A survey Video Over Wireless base on H.264

ศรัณย์ สิทธิพรหม, นิสิต ศิริมาลย์กิจ, ปิยะณัฐ อ่อนจันทร์, พิสิฐ วรรธนะไพสิฐ, มารุด คำภักดี,
ยศวริศ สุริสาร, รุ่งโรจน์ ยิ้มใย, วินัย มาลีลัย, สุเมธี เกษร และ เสกสรร แจ่มจ้อย

บทคัดย่อ— ในงานวิจัยนี้ พวกเราขอนำเสนอการสำรวจวิดีโอเครือข่ายไร้สายบนมาตรฐาน H.264 การส่งวิดีโอ (Transmission Video) จะมีประสิทธิภาพนั้นจะประกอบไปด้วย การสูญหายของแพ็กเก็ต (Packet Loss) และความหน่วง (Delay) มีการแก้ปัญหาที่แตกต่างกันออกไป คุณภาพของวิดีโอ (Quality of Service, Qos) ที่ส่งในเครือข่ายอินเตอร์เน็ต เป็นการจัดลำดับเพื่อให้ได้มาซึ่งคุณภาพของข้อมูลวิดีโอ การพัฒนาอย่างรวดเร็วของอินเตอร์เน็ตทำให้ต้องมีการรักษาความปลอดภัยเพิ่มมากขึ้น การเข้ารหัสวิดีโอ (Encryption Video) ซึ่งมีกระบวนการป้องกันหลากหลายรูปแบบ โดยในแต่ละแบบก็เหมาะสมกับการใช้ที่แตกต่างกัน เพื่อความถูกต้องในการส่งข้อมูลวิดีโอในเครือข่ายอินเตอร์เน็ตจะต้องมีการควบคุมความผิดพลาด (Error Control) ในการส่ง เพื่อให้ผู้รับได้รับข้อมูลที่ถูกต้องและครบถ้วน และสถาปัตยกรรมอินเตอร์เน็ตโปรโตคอล (Internet Protocol) ซึ่งเป็นข้อกำหนดในการส่งข้อมูลบนเครือข่ายที่ใช้สายหรือไร้สาย ได้นำโปรโตคอลแบบต่างๆ มาเปรียบเทียบเพื่อหาความเหมาะสมสำหรับนำไปใช้กับวีดีโอที่ส่งผ่านบนเครือข่ายไร้สาย

คำสำคัญ— การส่งผ่านวิดีโอ, คุณภาพของวิดีโอ, การเข้ารหัสวิดีโอ, การควบคุมความผิดพลาด, อินเตอร์เน็ตโปรโตคอล, H.264

I. INTRODUCTION

ความเจริญก้าวหน้าของเทคโนโลยีเครือข่ายไร้สายได้พัฒนาไปอย่างรวดเร็ว ไม่ว่าจะเป็นการติดต่อสื่อสาร การส่งข้อมูล นอกจากจะเป็นข้อมูลที่เป็นข้อความธรรมดาแล้ว ยังมีข้อมูลที่อยู่ในรูปแบบมัลติมีเดีย ทำให้ผู้บริโภคเข้าถึงข้อมูลได้อย่างรวดเร็ว แต่สำหรับเครือข่ายไร้สายยังมีข้อจำกัดที่จะต้องพิจารณาในด้านต่างๆ เช่น ความกว้างของช่องสัญญาณ (Bandwidth) ความปลอดภัย (Security) การควบคุมความผิดพลาด (Error Control) เป็นต้น

ในการพัฒนาการส่งวิดีโอ เพื่อนำมาใช้ในเครือข่ายไร้สายจะต้องพิจารณาองค์ประกอบต่างๆ ของความเข้ากันได้ เพื่อให้ได้ประสิทธิภาพของข้อมูลวิดีโอที่ส่งออกจากต้นทางไปยังปลายทาง (end-to-end) การแสดงผลและการแสดงข้อมูลวิดีโอ ตลอดจนการเข้ารหัสและการถอดรหัสวิดีโอ เทคโนโลยีที่ต่างกันจะให้การแสดงผลข้อมูลที่ต่างกันออกไปด้วย ซึ่งความถูกต้องของข้อมูลเป็นสิ่งที่สำคัญ โดยเฉพาะข้อมูลภาพวิดีโอที่ต้องการความละเอียดสูง เช่น ภาพแผนที่ทางทหาร ภาพวิดีโอทางด้านการแพทย์

มาตรฐานการเข้ารหัสวิดีโอที่ให้อัตราการส่งข้อมูลภาพวิดีโอต่ำ ที่กำลังเป็นที่นิยมในปัจจุบันนี้มีอยู่หลายมาตรฐาน สำหรับในมาตรฐานของ H.264 [1] วัตถุประสงค์ในการออกแบบใช้หลักการลดความซ้ำซ้อน (Redundancy) มีทั้งการลดความซ้ำซ้อนในเชิงพื้น (Spatial Redundancy) และการลดความซ้ำซ้อนในเชิงเวลา (Time Redundancy) เป็นการเข้ารหัสแบบผสมทั้งสองอย่าง ซึ่งเรียกว่า Hybrid Coding ทำให้มีความปลอดภัยเพิ่มมากขึ้นและเหมาะสำหรับที่จะนำไปใช้ในระบบเครือข่ายไร้สาย โครงข่ายโทรศัพท์สาธารณะ

ในงานวิจัยนี้จะนำเสนอองค์ประกอบที่เกี่ยวข้องกับวิดีโอเครือข่ายไร้สาย ซึ่งเนื้อหาทั้งหมดได้มีการนำเสนอการส่งวิดีโอจะกล่าวถึงในส่วนที่ 2 ในส่วนที่ 3 จะกล่าวถึงรายละเอียดของคุณภาพวิดีโอ การเข้ารหัสวิดีโอจะกล่าวถึงในส่วนที่ 4 การควบคุมความผิดพลาดอยู่ในส่วนที่ 5 อินเตอร์เน็ตโปรโตคอล อยู่ในส่วนที่ 6 สำหรับการอภิปรายผลและข้อสรุปจะอยู่ในส่วนที่ 7

II. VIDEO TRANSMISSION

A. Comparison Transmission Technique

ในอดีต การนำเสนอสื่อ Audio/Video บน Web จำเป็นต้องใช้วิธีการ download-and-play ซึ่งการที่จะรับชมสื่อนั้นๆได้นั้น จะต้องทำการ download ข้อมูลทั้งหมดมาก่อนจึงจะสามารถเล่นได้ แต่ในปัจจุบันสื่อผสม (Multimedia) สามารถนำเสนอผ่านweb browser ในระบบ intranet และ internet อย่างมีประสิทธิภาพมากขึ้น โดยที่วิธีการส่งข้อมูล Audio และ Video ผ่าน web browser มี ประเภทใหญ่ ๆ คือ การใช้ Web Server ในการนำข้อมูลส่งไปยังโปรแกรมที่ใช้นำเสนอสื่อนั้นๆ และอีกวิธีหนึ่งคือการใช้ Streaming Media Server ซึ่งจะใช้ Server โดยเฉพาะในการให้บริการข้อมูล Audio/Video โดยที่ Streaming Media file จะเริ่มเกือบจะในทันทีที่เล่น ระหว่างที่ข้อมูลกำลังถูกส่งผู้ชมสามารถรับฟัง/ชม สื่อนั้นๆได้ทันที โดยไม่จำเป็นต้องรอให้ download ข้อมูลทั้งหมดก่อน โดยมี Buffer เป็นตัวช่วย

โดยการส่งวิดีโอผ่านไอพี สามารถกระทำได้หลายหลากวิธี แต่ทั้งนี้ส่วนใหญ่จะมักพบกับปัญหาหลักๆอยู่ อย่าง คือ ปัญหาแพ็คเก็ตสูญหาย (Packet Loss) และปัญหาความหน่วง (Delay) จึงได้เกิดการแก้ปัญหาด้วยกระบวนต่างๆซึ่งในส่วนนี้จะเป็นการแสดงตารางเปรียบเทียบกระบวนการส่งวิดีโอบนเทคนิคที่ได้ศึกษามาดังนี้

The Legacy IEEE 802.11 MAC [2], OPTIMIZED BUFFERING [3], Overlay tree construction to distribute layered streaming by application layer multicast [4], Using Data Partitioning and Unequal Loss Protection [5], Forward Error Correction [6] โดยได้ เปรียบเทียบประสิทธิภาพการทำงานบน คุณสมบัติ ของ QoS สำหรับการส่งวิดีโอผ่านไอพีในเรื่อง ทรูพุท (Throughput) กลไกการตอบสนองระหว่างclient และ server (Feedback Mechanism), ความซับซ้อนของกระบวนการ (Complexity) อัตราการส่งที่มีเสถียรภาพ (Stable Transmission Rate) และเสถียรภาพการทำงาน (Stable Operation) โดยได้แบ่งการสื่อสารระหว่างเครื่องออกเป็นสองประเภทคือ Unicast และ Multicast ซึ่งได้ผลการเปรียบเทียบดังนี้

ตารางที่ 1 การเปรียบเทียบเทคนิคการส่งวิดีโอ โดยแยกตามลักษณะของปัญหา และ เปรียบเทียบประสิทธิภาพกระบวนการแก้ปัญหา

Video Transmission Technique	**Problem**		**Type**		**Performance Features QoS for Video over IP**		
	Packet Loss	**Delay**	**Unicast**	**Multicast**	**Throughput**	**Feedback Mechanism**	**Complexity**
The Legacy IEEE 802.11 MAC [2]	√		√			√	L
OPTIMIZED BUFFERING [3]		√				√	L
OVERLAY TREE CONSTRUCTION TO DISTRIBUTE LAYERED STREAMING BY APPLICATION LAYER MULTICAST [4]		√		√		√	
Using Data Partitioning and Unequal Loss Protection [5]	√					√	H
FORWARD ERROR CORRECTION [6]		√		√		√	H
√ = Yes , X = No , Blank = not mentioned , H= High, L = Low							

จากการเปรียบเทียบในตารางที่ 1 จะเห็นได้ว่าแต่ละวิธีที่ได้เสนอมา สามารถแก้ปัญหาหลักๆ ในเรื่องความหน่วงเวลาและการป้องกันแพ็คเก็ตสูญหายได้เป็นอย่างดี มีประสิทธิภาพเป็นตัวชี้วัดได้ ทั้งประเภท Unicast และ Multicast และหากพิจารณากระบวนการทั้งหมดที่กล่าวมา เราสามารถนำกระบวนการเหล่านี้มาประยุกต์เข้าด้วยกัน เพื่อพัฒนาวิธีการและกระบวนการที่อาจแก้ปัญหาเรื่องความหน่วง และ แพ็คเก็ตสูญหายพร้อม ๆ กันได้

ตารางที่ 2 การเปรียบเทียบเทคนิคการส่งวิดีโอ โดยแยกตามข้อดี ข้อเสีย ประสิทธิภาพและเทคนิคกระบวนการแก้ปัญหา

หัวข้อ	**ประสิทธิภาพ**	**เทคนิค**	**ข้อดี**	**ข้อเสีย**	**ราคา**
Effects of an Encoding Scheme on Perceived Video Quality Transmitted Over Lossy Internet Protocol Networks [7]	มีประสิทธิภาพที่ดีจากการทดสอบทางสถิติ	การตัดทอนบางส่วนของวีดีโอก่อนส่งขึ้นบนเครือข่าย	มีความหลากหลายของการส่งข้อมูล	มีการตัดทอนบางส่วนของวีดีโอออกไปทำให้เกิดการเสียหายของรายละเอียดของวีดีโอ	ปานกลาง
The Research on Video Transmission and Distribution System Based on Soft Switch Technology [8]	มีประสิทธิภาพที่สูงเนื่องจากมีการสร้างอุปกรณ์สำหรับการส่งวีดีโอโดยเฉพาะ	อุปกรณ์เฉพาะในการส่งวีดีโอ	-มีเทคโนโลยีเฉพาะในการส่งวีดีโอ -มีอุปกรณ์เฉพาะในการส่งวีดีโอ	-การส่งผ่านวีดีโอที่มีความจุเยอะๆ -ข้อจำกัดของการส่งวีดีโอขึ้นอยู่กับความกว้างของแบนด์วิทซ์	สูงมาก

หัวข้อ	ประสิทธิภาพ	เทคนิค	ข้อดี	ข้อเสีย	ราคา
Scalable Video transmission on overlay networks[9]	อินเตอร์เฟซใหม่ระหว่างแพลตฟอร์มที่ขยายขีดความสามารถในการประเมินผลวีดีโอ และเป็นการจำลองประสิทธิภาพการส่งผ่านการเข้ารหัสวีดีโอที่ปรับขนาดบิตสตรีมบนเครือข่ายซ้อนทับ	อินเตอร์เฟซใหม่ระหว่างแพลตฟอร์ม	มีความสามารถในการส่งวีดีโอที่ดีขึ้น	ต้องใช้เครือข่ายความเร็วสูง	ราคาสูง
Reliable Video Transmission Using Codes Close to the Channel Capacity [10]	ถือว่าดี ถ้าคิดในการส่งแบบที่มีค่าใช้จ่ายน้อย	ใช้ช่องสัญญาณ GF(216+1)	ค่าใช้จ่ายต่ำ	-มีน๊อยส์ และคุณภาพไม่ดี -มีการใช้โค้ดยาวจึงทำให้เกิดการส่งที่ล่าช้า -ส่ง MPEG 2 ไม่ได้	ราคาต่ำ

ใน [7], [9], [10] แต่ละงานก็มีข้อดีข้อเสียแตกต่างกันไป ดังนั้นการตัดสินใจในการเลือกใช้ในแต่ละหัวข้อก็ขึ้นอยู่กับ งบประมาณ และการใช้งาน อีกทั้ง ระบบ NETWORK ก็เป็นอีกปัจจัยที่สำคัญ โดยการเปรียบเทียบตามตางรางจะเห็นได้ว่าการใช้งานมีการควบคุมในตัวแปรต่างๆ ที่แตกต่างกันออกไป โดยที่ [7] มีประสิทธิภาพที่ดีจากการทดสอบทางสถิติ โดยใช้เทคนิคการตัดทอนบางส่วนของวีดีโอก่อนส่งขึ้นบนเครือข่าย และมีข้อดี คือ ความหลากหลายของการส่งข้อมูล และมีข้อเสียมีการตัดทอนบางส่วนของวีดีโอออกไปทำให้เกิดการเสียหายของซึ่งอาจทำให้บางส่วนบางตอนที่สำคัญหรือต้องการเน้นนั้น มีคุณภาพที่ต่ำลง แต่จะมีราคาปานกลาง เหมาะสำหรับการใช้งานที่มีงบประมาณพอเหมาะหรือปานกลาง [8] มีประสิทธิภาพที่สูงเนื่องจากมีการสร้างอุปกรณ์สำหรับการส่งวีดีโอโดยเฉพาะ เนื่องจากใช้เทคนิคที่คิดค้นขึ้นมาใหม่ในการส่งโดยมีข้อดีคือเทคโนโลยีเฉพาะในการส่งวีดีโอและอุปกรณ์เฉพาะในการส่งวีดีโอทำให้การส่งวีดีโอนั้นง่ายและมีประสิทธิภาพมากยิ่งขึ้น แต่จะมีข้อเสียคือจะมีการส่งผ่านไฟล์ขนาดใหญ่ทำให้ต้องอาศัยแบนด์วิธที่กว้างและดีจึงทำให้ต้องมีค่าใช้จ่ายที่สูง ไม่เหมาะกับการทำงานที่มีงบประมาณจำกัดและระบบเครือข่ายที่ช้า, [8] จะมีประสิทธิภาพคืออินเตอร์เฟซใหม่ระหว่างแพลตฟอร์มที่ขยายขีดความสามารถในการประเมินผลวีดีโอ และเป็นการจำลองประสิทธิภาพการส่งผ่านการเข้ารหัสวีดีโอที่ปรับขนาดบิตสตรีมบนเครือข่ายซ้อนทับ โดยใช้เทคนิคอินเตอร์เฟซใหม่ระหว่างแพลตฟอร์ม ข้อดีคือมีการส่งผ่านข้อมูลที่ดี แต่จะใช้การส่งผ่านโดยเครือข่ายที่มีความเร็วสูงซึ่งจะทำให้มีค่าใช้จ่ายที่สูงตามไปด้วย [10] ในหัวข้อนี้จะมีส่วนดีตรงที่ใช้มีค่าใช้จ่ายที่น้อยโดยใช้ช่องสัญญาณ GF(216+1) และมีข้อดีคือมีค่าใช้จ่ายที่ต่ำ แต่จะมีข้อเสียคือมีสัญญาณรบกวนและคุณภาพไม่ดีมีการใช้โค้ดยาวจึงทำให้เกิดการส่งที่ล่าช้าและส่ง MPEG 2 ไม่ได้เหมาะสำหรับงบประมาณที่ต่ำ

III. VIDEO ENCRYPTION

การเพิ่มขึ้นอย่างต่อเนื่องของการสื่อสารบนเครือข่ายอินเตอร์เน็ต คงจะปฏิเสธไม่ได้ว่าไม่มีหน่วยงานใดที่จะไม่มีการเชื่อมต่อการใช้งาน ในปัจจุบันมีการพัฒนาอินเตอร์เน็ตให้มีการใช้งานได้หลากหลายรูปแบบไม่ว่าจะเป็นที่ใช้สายหรือไร้สายหรือแม้แต่อุปกรณ์แบบพกพา การนำสื่อวิดีโอเพื่อแพร่ภาพบนอินเตอร์เน็ตก็เป็นเทคโนโลยีหนึ่งที่มีการประยุกต์ใช้งานบนอินเตอร์อย่างแพร่หลาย และได้มีการพัฒนาอย่าต่อเนื่อง เช่น การประชุมผ่านเครือข่าย การใช้งานทางด้านการแพทย์ การใช้งานทางด้านทหาร แต่ข้อมูลภาพวิดีที่ใช้สำหรับการส่งผ่านนั้นยังมีขนาดใหญ่ จึงต้องมีการเข้ารหัสข้อมูล (Encryption) ให้มีขนาดเล็กลง เพื่อให้เหมาะสมกับขนาดของความกว้างของช่องสัญญาณ การและสิ่งที่ต้องคำนึงถึงเป็นอย่างมากในใช้งานบนอินเตอร์เน็ตคือความปลอดภัยที่ส่งผ่านอินเตอร์เน็ต

มีวิธีการเข้ารหัสวิดีโอหลากหลายรูปแบบ ซึ่งแต่ละแบบก็มีความแตกต่างกันและมีความเหมาะสมที่ต่างกันในการใช้งาน ในการนำเสนอนี้ได้มุ่งเน้นความสำคัญการของวิธีการเข้ารหัสวิดีโอบนมาตรฐานของ H.264 ซึ่งทาง ITU-T [11] ได้มีการประกาศใช้ในปี ค .ศ.2003 เป็นมาตรฐานที่มีความสามารถในการบีบอัดภาพและเสียง และมีการเพิ่มอัตราการส่งผ่านเครือข่ายให้เร็วขึ้น เหมาะสมสำหรับกับการนำไปใช้ในโทรศัพท์เคลื่อนที่, Video Real-Time, Video Conference นอกจากนี้มาตรฐานของ H.264 ยังมีคุณสมบัติ ที่ใช้ Bandwidth ที่ต่ำมาก เมื่อเทียบกับมาตรฐานอื่นๆในการทดลอง

การเข้ารหัสวิดีโอได้เกิดขึ้น ใน [12] เป็นการนำเสนอการเข้ารหัสวีดีโอคุณลักษณะของภาพบางส่วนของวิดีโอจะถูกทำให้ลดลงด้วยการเข้ารหัส ได้ตระหนักถึงการเข้ารหัสที่มีประสิทธิภาพในการรับรู้ที่มีคุณภาพ ทดลองโดยการนำเข้าของวิดีโอขนาดต่างๆ และที่มีการเคลื่อนไหว โดยพิจารณาในส่วนของในการควบคุมสามส่วนได้แก่ psr, psd และ pmv ระหว่าง1 ถึง 0 ซึ่งจะทำการแทนค่าของทั้งสามปัจจัย ผลที่ได้จากการทดลองทำให้เป็นที่ยอมรับในด้านความปลอดภัยที่มีคุณภาพสูง และยังสามารถป้องกันการโจมตี ความสามารถอีกด้านหนึ่งของการแทนค่า คือ สามารถที่จะรองรับการใช้งานได้อย่างหลากหลายในสภาพการทำงานที่แตกต่างกัน คุณภาพที่ได้จากการเข้ารหัสด้วยวิธีนี้จะมีความคงคุณภาพของภาพวิดีโอเท่าเทียบกับภาพวิดีโอต้นฉบับ แต่ผลที่ได้ออกมาด้วยวิธีการดังกล่าวขนาดของภาพจะมีขนาดที่ใหญ่ และอัตราการส่งข้อมูลของภาพ

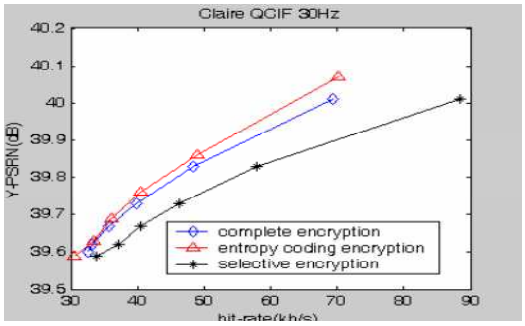
วิดีโอยังคงมีความล่าช้า สำหรับการทดลองการเข้ารหัสวิดีโอได้เกิดขึ้นอย่างต่อเนื่อง ทำให้มีการพัฒนาและคุณภาพของวิดีโอที่ได้จากการเข้ารหัสสูง และมีความปลอดภัยเพิ่มขึ้นเรื่อยๆ ในอีกการทดลองของ [13] ได้ทำการเข้ารหัสวิดีโอโดยการเลือกรูปแบบชั้นการเข้ารหัสสำหรับขยายขีดความสามารถในการเข้ารหัสวิดีโอ (Scalable Video Coding, SVC) ขั้นตอนการเข้ารหัสจะดำเนินการที่ระดับ Network Abstractor Layer (NAL) ดำเนินการทดลองวิธีการลำดับของการทดสอบของ SVC, “Foreman” จะใช้สำหรับทำการทดสอบ ลำดับที่จะถูกเข้ารหัสใน 2 ชั้น (CIF, QCIF) ในรูปแบบการเข้ารหัสนี้ ทำการเข้ารหัสวิดีโอสตรีมกับ NAL และทำให้แต่ละหน่วย NAL ที่มีส่วนสำคัญแตกต่างกัน ในการทดลองได้ตระหนักถึงการทำให้ข้อมูลตรงกัน หากเมื่อเกิดมีการส่งข้อมูลผิดพลาดเกิดขึ้น กล่าวคือ หากมีข้อผิดพลาดเกิดขึ้นในหน่วย NALขึ้น ในขณะที่คนอื่น ๆ จะยังคงสามารถถอดรหัสได้อย่างถูกต้องนอกจากนี้ ในส่วนที่สำคัญและรูปแบบการกระจายการรับประกัน รักษาความปลอดภัยและเพื่อเพิ่มคุณภาพในการส่งข้อมูลผิดพลาด ผลการทดลองแสดงให้เห็นว่าขั้นตอนวิธีการที่ทำการทดลองตอบสนองความต้องการการเข้ารหัส SVC และให้ความปลอดภัยสูงความคงสภาพของข้อมูลนั้นเหมือนกับต้นฉบับ

มาตรฐานการเข้ารหัสวิดีโอ H.264 [14] รองรับได้หลากหลายแอพพลิเคชั่นและวิธีเพื่อรับประกันความปลอดภัยที่มีอยู่แล้วกลายเป็นปัญหาเร่งด่วน ในงานวิจัยนี้ได้นำเสนออวิธีการเข้ารหัสวิดีโอสำหรับ H.264 ซึ่งรวมวิธี stream cipher algorithm กับกระบวนการการเข้ารหัส entropy มันได้รับการรักษาความปลอดภัยเนื้อหาวิดีโอจากการเข้ารหัส codeword index เพื่อหาตำแหน่งของ codeword การทดลองแสดงให้เห็นว่า การเสนออัลกอริทึมที่สามารถยอมรับได้ระหว่างความปลอดภัยและความซับซ้อนมีผลเล็กน้อยบนประสิทธิภาพการบีบอัด มันสามารถที่จะมีการนำไปใช้ในการประชุมวิดีโอ การจัดการสิทธิ์ดิจิตอลและการจัดเก็บข้อมูลมัลติมิเดีย อื่นๆ บทสรุปและแนวทางในอนาคตในงานวิจัยนี้ผู้วิจัยนำเสนออัลกอริทึมการเข้ารหัสวิดีโอบนพื้นฐานของการเข้ารหัส entropy H.264 นี่คืออัลกอริทึมที่สามารถแลกเปลี่ยนระหว่างความปลอดภัยและความซับซ้อนโดยไม่ยอมรับการบีบอัดประสิทธิภาพ มันเหมาะในการนำไปใช้เพื่อรักษาความปลอดภัยของการประชุมแบบวิดีโอ การจัดการสิทธิ์ดิจิตอล การจัดเก็บข้อมูลมัลติมีเดียอื่นๆ วิธีการนี้จะขยายและพัฒนาโดยการเพิ่มประสิทธิภาพอัลกอริทึม cipher และการเปลี่ยนแปลงตำแหน่งการเข้ารหัสนอกจากนี้ H.264 มีการนำเสนอวิธีการเข้ารหัส two entropy กับการวิจัยและแอพพลิเคชันของ H.264ในการส่งข้อมูลวิดีโอดิจิตอลแบบการกระจาย วิธีการเข้ารหัส bitsteam ใน CABAC (context-adaptive binary arithmetic coding) สนับสนุนจากโปรไฟล์หลักซึ่งควรถูกนำมาพิจารณาสิ่งเหล่านี้คือแนวทางการทำงานในอนาคต

(1) (2) (3)

รูปที่ 1 การวิเคราะห์ความปลอดภัย (**Security analysis**)

เปรียบเทียบ (1) วิดีโอที่ไม่ได้มีการเข้ารหัส (2) เป็นการเข้ารหัสด้วยวิธี selective (3) เป็นการเข้ารหัสด้วยวิธี entropy จะเห็นได้ว่ารูปที่ (3)มีความปลอดภัยมากกว่ารูปที่ ดังนั้นการเข้ารหัสด้วยวิธี (2) entropy จึงปลอดภัยกว่า เทคนิคที่ใช้ในงานวิจัยนี้ที่ใช้จะมีการใช้วิธี entropy coding , cipher algorithm , Encrypting the codewords indices และ RC4 cipher algorithm การวัดความซับซ้อนของงานวิจัยนี้ค่าคำนวณของความซับซ้อนมีค่าในระดับต่ำ พอที่จะรองรับการประมวลผลแบบเรียลไทม์

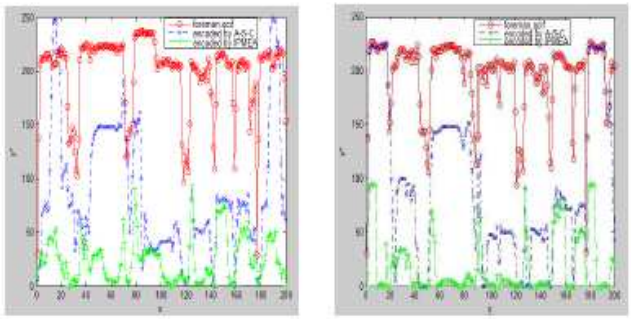


รูปที่ 2 Rate distortion performance (RD) ยิ่งอัตราการส่งมากประสิทธิภาพยิ่งดี และจะเห็นว่าวิธีการ entropy coding encryption มีผลที่ดีกว่าแบบอื่น

ใน [15] H.264 เป็นการเข้ารหัสวิดีโอแบบใหม่มาตรฐานโลกและการรักษาความปลอดภัยของวิดีโอแบบ H.264 เริ่มมีการวิจัย การวิจัยนี้ได้วิเคราะห์การรักษาความปลอดภัยที่ไม่ดีพอของ intra prediction mode (IPM) อัลกอริทึมการเข้ารหัสที่เสนอมาจากงานวิจัยของ Ahn J, Shim H J, Byeungwoo J, et al..., “Digital Video Scrambling Method Using Intra Prediction Mode”, PCM 2004 [C], LNCS 3333, 2004, pp. 386-393. จากมุมมองของการเข้าใจประสิทธิภาพการหาช่องว่าง plaintext และการรักษาความปลอดภัยของคีย์และจากนั้นนำเสนอการพัฒนาอัลกอริทึมการเข้ารหัส IPM (IPMEA) มันจะเข้ารหัส IPMs ทั้งหมดโดยการลำดับสุ่ม แทรกลงไปสำหรับครั้งที่สองจากนั้นหมุนเวียนลำดับที่ควบคุมโดยคีย์และช่วยให้โครงสร้างของคีย์กระจายและประสานกัน การวิเคราะห์ประสิทธิภาพและผลการทดลองแสดงให้เห็นว่า IPMEA สามารถรักษาความปลอดภัยได้สูงกว่าวิธีแบบเดิมและมีผลกระทบต่อความยาวโค้ดเพียงเล็กน้อย ขณะเดียวกันก็มีความซับซ้อนต่ำและมีคุณสมบัติเรียลไทม์ที่ดีดังนั้นจึงเหมาะสำหรับการส่งผ่านวิดีโอแบบเรียลไทม์ผ่านเครือข่าย

สรุปงานวิจัยนี้พูดถึงปัญหาการรักษาความปลอดภัยที่ไม่ดีพอของการวิเคราะห์อัลกอริทึมการเข้ารหัส IPM และเมื่อถูกพัฒนาเป็นอัลกอริทึมการเข้ารหัส IPMEA บนพื้นฐานของ H.264 คือสนับสนุน เลือก IPMs ทั้งหมดเป็น plaintext เพื่อเข้ารหัส จากนั้นขยายส่วนพื้นที่ scrambling นำมาใช้หมุนเวียนลำดับที่ควบคุมโดยคีย์ในการเข้ารหัส Intra_4 × 4 บล็อกจะ IPMs สองครั้งเพื่อให้พื้นที่ scrambling เป็นตัวขยายต่อไปและการรักษาความปลอดภัยของอัลกอริทึมจะถูกพัฒนาและเลือก chaotic pseudo-random Sequence เป็นคีย์กับการพิจารณาการอัพเดตและการใช้ความคิดในการใช้คีย์ร่วมกัน ดังนั้นการรักษาค่าคอส (Cost) ของการคำนวณจะถูกบันทึกไว้ การวิเคราะห์ประสิทธิภาพและ

ผลการทดลองแสดงให้เห็นว่า IPMEA สามารถรักษาความปลอดภัยได้สูงกว่าแบบเดิมที่มีอยู่และมีผลกระทบต่อความยาวโค้ดเพียงเล็กน้อย ในขณะเดียวกันมันก็มีความซับซ้อนต่ำและมีคุณสมบัติเรียลไทม์ที่ดีดังนั้นจึงเหมาะสำหรับการส่งผ่านวิดีโอแบบเรียลไทม์ผ่านเครือข่าย ถ้าเราใช้ IPMEA ร่วมกันกับแบบอื่นในอัลกอริทึมการเข้ารหัส การรักษาความปลอดภัยจะสูงขึ้นและสูงกว่าเดิม เทคนิคที่งานวิจัยนี้นำมาใช้คือการใช้อัลกอริทึมการเข้ารหัส IPMEA



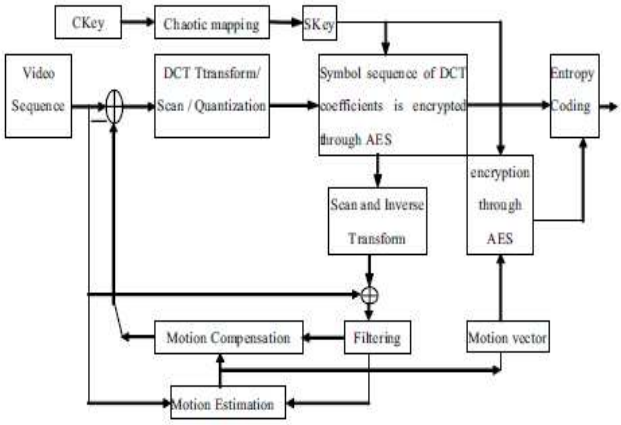
(1) (2)

รูปที่ 3 การเปรียบเทียบของ pixel เปลี่ยนหลังจากการเข้ารหัสภาพ (1) การเปลี่ยน pixel ของ I frame (2) การเปลี่ยน pixel ของ P frame

สีแดงเป็นกราฟของภาพวิดีโอปกติ, สีน้ำเงินเป็นภาพวิดีโอที่ถูก encryption ด้วย A-S-C, สีเขียวเป็นภาพวิดีโอที่ encryption ด้วย IPMEA จะเห็นว่าประสิทธิภาพของ IPMEA ดีกว่า

สำหรับใน [16] งานวิจัยนี้กล่าวถึงปัญหาเกี่ยวกับการรักษาความปลอดภัยวิดีโอบนพื้นฐานของมาตรฐานการเข้ารหัสการบีบอัดวิดีโอ H.264 ส่งต่อการออกแบบโครงสร้างของการเข้ารหัสการประชุมวิดีโอ ระบบการเข้ารหัสวิดีโอรวมกับอัลกอริทึม AES (Advanced Encryption Standard) H.264 และการเข้ารหัสซับซ้อน โครงสร้างนี้ AES ถูกใช้ในการเข้ารหัสค่าสัมประสิทธิ์ DCT และการเคลื่อนไหว เวกเตอร์ สัญลักษณ์ ลำดับของ H.264 การป้องกันของวิดีโอข้อมูลการเคลื่อนไหวและข้อมูลพื้นผิววิดีโอจะได้รับในระบบการเข้ารหัสการเข้ารหัสวิดีโอ เทคโนโลยีการเข้ารหัสที่สับสนจะถูกใช้เพื่อทำให้เกิดคีย์จากการประชุมวิดีโอเพื่อไปรับรองว่าจะไม่สามารถทายค่าคีย์ได้ การทดลองแสดงให้เห็นว่าระบบสามารถทำให้การคำนวณการเข้ารหัสวิดีโอรวดเร็วและการประชุมวิดีโอเป็นไปอย่างราบรื่น นอกจากนี้สามารถป้องกันข้อมูลวิดีโอจากการดักข้อมูลและโจมตี มันเพิ่มความน่าเชื่อถือของการสื่อสาร กลุ่มสมาชิกสามารถปลอดภัยและเป็นผลทำให้บริการมีความน่าเชื่อถือสามารถใช้ได้สำเร็จ

การวิจัยนี้ระบบการเข้ารหัสการประชุมวิดีโอสมบูรณ์ถูกสร้าง ปัญหาที่เกี่ยวกับการตรวจสอบ การกำหนดคีย์ การแจกคีย์ และการแก้ปัญหาของความน่าเชื่อถือของข้อมูลวิดีโอ การทำงานสมบูรณ์ในงานวิจัยนี้มีขั้นตอนดังนี้ 1) AES เป็นเครื่องมือที่ใช้การเข้ารหัสลำดับสัญลักษณ์ของค่าสัมประสิทธิ์ DCT และเวกเตอร์การเคลื่อนที่ของวิดีโอสตรีม H.264 การป้องกันของการเคลื่อนย้ายข้อมูลวิดีโอและข้อมูลพื้นผิววิดีโอที่ได้รับ



รูปที่ 4 โฟลว์ชาตร์ของการพัฒนาระบบการเข้ารหัสวิดิโอ

รูปที่ 5โฟลว์ชาตร์ของการพัฒนาระบบการเข้ารหัสวิดิโอ

2) เนื่องจากอัลกอริทึมที่รวดเร็วถูกใช้ในการทำให้เป็นจริงของ AES การเข้ารหัสที่รวดเร็วและการถอดรหัส สามารถทำสำเร็จ การประมาณอุปสรรคมีค่อนข้างน้อยที่ระบบ multicast และการประชุมของวิดีโอเล่นได้ราบรื่น การรักษาความปลอดภัยของอัลกอริทึมAES จะดีกว่าอัลกอริทึมแบบเก่า ดังนั้นข้อมูลวิดีโอสามารถป้องกันจากการดักข้อมูลและความน่าเชื่อถือของการสื่อสารถูกพัฒนาขึ้น 3) CKey และ SKey เป็นการสร้างจากอัลกอริทึม chaotic mapping ค่า CKey เป็นค่าเริ่มต้น เงื่อนไขของ SKey ดังนั้นการทำนายค่าของคีย์สามารถทำได้ คีย์สาธารณะอัลกอริทึม RSA ถูกใช้ในการกระจายคีย์และให้สิทธิ์ผู้ใช้ที่เวลาเดียวกัน ผลการทดลองแสดงให้เห็นว่าสมาชิกมีความปลอดภัยและเป็นผลให้บริการมีความน่าเชื่อถือสามารถนำไปใช้ได้

เทคนิคที่ใช้ คือ ระบบการเข้ารหัสวิดีโอรวมกับอัลกอริทึม AES (Advanced Encryption Standard) ผลการทดสอบของงานวิจัยนี้สรุปได้ว่ามีการเข้ารหัสที่มีความรวดเร็ว ภาพวิดีโอเล่นได้ราบรื่นไม่มีสะดุด การรักษาความปลอดภัยของข้อมูลภาพวิดีโอของอัลกอริทึม AES ดีกว่าอัลกอริทึมแบบเก่า

ตารางที่ 3 เปรียบเทียบคุณสมบัติของเทคนิคการเข้ารหัส

วิธีการเข้ารหัส	งานวิจัย	ขนาดของภาพ	อัตราการเข้ารหัส	ความเร็ว	ความปลอดภัย
Selective Encryption	[11] Compliant selective encryption for H.264/AVC video streams	เล็ก	20 – 30%	-	สูง
Layered Encryption	[12] Layered Encryption for Scalable Video Coding	ใหญ่	ต่ำ	ต่ำ	สูง
Perceptual Video Encryption	[13] Perceptual Video Encryption for Multimedia Applications	ใหญ่	-	ต่ำ	สูง
entropy coding encryption	[14] An H.264 Video Encryption Algorithm Based On Entropy Coding	-	ต่ำ	เร็ว	สูง
IPM encryption algorithm (IPMEA)	[15] An Intra Prediction Mode-based Video Encryption Algorithm in H.264 Abstract	ใหญ่	-	เร็ว	สูง
Advanced Encryption Standard	[16] The Design of Video-Conference Encryption System based on H.264	-	-	เร็ว	สูง

IV. Error Control Video

การควบคุมข้อผิดพลาดของข้อมูลหรือ error control คือ การที่ผู้ส่งต้องส่งข้อมูลไปใหม่อีกครั้งหนึ่ง ถ้าผู้รับไม่สามารถรับข้อมูลหรือได้รับข้อมูลที่ไม่ถูกต้อง สาเหตุที่ต้องมีการควบคุมก็เนื่องจากว่า ข้อมูลจะต้องเดินทางจากที่หนึ่งไปยังอีกที่หนึ่ง จึงมีความเป็นไปได้ที่ข้อมูลชุดนั้นจะเกิดสูญหายหรือเสียหายในระหว่างการเดินทางได้

A. การดำเนินการกับข้อผิดพลาด

เมื่อฝั่งรับตรวจพบข้อผิดพลาดจากข้อมูลที่ส่งมาฝั่งรับสามารถดาเนินการกับข้อผิดพลาดที่เกิดขึ้นได้ 3 กรณีคือ

1. ไม่ต้องดาเนินการใดๆ (Do nothing) จะปล่อยเฟรมข้อมูลที่ผิดพลาดไปแล้วให้ชั้นสื่อสารที่อยู่เหนือกว่าไปจัดการแทน
2. แจ้งกลับไปให้ฝั่งส่งรับทราบ (Return a message) เพื่อให้ฝั่งส่งทำการส่งข้อมูลส่วนที่เสียหายมาให้อีกครั้ง
3. ตรวจแก้ข้อผิดพลาด (Correct the Error) จะดำเนินการแก้ไขข้อผิดพลาดที่ฝั่งรับเองโดยไม่ต้องให้ฝั่งส่ง ส่งข้อมูลมาใหม่ซึ่งเป็นวิธีที่ซับซ้อนกว่าวิธีทั้งหมด

ชนิดของข้อผิดพลาด สาหรับข้อผิดพลาดที่ตรวจพบนั้นสามารถแบ่งเป็นชนิดของข้อผิดพลาด 2 ชนิด

1. เฟรมสูญหาย (Lost Frame) คือเฟรมข้อมูลที่ส่งไปไม่ถึงปลายทางซึ่งอาจเกิดจากสาเหตุของสัญญาณรบกวนที่ทาให้เฟรมข้อมูลเสียหายจนทำให้ฝั่งรับไม่สามารถตีความหรือไม่ทราบว่าเฟรมนั้นส่งมาถึง
2. เฟรมชำรุด (Damage Frame) คือเฟรมสามารถส่งไปถึงปลายทางแต่บิตของข้อมูลบางส่วนเกิดการเปลี่ยนแปลงระหว่างการส่ง

เทคนิคการควบคุมข้อผิดพลาดจะอยู่บนพื้นฐานของส่วนประกอบต่างๆดังนี้

- การตรวจจับข้อผิดพลาดปลายทางจะมีการนาเฟรมที่ได้รับมาทำการตรวจจับข้อผิดพลาดด้วยเทคนิควิธีการต่างๆ
- การตอบรับ ACK ปลายทางจะตอบรับ ACK เมื่อได้รับข้อมูลอย่างสมบูรณ์โดยไม่มีข้อผิดพลาดใดๆ
- การส่งข้อมูลรอบใหม่หลังจากรอจนหมดเวลา (Timeout) ฝั่งส่งจะทำการส่งเฟรมข้อมูลรอบใหม่ทันทีในกรณีที่ปลายทางไม่ตอบรับกลับมาภายในเวลาที่กาหนดก็คือเกิด Timeout
- การตอบรับ NAK และการส่งข้อมูลรอบใหม่ปลายทางจะมีการตอบรับ NAK (Negative Acknowledgement) กลับมาที่ฝั่งส่งในกรณีที่เฟรมที่ได้รับนั้นเกิดข้อผิดพลาดเมื่อฝั่งส่งได้รับการตอบรับ NAK ก็จะทราบว่าข้อมูลที่ส่งไปนั้นมีข้อผิดพลาดจะดำเนินการส่งเฟรมข้อมูลไปอีกครั้ง

B. ปัญหา

สำหรับการสื่อสารในรูปแบบ (video H.264) ผ่าน wireless ยังมีปัญหาในการส่งอยู่ เช่นถ้าอยู่ในชั้น UDP จะไม่สามารถรับประกันความถูกต้องของข้อมูลได้ บางตัวจะตอบสนองเฉพาะการส่งผ่านโทรศัพท์เท่านั้น ใช้ทรัพยากรของระบบค่อนข้างสูงขณะที่รายละเอียดภาพที่ได้จะมีคุณภาพไม่สูงมากนักหรือไม่ก็ทำให้เกิดดีเลย์มากในกรณีที่เกิดข้อผิดพลาดจากการส่งและข้อมูลที่กู้คืนจะได้ไม่ร้อยเปอร์เซ็นต์เป็นต้น ดังนั้นในบทความนี้จะนำเสนอวิธีการแก้ไขปัญหาข้างต้นเพื่อให้การส่ง รูปแบบ (video H.264) ผ่าน wireless มีความเสถียรมากขึ้น

C. วิธีการแก้ไขปัญหา

ใน [17] ใช้รหัส LDPC ในการจัดการแพ็กเก็ตที่เสียออกไปมีการประมวลแพ็กเก็ตที่เสียเลยทันทีเพื่อรองรับการส่งแพ็กเก็ตซ้ำอีกรอบ [18] ใช้ Rateless Code ในการส่งแพ็กเก็ตซ้ำทำให้ได้videoที่มีคุณภาพสูงในการส่งผ่านอุปกรณ์มือถือ [19] ออกแบบเครือข่าย H.264/AVC เป็นการจำลองเครือข่าย ซึ่งเหมาะกับสภาพแวดล้อมแบบไร้สายมากที่สุด [20] การเข้ารหัสแพ็กเก็ตที่มีขนาดเล็กกว่าขนาดบัฟเฟอร์ทำให้ไม่ต้องเปลืองหน่วยความจำเพื่อนำไปใช้บัฟเฟอร์ [21] การเพิ่มประสิทธิ์ภาพของเส้นทางการส่งโดยใช้ ECARS RD ทำให้สามารถเพิ่มขนาดเส้นทางการส่งแพ็กเก็ตได้ [22] การควบคุมลดค่า costs ในชั้น MAC สามารถแก้ไขข้อผิดพลาดในการส่งแพ็กเก็ตโดยสามารถแยกเป็นแต่ละระดับได้ [23] ใช้เทคนิค RESCU เพื่อช่วยให้มีเวลามากขึ้นสำหรับการกู้คืนแพ็กเก็ตมีคุณภาพสูงในการโต้ตอบแบบเรียวไทม์ [24] การปรับ Sub - Packet กลไก FEC (SPFEC) ปรับปรุงคุณภาพของข้อมูลวิดีโอสตรีมมิ่งผ่านเครือข่ายไร้สายพร้อมกันเพิ่มประสิทธิภาพการกู้คืน[25] วิธีการของห่วงโซ่มาร์คอฟ packet retransmissions กรอบการทำงานสามารถที่จะประเมินคำร้องขอทำซ้ำ [26] นำเสนอกลไก DM - FEC ใช้รูปแบบการวิเคราะห์ทางคณิตศาสตร์เพื่อกำหนดอัตราการส่งที่เหมาะสมความยาวบล็อก FEC และ FEC ความซ้ำซ้อนในแต่ละเส้นทางในสภาพแวดล้อมที่ multipath ดังนั้นกลไกการ DM - FEC ไม่ก่อให้เกิดผลกระทบที่เกิดปัญหาความแออัดของตนเอง

ตาราง 4 เปรียบเทียบการใช้เทคนิคจัดการกับข้อผิดพลาด

Paper	Do nothing	ACK	Timeout	NAK
17			yes	
18			yes	
19	yes			
20	yes			
21		yes		
22				yes
23				yes
24				yes
25			yes	
26				yes

จากตาราง จะเห็นได้ว่าการแก้ไขปัญหาที่เกิดจากข้อผิดพลาด error control ของแต่ละงานวิจัยจะเลือกวิธีการใดวิธีการหนึ่งเท่านั้น ซึ่งทางผู้เขียนเห็นว่ายังไม่เพียงพอต่อการนำไปใช้งานเพราะการจัดการกับปัญหาทั้ง3 ข้อจะมีทั้งข้อดีและข้อเสียที่แตกต่างกันไป เราจึงได้นำเสนอแนวคิดการแก้ไขปัญหาใหม่ซึ่งก็คือ การรวมเอาข้อดีของวิธีการจัดการกับ error control ทั้งสามข้อมาใช้เป็นวิธีการใหม่ ที่จะสามารถนำมาใช้ในการสื่อสารในรูปแบบ video ที่ใช้ code H.264 ผ่านทางสัญญาณ wireless โดยการเพิ่ม Error Frame เข้าไปด้วยในแต่ละแพ็กเก็ตก่อนที่จะส่ง ซึ่งจะเป็นตัวเช็คข้อผิดพลาดให้ แพ็กเก็ตทุกตัว หลักการคือ ErrorFrame จะทำหน้าที่กำหนด timeoutเพื่อเช็คแพ็กเก็ตที่เสียก่อนจะทำการส่งใหม่อีกรอบโดยไม่ต้องรอ timeout จากเครือข่าย

Header	Packet NO	ErrorTime (time out = 5 sec.)

รูปที่ 6 แสดงรายละเอียดของ Error Frame

ซึ่งประกอบไปด้วย 3 ส่วนคือ ส่วนหัวลำดับของแพ็กเก็ตและส่วนสุดท้ายคือ Error Time เป็นส่วนที่เช็คเมื่อ แพ็กเก็ตเกิดข้อผิดพลาดขึ้นให้ทำการส่งแพ็กเก็ตนั้นอีกรอบโดยใช้การนับเวลาเพื่อกำหนดTimeout

D. วิธีการแก้ไขปัญหาที่เกิดจากข้อผิดพลาดใหม่

การแก้ไขปัญหาที่เกิดจากข้อผิดพลาดในการส่งvideo ที่ใช้ code H.264 ผ่านทางสัญญาณ wireless โดยการแนบ Error Frame เข้าไปด้วยในการส่งทุกแพ็กเก็ต เมื่อแพ็กเก็ตเกิดการเสียหาย Error Frame ก็จะทำการนับเวลา time out แล้วก็ส่งแพ็กเก็ต NAK กลับมาทันทีโดยไม่ต้องรอ time out ของเครือข่ายเพื่อแจ้งให้ sender ทำให้การส่งแพ็กเก็ตที่เสียหายอีกรอบ ทำให้การรับข้อมูลเป็นไปอย่างรวดเร็ววีดีโอจะที่ได้จะไม่กระตุกเพราะไม่เกิดการดีเลย์มาก

V. PROTOCOL

โปรโตคอล (Protocol) คือระเบียบพิธีการในการติดต่อสื่อสาร เมื่อมาใช้กับเทคโนโลยีสื่อสารโทรคมนาคม จึงหมายถึงขั้นตอนการติดต่อสื่อสาร ซึ่งรวมถึงกฎ ระเบียบ และข้อกำหนดต่าง ๆ รวมถึงมาตรฐานที่ใช้ เพื่อให้ตัวรับและตัวส่งสามารถดำเนินกิจกรรมทางด้าน สื่อสารได้สำเร็จ ซึ่งโปรโตคอลมาตรฐานหลักๆคือ TCP และ UDP เป็นมาตรฐานที่ยอมรับกันและนำมาใช้ในการเชื่อมต่อระหว่างกัน แต่เนื่องจากโปรโตคอล TCP และ UDP มีข้อจำกัดในการใช้งานที่แตกต่างกันจึงมีการคิดค้นโปรโตคอลรูปแบบใหม่ออกมาเพื่อแก้ไขขีดจำกัดของ TCP และ UDP อยู่หลายโปรโตคอล ซึ่งในที่นี้ได้รวบรวมโปรโตคอลรูปแบบใหม่ที่คิดค้นออกมาเพื่อให้สามารถนำไปใช้งานได้อย่างมีประสิทธิภาพอยู่ 7โปรโตคอล ดังนี้

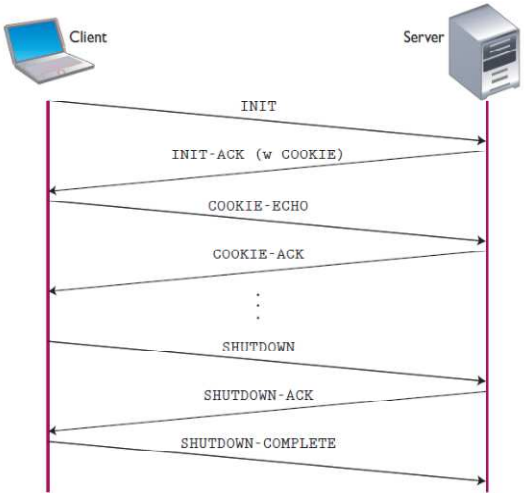
1. The Stream Control Transmission Protocol (SCTP)
2. DCCP : Transport Protocol with Congestion Control and Unreliability

3. Reducing Channel-Change Times with the Real-Time Transport Protocol (RTP)
4. MRTP: A Multiflow Real-Time Transport Protocol for Ad Hoc Networks
5. Licklider Transmission Protocol (LTP)-Based DTN for Cislunar Communications
6. Performance Study of eXtended Satellite Transport Protocol over Satellite Networks
7. Performance Evaluation of SSTP- a Transport Protocol for Satellite Channels

A.The Stream Control Transmission Protocol (SCTP)

The Stream Control Transmission Protocol (SCTP) [27] คือ การควบคุมและจัดการการส่งข้อมูลผ่านทางโปรโตคอล โดยมีวัตถุประสงค์ที่จะนำมาใช้ในการรับส่งข้อมูลบนระบบต่างๆ ที่มีการมุ่งเน้นไปในด้านการเชื่อมต่อที่มีความน่าเชื่อถือที่คล้ายกับ TCP และสามารถควบคุมการไหลของข้อมูลในที่ที่มีความแออัดของข้อมูลได้ รวมถึงสามารถรับส่งข้อมูลได้อย่างรวดเร็วที่คล้ายกับ UDP โดยที่ SCTP มีข้อแตกต่างจาก TCP และUDP คือ SCTP มีการให้บริการรับส่งข้อมูลที่มีประสิทธิภาพมากกว่าและสามารถรองรับกับการนำไปใช้ในระบบต่างๆได้อย่างหลากหลาย

กระบวนการในการทำงานของ SCTP คือ เมื่อมีการรับส่งข้อมูล ระหว่างเครื่องลูกข่ายและเครื่องแม่ข่าย ซึ่ง SCTP จะมีรูปแบบส่งข้อ ที่คล้ายกับ TCP ในลักษณะที่เน้นไปในด้านความน่าเชื่อถือของการรับส่ง รับส่งข้อมูล แต่ SCTP จะมีความแตกต่างจาก TCP ตรงส่วนของความ ปลอดภัยขณะรับส่งข้อมูล ซึ่ง SCTP นั้นจะมีการตรวจสอบความถูกต้อง ความปลอดภัย ของเครื่องลูกข่ายที่ทำการร้องขอในการรับส่งข้อมูลรวมถึงการยืนยันในการรับส่งข้อมูล โดยใช้ระบบคุกกี้แนบไปกับการรับส่งข้อมูลและการยืนยันในการรับส่งข้อมูลนั้นๆ ตามรูปด้านล่าง



รูปที่ 7 การรับส่งข้อมูลระหว่างเครื่องลูกข่ายและเครื่องแม่ข่าย

การรับส่งข้อมูลระหว่างเครื่องลูกข่ายและเครื่องแม่ข่าย ซึ่งเครื่องลูกข่ายจะต้องร้องขอมาที่เครื่องแม่ข่าย เครื่องแม่ข่ายจะทำการส่งข้อมูลที่ถูกร้องขอและจะแนบไฟล์คุกกี้กลับไปยังเครื่องลูกข่ายด้วย เมื่อเครื่องลูกข่ายทำการร้องขอมาอีกไฟล์คุกกี้จะถูกแนบมากับการร้องขอของเครื่องลูกข่ายด้วยเพื่อที่จะให้เครื่องแม่ข่ายสามารถทำการตรวจสอบความถูกต้อง ความปลอดภัยในการรับส่งข้อมูลได้

ข้อดีของ SCTP เมื่อเทียบกับโปรโตคอล TCP และ UDP ซึ่งสามารถเปรียบเทียบได้ดังนี้ Connection-oriented สามารถทำการค้นหาเส้นทางไว้ล่วงหน้าก่อนที่จะมีการรับส่งข้อมูล เพื่อรับประกันว่าข้อมูลที่ส่งไปจะครบสมบูรณ์

1. Message-based transfer สามารถจัดเก็บข้อมูลที่อยู่ในระหว่างการส่ง
2. Reliable data transfer มีความน่าเชื่อถือในการส่งข้อมูล
3. Partially reliable data transfer สามารถส่งข้อมูลที่ไม่สมบูรณ์ได้
4. Ordered data delivery สามารถส่งข้อมูลแบบเรียงลำดับข้อมูลได้
5. Unordered data delivery สามารถส่งข้อมูลได้โดยไม่ต้องเรียงลำดับ
6. Congestion and flow control สามารถควบคุมความแออัดของข้อมูล
7. Protection from spoofed SYN attacks สามารถป้องกันการโดนโจมตีจากโปรแกรม Spoofed
8. Allows half-closed connections ขณะที่เครื่องลูกข่ายส่งการยืนยันว่าหยุดการเชื่อมต่อสำเร็จแล้ว เครื่องแม่ข่ายจะไม่มีการตอบยืนยันกลับไปอีก
9. Multistreaming สามารถส่งข้อมูลได้หลายข้อมูลในเวลาเดียวกัน
10. Multihoming ในอุปกรณ์เครื่องเดียวที่มีเลข IP ชุดเดียวสามารถเชื่อมต่อไปยังอุปกรณ์เครื่องอื่นในเครือข่ายได้ในรูปแบบ end to end แต่ในเวลาเดียวกันที่กำลังเชื่อมต่อกับอุปกรณ์เครื่องหนึ่งอยู่ยังสามารถเชื่อมต่อกับอุปกรณ์เครื่องอื่นได้อีกในรูปแบบ end to end
11. Dynamic address reconfiguration สามารถกำหนดค่าในการเชื่อมต่อไปยังอุปกรณ์ที่มีการเปลี่ยนแปลงที่อยู่ได้

ซึ่งการเปรียบเทียบคุณสมบัติต่างๆจะพบได้จากตารางด้านล่าง

ตารางที่ 5 เปรียบเทียบคุณสมบัติระหว่างโปรโตคอล SCTP และ TCP , UDP

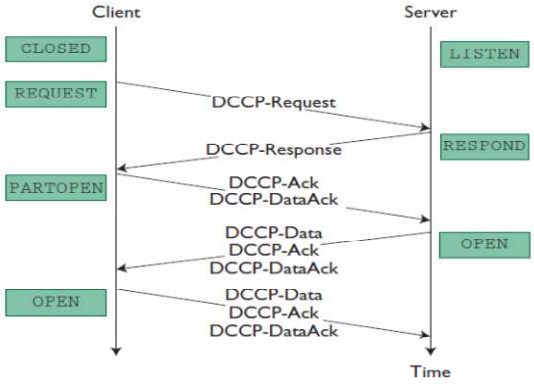
Services/features	SCTP	TCP	UDP
Connection-oriented	Yes	Yes	No
Message-based transfer	Yes	No	Yes
Reliable data transfer	Yes	Yes	No
Partially reliable data transfer	Yes	No	No
Ordered data delivery	Yes	Yes	No
Unordered data delivery	Yes	No	Yes
Congestion and flow control	Yes	Yes	No
Protection from spoofed SYN attacks	Yes	No	NA
Allows half-closed connections	No	Yes	NA
Multistreaming	Yes	No	No
Multihoming	Yes	No	No
Dynamic address reconfiguration	Yes	No	No

B. DCCP : Transport Protocol with Congestion Control and Unreliability

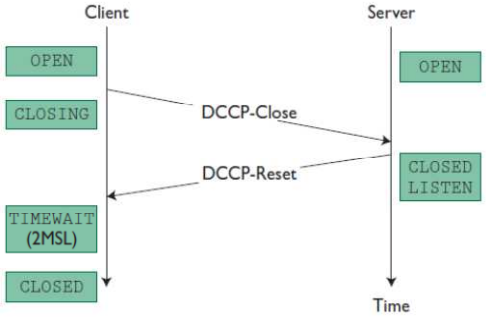
The Datagram Congestion Control Protocol (DCCP) [28] คือ โปรโตคอลที่ถูกออกแบบมาเพื่อรับส่งข้อมูลที่ได้มาตรฐานของ IETF เนื่องจาก DCCP มีความสามารถที่จะควบคุมการส่งข้อมูลเป็นจำนวนมากที่จะก่อให้เกิดความแออัดของข้อมูลและยังมุ่งเน้นให้มีความน่าเชื่อถือในการรับส่งข้อมูล DCCP จึงมีความเหมาสมอย่างยิ่งกับการนำไปใช้ในการส่งข้อมูลมัลติมีเดียหรือการนำไปใช้รับส่งข้อมูลบนระบบต่างๆ DCCP จะมีรูปแบบการทำงานอยู่สองรูปแบบคือ การสร้างความเหมาะสมให้กับการรับส่งข้อมูล และลดการเชื่อมต่อที่ไม่มีความน่าเชื่อถือให้น้อยลง โดยการนำเทคนิคการควบคุมความแออัดของข้อมูลเข้ามาใช้ในการแก้ไขการเชื่อมต่อที่ไม่มีความน่าเชื่อถือ ซึ่งมีลักษณะในการทำงานดังนี้

1. Unreliable data transfer คือ การรับส่งข้อมูลที่ไม่มีความน่าเชื่อถือ ซึ่งในขณะที่ทำการส่งข้อมูลอยู่นั้นหากข้อมูลเกิดการสูญหาย DCCP จะไม่ทำการส่งข้อมูลซ้ำ
2. Reliable connection establishment and feature negotiation คือ หากการเชื่อมต่อมีความน่าเชื่อถือ ซึ่งขณะที่ทำการรับส่งข้อมูลแล้วเกิดข้อผิดพลาดทำให้ข้อมูลขาดหาย DCCP จะทำการส่งข้อมูลซ้ำไปอีกครั้ง
3. Adequate packet options คือ DCCP มีรูปแบบในการทำงานของการรับส่งข้อมูลหลายแบบ เช่น มีการร้องขอและยืนยันในการรับส่งข้อมูล มีการตรวจหาว่าการรับส่งข้อมูลใดหยุดชะงักไปบ้าง
4. Dynamic choice of congestion control คือ DCCP มีรูปแบบในการควบคุมความแออัดของข้อมูลอยู่ วิธี คือ การใช้รูปแบบ 2 CCID2 หรือการใช้รูปแบบ CCID3 ซึ่งทั้งสองรูปแบบนี้สามารถเลือกได้ว่าจะใช้รูปแบบใด
5. Dynamic adjustment of acknowledgment rate คือ DCCP สามารถปรับความเร็วในการขอการยืนยันการรับส่งข้อมูลให้มีความเหมาะสมตามตามสถานะการปัจจุบันได้
6. Prevention of SYN flooding attack คือ DCCP มีระบบป้องกันการโจมตีในรูปแบบการส่งข้อมูลหรือการร้องขอเป็นจำนวนมากเข้ามาในเวลาติดต่อกันซึ่ง DCCP ได้มีการใช้คุกกี้ในการตรวจสอบสถานะเพื่อป้องกันปัญหาดังกล่าวและปัญหานี้โปรโตคอล TCP มักจะประสบบ่อย

กระบวนการในการทำงานของ DCCP คือ เมื่อมีการรับส่งข้อมูลระหว่างเครื่องลูกข่ายและเครื่องแม่ข่าย ซึ่ง DCCP จะมีรูปแบบในการรับส่งข้อมูลที่คล้ายกับ TCP ในลักษณะที่เน้นไปในด้านความน่าเชื่อถือของการรับส่งข้อมูล แต่ DCCP จะมีความแตกต่างจาก TCP ตรงส่วนของรูปแบบในการเชื่อมต่อ ซึ่ง DCCP นั้นจะมีการเชื่อมต่อเพื่อรับส่งข้อมูลที่เหมือนกับ TCP คือเป็นแบบ ทรีเวย์ แฮนเช็ค (three-way handshake) ตามรูปที่ 14 ส่วนการยกเลิกการเชื่อมต่อนั้น DCCP จะใช้แบบ ทูเวย์ แฮนเช็ค (two-way handshake) ตามรูปที่ 15 หรือจะใช้แบบ ทรีเวย์ แฮนเช็ค (three-way handshake) ตามรูปที่ 16 แต่ TCP เมื่อต้องการยกเลิกการเชื่อมต่อจะต้องใช้แบบ โฟรเวย์ แฮนเช็ค (Four-way handshake) ด้วยเหตุนี้จะพบว่า DCCP มีการยกเลิกการเชื่อมต่อไปเร็วกว่าเป็นสองเท่า ซึ่งความเร็วตรงนี้มีผลเป็นอย่างมากหากมีการเชื่อมต่อกับเครื่องลูกข่ายหลายเครื่อง

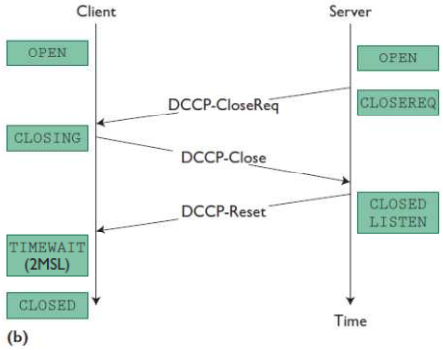


รูปที่ 8 เป็นการเชื่อมต่อระหว่างเครื่องลูกข่ายและเครื่องแม่ข่ายโดยใช้แบบทรีเวย์ แฮนเช็ค (three-way handshake)



รูปที่ 9 เป็นการร้องขอเพื่อยกเลิกการเชื่อมต่อ ซึ่งจะใช้แบบทูเวย์ แฮนเช็ค (two-way handshake)

โดยที่เครื่องลูกข่ายทำการแจ้งมายัง เครื่องแม่ข่ายว่าได้ทำการยกเลิกการเชื่อมต่อแล้ว จากนั้นเครื่องแม่ข่ายก็ส่งค่ายืนยันกลับไปที่เครื่องลูกข่าย



รูปที่ 10 เป็นการร้องขอเพื่อยกเลิกการเชื่อมต่อ ซึ่งจะใช้ แบบ ทรีเวย์ แฮนเช็ค (three-way handshake)

โดยที่เครื่องลูกข่ายจะทำการร้องขอมาที่เครื่องแม่ข่ายจากนั้นเครื่องแม่ข่ายทำการยืนยันกลับไป ต่อมาเครื่องลูกข่ายทำการตอบกลับมายังเครื่องแม่ข่ายว่าได้รับข้อมูลแล้ว

ข้อดีของ DCCP เมื่อเทียบกับโปรโตคอล TCP , UDP และ SCTP ซึ่งสามารถเปรียบเทียบได้ดังนี้

1. Setup connection เป็นแบบ ทรีเวย์ แฮนเช็ค (three-way handshake)
2. Shutdown connection คือ สามารถเลือกรูปแบบได้ทั้งแบบ ทูเวย์ แฮนเช็ค (two-way handshake) หรือ แบบ ทรีเวย์ แฮนเช็ค (three-3. way handshake)
3. Congestion control คือสามารถความคุมความแออัดของข้อมูลได้
4. Explicit congestion notification คือมีการแจ้งเตือนว่าการรับส่งข้อมูลมีมากน้อยเพียงใด
5. Selective acks คือสามารถเลือกรูปแบบการยืนยันการรับส่งข้อมูลได้
6. Dynamic congestion control mechanism คือ สามารถเปลี่ยนแปลงการรับส่งข้อมูลเพื่อป้องกันความแออัดของข้อมูลได้
7. Distinguish different kinds of losses สามารถตรวจหาสาเหตุของการสูญหายของข้อมูลได้
8. Path maximum transmission unit (PMTU) discovery คือสามารถทำการสืบค้นเส้นทางที่เหมาะสมได้
9. Protection against SYN flooding attack คือ สามารถป้องกันการส่งข้อมูลเป็นจำนวนมากเพื่อโจมตีเครื่องแม่ข่ายได้
10. Dynamic ack ratio คือ สามารถเปลี่ยนแปลงการยืนยันการรับส่งข้อมูลได้
11. Half-connection คือ สามารถทำการเชื่อมต่อได้หลายทางพร้อมๆกัน

ข้อจำกัดของ DCCP

1. Reliable data delivery คือ ขาดความน่าเชื่อถือในการจัดส่งข้อมูล
2. Flow control คือ ไม่สามารถควบคุมทิศทางการไหลของข้อมูลได้
3. Multistreaming คือ ไม่สามารถทำการส่งข้อมูลเป็นจวนมากในเวลาเดียวกันได้
4. Multihoming คือ ไม่สามารถทำการเชื่อมต่อเครือข่ายแบบ end to end มากกว่าหนึ่งการเชื่อมต่อในเวลาเดียวกันได้

C. Reducing Channel-Change Times with the Real-Time Transport Protocol

IETF ระบุ RTP ขึ้นในปี 1996 [29] เพื่อใช้ในการขนส่งแบบ end - to - end สำหรับบริการรับส่งข้อมูลแบบเรียลไทม์ผ่านเครือข่าย unicast และ multicast ต่อมา IETF ได้มีการค้นพบหลายประเด็นเกี่ยวกับกฎระเบียบ และขั้นตอนวิธีปรับปรุงความสามารถของ RTP IETF ได้ทำการปรับปรุงข้อกำหนด RTP กับ RFC 3550 ใน 2003.2 โดยกำหนดคุณสมบัติเพิ่มเติมที่ทันสมัยให้มากขึ้น RFC 3550 ปัจจุบันมีการใช้งานกันอย่างแพร่หลายในส่วนที่เกี่ยวกับเสียงและวิดีโอโปรแกรมการสื่อสารเพื่อตอบสนองตลาดใหม่เกี่ยวกับการใช้งานไอพีทีวีที่กำลังขยายตัว RTP จะทำงานอยู่บนพื้นฐานของ User Datagram Protocol (UDP) และคุณประโยชน์จากการสนับสนุนการตรวจสอบในการระบุแพ็กเก็ตที่เสียหาย เมื่อเทียบกับการขนส่ง UDP แบบธรรมดา RTP ให้บริการหลักดังต่อไปนี้

- มีการระบุรายละเอียดและฟอร์แม็ทต่างๆ เช่น ข้อมูลที่กำลังส่งนั้นเป็นข้อมูลเสียงที่เข้ารหัสในรูปแบบข้อมูล G.711 หรือวิดีโอเข้ารหัสมาในรูปแบบ H.264
- มีการเรียงลำดับหมายเลขเพื่อตรวจสอบแพ็คเก็ต RTP ที่มีการสูญหายระหว่างการขนส่ง ซึ่งถือเป็นวิธีการซ่อมแซมการสูญเสียแพ็คเก็ต
- การ Time-stamping ช่วยให้ผู้ส่ง และผู้รับตรวจสอบได้ว่าข้อมูลที่ได้ตรงกัน Time-stamping ยังมีประโยชน์สำหรับการคำนวณค่า delay jitter อีกด้วย

RTP ให้บริการเหล่านี้ผ่านทางค่า default ส่วน Header 12 ไบต์ อย่างไรก็ตาม โปรแกรมประยุกต์สามารถขยายฟังก์ชันการทำงาน RTP โดยใช้กลไกส่วนขยายที่ส่วน Header

D. MRTP: A Multiflow Real-Time Transport Protocol for Ad Hoc Networks

โปรโตคอล MRTP [30] ใช้สำหรับการขนส่งข้อมูลมัลติมีเดียแบบเรียลไทม์ผ่านอุปกรณ์เคลื่อนที่บนเครือข่าย โดยมีการสื่อสารบนความหลากหลายของเส้นทาง ซึ่ง MRTP เป็นส่วนขยายของ real-time transport protocols เช่น RTP/RTCP ที่ประกอบด้วยความสามารถในการขนส่งแบบหลายเส้นทาง โดยเป็นศูนย์กลางการขนส่งโปรโตคอล (เช่น SCTP) สำหรับการใช้งานมัลติมีเดียแบบเรียลไทม์ การรับส่งข้อมูลมัลติมีเดียแบบเรียลไทม์ นั้นต้องการคุณภาพของ QoS ที่สูง ซึ่งมักจะไม่ได้รับการสนับสนุนโดยสถาปัตยกรรมเครือข่าย Mobile ad hoc network ในปัจจุบัน ซึ่งการเปลี่ยนแปลงโครงสร้างและความล้มเหลวในการเชื่อมโยงทำให้เกิดการสูญเสียแพ็คเก็ตอย่างรุนแรงบ่อยครั้งส่งผลไปถึงการลดคุณภาพของสื่อที่ได้รับ อย่างไรก็ตามในเครือข่าย mesh ดังกล่าวมักจะมีแหล่งข้อมูลและโหนดปลายทางอยู่หลายเส้นทาง ความหลากหลายของเส้นทางดังกล่าวได้รับการแสดงให้เห็นถึงประสิทธิภาพในการต่อสู้กับความล้มเหลวและความแออัดในการเชื่อมโยง ซึ่งโปรโตคอล MRTP สามารถทำการส่งข้อมูลแบบ multipath ของข้อมูลมัลติมีเดียแบบเรียลไทม์ได้ การทดลองโปรโตคอล MRTP นี้ใช้การจำลองเครือข่ายเฉพาะกิจในพื้นที่สี่เหลี่ยมจัตุรัส ขั้นแรกแต่ละโหนดจะถูกวางสุ่ม ในพื้นที่โดยจะมีค่าคงที่ทั้งความเร็วและเวลาหยุด โดยเครือข่ายจะประกอบด้วย 16 โหนด ในพื้นที่ 600 ม. X 600 ม. ความเร็วในโหนดเป็น 5 เมตร วินาทีและเวลา / ที่หยุดชั่วคราวเป็น 2 s. เราใช้ IEEE 802.11 โปรโตคอลในชั้น MAC ที่ทำงานในโหมด DCF แบนด์วิดธ์ช่องทางคือ 1 Mbps และมีช่วงการส่งเป็น 250 เมตร

การส่งสัญญาณ MRTP และจำลองส่งสัญญาณ เส้นทางเดียว RTP (5 m/s ความเร็วและความสำคัญเวลาหยุด 2 s) (a) MRTP/MDSR สองกระแสกับ (b) RTP / DSR หนึ่งกระแส

ข้อดีของ MRTP คือ

1. มีความยืดหยุ่นที่มากกว่า RTP หรือ SCTP ตรงที่มีฟังค์ชั่นรองรับการทำงานในชั้น Application

2. ทำงานบนพื้นฐานของ UDP แต่มีตัวควบคุมความแออัดและทำงานร่วมกับ TCP ได้ดี
3. มีการซ่อมแซมแก้ไข ในกรณีเกิด packet loss
4. ใช้ทรัพยากรเส้นทางบนเครือข่ายได้อย่างคุ้มค่าเนื่องจากไม่ได้อิงหรือเน้นการส่งข้อมูลแบบเรียลไทม์ไปในเส้นทางหลักอย่างเดียว แต่เฉลี่ยการส่งไปได้หลายๆเส้นทาง

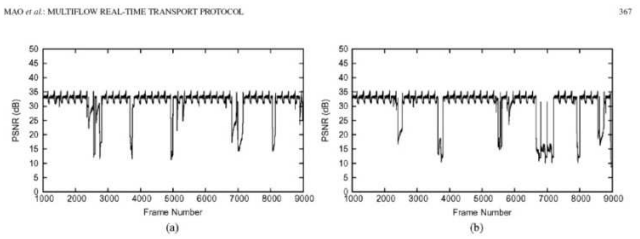
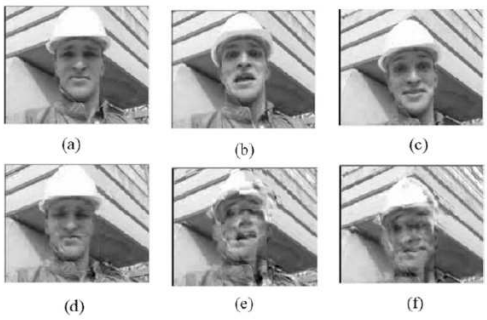


Fig. 13. PSNRs of the decoded frames from the two-flow MRTP and the single-flow RTP simulations (5 m/s nodal speed and 2 x pause time). (a) MRTP/MDSR with two flows and (b) RTP/DSR with one flow.

รูปที่ 11 PSNRs ของเฟรมถอดรหัส



รูปที่ 12 ถอดรหัสเฟรมจากจำลอง MRTP และ RTP

E. Licklider Transmission Protocol (LTP)-Based DTN for Cislunar Communications

สำหรับ [31] เป็นการประเมินผลการทดลองของสถาปัตยกรรม DTN โดยการจำลองช่องทางการสื่อสาร Cislunar ในระดับที่แตกต่างกันทั้งความล่าช้าในการเชื่อมโยงและการสูญหายของข้อมูล ด้วยการทดสอบ BP/LTPCL/UDP/IP stack เปรียบเทียบกับ protocol บนเครือข่าย DTN อีกสองประเภท คือ BP/TCPCL/TCP/IP และBP/UDPCL/UDP/IP การทดสอบนี้จัดทำโดยการดำเนินการถ่ายโอนไฟล์เหมือนจริงผ่านเครื่องคอมพิวเตอร์ เจตนาของการทำงานนี้คือการตรวจสอบประสิทธิภาพของโปรโตคอล LTPCL บนเครือข่าย DTN โดยเฉพาะในสภาพแวดล้อมที่มีความล่าช้าในการเชื่อมโยงระยะยาวและอัตราความผิดพลาดสูง โดยจำลองการส่งด้วย Cislunar จากการประเมินผลการทดลองDTN protocol stack, BP/LTPCL/UDP/IP ในการเปรียบเทียบ BP/TCPCL/TCP/IP และ BP/UDPCL/UDP/IP ผ่านการจำลองช่องทางสื่อสาร cislunar ลักษณะที่แตกต่างกันของระดับความล่าช้าในการเชื่อมโยงและอัตราความผิดพลาดในการส่ง บนพื้นฐานของการวิเคราะห์ทางสถิติในการทดลองได้ผลดังนี้

1. หนึ่งในจุดแข็งของ BP คือความสามารถในการใช้ประโยชน์จาก convergence-layer protocol stacks สำหรับสภาพแวดล้อมการสื่อสารที่แตกต่างกัน (ล่าช้า,BER,ฯลฯ)
2. LTPCL มีความได้เปรียบด้านประสิทธิภาพอย่างมีนัยสำคัญมากกว่า TCPCL สำหรับความล่าช้าในการเชื่อมโยงนานกว่า ms 4000 อัตรา bit error rateจะอยู่ในระดับ 10^{-6} หรือสูงกว่า สำหรับช่องทางที่มีการสูญเสียของข้อมูลมาก อัตรา bit error rate จะประมาณ 10^{-5}, LTPCL มี goodput อย่างมีนัยสำคัญมากกว่า TCPCL จากการศึกษาทุกระดับความล่าช้าในการเชื่อมโยงด้วยข้อได้เปรียบประมาณ 3000 B / S สำหรับความล่าช้าต่อไปอีกกว่า 1500 ms
3. LTPCL มีความได้เปรียบในเรื่องของค่า goodput ที่มากกว่า UDPCL อย่างมีนัยสำคัญประมาณ 2500–3000 B/s สำหรับทุกสภาพแวดล้อมการสื่อสารที่แตกต่างกัน (ล่าช้า, BER, ฯลฯ)
4. แตกต่างจาก TCPCL ที่อัตรา goodput ได้รับผลกระทบอย่างรุนแรงจากการเพิ่มความล่าช้าในการเชื่อมโยงและ / หรือสัญญาณรบกวนที่ความล่าช้าในการเชื่อมโยงและ BER ซึ่งมีเพียงผลกระทบเล็กน้อยต่อประสิทธิภาพการทำงานของ LTPCL

ตารางที่ 6 แสดงการเปรียบเทียบคุณสมบัติระหว่าง TCP และ LTP

Features for Comparison	TCP	LTP
Architectural elements	One durable, unbounded *connection* per pair of ports. "*Window*" is buffer of bytes in transit on connection.	One temporary, bounded *session* per transmission unit. "*Block*" is buffer of bytes in transit within session.
ACK mechanism	ACKs on ranges of bytes in window; SACK optional.	Selective NAKs on ranges of bytes in block.
Connections	Connections are dynamically opened, parameters negotiated.	No connection protocol. Parameters are managed and asserted.
Sites of retransmission	End-to-end. Retransmission sites are co-located with applications.	Point-to-point. Retransmission sites are co-located with routers.
Delivery order	Bytes delivered in-order within connection.	Bytes delivered in-order within session, but sessions may complete out of order.
Timers	Timeout interval computed from RTT history.	Timeout interval computed from known one-way-light-timer and link state schedule.
Flow control	Number of unacknowledged bytes in buffer is limited by each connection's window size.	Number of unacknowledged bytes in all blocks may be limited by max number of sessions.
Congestion control	Control window size for each connection; slow start, AIMD.	No congestion control; bundle protocol may do rate control.

โดยรวมแล้ว BP / LTPCL มีความเหมาะสมมากกว่าBP / TCPCL และ BP / UDPCLจากการทดสอบในระบบ ของ Cislunar โดยให้มี BER และ propagation delay ในระดับสูง

F. Performance Study of eXtended Satellite Transport Protocol over Satellite Networks

Satellite Transport Protocol

The Satellite Transport Protocol (STP) [32] นำเสนอโดย Katz และ Henderson เป็นโปรโตคอลการขนส่งซึ่งมีความเหมาะสมโดยเฉพาะสำหรับข้อจำกัดที่ไม่ซ้ำกันจากสภาพแวดล้อมของเครือข่ายดาวเทียม STP นั้นดีกว่า TCP ในสภาพแวดล้อมที่มีลักษณะ BER สูงอย่างรุนแรงและความไม่สมดุลจากความแตกต่างกันของค่า RTTs ซึ่งเป็นลักษณะโดยปกติของการเชื่อมต่อกับดาวเทียม LEO (Low Earth Orbit)

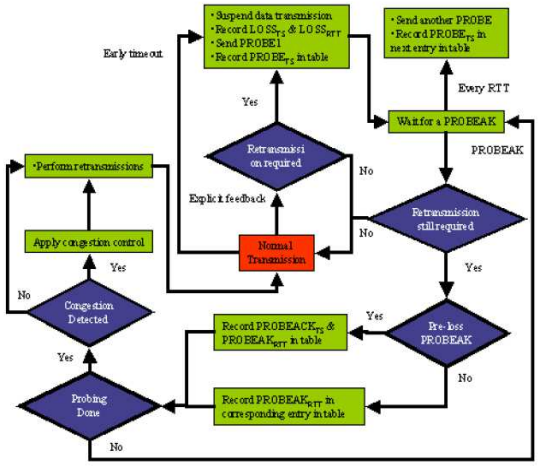
คุณสมบัติหลักของ STP สามารถสรุปได้ดังนี้

1. การแบ่งแยกระหว่างข้อมูลและการควบคุมข้อมูลเพื่อลดค่าใช้จ่ายการควบคุมในส่วนข้อมูลที่มีขนาดเล็ก
2. STP ใช้กลยุทธ์ที่มีประสิทธิภาพเกี่ยวกับส่วนของ acknowledgements คือ ทำงานด้วยการขอซ้ำโดยอัตโนมัติ (ARQ) ซึ่งกลไกนี้ใช้การเลือก negative acknowledgements (NACK) ด้วยการใช้กลไกนี้เพียงแค่การรายงานส่วนที่ขาดหายไปโดยฝั่งผู้รับก็จะมีการ retransmitted ข้อดีคือการจราจรภายในการเชื่อมโยงที่ลดลงเมื่อ loss มีเล็กน้อยและฟื้นตัวอย่างรวดเร็วเมื่อ loss มีมากขึ้น ซึ่งตรงกันข้ามกับ TCP เนื่องจากไม่มีกลไก RTO ใน STP ทำให้เกิดความยืดหยุ่นเพื่อให้เหมาะสมกับค่า RTT
3. กระบวนการซึ่งปรับไปใช้ปริมาณของการควบคุมอัตราที่จำเป็นในเครือข่าย เริ่มตั้งแต่การควบคุมอัตราที่ยังไม่มีการควบคุมอัตราที่ชัดเจน ซึ่งแตกต่างจากTCP ที่จะใช้ คุณสมบัติ self clocking STP จะขึ้นอยู่กับการจับเวลาความล่าช้าในการส่งเพื่อการส่งอย่างสม่ำเสมอโดยประมาณบนจาก RTT ประโยชน์หลักของกลไกการเว้นจังหวะคือการลดลงของความเสี่ยงจากการ large bursts ภายในเครือข่าย
4. มีการ overloading ในส่วนของ Segment type ซึ่งเป็นกลไกเพื่อรองรับการเริ่มต้นเชื่อมต่ออย่างรวดเร็ว

โดยสรุปแล้วสิ่งสำคัญคือแม้ว่า STPมีหลายหลักการพื้นฐานที่พบใน TCP ก็เป็นแต่เพียงการทำงานบางส่วน แต่ไม่ได้เทียบเท่ากับ TCP เลยทีเดียว โชคไม่ดีที่ STP โปรโตคอลสืบทอดการควบคุมความแออัดจากโปรโตคอลในตระกูลเดียวกัน (เช่น TCP, SSCOP) แม้ว่าจะเป็นโปรโตคอลที่สามารถกู้คืนความสูญเสียแบบหลาย round trip คล้ายๆกันได้อย่างมีประสิทธิภาพ แต่กลยุทธ์การกู้คืนความผิดพลาดอาจส่งผลในเชิงลบต่อประสิทธิภาพโดยรวม

eXtended Satellite Transport Protocol

XSTP คือการใช้งานซอฟต์แวร์ของโปรโตคอล STPใน PIX Framework (Protocol Implementation Framework for Linux) โปรโตคอลที่ใช้การหลักเกี่ยวกับข้อผิดพลาดใหม่ด้วยกลยุทธ์การควบคุมที่เรียกว่า XSTP - probing โดยปกติ XSTPโปรโตคอลสามารถทำงานด้านบนของ network protocol (เช่นIP) เป็นบริการ โปรโตคอลที่มีความน่าเชื่อถือในการเชื่อมต่อเชิงไบต์สตรีมมิ่ง ไปยังโปรโตคอลประยุกต์ (เช่น FTP) จากผลการวิจัยพบว่า XSTP มีประสิทธิภาพที่สูงมากในเรื่องของค่า throughput เมื่อเทียบกับโปรโตคอลตระกูล TCP ด้วยเงื่อนไขค่า BER ในระดับสูง นอกจากนี้ยังสังเกตได้ว่าค่าใช้จ่ายการส่งในช่องทางที่ส่งกลับเป็นสิ่งสำคัญในเงื่อนไขเมื่อค่าของ BER อยู่ในระดับสูงและค่าใช้จ่ายการส่งในช่องทางที่ส่งกลับควรจะต้องลดลง



รูปที่ 13 แสดงอัลกอริทึมขั้นพื้นฐานของ XSTP-probing mechanism

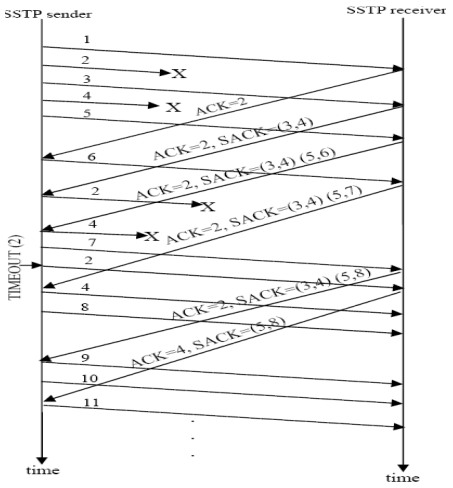
จากผลการวิจัยพบว่า XSTP มีประสิทธิภาพที่สูงมากในเรื่องของค่า throughput เมื่อเทียบกับโปรโตคอลตระกูล TCP ด้วยเงื่อนไขค่า BER ในระดับสูง นอกจากนี้ยังสังเกตได้ว่าค่าใช้จ่ายการส่งในช่องทางที่ส่งกลับเป็นสิ่งสำคัญในเงื่อนไขเมื่อค่าของ BER อยู่ในระดับสูงและค่าใช้จ่ายการส่งในช่องทางที่ส่งกลับควรจะต้องลดลง

G. Performance Evaluation of SSTP- a Transport Protocol for Satellite Channels

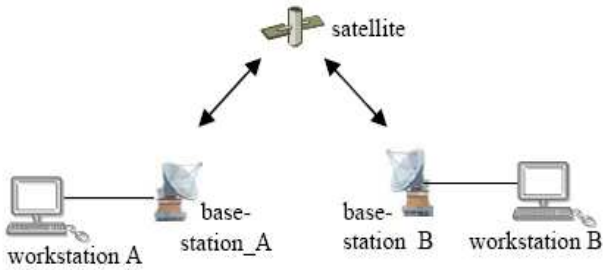
แม้ว่ากระบวนการติดต่อสื่อสารบนอินเทอร์เน็ตในปัจจุบันนั้น ได้มีการใช้ Transmission Control Protocol (TCP) เป็นโปรโตคอลหลักในการติดต่อสื่อสารในเครือข่ายก็ตาม แต่เมื่อมีการใช้อินเทอร์เน็ตผ่านสัญญาณดาวเทียม ทำให้ต้องเผชิญกับปัญหา long propagation delay และ bit error rates(BER) ในระดับสูง ซึ่งส่งผลต่อประสิทธิภาพการทำงานของ TCP อย่างยิ่งจึงได้มีการนำเสนอโปรโตคอลใหม่เพื่อแก้ปัญหาดังกล่าวที่ชื่อว่า SSTP

SSTP – Slidding and Selective Transport Protocol [33]

SSTP ถูกออกแบบมาเพื่อใช้งานในระบบเครือข่ายที่เกี่ยวข้องกับการเชื่อมต่อผ่านดาวเทียม โดยมองว่าการสูญเสียแพ็คเก็ตทั้งหมดเกิดจากข้อผิดพลาดในการส่ง แนวคิดพื้นฐานคือการรักษาการไหลของข้อมูลสูงสุด ในช่องสัญญาณดาวเทียมและการใช้ทรัพยากรการสื่อสารอย่างมีประสิทธิภาพ SSTP จะดำเนินการเกี่ยวกับ timeout , ACK (Acknowledgement) และ SACK (Selective ACK) พร้อมกับการนำเสนอเกี่ยวกับกลไก retransmission ใหม่ที่จะต้องทำงานร่วมกับขั้นตอน timeout และ SACK information เดิมที่ใช้อยู่เพื่อให้การกู้คืนข้อผิดพลาดในการส่งมีประสิทธิภาพที่มากขึ้น



รูปที่ 14 ลักษณะการทำงานของโปรโตคอล SSTP



รูปที่ 15 สถานการณ์จำลอง

ผลการดำเนินงานโดยมีตัวแปร"goodput" (บิต/วินาที) ตามที่กำหนด อัตราส่วนระหว่างปริมาณข้อมูลที่ส่ง (โดยไม่มี headers เช่น 1Mbytes) และระยะเวลาในการถ่ายโอนดังกล่าว ช่วงเวลานี้เริ่มต้นตั้งแต่ช่วงเวลาที่เวิร์กสเตชันส่งข้อมูลส่วนแรกและสิ้นสุดเวลาเมื่อได้รับ ACK ที่เกี่ยวข้องกับข้อมูลสุดท้ายที่ได้รับจากการส่ง มันจะไม่พิจารณาเวลาที่ใช้ในการเปิดและปิดการเชื่อมต่อในการจำลอง ดำเนินการโดยใช้ค่า BER ที่ต่างกันดังนี้ : 0, 10^{-3}, 10^{-5}, 10^{-7} เพื่อแสดงค่า goodput ระหว่างSSTP โปรโตคอล และ TCP โปรโตคอล

ตารางที่ 7 GOODPUT ที่ได้จากการเปรียบเทียบระหว่าง SSTP และ TCP

BER	0	10^{-7}	10^{-5}	10^{-3}
SSTP goodput	895051,41	811247,87	437405,86	**
TCP goodput	677664,04	109334,05	5302,95	**

โดยสรุปแล้วนั้น SSTP ประสบความสำเร็จมากกว่า TCP จากค่า goodput เห็นได้ชัดว่าการเพิ่มขึ้นของ BER ทำให้ลดประสิทธิภาพการทำงานของโปรโตคอลทั้งสองรูปแบบแต่จะมีผลต่อการทำงานของ SSTP น้อยกว่าการทำงานของ TCP การตรวจสอบเบื้องต้นนี้ผลการจำลองแสดงให้เห็นถึงประสิทธิภาพจากการปรับปรุงกลไกการทำงานในชั้นของการขนส่งเมื่อมีการสูญเสียแพ็คเก็ตเนื่องจากการส่งผิดพลาด แต่สิ่งสำคัญที่ควรวิเคราะห์ถึงลักษณะการทำงานของ SSTPในต่อไปก็คือ การทำงานที่มีความแออัดของเครือข่ายและสถานการณ์มีความซับซ้อนมากขึ้นในเครือข่าย

จากการกล่าวถึงโปรโตคอลทั้ง 7 แบบข้างต้นนั้นได้มีการสรุปเป็นตารางเพื่อทำการเปรียบเทียบคุณสมบัติของโปรโตคอลทั้ง 7 แบบได้แก่ SSTP, XSTP, SCTP, DCCP, RTP, MRTP, LTP และได้ทำการเปรียบเทียบกับโปรโตคอลหลักคือ TCP และ UDP ตามตารางด้านล่าง

สรุปคุณสมบัติทั้ง 23 คุณสมบัติ จากการเปรียบเทียบโปรโตคอลทั้งหมด 7 แบบ โปรโตคอลประเภท SCTP มีคุณสมบัติที่สามารถให้บริการได้ มากกว่าโปรโตคอลแบบอื่นและ มีความเหมาะสมที่จะนำมาใช้งานในการรับส่งข้อมูลภายในเครือข่าย

ตารางที่ 8 การเปรียบเทียบคุณสมบัติของโปรโตคอล SSTP,XSTP,SCTP , DCCP , RTP , MRTP , LTP และเปรียบเทียบกับโปรโตคอลหลักคือ TCP และ UDP

คุณสมบัติ	SSTP	XSTP	SCTP	DCCP	RTP	MRTP	LTP	TCP	UDP
Connection-oriented	✔	✔	✔	✘	✔	✔	✘	✔	✘
Message-based transfer	✘	✘	✔	✘	✔	✔	✔	✘	✔
Reliable data transfer	✔	✔	✔	✘	✔	✔	✔	✔	✘
Partially reliable data transfer	✘	✘	✔	✘	✔	✔	✘	✘	✘
Ordered data delivery	✔	✔	✔	✘	✔	✔	✔	✔	✘
Unordered data delivery	✘	✘	✔	✘	✘	✘	✘	✘	✔
Congestion and flow control	✘	✔	✔	✔	✘	✘	✘	✔	✘
Protection from spoofed SYN attacks	✘	✘	✔	✘	✘	✘	✘	✘	✘
Allows half-closed connections	✘	✔	✘	✘	✘	✘	✘	✔	✘
Multistreaming	✘	✘	✔	✘	✔	✔	✘	✘	✘
Multihoming	✘	✘	✔	✘	✘	✔	✘	✘	✘

คุณสมบัติ	SSTP	XSTP	SCTP	DCCP	RTP	MRTP	LTP	TCP	UDP
Dynamic address reconfiguration	✗	✗	✓	✗	✗	✗	✗	✗	✗
Congestion control	✗	✓	✓	✓	✗	✗	✗	✓	✗
Explicit congestion notification	✗	✓	✓	✓	✗	✗	✗	✓	✗
Selective acks	✓	✓	✓	✓	✗	✗	✗	✗	✗
Dynamic congestion control mechanism	✗	✗	✗	✓	✗	✗	✗	✗	✗
Distinguish different kinds of losses	✗	✗	✗	✓	✓	✓	✓	✗	✗
Path maximum transmission unit (PMTU) discovery	✓	✓	✓	✓	✓	✓	✓	✓	✗
Protection against SYN flooding attack	✗	✗	✓	✓	✗	✗	✗	✗	✗
Dynamic ack ratio	✗	✗	✗	✓	✗	✗	✗	✗	✗
Half-connection	✗	✗	✗	✓	✓	✓	✗	✗	✗
Specify data packet	✗	✗	✗	✗	✓	✓	✓	✗	✗
Time-stamping	✗	✗	✗	✗	✓	✓	✓	✗	✗

VI. QUALITY OF SERVICE (QOS)

ในช่วง 2 – 3 ปี ที่ผ่านความต้องการการใช้บริการในอินเตอร์เน็ตมีจำนวนของการเพิ่มขึ้นมากโดยเฉพาะความต้องการในรูปแบบที่เป็น ภาพและเสียง และมีเหตุผลอยู่หลายๆ ประการที่สนับสนุนว่าทำไมถึงมีความต้องการใช้อินเตอร์เน็ตมากขึ้น สามเหตุมาจาก

1. การพัฒนาเครือข่ายไร้สายให้นำมาในโทรศัพท์มือ และ PDA,
2. การเปลี่ยนแปลงของสภาพแวดล้อมในอยู่ในรูปแบบการติดสื่อสารแบบไร้สายทำให้คนทั่วไปสามารถเข้าถึงระบบอินเตอร์เน็ตได้ง่ายขึ้น เช่น ร้านกาแฟ สนามบิน หน่วยงานราชการ
3. โปรแกรมทางด้านมัลติมีเดียมีมากขึ้น ไม่ว่าจะอยู่ในรูปแบบ Mpeg-1,Mpeg-2,Mpeg-4,H.263 หรือแม้กระทั้งสื่อดิจิตอลต่างๆ

Quality of Service (Qos) คือ กระบวนการจัดลำดับความสำคัญของข้อมูลวิดีโอ เพื่อให้ได้มาซึ่งคุณภาพของวิดีโอที่ใช้งานอยู่บนเครือข่าย

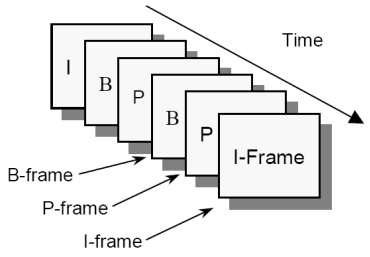
A. BASICS OF VIDEO COMPRESSION [34]

พื้นฐานการบีบอัดไฟล์วิดีโอจะต้องคำนึงความจริงอยู่ 2 ประการคือ 1. การบีบอัดข้อมูลที่ส่งจากต้นทางไปยังปลายทาง (end – to - end) ด้วย ถ้าต้นทางกับไปทางไม่สมดุลกันจะทำให้ไฟล์มัลติมีเดียจะถูกส่งออกไปจากต้นทางไปยังไปทางช้า และอาจจะต้องใช้ Hardware ที่มีราคาแพง 2. ไฟล์วิดีโอที่ผ่านการแปลงสัญญาณแล้วนั้น ซึ่งเป็นเรื่องทั่วไปที่คนส่วนใหญ่ยอมรับได้ เนื่องจากภาพวิดีโอที่ผ่านการบีบอัด จะไม่เหมือนไฟล์ต้นฉบับ

B. วิธีการแปลงสัญญาณภาพวิดีโอ [38]

ในส่วนนี้เราจะกล่าวถึงแนวความคิดเกี่ยวกับ การบีบอัดไฟล์ข้อมูลวิดีโอแบบ Mpeg Mpeg ย่อมาจาก Moving Picture Expert Group ซึ่งกำหนดโดย ISO และ IEC การบีบอัดไฟล์วิดีโอ Mpeg แบ่งออกเป็น 3 ประเภทคือ

1. I-frames (Intra-coded) ในส่วนนี้จะกล่าวถึง ความจริงที่เกี่ยวข้องกับการศูนย์เสียจากการการบีบอัดไฟล์ในเฟรมปัจจุบันโดยที่จะไม่เกี่ยวข้องกับเฟรมอื่นๆ
2. P-frames (Predictive) พิจารณาจากเฟรมที่จะต้องส่งไปข้างหน้า
3. B-frames (Bi-directional): พิจารณาเฟรมที่จะส่งไปข้างหน้าและสามารถย้อนกลับได้



รูปที่ 16 ชนิดของการบีบอัด

C. การคำณวนหาความต้องคุณภาพของไฟล์วิดีโอ [38]

โดยส่วนใหญ่เราตจะคำณวนหาค่าสูงสุดไปจนถึงค่าที่มีการสัญญาณรบกวนมากที่สุด(PSNR) เราจะพิจารณาจากจำนวนคุณภาพของการส่งไฟล์วิดีโอในระบบเครือข่าย

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\|I(i,j) - K(i,j)\|^2$$

$$\text{PSNR} = 20\log_{10}\left(\frac{MAX_i}{\sqrt{MSE}}\right)$$

จากตารางที่ 1 จะเห็นได้ว่าความต้องการ Voive over IP QOS ไฟล์ Streaming Audio มีความต้องการใช้ทรัพย์กรมากกว่า Voip

ตารางที่ 9 QoS Requirements for VoIP [38]

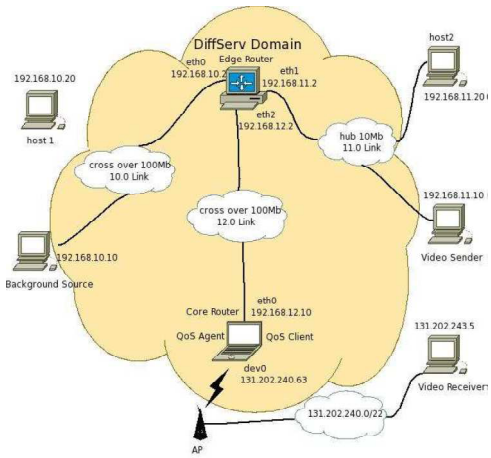
Quality	Delay(ms)	Jitter(ms)	Data Loss
Good	0-150	0-75	<3%
Medium	150-400	0-125	<7%
Poor	>400	0-255	>7%

ในส่วนหัวข้อนี้เราจะกล่าวถึงกระบวนการประเมินผลของ QoS technique เพื่อใช้ในการส่งข้อมูลแบบ real-time steaming video จากรูปเราทำการทดสอบว่า real-time video/audio streams มีลักษณะอย่างไรใน QOS Domain และการ

ตารางที่ 10 QoS Requirements for video over ip [38]

Quality	Delay (ms)	Jitter(ms)	Data Loss
Interactive Video	0-150	<30	<1%
Streaming Video	<400	NA	<5%

D. DIFFERENTIATED SERVICE (DIFFSERV) DOMAIN ARCHITECTURE [34]



รูปที่ 17 DiffServ Testbed Architecture

จัดหาช่องทางในการส่งข้อมูลอย่างไร DIFFSERV)DIFFERENTIATED SERVICE (Technology จะใช้กระบวนการ Qos mechanism, ในระบบเครือข่ายที่แตกต่างกัน DiffServ domain ประกอบไปด้วย Bandwidth broker(BB)

The Effective Solution: QoS Controls

โดยปกติแล้วเราต้องเตรียมระบบ Qos สำหรับ Vocip ไว้เพื่อรองรับปัญหาที่จะเกิดขึ้น เช่น ระบบเครือข่าย และอุปกรณ์ เป็นต้น ในรายงานฉบับนี้เราสามารถแบ่งปัญหาที่พบได้เป็น 2 ประเภทคือ

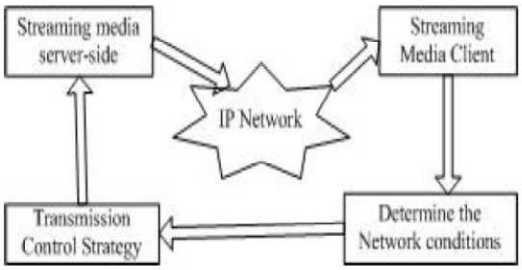
- *Network-levels controls* โดยปกติปัญหาเหล่านั้นจะถูกกำหนดโดยมีเงื่อนไขอยู่ เราเตอร์หรือhop ว่าจะส่งข้อมูลได้เร็วแค่ไหน
- *Auplication-levels controls* เป็นข้อกำหนดพื้นฐานของแต่ละโปรแกรมหรือผู้ใช้

การออกแบบ ระบบ Qos ที่ดีควรจะมีคุณสมบัติดังต่อไปนี้

1. ต้องมีความยืดหยุ่นสามารถรองรับระบบเครือข่ายในปัจจุบันได้
2. ต้องมีกระบวนการจัดการอย่างชาญฉลาดสำหรับการร้องขอที่ไม่ได้อยู่บนพื้นฐานของระบบปัจจุบัน
3. Qos เองต้องมีความสารมารถในการปรับตัวเพื่อให้เข้ากับอุปกรณ์ในการรับสัญญาณภาพทุกประเภท

E. THE PRINCIPLES OF TERMINAL QOS CONTROL MECHANISM [2]

จากรูปที่ 18 กระบวนการการควบคุม QOS ในแต่ละสถานการณ์ทำได้โดยอัลกอริทึมของแต่ละระบบเครือข่ายและกลยุทธ์ในการส่งผ่านข้อมูล กระบวนการที่มันจะทำก็คือ 1) ส่งข้อมูลไปยังเครื่องลูกข่ายในแบบวงกลมแล้วรอรับข้อมูลย้อนกลับมาที่เครื่องลูกข่าย 2) วิเคราะห์ข้อมูลที่ได้กลับมาแล้วนำมาคำนวณหาอัตราการสูญของข้อมูล 3) ตรวจสอบอัตราการสูญข้อมูลในระบบเครือข่ายภายใต้เงื่อนไขที่กำหนด 4) ปรับสถานะอัตราการส่งข้อมูลของระบบเครือข่าย ปรับอัตราเฟรมเรต และรวมทั้งการปรับเปลี่ยนค่า QP ของทั้งสองวิธี ระบบการควบคุมการส่งข้อมูลเป็นเรื่องสำคัญ ในการแก้ปัญหาความแออัดของระบบเครือข่าย และการแออัดของเครือข่ายก็เป็นเหตุให้เกิดการสูญเสียข้อมูลในเครือข่ายเป็นหลัก ค่า Qos ที่ถูกเลือกภายข้อมูลที่สูญเสียเป็นการแสดงสถานะของเครือข่าย

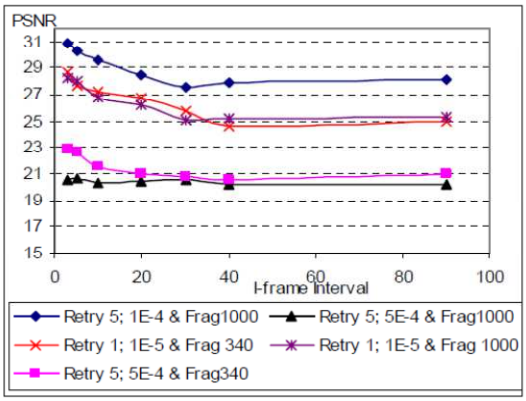


รูปที่ 18 Terminal Qos Control Mechanism

F. Refreshing with I-frames [37]

ความถี่ของการถอดรหัสโดยใช้ I – frame การรีเฟรชมีผลกับคุณภาพของวิดีโอ เป็นที่รู้จักกันอย่างสังหรณ์ใจว่าสูงกว่าค่าความถี่ในวิดีโอที่มีคุณภาพสูง แต่ความถี่ที่ค่าสูงกว่าหมายถึงที่อาจสูงต่อเนื่องจากต่อเกือบจะเป็นสัดส่วนกับขนาดของเฟรมที่สูงขึ้นและค่าความถี่ในอัตราร้อยละที่สูงขึ้นของเฟรมที่มีขนาดใหญ่ ดังนั้นเพื่อที่จะกำหนดของทั้งสองปัจจัยโดยตรวจสอบผลกระทบของการเปลี่ยนแปลงค่าความถี่และขนาดของเฟรม MAC ขนส่งระดับภายใต้เงื่อนไขบางเครือข่ายผ่านการทดสอบการจำลอง

การทดสอบที่เกี่ยวข้องกับการเข้ารหัสที่ 90 เฟรมลำดับหัวหน้า CIF ขนาดการใช้ซอฟต์แวร์อ้างอิง H.264, macroblocks ผลการวางลงใน RTP/UDP/ IP แพ็กเก็ตและจำลองการส่งแพ็กเก็ตเหล่านี้ผ่านช่องทางไร้สายข้อผิดพลาดง่าย เราใช้รายละเอียดพื้นฐานที่มีชุดที่ 28 QP, สำหรับการเข้ารหัสพร้อมกับกรอบการปกปิดข้อผิดพลาดการคัดลอกที่ตัวถอดรหัส วิดีโอที่เข้ารหัสมีอัตราของ 500Kbps รอบ หากสถานการณ์ PHY ที่แตกต่างกันได้รับการพิจารณาที่แตกต่างกันขนาดการกระจายตัวของ MAC (1000 และ 340 bytes), เบอร์)5x10 - 4, 10-4, 10-5 และและนโยบาย (retransmission (1 หรือ 5 ครั้ง(ได้ทดลองใช้สำหรับช่วงเวลาที่ I – frame ของหนึ่ง I – frame ทุก 3, 5, 10, 20, 30, 40, และ 90 เฟรม เพื่อให้แน่ใจว่า ผลลัพธ์ที่เชื่อถือได้ 876 statistically การทดลองซ้ำๆกัน 10 ครั้ง รูปแบบที่แตกต่างกันกับข้อผิดพลาดแบบสุ่มใน WLAN



รูปที่ 19 Effect of I – frame frequency

ระหว่าง I - FRAME ตั้งแต่ที่มีระยะห่างระหว่างความยาวต่อเนื่อง I - FRAME (เช่นเพิ่มเติม P เฟรมระหว่าง I - FRAME) จะเผยแพร่ข้อผิดพลาดและฉากจะไม่สามารถกู้คืนจนถึงเฟรมถัดไป ช่วงเวลาที่เฟรมลดลงอาจไม่จำเป็นต้องส่งผลในการลดลงใน PSNR ตั้งแต่เฟรมมีขนาดใหญ่กว่าพีเฟรม ดังนั้นจึงมีแนวโน้มที่จะมีแพ็คเก็ตน่าจะสูงกว่าการสูญเสีย ที่กำหนดเงื่อนไขช่องอธิบายไว้ข้างต้นรูปที่ 2 แสดงผลการจำลองของเรา เราทราบว่าเกือบทุกการจำลองการยกเว้นสำหรับกรณีที่มีอัตราการสูญเสียสูงสุด (ลองอีกครั้ง =5, BER = 5x10 - 4, และขนาดของการกระจายตัว =1000) เราจะเห็นลดลงคาดว่าใน PSNR กับการเพิ่มขึ้นในช่วงเวลา I - FRAME สำหรับกรณีหลังนี้ไม่มีการเปลี่ยนแปลงที่เห็นได้ชัดใน PSNR สำหรับรูปแบบในช่วงเวลา I - FRAME ดังนั้นจึงจะปรากฏเป็นกรณีที่สำหรับการส่งการด้อยค่าอย่างมีนัยสำคัญ)Bers สูงเช่น(เราอาจจะไม่สามารถที่จะเพิ่มคุณภาพของวิดีโอที่ได้โดยการเพิ่มความถี่ของ I - FRAME ที่ นี่คือการสังเกตที่สำคัญที่จะชี้ให้เห็นว่านอกเหนือจากความน่าจะเป็นสูญเสียตบางอย่างมันไม่เป็นประโยชน์ในการส่งเฟรมมากขึ้น

G. TESTING AND ANALYSIS [34]

ในหัวข้อนี้เรากล่าวถึงการทดสอบและวิเคราะห์ระบบวิดีโอแบบ Mpeg 2 เราต้องการทราบว่า ไฟล์วิดีโอแต่ละประเภทที่ทำการเลือกมาต้องการแบนด์วิดเท่าใด โดยคลิปวิดีโอที่ทำการเลือกมามีอยู่ด้วยกัน 3 ชนิด คือ 1 บทสัมภาษณ์ ที่เป็นฉากพื้นหลังไม่มีการเคลื่อนไหว 2 หนัง เป็นคลิปภาพยนต์ที่มีการเคลื่อนไหวน้อยแต่มีการเปลี่ยนแปลงพื้นหลัง 3 คลิปฟุตบอล เป็นคลิปที่มีการเคลื่อนที่อยู่ตลอดเวลา

1. คลิปบทสัมภาษณ์

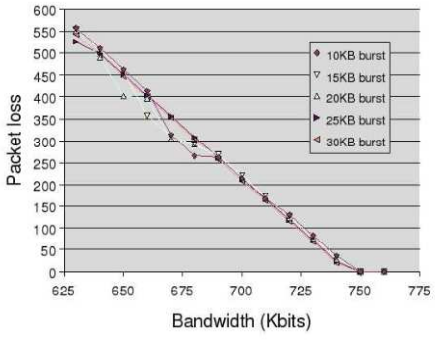
คุณสมบัติ มีดังนี้

- MPEG 1/2 Video decoder,
- Resolution = 320 × 240,
- Frame rate = 25.000 fps,
- File size = 3.92 MB,
- Duration = 52.2s,
- Estimated average rate = 626 kbits/sec.

สรุปผล คลิปที่ 1

เหตุผลที่เลือกคลิปนี้เพราะว่าการสัมภาษณ์ระหว่างบุคคลไม่มีการเปลี่ยนแปลงของฉาก และผลปรากฏว่า มีความต้องการ อัตราการส่งข้อมูล 626 kbits/sec

จากการทดลองเรายังมีสิ่งที่น่าสนใจมากกว่านั้นคือ ขนาดของไฟล์ไม่มีส่วนเกี่ยวของกับแพ็กเก็ตที่มีการสูญเสีย และเรายังสรุปได้ว่าอัตราเฉลี่ยในการส่งแพ็กเก็ตแต่ชนิดจะอยู่ที่ 120 kbits/sec



รูปที่ 20 Interview Clip

2. คลิปหนังสั้น

คุณสมบัติ มีดังนี้

• MPEG 1/2 Video decoder,

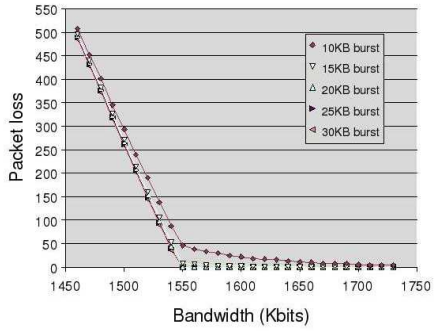
• Resolution = 320 × 240,

• Frame rate = 29.970 fps,

• File size = 10.8 MB,

• Duration = 62.6s,

• Estimated average rate = 1,448 Kbits/sec.



รูปที่ 21 Card Trick Clip

จากกราฟจะพบว่า เมื่อแบนด์วิดอยู่ที่ 1550 kbits/sec มีการสูญสายแพ็คเก็ตทุกๆ 100 kbits/sec เราต้องการค่าเฉลี่ยในการส่งข้อมูลอยู่ที่1480 – 1550 kits/sec

3.คลิปฟุตบอล

คุณสมบัติมีดังนี้

•MPEG 1/2 Video decoder,

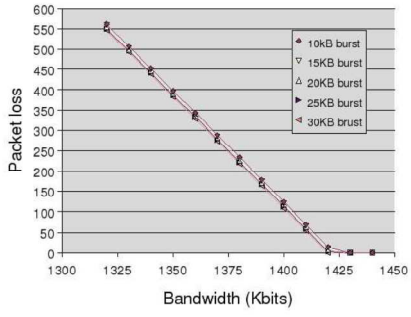
• Resolution = 320 × 240,

• Frame rate = 30.000 fps,

• File size = 9.48 MB,

• Duration = 60.5s,

• Estimated average rate = 1,315 Kbits/sec.



รูปที่ 22 Soccer Clip

เราสรุปได้ว่า ทุกๆ อัตราความเร็ว 115 Kbits/sec ต้องการอัตราการส่งข้อมูลอยู่ที่ 1430 -1315 Kbits/sec

ตารางที่ 11 สรุปผลรูปแบบการบีบอัดข้อมูล

Compression format	*ISO/IEC Issue date*	*Target bandwidth (bits/s)*	*Typical resolution (pixels)*	*Application*
H.261	1988–1990	384k–2M	176 × 144 or 352 × 288	Video-conferencing, low delay
H.263	1992	28.8k–768k	128 × 96 to 720 × 480	Video-conferencing
MPEG-1	11172	400k–1.5M	352 × 288	CD-ROM
MPEG-2, MP@ML	13818 1994	1.5M–15M	720 × 480	Broadcast television, DVD
MPEG-4	14496 1998	28.8k–500k	176 × 144 or 352 × 288	Multimedia

VII. CONCLUSION

ในอนาคตความต้องการของการใช้งานเครือข่ายไร้สายจะมีเพิ่มมากขึ้น โดยเฉพาะบนเครือข่ายโทรศัพท์เคลื่อนที่ เนื่องจากมีความสะดวกสบายและพร้อมทั้งยังมีความรวดเร็ว การสำรวจเทคนิคต่างๆ เพื่อหาความเหมาะสมของการส่งข้อมูลวิดีโอบนเครือข่ายไร้สาย ในมาตรฐานของ H. 264 ซึ่งการส่งข้อมูลมีความสิ้นเปลืองของทรัพยากรเครือข่ายสูง เนื่องจากข้อมูลวิดีโอเป็นข้อมูลที่มีขนาดใหญ่ ในขณะที่การแก้ปัญหาเพื่อหาความเหมาะสมในการส่งข้อมูลวิดีโอบนเครือข่ายไร้สายมีอยู่อย่างต่อเนื่อง เช่น ความปลอดภัยในการส่งในเครือข่ายไร้สาย คุณภาพของข้อมูล โปรโตคอลที่ใช้ในการจัดส่ง การบีบอัดข้อมูลวิดีให้มีขนาดเล็กเพื่อให้ส่งข้อมูลวิดีโอไปบนเครือข่ายไร้สายได้อย่างรวดเร็ว

REFERENCES

[1] H. Schwarz, D. Marpe, and T. Weigand, “Overview of the scalable video coding extension of the H.264/AVC standard,” IEEE Trans. on Circuits and Systems for Video Technology, vol. 17, no. 9, pp. 1103–1120, 2007.

[2] R. Dianat, F. Marvasti and M. Ghanbari, "Reliable Video Transmission Using Codes Close to the Channel Capacity," IEEE Transactions on Circuits and Systems for Video Technology, vol.16, no.12, pp.1550-1556, 2006.

[3] G. O. Young, “Synthetic structure of industrial plastics (Book style with paper title and editor),” in Plastics, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.

[4] P. Ferre, A. Doufexi, J. Chung-How, A.R. Nix, and D.R. Bull, "Robust Video Transmission Over Wireless LANs," IEEE Transactions on Vehicular Technology, vol.57, no.4, pp.2596-2602, 2008.

[5] T. Shida, T. Sato, H. Nakayama, H. Kosaka and K. Sugiyama, "Robust HD Video Stream Transmission for Wireless DTV," IEEE Transactions on Consumer Electronics, vol.53, no.1, pp.96-99, 2007.

[6] Hojin Ha**,** Changhoon Yim and Young Yong Kim, "Packet loss resilience using unequal forward error correction assignment for video transmission over communication networks," South Korea, 2007.

[7] R. Shmueli, O. Hadar, R. Huber, M. Maltz and M. Huber, "Effects of an Encoding Scheme on Perceived Video Quality Transmitted Over Lossy Internet Protocol Networks," IEEE Transactions on Broadcasting, vol.54, no.3, pp.628-640, 2008.

[8] Wu Zhenfeng, Guo Lin and Qin Xuan, "The research on video transmission and distribution system based on soft switch technology," in Proc.of 2nd International Conference on Power Electronics and Intelligent Transportation System (PEITS), 2009, vol.2, pp.342-345.

[9] Tien Anh Le, Hang Nguyen and Hongguang Zhang, "Scalable Video Transmission on Overlay Networks," in Proc.of Second International Conferences on Advances in Multimedia (MMEDIA), 2010, pp.180-184.

[10] Dianat, R.; Marvasti, F.; Ghanbari, M.; , "Reliable Video Transmission Using Codes Close to the Channel Capacity," IEEE Transactions on Circuits and Systems for Video Technology, vol.16, no.12, pp.1550-1556, 2006.

[11] C. Bergeron and C. Lamy-Bergot, "Complaint Selective encryption for H.264/AVC video streams," in Proc.of 7th Workshop on Multimedia Signal Processing, 2005, pp.1-4.

[12] Chunhua Li, Chun Yuan and Yuzhuo Zhong; , "Layered Encryption for Scalable Video Coding," in Proc.of 2nd International Congress on Image and Signal Processing, CISP 2009, pp.1-4.

[13] Potdar, U.; Talele, K.T.; Gandhe, S.T.; , "Perceptual Video Encryption for Multimedia Applications," in Proc.of Second International Conference on Computer Engineering and Applications (ICCEA), 2010, pp.587-589.

[14] Cai Mian, Jia Jia and Yan Lei, "An H.264 Video Encryption Algorithm Based On Entropy Coding," in Proc.of Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP 2007, pp.41-44.

[15] Jianguo Jiang, Shiyi Xing and Meibin Qi, "An Intra Prediction Mode-Based Video Encryption Algorithm in H.264," in Proc.of International Conference on Multimedia Information Networking and Security 2009, MINES 2009, pp.478-482.

[16] Hua-Zhen Yao and Ya-Tao Jing, "The Design of Video-Conference Encryption System Based on H.264," in Proc.of International Conference on Multimedia Technology (ICMT), 2010, pp.1-4, 29-31.

[17] Analysis of Packet-Level Forward Error Correction for Video TransmissionMatteoMazzotti, Enrico Paolini , Marco Chiani, Benjamin Gadat†, Cyril Bergeron†, Roberta FracchiaDEIS/WiLAB, University of Bologna, via Venezia 52, 47521 Cesena (FC), Italy†THALES Communications, 160 boulevard de Valmy, 92704 Colombes Cedex, France

[18] Error Resilient Packet-Switched Video Telephony with Adaptive Rateless Coding and Reference Picture SelectionMuneebDawood, RaoufHamzaoui, Shakeel Ahmad, Marwan Al-Akaidi Faculty of Technology, De Montfort University, Leicester, UK.

[19] Thomas Stockhammer, Miska M. Hannuksela, Thomas Wiegand "H.264/AVC in Wireless Environments" IEEE Transactions on Circuits and Systems for Video Technology 2003

[20] JordiRibas-corbera, Philip A. Chou, Senior Member and Shankar L. Regunathan "A Generalized Hypothetical Reference Decoder for H.264/AVC "IEEE Trans. Circuits Syst. Video Technol 2003

[21] Pei-chun Chen and Tsuhan Chen "Error Concealment Aware Rate Shaping for wireless video transmissionTrista"

[22] Jeong-Yong Choia and Jitae Shin a "cross Layer–Error Control with low overhead ARQ for video, H.264. Transmission of Wireless ANs" School of Information and Communication Engineering, Sungkyunkwan University.

[23] Injong Rhee y. Srinath R. Joshi "Error Recovery for Interactive Video Transmission over the Internet" Department of Computer Science North Carolina State University Raleigh, NC 27695-7534, USA.

[24] Ming-Fong Tsai & Ce-KuenShieh&Chih-HengKe & Der-Jiunn Deng "Sub-packet forward error correction mechanismfor video streaming over wireless networks",Springer Science Business Media, LLC 2009.

[25] Leonardo Badia*,* Nicola Baldo, , Marco Levorato, Michele Zorzi, "A Markov Framework for Error Control Techniques Based on Selective Retransmission in Video Transmission over Wireless Channels"*, IEEE*.

[26] Ming-Fong Tsai2, Naveen Chilamkurti1, and Ce-Kuen Shieh2,**"**Multipath Transmission with Forward Error Correction Mechanism for Delay-sensitive Video Communications",Department of Computer Science and Computer Engineering, La Trobe University, Melbourne, Australia.

[27] Natarajan, P., Baker, F., Amer, P.D., and Leighton, J.T., "SCTP: What, Why, and How," Internet Computing, IEEE , vol.13, no.5, Sept.-Oct. 2009, pp.81-85.

[28] Yuan-Cheng Lai, "DCCP: Transport Protocol with Congestion Control and Unreliability," IEEE Internet Computing, vol.12, no.5, pp.78-83, Sept.-Oct. 2008.

[29] Begen, A.C., Glazebrook, N., and Ver Steeg, W., "Reducing Channel-Change Times with the Real-Time Transport Protocol," Internet Computing, IEEE , vol.13, no.3, pp.40-47, May-June 2009.

[30] Shiwen Mao, Bushmitch, D., Narayanan, S., and Panwar, S.S., "MRTP: a multiflow real-time transport protocol for ad hoc networks," IEEE Transactions on Multimedia,vol.8, no.2, pp. 356- 369, 2006.

[31] Ruhai Wang, Scott C. Burleigh, Paavan Parikh, Che-Jen (Jerry) Lin, Bo Sun, "Licklider Transmission Protocol (LTP)-Based DTN for Cislunar Communications," Networking, IEEE/ACM Transactions on 2010, Volume 19, Issue 2, pp. 359 - 368, 2011.

[32] Burlacu, M.-M. Kohlenberg, J. Zidani, H.; Lorenz, "Performance Study of eXtended Satellite Transport Protocol over Satellite Networks," International Conference on (SPACOMM 2010) , pp. 116 - 121 , 13-19 June 2010.

[33] Canhoto, A.F. Anzaloni, A., "Performance Evaluation of SSTP - a Transport Protocol for Satellite Channels," International Conference on Advanced Information Networking and Applications Workshops 2009, pp. 334 - 337, 26-29 May 2009.

[34] Park, Shihyon, DeDourek and John," Quality of Service (QoS) for Video Transmission," in Proc.of Ubiquitous and Future Networks, 2009, ICUFN 2009, pp. 142 – 147.

[35] Xiaojun Liu, Chunxia Tu and Zhe Wu, "A Research on Terminal QoS Control Mechanism for H.264 Video Stream," Future Computer and Communication, 2009, pp : 69 – 71.

[36] Chun Tung Chou and Jian Zhang, "CROSS-LAYER QOS-OPTIMIZED EDCA ADAPTATION," Image Processing (ICIP), 2010 pp. 2925-2928 .

[37] Fallah, Yaser Pourmohammadi, Koskinen, Darrell, Shahabi, Avideh, Karim, Faizal, Nasiopoulos and Panos, "A Cross Layer Optimization Mechanism to Improve H.264 Video Transmission over WLANs FOR WIRELESS VIDEO STREAMING," Consumer Communications and Networking Conference, Jan. 2007, pp 875 – 879.

[38] Mahasweta Sarkar and Ramesh Goel "An Algorithm to Enhance QoS for Streaming Video over WLANs," World Congress on Engineering and Computer Science 2008, WCECS '08, Advances in Electrical and Electronics Engineering - IAENG Special Edition of the, 22-24 Oct. 2008, pp 76 – 85.