SAC-01-001

ระบบจำลองการจัดการเครือข่ายสำหรับการกระจายกุญแจเชิงควอนตัม ในชนบทและพื้นที่ห่างไกลของประเทศไทย

Network Management System Simulation for Quantum Key Distribution in Rural and Remote Thai Broadband Environments

ปิยะ เตชะธีราวัฒน์*
Piya Techateerawat*
ภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยธรรมศาสตร์
Department of Electrical and Computer Engineering
Faculty of Engineering, Thammasat University
tpiya@engr.tu.ac.th

บทคัดย่อ

การกระจายกุญแจเชิงควอนตัม (Quantum Key Distribution: QKD) ได้รับการพัฒนาขึ้นเพื่อปรับปรุงความปลอดภัยของเครือข่ายในด้านการแลกเปลี่ยนกุญแจ แม้ว่าจะมีการนำอุปกรณ์เครือข่าย QKD มาใช้งานประสบความสำเร็จหลายครั้ง แต่การกระจายกุญแจยังคงจำกัดอยู่ในขอบเขตแบบจุดต่อจุด ในบทความนี้ ได้ทำการจำลองเครือข่ายการเข้ารหัสเชิงควอนตัมโดยอ้างอิงจากบริการบรอดแบนด์จริงในประเทศไทย เพื่อขยายขีดความสามารถของจำนวนผู้ใช้ในเครือข่ายการเข้ารหัสเชิงควอนตัมในปัจจุบันจากแบบจุดต่อจุดไปสู่เครือข่ายผู้ใช้หลายคน และยังคงรักษาความปลอดภัยของเครือข่ายไว้ได้ ระบบที่พัฒนาขึ้นนี้ถูกนำมาใช้งานโดยอิงจากการเข้ารหัสเชิงควอนตัมที่มีอยู่เดิม โดยการจัดการการจับคู่ของระบบ QKD และข้อมูลจริงของโครงสร้างพื้นฐานและบริการในส่วน "ไมล์สุดท้าย" (Last-Mile) ของการพัฒนาบรอดแบนด์ในพื้นที่ชนบทและพื้นที่ห่างไกลของประเทศไทย ผลการจำลองแสดงให้เห็นถึงความเป็นไปได้ในการนำแนวคิดที่เสนอไปใช้งานจริง

คำสำคัญ: การกระจายกุญแจเชิงควอนตัม QKD การเข้ารหัสและความปลอดภัย

Abstract

This paper simulates a multi-user Quantum Key Distribution (QKD) network leveraging existing QKD systems and real-world last-mile broadband infrastructure in rural Thailand. Moving beyond traditional point-to-point limitations, our model demonstrates a feasible approach to scaling secure key exchange for a broader user base while maintaining network security. The simulation results validate the proposed system's practical implementation, showcasing a significant step towards widespread, secure quantum communication.

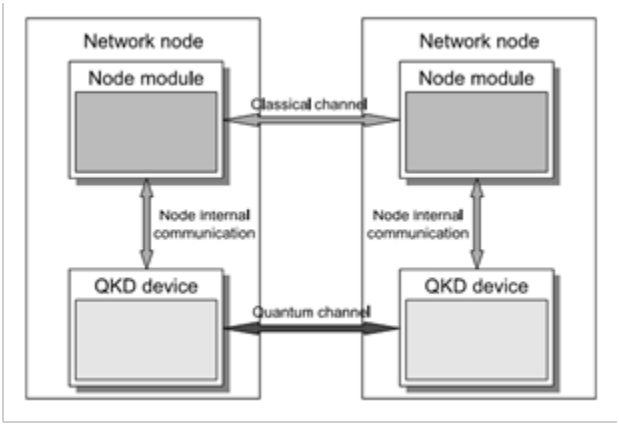
Keywords: Quantum Key Distribution, QKD, Cryptography and Security

บทนำ

การกระจายกุญแจเป็นขั้นตอนเริ่มต้นของพิธีสารความปลอดภัยหลายอย่างที่ให้บริการกุญแจแก่โฮสต์เฉพาะอย่างปลอดภัยปัจจุบัน การเข้ารหัสถูกนำมาใช้เพื่อรับรองความลับและความสมบูรณ์ของการกระจายกุญแจ โดยการกระจายกุญแจทั้งหมดอิงกับการเข้ารหัสทางคณิตศาสตร์ (Denning, 1945) อย่างไรก็ตาม มีการนำเสนอวิธีการกระจายกุญแจทางเลือกโดยใช้การเข้ารหัสเชิงควอนตัม ซึ่งสามารถรับรองความลับของกุญแจที่ส่งผ่านได้โดยอาศัยคุณสมบัติของควอนตัม เนื่องจากควอนตัมไม่สามารถถูกดักจับหรือสร้างขึ้นใหม่ได้ การกระจายกุญแจจึงได้นำคุณสมบัตินี้มาใช้เพื่อพัฒนาระบบการกระจายกุญแจเชิงควอนตัม (Quantum Key

Distribution: QKD) (Bennett & Brassard, 1984 และ Elliott et al., 2003) ช่องสัญญาณของระบบเครือข่ายการสื่อสารเชิงควอนตัมแบ่งออกเป็น 2 ช่อง คือ ช่องสัญญาณสาธารณะ และช่องสัญญาณควอนตัม ช่องสัญญาณสาธารณะใช้สำหรับแลกเปลี่ยนข้อมูลที่เข้ารหัส และช่องสัญญาณควอนตัมใช้สำหรับส่งกุญแจหรือ QKD ดังแสดงในภาพที่ 1 ข้อจำกัดของ QKD คือ การส่งผ่านข้อมูลจะจำกัดอยู่แค่ระหว่างสองโหนดเท่านั้น หรือเป็นการเชื่อมต่อแบบจุดต่อจุด ปัจจุบันมีการวิจัยที่นำเสนอวิธีการหลายอย่าง แต่ส่วนใหญ่เน้นไปที่ชั้นกายภาพ เช่น เราเตอร์ควอนตัมที่สามารถกำหนดเส้นทางสัญญาณควอนตัมได้ แต่มีความท้าทายในเรื่องการสูญเสียข้อมูล จำนวนการเชื่อมต่อ และระยะทาง (Lüthenhaus และ Zhang et al., 2006) ด้วยเหตุนี้ วัตถุประสงค์ของการวิจัยนี้คือการพัฒนาระบบการจัดการเครือข่ายสำหรับ QKD โดยอิงจากโครงสร้างพื้นฐานจริง ซึ่งจะช่วยขยายขีดความสามารถในการใช้ QKD เป็นเครือข่าย รวมถึงความสะดวกในการจัดการและต้นทุนที่ค่อนข้างต่ำ

การเข้ารหัสเชิงควอนตัม

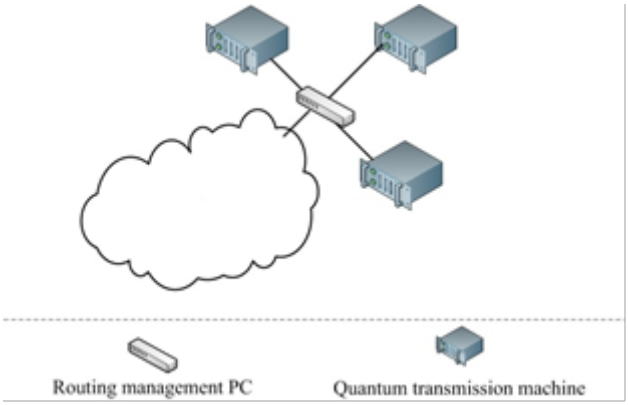


ภาพที่ 1 การสื่อสารข้อมูลในระบบ QKD

การเข้ารหัสเชิงควอนตัมประกอบด้วยระบบการกระจายกุญแจที่ใช้กฎของกลศาสตร์ควอนตัมเพื่อรับประกันการสื่อสารที่ปลอดภัย องค์ประกอบสำคัญของกลศาสตร์ควอนตัม เช่น หลักการความไม่แน่นอนของไฮเซนเบิร์ก ป้องกันไม่ให้ใครก็ตามวัดค่าบิตโดยตรงโดยไม่ทำให้เกิดข้อผิดพลาดที่สามารถตรวจจับได้ โฟตอนเดี่ยวไม่สามารถแบ่งแยกได้ ซึ่งหมายความว่าผู้ดักฟังไม่สามารถแยกสัญญาณควอนตัมเพื่อทำการวัดอย่างลับๆ ได้ การเข้ารหัสเชิงควอนตัมมีทฤษฎีการไม่สามารถโคลนควอนตัมได้ ทฤษฎีนี้แสดงให้เห็นว่าไม่สามารถรับโฟตอนเดี่ยวและทำซ้ำโฟตอนได้โดยไม่แจ้งให้ผู้อื่นทราบ มีสองโปรโตคอลหลักสำหรับการกระจายกุญแจเชิงควอนตัมได้แก่ โปรโตคอล BB84 และโปรโตคอล B92 (Heisenberg, 1927, Eli & Shamir, 1993 และ Ferguson et al., 2001)

โปรโตคอล BB84 (Bennett & Brassard, 1984) เป็นโปรโตคอลการเข้ารหัสเชิงควอนตัมแรกที่เสนอโดย Charles Bennett และ Gilles Brassard ในปี 1984 โปรโตคอลนี้ใช้ฐานโพลาไรเซชันสองฐานของโฟตอนเดี่ยว ได้แก่ ฐานแบบเส้นตรงและฐานแบบทแยงมุม โฟตอนเดี่ยวอาจมีสถานะโพลาไรเซชันสี่สถานะ: แนวนอน (|h>), แนวตั้ง (|v>), วงกลมซ้าย (|lcp>) และวงกลมขวา (|rcp>) สถานะโพลาไรเซชันแนวนอน (|h>) และวงกลมซ้าย (|lcp>) แสดงถึง '0' สถานะโพลาไรเซชันแนวตั้ง (|v>) และวงกลมขวา (|rcp>) แสดงถึง '1'

โปรโตคอล B92 (Bennett & Brassard, 1992) ที่เสนอโดย Charles Bennett และ Gilles Brassard ในปี 1992 คล้ายกับโปรโตคอล BB84 แต่ใช้เพียงสองสถานะควอนตัมที่ไม่ตั้งฉากกัน คือ |h> แทน '0' และ |rcp> แทน '1' ซึ่งเป็นครึ่งหนึ่งของโปรโตคอล BB84 ในการส่งกุญแจ

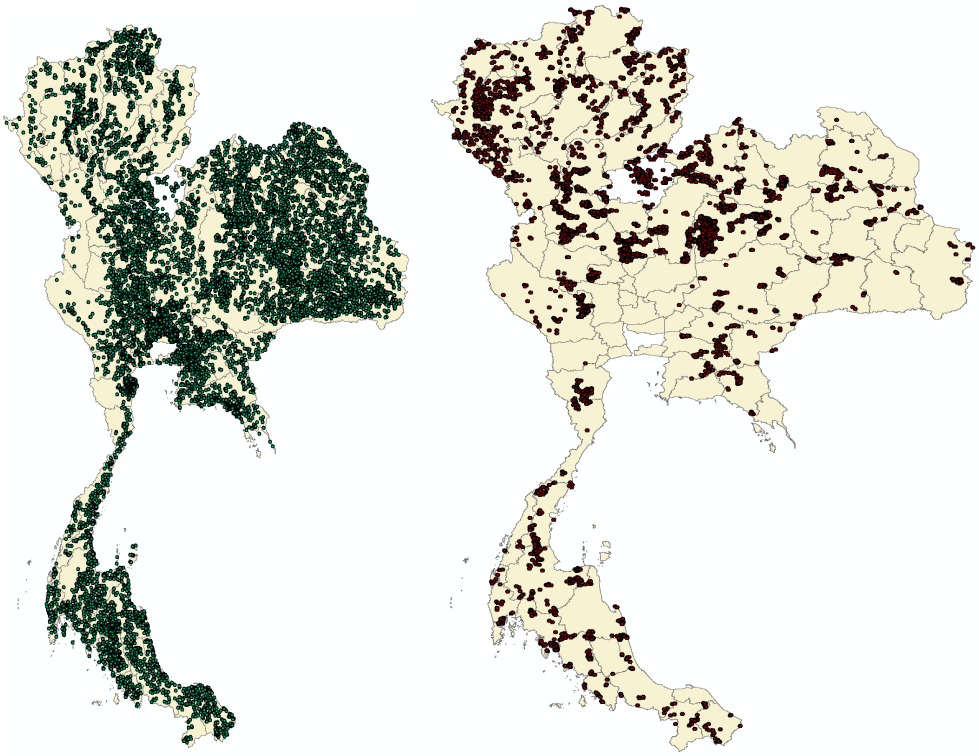


ภาพที่ 2 การออกแบบระบบ

บรอดแบนด์ในพื้นที่ชนบทและพื้นที่ห่างไกลในประเทศไทย

ในบทความนี้ การจำลองจะอิงจากโครงสร้างพื้นฐานจริงของบรอดแบนด์ชนบทในประเทศไทย ซึ่งให้บริการเทคโนโลยี "ไมล์สุดท้าย" (Last-Mile) สำหรับหมู่บ้านชนบท 15,732 แห่ง (โซน C) และหมู่บ้านห่างไกล 3,920 แห่ง (โซน C+) ที่ดำเนินการโดยคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) บทความนี้แสดงให้เห็นเทคโนโลยี "ไมล์สุดท้าย" ที่ปรับแต่งใหม่ซึ่งเหมาะสมกับพื้นที่ประเภทนี้ เทคโนโลยีเหล่านี้มีเป้าหมายเพื่อเป็นฐานในการสร้างระบบระดับภูมิภาคสำหรับการกระจายการเข้าถึงบรอดแบนด์ในหมู่บ้านชนบท 15,732 แห่ง และการเข้าถึงบรอดแบนด์/มือถือในพื้นที่ห่างไกล 3,920 แห่งทั่วประเทศ ดังแสดงในภาพที่ 3 ข้อสังเกตคือ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES) เป็นผู้รับผิดชอบการดำเนินการบรอดแบนด์ในหมู่บ้านชนบทที่เหลือ (24,700 หมู่บ้าน)

ข้อมูลบรอดแบนด์ที่นำเสนอในบทความนี้เป็นการดำเนินการ "ไมล์สุดท้าย" สำหรับหมู่บ้านห่างไกล 3,920 แห่งในประเทศไทย โดย กสทช. การพัฒนาและดำเนินการบรอดแบนด์นี้มีวัตถุประสงค์เพื่อ 1) ให้บริการอินเทอร์เน็ตความเร็วสูงในพื้นที่ 2) ขยายโครงสร้างพื้นฐานและบริการไปยังพื้นที่เพื่อให้ประชาชนในพื้นที่ห่างไกลสามารถเข้าถึงเทคโนโลยีดิจิทัลและข้อมูลได้อย่างเท่าเทียมกัน 3) สร้างสิ่งที่เรียกว่าเศรษฐกิจและสังคมดิจิทัลในพื้นที่ และ 4) ยกเครื่องเทคโนโลยีและบริการดิจิทัลสำหรับพื้นที่ หมู่บ้านห่างไกลที่ดำเนินการแล้ว 3,920 แห่งกระจายอยู่ในทุกพื้นที่ห่างไกลในประเทศไทยดังแสดงในภาพที่ 3 ส่วนใหญ่จะอยู่ในภาคเหนือของประเทศไทย ซึ่งเป็นพื้นที่ภูเขาที่มีภูเขาสูงขนานกับหุบเขาแม่น้ำที่ลาดชันและพื้นที่สูงซึ่งล้อมรอบที่ราบลุ่มภาคกลาง ในขณะที่หมู่บ้านชนบท 15,732 แห่ง (รายละเอียดแสดงในตารางที่ 1) กระจายอยู่ทั่วประเทศมากกว่า และส่วนใหญ่เข้าถึงได้ง่ายกว่าเมื่อเทียบกับพื้นที่ห่างไกล อย่างไรก็ตามมีประมาณ 20-30% ของพื้นที่ที่มีข้อจำกัดเช่นเดียวกับพื้นที่ห่างไกล



Zone C Zone C+

ภาพที่ 3 โครงสร้างพื้นฐานบรอดแบนด์: หมู่บ้านชนบท (โซน C) และหมู่บ้านห่างไกล (โซน C+)

ตารางที่ 1:
ข้อมูลเชิงพรรณนาของหมู่บ้านชนบทและหมู่บ้านห่างไกล (เก็บจากข้อมูลสำรวจของ กสทช.)

Area: Zone C	Targeted villages	Approximate population	Average population per village	no. of Teachers	no. of Students
North	4,140	2,460,432	594	19,716	241,340
South	2,052	1,713,722	835	14,288	182,610
Central and East	3,367	2,202,084	654	18,489	239,028
North-East	6,173	3,823,091	619	29,559	392,074
Total	**15,732**	**10,199,329**	**648**	**82,052**	**1,055,052**

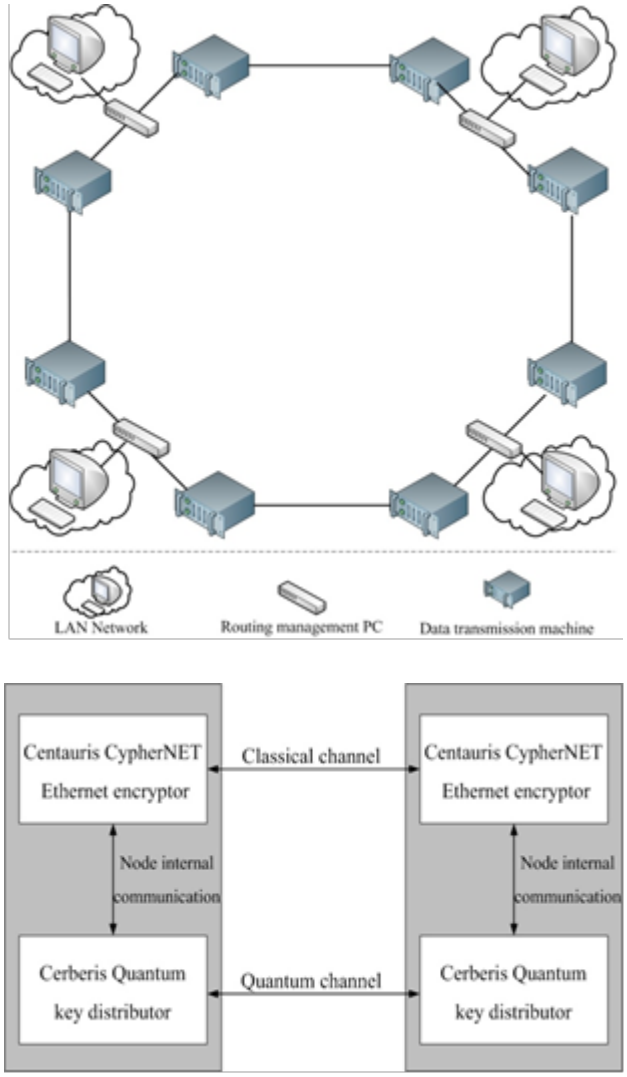
Area: Zone C+	Targeted villages	Approximate population	Average population per village	no. of Teachers	no. of Students
North	2,027	868,041	428	11,351	148,760
South	459	239,526	522	2,757	33,919
Central and East	349	182,122	522	1,755	27,237
North-East	1,085	534,209	492	5,120	66,473
Total	**3,920**	**1,823,898**	**465**	**20,983**	**276,389**

ระบบจัดการสำหรับการกระจายกุญแจเชิงควอนตัม (QKD)

ระบบของเราถูกออกแบบมาบน Application Layer เพื่อรองรับการเชื่อมต่อ ความสะดวก และต้นทุนที่เหมาะสม เราสันนิษฐานว่าเครื่อง QKD แต่ละเครื่องเป็นโฮสต์ที่เชื่อถือได้ และระบบของเรามีการป้องกันทางกายภาพจากการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งอิงตามเครือข่ายที่มีโครงสร้าง (Gisin et al., 2002 และ Steenstrup, 1995) เครื่องส่งสัญญาณควอนตัมใช้โปรโตคอล BB84 เป็นโปรโตคอลเริ่มต้น

ฮาร์ดแวร์

จากการเชื่อมต่อทางกายภาพ มี 3 ส่วนหลัก ได้แก่ 1) กลุ่มเครือข่าย 2) เครื่องคอมพิวเตอร์จัดการเส้นทาง 3) เครื่องส่งข้อมูล ดังแสดงในภาพที่ 2 ในระบบของเรา เราใช้ฮาร์ดแวร์การเข้ารหัสและฮาร์ดแวร์การกระจายกุญแจเชิงควอนตัม ดังนั้นแต่ละกลุ่มเครือข่ายจึงเชื่อมต่อกับเครื่องคอมพิวเตอร์จัดการเส้นทาง จากนั้นจึงเชื่อมต่อไปยังเครื่องส่งข้อมูล ดังแสดงในภาพที่ 4 สำหรับส่วนการกำหนดเส้นทางแพ็กเกจ เราออกแบบและพัฒนาระบบของเราโดยใช้ซอฟต์แวร์โอเพนซอร์สและไลบรารีที่จำเป็น และติดตั้งลงในเครื่องคอมพิวเตอร์จัดการเส้นทาง

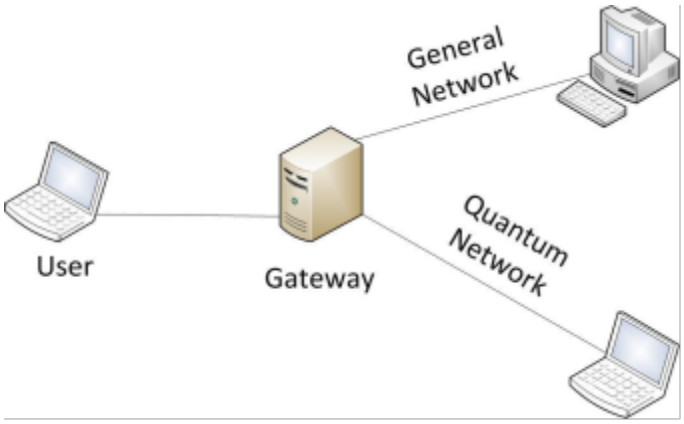


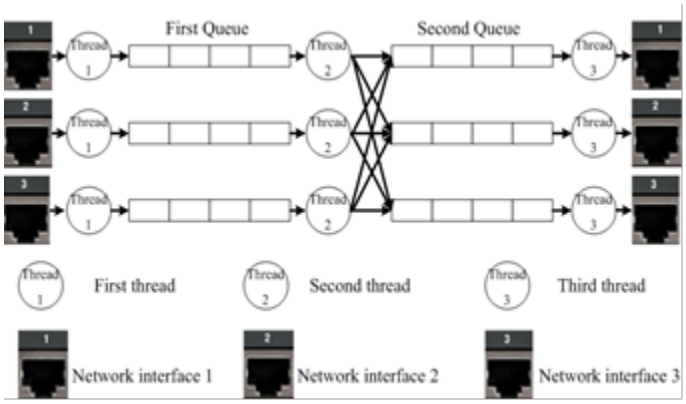
ภาพที่ 4 การเชื่อมต่อเครือข่ายในการทดสอบและโครงสร้างเส้นทางการส่งข้อมูล

ซอฟต์แวร์

ในระบบ ซอฟต์แวร์การจัดการถูกติดตั้งบนคอมพิวเตอร์จัดการเส้นทาง ซอฟต์แวร์การตัดสินใจในการกำหนดเส้นทางได้รับการพัฒนาบน Linux Ubuntu 9.04, Netbeans IDE 6.7.1, ไลบรารี JNetPCap และ iproute2

ซอฟต์แวร์ควบคุมแบ่งออกเป็นสองส่วนหลัก: 1) ซอฟต์แวร์การเลือกเส้นทาง 2) ซอฟต์แวร์การกำหนดเส้นทาง ซอฟต์แวร์การเลือกเส้นทางเป็นส่วนแรกที่แพ็กเกจจะถูกกรอง โดยจะคัดกรองเฉพาะแพ็กเกจที่ปลอดภัยเท่านั้นที่จะผ่านระบบ QKD และยังตรวจสอบว่าแพ็กเกจที่ปลอดภัยมาจากอินเทอร์เฟซที่เหมาะสม วิธีการหลักคือการแยกแพ็กเกจที่ปลอดภัยไปยังระบบ QKD และปล่อยให้แพ็กเกจที่ไม่ปลอดภัยไปยังเครือข่ายทั่วไปดังแสดงในภาพที่ 5 ซอฟต์แวร์การกำหนดเส้นทางเป็นส่วนภายในสำหรับระบบ QKD ซึ่งเกี่ยวข้องกับเฉพาะแพ็กเกจที่ปลอดภัยที่เลือกไว้ซึ่งเดินทางในระบบ QKD การทำงานหลักคือการกำหนดเส้นทางแพ็กเกจที่ปลอดภัยและจัดการคิวและบัฟเฟอร์





ภาพที่ 5 การคัดกรองแพ็กเกจสำหรับระบบ QKD และระบบคิวและบัฟเฟอร์

การทำงาน

การทำงานของระบบบนเครื่องคอมพิวเตอร์จัดการเส้นทางคือการกรองและกำหนดเส้นทางแพ็กเกจไปยังปลายทางที่เหมาะสมในระบบ แต่ละงานจะถูกแยกออกเป็นเธรด ในแต่ละเธรด คิวจะถูกสร้างขึ้นเพื่อรองรับการจัดเก็บและการจัดคิวแบบเข้าก่อนออกก่อน (FIFO) ดังแสดงในภาพที่ 5

ระบบนี้ต้องการให้แพ็กเกจถูกห่อหุ้มด้วยเฮดเดอร์ใหม่เพื่อประโยชน์หลักสองประการในระบบ QKD ของเรา ประการแรกคือการใช้เฮดเดอร์ใหม่นี้เพื่อรองรับเครือข่าย QKD ของเรา การกำหนดเส้นทางสามารถเปลี่ยนเส้นทางได้เร็วขึ้นในเครือข่ายที่กำหนดไว้ของเรา ประการที่สองคือการรับประกันว่าแพ็กเกจที่ปลอดภัยจะเดินทางในเครือข่าย QKD ที่ปลอดภัยของเราเท่านั้น

คิวถูกสร้างขึ้นเพื่อรองรับแต่ละอินเทอร์เฟซแยกกัน มีคิวสองส่วนในระบบของเราและแต่ละคิวมีหน้าที่ของตนเอง คิวแรกคือบัฟเฟอร์สำหรับรับแพ็กเกจ คิวที่สองคือบัฟเฟอร์สำหรับส่งแพ็กเกจ

เธรดของระบบการจัดการถูกแยกออกเป็น 3 ส่วนตามงาน เธรดแรกจัดการแพ็กเกจที่เข้ามาจากอินเทอร์เฟซของตัวเองและใส่แพ็กเกจที่ถูกจับลงในคิวแรก เธรดที่สองนำแพ็กเกจออกจากคิวแรก ค้นหาปลายทางของพวกมัน จากนั้นแทนที่เฮดเดอร์ Ethernet ด้วยเฮดเดอร์ที่เหมาะสมและแทรกแพ็กเกจที่แก้ไขแล้วลงในคิวที่สอง เธรดที่สามนำแพ็กเกจออกจากคิวที่สองและส่งแพ็กเกจไปยังอินเทอร์เฟซที่เกี่ยวข้อง

การดำเนินการและบริการบรอดแบนด์

สำหรับหมู่บ้านห่างไกล หมู่บ้านส่วนใหญ่ตั้งอยู่บนภูเขาหรือล้อมรอบด้วยภูเขา จากตารางที่ 1 มีประชากรรวมประมาณ 1,823,898 คน โดยมีประชากรเฉลี่ย 465 คนต่อหมู่บ้าน ตำแหน่งของครัวเรือนกระจัดกระจายและไม่สม่ำเสมอ บางแห่งอาจพบเป็นกลุ่มครัวเรือนเฉลี่ย 20-30 ครัวเรือน ในขณะที่สำหรับพื้นที่ชนบท จากตารางที่ 1 มีประชากรรวมประมาณ 10,199,329 คน โดยมีประชากรเฉลี่ย 648 คนต่อหมู่บ้าน โดยสรุป หมู่บ้านห่างไกลเป็นพื้นที่ที่มีความหนาแน่นต่ำมาก ในขณะที่หมู่บ้านชนบทเป็นพื้นที่ที่มีความหนาแน่นของที่อยู่อาศัยกระจัดกระจาย ดังแสดงในภาพที่ 6 ตามลำดับ ในการดำเนินการ "ไมล์สุดท้าย" สำหรับพื้นที่ทั้งสองประเภท ตำแหน่งชนบท/ห่างไกลเชิงพรรณนาอาจทำให้ต้นทุนรวมในการเป็นเจ้าของสูงขึ้นอย่างมีนัยสำคัญในแง่ของการขนส่งและการบำรุงรักษา รวมถึงค่าแรงและค่าก่อสร้าง แม้ว่าราคาฮาร์ดแวร์และซอฟต์แวร์จะลดลงก็ตาม

ภาพที่ 6 หมู่บ้านห่างไกลทางภาคเหนือของประเทศไทย

การไม่พร้อมใช้งานของแหล่งจ่ายไฟที่เชื่อถือได้

การพัฒนาแหล่งจ่ายไฟจากระบบโครงข่ายไฟฟ้าที่เชื่อถือได้ในประเทศไทยยังไม่รวดเร็วเท่ากับการแพร่กระจายของโครงสร้างพื้นฐานโทรคมนาคมและบรอดแบนด์ โดยเฉพาะในพื้นที่ห่างไกล ประมาณ 5-10% ของหมู่บ้าน 3,920 แห่งไม่มีไฟฟ้าใช้เลย หรือมีแหล่งจ่ายไฟไม่เพียงพอ ในกรณีนี้ แหล่งจ่ายไฟสำรอง เช่น พลังงานแสงอาทิตย์ ถูกพิจารณาให้เป็นแหล่งพลังงานที่พึ่งพาตนเองได้และสามารถจ่ายไฟให้กับอุปกรณ์บรอดแบนด์และมือถือได้ อย่างไรก็ตาม จากข้อมูลการสำรวจของเรา พบว่ามีพื้นที่ชนบทเพียง 1-2% เท่านั้นที่มีข้อจำกัดด้านพลังงานดังกล่าว

ประเด็นโครงสร้างพื้นฐาน

ดังที่เห็น การเติบโตของการเข้าถึงบรอดแบนด์ในพื้นที่ห่างไกลเป็นหนึ่งในความท้าทาย เนื่องจากโครงสร้างพื้นฐานหรือโครงข่ายเชื่อมโยงกลับ (Backhaul) ไม่เพียงพอ การติดตั้งโครงสร้างพื้นฐานบรอดแบนด์หรือมือถือในพื้นที่ห่างไกลต้องใช้ผู้เชี่ยวชาญมากขึ้นและมีต้นทุนรวมในการเป็นเจ้าของสูงขึ้น ซึ่งผู้ให้บริการเครือข่ายเอกชนไม่น่าจะคุ้มค่ากับการลงทุนในเครือข่ายระยะไกลที่มีความหนาแน่นของประชากรต่ำ (Hollifield & Donnermeyer, 2003) ดังนั้น การดำเนินการ "ไมล์สุดท้าย" ควรมีความน่าเชื่อถือ ราคาไม่

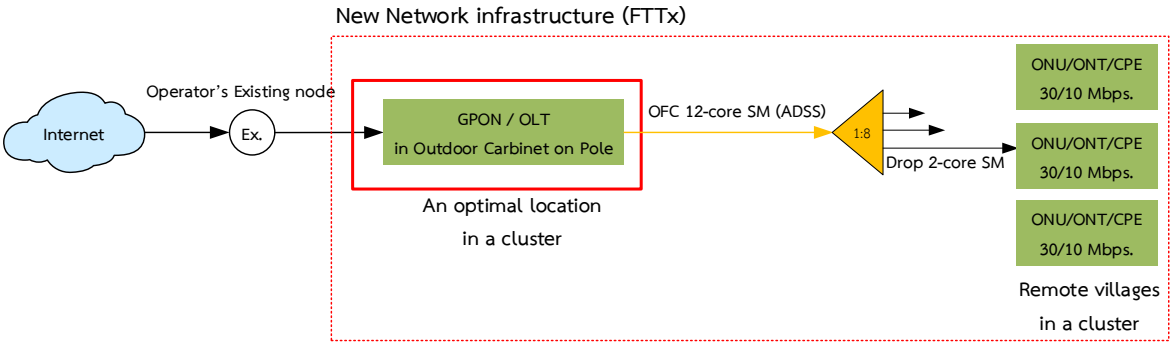
แพง ปรับขนาดได้ และมีความเป็นไปได้ทางการเงิน เทคโนโลยีที่หลากหลายอาจเหมาะสมสำหรับการดำเนินการบรอดแบนด์ "ไมล์สุดท้าย" เป็นโครงข่ายเชื่อมโยงกลับในพื้นที่ห่างไกล เช่น ไฟเบอร์ (Passive Optical Network: GPON), ดาวเทียม หรือไมโครเวฟ เทคโนโลยีแต่ละประเภทมีข้อดีและข้อเสียในด้านราคา ประสิทธิภาพ และต้นทุนรวมในการเป็นเจ้าของ (TCO) ด้วยเหตุนี้ จึงไม่มีโซลูชันเทคโนโลยีใดที่สามารถแก้ปัญหาได้ทุกสถานการณ์ในพื้นที่ห่างไกล ประมาณ 60% ของหมู่บ้าน 3,920 แห่งไม่มีอินเทอร์เน็ตเข้าถึงเลย (ไม่มีการเชื่อมต่อเครือข่ายอยู่ก่อนแล้ว) อย่างไรก็ตาม จากข้อมูลการสำรวจของเรา ไม่พบอุปสรรคดังกล่าวในพื้นที่ชนบทส่วนใหญ่ที่มีอินเทอร์เน็ตเข้าถึงผ่านผู้ให้บริการเครือข่ายสาธารณะและ/หรือส่วนตัวอยู่แล้ว

โมเดลบรอดแบนด์ในการจำลอง

ด้วยข้อจำกัดทางเทคนิคที่กล่าวถึงในส่วนก่อนหน้า สำหรับการดำเนินการบรอดแบนด์ มีข้อพิจารณาหลักสองประการที่จำเป็นต้องหาแนวทางแก้ไขสำหรับพื้นที่ห่างไกล เนื่องจากในพื้นที่ชนบทมีโครงสร้างพื้นฐานเครือข่ายและการเข้าถึงอยู่แล้ว แนวทางแก้ไขที่สองจึงเป็นเพียงแนวทางเดียวที่ตระหนักถึง การใช้การกระจายทางภูมิศาสตร์จะนำไปสู่แผนพัฒนาด้วยเทคนิคการจัดกลุ่ม เช่น K-means Clustering หรือ Self-Organizing Map (Kanungo et al., 2002) ด้วยแนวทางการจัดกลุ่มเหล่านี้ โครงสร้างพื้นฐานบรอดแบนด์สามารถแบ่งหมู่บ้านห่างไกลออกเป็นหลายกลุ่มในแง่ของปัญหาโครงสร้างพื้นฐานและการขาดความรู้ เพื่อให้บรรลุข้อจำกัดทางเศรษฐกิจ ตำแหน่งที่เหมาะสมที่สุดในกลุ่มจะถูกกำหนดโดยการแก้ปัญหาการเพิ่มประสิทธิภาพ:

Factors	Description
Users	Stakeholders, Gender, Age, Internet experience, Self- efficacy, Education
Physical	Location, geographic limitation, Accessibility, Landmarks) School, Temple, Hospital, etc(.
Social	Usages, Activities, federal, state, and local agencies
Facility	Electricity, Water, Energy
Infrastructure & Communication	Current Broadband and mobile service
Cost	Implementation and Maintenance

เป็นผลให้โซลูชันการดำเนินการบรอดแบนด์ให้บริการสองระดับ: 1) โครงสร้างพื้นฐานเครือข่าย (Backhaul) และ 2) บริการและแอปพลิเคชันดิจิทัลผ่านเทคโนโลยี Wi-Fi และศูนย์การเรียนรู้ สำหรับหมู่บ้านห่างไกล อันดับแรก หากทำได้ เทคโนโลยีไฟเบอร์ (Passive Optical Network: GPON) จะถูกนำมาใช้ โดยมีการติดตั้ง Optical Line Termination (OLT) ณ ตำแหน่งที่เหมาะสมที่สุดในกลุ่ม ดังแสดงในภาพที่ 7 มี OLT รวม 881 ตัวเพื่อรองรับบริการ 4,760 จุด (Customer-Premises Equipment (CPE)/Optical Network Unit (ONU)) ในหมู่บ้านห่างไกล 1,909 แห่ง (ที่ไม่มีโครงสร้างพื้นฐานอินเทอร์เน็ตอยู่ก่อน) เทคโนโลยีนี้สามารถรองรับการเข้าถึงอินเทอร์เน็ตความเร็วสูงด้วยอัตราข้อมูลมากกว่า 30/10 Mbps (ดาวน์โหลด/อัปโหลด) ต่อจุดบริการ (ONU) ในกรณีที่มีข้อจำกัดทางภูมิศาสตร์ที่ระยะทางยาวเกินไปสำหรับเทคโนโลยีไฟเบอร์ในแง่ของข้อจำกัดทางเทคนิคและต้นทุน ความจุของดาวเทียมบรอดแบนด์สามารถนำมาใช้เพื่อให้บริการโครงข่ายเชื่อมโยงกลับอินเทอร์เน็ตสำหรับบริการบรอดแบนด์ด้วยอัตราข้อมูลมากกว่า 30/5 Mbps (ดาวน์โหลด/อัปโหลด) ต่อจุดบริการ (CPE) ในพื้นที่ห่างไกล



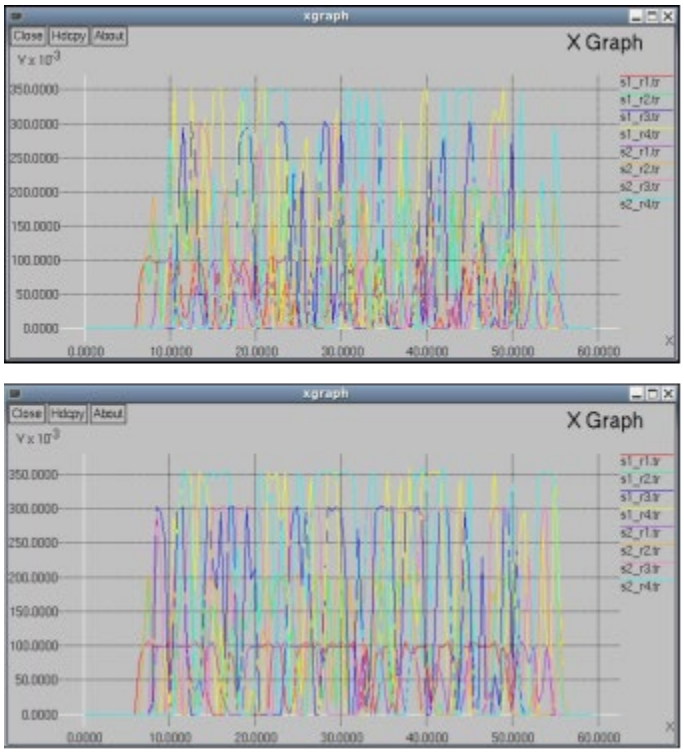
ภาพที่ 7 โครงสร้างพื้นฐานเครือข่าย GPON (Backhaul)

การอภิปราย

การจำลองนี้มีวัตถุประสงค์เพื่อตรวจสอบแนวคิดอัลกอริทึมจาก 3 มุมมองหลัก: 1) การส่งข้อมูล: เพื่อตรวจสอบความเป็นไปได้ของการเชื่อมต่อแบบ end-to-end สำหรับการใช้งานจริง 2) ความปลอดภัย: เพื่อตรวจสอบว่าระบบไม่เปิดเผยข้อมูลสู่เครือข่ายภายนอก 3) ประสิทธิภาพ: เพื่อเปรียบเทียบกับเครือข่าย Ethernet ทั่วไปในสถานการณ์ที่มีปริมาณการรับส่งข้อมูลสูงและต่ำ

```
Construct Thread1, Thread2, Thread3
Construct Queue1[ ], Queue2[ ]
  THREAD1( )
   int_Name      ← get available interface number
   Pkt_cap       ← capture packets from int_Name
   Insert pkt_cap to Queue1[int_Name]
     THREAD2( )
REPEAT WHILE true
    IF Queue1 is not empty
        THEN
        Pkt_Queue1       ← packet removed from Queue1
         Proper_Int      ← find proper interface for send
                             packet from Queue1
        pkt_Edited       ← replace a new Ethernet header
                             of pkt_Queue1
        put pkt_Edited into Queue2[Proper_Int]
   ENDIF
END REPEAT
THREAD3( )
   REPEAT WHILE true
      IF Queue2 is not null
         THEN IF Queue2 is not empty
                      THEN
                        Remove packet from Queue2
                        Send the packet off
                    ENDIF
      ENDIF
END REPEAT
```

ภาพที่ 8 ขั้นตอนวิธีของระบบการจัดคิว



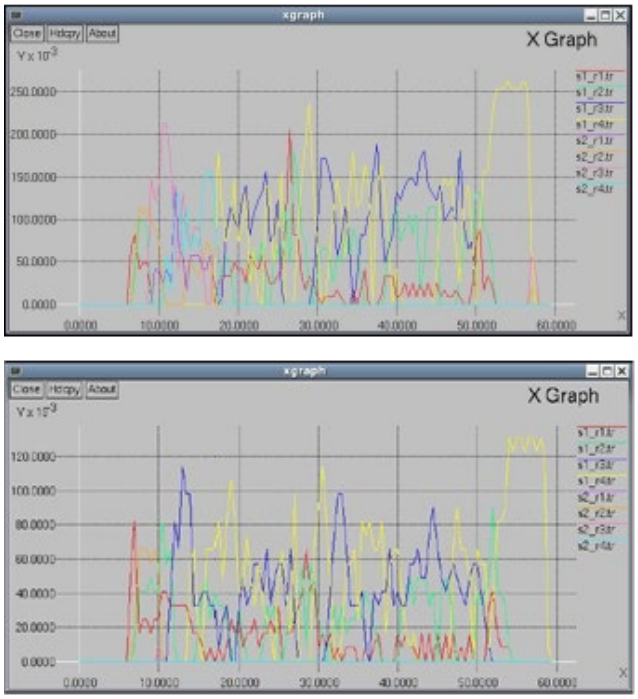
ภาพที่ 9 กราฟแสดงการเปรียบเทียบปริมาณงานของเครือข่ายระหว่างระบบ QKD (s1) และการรับส่งข้อมูลปกติ (s2) ในสถานการณ์ที่มีปริมาณการรับส่งข้อมูลสูง

การส่งข้อมูล

ผลลัพธ์จากระบบแสดงให้เห็นว่าระบบ QKD ที่เชื่อมต่อทั้งหมดสามารถแลกเปลี่ยนข้อมูลในเส้นทางที่สั้นที่สุดได้อย่างเหมาะสม คิวจำเป็นต้องจัดเตรียมให้มีขนาดใหญ่เพียงพอในกรณีที่เกิดปริมาณการรับส่งข้อมูลสูง มิฉะนั้นอาจทำให้เกิดการสูญเสียแพ็กเกจ ระหว่างการจำลองที่มีขนาดใหญ่ แนะนำให้ใช้บัฟเฟอร์อย่างน้อย 100 MB ในกรณีที่เกิดปริมาณการรับส่งข้อมูลสูง

ความปลอดภัย

กุญแจอาศัยระบบ QKD ซึ่งกระจายผ่านช่องสัญญาณควอนตัม ดังนั้นผู้ดักฟังไม่สามารถดักจับกุญแจที่กระจายได้ ในกรณีที่ผู้ดักฟังดักจับกุญแจ ระบบ QKD จะตรวจจับได้และกุญแจจะถูกละทิ้งและส่งใหม่ หากผู้โจมตีพยายามดักจับและสร้างกุญแจใหม่ QKD สามารถตรวจจับกุญแจนี้ว่าเป็นข้อผิดพลาดได้เนื่องจากคุณสมบัติควอนตัมใน BB84 ดังนั้นการส่งกุญแจจึงสามารถเชื่อถือได้ในระบบ อย่างไรก็ตาม ระบบส่งและจัดคิวจำเป็นต้องเป็นโฮสต์ที่เชื่อถือได้ มิฉะนั้นอาจถูกบิดเบือนหรือโจมตีจากผู้บุกรุกได้



ภาพที่ 10 การเปรียบเทียบปริมาณงานของเครือข่ายระหว่างระบบ QKD (s1) และการรับส่งข้อมูลปกติ (s2) ในสถานการณ์ที่มีปริมาณการรับส่งข้อมูลต่ำ

ประสิทธิภาพ

การเปรียบเทียบเครือข่ายทั่วไปที่ใช้ Ethernet LAN และระบบ QKD ของเราโดยใช้การจำลอง NS-2 การจำลองใช้ความล่าช้าและพฤติกรรมจริงที่บันทึกจากฮาร์ดแวร์จริง (Ceberis) รวมถึงตัวเข้ารหัสแพ็กเกจ (Centauris CypherNet)

ภาพที่ 9 แสดงการเปรียบเทียบปริมาณงานของเครือข่ายระหว่างระบบ QKD (s1) และ LAN ปกติ (s2) ในสถานการณ์ที่มีปริมาณการรับส่งข้อมูลสูง ผลลัพธ์ข้อมูลดิบแสดงให้เห็นว่าระบบ QKD มีปริมาณงานต่ำกว่าเครือข่ายปกติทั่วไปประมาณ 12% ซึ่งเกิดจากความล่าช้าในการกระจายกุญแจและการประยุกต์ใช้แพ็กเกจ (เช่น การประชุมทางวิดีโอ) ซึ่งส่งผลกระทบต่อเวลาทั้งหมดของการถ่ายโอนไฟล์ขนาดใหญ่ (เช่น ไฟล์ขนาด 4 GB) ด้วยเหตุนี้ โครงสร้างเครือข่ายที่ซับซ้อนที่มีปริมาณการรับส่งข้อมูลสูงอาจต้องใช้แนวคิดของระบบ QKD ที่ได้รับการปรับปรุง

ภาพที่ 10 แสดงการเปรียบเทียบปริมาณงานของเครือข่ายระหว่างระบบ QKD (s1) และ Ethernet LAN (s2) ในสถานการณ์ที่มีปริมาณการรับส่งข้อมูลต่ำ ผลลัพธ์ข้อมูลดิบแสดงให้เห็นว่าระบบ QKD ไม่ได้มีปริมาณงานต่ำกว่าเครือข่ายปกติทั่วไปโดยเฉลี่ย ดังนั้น ระบบ QKD ที่มีเนื้อหาผสมในปริมาณน้อยจึงไม่ส่งผลกระทบต่อประสิทธิภาพของปริมาณงานเมื่อเทียบกับเครือข่ายปกติ ด้วยเหตุนี้ ในฐานะช่องสัญญาณที่ปลอดภัยที่มีปริมาณน้อย ระบบ QKD จึงมีประสิทธิภาพเพียงพอที่จะทำงานได้

สรุปผลการวิจัย

ในบทความนี้ เรานำเสนอการจัดการเครือข่ายสำหรับ QKD ระบบนี้ใช้ประโยชน์จากความปลอดภัยสูงของช่องสัญญาณควอนตัมแบบจุดต่อจุดเพื่อเชื่อมต่อเป็นเครือข่ายโดยอิงจากโครงสร้างพื้นฐานบรอดแบนด์จริงในประเทศไทย วัตถุประสงค์ของระบบคือการจัดให้มีการเชื่อมต่อ ความสะดวก และต้นทุนต่ำในระดับแอปพลิเคชัน

เนื่องจากโปรโตคอลควอนตัมสามารถให้ความปลอดภัยที่แข็งแกร่งดังที่แสดงใน BB84 และ B92 การกระจายกุญแจจึงถูกใช้ในช่องสัญญาณที่ปลอดภัยนี้ การเข้ารหัสเชิงควอนตัมสามารถให้คุณสมบัติที่รับประกันว่าจะไม่มีการดักจับ เมื่อผู้ดักจับดักจับข้อความควอนตัม ระบบ QKD สามารถตรวจจับได้ นอกจากนี้ การสร้างใหม่หรือการโคลนข้อความควอนตัมเป็นไปไม่ได้ด้วยเทคโนโลยีปัจจุบัน ดังนั้น ช่องสัญญาณควอนตัมจึงให้ความปลอดภัยที่แข็งแกร่งสำหรับระบบ QKD ของเรา

ระบบ QKD ของเราได้รับการออกแบบโดยใช้คอมพิวเตอร์จัดการเส้นทางและการส่งข้อมูล การออกแบบนี้อิงตามข้อสันนิษฐานว่าช่องสัญญาณควอนตัมเป็นโฮสต์ที่เชื่อถือได้และมีการป้องกันทางกายภาพสำหรับเครื่อง อุปกรณ์ทั้งสองนี้ได้รับการออกแบบมาเพื่อเชื่อมต่อช่องสัญญาณควอนตัมเป็นเครือข่าย รวมถึงการกรองและการกำหนดเส้นทางแพ็กเกจ

การจำลองในระบบของเราใช้ข้อมูลจริงจาก Ceberis และ Centauris CypherNet และโครงสร้างพื้นฐานจริงของบรอดแบนด์ในประเทศไทย ผลลัพธ์แสดงให้เห็นว่าระบบ QKD ให้การเชื่อมต่อ ความปลอดภัย และประสิทธิภาพในสถานการณ์ที่มีปริมาณน้อย อย่างไรก็ตาม เมื่อมีการสร้างปริมาณการรับส่งข้อมูลสูง ความล่าช้าจากตัวเข้ารหัสและการกระจายกุญแจส่งผลกระทบต่อผลลัพธ์ประมาณ 12% เมื่อเทียบกับเครือข่ายปกติ และแนะนำให้ใช้ช่องสัญญาณอย่างน้อย 100 MB สำหรับระบบ QKD โดยเฉพาะ ดังนั้น ระบบ QKD จึงเป็นที่ยอมรับและมีความเป็นไปได้ในเครือข่ายที่ปลอดภัยสำหรับปริมาณน้อยจากการจำลองของเรา ในกรณีที่มีการใช้งานสูง ผลลัพธ์แนะนำให้ใช้ช่องสัญญาณอย่างน้อย 100 MB สำหรับ QKD โดยเฉพาะ

กิตติกรรมประกาศ

สำหรับบทความนี้ ขอขอบคุณคณะวิศวกรรมศาสตร์ มหาวิทยาลัยธรรมศาสตร์ และมหาวิทยาลัยธรรมศาสตร์ งานวิจัยนี้ได้รับการสนับสนุนจากโครงการของคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) โดยมีมหาวิทยาลัยธรรมศาสตร์เป็นที่ปรึกษา ผู้เขียนขอขอบพระคุณ กสทช. เป็นอย่างสูงสำหรับความสนับสนุน ความคิดเห็น ข้อค้นพบ ข้อสรุป หรือข้อเสนอแนะใดๆ ที่แสดงในบทความนี้เป็นของผู้เขียนและไม่จำเป็นต้องสะท้อนถึงมุมมองของ กสทช.

เอกสารอ้างอิง

Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing (pp. 175-179).

Bennett, H., & Brassard, G. (1984). *Quantum cryptography: Public key distribution and coin tossing*. In *Proceeding of IEE International Conference on Computers, Systems and Signal Processing* (pp. 175-179).

Bennett, H., & Brassard, G. (1992). Quantum cryptography using any two non-orthogonal states. *Physical Review Letters*, *68*(21), 3121-3124.

Denning, D. E. (1945). *Cryptography and data security*. Addison-Wesley.

Eli, B., & Shamir, A. (1993). Differential cryptanalysis of the data encryption standard. Springer Verlag.

Elliott, C., Pearson, D., Troxel, G. (2003). *Quantum cryptography in practice*. In *Proc. ACM SIGCOMM 2003* (pp. 227-238).

Ferguson, N., Schroeppel, R., Whiting, D. (2001). A simple algebraic representation of Rijndael. In *Proceedings of Selected Areas in Cryptography, Lecture Notes in Computer Science* (pp. 103–111). Springer-Verlag.

Gisin, N., Ribordy, G., Tittel, W., Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, *74*(1), 145-195.

Heisenberg, W. (1927). Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik [On the visualizable content of the quantum-theoretical kinematics and mechanics]. *Zeitschrift für Physik*, *43*(3-4), 172–198.

Hollifield, C. A., & Donnermeyer, J. F. (2003). Creating demand: Influencing information technology diffusion in rural communities. *Government Information Quarterly*, 20(2), 135–150.

Kanungo, T., Mount, D. M., Netanyahu, N. S., Piatko, C. D., Silverman, R., Wu, A. Y. (2002). An efficient k-means clustering algorithm: analysis and implementation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *24*(7), 881-892.

Lüthenhaus, N. (1999). Quantum key distribution. *Applied Physics B,* 69(5), 395-400.

Steenstrup, M. E. (1995). *Routing in communications networks*. Prentice Hall.

Zhang, T., Han, A.-F., Mo, X.-F., Guo, G.-C. (2006). *Extensible router for multi-user quantum key distribution network*. Key Laboratory of Quantum Information, University of Science and Technology of China (CAS).