Delay Tolerant And Opportunistic Networking

อริสรา ชัยสิทธิ์, เตชิต ชื่นประทุมทอง, เพ็ญศิริ คงนาค, อนุวัฒน์ ใจดี, สาวิตรี จูมเกตุ, ทวีพงษ์ ทุมพัง, เชิดพงศ์ ตาปราบ,
ณัฐพงษ์ ตุวันโน, นราศักดิ์ ธัญญารักษ์, วิจิตรา ขจร, อาทิตยาพร โรจรัตน์ และ เทวิกา จันทอง
สาขาเทคโนโลยีสารสนเทศ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น

บทคัดย่อ—ความล่าช้าของเครือข่าย (DTN – Delay Tolerant Networks) เป็นชั้นของเครือข่ายที่ขาดการเชื่อมต่อกันอย่างต่อเนื่อง ระหว่างโหนด ครอบคลุมไปถึงการจำกัดของเครือข่ายไร้สาย, การกระจายของโหนด, แหล่งพลังงานที่จำกัด, การรบกวนในระดับสูงหรือการลดคุณภาพของการเชื่อมต่อผ่านช่องทางอื่นๆ ในพื้นที่ของ DTN เครือข่ายจะมีการหยุดเป็นบางครั้งบางคราว การไม่เชื่อมต่อของเครือข่ายเกิดจากระยะเวลาที่ยาวนานในเส้นทางของ DTN ในบทความนี้ จะศึกษาสถานะของการกำหนดเส้นทางโปรโตคอล, การค้นหาเส้นทางการฉวยโอกาส, การ Multicasting, Routing และการรักษาความปลอดภัยใน DTN

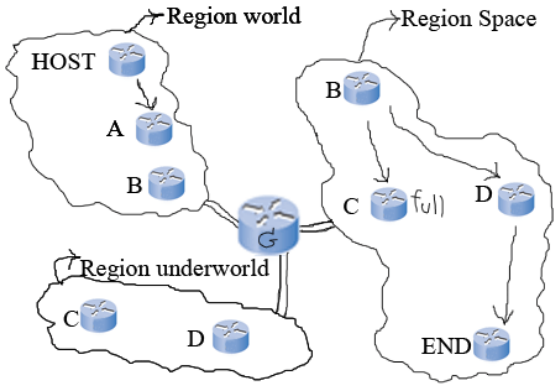
คำหลัก-Routing, Delay Tolerant Network, Opportunistic, Muilicasting, Security of DTN

I.บทนำ

Protocol TCP/IP ในยุคปัจจุบันนี้ ได้รับการยอมรับในการใช้ส่งข้อมูลหากันไปทั่วโลก แต่การรับส่งไฟล์ไม่ได้มีแค่ในโลกนี้เท่านั้น ยังมีการรับส่งไฟล์ข้อมูลบนอวกาศ หรือ รับส่งไฟล์ระหว่างดาวเคราะห์ดวงนึ่ง ไปยังดาวเคราะห์ดวงหนึ่งซึ่งมีระยะทางที่ไกลกว่าการรับส่งไฟล์บนโลกมาก จึงทำให้การรับส่งข้อมูลด้วย Protocol TCP/IP ไม่มีประสิทธิภาพ

อีกตัวอย่างหนึ่งคือ ในสภาวะแวดล้อมที่ย่ำแย่เช่น มีการสู้รบกันเกิดการยิงจรวดมิสซายกันอย่างหนัก อีกทั้งเครื่องบินก็บินรบกันบนท้องฟ้าเป็น พันๆลำ แต่ป้าเอมม่า ต้องการส่ง ข้อมูลภารกิจให้เจมส์บอนทางโทรศัพมือถือแต่ผลปรากฏว่า เจมส์บอนไมสามารถรับข้อมูลภารกิจได้เนื่องจากสภาพแวดล้อมที่ย่ำแย่

จากตัวอย่างดังกล่าวจึงทำให้มีการวิจัยเพื่อแก้ปัญหานี้และได้มีการคิดค้น Protocol Delay Tolerant ขึ้นมาเพื่อแก้ปัญหาดังกล่าว



รูปที่ 1 ภาพรวมการทำงานของ DTN

host จะส่ง Bundle ผ่าน router ผ่านเกตเวย์ ไปยังให้โหนดถัดไปโหนด A เมื่อ โหนด A ได้รับ Bundle แล้ว ก็จะทำการตอบกลับไปยัง host ที่ส่ง bundle มาว่าได้รับbundleแล้ว แล้วโหนด A ก็จะกลายเป็น host แล้ว โหนด A ก็จะทำการส่ง bundle ไปยังโหนด B เมื่อ โหนด B ได้รับ bundle แล้วก็จะทำการตอบกลับไปหา โหนด A ว่าได้รับ bundle แล้ว แล้วโหนด B ก็จะทำการส่ง bundle ไปให้ โหนด C แต่ปรากฏว่า โหนด C เกิดข้อมูลเต็ม โหนด B ก็จะส่ง bundle ไปให้โหนด D แล้วโหนด D ก็จะตอบกลับไปหาโหนด B ว่าได้รับ bundle แล้ว แล้วโหนด D ก็จะกลายเป็นโฮสต์ แล้วโหนด D จะทำการส่งข้อมูลไปให้โหนดปลายทาง แต่ปรากฏว่าโหนดปลายทาง เกิดเหตุขัดข้องไม่สามารถติดต่อกับโหนด D ได้ข้อมูลก็จะถูกพักไว้ที่โหนด D และเมื่อโหนดปลายทางสามารถติดต่อได้แล้ว โหนด D ก็จะทำการส่งข้อมูลไปหาโหนดปลายทาง แล้วโหนดปลายทางก็จะตอบกลับไปหาโหนด D ว่าได้รับ bundle แล้ว ก็จะจบขั้นตอนการทำงาน

bundle คือ เหมือนแพ็กเก็ต ซึ่งจะเก็บ name tuples ของ dtn และ ข้อมูลที่ต้องการส่งไว้ข้างใน name tuples คือ ชื่อที่ใช้อ้างอิงเพื่อค้นหาเส้นทางส่งข้อมูลไปให้โหนดปลายทาง ซึ่งจะประกอบด้วย 2 ส่วน คือ region name และ entity name

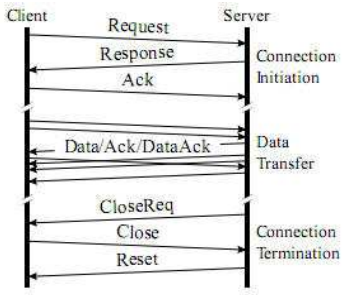
1. *region name* คือ ชื่อของกลุ่มเครือข่าย DTN โดยจะไม่มีชื่อซ้ำกัน ทำหน้าที่ในการเป็นตัวบอกให้ DTN gateway ทราบว่า node ปลายทางอยู่ region ไหน
2. *entityname* คือ ชื่อของโหนดไว้ใช้อ้างอิงเฉพาะใน region

Router คือ ที่ทำการเก็บข้อมูลและส่งต่อข้อมูล

Gateway คือ ที่ทำการเก็บข้อมูล และส่งต่อข้อมูล และค้นหา entity name ปลายทาง และรายงานค่า delay time

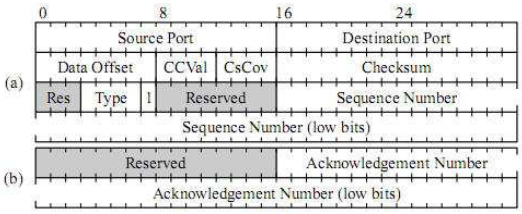
II. โปรโตคอล

A. *DCCP Protocol*



รูปที่ 2 การทำงานของ DCCP Protocol

เริ่มต้นจาก เครื่อง client จะทำการติดต่อไปยังเครื่อง server เมื่อ server ได้รับการติดต่อ server ก็จะทำการติดต่อกลับไปหา client แล้ว client ก็จะส่ง Ack(หมายเลขลำดับการส่งข้อมูลเครื่อง client) กลับมาหา server แล้ว server ก็จะทำการส่ง data(ข้อมูล) + ack + data ack(หมายเลขลำของเครื่อง server) ไปพร้อมกัน โดยรูปแบบการส่งข้อมูลจะเป็นแบบ packet เมื่อเครื่อง client ได้รับข้อมูล ก็จะการส่ง data+ ack + data ack กลับไปหา server เมื่อต้องการยกเลิกการส่งข้อมูล server ก็จะส่ง close request มาที่ client เพื่อร้องขอให้เครื่อง client ปิดการเชื่อมต่อ เมื่อเครื่อง client ได้รับการร้องขอก็จะทำการปิดการเชื่อมต่อแล้วส่ง response ไปหา server แล้วserver ก็จะทำการปิดการเชื่อมต่อ



รูปที่ 3 Header DCCP Protocol

ข้อมูลใน packet จะประกอบไปด้วย header และ data ดังนี้

Source port = port ต้นทาง

Dest port = port ปลายทาง

Data of set = หมายเลข packet

CCval = ข้อมูลheader ที่เข้ารหัส

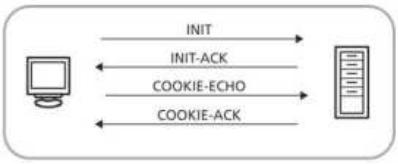
Checksum Coverage = เช็คความถูกต้องของ packet

Checksum: เช็คบิท

Type: ประเภทของรูปแบบคำสั่ง

Sequence Number : หมายเลขลำดับ

B. SCTP Protocol



รูปที่ 4 การทำงานของ SCTP Protocol

การทำงานของ SCTP จะเริ่มจาก เครื่อง client ส่ง init ไปหาเครื่อง server แล้วเครื่อง server จะทำการ ส่ง int , ack กลับไปหาเครื่อง client แล้ว เครื่อง client จะทำการสร้าง cookie แล้วทำการตอบกลับไป server เพื่อให้ server ทราบว่า client ได้สร้าง cookie แล้ว เมื่อ server ได้รับ ข้อมูลแล้ว ก็จะทำการสร้าง cookie เพื่อใช้ติดต่อกับเครื่อง client แล้วทำการตอบกลับไปหา client พร้อมทั้งส่ง ack กลับไปหาเครื่อง client ด้วย ก็จะเป็นการเสร็จขั้นตอนการติดต่อ

รูปที่ 5 การปิดการเชื่อมต่อ SCTP

เครื่อง client ทำการปิดการเชื่อมต่อ แล้วจะส่งข้อมูลไปบอก server ว่าได้ทำการปิดการเชื่อมต่อแล้ว เมื่อ server ได้รับข้อมูล ก็จะทำการ ปิดการเชื่อมต่อ และส่ง ack และ ข้อมูลกลับไปหา client เมื่อ client ได้รับข้อมูลก็จะทำการตอบกลับไปหา server ว่าได้รับข้อมูลการปิดการเชื่อมต่อแล้ว ก็จะเป็นอันเสร็จสิ้นการปิดการเชื่อมต่อ

ข้อมูลของ SCTP จะเป็นการส่งแบบ packet ซึ่ง packet จะประกอบด้วย header และ chunk Header จะประกอบด้วย

Source Port Number	Destination Port Number
Verification Tag	
Checksum	

รูปที่ 6 header SCTP

Source Port Number = หมายเลข port ต้นทาง

Destination Port Number = หมายเลข port ปลายทาง

Verification Tag = การตรวจสอบความถูกต้องของข้อมูลและผู้ส่ง

Checksum = เช็คความถูกต้องของ packet

จึงทำให้สรุปข้อแตกต่างระหว่าง protocol TPC กับ delay tolerant network ได้ว่า SCTP เป็นโปรโตคอลที่มีความน่าเชื่อถือในการรับส่งข้อมูล เนื่องจากข้อมูลที่ถูกส่งไปจะได้รับการยืนยันแน่นอนว่า ข้อมูลนั้น จะถึงโหนดปลายทางครบอย่างแน่นอน แต่ทว่า หากทำการส่งข้อมูลในสภาพแวดล้อมที่ไม่เอื้ออำนวย เช่น ส่งข้อมูลไปดาวอังคารซึ่งมีระยะทางที่ไกล หากเกิดไม่สามารถติดต่อกับโหนดปลายทางได้ ก็ต้องทำให้ โหนดต้นทางทำการส่งข้อมูลซ้ำอีกครั้ง ซึ่งเป็นปัญหาอย่างมากในการรับส่งข้อมูล ด้วย protocol SCTP และการรับ-ส่งข้อมูลจะเป็นการส่งข้อมูลระหว่างต้นทาง-ปลายทาง ซึ่งหากต้นทางและปลายทางมีระยะทางที่ไกลกันมาก จะทำให้การยืนยันการรับส่งข้อมูลใช้เวลานานมากกว่าจะได้รับการตอบกลับ และถ้าใช้การรับส่งข้อมูลด้วย DCCP Protocol ซึ่งการรับส่งข้อมูลจะเป็นแบบไม่มีความน่าเชื่อถือว่าข้อมูลจะส่งครบ จึงไม่เหมาะที่จะนำไปใช้ในการส่งข้อมูลที่ต้องการข้อมูลครบ 100% และทั้ง 2 protocol นี้จะมีขั้นตอนในการติดต่อเริ่มต้นกระบวนการ รับ-สั่ง ข้อมูลกันระหว่างโหนดต้นทางกับปลายทางซึ่งจะทำให้เสียเวลาในการทำการรับ-ส่งข้อมูล

แต่ถ้าหากใช้ protocol delay tolerant ข้อมูลที่ถูกส่งจากโหนดต้นทาง จะถูกส่งต่อมาหาโหนดถัดไปเรื่อยๆ ซึ่งหากเกิดข้อผิดพลาด เช่นไม่สามารถติดต่อกับโหนดปลายทางได้ ข้อมูลที่ถูกส่งออกไปหาโหนดปลายทางก็จะถูกเก็บไว้ที่โหนดกลางทางที่เป็นตัวเชื่อมในการส่งข้อมูลหาโหนดปลายทาง เมื่อทำการ

ติดต่อโหนดปลายทางได้แล้วโหนดที่เก็บข้อมูลที่อยู่กลางทางก็จะทำการส่งข้อมูลให้โหนดปลายทาง ซึ่ง Delay tolerant network จะสามารถทำงานได้ดีกว่าการใช้ SCTP และ DCCP ในการรับส่งข้อมูลระยะไกลหรือในสภาพแวดล้อมที่ไม่เอื้ออำนวย

ตารางที่ 1 เปรียบเทียบข้อแตกต่างระหว่าง DTN กับ SCTP และ DCCP

Feature/Service	DTN	SCTP	DCCP
reliable	√	√	-
Hand chake	-	√	√
Store data	√	-	-
End To End	-	√	√
multicast	√	√	-

C. *ข้อมูลใหม่ที่ส่งผ่านโปรโตคอลใน DTN*

การทนต่อความล่าช้าในเครือข่ายตัวรับรู้แบบไร้สายบนโทรศัพท์มือถือ *(Delay Tolerant Mobile Sensor Networks DTMSN)* ประกอบด้วยโหนด *(nodes)* 2 ชนิด คือ โหนดตัวรับรู้ไร้สายของโทรศัพท์มือถือ *(modile sensor nodes)* และโหนดปลายทาง *(sink node)* ต่างจากเครือข่ายรับรู้ไร้สายแบบเดิม โดย DTMSN มีอักขระที่ไม่ซ้ำกัน เช่น การเคลื่อนที่ของโหนด *(node mobility)* ความห่างระหว่างโหนดในการเชื่อมต่อ *(sparse connectivity between node)* ความล่าช้าที่ไม่แน่นอนของการส่งข้อมูล *(unpredictable delays of data transmission)* แต่ก็ยังมีคุณสมบัติที่เหมือนกันกับเครือข่ายรับรู้ไร้สายแบบเดิม พลังงานที่ไม่เพียงพอของพื้นที่ที่จำกัดที่ใช้จัดเก็บโหนด

ใน DTMSN มีการโต้ตอบอย่างต่อเนื่องระหว่างโหนดในเครือข่าย และการเคลื่อนที่ของโหนด โครงสร้างของเครือข่ายจึงเป็นแบบไดนามิก *(dynamic)* ซึ่งชี้ให้เห็นความท้าทายใหม่สำหรับการออกแบบการ routing protocols ที่มีประสิทธิภาพสูงกว่าเดิม ดังนั้น การส่งข้อมูลโปรโตคอลแบบเดิม จึงไม่สามารถทำให้ประสิทธิภาพดีขึ้นกว่าเดิมได้ กลไกใหม่จึงต้องนำมาปรับให้เข้ากับการใช้งานพิเศษอีกหลายอย่าง

งานวิจัยนี้ เราเสนอในเรื่องของการส่งข้อมูลโปรโตคอลแบบใหม่ ซึ่งสามารถประยุกต์กับ DTMSN ได้ โปรโตคอลนี้กระบวนการส่งข้อมูลจะแบ่งออกเป็น 2 ขั้นตอน คือ ขั้นตอนการรับข้อมูลและขั้นตอนการส่งต่อข้อมูล ขั้นตอนการรับข้อมูลนั้นหน้าที่หลัก คือ เลือกโหนดข้อมูลที่ได้รับ และขั้นตอนการส่งต่อข้อมูลมีหน้าที่หลัก คือ เลือกโหนดที่ดีที่สุดจากโหนดที่ได้รับและทำการส่งต่อ การเลือกโหนดที่จะส่งต่อไปนั้นจะขึ้นอยู่กับ “กลไกการใช้มือ” ผลลัพธ์จากการทดลองแสดงให้เห็นว่า การส่งข้อมูลผ่านโปรโตคอลใหม่นี้จะทำให้อัตราการส่งข้อมูลสูงกว่าเดิม ใช้พลังงานน้อยลงรวมไปถึงลดความล่าช้าของการส่งข้อมูล (data delay)

“การกำหนดเส้นทางความน่าจะเป็นระยะการเชื่อมต่อของเครือข่าย” ผู้เขียนเสนอถึงกลไกการกำหนดเส้นทางในการส่งต่อที่ไม่สม่ำเสมอในการเชื่อมต่อของเครือข่าย ความน่าจะเป็นของกลไกการกำหนดเส้นทาง ความคิดหลักต้องอาศัยข้อมูลประวัติศาสตร์แต่ละโหนด (การคาดการณ์การส่ง) ทุกโหนดมีความน่าจะเป็นที่จะได้พบกับมัน ถ้า 2 โหนดมาเจอกัน การคาดการณ์การส่งระหว่างทั้งสองโหนดจะมีโอกาสเพิ่มขึ้น ถ้า 2 โหนดไม่ได้เจอกันเป็นระยะเวลานาน การคาดการณ์การส่งจะมีโอกาสลดลง กลไกของกลยุทธ์การส่งต่อข้อมูลเป็น 1 โหนดที่จะส่งต่อเฉพาะโหนดที่มีขนาดใหญ่กว่า

ใน [58] ผู้เขียนได้เสนอถึงการ routing protocol ขึ้นอยู่กับบริบท *(based context-aware)* ความคิดหลักคือข้อมูลนั้น ๆ จะส่งต่อในทิศทางไปตามปลายทางถึงต้นทางตามการคาดเดา ตามลำดับการแก้ไขปัญหาข้อมูลผิดพลาด เพราะโหนดมีข้อผิดพลาดอยู่เป็นประจำ ใช้กลไกการเลือกหลายเส้นทาง โหนดนี้อาจจะคัดลอกข้อมูลและส่งข้อมูลไปยังโหนดใกล้เคียง ผลลัพธ์ของวิธี SCAR ในความซ้ำซ้อนของข้อมูลที่มีมาก

ส่วนที่เพิ่มเข้ามา ความคิดหลักของ RED protocol ที่นำเสนอใน [59] และ FAD protocol ใน [60] คือการส่งต่อข้อมูลขึ้นอยู่กับความน่าจะเป็นของการส่งข้อมูล ในความน่าจะเป็นการส่งข้อมูล ของโหนดตัวรับรู้ *(sensor nodes)* สามารถคำนวณโดยขึ้นอยู่กับข้อมูลประวัติของโหนดเหล่านี้ โหนดจะคัดลอกเฉพาะข้อมูลที่มีความน่าจะเป็นการส่งข้อมูลเป็นโหนดที่มีขนาดใหญ่กว่าของตัวเอง

D. *รายละเอียดของโปรโตคอล*

แบ่งกระบวนการส่งข้อมูลเป็น 2 ขั้นตอน คือ ขั้นตอนการรับข้อมูลและขั้นตอนการส่งต่อข้อมูล ในขั้นตอนการรับข้อมูลนั้น เมื่อโหนดมีข้อมูลที่จะส่งไม่ใช่โหนดทั้งหมดที่ใกล้เคียงจะรับข้อมูล เฉพาะโหนดเหล่านั้นซึ่งตอบสนองความต้องการ สามารถรับข้อมูลและต่อจากนั้นก็จะได้รับโหนด ส่วนของขั้นตอนการส่งต่อข้อมูลหลังจากได้รับข้อมูลแล้ว กลไกที่นำมาในขั้นตอนนี้เรียกว่า “กลไกการใช้มือ *(hand up mechanism)*” โหนดการคำนวณเวลาที่ใช้มือและระยะทางถึงโหนดปลายทาง พลังงานที่เหลือมากขึ้นของโหนดรับข้อมูลและใกล้กับโหนดปลายทาง ซึ่งการกลไกการใช้มือใช้เวลาน้อยลงกว่าเดิม โหนดนั้นใช้เวลาน้อยที่สุดโดยสามารถส่งคำร้องข้อ packet ในขั้นตอนแรกในการส่งโหนดและต่อจากนั้นจะส่งข้อมูลออกไปจากโหนด ในขณะที่โหนดอื่น ๆ ละทิ้งข้อมูลโหนดนี้จะมีการรับข้อมูล

1. ขั้นตอนการรับข้อมูล

ในขั้นตอนการรับข้อมูล กลไกนี้จะทำให้โหนดส่งข้อมูลได้ทันทีต่อจากนั้นจะเลือกโหนดที่เหมาะสมที่จะเป็นโหนดเพื่อรับข้อมูล อย่างไรก็ตามในโปรโตคอลก่อนหน้านี้เป็นโหนดที่ส่งข้อมูลจะติดต่อกับโหนดใกล้เคียงเป็นอันดับแรกและต่อจากนั้นบางโหนดใกล้เคียงนี้จะเลือกรับโหนดก่อนที่จะส่งข้อมูลต่อ แต่ในงานวิจัยของเรา โหนดจะส่งข้อมูลได้ทันทีและต่อจากนั้นโหนดใกล้เคียงจะตัดสินถ้าสามารถรับโหนดด้วยตัวเอง ซึ่งเพิ่มประสิทธิภาพอัตราความสำเร็จของกรส่งข้อมูล และลดความเสียหายของข้อมูลเกิดจากการเคลื่อนที่ของโหนด

หน้าที่หลักของขั้นตอนนี้คือการเลือกข้อมูลของการรับโหนด โหนดใกล้เคียงทั้งหมดจะวิเคราะห์ข้อมูลของตนเองในการตัดสิน ถ้าโหนดตรงตามเงื่อนไขทั้งหมดจะได้รับโหนด ซึ่งเฉพาะการรับโหนดสามารถรับข้อมูลที่จะเป็นข้อมูลที่รับโหนด โหนดจะต้องตอบสนองกฎ 3 ข้อดังต่อไปนี้

กฎข้อที่ 1 : ถ้าระยะทางระหว่างโหนดใกล้เคียงกับโหนดปลายทางมีขนาดเล็กกว่าระยะทางระหว่างโหนดที่ส่งข้อมูลกับปลายทาง โหนดใกล้เคียงจะรับข้อมูลจากโหนด

กฎข้อที่ 2 : เมื่อมีข้อมูลเข้ามา โหนดใกล้เคียงจะตรวจสอบพื้นที่ว่างของ buffer และถ้าพื้นที่ว่างของ buffer เพียงพอ มันจะรับข้อมูลจากโหนด

กฎข้อที่ 3 : ในวงจรเวลาการส่งข้อมูล ถ้าโหนดใกล้เคียงจะไม่นำข้อมูลออกจากโซนการสื่อสาร กับโหนดที่ส่งโหนดนี้จะรับข้อมูลจากโหนด

วัตถุประสงค์ของการเลือกรับข้อมูลจากโหนดคือโหนดจะส่งข้อมูลทันทีและโหนดใกล้เคียงจะตรวจสอบถ้ามันตอบสนองกฎพื้นฐาน 3 ข้อ

ตอนนี้เราจะวิเคราะห์ วิธีการตรวจสอบว่าโหนดตรงกับกฎทั้ง 3 ข้อ

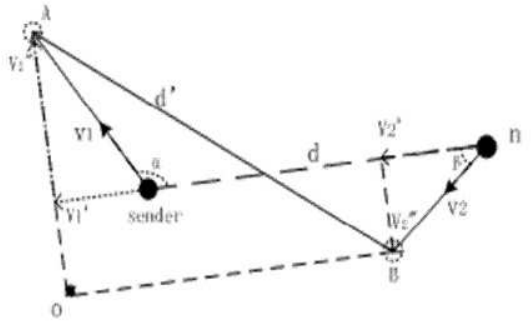
โหนดที่มีการเคลื่อนที่ เพื่อที่จะกำหนดว่าโหนดจะนำข้อมูลออกจากโซนการสื่อสารของข้อมูลภายในวงจรการสื่อสาร ในขอบเขตของการสื่อสาร เราต้องการวิเคราะห์การเคลื่อนที่ที่สัมพันธ์กันระหว่างโหนด และต่อจากนั้นจะตัดสินใจว่า มันสามารถจะกลายเป็นโหนดรับ ความสัมพันธ์การเคลื่อนที่ระหว่าง 2 โหนดคือการวิเคราะห์ ดังรูปที่ 6

ตัวแปรหลักพิจารณาจากความเร็วของโหนดการส่งข้อมูลและรับข้อมูล (V1, V2) คือมุมระหว่างทิศทางการเคลื่อนที่และทิศทางการเชื่อมต่อของทั้ง 2 โหนดคือ (α, β) ขอบเขตของการติดต่อสื่อสารแต่ละโหนดคือ R ระยะทางระหว่างโหนดส่งข้อมูลและโหนดใกล้เคียงคือ d วงจรเวลาการติดต่อสื่อสารคือ T

รูปที่ 6 โหนดที่ทำเครื่องหมายว่า “ผู้ส่ง *(sender)*” คือโหนดส่งข้อมูลซึ่งมีข้อมูลที่จะส่ง โหนดที่ทำเครื่องหมาย “n” คือโหนดใกล้เคียงของโหนดส่งข้อมูล ภายหลังจากระยะเวลาของ T เราต้องการวิเคราะห์ว่าโหนดใกล้เคียงจะนำออกจากโซนการติดต่อสื่อสาร หลังจากเวลา T โหนด “ผู้ส่ง *(sender)*” เคลื่อนย้ายไปที่ตำแหน่ง A และโหนด n เคลื่อนไปที่ตำแหน่ง B “d” คือระยะทางระหว่างทั้ง 2 โหนดในเวลานั้น ๆ ตามที่ได้วิเคราะห์การเคลื่อนที่ที่สัมพันธ์กัน เราทราบได้ดังนี้

ในทิศทางของการขนานด้วยการเชื่อมต่อระหว่าง 2 โหนด ความยาวระหว่าง 2 โหนดคือ |BO|

$$|BO| = d-(V1*\cos \quad a+V2*\cos\ \beta)*T \qquad (1)$$



รูปที่ 6 รูปแบบของความสัมพันธ์การเคลื่อนไหวระหว่างโหนด [22]

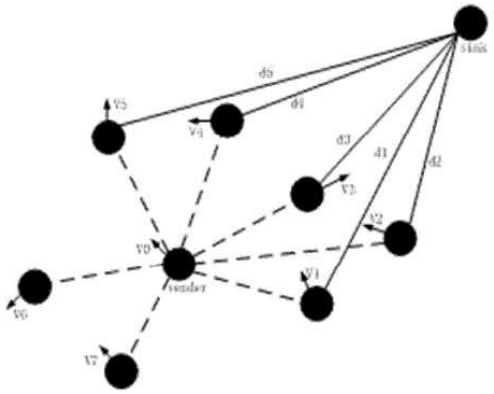
ทิศทางในแนวตั้งของการเชื่อมต่อทั้ง 2 โหนด ความยาวระหว่าง 2 โหนดคือ |AO|

$$|AO| = (V1*\sin a+V2*\sin\ \beta)*T \qquad (2)$$

หลังจากเวลา T โดย (1), (2) เราจะได้ระยะทางระหว่าง 2 โหนดคือ d’

$$D' = \sqrt{|AO|^2 + |BO|^2} \qquad (3)$$

โหนดสามารถตัดสินว่ามันจะรับข้อมูลโหนดได้ โดยเปรียบเทียบ d’ กับขอบเขตของการติดต่อสื่อสาร R ถ้า d’ น้อยกว่า R โหนดจะไม่ย้ายออกจากโซนการติดต่อสื่อสาร ดังนั้นจึงสามารถรับข้อมูลจากโหนดได้ ในทางตรงกันข้ามโหนดจะไม่สามารถรับข้อมูลได้ รูปที่ 7 คือแผนภาพของการเลือกโหนดขึ้นอยู่กับกลไกลในข้างต้น



รูปที่ 7 การเลือกของโหนดรับข้อมูล [22]

2. ขั้นตอนการส่งข้อมูล

หลังจากที่ได้รับข้อมูลโดยโหนดรับข้อมูลทั้งหมดแล้ว ตอนนี้จะเป็นการป้อนข้อมูลเข้าไปสู่ขั้นตอนการส่งต่อข้อมูลในขั้นตอนนี้หน้าที่หลักคือการเลือกข้อมูลเพื่อส่งต่อไปยังโหนด หลังจากการเลือกข้อมูลของโหนดรับข้อมูลแล้ว โหนดรับข้อมูลทั้งหมดจะไม่นำออกจากโซนการติดต่อสื่อสารหลังจากเวลา T ดังนั้น โหนดรับข้อมูลสามารถโต้ตอบกับโหนดส่งข้อมูล ต่อจากนั้นก็จะตัดสินซึ่งจะกลายมาเป็นข้อมูลส่งต่อไปยังโหนด โหนดที่มีคุณสมบัติเพียงพอถึงจะได้รับการส่งต่อ โหนดรับข้อมูลอื่น ๆ ก็จะทำการทิ้งข้อมูลโดยตรง

กลไกสำหรับการแข่งที่จะเป็นโหนดส่งข้อมูลนั้นคือ “กลไกการใช้มือ *(Hadn up Mechanism)*” ความคิดหลักของกลไกนี้คือการคำนวณของโหนดรับข้อมูล “กลไกการใช้มือ *(Hadn up Mechanism)*” โดยการใช้ลักษณะพิเศษของบริบท *(context parameters)* เมื่อหมดเวลาที่ใช้กลไก โหนดรับข้อมูลจะตรวจพบสัญญาณไม่ว่าง *(busy tone)* ในโหนดใกล้เคียงเป็นอันดับแรก ถ้าไม่ มันจะส่งข้อมูล packet ที่ได้รับการร้องขอจากโหนดส่งข้อมูลไปยังการร้องขอการส่งข้อมูลทันที เมื่อโหนดส่งข้อมูลรับคำร้องขอ packet มันจะทำให้ “สัญญาณไม่ว่าง *(busy tone)*” การป้องกันจากโหนดอื่นส่งคำร้องขอ packets สิ่งนี้จะทำให้โหนดส่งคำร้องขอ packet ได้สำเร็จถึงโหนดส่งข้อมูลจะกลายเป็นโหนดรับข้อมูลเป็นอันดับแรก ซึ่งสามารถส่งข้อมูลออกไปและได้รับข้อมูล

เวลาใช้กลไกสามารถคำนวณได้ โดย 3 พารามิเตอร์ พลังงานที่เหลือ (E) และระยะทาง(d) ถึงโหนดปลายทาง วงจรเวลาการติดต่อสื่อสารคือ (T)

$$Time = k*(d/E)*T \quad (4)$$

ใน (4) คือระยาทางระหว่างโหนดและโหนดปลายทาง E คือพลังงานที่ยังเหลืออยู่ของโหนดรับ T คือค่าของระยะเวลาที่กำหนดไว้ k คือปริมาณงานที่ทำได้

เพื่อที่จะบรรลุความสมดุลของการบริโภคพลังงานในหมู่โหนด เราพิจารณาพารามิเตอร์พลังงานใน (4) เพื่อที่จะลดจำนวนของ hops เราพิจารณาระยะทางระหว่างโหนดและโหนดปลายทาง พลังงานที่โหนดเหลืออยู่ และระยะทางที่เล็กกว่าระหว่างโหนดและปลายทาง เราสามารถทำให้ใช้เวลาน้อยกว่าเดิมโดยกลไกการใช้มือ ดังนั้นโหนดสามารถเป็นโหนดแรกที่จะส่งคำร้องขอ packet ถึงโหนดส่งข้อมูล ที่จะเป็นโหนดส่งต่อข้อมูล และต่อจากนั้นมันจะสามารถส่งต่อข้อมูล

โปรโตคอลใหม่เราได้เสนอว่าสามารถตรวจสอบให้แน่ใจถึงอัตราความสำเร็จการส่งข้อมูลที่สูงกว่า เพราะวงจรเวลาการติดต่อสื่อสารทั้งหมด จะไม่มีการรับโหนดและสูญเสียการติดต่อกับโหนดที่ส่ง มันสามารถควบคุมอัตราความสำเร็จการส่งข้อมูล มันสามารถสร้างความสมดุลในการใช้พลังงานระหว่างโหนด นอกจากนี้ เพียงโหนดรับเท่านั้นที่จะสามารถเลือกส่งต่อข้อมูลไปยังโหนดได้ ความซ้ำซ้อนของข้อมูลจะลดลง

III.เร้าติ้ง

ในการกำหนดเส้นทางใน Delay Tolerant Networks (DTN) ไม่สามารถใช้วิธีการกำหนดเส้นทาง แบบที่เครือข่ายปกติใช้ได้ เนื่องจากโหนดที่อยู่บนเส้นทางของการส่งข้อมูลอาจมีการขาดหายไปได้ในบางช่วงเวลา ซึ่งอาจทำให้เกิดการส่งข้อมูลที่ล่าช้าและเกิดการสูญหายของข้อมูลได้มาก จึงมีการกำหนดวิธีการกำหนดเส้นทางและส่งข้อมูลใน DTN โดยทั่วไปการกำหนดเส้นทางนั้นมีสามรูปแบบด้วยกันคือ วิธีการกระจายสำเนาข้อมูล (Flooding Strategy), การส่งต่อข้อมูล (Forward Strategy) และการส่งแบบเข้ารหัส (Coding Strategy)

A. การส่งแบบกระจายสำเนาข้อมูล (Flooding Strategy)

วิธีการกำหนดเส้นทางและส่งข้อมูลแบบ Flooding เป็นวิธีที่ง่ายที่สุดในการส่งข้อมูลใน DTN โดยโหนดต้นทางจะทำการสำเนาข้อมูลไว้หลายๆชุด ก่อนที่จะทำการส่งไปยังทุกๆโหนดที่สามารถติดต่อได้ รวมถึงโหนดปลายทาง หากการติดต่อสื่อสารเกิดปัญหาขึ้น แล้วโหนดปลายทางยังไม่ได้รับข้อมูล โหนดต้นทางและโหนดอื่นๆจะทำการส่งข้อมูลสำเนาที่มีอยู่ ซ้ำไปเรื่อยๆ จนกระทั่งปลายทางได้รับข้อมูลสำเร็จ วิธีการนี้สามารถทำได้ง่าย และมีประสิทธิภาพในการส่งข้อมูลสูง แต่จะสิ้นเปลืองทรัพยากรในเครือข่ายมาก เนื่องจากมีการกระจายข้อมูลอยู่บนทุกๆโหนด งานวิจัยทางด้านอัลกอรึทึม วิธีการส่งข้อมูลแบบกระจายสำเนามีอยู่หลายวิธีด้วยกันดังนี้

Single-Copy Replication routing (SCR) เป็นการส่งข้อมูลที่จะสำเนาข้อมูลขึ้นมาเพียงชุดเดียว แล้วส่งข้อมูลไปยังโหนดที่อยู่ฮอบถัดไป หากข้อมูลสูญหายก็จะสำเนาข้อมูลขึ้นมาใหม่แล้วส่งไปอีกครั้ง ทีละฮอบจนถึงปลายทาง วิธีนี้จะช่วยลดการใช้ทรัพยากรของเครือข่ายลงไปได้ เนื่องจากเมื่อปลายทางได้รับข้อมูลแล้ว จะสามาลบจำนวนสำเนาที่ค้างอยู่ได้อย่างรวดเร็ว

A-SMART เป็นการส่งแบบ Multi-Copy Replication routing(MCR) โดยจะมี Routing table สำหรับจัดกลุ่มของโหนดในแต่ละฮอบ เพื่อกำหนดจำนวนของสำเนาแล้วทำการกระจายข้อมูลไปยังกลุ่มนั้นๆ ทำให้เส้นทางการส่งข้อมูลมีหลายหลากขึ้น

Spray and Focus เป็นการส่งแบบ SCR วิธีหนึ่ง โดยจะแบ่งออกเป็นสองระยะ ระยะแรกจะทำการสำเนาข้อมูลขึ้นมาแล้วส่งไปยังทุกโหนด แล้วจะเข้าสู่ระยะที่สองเพื่อทำการดูว่าโหนดใดที่ยังไม่มีสำเนาจะทำการกำหนดเส้นทางและส่งออกไปให้ โดยทุกโหนดที่มีสำเนาแล้วก็จะทำการคัดลอกแล้วจะกระจายสำเนาไปเรื่อยๆจนกระทั่งข้อมูลถึงปลายทาง

Dynamic Spray and Wait with Quality of Node มีลักษณะคล้าย Spray and Focus จะมีการสร้างสำเนาไว้หลายๆสำเนาในแต่ละโหนด โดยจะมีการกำหนดจำนวนสำเนาตามคุณภาพของโหนด(QoN) ได้แก่จำนวนโหนดเพื่อนบ้านที่สามารถติดต่อได้ และจำนวนกิจกรรมที่เกิดขึ้นของโหนดนั้น

B. การส่งแบบส่งต่อข้อมูล (Forward Strategy)

วิธีการกำหนดเส้นทางแบบนี้จะเป็นการส่งข้อมูล โดยจะใช้วิธีการเก็บข้อมูลของเครื่อข่ายมาไว้ที่โหนดก่อน เพื่อใช้ในการกำหนดเส้นทางการส่งข้อมูลแล้วส่งไปเพียงเส้นทางเดียว ซึ่งข้อมูลต่างๆของแต่ละโหนดจะเรียกว่าเมตริก เช่น ระยะเวลาการทำงานของโหนด, ขนาดของบัพเฟอร์ ลักษณะการเคลื่อนที่ของโหนด จำนวนโหนดเพื่อนบ้านเป็นต้น ซึ่งข้อมูลเมตริกเหล่านี้จะนำมาใช้ในการกำหนดค่าน้ำหนักในแต่ละโหนด แล้วใช้อัลกอรึทึมในการค้นหาเส้นทางเพื่อกำหนดเส้นทางตามโหนดที่มีค่าน้ำหนักที่ดีที่สุด ซึ่งวิธีนี้จะไม่ต้องสำเนาและกระจายข้อมูล และใช้เส้นทางเพียงเส้นทางเดียวซึ่งจะทำให้ประหยัดทรัพยากรลงได้มาก แต่อัตราการส่งของข้อมูล ก็จะลดลงตามไปด้วย อีกทั้งยังอาจเกิดปัญหาการวนลูปของเส้นทางได้ซึ่งจะทำให้เวลาในการส่งข้อมูลเพิ่มมากขึ้น งานวิจัยทางด้านอัลกอรึทึม Forward Strategy มีหลายแบบ โดยจะแตกต่างกันที่เมตริกที่นำมาใช้กำหนดค่าน้ำหนักดังนี้

extended information model จะเป็นการนำความถี่ของโหนดที่ติดต่อกับต้นทางมาใช้ในการกำหนดค่าน้ำหนักแล้วใช้ฟังก์ชั่นถดถอยในการคำนวนหาความถี่ที่จะเกิดขึ้นในอนาคต เพื่อให้ได้ค่าน้ำหนักที่ดีขึ้น ในการกำหนดเส้นทาง

Directional Forward Routing (DFR) จะเก็บข้อมูลเกี่ยวกับ จำนวนสำเนาของข้อมูล อัตราความสำเร็จในการส่งข้อมูลไปยังโหนดนั้น ระยะเวลาการทำงานของโหนด ในกำหนดค่าน้ำหนักเพื่อกำหนดเส้นทาง และจะมีการใช้รอ ACK เพื่อทำการลบสำเนาที่เหลือค้างอยู่ในระบบได้

C. การส่งแบบเข้ารหัส (Coding Strategy)

จะเป็นการส่งข้อมูลโดยจะต้องมีการเข้ารหัสข้อมูลที่ต้นทางก่อน แล้วจะทำการแบ่งข้อมูลออกเป็นหลายๆส่วน แล้วส่งออกไป โดยการส่งอาจเป็นได้ทั้งแบบ เส้นทางเดียว หรือการกระจายสำเนาของแต่ละชิ้นส่วนก็ได้ วิธีการเข้ารหัสเพื่อแบ่งส่วนข้อมูลนี้จะทำให้สามารถกำหนดจำนวนของการใช้ทรัพยากรในเครือข่ายได้จำนวนหนึ่ง งานวิจัยทางด้านการส่งข้อมูลแบบนี้ได้แก่ จากนั้นจะส่งสำเนาของ ชิ้นส่วนของข้อมูลของโหนดนั้นไปเรื่อยๆ จนกว่า

Vehicular Coding-Based Forwarding Protocol (VCF) ซึ่งเป็นการส่งข้อมูลที่ใช้การเข้ารหัสและแบ่งส่วนของข้อมูลก่อน จากนั้นจะทำกำหนดเส้นทางตาม

วิธี Forward Strategy โดยจะกำหนดเส้นทางตามโหนดที่มีอัตราการติดต่อสื่อสารได้สำเร็จ และเมื่อปลายทางได้รับข้อมูลครบทุกส่วนแล้วก็จะสามารถทำการถอดรหัสและนำเอาข้อมูลไปใช้ได้

ตารางที่ 2 เปรียบเทียบการกำหนดเส้นทาง

	Number of Copy	Resource Consumption	Information Usage	Delivery Ratio	Routing Table
SCR	1	Low	Low	Low	No
A SMART	1 per Contract Node	High	Low	High	Yes
Spray and Focus	1 per Contract Node	High	Low	High	No
Dynamic Spray and Wait with Quality of Node	Many	High	Medium	High	No
Extended Information model	None	Low	High	Low	No
DFR	None	Low	High	Low	Yes
VCF	Many	Medium	Very High	Medium	No

IV.การค้นหาเส้นทางใน Opportunistic

การค้นหาเส้นทางการฉวยโอกาสเป็นแนวโน้มของการออกแบบแบบใหม่ของโปรโตคอลการค้นหาเส้นทางบนเครือข่ายไร้สาย ใช้ข้อได้เปรียบที่ดีของธรรมชาติการส่งผ่านทางอากาศของเครือข่ายไร้สาย แหล่งที่มาสามารถใช้เส้นทางที่มีศักยภาพหลายๆเส้นทางในการส่งต่อแพคเกจไปยังปลายทาง ตัวชี้วัดในการค้นหาเส้นทางใช้สำหรับเลือกรายการส่งเป็นสิ่งสำคัญมากสำหรับการออกแบบโครงสร้างการค้นหาเส้นทางการฉวยโอกาส ในด้านตัวชี้วัดการค้นหาเส้นทางจะใช้ตัวชี้วัดการค้นหาเส้นทาง STR (อัตราการส่งประสบความสำเร็จ) เพื่อเลือกรายการที่จะส่ง จะพิจารณาผลงานจากหลายๆการเชื่อมโยง แทนหนึ่งการเชื่อมโยงที่ดีที่สุดเชื่อมโยงข้อมูลที่ใช้ใน ETX นอกจากนี้จะเสนอการค้นหาเส้นทางแบบการค้นหาเส้นทางการฉวยโอกาสที่ยุติธรรม(Fair)กับการเข้ารหัสแบบเส้นตรงโครงสร้าง (FORLC) โดยใช้ STR เป็นตัวชี้วัด

A. Fair and Unfair opportunistic routing Scheme

รูปแบบการค้นหาเส้นทางการฉวยโอกาสมีอยู่ 2 รูปแบบคือการค้นหาเส้นทางการฉวยโอกาสแบบ unfair/fair

1. รูปแบบของการค้นหาเส้นทางการฉวยโอกาสแบบ unfair

มักจะสร้างเป็นชุดการส่งต่อแบบ candidate ซึ่งส่งต่อจำนวนมากจะถูกจัดลำดับความสำคัญในรายการ ลำดับความสำคัญที่สูงขึ้นบ่งชี้ว่าโหนดอยู่ใกล้กับปลายทาง ดังนั้นใน EXOR ทุกๆโหนดที่เลือกจะจัดลำดับความสำคัญสูงสุดในการส่งต่อแพ็กเก็ตที่ได้รับครั้งแรกและโหนดที่มีการจัดลำดับความสำคัญที่ต่ำกว่าจะต้องรอและฟังโหนดที่มีการจัดลำดับความสำคัญสูงกว่า เพื่อให้ทุกโหนดส่งเฉพาะแพ็กเก็ตที่ยังไม่ได้รับการตอบรับโดยโหนดที่มีความสำคัญที่สูงขึ้น

2. รูปแบบของการค้นหาเส้นทางการฉวยโอกาสแบบ fair

ยังสร้างเป็นชุดการส่งต่อแบบ candidate แต่ทุกโหนดในนั้นมีความยุติธรรมโดยไม่มีการจัดลำดับความสำคัญใด ๆ มีเพียงแค่บางบางชุดของโหนดที่ใกล้ชิดกับปลายทางมากกว่าแหล่งที่มา MORE เป็นการค้นหาเส้นทางการฉวยโอกาสแบบ fair การส่งต่อโหนดแบบแพคเกจการเข้ารหัสข้อมูล เมื่อได้รับแพ็คเก็ตที่สิ่งใหม่จากโหนดอื่น ๆและค่าความน่าเชื่อถือในทางที่ดี โหนดไม่จำเป็นจะต้องมีรายการพิเศษเพื่อประสานงานกับเร้าเตอร์อื่น

ในด้านโครงสร้างของ Opportunistic Routing (OR) ประสิทธิภาพของการทำงานของโครงสร้าง OR จะขึ้นอยู่กับค่าบิตเรท ด้วยการเลือกค่าบิตเรทแบบไดนามิก บิตเรท ก่อนอื่นต้องกำหนดตัวชี้วัดใหม่ เวลาที่คาดว่าเส้นทางใดๆจะใช้ในการติดต่อสื่อสารกัน (ExACT) การจับเวลาที่ใช้ในการส่งแพคเกจไปยังปลายทางด้วยอัตราที่กำหนดที่แต่ละฮอปภายใต้ OR จากนั้นจะนำเสนอการเลือกบิตเรทสำหรับวิธีการค้นหาเส้นทางการฉวยโอกาส (BitSOR) ที่ช่วยลด ExACT สำหรับโหนดแต่ละคู่ในเครือข่าย เราจะประเมินประสิทธิภาพการทำงานของ BitSOR โดยใช้ MIT Roofnet ติดตามและแสดงให้เห็นการปรับปรุงศักยภาพที่สำคัญด้วยไดนามิกเรทที่มากกว่า OR ด้วยอัตราคงที่ที่ดีที่สุด

B. การเลือกอัตราบิต

การเลือกอัตราบิตจะมีวิธีการที่เกี่ยวข้องดังนี้

1. ตัวชี้วัดการกำหนดเส้นทาง

ตัวชี้วัดที่ใช้นับฮอปที่ต่ำที่สุดใช้สำหรับการค้นหาเส้นทาง แสดงให้เห็นว่าไม่จำเป็นต้องเพิ่มทรูพุทของการไหลในเครือข่ายไร้สาย จำนวนคาดหวังของการส่งผ่าน(ETX) ประมาณจำนวนของการส่งที่จำเป็นในการส่งแพคเกจ โดยการวัดอัตราการสูญเสียของแพคเกจที่ถูกส่งผ่านอากาศระหว่างคู่ของโหนดเพื่อนบ้าน (ข้างเคียงกัน) อัตราการเชื่อมโยงต่ำกับ ETX ที่มีขนาดเล็กอาจจะช้ากว่าอัตราการเชื่อมโยงสูงกับ ETX ที่มีขนาดใหญ่ เวลาที่คาดหวังที่ใช้ในการส่ง(ETT) มีข้อจำกัดด้านที่อยู่ของ ETX โดยบัญชีสำหรับ bit-rate ETX และETT สมมุติให้แพคเกจเดินทางไปตามเส้นทางเดียวจากแหล่งกำเนิดไปยังปลายทาง คำกล่าวนี้ไม่เป็นจริงสำหรับการค้นหาเส้นทางการฉวยโอกาส แพคเกจอาจจะเดินทางไปตามเส้นทางใดเส้นทางหนึ่งที่มีศักยภาพมากๆที่ช่วยในการส่งต่อ

นำเสนอตัวชี้วัดใหม่ Expected Anypath Transmissions (EAX) จะสะท้อนให้เห็นถึงจำนวนของการส่งที่จำเป็นในการส่งมอบแพคเกจจากโหนดไปยังปลายทางภายใต้ OR

2. การค้นหาเส้นทางการฉวยโอกาส

เครือข่ายไร้สายแบบมัลติฮอปมักจะใช้เทคนิคการค้นหาเส้นทางที่คล้ายกับในเครือข่ายแบบมีสาย Extremely opportunistic routing (ExOR) เป็นหนึ่งในโครงสร้างการค้นหาเส้นทางสำหรับในแต่ละปลายทาง

3. การเลือกอัตราบิต

เดิมขั้นตอนวิธีการเลือกอัตราบิตถูกสร้างขึ้นสำหรับ WaveLAN - II 802.11 เป็นบัตรที่เรียกว่า Auto Rate Fallback (ARF) Adaptive Auto Rate Fallback (AARF) เป็นส่วนขยายของ ARF ที่มีพารามิเตอร์เพิ่มขึ้นเป็นสองเท่าทุกๆเวลาขั้นตอนวิธีการพยายามจะเพิ่ม bit-rate และหลังจากแพคเกจล้มเหลว จะเป็นประโยชน์เมื่อแพคเกจที่ล้มเหลวใช้เวลาส่งเป็นจำนวนมาก

ไดรฟ์เวอร์ของอุปกรณ์ MadWifiสำหรับบัตร Atheros ใช้ขั้นตอนวิธีการ Onoe ที่มีความไวต่อความล้มเหลวของแต่ละแพคเกจน้อยมากกว่าขั้นตอนวิธีการแบบ ARF และโดยทั่วไปจะพยายามที่จะหาอัตราบิตสูงสุดที่มีเปอร์เซนต์ของอัตราการสูญเสียน้อยกว่า 50%

C. การเพิ่มประสิทธิภาพในการป้องกันการเข้าถึงสถานที่ตั้งของแหล่งที่มา

หลักการของการค้นหาเส้นทางและการป้องกันความเป็นส่วนตัว

ในส่วนนี้ เราจะอธิบายหลักการพื้นฐานของรูปแบบการค้นหาเส้นทาง phantom และนำเสนอโครงสร้างแบบ opportunistic แล้วเปรียบเทียบในแง่ของความเป็นส่วนตัวของแหล่งที่มาสถานที่

1. Phantom routing principles

โปรโตคอลการค้นหาเส้นทาง phantom มี 2 ขั้นตอนคือ

- random walk สำหรับนับจำนวน hop และการ Flooding/ใช้หนึ่งเส้นทางในการส่งต่อไปยังปลายทางในช่วง random walk เมื่อไหร่ที่แหล่งที่มามีการส่งแพคเกจ จะมีการส่งแพคเกจไปแบบสุ่ม โหนดที่รับแพคเกจหลังจากช่วง random walk จะกลายเป็นแหล่งที่มาใหม่เรียกว่า phantom โหนดจะส่งข้อความไปยังปลายทางผ่าน flooding/ใช้หนึ่งเส้นทางในการส่งต่อไปยังปลายทาง

2. Opportunistic Routing Principles

- ในช่วงที่ผ่านมา จำนวนโปรโตคอลที่ได้รับการพัฒนาเพื่อปรับปรุงประสิทธิภาพในเครือข่ายเฉพาะกิจ วิธีการหนึ่งที่มีแนวโน้มเรียกว่าเป็นเส้นทางการฉวยโอกาส ที่กลุ่มของโหนดที่เป็นแคนดิเดทให้บริการการถ่ายทอด และระหว่างหนึ่งโหนดก็จะมีการถ่ายทอดแพคเกจ การถ่ายทอดโหนดจะตัดสินใจโอกาสตามเงื่อนไขแบบไดนามิก เช่น การถูกรบกวนของสถานะช่องสัญญาณและความแออัดของช่องสัญญาณ หลักการของการค้นหาเส้นทางการฉวยโอกาสยังได้พัฒนาเครือข่าย Opportunistic mesh และแนวคิดเครือข่ายทางปัญญาซึ่งต่อไปจะใช้ประโยชน์จากความคล่องตัวของช่วงคลื่นนอกเหนือจากพื้นฐานของการค้นหาเส้นทางการฉวยโอกาส

โปรโตคอลที่เกี่ยวข้องกับการค้นหาเส้นทางยังสามารถให้ความเป็นส่วนตัวกับสถานที่ตั้งของแหล่งที่มา มีการเพิ่มประสิทธิภาพความเป็นส่วนตัวให้กับสถานที่ตั้งของแหล่งที่มาในเครือข่ายไร้สาย จึงได้นำเสนอการใช้งานรูปแบบการค้นหาเส้นทางการฉวยโอกาส จากการสำรวจงานวิจัยสามารถแบ่งได้ 2 แบบ คือ แบบขั้นตอนการเดินสุ่มและแบบ flooding / การค้นหาเส้นทางแบบ single path และใช้ตัวชี้วัด LAOR โดยใช้แบบจำลอง NS-2 ในการเปรียบเทียบ การป้องกันการเข้าถึงสถานที่ตั้งของแหล่งที่มาในแบบที่มีตัวชี้วัด LAOR สามารถป้องกันได้ดีกว่าแบบที่ใช้ตัวชี้วัด Phan-tom routing protocol โดยลดค่า overhead และการส่งซ้ำของโหนด

การใช้ตัวชี้วัด LAOR ยังช่วยลดการติดตามของโหนดที่เป็นศัตรูที่จะติดตามเพื่อทำลายไปยังสถานที่ตั้งของแหล่งที่มาซึ่งเป็นแหล่งข้อมูลหลักในระบบ ฝ่ายตรงข้ามจะถือว่ามีลักษณะดังต่อไปนี้ :

- ฝ่ายตรงข้ามรู้ว่าสถานที่ตั้งของปลายทางและสามารถกำหนดตำแหน่งของผู้ส่งเซ็นเซอร์จากตัวอย่างของแพคเกจที่มันได้ยิน
- ฝ่ายตรงข้ามสามารถย้ายจากเซ็นเซอร์หนึ่งไปยังอีกเซ็นเซอร์หนึ่งและมีจำนวนไม่จำกัดของการใช้พลังงาน
- ฝ่ายตรงข้ามจะไม่รบกวนการทำงานที่เหมาะสมของเครือข่ายต่อไป

จะอธิบายถึงสองหลักการของการค้นหาเส้นทางที่แตกต่างกันและปกป้องความเป็นส่วนตัวที่สอดคล้องกัน

D. การเข้ารหัสข้อมูล

ประสิทธิภาพในการถ่ายทอดช่องสัญญาณแบบไร้สายของเครือข่ายการค้นหาเส้นทางการฉวยโอกาสขึ้นอยู่กับการเข้ารหัสเครือข่ายเชิงเส้นแบบสุ่มและการเข้ารหัสเชิงเส้นตามกลไกของเส้นทางการฉวยโอกาส จากการสำรวจงานวิจัยพบว่าการเปรียบเทียบระหว่างการเข้ารหัสทั้งสอง วิธีการเข้ารหัสเชิงเส้นตามกลไกของเส้นทางการฉวยโอกาสสามารถช่วยเพิ่มประสิทธิภาพของการค้นหาเส้นทางการฉวยโอกาสได้ดีกว่าการเข้ารหัสเครือข่ายแบบสุ่มโดยตัวชี้วัด OR-PLC ในการเปรียบเทียบ การเข้ารหัสแบบนี้ทำให้ค่า Throughput สูงขึ้น ค่า ETX เวลาที่คาดหวังในการส่งน้อยลงและoverhead ในระบบลดลง

รายละเอียดการทำงานของProtocol

1. Original Node: ประการแรกที่โหนดเดิมมีการแบ่งข้อมูลลงในบล็อกข้อมูลจำนวนมาก รวมทั้งข้อมูลในแพคเกจ K บล็อกข้อมูลที่แตกต่างกันสามารถมีจำนวนที่แตกต่างกันของข้อมูลแพคเกจเพราะความยาวที่แตกต่างกันของข้อมูลเดิม โหนดเดิมมีการสร้างชุดของการสุ่มตัวเลขที่เรียกว่า การเข้ารหัสเวกเตอร์และจำนวนตัวเลขเหมือนกันกับจำนวนของบล็อกข้อมูล ใช้การเข้ารหัสเวกเตอร์และข้อมูลแพคเกจในบล็อกข้อมูล มันสร้างการเข้ารหัสแพคเกจใหม่ผ่านการรวมกันแบบเชิงเส้นและเพิ่มแพคเกจเฮดเดอร์ไปยังบอร์ดคลาส สร้างการเข้ารหัสแพคเกจใหม่และการบอร์ดคลาสด้านนอกจนกว่าจะได้รับ ACK ของข้อมูลไปยังบล็อกขอมูลปัจจุบันจากโหนดเป้าหมาย จากนั้นโหนดเดิมจะเริ่มการส่งไปยังบล็อกข้อมูลถัดไป

2. ตรวจสอบข้อมูลทั้งหมดที่ส่งได้ตลอดเวลา เมื่อโหนดได้รับข้อมูลแพคเกจ มันจะตรวจสอบไปว่าจะเป็นในเซตของการส่งข้อมูลของโหนดหรือไม่ ถ้าไม่อยู่ในเซตของโหนดมันจะทิ้งข้อมูลแพคเกจที่ได้รับ การตัดสินว่าจะเป็นการเข้ารหัสเวกเตอร์ของข้อมูลแพคเกจปัจจุบันมีความสัมพันธ์กับการเข้ารหัสเวกเตอร์ของข้อมูลแพคเกจที่ได้รับก่อนหน้านี้ โหนดทิ้งข้อมูลแพคเกจที่มีความสัมพันธ์เชิงเส้นและเก็บข้อมูลแพคเกจแบบเชิงเส้นอย่างอิสระในการแคชข้อมูล

3. Target Node: เมื่อโหนดเป้าหมายได้รับข้อมูลแพคเกจตอนแรกจะตรวจสอบความสัมพันธ์กับข้อมูลแพคเกจที่ได้รับก่อน ถ้าเป็นความสัมพันธ์เชิงเส้นของโหนดเป้าหมายมันจะทิ้งหรือมิฉะนั้นจะจัดเก็บข้อมูลแพคเกจลงในแคช เมื่อโหนดถอดรหัสบล็อกข้อมูลทั้งหมดแล้วส่งข้อความ ACK รวมถึงจำนวนของบล็อกข้อมูลไปยังโหนดเดิมผ่านเส้นทางที่แย่ที่สุดในโปรโตคอล ถ้าโหนดกลางได้รับข้อความ ACK มันจะหยุดส่งข้อมูลแพคเกจที่สร้างขึ้นจากบล็อกในปัจจุบันและล้างแคชออก หลังจากได้รับข้อความ ACK โหนดเดิมจะหยุดการส่งข้อมูลแพคเกจที่สร้างขึ้นจากบล็อกในปัจจุบันและเตรียมความพร้อมในการส่งบล็อกข้อมูลถัดไป

ตารางที่ 3 ข้อดี-ข้อเสียของการค้นหาเส้นทางการฉวยโอกาสแต่ละแบบ

Opportunistic Routing	ข้อดี	ข้อเสีย
Opportunistic routing using location		
Location-Aided Opportunistic Routing for Mobile Ad Hoc Networks	-LAOR ช่วยลดการใช้ทรัพยากรและการส่งซ้ำกันอย่างไม่มีเหตุผลในการเลือกการส่งต่อโหนด -ป้องกันการสูญเสียแพคเกจ -LAOR มีความยืดหยุ่นมากกว่าสำหรับการเคลื่อนที่ของโหนด	-ถ้าออกแบบเส้นทางโปรโตคอลไม่ดีจะมีผลต่อความน่าเชื่อของการขนส่ง
Opportunistic Routing for Enhanced Source-Location Privacy in Wireless Sensor Networks	-เพิ่มประสิทธิภาพความเป็นส่วนตัวให้กับสถานที่ตั้งของแหล่งที่มา -ยากสำหรับฝ่ายตรงข้ามที่จะ backtrack ไปยังที่มาของข้อมูลเซ็นเซอร์ -มีความหลากหลายของแอพพลิเคชั่นสำหรับการเก็บรวบรวมข้อมูล -ใช้งานการดักฟังเพื่อวิเคราะห์และหาผู้ป่วยที่มีความเสี่ยงจะเป็นโรคหัวใจ	-การแพร่กระจายผ่านอากาศของข้อความที่ปลอมแปลงขึ้นสิ้นเปลืองจำนวนที่สำคัญของพลังงานที่มีจำกัด -เพิ่มจำนวนของการชนกันและทำให้อัตราการส่งแพคเกจลดลง -ไม่เหมาะอย่างยิ่งสำหรับเครือข่ายเซ็นเซอร์ไร้สายขนาดใหญ่
Opportunistic Routing using bit		
On Bit-Rate Selection for Opportunistic Routing	-การเลือกอัตราการดำเนินงานแบบไดนามิกดีกว่าแบบ OR ด้วยอัตราคงที่ที่ดีที่สุด -ที่ช่วยลด ExACT สำหรับโหนดแต่ละคู่ในเครือข่าย -สามารถเพิ่มประสิทธิภาพการปรับปรุงศักยภาพที่สำคัญด้วยไดนามิกบิตเรทที่มากกว่าตัวชี้วัดแบบเดิม	-ไม่เหมาะสำหรับการส่งผ่านอากาศไปยังผู้รับหลายๆตัวภายใต้ OR
Opportunistic routing transmission coordination using bit map	-ช่วยลดการสื่อสารและการคำนวณ overhead -ลดจำนวนรวมของการส่งแพคเกจเพื่อให้เป็นการปรับปรุงปริมาณของข้อมูลที่ขนถ่าย -สามารถปรับปรุงประสิทธิภาพปริมาณของข้อมูลที่ขนถ่ายที่ได้รับแบบ end-to-end	-การส่งอาจถูกรบกวนเนื่องจากการส่งผ่านอากาศในลักษณะของสื่อไร้สาย -ต้องมีการประสานงานร่วมกันกับโหนดอื่นๆถึงจะสามารถส่งต่อโหนดได้
Opportunistic Routing using coding		
An Opportunistic Routing Protocol Based on Random Linear Network Coding in Wireless Sensor Networks	-สามารถเอาชนะข้อบกพร่องของความไม่แน่นอนของคุณภาพช่องสัญญาณแบบไร้สายและการเชื่อมโยงสัญญาณที่ไม่น่าเชื่อถือ -ปรับปรุงประสิทธิภาพของthroughput และความล่าช้าแบบ end-to-end -เพิ่มประสิทธิภาพช่องสัญญาณของเครือข่าย -ช่วยลดต้นทุนของพลังงานในเครือข่ายและทรัพยากร -ประสิทธิภาพของเวลาความล่าช้าในการส่งข้อมูลลดลง	-คุณภาพของห่วงโซ่โดยทั่วไปอยู่ในระดับต่ำเนื่องจาก สภาพแวดล้อมทางภูมิศาสตร์ เป็นผลในการลดความน่าเชื่อถือของเครือข่ายและthroughput
Priority Linear Coding Based Opportunistic Routing for Video Streaming in Ad Hoc Networks	-สามารถลดปัญหาการแพร่กระจายข้อมูลที่ผิดพลาด -เพื่อเพิ่มคุณภาพของวิดีโอในการรับข้อมูล -ลดความล่าช้าโดยความก้าวหน้าของการเข้ารหัสและถอดรหัส -สามารถรักษาคุณภาพของวิดีโอที่มี overhead ต่ำ -เวลาสำหรับแหล่งที่มาและปลายทางที่จะรอข้อมูลที่เพียงพอจะลดลงอย่างมาก -เป็นระบบแรกที่ใช้เส้นทางการฉวยโอกาสสำหรับแอพพลิเคชั่นวิดีโอแบบ real-time - OR-PLC ช่วยลดการแสดงผลล่าช้าไปประมาณ 30%	-มีข้อจำกัดแบนด์วิดธ์ของเครือข่าย -ความสามารถในการกู้คืนส่วนย่อยบางส่วนที่สำคัญของข้อมูลเดิมที่มีลำดับความสำคัญสูงขึ้น

ตารางที่ 4 เปรียบเทียบการค้นหาเส้นทางการฉวยโอกาส

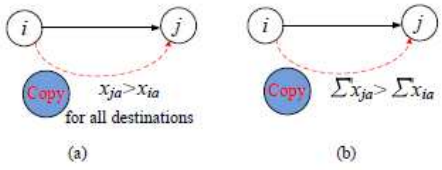
Opportunistic Routing	ตัวชี้วัด	Through put	bandwidth	ETX	overhead	ส่งซ้ำ	User	การเข้ารหัสแพคเกจ
Opportunistic routing using location								
Opportunistic Routing for Enhanced Source-Location Privacy in Wireless Sensor Networks	Phan-tom routing protocol	ไม่เพิ่ม	มีผล	น้อยลง	เพิ่มขึ้น	เพิ่มขึ้น	Single, Multi	ไม่มีการเข้ารหัส
Location-Aided Opportunistic Routing for Mobile Ad Hoc Networks	LAOR, แบบจำลอง NS-2	ไม่เพิ่ม	มีผล	มากขึ้น	ลดลง	ลดลง	Single	มีการเข้ารหัส
Opportunistic Routing using bit								
On Bit-Rate Selection for Opportunistic Routing	BitSOR, ExACT	ไม่เพิ่ม	มีผล	น้อยลง	ไม่ลดลง	ลดลง	Single	ไม่มีการเข้ารหัส
Opportunistic routing transmission coordination using bit map	TCM	สูงขึ้น	มีผล	มากขึ้น	ลดลง	ลดลง	Single	ไม่มีการเข้ารหัส
Opportunistic Routing using coding								
An Opportunistic Routing Protocol Based on Random Linear Network Coding in Wireless Sensor Networks	random linear coding	สูงขึ้น	มีผล	น้อยลง	ลดลง	ลดลง	Multi	มีการเข้ารหัส
Priority Linear Coding Based Opportunistic Routing for Video Streaming in Ad Hoc Networks	OR-PLC	สูงขึ้น	มีผล	น้อยลง	ลดลง	ลดลง	Single, Multi	มีการเข้ารหัส

V.Multicasting

Delay Tolerant Network หรือ DTN คือคือข่ายที่ทนต่อความล่าช้า โดยทั่วไปมักจะนำไปใช้กับการสื่อสารประเภทการสื่อสารแบบไร้สาย อาทิเช่น เครือข่ายบนโทรศัพท์มือถือ การสื่อสารบนอวกาศ การสื่อสารในสนามรบของทางทหาร ซึ่งเกิดการสูญเสียของสัญญาณในการจัดส่งข้อมูลหรือแพ็กเก็ต ซึ่งก่อให้เกิดปัญหาในการจัดส่งคือ ข้อมูลไม่สามารถส่งไปยังปลายทางได้อย่างสมบูรณ์ อังเนื่องมาจากการสูญหายของข้อมูลในระหว่างการจัดส่ง หรือความล่าช้าในการจัดส่งข้อความ ซึ่งโดยทั่วไป DTN จะมีลักษณะการเชื่อมต่อแบบ end-to-end คือการส่งข้อมูลแบบโหนดต่อโหนด จากเครื่องต้นทางหนึ่ง ไปยังปลายทางเพียงจุดเดียว จึงได้มีการนำเอาเทคโนโลยีการ multicast มาใช้ในการส่งข้อมูลเพื่อให้เกิดประสิทธิภาพ และประหยัดทั้งด้านทรัพยากรและค่าใช้จ่ายในการดำเนินงาน

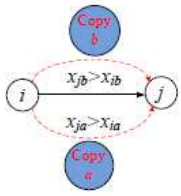
การ Multicasting ใน Delay Tolerant Network เป็นการนำเอาวิธีการ multicast มาประยุกต์ใช้กับ DTN เพื่อให้เกิดประสิทธิภาพในการทำงานที่มากขึ้น โดยสามารถส่งข้อมูลหรือแพ็กเก็ตจากเครื่องต้นทางเพียงเครื่องเดียว ไปยังเครื่องปลายทางได้หลาย ๆ เครื่อง ทำให้ได้รับข้อมูลอย่างกว้างขวาง ลดการใช้ทรัพยากรที่มีอยู่อย่างจำกัด และลดความล่าช้าที่เกิดจากการส่งข้อมูล โดยที่เครื่องต้นทางจะทำการส่งข้อมูลไปยังเครื่องปลายทางได้หลาย ๆ เครื่อง และเครื่องต้นทางสามารถกลับมาเป็นผู้ส่งไปยังเครื่องอื่น ๆ ที่อยู่ในกลุ่มเดียวกันหรือกลุ่มอื่น ๆ ได้

Single copy multicasting เป็นการส่งข้อมูลแบบ multicast ที่มีการทำสำเนาข้อมูลเพียงสำเนาเดียวเพื่อที่จะส่งข้อมูลไปยัง hop ที่อยู่ถัดไป หากข้อมูลดังกล่าวเกิดการสูญหาย node ต้นทางก็จะทำการส่งสำเนาไปให้ใหม่ โดย node ต้นทางจะส่งสำเนาข้อมูลไปยังเฉพาะโหนดที่มีคุณภาพสูงกว่า ซึ่งวิธีนี้ เป็นวิธีที่มีจำนวนการ forwarding น้อยที่สุด และมีอัตราการส่งข้อมูลต่ำ



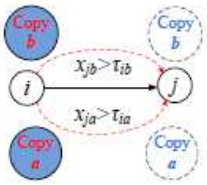
รูปที่ 8 single copy multicast ใน DTNs [33]

Multiple copy multicasting วิธีการนี้จะมีการสร้างสำเนาข้อมูลจาก node ต้นทาง เป็นชุด ๆ ไว้ก่อนที่จะมีการส่งต่อไปยังปลายทาง หากข้อมูลเกิดการสูญหาย node ต้นทาง และ node อื่น ๆ ที่ได้ทำการสำเนาข้อมูลไว้ก็จะทำการสำเนาข้อมูลเพิ่มขึ้นอีก ก่อนที่จะส่งต่อไปยัง node ที่ต้องการข้อมูล ถึงแม้ว่าจะเป็นวิธีที่ค่อนข้างมีประสิทธิภาพ แต่วิธีการนี้ยังคงใช้งานบัฟเฟอร์มากพอสมควร ซึ่งส่งผลให้ค่าใช้จ่ายเพิ่มขึ้นตามบัฟเฟอร์ที่ใช้เพิ่มขึ้นด้วย



รูปที่ 9 Multiple copy multicast in DTNs [33]

Delegation forwarding multicasting (DF) วิธีการนี้โหนดแต่ละโหนดจะทำการสร้างสำเนา และส่งต่อไปยังโหนดที่พบว่ามีคุณภาพสูงกว่าโหนดก่อนหน้านี้ทั้งหมด จนกระทั่งถึงโหนดปลายทางที่ต้องการข้อมูล ซึ่งวิธีการนี้เป็นวิธีการที่เรียบง่ายและมีประสิทธิภาพในการทำงานสูง มีอัตราการส่งข้อมูลสูง และเป็นวิธีที่มีจำนวน latency น้อยที่สุด



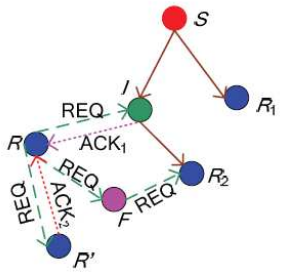
รูปที่ 10 Delegation forwarding multicast ใน DTNs [33]

เนื่องจากประสิทธิภาพการทำงานของ DF มีความสามารถในการลดต้นทุนใน DTNs

(1) จำนวน forwardings : จำนวน forwardings สำหรับกระบวนการ multicast ถือว่าเป็นค่าใช้จ่ายสำหรับการบนการ multicast นั้น

(2) latency : ระยะเวลาเฉลี่ยระหว่างรุ่นของข้อความและเวลาที่เดินทางไปถึงปลายทางสุดท้าย “ประสิทธิภาพสูง” หมายถึงจำนวนของ forwarding ที่น้อยลง และความล่าช้าที่มีขนาดเล็ก

Flexible multicast Routing (FMR) วิธีการนี้จะมีกระบวนการส่งข้อมูลโดยไม่จำเป็นต้องทราบถึงโครงสร้างของเครือข่าย สามารถอนุญาตให้ node สามารถเข้า และออกจากกลุ่มได้อย่างอิสระ เมื่อมีการรับหรือส่งข้อมูลเรียบร้อยแล้วอาจจะออกจากเครือข่ายไปได้ ซึ่งวิธีการนี้ เป็นวิธีการมีค่าใช้จ่ายในการส่ง และบัฟเฟอร์ สูง แต่วิธีการนี้ยังจะสามารถส่งข้อมูลในอัตราการส่งที่สูงเช่นกัน



รูปที่ 11 รูปแบบการทำงานของ Flexible multicast Routing (FMR) [35]

ทุกครั้งขณะที่รับข้อมูลจะเริ่มต้นเข้าสู่ tree multicast ดังรูปที่ 4 ผู้รับข้อมูล R ได้ทำการส่ง บรอดแคสท์ REQ ไปยังทุกโหนดที่อยู่ติดกับตัวเองในลักษณะโครงสร้างแบบต้นไม้ ถ้าไม่ได้รับ ACK จากโหนดใดในช่วงระยะเวลาหนึ่งแสดงว่าโหนดนั้นส่งข้อมูลต่อให้โหนดเพื่อนบ้าน(NSet) โหนด I ได้ส่ง ACK1 กลับมายัง R เมื่อ R ได้รับ ACK1 จาก I แล้วจะสร้างการเชื่อมต่อระหว่าง R กับ I (ถ้าต้นไม้มัลติแคสท์ส่ง REQ ไปมากกว่าหนึ่งโหนดแล้วได้รับ ACK1 พร้อมกัน R จะพิจารณาโหนดที่มีจำนวนฮ็อพน้อยที่สุด) และจะบันทึกจำนวนสมาชิกในต้นไม้มัลติแคสท์ทั้งหมดของ R เรียกว่า In-Tree Set TRUE ในขณะที่ R เข้าร่วมต้นไม้มัลติแคสท์ถ้าโหนดเพื่อนบ้านไม่ได้อยู่ในต้นไม้มัลติแคสท์ เช่น โหนด F (โหนดส่งต่อ) ได้รับ REQ และบรอดคาสท์ต่อไปยังโหนดเพื่อนบ้านและ R’ เป็นโหนดเพื่อนบ้านของ R เมื่อ R’ ส่ง ACK2 กลับไปยัง R เพื่อสร้างการเชื่อมต่อระหว่างกัน ทันทีที่หนึ่งในโหนดเพื่อนบ้านของ R ส่ง ACK1 กลับมา มันจะส่งข้อความไปยังทุกโหนดและทำการเชื่อมต่อระหว่างกันพร้อมกับหยุดส่ง REQs ทันที เพื่อตรวจสอบสถานะการเชื่อมต่อจะส่งข้อความ HELLO ระหว่างกันในทุกๆ 500 ms ถ้าโหนดได้รับข้อความยังอยู่ก็จะส่ง ACK3 กลับไปยังโหนดต้นทาง เรียกว่า In-Tree Flag To FALSE

Probability and Receiver List (PRL) วิธีการนี้เป็นวิธีที่ช่วยเพิ่มประสิทธิภาพของขั้นตอนวิธีการกำหนดเส้นทางอย่างมีนัยสำคัญ ซึ่ง PRL จะคำนวณความน่าจะเป็นที่จะมีการพบกันของ node ปลายทางทุกครั้ง เพื่อหาเส้นทางที่ดีที่สุดในการส่งข้อมูล ซึ่งวิธีการนี้เป็นวิธีที่มีอัตราการส่งข้อมูลสูง latency ต่ำ และค่าใช้จ่ายต่ำ การใช้งานบัฟเฟอร์อยู่ในระดับปานกลาง

Source-Based Delivery (SBD) เป็นวิธีการที่ง่ายที่สุดเพื่อให้บรรลุการัดส่งไปยังกลุ่มของตนเอง ซึ่งอาจจะมีเหตุการณ์ที่ผู้ส่งจะพยายามที่จะส่งแพ็คเก็ตไปยังสมาชิกภายในกลุ่มโดยตรง ซึ่งจะมีการจัดส่งข้อมูลจากแหล่งที่มา ซึ่งวิธีการนี้จะมีการทำงานคล้ายกับการ unicast หลาย ๆ รายการเพื่อให้บรรลุ การจัดส่ง วิธีการนี้จะมีการทำสำเนาข้อมูลเฉพาะ node ต้นทาง latency ในการส่งสูง แต่ในทางกลับกันวิธีการนี้จะใช้งานบัฟเฟอร์ต่ำ ค่าใช้จ่ายต่ำ อัตราการส่งสูง

Group-Based Routing (GBR) วิธีการนี้ในแต่ละกลุ่มจะสามารถส่งข้อมูลไปยังสมาชิกภายในกลุ่ม หรือกลุ่มที่ต่ำกว่ากลุ่มของตนเอง ซึ่ง node ต้นทางที่ส่งข้อมูล จะส่งข้อมูลไปเพียงเฉพาะข้อความที่ node ปลายทางไม่ได้รับเท่านั้น ซึ่งวิธีการนี้ จะเป็นกลไกการแลกเปลี่ยนข้อมูลที่มีประสิทธิภาพ มีการใช้งานบัฟเฟอร์ต่ำ อัตราการส่งข้อมูลต่ำ

Epidemic routing (ER) วิธีการนี้สมาชิกภายในกลุ่มจะมีการแลกเปลี่ยนข้อมูลภายในกลุ่มของตนเองและที่เป็นสมาชิกกับกลุ่มอื่น ๆ ด้วย ซึ่งวิธีการนี้เป็นวิธีการที่มีการนำทรัพยากรข้อมูลมาใช้งานได้อย่างมีประสิทธิภาพ ค่า latency ต่ำ และอัตราการส่งข้อมูลสูงที่สุดในบรรดารูปแบบการกำหนดเส้นทางทั้งหมด สำหรับวิธีการนี้จะมีปัญหาเมื่อมีการใช้งานในสถานการณ์ที่โปรแกรมประยุกต์มีจำนวนมากเนื่องจากความต้องการส่งสูง

ซึ่งจากการนำเอาวิธีการต่าง ๆ มาใช้งานร่วมกับวิธีการ multicast จึงสามารถสรุปประสิทธิภาพการทำงานได้ดังต่อไปนี้

ตารางที่ 5 เปรียบเทียบประสิทธิภาพการทำงานของ Multicasting

เทคโนโลยี		การทำสำเนา	การใช้บัฟเฟอร์	อัตราการส่ง	Latency	ค่าใช้จ่าย
[1]	Single copy multicasting	1	ต่ำ	ต่ำ	สูง	ต่ำ
[2]	Multiple copy multicasting	Many	ปานกลาง	สูง	ต่ำ	ปานกลาง
[3]	DF	Many	สูง	สูง	ต่ำ	ต่ำ
[4]	FMR	Many	สูง	สูง	ต่ำ	สูง
[5]	PRL	Many	ปานกลาง	สูง	ต่ำ	ต่ำ
[6]	SBD	1	ต่ำ	ต่ำ	สูง	ต่ำ
[7]	GBR	Many	ต่ำ	ต่ำ	สูง	ต่ำ
[8]	ER	Many	ปานกลาง	สูง	ต่ำ	ปานกลาง

จากการศึกษาถึงพฤติกรรมของการส่งข้อความ การ Multicast ใน Delay Tolerant Network ในการส่งข้อความแต่ละข้อความไม่ได้เพิ่มความล่าช้าในการส่งข้อความและค่าใช้จ่าย ในขณะที่ความเห็นแก่ตัวของผู้ใช้งานนั้นจะทำให้ความล่าช้าในการส่งข้อมูลเพิ่มขึ้น แต่ในทางกลับกันจะเป็นการประหยัดค่าใช้จ่ายในการส่ง หรือในแง่ของการถ่ายทอดไปยังโครงสร้างของเครือข่ายที่มีความแตกต่างกัน ซึ่งการเพิ่มจำนวนของ hop ใน multicast จะเพิ่มความล่าช้าในการส่งข้อความและเพิ่มค่าใช้จ่ายด้วย ซึ่งมีการพัฒนา Probability and Receiver List เพื่อเพิ่มประสิทธิภาพและความสามารถในการส่งข้อมูลในอัตราสูงและการหน่วงเวลาส่งต่ำ

ข้อดีของการ multicasting ใน Delay Tolerant Networks

1. สนับสนุนการกระจายไปยังกลุ่มผู้ใช้งาน ทำให้สามารถส่งข้อมูลไปยังผู้ใช้บริการได้หลาย ๆ ที่ในเวลาเดียวกัน
2. ประหยัดแบรนด์วิธ
3. ประหยัดค่าใช้จ่าย
4. การใช้ทรัพยากรมีประสิทธิภาพมากขึ้น

ข้อเสียของการ multicasting ใน Delay Tolerant Networks

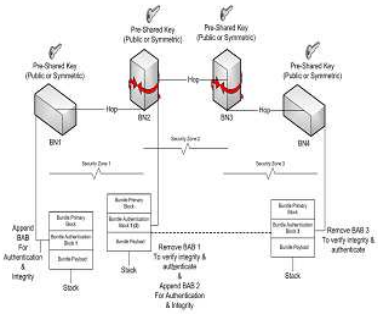
1. หากมีการเพิ่มจำนวนของ hop ในเครือข่ายจะส่งผลให้เครือข่ายเกิดการส่งข้อมูลล่าช้าและ ค่าใช้จ่ายจะสูงขึ้นตามไปด้วย
2. เปลือง buffer

VI.Security

A. สถาปัตยกรรมความปลอดภัยของ DTN

สถาปัตยกรรมความปลอดภัยของ DTN เป็นการรักษาความปลอดภัยและโซลูชั่นสำหรับการไม่เปิดเผยชื่อของ DTN จะขึ้นอยู่กับ IBC (Identity – Based Cryptography) โดยเฉพาะอย่างยิ่งการแก้ปัญหาและรูปแบบการเข้ารหัสตัวตนตามลำดับชั้น (HIBC) ที่ให้บริการโซลูชั่นที่มีประสิทธิภาพและการปฏิบัติเพื่อแก้ไขปัญหา IHBC (Hierarchical Identity–Based Cryptography) การเข้ารหัสข้อมูลตามลำดับชั้น เป็นกลไกสำหรับการถ่ายโอนข้อความที่ปลอดภัย ซึ่งจะใช้ประโยชน์จากการเข้ารหัสลับ (IBE–Identity-based encryption) สำหรับการรักษาความลับของข้อความและการตรวจสอบแหล่งที่มาจะใช้ IBS (Identity – based signatures) สำหรับตรวจสอบแหล่งที่มา

นอกจากนี้ สถาปัตยกรรมความปลอดภัยยังสนับสนุนการตรวจสอบแบบ hop - by - hop และการตรวจสอบความสมบูรณ์เพื่อให้มั่นใจว่าข้อความที่ส่งไปนั้นมีความถูกต้องโดยใช้ Bundle (Bab) ในการตรวจสอบเพื่อให้มั่นใจว่าข้อความที่ส่งจากผู้ส่งไปยังผู้รับนั้นมีความปลอดภัยในทำนองเดียวกันสำหรับแบบ end – to – end จะมีการรักษาความปลอดภัยโดยการบล็อก Integity Payload (PIB) และมีการรักษาความลับที่ถูกบล็อกโดย Payload (PCB) ดังแสดงในรูปที่ 6



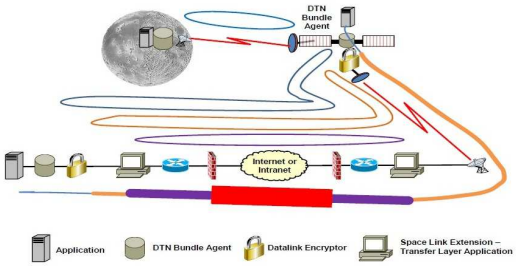
รูปที่ 12 การตรวจสอบ hop by hop [6]

ในการรักษาความปลอดภัย เช่น การรักษาความลับ หรือความสมบูรณ์จะต้องมีการจัดแบบ end-to-end และ hop-by-hop ซึ่งภายในโครงสร้างพื้นฐานของ DTN การจัดการคีย์เป็นปัญหาที่ยากที่สุดในการจัดการความปลอดภัย จึงจำเป็นที่จะต้องมีการรับรองความถูกต้องและความสมบูรณ์ของการตรวจสอบ

โดยทั่วไปผู้เชี่ยวชาญด้านการรักษาความปลอดภัยสถาปัตยกรรมเครือข่ายที่ดี มีแนวคิดที่สามารถเข้าใจการไหลของข้อมูลและเครือข่ายที่มีประสิทธิภาพสามารถใช้ประโยชน์ได้ดังนี้

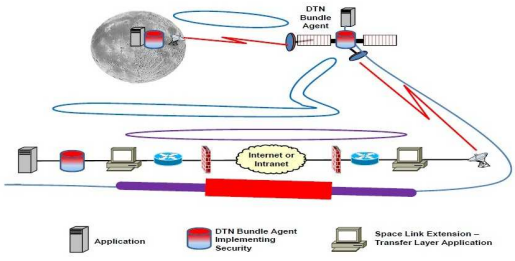
- สามารถใส่กลไกรักษาความปลอดภัยในสถานที่ที่มีจุดอ่อนเพิ่มขึ้น สามสถาปัตยกรรมอย่างง่ายในภาพที่ 1, 2 และ 3 การวิเคราะห์ข้อดีและข้อเสียของแต่ละอันที่ให้ไว้
- มีตัวแทน DTN บันเดิ้ลในการดำเนินภารกิจและตัวแทนบันเดิ้ลฮอปตัวถัดไปบนยานอวกาศ
- มีตัวแทนบันเดิ้ล DTN ในแต่ละสถานีภาคพื้นดินสำหรับสถาปัตยกรรมเหล่านี้ เราสมมุติว่าปฏิบัติการผ่านทางระบบอินเทอร์เน็ตเวิร์กระหว่างประเทศ เช่นนี้เป็นกรณีทั่วไปส่วนใหญ่ ดังนั้นถือว่าศูนย์รวมการดำเนินภารกิจ (Mission Operations) นั้นคือการส่งข้อมูลผ่านทางสถานีภาคพื้นดินของบุคคลที่สาม ในกรณีเช่นนี้ มันไม่น่าที่อย่างใดอย่างหนึ่งจะเป็นการเข้ารหัสลับการเชื่อมต่อที่สถานีภาคพื้นดิน ดังนั้นกรณีที่ 1 และ 2 มีดาต้าลิงค์เข้ารหัสที่ศูนย์ Mission Operations และถอดรหัสที่ยานอวกาศ สถานการณ์เหล่านี้ยังถือว่ามีการเข้ารหัสลับเชื่อมต่อที่ดาต้าลิงค์เลเยอร์หรือเน็ตเวิร์กเลเยอร์ที่ชั้น DTN อย่างน้อยที่สุด สำหรับ

สถานการณ์เหล่านี้เราถือว่าอินเทอร์เน็ตโปรโตคอลหยุดที่พื้นดิน และโปรโตคอล CCSDS จะใช้สำหรับการเชื่อมโยงการสื่อสารพื้นที่/พื้นดิน หนึ่งสามารถเรียกใช้ DTN ผ่านเครือข่าย และใช้ IPsec หรือการรวมกันของ IPsec และ DTN security เพื่อรักษาความปลอดภัยของระบบ



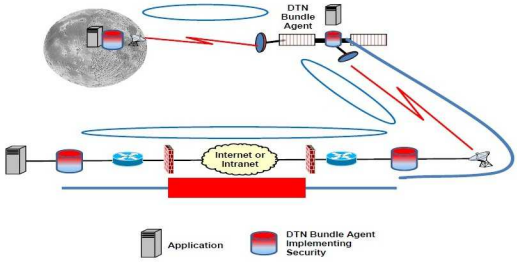
รูปที่ 13 DTN มากกว่าเข้ารหัสดาต้าลิงค์ที่ใช้บริการถ่ายโอน SLE [1]

จากรูปที่ 13 แสดงให้เห็นถึงสถานการณ์ที่ DTN node อยู่ที่ Mission Operations และ hop ตัวถัดไป DTN node อยู่บนยานอวกาศ เราสมมุติการเข้ารหัสที่จำเป็นและสถานีภาคพื้นดินบุคคลที่สามนั้นถูกใช้ ดังนั้นดาต้าลิงค์จะต้องได้รับการเข้ารหัส/ถอดรหัสระหว่าง Mission Operations และยานอวกาศเพื่อประสานข้อมูลบิตสตรีม, การเข้ารหัส/ถอดรหัสดาต้าลิงค์พิเศษเป็นสิ่งจำเป็นใน Mission Operations การเข้ารหัสข้อมูลผ่านทางส่วนขยายของการเชื่อมโยงพื้นที่ แอพลิเคชั่นการถ่ายโอนบริการและอุโมงค์แอพลิเคชั่นเลเยอร์ และลูปการควบคุมจะจัดตั้งขึ้น ข้อมูลจะถูกส่งมาจาก Mission Operation ไปยังสถานีภาคพื้นดินที่เหมาะสมผ่านทางอุโมง IPsec รักษาความปลอดภัยที่จัดตั้งขึ้นระหว่าง Mission Operation และสถานีไฟร์วอลล์ภาคพื้นดิน ที่สถานีภาคพื้นดิน ข้อมูลดาต้าลิงค์จะถูกแยกจากอุโมงค์ SLE-TS และส่งต่อไปยังยานอวกาศ ที่ยานอวกาศ DTN บันเดิ้ลสามารถแยกและส่งต่อไปยังตัวแทนทบันเดิ้ลที่เหมาะสมต่อไป



รูปที่ 14 การรักษาความปลอดภัย DTN ที่ใช้บริการถ่ายโอน SLE [1]

จากรูปที่ 14 คล้ายกับภาพที่ 13 ในการแสดงให้เห็นถึงสถานการณ์ที่ DTN node อยู่ที่ Mission Operations และ hop ตัวถัดไป DTN node บนยานอวกาศ อย่างไรก็ตาม ที่นี่การรักษาความปลอดภัย DTN บันเดิ้ลแทนที่การรักษาความปลอดภัยดาต้าลิงค์ (แม้ว่าทั้งสองสามารถใช้ประโยชน์ได้) เราถือว่าการเข้ารหัสลับที่จำเป็นและสถานีภาคพื้นดินบุคคลที่สามนั้นถูกใช้ ที่นี่บันเดิ้ลมีความปลอดภัยระหว่าง Mission Operation และปลายทางที่เหมาะสม ไม่ว่าจะเป็นยานอวกาศของโหนดดวงจันทร์ การเข้ารหัสผ่านบันเดิ้ลผ่านแอพลิเคชั่นบริการถ่ายโอนส่วนขยายของการเชื่อมโยงพื้นที่ และอุโมงค์แอพลิเคชั่นเลเยอร์และลูปการควบคุมจะจัดตั้งขึ้น ข้อมูลจะถูกส่งต่อจาก Mission Operation ไปยังสถานีภาคพื้นดินที่เหมาะสม ผ่านอุโมงค์รักษาความปลอดภัย IPsec ซึ่งได้ก่อตั้งขึ้นระหว่าง Mission Operation และสถานีไฟร์วอลล์ภาคพื้นดิน ที่สถานีภาคพื้นดิน ข้อมูลดาต้าลิงค์จะถูกแยกจากอุโมง SLE-TS และส่งต่อไปยังยานอวกาศ ที่ยานอวกาศ DTN บันเดิ้ลสามารถแยกจากดาต้าลิงค์สตรีมและส่งต่อไปยังตัวแทนบันเดิ้ลที่เหมาะสมต่อไป



รูปที่ 15 การรักษาความปลอดภัย DTN โดยไม่ต้องใช้บริการถ่ายโอน SLE [1]

รูปที่ 15 ตัวแทน DTN บันเดิ้ลจะอยู่ในแต่ละสถานีภาคพื้นดิน ตั้งแต่การสื่อสารเป็น hop-by-hop ไม่มีความจำเป็นต้องขยายพื้นที่ของการเชื่อมโยง ดังนั้น SLE การขนส่งบริการแอพลิเคชั่นเกตเวย์สามารถลบออกได้ นอกจากนี้การเชื่อมโยงสามารถเพิ่มประสิทธิภาพระหว่างแต่ละโหนดบันเดิ้ลผ่านทางเลือกที่เหมาะสมของชั้นคอนเวอร์เจนซ์ ตัวอย่างเช่น แทนที่จะทำงาน LTP ระหว่างดาวเทียมที่ถ่ายทอดดวงจันทร์และ Mission Operations และอาจจะทำเพื่อสถานการณ์ 1 และ 2 สามารถเรียกใช้ TCP คอนเวอร์เจนซ์เลเยอร์ระหว่าง Mission Operations และสถานีภาคพื้นดิน และ LTP ระหว่างสถานีภาคพื้นดินและการถ่ายทอด จึงเพิ่มประสิทธิภาพของทรานสปอร์ตโปรโตคอลสำหรับแต่ละการเชื่อมโยง DTN

สองรายการสำคัญที่ควรทราบจากสามสถานการณ์ :

(1) ความซับซ้อนของสถาปัตยกรรมจะต่ำลงมาก ถ้ายินดีที่จะอนุญาติ DTN ในการจัดการการรักษาความปลอดภัย ลดความซับซ้อนของสถาปัตยกรรมช่วยให้หนึ่งเพื่อทำความเข้าใจและจุดอ่อนที่อยู่ในเครือข่าย และผลลัพธ์ในพื้นที่น้อยที่สามารถใช้ประโยชน์และระบบความปลอดภัยมากขึ้น

(2) จำนวนลูปการควบคุมจะลดลงอย่างมาก แต่ละกลไกรักษาความปลอดภัยสามารถทำงานภายในลักษณะของภายใต้ทรานสปอร์ตโปรโตคอลและกลไกอุโมงค์ (tunnel) และแต่ละทรานสปอร์ตโปรโตคอลต้องสามารถดำเนินการกับนิสัยเฉพาะของลูปควบคุมการฝังตัว ปฏิสัมพันธ์ระหว่างทรานสปอร์ตโปรโตคอลและกลไกรักษาความปลอดภัยจะค่อนข้างบอบบาง ดังนั้นการลดจำนวนของการห่อหุ้ม (encapsulation) เป็นประโยชน์อย่างมาก

ตารางที่ 6 เปรียบเทียบสถาปัตยกรรม DTN และการรักษาความปลอดภัย

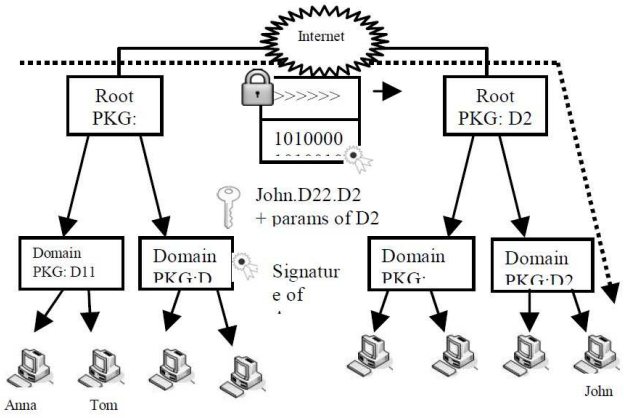
[1]	DTN มากกว่าเข้ารหัสดาต้าลิงค์ที่ใช้บริการถ่ายโอน SLE	สถานการณ์ที่โหนด DTN อยู่ที่ Mission Operations และโหนด DTN ฮอปตัวถัดไปอยู่บนยานอวกาศ
[2]	การรักษาความปลอดภัย DTN ที่ใช้บริการถ่ายโอน SLE	คล้ายกับ [1] ในสถานการณ์ที่โหนด DTN อยู่ที่ Mission Operations และโหนด DTN ฮอปตัวถัดไปบนยานอวกาศ อย่างไรก็ตามที่นี่การรักษาความปลอดภัย DTN บันเดิ้ลแทนที่การรักษาความปลอดภัยดาต้าลิงค์
[3]	การรักษาความปลอดภัย DTN โดยไม่ต้องใช้บริการถ่ายโอน SLE	ตัวแทน DTN บันเดิ้ลจะอยู่ในแต่ละสถานีภาคพื้นดิน ตั้งแต่การสื่อสารเป็น hop-by-hop ไม่มีความจำเป็นต้องขยายพื้นที่ของการเชื่อมโยง ดังนั้น SLE-Transport Service Application gateways สามารถลบออกได้

B. การสื่อสารที่ปลอดภัยระหว่างพื้นที่

ผู้ส่งและผู้รับข้อความอาจเป็นสองพื้นที่ที่ใช้สถาปัตยกรรมความปลอดภัยเหมือนหรือต่างกัน หากต้องการให้แน่ใจว่าการสื่อสารปลอดภัย เราได้นำเสนอกลไกที่สามารถนำมาใช้ในทั้งสองสถานการณ์

1) พื้นที่ของสถาปัตยกรรมความปลอดภัยเดียวกัน

หากทั้งสองพื้นที่ใช้ HIBC แล้วผู้ส่งใช้รหัสและ public parameter ของ root PKG ของผู้รับสำหรับการเข้ารหัสข้อมูล ในทำนองเดียวกันผู้รับใช้รหัสและ public parameter ของ root PKG ของผู้ส่งสำหรับตรวจสอบลายเซ็นต์ ต้องมีความน่าเชื่อถือระหว่าง root PKGs ของพื้นที่ที่ต่างกัน เอนทิตีจะได้รับ public parameter ของ root PKG ในการสื่อสารเอนทิตีจาก PKG ของตนเองผ่านการร้องขอ หรือ PKG อาจถ่ายทอด public parameter ของพื้นที่ที่ต่างกันเป็นระยะตลอดทั้งโดเมน



รูปที่ 16 การถ่ายโอนข้อมูลการรักษาความปลอดภัยระหว่างสองพื้นที่โดยใช้วิธีการ HIBC [2]

ตามสมมติฐานของเราตั้งแต่อินเทอร์เน็ตเป็นพื้นที่หลักซึ่งส่วนที่เหลือของพื้นที่มีการเชื่อมต่อ ดังนั้นข้อความจากพื้นที่ DTN หนึ่งลัดเลาะพื้นที่อินเทอร์เน็ตไปถึงพื้นที่ปลายทาง

2) พื้นที่ของสถาปัตยกรรมความปลอดภัยที่แตกต่างกัน

พิจารณาสถานการณ์ที่มีแหล่งที่มาเป็นของพื้นที่ที่ใช้กลไก HIBC และเอนทิตีปลายทางอยู่ในอินเทอร์เน็ต โดยใช้วิธีการ PKI แหล่งที่มาของการเข้ารหัสข้อความโดยใช้รหัสและ public parameter ของ PKG หลักและลายเซ็นต์ดิจิตอล root PKG ยืนยันการตรวจสอบข้อความและถอดรหัสข้อความ root PKG ดึงข้อมูล public key ของเอนทิตีปลายทางจาก CA ที่เชื่อถือในพื้นที่อินเทอร์เน็ต เข้ารหัสข้อความโดยใช้ public key ของปลายทางและลายเซ็นต์ข้อความที่ใช้ private key ซึ่ง private key นี้เป็นไปตาม PKI

ตามสมมติฐาน เกตเวย์แต่ละพื้นที่มีการเชื่อมต่อแบบ end-to-end กับอินเทอร์เน็ตโหนด, PKG หลักมี Public keys สองคู่ หนึ่งใช้ในการตัดการเชื่อมต่อพื้นที่และได้รับการอนุมัติโดย CA ภายใต้ระบบ PKI ในอินเทอร์เน็ต รหัสกุญแจสมมาตรใช้ภายในพื้นที่ตัดการเชื่อมต่อในขณะที่ PKI ใช้ภายในอินเทอร์เน็ต

ถ้าแหล่งที่มาจากอินเทอร์เน็ตและเอนทิตีปลายทางจากพื้นที่ตัดการเชื่อมต่อแล้วดาวน์โหลด public key ของ PKG หลักของพื้นที่ปลายทางจาก CA เข้ารหัสข้อความโดยใช้ public key และลายเซ็นต์โดยใช้ private key ของตัวเอง PKG หลักหลังจากตรวจสอบการถอดรหัสข้อความโดยใช้ private key ตามกลไก PKI มันจะเข้ารหัสข้อความโดยใช้ public parameter และรหัสของเอนทิตีปลายทางนี่คือข้อความที่เข้ารหัสและส่งต่อไปยังเอนทิตีปลายทาง

C. *การรักษาความปลอดภัยของ DTN*

ในงานวิจัยทางด้านการรักษาความปลอดภัยบน DTN นั้น มีทั้งในรูปแบบของการกำหนดโปรโตคอลกำหนดเส้นทาง เช่น งานวิจัยของ Feng Cheng Lee [52] ใช้วิธีการเข้าติดตามคุณสมบัติของความน่าจะเป็น เรียกว่า Probabilistic Routing Protocol using History of Encounters and Transitivity (PRoPHET) จะใช้ประวัติการเคลื่อนที่ของโหนดเป็นตัวแปรในการตัดสินใจเพื่อกำหนดเส้นทาง นอกจากนั้นตัวแปรเหล่านี้ยังสามารถใช้ในการรักษาความปลอดภัยใน DTN ได้ด้วย โดยที่ PRoPHET สามารถทำงานได้โดยไม่จำเป็นที่จะต้องทราบข้อมูลโครงสร้างต่างๆภายในเครือข่ายทั้งหมด จึงมีความเหมาะสมกับการทำงานบน DTN ในงานวิจัยนี้มี attack คือ การโจมตีแบบฟลัด (flooding attack) และงานวิจัยของ Ahmad [44] ใช้ CSP ที่มีการคำนวณใหม่โดยใช้ Failure Divergence Model (FDR) สำหรับการเช็ค เป็นการรักษาความปลอดภัยในเครือข่ายที่ทนต่อความล่าช้าโดยไม่ได้อาศัยการเข้ารหัสข้อมูล แต่ใช้การคำนวณค่า Failure และมีการเปรียบเทียบกับ CSP ที่ยังไม่มีการคำนวณ เพื่อป้องกันการโจมตีแบบ Denial of Service (DOS)

นอกจากนั้นยังมีการรักษาความปลอดภัยแบบบน DTN ที่ใช้การเข้ารหัสข้อมูลแบบต่างๆ เช่น การเข้ารหัสแบบ BEK [44] หรือเรียกว่า bundle

encrypting key ที่มีการทำงานคล้ายกับ PKI ซึ่งสามารถใช้งานได้ดีแต่ยังมีข้อบกพร่องทางด้านความล่าช้าเมื่อนำมาใช้งานใน DTN การรักษาความปลอดภัยแบบอื่นๆที่ IBC ที่พัฒนามาจาก PKI มาใช้งานเพื่อป้องกันการโจมตีในสภาวะแวดล้อมแบบต่างๆ และลดภาระการส่งข้อมูลจากการใช้ PKI เช่น งานวิจัยของ M.R. Fida [50], Farrell S. และ Cahill V [55], A. Seth และ S. Keshav [48], P.T. Edelman [47] เพื่อยืนยันตัวตนเข้ารหัสข้อมูล และป้องกันการโจมตีแบบ DOS ได้ และมีการใช้ในการป้องกันการโจมตีแบบ pollution attack [54] ได้อีกด้วย

การใช้งาน IBC ได้มีการพัฒนาในรูปแบบต่างๆเพื่อให้รองรับเครือข่ายที่มีขนาดใหญ่ขึ้นซึ่งเรียกว่า Hierarchical Identity Based Cryptography (HIBC) [51] และการเข้ารหัสแบบ SOK [53] ซึ่งทั้งสองมีการทำงานที่คล้ายกันคือใช้ PKG สองชุดต่อหนึ่งยูสเซอร์ ชุดแรกเรียกว่า Local PKG ใช้สำหรับติดต่อสื่อสารระหว่างยูสเซอร์ที่อยู่ภายในโดเมนหรือเราท์เตอร์เดียวกัน อีกชุดเรียกว่า Long Range PKG สำหรับสื่อสารนอกโดเมน โดยมีการเรียงลำดับชั้นของ PKG ในรูปแบบของผังต้นไม้เพื่อลดภาระการทำงานของ PKG เมื่อใช้งานในเครือข่ายที่มีขนาดใหญ่

ตารางที่ 7 ปัญหาและวิธีการแก้ปัญหาใน DTN

ปัญหา	วิธีการแก้ปัญหา
1. การซ้อนทับของข้อมูล	มีการควบคุมการเข้าถึงของข้อมูลโดยการเข้ารหัส (HIBC) เพื่อรักษาความปลอดภัยสำหรับการสื่อสารในกลุ่มเส้นทางที่ไม่น่าเชื่อถือ และยังสามารถตรวจสอบแหล่งที่มาของข้อมูลที่ส่งมาได้
2. การรักษาความปลอดภัยของผู้ส่งไปยังผู้รับการรักษาความปลอดภัย	สร้างตัวกลางในการเชื่อมต่อเช่น Gateway ของเครือข่ายเซ็นเซอร์จะทำงานเป็นระบบรักษาความปลอดภัยผู้ส่ง โดยการเข้ารหัสการรวมกลุ่ม ซึ่งทำหน้าที่เป็นการรักษาความปลอดภัยปลายทางและการตรวจสอบการรวมกลุ่มที่ได้รับทั้งหมดโดยใช้รหัสก่อนที่จะส่งต่อไปยังผู้รับจริงทั้งมีอินเทอร์เน็ตและไม่มีอินเทอร์เน็ต
3. การโจมตีระหว่างโหนดที่เป็นปฏิปักษ์กัน	ใช้การเข้ารหัสเครือข่าย โดยอาศัยโครงสร้างพื้นฐาน PKI
4. การรักษาความลับ	มีการใช้กลไกการเข้ารหัสแบบดั้งเดิมซึ่งในการส่งนั้น ผู้รับจะได้เฉพาะคีย์ในการเข้ารหัสลับ ซึ่งจะเป็นกลไกแบบ end-to-end สำหรับการป้องกันการประยุกต์ใช้งานในเครือข่าย และกลไกแบบ hop-by-hop สำหรับการป้องกันโครงสร้างพื้นฐาน
5. การเข้าถึงที่ไม่ได้รับอนุญาต	ใช้หลักการเข้ารหัสแบบเอกลักษณ์แบบลำดับชั้น (IBC) จะช่วยในการกระจายคีย์ ซึ่งมีประสิทธิภาพในพื้นที่เครือข่ายที่ทนต่อความล่าช้า
6. โครงสร้างและการบำรุงรักษา	พิจารณาจากวิธีการที่แตกต่างกันสำหรับการจัดโครงสร้างและการบำรุงรักษา

D. การเข้ารหัสข้อมูลที่เป็นเอกลักษณ์แบบลำดับชั้นสำหรับการรักษาความปลอดภัยแบบ End-to-End ใน DTN (Hierachical Identity Based Cryptography for End-to-End Security in DTNs)

ความต้องการที่สำคัญของสถาปัตยกรรมระบบรักษาความปลอดภัยในเครือข่ายที่ทนต่อความล่าช้า มีแนวคิดจากกลไก hop-by-hop สำหรับการป้องกันโครงสร้างพื้นฐานและกลไก end-to-end สำหรับการป้องกันโปรแกรมประยุกต์

1. การป้องกันโครงสร้างพื้นฐาน

จุดมุ่งหมายคือการป้องกันโครงสร้างพื้นฐานของเครือข่ายที่ทนต่อความล่าช้าจากการใช้งานที่ไม่ได้รับอนุญาต การให้บริการรักษาความปลอดภัยที่สำคัญจำเป็นต้องมีการควบคุมการเข้าถึงเพื่อให้แน่ใจว่าจะมีการประยุกต์ใช้งานที่ถูกต้องตามกฎหมายเท่านั้นที่จะยัดเข้าไปในการจราจรของเครือข่ายที่ทนต่อความล่าช้าได้ และการตรวจสอบผู้ส่งแบบ hop-by-hop และความสมบูรณ์สำหรับการตรวจสอบเอกลักษณ์ของผู้ส่งและเพื่อให้แน่ใจว่าการรวมกลุ่มยังไม่ได้รับการแก้ไขโดยบุคคลที่เป็นอันตรายในขณะกำลังมีการส่ง ความต้องการที่เกี่ยวข้องที่จะนำเสนอการจำกัดจำนวนของความสามารถในการควบคุมการเข้าถึงการประยุกต์ใช้งานที่ได้รับอนุญาตให้มีการรวมกลุ่มการส่งเท่านั้นในระดับที่จำกัดของการให้บริการ การควบคุมการเข้าถึงนี้จะช่วยให้เราเตอร์ในเครือข่ายที่ทนต่อความล่าช้าลดการจราจรที่ผิดกฎหมายในเครือข่าย โดยการตรวจสอบการรวมกลุ่มที่จะยัดเข้าไปโดยเราเตอร์ที่เป็นอันตรายหรือบุคคลที่พยายามที่จะใช้ระดับของการบริการที่ไม่ได้รับอนุญาต

การรวมกลุ่มโปรโตคอลในเครือข่ายที่ทนต่อความล่าช้าให้ Bundle Authentication Header (BAH) ที่สามารถใช้สำหรับความต้องการดังกล่าวข้างต้น BAH ถูกสร้างขึ้นและตรวจสอบโดยตัวแทนของทุกๆการรวมกลุ่มที่ได้รับบนพื้นฐานแบบ hop-by-hop ตลอดจนการรวมกลุ่มเส้นทางแบบ end - to – end

2. การประยุกต์การป้องกัน

จุดมุ่งหมายคือการให้บริการรักษาความปลอดภัยแบบ end - to - end เพื่อการใช้งานในเครือข่ายที่ทนต่อความล่าช้า ซึ่งรวมถึงการตรวจสอบแหล่งที่มาเพื่อยืนยันตัวตนของบุคคลจากแหล่งที่มาในเครือข่ายที่ทนต่อความล่าช้า การตรวจสอบปลายทางเพื่อตรวจสอบการรวมกลุ่มปลายทางที่แน่นอนเพื่อ entity ในเครือข่ายที่ทนต่อความล่าช้าลำดับสุดท้าย การรักษาความสมบูรณ์ของการรวมกลุ่มแบบ end-to-end เพื่อให้แน่ใจว่าการรวมกลุ่ม payload หรือส่วนหัว

อื่นๆ ยังไม่ได้รับการปรับเปลี่ยนในตอนส่งและความลับของข้อมูลเพื่อให้ข้อมูลในระดับประยุกต์จะถูกเก็บไว้เป็นความลับไปยังตัวแทนของบริษัทผู้ผลิตในเครือข่าย

การรวมโปรโตคอลในเครือข่ายที่ทนต่อความล่าช้าให้ Payload Security Header (PSH) ที่สามารถใช้สำหรับการรักษาความลับแบบ end - to – end ความสมบูรณ์และการตรวจสอบ PSH ถูกสร้างขึ้นและตรวจสอบบนพื้นฐาน end-to-end ระหว่างแหล่งที่มาและการสื่อสารปลายทางของตัวแทนการรวมกลุ่มที่จุดปลายทาง

3. นโยบายการควบคุมการเข้าถึง

มีจุดมุ่งหมายเพื่อให้กลไกของเราเตอร์แต่ละตัวในเครือข่ายที่ทนต่อความล่าช้า สามารถบังคับใช้นโยบายการควบคุมการเข้าถึงของตัวเองบนพื้นฐานของตัวตนของแหล่งที่มาและสิทธิ์ของการรวมกลุ่ม สิ่งที่ช่วยอำนวยความสะดวกเหล่านี้จะเป็นประโยชน์อย่างยิ่งสำหรับ edge หรือเกตเวย์เราเตอร์ของพื้นที่ในการบริหารเฉพาะของเครือข่ายที่ทนต่อความล่าช้า ที่เราต้องการที่จะกำหนดควบคุมการเข้าถึงที่เข้มงวดและไม่ต้องพึ่งพาการตัดสินใจที่ทำโดยเราเตอร์ในพื้นที่อื่น ๆ ที่อาจมีการรวมกลุ่มการส่งต่อ

แนวคิดของการเข้ารหัสข้อมูลที่ได้รับการแนะนำครั้งแรกโดย Shamir รูปแบบ IBE ในทางปฏิบัติครั้งแรกถูกนำเสนอในปี 2001 โดย Boneh และ Franklin ถึงแม้ว่างานของ IBE จะมาก ก็ได้มีการมุ่งเน้นรูปแบบที่มีโครงสร้างพื้นฐานที่เชื่อถือได้อย่างหนึ่งของโลกและหนึ่งในเครื่องกำเนิดไฟฟ้า IBE ที่สำคัญที่เชื่อถือได้ ด้วยการทำงานที่มากขึ้น ล่าสุดได้เริ่มที่จะอธิบายพื้นฐานที่ทำงานร่วมกับโมเดลที่เชื่อถือได้ที่มีข้อจำกัดที่น้อยกว่า ซึ่งรวมถึงการทำงานเกี่ยวกับการออกแบบของโปรโตคอลที่ทำงานระหว่างผู้ใช้ในโดเมนที่มีความน่าเชื่อถือที่แตกต่างกันและยังเกี่ยวกับองค์กรแบบลำดับชั้นของ IBC ที่เป็นศูนย์กลางความน่าเชื่อถือ

Appenzeller และ Lynn มีการเสนอให้เป็นโปรโตคอลการรักษาความปลอดภัยในลำดับชั้นเครือข่ายที่ช่วยให้การเข้ารหัสและรับรองความถูกต้องในการสื่อสารระหว่างโฮสต์โดยใช้แบบที่ไม่มีปฏิสัมพันธ์ระหว่างกันให้ความสำคัญพื้นฐานของตัวตน โปรโตคอลการแลกเปลี่ยนขึ้นอยู่กับความคิดที่แสดงออก อย่างไรก็ตาม ไม่เหมือนกับรูปแบบของเรา งานของพวกเขาเพียงแต่สนับสนุนการสื่อสารระหว่างโฮสต์ที่ต้องอยู่ในโดเมนเดียวกันกับ IBC ที่มีความน่าเชื่อถือ

Smetters และ Durfee นำเสนอวิธีการใช้ IBE ข้ามโดเมนที่น่าเชื่อถือได้หลายโดเมน โดยในแต่ละโดเมนจะมี PKG เป็นของตัวเอง ลำดับชั้นของโดเมนที่เชื่อถือได้เป็นคู่ขนานบนสัมพันธ์แน่นหนากับลำดับชั้นของเครือข่ายที่ทนต่อความล่าช้า พวกเขาใช้ลำดับชั้นนี้เฉพาะสำหรับให้ความสำคัญกับการกระจายที่มีประสิทธิภาพในขณะที่พวกเขาทำงาน เราใช้การเข้ารหัสแบบลำดับชั้นสำหรับการเรียกคืนในช่วงเวลาที่แตกต่างกันได้พร้อมๆกัน และยังมีการควบคุมการเข้าถึงอย่างละเอียดนอกเหนือไปจากการกระจายที่มีประสิทธิภาพ

การให้บริการรักษาความปลอดภัยในรูปแบบของการรักษาความลับ ความสมบูรณ์ การตรวจสอบ end-to-end และ hop-by-hop และควบคุมการเข้าถึงเพื่อปกป้องโครงสร้างพื้นฐานสำหรับเครือข่ายที่ทนต่อความล่าช้า เป็นเป้าหมายที่ท้าทายมากจากข้อจำกัดในการดำเนินงานที่มีอยู่มากของการเชื่อมต่อที่ไม่ได้บ่อยครั้งและเวลาทั้งหมดที่มีมากขึ้นในการเดินทางของสัญญาณจากต้นทางถึงปลายทางและย้อนกลับมาที่ต้นทางอีกที

ในงานวิจัยนี้ เราเสนอรูปแบบการรักษาความปลอดภัยสำหรับเครือข่ายที่ทนต่อความล่าช้าขึ้นอยู่กับการเข้ารหัสข้อมูลที่เป็นเอกลักษณ์แบบลำดับชั้น รูปแบบนี้จะช่วยให้การกระจายคีย์มีประสิทธิภาพในพื้นที่เครือข่ายที่ทนต่อความล่าช้า ช่วยให้ควบคุมการเรียกคืนข้อมูลได้ง่ายขึ้นและยังช่วยให้การควบคุมการเข้าถึงอย่างละเอียด นอกจากนี้ยังมีการแสดงความคิดเห็นเกี่ยวกับส่วนของการดำเนินงานที่เราต้องเผชิญเกี่ยวกับการรวมข้อกำหนดของโปรโตคอล

แม้ว่า IBC จะมีจำนวนข้อเสียและมีความจำเป็นสำหรับการวิจัยมากขึ้น เราเชื่อว่าข้อจำกัดของความผิดปกติของการดำเนินการในเครือข่ายที่ทนต่อความล่าช้าทำให้ IBC เป็นแนวทางที่น่าสนใจมากขึ้นกว่า PKI เดิมด้วยเหตุผลดังต่อไปนี้ การกระจายของคีย์มีความแน่นอน ได้รับการรับรองโดยนัยสำคัญและการเรียกข้อมูลโดยใช้แบนด์วิดธ์ที่ต่ำกว่า

E. *การเข้ารหัสเครือข่ายความปลอดภัยใน DTN*

การประยุกต์ใช้การเข้ารหัสเครือข่ายที่มีนัยสำคัญสามารถปรับปรุงประสิทธิภาพของการจัดส่งข้อความในเครือข่ายที่ทนต่อความล่าช้า สมมติว่าผู้เข้าร่วมทั้งหมดมีการทำงานแบบซื่อสัตย์ อย่างไรก็ตาม ถ้าโหนดบางโหนดของเครือข่ายมีการบุกรุกฝ่ายตรงข้ามสามารถเปิดภาวการณ์โจมตีและวิธีนี้สามารถทำลายข้อมูลจำนวนมากด้วยความพยายามเพียงเล็กน้อย ปัจจุบันการแก้ปัญหาจากภาวการณ์โจมตีต้องใช้โครงสร้างพื้นฐานกุญแจสาธารณะ ที่มักจะไม่สามารถใช้ได้ในเครือข่ายไร้สาย ad-hoc ข้อเสนอของเราช่วยให้มีการตรวจสอบแต่ละแพคเกจ ด้วยเหตุนี้โหนดเหล่านั้นจึงสามารถตัดสินใจได้ว่าแพ็กเก็ตเหล่านี้จะสามารถเข้ารหัสด้วยกันได้โดยไม่ต้องมีการตรวจสอบแหล่งที่มา

F. *การพิจารณาความปลอดภัยในอวกาศและ DTN*

สถานที่หลักสำหรับเครือข่ายที่ทนต่อความล่าช้า งานที่เกี่ยวข้องกับการรักษาความปลอดภัยคือInternet Research Task Force's (IRTF) [56] Delay Tolerant Networking Research Group (DTNRG) [57] วัตถุประสงค์หลักในที่นี้คือการทำให้เกิดการเสนอความคิดเห็นร่วมกันระหว่างผู้เชี่ยวชาญด้านไอทีในภารกิจบนอวกาศและผู้ให้บริการด้านการรักษาความปลอดภัยสำหรับเครือข่ายที่ทนต่อความล่าช้าและเครือข่ายที่คล้ายกัน

เช่นเดียวกับเครือข่ายอื่นๆ เครือข่ายที่ทนต่อความล่าช้าหรือเครือข่ายของภารกิจบนอวกาศอาจใช้ข้อมูลการเข้ารหัสลับในการรักษาความลับและการบริการที่ซื่อสัตย์ อย่างไรก็ตาม ยังขาดการเชื่อมต่อแบบ end-to-end และอาจเกิดความไม่สมมาตรอย่างมากในด้านของความสามารถและการเชื่อมต่อ หมายความว่าจำเป็นต้องกำหนดสิ่งที่เกิดผิดปกติสำหรับบริการดังกล่าว ไม่เพียงแต่มีแหล่งที่มาและปลายทางสำหรับข้อมูล แต่แหล่งที่มาและปลายทางของการรักษาความปลอดภัยที่แตกต่างกันอาจเกิดขึ้น การพิจารณาการทำงานในปัจจุบันในหัวข้อนี้และที่เกี่ยวข้องกับส่วนนี้ ตัวอย่างเช่น หัวใจสำคัญของการจัดการสำหรับสภาพแวดล้อมที่มีความล่าช้าที่สูงปัจจุบันยังไม่มีวิธีการแก้ปัญหาที่ชัดเจนที่นำไปใช้ได้

นอกเหนือจากการให้บริการรักษาความปลอดภัยการเข้ารหัสลับ เราได้เรียนรู้จากอินเทอร์เน็ตว่าให้ใส่ใจไปยังส่วนของการดำเนินการ ชี้นำ ตัวอย่างเช่น ไฟร์วอลล์แยกเครือข่ายโดเมนรักษาความปลอดภัยที่แตกต่างกันที่มีความเชื่อมั่นว่ามีเพียงการจราจรที่ถูกเสนอเท่านั้นที่จะได้รับการอนุมัติให้เป็นปัจจุบันในแต่ละโดเมน อย่างไรก็ตาม ยังเกิดขึ้นเสมอในการแลกเปลี่ยนระหว่าง “การรักษาความปลอดภัย” และ “สิ่งที่ถูกใช้งาน” ในสภาพแวดล้อมเช่นนี้และประสบการณ์บนอินเทอร์เน็ต คือมันเป็นไปได้ที่จะแทรกการจราจรที่ไม่ได้รับอนุญาตในโดเมนการรักษาความปลอดภัยใดๆ ดังนั้นจึงยังมีช่องโหว่ของเค้าโครงที่เกี่ยวกับการดำเนินการบางอย่าง โดยเฉพาะในผู้ที่อาจต้องมีการพิจารณาเฉพาะในภารกิจบนอวกาศ

นอกจากนี้ยังตรวจสอบบางส่วนของศักยภาพการแลกเปลี่ยนที่เกิดขึ้นเป็นเครือข่ายที่ซับซ้อนมากขึ้นตามพื้นที่ที่มีการเชื่อมต่ออย่างใกล้ชิดมากกับอินเทอร์เน็ต ตัวอย่างเช่น ภารกิจบนอวกาศที่ต้องใช้วิธีการต่างๆเพื่อให้ยานอวกาศเริ่มต้นการตั้งค่าใหม่ แท้จริงแล้วทุกๆรูปแบบสามารถขัดขวางหรือก่อกวนระบบเครือข่าย การโจมตีทำให้มีผลกระทบต่อภารกิจบนอวกาศอาจจะทำให้เกิดหายนะ

ประโยชน์ที่สำคัญของการตรวจสอบบริการรักษาความปลอดภัยรวมทั้งส่วนของการดำเนินการเป็นความรู้ที่เพิ่มขึ้นที่เป็นไปได้ และการพิจารณาการรักษาความปลอดภัยที่เกิดขึ้นทำให้ภารกิจบนอวกาศดีขึ้น และการใช้ประโยชน์จากอินเทอร์เน็ตบนโลกและเทคโนโลยีที่เกี่ยวข้อง มีผลมาจากงานอาจรวมถึงลักษณะของความต้องการความปลอดภัยสำหรับภารกิจบนอวกาศในอนาคตขึ้นอยู่กับภัยคุกคามทางอินเทอร์เน็ตในปัจจุบันแต่คำนึงถึงปัญหาที่อธิบายไว้

DTNRG คือการพัฒนาทั้งสองโปรโตคอลหลักที่ทนต่อความล่าช้า bundle protocol กำหนดเครือข่ายซ้อนทับและ Licklider Transmission Protocol (LTP) เป็นโปรโตคอลแบบ point-to-point รูปแบบเหล่านี้พื้นฐานสำหรับความคิดเห็นที่จะนำเสนอต่อไปนี้

1. LTP Security

ตั้งแต่ LTP เป็นโปรโตคอลแบบ point-to-point การพิจารณาความปลอดภัยของมันจะง่ายกว่า bundle protocol LTP เป็นแบบจำลองบน CCSDS เป็นโปรโตคอลที่ใช้ในการจัดส่งไฟล์และให้บริการอื่นที่คล้ายกัน แต่จะกำหนดไว้ในสไตล์ของอินเทอร์เน็ต ค่อนข้างจะมากกว่าสไตล์ OSI ของรายละเอียด CCSDS ระบุว่า LTP เป็นโปรโตคอลแบบ point-to-point คาดหวังว่าการพิจารณาความปลอดภัยที่มากที่สุดอาจจะได้รับการดูแลที่ชั้นอื่น อย่างใดอย่างหนึ่งข้างต้น LTP หรืออื่นๆใต้ชั้น MAC สำหรับเหตุผลของ LTP ไม่ได้กำหนดกลไกที่เป็นความลับแต่เป็นกลไกที่สมบูรณ์ของข้อมูลเท่านั้น เหตุผลในการรวมทีหลังคือ LTP สามารถนำมาใช้ในสภาพแวดล้อมที่สามารถกระจายผ่านอากาศได้ ในความเป็นจริง การพิจารณาการรักษาความปลอดภัยหลักด้วย LTP หลีกเลี่ยงการขัดขวางหรือก่อกวนระบบเครือข่ายและโดยเฉพาะอย่างยิ่งการโจมตีโดยการปิดเส้นทาง พวกเขาคิดว่ามันเป็นไปได้ การขัดขวางหรือก่อกวนระบบเครือข่ายโดยการปิดเส้นทางสามารถติดตั้งได้ทุกที่ที่มีอินเตอร์เน็ต ยากที่จะติดตามและยังอนุญาตให้ผู้โจมตีเพิ่มระดับที่จะโจมตี การขัดขวางหรือก่อกวนระบบเครือข่ายโดยการปิดเส้นทางสามารถทำลายล้างได้มากสำหรับระบบบนพื้นดิน เช่น LTP ที่เป็นระดับชั้นบนของ IP หรือ UDP และแน่นอนว่าจะให้สำหรับยานอวกาศ

บางคุณสมบัติของ LTP เบื้องต้น ในความเป็นจริงออกแบบให้มีความแข็งแกร่งในการเผชิญกับการขัดขวางหรือก่อกวนระบบเครือข่าย ตัวอย่างเช่น แนะนำการใช้งานของตัวระบุแบบสุ่มแทนที่จะเริ่มต้นนับจาก 1 ฯลฯ และเพื่อให้การขัดขวางหรือก่อกวนระบบเครือข่ายโดยการปิดเส้นทางยากขึ้น LTP ยังมีกลไก cookie ที่ทนต่อความล่าช้าที่สามารถเปิดการคัดเลือก กลไกนี้เป็นหลักในการสร้างสภาพที่ใช้ร่วมกันใหม่ระหว่างเพียร์ที่มีการติดต่อสื่อสารที่สันนิษฐานว่าใช้งานไม่ได้แล้วจากการขัดขวางหรือก่อกวนระบบเครือข่ายโดยการปิดเส้นทาง ทั้งความสมบูรณ์ของข้อมูลและกลไก cookie ที่เป็นส่วนขยายของ LTP และเพื่อให้เป็นตัวเลือกในการดำเนินการ

2. Bundle Protocol Security

bundle protocol เป็นเครือข่ายซ้อนทับ เสี่ยงต่อการถูกโจมตีมากกว่า LTP ตั้งแต่การผสมผสานเทคโนโลยีต่างๆที่มีประสิทธิภาพ (เช่น ต่ำกว่า) ระดับชั้นของโปรโตคอลในการพิจารณาความปลอดภัยสามารถนำมาประยุกต์ใช้กับ bundle protocol ได้

เราได้ให้ภาพรวมของสถานะปัจจุบันของการทำงานเกี่ยวกับการรักษาความปลอดภัยสำหรับเครือข่ายที่ทนต่อความล่าช้าและจดจำนวนของส่วนที่เราต้องการจะได้รับข้อมูลจากผู้เชี่ยวชาญด้านไอทีในภารกิจบนอวกาศที่เป็นไปตามข้อกำหนด เป็นผู้เข้าร่วมในการพัฒนา bundle security protocol คำถามที่จะถามผู้เชี่ยวชาญด้านไอทีในภารกิจบนอวกาศ ดังนี้

ในหน้าของการเชื่อมต่อที่เพิ่มมากขึ้นระหว่างการสื่อสารของยานอวกาศและอินเตอร์เน็ตบนพื้นโลก vpn ชนิดไหนที่จะติดตั้งในภารกิจบนอวกาศ ?

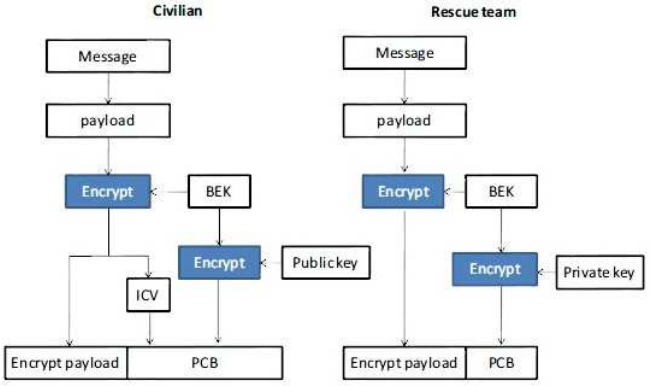
เราหวังว่าได้รับการตอบคำถามเหล่านี้จากผู้เชี่ยวชาญด้านไอทีในภารกิจบนอวกาศ เพื่อจะได้แน่ใจว่ากลไกในการรักษาความปลอดภัยจะตอบสนองความต้องการในภารกิจจริงได้

G. *ปัญหาด้านความปลอดภัยสำหรับ DTN ในสภาวะฉุกเฉิน*

มีคุณสมบัติคล้ายกันเหมือนโทรศัพท์เครือข่ายเฉพาะกิจ เปิดช่องทางและส่งผ่าน multi-hop ทำ DTNs เสี่ยงต่อภัยคุกคามความปลอดภัยต่างๆ ช่องโหว่ความปลอดภัยของเลเยอร์ล่างชั้นบันเดิ้ล เช่น network layer หรือจะมีผลต่อความปลอดภัยของ DTN เป็นคุณลักษณะภาพซ้อนทับของโปรโตคอลบันเดิ้ล ตั้งแต่ปี 2005 DTNRG ได้เริ่มทำงานในข้อกำหนดโปรโตคอลรักษาความปลอดภัยบันเดิ้ล ซึ่งให้ความสมบูรณ์ของข้อมูลและบริการรักษาความลับสำหรับโปรโตคอลบันเดิ้ล สี่บล็อกมากขึ้นมีการกำหนดในบันเดิ้ลสำหรับรักษาความปลอดภัย บล็อกตรวจสอบความถูกต้องบันเดิ้ล (BAB), บล็อกสมบูรณ์ที่สามารถบรรทุกได้ (PIB), บล็อกขยายการรักษาความปลอดภัย (ESB) อย่างไรก็ตาม ยังได้รับการแสดงให้เห็นว่า DTN ยืดหยุ่นต่อการโจมตี โดยเฉพาะอย่างยิ่งถ้าจำลอง DTN เร้าติ้งโปรโตคอลที่ใช้ สำหรับตัวอย่างเช่น รายงานขณะที่โจมตีมีความเสียหาย 20% ของโหนด, 45% ของแพ็คเก็ตถูกส่งเรียบร้อย, เปรียบเทียบกับ 70% เมื่อไม่มีการโจมตีในปัจจุบัน

การประมวลผลและทรัพยากรการจัดเก็บมีจำกัดในโทรศัพท์มือถือ มีความท้าทายมากขึ้นเมื่อใช้การรักาความปลอดภัยในเครือข่ายโทรศัพท์มือถือ

โดยเฉพาะอย่างยิ่งในสถานการณ์ฉุกเฉิน การสื่อสารมักจะจำกัด เนื่องจากโครงสร้างที่มีอยู่ถูกทำลาย หรือเหตุการณ์ที่เกิดขึ้นในพื้นที่นอกเหนือโครงสร้างพื้นฐาน ต่อไปมักจะเป็นไปไม่ได้ที่จะเข้าถึงฐานข้อมูลระยะไกลหรือเซิร์ฟเวอร์รับรอง ในกรณีฉุกเฉิน ปัญหาการรักาความปลอดภัยหลักสำหรับ DTNs เป็นวิธีการที่จะให้บริการเป็นความลับและป้องกันจากการใช้งานที่ไม่ได้รับอนุญาต และการโจมตี สามประเด็นที่จะกล่าวถึงในบทความนี้ 1) ระบุผู้ใช้ 2) การรักษาความลับของข้อความ 3) การจำกัดทรัพยากรการเข้าถึงผู้ใช้ที่ไม่ได้รับอนุญาต และป้องกันการใช้งานที่ได้รับอนุญาตจากการเข้าถึงระดับที่สูงขึ้นของบริการที่พวกเขามีสิทธิ



รูปที่ 17 การเข้ารหัสด้วยกุญแจสาธารณะ

ในกรณีฉุกเฉิน การระบุผู้ส่งเป็นสิ่งจำเป็นมากสำหรับทีมกู้ภัยหรือเจ้าหน้าที่พยาบาล โดยเฉพาะอย่างยิ่งสำหรับการให้บริการการถ่ายทอดข้อมูล การรักษาความลับของข้อความจะปรับตัวตามความต้องการของผู้ใช้ เช่น เพิ่มความต้องการคอมพิวเตอร์และการใช้งานแบตเตอรี่ ในงานวิจัยนี้ PCB ที่ใช้ในการรับมือกับการเข้ารหัสลับ, การป้องกันความสมบูรณ์ และการตรวจสอบ สองกรณีที่จะพิจารณา หนึ่งคือการรักษาความลับของข้อความ เมื่อประชาชนต้องการที่จะส่งข้อความไปยังทีมกู้ภัย และอีกหนึ่งเป็นการระบุผู้ใช้เมื่อทีมกู้ภัยถ่ายทอดข้อมูล รูปแบบการเข้ารหัสข้อความที่แสดงในรูปที่ 4 เมื่อประชาชน (โหนด DTN) ส่งข้อความไปยังทีมกู้ภัยที่จะสามารถเข้ารหัส payload โดยใช้การสุ่มจับ “เซสชัน (session)” กุญแจเข้ารหัสบันเดิ้ล (BEK) และการสร้างแท็กการตรวจสอบ (PCB ค่าตรวจสอบความสมบูรณ์ (ICV) BEK ใช้เพื่อลดความต้องการประมวลผลของการเข้ารหัสกุญแจสาธารณะ (แต่ละกุญแจจะมีความยาว 1024 ถึง 2048 บิต) การสุ่มจับ BEK จะได้รับการเข้ารหัสโดยใช้กุญแจสาธารณะที่เกี่ยวข้องกับทีมกู้ภัย PCB จะถูกส่งไปพร้อมกับการเข้ารหัส payload ซึ่งรวมถึง ICV และการเข้ารหัส BEK ทีมกู้ภัยสามารถถอดรหัส BEK และ payload ซึ่งรับรองความถูกต้องโดยพิสูจน์ทีมกู้ภัยรู้กุญแจส่วนตัวที่เกี่ยวข้อง การป้องกันความสมบูรณ์ที่มีให้โดยการคำนวณ ICV เมื่อทีมกู้ภัยถ่ายทอดข้อมูล กระบวนการคล้ายกันมากยกเว้นพวกเขาใช้กุญแจส่วนตัวในการเข้ารหัส BEK (ลายเซ็นต์ดิจิตอล) เมื่อประชาชนถอดรหัสสำเร็จ ข้อความออกอากาศจะรับรองความถูกต้องและตรวจสอบครบวงจร มีเพียงทีมกู้ภัยเท่านั้นที่รู้กุญแจส่วนตัวที่เกี่ยวข้อง

H. Anonymity and Security in Delay Tolerant Networks

ในเครือข่ายทั่วไปนั้นโดยส่วนมากจะใช้เทคนิคการเข้ารหัสข้อมูลแบบ PKI (Public Key Infrastructure) ซึ่งแต่ละ user จะต้องมีการแจกจ่าย Public key ให้ user อื่นๆเพื่อใช้ในการยืนยันตนลงใน Certificate Authority(CA) ติดต่อสื่อสารกับตน แต่ใน DTN นั้น ยังไม่มีส่วนที่ใช้ในจัดการในเรื่องของ Public Key และ CA การส่งข้อมูลแบบเข้ารหัสด้วยวิธีเดิมจึงไม่สามารถทำได้ในงานวิจัยนี้จึงได้นำวิธีการเข้ารหัสข้อมูลที่เรียกว่า Sakai-Ohgishi-Kasahara (SOK) Key Agreement Scheme มาประยุกต์ใช้ในการติดต่อสื่อสารใน DTN โดยมีขั้นตอนดังนี้

1. การติดตั้งระบบและลงทะเบียนผู้ใช้งาน

ใน SOK นั้นแต่ละ user จะมีการใช้ Private Key Generater สำหรับสร้าง Private key ให้กับตนเอง และแต่ละ user จะสามารถใช้ PKG ในการคำนวนหา Public key ของ user อื่นๆเองได้

ในขั้นตอนการเตรียมการจะมีการแบ่งการสื่อสารออกเป็นสองแบบคือการสื่อสารในระยะไกล้และการสื่อสารระยะไกล โดยแต่ละ user จะมี PKG สองชุดสำหรับการติดต่อสื่อสารทั้งสองแบบ โดย Public key ของ PKG ในระยะไกล้หรือในโดเมนเดียวกันจะเรียกว่า Local key ใช้สำหรับเข้ารหัสเพื่อสื่อสารกับเราท์เตอร์ user อื่นๆในโดเดมนเดียวกัน ส่วน Public key ของ PKG ในการสื่อสารระยะไกลเรียกว่า Long Distance Key จะใช้เข้ารหัสเพื่อสื่อสารปลายทางที่ต้องการ

ในการลงทะเบียนผู้ใช้งานในระบบ DTN นี้ user จะได้รับหมายเลขประจำ user และ PKG ทั้งสองแบบ จากโดเมนที่ตนเองใช้งานอยู่

2. การรักษาความปลอดภัยในการสื่อสาร

ในการรักษาความปลอดภัยของการสื่อสาร ในขั้นตอนแรกแต่ละ user ที่จะสื่อสารกันจะต้องมีการยืนยันตนก่อน โดยแต่ละ user จะใช้ PKG ที่สองแบบที่ได้รับมาทำการสร้าง Public Key ด้วยตัวเองจากค่าพารามิเตอร์ที่กำหนดไว้ใน PKG เช่น Mac Addressของปลายทางเป็นต้น โดยไม่จำเป็นที่จะต้องรอการแจกจ่าย Public Key จากต้นทางเหมือนกับการติดต่อสื่อสารแบบปกติ ซึ่งการใช้ PKG นี้จะทำให้ลดภาระในการติดต่อสื่อสารระหว่างการยืนยันตนนั้นให้น้อยลงได้

หลักจากมีการยืนยันตนเสร็จและได้รับคีย์เรียบร้อยแล้ว ยูสเซอร์หากเป็นการสื่อสารภายในโดเมนเดียวกัน ก็จะใช้ Local Public Key เข้ารหัสข้อมูลเพื่อส่งไปหา user อื่นๆ เมื่อยูสเซอร์นั้นได้รับข้อมูลแล้วก็จะใช้ Private Key ของตนถอดรหัสข้อมูลได้

หากยูสเซอร์ต้องการสื่อสารในระดับนอกโดเมน user จะใช้ Long Distance Key เพื่อเข้ารหัสข้อมูลก่อน จากนั้นก็จะเข้ารหัสด้วย Local Public Key อีกครั้งเพื่อส่งข้อมูลไปหาเราท์เตอร์เพื่อให้เราท์เตอร์ทำการค้นหาเส้นทางและส่งข้อมูลต่อไปจนถึงยูสเซอร์ปลายทาง

I. โครงสร้างแรงจูงใจในการรักษาความปลอดภัยหลายชั้นสำหรับ DTN (SMART)

SMART scheme สามารถใช้กระตุ้นให้เกิดการกำหนดเส้นทางและข้อมูลการส่งต่อใน DTNs ในส่วนนี้เรายังหารือเกี่ยวกับความท้าทายอื่นๆ ที่เกี่ยวข้องกับการออกแบบแรงจูงใจในการรักษาความปลอดภัยใน DTNs

1. การเพิกถอนกุญแจสาธารณะใน DTNs

การจัดการคีย์สาธารณะเป็นรากฐานของโปรโตคอลรักษาความปลอดภัยใดๆ สำหรับโครงสร้างแรงจูงใจในการรักษาความปลอดภัย, ทำงานผิดปกติหรือ โหนดที่เป็นอันตรายจะจ่ายค่าปรับของการเพิกถอนใบรับรองคีย์สาธารณะของเรา แม้สำหรับโหนดเห็นแก่ตัวเหล่านั้นวิ่งออกจากเครดิตของพวกเขา, การกระทำการลงโทษอย่างใดอย่างหนึ่งที่เป็นไปได้คือการยกเลิกใบรับรองของพวกเขา หรือลดสิทธิ CoS โดยการทบทวนใบรับรองของพวกเขา อย่างไรก็ตาม การเพิกถอดคีย์สาธารณะยังคงเป็นความท้าทายที่ดีใน DTNs ในโครงสร้างพื้นฐานของคีย์สาธารณะแบบดั้งเดิม ใบรับรองโครงสร้าง รูปแบบการเพิกถอนใบรับรองทั่วไปส่วนใหญ่จะผ่านรายการเพิกถอนใบรับรอง (CRL) ซึ่งเป็นรายการใบรับรองที่ถูกเพิกถอนที่เก็บไว้ในคลังส่วนกลางจัดทำโดยหน่วยงานรับรอง อย่างไรก็ตามใน DTN โหนดอาจประสบจากความล่าช้า หรือการสูญเสียบ่อยครั้งของการเชื่อมต่อไปยังเซิร์ฟเวอร์ CRL การปรับปรุงการใช้คีย์สาธารณะเป็นระยะเป็นข้อเสนอแนะในการแทนที่การเพิกถอนคีย์สาธารณะแบบดั้งเดิม แม้ว่าในโลกแห่งความเป็นจริง การกระจายคีย์สาธารณะยังเป็นปัญหาที่ท้าทายและอาจนำไปสู่ค่าใช้จ่ายในการจัดการเสริมจำนวนมาก อีกวิธีหนึ่งที่เป็นไปได้ที่จะเพิกถอนคีย์สาธารณะใน DTNs โดยใช้การกระจาย CRL ซึ่งต้องตรวจสอบต่อไปเพื่อหาวิธีปรับปรุง

2. การเข้ากุญแจสาธารณะเมื่อเทียบกับ IBC

การเข้ารหัสตามใบรับรองคีย์สาธารณะแบบดั้งเดิมเป็นเครื่องมือในการเข้ารหัสลับขั้นพื้นฐานที่จะตระหนักถึง SMART scheme วิธีการหนึ่งที่เป็นไปได้เพื่อปรับปรุงประสิทธิภาพของ SMART คือใช้การเข้ารหัสแบบเอกลักษณ์ (IBC) ที่จะออกแบบโปรโตคอลที่ใช้ใบรับรองคีย์สาธารณะปัจจุบัน IBC เป็นวิธีการเข้ารหัสที่ค่อนข้างใหม่ และยังเป็นทางเลือกที่มีประสิทธิภาพเพื่อการเข้ารหัสตามแบบดั้งเดิม แนวคิดหลักคือการทำให้คีย์สาธารณะของกิจการโดยตรงมาจากข้อมูลที่รู้จักกันในสาธารณะ เช่น e-mail address เมื่อเร็วๆนี้ได้มีหลายงานวิจัยที่มีปัญหาการยอมรับของ IBC ตระหนักถึงการตรวจสอบบันเดิ้ลที่มีประสิทธิภาพใน DTNs อย่างไรก็ตาม มันเป็นตรงไปตรงมาในการแปลงใบรับรองคีย์สาธารณะของเรา ดังนั้นการใช้ IBC จะไม่ส่งผลกระทบต่อผลของการวิจัยนี้

ตารางที่ 8 เปรียบเทียบการรักษาความปลอดภัยใน DTN ด้วยเทคนิคแบบต่างๆ

Security of DTN		วิธีการ	ประเภทการถูกโจมตี	เปรียบเทียบ	โปรโตคอล	สภาพแวดล้อม
[1]	Anonymity and Security in Delay Tolerant Networks	มีการเข้ารหัสข้อมูลแบบ SOK	No attack	มีการเปรียบเทียบกับการเข้ารหัสแบบ PKI	ไม่มี	มีผล
[2]	Practical Security for Disconnected Nodes	มีการเข้ารหัสแบบ IBC	redirection attacks, DoS attack	มีการเปรียบเทียบกับการเข้ารหัสแบบ PKI	RTT Protocol	มีผล
[3]	Security Analysis of DTN Architecture and Bundle Protocol Specification for Space-Based Networks	ใช้ข้อมูลการเข้ารหัสลับในการรักษาความปลอดภัย	No attack	ไม่มี	Bundle Protocol	มีผล
[4]	Region-Based Security Architecture for DTN	มีการเข้ารหัสข้อมูลแบบ IBC	No attack	มีการเปรียบเทียบกับการเข้ารหัสแบบ PKI	ไม่มี	มีผล
[5]	Hierarchical Identity Based Cryptography for End-to-End Security in DTNs	มีการเข้ารหัสข้อมูลแบบ IBC	No attack	มีการเปรียบเทียบกับการเข้ารหัสแบบ PKI	BAH, PSH	มีผล
[6]	Secure Network Coding in DTNs	ใช้ลายเซ็นต์เข้ารหัสเครือข่ายความปลอดภัย	pollution attack	มีการเปรียบเทียบกับการเข้ารหัสแบบ PKI	ไม่มี	ไม่มีผล
[7]	Security Considerations in Space and Delay Tolerant Networks	ใช้ข้อมูลการเข้ารหัสลับในการรักษาความปลอดภัย	DoS attack	มีการเปรียบเทียบระหว่างโปรโตคอล LTP และ Bundle Protocol	LTP, Bundle Protocol	มีผล
[8]	Pseudonymised communication in delay tolerant networks	ใช้ CSP ที่มีการคำนวณใหม่โดยใช้ Failure Divergence Model (FDR) สำหรับการเช็ค	DoS attacks, Traffic analysis attack	มีการเปรียบเทียบกับ CSP ที่ยังไม่มีการคำนวณ	TCP/IP protocol, Bundle Protocol	ไม่มี
[9]	Adaptive Service Provisioning for Emergency Communications with DTN	การเข้ารหัส BEK (ลายเซ็นต์ดิจิตอล)	No attack	ไม่มี	Bundle Protocol	ไม่มี
[10]	SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks	SMART scheme, มีการเข้ารหัสข้อมูลแบบ IBC	No attack	มีการเปรียบเทียบกับการเข้ารหัสแบบ PKI	DTN routing protocol, SWB protocol	มีผล
[11]	Queuing Mechanism to Alleviate Flooding Attacks in Probabilistic Delay Tolerant Networks	วิธีการเข้าติดตามคุณสมบัติของความน่าจะเป็น	Flooding attack	มีการเปรียบเทียบกับการเข้ารหัสแบบ PKI	ProPHET	มีผล
[12]	Secure Group Communications for Delay-Tolerant Networks	มีการเข้ารหัสข้อมูลแบบ IBC	No attack	มีการเปรียบเทียบกับการเข้ารหัสแบบเดิม	Bundle Protocol, SGCP, SGA	มีผล

VII. สรุปผลการวิจัย

ในบทความนี้เรามีการนำเสนอการเปรียบเทียบข้อแตกต่างระหว่างโปรโตคอลที่เกี่ยวข้องกับ DTN ได้แก่ DCCP และ SCTP รูปแบบการกำหนดเส้นทางและส่งข้อมูลใน DTN ซึ่งโดยทั่วไปมี 3 รูปแบบด้วยกันคือ แบบกระจายสำเนาข้อมูล, แบบส่งต่อข้อมูล และแบบเข้ารหัส การค้นหาเส้นทางฉวยโอกาสใช้สถานที่ตั้ง, อัตราบิต และการเข้ารหัส ในการเพิ่มประสิทธิภาพในการค้นหาเส้นทาง มีการนำเทคโนโลยีมาใช้ในการทดสอบประสิทธิภาพการทำงานของ Multicasting ใน DTN การรักษาความปลอดภัยใน DTN มีวิธีการป้องกันการถูกโจมตีหลายประเภท จากการเปรียบเทียบด้วยเทคนิคต่างๆ วิธีการที่ดีที่สุดในการรักษาความปลอดภัย คือการเข้ารหัสแบบ IBC

เอกสารอ้างอิง

[1] W.D. Ivancic, “Security analysis of DTN architecture and Bundle Protocol Specification for space-based networks,” in Proc.of 2010 IEEE Aerospace Conference, 2010, pp. 1-12.

[2] M.R. Fida, M. Ali, A. Adnan, A.S. Arsalaan, “Region-Based Security Architecture for DTN,” in Proc.of 2011 Eighth International Conference on Information Technology: New Generations (ITNG), 2011, pp. 387-392.

[3] C. Caini, H. Cruickshank, S. Farrell, M. Marchese, “Delay- and Disruption-Tolerant Networking (DTN): An Alternative Solution for Future Satellite Networking Applications,” in Proc.of IEEE, 2011, pp. 1-18.

[4] L. Czap, I. Vajda, “Secure Network Coding in DTNs,” in Proc.of IEEE Communications Letters, 2011, pp. 28-30.

[5] D. Jingzhe, E. Kranakis, A. Nayak, “Distributed Key Establishment in Disruption Tolerant Location Based Social Wireless Sensor and Actor Network,” in Proc.of 2011 Ninth Annual Communication Networks and Services Research Conference (CNSR), 2011, pp. 109-116.

[6] A. Kate, G. Zaverucha and U. Hengartner, "Anonymity and security in delay tolerant networks", in Proc. of SecureComm 2007 3th International Conference on Security and Privacy in Communications Networks and the Workshops, pp.504-513.

[7] N. Bhutta , G. Ansa , E. Johnson, et.al, " Securty analysis for Delay/Disruption Tolerant satellite and sensor networks", in Proc. of 2009 International Workshop on Satellite and Communications (IWSSC),pp.385-389,Sept 2009.

[8] A. Seth, S. Keshav, "Practical security for disconnected nodes", in Proc. of 1st IEEE ICNP Workshop on Secure Network Protocols, 2005, pp.31-36.

[9] P.T. Edelman, M.J. Doonahoo, D.B. Sturgill, "Secure group communications for Delay-Tolerant Networks", Proc. of International Conference for Internet Technology and Secured Transactions (ICITST),2010,pp.1-8.

[10] E. Kohler, M. Handley, and S. Floyd. Datagram Congestion Control Protocol.

[11] R. Stewart, Q. Xie , K. Morneault , C. Sharp , H. Schwarzbauer , T. Taylor , I. Rytina , M. Kalla , L. Zhang , V. Paxson

[12] V. Cerf , S. Burleigh , A. Hooke , L. Torgerson , R. Durst , K. Scott , K. Fall , H. Weiss , Delay-Tolerant Networking Architecture,RFC4838, Internet Engineering Task Force, April 2007

[13] Kevin Fall, “A Delay-Tolerant Network Architecture for Challenged Internets,” in Proceedings of the ACM SIGCOMM, Karlsruhe, Germany, August 2003.

[14] Xiao Chena, Jian Shenb, Jie Wuc, “Improving routing protocol performance in delay tolerant networks using extended information”, Journal of Systems and Software, 2010, pp. 1301-1309.

[15] Xin Wang, Yantai Shu, Zhigang Jin, Huan Chen, “Directional Forward Routing for Disruption Tolerant Networks”, Proceedings of the 15th Asia-Pacific Conference on Communications, 2009, pp. 355-358.

[16] Chung, K.-C., Li, Y.-C., & Liao, W., “Exploiting Network Coding for Data Forwarding in Delay Tolerant Networks” Vehicular Technology Conference VTC, 2010, pp. 1-5

[17] J. Wu and N. Wang, "A-SMART: A Advanced Controlled-Flooding Routing with Group Structures for Delay Tolerant Networks, " in Proceeding of 2010 Scond Interational Conerence on Network Scurit, Wireless Communications and Trusted Computing, pp. 192-196, 2010.

[18] Lei Yin, Hui-mei Lu and Y. Cao, "A Novel Single Copy Replication Routing Strategy for Delay Tolerant Networks, " in Proceeding of IEEE 2009.

[19] T. Spyropoulos, K. Psounis and C. S. Raghvendra, " Spray and Focus: Efficient Mobility-Assisted Routing for Heterogeneous and Correlated Mobility, " in Proceeding of workhop on PerCom aos, pp. 79-85.,2007.

[20] Evan P.C. Jones and Paul A. S. Ward, "Routing Strategies for Delay - Tolerant Networks," in Joural oj Computer Communication Journal , 2008.

[21] G. Wang, B. Wang, Y. Gao, " Dynamic Spray and Wait Routing Algorithm with Quality of Node in Delay Tolerant Network," in Proceeding of Interational Conerence on Communications and Mobile Computing , published by IEEE Computer SOCiet, pp. 452-456,2010.

[22] Xu Jian-bo, Hou Jia-tao “A New Data Transmission Protocol in Delay Tolerant Mobile Wireless Sensor Networks”, in Proc.of 3rd 2010 International Symposium on Information Processing(ISIP’ 10), 2010, pp. 178-180.

[23] BaiJun Wu, Feng Lin, JiLiu Zhou “Adaptive Routing in Delay-Tolerant Mobile Sensor Network”, in Proc.of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery(CyberC’10), 2010, pp. 79-86.

[24] Jie Li, Yu-gui Qu, Qi-yue Li, Bao-hua Zhao “A queue management MAC protocol for Delay-Tolerant Mobile Sensor Networks”, in Proc.of 2nd International Conference on Advanced Computer Control(ICACC’10), 2010, pp. 426-430.

[25] Hui Li, FaXin, XiaoLin Zhou, Hao Luo “Connections characteristics analysis in delay tolerant mobile networks”, in Proc.of international Conference on Advanced Intelligence and Awarenss Internet (AIAI’10), 2010.

[26] Yu Wang, Hongyi Wu, Ha Dang “Analytic study of Delay/Fault-Tolerant Mobile Sensor Networks (DFT-MSN’s)”, in Proc.of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks & Workshop (WoWMoM’09), 2009.

[27] Yong Li, Yurong Jiang, Depeng Jin, Li Su, Lieguang Zeng, Dapeng Wu “Energy-Efficient Optimal Opportunistic Forwarding for Delay-Tolerant Networks”, in Proc.of IEEE Transactions on Vehicular Technology, 2010, pp. 4500-4512.

[28] LEI YIN, HUI-MEI LU,KE LONG, YUAN-DA CAO, “A FLEXIBLE MULTICAST ROUTING SCHEME FOR MULTICASTING IN DELAY TOLERANT NETWORKS,” IN PROC.OF FOURTH INTERNATIONAL CONFERENCE COMMUNICATIONS AND NETWORKING IN CHINA, 2009.

[29] LEE U, SOON YOUNG OH, KANG-WON LEE, GERLA M, “RELAYCAST: SCALABLE MULTICAST ROUTING IN DELAY TOLERANT NETWORKS,” IN PROC.OF IEEE INTERNATIONAL CONFERENCE ON NETWORK PROTOCOLS (ICNP), PP 218-227, 2008.

[30] ABDULLA M, SIMON R, “CONTROLLED EPIDEMIC ROUTING FOR MULTICAST IN DELAY TOLERANT NETWORKS,” IN PROC.OF IEEE MODELING ANALYSIS AND SIMULATION OF COMPUTERS AND TELECOMMUNICATION SYSTEMS (MASCOTS), PP 1-10, 2008.

[31] JIE WU, YUNSHENG WANG, “A NON-REPLICATION MULTICASTING SCHEME IN DELAY TOLERANT NETWORKS,” IN PROC.OF IEEE INTERNATIONAL CONFERENCE MOBILE ADHOC AND SENSOR SYSTEMS (MASS), PP 89-98, 2010.

[32] NARMAWALA Z, SRIVASTAVA S, “MIDTONE: MULTICAST IN DELAY TOLERANT NETWORKS,” FOURTH INTERNATIONAL CONFERENCE ON COMMUNICATIONS AND NETWORKING IN CHINA, PP 1-8, 2009.

[33] W. Zhao, M. Ammar and E. Zegura, “Multicasting in delay tolerant networks:semantic models and routing algorithms”, in Proc. SIGCCOM Workshop in DTN, pp.268-275, 2005.

[34] Abdulla M, Simon R, "A Simulation Analysis of Multicasting in Delay Tolerant Networks", in Proc Of Winter Simulation Conference (WSC), pp.2234-2241, 2006.

[35] Lei Yin, Hui-mei Lu, Ke Long, Yuan-da Cao, "A Flexible Multicast Routing Scheme for Multicasting in Delay Tolerant Networks", in Proc Of Comunications and Networking Fourth International Conference, 2009

[36] Lei Yin, Yuan-da Cao, Ke Long, "Delay Modeling and Analysis in DTN Multicasting", in Proc Of International Colloquium Computing Communication Control, pp.177-181, 2009.

[37] Kuang Zhufang, "An Multicast Routing Based on Ant Colony Optimization Algorithm for DTN", International Conference Genetic and Evolutionary Computing(ICGEC), 2010.

[38] Jie Wu, Yunsheng Wang, "A Non-Replication Multicasting Scheme in Delay Tolerant Networks", in Proc Of International Conference on Mobile Adhoc and Sensor Systems (MASS), pp.89-98, 2010.

[39] Zhigang Jin, Jia Wang, Sainan Zhang, Yantai Shu, "Epidemic-Based Controlled Flooding and Adaptive Multicast for Delay Tolerant Networks", in Proc Of Ubiquitous Intelligence & Computing International Conference on Autonomic & Trusted Computing (UIC/ATC), 2010.

[40] Kuang Zhufang, "An Multicast Routing Based On Ant Colony Optimization Algorithm for DTN", in Proc Of Fourth International Conference on Genetic and Evolutionary Computing, 2010.

[41] Minghui Ma, Zhaoxiang Zhang, Xudong An, Chao Li, Yuanda Cao, "Probability and Receiver List Based Multicast Routing in DTNs", in Proc Of International Conference on Advanced Communication Technology (ICACT), 2010.

[42] Yunsheng Wang, Xiaoguang Li, Jie Wu, "Multicasting in Delay Tolerant Networks: Delegation Forwarding", in Proc Of IEEE Global Telecommunications Conference, 2010.

[43] Young Li, Guolong Su, Wu D.O, Depeng Jin, Li Su, Lieguang Zeng, "Teh Impact of Node Selfishness on Multicasting in Delay Tolerant Networks", in Proc Of IEEE Transactions Vehicular Technology, 2011.

[44] N. Ahmad, H. Cruickshank, S. Zhili and M. Asif, "Pseudonymised communication in delay tolerant networks," in Proc.of 2011 Ninth Annual International Conference on Privacy, Security and Trust (PST), 2011, pp.1-6.

[45] J. Peng, J. Bigham, and E. Bodanese, “Adaptive Service Provisioning for Emergency Communications with DTN,” in Proc.of 2011 IEEE Wireless Communications and Networking Conference (WCNC), 2011, pp.2125-2130.

[46] Z. Haojin, L. Xiaodong, L. Rongxing , F. Yanfei Fan and S. Xuemin Shen, “SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks,” in Proc.of IEEE Transactions on Vehicular Technology, 2011, pp.4628-4639.

[47] P.T. Edelman, M.J. Doonahoo, D.B. Sturgill, "Secure group communications for Delay-Tolerant Networks", Proc. of International Conference for Internet Technology and Secured Transactions (ICITST),2010,pp.1-8.

[48] A. Seth, S. Keshav, "Practical security for disconnected nodes" in Proc. of 1st IEEE ICNP Workshop on Secure Network Protocols, 2005, pp.31-36.

[49] W.D. Ivancic, “Security analysis of DTN architecture and Bundle Protocol Specification for space-based networks,” in Proc.of 2010 IEEE Aerospace onference, 2010, pp. 1-12.

[50] M.R. Fida, M. Ali, A. Adnan, A.S. Arsalaan, “Region-Based Security Architecture for DTN,” in Proc.of 2011 Eighth International Conference on Information Technology: New Generations (ITNG), 2011, pp. 387-392.

[51] R.Patra,S.Surana and S.Nedevschi, "Hierarchical Identity Based Cryptography for End-to-End Security in DTNs",in Proc.of 4th International Conference on Intelligent Computer Communication and Processing,pp.223 - 230,2008

[52] Feng Cheng Lee, Weihan Goh and Chai Kiat Yeo, "A Queuing Mechanism to Alleviate Flooding Attacks in Probabilistic Delay Tolerant Networks ", Telecommunications (AICT), 2010 Sixth Advanced International Conference on, 2010, pp. 329 - 334.

[53] Kate, Aniket, Zaverucha Gregory M. and Hengartner Urs, "Anonymity and security in delay tolerant networks", Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on , 2007, pp.504 - 513.

[54] Czap L.,Vajda I., "Secure Network Coding in DTNs ", Communications Letters, IEEE, 2011, pp.28 - 30.

[55] Farrell S. Cahill V., “Security considerations in space and delay tolerant networks”, Space Mission Challenges for Information Technology, 2006. SMC-IT 2006. Second IEEE International Conference on, 2006, pp.8 – 38.

[56] Internet Research Task Force, http://www.irtf.org/.

[57] Delay Tolerant Networking Research Group, http://www.dtnrg.org/.

[58] Cecilia Mascolo, Mirco Musolesi. SCAR: Context aware Adaptive Routing in Delay Tolerant Mobile Sensor Networks. IWCMC’06, July 3–6, 2006.

[59] Wang Y, Wu HY. Replication-Based efficient data delivery scheme (RED) for delay/fault-tolerant mobile sensor network (DFT-MSN). In: Gregori E, ed. Proc. of the 4th Annual IEEE Int’l Conf. on Pervasive Computing and Communications Workshops. Washington: IEEE Computer Society Press, 2006. 485-489.

[60] Wang Y, Wu HY, Dang H, Lin F. Analytic, simulation, and empirical evaluation of delay/fault-tolerant mobile sensor networks. IEEE Trans. on Wireless Communications, 2007,1(11):3287-3296.