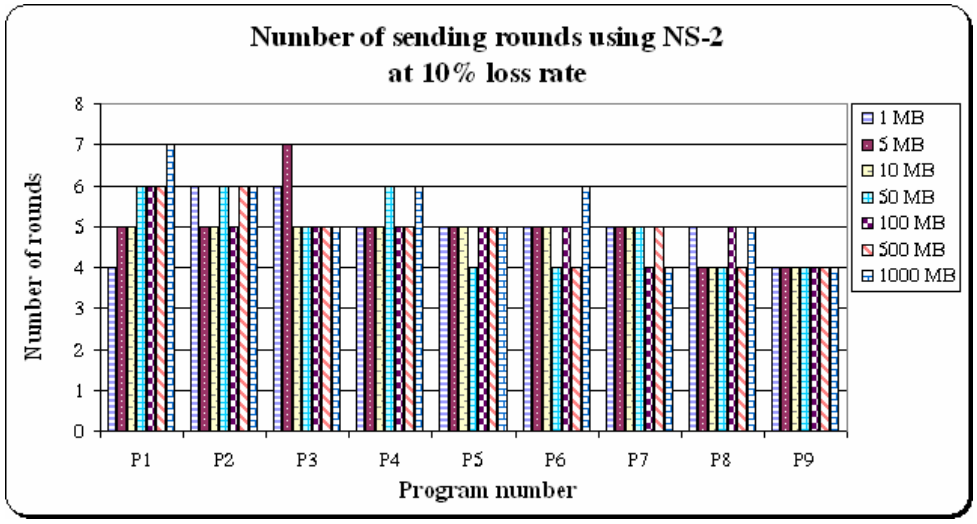


ภาพผนวกที่ 6 จำนวนรอบสูงสุดที่ใช้ในการส่งข้อมูลผ่านเครือข่ายดาวเทียม

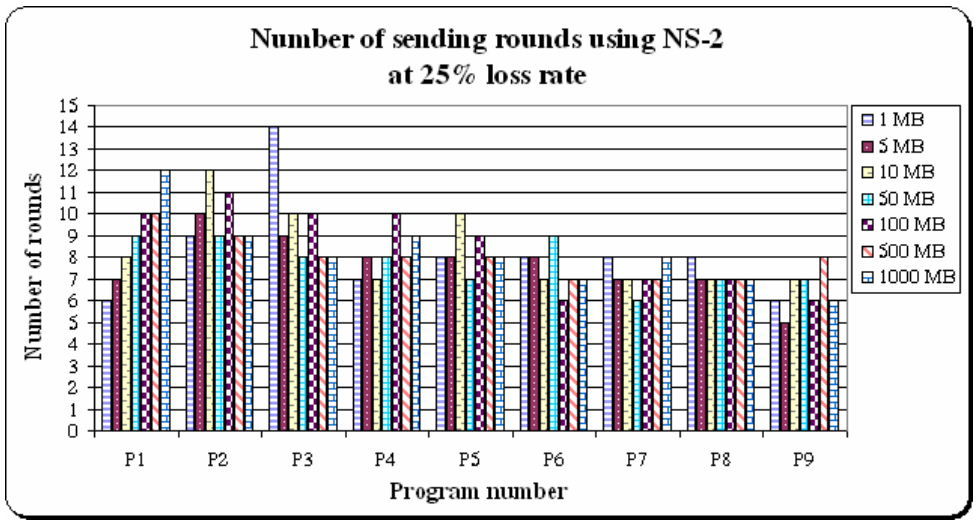
เครือข่ายจำลอง NS-2



ภาพผนวกที่ 7 จำนวนรอบสูงสุดที่ใช้ในการส่งข้อมูลบนเครือข่ายจำลอง NS-2 ที่อัตราการสูญหาย 1%

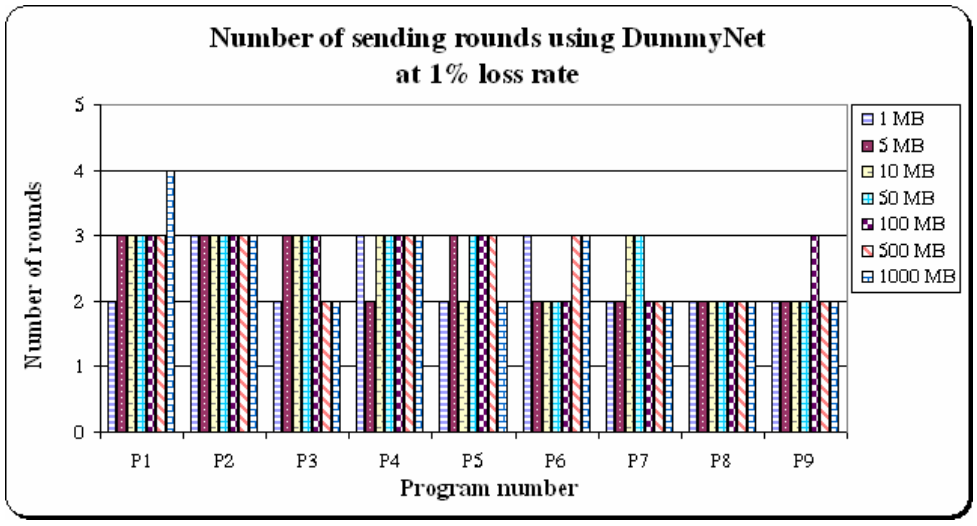


ภาพผนวกที่ 8 จำนวนรอบสูงสุดที่ใช้ในการส่งข้อมูลบนเครือข่ายจำลอง NS-2 ที่อัตราการสูญหาย 10%

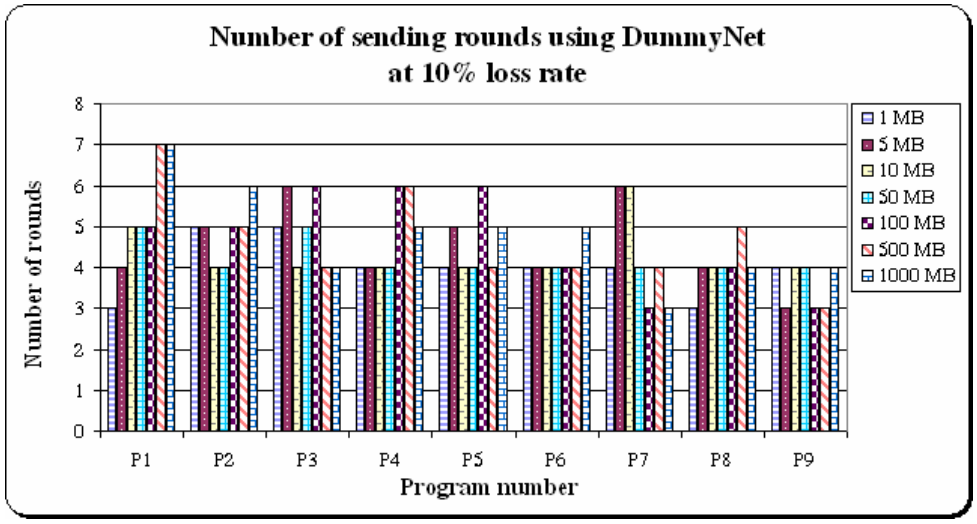


ภาพผนวกที่ 9 จำนวนรอบสูงสุดที่ใช้ในการส่งข้อมูลบนเครือข่ายจำลอง NS-2 ที่อัตราการสูญหาย 25%

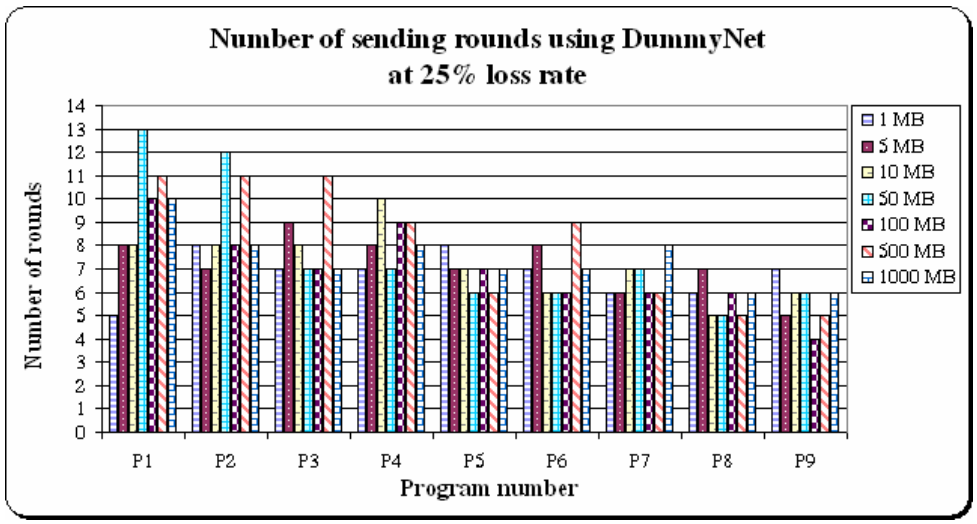
เครือข่ายจำลอง Dummynet



ภาพผนวกที่ 10 จำนวนรอบสูงสุดที่ใช้ในการส่งข้อมูลบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 1%



ภาพผนวกที่ 11 จำนวนรอบสูงสุดที่ใช้ในการส่งข้อมูลบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 10%

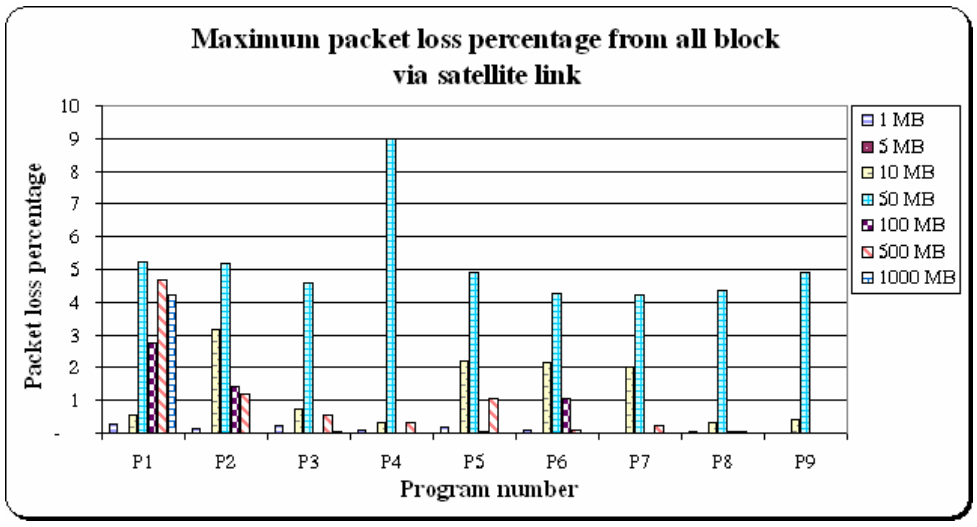


ภาพผนวกที่ 12 จำนวนรอบสูงสุดที่ใช้ในการส่งข้อมูลบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 25%

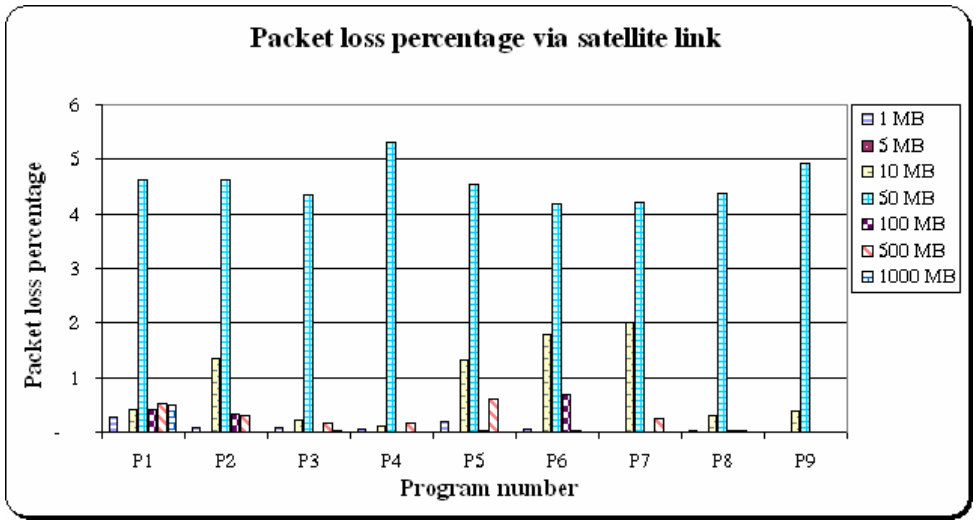
ผลการ ทดลองการสร้างความน่าเชื่อถือด้วยวิธีการ FEC

(Reed-Solomon พัฒนาด้วย Cauchy Matrices)

เครือข่ายดาวเทียม AI3

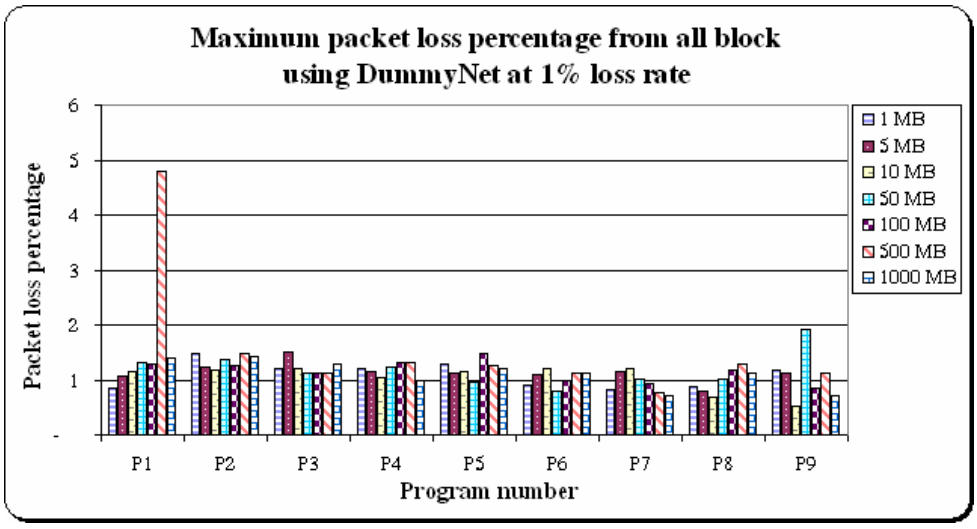


ภาพผนวกที่ 13 อัตราการสูญหายจากบล็อคที่มีอัตราการสูญหายสูงสุดผ่านเครือข่ายดาวเทียม

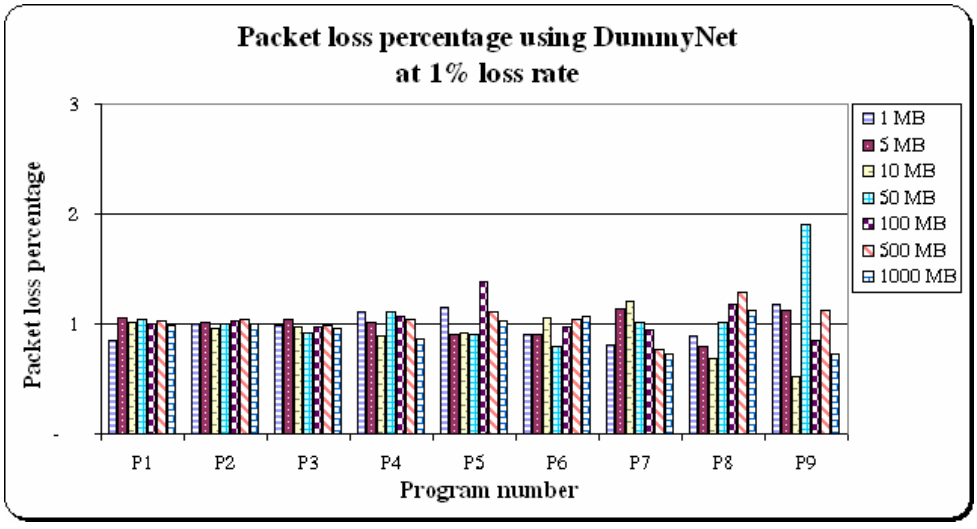


ภาพผนวกที่ 14 อัตราการสูญหายเฉลี่ยจากทุกบล็อคผ่านเครือข่ายดาวเทียม

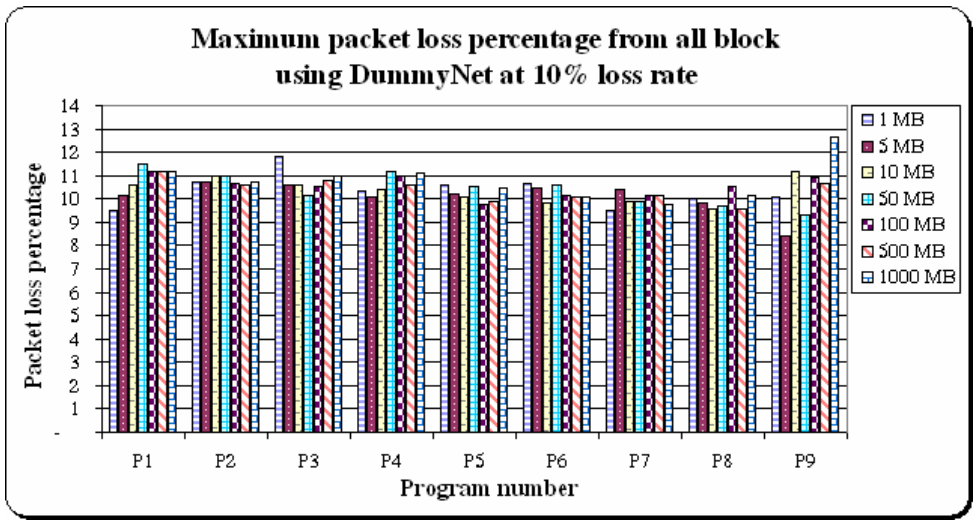
เครือข่ายจำลอง Dummynet



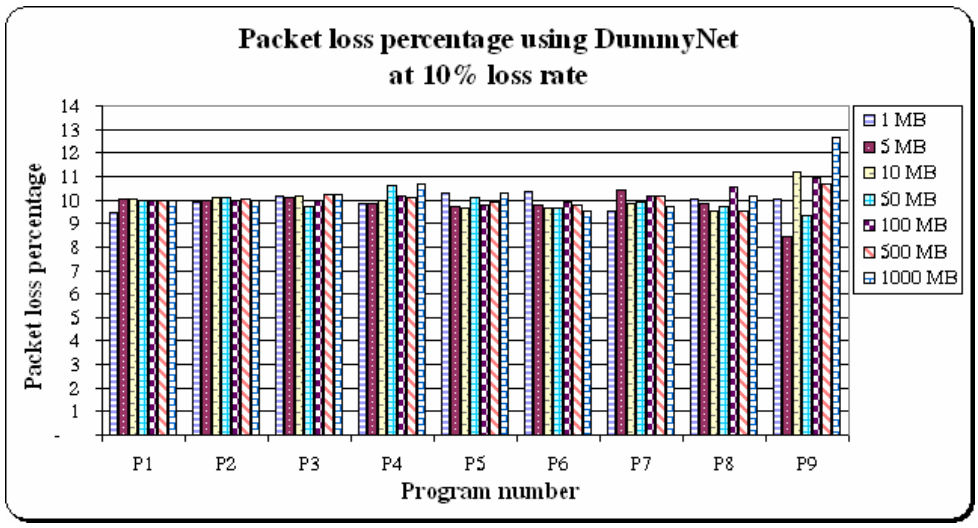
ภาพผนวกที่ 15 อัตราการสูญหายจากบล็อคที่มีอัตราการสูญหายสูงสุดบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 1%



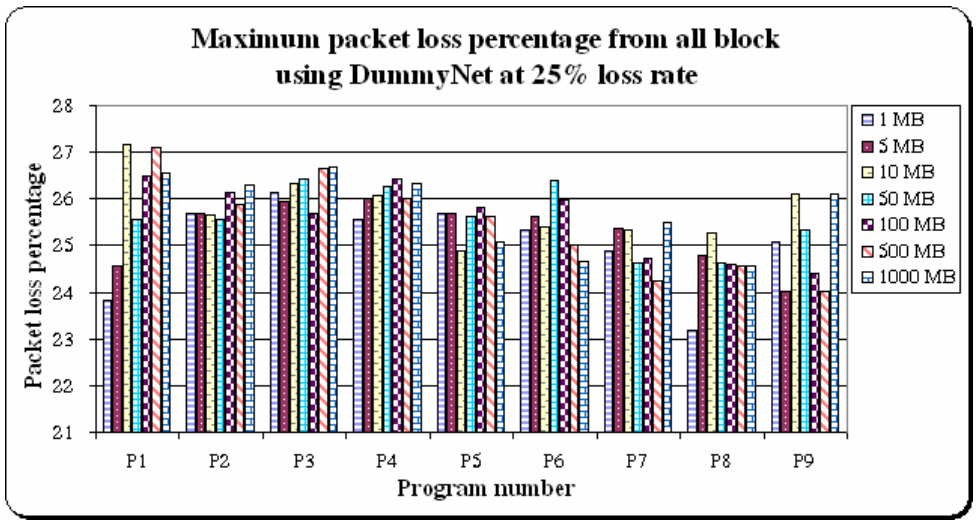
ภาพผนวกที่ 16 อัตราการสูญหายเฉลี่ยจากทุกบล็อคบนเครือข่ายจำลอง Dummynet ที่อัตราการ สูญหาย 1%



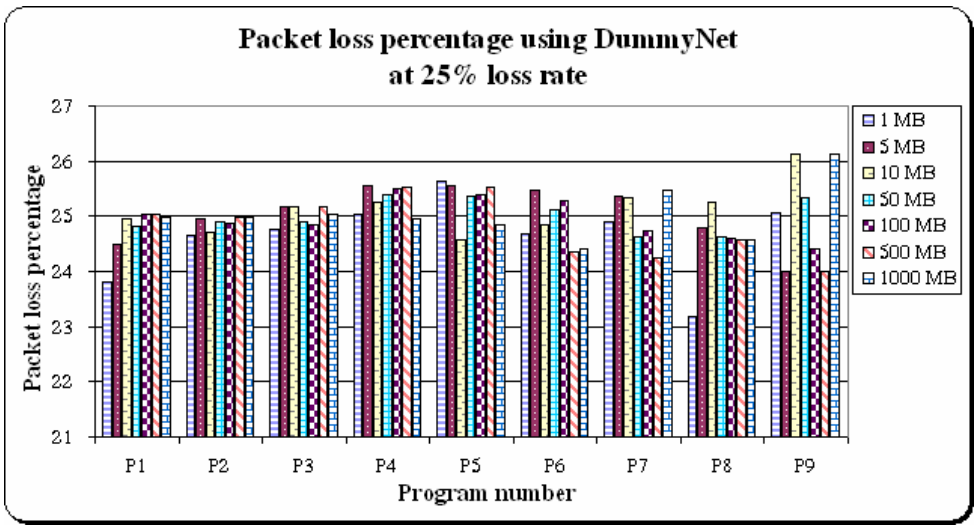
ภาพผนวกที่ 17 อัตราการสูญหายจากบล็อคที่มีอัตราการสูญหายสูงสุดบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 10%



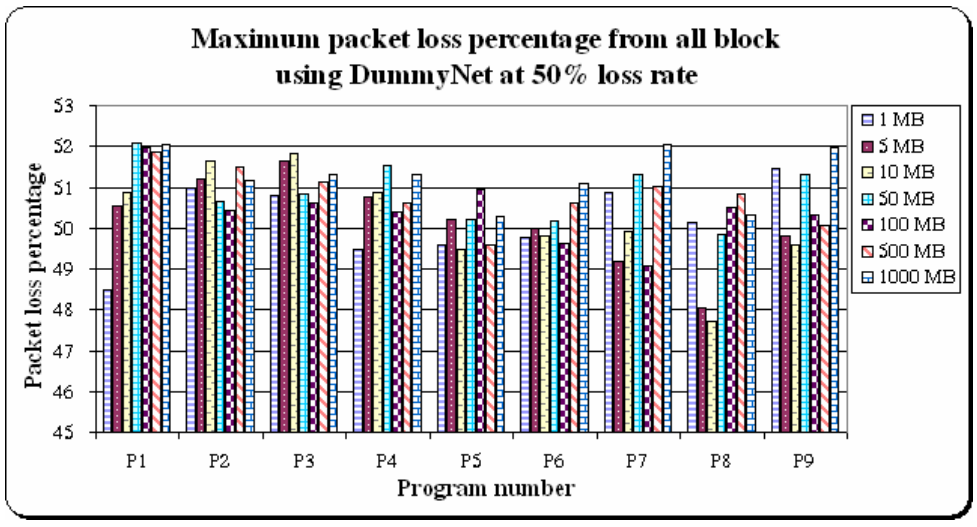
ภาพผนวกที่ 18 อัตราการสูญหายเฉลี่ยจากทุกบล็อคบนเครือข่ายจำลอง Dummynet ที่อัตราการ สูญหาย 10%



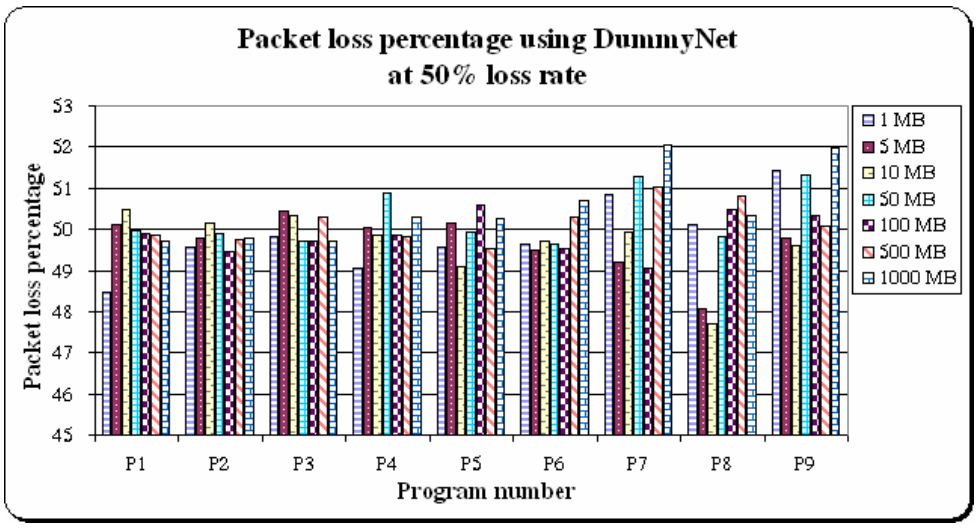
<u>ภาพผนวกที่ 19</u> อัตราการสูญหายจากบล็อคที่มีอัตราการสูญหายสูงสุดบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 25%



<u>ภาพผนวกที่ 20</u> อัตราการสูญหายเฉลี่ยจากทุกบล็อคบนเครือข่ายจำลอง Dummynet ที่อัตราการ สูญหาย 25%



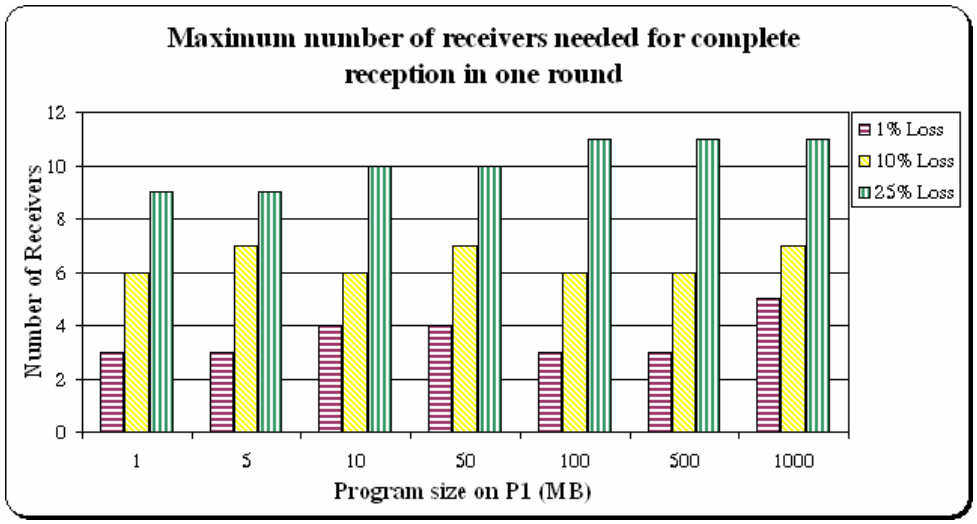
ภาพผนวกที่ 21 อัตราการสูญหายจากบล็อคที่มีอัตราการสูญหายสูงสุดบนเครือข่ายจำลอง Dummynet ที่อัตราการสูญหาย 50%



ภาพผนวกที่ 22 อัตราการสูญหายเฉลี่ยจากทุกบล็อคบนเครือข่ายจำลอง Dummynet ที่อัตราการ สูญหาย 50%

ผลการทดลองการสร้างความน่าเชื่อถือด้วยวิธีการ Peer-to-Peer Sharing

เครือข่ายจำลอง NS-2



ภาพผนวกที่ 23 จำนวนผู้รับอย่างน้อยสำหรับการแลกเปลี่ยนข้อมูลในกลุ่มผู้รับบนเครือข่ายจำลอง NS-2

ประวัติการศึกษา

ชื่อ นายพรชัย บัวบานพร้อม

เกิดวันที่ 24 เมษายน พ.ศ. 2519

สถานที่เกิด อำเภอบางรัก จังหวัดกรุงเทพมหานคร

ประวัติการศึกษา บธ.บ. (คอมพิวเตอร์บริหารธุรกิจ) มหาวิทยาลัยสยาม พ.ศ. 2541

ตำแหน่งปัจจุบัน เจ้าหน้าที่อาวุโสส่วนดาต้าแวร์เฮ้าส์

สถานที่ทำงานปัจจุบัน บริษัทฟิลิปส์เซมิคอนดักส์เตอร์ (ประเทศไทย) จำกัด

ผลงานทางวิชาการ

IP Multicasting Experience Using Broadcast Disk Techinque Over Unidirectional Satellite Link ในงานประชุมวิชาการ The 3rd International Conference on Advance In Mobile Multimedia (MoMM 2005) ระหว่างวันที่ 19-21 กันยายน 2548 กัวลาลัมเปอร์ มาเลเซีย

ทุนการศึกษาที่ได้รับ ได้รับทุนสนับสนุนการทำวิทยานิพนธ์จากโครงการปริญญาโท สาขาวิทยาการคอมพิวเตอร์) ภาคพิเศษ (คณะวิทยาศาสตร์ มหาวิทยาลัยเกษตรศาสตร์) พ.ศ. 2548