โปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงสำหรับการสื่อสารความเร็วสูงและความปลอดภัยสูงโดยใช้อุปกรณ์เชิงแสงทั้งหมด

OPTICAL TRANSMISSION AND ADDRESSING PROTOCOL FOR HIGH SPEED AND HIGH SECURITY COMMUNICATION USING ALL OPTICAL DEVICES

ภากร จูเหล็ง

PAKORN JULEANG

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรดุษฎีบัณฑิต

สาขาวิชาวิศวกรรมไฟฟ้า

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2559

KMITL-2016-EN-D-018-170

โปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงสำหรับการสื่อสารความเร็วสูงและความปลอดภัยสูงโดยใช้อุปกรณ์เชิงแสงทั้งหมด

OPTICAL TRANSMISSION AND ADDRESSING PROTOCOL FOR HIGH SPEED AND HIGH SECURITY COMMUNICATION USING ALL OPTICAL DEVICES

ภากร จูเหล็ง

PAKORN JULEANG

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรดุษฎีบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ.2559

KMITL-2016-EN-D-018-170

OPTICAL TRANSMISSION AND ADDRESSING PROTOCOL FOR HIGH SPEED AND HIGH SECURITY COMMUNICATION USING ALL OPTICAL DEVICES

PAKORN JULEANG

A THESIS SUBMITTED IN FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
DOCTOR OF ENGINEERING IN ELECTRICAL ENGINEERING
FACULTY OF ENGINEERING
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
2016

KMITL-2016-EN-D-018-170

คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ โปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงสำหรับการสื่อสารความเร็วสูงและความปลอดภัยสูงโดยใช้อุปกรณ์เชิงแสงทั้งหมด

Thesis Title Optical Transmission and Addressing Protocol for High Speed and High Security Communication Using all Optical Devices

นักศึกษา นายภากร จูเหล็ง

รหัสประจำตัว 53610137

ปริญญา วิศวกรรมศาสตรดุษฎีบัณฑิต

สาขาวิชา วิศวกรรมไฟฟ้า

อาจารย์ที่ปรึกษาวิทยานิพนธ์ รศ.ดร.สมศักดิ์ มิตะถา

หมายเลขวิทยานิพนธ์ KMITL-2016-EN-D-018-170

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
รศ.ดร.สุริภณ	สมควรพาณิชย์	
ดร.วัชระ	ฉัตรวิริยะ	
รศ.ดร.จิระศักดิ์	ชาญวุฒิธรรม	
ดร.ปกรณ์	วัฒนจตุรพร	
รศ.ดร.สมศักดิ์	มิตะถา	

วัน / เดือน/ ปี ที่สอบ วันพฤหัสบดีที่ 19 พฤษภาคม พ.ศ. 2559 เวลา 09.30-11.30 น.
สถานที่สอบ ณ อาคาร A ชั้น 5 ห้องประชุม 1

คณะวิศวกรรมศาสตร์ รับรองแล้ว

(รองศาสตราจารย์ ดร. คมสัน มาลีสี)
คณบดี คณะวิศวกรรมศาสตร์
วันที่ 19 พฤษภาคม พ.ศ. 2559

หัวข้อวิทยานิพนธ์	โปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงสำหรับการสื่อสารความเร็วสูงและความปลอดภัยสูงโดยใช้อุปกรณ์เชิงแสงทั้งหมด
นักศึกษา	นายภากร จูเหล็ง
รหัสประจำตัว	53610137
ปริญญา	วิศวกรรมศาสตรดุษฎีบัณฑิต
สาขาวิชา	วิศวกรรมไฟฟ้า
พ.ศ.	2559
อาจารย์ที่ปรึกษาวิทยานิพนธ์	รศ.ดร. สมศักดิ์ มิตะถา

บทคัดย่อ

วิทยานิพนธ์นี้ นำเสนอโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงสำหรับการสื่อสารความเร็วสูงและความปลอดภัยสูงโดยใช้อุปกรณ์เชิงแสงทั้งหมด เพื่อแก้ปัญหาการห่อหุ้มข้อมูลระหว่างระดับชั้นย่อยและการระบุที่อยู่ในเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด รวมถึงปรับปรุงความปลอดภัยในการส่งข้อมูลให้มากขึ้น โดยพัฒนาจากอุปกรณ์เชิงแสง คือ วงแหวนเพิ่มและลดสัญญาณวงแหวนสั่นพ้องแพนด้า และอุปกรณ์ที่ใช้หลักการของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์

โปรโตคอลที่นำเสนอประกอบด้วย 4 ระดับชั้นย่อย กล่าวคือ ระดับชั้นย่อย Physical ทำหน้าที่ส่งสัญญาณที่ถูกเข้ารหัสผ่านตัวกลางของการสื่อสารข้อมูล ระดับชั้นย่อย Network ทำหน้าที่ในการส่งข้อมูลถึงผู้รับข้อมูลอย่างถูกต้องด้วยที่อยู่เชิงแสง ระดับชั้นย่อย Security ทำหน้าที่ให้การสื่อสารข้อมูลเป็นไปอย่างปลอดภัยด้วยการซ่อนกุญแจและการกู้คืนกุญแจ โดยใช้สัญญาณรูปปากและเครือข่ายส่วนตัวเสมือนเชิงแสง ระดับชั้นย่อย Application ทำหน้าที่เป็นตัวกลางติดต่อระหว่างโปรแกรมกับระดับชั้นอื่น ๆ รวมถึงทำหน้าที่ปรับข้อมูลในฝั่งผู้รับข้อมูลให้เป็นข้อมูลที่สมบูรณ์ก่อนส่งให้กับโปรแกรมอื่น ๆ

จากการทดสอบสมมติฐาน พบว่า ข้อจำกัดการทำงานของโปรโตคอลมีดังนี้ ความเข้มแสงที่เหมาะสมของสัญญาณข้อมูล คือ น้อยกว่า 200 % ของความเข้มแสงของสัญญาณที่ใช้สร้างกุญแจเชิงแสงและที่อยู่เชิงแสง อีกทั้งค่าความผิดพลาดมากที่สุดของวงแหวนเพิ่มและลดสัญญาณ ที่เป็นอุปกรณ์ที่ใช้ในการกู้คืนกุญแจเชิงแสง (เป็นข้อจำกัดในการกู้คืนกุญแจเชิงแสง) คือ พารามิเตอร์ขนาดวงแหวนเท่ากับ 0.0005 % ค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 เท่ากับ 0.06 และค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 เท่ากับ 0.03

สุดท้ายนี้ การจำลองเครือข่าย พบว่า โปรโตคอลที่นำเสนอสามารถทำงานได้ถูกต้อง ส่งข้อมูลถึงผู้รับข้อมูลได้อย่างถูกต้อง ถ้าผู้มีผู้ไม่หวังดีในเครือข่ายสื่อสารจะไม่สามารถทราบข้อมูลของผู้ส่งข้อมูลได้

Thesis Title	Optical transmission and addressing protocol for high speed and high security communication using all optical devices
Student	Mr. Pakorn Juleang
Student ID.	53610137
Degree	Doctor of Engineering
Program	Electrical Engineering
Year	2016
Thesis Advisor	Assoc. Prof. Dr. Somsak Mitatha

ABSTRACT

This study reveals the protocol of data transmission and the confirmation of the optical substance used for high speed and high security communication by handling it with all of the optical equipment. The mentioned action above has been done to rectify the data wrapping between sub layers and to affirm the substance in all network, which uses all of optical equipment, including providing more adjustment on data transmission security by developing from the optical equipment as follows: Add Drop Filter, Panda Ring Resonator and Mach-Zehnder Interferometer.

The presented protocol consists of 4 sub layers: Physical sub layer, transmits encrypted signal via the medium of data communication. Network sub layer, transmits the data to the data receiver correctly with Optical Address. Security sub layer, provides security for data communication process by using Key Suppression and Recovery, Lip Signal, and Optical Private Tunnel. Application sub layer, executes as the medium connecting between the program and the other layer including adjusting the receiver's data to be completed data prior to deliver to the other program.

According the test, restrictions on the operation of the protocol, various parameters of the equipment affect to data communication signal, especially to the intensity of various signals: the intensity of suitable ray of the data signal of which is less than 200% of the ray intense of the signal used to build the Optical Key and the Optical Address. Then, the mistake most of the parameters of Add Drop Filter which is used to recover the optical key are 0.0005 % of ring size, 0.06 of coupling coefficient κ_1 and 0.03 of coupling coefficient κ_2

Finally, according the simulation, the conclusion reveals that the presented protocol correctly runs and transmits the data to the receiver correctly. Sender's data cannot be perceived by interferer.

กิตติกรรมประกาศ

วิทยานิพนธ์นี้สำเร็จลุล่วงได้ด้วยการสนับสนุน และให้คำแนะนำจากอาจารย์ที่ปรึกษาวิทยานิพนธ์ของผู้วิจัย รศ.ดร.สมศักดิ์ มิตะถา และ รศ.ดร.ปรีชา ยุพาพิน ซึ่งได้กรุณาให้คำปรึกษาทั้งในด้านวิชาการ ประสบการณ์ในการทำงานรวมทั้งโอกาสในการศึกษาเล่าเรียน ผู้วิจัยรู้สึกซาบซึ้งในความอนุเคราะห์ และความปรารถนาดีที่ได้รับเสมอมาตลอดช่วงเวลาที่ได้ทำการศึกษาวิจัย และขอขอบพระคุณเป็นอย่างสูงไว้ ณ โอกาสนี้

ขอขอบพระคุณ คุณครู อาจารย์ทุก ๆ ท่าน โดยเฉพาะอย่างยิ่งอาจารย์สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ที่ได้ประสิทธิ์ประสาทวิชาให้กับข้าพเจ้า

ขอบคุณเพื่อนสมาชิกจากห้องปฏิบัติการ HCRL ขอบคุณเพื่อนที่เรียนร่วมกัน ขอบคุณเพื่อนที่ใช้ชีวิตร่วมกัน สำหรับมิตรภาพที่ดี และพร้อมที่จะให้ความช่วยเหลือซึ่งกันและกันในทุก ๆ ด้าน

สุดท้ายนี้ ขอกราบขอบพระคุณ คุณพ่อสุรพงษ์ จูเหล็ง คุณแม่ดวงพร จูเหล็ง อีกทั้งญาติพี่น้องทุก ๆ ท่าน ที่ได้มอบความรัก ความเชื่อมั่น ความห่วงใย และสนับสนุนผู้วิจัยในทุก ๆ ด้านอย่างดีที่สุดเสมอมา

คุณค่าและประโยชน์จากการค้นคว้าอันพึงมีของวิทยานิพนธ์นี้ ผู้วิจัยขอมอบทดแทนบุญคุณต่อบิดา มารดา ครูอาจารย์ ตลอดจนผู้มีพระคุณทุกท่าน ที่ได้อบรมสั่งสอนศิษย์ตลอดมา

ภากร จูเหล็ง

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในสภาวการณ์ปัจจุบัน การสื่อสารข้อมูลถือว่ามีความสำคัญอย่างยิ่งทั้งในด้านของการทำธุรกิจ ในด้านของการใช้ชีวิตประจำวันของบุคคลทั่วไป เช่น การใช้งานของ Smart Phone หรือในการใช้งานเฉพาะด้าน เช่น การสื่อสารภายในของระบบทหาร เป็นต้น โดยความต้องการหลักในการสื่อสาร คือ ความเร็วที่สูงมากขึ้นและความปลอดภัยที่เพิ่มสูงขึ้น ตัวอย่างงานวิจัยที่เน้นในการเพิ่มความเร็วในการสื่อสารข้อมูล เช่น [1-3] ตัวอย่างงานวิจัยที่เน้นในการเพิ่มความปลอดภัยในการสื่อสารข้อมูล เช่น [4]

อีกทั้งการสื่อสารด้วยแสง (Optical Communication) ในปัจจุบันมีการใช้งานแพร่หลายมากขึ้น [5-6] เนื่องจากการสื่อสารด้วยแสงมีข้อดีที่เกิดจากคุณสมบัติของแสง คือ ให้แบนด์วิดท์ที่กว้าง กล่าวคือ การใช้คลื่นพาห์ที่มีความถี่สูงในระบบสื่อสารทำให้แบนด์วิดท์ของสัญญาณกว้างมากขึ้น มีขนาดเล็กและน้ำหนักเบา ใยแก้วนำแสงเพียงเส้นเดียวสามารถแทนสายทองแดงขนาดใหญ่ได้ มีการสูญเสียต่ำ ใยแก้วนำแสงมีค่าการสูญเสียเนื่องจากการลดทอนน้อยกว่าสายคู่บิดเกลียว (Twisted Pair) หรือสายเคเบิลร่วมแกน (Coaxial Cable) แสงไม่ถูกรบกวนจากคลื่นแม่เหล็กไฟฟ้า เนื่องจากใยแก้วนำแสงไม่ได้สร้างจากเส้นลวดโลหะ มีความคงทนและไม่ถูกรบกวนโดยสภาพดินฟ้าอากาศ เป็นต้น

เทคโนโลยีปัจจุบัน การใช้งานอุปกรณ์เชิงแสงขนาดเล็กมีมากขึ้น ได้รับความสนใจในการคิดค้นวิจัยและพัฒนาอย่างต่อเนื่อง ตัวอย่างเช่น การใช้งานในด้านเซนเซอร์ต่าง ๆ [7-8] การใช้งานในด้านการประมวลผลข้อมูล [9-10] รวมถึงการใช้งานในด้านอื่น ๆ [11-12] อุปกรณ์เชิงแสงขนาดเล็กที่เกี่ยวข้องกับวิทยานิพนธ์นี้ ตัวอย่างเช่น วงแหวนสั่นพ้องขนาดเล็ก (Micro Ring Resonator) และวงแหวนเพิ่มหรือลดสัญญาณ (Add Drop Filter) เป็นต้น ซึ่งมีการนำไปประยุกต์ใช้งานมากมาย กล่าวคือ [13-16]

การสื่อสารเชิงแสงด้วยอุปกรณ์เชิงแสงขนาดเล็กระดับไมโครเมตร (Micro Optical Devices) มีการนำมาใช้งานเพื่อการเพิ่มความเร็วในการสื่อสารข้อมูล ตัวอย่างเช่น [17-18] และมีการนำมาใช้งานเพื่อการเพิ่มความปลอดภัยในการสื่อสารข้อมูล ตัวอย่างเช่น [19-26] ซึ่งวิทยานิพนธ์นี้ นำเสนอโปรโตคอลในการสื่อสารข้อมูลโดยใช้อุปกรณ์เชิงแสงขนาดเล็กระดับไมโครเมตร (Micro Optical Devices) ทั้งหมด เพื่อการสื่อสารที่มีความเร็วสูงและความปลอดภัยสูง

จากข้อมูลต่าง ๆ ที่กล่าวมาข้างต้น วิทยานิพนธ์นี้นำเสนอโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงสำหรับการสื่อสารความเร็วสูงและความปลอดภัยสูงโดยใช้อุปกรณ์เชิงแสงทั้งหมด เพื่อให้เกิดประโยชน์อย่างมากต่อการใช้งานที่ต้องการความเร็วและความปลอดภัยในคราวเดียวกัน เช่น การสื่อสารข้อมูลทางการทหาร เป็นต้น

1.2 จุดประสงค์

1.2.1 วิจัยและพัฒนาโปรโตคอลการส่งข้อมูลและการระบุที่อยู่ (Transmission and Addressing Protocol) ที่สนับสนุนการทำงานด้วยอุปกรณ์เชิงแสง (Optical Devices)

1.2.2 วิจัยและพัฒนาโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง (Optical Transmission and Addressing Protocol) สำหรับการสื่อสารข้อมูลความเร็วสูง (High Speed Communication)

1.2.3 วิจัยและพัฒนาโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง (Optical Transmission and Addressing Protocol) สำหรับการสื่อสารข้อมูลแบบปลอดภัยสูง (High Security Communication)

1.3 จุดมุ่งหมายของการศึกษา

วิทยานิพนธ์ฉบับนี้มุ่งหวังเพื่อศึกษาและพัฒนาโปรโตคอลการส่งข้อมูลและการระบุที่อยู่ (Transmission and Addressing Protocol) ที่ทำงานด้วยอุปกรณ์เชิงแสงทั้งหมด (All Optical Devices) โดยการสื่อสารข้อมูลด้วยอุปกรณ์เชิงแสงทั้งหมดเป็นผลสำคัญให้เครือข่ายสื่อสารมีความเร็วสูงและมีความปลอดภัยสูง ซึ่งเป็นประโยชน์อย่างมากต่อการใช้งานเฉพาะด้านที่ต้องการความเร็วและความปลอดภัยในคราวเดียวกัน โดยที่รูปแบบของเครือข่ายสื่อสาร (Network Topology) ที่โปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง (Optical Transmission and Addressing Protocol) ที่นำเสนอครอบคลุม คือเครือข่ายแบบบัส (Bus Topology) และเครือข่ายแบบวงแหวน (Ring Topology)

1.4 ทฤษฎีและแนวคิดที่ใช้ในการวิจัย

โปรโตคอลการส่งข้อมูลและการระบุที่อยู่ (Transmission and Addressing Protocol) ที่นำเสนอมุ่งหวังให้การทำงานของการส่งข้อมูลภายในเครือข่ายสื่อสารทำงานด้วยอุปกรณ์เชิงแสงทั้งหมด (All Optical Devices) ซึ่งใช้ทฤษฎีทางด้านการสื่อสารด้วยแสงเป็นพื้นฐานของการวิจัย โดยที่อุปกรณ์เชิงแสงที่ศึกษาและใช้ในการส่งข้อมูลและการระบุที่อยู่เชิงแสง คือวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) วงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) และอุปกรณ์ที่ใช้หลักการของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer)

โปรโตคอลที่นำเสนอมีการส่งข้อมูลระหว่างระดับชั้นย่อย (Sub Layer) ใช้วิธีการที่เรียกว่า การห่อหุ้มเชิงแสง (Optical Encapsulation) อีกทั้งมีการระบุที่อยู่ภายในเครือข่ายโดยใช้แสง ใช้วิธีการที่เรียกว่า ที่อยู่เชิงแสง (Optical Address) ซึ่งเป็นการระบุที่อยู่บุคคลในเครือข่ายโดยใช้สัญญาณอ้างอิง และในด้านของความปลอดภัยในการสื่อสาร ใช้วิธีการที่เรียกว่า การซ่อนกุญแจและการกู้คืนกุญแจ (Key Suppression and Recovery) และท่อเสมือนเชิงแสง (Optical Private Tunnel) โดยเป็นการใช้สัญญาณที่เรียกว่า สัญญาณรูปปาก (LIP Signal) ในการแลกเปลี่ยนกุญแจที่ใช้ในการสื่อสารข้อมูลเพื่อให้มีความปลอดภัยในการสื่อสารข้อมูลสูงสุด

1.5 สมมติฐานของการศึกษา

โปรโตคอลการสื่อสารข้อมูลที่ใช้งานแพร่หลาย เป็นมาตรฐานในการใช้งานปัจจุบัน และใช้อ้างอิงในการศึกษา คือ TCP/IP Protocol รวมถึงใช้แบบจำลอง Open System Interconnection (OSI Model) ซึ่งเป็นการสื่อสารข้อมูลผ่านสื่อหรืออุปกรณ์การประมวลผลที่อยู่ในรูปแบบของกระแสไฟฟ้า โดยที่วิทยานิพนธ์นี้เสนอการสื่อสารข้อมูลที่มีความเร็วสูงและมีความปลอดภัยสูง (High Speed and High Security) โดยพัฒนาโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง (Optical Transmission and Addressing Protocol) ที่สนับสนุนการทำงานด้วยอุปกรณ์เชิงแสง (Optical Devices) กล่าวคือ เป็นการสื่อสารข้อมูลผ่านสื่อและอุปกรณ์การประมวลผลที่อยู่ในรูปแบบแสงทั้งหมด ซึ่งการใช้แสงในการสื่อสารข้อมูลเป็นส่วนสำคัญที่ทำให้โปโตคอลการสื่อสารข้อมูลที่นำเสนอมีความเร็วสูงและมีความปลอดภัยสูง

การสื่อสารข้อมูลโดยใช้โปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง (Optical Transmission and Addressing Protocol) ที่นำเสนอเป็นการใช้แสงในการสื่อสารทั้งหมด การที่จะให้ผลของการทำงานของแบบจำลองเครือข่ายเกิดประสิทธิภาพและประสิทธิผลสูงสุด ทำให้การส่งผ่านข้อมูลระหว่างระดับชั้นย่อย (Sub Layer) ในโปรโตคอล จะต้องใช้สัญญาณแสงในการห่อหุ้มสัญญาณ (Optical Encapsulation) รวมถึงการยืนยันบุคคลภายในเครือข่าย จะต้องใช้สัญญาณแสงเป็นสิ่งที่ใช้ในการระบุที่อยู่ภายในเครือข่าย (Optical Address) ด้วยเช่นกัน และการเข้ารหัสสัญญาณต้องใช้สัญญาณแสงในการประมวลข้อมูลทั้งหมด (Optical Cryptography)

1.6 ขอบเขตการวิจัย

1.6.1 เป็นการศึกษาวิจัยโดยใช้การจำลองทางคณิตศาสตร์ (Simulation) เพื่อทดสอบโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง (Optical Transmission and Addressing Protocol) ที่นำเสนอเท่านั้น ไม่มีการสร้าง (Fabrication) อุปกรณ์ทางแสงเพื่อการทดสอบโปรโตคอลดังกล่าว

1.6.2 เป็นการศึกษาวิจัยโดยใช้การจำลองเครือข่ายสื่อสาร เพื่ออธิบายผลการทำงานของเครือข่ายในด้านความปลอดภัยของการสื่อสารข้อมูลเท่านั้น ไม่มีการทดสอบการโจมตีด้วยวิธีการจริง

1.6.3 เป็นการศึกษาวิจัยการสื่อสารข้อมูลภายในเครือข่ายโดยใช้โปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง (Optical Transmission and Addressing Protocol) ที่พัฒนาขึ้นโดยไม่รวมถึงการ Synchronization สัญญาณที่ส่งภายในเครือข่ายสื่อสาร

1.6.4 เป็นการศึกษาวิจัยการสื่อสารข้อมูลภายในเครือข่ายโดยใช้โปรโตคอลที่พัฒนาขึ้นโดยไม่รวมถึงการสูญเสียระหว่างอุปกรณ์เชิงแสง

1.7 เนื้อหาวิทยานิพนธ์

วิทยานิพนธ์ฉบับนี้ แบ่งเนื้อหาออกเป็น 7 บท คือ

บทที่ 1 กล่าวถึงที่มาและความสำคัญของวิทยานิพนธ์ เป้าหมายของการวิจัยและวัตถุประสงค์ สมมติฐาน จุดมุ่งหมายของการศึกษา ทฤษฎีที่ใช้ และขอบเขตของการวิจัย

บทที่ 2 กล่าวถึงทฤษฎีพื้นฐานที่ใช้ในการวิจัย พื้นฐานของการสื่อสารข้อมูลด้วยแสง และทฤษฎีที่ใช้ในการพัฒนาโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง (Optical Transmission and Addressing Protocol) ซึ่งประกอบด้วย การสื่อสารข้อมูลด้วยแสง โซลิตอนแสง (Optical Soliton) วงแหวนสั่นพ้อง (Ring Resonator) เป็นต้น และมีการกล่าวถึงงานวิจัยที่เกี่ยวข้อง

บทที่ 3 กล่าวถึงโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง (Optical Transmission and Addressing Protocol) อธิบายถึงรูปแบบของเครือข่ายที่โปรโตคอลที่นำเสนอรองรับ ผลการจำลองเครือข่ายเชิงแสง รวมถึงสรุปผลการจำลองโปรโตคอลการส่งข้อมูลที่นำเสนอในวิทยานิพนธ์นี้

บทที่ 4 กล่าวถึงการสื่อสารข้อมูลด้วยโปรโตคอลที่นำเสนอ อธิบายการส่งข้อมูลระหว่างระดับชั้นย่อย การส่งข้อมูลภายในเครือข่าย การส่งกุญแจเชิงแสงภายในเครือข่าย และผลของพารามิเตอร์ต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ด้านการสื่อสารข้อมูล รวมถึงข้อจำกัดการทำงานของโปรโตคอลด้านการสื่อสารข้อมูล

บทที่ 5 กล่าวถึงการระบุที่อยู่ภายในเครือข่ายด้วยโปรโตคอลที่นำเสนออธิบายที่อยู่เชิงแสง (Optical Address) การเปรียบเทียบที่อยู่เชิงแสงกับ IP Address v4 และผลของพารามิเตอร์ต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ด้านการระบุที่อยู่ภายในเครือข่าย รวมถึงข้อจำกัดการทำงานของโปรโตคอลด้านการระบุที่อยู่ภายในเครือข่าย

บทที่ 6 กล่าวถึงความปลอดภัยในการส่งข้อมูลของโปรโตคอลที่นำเสนอ อธิบายการซ่อนกุญแจและการกู้คืนกุญแจ (Key Suppression and Recovery) เครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) ผลของพารามิเตอร์ต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ด้านความปลอดภัยในการส่งข้อมูล และข้อจำกัดการทำงานของโปรโตคอลด้านความปลอดภัยในการส่งข้อมูล รวมถึงอธิบายการป้องกันการโจมตีด้วยโปรโตคอลที่นำเสนอ

บทที่ 7 กล่าวถึงบทสรุปผลการวิจัยและแนวทางการศึกษาวิจัยในอนาคต

บทที่ 2
ทฤษฎีพื้นฐานและงานวิจัยที่เกี่ยวข้อง

ในส่วนของบทนี้เป็นการกล่าวถึงทฤษฎีพื้นฐาน กล่าวคือ ทำความเข้าใจเรื่องแสงเพื่อใช้เป็นพื้นฐานในการศึกษาวิจัยในลำดับต่อไป รวมถึงอุปกรณ์เชิงแสงที่ใช้ในการพัฒนาโปรโตคอลที่นำเสนอ ซึ่งเนื้อหาทั้งหมดจำเป็นสำหรับการศึกษาวิจัย โดยมีหัวข้อต่าง ๆ ดังนี้

- คุณสมบัติของแสง
- การลดทอนของแสงภายในเส้นใยแก้วนำแสง
- การหักเหแสงแบบไม่เป็นเชิงเส้น (Nonlinear Refraction: Optical Kerr Effect)
- การโพลาไรซ์ของแสง (Polarization of Light)
- โซลิตอนแสง (Optical Soliton)
- วงแหวนสั่นพ้อง (Ring Resonator)
    - พื้นฐานและโครงสร้างของวงแหวนสั่นพ้อง
    - วงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter)
    - วงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator)
- ขนาดของวงแหวนสั่นพ้อง (Ring Resonator) ที่สร้างได้
- มัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer)
- ไมเคิลสันอินเตอร์เฟียร์โรมิเตอร์ (Michelson Interferometer)
- งานวิจัยที่เกี่ยวข้อง
    - Optical Transport Network (OTN)

2.1 คุณสมบัติของแสง

แสงเป็นคลื่นแม่เหล็กไฟฟ้าชนิดหนึ่ง ซึ่งเกิดจากการเคลื่อนที่ของอนุภาคโฟตอนไปในทุก ๆ ความยาวคลื่นของแสง โดยคุณสมบัติพื้นฐานที่สำคัญของคลื่นแสงมีดังนี้ [27–30]

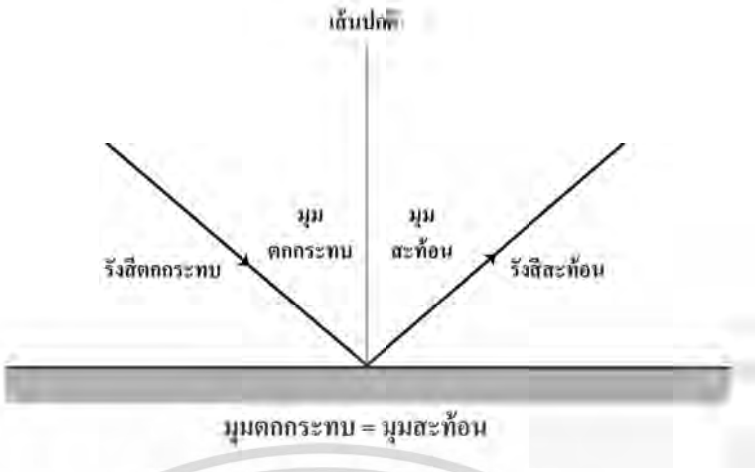
1) แสงเดินทางเป็นเส้นตรง ในตัวกลางที่มีค่าดัชนีหักเห (Refractive Index, n) เท่ากันแสงจะเดินทางเป็นเส้นตรง ซึ่งดัชนีหักเหของแสงคืออัตราส่วนความเร็วแสงที่เคลื่อนที่ภายในวัสดุชนิดนั้นเทียบกับความเร็วแสงในสุญญากาศ โดยค่าดัชนีหักเหของวัตถุ (n) สามารถหาได้จากสมการ (2.1)

$$n = c / v \tag{2.1}$$

เมื่อ n คือ ดัชนีหักเหของวัตถุ c คือ ความเร็วแสงในสูญญากาศ (3×10^8 m/s) และ v คือ ความเร็วแสงในตัวกลางนั้น

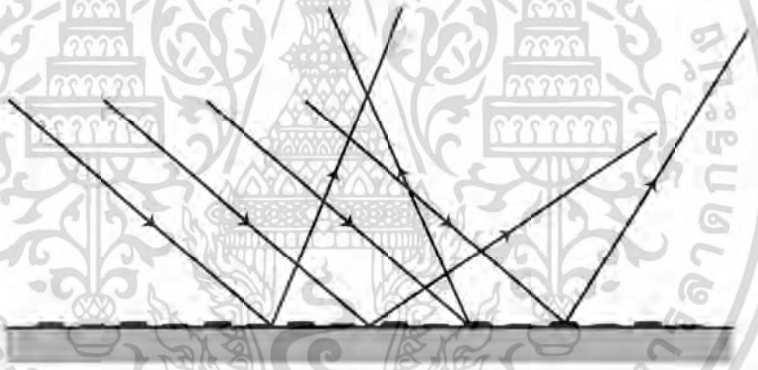
2) การสะท้อน เมื่อแสงตกกระทบวัตถุจะเกิดการสะท้อนซึ่งเป็นไปตามกฎการสะท้อน (Law of Reflection) ของแสงที่ว่า มุมตกกระทบมีค่าเท่ากับมุมสะท้อนเสมอ การสะท้อนของแสงสามารถแบ่งได้เป็น 2 ลักษณะ

- การสะท้อนแบบปกติ (Regular Reflection) เกิดขึ้นเมื่อแสงตกกระทบวัตถุผิวมันวาว แสดงดังรูปที่ 2.1



รูปที่ 2.1 การสะท้อนแบบปกติ (Regular Reflection)

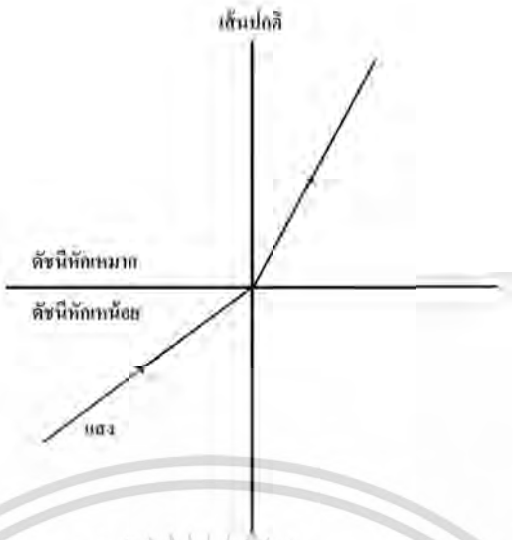
- การสะท้อนแบบกระจาย (Diffuse Reflection) เกิดขึ้นเมื่อแสงเคลื่อนที่ตกกระทบวัตถุที่มีพื้นผิวขรุขระ แสดงดังรูปที่ 2.2



รูปที่ 2.2 การสะท้อนแบบกระจาย (Diffuse Reflection)

3) การหักเห เมื่อแสงเคลื่อนที่ผ่านตัวกลางที่มีค่าดัชนีหักเหไม่เท่ากันโดยลำแสงที่ตกกระทบจะต้องไม่ทำมุมตั้งฉากกับวัตถุและมุมตกกระทบต้องมีค่าน้อยกว่ามุมวิกฤตหรือมุมตกกระทบที่ทำให้แสงท้อนกลับหมด โดยการหักเหของแสงสามารถแบ่งได้เป็น 2 ลักษณะ

- เมื่อแสงเคลื่อนที่จากตัวกลางที่มีค่าดัชนีหักเหน้อยไปยังตัวกลางที่มีค่าดัชนีหักเหมาก แล้วลำแสงจะหักเหเบนเข้าหาเส้นปกติแสดงดังรูปที่ 2.3



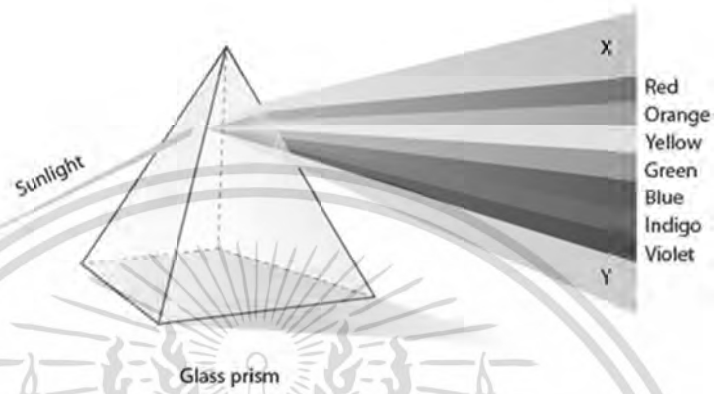
รูปที่ 2.3 การหักเหเมื่อแสงเคลื่อนที่จากตัวกลางที่มีค่าดัชนีหักเหน้อยไปยังตัวกลางที่มีค่าดัชนีหักเหมาก

- เมื่อแสงเคลื่อนที่จากตัวกลางที่มีค่าดัชนีหักเหมากไปยังตัวกลางที่มีค่าดัชนีหักเหน้อย แล้วลำแสงจะหักเหเบนออกจากเส้นปกติแสดงดังรูปที่ 2.4

รูปที่ 2.4 การหักเหเมื่อแสงเคลื่อนที่จากตัวกลางที่มีค่าดัชนีหักเหมากไปยังตัวกลางที่มีค่าดัชนีหักเหน้อย

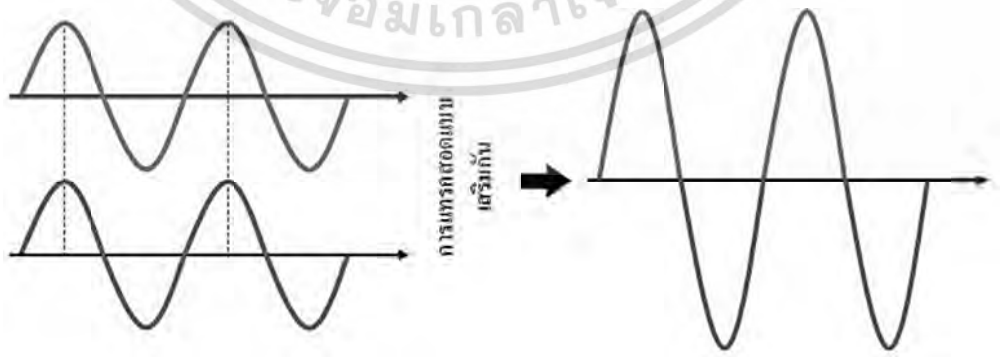
4) การกระจาย โดยธรรมชาติแสงประกอบด้วยหลายความยาวคลื่นผสมกัน เช่นแสงขาวที่มองเห็นโดยทั่วไปนั้นสามารถแยกเป็นสีต่าง ๆ โดยใช้แท่งปริซึมซึ่งการที่แสงแยกออกมานี่เรียกว่าการกระจาย (Dispersion) ซึ่งกระบวนการนี้เกิดขึ้นได้เนื่องจากแสงแต่ละความยาวคลื่น (แต่ละความยาวคลื่นจะมีสีที่แตกต่างกัน) จะเคลื่อนที่ผ่านตัวกลางใด ๆ ที่ไม่ใช่สูญญากาศด้วยความเร็วที่ต่างกัน

ซึ่งโดยปกติแล้วแสงที่เคลื่อนที่ผ่านตัวกลางที่ประกอบด้วยอะตอมและอิเล็กตรอนที่มีการเคลื่อนที่ตลอดเวลา ทำให้การเปลี่ยนแปลงสนามแม่เหล็กและสนามไฟฟ้าของแสงที่มีความถี่สูงทำได้ยากกว่า จึงเป็นผลทำให้แสงความถี่สูงจะเคลื่อนที่ได้ช้ากว่าแสงที่มีความถี่ต่ำในตัวกลางเดียวกันแสดงดังรูปที่ 2.5 แต่ในวัสดุสารกึ่งตัวนำแบบไม่เชิงเส้นหรืออภิวัสดุ (Meta Material) บางประเภทอาจให้ผลที่แตกต่างไปตามค่าพารามิเตอร์

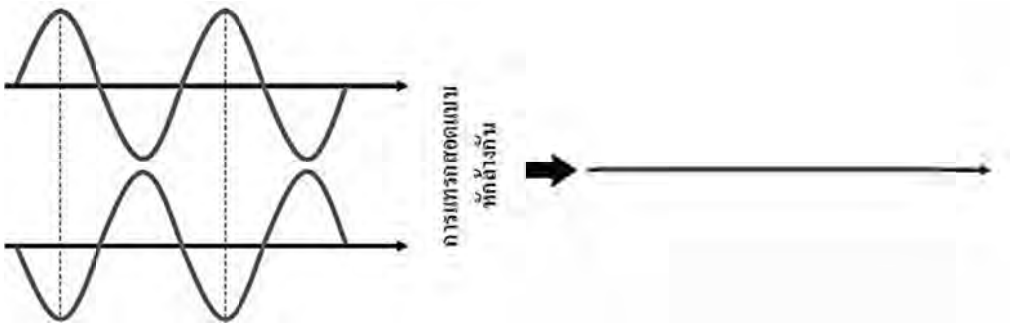


รูปที่ 2.5 การแยกแสงสีต่าง ๆ โดยใช้แท่งปริซึม

5) การแทรกสอด คือ การรวมกันของคลื่นตั้งแต่สองขบวนขึ้นไป โดยผลลัพธ์การรวมคลื่นจะหาได้จากการรวมกันแบบพีชคณิตโดยตรง ซึ่งการรวมกันของคลื่นแบ่งออกเป็น 2 ลักษณะที่สำคัญคือ การรวมแบบเสริมกัน ตามรูปที่ 2.6 และการรวมแบบหักล้างกัน ตามรูปที่ 2.7 เมื่อมีแหล่งกำเนิดแสงหลายแหล่งจะเกิดการรวมคลื่นเสมอ แต่อาจไม่เห็นผลของการแทรกสอดเนื่องจากแหล่งกำเนิดแสงต่างเป็นอิสระจากกัน ทำให้ความต่างเฟสของแสงจากแต่ละแหล่งไม่คงที่และเปลี่ยนแปลงไปตามเวลา จึงไม่เห็นผลของการแทรกสอด ดังนั้นเงื่อนไขสำคัญเพื่อสังเกตุผลของการแทรกสอด คือความต่างเฟสที่คงตัว แม้ว่าเฟสของคลื่นจะเปลี่ยนตามเวลาแต่แหล่งกำเนิดมีความต่างเฟสคงที่ เรียกว่าแหล่งกำเนิดอาพันธ์ (Coherent) และแหล่งกำเนิดแสงนั้นควรจะมีสีเดียว (Monochromatic) หรือมีความยาวคลื่นหรือความถี่ค่าเดียวกัน



รูปที่ 2.6 การแทรกสอดแบบเสริมกัน



รูปที่ 2.7 การแทรกสอดแบบหักล้างกัน

2.2 การลดทอนของแสงภายในเส้นใยแก้วนำแสง

ในการส่งสัญญาณแสงไปบนเส้นใยแก้วนำแสงนั้นมีหลายปัจจัยที่ทำให้เกิดการลดทอนของแสงภายในเส้นใยแก้วนำแสง ดังต่อไปนี้

1) จากการดูดกลืนแสง (Absorption Loss) เกิดจากพวกไฮดรอกไซด์ไอออน (OH^-) ที่ประกอบด้วยอะตอมออกซิเจนและไฮโดรเจนยึดเข้าด้วยกันอยู่ในใยแก้วนำแสง

2) จากการกระจายแสงแบบเรย์ลี (Reyleigh Scattering Loss) เกิดจากความยาวคลื่นแสงมีขนาดเท่ากับองค์ประกอบที่อยู่ในสายทำให้แสงเกิดการกระจัดกระจาย

3) จากการกระจายแสงอันเนื่องมาจากความไม่สม่ำเสมอของโครงสร้างในใยแก้วนำแสง (uniformity loss) เนื่องจากการผลิตที่ไม่ได้มาตรฐาน ทำให้ใยแก้วนำแสงไม่มีความเรียบ เมื่อแสงกระทบจึงเกิดการกระจัดกระจายของแสงออกไป

4) จากการกระจายแสงอันเนื่องมาจากการโค้งงอของใยแก้วนำแสง (Bending Loss) เนื่องจากการติดตั้งใยแก้วนำแสงมีการโค้งงอมากเกินข้อกำหนด ทำให้แสงที่ตกกระทบบริเวณที่โค้งงอทำให้เกิดการกระจัดกระจายของแสง

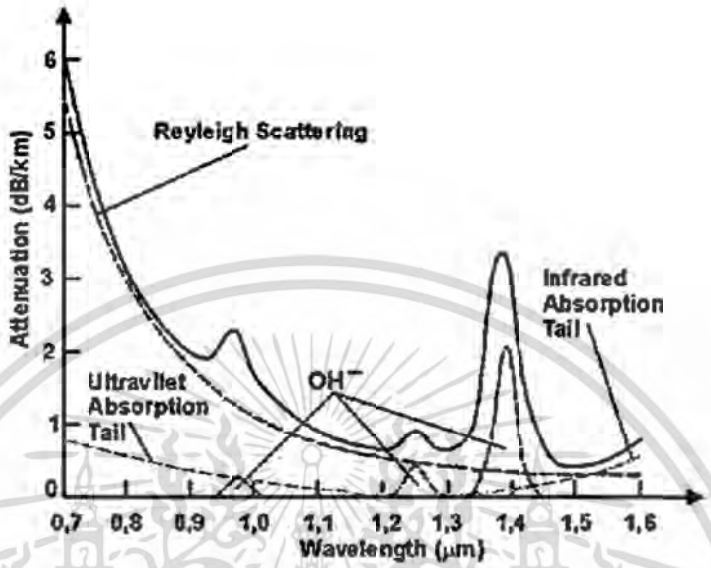
5) จากการกระจายแสงอันเนื่องมาจากการโค้งงอแบบ Micro Bending เนื่องจากมีแรงจากภายนอกมากระทำกับใยแก้วนำแสงแล้วทำให้ใยแก้วนำแสงเกิดการบิดงอออกไป

6) จากการต่อเชื่อมใยแก้วนำแสง การต่อเชื่อมเส้นใยแก้วนำแสงจะต้องทำให้ส่วนของแกนตรงกันสนิท มิเช่นนั้นจะทำให้แสงไม่สามารถเดินทางผ่านได้

7) การลดทอนแสง (Attenuation) โดยกำลังของแสงจากแหล่งกำเนิดแสง (P_i) ที่ถูกส่งเข้าไปในใยแก้วนำแสงยาว L กิโลเมตรแล้วกำลังของแสงที่ออกจากเส้นใยแก้วนำแสง (P_o) เมื่อพิจารณาที่ $P_o < P_i$ โดยทั่วไปแล้วการสูญเสียกำลังของแสงในใยแก้วนำแสงจะถูกกำหนดค่าสัมประสิทธิ์การลดทอน (Attenuation Coefficient, α) เมื่อ f คือความถี่ของแสง ซึ่งแทนด้วยความสัมพันธ์ คือ

$$Attenuation = \alpha Lf = 10\log(\frac{P_0}{P_i}) \quad (2.2)$$

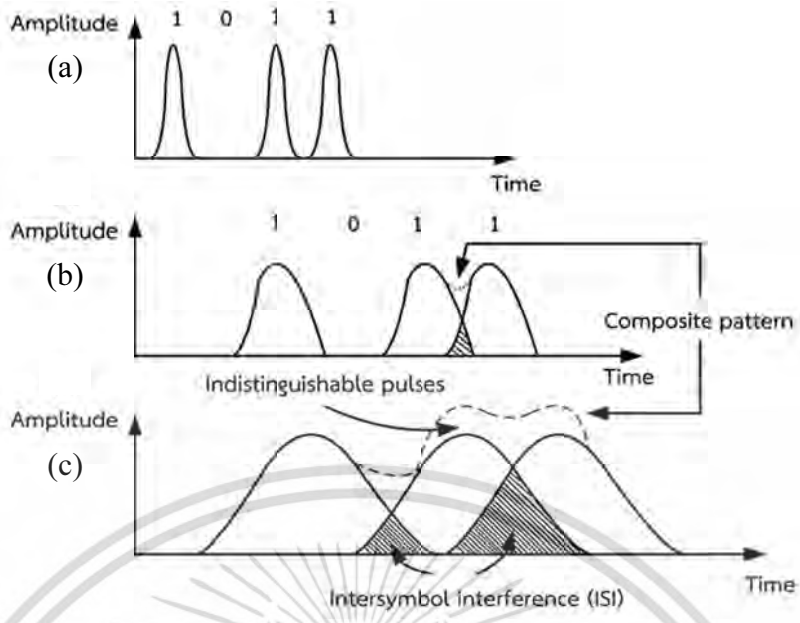
เมื่อการลดทอนกำลังของแสงในใยแก้วนำแสงนั้นมีผลมาจากการดูดกลืนแสงของตัวกลาง หรือการสะท้อนรังสีของแสง รวมถึงการโค้งงอของใยแก้วนำแสง โดยที่แต่ละช่วงความยาวคลื่นแสงนั้นมีค่าการลดทอนของแสงไม่เท่ากันแสดงดังรูปที่ 2.8



รูปที่ 2.8 การลดทอนของแสงในใยแก้วนำแสงสัมพันธ์กับความยาวคลื่น

8) การกระจายแสง (Dispersion) การกระจายแสงเป็นการกว้างออก (Broadening) หรือผิดเพี้ยน (Distortion) ของสัญญาณแสง (Optical Signal) ที่เคลื่อนที่ในใยแก้วนำแสง กล่าวคือ เมื่อป้อนแสงที่เป็นพัลส์เข้าที่ปลายข้างหนึ่งของใยแก้วนำแสง แสงที่ออกจากปลายอีกข้างหนึ่งจะมีความกว้างของพัลส์เพิ่มขึ้นจากเดิม เรียกการขยายออกในลักษณะนี้ว่าการกระจายแสง

เมื่อพัลส์แสงเคลื่อนที่ไปในใยแก้วนำแสงจะเกิดการขยายออกและซ้อนทับ (Overlaps) กับพัลส์ข้างเคียงเกิดการแทรกสอดระหว่างกัน (Inter Symbol Interference, ISI) ทำให้พัลส์แสงที่ออกจากใยแก้วนำแสงมีลักษณะเป็นพัลส์ที่ไม่สามารถจำแนกได้ (Indistinguishable pulse) แสดงตัวอย่างดังรูป 2.9



รูปที่ 2.9 สัญญาณ Output เมื่อเกิดการกระจาย

โดยสัญญาณนำเข้า (Input) มีลักษณะแสดงด้วยกราฟของความสัมพันธ์ระหว่างแอมพลิจูด (Amplitude) กับเวลา ดังรูปที่ 2.9 (a) โดยมีลักษณะของสัญญาณส่งออกแสดงดังรูปที่ 2.9 (b) – 2.9 (c) ซึ่งมีลักษณะเป็นแบบเชิงซ้อน (Composite Pattern)

2.3 การหักเหแสงแบบไม่เป็นเชิงเส้น (Nonlinear refraction: Optical Kerr Effect)

ในปัจจุบันนี้ การใช้วัสดุที่มีผลตอบสนองทางแสงแบบไม่เป็นเชิงเส้น มาเป็นส่วนประกอบในการสร้างตัวนำคลื่นกำลังได้รับความสนใจ และมีการศึกษาวิจัยกันอย่างกว้างขวาง เนื่องจากสามารถนำปรากฏการณ์แบบไม่เป็นเชิงเส้นของแสงมาประยุกต์ใช้งานร่วมกับโครงข่ายการสื่อสารด้วยแสงได้หลายรูปแบบ เช่น การประมวลผลสัญญาณด้วยแสงโดยตรง [31-33] การประยุกต์ใช้งานทางด้านความปลอดภัยของข้อมูล [34] และการสร้างแหล่งกำเนิดแสงชนิดพิเศษที่ไม่สามารถสร้างขึ้นได้ด้วยวิธีการทำงานแบบปกติ [35] การหักเหแบบไม่เป็นเชิงเส้นของแสง [36,37] จะเริ่มต้นพิจารณาได้จากคลื่นแสงที่เป็นปริมาณค่าจริง ซึ่งมักจะอยู่ในรูปของสมการ (2.3)

$$E(t) = E_{\omega} \cos(\omega t) \tag{2.3}$$

โดย E_{ω} คือเวกเตอร์ขนาดของคลื่นแสงที่พิจารณา ค่าดัชนีหักเหของแสงที่ไม่เป็นเชิงเส้นเป็นผลเนื่องมาจาก ค่าความไม่เป็นเชิงเส้นลำดับที่สาม $\chi^{(3)}$ ซึ่งส่งผลให้เกิดการเปลี่ยนแปลงของความเข้มแสงแบบไม่เป็นเชิงเส้น โดยความเข้มของแสงที่เดินทางผ่านตัวกลางจะมีค่าขึ้นอยู่กับดัชนีหักเหของวัสดุที่ใช้สร้างตัวกลางนั้น กล่าวคือค่าดัชนีหักเหของวัสดุจะเปลี่ยนไปเมื่อทำการเปลี่ยนความเข้มของแสงที่เดินทางผ่านวัสดุนั้น ขณะเดียวกันเมื่อดัชนีหักเหของวัสดุเปลี่ยนก็จะส่งผลให้ความเข้ม

ของแสงที่เดินทางผ่านวัสดุนั้นเปลี่ยนแปลงไปเช่นกัน ในวัสดุสารที่เป็นชนิดไอโซทรอปิค (Isotropic Material เช่น silica) เพื่อง่ายต่อการพิจารณาจะสามารถกำหนดให้ $\chi^{(2)} = 0$ เนื่องจากความสมมาตรของวัสดุสาร [38] ดังนั้นการโพลาไรซ์เมื่อคิดเฉพาะเทอมที่เป็นค่าเชิงเส้นและค่าความไม่เป็นเชิงเส้นลำดับที่สาม $\chi^{(3)}$ จะสามารถแสดงได้ดังสมการ (2.4)

$$P \cong \varepsilon_0 \left[\chi^{(1)} + \frac{3}{4}\chi^{(3)}|E_\omega|^2 \right] E_\omega \cos 3(\omega t) \tag{2.4}$$

และได้ค่าคงที่ไดอิเล็กตริกรวม (Total Dielectric Constant) คือ

$$\varepsilon_r^{tot} = \varepsilon_r + \Delta\varepsilon_r \tag{2.5}$$

เมื่อ $\varepsilon_r = 1 + \chi^{(1)} = n_0^2$ และ $\Delta\varepsilon = \frac{3}{4}\chi^{(3)}|E_x|^2$ ซึ่งค่าดัชนีหักเหของแสงจะมีค่าสัมพันธ์กับค่าคงที่ไดอิเล็กตริก คือ

$$n = \sqrt{\varepsilon_r + \Delta\varepsilon_r} \approx \sqrt{\varepsilon_r} + \frac{\Delta\varepsilon_r}{2\sqrt{\varepsilon_r}} = n_0 + \frac{3\chi^{(3)}}{8n_0}|E_x|^2 \tag{2.6}$$

ความเข้ม I ของคลื่นแสง จะแปรผันตรงกับ $|E|^2$ โดยที่ $I = \frac{1}{2\eta}|E|^2$ เมื่อ η คือความต้านทานของตัวกลางที่คลื่นแสงแพร่กระจายผ่าน ซึ่งเมื่อเปรียบเทียบผลตอบสนองของแสงในตัวกลางชนิดเดียวกัน เพื่อให้ง่ายต่อการพิจารณาจะถือได้ว่า $I = |E|^2$ และค่าดัชนีหักเหส่วนที่ไม่เป็นเชิงเส้นที่สามารถระบุได้โดยค่าความไม่เป็นเชิงเส้นลำดับที่สาม (Third-order Susceptibility) คือ

$$n_2 = \frac{3\chi^{(3)}}{8n_0} \tag{2.7}$$

ดังนั้นความเข้มแสงที่มีค่าขึ้นอยู่กับดัชนีหักเหของวัสดุแบบไม่เป็นเชิงเส้นจะเท่ากับ

$$n = n_0 + n_2 I \tag{2.8}$$

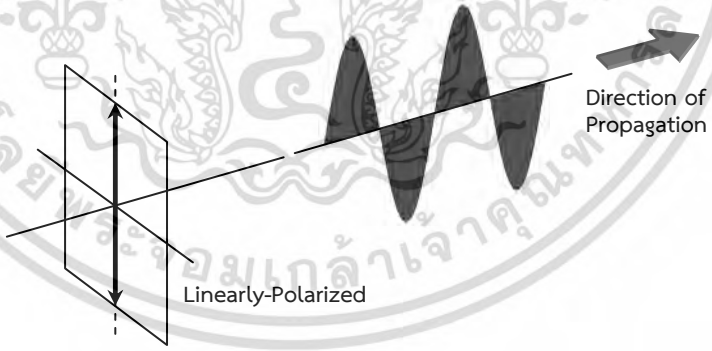
โดยที่ n_0 คือค่าดัชนีการหักเหเชิงเส้น (Linear Refractive Index) n_2 คือค่าดัชนีหักเหแบบไม่เป็นเชิงเส้นลำดับที่สอง (Second-order Nonlinear Refractive Index) และ I คือความเข้มแสง ซึ่งจะส่งผลให้ค่าดัชนีหักเหของตัวนำคลื่นมีการเปลี่ยนแปลงไปตามความเข้มแสงในช่วงที่คลื่นแสงแพร่กระจายผ่านตัวนำคลื่นชนิดไม่เป็นเชิงเส้น

2.4 การโพลาไรซ์ของแสง (Polarization of Light)

แสงเป็นคลื่นแม่เหล็กไฟฟ้าที่มีการเคลื่อนที่ของสนามไฟฟ้าและสนามแม่เหล็กที่สั่น (Oscillate) ไปตามตำแหน่งและเวลา เนื่องจากแสง ณ ตำแหน่งและเวลาใด ๆ จะมีทั้งสนามไฟฟ้าและสนามแม่เหล็กที่ตั้งฉากกัน และสนามทั้งสองยังตั้งฉากกับทิศการเคลื่อนที่ของแสงเสมอ โดยมีขนาดที่สัมพันธ์กันกับอัตราเร็วของแสง ขนาดและทิศทางของสนามแม่เหล็กจะถูกกำหนดด้วยขนาดและทิศทางของสนามไฟฟ้า ดังนั้นเพื่อความสะดวกในการวิเคราะห์คุณสมบัติของแสงจะพิจารณาแต่เพียงสนามไฟฟ้าเท่านั้น และเรียกทิศของสนามไฟฟ้าของแสงว่า ทิศทางการโพลาไรซ์ของแสง

คลื่นแม่เหล็กไฟฟ้าที่ปลดปล่อยออกมาจากการสั่นของอะตอมที่อุณหภูมิสูง (Thermal Light) จะมีทิศของการโพลาไรซ์ตามทิศการสั่นของอะตอม แต่เนื่องจากแหล่งกำเนิดแสงแบบนี้จะมีอะตอมที่ให้กำเนิดแสงจำนวนมาก ซึ่งทิศการสั่นของอะตอมเหล่านี้จะเป็นแบบสุ่ม (Randomly) ดังนั้น แสงที่ได้ออกมาจากแหล่งกำเนิดแสงจึงมีทิศการโพลาไรซ์แบบสุ่มเช่นกัน โดยจะเรียกว่าเป็นแสงที่ไม่โพลาไรซ์ (Non-polarized Light) หรือ แสงธรรมชาติ (Natural Light) แต่ถ้าหากนำแสงที่ไม่โพลาไรซ์นี้มาผ่านตัวกรองโพลาไรซ์ (Polarizer) ซึ่งเป็นอุปกรณ์ที่ยอมให้แสงที่มีทิศของการโพลาไรซ์เฉพาะค่าเท่านั้นผ่านออกมาได้ แสงที่ผ่านมาได้นี้จะกลายเป็นแสงที่มีทิศของการโพลาไรซ์ที่แน่นอนและคงที่ เรียกว่า แสงโพลาไรซ์เชิงเส้น (Linearly Polarized Light) หรือแสงโพลาไรซ์แบบระนาบ (Plane Polarized Light) ดังแสดงในรูปที่ 2.10

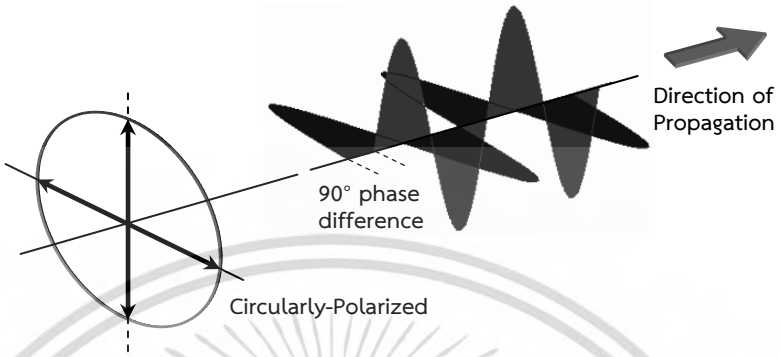
สำหรับแสงที่มีการโพลาไรซ์ไม่คงที่ แต่มีการเปลี่ยนแปลงมุมโพลาไรซ์ไปตามตำแหน่งและเวลาที่แน่นอนสม่ำเสมอ จะเรียกได้ว่าเป็นแสงที่มีการโพลาไรซ์เช่นกัน แต่จะถูกกำหนดให้เป็นการโพลาไรซ์ในอีกสถานะหนึ่ง ซึ่งแบ่งออกได้เป็นแสงโพลาไรซ์แบบวงกลม (Circularly Polarized Light) และแสงโพลาไรซ์แบบวงรี (Elliptically Polarized Light)



รูปที่ 2.10 แสงที่มีการโพลาไรซ์แบบเชิงเส้น

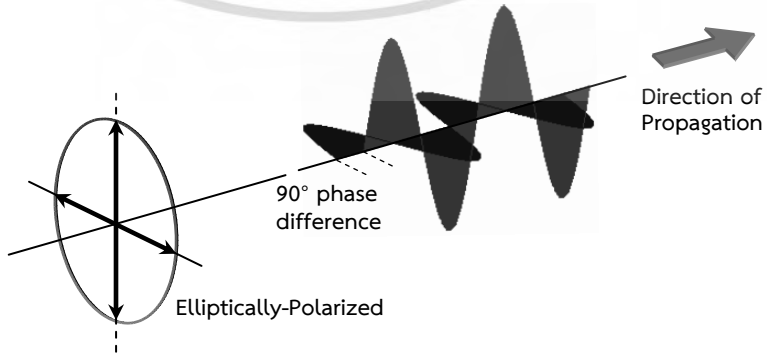
โดยที่แสงโพลาไรซ์แบบวงกลมจะเป็นแสงที่มีองค์ประกอบของเวกเตอร์สนามไฟฟ้าทั้งสององค์ประกอบตั้งฉากกัน มีขนาด (Amplitude) เท่ากัน แต่องค์ประกอบทั้งสองจะมีเฟสต่างกันอยู่ 90° เมื่อพิจารณาสนามไฟฟ้ารวมที่ตำแหน่งหนึ่ง ๆ จะพบว่าทิศของสนามไฟฟ้า หรือทิศของการโพลาไรซ์ของแสงที่ผ่านตำแหน่งนั้น จะหมุนเปลี่ยนไปในลักษณะทวนหรือตามเข้มนาฬิกาแบบใดแบบหนึ่งตามเวลาเสมอ โดยที่มีขนาดคงที่และมีคาบของการหมุนเท่ากับคาบของคลื่นแม่เหล็กไฟฟ้านั้น ๆ หรือถ้าพิจารณาแสง ณ เวลาหนึ่ง ๆ ทิศของสนามไฟฟ้ารวม หรือทิศของการโพลาไรซ์ของแสงที่ผ่านตำแหน่ง

ต่าง ๆ ในเวลานั้น จะหมุนทวน หรือตามเข็มนาฬิกาแบบใดแบบหนึ่งไปตามตำแหน่งเสมอ โดยมีขนาดที่คงที่และมีคาบของการหมุนกลับมาซ้ำทิศทางเดิมเท่ากับความยาวคลื่นของแสงดังแสดงในรูปที่ 2.11



รูปที่ 2.11 แสงที่มีการโพลาไรซ์แบบวงกลม

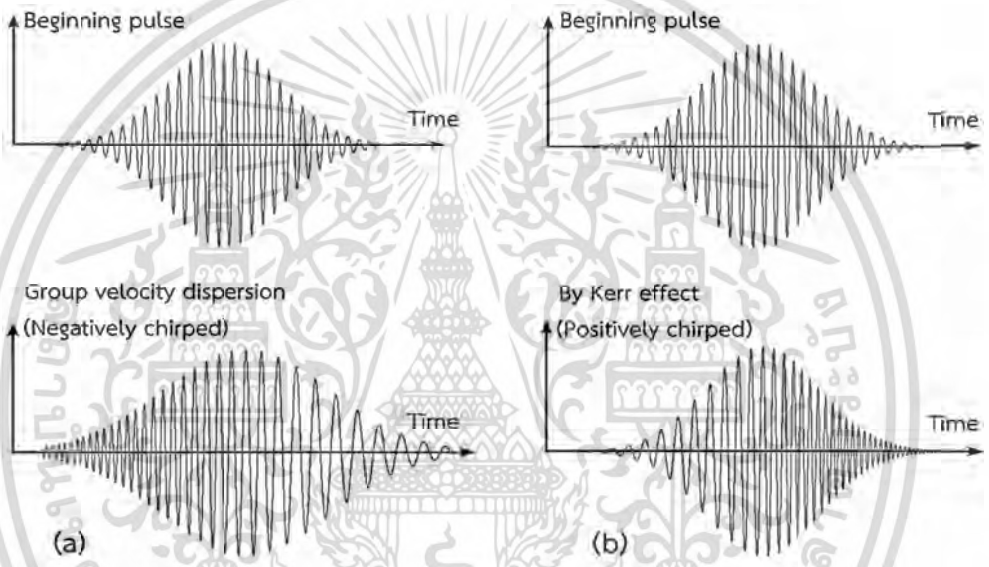
สำหรับแสงที่มีองค์ประกอบของเวกเตอร์สนามไฟฟ้าที่แตกต่างไปจากรูปแบบข้างต้น กล่าวคือแสงที่มีองค์ประกอบของเวกเตอร์สนามไฟฟ้าที่ตั้งฉากกันทั้งสององค์ประกอบ และมีขนาดที่เท่ากัน แต่มีเฟสที่ต่างกันไม่เท่ากับ 0° หรือ 90° หรือองค์ประกอบของเวกเตอร์สนามไฟฟ้าที่ตั้งฉากกันทั้งสององค์ประกอบ มีเฟสต่างกันเท่ากับ 90° แต่มีขนาดที่ต่างกัน เมื่อพิจารณาสนามไฟฟ้ารวมที่ตำแหน่งหนึ่ง ๆ จะพบว่า ทิศของสนามไฟฟ้า หรือทิศของการโพราไรซ์ของแสงที่ผ่านตำแหน่งนั้น จะหมุนเปลี่ยนไปในทิศทางทวน หรือตามเข็มนาฬิกาแบบใดแบบหนึ่งตามเวลาเสมอ โดยที่มีขนาดไม่คงที่ และเสมือนกับว่าสนามไฟฟ้าหมุนรอบตำแหน่งนั้นเป็นรูปวงรี โดยที่มีคาบของการหมุนเท่ากับคาบของคลื่นแม่เหล็กไฟฟ้า หรือถ้าพิจารณาแสง ณ เวลาหนึ่ง ๆ ทิศของสนามไฟฟ้ารวม หรือทิศของการโพราไรซ์ของแสงที่ผ่านตำแหน่งต่าง ๆ ในเวลานั้น จะหมุนทวนหรือหมุนตามเข็มนาฬิกาแบบใดแบบหนึ่งไปตามตำแหน่งเสมอ โดยมีขนาดที่ไม่คงที่ แต่มีทิศการเคลื่อนที่เป็นรูปวงรี และมีคาบของการหมุนกลับมาซ้ำทิศทางเดิมเท่ากับความยาวคลื่นของแสง จะเรียกการโพลาไรซ์ในรูปแบบนี้ว่าแสงโพลาไรซ์แบบวงรี ดังแสดงในรูปที่ 2.12



รูปที่ 2.12 แสงที่มีการโพลาไรซ์แบบวงรี

2.5 โซลิตอนแสง (Optical Soliton)

โดยปกติแล้วขณะที่พัลส์ของคลื่นแสงแพร่กระจาย (Propagation) ไปตามตัวนำคลื่นจะเกิดการกระจายตัวเนื่องจากความเร็วกลุ่ม (Group Velocity Dispersion: GVD) ซึ่งช่วงคลื่นหนึ่งจะประกอบด้วยคลื่นที่มีความถี่ต่าง ๆ กันหลายความถี่และจะแพร่กระจายผ่านตัวนำคลื่นด้วยความเร็วที่ไม่เท่ากัน ดังนั้น เมื่อพัลส์คลื่นแสงเดินทางไปในตัวนำคลื่นได้ระยะหนึ่ง คลื่นส่วนที่มีความถี่ต่ำกว่าจะแยกตัวออกมาทางด้านหลังของพัลส์เนื่องจากมีความเร็วในการเดินทางผ่านตัวนำคลื่นน้อยกว่า (Anomalously Dispersive Medium) ส่งผลให้พัลส์คลื่นมีลักษณะที่ฐานคลื่นขยายตัวไปด้านหลังและพัลส์คลื่นมีขนาดลดลง (Negatively Chirped หรือ Down-chirped) ดังแสดงในรูปที่ 2.13 (a) ซึ่งเป็นสาเหตุหนึ่งที่ทำให้ไม่สามารถส่งสัญญาณพัลส์คลื่นแสงไปในระยะทางไกล ๆ โดยคงรูปเดิมไว้ได้



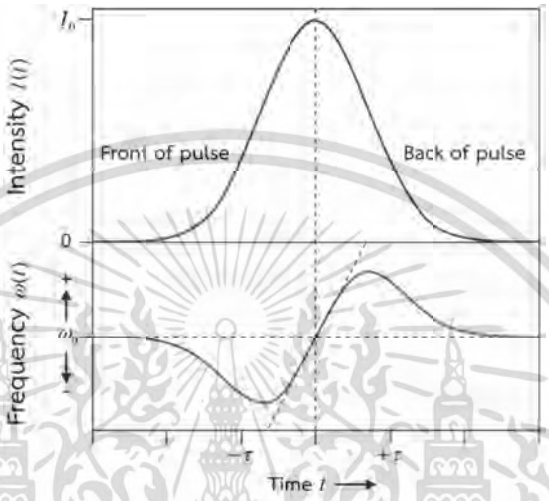
รูปที่ 2.13 พัลส์คลื่นที่ได้รับผลกระทบจาก (a) Group Velocity Dispersion และ (b) Kerr Effect

ปรากฏการณ์แบบไม่เป็นเชิงเส้น (ดัชนีหักเหเป็นฟังก์ชันของความเข้มแสง หรือ Kerr Effect) ยังส่งผลกระทบต่อรูปร่างของพัลส์คลื่นเช่นกัน โดยพิจารณาได้จากเฟสของสนามไฟฟ้าที่แพร่กระจายภายในตัวนำคลื่นดังสมการที่ (2.9) และสามารถพิจารณาความถี่ของสนามไฟฟ้าในช่วงเวลาที่พัลส์คลื่นแสงเดินทางผ่านตัวกลาง ณ ตำแหน่งใด ๆ ได้ดังสมการที่ (2.10) เมื่อ ϕ คือเฟสของสนามไฟฟ้าที่แพร่กระจาย k คือเทอมที่ใช้แทนค่าความไม่เป็นเชิงเส้น ω_0 คือการเลื่อนความถี่ของพัลส์ ω คือความถี่ของสนามไฟฟ้าในช่วงเวลาที่พัลส์คลื่นแสงเดินทางผ่านตัวกลาง

$$\phi(t) = \omega_0 t - kx = \omega_0 t - \frac{2\pi}{\lambda_0}\left[n_0 + n_2 I(t)\right]L \tag{2.9}$$

$$\omega(t) = \frac{d\phi(t)}{dt} = \omega_0 - \left[\frac{2\pi n_2 L}{\lambda_0}\right]\frac{dI(t)}{dt} \tag{2.10}$$

เนื่องจากผลของปรากฏการณ์แบบไม่เป็นเชิงเส้น (Kerr Effect) ความสัมพันธ์ระหว่างอัตราการเปลี่ยนแปลงความเข้มของแสง และความถี่ของคลื่นแสงที่แพร่กระจายไปตามตัวนำคลื่นจะสามารถพิจารณาได้ดังรูปที่ 2.14 โดยพัลส์คลื่นแสงเมื่อเดินทางไปในตัวนำคลื่นได้ระยะหนึ่ง พัลส์คลื่นจะมีลักษณะที่ช่วงหน้าของพัลส์จะประกอบด้วยคลื่นที่มีความถี่ต่ำกว่าช่วงหลังของพัลส์ (คลื่นแสงในช่วงหลังของพัลส์จะมีความถี่สูงกว่าเรียกว่า Positively Chirped หรือ Up Chirped) ดังแสดงในรูปที่ 2.13 (b) ส่งผลให้รูปร่างของพัลส์คลื่นแสงเปลี่ยนแปลงไปเมื่อเดินทางไปถึงปลายทาง



รูปที่ 2.14 ผลกระทบจากปรากฏการณ์ Self Phase Modulation ต่อความถี่ของสัญญาณพัลส์

ปรากฏการณ์ทั้งสองข้างต้นที่ทำให้รูปร่างของพัลส์คลื่นเปลี่ยนแปลงไปนี้ สามารถส่งผลต้านทานซึ่งกันและกันเมื่อมีเงื่อนไขที่เหมาะสม โดยสามารถทำให้ไม่เกิดการกระจายตัวเนื่องจากความเร็วกลุ่ม และความถี่ของพัลส์คลื่นที่แพร่กระจายผ่านตัวนำไม่ขึ้นอยู่กับอัตราการเปลี่ยนแปลงของความเข้มแสง ซึ่งส่งผลให้สามารถส่งสัญญาณพัลส์คลื่นแสงไปในระยะทางไกล ๆ ได้ โดยที่รูปร่างของพัลส์คลื่นยังคงไม่เปลี่ยนแปลง พัลส์คลื่นชนิดพิเศษนี้เรียกว่า โซลิตอน (Soliton) ซึ่งในการวิเคราะห์ทางด้านคณิตศาสตร์สำหรับการหาผลเฉลยของสมการคลื่นแบบไม่เป็นเชิงเส้นสามารถพิจารณาได้จาก [39-41] โดยวิทยานิพนธ์นี้จะเริ่มต้นจาก คลื่นแสงที่แพร่กระจายในตัวนำคลื่นที่มีค่าดัชนีหักเหเปลี่ยนแปลงตามความเข้มของแสง ($n = n_0 + n_2 I$) พิจารณาได้โดย Maxwell Equation และ Nonlinear Schrödinger Equation ซึ่งสามารถแสดงได้ดังสมการ (2.11)

$$i\frac{\partial \psi}{\partial t} = -\frac{1}{2}\frac{\partial^2 \psi}{\partial x^2} + \kappa|\psi|^2\psi \qquad (2.11)$$

โดย κ คือเทอมที่ใช้แทนค่าความไม่เป็นเชิงเส้น และ ψ คือสนามไฟฟ้าของคลื่นที่แพร่กระจายผ่านตัวกลางที่ไม่เป็นเชิงเส้น [42] จากสมการ (2.11) จะสามารถหาผลเฉลยได้ดังสมการที่ (2.12) และ (2.13)

$$\text{Bright Soliton}: \psi(t) = \sqrt{\psi_0}\,\sec h\left[\frac{T}{T_0}\right]\exp\left[\left(\frac{z}{2L_D}\right) - i\omega_0 t\right] \tag{2.12}$$

$$\text{Dark Soliton}: \psi(t) = \sqrt{\psi_0}\,\tan h\left[\frac{T}{T_0}\right]\exp\left[\left(\frac{z}{2L_D}\right) - i\omega_0 t\right] \tag{2.13}$$

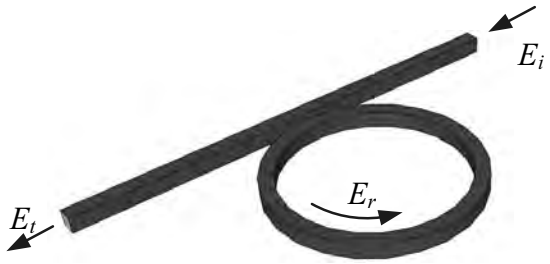
โดยที่ ψ_0 และ z คือขนาดของสนามไฟฟ้าและระยะการแพร่กระจาย (Propagation Distance) ของสนามไฟฟ้าตามลำดับ $T = t - \beta_1 z$ คือเวลาในการแพร่กระจายของพัลส์โซลิตอน (ความกว้างของพัลส์) ในขณะที่คลื่นโซลิตอนเคลื่อนที่ไปตามตัวนำคลื่น โดย β_1 และ β_2 คือ สัมประสิทธิ์การกระจายตัวเชิงเส้น (Linear Dispersive Coefficient) และสัมประสิทธิ์การกระจายตัวไม่เป็นเชิงเส้น (Non-Linear Dispersive Coefficient) ของการกระจายค่าคงที่เฟส ตามลำดับ t คือเวลาในการเลื่อนเฟสของพัลส์โซลิตอน (Soliton Phase Shift Time) $L_D = T_0^2/|\beta_2|$ คือระยะการกระจายตัว (Dispersion Length) ของพัลส์โซลิตอน T_0 คือเวลาในการแพร่กระจายของพัลส์โซลิตอน (ความกว้างของพัลส์) ในขณะเริ่มต้นป้อนเป็นสัญญาณอินพุท และ ω_0 คือการเลื่อนความถี่ (Frequency Shift) ของพัลส์โซลิตอน สำหรับพัลส์โซลิตอนเมื่อแพร่กระจายในวงแหวนสั่นพ้องนี้ ระยะการกระจายตัวเชิงเส้น L_D และระยะการกระจายตัวไม่เป็นเชิงเส้น $L_{NL} = 1/(n_2 k_0 \phi_{NL})$ ต้องสมดุลกัน ดังนั้น $L_D = L_{NL}$ [43]

สมการ (2.12) และ (2.13) จะสามารถรักษารูปร่างและขนาดของพัลส์สัญญาณได้คงที่ตลอดการแพร่กระจาย ซึ่งผลทางคณิตศาสตร์ในขณะนี้ยังไม่สามารถใช้อธิบายคลื่นโซลิตอนในธรรมชาติได้โดยสมบูรณ์ เนื่องจากสัญญาณรบกวนในระบบอาจส่งผลให้เงื่อนไขค่าเริ่มต้นของสมการทางคณิตศาสตร์เปลี่ยนแปลงไป อย่างไรก็ตาม หากขนาดของสัญญาณพัลส์คลื่นที่พิจารณานั้น ๆ ไม่ขึ้นอยู่กับทิศทางการแพร่กระจายของคลื่นก็จะสามารถพิจารณาให้เป็นพัลส์คลื่นโซลิตอนได้ [32]

2.6 วงแหวนสั่นพ้อง (Ring Resonator)

2.6.1 พื้นฐานและโครงสร้างของวงแหวนสั่นพ้อง

การประยุกต์ใช้วงแหวนสั่นพ้องสำหรับการทำงานเป็นตัวกรองช่วงความถี่ผ่าน (Band Pass Filter) ได้ถูกนำเสนอโดย E.A. Marcatili ในปี ค.ศ. 1969 [44] โดยตัวกรองความถี่ดังกล่าวประกอบด้วยตัวนำคลื่นที่มีภาคตัดขวางเป็นรูปสี่เหลี่ยม ชั้นในของตัวนำคลื่นนี้จะใช้วัสดุสารที่มีค่าดัชนีหักเหของแสง (Refractive Index) ค่าหนึ่ง แล้วทำการหุ้มตัวนำคลื่นนี้อีกชั้นหนึ่ง ด้วยวัสดุสารที่มีค่าดัชนีหักเหของแสงที่น้อยกว่า

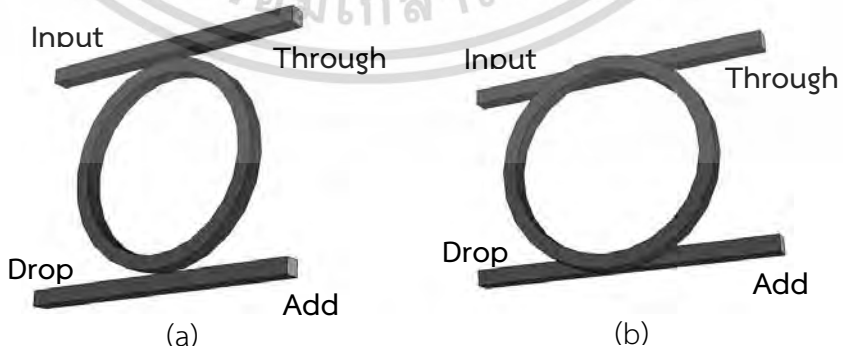


รูปที่ 2.15 แผนภาพแสดงวงแหวนสั่นพ้องที่มีการคัปปลิ้งกับแท่งตัวนำคลื่นแบบเส้นตรงหนึ่งแท่ง

วงแหวนสั่นพ้องที่มีโครงสร้างอย่างง่ายสามารถแสดงได้ดังรูปที่ 2.15 เมื่อป้อนสัญญาณอินพุทเป็นสนามไฟฟ้า E_i ผ่านตัวคัปปลิ้ง (Coupling) สัญญาณส่วนหนึ่งจะถูกแบ่งผ่านเข้าไปในส่วนของตัวนำวงแหวน ได้เป็นสนามไฟฟ้า E_r และสัญญาณส่วนที่เหลือจากการแบ่งผ่านข้างต้น จะส่งผ่านออกไปที่ปลายอีกข้างหนึ่งของตัวนำคลื่นที่เป็นเส้นตรงได้เป็นสนามไฟฟ้า E_t โดยการพิจารณาค่าของการคัปปลิ้งระหว่างแท่งตัวนำคลื่นเส้นตรงกับตัวนำคลื่นวงแหวน จะทำให้สามารถคำนวณหาปริมาณของสัญญาณที่ถูกคัปปลิ้งจากตัวนำคลื่นเส้นตรง ไปยังตัวนำคลื่นวงแหวน หรือจากตัวนำคลื่นวงแหวนไปยังตัวนำคลื่นเส้นตรงได้ โดยค่าการคัปปลิ้งนี้จะขึ้นอยู่กับระยะห่างและความยาวของช่วงใกล้สัมผัสระหว่างตัวนำทั้งสอง จากโครงสร้างของวงแหวนสั่นพ้องเช่นนี้ จะมีผลให้สัญญาณที่มีความยาวคลื่นบางช่วงเท่านั้นที่จะเกิดกำทอน (Resonance) ขึ้นภายในตัวนำคลื่นแบบวงแหวน และสามารถประยุกต์ใช้งานสำหรับการเลือกกรองสัญญาณในช่วงความยาวคลื่นที่ต้องการได้ โดยการเลือกปรับขนาดของวงแหวนสั่นพ้องที่เหมาะสม ซึ่งเป็นไปตามสมการ (2.14)

$$m\lambda_m = nL, \quad m = \text{เลขจำนวนเต็ม} \tag{2.14}$$

โดย m คือ Longitudinal Mode Number, λ_m คือช่วงความยาวคลื่นที่เกิดกำทอน, n คือดัชนีหักเหของวัสดุที่ใช้ทำตัวนำคลื่นแบบวงแหวน และ L คือความยาวเส้นรอบวงของวงแหวนสั่นพ้อง

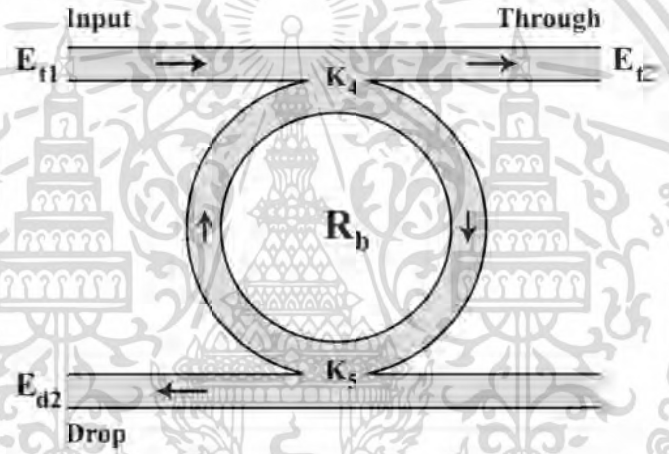


รูปที่ 2.16 โครงสร้างของวงแหวนสั่นพ้องมีสองรูปแบบคือ (a) Horizontal coupling scheme และ (b) Vertical coupling scheme

วงแหวนสั่นพ้องสามารถนำไปประยุกต์ใช้งานในลักษณะของตัวกรองช่วงความยาวคลื่น ตัวมัลติเพล็กซ์ หรือดีมัลติเพล็กซ์สัญญาณแสง ตัวแปลงสัญญาณ และประยุกต์ใช้งานโครงข่ายเส้นทาง (Network routing) ได้ โดยทั่วไปวงแหวนสั่นพ้องที่ใช้เป็นตัวกรองสัญญาณจะมีโครงสร้าง 2 แบบ แสดงดังรูปที่ 2.16 กล่าวคือมีลักษณะที่วงแหวนวางอยู่ระหว่างท่อนำคลื่นแบบขนานสองแท่งในระนาบเดียวกัน หรือวงแหวนวางทับอยู่บนท่อนำคลื่น ซึ่งรูปแบบทั้งสองนี้ จะมี Port ที่สามารถเชื่อมต่อกับระบบภายนอกได้ทั้งหมด 4 port ประกอบด้วยส่วนที่ใช้สำหรับป้อนสัญญาณเข้าได้แก่ Input port และ Add port และส่วนที่ให้สัญญาณออกคือ Through port และ Drop port

จากลักษณะที่วงแหวนวางอยู่ระหว่างท่อนำคลื่นมี 2 แบบ ทั้งแบบระนาบเดียวกันหรือแบบวางทับกัน วิทยานิพนธ์นี้จึงนำเสนอสัญลักษณ์ของวงแหวนสั่นพ้องในลักษณะตามรูปที่ 2.17 – 2.18 เพื่อแทนโครงสร้างทั้ง 2 แบบ

2.6.2 วงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter)



รูปที่ 2.17 วงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter)

วงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) มีลักษณะตามรูปที่ 2.17 โดย E_{t1} แทนสนามไฟฟ้าขาเข้าที่ Input port, E_{t2} แทนสนามไฟฟ้าขาออกที่ Through port, E_{d2} แทนสนามไฟฟ้าขาออกที่ Drop port κ_1 และ κ_2 คือสัมประสิทธิ์การคัปปลิ้งระหว่างตัวนำคลื่นเส้นตรงกับตัวนำคลื่นวงแหวน α คือการลดทอนของความเข้มของแสงภายในตัวนำคลื่น ดังนั้น สนามไฟฟ้าที่ขาออก E_{i2} ที่ Through port คือ [46]

$$E_{t2} = E_{t1}\frac{-\sqrt{1-\kappa_4}\,e^{-\frac{\alpha}{2}L_b - jk_nL_b} + \sqrt{1-\kappa_4}}{1-\sqrt{1-\kappa_4}\sqrt{1-\kappa_5}\,e^{-\frac{\alpha}{2}L_b - jk_nL_b}} \quad (2.15)$$

โดยที่ $L_b = 2\pi R_b$, R_b คือขนาดรัศมีของวงแหวน และกำลังของสัญญาณที่ส่งออกที่ Through Port คือ

$$P_{t2} = (E_{t2}) \cdot (E_{t2})^* = |E_{t2}|^2 \tag{2.16}$$

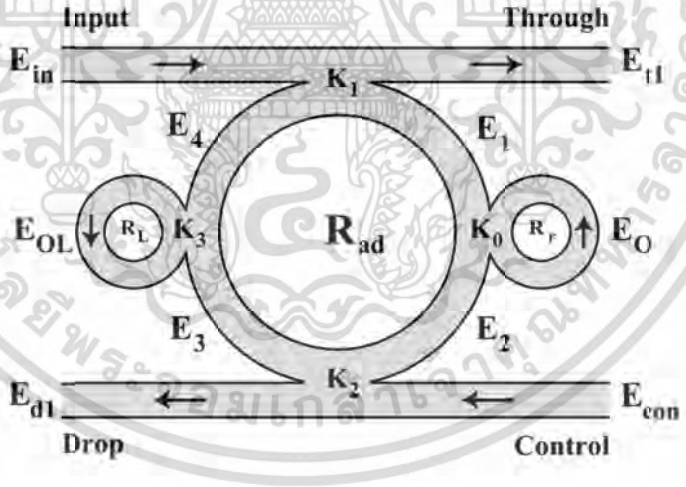
สนามไฟฟ้าที่ขาออก E_{d2} ที่ Drop port คือ

$$E_{d2} = E_{t1} \frac{-\sqrt{\kappa_4 \kappa_5}\, e^{-\frac{\alpha}{2}\frac{L_b}{2} - jk_n \frac{L_b}{2}}}{1 - \sqrt{1-\kappa_4}\sqrt{1-\kappa_5}\, e^{-\frac{\alpha}{2}L_b - jk_n L_b}} \tag{2.17}$$

กำลังของสัญญาณที่ส่งออกที่ Through Port คือ

$$P_{d2} = (E_{d2}) \cdot (E_{d2})^* = |E_{d2}|^2 \tag{2.18}$$

2.6.3 วงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator)



รูปที่ 2.18 วงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator)

วงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) มีลักษณะตามรูปที่ 2.18 ซึ่งวิทยานิพนธ์นี้ใช้ในการสร้างสัญญาณแสงที่ใช้ในการส่งกุญแจเชิงแสง (Optical Key) อย่างปลอดภัย โดยมีสมการทางคณิตศาสตร์ที่เกี่ยวข้อง กล่าวคือ เมื่อมีการนำสัญญาณแสงเข้าทาง Input Port ที่จุดคัปปลิ้งแรก สามารถอธิบายเป็นสมการทางคณิตศาสตร์ได้ ดังนี้ [47]

$$E_{t1} = \sqrt{1-\gamma_1}\left[\sqrt{1-\kappa_1}E_{in} + j\sqrt{\kappa_1}E_4\right] \tag{2.19}$$

$$E_1 = \sqrt{1-\gamma_1}\left[\sqrt{1-\kappa_1}E_4 + j\sqrt{\kappa_1}E_{in}\right] \tag{2.20}$$

$$E_2 = E_0 E_1 e^{-\frac{\alpha}{2}\frac{L}{2} - jk_n\frac{L}{2}} \tag{2.21}$$

โดยที่ κ_1 คือสัมประสิทธิ์การคัปปลิ้งระหว่างตัวนำคลื่นเส้นตรงกับตัวนำคลื่นวงแหวน α คือการลดทอนของความเข้มของแสงภายในตัวนำคลื่นและ γ_1 คือสัมประสิทธิการสูญเสียเนื่องจากการคัปปลิ้ง (Intensity Insertion Loss) $k_n = \frac{2\pi}{\lambda}$ คือค่าคงที่ของการแพร่กระจายคลื่น เมื่อ λ คือความยาวคลื่นของสัญญาณเข้า และ $L = 2\pi R_{ad}$, R_{ad} คือขนาดรัศมีของวงแหวนกลาง

ที่จุดคัปปลิ้งที่สอง สามารถอธิบายเป็นสมการทางคณิตศาสตร์ได้ ดังนี้

$$E_{d1} = \sqrt{1-\gamma_2}\left[\sqrt{1-\kappa_2}E_{con} + j\sqrt{\kappa_2}E_2\right] \tag{2.22}$$

$$E_3 = \sqrt{1-\gamma_2}\left[\sqrt{1-\kappa_2}E_2 + j\sqrt{\kappa_2}E_{con}\right] \tag{2.23}$$

$$E_4 = E_{0L}E_3 e^{-\frac{\alpha}{2}\frac{L}{2} - jk_n\frac{L}{2}} \tag{2.24}$$

โดยที่ κ_2 คือสัมประสิทธิ์การคัปปลิ้งระหว่างตัวนำคลื่นเส้นตรงกับตัวนำคลื่นวงแหวน และ γ_2 คือสัมประสิทธิการสูญเสียเนื่องจากการคัปปลิ้ง E_0 และ E_{0L} คือสนามไฟฟ้าบริเวณวงแหวนข้าง R_r และ R_L คือขนาดรัศมีของวงแหวนข้างฝั่งขวา (RHS) และฝั่งซ้าย (LHS) ตามลำดับ บริเวณวงแหวนข้างด้านขวาสามารถอธิบายเป็นสมการทางคณิตศาสตร์ได้ ดังนี้

$$E_2 = \sqrt{1-\gamma}\left[\sqrt{1-\kappa_0}E_1 + j\sqrt{\kappa_0}E_{r2}\right] \tag{2.25}$$

$$E_{r1} = \sqrt{1-\gamma}\left[\sqrt{1-\kappa_0}E_{r2} + j\sqrt{\kappa_0}E_1\right] \tag{2.26}$$

$$E_{r2} = E_{r1}e^{-\frac{\alpha}{2}L_1 - jk_nL_1} \tag{2.27}$$

โดยที่ κ_0 คือสัมประสิทธิ์การคัปปลิ้งระหว่างตัวนำคลื่นเส้นตรงกับตัวนำคลื่นวงแหวน α คือการลดทอนของความเข้มของแสงภายในตัวนำคลื่นและ γ คือสัมประสิทธิการสูญเสียเนื่องจากการคัปปลิ้ง (Intensity Insertion Loss) $k_n = \frac{2\pi}{\lambda}$ คือค่าคงที่ของการแพร่กระจายคลื่น เมื่อ λ คือความยาวคลื่นของสัญญาณเข้า และ $L_1 = 2\pi R_r$, R_r คือขนาดรัศมีของวงแหวนข้างด้านขวา

จากสมการที่ (2.25)-(2.27) ที่วงแหวนข้างด้านขวา (RHS) ถ้าแสงมีการเคลื่อนที่รอบวงแหวน สามารถสรุปเป็นสมการได้ ดังนี้

$$E_{r1} = \frac{j\sqrt{1-\gamma}\sqrt{\kappa_0}E_1}{1-\sqrt{1-\gamma}\sqrt{1-\kappa_0}e^{-\frac{\alpha}{2}L_1 - jk_nL_1}} \tag{2.28}$$

$$E_{r2} = \frac{j\sqrt{1-\gamma}\sqrt{\kappa_0}E_1 e^{-\frac{\alpha}{2}L_1 - jk_nL_1}}{1-\sqrt{1-\gamma}\sqrt{1-\kappa_0}e^{-\frac{\alpha}{2}L_1 - jk_nL_1}} \tag{2.29}$$

ดังนั้น E_0 ของวงแหวนข้างด้านขวาของวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) สามารถสรุปเป็นสมการได้ ดังนี้

$$E_0 = E_1\left\{\frac{\sqrt{(1-\gamma)(1-\kappa_0)} - (1-\gamma)e^{-\frac{\alpha}{2}L_1 - jk_nL_1}}{1-\sqrt{(1-\gamma)(1-\kappa_0)}e^{-\frac{\alpha}{2}L_1 - jk_nL_1}}\right\} \tag{2.30}$$

ในทำนองเดียวกัน E_{0L} ของวงแหวนข้างด้านซ้ายของวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) สามารถสรุปเป็นสมการได้ ดังนี้

$$E_{0L} = E_3\left\{\frac{\sqrt{(1-\gamma_3)(1-\kappa_3)} - (1-\gamma_3)e^{-\frac{\alpha}{2}L_2 - jk_nL_2}}{1-\sqrt{(1-\gamma_3)(1-\kappa_3)}e^{-\frac{\alpha}{2}L_2 - jk_nL_2}}\right\} \tag{2.31}$$

โดยที่ κ_3 คือสัมประสิทธิ์การคัปปลิ้งระหว่างตัวนำคลื่นเส้นตรงกับตัวนำคลื่นวงแหวน α คือการลดทอนของความเข้มของแสงภายในตัวนำคลื่นและ, γ_3 คือสัมประสิทธิการสูญเสียเนื่องจากการคัปปลิ้ง (Intensity Insertion Loss) , $k_n = 2\pi/\lambda$ ค่าคงที่ของการแพร่กระจายคลื่น เมื่อ λ คือความยาวคลื่นของสัญญาณเข้า และ $L_2 = 2\pi R_L$, R_L คือขนาดรัศมีของวงแหวนข้างด้านซ้าย

จากสมการที่ (2.19)-(2.31) E_1, E_3 and E_4 สามารถอธิบายเป็นสมการคณิตศาสตร์ได้ดังนี้ โดยให้ $x_1 = (1-\gamma_1)^{1/2}$, $x_2 = (1-\gamma_2)^{1/2}$, $y_1 = (1-\kappa_1)^{1/2}$ และ $y_2 = (1-\kappa_2)^{1/2}$

$$E_1 = \frac{jx_1\sqrt{\kappa_1}E_{in} + jx_1x_2y_1\sqrt{\kappa_2}E_{0L}E_{con}e^{-\frac{\alpha}{2}\frac{L}{2} - jk_n\frac{L}{2}}}{1-x_1x_2y_1y_2E_0E_{0L}e^{-\frac{\alpha}{2}L - jk_nL}} \tag{2.32}$$

$$E_3 = x_2y_2E_0E_1e^{-\frac{\alpha}{2}\frac{L}{2} - jk_n\frac{L}{2}} + jx_2\sqrt{\kappa_2}E_{con} \tag{2.33}$$

$$E_4 = x_2y_2E_0E_{0L}E_1e^{-\frac{\alpha}{2}L - jk_nL} + jx_2\sqrt{\kappa_2}E_{0L}E_{con}e^{-\frac{\alpha}{2}\frac{L}{2} - jk_n\frac{L}{2}} \tag{2.34}$$

จากสมการที่ (2.19), (2.21), (2.32)-(2.34) สัญญาณออกที่ Through Port (E_{t1}) คือ

$$E_{t1} = x_1 y_1 E_{in} + \begin{pmatrix} jx_1 x_2 y_2 \sqrt{\kappa_1} E_0 E_{0L} E_1 \\ -x_1 x_2 \sqrt{\kappa_1 \kappa_2} E_{0L} E_{i2} \end{pmatrix} e^{-\frac{\alpha}{2}\frac{L}{2} - jk_n \frac{L}{2}} \tag{2.35}$$

กำลังของสัญญาณที่ส่งออกที่ Through Port (P_{t1}) คือ

$$P_{t1} = \left(E_{t1}\right) \cdot \left(E_{t1}\right)^* = \left|E_{t1}\right|^2 \tag{2.36}$$

ในทำนองเดียวกัน จากสมการที่ (2.21), (2.22), (2.32)-(2.34) สัญญาณออกที่ Drop Port (E_{d1}) คือ

$$E_{d1} = x_2 y_2 E_{con} + jx_2 \sqrt{\kappa_2} E_0 E_1 e^{-\frac{\alpha}{2}\frac{L}{2} - jk_n \frac{L}{2}} \tag{2.37}$$

กำลังของสัญญาณที่ส่งออกที่ Through Port (P_{d1}) คือ

$$P_{d1} = \left(E_{d1}\right) \cdot \left(E_{d1}\right)^* = \left|E_{d1}\right|^2 \tag{2.38}$$

2.7 ขนาดของวงแหวนสั่นพ้อง (Ring Resonator) ที่สร้างได้

ในส่วนนี้จะกล่าวถึงขนาดวงแหวนสั่นพ้อง ซึ่งขนาดของวงแหวนสั่นพ้องจะมีผลต่อสัญญาณที่ส่งออกมาจากวงแหวนสั่นพ้องเป็นอย่างมาก ดังนั้น ส่วนนี้แสดงให้เห็น การสำรวจขนาดของวงแหวนสั่นพ้องที่สามารถสร้างได้จริง จากปี 2002 ถึงปี 2016 สำหรับในช่วงทศวรรษที่ผ่านมาผลการสำรวจได้ชี้ให้เห็นว่า เทคโนโลยีที่สูงมากขึ้นจะช่วยให้ลดขนาดวงแหวนสั่นพ้องจาก 200 μm ถึง 1 μm ดังแสดงในตารางที่ 2.1 พารามิเตอร์ขนาดวงแหวนที่มีการพัฒนาเผยแพร่ โดยโปรโตคอลการส่งข้อมูลที่นำเสนอในวิทยานิพนธ์นี้ จะต้องคำนึงขนาดของวงแหวนสั่นพ้องให้อยู่ในช่วงที่สามารถสร้างได้จริง

ตารางที่ 2.1 พารามิเตอร์ขนาดวงแหวนที่มีการพัฒนาเผยแพร่

ลำดับ	ปีที่มีการเผยแพร่	ขนาดของวงแหวน (μm)	ผู้เขียน	เอกสารอ้างอิง
1	2002	10	V. Van et. Al	[48]
2	2003	20-200	Z. Bian et. Al	[49]
3	2004	5	T. Barwicz et. Al	[50]
4	2005	5, 20	Y. Kokuban et. Al	[51]
5	2006	8.004	T. Barwicz et. Al	[52]
6	2006	60	A. Yalçın et. Al	[53]
7	2008	1.5	Q. Xu et. Al	[54]
8	2010	20	H. Cai et. Al	[55]
9	2012	1, 5, 10	W. Bogaerts et. Al	[56]
10	2013	80	P. Rabiei et. Al	[57]
11	2016	5	D. Wu et. Al	[58]

2.8 มัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer)

รูปที่ 2.19 อุปกรณ์ที่ใช้หลักการของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer)

โปรโตคอลที่นำเสนอในวิทยานิพนธ์นี้ ใช้อุปกรณ์ที่ใช้หลักการของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer) ดังรูปที่ 2.19 จะเห็นว่า ที่ Output Port จะมีสนามไฟฟ้าเท่ากับที่ Input Port และจะมีถ้าพิจารณาที่จุด B สามารถสรุปเป็นสมการได้ ดังนี้ [59]

$$E_t = E_{i1} + E_{i2} \tag{2.39}$$

กำลังของสัญญาณที่ส่งออกที่ Output Port (P_t) คือ

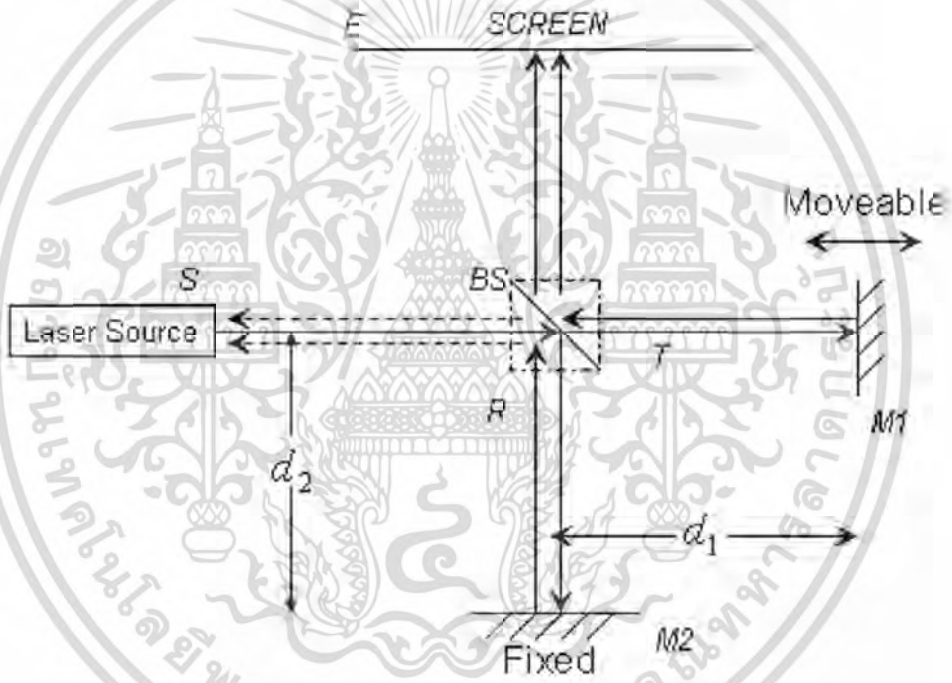
$$P_t = (E_t) \cdot (E_t)^* = |E_t|^2 \tag{2.40}$$

2.9 ไมเคิลสันอินเตอร์เฟียร์โรมิเตอร์ (Michelson Interferometer)

ไมเคิลสันอินเทอร์เฟียร์โรมิเตอร์ (Michelson Interferometer) [60] เป็นเครื่องมือที่อาศัยหลักการแทรกสอดของคลื่นแสงสองขบวน โดยอาศัยหลักการทางแสงของอินเทอร์เฟียโรมิเตอร์สามารถวัดระยะทางในเทอมของความยาวคลื่นได้ ซึ่งนำไปประยุกต์ใช้งานในด้านต่าง ๆ มากมาย เช่น [61-63]

หลักการพื้นฐานของไมเคิลสันอินเทอร์เฟียร์โรมิเตอร์ (Michelson Interferometer)

จากรูปที่ 2.20 แหล่งกำเนิดแสงเดียวกันลำแสงจะถูกแยกออกเป็นแสงสองขบวนด้วย Beam Splitter (BS) โดยปกติลำแสงส่วนหนึ่งจะสะท้อน Reflected (R) และอีกส่วนหนึ่งจะถูกส่งผ่าน Transmitted (T) โดย Beam Splitter (BS) กระบวนการแทรกสอดของแสงโดยหลักของไมเคิลสันอินเทอร์เฟียร์โรมิเตอร์ (Michelson Interferometer) เป็นการแทรกสอดแบบแบ่งแอมปริจูด



รูปที่ 2.20 ไมเคิลสันอินเทอร์เฟียร์โรมิเตอร์ (Michelson Interferometer)

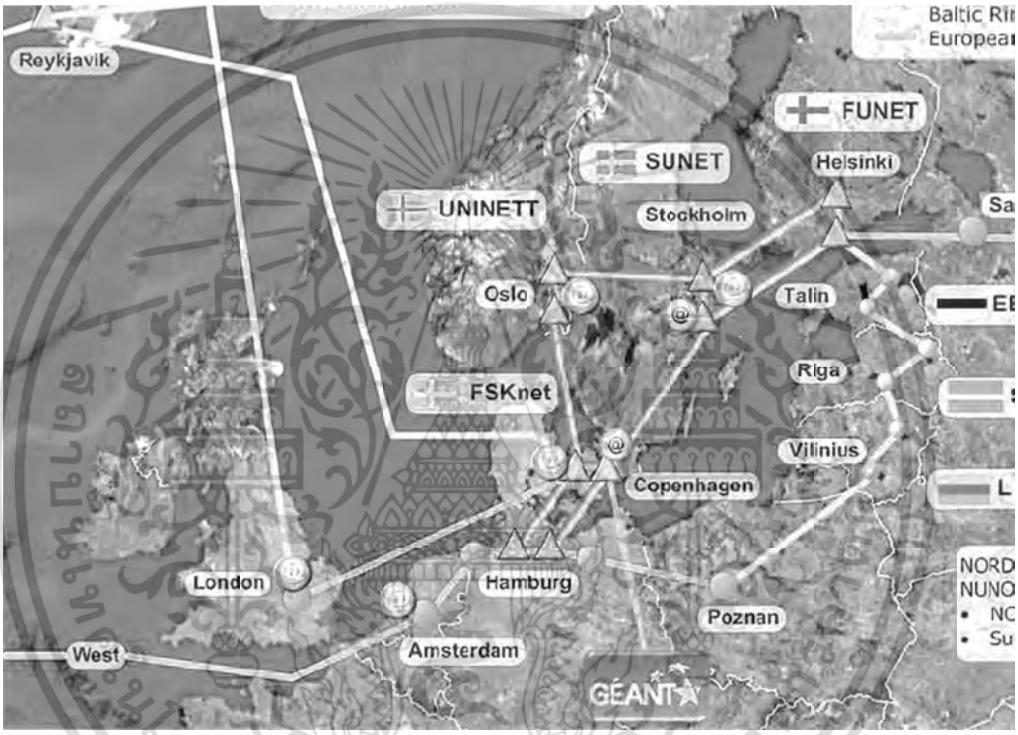
ในหลักพื้นฐานของไมเคิลสันอินเทอร์เฟียร์โรมิเตอร์ (Michelson Interferometer) อธิบายได้ตามรูปที่ 2.20 แหล่งกำเนิดแสง S จะถูกแบ่งลำแสง 50% โดย Beam Splitter (BS) ที่วางขวาง 45 องศากับลำแสง ลำแสงที่ถูกส่งผ่านจะเดินทางไปตกกระทบกระจก M1 และสะท้อนกลับมายัง Beam Splitter (BS) และส่วนหนึ่งหักเหเป็นมุม 90 องศาไปตกกระทบบนฉาก E (แสงอีกส่วนหนึ่งจะส่งผ่านไปยังแหล่งกำเนิดแสงแต่จะไม่สนใจในกรณีนี้) ลำแสงจากแหล่งกำเนิดส่วนที่สะท้อนจาก Beam Splitter (BS) จะเดินทางไปตกกระทบกระจก M2 และจะสะท้อนกลับมาอีกครั้งโดยกระจก แสงที่สะท้อนจากกระจกส่วนหนึ่งจะส่งผ่าน Beam Splitter (BS) ไปตกกระทบฉากที่จุด E (แสงอีกส่วนหนึ่งจะสะท้อนไปยังแหล่งกำเนิดแสงแต่จะไม่สนใจในกรณีนี้) แสงทั้งสองขบวนที่ไปตกกระทบฉากที่จุด E จะเกิดการแทรกสอดกันขึ้นที่ฉาก

2.10 งานวิจัยที่เกี่ยวข้อง

2.10.1 Optical Transport Network (OTN) [64]

2.10.1.1 ภาพรวมของบทความ

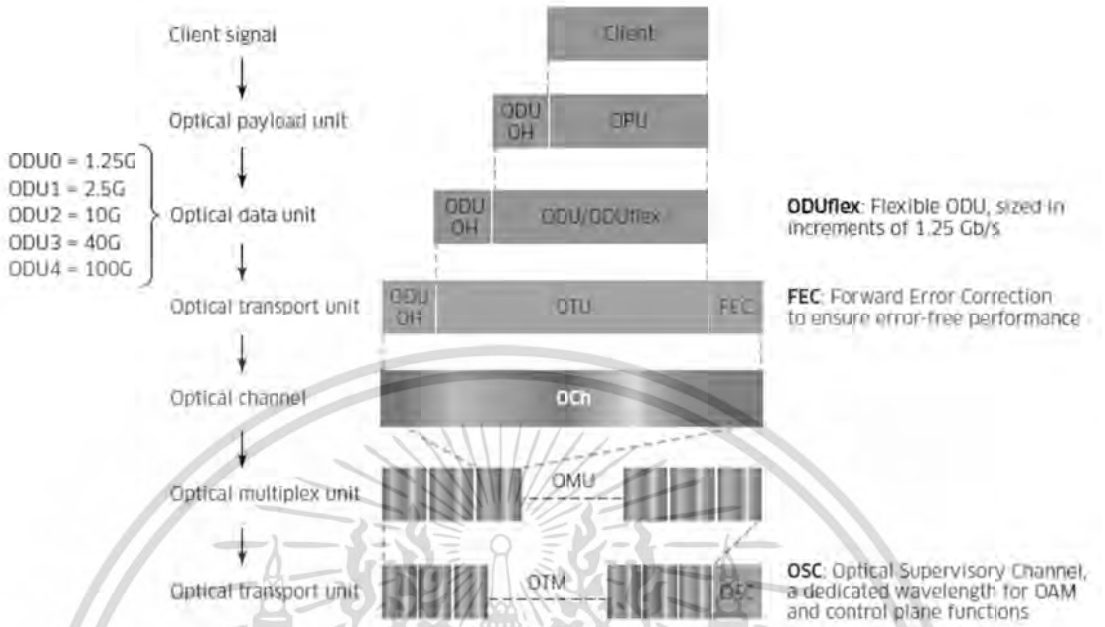
บทความนี้เป็น Technical White Paper ของบริษัท Alcatel-Lucent นำเสนอเรื่อง The Alcatel-Lucent / NORDUnet Project : Transforming a Legacy Network to an Agile Optical Network แสดงให้เห็นถึงการเปลี่ยนแปลงเครือข่ายแบบเดิมให้เป็นเครือข่ายในรุ่นต่อไป โดยที่มีการทดลองใช้งาน Optical Network ที่ใช้ Optical Transport Network (OTN) ในเครือข่าย NORDUnet ตามรูปที่ 2.21



รูปที่ 2.21 NORDUnet : A collaboration of Nordic NRENs

จากรูปที่ 2.21 NORDUnet : A collaboration of Nordic NRENs NORDUnet คือ เครือข่ายขององค์กร Nordic National Research and Education Networks 5 ประเทศ กล่าวคือ Denmark (Forskningsnettet), Finland (Funet), Iceland (RHnet), Norway (Uninett) และ Sweden (SUNET) (มีระยะของการสื่อสารในเครือข่ายประมาณ 2,000 กิโลเมตร) โดยที่เป็นเครือข่ายที่มีการใช้เทคโนโลยี Optical Transport Network (OTN) เพื่อประโยชน์ทางด้านการสื่อสาร และเป็นต้นแบบของระบบสื่อสารในอนาคต

2.10.1.2 ระดับชั้น Optical Transport Network (OTN)



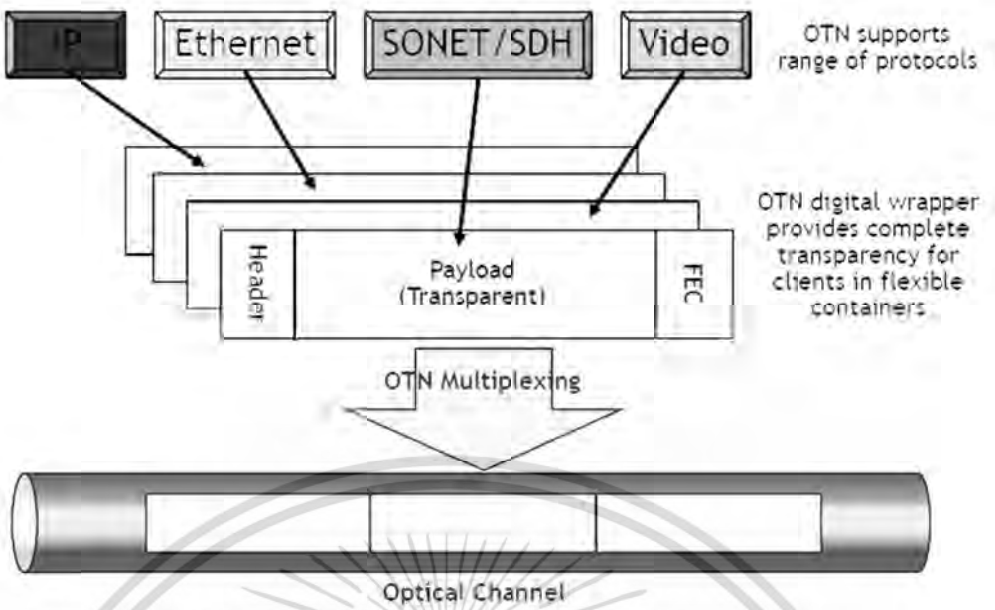
รูปที่ 2.22 OTN hierarchy

จากรูปที่ 2.22 OTN hierarchy แสดงระดับชั้นต่าง ๆ ของ Optical Transport Network (OTN) อธิบายได้ว่า ประกอบด้วย 2 ส่วนหลักคือ Electrical Domain และ Optical Domain โดยที่สัญญาณ OCh ประกอบด้วย Optical Payload Unit (OPU), Optical Channel Data Unit (ODU) และ Optical Channel Transport Unit (OTU)

Optical Payload Unit (OPU) ใช้ในการ Mapping สัญญาณของเครื่องลูกข่าย

Optical Channel Data Unit (ODU) ใช้ในการบริหารจัดการการส่งข้อมูลในเครือข่าย

Optical Channel Transport Unit (OTU) ใช้ในการจัดรูปแบบของสัญญาณที่ซึ่งถูกส่งผ่านไปบนความยาวคลื่น ซึ่งเป็นส่วนหนึ่งของ OCh



รูปที่ 2.23 OTN Supports Variety of Protocols

จากรูปที่ 2.23 OTN Supports Variety of Protocols อธิบายได้ว่า Optical Transport Network (OTN) สนับสนุนการทำงานของโปรโตคอลสื่อสารอื่น ๆ เช่น IP Ethernet เป็นต้น ทำให้ง่ายต่อการใช้งาน Optical Transport Network (OTN) กับเครือข่ายสื่อสารในปัจจุบัน

2.10.1.3 สรุปผลของบทความ

ในการทดสอบการใช้งานกับ NORDUnet อธิบายได้ว่า Optical Transport Network (OTN) ง่ายมากต่อการใช้งานร่วมกับระบบเครือข่ายสื่อสารเดิม เนื่องจาก Optical Transport Network (OTN) สนับสนุนการทำงานของโปรโตคอลสื่อสารดั้งเดิม Optical Transport Network (OTN) มีประโยชน์ทำให้ประสิทธิภาพของ DWDM ดีขึ้น ทำให้เครือข่ายที่มีการใช้งาน Optical Transport Network (OTN) เป็นเครือข่ายในอนาคตที่มีประสิทธิภาพและประสิทธิผลมากกว่าในเครือข่ายปัจจุบัน

บทที่ 3
โปรโตคอลการสื่อสารข้อมูลที่นำเสนอ

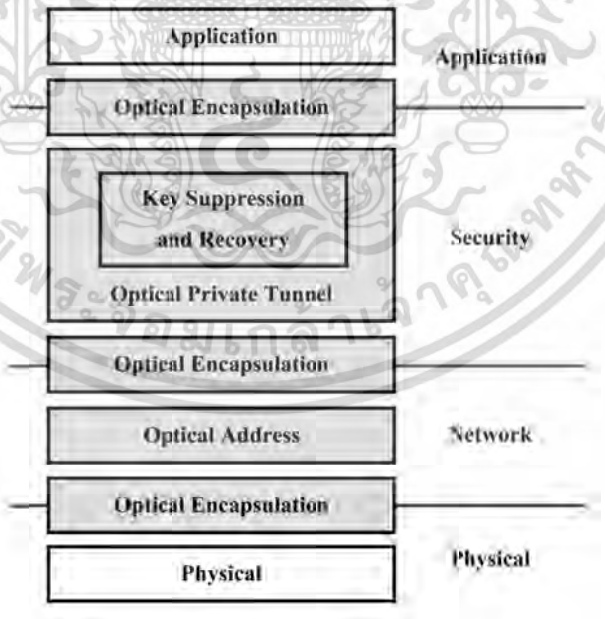
ในส่วนของบทนี้เป็นการกล่าวถึงโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงที่นำเสนอในงานวิจัยนี้ โดยกล่าวถึงรูปแบบของเครือข่ายสื่อสาร (Network Topology) ที่โปรโตคอลที่นำเสนอสามารถใช้งานได้ รวมถึงอธิบายการทำงานของโปรโตคอลที่นำเสนอ และผลของการจำลองการทำงานของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง โดยมีหัวข้อต่าง ๆ ดังนี้

- โปรโตคอลการสื่อสารข้อมูลที่นำเสนอ
- รูปแบบเครือข่ายสื่อสาร (Network Topology)
- การจำลองเครือข่ายเพื่ออธิบายโปรโตคอลที่นำเสนอ
- ระดับชั้นย่อยของโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ
- สรุปผลการทำงานโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง

3.1 โปรโตคอลการสื่อสารข้อมูลที่นำเสนอ

3.1.1 ภาพรวมของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงที่นำเสนอ

เพื่อให้ทราบถึงภาพรวมของปัญหา และวิธีการแก้ไขปัญหาทั้งหมดของโปรโตคอลการส่งข้อมูล และการระบุที่อยู่เชิงแสงสำหรับการสื่อสารความเร็วสูงและความปลอดภัยสูงโดยใช้อุปกรณ์เชิงแสงทั้งหมดที่นำเสนอ ในส่วนนี้จึงกล่าวถึงภาพรวมของโปรโตคอลที่นำเสนอ มีรายละเอียดดังนี้



รูปที่ 3.1 โปรโตคอลการสื่อสารข้อมูลในสื่อเชิงแสงที่นำเสนอ

จากรูปที่ 3.1 แสดงโปรโตคอลการสื่อสารข้อมูลในสื่อเชิงแสงที่นำเสนอ ซึ่งนำเสนอผลงานตามภาคผนวก ก [8] โดยแต่ละส่วนมีการแก้ไขปัญหาให้โปรโตคอลที่นำเสนอสามารถทำงานได้ ดังนี้

1) Optical Encapsulation / Optical De-encapsulation หรือการห่อหุ้มเชิงแสง / การถอดข้อมูลเชิงแสง เพื่อให้โปรโตคอลที่นำเสนอทำงานเป็นชั้น (Layer) ได้และเพื่อให้โปรโตคอลที่นำเสนอรองรับการทำงานด้วยอุปกรณ์เชิงแสงทั้งหมด ซึ่งนำเสนอผลงานตามภาคผนวก ก [7]

2) Optical Address หรือที่อยู่เชิงแสง เพื่อให้โปรโตคอลที่นำเสนอระบุที่อยู่เชิงแสงภายในเครือข่ายได้ และเพื่อให้โปรโตคอลที่นำเสนอรองรับการทำงานด้วยอุปกรณ์เชิงแสงทั้งหมด ซึ่งนำเสนอผลงานตามภาคผนวก ก [5,9]

3) Key Suppression and Recovery หรือการซ่อนกุญแจและการกู้คืนกุญแจ เพื่อให้โปรโตคอลที่นำเสนอมีวิธีการส่งกุญแจที่ใช้ในการเข้ารหัสข้อมูลมีความปลอดภัยสูง และเพื่อให้โปรโตคอลที่นำเสนอรองรับการทำงานด้วยอุปกรณ์เชิงแสงทั้งหมด ซึ่งนำเสนอผลงานตามภาคผนวก ก [1,2,3,6]

4) Optical Private Tunnel หรือเครือข่ายส่วนตัวเสมือนเชิงแสง เพื่อให้โปรโตคอลที่นำเสนอมีความปลอดภัยสูง และเพื่อให้โปรโตคอลที่นำเสนอรองรับการทำงานด้วยอุปกรณ์เชิงแสงทั้งหมด ซึ่งนำเสนอผลงานตามภาคผนวก ก [4,10]

ข้อปรับปรุงเมื่อเทียบกับบทความที่เกี่ยวข้อง จากบทที่ 2 หัวข้อที่ 2.10 งานวิจัยที่เกี่ยวข้อง [64] โดยที่โปรโตคอลการสื่อสารข้อมูลในสื่อเชิงแสงที่นำเสนอพัฒนาปรับปรุงเมื่อเทียบกับงานวิจัยที่เกี่ยวข้อง อธิบายได้ดังนี้ Optical Encapsulation/ Optical De-encapsulation หรือการห่อหุ้มเชิงแสง/การถอดข้อมูลเชิงแสง พัฒนาต่อจากงานวิจัยดังกล่าวในเรื่องของการทำงานเป็นระดับชั้น เพื่อให้การพัฒนาโปรโตคอลสามารถทำได้ง่ายมากขึ้น Key Suppression and Recovery หรือการซ่อนกุญแจและการกู้คืนกุญแจ และ Optical Private Tunnel หรือเครือข่ายส่วนตัวเสมือนเชิงแสง พัฒนาต่อจากงานวิจัยดังกล่าวในเรื่องของความปลอดภัยในการสื่อสารข้อมูล Optical Address หรือที่อยู่เชิงแสง พัฒนาต่อจากงานวิจัยดังกล่าวในเรื่องของการระบุที่อยู่ภายในเครือข่ายให้สามารถระบุตัวตนผู้รับข้อมูลภายในเครือข่ายได้

3.1.2 อธิบายระดับชั้นย่อย (Sub Layer) ของโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ

จากรูปที่ 3.1 โปรโตคอลการสื่อสารข้อมูลในสื่อเชิงแสงที่นำเสนอ ประกอบด้วย 4 ระดับชั้นย่อย ซึ่งเทียบได้กับระดับชั้น Physical ของ OSI Model [65] กล่าวคือโปรโตคอลการสื่อสารข้อมูลในสื่อเชิงแสงนำเสนอ Physical ที่รองรับการทำงานด้านการระบุที่อยู่ภายในเครือข่ายสื่อสารและรองรับด้านความปลอดภัยในการสื่อสาร โดยระดับชั้นย่อยอธิบายได้ดังนี้

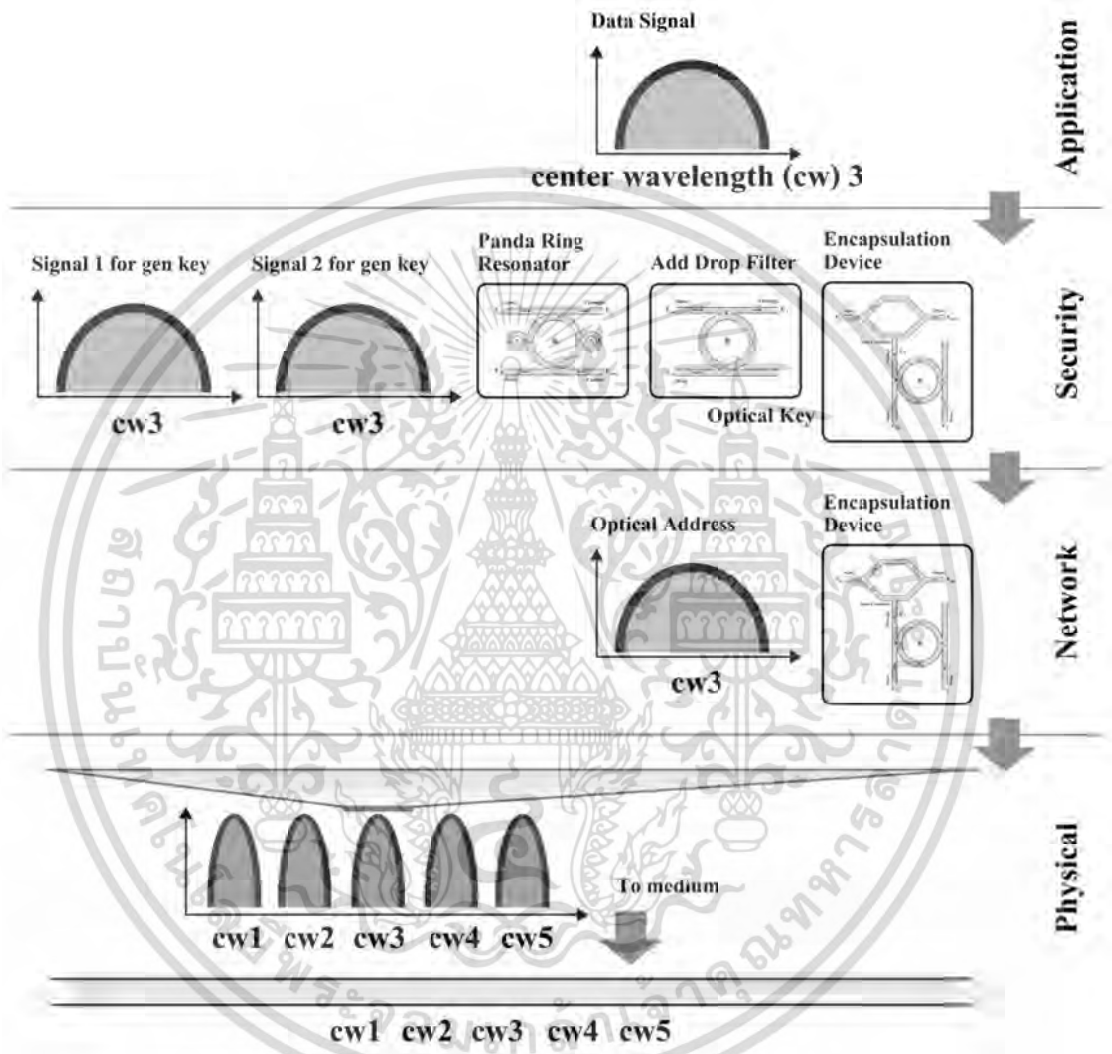
1) ระดับชั้นย่อย Physical มีคุณสมบัติในการทำหน้าที่เกี่ยวข้องโดยตรงกับอุปกรณ์สื่อสารต่าง ๆ ทำหน้าที่ในการกำหนดวิธีควบคุมการรับและการส่งข้อมูลระหว่างอุปกรณ์ภายในเครือข่ายสื่อสาร ทำหน้าที่ส่งสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ผ่านตัวกลางของการสื่อสารข้อมูล

2) ระดับชั้นย่อย Network มีคุณสมบัติในการทำหน้าที่การควบคุมการติดต่อรับ-ส่งข้อมูลระหว่างอุปกรณ์ต่าง ๆ ในระบบเครือข่ายให้เป็นไปด้วยความเรียบร้อย ถึงผู้รับข้อมูลถูกต้องตามที่ผู้ส่งข้อมูลต้องการด้วยที่อยู่เชิงแสง (Optical Address)

3) ระดับชั้นย่อย Security มีคุณสมบัติในการทำหน้าที่ให้การสื่อสารข้อมูลภายในเครือข่ายเป็นไปอย่างปลอดภัย ด้วยวิธีการซ่อนกุญแจเชิงแสงและการก็คืนกุญแจเชิงแสง (Key Suppression and Recovery) รวมถึงสร้างช่องทางการสื่อสารปลอดภัยด้วยเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel)

4) ระดับชั้นย่อย Application มีคุณสมบัติในการทำหน้าที่เป็นตัวกลางหรือส่วนติดต่อระหว่างโปรแกรมกับระดับชั้นอื่น ๆ ในโปรโตคอลการส่งข้อมูลและการยืนยันตัวตนเชิงแสงที่นำเสนอ รวมถึงมีการปรับข้อมูลในฝั่งผู้รับข้อมูลให้เป็นข้อมูลที่สมบูรณ์ก่อนส่งให้กับโปรแกรมอื่น ๆ ต่อไป

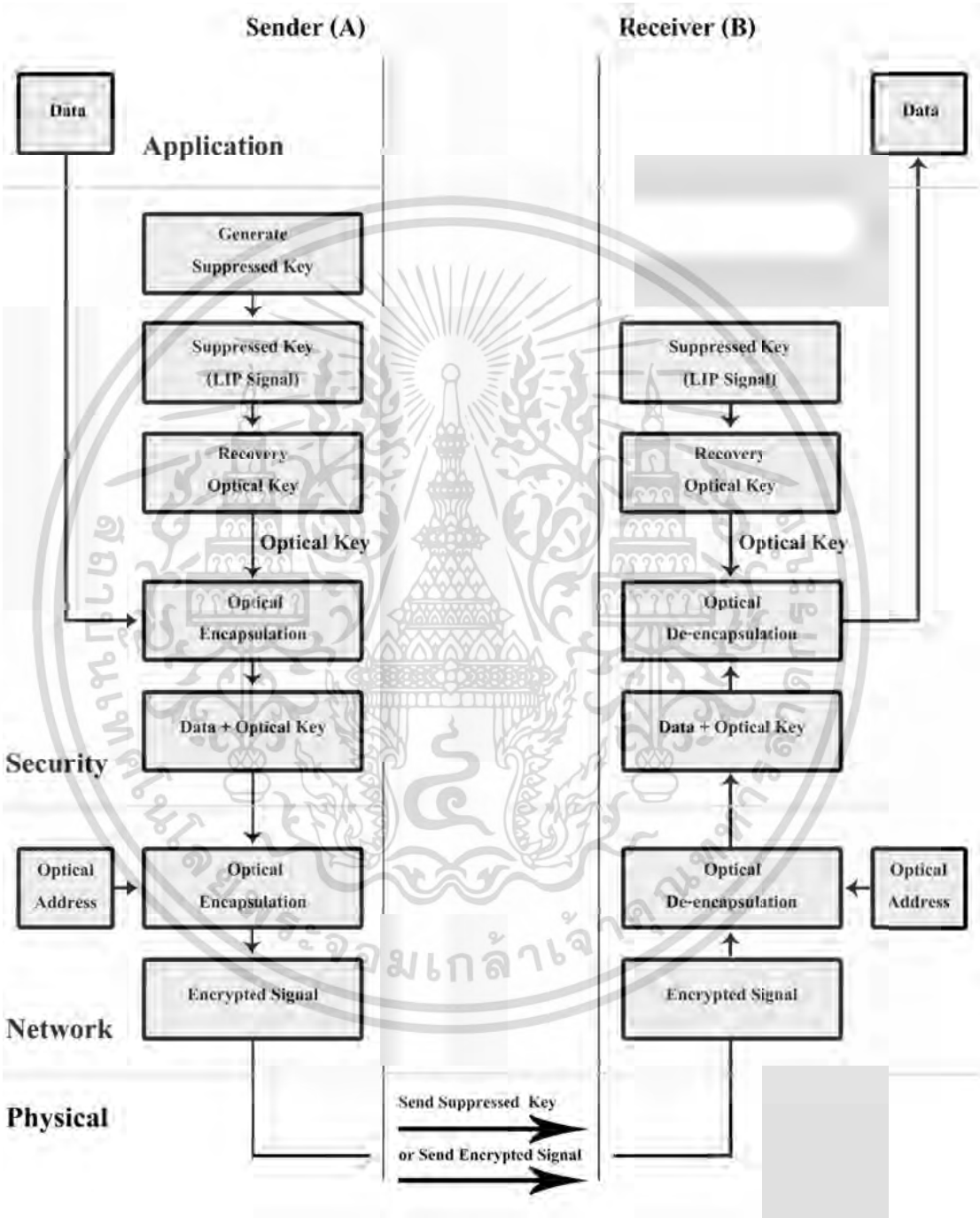
3.1.3 อธิบายโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ



รูปที่ 3.2 ไดอะแกรมของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง

จากรูปที่ 3.2 แสดงไดอะแกรมของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง อธิบายว่าในแต่ละระดับชั้นย่อยมีอุปกรณ์และสัญญาณใดบ้างที่เกี่ยวข้อง กล่าวคือ ในระดับชั้นย่อย Physical เป็นการใช้ตัวกลางเชิงแสงในการส่งข้อมูลไปยังผู้รับข้อมูล ในระดับ Network มีการใช้สัญญาณที่อยู่เชิงแสง (Optical Address) และอุปกรณ์ห่อหุ้มและถอดข้อมูลเชิงแสง ในระดับชั้นย่อย Security มีการใช้สัญญาณสำหรับสร้างกุญแจเชิงแสง 2 สัญญาณ และมีการใช้วงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) วงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) และอุปกรณ์ห่อหุ้มและถอดข้อมูลเชิงแสง ในระดับชั้นย่อย Application มีการใช้สัญญาณข้อมูล (Data Signal) จากรูป 3.2 เห็น

ได้ว่าในการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูลต้องใช้ศูนย์กลางช่วงคลื่น (Center Wavelength) เดียวกันในการส่งข้อมูล แต่ในเครือข่าย Physical เดียวกันสามารถใช้งานศูนย์กลางช่วงคลื่น (Center Wavelength) ที่ไม่เหมือนกันได้ โดยจะเป็นการส่งข้อมูลระหว่างผู้ส่งข้อมูลกับผู้รับข้อมูลคนละเครือข่าย Logical กัน



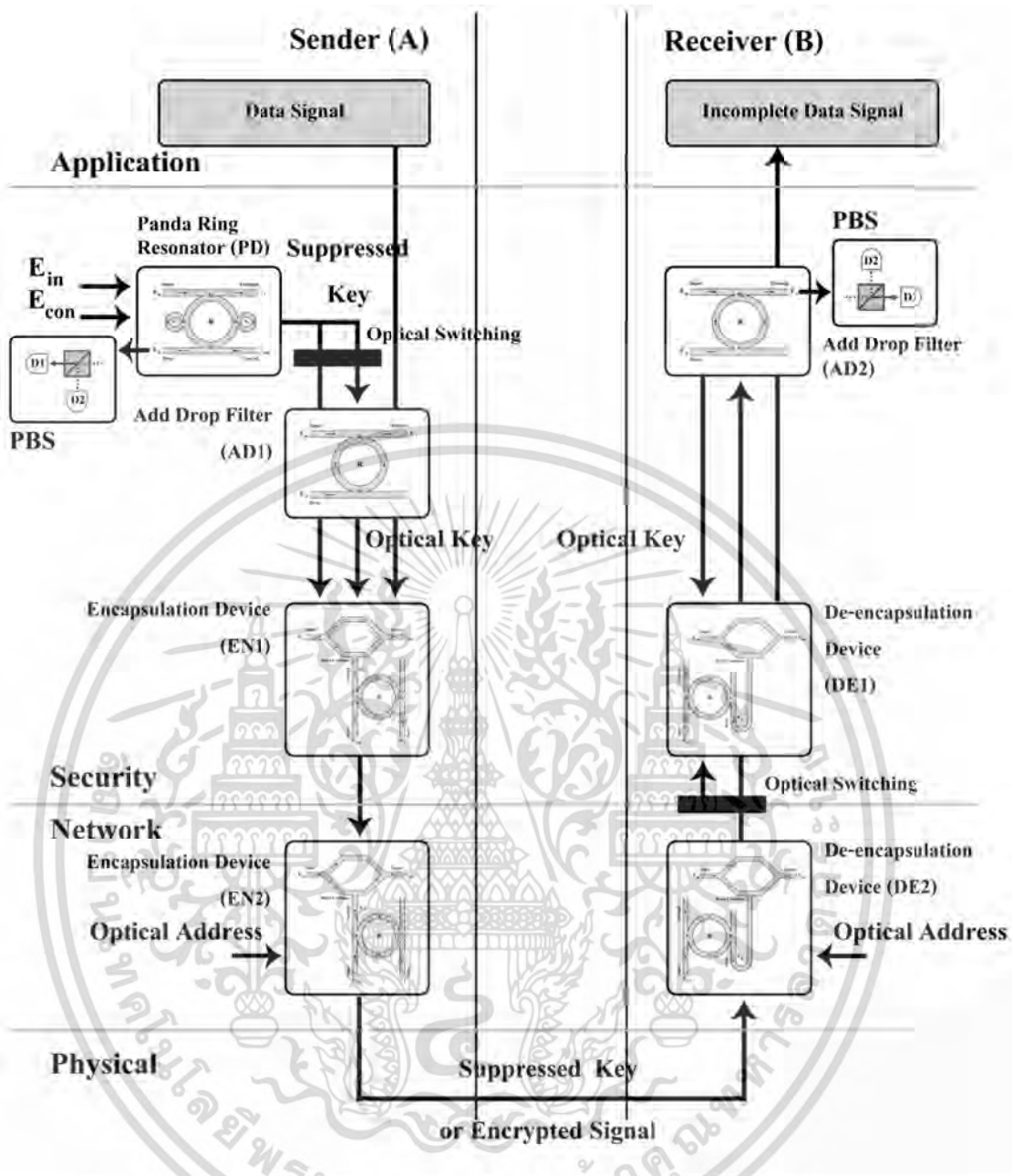
รูปที่ 3.3 แผนภาพแสดงหลักการทำงานของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง

จากรูป 3.3 แสดงแผนภาพแสดงหลักการทำงานของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง อธิบายได้ว่า

ฝั่งผู้ส่งข้อมูล (Sender (A)) มีการสร้างสัญญาณกุญแจเชิงแสง (Optical Key) ที่ห่อหุ้มด้วยสัญญาณรูปปาก (LIP Signal) และกู้คืนกุญแจเชิงแสง (Optical Key) จากนั้นส่งสัญญาณกุญแจเชิงแสง (Optical Key) ที่ห่อหุ้มด้วยสัญญาณรูปปาก (LIP Signal) ให้กับผู้รับข้อมูล (Receiver (B)) เพื่อกู้คืนกุญแจเชิงแสง (Optical Key) ที่ใช้ในการส่งข้อมูล จากนั้นฝั่งผู้ส่งข้อมูล (Sender (A)) นำสัญญาณข้อมูลห่อหุ้มเชิงแสง (Optical Encapsulation) และนำสัญญาณที่ได้ไปห่อหุ้มเชิงแสง (Optical Encapsulation) กับที่อยู่เชิงแสง (Optical Address) ได้เป็นสัญญาณที่ใช้ในการส่งข้อมูล (Encrypted Signal)

ฝั่งผู้รับข้อมูล (Receiver (B)) รับสัญญาณที่ได้รับมากจากการส่งข้อมูล (Encrypted Signal) จากผู้ส่งข้อมูล (Sender (A)) จากนั้นนำมาถอดข้อมูลเชิงแสง (Optical De-Encapsulation) ด้วยที่อยู่เชิงแสงของผู้รับข้อมูล (Receiver (B)) จากนั้น นำสัญญาณที่ได้นำมาถอดข้อมูลเชิงแสง (Optical De-Encapsulation) ด้วยกุญแจเชิงแสง (Optical Key) ที่กู้คืนมาจากสัญญาณรูปปาก (LIP Signal) ที่ห่อหุ้มกุญแจเชิงแสง (Optical Key) อยู่ภายในที่ผู้ส่งข้อมูลส่งให้ ซึ่งจะได้สัญญาณข้อมูลที่ผู้ส่งข้อมูลต้องการส่งให้

การส่งสัญญาณข้อมูลภายในเครือข่าย มีการส่งสัญญาณ 2 ลักษณะคือ การส่งสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) และการส่งสัญญาณกุญแจเชิงแสง (Optical Key) ที่ห่อหุ้มด้วยสัญญาณรูปปาก (LIP Signal) ซึ่งจะมีวิธีการส่งสัญญาณและข้อแตกต่างระหว่างการส่งสัญญาณทั้ง 2 ลักษณะ มีการอธิบายในลำดับถัดไป ในหัวข้อ 4.3 อธิบายการส่งข้อมูลภายในเครือข่าย



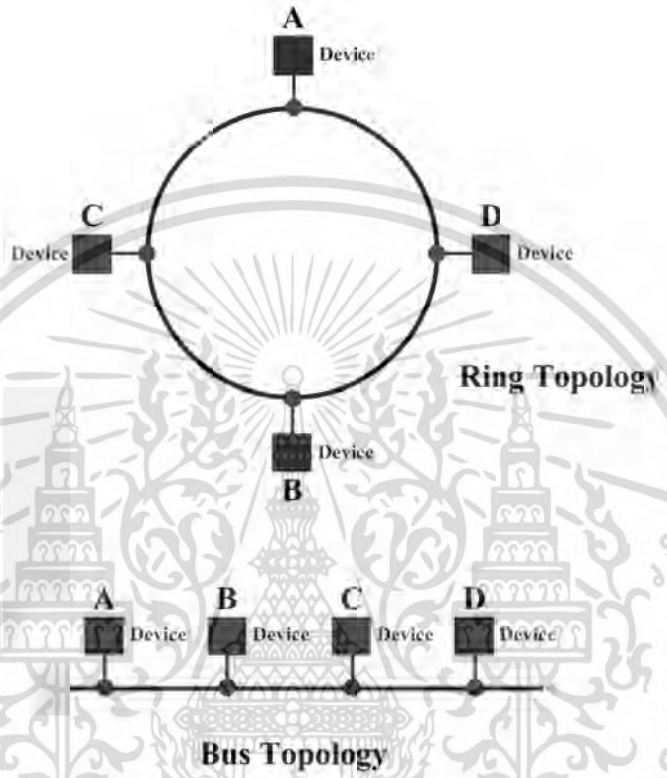
รูปที่ 3.4 อุปกรณ์ที่เกี่ยวข้องของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง

จากรูปที่ 3.4 อุปกรณ์ที่เกี่ยวข้องของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง การส่งข้อมูลและกุญแจเชิงแสงทำได้โดย ในฝั่งผู้ส่งข้อมูลและฝั่งผู้รับข้อมูลมีการกำหนด Reference Port เพื่อใช้ในการอ้างอิงสถานะของการส่งสัญญาณภายในเครือข่าย ว่าขณะนี้เป็นการส่งสัญญาณข้อมูลหรือเป็นการส่งสัญญาณรูปปาก (LIP Signal) ซึ่งสัญญาณแสงจาก Reference Port จะผ่าน Polarizing Beam Splitter (PBS) ซึ่งจะถูกส่งไปยังตัวตรวจจับ (Detector) D1 และ D2 เพื่อนำค่าสัญญาณที่ตรวจจับได้ไปใช้ในการอ้างอิงการส่งข้อมูลต่อไป โดยจะกล่าวถึงรายละเอียดในบทถัดไป

และจากรูปที่ 3.4 ใช้ในการอธิบายรายละเอียดของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงในลำดับถัดไป ที่กล่าวถึงการจำลองโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง

3.2 รูปแบบเครือข่ายสื่อสาร (Network Topology)

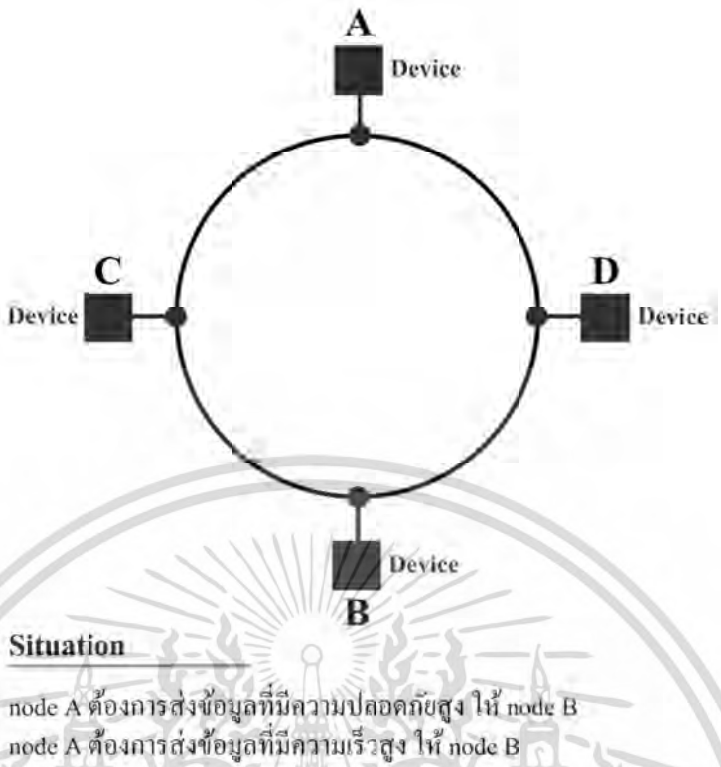
ในการสื่อสารข้อมูลระหว่างบุคคลที่อยู่ในเครือข่ายสื่อสารโดยใช้โปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงที่ใช้อุปกรณ์เชิงแสงทั้งหมดที่นำเสนอ มีรูปแบบเครือข่ายสื่อสารที่รองรับโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง โดยมีรายละเอียดดังนี้



รูปที่ 3.5 รูปแบบเครือข่ายสื่อสารที่รองรับโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง

โปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงที่ใช้อุปกรณ์เชิงแสงทั้งหมดที่นำเสนอครอบคลุมรูปแบบของเครือข่ายสื่อสาร (Network Topology) แบบบัส (Bus Topology) และเครือข่ายแบบวงแหวน (Ring Topology) เท่านั้น เนื่องจากไม่มีอุปกรณ์หรือการพัฒนาอุปกรณ์เราเตอร์เชิงแสง (Optical Router) หรือฮับเชิงแสง (Optical Hub) ที่ทำงานร่วมกับโปรโตคอลการสื่อสารข้อมูลที่นำเสนอได้ ดังแสดงตามรูปที่ 3.5 รูปแบบเครือข่ายสื่อสารที่รองรับโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง

จากรูปแบบเครือข่ายสื่อสาร (Network Topology) ที่สามารถใช้โปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงที่ใช้อุปกรณ์เชิงแสงทั้งหมดที่นำเสนอสามารถใช้งานได้กับระบบเครือข่ายสื่อสารที่ต้องการความเร็วในการส่งข้อมูลสูงและระบบเครือข่ายสื่อสารที่ต้องการความปลอดภัยในการส่งข้อมูลสูง ตัวอย่างเช่น



รูปที่ 3.6 ตัวอย่างเครือข่ายสื่อสารที่สามารถใช้โปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง

จากรูปที่ 3.6 แสดงตัวอย่างเครือข่ายสื่อสารที่สามารถใช้โปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปยังผู้รับข้อมูล B โดยที่ความเร็วและความปลอดภัยในการสื่อสารข้อมูลเกิดจากเหตุผลต่าง ๆ ดังนี้

1) ผู้ส่งข้อมูล A ส่งข้อมูลไปยังผู้รับข้อมูล B มีการเข้ารหัสข้อมูลด้วยวิธีการเข้ารหัสเชิงแสง (Optical Cryptography)

2) ผู้ส่งข้อมูล A สามารถเปลี่ยนกุญแจ (Key) ที่ใช้ในการเข้ารหัสข้อมูลได้ทุก ๆ ครั้งที่มีการส่งชุดข้อมูลไปยังผู้รับข้อมูล B

3) ผู้ส่งข้อมูล A ส่งกุญแจ (Key) ที่ใช้ในการเข้ารหัสด้วยวิธีการซ่อนข้อมูลและการกู้คืนข้อมูล (Suppression and Recovery)

4) ผู้ส่งข้อมูล A ใช้ที่อยู่เชิงแสงของผู้รับข้อมูล B

5) ระหว่างการสื่อสารระหว่างผู้ส่งข้อมูล A และผู้รับข้อมูล B มีการใช้งานเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel)

6) ระหว่างการสื่อสารระหว่างผู้ส่งข้อมูล A และผู้รับข้อมูล B มีการใช้อุปกรณ์เชิงแสงทั้งหมด

3.3 การจำลองเครือข่ายเพื่ออธิบายโปรโตคอลที่นำเสนอ

3.3.1 ข้อจำกัดของแบบจำลองที่ใช้จำลอง

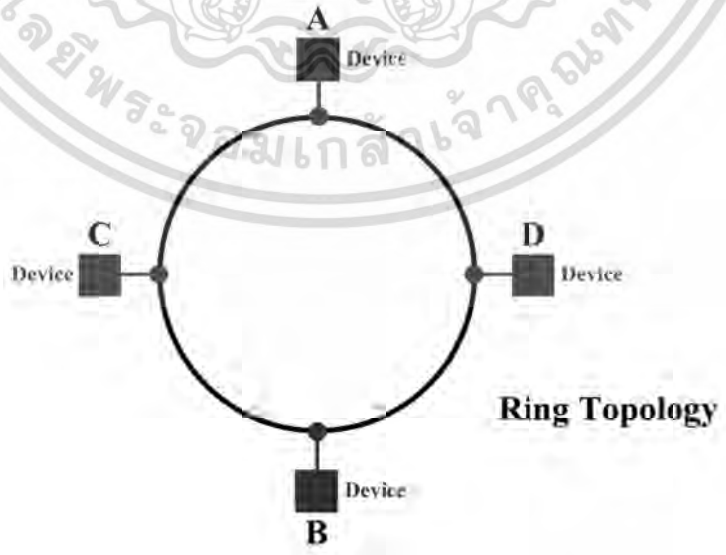
เป็นการศึกษาการสื่อสารข้อมูลภายในเครือข่ายโดยใช้โปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง (Optical Transmission and Addressing Protocol) ที่พัฒนาขึ้นโดยไม่รวมถึงการ Synchronization สัญญาณที่ส่งภายในเครือข่ายสื่อสาร

เป็นการศึกษาการสื่อสารข้อมูลภายในเครือข่ายโดยใช้โปรโตคอลที่พัฒนาขึ้นโดยไม่รวมถึงการสูญเสียระหว่างอุปกรณ์เชิงแสง

เป็นการศึกษาโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง (Optical Transmission and Addressing Protocol) ครอบคลุมรูปแบบของเครือข่ายสื่อสาร (Network Topology) แบบบัส (Bus Topology) และเครือข่ายแบบวงแหวน (Ring Topology) เท่านั้น เนื่องจากไม่มีอุปกรณ์หรือการพัฒนาเราเตอร์เชิงแสง (Optical Router) หรือฮับเชิงแสง (Optical Hub) ที่ทำงานร่วมกับโปโตคอลการสื่อสารข้อมูลที่นำเสนอได้

3.3.2 รูปแบบเครือข่ายแบบจำลอง

การจำลองรูปแบบของเครือข่ายที่ศึกษา จะจำลองเครือข่ายสื่อสารเชิงแสงที่มีผู้ส่งข้อมูลภายในเครือข่ายเชิงแสง 1 บุคคล ผู้รับข้อมูลภายในเครือข่ายเชิงแสง 1 บุคคล และผู้ประสงค์ร้ายภายในเครือข่ายเชิงแสง 1 บุคคล โดยเป็นเครือข่ายสื่อสาร (Network Topology) ที่เป็นแบบวงแหวน (Ring Topology) เท่านั้น ตามรูปที่ 3.7 รูปแบบเครือข่ายแบบจำลองที่ใช้ในการจำลองโปรโตคอล เนื่องจากรูปแบบของเครือข่ายสื่อสาร (Network Topology) แบบบัส (Bus Topology) และเครือข่ายแบบวงแหวน (Ring Topology) ที่ใช้งานโปรโตคอลที่นำเสนอจะได้ผลของการจำลองเหมือนกัน เนื่องจากขอบเขตของงานวิจัยนี้ไม่รวมถึงการ Synchronization สัญญาณที่ส่งภายในเครือข่ายสื่อสาร

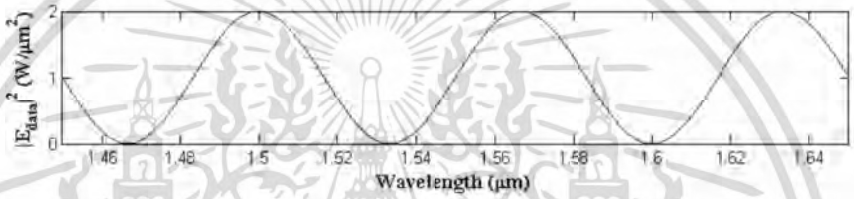


รูปที่ 3.7 รูปแบบเครือข่ายแบบจำลองที่ใช้ในการจำลอง

จากรูปที่ 3.7 แสดงรูปแบบเครือข่ายแบบจำลองที่ใช้ในการจำลองเครือข่าย เป็นแครือข่ายแบบจำลองที่อธิบายให้เห็นถึงการส่งข้อมูลภายในเครือข่ายสื่อสารเชิงแสงทั้งการสื่อสารเชิงแสงที่เป็นไปตามความต้องการของผู้ส่งข้อมูล หรือการส่งข้อมูลภายในเครือข่ายสื่อสารเชิงแสงที่ไม่เป็นไปตามต้องการของผู้ส่งข้อมูล (มีผู้ประสงค์ร้ายต้องการข้อมูลภายในเครือข่าย) โดยมีอุปกรณ์ที่เกี่ยวข้องของโปรโตคอลที่ใช้ในการจำลองเครือข่ายตามรูปที่ 3.4

3.3.3 ลักษณะของสัญญาณข้อมูลที่ใช้ในการจำลอง

ในการทดสอบการจำลองเครือข่าย สัญญาณข้อมูลที่ส่งจากผู้ส่งข้อมูลภายในเครือข่ายสื่อสารจะมีข้อมูลลักษณะตามรูปที่ 3.8 กล่าวคือ เป็นสัญญาณข้อมูลที่ไม่มีความซับซ้อนของข้อมูล เนื่องจากให้ง่ายต่อการศึกษา กล่าวคือ ในแต่ละการจำลองให้ง่ายต่อการตรวจสอบผลสำเร็จของการส่งข้อมูลอีกทั้งยังให้ง่ายต่อการศึกษาผลกระทบต่อสัญญาณเมื่อผ่านระดับชั้นย่อยต่าง ๆ



รูปที่ 3.8 ลักษณะของสัญญาณข้อมูลที่ใช้ในการจำลอง

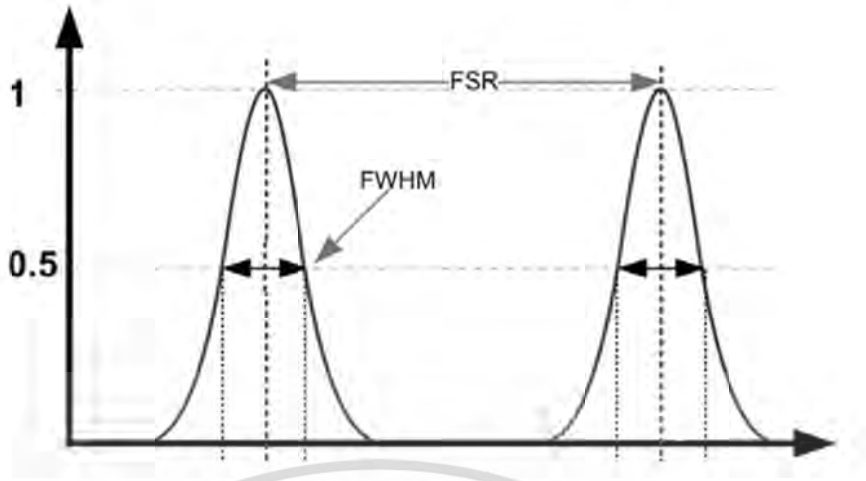
<u>หมายเหตุ</u> ในการส่งสัญญาณข้อมูลจริงภายในเครือข่ายด้วยโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงที่นำเสนอ จะกล่าวถึงรายละเอียดในบทที่ 4 หัวข้อ 4.3.1 การส่งข้อมูลภายในเครือข่าย

3.3.4 การวัดผลสำเร็จของการส่งข้อมูลในเครือข่ายสื่อสาร

การวัดผลสำเร็จของการส่งข้อมูลในเครือข่ายสื่อสาร วิทยานิพนธ์นี้ ใช้วิธีการวัดประสิทธิภาพของรูปคลื่นซึ่งใช้ค่าพิสัยสเปกตรัมอิสระ (Free Spectral Range : FSR) และค่าความกว้างเต็มที่ครึ่งหนึ่งของรูปคลื่น (Full Width at Half Maximum : FWHM) [66] โดยที่

ถ้าค่าพิสัยสเปกตรัมอิสระ (FSR) และค่าความกว้างเต็มที่ครึ่งหนึ่งของรูปคลื่น (FWHM) ของสัญญาณข้อมูลจากผู้ส่งข้อมูลและค่าพิสัยสเปกตรัมอิสระ (FSR) และค่าความกว้างเต็มที่ครึ่งหนึ่งของรูปคลื่น (FWHM) ของสัญญาณข้อมูลที่ผู้รับข้อมูลได้รับเท่ากัน การจำลองการส่งข้อมูลครั้งนั้นถือว่าส่งข้อมูลสำเร็จ

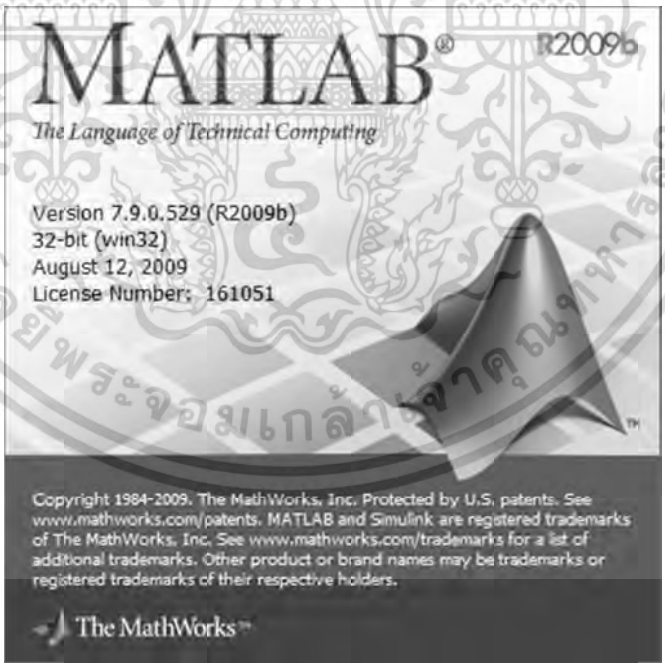
ถ้าค่าพิสัยสเปกตรัมอิสระ (FSR) และค่าความกว้างเต็มที่ครึ่งหนึ่งของรูปคลื่น (FWHM) ของสัญญาณข้อมูลจากผู้ส่งข้อมูลและค่าพิสัยสเปกตรัมอิสระ (FSR) และค่าความกว้างเต็มที่ครึ่งหนึ่งของรูปคลื่น (FWHM) ของสัญญาณข้อมูลที่ผู้รับข้อมูลได้รับไม่เท่ากัน การจำลองการส่งข้อมูลครั้งนั้นถือว่าส่งข้อมูลไม่สำเร็จ โดยค่าการวัดประสิทธิภาพของรูปคลื่นหาได้แสดงดังรูปที่ 3.9



รูปที่ 3.9 การวัดประสิทธิภาพของรูปคลื่น

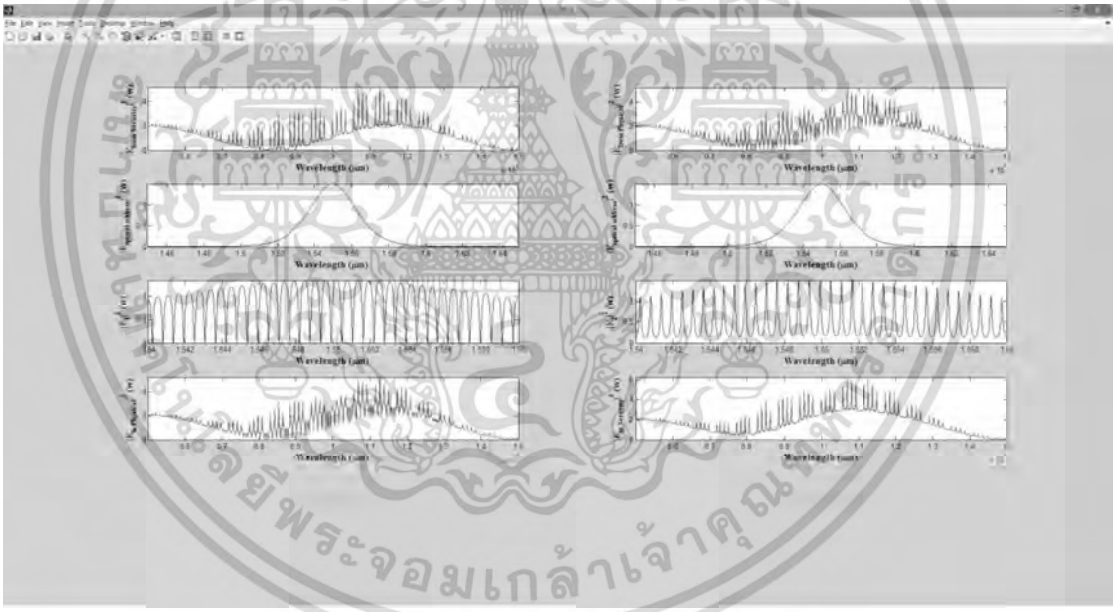
3.3.5 วิธีการจำลองเครือข่ายเพื่อทดสอบการทำงานของโปรโตคอล

ในการทดสอบการทำงานของโปรโตคอล ใช้วิธีการจำลองการทำงานของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงสำหรับการสื่อสารความเร็วสูง และความปลอดภัยสูงโดยใช้อุปกรณ์เชิงแสงทั้งหมด ด้วยโปรแกรม Matlab ตามรูปที่ 3.10 – 3.12 โดยผลจากการจำลองเครือข่ายอยู่ในรูปแบบของกราฟตามแต่ละการจำลองเครือข่ายต้องการศึกษา



รูปที่ 3.10 โปรแกรม Matlab ที่ใช้ในการทดสอบสมมติฐาน

รูปที่ 3.11 ตัวอย่างวิธีการทดสอบสมมติฐานด้วยโปรแกรม Matlab



รูปที่ 3.12 ตัวอย่างผลการทดสอบสมมติฐานด้วยโปรแกรม Matlab

3.3.6 พารามิเตอร์ที่ใช้ในการจำลองเครือข่ายเพื่ออธิบายโปรโตคอลที่นำเสนอ

จากรูปที่ 3.4 อุปกรณ์ที่เกี่ยวข้องของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง เพื่อใช้ในการอธิบายรายละเอียดของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงในหัวข้อถัดไป ที่กล่าวถึงการจำลองระดับชั้นย่อยของโปรโตคอลที่นำเสนอ โดยมีพารามิเตอร์ที่ใช้ในการจำลองโปรโตคอล (เป็นพารามิเตอร์ที่เหมาะสมของโปรโตคอลที่นำเสนอ) ดังนี้

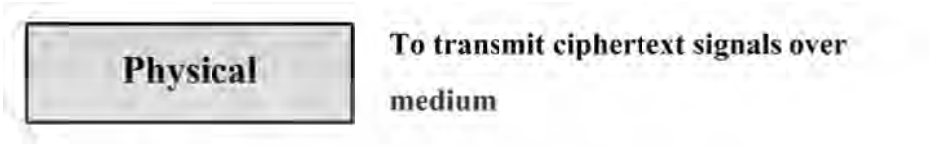
ตารางที่ 3.1 พารามิเตอร์ที่ใช้ในการจำลองโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง

อุปกรณ์ , สัญญาณ	พารามิเตอร์	ค่าพารามิเตอร์
ทุกอุปกรณ์	ชนิดของวัสดุ	InGaAsP/InP
	ค่าดัชนีหักเหเชิงเส้นของตัวนำคลื่น : n_0	3.4
	ค่าดัชนีหักเหไม่เชิงเส้นของตัวนำคลื่น : n_2	1.3×10^{-13} m^2/W
	การสูญเสียภายในตัวนำคลื่น : α	0.05 dB mm^{-1}
	ค่าการสูญเสียความเข้มแสงเนื่องจากคัปปลิ้ง : γ	0.01
	ขนาดพื้นที่หน้าตัดของตัวนำคลื่น : A_{eff}	0.25 μm^2
Panda Ring Resonator (PD)	ขนาดวงแหวนกลาง	200 μm
	ขนาดวงแหวนข้างซ้ายและข้างขวา	15 μm
	สัมประสิทธิ์การคัปปลิ้ง κ_1	0.2
	สัมประสิทธิ์การคัปปลิ้ง κ_2	0.2
	สัมประสิทธิ์การคัปปลิ้ง κ_3	0.1
	สัมประสิทธิ์การคัปปลิ้ง κ_4	0.1
Add Drop Filter (AD1,AD2)	ขนาดวงแหวน	200 μm
	สัมประสิทธิ์การคัปปลิ้ง κ_1	0.5
	สัมประสิทธิ์การคัปปลิ้ง κ_2	0.2
Add Drop Filter (EN1,DE1)	ขนาดวงแหวน	20 μm
	สัมประสิทธิ์การคัปปลิ้ง κ_1	0.5
	สัมประสิทธิ์การคัปปลิ้ง κ_2	0.5
Add Drop Filter (EN2,DE2)	ขนาดวงแหวน	200 μm
	สัมประสิทธิ์การคัปปลิ้ง κ_1	0.5
	สัมประสิทธิ์การคัปปลิ้ง κ_2	0.5
สัญญาณ	ศูนย์กลางช่วงคลื่น : λ_0	1.55 μm
	ความเข้มสัญญาณ Input ที่ PD (Input) : E_{in}	1.2 $W/\mu m^2$
	ความเข้มสัญญาณ Input ที่ PD (Control) : E_{con}	1.2 $W/\mu m^2$
	ความเข้มสัญญาณ Optical Address	1.5 $W/\mu m^2$
	ความเข้มสัญญาณ Data	2.0 $W/\mu m^2$

3.4 ระดับชั้นย่อยของโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ

3.4.1 ระดับชั้นย่อย Physical (Physical Sub Layer)

3.4.1.1 ภาพรวมโปรโตคอลในระดับชั้นย่อย Physical



รูปที่ 3.13 แผนภาพคุณสมบัติของระดับชั้นย่อย Physical

จากรูปที่ 3.13 แสดงแผนภาพคุณสมบัติของระดับชั้นย่อย Physical มีคุณสมบัติในการทำหน้าที่เกี่ยวข้องโดยตรงกับอุปกรณ์สื่อสารต่าง ๆ ทำหน้าที่ในการกำหนดวิธีควบคุมการรับและการส่งข้อมูลระหว่างอุปกรณ์ภายในเครือข่ายสื่อสาร ทำหน้าที่ส่งสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ผ่านตัวกลางของการสื่อสารข้อมูล

3.4.1.2 รายละเอียดโปรโตคอลในระดับชั้นย่อย Physical

รูปที่ 3.14 แผนภาพอุปกรณ์โปรโตคอลในระดับชั้นย่อย Physical

จากรูปที่ 3.14 แสดงแผนภาพอุปกรณ์โปรโตคอลในระดับชั้นย่อย Physical มีขั้นตอนการทำงานในระดับชั้นย่อยนี้ ดังนี้

ขั้นตอนการทำงานของโปรโตคอลในระดับชั้นย่อย Physical (ฝั่งผู้ส่งข้อมูล)

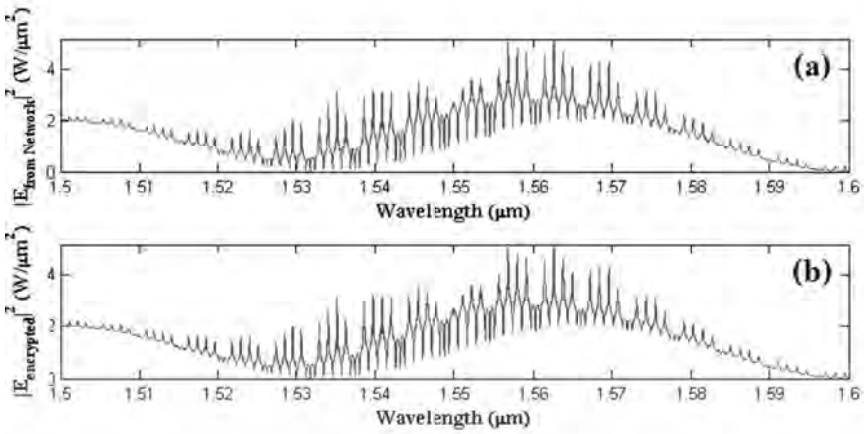
ขั้นตอนที่ 1 : รับสัญญาณจากระดับชั้นย่อย Network

ขั้นตอนที่ 2 : ส่งสัญญาณจากขั้นตอนที่ 1 ให้กับผู้รับข้อมูลผ่านสื่อเชิงแสง

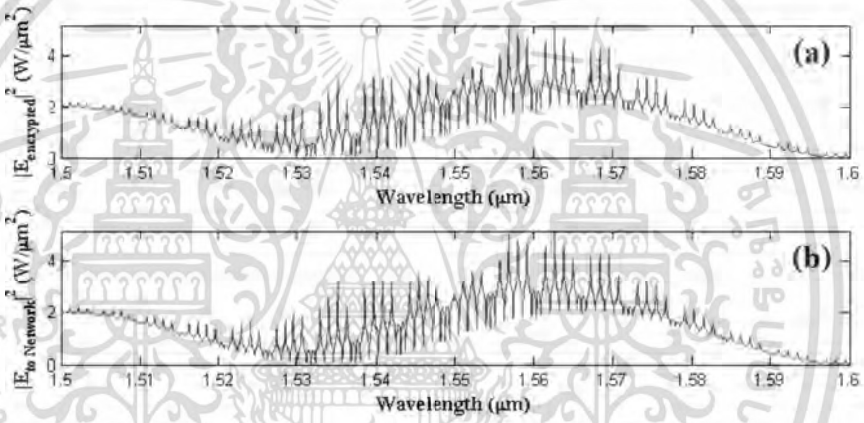
ขั้นตอนการทำงานของโปรโตคอลในระดับชั้นย่อย Physical (ฝั่งผู้รับข้อมูล)

ขั้นตอนที่ 1 : รับสัญญาณจากสื่อเชิงแสง

ขั้นตอนที่ 2 : นำสัญญาณจากขั้นตอนที่ 1 ส่งต่อไปยังระดับชั้นย่อย Network



รูปที่ 3.15 ตัวอย่างกราฟการทำงานฝั่งผู้ส่งข้อมูลระดับชั้นย่อย Physical



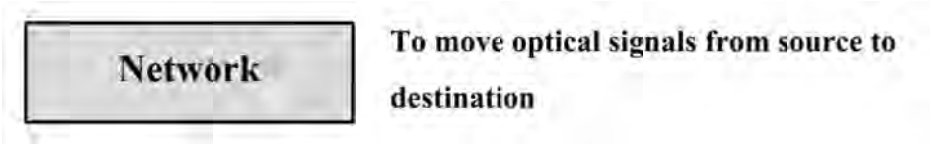
รูปที่ 3.16 ตัวอย่างกราฟการทำงานฝั่งผู้รับข้อมูลระดับชั้นย่อย Physical

จากรูปที่ 3.15 ตัวอย่างกราฟการทำงานฝั่งผู้ส่งข้อมูลระดับชั้นย่อย Physical รูปที่ 3.15 (a) แสดงสัญญาณจากระดับชั้นย่อย Network รูปที่ 3.15 (b) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่ Sender (A) ใช้ในการสื่อสารข้อมูลไปยัง Receiver (B) โดยที่ รูปที่ 3.15 (a) และรูปที่ 3.15 (b) มีลักษณะสัญญาณเหมือนกันเนื่องจากระดับชั้นย่อย Physical ทำหน้าที่หลักในการส่งสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ผ่านตัวกลางของการสื่อสารข้อมูล จากสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่ใช้ในการส่งข้อมูลเห็นว่ามีลักษณะสัญญาณคล้ายกับสัญญาณรบกวน (Noiselike)

จากรูปที่ 3.16 ตัวอย่างกราฟการทำงานฝั่งผู้รับข้อมูลระดับชั้นย่อย Physical รูปที่ 3.16 (a) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่รับจากผู้ส่งข้อมูล Sender (A) รูปที่ 3.16 (a) แสดงสัญญาณที่จะส่งไปยังระดับชั้นย่อย Network โดยที่ รูปที่ 3.16 (a) และรูปที่ 3.16 (b) มีลักษณะสัญญาณเหมือนกันเนื่องจากระดับชั้นย่อย Physical ทำหน้าที่หลักในการส่งสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ผ่านตัวกลางของการสื่อสารข้อมูล

3.4.2 ระดับชั้นย่อย Network (Network Sub Layer)

3.4.2.1 ภาพรวมโปรโตคอลในระดับชั้นย่อย Network

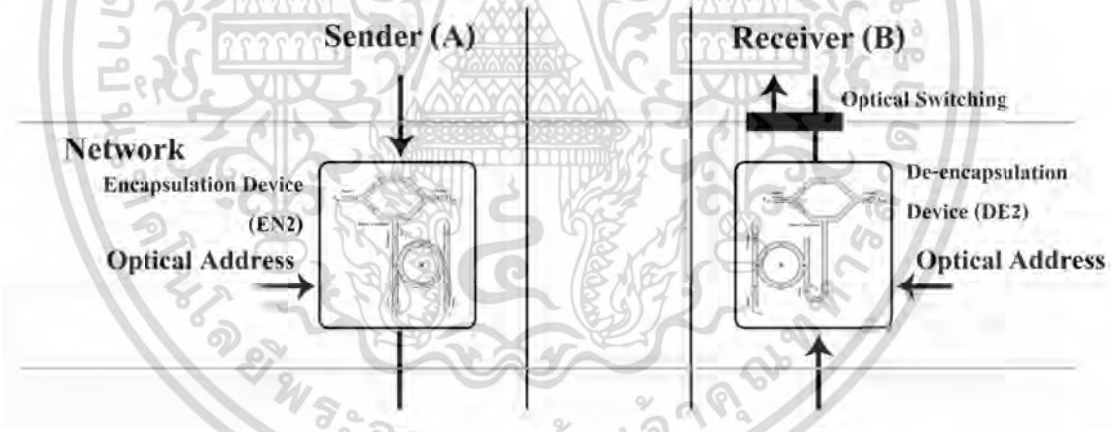


รูปที่ 3.17 แผนภาพคุณสมบัติของระดับชั้นย่อย Network

จากรูปที่ 3.17 แสดงแผนภาพคุณสมบัติของระดับชั้นย่อย Network มีคุณสมบัติในการทำหน้าที่การควบคุมการติดต่อรับหรือส่งข้อมูลระหว่างอุปกรณ์ต่าง ๆ ในระบบเครือข่ายให้เป็นไปด้วยความเรียบร้อย ถึงผู้รับข้อมูลถูกต้องตามที่ผู้ส่งข้อมูลต้องการด้วยที่อยู่เชิงแสง (Optical Address)

ที่อยู่เชิงแสง (Optical Address) หมายถึง Bright Soliton โดยมีคุณลักษณะเฉพาะตัวที่สามารถระบุที่อยู่ภายในเครือข่ายเชิงแสงได้ เพื่อนำไปใช้ในการแทนบุคคลใดบุคคลหนึ่งภายในเครือข่ายเชิงแสง ซึ่งจะกล่าวถึงรายละเอียดในบทที่ 5 ต่อไป

3.4.2.2 รายละเอียดโปรโตคอลในระดับชั้นย่อย Network



รูปที่ 3.18 แผนภาพอุปกรณ์โปรโตคอลในระดับชั้นย่อย Network

จากรูปที่ 3.18 แสดงแผนภาพอุปกรณ์โปรโตคอลในระดับชั้นย่อย Network มีขั้นตอนการทำงานในระดับชั้นย่อยนี้ ดังนี้

ขั้นตอนการทำงานของโปรโตคอลในระดับชั้นย่อย Network (ฝั่งผู้ส่งข้อมูล)

ขั้นตอนที่ 1 : รับสัญญาณจากระดับชั้นย่อย Security

ขั้นตอนที่ 2 : นำสัญญาณจากขั้นตอนที่ 1 ห่อหุ้มเชิงแสง (Optical Encapsulation) ด้วยที่อยู่เชิงแสง (Optical Address) ของผู้รับข้อมูล (Receiver (B))

ขั้นตอนที่ 3 : นำสัญญาณจากขั้นตอนที่ 2 ส่งต่อไปยังระดับชั้นย่อย Physical

ขั้นตอนการทำงานของโปรโตคอลในระดับชั้นย่อย Network (ฝั่งผู้รับข้อมูล)

ขั้นตอนที่ 1 : รับสัญญาณจากระดับชั้นย่อย Physical

ขั้นตอนที่ 2 : นำสัญญาณจากขั้นตอนที่ 1 ถอดข้อมูลเชิงแสง (Optical De-encapsulation) ด้วยที่อยู่เชิงแสง (Optical Address) ของผู้รับข้อมูล (Receiver (B))

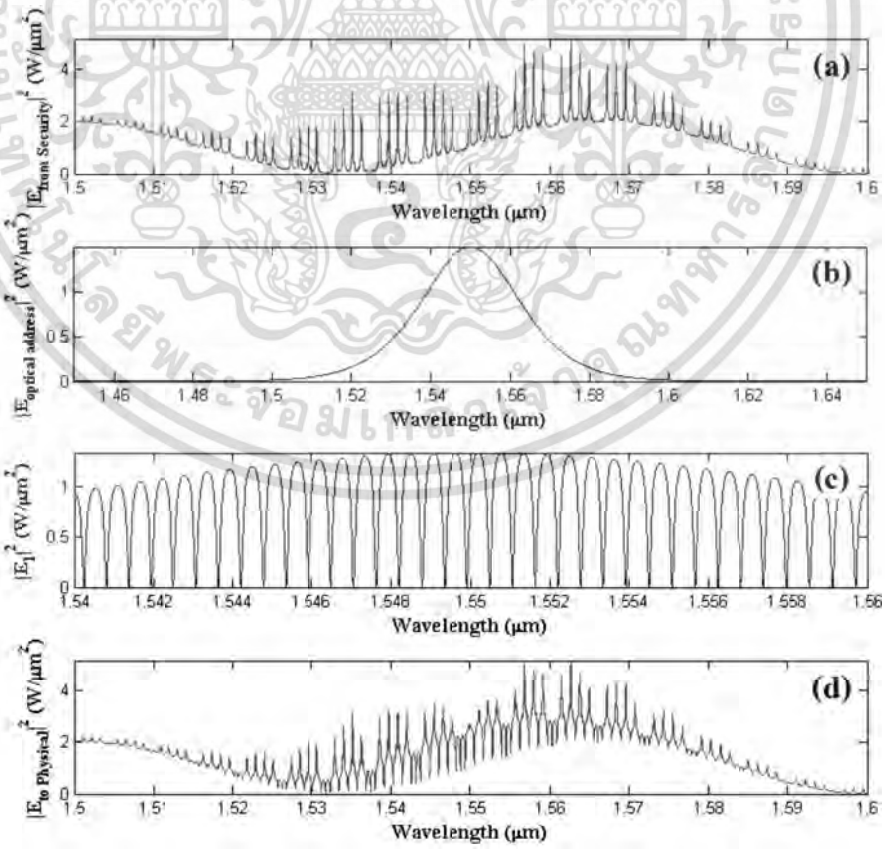
ขั้นตอนที่ 3 : นำสัญญาณจากขั้นตอนที่ 2 ส่งต่อไปยังระดับชั้นย่อย Security

3.4.2.3 การจำลองโปรโตคอลในระดับชั้นย่อย Network

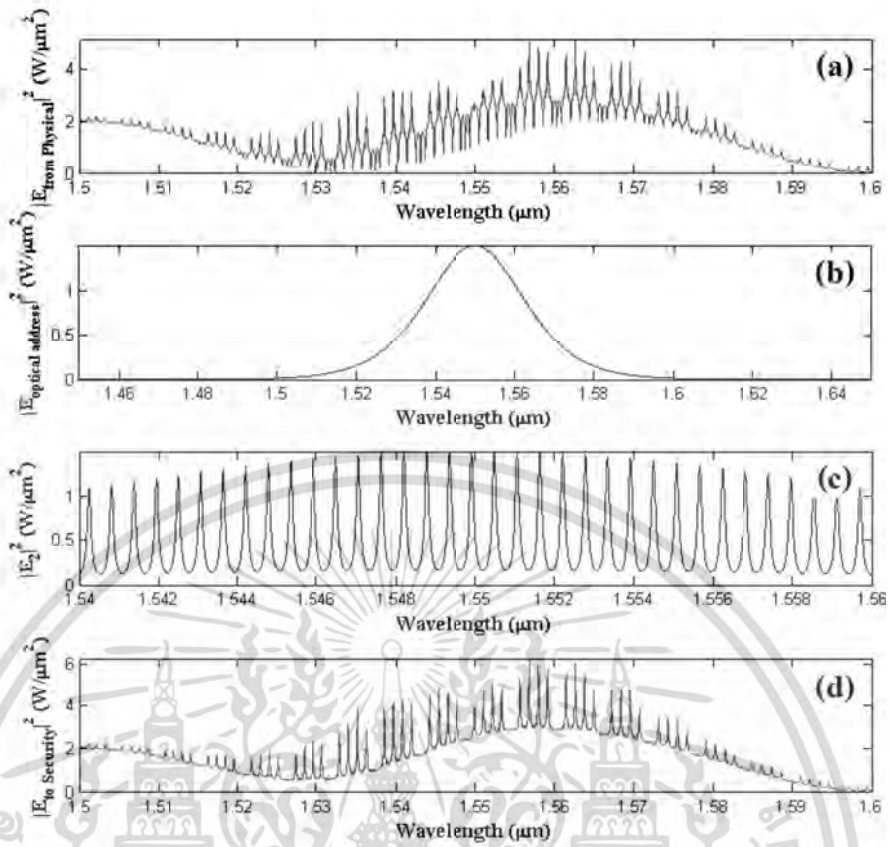
ในหัวข้อนี้เป็นการจำลองโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง (Optical Transmission and Addressing Protocol) ในระดับชั้นย่อย Network โดยยกตัวอย่างการจำลองการส่งข้อมูลจากผู้ส่งไปยังผู้รับ โดยมีแผนภาพอุปกรณ์โปรโตคอลในระดับชั้นย่อย Network ตามรูปที่ 3.18 โดยมีรายละเอียดการจำลองดังนี้

ตารางที่ 3.2 พารามิเตอร์ของอุปกรณ์ที่ใช้ในการจำลองโปรโตคอลในระดับชั้นย่อย Network

อุปกรณ์	พารามิเตอร์	ค่าพารามิเตอร์
Add Drop Filter (EN2,DE2)	ขนาดวงแหวน	200 μm
	สัมประสิทธิ์การคัปปลิ้ง κ_1	0.5
	สัมประสิทธิ์การคัปปลิ้ง κ_2	0.5



รูปที่ 3.19 ผลการจำลองโปรโตคอลในระดับชั้นย่อย Network ของฝั่งผู้ส่งข้อมูล



รูปที่ 3.20 ผลการจำลองโปรโตคอลในระดับชั้นย่อย Network ของฝั่งผู้รับข้อมูล

จากรูปที่ 3.19 ผลการจำลองโปรโตคอลในระดับชั้นย่อย Network ของฝั่งผู้ส่งข้อมูล รูปที่ 3.19 (a) แสดงสัญญาณจากระดับชั้นย่อย Security รูปที่ 3.19 (b) แสดงสัญญาณที่อยู่เชิงแสง (Optical Address) ของผู้รับข้อมูล รูปที่ 3.19 (c) แสดงสัญญาณที่ออกมาทาง Through Port ของอุปกรณ์วงแหวนเพิ่มลดสัญญาณภายในอุปกรณ์ห่อหุ้มเชิงแสง (Optical Encapsulation) ที่นำสัญญาณที่อยู่เชิงแสงเข้าไป Input Port รูปที่ 3.19 (d) แสดงสัญญาณที่เกิดจากการห่อหุ้มเชิงแสงระหว่างสัญญาณจากระดับชั้นย่อย Security (รูปที่ 3.19 (a)) กับสัญญาณที่อยู่เชิงแสง (Optical Address) (รูปที่ 3.19 (b)) โดยที่จะเป็นสัญญาณที่ส่งต่อไปยังระดับชั้นย่อย Physical ต่อไป

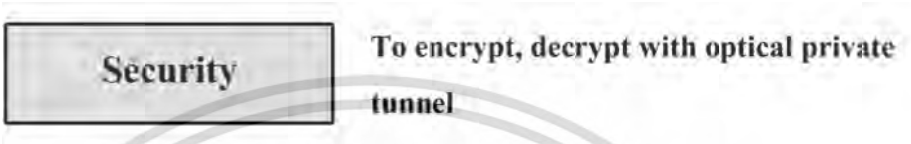
จากรูปที่ 3.20 ผลการจำลองโปรโตคอลในระดับชั้นย่อย Network ของฝั่งผู้รับข้อมูล รูปที่ 3.20 (a) แสดงสัญญาณจากระดับชั้นย่อย Physical รูปที่ 3.20 (b) แสดงสัญญาณที่อยู่เชิงแสง (Optical Address) ของผู้รับข้อมูล รูปที่ 3.20 (c) แสดงสัญญาณที่ออกมาทาง Drop Port ของอุปกรณ์วงแหวนเพิ่มลดสัญญาณภายในอุปกรณ์ถอดข้อมูลเชิงแสง (Optical De-encapsulation) ที่นำสัญญาณที่อยู่เชิงแสงเข้าไป Input Port รูปที่ 3.20 (d) แสดงสัญญาณที่เกิดจากการถอดข้อมูลเชิงแสงระหว่างสัญญาณจากระดับชั้นย่อย Network (รูปที่ 3.20 (a)) กับสัญญาณที่อยู่เชิงแสง (Optical Address) (รูปที่ 3.20 (b)) โดยที่จะเป็นสัญญาณที่ส่งต่อไปยังระดับชั้นย่อย Security ต่อไป

จากรูปที่ 3.19 (c) และรูปที่ 3.20 (c) จะเห็นได้ว่าสัญญาณทั้งสองมีความแตกต่างกัน แต่สัญญาณมีลักษณะตรงข้ามกัน เนื่องจากอุปกรณ์ห่อหุ้มเชิงแสง (Optical Encapsulation) และอุปกรณ์ถอดข้อมูลเชิงแสง (Optical De-encapsulation) มีการนำสัญญาณจากอุปกรณ์วงแหวนเพิ่ม

ลดสัญญาณมาใช้งานคนละ Port กัน โดยที่การห่อหุ้มเชิงแสงมีการใช้งานสัญญาณจาก Through Port และการถอดข้อมูลเชิงแสงมีการใช้งานสัญญาณจาก Drop Port ซึ่งถ้าพารามิเตอร์ของอุปกรณ์วงแหวนเพิ่มลดสัญญาณเหมือนกัน สัญญาณจากทั้งสอง Port จะให้ผลลักษณะตรงข้ามกัน เป็นผลให้เกิดความแตกต่างกันของ 2 สัญญาณดังกล่าว

3.4.3 ระดับชั้นย่อย Security (Security Sub Layer)

3.4.3.1 ภาพรวมโปรโตคอลในระดับชั้นย่อย Security

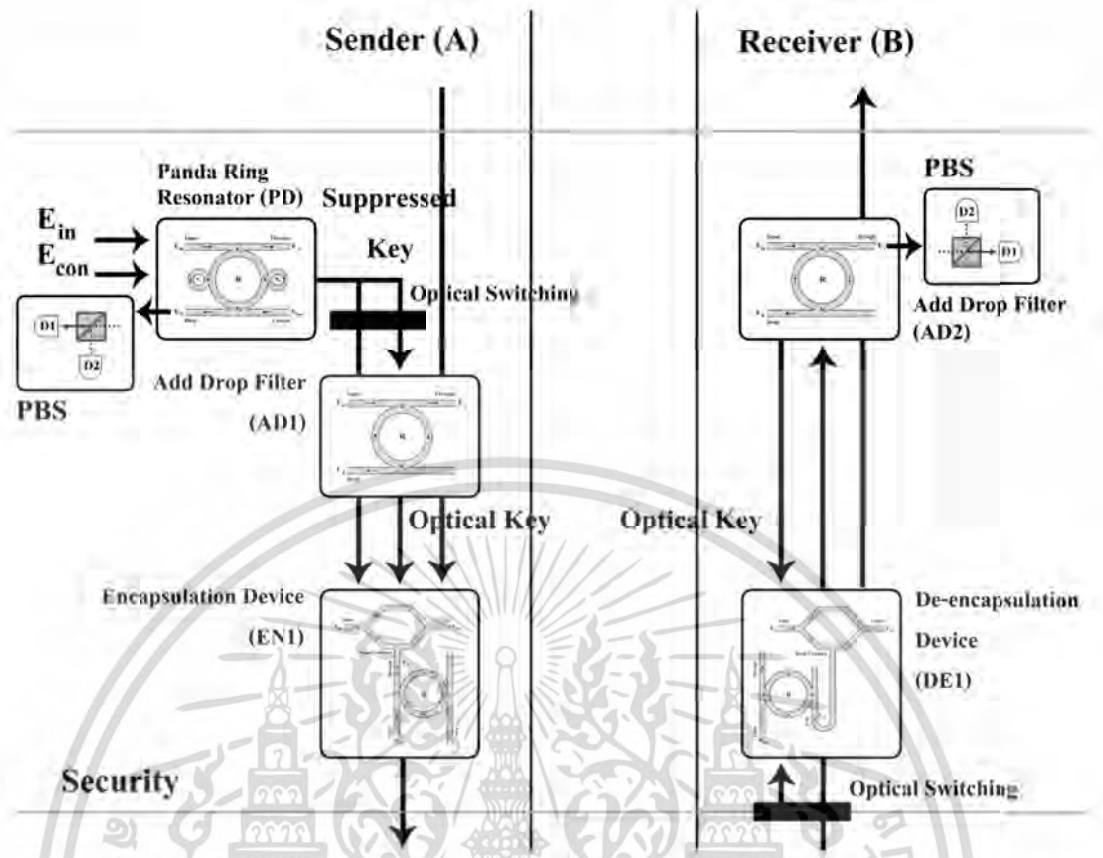


รูปที่ 3.21 แผนภาพคุณสมบัติของระดับชั้นย่อย Security

จากรูปที่ 3.21 แสดงแผนภาพคุณสมบัติของระดับชั้นย่อย Security มีคุณสมบัติในการทำหน้าที่ให้การสื่อสารข้อมูลภายในเครือข่ายเป็นไปอย่างปลอดภัย ด้วยวิธีการซ่อนกุญแจเชิงแสงและการกู้คืนกุญแจเชิงแสง (Key Suppression and Recovery) รวมถึงสร้างช่องทางการสื่อสารปลอดภัยด้วยเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel)

กุญแจเชิงแสง (Optical Key) หมายถึง ข้อมูลสัญญาณแสงที่นำไปใช้ในการเข้ารหัสเชิงแสง (Optical Cryptography) โดยเป็นข้อมูลสัญญาณแสงที่ผ่านวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) เพื่อให้ข้อมูลสัญญาณแสงเป็นแบบสุ่ม และเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) หมายถึง ช่องทางในการสื่อสารเชิงแสงเสมือนจากผู้ส่งข้อมูลไปยังผู้รับข้อมูลโดยตรง โดยเป็นช่องทางที่มีการเข้ารหัสเชิงแสง (Optical Cryptography) ด้วยกุญแจเชิงแสง (Optical Key) ซึ่งจะกล่าวถึงรายละเอียดในบทที่ 6 ต่อไป

3.4.3.2 รายละเอียดโปรโตคอลในระดับชั้นย่อย Security



รูปที่ 3.22 แผนภาพอุปกรณ์โปรโตคอลในระดับชั้นย่อย Security

จากรูปที่ 3.22 แสดงแผนภาพอุปกรณ์โปรโตคอลในระดับชั้นย่อย Security ขั้นตอนการทำงานในระดับชั้นย่อยนี้ ดังนี้

ขั้นตอนการทำงานของโปรโตคอลในระดับชั้นย่อย Security (ฝั่งผู้ส่งข้อมูล)

ขั้นตอนที่ 1 : รับสัญญาณจากระดับชั้นย่อย Application

ขั้นตอนที่ 2 : ผู้ส่งข้อมูล (Sender (A)) ใช้การซ่อนกุญแจเชิงแสง (Optical Key Suppression) เพื่อสร้างกุญแจเชิงแสง (Optical Key) ในการสื่อสารข้อมูล และส่งสัญญาณกุญแจที่ถูกซ่อนด้วยสัญญาณรูปปากให้ผู้รับข้อมูล (Receiver (B))

ขั้นตอนที่ 3 : นำกุญแจเชิงแสง (Optical Key) ที่ได้จากการซ่อนกุญแจเชิงแสง (Optical Key Suppression) ในขั้นตอนที่ 2 ห่อหุ้มเชิงแสง (Optical Encapsulation) กับสัญญาณจากขั้นตอนที่ 1

ขั้นตอนที่ 4 : นำสัญญาณจากขั้นตอนที่ 3 ส่งต่อไปยังระดับชั้นย่อย Network

ขั้นตอนการทำงานของโปรโตคอลในระดับชั้นย่อย Security (ฝั่งผู้รับข้อมูล)

ขั้นตอนที่ 1 : รับสัญญาณจากระดับชั้นย่อย Network

ขั้นตอนที่ 2 : ผู้รับข้อมูล (Receiver (B)) กู้คืนกุญแจเชิงแสง (Optical Key Recovery) จากสัญญาณกุญแจที่ถูกซ่อนด้วยสัญญาณรูปปากที่ส่งมากจากผู้ส่งข้อมูล (Sender (A))

ขั้นตอนที่ 3 : นำสัญญาณจากขั้นตอนที่ 1 ถอดข้อมูลเชิงแสง (Optical De-encapsulation) ด้วยกุญแจเชิงแสง (Optical Key) ที่ได้จากขั้นตอนที่ 2

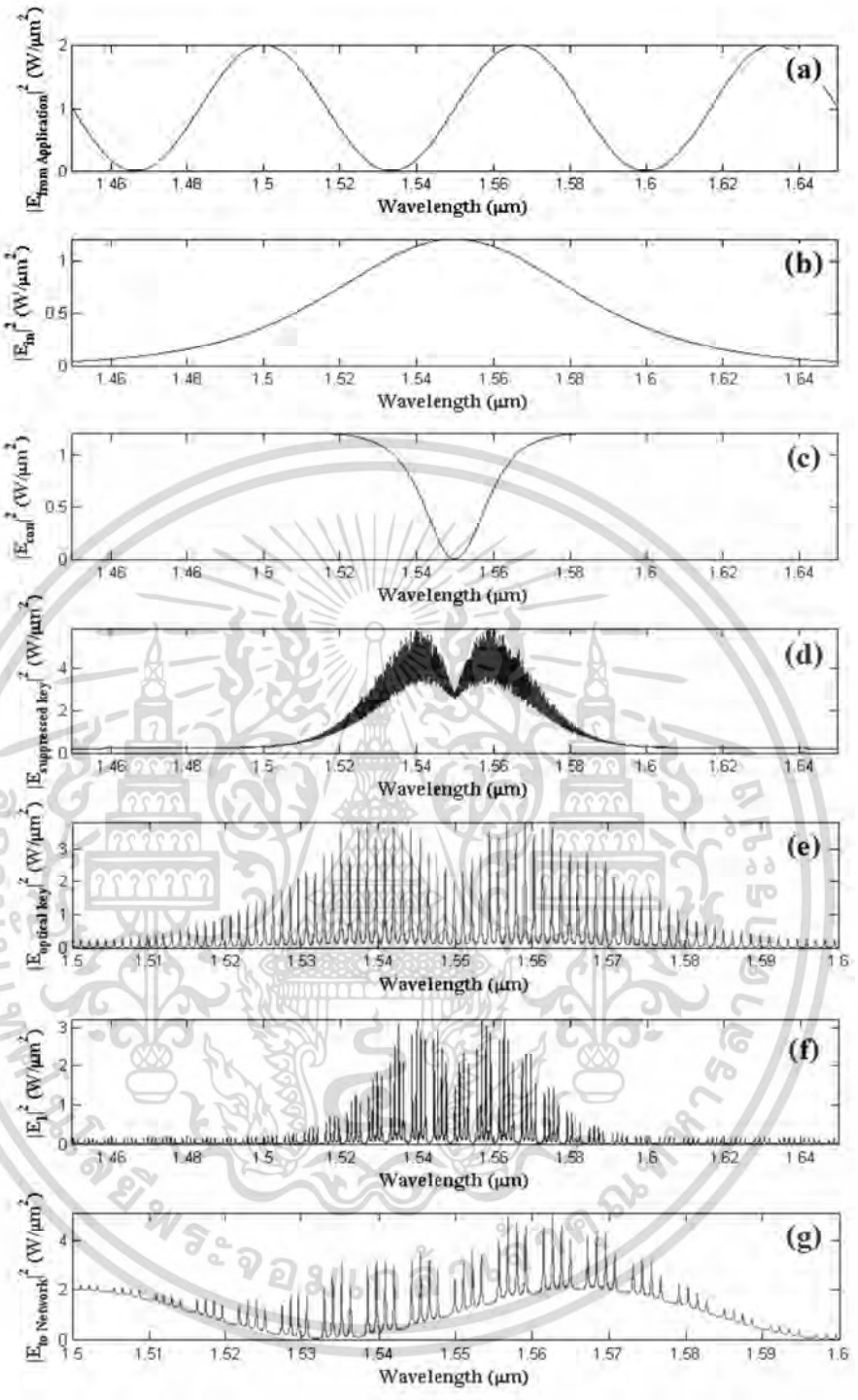
ขั้นตอนที่ 4 : นำสัญญาณจากขั้นตอนที่ 3 ส่งต่อไปยังระดับชั้นย่อย Application

3.4.3.3 การจำลองโปรโตคอลในระดับชั้นย่อย Security

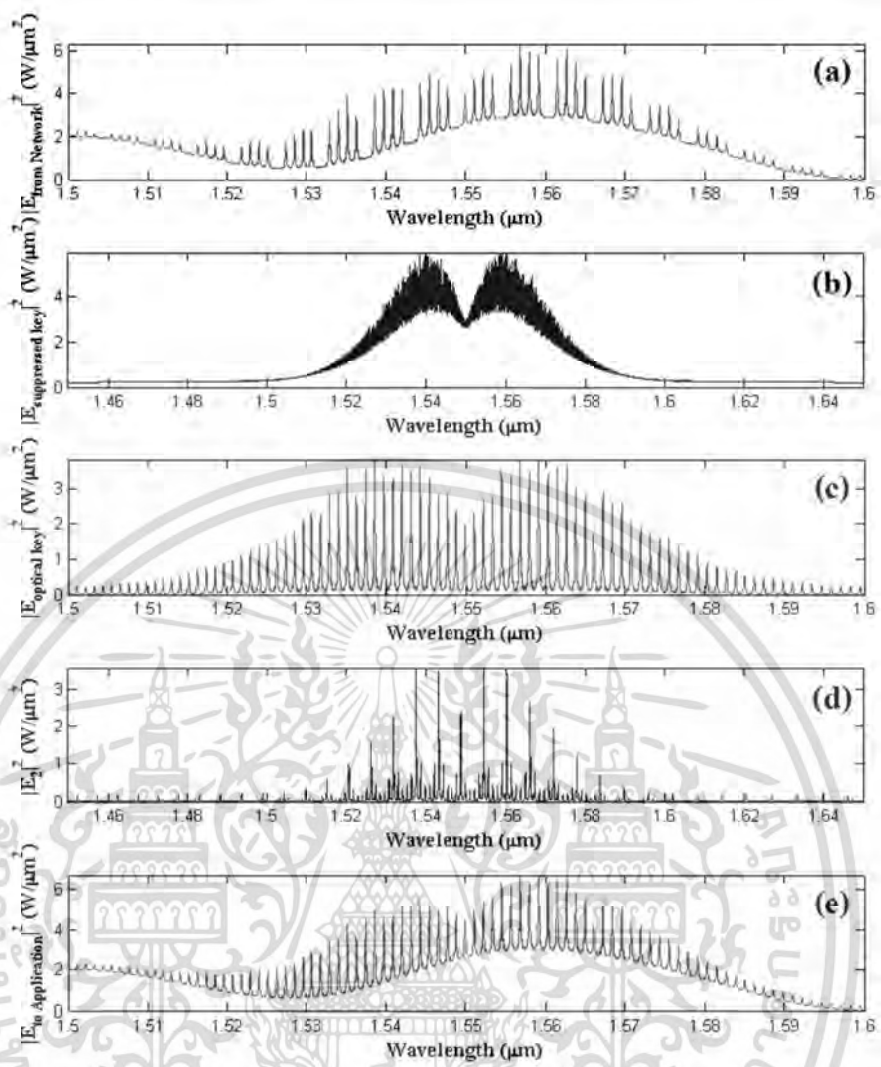
ในหัวข้อนี้เป็นการจำลองโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง (Optical Transmission and Addressing Protocol) ในระดับชั้นย่อย Security โดยยกตัวอย่างการจำลองการส่งข้อมูลจากผู้ส่งไปยังผู้รับ โดยมีแผนภาพอุปกรณ์โปรโตคอลในระดับชั้นย่อย Security ตามรูปที่ 3.22 โดยมีรายละเอียดการจำลองดังนี้

ตารางที่ 3.3 พารามิเตอร์ของอุปกรณ์ที่ใช้ในการจำลองโปรโตคอลในระดับชั้นย่อย Security

อุปกรณ์ , สัญญาณ	พารามิเตอร์	ค่าพารามิเตอร์
Panda Ring Resonator (PD)	ขนาดวงแหวนกลาง	200 μm
	ขนาดวงแหวนข้างซ้ายและข้างขวา	15 μm
	สัมประสิทธิ์การคัปปลิ้ง κ_1	0.2
	สัมประสิทธิ์การคัปปลิ้ง κ_2	0.2
	สัมประสิทธิ์การคัปปลิ้ง κ_3	0.1
	สัมประสิทธิ์การคัปปลิ้ง κ_4	0.1
Add Drop Filter (AD1,AD2)	ขนาดวงแหวน	200 μm
	สัมประสิทธิ์การคัปปลิ้ง κ_1	0.5
	สัมประสิทธิ์การคัปปลิ้ง κ_2	0.2
Add Drop Filter (EN1,DE1)	ขนาดวงแหวน	20 μm
	สัมประสิทธิ์การคัปปลิ้ง κ_1	0.5
	สัมประสิทธิ์การคัปปลิ้ง κ_2	0.5



รูปที่ 3.23 ผลการจำลองโปรโตคอลในระดับชั้นย่อย Security ของฝั่งผู้ส่งข้อมูล



รูปที่ 3.24 ผลการจำลองโปรโตคอลในระดับชั้นย่อย Security ของฝั่งผู้รับข้อมูล

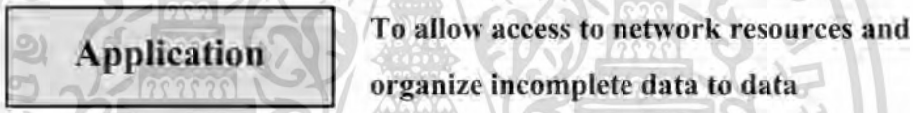
จากรูปที่ 3.23 ผลการจำลองโปรโตคอลในระดับชั้นย่อย Security ของฝั่งผู้ส่งข้อมูล รูปที่ 3.23 (a) แสดงสัญญาณจากระดับชั้นย่อย Application รูปที่ 3.23 (b) และรูปที่ 3.23 (c) แสดงสัญญาณ E_{in} และ E_{con} ตามลำดับ ซึ่งเป็นสัญญาณที่ส่งเข้าทาง Input Port และ Control Port ของวงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) เพื่อใช้ในการสร้างสัญญาณรูปปาก (LIP Signal) ทาง Through Port ตามรูปที่ 3.23 (d) รูปที่ 3.23 (e) แสดงสัญญาณกุญแจเชิงแสง (Optical Key) ที่เกิดจากการนำสัญญาณรูปปาก (LIP Signal) เข้าทาง Input Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) และที่ Drop Port คือ สัญญาณกุญแจเชิงแสง (Optical Key) ที่นำไปใช้ในการสร้างเครือข่ายส่วนตัวเสมือนเชิงแสงเพื่อการสื่อสารอย่างปลอดภัย รูปที่ 3.23 (f) แสดงกุญแจเชิงแสง (Optical Key) ที่นำสัญญาณเข้าไป Input Port ของอุปกรณ์วงแหวนเพิ่มลดสัญญาณภายในอุปกรณ์ห่อหุ้มเชิงแสง (Optical Encapsulation) และได้สัญญาณออกมาทาง Through Port รูปที่ 3.23 (g) แสดงสัญญาณที่เกิดจากการห่อหุ้มเชิงแสงระหว่างสัญญาณจาก

ระดับชั้นย่อย Application (รูปที่ 3.23 (a)) กับสัญญาณกุญแจเชิงแสง (Optical Key) (รูปที่ 3.23 (c)) โดยที่จะเป็นสัญญาณที่ส่งต่อไปยังระดับชั้นย่อย Network ต่อไป

รูปที่ 3.24 ผลการจำลองโปรโตคอลในระดับชั้นย่อย Security ของฝั่งผู้รับข้อมูล รูปที่ 3.24 (a) แสดงสัญญาณจากระดับชั้นย่อย Network รูปที่ 3.24 (b) แสดงสัญญาณรูปปาก (LIP Signal) รูปที่ 3.24 (c) แสดงสัญญาณกุญแจเชิงแสง (Optical Key) ที่เกิดจากการนำสัญญาณรูปปาก (LIP Signal) เข้าทาง Input Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) และที่ Drop Port คือ สัญญาณกุญแจเชิงแสง (Optical Key) ที่นำไปใช้ในการสื่อสารอย่างปลอดภัย รูปที่ 3.24 (d) แสดงกุญแจเชิงแสง (Optical Key) ที่นำสัญญาณเข้าไป Input Port ของอุปกรณ์วงแหวนเพิ่มลดสัญญาณภายในอุปกรณ์ห่อหุ้มเชิงแสง (Optical Encapsulation) และได้สัญญาณออกมาทาง Drop Port รูปที่ 3.24 (e) แสดงสัญญาณที่เกิดจากการห่อหุ้มเชิงแสงระหว่างสัญญาณจากระดับชั้นย่อย Network (รูปที่ 3.24 (a)) กับสัญญาณกุญแจเชิงแสง (Optical Key) (รูปที่ 3.24 (c)) โดยที่จะเป็นสัญญาณที่ส่งต่อไปยังระดับชั้นย่อย Application ต่อไป

3.4.4 ระดับชั้นย่อย Application (Application Sub Layer)

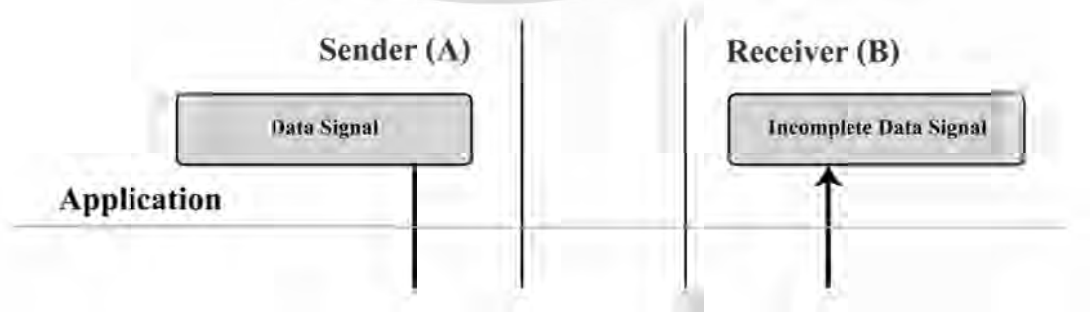
3.4.4.1 ภาพรวมโปรโตคอลในระดับชั้นย่อย Application



รูปที่ 3.25 แผนภาพคุณสมบัติของระดับชั้นย่อย Application

จากรูปที่ 3.25 แสดงแผนภาพคุณสมบัติของ ระดับชั้นย่อย Application มีคุณสมบัติในการทำหน้าที่เป็นตัวกลางหรือส่วนติดต่อระหว่างโปรแกรมกับระดับชั้นย่อยอื่น ๆ ในโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงที่นำเสนอ รวมถึงมีการปรับข้อมูลในฝั่งผู้รับข้อมูลให้เป็นข้อมูลที่สมบูรณ์ก่อนส่งให้กับโปรแกรมอื่น ๆ ต่อไป

3.4.4.2 รายละเอียดโปรโตคอลในระดับชั้นย่อย Application



รูปที่ 3.26 แผนภาพอุปกรณ์โปรโตคอลในระดับชั้นย่อย Application

จากรูปที่ 3.26 แสดงแผนภาพอุปกรณ์โปรโตคอลในระดับชั้นย่อย Physical ขั้นตอนการทำงานในระดับชั้นย่อยนี้ ดังนี้

ขั้นตอนการทำงานของโปรโตคอลในระดับชั้นย่อย Application (ฝั่งผู้ส่งข้อมูล)

ขั้นตอนที่ 1 : นำสัญญาณข้อมูล (Data Signal) ส่งต่อไปยังระดับชั้นย่อย Security

ขั้นตอนการทำงานของโปรโตคอลในระดับชั้นย่อย Application (ฝั่งผู้รับข้อมูล)

ขั้นตอนที่ 1 : รับสัญญาณจากระดับชั้นย่อย Security

ขั้นตอนที่ 2 : สัญญาณจากขั้นตอนที่ 1 คือ สัญญาณที่ไม่สมบูรณ์ที่ส่งมากจาก Sender (A)

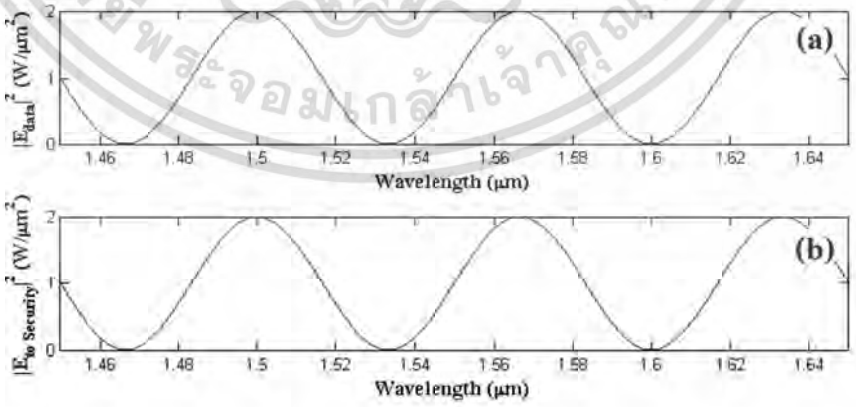
ขั้นตอนที่ 3 : สัญญาณข้อมูล (Data Signal) ที่สมบูรณ์ที่ส่งมาจาก Sender (A) คำนวณจากสมการที่ 3.1

สัญญาณสมบูรณ์ที่ส่งจาก Sender (A) =
สัญญาณในขั้นตอนที่ 2 – (ที่อยู่เชิงแสง + กุญแจเชิงแสง) (3.1)

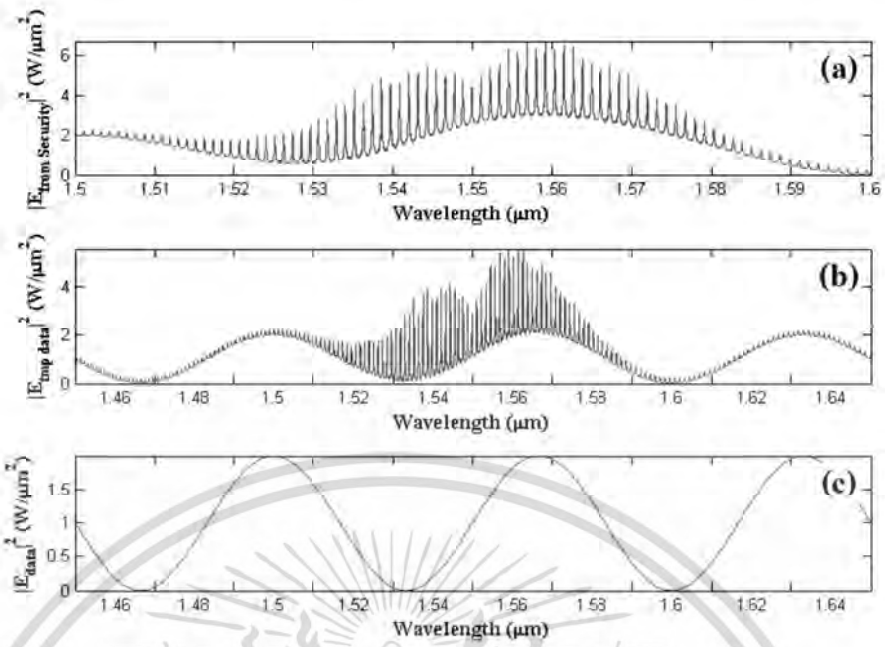
ในทางปฏิบัติการลบกันของสัญญาณแสงสามารถประยุกต์ใช้ไมเคิลสันอินเทอร์เฟียร์โรมิเตอร์ (Michelson Interferometer) มาทำงานในส่วนนี้ได้ โดยเกิดขึ้นได้เนื่องจากใช้หลักการแทรกสอดแบบหักล้าง

3.4.4.3 การจำลองโปรโตคอลในระดับชั้นย่อย Application

ในหัวข้อนี้เป็นการจำลองโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง (Optical Transmission and Addressing Protocol) ในระดับชั้นย่อย Physical โดยยกตัวอย่างการจำลองการส่งข้อมูลจากผู้ส่งไปยังผู้รับ โดยมีแผนภาพอุปกรณ์โปรโตคอลในระดับชั้นย่อย Application ตามรูปที่ 3.26 โดยมีรายละเอียดการจำลองดังนี้



รูปที่ 3.27 ผลการจำลองโปรโตคอลในระดับชั้นย่อย Application ของฝั่งผู้รับข้อมูล



รูปที่ 3.28 ผลการจำลองโปรโตคอลในระดับชั้นย่อย Application ของฝั่งผู้รับข้อมูล

จากรูปที่ 3.27 ผลการจำลองโปรโตคอลในระดับชั้นย่อย Application ของฝั่งผู้รับข้อมูล รูปที่ 3.27 (a) แสดงสัญญาณข้อมูลที่ Sender (A) ต้องการส่งข้อมูลไปยัง Receiver (B) รูปที่ 3.27 (b) แสดงสัญญาณที่ส่งต่อไปยังระดับชั้นย่อย Security โดยที่ รูปที่ 3.27 (a) และรูปที่ 3.27 (b) มีลักษณะสัญญาณเหมือนกัน เนื่องจากในฝั่งผู้ส่งข้อมูลระดับ Application หน้าที่เป็นตัวกลางหรือส่วนติดต่อระหว่างโปรแกรมกับระดับชั้นย่อยอื่น ๆ เท่านั้น

จากรูปที่ 3.28 ผลการจำลองโปรโตคอลในระดับชั้นย่อย Application ของฝั่งผู้รับข้อมูล รูปที่ 3.28 (a) แสดงสัญญาณจากระดับชั้นย่อย Security ซึ่งคือสัญญาณข้อมูลจาก Sender (A) ที่ไม่สมบูรณ์ ฝั่งผู้รับข้อมูลในระดับชั้นย่อย Application ต้องมีการปรับข้อมูลในฝั่งผู้รับข้อมูลให้เป็นข้อมูลที่สมบูรณ์ก่อนส่งให้กับโปรแกรมอื่น ๆ กล่าวคือ รูปที่ 3.28 (b) แสดงสัญญาณข้อมูลที่ไม่สมบูรณ์ที่มีการปรับข้อมูลโดยการ – กุญแจเชิงแสง (Optical Key) รูปที่ 3.28 (c) แสดงสัญญาณข้อมูลจาก Sender (A) ที่สมบูรณ์ ซึ่งเกิดจากสัญญาณตามรูปที่ 3.28 (b) – ที่อยู่เชิงแสง (Optical Address) ซึ่งจะเห็นว่าจากการวัดผลสำเร็จของการส่งข้อมูลในเครือข่ายสื่อสารในหัวข้อ 3.3.4 สัญญาณข้อมูลจาก Sender (A) สามารถส่งไปยัง Receiver (B) ได้สำเร็จ เนื่องจาก Receiver (B) มีที่อยู่เชิงแสง (Optical Address) และกุญแจเชิงแสง (Optical Key) ที่ถูกต้อง

3.5 สรุปผลการทำงานโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง

จากการจำลองเพื่ออธิบายโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงสำหรับการสื่อสารความเร็วสูงและความปลอดภัยสูงโดยใช้อุปกรณ์เชิงแสงทั้งหมดพบว่า โปรโตคอลที่นำเสนอทำให้การส่งข้อมูลระหว่างผู้ส่งข้อมูลและผู้รับข้อมูลถูกต้อง มีวิธีการส่งข้อมูลภายในเครือข่าย รวมถึงการส่งข้อมูลระหว่างระดับชั้นย่อยด้วยวิธีการห่อหุ้มเชิงแสง (Optical Encapsulation) ซึ่งจะกล่าวรายละเอียดในบทที่ 4 และเป็นการส่งข้อมูลที่ระบุที่อยู่ของผู้รับได้เนื่องจากมีการใช้งานที่อยู่เชิงแสง

(Optical Address) ซึ่งจะกล่าวรายละเอียดในบทที่ 5 อีกทั้งยังเป็นการส่งข้อมูลที่มีความปลอดภัยสูง เนื่องจากมีการใช้งานการซ่อนและการกู้คืนกุญแจเชิงแสง (Key Suppression and Recovery) และเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) ซึ่งจะกล่าวรายละเอียดในบทที่ 6 ต่อไป

บทที่ 4
การสื่อสารข้อมูลด้วยโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ

ในส่วนของบทนี้เป็นการกล่าวถึงการสื่อสารข้อมูลด้วยโปรโตคอลที่นำเสนอ อธิบายการส่งข้อมูลระหว่างระดับชั้นย่อย การส่งข้อมูลภายในเครือข่าย การส่งกุญแจเชิงแสงภายในเครือข่าย และผลของพารามิเตอร์ต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ด้านการสื่อสารข้อมูล รวมถึงข้อจำกัดการทำงานของโปรโตคอลด้านการสื่อสารข้อมูล โดยมีหัวข้อต่าง ๆ ดังนี้

- ปัญหาและประเด็นสำคัญ
- อธิบายการส่งข้อมูลระหว่างระดับชั้นย่อย (การห่อหุ้มเชิงแสงและการถอดข้อมูลเชิงแสง)
  ความหมายของการห่อหุ้มเชิงแสงและการถอดข้อมูลเชิงแสง
- อธิบายการส่งข้อมูลภายในเครือข่าย
  การส่งข้อมูลภายในเครือข่าย
  การส่งกุญแจเชิงแสงภายในเครือข่าย
- การจำลองการส่งข้อมูลในเครือข่าย
- ผลของพารามิเตอร์ต่อสัญญาณที่ถูกเข้ารหัสด้านการสื่อสารข้อมูล
- ข้อจำกัดการทำงานของโปรโตคอลด้านการสื่อสารข้อมูล
- อภิปรายสรุปการสื่อสารข้อมูลด้วยโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ

4.1 ปัญหาและประเด็นสำคัญ

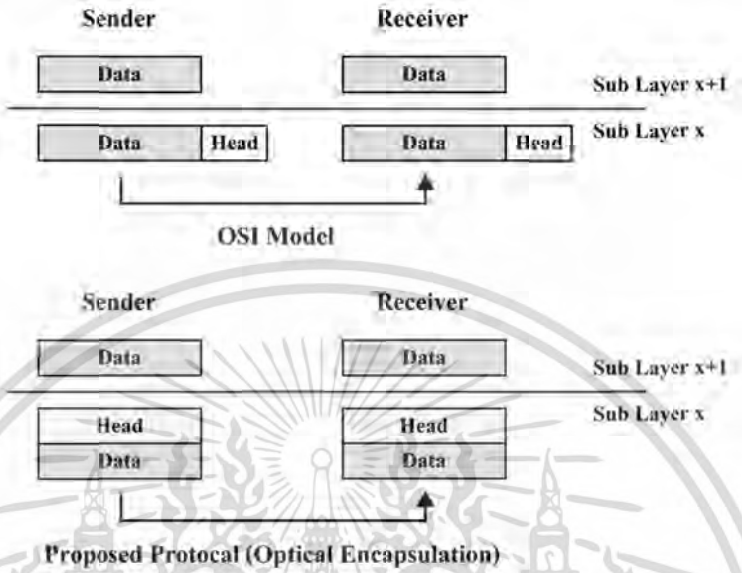
ในส่วนของหัวข้อนี้กล่าวถึงการสื่อสารข้อมูลด้วยโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ ซึ่งกล่าวถึง 2 ประเด็นคือ การสื่อสารข้อมูลระหว่างระดับชั้นย่อยและการสื่อสารข้อมูลภายในเครือข่าย โดยมีภาพรวมดังนี้

การสื่อสารข้อมูลระหว่างระดับชั้นย่อย ในการพัฒนาโปรโตคอลที่เกี่ยวข้องกับการสื่อสารที่อ้างอิงการทำงานในลักษณะของระดับชั้นเหมือนกับ OSI Model ซึ่งเป็นรูปแบบมาตรฐานที่มีการใช้งานกันทั่วไป ซึ่งงานวิจัยนี้ก็พัฒนาโปรโตคอลการสื่อสารโดยแบ่งการทำงานเป็นระดับชั้นเหมือนกัน โดยที่กระบวนหนึ่งที่สำคัญของการทำงานเป็นระดับชั้น คือ การห่อหุ้ม (Encapsulation) กล่าวคือ เป็นการจัดเตรียมข้อมูลให้มีความเหมาะสมในการสื่อสารข้อมูลในแต่ละระดับชั้น ในทางตรงกันข้ามฝั่งผู้รับข้อมูลในการส่งข้อมูลในแต่ละระดับชั้น ก็จำเป็นต้องมีกระบวนการถอดข้อมูล (De-encapsulation) กล่าวคือ เป็นการนำข้อมูลที่เหมาะสมกับระดับชั้นนั้น ออกจากการห่อหุ้ม (Encapsulation) โดยการพัฒนาโปรโตคอลในงานวิจัยนี้ เป็นการพัฒนาโปรโตคอลการสื่อสารข้อมูลโดยใช้อุปกรณ์เชิงแสงทั้งหมด ทำให้การส่งผ่านข้อมูลระหว่างระดับชั้น คือการห่อหุ้ม (Encapsulation) และการถอดข้อมูล (De-encapsulation) จำเป็นต้องพัฒนาอุปกรณ์และวิธีการที่จะสนับสนุนรูปแบบการสื่อสารเชิงแสงแบบดังกล่าว

การสื่อสารข้อมูลภายในเครือข่าย ในการพัฒนาโปรโตคอลนี้มีการส่งสัญญาณ 2 ลักษณะคือ การส่งสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) และการส่งสัญญาณกุญแจเชิงแสง (Optical Key) ที่ห่อหุ้มด้วยสัญญาณรูปปาก (LIP Signal) ซึ่งจะมีวิธีการส่งสัญญาณและข้อแตกต่างระหว่างการส่งสัญญาณทั้ง 2 ลักษณะ มีการอธิบายในลำดับถัดไปในหัวข้อ 4.3 อธิบายการส่งข้อมูลภายในเครือข่าย

4.2 อธิบายการส่งข้อมูลระหว่างระดับชั้นย่อย

4.2.1 ความหมายของการห่อหุ้มเชิงแสงและการถอดข้อมูลเชิงแสง



รูปที่ 4.1 การเปรียบเทียบการห่อหุ้มเชิงแสงและการห่อหุ้มข้อมูลใน OSI Model

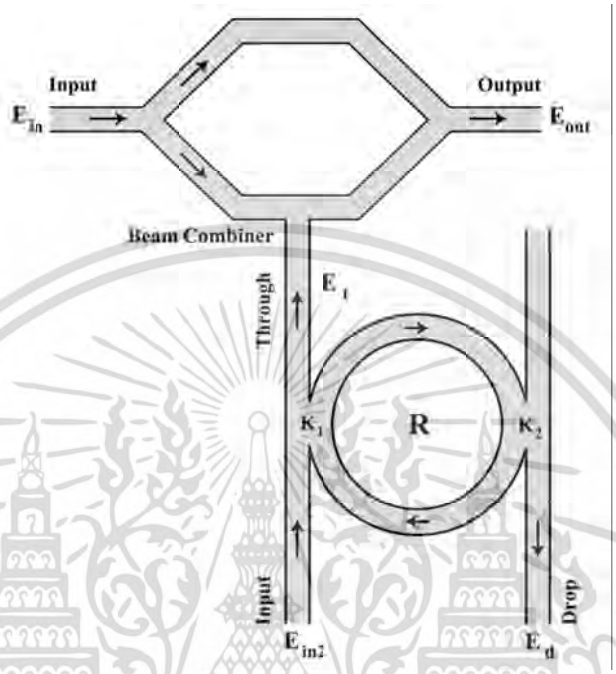
จากรูปที่ 4.1 เป็นการแสดงการเปรียบเทียบการห่อหุ้มเชิงแสงและการห่อหุ้มข้อมูลใน OSI Model กล่าวคือ การห่อหุ้มข้อมูล (Encapsulation) ใน OSI Model เป็นการนำข้อมูลการสื่อสารในระดับชั้น (Layer) นั้นมาไว้ข้างหน้าและ/หรือไว้ข้างหลังของข้อมูลที่ถูกส่งมาจากระดับชั้น (Layer) ก่อนหน้า แต่การห่อหุ้มเชิงแสง (Optical Encapsulation) เป็นการนำข้อมูลการสื่อสารในระดับชั้น (Layer) นั้น มาซ้อนทับ (หรือการแทรกสอด) ข้อมูลที่ถูกส่งมาจากระดับชั้น (Layer) ก่อนหน้า ในส่วนของการถอดข้อมูล (De-encapsulation) ใน OSI Model เป็นการนำข้อมูลการสื่อสารในระดับชั้น (Layer) นั้นออกจากข้างหน้าและ/หรือข้างหลังข้อมูลที่ถูกส่งมาจากระดับชั้น (Layer) ก่อนหน้า แต่การถอดข้อมูลเชิงแสง (Optical De-encapsulation) เป็นการนำข้อมูลการสื่อสารในระดับชั้น (Layer) นั้น มาซ้อนทับข้อมูลที่ถูกส่งมาจากระดับชั้น (Layer) ก่อนหน้าเหมือนกับการห่อหุ้มเชิงแสง (Optical Encapsulation) แต่จะมีการหักลบข้อมูลออกในระดับชั้นย่อยสุดท้ายระดับชั้นย่อย Application

การห่อหุ้มเชิงแสง (Optical Encapsulation) หมายถึง การจัดเตรียมข้อมูลให้มีความเหมาะสมในการสื่อสารข้อมูลในแต่ละระดับชั้นย่อย (Sub Layer) โดยข้อมูลของระดับชั้นย่อยก่อนหน้าเป็นข้อมูลสัญญาณแสงและข้อมูลที่จะมีการห่อหุ้มในระดับชั้นย่อยนั้นก็เป็นข้อมูลสัญญาณแสงเช่นกัน

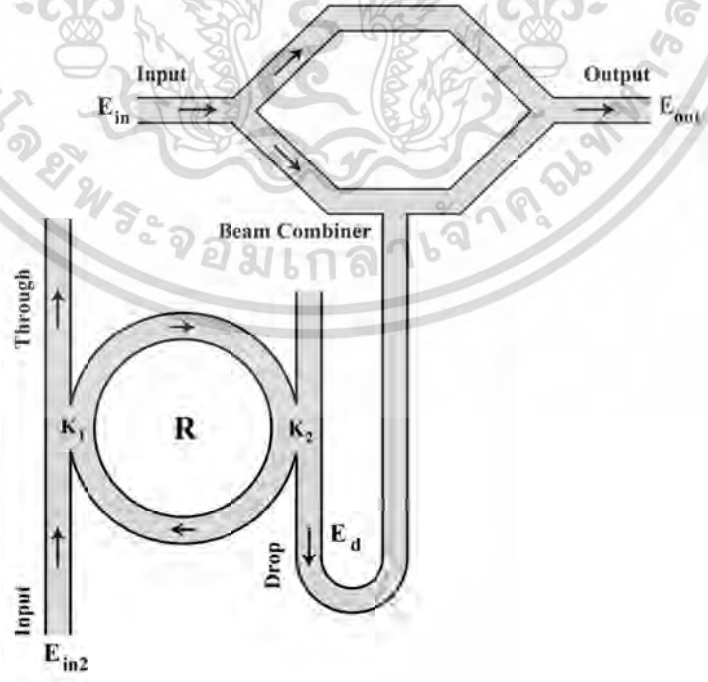
การถอดข้อมูลเชิงแสง (Optical De-encapsulation) หมายถึง เป็นการนำข้อมูลที่เหมาะสมกับระดับชั้นย่อย (Sub Layer) นั้น ออกจากการห่อหุ้มเชิงแสง (Optical Encapsulation) โดยข้อมูลในระดับชั้นย่อยนั้นที่ต้องการถอดข้อมูลออกเป็นข้อมูลสัญญาณแสงและข้อมูลที่ส่งต่อไปยังระดับถัดไปเป็นข้อมูลสัญญาณแสงเช่นกัน

4.2.2 วิธีการห่อหุ้มและถอดข้อมูลเชิงแสง

วิธีการห่อหุ้มและถอดข้อมูลเชิงแสง (Optical Encapsulation / De-encapsulation) ทำได้โดยใช้หลักการของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) และอุปกรณ์ที่ใช้หลักการของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer) อธิบายได้ดังนี้



รูปที่ 4.2 อุปกรณ์ที่ใช้ในการห่อหุ้มข้อมูลเชิงแสง



รูปที่ 4.3 อุปกรณ์ที่ใช้ในการถอดข้อมูลเชิงแสง

จากรูปที่ 4.2 เป็นการแสดงอุปกรณ์ที่ใช้ในการห่อหุ้มข้อมูลเชิงแสง ซึ่งประกอบด้วยวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) และอุปกรณ์ที่ใช้หลักการของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer) (ตามรูปที่ 2.17 และรูปที่ 2.19) และจากรูปที่ 4.3 เป็นการแสดงอุปกรณ์ที่ใช้ในการถอดข้อมูลเชิงแสง ประกอบด้วยอุปกรณ์เชิงแสงเหมือนกับวิธีการห่อหุ้มข้อมูลเชิงแสง ซึ่งมีวิธีการดังนี้

วิธีการห่อหุ้มเชิงแสง (Optical Encapsulation)

(จากรูปที่ 4.2 สัญญาณ E_{in2} ต้องการถูกห่อหุ้มเชิงแสงด้วยสัญญาณ E_{in})

ขั้นตอนที่ 1 : นำสัญญาณ E_{in} เข้าทาง Input Port ของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer)

ขั้นตอนที่ 2 : นำสัญญาณ E_{in2} เข้าทาง Input Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter)

ขั้นตอนที่ 3 : นำสัญญาณที่ออกจาก Through Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) รวมกับผลของสัญญาณในขั้นตอนที่ 1 ด้วย Beam Combiner

ขั้นตอนที่ 4 : สัญญาณที่ออกจาก Output Port ของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer) คือ สัญญาณ E_{in2} ที่ถูกห่อหุ้มเชิงแสงด้วยสัญญาณ E_{in}

วิธีการถอดข้อมูลเชิงแสง (Optical De-encapsulation)

(จากรูปที่ 4.3 สัญญาณ E_{in2} ต้องการถอดข้อมูลเชิงแสงด้วยสัญญาณ E_{in})

ขั้นตอนที่ 1 : นำสัญญาณ E_{in} เข้าทาง Input Port ของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer)

ขั้นตอนที่ 2 : นำสัญญาณ E_{in2} เข้าทาง Input Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter)

ขั้นตอนที่ 3 : นำสัญญาณที่ออกจาก Drop Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) รวมกับผลของสัญญาณในขั้นตอนที่ 1 ด้วย Beam Combiner

ขั้นตอนที่ 4 : สัญญาณที่ออกจาก Output Port ของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer) คือ สัญญาณที่ไม่สมบูรณ์ของ E_{in2} ที่ถอดข้อมูลเชิงแสงด้วยสัญญาณ E_{in}

ขั้นตอนที่ 5 : นำผลของสัญญาณในขั้นตอนที่ 4 – สัญญาณ E_{in2} (ถ้าการถอดข้อมูลมีมากกว่า 1 ครั้ง ให้ – สัญญาณที่ต้องการถอดข้อมูลเชิงแสง ทุก ๆ ครั้ง)

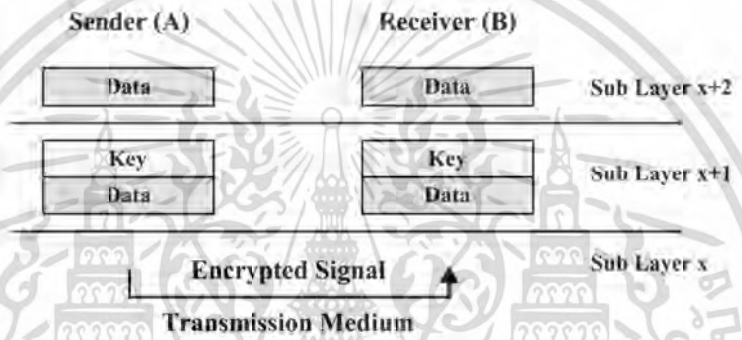
ขั้นตอนที่ 6 : ผลของสัญญาณในขั้นตอนที่ 5 คือ สัญญาณ E_{in2} ที่ถอดข้อมูลเชิงแสงด้วยสัญญาณ E_{in}

หมายเหตุ ในทางปฏิบัติการลบกันของสัญญาณแสงในขั้นตอนที่ 5 สามารถประยุกต์ใช้ไมเคิลสันอินเทอร์เฟียร์โรมิเตอร์ (Michelson Interferometer) มาทำงานในส่วนนี้ได้ โดยการประยุกต์ใช้งานไมเคิลสันอินเทอร์เฟียร์โรมิเตอร์ (Michelson Interferometer) เช่น การประยุกต์ใช้งานในการพัฒนาลอจิกเกตเชิงแสง (Optical Logic Gate) [67] การประยุกต์ใช้งานทางด้านอุปกรณ์ตรวจจับ [68] รวมถึงมีการประยุกต์ใช้งานด้านอื่น ๆ [69-71] ซึ่งการลบกันของสัญญาณแสงที่ใช้ไมเคิลสันอิน

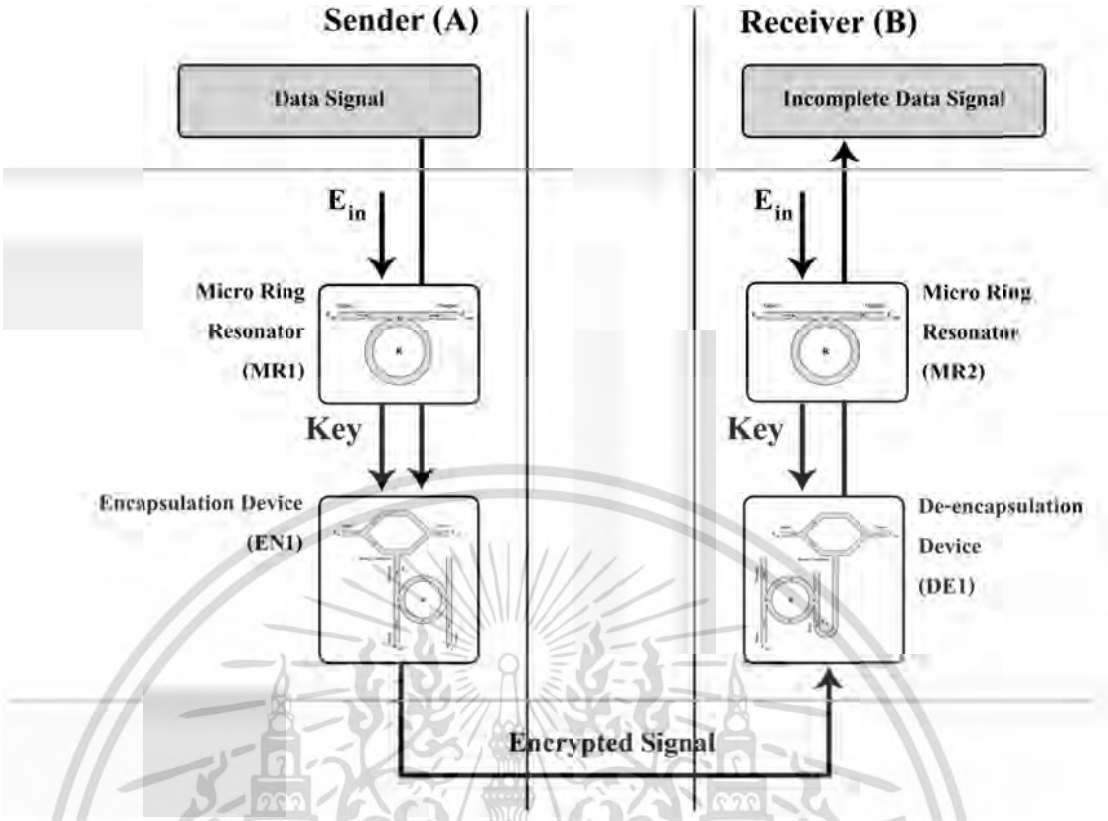
เทอร์เฟียร์โรมิเตอร์ (Michelson Interferometer) เกิดขึ้นได้เนื่องจากใช้หลักการแทรกสอดแบบหักล้าง

4.2.3 การจำลอง

ในหัวข้อนี้เป็นการจำลองวิธีการห่อหุ้มเชิงแสง (Optical Encapsulation) และวิธีการถอดข้อมูลเชิงแสง (Optical De-encapsulation) โดยยกตัวอย่างการจำลองการส่งข้อมูลที่ถูกห่อหุ้มด้วยกุญแจเชิงแสง (Key) จากผู้ส่งไปยังผู้รับ โดยมีแผนภาพแสดงสถานะการณ์การจำลองตามรูปที่ 4.4 กล่าวคือ ผู้ส่งต้องการส่งข้อมูล 1 ชุด ให้กับผู้รับโดยที่ข้อมูลที่ถูกส่งถูกห่อหุ้มเชิงแสงด้วยกุญแจเชิงแสง (Optical Key) และแผนภาพแสดงอุปกรณ์เชิงแสงในการจำลองการห่อหุ้มเชิงแสงตามรูปที่ 4.5 รวมถึงมีพารามิเตอร์ที่ใช้ในการจำลองตามตารางที่ 4.1 โดยมีรายละเอียดการจำลองดังนี้



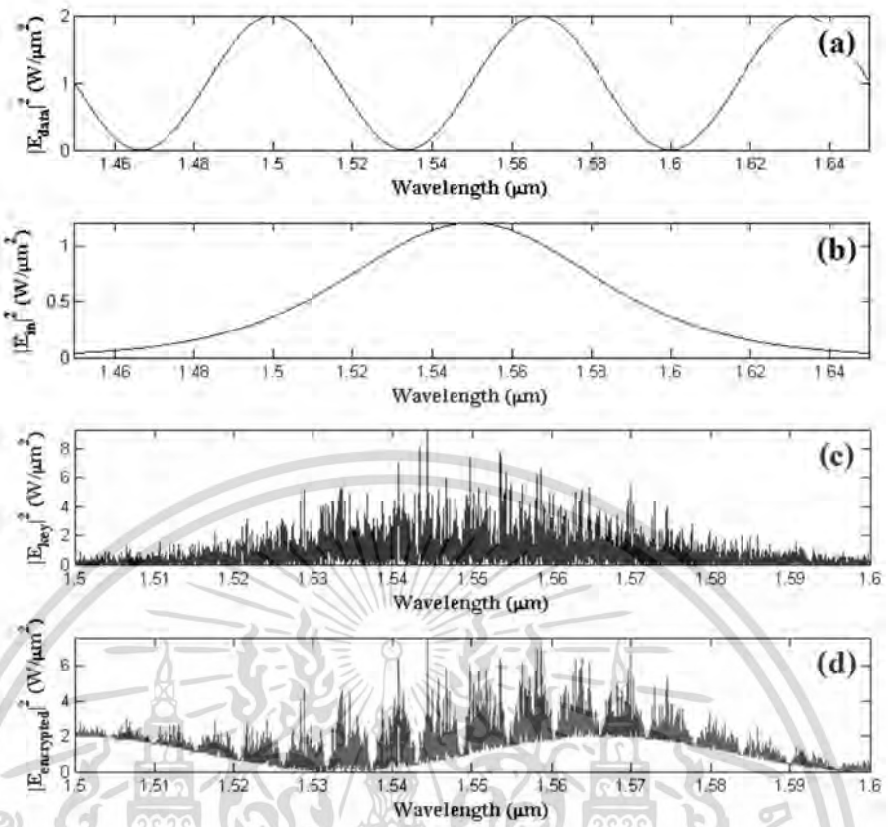
รูปที่ 4.4 แผนภาพแสดงสถานะการณ์การจำลองการห่อหุ้มเชิงแสง



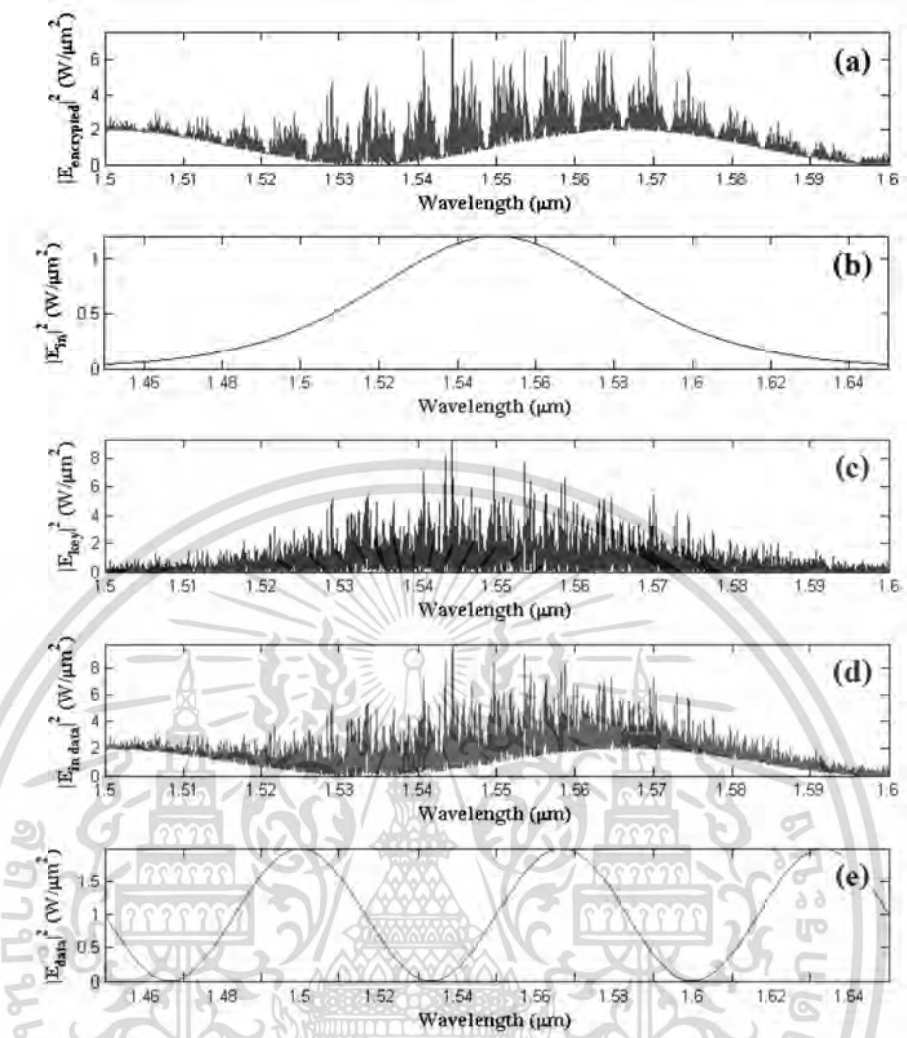
รูปที่ 4.5 แผนภาพแสดงอุปกรณ์เชิงแสงในการจำลองการห่อหุ้มเชิงแสง

ตารางที่ 4.1 พารามิเตอร์ที่ใช้ในการจำลองวิธีการห่อหุ้มเชิงแสง (Optical Encapsulation) และวิธีการถอดข้อมูลเชิงแสง (Optical De-encapsulation)

อุปกรณ์ , สัญญาณ	พารามิเตอร์	ค่าพารามิเตอร์
ทุกอุปกรณ์	ชนิดของวัสดุ	InGaAsP/InP
	ค่าดัชนีหักเหเชิงเส้นของตัวนำคลื่น : n_0	3.4
	ค่าดัชนีหักเหไม่เชิงเส้นของตัวนำคลื่น : n_2	1.3×10^{-13} m^2/W
	การสูญเสียภายในตัวนำคลื่น : α	0.05 dB mm^{-1}
	ค่าการสูญเสียความเข้มแสงเนื่องจากคัปปลิ้ง : γ	0.01
	ขนาดพื้นที่หน้าตัดของตัวนำคลื่น : A_{eff}	0.25 μm^2
Add Drop Filter (EN,DE)	ขนาดวงแหวน	20 μm
	สัมประสิทธิ์การคัปปลิ้ง κ_1	0.5
	สัมประสิทธิ์การคัปปลิ้ง κ_2	0.5
สัญญาณ	ศูนย์กลางช่วงคลื่น : λ_0	1.55 μm
	ความเข้มสัญญาณ E_{in}	1.2 W/μm^2
	ความเข้มสัญญาณ Data	2.0 W/μm^2



รูปที่ 4.6 ผลการจำลองของฝั่งผู้ส่งข้อมูล



รูปที่ 4.7 ผลการจำลองของฝั่งผู้รับข้อมูล

จากรูปที่ 4.6 ผลการจำลองของฝั่งผู้ส่งข้อมูล รูปที่ 4.6 (a) แสดงสัญญาณข้อมูลที่ Sender (A) ต้องการส่งข้อมูลไปยัง Receiver (B) รูปที่ 4.6 (b) แสดงสัญญาณ E_{in} ที่ใช้ในการส่งเข้า Input Port ของวงแหวนสั่นพ้องขนาดเล็ก (Micro Ring Resonator) (ภาคผนวก ก [2]) เพื่อสร้างกุญแจเชิงแสง (Key) ตามรูปที่ 4.6 (c) และรูปที่ 4.6 (d) แสดงสัญญาณที่เกิดจากการห่อหุ่มเชิงแสง (Optical Encapsulation) ระหว่างสัญญาณข้อมูล (รูปที่ 4.6 (a)) กับกุญแจเชิงแสง (รูปที่ 4.6 (c)) ซึ่งเป็นสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่ใช้ในการส่งข้อมูลอย่างปลอดภัยจาก Sender (A) ไปยัง Receiver (B) กล่าวคือ สัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่ส่งออกไปคือ สัญญาณข้อมูลที่ถูกห่อหุ้มเชิงแสงด้วยกุญแจเชิงแสง

จากรูปที่ 4.7 ผลการจำลองของฝั่งผู้รับข้อมูล รูปที่ 4.7 (a) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่ใช้ในการส่งข้อมูลอย่างปลอดภัยจาก Sender (A) รูปที่ 4.7 (b) แสดงสัญญาณ E_{in} ที่ใช้ในการส่งเข้า Input Port ของวงแหวนสั่นพ้องขนาดเล็ก (Micro Ring Resonator) เพื่อสร้างกุญแจเชิงแสง (Key) ตามรูปที่ 4.7 (c) และรูปที่ 4.7 (d) แสดงสัญญาณข้อมูลจาก Sender (A) ที่ไม่สมบูรณ์ที่เกิดจากการถอดข้อมูลเชิงแสง (Optical De-Encapsulation) ระหว่างสัญญาณที่

ถูกเข้ารหัส (Encrypted Signal) (รูปที่ 4.7 (a)) กับกุญแจเชิงแสง (รูปที่ 4.7 (c)) รูปที่ 4.7 (e) แสดงสัญญาณข้อมูลจาก Sender (A) ที่สมบูรณ์ ซึ่งเกิดจากสัญญาณข้อมูลจาก Sender (A) ที่ไม่สมบูรณ์ - กุญแจเชิงแสง (Key)

4.3 อธิบายการส่งข้อมูลภายในเครือข่าย

4.3.1 การส่งข้อมูลภายในเครือข่าย

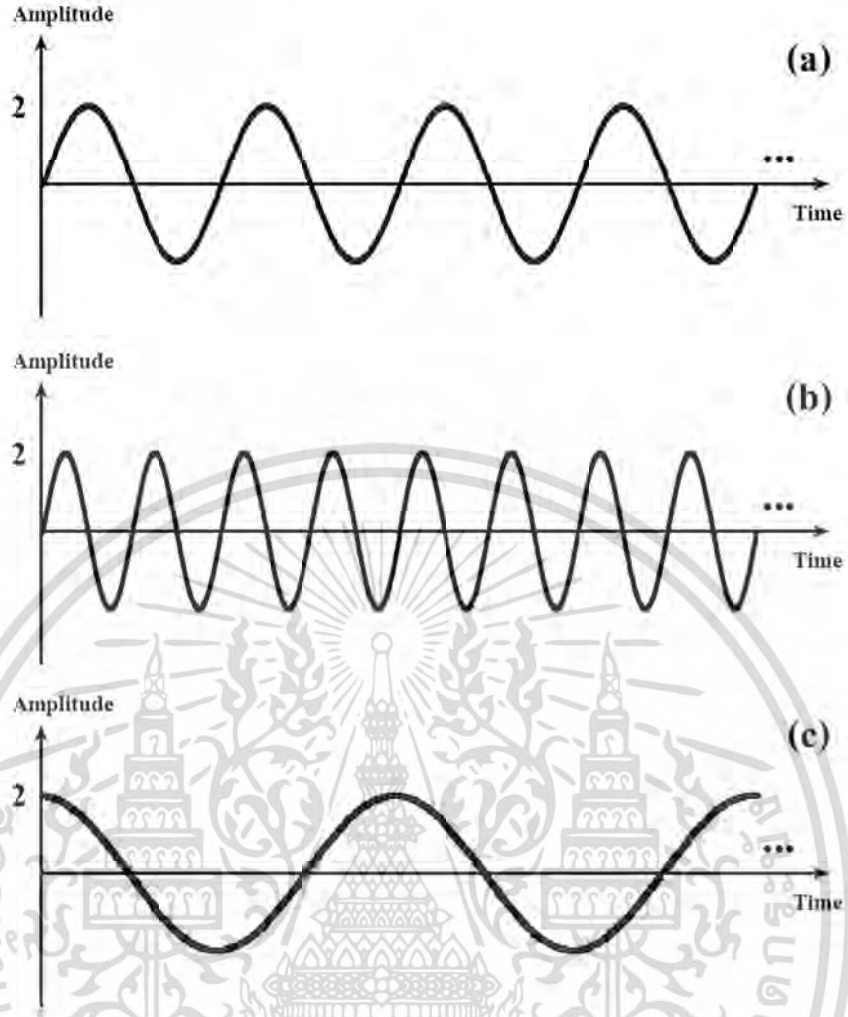
การส่งข้อมูลจริงภายในเครือข่ายเชิงแสงด้วยโปรโตคอลที่นำเสนอ เป็นการส่งข้อมูลด้วยสัญญาณอนาล็อก (Analog Signal) [72] โดยที่ข้อมูลที่ใช้ในการสื่อสารอยู่ในรูปของสัญญาณอนาล็อก (Analog Signal) หรือสัญญาณดิจิตอล (Digital Signal) ตัวอย่างของสัญญาณอนาล็อก (Analog Signal) เช่น เสียงของมนุษย์ เมื่อมีการพูดออกไปของสัญญาณอนาล็อก (Analog Signal) ก็จะถูกสร้างขึ้น โดยที่สัญญาณเสียงนี้จะถูกตรวจจับได้ด้วยไมโครโฟน ซึ่งไมโครโฟนจะทำหน้าที่ในการเปลี่ยนจากสัญญาณอนาล็อก (Analog Signal) เป็นสัญญาณดิจิตอล (Digital Signal) เพื่อที่จะใช้ในการประมวลผลหรือส่งสัญญาณไปใช้ในการทำงานอื่น ๆ ต่อไป โดยที่สัญญาณอนาล็อก (Analog Signal) สามารถอธิบายได้ด้วย Sine Wave ดังรูปที่ 4.8

รูปที่ 4.8 Sine Wave

Sine Wave อธิบายด้วยสมการคณิตศาสตร์ได้ดังนี้

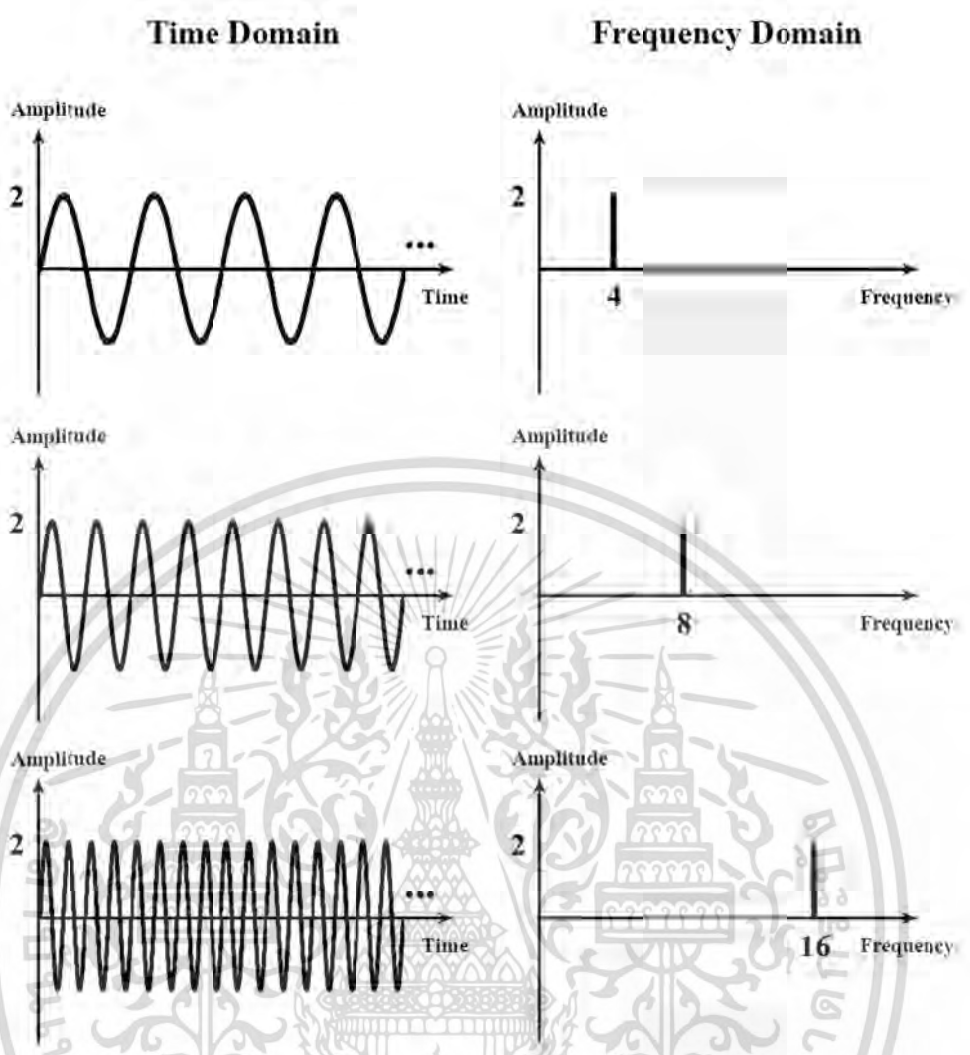
$$s(t) = A\sin(2\pi ft + \phi) \tag{4.1}$$

เมื่อ A คือแอมพลิจูดสูงสุดของสัญญาณ f คือความถี่ของสัญญาณและ ϕ คือเฟสของสัญญาณ โดยที่ตัวอย่างของ Sine Wave มีลักษณะตามรูปที่ 4.9



รูปที่ 4.9 ตัวอย่างของ Sine Wave

จากรูปที่ 4.9 แสดงตัวอย่างของ Sine Wave รูปที่ 4.9 (a) แสดง Sine Wave ตามสมการ $s(t) = 2\sin(2\pi 4t + 0)$ รูปที่ 4.9 (b) แสดง Sine Wave ตามสมการ $s(t) = 2\sin(2\pi 8t + 0)$ และรูปที่ 4.9 (c) แสดง Sine Wave ตามสมการ $s(t) = 2\sin(2\pi 2t + (\pi/4))$ ซึ่งอธิบายคุณสมบัติด้านแอมพลิจูดของสัญญาณ ความถี่ของสัญญาณและเฟสของสัญญาณ โดยเรียกว่า Time Domain Plot ซึ่งจะแสดงให้เห็นถึงการเปลี่ยนแปลงของแอมพลิจูในเวลาต่าง ๆ ถ้าจะแสดงความสัมพันธ์ระหว่างแอมพลิจูดสูงสุดของสัญญาณและความถี่ของสัญญาณ ต้องอธิบายโดยใช้วิธีการที่เรียกว่า Frequency Domain Plot โดยที่อธิบายเปรียบเทียบระหว่าง Time Domain Plot และ Frequency Domain Plot ดังรูปที่ 4.10



รูปที่ 4.10 เปรียบเทียบระหว่าง Time Domain Plot และ Frequency Domain Plot

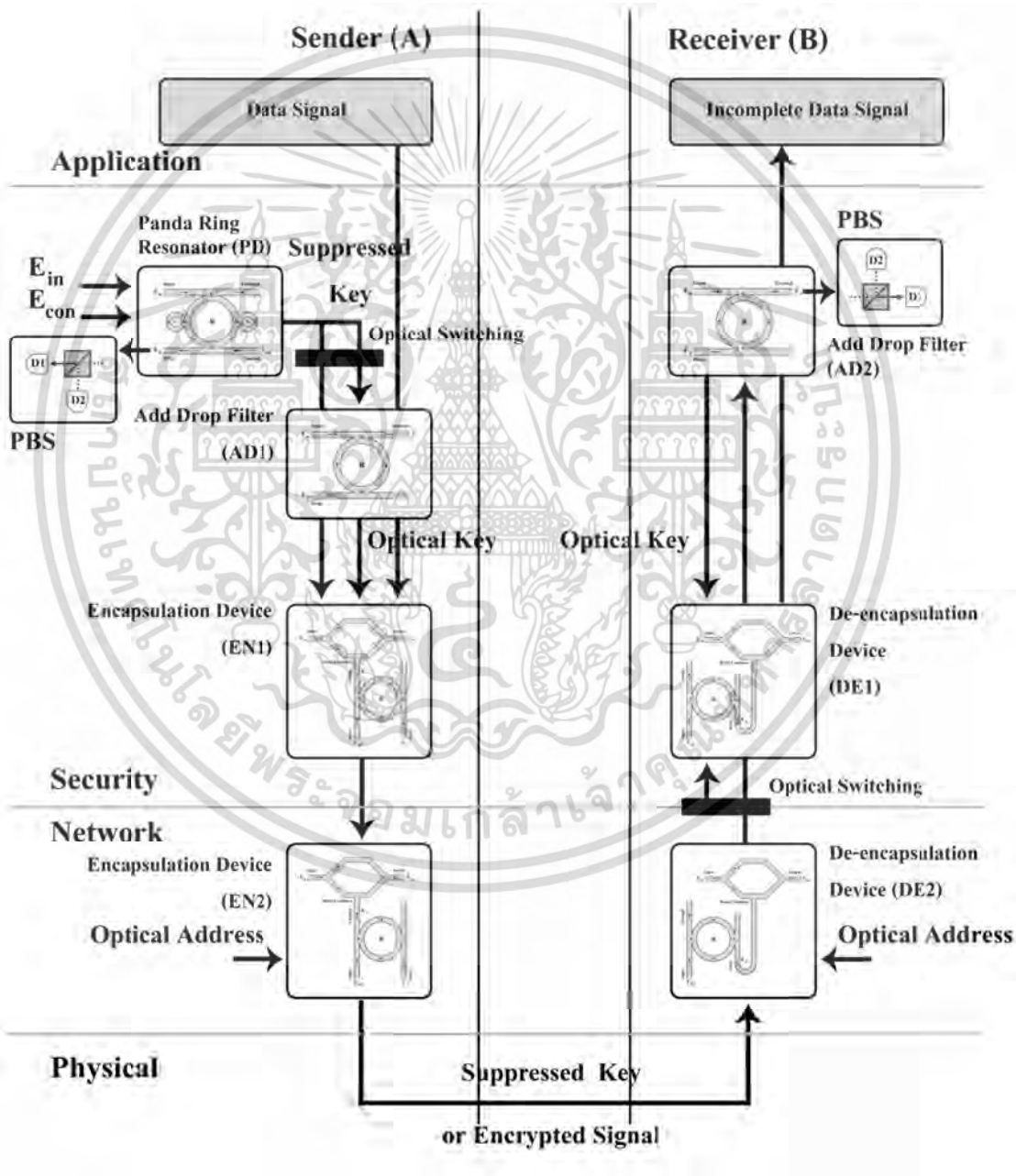
จากรูปที่ 4.10 จะเห็นว่าสามารถอธิบายคุณสมบัติด้านแอมพลิจูดของสัญญาณและความถี่ของสัญญาณใน Frequency Domain Plot ด้วยแท่งตรงเพียง 1 แท่ง ซึ่งกระชับกว่าการแสดงด้วย Time Domain Plot ของสัญญาณ ดังนั้นสัญญาณ Frequency Domain Plots จึงเหมาะสำหรับใช้อธิบายสัญญาณอนาล็อก (Analog Signal)

สัญญาณประเภท Sine Wave หนึ่งสัญญาณ เป็นการเปลี่ยนแปลงระดับพลังงานในรูปแบบซ้ำกัน ซึ่งไม่สามารถบรรจุปริมาณข้อมูลได้เพียงพอต่อการสื่อสารได้ ดังนั้นหากต้องการใช้ Sine Wave ในการสื่อสาร จำเป็นต้องมีการปรับแต่งคุณลักษณะของสัญญาณ ได้แก่ แอมพลิจูดของสัญญาณ เฟสของสัญญาณและความถี่ของสัญญาณ อย่างใดอย่างหนึ่งหรือหลายอย่างประกอบกัน การสื่อสารข้อมูลที่ประกอบด้วยการปรับแต่งคุณลักษณะ (Characteristics) ของสัญญาณตามข้อมูลที่ต้องการส่งไปยังผู้รับอื่น ๆ ภายในเครือข่าย ก่อให้เกิดสัญญาณชนิดใหม่เรียกว่า สัญญาณผสม (Composite Signal) ซึ่งประกอบด้วย Sine Wave หลายสัญญาณ การเปลี่ยนแปลงคุณลักษณะสัมพันธ์กับความถี่ของสัญญาณ ดังนั้นจำนวนความถี่ของสัญญาณผสม (Composite Signal) จึงแปรผันโดยตรงกับความหลากหลายของกลุ่มคุณลักษณะเหล่านั้น ดังนั้น การส่งข้อมูลจริงภายในเครือข่าย

เชิงแสงด้วยโปรโตคอลที่นำเสนอ ทำได้โดยการส่งข้อมูลด้วยสัญญาณอนาล็อก (Analog Signal) ดังกล่าวข้างต้น

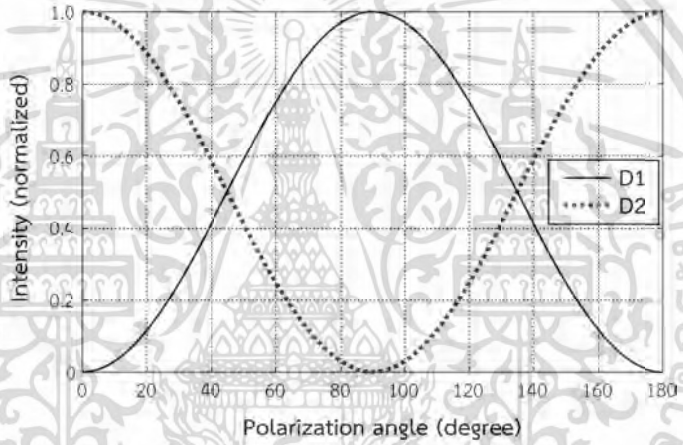
แต่ในการทดสอบการจำลองเครือข่ายในวิทยานิพนธ์นี้ สัญญาณข้อมูลที่ส่งจากผู้ส่งข้อมูลภายในเครือข่ายสื่อสารจะมีข้อมูลลักษณะตามรูปที่ 3.8 เนื่องจากให้ง่ายต่อการศึกษา กล่าวคือ ให้ง่ายต่อการตรวจสอบผลสำเร็จของการส่งข้อมูล อีกทั้งยังให้ง่ายต่อการศึกษาผลกระทบต่อสัญญาณเมื่อผ่านระดับชั้นย่อยต่าง ๆ

4.3.2 วิธีการส่งข้อมูลภายในเครือข่าย



รูปที่ 4.11 อุปกรณ์ที่เกี่ยวข้องของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง

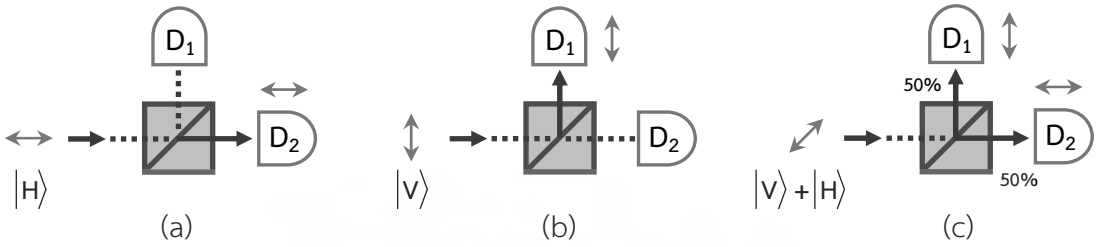
ในส่วนนี้เป็นการอธิบายถึงการส่งกุญแจเชิงแสง (Optical Key) และการส่งข้อมูล (Data) จากผู้ส่งข้อมูลไปยังผู้รับข้อมูล จากรูปที่ 4.11 อุปกรณ์ที่เกี่ยวข้องของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง จะเห็นว่าที่ฝั่งผู้ส่งข้อมูลมีการใช้งาน Polarizing Beam Splitter (PBS) และที่ฝั่งผู้รับข้อมูลมีการใช้งาน Polarizing Beam Splitter (PBS) เช่นกัน โดยที่ฝั่งผู้ส่งข้อมูลมีการนำสัญญาณแสงที่ออกจาก Drop Port ของวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) (PD) ผ่าน Polarizing Beam Splitter (PBS) เพื่อแยกสัญญาณแสงให้เดินทางไปในทิศทางที่ตัวตรวจจับสัญญาณจะสามารถรับสัญญาณได้เรียก Drop Port ของวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) ของฝั่งผู้ส่งข้อมูลว่า Reference Port ในทำนองเดียวกัน ที่ฝั่งผู้รับข้อมูลมีการนำสัญญาณแสงที่ออกจาก Through Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (AD2) เพื่อแยกสัญญาณแสงให้เดินทางไปในทิศทางที่ตัวตรวจจับสัญญาณจะสามารถรับสัญญาณได้เรียก Through Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ของฝั่งผู้รับข้อมูลว่า Reference Port



รูปที่ 4.12 ค่าความเข้มแสงเทียบกับมุมโพลาไรซ์ของโฟตอนแสงขาออกที่ตรวจจับได้โดยตัวตรวจจับ

รูปที่ 4.12 แสดงค่าความเข้มของสัญญาณแสงเมื่อถูกส่งผ่าน Polarizing Beam Splitter (PBS) โดยขนาดความเข้มแสงที่ตรวจวัดได้นี้จะขึ้นอยู่กับมุมโพลาไรซ์ของสัญญาณแสงที่ป้อนเข้าสู่ Polarizing Beam Splitter (PBS) กล่าวคือ หากสัญญาณแสงมีมุมโพลาไรซ์เป็น 0° (หรือ 180°) สัญญาณแสงจะถูกส่งออกจาก Polarizing Beam Splitter (PBS) เฉพาะในทิศทางตัวตรวจจับ (Detector) D2 เท่านั้นที่จะตรวจจับสัญญาณได้ ในขณะที่ตัวตรวจจับ (Detector) D1 จะตรวจไม่พบสัญญาณขาออกเนื่องจากไม่มีสัญญาณแสงที่มีมุมโพลาไรซ์ในทิศทางตัวตรวจจับ D1 ถูกส่งออกมาจาก Polarizing Beam Splitter (PBS) ดังแสดงในรูปที่ 4.13 (a) ในทางตรงกันข้าม หากสัญญาณแสงที่ป้อนเข้าสู้ PBS มีมุมโพลาไรซ์เป็น 90° สัญญาณแสงจะถูกส่งออกจาก Polarizing Beam Splitter (PBS) เฉพาะในทิศทางตัวตรวจจับ D1 เท่านั้นที่จะตรวจจับสัญญาณได้ ในขณะที่ตัวตรวจจับ D2 จะตรวจไม่พบสัญญาณขาออกเนื่องจากไม่มีสัญญาณแสงที่มีมุมโพลาไรซ์ในทิศทางตัวตรวจจับ D2 ถูกส่งออกมาจาก Polarizing Beam Splitter (PBS) ดังแสดงในรูปที่ 4.13 (b) และหากสัญญาณแสงที่ป้อนเข้าสู้ Polarizing Beam Splitter (PBS) มีมุมโพลาไรซ์เป็น $0° < \Phi < 90°$ หรือ $90° < \Phi < 180°$

สัญญาณแสงจะถูกส่งออกจาก Polarizing Beam Splitter (PBS) ในทั้งสองทิศทางโดยขนาดความเข้มแสงที่ตัวตรวจจับ D1 และ D2 ตรวจจับได้จะเปลี่ยนแปลงไปในลักษณะเชิงผกผันซึ่งกันและกัน และจะมีขนาดความเข้มแสงเท่ากันที่มุมโพลาไรซ์ 45° และ 135° ดังแสดงในรูปที่ 4.13 (c)



รูปที่ 4.13 การทำงานของ Polarizing Beam Splitter และการตรวจจับสัญญาณของตัวตรวจจับ

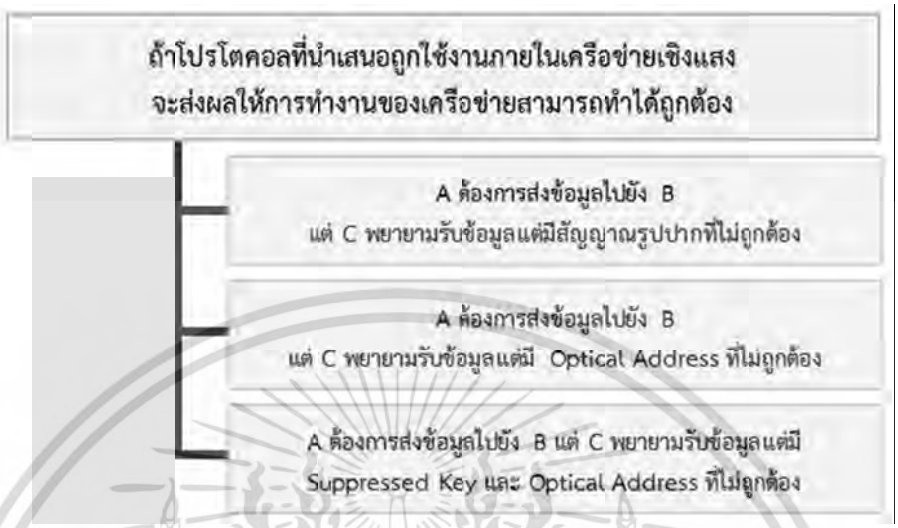
โดยที่ความเข้มของสัญญาณแสงที่ออกจาก Reference Port ที่ตัวตรวจจับ (Detector) D1 และ D2 ตรวจจับได้ทั้งฝั่งผู้ส่งข้อมูลและฝั่งผู้รับข้อมูล ในโปรโตคอลที่นำเสนอนี้ถูกใช้ในการอ้างอิงเพื่อกำหนดว่า ขณะนี้ผู้ส่งข้อมูลต้องการที่จะส่งกุญแจเชิงแสง (Optical Key) หรือต้องการที่จะส่งข้อมูล (Data) ไปในเครือข่ายให้กับผู้รับข้อมูล ซึ่งการใช้งาน Polarizing Beam Splitter (PBS) เพื่อเป็น Reference Port ของระบบการส่งข้อมูลมีตัวอย่างการใช้งาน เช่น [73-75]

4.3.3 วิธีการส่งกุญแจเชิงแสงภายในเครือข่าย

ความแตกต่างของการส่งสัญญาณรูปปาก (LIP Signal) กับข้อมูล (Data) ภายในเครือข่ายคือ การส่งสัญญาณรูปปาก (LIP Signal) คือการส่งสัญญาณที่ไม่มีสัญญาณข้อมูล (Data Signal) และสัญญาณที่อยู่เชิงแสง (Optical Key) โดยที่ผู้ส่งข้อมูลและผู้รับข้อมูลทราบจาก Reference Port ว่าขณะนี้เป็นการส่งสัญญาณรูปปาก (LIP Signal) อุปกรณ์ Optical Switching ก็จะส่งสัญญาณเพื่อไปกู้คืนกุญแจเชิงแสง (Optical Key) และเก็บไว้ใช้งาน [76,77] ในการเข้ารหัสและถอดรหัสข้อมูลต่อไป แต่ถ้าผู้ส่งข้อมูลและผู้รับข้อมูลทราบจาก Reference Port ว่าขณะนี้เป็นการส่งข้อมูล อุปกรณ์ Optical Switching ก็จะส่งสัญญาณเพื่อทำงานตามระดับชั้นย่อยของโปรโตคอลต่อไป

4.4 การทดสอบจำลองการส่งข้อมูลในเครือข่าย

4.4.1 สมมุติฐาน



รูปที่ 4.14 สถานการณ์ของการทดสอบสมมติฐานที่ 4.1

จากรูป 4.14 สถานการณ์ของการทดสอบสมมติฐานที่ 4.1 เพื่อเป็นการทดสอบการทำงานเป็นเครือข่ายของโปรโตคอลที่นำเสนอ กำหนดสมมติฐานที่ 4.1 ได้ดังนี้ ถ้าโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดถูกใช้งานภายในเครือข่ายเชิงแสงจะส่งผลต่อการทำงานของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมดสามารถทำได้ถูกต้อง

สมมติฐานย่อยที่ 4.1.1 ถ้าโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดถูกใช้งานภายในเครือข่ายเชิงแสงจะส่งผลต่อวิธีการระบุที่อยู่ (Addressing) ของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมดสามารถทำได้ถูกต้อง

สมมติฐานย่อยที่ 4.1.2 ถ้าโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดถูกใช้งานภายในเครือข่ายเชิงแสงจะส่งผลต่อวิธีการเข้ารหัสข้อมูลเชิงแสง (Optical Cryptography) ของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมดสามารถทำได้ถูกต้อง

สมมติฐานย่อยที่ 4.1.3 ถ้าโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดถูกใช้งานภายในเครือข่ายเชิงแสงจะส่งผลต่อการส่งข้อมูลอย่างปลอดภัยและรวดเร็ว (High Speed and High Security Communication) ของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมดสามารถทำได้ถูกต้อง

4.4.2 วิธีการทดสอบสมมติฐาน

การทดสอบสมมติฐานมีข้อจำกัดของแบบจำลองที่ใช้ในการทดสอบสมมติฐานตามหัวข้อ 3.3.1 ข้อจำกัดของแบบจำลองที่ใช้จำลอง มีรูปแบบเครือข่ายสื่อสารที่ใช้ในการทดสอบสมมติฐานตามหัวข้อ 3.3.2 รูปแบบเครือข่ายแบบจำลอง อีกทั้งมีเหตุผลการกำหนดลักษณะของสัญญาณข้อมูลที่ใช้ในการทดสอบสมมติฐานตามหัวข้อ 3.3.3 ลักษณะของสัญญาณข้อมูลที่ใช้ในการจำลอง และมี

วิธีการทดสอบสมมติฐานตามหัวข้อ 3.3.5 วิธีการจำลองเครือข่ายเพื่อทดสอบการทำงานของโปรโตคอล

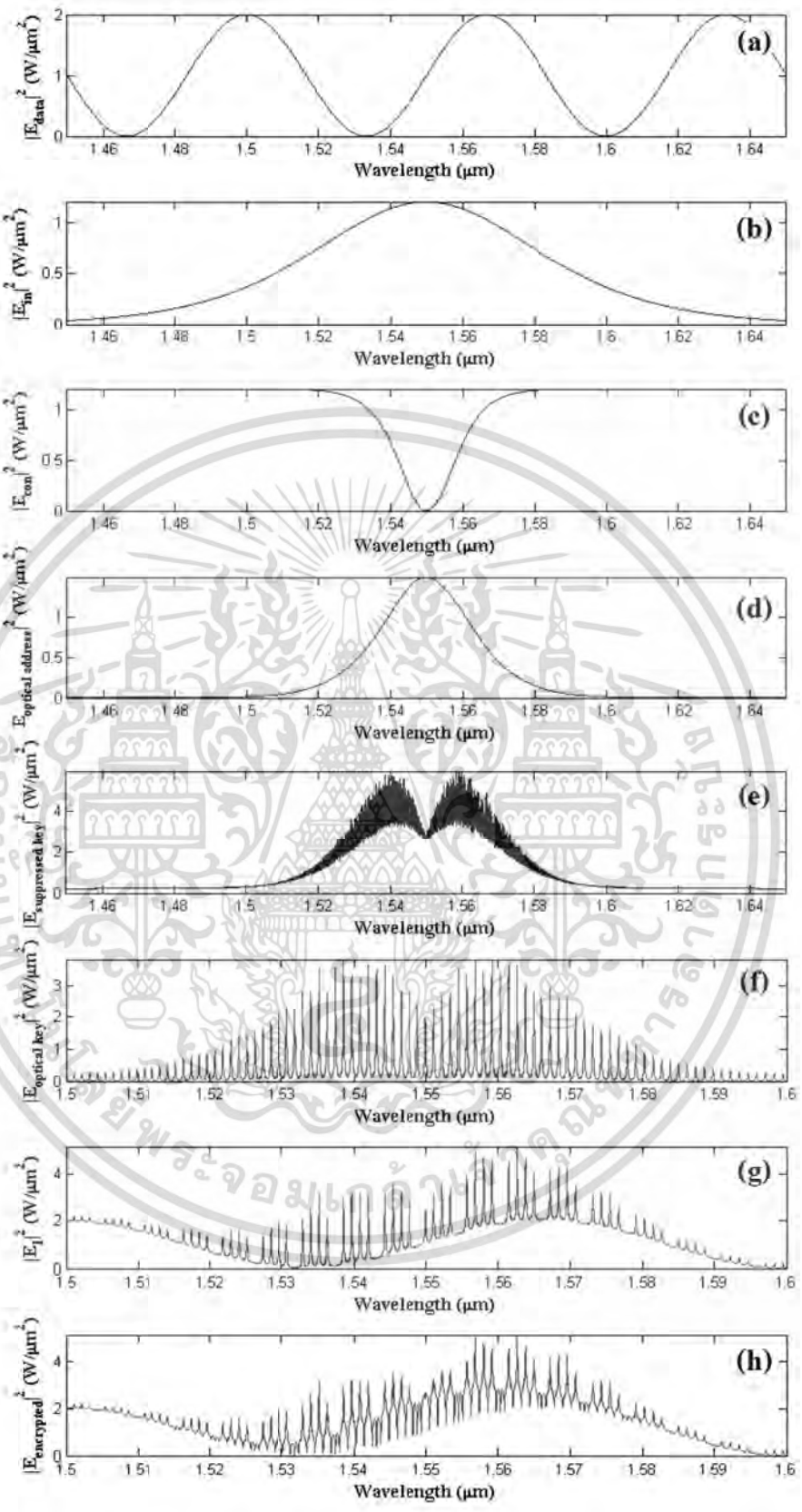
4.4.3 พารามิเตอร์ที่ใช้ในการจำลองเครือข่ายเพื่อทดสอบสมมติฐาน

การทดสอบสมมติฐานที่ 4.1.1 ถ้าโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดถูกใช้งานภายในเครือข่ายเชิงแสงจะส่งผลต่อวิธีการเข้ารหัสข้อมูลเชิงแสง (Optical Cryptography) ของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมดสามารถทำได้ถูกต้อง โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B มี C เป็นผู้รับข้อมูลที่ไม่ถูกต้อง (ผู้ไม่หวังดีในเครือข่าย) และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 4.1.1 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการกำหนดพารามิเตอร์ฝั่งผู้รับข้อมูลที่ไม่ถูกต้อง คือ มีการเปลี่ยนแปลงสัญญาณ Input ที่ PD (Input) : E_{in} และสัญญาณ Input ที่ PD (Control) : E_{con} เพื่อเป็นการอธิบายว่า ถ้าผู้รับข้อมูลไม่มี Suppressed Key ที่ถูกต้องจะไม่สามารถรับข้อมูลที่ถูกต้องได้

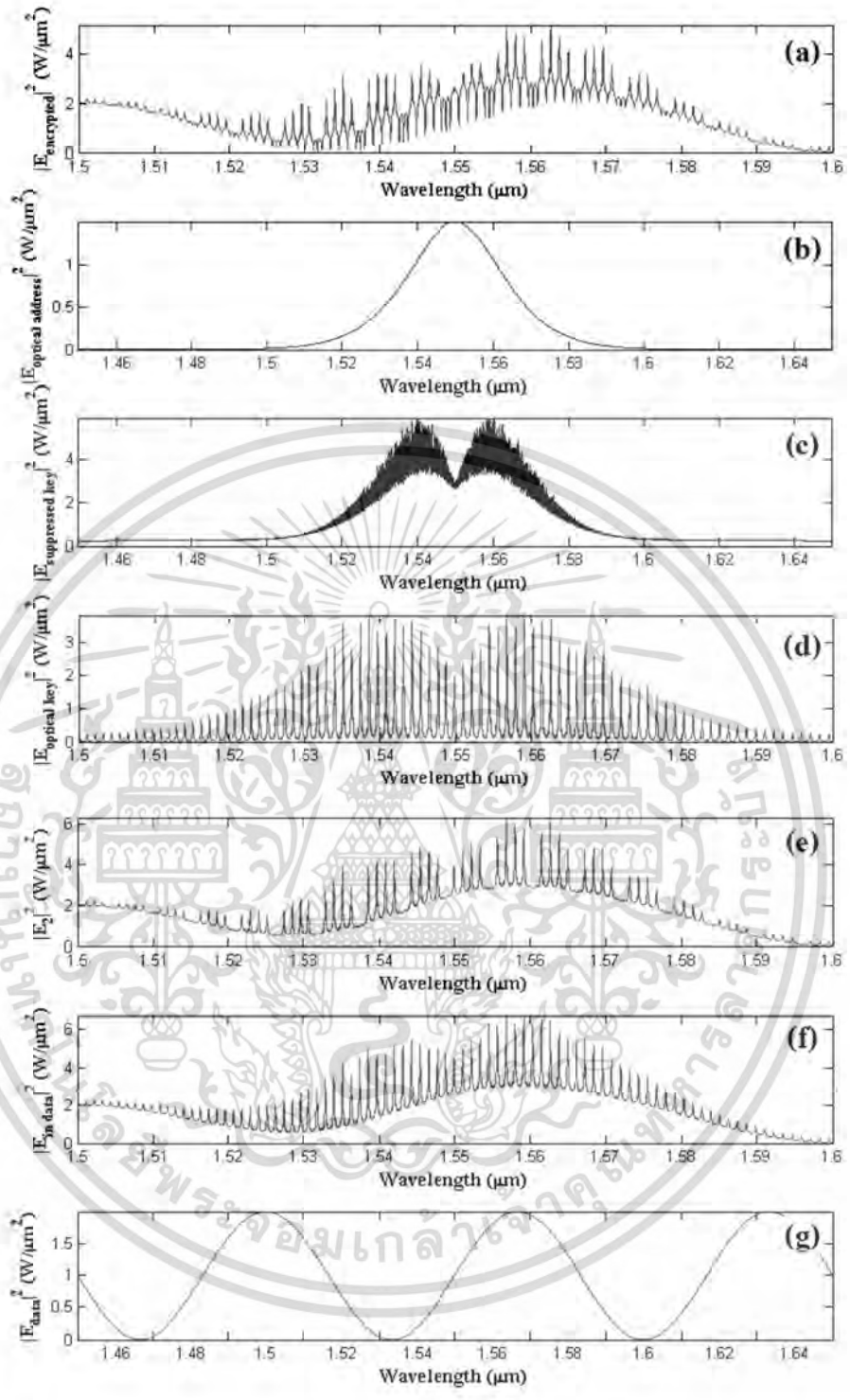
การทดสอบสมมติฐานที่ 4.1.2 ถ้าโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดถูกใช้งานภายในเครือข่ายเชิงแสงจะส่งผลต่อวิธีการระบุที่อยู่ (Addressing) ของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมดสามารถทำได้ถูกต้อง โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B มี C เป็นผู้รับข้อมูลที่ไม่ถูกต้อง (ผู้ไม่หวังดีในเครือข่าย) และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 4.1.2 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการกำหนดพารามิเตอร์ฝั่งผู้รับข้อมูลที่ไม่ถูกต้อง คือ มีการเปลี่ยนแปลงสัญญาณ Optical Address เพื่อเป็นการอธิบายว่า ถ้าผู้รับข้อมูลไม่มี Optical Address ที่ถูกต้องตามที่ผู้ส่งข้อมูลต้องการส่ง จะไม่สามารถรับข้อมูลที่ถูกต้องได้

การทดสอบสมมติฐานที่ 4.1.3 ถ้าโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดถูกใช้งานภายในเครือข่ายเชิงแสงจะส่งผลต่อการส่งข้อมูลอย่างปลอดภัยและรวดเร็ว (High Speed and High Security Communication) ของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมดสามารถทำได้ถูกต้อง โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B มี C เป็นผู้รับข้อมูลที่ไม่ถูกต้อง (ผู้ไม่หวังดีในเครือข่าย) และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 4.1.3 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการกำหนดพารามิเตอร์ฝั่งผู้รับข้อมูลที่ไม่ถูกต้อง คือ มีการเปลี่ยนแปลงสัญญาณ Input ที่ PD (Input) : E_{in} และสัญญาณ Input ที่ PD (Control) : E_{con} เพื่อเป็นการอธิบายว่า ถ้าผู้รับข้อมูลไม่มี Suppressed Key ที่ถูกต้องจะไม่สามารถรับข้อมูลที่ถูกต้องได้ และรวมถึงมีการเปลี่ยนแปลงสัญญาณ Optical Address เพื่อเป็นการอธิบายว่า ถ้าผู้รับข้อมูลไม่มี Optical Address ที่ถูกต้องตามที่ผู้ส่งข้อมูลต้องการส่ง จะไม่สามารถรับข้อมูลที่ถูกต้องได้

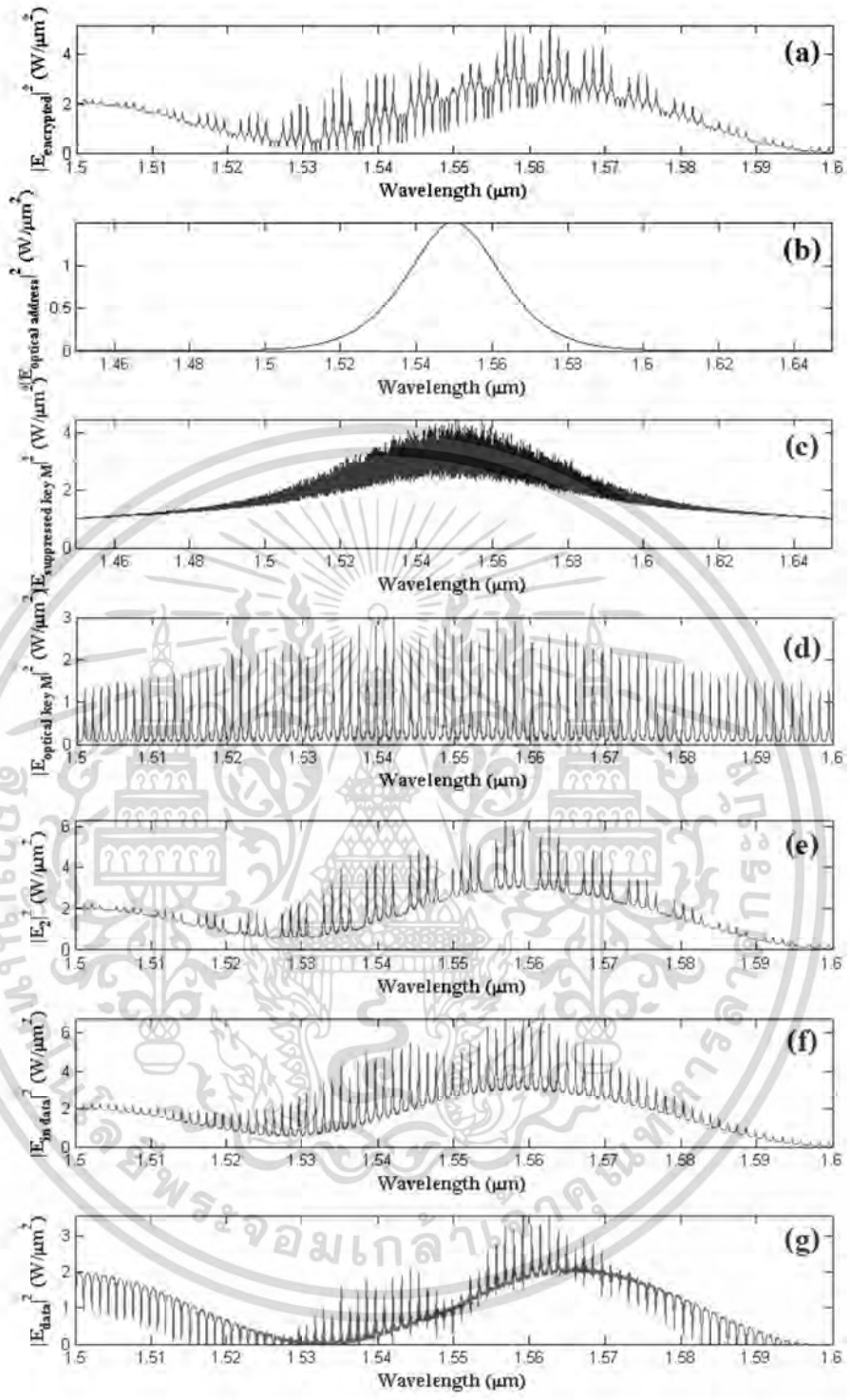
4.4.4 ผลการจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 4.1.1



รูปที่ 4.15 ผลการจำลองของฝั่งผู้ส่งข้อมูลของการทดสอบสมมติฐานที่ 4.1.1



รูปที่ 4.16 ผลการจำลองของฝั่งผู้รับข้อมูลที่ถูกต้องของการทดสอบสมมติฐานที่ 4.1.1



รูปที่ 4.17 ผลการจำลองของฝั่งผู้รับข้อมูลที่ไม่ถูกต้องของการทดสอบสมมติฐานที่ 4.1.1

จากรูปที่ 4.15 ผลการจำลองของฝั่งผู้ส่งข้อมูลของการทดสอบสมมติฐานที่ 4.1.1 รูปที่ 4.15 (a) แสดงสัญญาณข้อมูลที่ Sender (A) ต้องการส่งข้อมูลไปยัง Receiver (B) ซึ่งเป็นผู้รับข้อมูลที่ถูกต้องในเครือข่ายสื่อสาร รูปที่ 4.15 (b) และรูปที่ 4.15 (c) แสดงสัญญาณ E_{in} และ E_{con} ตามลำดับ ซึ่งเป็นสัญญาณที่ส่งเข้าทาง Input Port และ Control Port ของวงแหวนสั่นพ้องรูป

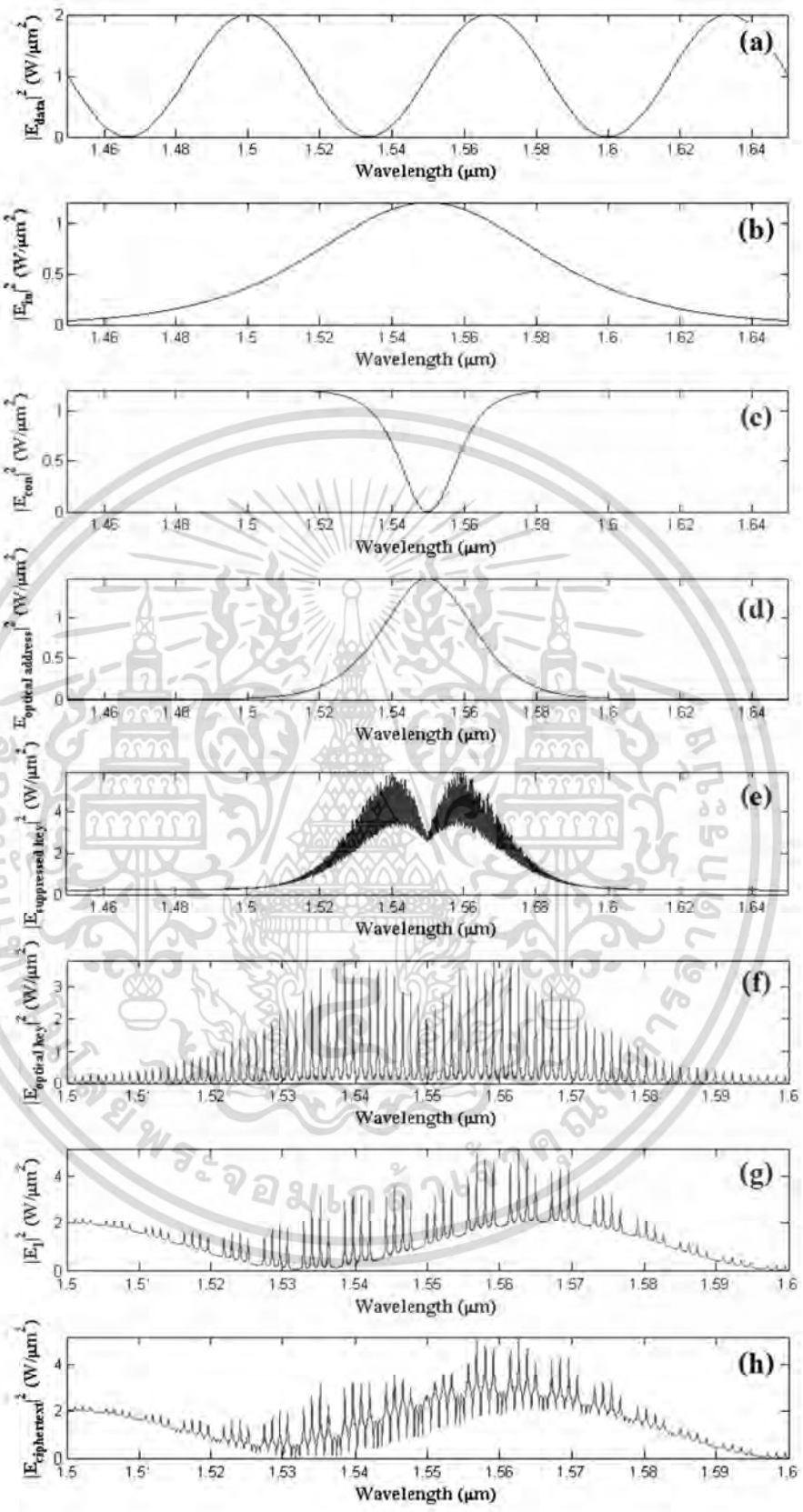
แพนด้า (Panda Ring Resonator) เพื่อใช้ในการสร้างสัญญาณรูปปาก (LIP Signal) ทาง Through Port ตามรูปที่ 4.15 (e) รูปที่ 4.15 (f) แสดงสัญญาณกุญแจเชิงแสง (Optical Key) ที่เกิดจากการนำสัญญาณรูปปาก (LIP Signal) เข้าทาง Input Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) และที่ Drop Port คือ สัญญาณกุญแจเชิงแสง (Optical Key) ที่นำไปใช้ในการสื่อสารอย่างปลอดภัย รูปที่ 4.15 (g) แสดงสัญญาณที่เกิดจากการห่อหุ้มเชิงแสงระหว่างสัญญาณข้อมูล (รูปที่ 4.15 (a)) กับสัญญาณกุญแจเชิงแสง (Optical Key) (รูปที่ 4.15 (f)) รูป 4.15 (d) แสดงสัญญาณที่อยู่เชิงแสง (Optical Address) ของผู้รับข้อมูล รูปที่ 4.15 (h) แสดงสัญญาณที่เกิดจากการห่อหุ้มเชิงแสงระหว่างสัญญาณรูปที่ 4.15 (g) กับสัญญาณที่อยู่เชิงแสง (Optical Address) (รูปที่ 4.15 (d)) โดยที่จะเป็นสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่ Sender (A) ใช้ในการสื่อสารข้อมูลไปยัง Receiver (B) มีลักษณะสัญญาณคล้ายกับสัญญาณรบกวน (Noiselike) ทำให้การสื่อสารข้อมูลระหว่าง Sender (A) และ Receiver (B) มีความปลอดภัยสูง ยากต่อการดักข้อมูลระหว่างทาง

จากรูปที่ 4.16 ผลการจำลองของฝั่งผู้รับข้อมูลที่ถูกต้องของการทดสอบสมมติฐานที่ 4.1.1 รูปที่ 4.16 (a) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่ใช้ในการส่งข้อมูลอย่างปลอดภัยจาก Sender (A) รูปที่ 4.16 (b) แสดงสัญญาณที่อยู่เชิงแสง (Optical Address) ซึ่งตรงกับที่อยู่เชิงแสง (Optical Address) ที่อยู่ภายในสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) รูปที่ 4.16 (c) แสดงสัญญาณรูปปาก (LIP Signal) หรือสัญญาณที่มีกุญแจเชิงแสงซ่อนอยู่ภายใน (Suppressed Key) รูปที่ 4.16 (d) แสดงสัญญาณกุญแจเชิงแสง (Optical Key) ที่กู้คืนมาจากสัญญาณรูปปาก (LIP Signal) รูปที่ 4.16 (e) แสดงสัญญาณที่เกิดจากการถอดข้อมูลเชิงแสง (Optical De-Encapsulation) ระหว่างสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) (รูปที่ 4.16 (a)) กับที่อยู่เชิงแสง (Optical Address) (รูปที่ 4.16 (b)) รูปที่ 4.16 (f) แสดงสัญญาณข้อมูลจาก Sender (A) ที่ไม่สมบูรณ์ที่เกิดจากการถอดข้อมูลเชิงแสง (Optical De-Encapsulation) ระหว่างสัญญาณรูปที่ 4.16 (e) กับกุญแจเชิงแสง (Optical Key) (รูปที่ 4.16 (d)) รูป 4.16 (g) แสดงสัญญาณข้อมูลจาก Sender (A) ที่สมบูรณ์ ซึ่งเกิดจากสัญญาณข้อมูลจาก Sender (A) ที่ไม่สมบูรณ์ – (ที่อยู่เชิงแสง (Optical Address) + กุญแจเชิงแสง (Optical Key)) ซึ่งจะเห็นว่าจากการวัดผลสำเร็จของการส่งข้อมูลในเครือข่ายสื่อสารในหัวข้อ 3.3.4 สัญญาณข้อมูลจาก Sender (A) สามารถส่งไปยัง Receiver (B) ได้สำเร็จ แสดงให้เห็นว่าผู้รับข้อมูลสามารถถอดข้อมูลที่ถูกต้องเนื่องจากมีที่อยู่เชิงแสง (Optical Address) และกุญแจเชิงแสง (Optical Key) ที่ถูกต้อง

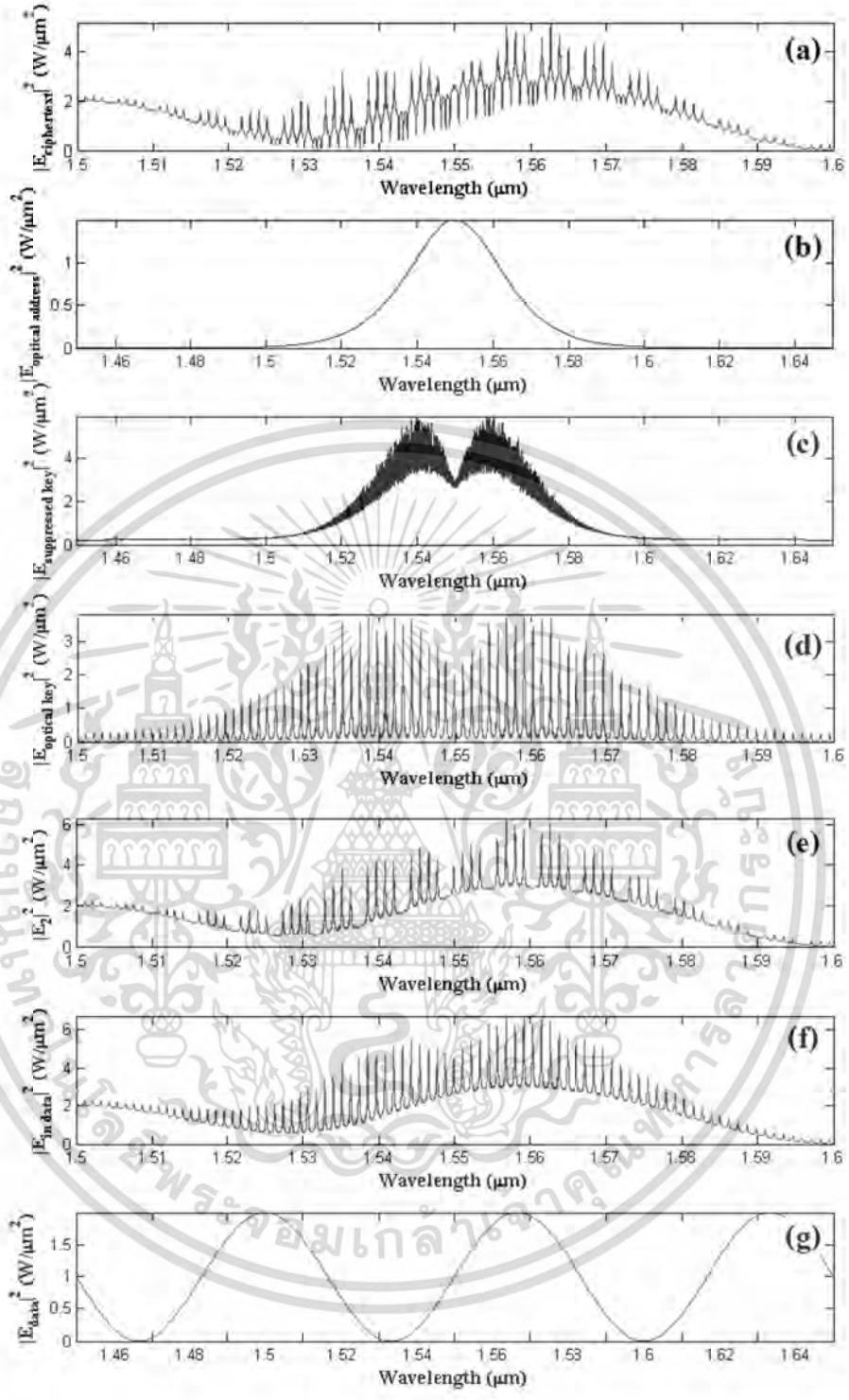
จากรูปที่ 4.17 ผลการจำลองของฝั่งผู้รับข้อมูลที่ไม่ถูกต้องของการทดสอบสมมติฐานที่ 4.1.1 แสดงให้เห็นว่า ถ้าผู้ที่รับข้อมูลในเครือข่ายไม่มีกุญแจเชิงแสงที่ถูกต้อง (รูปที่ 4.17 (d)) จะไม่สามารถทราบสัญญาณข้อมูลที่ถูกต้องจากผู้ส่งข้อมูล Sender (A) ได้ กล่าวคือ รูปที่ 4.17 (a) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่ใช้ในการส่งข้อมูลอย่างปลอดภัยจาก Sender (A) รูปที่ 4.17 (b) แสดงสัญญาณที่อยู่เชิงแสง (Optical Address) ซึ่งตรงกับที่อยู่เชิงแสง (Optical Address) ที่อยู่ภายในสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) รูปที่ 4.17 (c) แสดงสัญญาณรูปปาก (LIP Signal) หรือสัญญาณที่มีกุญแจเชิงแสงซ่อนอยู่ภายใน (Suppressed Key) ซึ่งไม่ตรงกันสัญญาณที่ผู้ส่งข้อมูลส่งให้กับทางผู้รับข้อมูลที่แท้จริง รูปที่ 4.17 (d) แสดงสัญญาณกุญแจเชิงแสง (Optical Key) ที่ไม่ถูกต้อง ที่กู้คืนมาจากสัญญาณรูปปาก (รูปที่ 4.17 (c)) รูปที่ 4.17 (e) แสดงสัญญาณที่เกิดจากการถอดข้อมูลเชิงแสง (Optical De-Encapsulation) ระหว่างสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) (รูปที่ 4.17 (a)) กับที่อยู่เชิงแสง (Optical Address) (รูปที่ 4.17 (b)) รูปที่ 4.17 (f) แสดง

สัญญาณข้อมูลจาก Sender (A) ที่ไม่สมบูรณ์ที่เกิดจากการถอดข้อมูลเชิงแสง (Optical De-Encapsulation) ระหว่างสัญญาณรูปที่ 4.17 (e) กับกุญแจเชิงแสง (Optical Key) รูป 4.17 (g) แสดงสัญญาณข้อมูลที่เกิดจากสัญญาณรูปที่ 4.17 (f) – (ที่อยู่เชิงแสง (Optical Address) + กุญแจเชิงแสง (Optical Key)) ซึ่งจะเห็นว่าจากการวัดผลสำเร็จของการส่งข้อมูลในเครือข่ายสื่อสารในหัวข้อ 3.3.4 สัญญาณข้อมูลจาก Sender (A) ไม่สามารถส่งไปยัง Receiver (B) ได้สำเร็จ แสดงให้เห็นว่าผู้รับข้อมูลไม่สามารถถอดข้อมูลที่ถูกต้องเนื่องจากมีกุญแจเชิงแสง (Optical Key) ที่ไม่ถูกต้อง

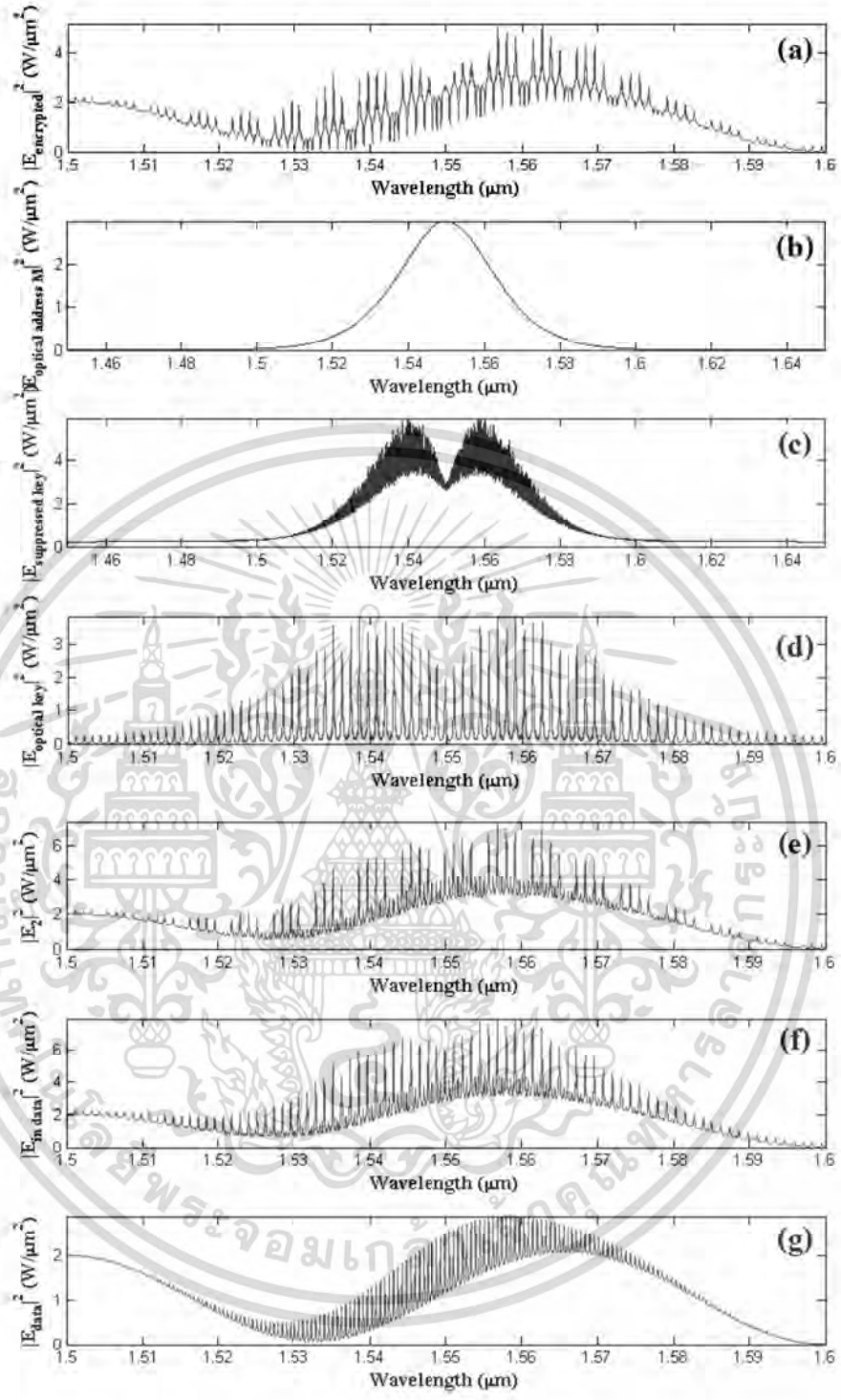
4.4.5 ผลการจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 4.1.2



รูปที่ 4.18 ผลการจำลองของฝั่งผู้ส่งข้อมูลของการทดสอบสมมติฐานที่ 4.1.2



รูปที่ 4.19 ผลการจำลองของฝั่งผู้รับข้อมูลที่ถูกต้องของการทดสอบสมมติฐานที่ 4.1.2



รูปที่ 4.20 ผลการจำลองของฝั่งผู้รับข้อมูลที่ไม่ถูกต้องของการทดสอบสมมติฐานที่ 4.1.2

จากรูปที่ 4.18 ผลการจำลองของฝั่งผู้ส่งข้อมูลของการทดสอบสมมติฐานที่ 4.1.2 รูปที่ 4.18 (a) แสดงสัญญาณข้อมูลที่ Sender (A) ต้องการส่งข้อมูลไปยัง Receiver (B) ซึ่งเป็นผู้รับข้อมูลที่ถูกต้องในเครือข่ายสื่อสาร รูปที่ 4.18 (b) และรูปที่ 4.18 (c) แสดงสัญญาณ E_{in} และ E_{con} ตามลำดับ ซึ่งเป็นสัญญาณที่ส่งเข้าทาง Input Port และ Control Port ของวงแหวนสั่นพ้องรูปแพนด้า (Panda

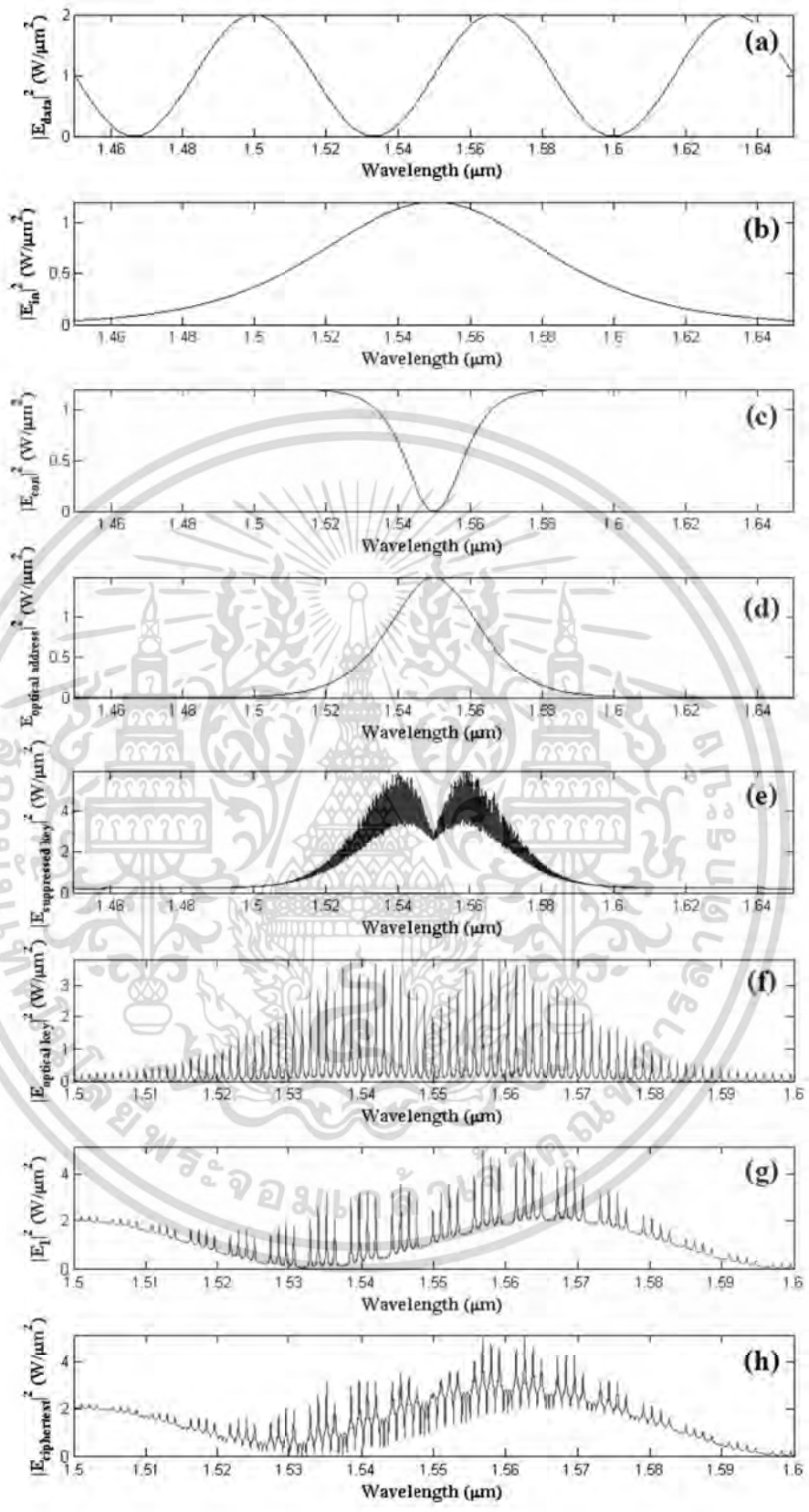
Ring Resonator) เพื่อใช้ในการสร้างสัญญาณรูปปาก (LIP Signal) ทาง Through Port ตามรูปที่ 4.18 (e) รูปที่ 4.18 (f) แสดงสัญญาณกุญแจเชิงแสง (Optical Key) ที่เกิดจากการนำสัญญาณรูปปาก (LIP Signal) เข้าทาง Input Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) และที่ Drop Port คือ สัญญาณกุญแจเชิงแสง (Optical Key) ที่นำไปใช้ในการสื่อสารอย่างปลอดภัย รูปที่ 4.18 (g) แสดงสัญญาณที่เกิดจากการห่อหุ้มเชิงแสงระหว่างสัญญาณข้อมูล (รูปที่ 4.18 (a)) กับสัญญาณกุญแจเชิงแสง (Optical Key) (รูปที่ 4.18 (f)) รูป 4.18 (d) แสดงสัญญาณที่อยู่เชิงแสง (Optical Address) ของผู้รับข้อมูล รูปที่ 4.18 (h) แสดงสัญญาณที่เกิดจากการห่อหุ้มเชิงแสงระหว่างสัญญาณรูปที่ 4.18 (g) กับสัญญาณที่อยู่เชิงแสง (Optical Address) (รูปที่ 4.18 (d)) โดยที่จะเป็นสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่ Sender (A) ใช้ในการสื่อสารข้อมูลไปยัง Receiver (B) มีลักษณะสัญญาณคล้ายกับสัญญาณรบกวน (Noiselike) ทำให้การสื่อสารข้อมูลระหว่าง Sender (A) และ Receiver (B) มีความปลอดภัยสูง ยากต่อการดักข้อมูลระหว่างทาง

จากรูปที่ 4.19 ผลการจำลองของฝั่งผู้รับข้อมูลที่ถูกต้องของการทดสอบสมมติฐานที่ 4.1.2 รูปที่ 4.19 (a) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่ใช้ในการส่งข้อมูลอย่างปลอดภัยจาก Sender (A) รูปที่ 4.19 (b) แสดงสัญญาณที่อยู่เชิงแสง (Optical Address) ซึ่งตรงกับที่อยู่เชิงแสง (Optical Address) ที่อยู่ภายในสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) รูปที่ 4.19 (c) แสดงสัญญาณรูปปาก (LIP Signal) หรือสัญญาณที่มีกุญแจเชิงแสงซ่อนอยู่ภายใน (Suppressed Key) รูปที่ 4.19 (d) แสดงสัญญาณกุญแจเชิงแสง (Optical Key) ที่กู้คืนมาจากสัญญาณรูปปาก (LIP Signal) รูปที่ 4.19 (e) แสดงสัญญาณที่เกิดจากการถอดข้อมูลเชิงแสง (Optical De-Encapsulation) ระหว่างสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) (รูปที่ 4.19 (a)) กับที่อยู่เชิงแสง (Optical Address) (รูปที่ 4.19 (b)) รูปที่ 4.19 (f) แสดงสัญญาณข้อมูลจาก Sender (A) ที่ไม่สมบูรณ์ที่เกิดจากการถอดข้อมูลเชิงแสง (Optical De-Encapsulation) ระหว่างสัญญาณรูปที่ 4.19 (e) กับกุญแจเชิงแสง (Optical Key) (รูปที่ 4.19 (d)) รูป 4.19 (g) แสดงสัญญาณข้อมูลจาก Sender (A) ที่สมบูรณ์ ซึ่งเกิดจากสัญญาณข้อมูลจาก Sender (A) ที่ไม่สมบูรณ์ – (ที่อยู่เชิงแสง (Optical Address) + กุญแจเชิงแสง (Optical Key)) ซึ่งจะเห็นว่าจากการวัดผลสำเร็จของการส่งข้อมูลในเครือข่ายสื่อสารในหัวข้อ 3.3.4 สัญญาณข้อมูลจาก Sender (A) สามารถส่งไปยัง Receiver (B) ได้สำเร็จ แสดงให้เห็นว่าผู้รับข้อมูลสามารถถอดข้อมูลที่ถูกต้องเนื่องจากมีที่อยู่เชิงแสง (Optical Address) และกุญแจเชิงแสง (Optical Key) ที่ถูกต้อง

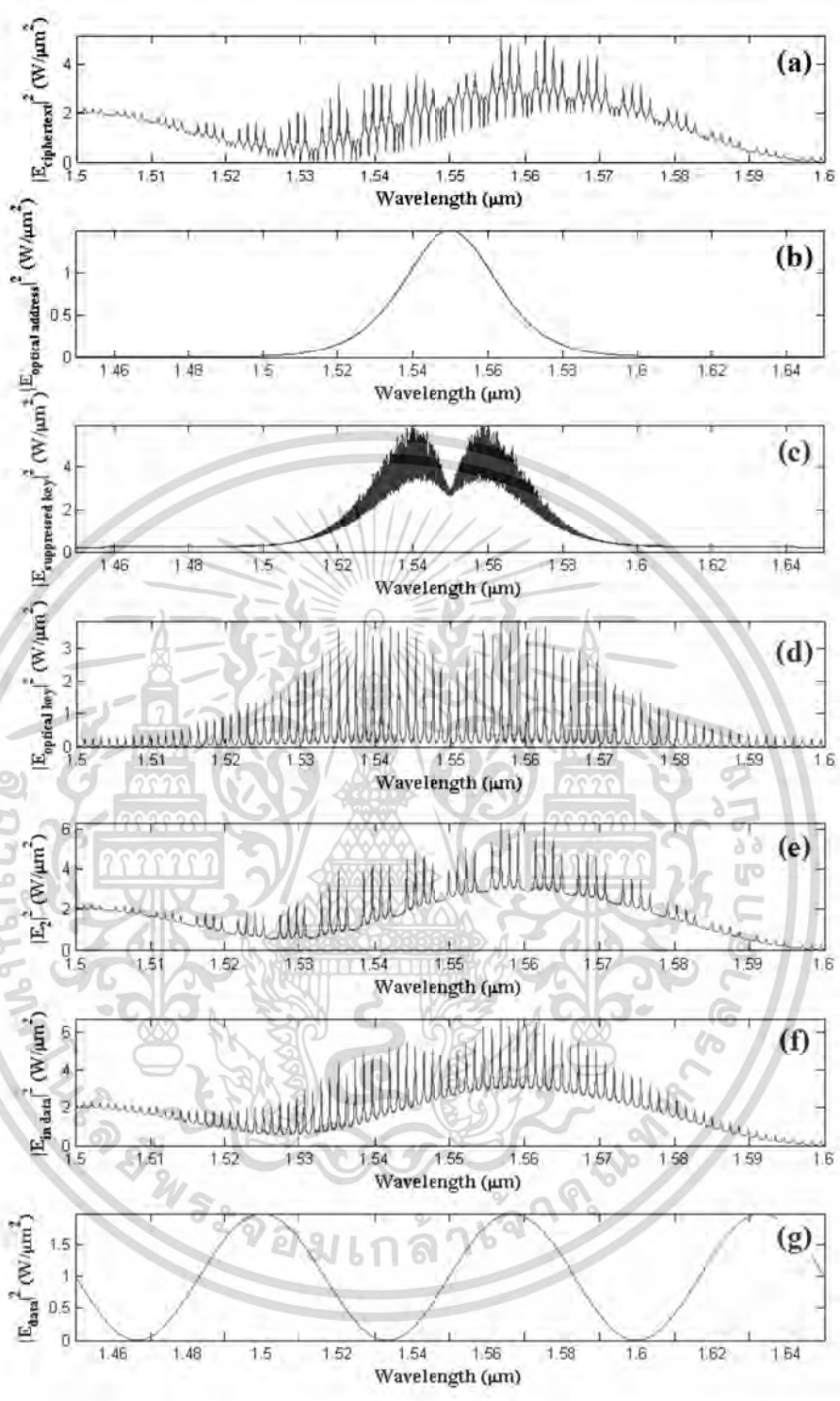
จากรูปที่ 4.20 ผลการจำลองของฝั่งผู้รับข้อมูลที่ไม่ถูกต้องของการทดสอบสมมติฐานที่ 4.1.2 แสดงให้เห็นว่า ถ้าผู้ที่รับข้อมูลในเครือข่ายไม่ถูกต้อง คือมีที่อยู่เชิงแสง (Optical Address) ไม่ตรงกับผู้รับข้อมูลที่ผู้ส่งข้อมูลต้องการส่ง (รูปที่ 4.20 (b)) จะไม่สามารถทราบสัญญาณข้อมูลที่ถูกต้องจากผู้ส่งข้อมูล Sender (A) ได้ กล่าวคือ รูปที่ 4.20 (a) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่ใช้ในการส่งข้อมูลอย่างปลอดภัยจาก Sender (A) รูปที่ 4.20 (b) แสดงสัญญาณที่อยู่เชิงแสง (Optical Address) ซึ่งไม่ตรงกับที่อยู่เชิงแสง (Optical Address) ที่อยู่ภายในสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) รูปที่ 4.20 (c) แสดงสัญญาณรูปปาก (LIP Signal) หรือสัญญาณที่มีกุญแจเชิงแสงซ่อนอยู่ภายใน (Suppressed Key) ซึ่งตรงกันสัญญาณที่ผู้ส่งข้อมูลส่งให้กับทางผู้รับข้อมูลที่แท้จริง รูปที่ 4.20 (d) แสดงสัญญาณกุญแจเชิงแสง (Optical Key) ที่ถูกต้อง ที่กู้คืนมาจากสัญญาณรูปปาก (รูปที่ 4.20 (c)) รูปที่ 4.20 (e) แสดงสัญญาณที่เกิดจากการถอดข้อมูลเชิงแสง (Optical De-Encapsulation) ระหว่างสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) (รูปที่ 4.20 (a)) กับที่อยู่เชิง

แสงที่ไม่ถูกต้อง (Optical Address) (รูปที่ 4.20 (b)) รูปที่ 4.20 (f) แสดงสัญญาณข้อมูลจาก Sender (A) ที่ไม่สมบูรณ์ที่เกิดจากการถอดข้อมูลเชิงแสง (Optical De-Encapsulation) ระหว่างสัญญาณรูปที่ 4.20 (e) กับกุญแจเชิงแสง (Optical Key) รูป 4.20 (g) แสดงสัญญาณข้อมูลที่เกิดจากสัญญาณรูปที่ 4.20 (f) – (ที่อยู่เชิงแสง (Optical Address) + กุญแจเชิงแสง (Optical Key)) ซึ่งจะเห็นว่าจากการวัดผลสำเร็จของการส่งข้อมูลในเครือข่ายสื่อสารในหัวข้อ 3.3.4 สัญญาณข้อมูลจาก Sender (A) ไม่สามารถส่งไปยัง Receiver (B) ได้สำเร็จ แสดงให้เห็นว่าผู้รับข้อมูลไม่สามารถถอดข้อมูลที่ถูกต้องเนื่องจากมีที่อยู่เชิงแสง (Optical Address) ที่ไม่ตรงกันที่อยู่เชิงแสงของผู้รับข้อมูลที่ผู้ส่งข้อมูลต้องการส่งข้อมูลในเครือข่าย

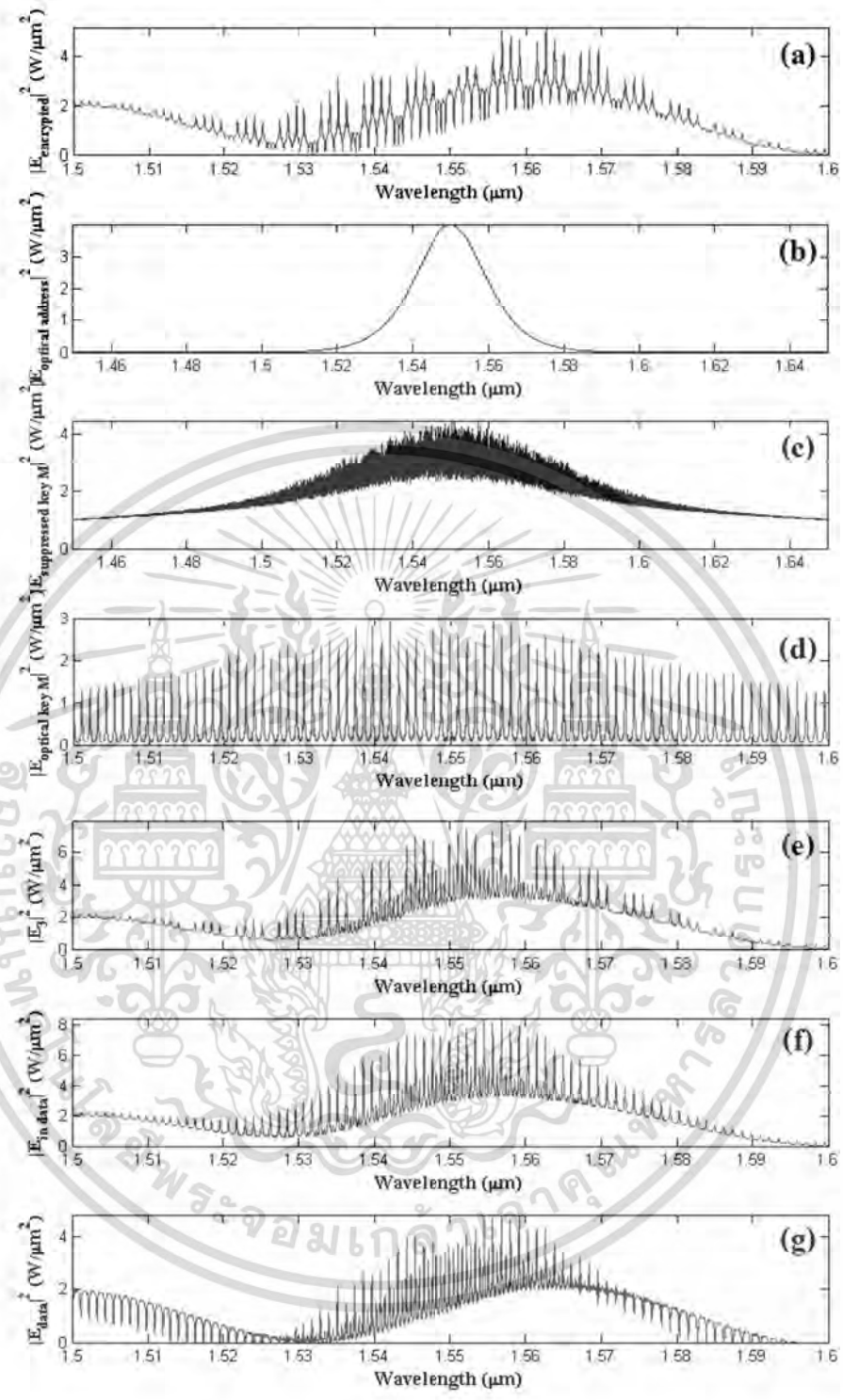
4.4.6 ผลการจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 4.1.3



รูปที่ 4.21 ผลการจำลองของฝั่งผู้ส่งข้อมูลของการทดสอบสมมติฐานที่ 4.1.3



รูปที่ 4.22 ผลการจำลองของฝั่งผู้รับข้อมูลที่ถูกต้องของการทดสอบสมมติฐานที่ 4.1.3



รูปที่ 4.23 ผลการจำลองของฝั่งผู้รับข้อมูลที่ไม่ถูกต้องของการทดสอบสมมติฐานที่ 4.1.3

จากรูปที่ 4.21 ผลการจำลองของฝั่งผู้ส่งข้อมูลของการทดสอบสมมติฐานที่ 4.1.3 รูปที่ 4.21 (a) แสดงสัญญาณข้อมูลที่ Sender (A) ต้องการส่งข้อมูลไปยัง Receiver (B) ซึ่งเป็นผู้รับข้อมูลที่ถูกต้องในเครือข่ายสื่อสาร รูปที่ 4.21 (b) และรูปที่ 4.21 (c) แสดงสัญญาณ E_{in} และ E_{con} ตามลำดับ ซึ่งเป็นสัญญาณที่ส่งเข้าทาง Input Port และ Control Port ของวงแหวนสั่นพ้องรูปแพนด้า (Panda

Ring Resonator) เพื่อใช้ในการสร้างสัญญาณรูปปาก (LIP Signal) ทาง Through Port ตามรูปที่ 4.21 (e) รูปที่ 4.21 (f) แสดงสัญญาณกุญแจเชิงแสง (Optical Key) ที่เกิดจากการนำสัญญาณรูปปาก (LIP Signal) เข้าทาง Input Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) และที่ Drop Port คือ สัญญาณกุญแจเชิงแสง (Optical Key) ที่นำไปใช้ในการสื่อสารอย่างปลอดภัย รูปที่ 4.21 (g) แสดงสัญญาณที่เกิดจากการห่อหุ้มเชิงแสงระหว่างสัญญาณข้อมูล (รูปที่ 4.21 (a)) กับสัญญาณกุญแจเชิงแสง (Optical Key) (รูปที่ 4.21 (f)) รูป 4.21 (d) แสดงสัญญาณที่อยู่เชิงแสง (Optical Address) ของผู้รับข้อมูล รูปที่ 4.21 (h) แสดงสัญญาณที่เกิดจากการห่อหุ้มเชิงแสงระหว่างสัญญาณรูปที่ 4.21 (g) กับสัญญาณที่อยู่เชิงแสง (Optical Address) (รูปที่ 4.21 (d)) โดยที่จะเป็นสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่ Sender (A) ใช้ในการสื่อสารข้อมูลไปยัง Receiver (B) มีลักษณะสัญญาณคล้ายกับสัญญาณรบกวน (Noiselike) ทำให้การสื่อสารข้อมูลระหว่าง Sender (A) และ Receiver (B) มีความปลอดภัยสูง ยากต่อการดักข้อมูลระหว่างทาง

จากรูปที่ 4.22 ผลการจำลองของฝั่งผู้รับข้อมูลที่ถูกต้องของการทดสอบสมมติฐานที่ 4.1.3 รูปที่ 4.22 (a) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่ใช้ในการส่งข้อมูลอย่างปลอดภัยจาก Sender (A) รูปที่ 4.22 (b) แสดงสัญญาณที่อยู่เชิงแสง (Optical Address) ซึ่งตรงกับที่อยู่เชิงแสง (Optical Address) ที่อยู่ภายในสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) รูปที่ 4.22 (c) แสดงสัญญาณรูปปาก (LIP Signal) หรือสัญญาณที่มีกุญแจเชิงแสงซ่อนอยู่ภายใน (Suppressed Key) รูปที่ 4.22 (d) แสดงสัญญาณกุญแจเชิงแสง (Optical Key) ที่กู้คืนมาจากสัญญาณรูปปาก (LIP Signal) รูปที่ 4.22 (e) แสดงสัญญาณที่เกิดจากการถอดข้อมูลเชิงแสง (Optical De-Encapsulation) ระหว่างสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) (รูปที่ 4.22 (a)) กับที่อยู่เชิงแสง (Optical Address) (รูปที่ 4.22 (b)) รูปที่ 4.22 (f) แสดงสัญญาณข้อมูลจาก Sender (A) ที่ไม่สมบูรณ์ที่เกิดจากการถอดข้อมูลเชิงแสง (Optical De-Encapsulation) ระหว่างสัญญาณรูปที่ 4.22 (e) กับกุญแจเชิงแสง (Optical Key) (รูปที่ 4.22 (d)) รูป 4.22 (g) แสดงสัญญาณข้อมูลจาก Sender (A) ที่สมบูรณ์ ซึ่งเกิดจากสัญญาณข้อมูลจาก Sender (A) ที่ไม่สมบูรณ์ – (ที่อยู่เชิงแสง (Optical Address) + กุญแจเชิงแสง (Optical Key)) ซึ่งจะเห็นว่าจากการวัดผลสำเร็จของการส่งข้อมูลในเครือข่ายสื่อสารในหัวข้อ 3.3.4 สัญญาณข้อมูลจาก Sender (A) สามารถส่งไปยัง Receiver (B) ได้สำเร็จ แสดงให้เห็นว่าผู้รับข้อมูลสามารถถอดข้อมูลที่ถูกต้องเนื่องจากมีที่อยู่เชิงแสง (Optical Address) และกุญแจเชิงแสง (Optical Key) ที่ถูกต้อง

จากรูปที่ 4.23 ผลการจำลองของฝั่งผู้รับข้อมูลที่ไม่ถูกต้องของการทดสอบสมมติฐานที่ 4.1.3 แสดงให้เห็นว่า ถ้าผู้ที่รับข้อมูลในเครือข่ายไม่ถูกต้อง คือมีที่อยู่เชิงแสง (Optical Address) ไม่ตรงกับผู้รับข้อมูลที่ผู้ส่งข้อมูลต้องการส่ง (รูปที่ 4.23 (b)) และผู้ที่รับข้อมูลในเครือข่ายไม่มีกุญแจเชิงแสงที่ถูกต้อง (รูปที่ 4.23 (d)) จะไม่สามารถทราบสัญญาณข้อมูลที่ถูกต้องจากผู้ส่งข้อมูล Sender (A) ได้ กล่าวคือ รูปที่ 4.23 (a) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่ใช้ในการส่งข้อมูลอย่างปลอดภัยจาก Sender (A) รูปที่ 4.23 (b) แสดงสัญญาณที่อยู่เชิงแสง (Optical Address) ซึ่งไม่ตรงกับที่อยู่เชิงแสง (Optical Address) ที่อยู่ภายในสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) รูปที่ 4.23 (c) แสดงสัญญาณรูปปาก (LIP Signal) หรือสัญญาณที่มีกุญแจเชิงแสงซ่อนอยู่ภายใน (Suppressed Key) ซึ่งไม่ตรงกันสัญญาณที่ผู้ส่งข้อมูลส่งให้กับทางผู้รับข้อมูลที่แท้จริง รูปที่ 4.23 (d) แสดงสัญญาณกุญแจเชิงแสง (Optical Key) ที่ไม่ถูกต้อง ที่กู้คืนมาจากสัญญาณรูปปาก (รูปที่ 4.23 (c)) รูปที่ 4.23 (e) แสดงสัญญาณที่เกิดจากการถอดข้อมูลเชิงแสง (Optical De-Encapsulation)

ระหว่างสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) (รูปที่ 4.23 (a)) กับที่อยู่เชิงแสงที่ไม่ถูกต้อง (Optical Address) (รูปที่ 4.23 (b)) รูปที่ 4.23 (f) แสดงสัญญาณข้อมูลจาก Sender (A) ที่ไม่สมบูรณ์ที่เกิดจากการถอดข้อมูลเชิงแสง (Optical De-Encapsulation) ระหว่างสัญญาณรูปที่ 4.23 (e) กับกุญแจเชิงแสง (Optical Key) รูป 4.23 (g) แสดงสัญญาณข้อมูลที่เกิดจากสัญญาณรูปที่ 4.23 (f) – (ที่อยู่เชิงแสง (Optical Address) + กุญแจเชิงแสง (Optical Key)) ซึ่งจะเห็นว่าจากการวัดผลสำเร็จของการส่งข้อมูลในเครือข่ายสื่อสารในหัวข้อ 3.3.4 สัญญาณข้อมูลจาก Sender (A) ไม่สามารถส่งไปยัง Receiver (B) ได้สำเร็จ แสดงให้เห็นว่าผู้รับข้อมูลไม่สามารถถอดข้อมูลที่ถูกต้องเนื่องจากมีที่อยู่เชิงแสง (Optical Address) ที่ไม่ตรงกันที่อยู่เชิงแสงของผู้รับข้อมูลที่ผู้ส่งข้อมูลต้องการส่งข้อมูลในเครือข่าย และมีกุญแจเชิงแสง (Optical Key) ที่ไม่ถูกต้อง

4.5 ผลของพารามิเตอร์ต่อสัญญาณที่ถูกเข้ารหัสด้านการสื่อสารข้อมูล

4.5.1 สมมุติฐาน

การทดสอบสมมติฐานที่ 4.2 เพื่อเป็นการทดสอบการทำงานของโปรโตคอลที่นำเสนอ โดยศึกษาผลกระทบของความเข้มแสงของสัญญาณต่าง ๆ ที่ใช้ในโปรโตคอลที่นำเสนอ ว่ามีผลต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลอย่างไรบ้าง กำหนดสมมติฐานที่ 4.2 ได้ดังนี้ ถ้าความเข้มแสงของสัญญาณต่าง ๆ ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยมีสมมติฐานย่อย ดังนี้

สมมติฐานย่อยที่ 4.2.1 ถ้าความเข้มแสงของสัญญาณ Input ที่ Input Port ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

สมมติฐานย่อยที่ 4.2.2 ถ้าความเข้มแสงของสัญญาณ Input ที่ Control Port ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

สมมติฐานย่อยที่ 4.2.3 ถ้าความเข้มแสงของสัญญาณที่อยู่เชิงแสง (Optical Address) ที่ส่งข้อมูลด้วยโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

สมมติฐานย่อยที่ 4.2.4 ถ้าความเข้มแสงของสัญญาณข้อมูล (Data Signal) ที่ส่งข้อมูลด้วยโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

4.5.2 วิธีการทดสอบสมมติฐาน

การทดสอบสมมติฐานมีข้อจำกัดของแบบจำลองที่ใช้ในการทดสอบสมมติฐานตามหัวข้อ 3.3.1 ข้อจำกัดของแบบจำลองที่ใช้จำลอง มีรูปแบบเครือข่ายสื่อสารที่ใช้ในการทดสอบสมมติฐานตามหัวข้อ 3.3.2 รูปแบบเครือข่ายแบบจำลอง อีกทั้งมีเหตุผลการกำหนดลักษณะของสัญญาณข้อมูลที่ใช้ในการทดสอบสมมติฐานตามหัวข้อ 3.3.3 ลักษณะของสัญญาณข้อมูลที่ใช้ในการจำลอง และมี

วิธีการทดสอบสมมติฐานตามหัวข้อ 3.3.5 วิธีการจำลองเครือข่ายเพื่อทดสอบการทำงานของโปรโตคอล

4.5.3 พารามิเตอร์ที่ใช้ในการจำลองเครือข่ายเพื่อทดสอบสมมติฐาน

การทดสอบสมมติฐานที่ 4.2.1 ถ้าความเข้มแสงของสัญญาณ Input ที่ Input Port ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 4.2.1 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการเปลี่ยนแปลงพารามิเตอร์เพื่อเป็นตัวแปรต้นในการทดสอบสมมติฐาน คือ ความเข้มแสงของสัญญาณ Input ที่ Input Port ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) (PD) : E_{in} โดยกำหนดค่าเป็น 0.8,1.2,1.6 W/μm^2 ตามลำดับ

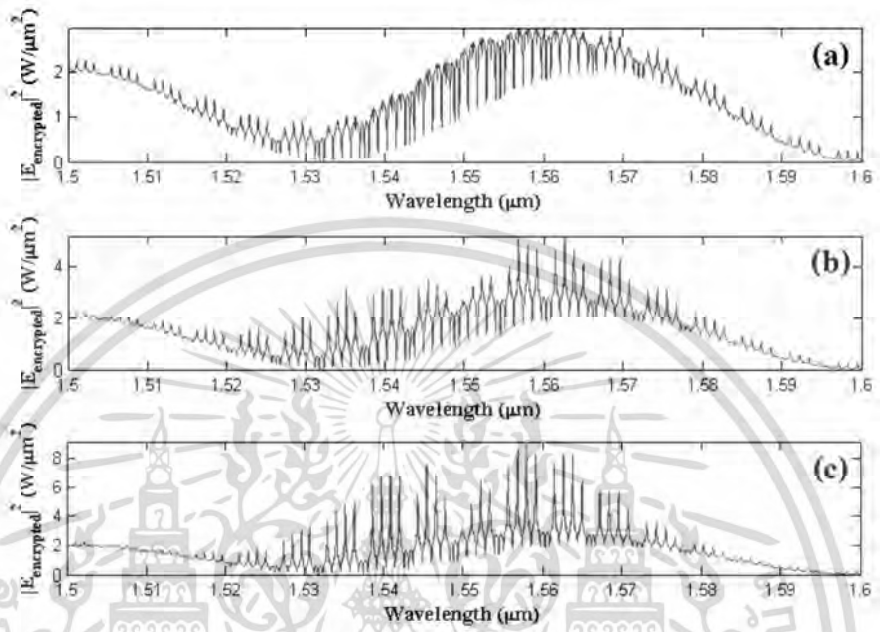
การทดสอบสมมติฐานที่ 4.2.2 ถ้าความเข้มแสงของสัญญาณ Input ที่ Control Port ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 4.2.2 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการเปลี่ยนแปลงพารามิเตอร์เพื่อเป็นตัวแปรต้นในการทดสอบสมมติฐาน คือ ความเข้มแสงของสัญญาณ Input ที่ Control Port ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) (PD) : E_{con} โดยกำหนดค่าเป็น 0.8,1.2,1.6 W/μm^2 ตามลำดับ

การทดสอบสมมติฐานที่ 4.2.3 ถ้าความเข้มแสงของสัญญาณที่อยู่เชิงแสง (Optical Address) ที่ส่งข้อมูลด้วยโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 4.2.3 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการเปลี่ยนแปลงพารามิเตอร์เพื่อเป็นตัวแปรต้นในการทดสอบสมมติฐาน คือ ความเข้มแสงของสัญญาณที่อยู่เชิงแสง (Optical Address) โดยกำหนดค่าเป็น 1.5,3.0,4.5 W/μm^2 ตามลำดับ

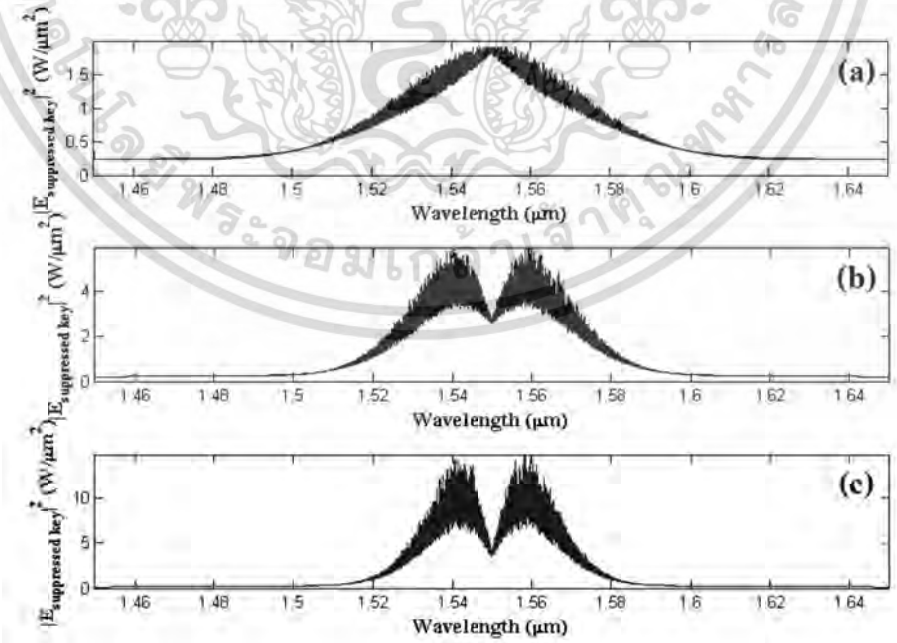
การทดสอบสมมติฐานที่ 4.2.4 ถ้าความเข้มแสงของสัญญาณข้อมูล (Data Signal) ที่ส่งข้อมูลด้วยโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 4.2.4 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตาม

ตารางที่ 3.1 แต่มีการเปลี่ยนแปลงพารามิเตอร์เพื่อเป็นตัวแปรต้นในการทดสอบสมมติฐาน คือ ความเข้มแสงของสัญญาณ Data โดยกำหนดค่าเป็น 2.0,4.0,6.0 W/μm^2 ตามลำดับ

4.5.4 ผลการจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 4.2.1



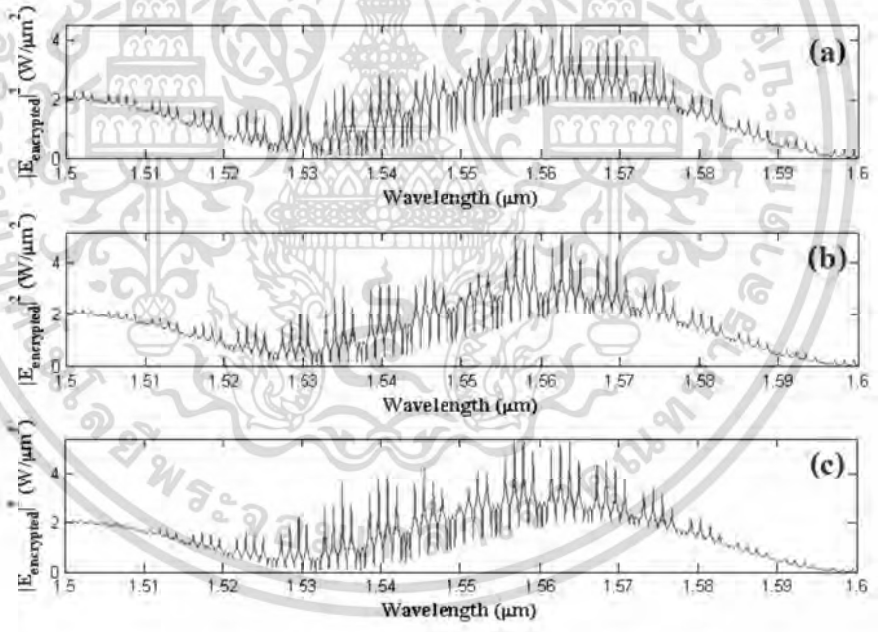
รูปที่ 4.24 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 4.2.1



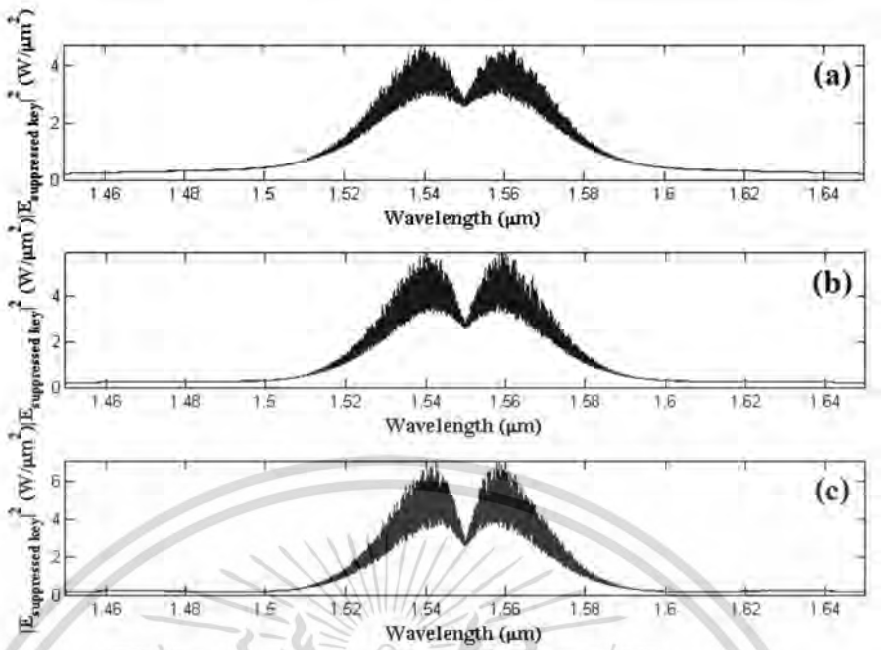
รูปที่ 4.25 เปรียบเทียบผลการจำลอง Suppressed Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 4.2.1

จากรูปที่ 4.24 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 4.2.1 รูปที่ 4.24 (a) รูปที่ 4.24 (b) และรูปที่ 4.24 (c) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ของการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล โดยที่ความเข้มสัญญาณ Input ที่ PD (Input) : E_{in} เท่ากับ 0.8, 1.2, 1.6 W/μm^{2}ตามลำดับ จากรูปที่ 4.25 เปรียบเทียบผลการจำลอง Suppressed Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 4.2.1 รูปที่ 4.25 (a) รูปที่ 4.25 (b) และรูปที่ 4.25 (c) แสดงสัญญาณ Suppressed Key โดยที่ความเข้มสัญญาณ Input ที่ PD (Input) : E_{in} เท่ากับ 0.8, 1.2, 1.6 W/μm^2 ตามลำดับ จากการจำลองพบว่าพารามิเตอร์ความเข้มสัญญาณ Input ที่ PD (Input) : E_{in} มีผลต่อการสร้างสัญญาณ Suppressed Key โดยที่ความเข้มสัญญาณที่เปลี่ยนไปส่งผลต่อการสร้างสัญญาณรูปปาก (LIP Signal) และส่งผลต่อความเข้มของสัญญาณ Suppressed Key ทำให้ความเข้มของสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) เปลี่ยนแปลงด้วย ซึ่งความเข้มของสัญญาณต่าง ๆ มีผลอย่างมากต่อโปรโตคอลที่นำเสนอ เนื่องจากการห่อหุ้มเชิงแสง (Optical Encapsulation) ใช้วิธีการแทรกสอดกันของสัญญาณ

4.5.5 ผลการจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 4.2.2



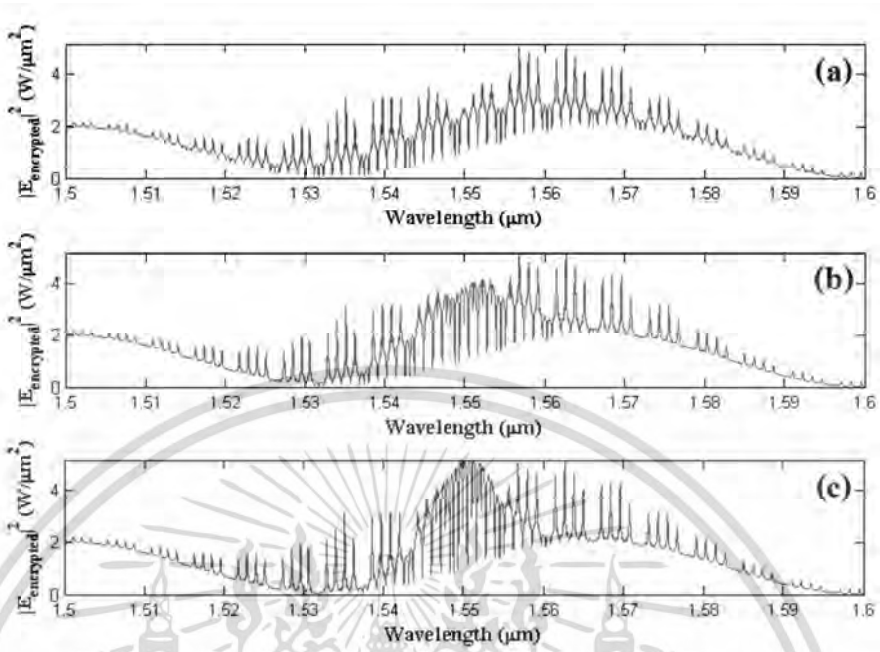
รูปที่ 4.26 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 4.2.2



รูปที่ 4.27 เปรียบเทียบผลการจำลอง Suppressed Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 4.2.2

จากรูปที่ 4.26 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 4.2.2 รูปที่ 4.26 (a) รูปที่ 4.26 (b) และรูปที่ 4.26 (c) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ของการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล โดยที่ความเข้มสัญญาณ Input ที่ PD (Control) : E_{con} เท่ากับ 0.8, 1.2, 1.6 W/μm^2 ตามลำดับ รูปที่ 4.27 เปรียบเทียบผลการจำลอง Suppressed Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 4.2.2 รูปที่ 4.27 (a) รูปที่ 4.27 (b) และรูปที่ 4.27 (c) แสดงสัญญาณ Suppressed Key โดยที่ความเข้มสัญญาณ Input ที่ PD (Control) : E_{con} เท่ากับ 0.8, 1.2, 1.6 W/μm^2 ตามลำดับ จากการจำลองพบว่าพารามิเตอร์ความเข้มสัญญาณ Input ที่ PD (Con) : E_{con} ไม่มีผลต่อการสร้างสัญญาณ Suppressed Key ที่จะทำให้ลักษณะของการสื่อสารข้อมูลเปลี่ยนแปลงไป

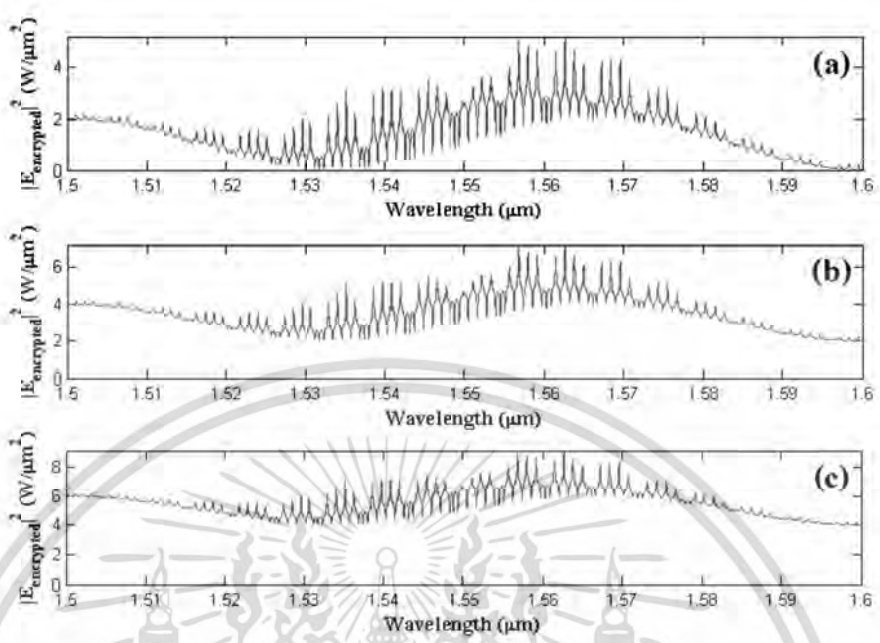
4.5.6 ผลการจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 4.2.3



รูปที่ 4.28 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 4.2.3

จากรูปที่ 4.28 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 4.2.3 รูปที่ 4.28 (a) รูปที่ 4.28 (b) และรูปที่ 4.28 (c) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ของการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล โดยที่ความเข้มสัญญาณ Optical Address เท่ากับ 1.5, 3.0, 4.5 W/μm^2 ตามลำดับ จากการจำลองพบว่าพารามิเตอร์ความเข้มสัญญาณ Optical Address มีผลต่อความเข้มของสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ซึ่งความเข้มของสัญญาณต่าง ๆ มีผลอย่างมากต่อโปรโตคอลที่นำเสนอเนื่องจากการห่อหุ้มเชิงแสง (Optical Encapsulation) ใช้วิธีการแทรกสอดกันของสัญญาณ

4.5.7 ผลการจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 4.2.4



รูปที่ 4.29 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 4.2.4

จากรูปที่ 4.29 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 4.2.4 รูปที่ 4.29 (a) รูปที่ 4.29 (b) และรูปที่ 4.29 (c) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ของการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล โดยที่ความเข้มสัญญาณ Data เท่ากับ 1.5, 3.0, 4.5 $W/\mu m^2$ ตามลำดับ จากการจำลองพบว่าพารามิเตอร์ความเข้มสัญญาณ Data มีผลต่อความเข้มของสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ซึ่งความเข้มของสัญญาณต่าง ๆ มีผลอย่างมากต่อโปรโตคอลที่นำเสนอ เนื่องจากการห่อหุ่มเชิงแสง (Optical Encapsulation) ใช้วิธีการแทรกสอดกันของสัญญาณ กล่าวคือ ความเข้มสัญญาณ Data ไม่ควรมีความเข้มมากกว่า 2 เท่าของความเข้มสัญญาณ Input ที่ PD (Input) : E_{in} หรือความเข้มสัญญาณ Optical Address เพราะจะทำให้การห่อหุ่มเชิงแสงของสัญญาณกุญแจเชิงแสงหรือสัญญาณที่อยู่เชิงแสงไม่ครอบคลุมสัญญาณ Data ทำให้ผู้ไม่หวังดีในเครือข่ายอาจจะดักข้อมูลระหว่างทางได้

4.6 ข้อจำกัดการทำงานของโปรโตคอลด้านการสื่อสารข้อมูล

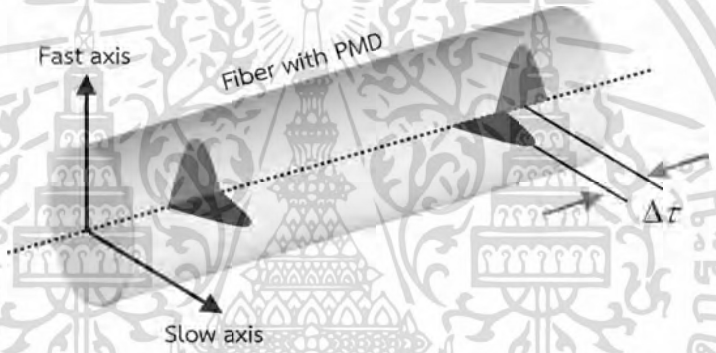
4.6.1 ระยะทางที่สามารถส่งข้อมูลในเครือข่าย

การกระจายตัวแบบ Polarization Mode Dispersion (PMD) เป็นปรากฏการณ์ที่ส่งผลกระทบต่อสถานะการโพลาไรซ์ของโฟตอนแสง โดยที่พัลส์ของสัญญาณแสงเมื่อถูกส่งไปตามตัวนำคลื่นในระยะทางหนึ่งจะเกิดความต่างเฟสขึ้นระหว่างองค์ประกอบของคลื่นแสงในแนวตั้งและแนวนอนดังแสดงในรูปที่ 4.30 ส่งผลให้มุมโพลาไรซ์ของสัญญาณแสงมีการเปลี่ยนแปลงไป [78-80]

เมื่อพิจารณาถึงผลกระทบดังกล่าวจะพบว่าการส่งข้อมูลภายในเครือข่าย จะสามารถทำได้ในระยะทางจำกัดค่าหนึ่งที่ PMD จะไม่ส่งผลกระทบต่อการทำงานซึ่งสามารถพิจารณาได้จากสมการ (4.2)

$$L_{\max} = \frac{0.02}{(\Delta\tau)^2 \times R^2} \tag{4.2}$$

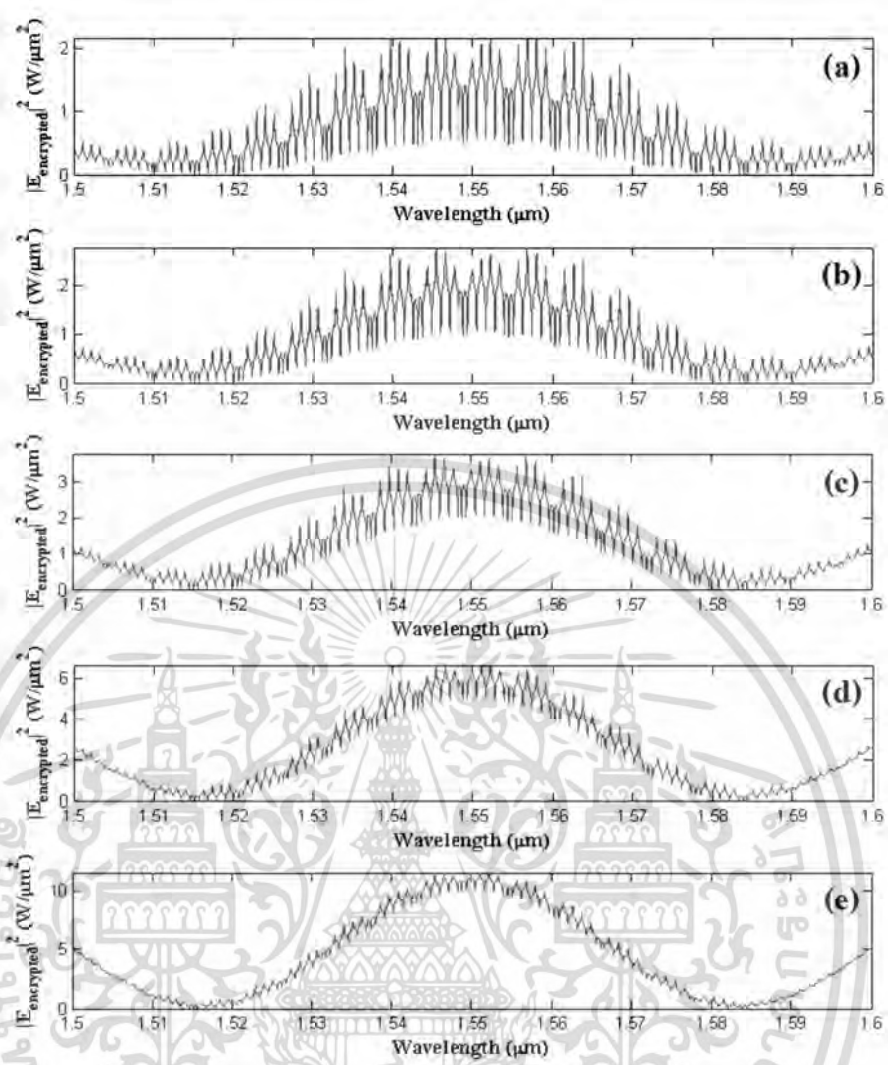
โดย L_{max} คือระยะทางสูงสุดที่สามารถส่งสัญญาณแสงผ่านตัวนำคลื่นได้โดยไม่คิดผลกระทบจาก PMD, R คืออัตรา Bit rate ของการส่งสัญญาณ $\Delta\tau$ คือค่า Differential group delay (DGD) ของตัวนำคลื่น หรือใยแก้วนำแสงที่พิจารณาซึ่งจะถูกกำหนดค่ามาจากโรงงานผู้ผลิต เนื่องจากโครงข่ายใยแก้วนำแสงของระบบสื่อสารสมัยใหม่ในปัจจุบันจะมีค่า $\Delta\tau$ เท่ากับ 0.1 ps/km ถ้าทำการส่งข้อมูลในอัตรา 10 Gbps จะสามารถคำนวณหาค่า L_{max} ได้เท่ากับ 20,000 km [81] และถ้าทำการส่งข้อมูลในอัตรา Tbps จะสามารถคำนวณหาค่า L_{max} ได้เท่ากับ 2 km



รูปที่ 4.30 ผลกระทบจาก PMD ที่มีต่อองค์ประกอบของแสงที่แพร่กระจายผ่านใยแก้วนำแสง

4.6.2 ผลของความเข้มของสัญญาณต่อการสื่อสารข้อมูล

จากการทดสอบสมมติฐานที่ 4.2.1 – 4.2.4 พบว่า ค่าความเข้มแสงของสัญญาณต่าง ๆ มีผลต่อความเข้มแสงของสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ซึ่งความเข้มแสงของสัญญาณต่าง ๆ มีผลอย่างมากต่อโปรโตคอลที่นำเสนอ เนื่องจากการห่อหุ้มเชิงแสง (Optical Encapsulation) ใช้วิธีการแทรกสอดกันของสัญญาณ โดยเฉพาะอย่างยิ่งจากการทดสอบสมมติฐานที่ 4.2.4 โดยความเข้มแสงของสัญญาณข้อมูล (Data Signal) จะส่งผลต่อความปลอดภัยของการสื่อสารข้อมูลโดยตรง เพราะถ้าความเข้มแสงของสัญญาณข้อมูล (Data Signal) มากกว่าความเข้มแสงของสัญญาณกุญแจเชิงแสง (Optical Key) และที่อยู่เชิงแสง (Optical Address) หลายเท่า จะส่งผลให้กุญแจเชิงแสง (Optical Key) และที่อยู่เชิงแสง (Optical Address) ไม่สามารถห่อหุ้มข้อมูลได้ อธิบายได้ดังนี้



รูปที่ 4.31 ผลของความไม่เหมาะสมของค่าพารามิเตอร์ความเข้มแสงของสัญญาณต่าง ๆ

จากรูปที่ 4.31 แสดงผลของความไม่เหมาะสมของค่าพารามิเตอร์กำลังสัญญาณต่าง ๆ รูปที่ 4.31 (a-e) แสดงรูปแบบสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่สัญญาณข้อมูล (Data Signal) มีค่าความเข้มแสงเท่ากับ 50 %, 100 %, 200 %, 500 % และ 1000 % ของความเข้มแสงของสัญญาณที่ใช้สร้างกุญแจเชิงแสง (Optical Key) และที่อยู่เชิงแสง (Optical Address) ตามลำดับ พบว่าถ้าความเข้มแสงของสัญญาณข้อมูล (Data Signal) มากกว่าความเข้มแสงของสัญญาณที่ใช้สร้างกุญแจเชิงแสง (Optical Key) และที่อยู่เชิงแสง (Optical Address) มากขึ้นเรื่อย ๆ สัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ก็เหมือนมีสัญญาณ Noiselike ห่อหุ้มสัญญาณข้อมูล (Data Signal) น้อยลงเรื่อย ๆ โดยโปรโตคอลที่นำเสนอนี้ ความเข้มแสงที่เหมาะสมของสัญญาณข้อมูล (Data Signal) คือ น้อยกว่า 200 % ของความเข้มแสงของสัญญาณที่ใช้สร้างกุญแจเชิงแสง (Optical Key) และที่อยู่เชิงแสง (Optical Address)

4.7 อภิปรายสรุปการสื่อสารข้อมูลด้วยโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ

ในบทนี้เป็นการอธิบายการสื่อสารข้อมูลด้วยโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ โดยกล่าวถึง 2 ประเด็นคือ การสื่อสารข้อมูลระหว่างระดับชั้นย่อยและการสื่อสารข้อมูลภายในเครือข่าย

การสื่อสารข้อมูลระหว่างระดับชั้นย่อย พัฒนาวิธีการที่เรียกว่า การห่อหุ้มเชิงแสงและถอดข้อมูลเชิงแสง (Optical Encapsulation / De-encapsulation) เนื่องจากต้องการให้โปรโตคอลนี้ทำงานเป็นระดับชั้นย่อย (Sub Layer) และทำงานด้วยอุปกรณ์เชิงแสงทั้งหมด

การสื่อสารข้อมูลภายในเครือข่าย มีการส่งสัญญาณ 2 ลักษณะคือ การส่งสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) และการส่งสัญญาณกุญแจเชิงแสง (Optical Key) ที่ห่อหุ้มด้วยสัญญาณรูปปาก (LIP Signal) โดยที่ทั้ง 2 ลักษณะสามารถแยกกันได้ด้วยการตรวจสอบสัญญาณของ Reference Port ของฝั่งส่งข้อมูลและฝั่งรับข้อมูลที่ผ่าน Polarizing Beam Splitter (PBS) ที่ตัวตรวจจับ

การจำลองการส่งข้อมูลในเครือข่าย จากการทดสอบสมมติฐานที่ 4.1 พบว่า ถ้าโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดถูกใช้งานภายในเครือข่ายเชิงแสงจะส่งผลต่อการทำงานของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมดสามารถทำได้ถูกต้อง พบว่าโปรโตคอลสามารถทำงานได้ถูกต้อง ส่งข้อมูลถึงผู้รับข้อมูลได้อย่างถูกต้อง ถ้าผู้มีผู้ไม่หวังดีในเครือข่ายสื่อสารจะไม่สามารถทราบข้อมูลของผู้ส่งข้อมูลได้

ผลของพารามิเตอร์ต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ด้านการสื่อสารข้อมูลจากการทดสอบสมมติฐานที่ 4.2 พบว่า พารามิเตอร์ความเข้มสัญญาณต่าง ๆ มีผลต่อความเข้มของสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ซึ่งความเข้มของสัญญาณต่าง ๆ มีผลอย่างมากต่อโปรโตคอลที่นำเสนอ เนื่องจากการห่อหุ่มเชิงแสง (Optical Encapsulation) ใช้วิธีการแทรกสอดกันของสัญญาณ กล่าวคือ ความเข้มสัญญาณ Data ไม่ควรมีความเข้มมากกว่าความเข้มสัญญาณ Input ที่ PD (Input): E_{in} หรือความเข้มสัญญาณ Optical Addressเพราะจะทำให้การห่อหุ่มเชิงแสงของสัญญาณกุญแจเชิงแสงหรือสัญญาณที่อยู่เชิงแสงไม่ครอบคลุมสัญญาณ Data ทำให้ผู้ไม่หวังดีในเครือข่ายอาจจะดักข้อมูลระหว่างทางได้

ข้อจำกัดการทำงานของโปรโตคอลด้านการสื่อสารข้อมูล โปรโตคอลที่นำเสนอรองรับระยะทางของการส่งข้อมูลในเครือข่ายสูงสุด 20,000 km ถ้าทำการส่งข้อมูลในอัตรา 10 Gbps และระยะทางของการส่งข้อมูลในเครือข่ายสูงสุด 2 km ถ้าทำการส่งข้อมูลในอัตรา Tbps และความเข้มแสงที่เหมาะสมของสัญญาณข้อมูล (Data Signal) คือน้อยกว่า 200 % ของความเข้มแสงของสัญญาณที่ใช้สร้างกุญแจเชิงแสง (Optical Key) และที่อยู่เชิงแสง (Optical Address) เพราะจะทำให้การห่อหุ้มเชิงแสงของสัญญาณกุญแจเชิงแสงหรือสัญญาณที่อยู่เชิงแสงครอบคลุมสัญญาณข้อมูล (Data Signal)

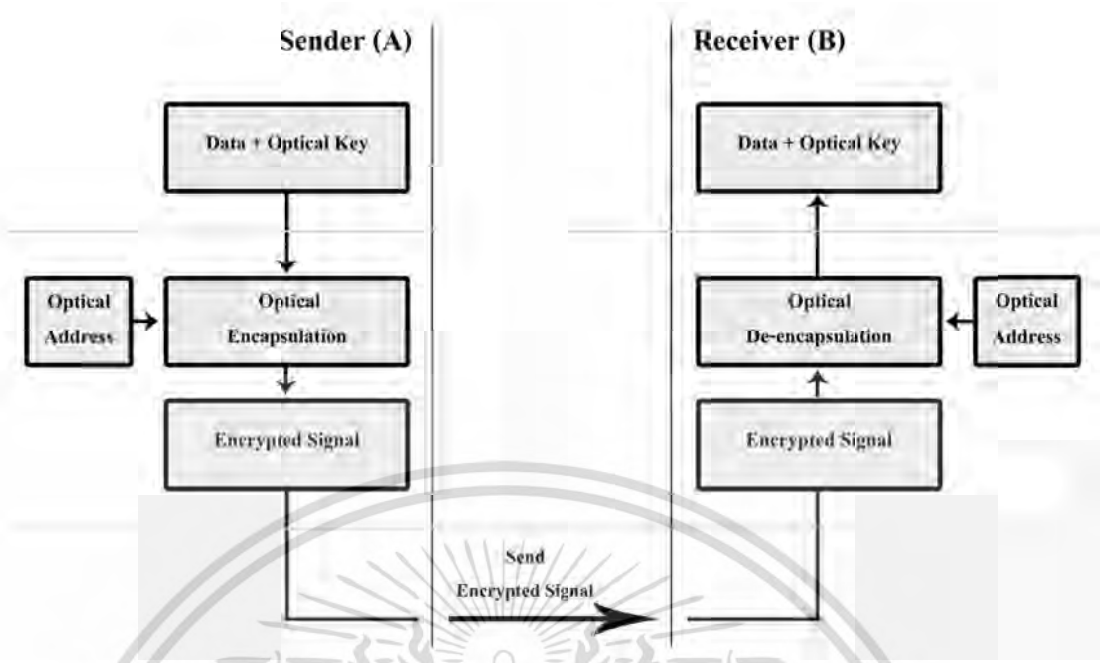
บทที่ 5
การระบุที่อยู่ภายในเครือข่ายด้วยโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ

ในส่วนของบทนี้เป็นการกล่าวถึงการระบุที่อยู่ภายในเครือข่ายด้วยโปรโตคอลที่นำเสนอ อธิบายที่อยู่เชิงแสง (Optical Address) การเปรียบเทียบที่อยู่เชิงแสงกับ IP Address v4 และผลของพารามิเตอร์ต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ด้านการระบุที่อยู่ภายในเครือข่าย รวมถึงข้อจำกัดการทำงานของโปรโตคอลด้านการระบุที่อยู่ภายในเครือข่าย โดยมีหัวข้อต่าง ๆ ดังนี้

- ปัญหาและประเด็นสำคัญ
- อธิบายที่อยู่เชิงแสง (Optical Address)
  - ความหมายของที่อยู่เชิงแสง
  - การใช้งานและจำนวนของที่อยู่เชิงแสง
  - การเปรียบเทียบที่อยู่เชิงแสงกับ IP Address v4
- ผลของพารามิเตอร์ต่อสัญญาณที่ถูกเข้ารหัสด้านการระบุที่อยู่ภายในเครือข่าย
- ข้อจำกัดการทำงานของโปรโตคอลด้านการระบุที่อยู่ภายในเครือข่าย
- อภิปรายสรุปการระบุที่อยู่ภายในเครือข่ายด้วยโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ

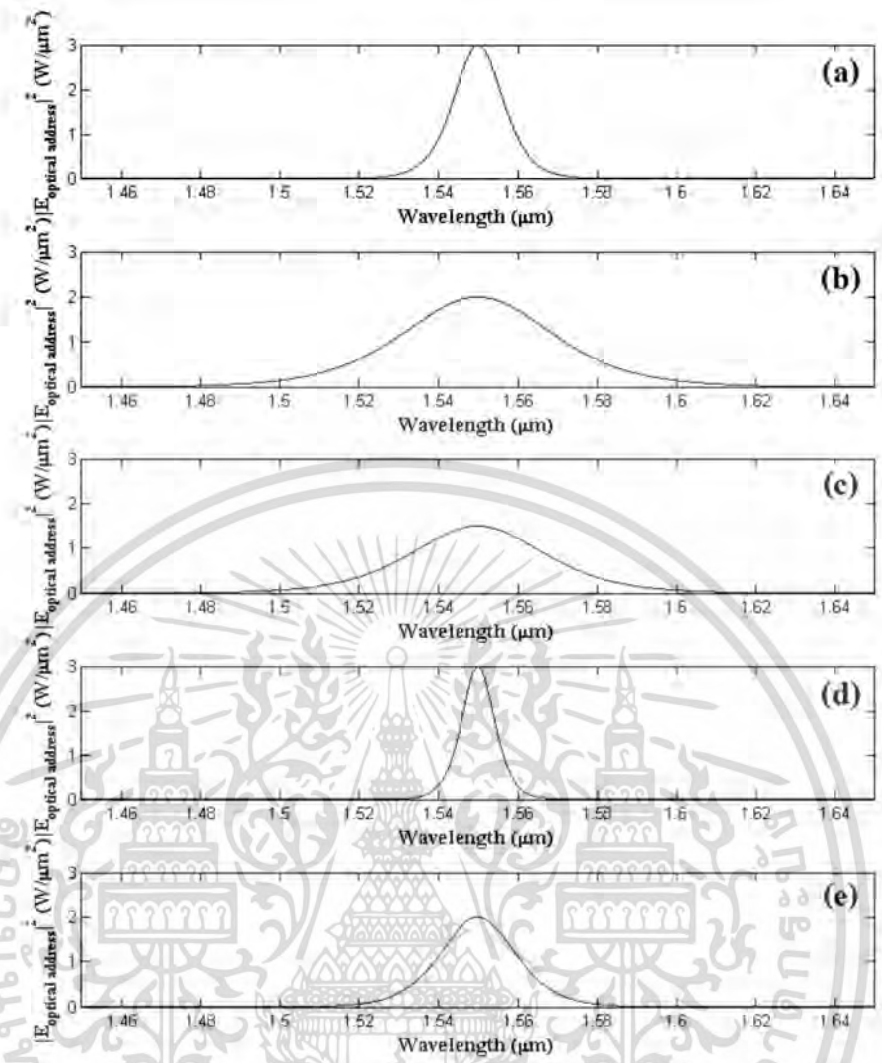
5.1 ปัญหาและประเด็นสำคัญ

ในส่วนของหัวข้อนี้กล่าวถึงการระบุที่อยู่ภายในเครือข่ายด้วยโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ ซึ่งในการพัฒนาโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงสำหรับการสื่อสารความเร็วสูงและความปลอดภัยสูงที่นำเสนอในงานวิจัยนี้ เป็นการนำเสนอวิธีการสื่อสารที่ใช้อุปกรณ์เชิงแสงทั้งหมดในการทำงาน ซึ่งในการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูลมีขั้นตอนที่สำคัญเพื่อให้ข้อมูลที่ส่งนั้น ถูกส่งไปยังผู้รับที่ถูกต้องตามที่ผู้ส่งข้อมูลต้องการได้ คือขั้นตอนในการระบุที่อยู่ภายในเครือข่าย โดยมีการทำงานอธิบายได้ดังรูปที่ 5.1



รูปที่ 5.1 แผนภาพแสดงหลักการทำงานของการระบุที่อยู่เชิงแสง

จากรูปที่ 5.1 แผนภาพแสดงหลักการทำงานของการระบุที่อยู่เชิงแสง แสดงให้เห็นว่าโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงสำหรับการสื่อสารความเร็วสูงและความปลอดภัยสูงที่นำเสนอใช้ที่อยู่เชิงแสง (Optical Address) ในการระบุที่อยู่ภายในเครือข่าย เพื่อให้สามารถใช้งานได้กับอุปกรณ์เชิงแสงทั้งหมด โดยมีตัวอย่างที่อยู่เชิงแสง (Optical Address) ตามรูปที่ 5.2



รูปที่ 5.2 ภาพแสดงตัวอย่างที่อยู่เชิงแสง

5.2 อธิบายที่อยู่เชิงแสง (Optical Address)

5.2.1 ความหมายของที่อยู่เชิงแสง

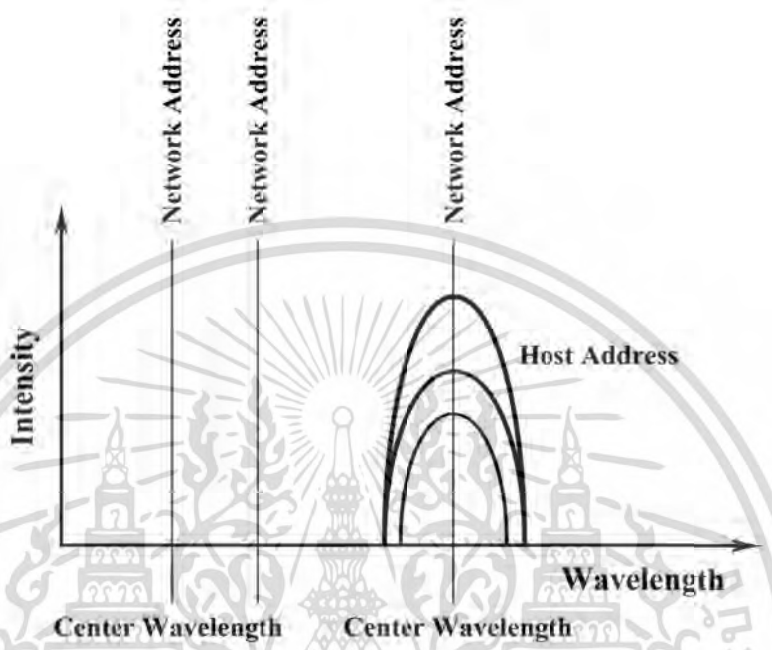
ที่อยู่เชิงแสง (Optical Address) หมายถึง Bright Soliton โดยมีคุณลักษณะเฉพาะตัวที่สามารถระบุที่อยู่ภายในเครือข่ายเชิงแสงได้ เพื่อนำไปใช้ในการแทนบุคคลใดบุคคลหนึ่งภายในเครือข่ายเชิงแสง ดังตัวอย่างตามรูปที่ 5.2 ภาพแสดงตัวอย่างที่อยู่เชิงแสง โดยมีสมการคณิตศาสตร์ของที่อยู่เชิงแสง (Optical Address) ตามสมการที่ (3.1)

ที่อยู่เชิงแสง (Optical Address) : $$\psi(t) = \sqrt{\psi_0}\,\sec h\left[\frac{T}{T_0}\right]\exp\left[\left(\frac{z}{2L_D}\right) - i\omega_0 t\right] \qquad (3.1)$$

โดยรายละเอียดของสมการที่ (3.1) ตามสมการที่ (2.12)

5.2.2 การใช้งานและจำนวนของที่อยู่เชิงแสง

จากหัวข้อก่อนหน้า โปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงสำหรับการสื่อสารความเร็วสูงและความปลอดภัยสูงที่นำเสนอ มีการใช้ที่อยู่เชิงแสง (Optical Address) ในการระบุที่อยู่ภายในเครือข่าย โดยมีโครงสร้างของที่อยู่เชิงแสงตามรูปที่ 5.3



รูปที่ 5.3 โครงสร้างที่อยู่เชิงแสง

จากรูปที่ 5.3 โครงสร้างที่อยู่เชิงแสงอธิบายได้ว่า สำหรับโปรโตคอลที่นำเสนอมีที่อยู่เชิงแสง (Optical Address) ที่สามารถระบุที่อยู่ภายในเครือข่ายเดียวกันได้ ต้องเป็นที่อยู่เชิงแสง (Optical Address) ที่มีศูนย์กลางช่วงคลื่น (Center Wavelength) เดียวกันเท่านั้น และกล่าวได้ว่า บุคคลที่มีการใช้ที่อยู่เชิงแสง (Optical Address) ที่มีศูนย์กลางช่วงคลื่น (Center Wavelength) ไม่เหมือนกันเป็นบุคคลที่อยู่คนละเครือข่ายกัน

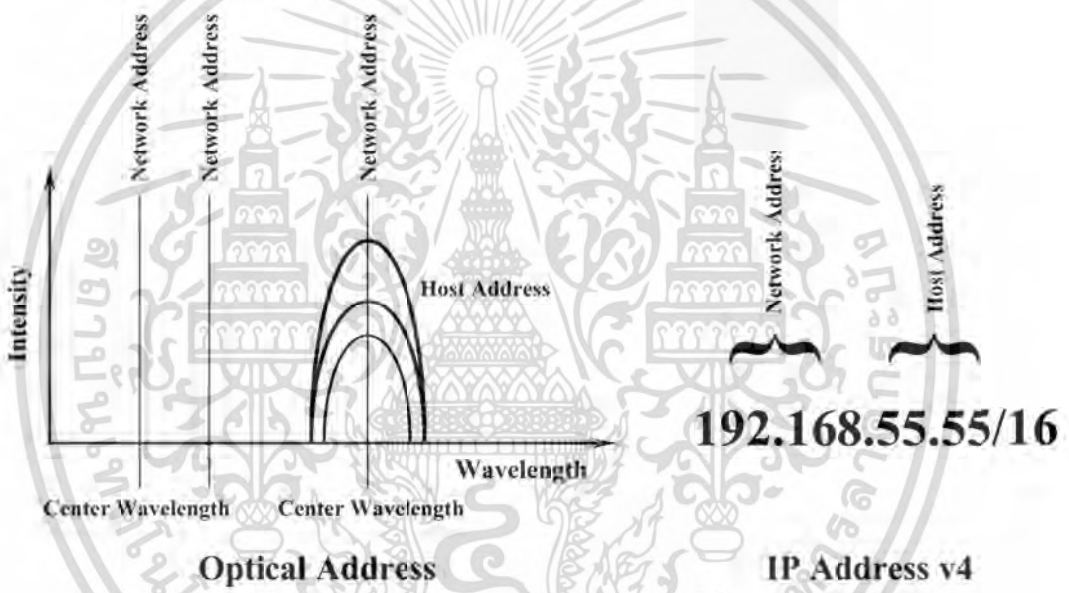
จำนวนของบุคคลที่อยู่ในเครือข่ายเดียวกัน ในทางทฤษฎีตามสมการที่ (3.1) สามารถเปลี่ยนค่าพารามิเตอร์ ψ_0 คือขนาดของสนามไฟฟ้า z คือระยะการแพร่กระจาย (Propagation Distance) ของสนามไฟฟ้า T คือเวลาในการแพร่กระจายของพัลส์โซลิตอน (ความกว้างของพัลส์) T_0 คือเวลาในการแพร่กระจายของพัลส์โซลิตอน (ความกว้างของพัลส์) ในขณะเริ่มต้น และ L_D คือระยะการกระจายตัว (Dispersion Length) ของพัลส์โซลิตอน ซึ่งค่าพารามิเตอร์ต่างๆเหล่านี้สามารถเปลี่ยนแปลงได้ไม่จำกัด ทำให้กล่าวได้ว่า ในทางทฤษฎีจำนวนของบุคคลที่อยู่ในเครือข่ายเดียวกันมีไม่จำกัด

จำนวนของจำนวนของบุคคลที่อยู่ในเครือข่ายเดียวกัน ในทางปฏิบัติการวิจัยเพื่อสร้าง Bright Soliton สามารถทำได้ด้วยวิธีการหลายหลาก [82-84] โดยจะกล่าวถึงตัวอย่างการสร้าง Bright Soliton ด้วยอุปกรณ์เชิงแสงขนาดเล็ก [85,86] ซึ่งทั้ง 2 วิธีการ เป็นการสร้าง Bright Soliton โดยใช้อุปกรณ์เชิงแสงขนาดเล็ก (วงแหวนสั่นพ้อง) 3 อุปกรณ์ และจากการสำรวจขนาดของวงแหวนสั่นพ้อง

ที่สามารถสร้างได้จริง จากปี 2002 ถึงปี 2016 (หัวข้อที่ 2.7) มีการสร้างวงแหวนสั่นพ้องได้ในขนาด 1 μm ถึง 200 μm และจากการสำรวจขนาดของวงแหวนสั่นพ้องที่สร้างได้จริง ส่วนใหญ่เป็นขนาดที่หาร 5 ได้ลงตัว เช่น 5 μm และ 10 μm เป็นต้น ทำให้อนุมานว่าจำนวนขนาดของวงแหวนสั่นพ้องที่สามารถสร้างได้จริง คือ 40 ขนาด เมื่อพิจารณาการสร้าง Bright Soliton ด้วยอุปกรณ์เชิงแสงขนาดเล็กที่ต้องใช้แหวนสั่นพ้อง 3 อุปกรณ์ โดยเงื่อนไขมีสัญญาณแสงสำหรับสร้าง Bright Soliton 1 รูปแบบ ทำให้กล่าวได้ว่า ในทางปฏิบัติจำนวนของบุคคลที่อยู่ในเครือข่ายเดียวกันเท่ากับ 40 x 40 x 40 = 64,000 บุคคล

5.2.3 การเปรียบเทียบที่อยู่เชิงแสงกับ IP Address v4

จากการอธิบายที่อยู่เชิงแสง (Optical Address) ที่นำเสนอในวิทยาพิพนธ์นี้ สามารถเปรียบเทียบกับ IP Address v4 ได้ตามรูปที่ 5.4

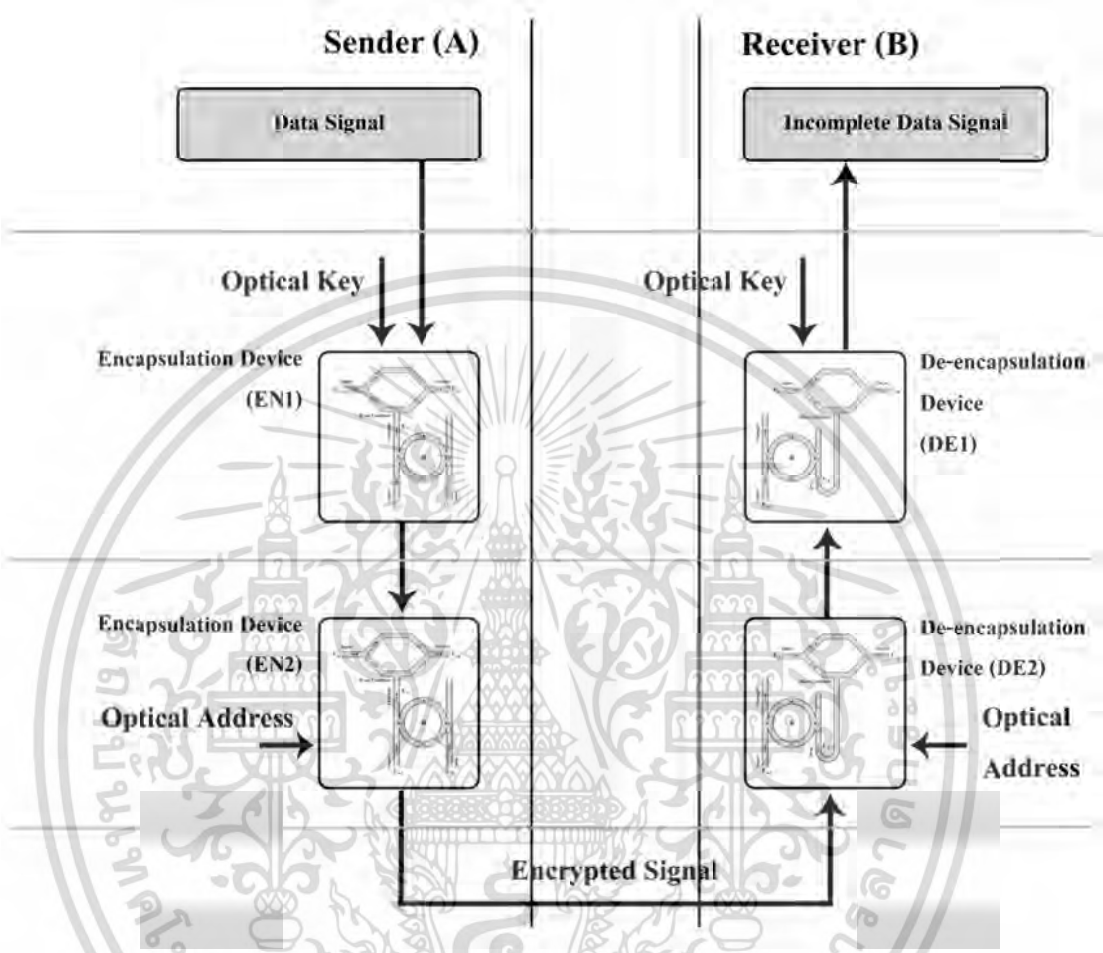


รูปที่ 5.4 เปรียบเทียบที่อยู่เชิงแสงกับ IP Address v4

จากรูปที่ 5.4 เปรียบเทียบที่อยู่เชิงแสง (Optical Address) กับ IP Address v4 อธิบายความแตกต่างได้ดังนี้ IP Address v4 มีการกำหนดหมายเลขเครือข่าย (Network Address) อยู่ภายใน IP Address v4 ซึ่งจะนำไปใช้ในการแบ่งเครือข่าย รวมถึงการส่งข้อมูลระหว่างเครือข่าย แต่ในส่วนของที่อยู่เชิงแสง (Optical Address) จะมีการแบ่งเครือข่าย ซึ่งกำหนดโดยศูนย์กลางช่วงคลื่น (Center Wavelength) กล่าวคือ ถ้าบุคคลในเครือข่ายใช้ศูนย์กลางช่วงคลื่น (Center Wavelength) เดียวกันจะอยู่ในเครือข่ายเดียวกัน ถ้าบุคคลในเครือข่ายใช้ศูนย์กลางช่วงคลื่น (Center Wavelength) ไม่เหมือนกันจะอยู่คนละเครือข่ายกัน

5.2.4 วิธีการอ้างอิงที่อยู่เชิงแสง

วิธีการอ้างอิงที่อยู่เชิงแสง (Optical Address) ทำได้โดยใช้หลักการของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) และอุปกรณ์ที่ใช้หลักการของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer) อธิบายได้ดังนี้



รูปที่ 5.5 อุปกรณ์ที่ใช้ในการอ้างอิงที่อยู่เชิงแสง

จากรูปที่ 5.5 (ฝั่ง Sender (A)) เป็นการแสดงอุปกรณ์ที่ใช้ในการอ้างอิงที่อยู่เชิงแสง : ฝั่งผู้ส่งข้อมูล ซึ่งประกอบด้วยวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (รูปที่ 2.17) และอุปกรณ์ที่ใช้หลักการของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer) (รูปที่ 2.19) และจากรูปที่ 5.5 (ฝั่ง Receiver (B)) เป็นการแสดงอุปกรณ์ที่ใช้ในการอ้างอิงที่อยู่เชิงแสง : ฝั่งผู้รับข้อมูล ประกอบด้วยวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (รูปที่ 2.17) และอุปกรณ์ที่ใช้หลักการของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer) (รูปที่ 2.19) เช่นกัน ซึ่งมีวิธีการดังนี้

วิธีการส่งข้อมูลด้วยการอ้างอิงที่อยู่เชิงแสง : ฝั่งผู้ส่งข้อมูล

(จากรูปที่ 5.5 Sender (A) ต้องการส่งข้อมูลให้ Receiver (B) ด้วยการเข้ารหัสข้อมูลด้วยกุญแจเชิงแสงและกำหนดปลายทางผู้รับเป็น Receiver (B) ด้วยที่อยู่เชิงแสง (Optical Address)

ขั้นตอนที่ 1 : Sender (A) นำสัญญาณข้อมูลห่อหุ้มเชิงแสง (Optical Encapsulation) ด้วยกุญแจเชิงแสง (Optical Key)

ขั้นตอนที่ 2 : นำสัญญาณที่ได้จากขั้นตอนที่ 1 ห่อหุ้มเชิงแสง (Optical Encapsulation) ด้วยที่อยู่เชิงแสง (Optical Address) ของ Receiver (B)

ขั้นตอนที่ 3 : ผลของสัญญาณจากขั้นตอนที่ 2 คือสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่ส่งให้ Receiver (B)

วิธีการส่งข้อมูลด้วยการอ้างอิงที่อยู่เชิงแสง : ฝั่งผู้รับข้อมูล

(จากรูปที่ 5.5 Receiver (B) รับข้อมูลจาก Sender (A) และถอดรหัสข้อมูลด้วยกุญแจเชิงแสงและตรวจสอบผู้รับปลายทางด้วยที่อยู่เชิงแสง (Optical Address) ของ Receiver (B)

ขั้นตอนที่ 1 : Receiver (B) รับสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) จาก Sender (A)

ขั้นตอนที่ 2 : นำสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ถอดข้อมูลเชิงแสง (Optical De-encapsulation) ด้วยที่อยู่เชิงแสง (Optical Address) ของ Receiver (B)

ขั้นตอนที่ 3 : นำสัญญาณที่ได้จากขั้นตอนที่ 2 ถอดข้อมูลเชิงแสง (Optical De-encapsulation) ด้วยกุญแจเชิงแสง (Optical Key)

ขั้นตอนที่ 4 : ผลของสัญญาณจากขั้นตอนที่ 3 คือ ข้อมูลที่ส่งจาก Sender (A)

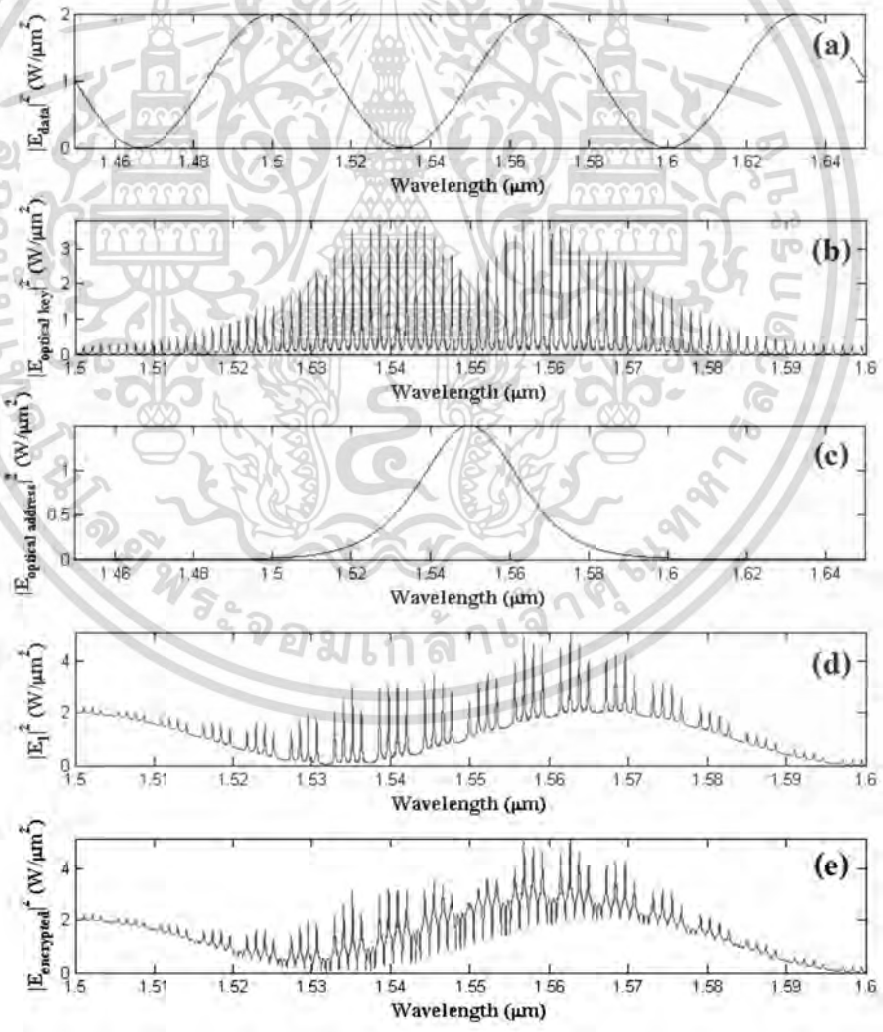
5.2.5 ผลการจำลอง

ในหัวข้อนี้เป็นการจำลองวิธีการส่งข้อมูลด้วยการอ้างอิงที่อยู่เชิงแสง (Optical Address) โดยยกตัวอย่างการจำลองการส่งข้อมูลจากผู้ส่งไปยังผู้รับ ด้วยวิธีการระบุที่อยู่เชิงแสงโดยใช้ที่อยู่เชิงแสง (Optical Address) ในการระบุที่อยู่ ซึ่งจะแสดงให้เห็นว่าถ้าข้อมูลจากผู้ส่งข้อมูลส่งไปยังผู้รับข้อมูลที่ถูกต้อง ผู้รับข้อมูลจะได้รับข้อมูลจากผู้ส่งข้อมูล และถ้าข้อมูลจากผู้ส่งข้อมูลส่งไปยังผู้รับข้อมูลที่ไม่ถูกต้อง ผู้รับข้อมูลจะไม่ได้รับข้อมูลที่ถูกต้องจากผู้ส่งข้อมูล โดยมีแผนภาพแสดงอุปกรณ์เชิงแสงในการจำลองวิธีการส่งข้อมูลด้วยการอ้างอิงที่อยู่เชิงแสงตามรูปที่ 5.5 รวมถึงมีพารามิเตอร์ที่ใช้ในการจำลองตามตารางที่ 5.1 โดยมีรายละเอียดการจำลองดังนี้

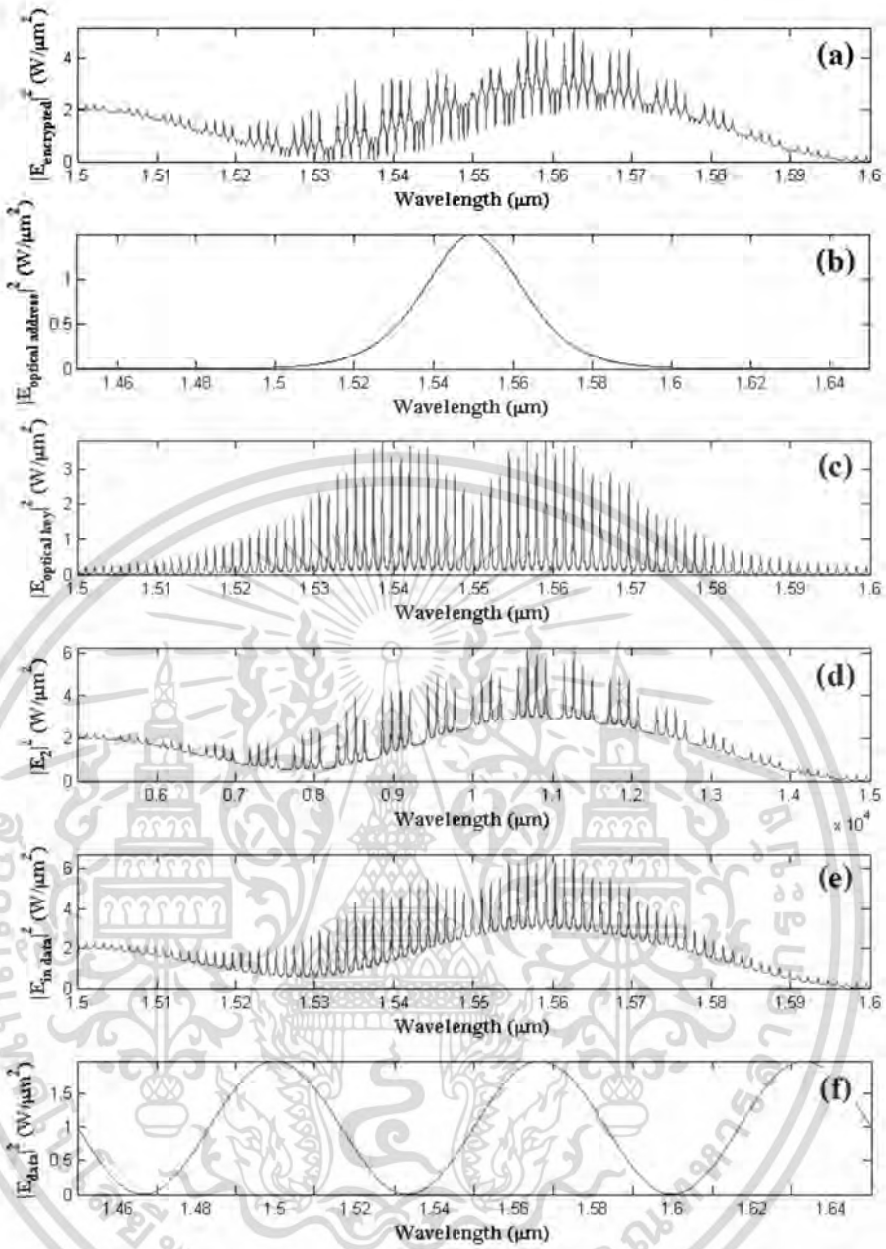
ตารางที่ 5.1 พารามิเตอร์ที่ใช้ในการจำลองวิธีการส่งข้อมูลด้วยการอ้างอิงที่อยู่เชิงแสง (Optical Address)

อุปกรณ์ , สัญญาณ	พารามิเตอร์	ค่าพารามิเตอร์
ทุกอุปกรณ์	ชนิดของวัสดุ	InGaAsP/InP
	ค่าดัชนีหักเหเชิงเส้นของตัวนำคลื่น : n_0	3.4
	ค่าดัชนีหักเหไม่เชิงเส้นของตัวนำคลื่น : n_2	1.3×10^{-13} m^2/W
	การสูญเสียภายในตัวนำคลื่น : α	0.05 dB mm^{-1}
	ค่าการสูญเสียความเข้มแสงเนื่องจากคัปปลิ้ง : γ	0.01
	ขนาดพื้นที่หน้าตัดของตัวนำคลื่น : A_{eff}	0.25 μm^2

อุปกรณ์ , สัญญาณ	พารามิเตอร์	ค่าพารามิเตอร์
Add Drop Filter (EN1,DE1)	ขนาดวงแหวน	20 μm
	สัมประสิทธิ์การคัปปลิ้ง κ_1	0.5
	สัมประสิทธิ์การคัปปลิ้ง κ_2	0.5
Add Drop Filter (EN2,DE2)	ขนาดวงแหวน	200 μm
	สัมประสิทธิ์การคัปปลิ้ง κ_1	0.5
	สัมประสิทธิ์การคัปปลิ้ง κ_2	0.5
สัญญาณ	ศูนย์กลางช่วงคลื่น : λ_0	1.55 μm
	ความเข้มสัญญาณ Optical Address	1.5 W/μm^2
	ความเข้มสัญญาณ Data	2.0 W/μm^2



รูปที่ 5.6 ผลการจำลองของฝั่งผู้ส่งข้อมูล



รูปที่ 5.7 ผลการจำลองของฝั่งผู้รับข้อมูลที่ถูกต้อง

จากรูปที่ 5.6 ผลการจำลองของฝั่งผู้ส่งข้อมูล รูปที่ 5.6 (a) แสดงสัญญาณข้อมูลที่ Sender (A) ต้องการส่งข้อมูลไปยัง Receiver (B) รูปที่ 5.6 (b) แสดงสัญญาณกุญแจเชิงแสง (Optical Key) เพื่อทำให้การสื่อสารข้อมูลปลอดภัย รูปที่ 5.6 (c) แสดงสัญญาณที่อยู่เชิงแสง (Optical Address) ของผู้รับข้อมูล รูปที่ 5.6 (d) แสดงสัญญาณที่เกิดจากการห่อหุ้มเชิงแสงระหว่างสัญญาณข้อมูล (รูปที่ 5.6 (a)) กับ สัญญาณกุญแจเชิงแสง (Optical Key) (รูปที่ 5.6 (b)) รูปที่ 5.6 (e) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่เกิดจากการห่อหุ้มเชิงแสงระหว่างสัญญาณข้อมูลที่ถูกห่อหุ้มด้วยกุญแจเชิงแสง (รูปที่ 5.6 (d)) กับ สัญญาณสัญญาณที่อยู่เชิงแสง (Optical Address) (รูปที่ 5.6 (c)) ที่ซึ่งเป็นสัญญาณที่มีที่อยู่เชิงแสงของผู้รับข้อมูลอยู่ภายใน ถ้าผู้รับสัญญาณที่ถูกเข้ารหัส (Encrypted

Signal) มีที่อยู่เชิงแสง (Optical Address) ตรงกับรูปที่ 5.6 (c) ก็จะสามารถรับสัญญาณข้อมูลจากผู้ส่งข้อมูลได้

จากรูปที่ 5.7 ผลการจำลองของฝั่งผู้รับข้อมูลที่ถูกต้อง รูปที่ 5.7 (a) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่ใช้ในการส่งข้อมูลอย่างปลอดภัยจาก Sender (A) รูปที่ 5.7 (b) แสดงสัญญาณกุญแจเชิงแสง (Optical Key) เพื่อทำให้การสื่อสารข้อมูลปลอดภัย รูปที่ 5.7 (c) แสดงสัญญาณที่อยู่เชิงแสง (Optical Address) ซึ่งตรงกับที่อยู่เชิงแสง (Optical Address) ที่อยู่ภายในสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) รูปที่ 5.7 (d) แสดงสัญญาณที่เกิดจากการถอดข้อมูลเชิงแสง (Optical De-Encapsulation) ระหว่างสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) (รูปที่ 5.7 (a)) กับที่อยู่เชิงแสง (Optical Address) (รูปที่ 5.7 (c)) รูปที่ 5.7 (e) แสดงสัญญาณข้อมูลจาก Sender (A) ที่ไม่สมบูรณ์ที่เกิดจากการถอดข้อมูลเชิงแสง (Optical De-Encapsulation) ระหว่างสัญญาณรูปที่ 5.7 (d) กับกุญแจเชิงแสง (Optical Key) (รูปที่ 5.7 (b)) รูป 5.7 (f) แสดงสัญญาณข้อมูลจาก Sender (A) ที่สมบูรณ์ ซึ่งเกิดจากสัญญาณข้อมูลจาก Sender (A) ที่ไม่สมบูรณ์ – (ที่อยู่เชิงแสง (Optical Address) + กุญแจเชิงแสง (Optical Key)) แสดงให้เห็นว่าผู้รับข้อมูลสามารถถอดข้อมูลที่ถูกต้องเนื่องจากมีที่อยู่เชิงแสง (Optical Address) และกุญแจเชิงแสง (Optical Key) ที่ถูกต้อง

5.3 ผลของพารามิเตอร์ต่อสัญญาณที่ถูกเข้ารหัสด้านการระบุที่อยู่ภายในเครือข่าย

5.3.1 สมมุติฐาน

การทดสอบสมมติฐานที่ 5.1 เพื่อเป็นการทดสอบการทำงานของโปรโตคอลที่นำเสนอ โดยศึกษาผลของพารามิเตอร์ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ในระดับชั้นย่อย Network ว่ามีผลต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลอย่างไรบ้าง กำหนดสมมติฐานที่ 5.1 ได้ดังนี้ ถ้าพารามิเตอร์ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ในระดับชั้นย่อย Network ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยมีสมมติฐานย่อยดังนี้

สมมติฐานย่อยที่ 5.1.1 ถ้าขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ในระดับชั้นย่อย Network ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

สมมติฐานย่อยที่ 5.1.2 ถ้าค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ในระดับชั้นย่อย Network ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

สมมติฐานย่อยที่ 5.1.3 ถ้าค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ในระดับชั้นย่อย Network ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

5.3.2 วิธีการทดสอบสมมติฐาน

การทดสอบสมมติฐานมีข้อจำกัดของแบบจำลองที่ใช้ในการทดสอบสมมติฐานตามหัวข้อ 3.3.1 ข้อจำกัดของแบบจำลองที่ใช้จำลอง มีรูปแบบเครือข่ายสื่อสารที่ใช้ในการทดสอบสมมติฐานตามหัวข้อ 3.3.2 รูปแบบเครือข่ายแบบจำลอง อีกทั้งมีเหตุผลการกำหนดลักษณะของสัญญาณข้อมูลที่ใช้ในการทดสอบสมมติฐานตามหัวข้อ 3.3.3 ลักษณะของสัญญาณข้อมูลที่ใช้ในการจำลอง และมีวิธีการทดสอบสมมติฐานตามหัวข้อ 3.3.5 วิธีการจำลองเครือข่ายเพื่อทดสอบการทำงานของโปรโตคอล

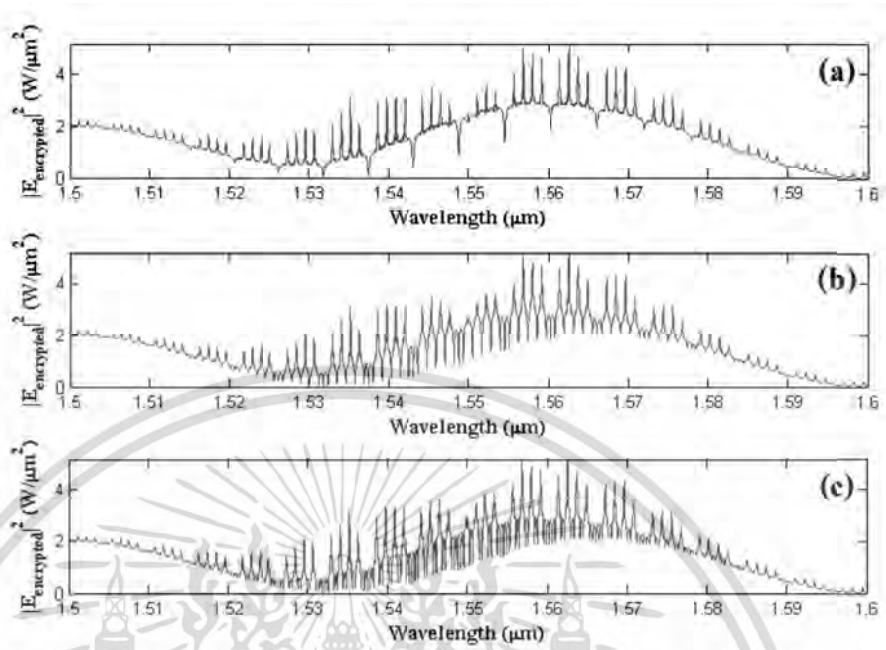
5.3.3 พารามิเตอร์ที่ใช้ในการจำลองเครือข่ายเพื่อทดสอบสมมติฐาน

การทดสอบสมมติฐานที่ 5.1.1 ถ้าขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ในระดับชั้นย่อย Network ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 5.1.1 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการเปลี่ยนแปลงพารามิเตอร์เพื่อเป็นตัวแปรต้นในการทดสอบสมมติฐาน คือ ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณในระดับชั้นย่อย Network (Add Drop Filter) (EN2,DE2) โดยกำหนดค่าเป็น 100,200,300 μm ตามลำดับ

การทดสอบสมมติฐานที่ 5.1.2 ถ้าค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ในระดับชั้นย่อย Network ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 5.1.2 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการเปลี่ยนแปลงพารามิเตอร์เพื่อเป็นตัวแปรต้นในการทดสอบสมมติฐาน คือ ค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณในระดับชั้นย่อย Network (Add Drop Filter) (EN2,DE2) โดยกำหนดค่าเป็น 0.1,0.5,0.9 ตามลำดับ

การทดสอบสมมติฐานที่ 5.1.3 ถ้าค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ในระดับชั้นย่อย Network ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 5.1.3 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการเปลี่ยนแปลงพารามิเตอร์เพื่อเป็นตัวแปรต้นในการทดสอบสมมติฐาน คือ ค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณ ในระดับชั้นย่อย Network (Add Drop Filter) (EN2,DE2) โดยกำหนดค่าเป็น 0.1,0.5,0.9 ตามลำดับ

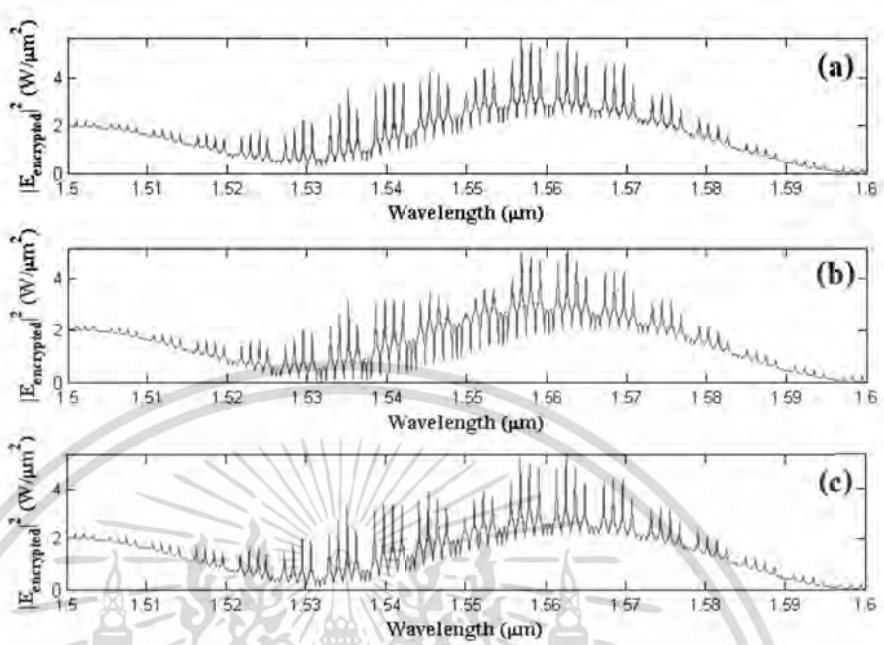
5.3.4 ผลการจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 5.1.1



รูปที่ 5.8 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 5.1.1

จากรูปที่ 5.8 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 5.1.1 รูปที่ 5.8 (a) รูปที่ 5.8 (b) และรูปที่ 5.8 (c) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ของการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล โดยที่ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN2,DE2) เท่ากับ 100, 200, 300 μm ตามลำดับ จากการจำลองพบว่า วงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN2,DE2) พารามิเตอร์ขนาดวงแหวนมีผลต่อสัญญาณจากระดับชั้นย่อย Security ในฝั่งผู้ส่งข้อมูล โดยที่ค่าพารามิเตอร์ที่ใหญ่ขึ้น จะส่งผลให้ค่าพิสัยสเปกตรัมอิสระ (FSR) น้อยลง

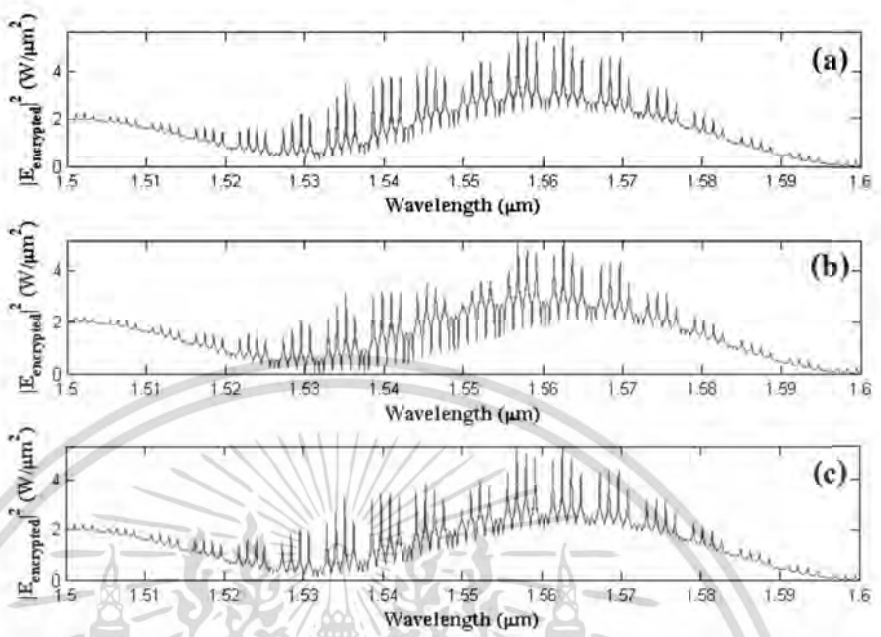
5.3.5 ผลการจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 5.1.2



รูปที่ 5.9 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 5.1.2

จากรูปที่ 5.9 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 5.1.2 รูปที่ 5.9 (a) รูปที่ 5.9 (b) และรูปที่ 5.9 (c) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ของการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล โดยที่สัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN2,DE2) เท่ากับ 0.1, 0.5, 0.9 ตามลำดับ จากการจำลองพบว่า วงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN2,DE2) พารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_1 ไม่มีผลต่อการสร้างสัญญาณ Optical Key อย่างมีนัยสำคัญ กล่าวคือการส่งข้อมูลทำได้อย่างปลอดภัย

5.3.6 ผลการจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 5.1.3



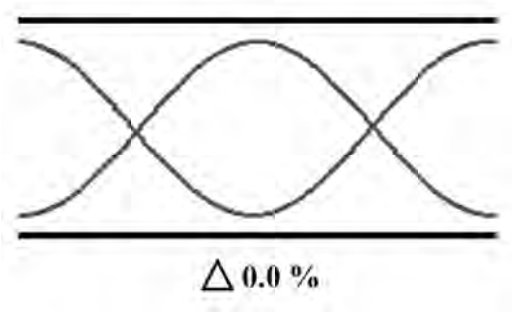
รูปที่ 5.10 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 5.1.3

จากรูปที่ 5.10 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 5.1.3 รูปที่ 5.10 (a) รูปที่ 5.10 (b) และรูปที่ 5.10 (c) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ของการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล โดยที่สัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN2,DE2) เท่ากับ 0.1, 0.5, 0.9 ตามลำดับ จากการจำลองพบว่าวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN2,DE2) พารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_2 ไม่มีผลต่อการสร้างสัญญาณ Optical Key อย่างมีนัยสำคัญ กล่าวคือการส่งข้อมูลทำได้อย่างปลอดภัย

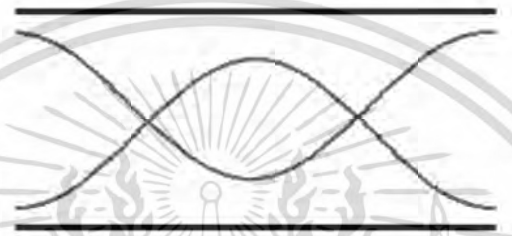
5.4 ข้อจำกัดการทำงานของโปรโตคอลด้านการระบุที่อยู่ภายในเครือข่าย

5.4.1 อธิบายค่าความผิดพลาดของพารามิเตอร์ในฝั่งผู้รับข้อมูลที่สามารถรับข้อมูลได้

จากรูปที่ 3.4 อุปกรณ์ที่เกี่ยวข้องของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงสำหรับการสื่อสารความเร็วสูง และความปลอดภัยสูงโดยใช้อุปกรณ์เชิงแสงทั้งหมดที่นำเสนอ ในฝั่งผู้รับข้อมูลมีการใช้อุปกรณ์เชิงแสงขนาดเล็ก คือ อุปกรณ์ที่ใช้ในการถอดข้อมูลเชิงแสง 2 อุปกรณ์ ในระดับชั้นย่อย Network และระดับชั้นย่อย Security (ซึ่งภายในประกอบด้วยวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter)) และวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ในระดับชั้นย่อย Security โดยในส่วนนี้จะพิจารณาค่าความผิดพลาดของพารามิเตอร์วงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ในฝั่งผู้รับข้อมูลว่ามีค่าความผิดพลาดมากที่สุดเท่าใด ที่โปรโตคอลที่นำเสนอสามารถทำงานได้ โดยเทียบจากพารามิเตอร์ของฝั่งผู้ส่งข้อมูลที่เหมาะสมตามตารางที่ 3.1



รูปที่ 5.11 Eye Diagram กรณีค่าความผิดพลาดของพารามิเตอร์ทั้งหมดเท่ากับ 0

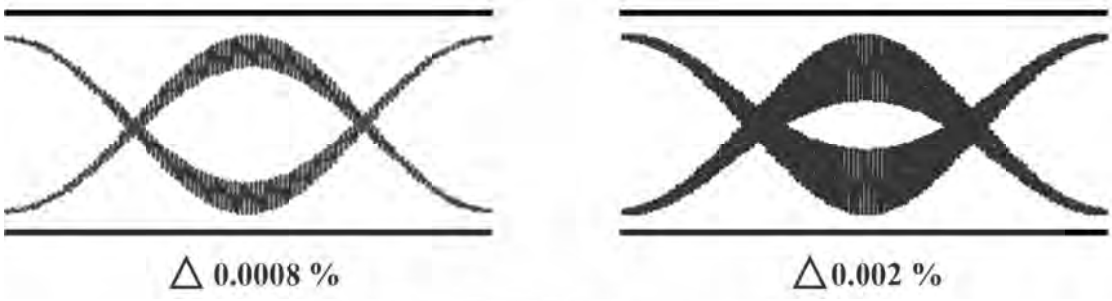


รูปที่ 5.12 Eye Diagram กรณีค่าความผิดพลาดของพารามิเตอร์ที่ทำให้สัญญาณเปลี่ยนแปลง 10 %

จากรูปที่ 5.11 แสดง Eye Diagram กรณีค่าความผิดพลาดของพารามิเตอร์ทั้งหมดเท่ากับ 0 กล่าวคือ ในสภาวะปกติที่การรับส่งถูกต้องไม่มีข้อผิดพลาดรูปแบบดวงตานี้ก็จะเปิดกว้าง ถ้าเกิดมีสัญญาณรบกวน หรือเกิดค่าความผิดพลาดของพารามิเตอร์ของฝั่งผู้รับข้อมูล จะทำให้รูปแบบดวงตานี้ปิดลง การวัดโดยการดูรูปแบบดวงตาของ Eye Diagram เป็นวิธีที่ดีวิธีหนึ่งในการตรวจสอบคุณภาพของสัญญาณที่รับได้

จากรูปที่ 5.12 แสดง Eye Diagram กรณีค่าความผิดพลาดของพารามิเตอร์ที่ทำให้สัญญาณเปลี่ยนแปลง 10 % โดยที่กำหนดให้สัญญาณที่ผู้รับข้อมูลรับสัญญาณได้เปลี่ยนแปลง 10 % จากสัญญาณที่ผู้ส่งข้อมูลส่งมา เป็นสัญญาณที่มีความผิดพลาดมากที่สุดที่ผู้รับสามารถรับแล้วสามารถนำสัญญาณที่รับได้ไปใช้งานได้ กล่าวคือเป็น Eye Diagram กรณีค่าความผิดพลาดของสัญญาณที่ผู้รับสามารถรับได้แล้วสามารถนำสัญญาณที่รับได้ไปทำงานต่อได้ โดยวิทยานิพนธ์นี้ จำลองเครือข่ายเพื่อหาค่าความผิดพลาดของพารามิเตอร์ของฝั่งผู้รับข้อมูลมากที่สุด ที่ยังสามารถนำสัญญาณที่รับได้ไปทำงานต่อได้ โดยเปรียบเทียบให้อยู่ในขอบเขตของ Eye Diagram ตามรูปที่ 5.12

5.4.2 ค่าความผิดพลาดของพารามิเตอร์ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณ (DE2) ในระดับชั้นย่อย Network ที่สามารถรับข้อมูลได้

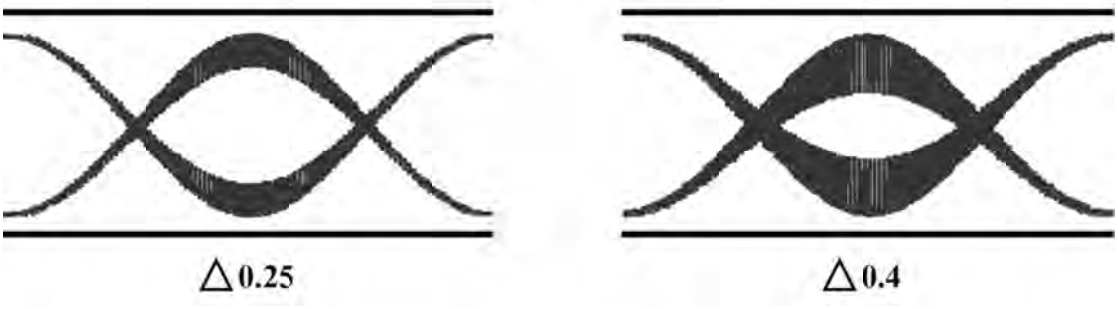


รูปที่ 5.13 Eye Diagram กรณีมีค่าความผิดพลาดของพารามิเตอร์ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณ (DE2) ในระดับชั้นย่อย Network

จากหัวข้อ 5.4.1 อธิบายค่าความผิดพลาดของพารามิเตอร์ในฝั่งผู้รับข้อมูลที่สามารถรับข้อมูลได้ และจากรูปที่ 5.13 แสดง Eye Diagram กรณีมีค่าความผิดพลาดของพารามิเตอร์ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณ (DE2) ในระดับชั้นย่อย Network พบว่า ค่าความผิดพลาดมากที่สุดของพารามิเตอร์ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณ (DE2) ที่โปรโตคอลที่นำเสนอสามารถทำงานได้ เท่ากับ 0.0008 %

รูปที่ 5.14 Eye Diagram กรณีมีค่าความผิดพลาดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณ (DE2) ในระดับชั้นย่อย Network

จากหัวข้อ 5.4.1 อธิบายค่าความผิดพลาดของพารามิเตอร์ในฝั่งผู้รับข้อมูลที่สามารถรับข้อมูลได้ และจากรูปที่ 5.14 แสดง Eye Diagram กรณีมีค่าความผิดพลาดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณ (DE2) ในระดับชั้นย่อย Network พบว่า ค่าความผิดพลาดมากที่สุดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณ (DE2) ที่โปรโตคอลที่นำเสนอสามารถทำงานได้ เท่ากับ 0.25



รูปที่ 5.15 Eye Diagram กรณีมีค่าความผิดพลาดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณ (DE2) ในระดับชั้นย่อย Network

จากหัวข้อ 5.4.1 อธิบายค่าความผิดพลาดของพารามิเตอร์ในฝั่งผู้รับข้อมูลที่สามารถรับข้อมูลได้ และจากรูปที่ 5.15 แสดง Eye Diagram กรณีมีค่าความผิดพลาดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณ (DE2) ในระดับชั้นย่อย Network พบว่า ค่าความผิดพลาดมากที่สุดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณ (DE2) ที่โปรโตคอลที่นำเสนอสามารถทำงานได้ เท่ากับ 0.25

5.5 อภิปรายสรุปการระบุที่อยู่ภายในเครือข่ายด้วยโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ

ในบทนี้เป็นการอธิบายการระบุที่อยู่ภายในเครือข่ายด้วยโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ พัฒนาวิธีการที่เรียกว่า ที่อยู่เชิงแสง (Optical Address) เนื่องจากต้องการให้โปรโตคอลนี้สามารถระบุที่อยู่ภายในเครือข่ายได้และทำงานด้วยอุปกรณ์เชิงแสงทั้งหมด โดยการใช้ Bright Soliton แทนบุคคลในเครือข่าย อีกทั้งการใช้งานที่อยู่เชิงแสง (Optical Address) เพื่อแยกเครือข่ายการสื่อสาร คือ บุคคลที่มีการใช้ที่อยู่เชิงแสง (Optical Address) ที่มีศูนย์กลางช่วงคลื่น (Center Wavelength) ไม่เหมือนกัน เป็นบุคคลที่อยู่คนละเครือข่ายกัน และในทางทฤษฎีจำนวนของที่อยู่เชิงแสง (Optical Address) ที่อยู่ในเครือข่ายเดียวกันมีไม่จำกัด แต่ในทางปฏิบัติจำนวนของบุคคลที่อยู่ในเครือข่ายเดียวกันเท่ากับ 64,000 บุคคล เป็นผลมาจากวิธีการสร้าง Bright Soliton ซึ่งตัวอย่างนี้คำนวนจากวิธีการสร้าง Bright Soliton ตาม [85,86]

ผลของพารามิเตอร์ต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ด้านการระบุที่อยู่ภายในเครือข่าย จากการทดสอบสมมติฐานที่ 5.1 พบว่า วงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN2,DE2) พารามิเตอร์ขนาดวงแหวนกลางและสัมประสิทธิ์การคัปปลิ้งต่าง ๆ ต้องมีความเหมาะสมเพื่อให้สัญญาณที่ถูกเข้ารหัส (Encrypted Signal) เหมาะสม แต่จะไม่ส่งผลทำให้การสื่อสารของภายในเครือข่ายผิดพลาด เนื่องจากมีฝั่งผู้ส่งข้อมูลมีการห่อหุ้มเชิงแสง (Optical Encapsulation) และฝั่งผู้รับข้อมูลมีการถอดข้อมูลเชิงแสง (Opical De-Encapsulation) ซึ่งมีผลของการทำงานคล้ายกับตรงข้ามกัน

ข้อจำกัดการทำงานของโปรโตคอลด้านการระบุที่อยู่ภายในเครือข่าย ค่าความผิดพลาดมากที่สุดของวงแหวนเพิ่มและลดสัญญาณในระดับชั้นย่อย Network (DE2) ที่ผู้รับข้อมูลสามารถรับข้อมูล

ได้ คือพารามิเตอร์ขนาดวงแหวนเท่ากับ 0.0008 % ค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 เท่ากับ 0.25 ค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 เท่ากับ 0.25

บทที่ 6
ความปลอดภัยในการส่งข้อมูลของโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ

ในส่วนของบทนี้เป็นการกล่าวถึงความปลอดภัยในการส่งข้อมูลของโปรโตคอลที่นำเสนอ อธิบายการซ่อนกุญแจและการกู้คืนกุญแจ (Key Suppression and Recovery) เครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) ผลของพารามิเตอร์ต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ด้านความปลอดภัยในการส่งข้อมูล และข้อจำกัดการทำงานของโปรโตคอลด้านความปลอดภัยในการส่งข้อมูล รวมถึงอธิบายการป้องกันการโจมตีด้วยโปรโตคอลที่นำเสนอ โดยมีหัวข้อต่าง ๆ ดังนี้

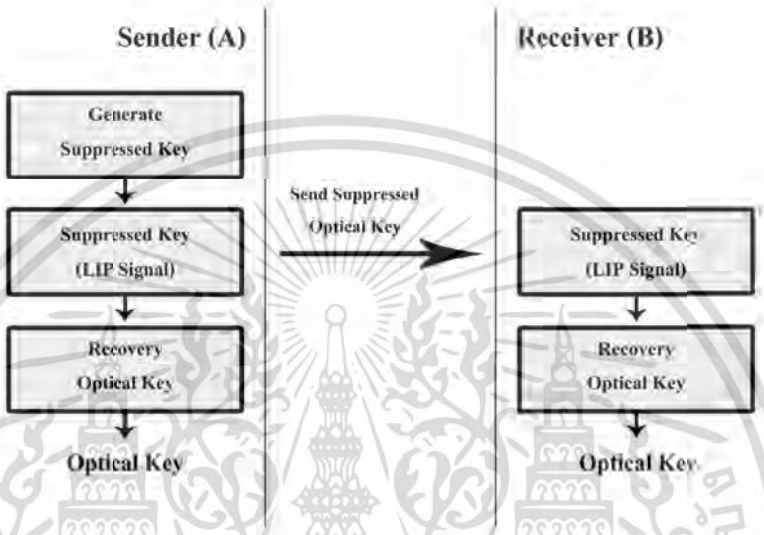
- ปัญหาและประเด็นสำคัญ
- อธิบายการซ่อนกุญแจและการกู้คืนกุญแจ (Key Suppression and Recovery)
  - ความหมายและลักษณะสำคัญของสัญญาณรูปปาก (LIP Signal)
  - ข้อสำคัญที่ทำให้เกิดสัญญาณรูปปาก (LIP Signal)
  - ความหมายและลักษณะสำคัญของกุญแจเชิงแสง
- อธิบายเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel)
  - ความหมายของเครือข่ายส่วนตัวเสมือนเชิงแสง
- ผลของพารามิเตอร์ต่อสัญญาณที่ถูกเข้ารหัสด้านความปลอดภัยในการส่งข้อมูล
- ข้อจำกัดการทำงานของโปรโตคอลด้านความปลอดภัยในการส่งข้อมูล
- อธิบายการป้องกันการโจมตีของโปรโตคอลที่นำเสนอ
- อภิปรายสรุปความปลอดภัยในการส่งข้อมูลของโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ

6.1 ปัญหาและประเด็นสำคัญ

ในส่วนของหัวข้อนี้กล่าวถึงความปลอดภัยในการส่งข้อมูลของโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ ซึ่งวิทยานิพนธ์นี้พัฒนาด้านความปลอดภัย 2 เรื่องคือ การซ่อนกุญแจและการกู้คืนกุญแจ (Key Suppression and Recovery) และเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) โดยมีภาพรวมดังนี้

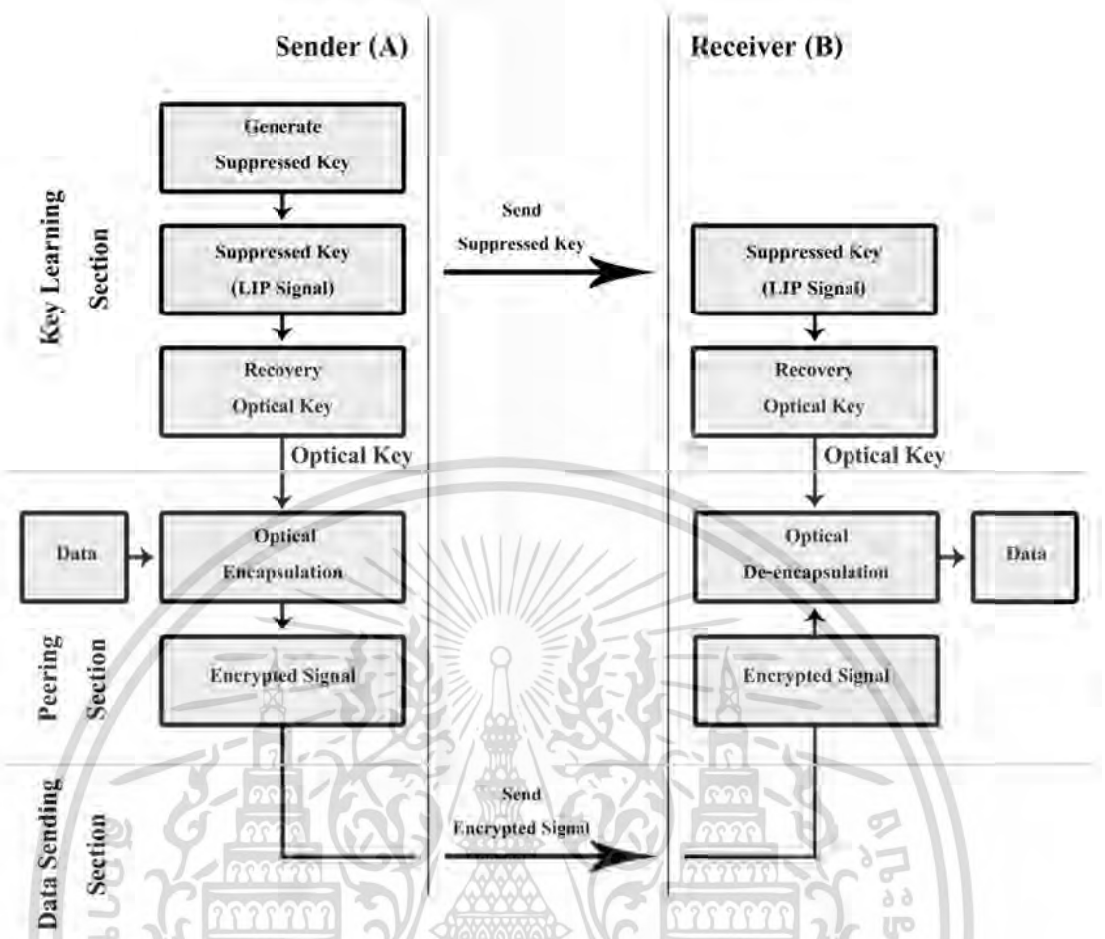
การซ่อนกุญแจและการกู้คืนกุญแจ (Key Suppression and Recovery) ในการพัฒนาโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงสำหรับการสื่อสารความเร็วสูงและความปลอดภัยสูงที่นำเสนอในงานวิจัยนี้ ให้ความสำคัญกับความปลอดภัยของการสื่อสารข้อมูล โดยการสื่อสารข้อมูลมีการใช้กุญแจเชิงแสง (Optical Key) สำหรับการเข้ารหัสในการสื่อสารเพื่อสร้างเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) ในการส่งกุญแจเชิงแสง (Optical Key) จากผู้ส่งข้อมูลไปยังผู้รับข้อมูลเป็นส่วนหนึ่งที่มีความสำคัญมาก กล่าวคือ ถ้าวิธีการส่งกุญแจเชิงแสง (Optical Key) ระหว่างผู้ส่งข้อมูลกับผู้รับข้อมูลไม่ปลอดภัย จะส่งผลให้เกิดปัญหา Man in The Middle ได้ ทำให้ข้อมูลถูกขโมยจากผู้ไม่หวังดีได้ง่ายมากขึ้น ในงานวิจัยนี้ มีการพัฒนาวิธีการส่งกุญแจเชิงแสง (Optical Key) ที่มีความปลอดภัยสูง เพื่อให้ข้อมูลที่ส่งด้วยกุญแจเชิงแสง (Optical Key) นี้ มีความ

ปลอดภัยสูงขึ้นตามไปด้วย โดยที่ผู้ส่งข้อมูลจะใช้วิธีการซ่อนกุญแจเชิงแสง (Optical Key) ไปกับสัญญาณรูปปาก (LIP Signal) ซึ่งสัญญาณรูปปากจะเหมือนกับสัญญาณที่มีสัญญาณรบกวนครอบอยู่ (จะกล่าวถึงในส่วนถัดไป) และทางผู้รับข้อมูลสามารถกู้คืนกุญแจเชิงแสงจากสัญญาณรูปปาก (LIP Signal) ได้ เพื่อที่ทำให้ทั้งฝั่งผู้ส่งข้อมูลและฝั่งผู้รับข้อมูลสามารถนำกุญแจเชิงแสง (Optical Key) ไปใช้ในการส่งข้อมูลที่ปลอดภัยระหว่างกันได้ อธิบายได้ดังรูปที่ 6.1 แผนภาพแสดงหลักการทำงานของการซ่อนกุญแจ การกู้คืนกุญแจและการเข้ารหัสข้อมูล ดังนี้



รูปที่ 6.1 แผนภาพแสดงหลักการทำงานของการซ่อนกุญแจและการกู้คืนกุญแจ

เครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) ในการพัฒนาโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงสำหรับการสื่อสารความเร็วสูงและความปลอดภัยสูงที่นำเสนอในงานวิจัยนี้ ให้ความสำคัญกับความปลอดภัยของการสื่อสารข้อมูล ซึ่งมีวิธีการซ่อนกุญแจและการกู้คืนกุญแจสำหรับการส่งข้อมูล (Key Suppression and Recovery) ที่ได้กล่าวมาแล้วนั้น โดยที่กุญแจที่ถูกซ่อนโดยฝั่งผู้ส่งข้อมูลและกุญแจที่ถูกกู้โดยฝั่งผู้รับข้อมูล ถูกนำไปใช้ในการสร้างเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) เพื่อให้การส่งข้อมูลระหว่างผู้ส่งกับผู้รับข้อมูลมีความปลอดภัยสูง อีกทั้งเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) สามารถเปลี่ยนแปลงกุญแจที่ใช้ในการสร้างเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) ได้ เพื่อให้ความปลอดภัยในการส่งข้อมูลมีสูงมากขึ้น



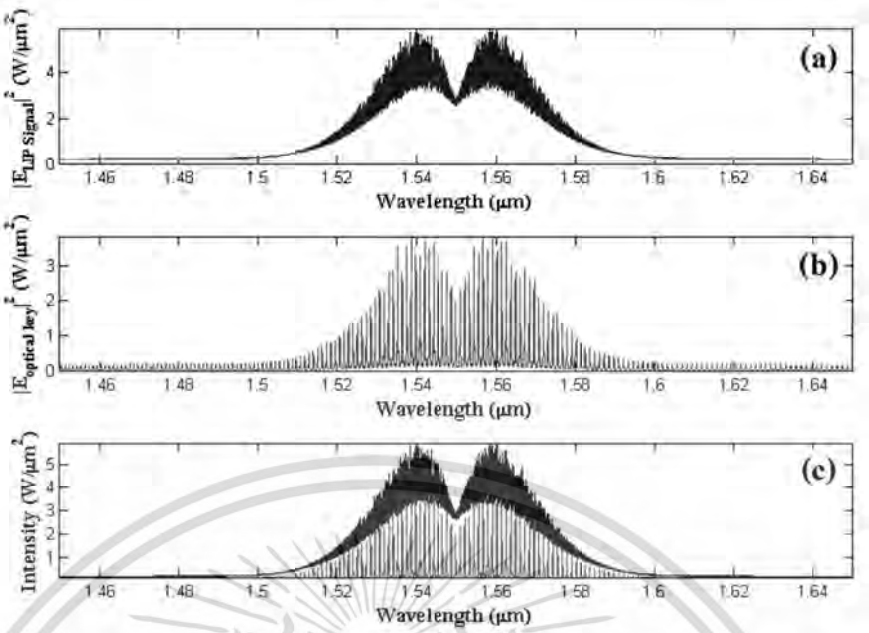
รูปที่ 6.2 แผนภาพแสดงหลักการทำงานของเครือข่ายส่วนตัวเสมือนเชิงแสง

จากรูปที่ 6.2 แผนภาพแสดงหลักการทำงานของเครือข่ายส่วนตัวเสมือนเชิงแสงแสดงให้เห็นว่า ระหว่างผู้ส่งข้อมูลและผู้รับข้อมูลมีการส่งข้อมูลที่ถูกเข้ารหัสด้วยกุญแจเชิงแสง (Optical Key) ทำให้เหมือนกับว่า ระหว่างผู้ส่งข้อมูลและผู้รับข้อมูลมีการส่งข้อมูลที่มีความเป็นส่วนตัวและมีความปลอดภัยสูงมากขึ้น จากการที่สามารถเปลี่ยนกุญแจที่ใช้ในการสร้างเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) ได้ด้วยวิธีการส่งกุญเชิงแสง (Optical Key) ที่มีความปลอดภัย คือการการซ่อนกุญแจและการกู้คืนกุญแจสำหรับการส่งข้อมูล (Key Suppression and Recovery)

6.2 อธิบายการซ่อนกุญแจและการกู้คืนกุญแจ (Key Suppression and Recovery)

6.2.1 ความหมายและลักษณะสำคัญของสัญญาณรูปปาก (LIP Signal)

จากรูปที่ 6.1 แผนภาพแสดงหลักการทำงานของการซ่อนกุญแจและการกู้คืนกุญแจ การซ่อนกุญแจเชิงแสง (Optical Key) จากผู้ส่งข้อมูลไปยังผู้รับข้อมูล ถูกซ่อนไปในสัญญาณรูปปาก (LIP Signal) หรือ Suppressed Key โดยที่สัญญาณรูปปาก (LIP Signal) มีลักษณะดังนี้



รูปที่ 6.3 สัญญาณรูปปาก (LIP Signal)

สัญญาณรูปปาก (LIP Signal) หรือ Suppressed Key หมายถึง สัญญาณที่สร้างจากอุปกรณ์วงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) ตามรูปที่ 2.18 โดยมีลักษณะ Noiselike รูปปากเพื่อใช้ในการซ่อนข้อมูลภายในปากตามรูปที่ 6.3 ซึ่งนำเสนอเพื่อใช้งานทางด้านความปลอดภัยในการสื่อสาร เช่น ภาคผนวก ก [1,2,4,5,6,9,10]

วิทยานิพนธ์นี้ใช้สัญญาณรูปปาก (LIP Signal) เพื่อให้วิธีการซ่อนกุญแจเชิงแสงและการกู้คืนกุญแจเชิงแสง (Optical Key Suppression and Recovery) มีประสิทธิผลยากต่อการเกิดปัญหา Man in The Middle เนื่องจากสัญญาณรูปปาก (LIP Signal) มีลักษณะ Noiselike โดยที่ผู้รับข้อมูลต้องทราบถึงวิธีการกู้คืนกุญแจเชิงแสง (Optical Key) จากสัญญาณรูปปาก (LIP Signal) เท่านั้น จึงจะสามารถทราบถึงกุญแจเชิงแสง (Optical Key) ที่ผู้ส่งข้อมูลใช้ในการส่งข้อมูลได้

6.2.2 ข้อสำคัญที่ทำให้เกิดสัญญาณรูปปาก (LIP Signal)

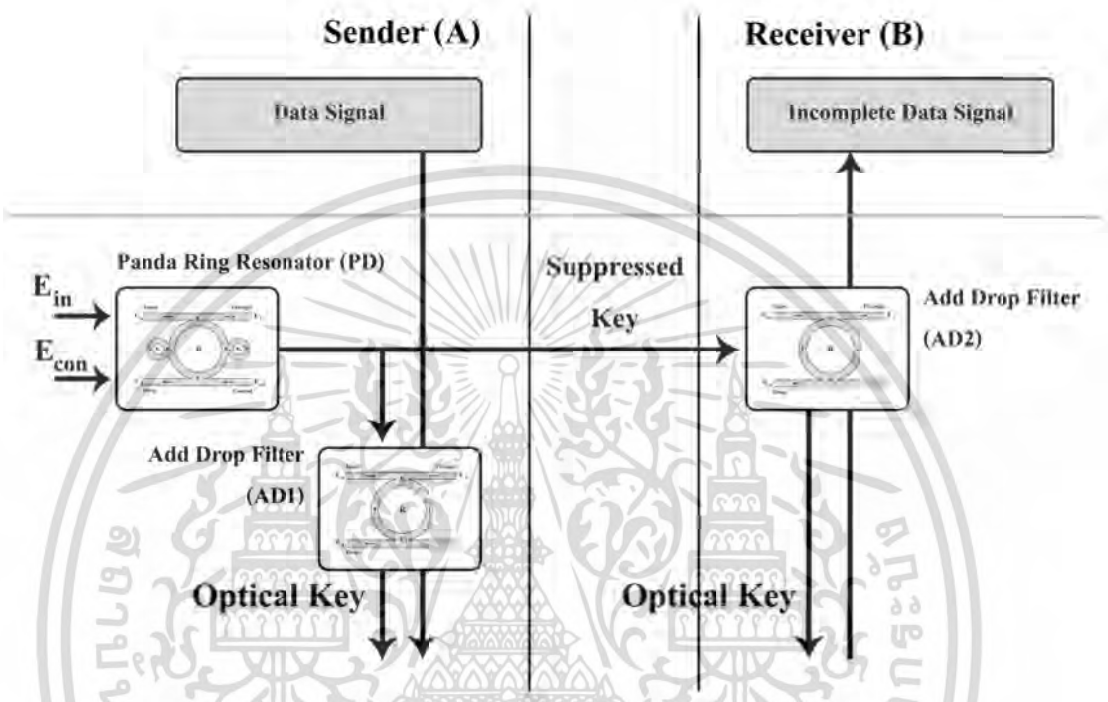
สัญญาณรูปปาก (LIP Signal) เกิดจากการนำสัญญาณ Bright Soliton เข้าทาง Input Port วงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) และนำสัญญาณ Dark Soliton เข้าทาง Control Port วงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) เท่านั้น โดยที่พารามิเตอร์ของวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) และพารามิเตอร์ของสัญญาณ Soliton จะต้องมีความเหมาะสม ซึ่งจะกล่าวถัดไป

6.2.3 ความหมายและลักษณะสำคัญของกุญแจเชิงแสง

กุญแจเชิงแสง (Optical Key) หมายถึง ข้อมูลสัญญาณแสงที่นำไปใช้ในการเข้ารหัสเชิงแสง (Optical Cryptography) โดยเป็นข้อมูลสัญญาณแสงที่ผ่านวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) เพื่อให้ข้อมูลสัญญาณแสงเป็นแบบสุ่มตามภาคผนวก ก [2] และ [50]

6.2.4 วิธีการซ่อนกุญแจและการกู้คืนกุญแจสำหรับการส่งข้อมูล

วิธีการซ่อนกุญแจและการกู้คืนกุญแจสำหรับการส่งข้อมูล (Key Suppression and Recovery) ทำได้โดยใช้หลักการของวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) วงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) และอุปกรณ์ที่ใช้หลักการของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer) อธิบายได้ดังนี้



รูปที่ 6.4 อุปกรณ์ที่ใช้ในการซ่อนกุญแจเชิงแสงและการกู้คืนกุญแจเชิงแสง

จากรูปที่ 6.4 (ฝั่ง Sender (A)) เป็นการแสดงอุปกรณ์ใช้ในการซ่อนกุญแจเชิงแสงซึ่งประกอบด้วยวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) (รูปที่ 2.18) วงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (รูปที่ 2.17) และอุปกรณ์ที่ใช้หลักการของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer) (รูปที่ 2.19) และจากรูปที่ 6.4 (ฝั่ง Receiver (B)) เป็นการแสดงอุปกรณ์ที่ใช้ในที่ใช้ในการกู้คืนกุญแจเชิงแสงประกอบด้วยวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (รูปที่ 2.17) และอุปกรณ์ที่ใช้หลักการของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer) (รูปที่ 2.19) ซึ่งมีวิธีการดังนี้

วิธีการซ่อนกุญแจเชิงแสง (Optical Key Suppression)

(จากรูปที่ 6.4 Sender (A) ต้องการซ่อน Optical Key ให้ Receiver (B))

<u>ขั้นตอนที่ 1</u> : นำสัญญาณ E_{in} (Bright Soliton) เข้าทาง Input Port ของวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator)

<u>ขั้นตอนที่ 2</u> : นำสัญญาณ E_{con} (Dark Soliton) เข้าทาง Control Port ของวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator)

ขั้นตอนที่ 3 : สัญญาณที่ออกจาก Through Port ของวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) คือ สัญญาณกุญแจที่ถูกซ่อนด้วยสัญญาณรูปปากซึ่งจะถูกส่งให้กับให้ Receiver (B) เพื่อกู้คืนกุญแจเชิงแสง

ขั้นตอนที่ 4 : Sender (A) นำสัญญาณกุญแจที่ถูกซ่อนด้วยสัญญาณรูปปากเข้าทาง Input Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter)

ขั้นตอนที่ 5 : สัญญาณที่ออกจาก Drop Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) คือ กุญแจเชิงแสง (Optical Key) ที่ถูกส่งให้ Receiver (B)

วิธีการกู้คืนกุญแจเชิงแสง (Optical Key Recovery)

(จากรูปที่ 6.4 Receiver (B) ต้องการกู้คืนกุญเชิงแสงที่ซ่อนมาด้วยสัญญาณรูปปาก)

ขั้นตอนที่ 1 : Receiver (B) นำสัญญาณกุญแจที่ถูกซ่อนด้วยสัญญาณรูปปาก (LIP Signal) เข้าทาง Input Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter)

ขั้นตอนที่ 2 : สัญญาณที่ออกจาก Drop Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) คือ กุญแจเชิงแสง (Optical Key) ที่ Sender (A) ส่งให้ Receiver (B)

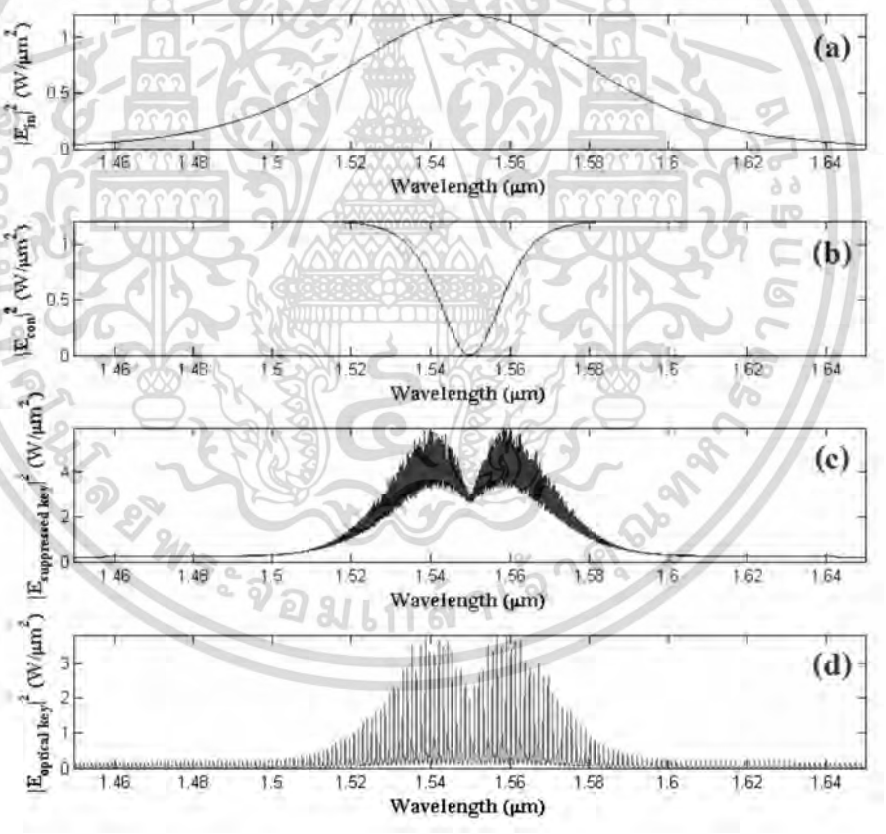
6.2.5 ผลการจำลอง

ในหัวข้อนี้เป็นการจำลองวิธีการซ่อนกุญแจเชิงแสง (Optical Key Suppression) และวิธีการกู้คืนกุญแจเชิงแสง (Optical Key Recovery) โดยยกตัวอย่างการจำลองการส่งกุญแจเชิงแสง (Optical Key) จากผู้ส่งไปยังผู้รับ โดยมีแผนภาพแสดงอุปกรณ์เชิงแสงในการจำลองการซ่อนและการกู้คืนเชิงแสงตามรูปที่ 6.4 โดยผู้ส่งต้องการส่งกุญแจเชิงแสง (Optical Key) 1 ชุด ให้กับผู้รับโดยกุญแจเชิงแสง (Optical Key) ที่ส่งเหมือนกับถูกซ่อนด้วยสัญญาณรูปปาก (LIP Signal) รวมถึงมีพารามิเตอร์ที่ใช้ในการจำลองตามตารางที่ 6.1 โดยมีรายละเอียดการจำลองดังนี้

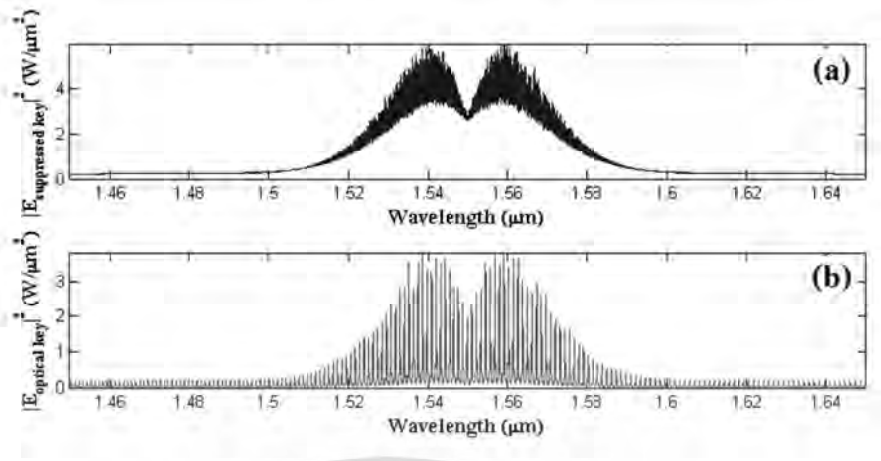
ตารางที่ 6.1 พารามิเตอร์ที่ใช้ในการจำลองวิธีการซ่อนกุญแจเชิงแสง (Optical Key Suppression) และวิธีการกู้คืนกุญแจเชิงแสง (Optical Key Recovery)

อุปกรณ์ , สัญญาณ	พารามิเตอร์	ค่าพารามิเตอร์
ทุกอุปกรณ์	ชนิดของวัสดุ	InGaAsP/InP
	ค่าดัชนีหักเหเชิงเส้นของตัวนำคลื่น : n_0	3.4
	ค่าดัชนีหักเหไม่เชิงเส้นของตัวนำคลื่น : n_2	1.3×10^{-13} m^2/W
	การสูญเสียภายในตัวนำคลื่น : α	0.05 dB mm^{-1}
	ค่าการสูญเสียความเข้มแสงเนื่องจากคัปปลิ้ง : γ	0.01
	ขนาดพื้นที่หน้าตัดของตัวนำคลื่น : A_{eff}	0.25 μm^2
Panda Ring Resonator (PD)	ขนาดวงแหวนกลาง	200 μm
	ขนาดวงแหวนข้างซ้ายและข้างขวา	15 μm
	สัมประสิทธิ์การคัปปลิ้ง κ_1	0.2

อุปกรณ์ , สัญญาณ	พารามิเตอร์	ค่าพารามิเตอร์
	สัมประสิทธิ์การคัปปลิ้ง κ_2	0.2
	สัมประสิทธิ์การคัปปลิ้ง κ_3	0.1
	สัมประสิทธิ์การคัปปลิ้ง κ_4	0.1
Add Drop Filter (AD1,AD2)	ขนาดวงแหวน	200 μm
	สัมประสิทธิ์การคัปปลิ้ง κ_1	0.5
	สัมประสิทธิ์การคัปปลิ้ง κ_2	0.2
สัญญาณ	ศูนย์กลางช่วงคลื่น : λ_0	1.55 μm
	ความเข้มสัญญาณ Input ที่ PD (Input) : E_{in}	1.2 W/μm^2
	ความเข้มสัญญาณ Input ที่ PD (Control) : E_{con}	1.2 W/μm^2



รูปที่ 6.5 ผลการจำลองของฝั่งผู้ส่งข้อมูล



รูปที่ 6.6 ผลการจำลองของฝั่งผู้รับข้อมูล

จากรูปที่ 6.5 ผลการจำลองของฝั่งผู้ส่งข้อมูล รูปที่ 6.5 (a) และรูปที่ 6.5 (b) แสดงสัญญาณ E_{in} และ E_{con} ตามลำดับ ซึ่งเป็นสัญญาณที่ส่งเข้าทาง Input Port และ Control Port ของวงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) เพื่อใช้ในการสร้างสัญญาณรูปปาก (LIP Signal) ทาง Through Port ตามรูปที่ 6.5 (c) โดยที่สัญญาณนี้คือสัญญาณกุญแจเชิงแสงที่ถูกซ่อนมาด้วยสัญญาณลักษณะสัญญาณรบกวน (Noise like) ซึ่งสัญญาณนี้จะใช้ในการส่งจากผู้ส่งข้อมูล Sender (A) ไปยังผู้รับข้อมูล Receiver (B) ทำให้การแลกเปลี่ยนกุญแจระหว่างผู้ส่งข้อมูลและผู้รับข้อมูลเป็นไปอย่างปลอดภัย รูปที่ 6.5 (d) แสดงสัญญาณกุญแจเชิงแสง (Optical Key) ที่เกิดจากการนำสัญญาณรูปปาก (LIP Signal) เข้าทาง Input Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) และที่ Drop Port คือ สัญญาณกุญแจเชิงแสง (Optical Key) ที่สามารถนำไปใช้การเข้ารหัสข้อมูลได้

จากรูปที่ 6.6 ผลการจำลองของฝั่งผู้รับข้อมูล รูปที่ 6.6 (a) แสดงสัญญาณรูปปาก (LIP Signal) ที่ได้รับจาก Sender (A) รูปที่ 6.6 (b) แสดงสัญญาณกุญแจเชิงแสง (Optical Key) ที่เกิดจากการนำสัญญาณรูปปาก (LIP Signal) เข้าทาง Input Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) และที่ Drop Port คือ สัญญาณกุญแจเชิงแสง (Optical Key) ที่สามารถนำไปใช้การสื่อสารข้อมูลได้

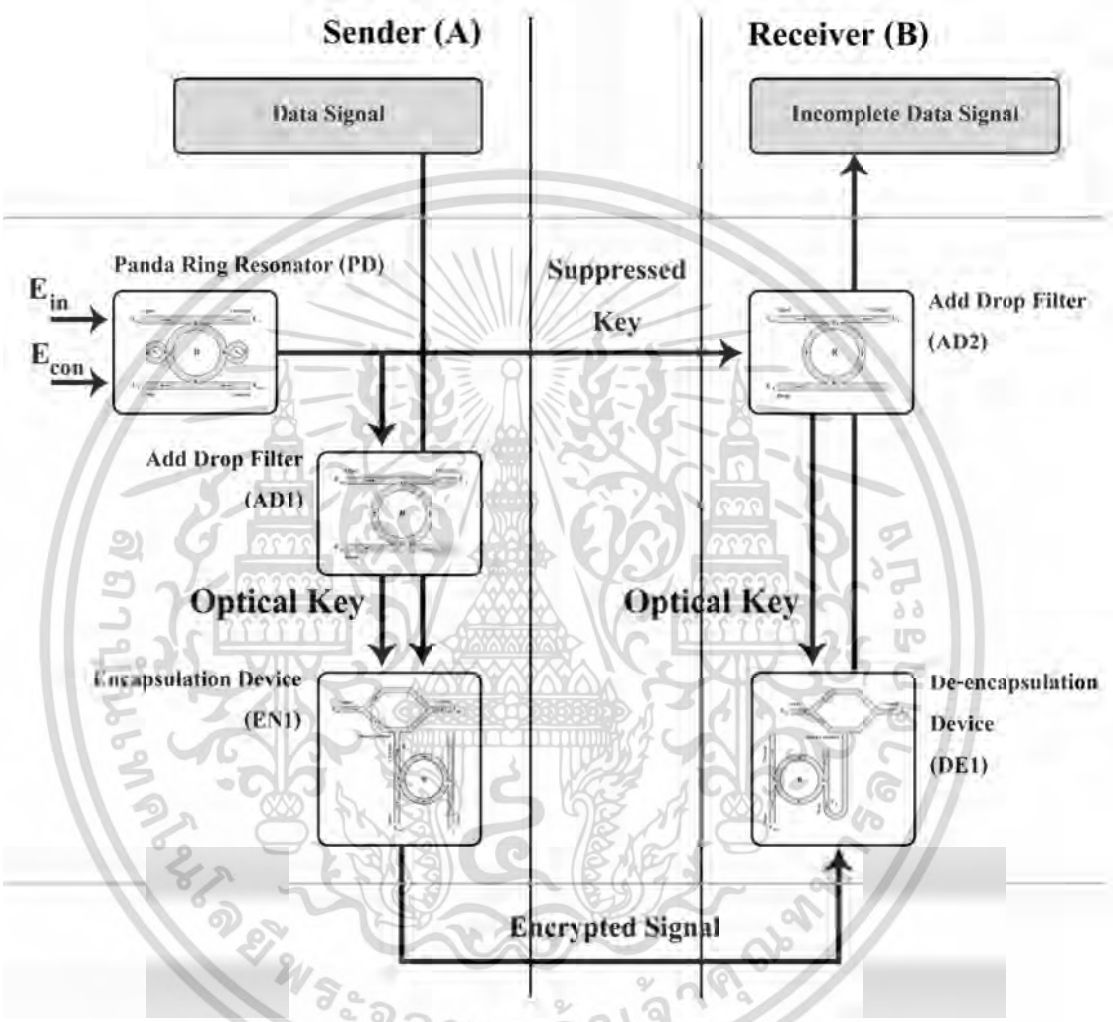
6.3 อธิบายเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel)

6.3.1 ความหมายของเครือข่ายส่วนตัวเสมือนเชิงแสง

เครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) หมายถึง ช่องทางในการสื่อสารเชิงแสงเสมือนจากผู้ส่งข้อมูลไปยังผู้รับข้อมูลโดยตรง โดยเป็นช่องทางที่มีการเข้ารหัสเชิงแสง (Optical Cryptography) ด้วยกุญแจเชิงแสง (Optical Key) ทำให้ช่องทางในการสื่อสารเชิงแสงเสมือนคล้ายกับท่อของการส่งข้อมูลที่มีรูปแบบของท่อเป็นกุญแจเชิงแสง (Optical Key) ข้อมูลที่ต้องการส่งเสมือนกับส่งเข้าไปในท่อดังกล่าวที่มีการเข้ารหัสอย่างปลอดภัย

6.3.2 วิธีการส่งข้อมูลด้วยเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel)

วิธีการส่งข้อมูลด้วยเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) ทำได้โดยใช้หลักการของวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) วงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) และอุปกรณ์ที่ใช้หลักการของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer) อธิบายได้ดังนี้



รูปที่ 6.7 อุปกรณ์ที่ใช้ในการส่งและรับข้อมูลด้วยเครือข่ายส่วนตัวเสมือนเชิงแสง

จากรูปที่ 6.7 (ฝั่ง Sender (A)) เป็นการแสดงอุปกรณ์ที่ใช้ในการส่งข้อมูลด้วยเครือข่ายส่วนตัวเสมือนเชิงแสง : ฝั่งผู้ส่งข้อมูลซึ่งประกอบด้วยวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) (รูปที่ 2.18) วงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (รูปที่ 2.17) และอุปกรณ์ที่ใช้หลักการของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer) (รูปที่ 2.19) และจากรูปที่ 6.7 (ฝั่ง Receiver (B)) เป็นการแสดงอุปกรณ์ที่ใช้ในการส่งข้อมูลด้วยเครือข่ายส่วนตัวเสมือนเชิงแสง : ฝั่งผู้รับข้อมูล ประกอบด้วยวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (รูปที่ 2.17) และอุปกรณ์ที่ใช้หลักการของมัค-เซนเดอร์ อินเตอร์เฟียร์โรมิเตอร์ (Mach-Zehnder Interferometer) (รูปที่ 2.19) ซึ่งมีวิธีการดังนี้

วิธีการส่งข้อมูลด้วยเครือข่ายส่วนตัวเสมือนเชิงแสง : ฝั่งผู้ส่งข้อมูล

(จากรูปที่ 6.7 Sender (A) ต้องการส่งข้อมูลให้ Receiver (B) ด้วยเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel))

ขั้นตอนที่ 1 : Sender (A) ใช้การซ่อนกุญแจเชิงแสง (Optical Key Suppression) เพื่อสร้างกุญแจเชิงแสง (Optical Key) ในการสื่อสารข้อมูล และส่งสัญญาณกุญแจที่ถูกซ่อนด้วยสัญญาณรูปปากให้ Receiver (B)

ขั้นตอนที่ 2 : นำกุญแจเชิงแสง (Optical Key) ที่ได้จากการซ่อนกุญแจเชิงแสง (Optical Key Suppression) ห่อหุ้มเชิงแสง (Optical Encapsulation) กับข้อมูลที่ต้องการส่งให้ Receiver (B)

ขั้นตอนที่ 3 : ผลของสัญญาณจากขั้นตอนที่ 2 คือสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่ส่งให้ Receiver (B)

วิธีการส่งข้อมูลด้วยเครือข่ายส่วนตัวเสมือนเชิงแสง : ฝั่งผู้รับข้อมูล

(จากรูปที่ 6.7 Receiver (B) ต้องการรับข้อมูลจาก Sender (A) ที่ส่งข้อมูลมาด้วยเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel))

ขั้นตอนที่ 1 : Receiver (B) รับสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) จาก Sender (A)

ขั้นตอนที่ 2 : Receiver (B) กู้คืนกุญแจเชิงแสง (Optical Key Recovery) จากสัญญาณกุญแจที่ถูกซ่อนด้วยสัญญาณรูปปากที่ส่งมากจาก Sender (A)

ขั้นตอนที่ 3 : นำสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ถอดข้อมูลเชิงแสง (Optical De-encapsulation) ด้วยกุญแจเชิงแสง (Optical Key) จากขั้นตอนที่ 2

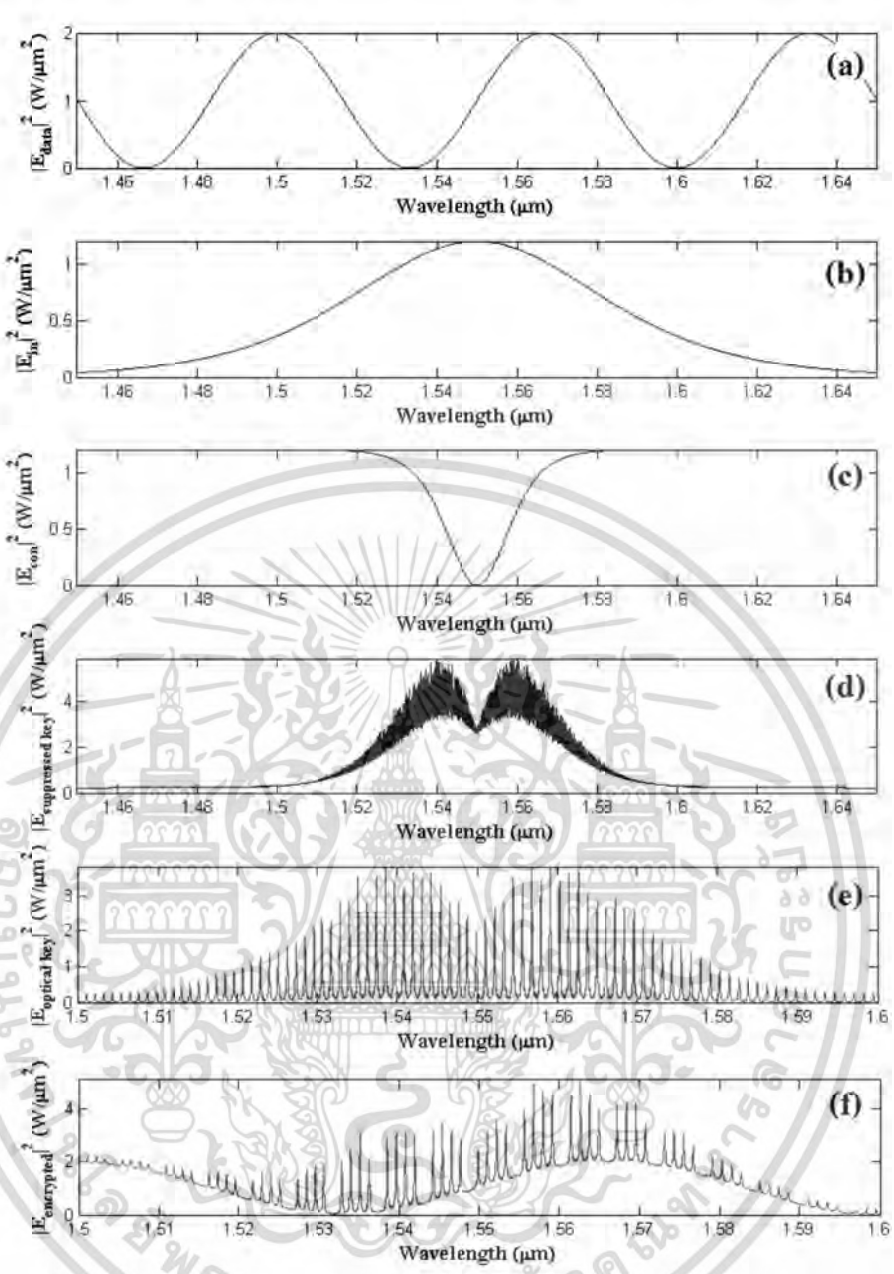
ขั้นตอนที่ 4 : ผลของสัญญาณจากขั้นตอนที่ 3 คือ ข้อมูลที่ส่งจาก Sender (A)

6.3.3 ผลการจำลอง

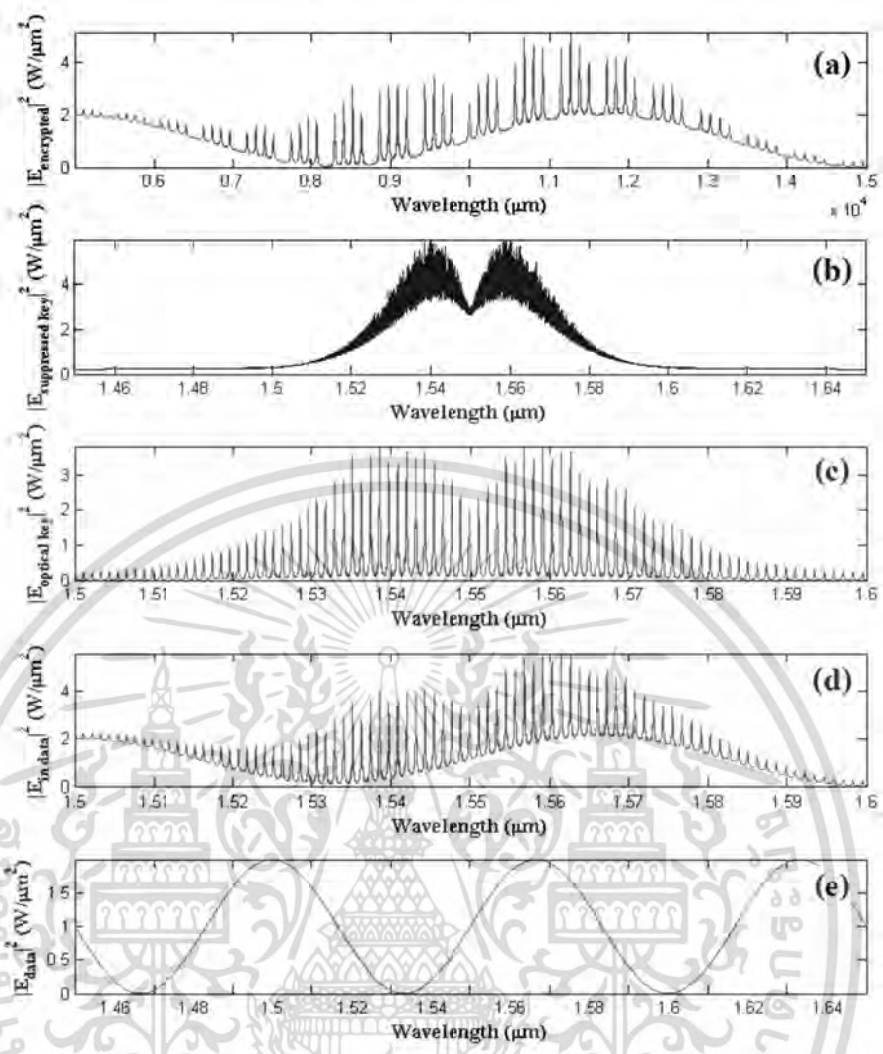
ในหัวข้อนี้เป็นการจำลองวิธีการส่งข้อมูลด้วยเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) โดยยกตัวอย่างการจำลองการส่งกุญแจเชิงแสง (Optical Key) จากผู้ส่งไปยังผู้รับด้วยวิธีการซ่อนกุญแจและการกู้คืนกุญแจสำหรับการส่งข้อมูล (Key Suppression and Recovery) และจากนั้นนำกุญแจดังกล่าวการสร้างครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) โดยมีแผนภาพแสดงอุปกรณ์เชิงแสงในการจำลองวิธีการส่งข้อมูลด้วยเครือข่ายส่วนตัวเสมือนเชิงแสงตามรูปที่ 6.7 รวมถึงมีพารามิเตอร์ที่ใช้ในการจำลองตามตารางที่ 6.2 โดยมีรายละเอียดการจำลองดังนี้

ตารางที่ 6.2 พารามิเตอร์ที่ใช้ในการจำลองวิธีการส่งข้อมูลด้วยเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel)

อุปกรณ์ , สัญญาณ	พารามิเตอร์	ค่าพารามิเตอร์
ทุกอุปกรณ์	ชนิดของวัสดุ	InGaAsP/InP
	ค่าดัชนีหักเหเชิงเส้นของตัวนำคลื่น : n_0	3.4
	ค่าดัชนีหักเหไม่เชิงเส้นของตัวนำคลื่น : n_2	1.3×10^{-13} m^2/W
	การสูญเสียภายในตัวนำคลื่น : α	0.05 dB mm^{-1}
	ค่าการสูญเสียความเข้มแสงเนื่องจากคัปปลิ้ง : γ	0.01
	ขนาดพื้นที่หน้าตัดของตัวนำคลื่น : A_{eff}	0.25 μm^2
Panda Ring Resonator (PD)	ขนาดวงแหวนกลาง	200 μm
	ขนาดวงแหวนข้างซ้ายและข้างขวา	15 μm
	สัมประสิทธิ์การคัปปลิ้ง κ_1	0.2
	สัมประสิทธิ์การคัปปลิ้ง κ_2	0.2
	สัมประสิทธิ์การคัปปลิ้ง κ_3	0.1
	สัมประสิทธิ์การคัปปลิ้ง κ_4	0.1
Add Drop Filter (AD1,AD2)	ขนาดวงแหวน	200 μm
	สัมประสิทธิ์การคัปปลิ้ง κ_1	0.5
	สัมประสิทธิ์การคัปปลิ้ง κ_2	0.2
Add Drop Filter (EN1,DE1)	ขนาดวงแหวน	20 μm
	สัมประสิทธิ์การคัปปลิ้ง κ_1	0.5
	สัมประสิทธิ์การคัปปลิ้ง κ_2	0.5
สัญญาณ	ศูนย์กลางช่วงคลื่น : λ_0	1.55 μm
	ความเข้มสัญญาณ Input ที่ PD (Input) : E_{in}	1.2 $W/\mu m^2$
	ความเข้มสัญญาณ Input ที่ PD (Control) : E_{con}	1.2 $W/\mu m^2$
	ความเข้มสัญญาณ Data	2.0 $W/\mu m^2$



รูปที่ 6.8 ผลการจำลองของฝั่งผู้ส่งข้อมูล



รูปที่ 6.9 ผลการจำลองของฝั่งผู้รับข้อมูล

จากรูปที่ 6.8 ผลการจำลองของฝั่งผู้ส่งข้อมูล รูปที่ 6.8 (a) แสดงสัญญาณข้อมูลที่ Sender (A) ต้องการส่งข้อมูลไปยัง Receiver (B) รูปที่ 6.8 (b) และรูปที่ 6.8 (c) แสดงสัญญาณ E_{in} และ E_{con} ตามลำดับ ซึ่งเป็นสัญญาณที่ส่งเข้าทาง Input Port และ Control Port ของวงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) เพื่อใช้ในการสร้างสัญญาณรูปปาก (LIP Signal) ทาง Through Port ตามรูปที่ 6.8 (d) รูปที่ 6.8 (e) แสดงสัญญาณกุญแจเชิงแสง (Optical Key) ที่เกิดจากการนำสัญญาณรูปปาก (LIP Signal) เข้าทาง Input Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) และที่ Drop Port คือ สัญญาณกุญแจเชิงแสง (Optical Key) ที่นำไปใช้ในการสร้างเครือข่ายส่วนตัวเสมือนเชิงแสง รูปที่ 6.8 (f) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่เกิดจากการห่อหุ้มเชิงแสงระหว่างสัญญาณข้อมูล (รูปที่ 6.8 (a)) กับ สัญญาณกุญแจเชิงแสง (Optical Key) (รูปที่ 6.8 (e)) โดยสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) จะถูกส่งจากผู้ส่งข้อมูลไปยังผู้รับข้อมูลทำให้เสมือนกับเป็นเครือข่ายส่วนตัว กล่าวคือ มีท่อ (Tunnel) ในการสื่อสารเป็นลักษณะสัญญาณกุญแจเชิงแสง (Optical Key)

จากรูปที่ 6.9 ผลการจำลองของฝั่งผู้รับข้อมูล รูปที่ 6.9 (a) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ที่ใช้ในการส่งข้อมูลอย่างปลอดภัยจาก Sender (A) รูปที่ 6.9 (b) แสดงสัญญาณรูปปาก (LIP Signal) ที่ได้รับจาก Sender (A) รูปที่ 6.9 (c) แสดงสัญญาณกุญแจเชิงแสง (Optical Key) ที่เกิดจากการนำสัญญาณรูปปาก (LIP Signal) เข้าทาง Input Port ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) และที่ Drop Port คือ สัญญาณกุญแจเชิงแสง (Optical Key) ที่นำไปใช้ในการถอดข้อมูลจากเครือข่ายสวนตัวเสมือนเชิงแสง รูปที่ 6.9 (d) แสดงสัญญาณข้อมูลจาก Sender (A) ที่ไม่สมบูรณ์ที่เกิดจากการถอดข้อมูลเชิงแสง (Optical De-Encapsulation) ระหว่างสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) (รูปที่ 6.9 (a)) กับกุญแจเชิงแสง (รูปที่ 6.9 (c)) รูปที่ 6.9 (e) แสดงสัญญาณข้อมูลจาก Sender (A) ที่สมบูรณ์ ซึ่งเกิดจากสัญญาณข้อมูลจาก Sender (A) ที่ไม่สมบูรณ์ - กุญแจเชิงแสง (Key) แสดงให้เห็นว่าผู้รับข้อมูลสามารถถอดข้อมูลที่ถูกต้องจากเครือข่ายส่วนตัวเสมือนเชิงแสงได้

6.4 ผลของพารามิเตอร์ต่อสัญญาณที่ถูกเข้ารหัสด้านความปลอดภัยในการส่งข้อมูล

6.4.1 สมมุติฐาน

การทดสอบสมมติฐานที่ 6.1 เพื่อเป็นการทดสอบการทำงานของโปรโตคอลที่นำเสนอ โดยศึกษาผลของพารามิเตอร์ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) ว่ามีผลต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลอย่างไรบ้าง กำหนดสมมติฐานที่ 6.1 ได้ดังนี้ ถ้าพารามิเตอร์ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

สมมติฐานย่อยที่ 6.1.1 ถ้าขนาดวงแหวนกลางของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator (Middle Ring)) ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

สมมติฐานย่อยที่ 6.1.2 ถ้าขนาดวงแหวนข้างของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator (Ear Rings)) ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

สมมติฐานย่อยที่ 6.1.3 ถ้าค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

สมมติฐานย่อยที่ 6.1.4 ถ้าค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

สมมติฐานย่อยที่ 6.1.5 ถ้าค่าสัมประสิทธิ์การคัปปลิ้ง κ_3 หรือ κ_4 ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

การทดสอบสมมติฐานที่ 6.2 เพื่อเป็นการทดสอบการทำงานของโปรโตคอลที่นำเสนอ โดยศึกษาผลของพารามิเตอร์ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ตัวที่ 1 ในระดับชั้นย่อย Security ว่ามีผลต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลอย่างไรบ้าง กำหนดสมมติฐานที่ 6.2 ได้ดังนี้ ถ้าพารามิเตอร์ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ตัวที่ 1 ในระดับชั้นย่อย Security ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

สมมติฐานย่อยที่ 6.2.1 ถ้าขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ตัวที่ 1 ในระดับชั้นย่อย Security ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์

สมมติฐานย่อยที่ 6.2.2 ถ้าค่าสัมประสิทธิ์การคัปปลิ้ง ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ตัวที่ 1 ในระดับชั้นย่อย Security ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

สมมติฐานย่อยที่ 6.2.3 ถ้าค่าสัมประสิทธิ์การคัปปลิ้ง ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ตัวที่ 1 ในระดับชั้นย่อย Security ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

การทดสอบสมมติฐานที่ 6.3 เพื่อเป็นการทดสอบการทำงานของโปรโตคอลที่นำเสนอ โดยศึกษาผลของพารามิเตอร์ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ตัวที่ 2 ในระดับชั้นย่อย Security ว่ามีผลต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลอย่างไรบ้าง กำหนดสมมติฐานที่ 6.3 ได้ดังนี้ ถ้าพารามิเตอร์ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ตัวที่ 2 ในระดับชั้นย่อย Security ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

สมมติฐานย่อยที่ 6.3.1 ถ้าขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ตัวที่ 2 ในระดับชั้นย่อย Security ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

สมมติฐานย่อยที่ 6.3.2 ถ้าค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ตัวที่ 2 ในระดับชั้นย่อย Security ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

สมมติฐานย่อยที่ 6.3.3 ถ้าค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ตัวที่ 2 ในระดับชั้นย่อย Security ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด

6.4.2 วิธีการทดสอบสมมติฐาน

การทดสอบสมมติฐานมีข้อจำกัดของแบบจำลองที่ใช้ในการทดสอบสมมติฐานตามหัวข้อ 3.3.1 ข้อจำกัดของแบบจำลองที่ใช้จำลอง มีรูปแบบเครือข่ายสื่อสารที่ใช้ในการทดสอบสมมติฐานตามหัวข้อ 3.3.2 รูปแบบเครือข่ายแบบจำลอง อีกทั้งมีเหตุผลการกำหนดลักษณะของสัญญาณข้อมูลที่ใช้ในการทดสอบสมมติฐานตามหัวข้อ 3.3.3 ลักษณะของสัญญาณข้อมูลที่ใช้ในการจำลอง และมีวิธีการทดสอบสมมติฐานตามหัวข้อ 3.3.5 วิธีการจำลองเครือข่ายเพื่อทดสอบการทำงานของโปรโตคอล

6.4.3 พารามิเตอร์ที่ใช้ในการจำลองเครือข่ายเพื่อทดสอบสมมติฐาน

การทดสอบสมมติฐานที่ 6.1.1 ถ้าขนาดวงแหวนกลางของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator (Middle Ring)) ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 6.1.1 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการเปลี่ยนแปลงพารามิเตอร์เพื่อเป็นตัวแปรต้นในการทดสอบสมมติฐาน คือ ขนาดวงแหวนกลางของวงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) (PD) โดยกำหนดค่าเป็น 100,200,300 μm ตามลำดับ

การทดสอบสมมติฐานที่ 6.1.2 ถ้าขนาดวงแหวนข้างของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator (Ear Rings)) ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 6.1.2 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการเปลี่ยนแปลงพารามิเตอร์เพื่อเป็นตัวแปรต้นในการทดสอบสมมติฐาน คือ ขนาดวงแหวนข้างซ้ายและข้างขวาของวงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) (PD) โดยกำหนดค่าเป็น 5,25,150 μm ตามลำดับ

การทดสอบสมมติฐานที่ 6.1.3 ถ้าค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 6.1.3 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการเปลี่ยนแปลงพารามิเตอร์เพื่อเป็นตัวแปรต้นในการทดสอบสมมติฐาน คือ ค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) (PD) โดยกำหนดค่าเป็น 0.2,0.5,0.8 ตามลำดับ

การทดสอบสมมติฐานที่ 6.1.4 ถ้าค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยที่

มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 6.1.4 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการเปลี่ยนแปลงพารามิเตอร์เพื่อเป็นตัวแปรต้นในการทดสอบสมมติฐาน คือ ค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) (PD) โดยกำหนดค่าเป็น 0.2,0.5,0.8 ตามลำดับ

การทดสอบสมมติฐานที่ 6.1.5 ถ้าค่าสัมประสิทธิ์การคัปปลิ้ง κ_3 และ κ_4 ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 6.1.5 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการเปลี่ยนแปลงพารามิเตอร์เพื่อเป็นตัวแปรต้นในการทดสอบสมมติฐาน คือ ค่าสัมประสิทธิ์การคัปปลิ้ง κ_3 และ κ_4 ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) (PD) โดยกำหนดค่าเป็น 0.1,0.5,0.9 ตามลำดับ

การทดสอบสมมติฐานที่ 6.2.1 ถ้าขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ตัวที่ 1 ในระดับชั้นย่อย Security ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 6.2.1 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการเปลี่ยนแปลงพารามิเตอร์เพื่อเป็นตัวแปรต้นในการทดสอบสมมติฐาน คือ ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณตัวที่ 1 ในระดับชั้นย่อย Security (Add Drop Filter) (AD1,AD2) โดยกำหนดค่าเป็น 20,100,180 μm ตามลำดับ

การทดสอบสมมติฐานที่ 6.2.2 ถ้าค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ตัวที่ 1 ในระดับชั้นย่อย Security ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 6.2.2 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการเปลี่ยนแปลงพารามิเตอร์เพื่อเป็นตัวแปรต้นในการทดสอบสมมติฐาน คือ ค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณตัวที่ 1 ในระดับชั้นย่อย Security (Add Drop Filter) (AD1,AD2) โดยกำหนดค่าเป็น 0.1,0.5,0.9 ตามลำดับ

การทดสอบสมมติฐานที่ 6.2.3 ถ้าค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ตัวที่ 1 ในระดับชั้นย่อย Security ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล

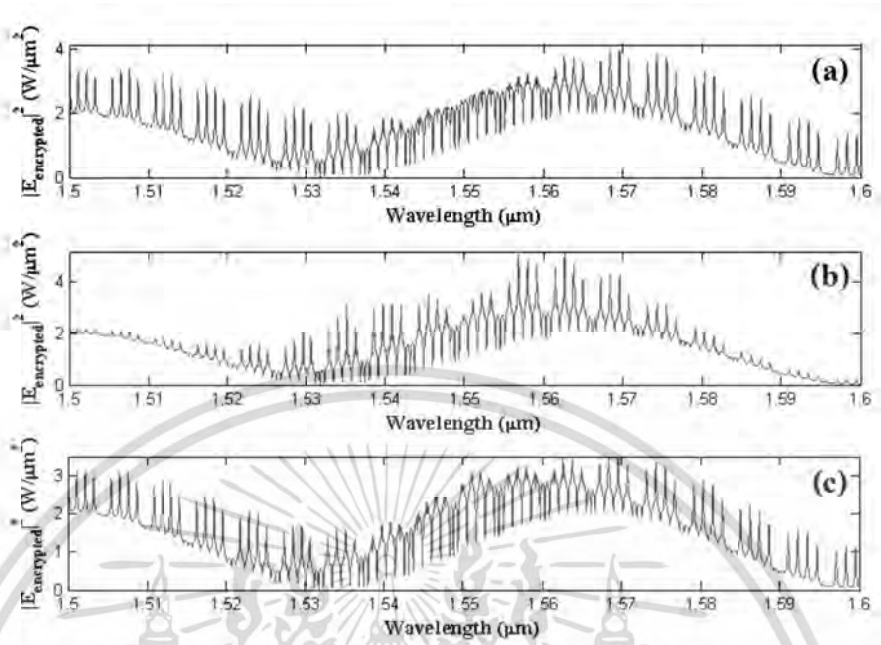
A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 6.2.3 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการเปลี่ยนแปลงพารามิเตอร์เพื่อเป็นตัวแปรต้นในการทดสอบสมมติฐาน คือ ค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณตัวที่ 1 ในระดับชั้นย่อย Security (Add Drop Filter) (AD1,AD2) โดยกำหนดค่าเป็น 0.2,0.5,0.8 ตามลำดับ

การทดสอบสมมติฐานที่ 6.3.1 ถ้าขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ตัวที่ 2 ในระดับชั้นย่อย Security ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 6.3.1 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการเปลี่ยนแปลงพารามิเตอร์เพื่อเป็นตัวแปรต้นในการทดสอบสมมติฐาน คือ ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณตัวที่ 2 ในระดับชั้นย่อย Security (Add Drop Filter) (EN1,DE1) โดยกำหนดค่าเป็น 20,60,100 μm ตามลำดับ

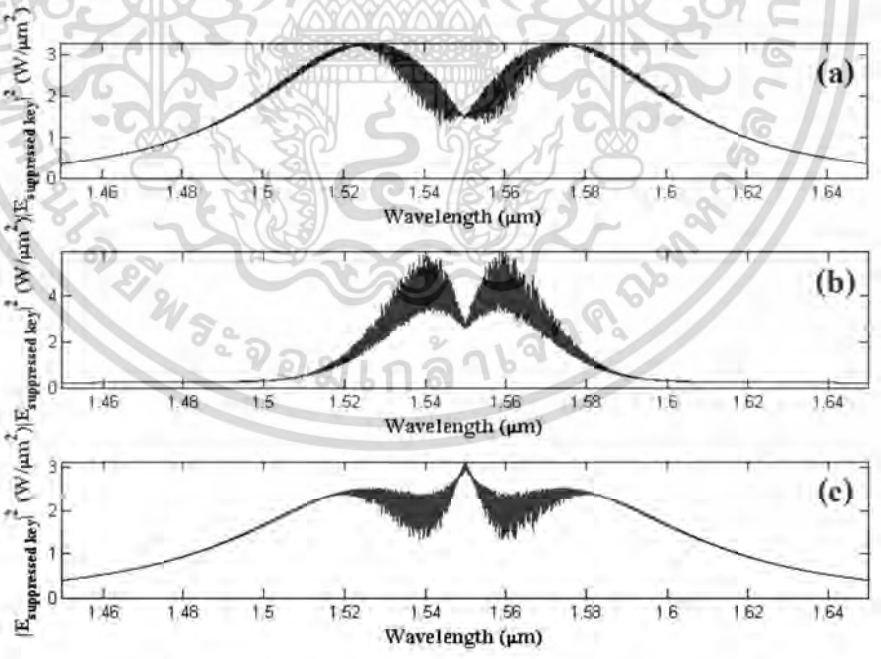
การทดสอบสมมติฐานที่ 6.3.2 ถ้าค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ตัวที่ 2 ในระดับชั้นย่อย Security ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 6.3.2 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการเปลี่ยนแปลงพารามิเตอร์เพื่อเป็นตัวแปรต้นในการทดสอบสมมติฐาน คือ ค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณตัวที่ 2 ในระดับชั้นย่อย Security (Add Drop Filter) (EN1,DE1) โดยกำหนดค่าเป็น 0.1,0.5,0.9 ตามลำดับ

การทดสอบสมมติฐานที่ 6.3.3 ถ้าค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ตัวที่ 2 ในระดับชั้นย่อย Security ของโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมดต่างกันจะส่งผลต่อประสิทธิผลของเครือข่ายที่ใช้อุปกรณ์เชิงแสงทั้งหมด โดยที่มีรูปแบบเครือข่ายที่ใช้ในการจำลองตามรูปที่ 3.7 กล่าวคือ ผู้ส่งข้อมูล A ต้องการส่งข้อมูลไปให้ผู้รับข้อมูล B และอุปกรณ์ภายในเครือข่ายตามรูปที่ 3.4 จากสมมติฐานที่ 6.3.3 กำหนดพารามิเตอร์ของการจำลองเครือข่าย ตามตารางที่ 3.1 แต่มีการเปลี่ยนแปลงพารามิเตอร์เพื่อเป็นตัวแปรต้นในการทดสอบสมมติฐาน คือ ค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณตัวที่ 2 ในระดับชั้นย่อย Security (Add Drop Filter) (EN1,DE1) โดยกำหนดค่าเป็น 0.1,0.5,0.9 ตามลำดับ

6.4.4 การจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 6.1.1



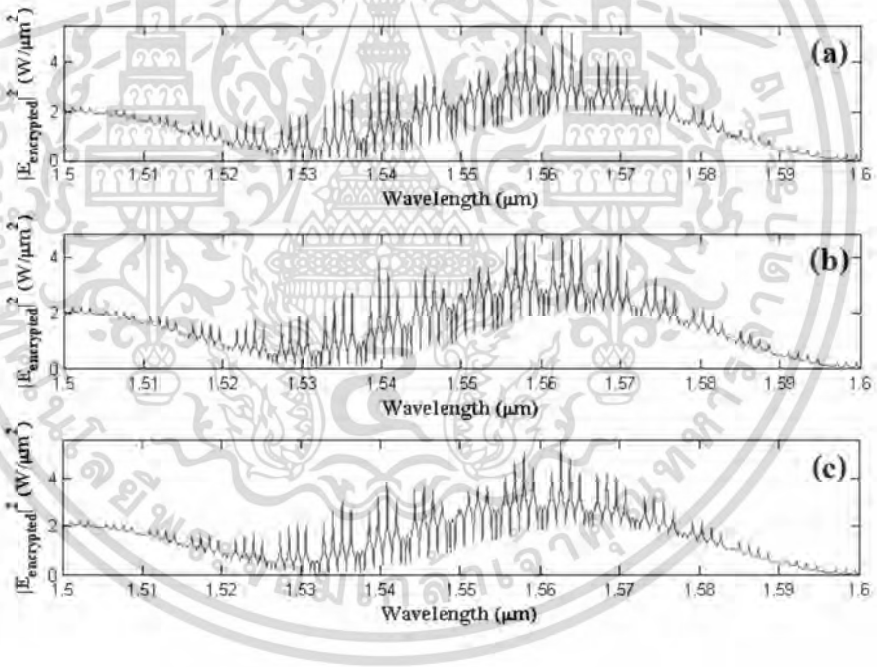
รูปที่ 6.10 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.1



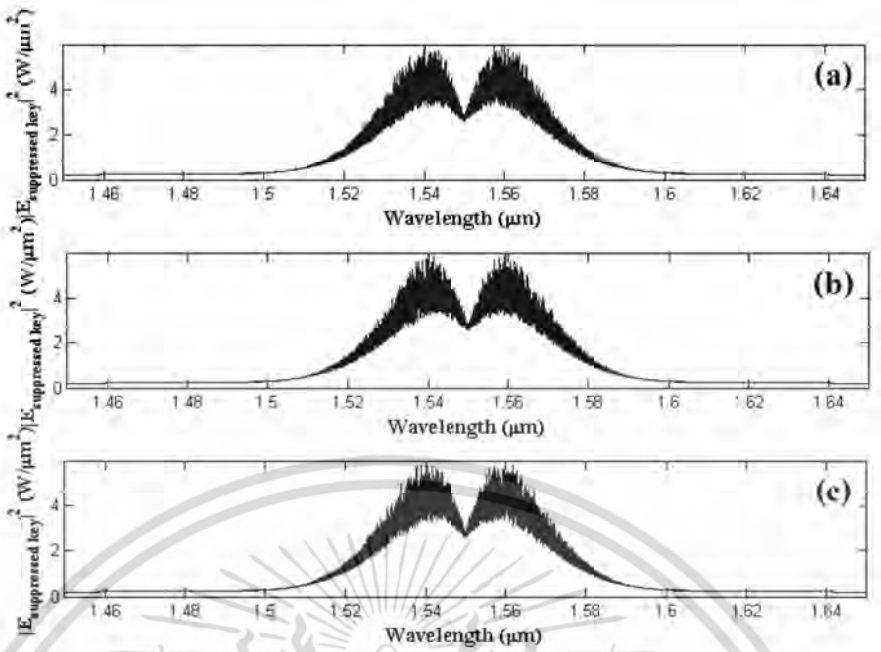
รูปที่ 6.11 เปรียบเทียบผลการจำลอง Suppressed Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.1

จากรูปที่ 6.10 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.1 รูปที่ 6.10 (a) รูปที่ 6.10 (b) และรูปที่ 6.10 (c) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ของการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล โดยที่ขนาดวงแหวนกลางของวงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) เท่ากับ 100, 200, 300 μm ตามลำดับ รูปที่ 6.11 เปรียบเทียบผลการจำลอง Suppressed Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.1 รูปที่ 6.11 (a) รูปที่ 6.11 (b) และรูปที่ 6.11 (c) แสดง Suppressed Key โดยที่ขนาดวงแหวนกลางของวงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) เท่ากับ 100, 200, 300 μm ตามลำดับ จากการจำลองพบว่า วงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) พารามิเตอร์ขนาดวงแหวนกลางมีผลต่อการสร้างสัญญาณรูปปาก (LIP Signal) หรือสัญญาณที่ซ่อนกุญแจเชิงแสงที่มีลักษณะสัญญาณ Noiselike โดยที่ค่าพารามิเตอร์ที่เหมาะสมจะทำให้สร้างสัญญาณรูปปาก (LIP Signal) ที่มีลักษณะสัญญาณ Noiselike ครอบคลุมตลอดช่วงสัญญาณได้

6.4.5 การจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 6.1.2



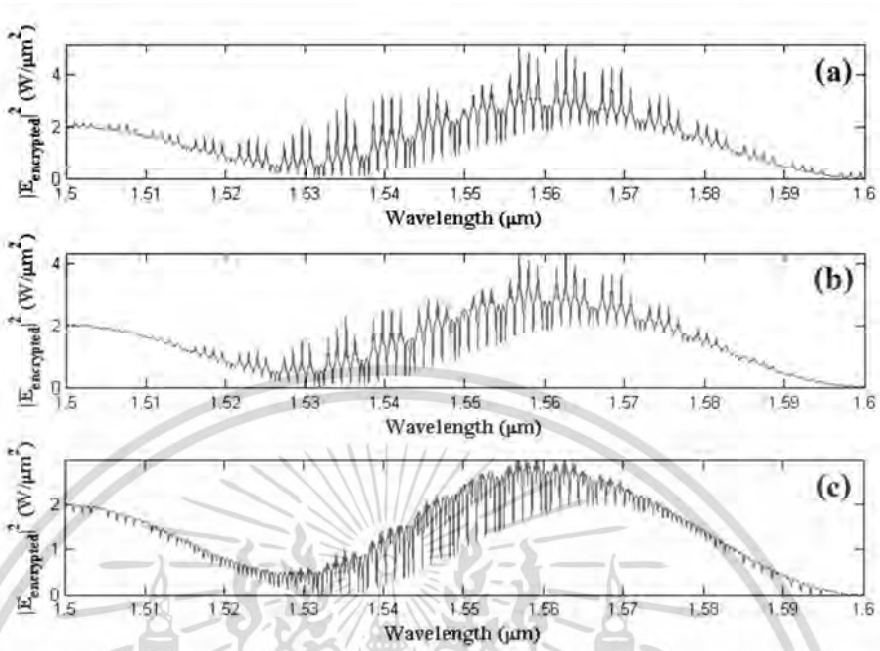
รูปที่ 6.12 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.2



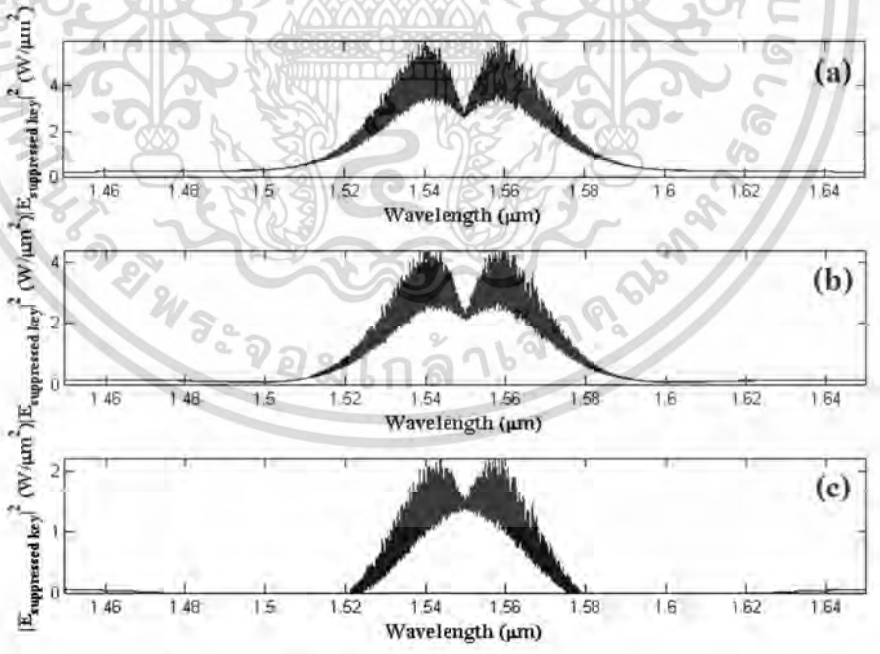
รูปที่ 6.13 เปรียบเทียบผลการจำลอง Suppressed Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.2

จากรูปที่ 6.12 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.2 รูปที่ 6.12 (a) รูปที่ 6.12 (b) และรูปที่ 6.12 (c) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ของการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล โดยที่ขนาดวงแหวนข้างซ้ายและข้างขวาของวงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) เท่ากับ 5, 25, 150 μm ตามลำดับ รูปที่ 6.13 เปรียบเทียบผลการจำลอง Suppressed Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.2 รูปที่ 6.13 (a) รูปที่ 6.13 (b) และรูปที่ 6.13 (c) แสดง Suppressed Key โดยที่ขนาดวงแหวนข้างซ้ายและข้างขวาของวงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) เท่ากับ 5, 25, 150 μm ตามลำดับ จากการจำลองพบว่า วงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) พารามิเตอร์ขนาดวงแหวนข้างไม่มีผลอย่างมีนัยสำคัญต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) หรือสัญญาณรูปปาก (LIP Signal)

6.4.6 การจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 6.1.3



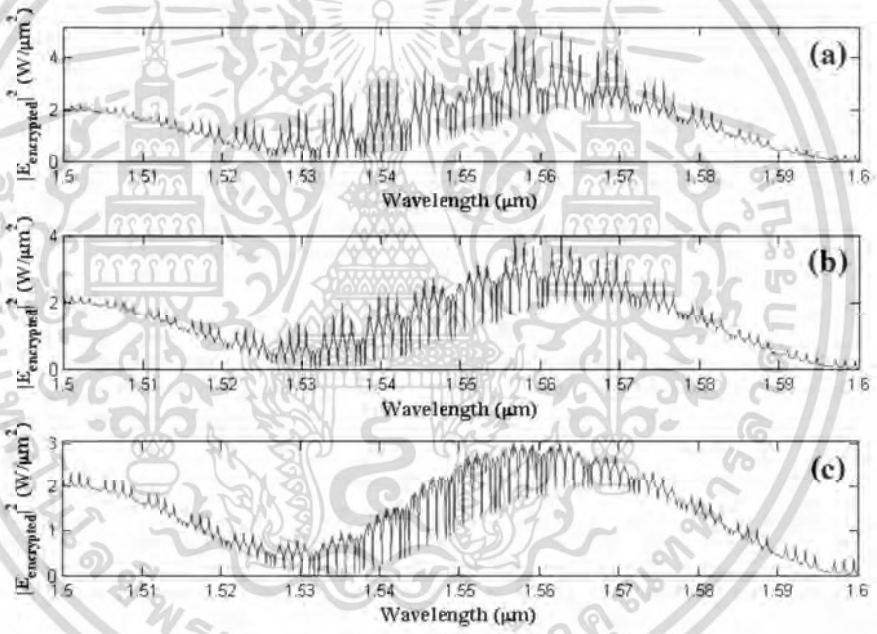
รูปที่ 6.14 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.3



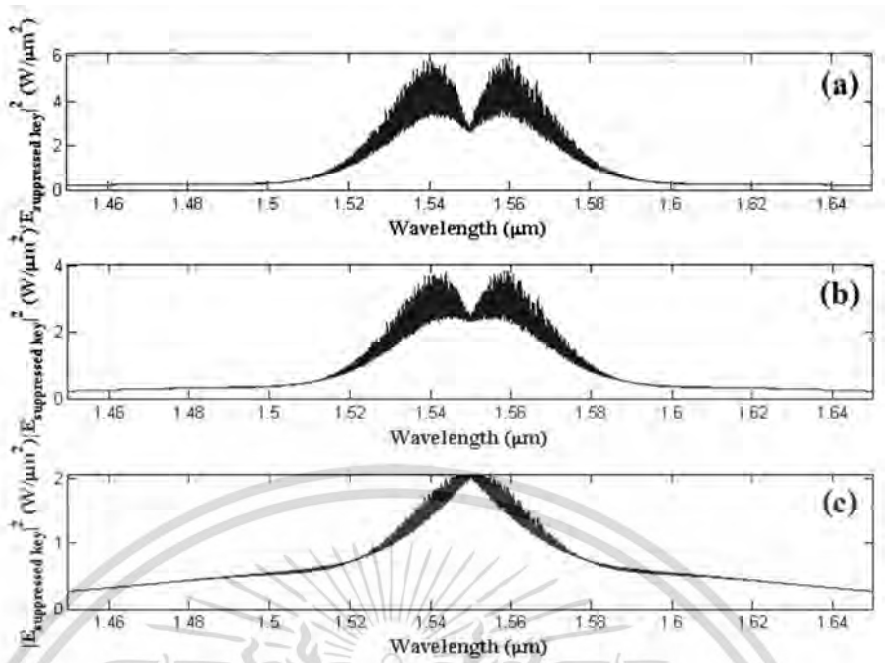
รูปที่ 6.15 เปรียบเทียบผลการจำลอง Suppressed Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.3

จากรูปที่ 6.14 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.3 รูปที่ 6.14 (a) รูปที่ 6.14 (b) และรูปที่ 6.14 (c) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ของการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล โดยที่สัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) เท่ากับ 0.2, 0.5, 0.8 ตามลำดับ จากการจำลองพบว่า จากรูปที่ 6.15 เปรียบเทียบผลการจำลอง Suppressed Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.3 รูปที่ 6.15 (a) รูปที่ 6.15 (b) และรูปที่ 6.15 (c) แสดงสัญญาณ Suppressed Key โดยที่สัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) เท่ากับ 0.2, 0.5, 0.8 ตามลำดับ จากการจำลองพบว่า วงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) พารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_1 ไม่มีผลอย่างมีนัยสำคัญต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) หรือสัญญาณรูปปาก (LIP Signal)

6.4.7 การจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 6.1.4



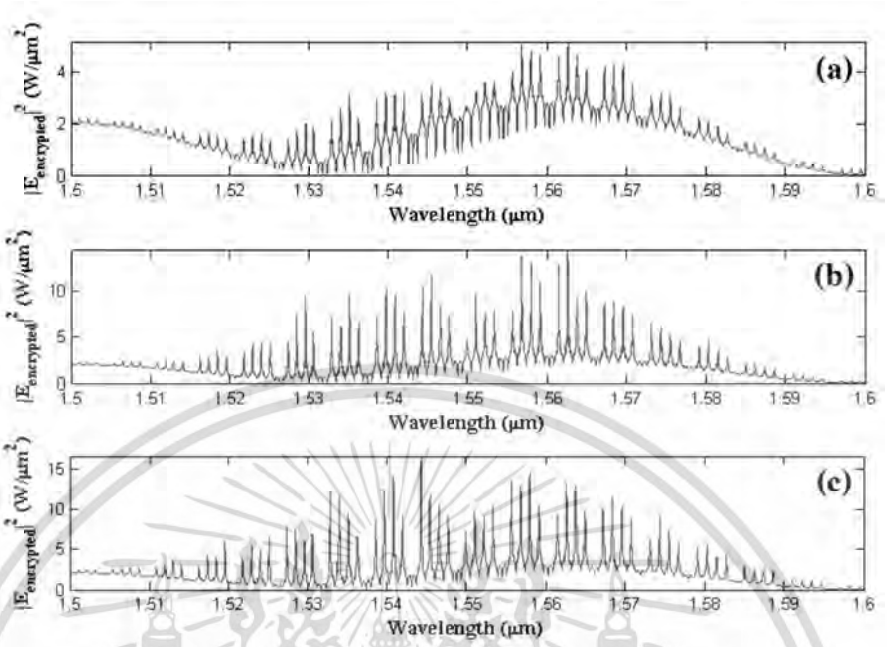
รูปที่ 6.16 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.4



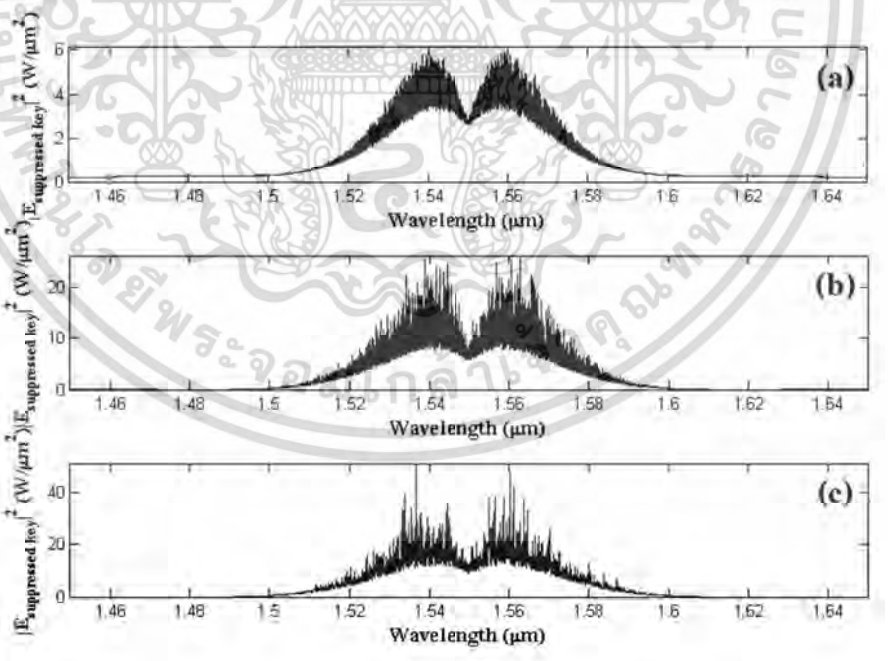
รูปที่ 6.17 เปรียบเทียบผลการจำลอง Suppressed Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.4

จากรูปที่ 6.16 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.4 รูปที่ 6.16 (a) รูปที่ 6.16 (b) และรูปที่ 6.16 (c) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ของการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล โดยที่สัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) เท่ากับ 0.2, 0.5, 0.8 ตามลำดับ รูปที่ 6.17 เปรียบเทียบผลการจำลอง Suppressed Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.4 รูปที่ 6.17 (a) รูปที่ 6.17 (b) และรูปที่ 6.17 (c) แสดงสัญญาณ Suppressed Key โดยที่สัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) เท่ากับ 0.2, 0.5, 0.8 ตามลำดับ จากการจำลองพบว่า วงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) พารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_2 มีผลต่อการสร้างสัญญาณรูปปาก (LIP Signal) หรือสัญญาณที่ซ่อนกุญแจเชิงแสงที่มีลักษณะสัญญาณ Noiselike โดยที่ค่าพารามิเตอร์ที่เหมาะสมจะทำให้สร้างสัญญาณรูปปาก (LIP Signal) ที่มีลักษณะสัญญาณ Noiselike ครอบคลุมตลอดช่วงสัญญาณได้

6.4.8 การจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 6.1.5



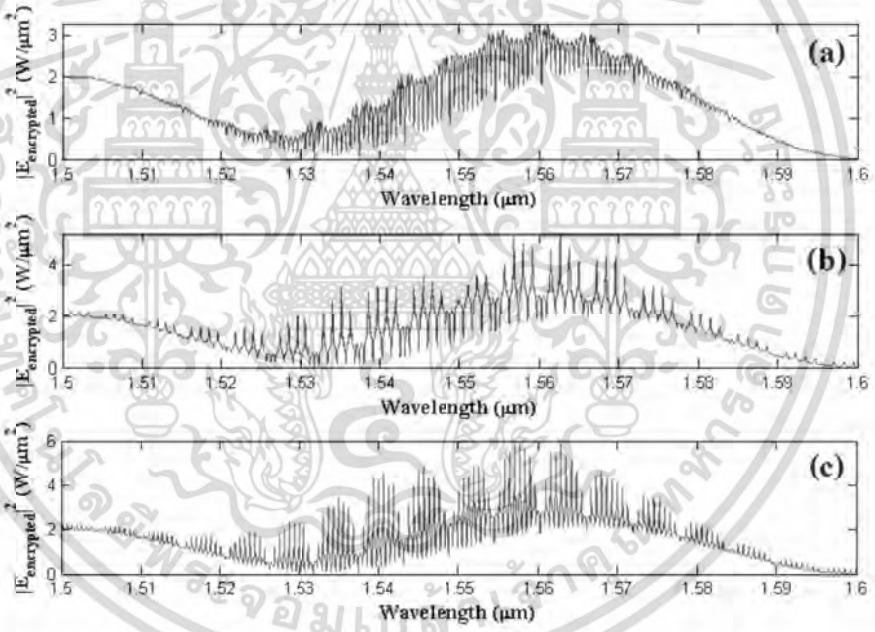
รูปที่ 6.18 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.5



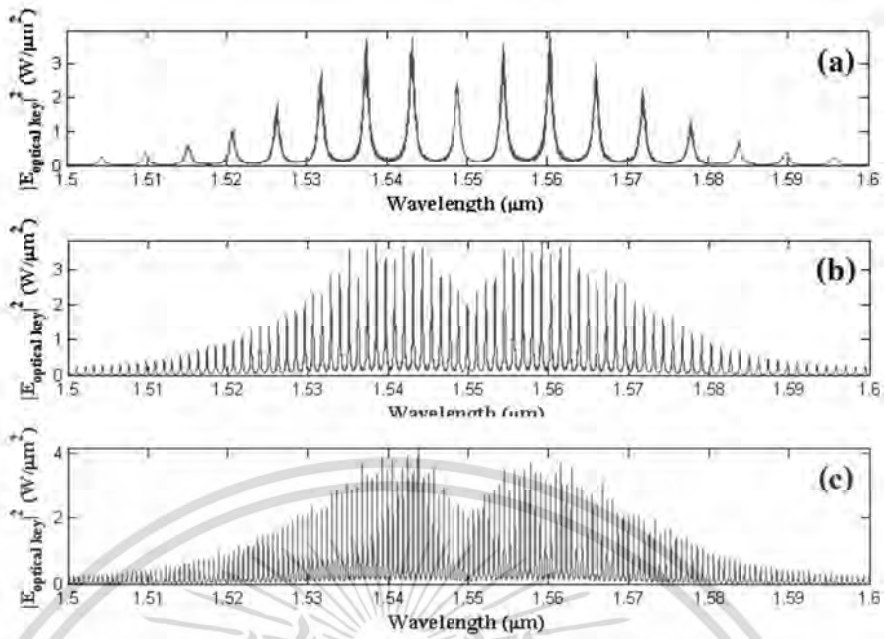
รูปที่ 6.19 เปรียบเทียบผลการจำลอง Suppressed Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.5

จากรูปที่ 6.18 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.5 รูปที่ 6.18 (a) รูปที่ 6.18 (b) และรูปที่ 6.18 (c) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ของการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล โดยที่สัมประสิทธิ์การคัปปลิ้ง κ_3 และ κ_4 ของวงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) เท่ากับ 0.1, 0.5, 0.9 ตามลำดับ รูปที่ 6.19 เปรียบเทียบผลการจำลอง Suppressed Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.1.5 รูปที่ 6.19 (a) รูปที่ 6.19 (b) และรูปที่ 6.19 (c) แสดงสัญญาณ Suppressed Key โดยที่สัมประสิทธิ์การคัปปลิ้ง κ_3 และ κ_4 ของวงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) เท่ากับ 0.1, 0.5, 0.9 ตามลำดับ จากการจำลองพบว่า วงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) พารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_3 และ κ_4 มีผลต่อการสร้างสัญญาณรูปปาก (LIP Signal) หรือสัญญาณที่ซ่อนกุญแจเชิงแสงที่มีลักษณะสัญญาณ Noiselike โดยที่มีผลลักษณะสัญญาณ Noiselike ที่ครอบคลุมกุญแจเชิงแสง ตามรูปที่ 6.3

6.4.9 การจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 6.2.1



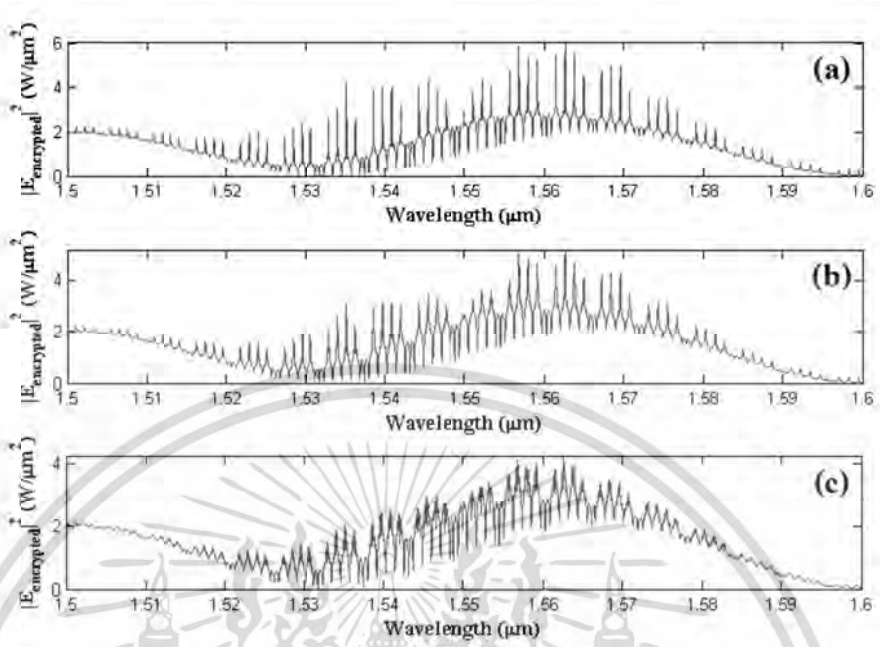
รูปที่ 6.20 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.2.1



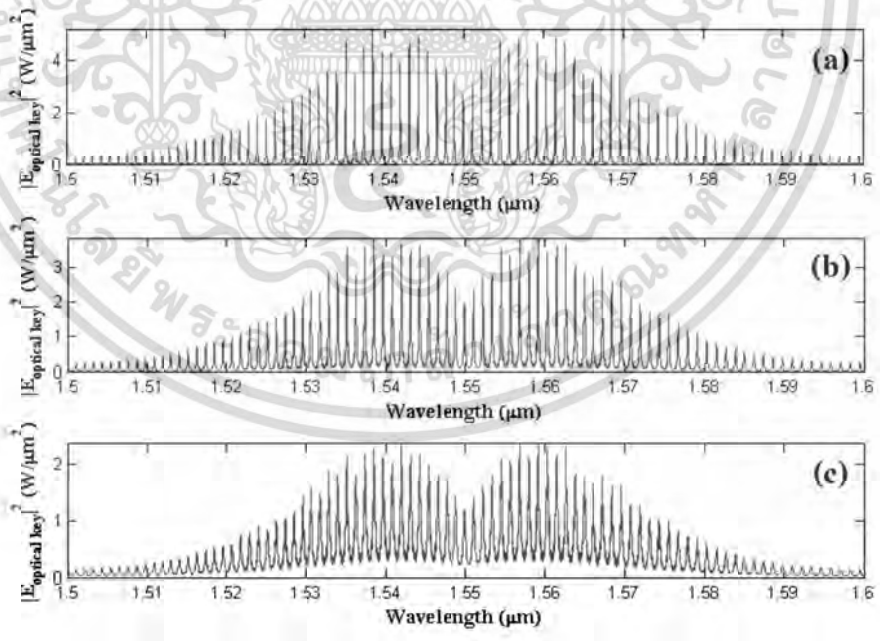
รูปที่ 6.21 เปรียบเทียบผลการจำลอง Optical Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.2.1

จากรูปที่ 6.20 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.2.1 รูปที่ 6.20 (a) รูปที่ 6.20 (b) และรูปที่ 6.20 (c) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ของการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล โดยที่ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (AD1,AD2) เท่ากับ 20, 100, 180 μm ตามลำดับ รูปที่ 6.21 เปรียบเทียบผลการจำลอง Optical Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.2.1 รูปที่ 6.21 (a) รูปที่ 6.21 (b) และรูปที่ 6.21 (c) แสดง Optical Key โดยที่ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (AD1,AD2) เท่ากับ 20, 100, 180 μm ตามลำดับ จากการจำลองพบว่า วงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (AD1,AD2) พารามิเตอร์ขนาดวงแหวนมีผลต่อการสร้างสัญญาณกุญแจเชิงแสง (Optical Key) โดยที่ค่าพารามิเตอร์ที่ใหญ่ขึ้น จะส่งผลให้ค่าค่าพิสัยสเปกตรัมอิสระ (FSR) น้อยลง ซึ่งจะส่งผลต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) โดยสำคัญ

6.4.10 การจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 6.2.2



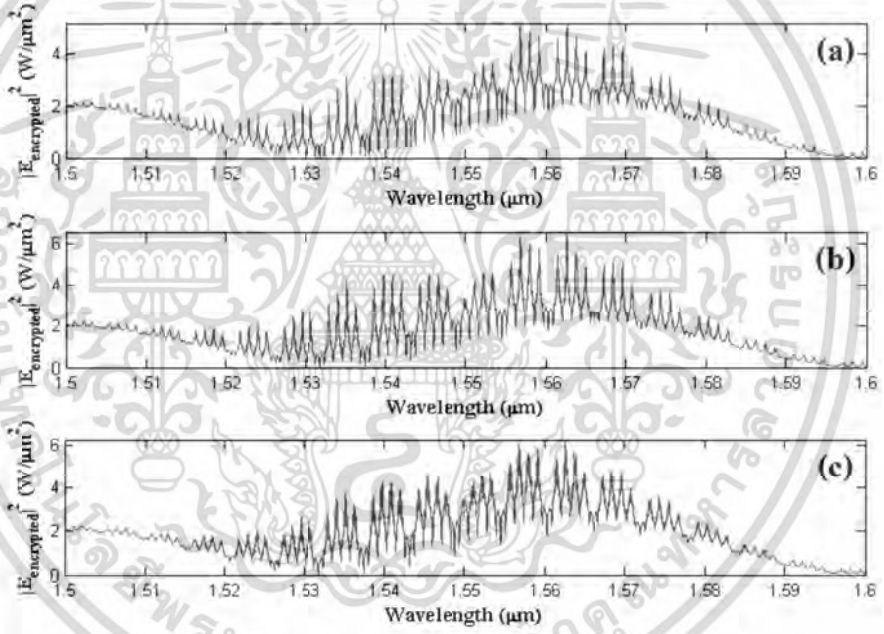
รูปที่ 6.22 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.2.2



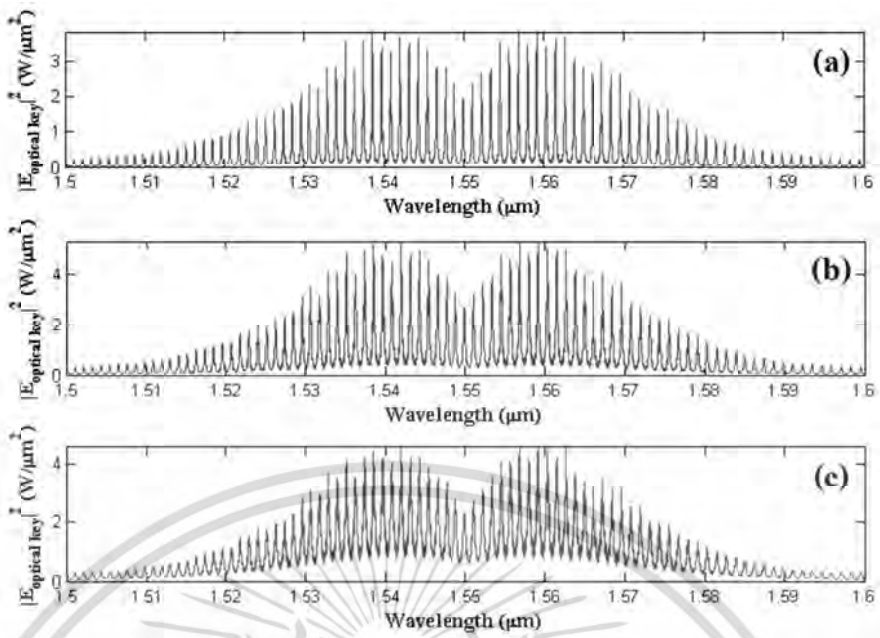
รูปที่ 6.23 เปรียบเทียบผลการจำลอง Optical Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.2.2

จากรูปที่ 6.22 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.2.2 รูปที่ 6.22 (a) รูปที่ 6.22 (b) และรูปที่ 6.22 (c) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ของการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล โดยที่สัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (AD1,AD2) เท่ากับ 0.2, 0.5, 0.8 ตามลำดับ รูปที่ 6.23 เปรียบเทียบผลการจำลอง Optical Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.2.2 รูปที่ 6.23 (a) รูปที่ 6.23 (b) และรูปที่ 6.23 (c) แสดงสัญญาณ Optical Key โดยที่สัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (AD1,AD2) เท่ากับ 0.2, 0.5, 0.8 ตามลำดับ จากการจำลองพบว่าวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (AD1,AD2) พารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_1 ไม่มีผลต่อการสร้างสัญญาณ Optical Key อย่างมีนัยสำคัญ

6.4.11 การจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 6.2.3



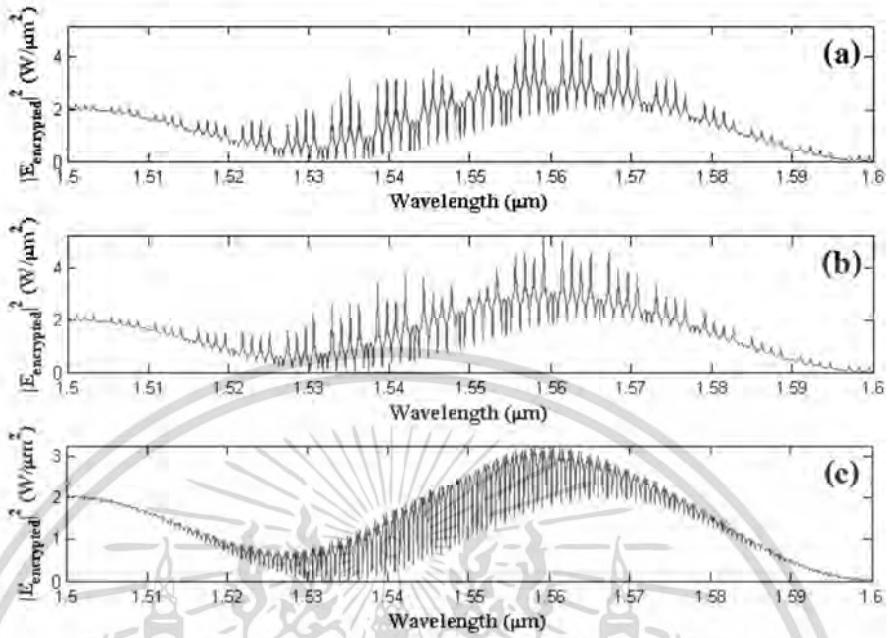
รูปที่ 6.24 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.2.3



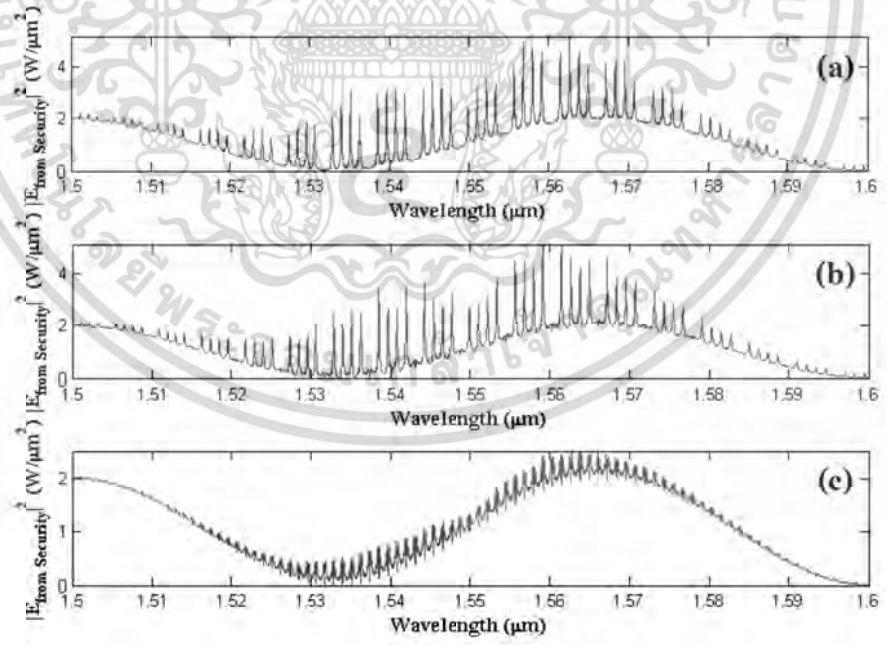
รูปที่ 6.25 เปรียบเทียบผลการจำลอง Optical Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.2.3

จากรูปที่ 6.24 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.2.3 รูปที่ 6.24 (a) รูปที่ 6.24 (b) และรูปที่ 6.24 (c) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ของการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล โดยที่สัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (AD1,AD2) เท่ากับ 0.2, 0.5, 0.8 ตามลำดับ รูปที่ 6.25 เปรียบเทียบผลการจำลอง Optical Key ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.2.3 รูปที่ 6.25 (a) รูปที่ 6.25 (b) และรูปที่ 6.25 (c) แสดงสัญญาณ Optical Key โดยที่สัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (AD1,AD2) เท่ากับ 0.2, 0.5, 0.8 ตามลำดับ จากการจำลองพบว่าวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (AD1,AD2) พารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_2 ไม่มีผลต่อการสร้างสัญญาณ Optical Key อย่างมีนัยสำคัญ

6.4.12 การจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 6.3.1



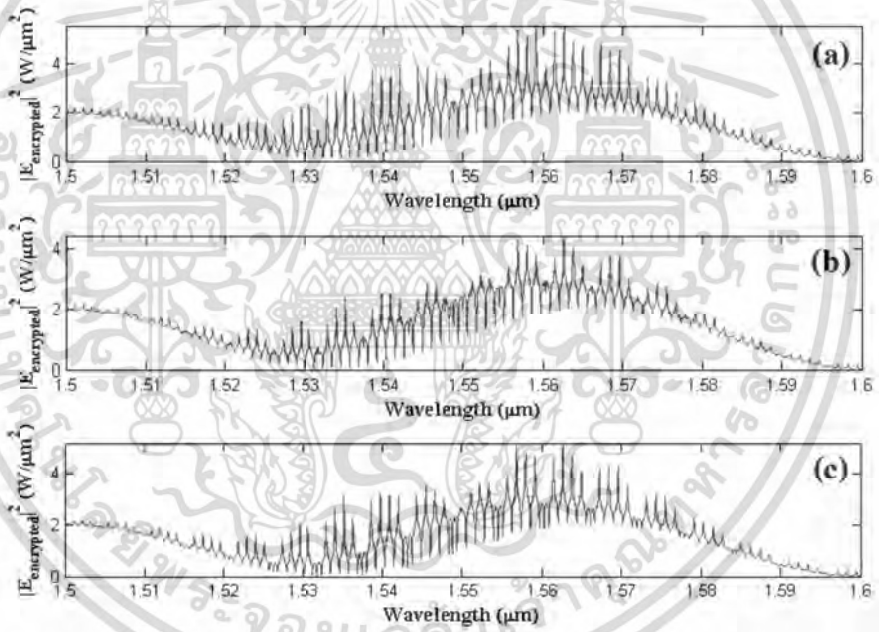
รูปที่ 6.26 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.3.1



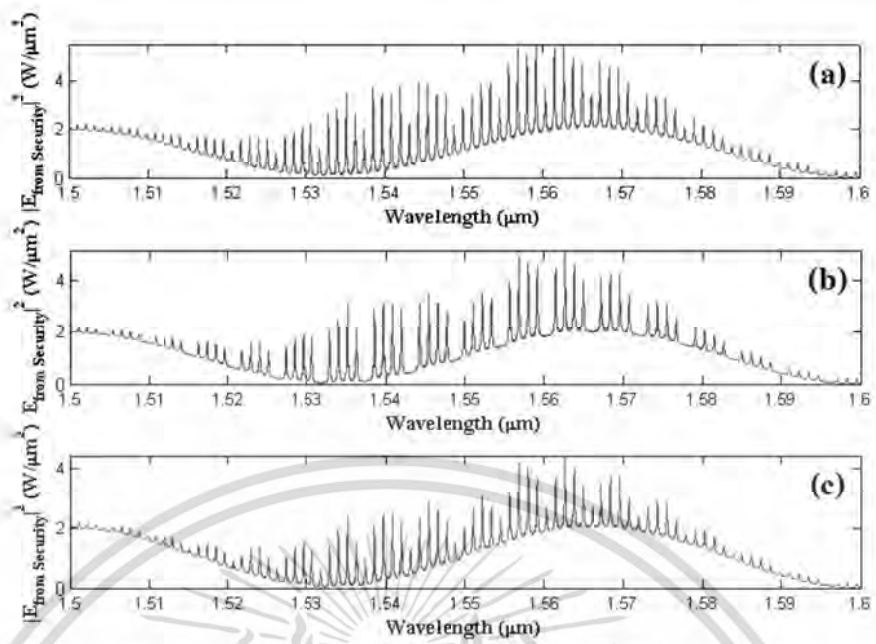
รูปที่ 6.27 เปรียบเทียบผลการจำลองสัญญาณจากระดับชั้นย่อย Security ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.3.1

จากรูปที่ 6.26 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.3.1 รูปที่ 6.26 (a) รูปที่ 6.26 (b) และรูปที่ 6.26 (c) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ของการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล โดยที่ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN1,DE1) เท่ากับ 20, 60, 100 μm ตามลำดับ รูปที่ 6.27 เปรียบเทียบผลการจำลองสัญญาณจากระดับชั้นย่อย Security ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.3.1 รูปที่ 6.27 (a) รูปที่ 6.27 (b) และรูปที่ 6.27 (c) แสดงสัญญาณจากระดับชั้นย่อย Security โดยที่ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN1,DE1) เท่ากับ 20, 60, 100 μm ตามลำดับ จากการจำลองพบว่า วงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN1,DE1) พารามิเตอร์ขนาดวงแหวนมีผลต่อสัญญาณจากระดับชั้นย่อย Security ในฝั่งผู้ส่งข้อมูล โดยที่ค่าพารามิเตอร์ที่ใหญ่ขึ้น จะส่งผลให้ค่าค่าพิสัยสเปกตรัมอิสระ (FSR) ของน้อยลง

6.4.13 การจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 6.3.2



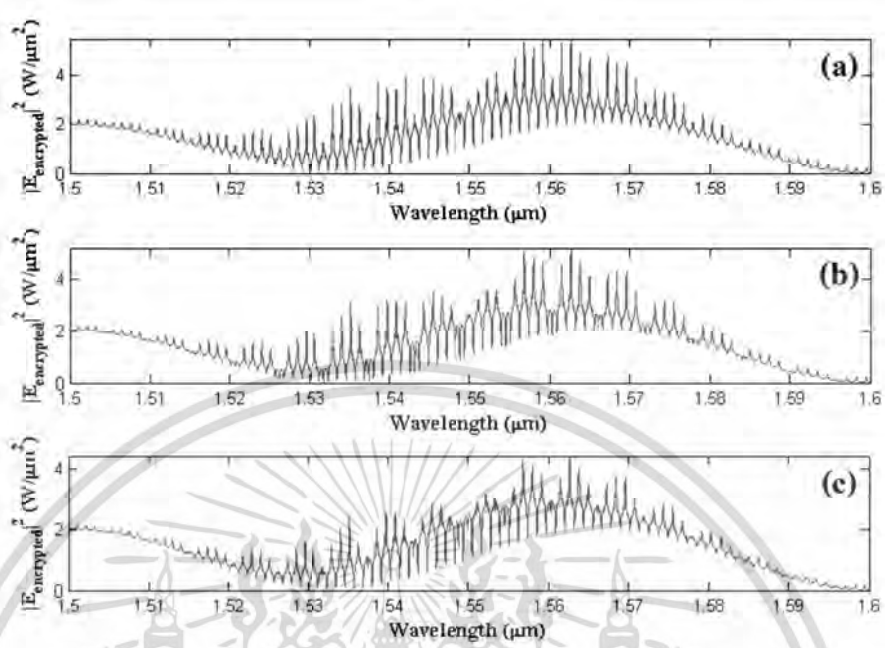
รูปที่ 6.28 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.3.2



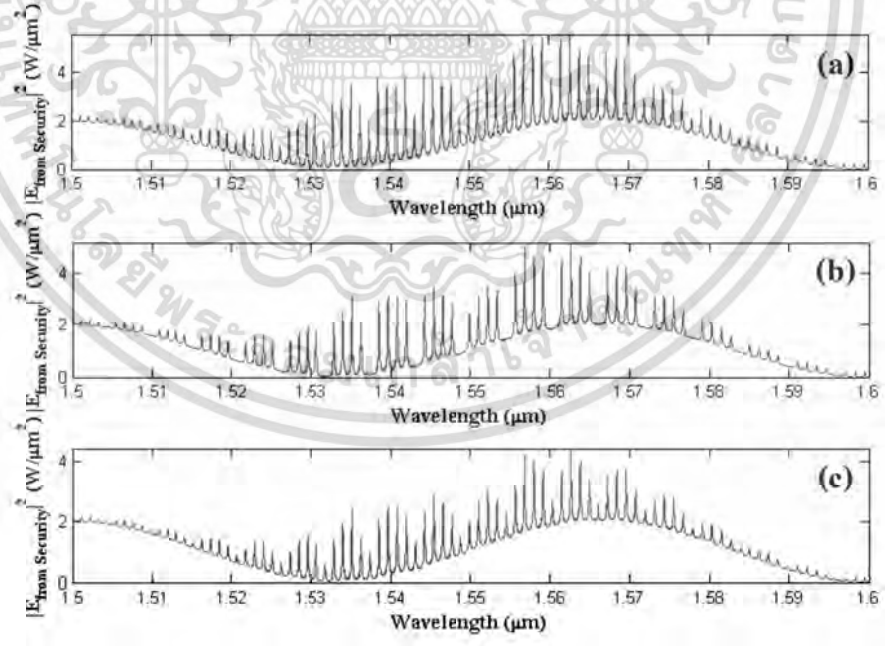
รูปที่ 6.29 เปรียบเทียบผลการจำลองสัญญาณจากระดับชั้นย่อย Security ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.3.2

จากรูปที่ 6.28 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.3.2 รูปที่ 6.28 (a) รูปที่ 6.28 (b) และรูปที่ 6.28 (c) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ของการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล โดยที่สัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN1,DE1) เท่ากับ 0.1, 0.5, 0.9 ตามลำดับ รูปที่ 6.29 เปรียบเทียบผลการจำลองสัญญาณจากระดับชั้นย่อย Security ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.3.2 รูปที่ 6.29 (a) รูปที่ 6.29 (b) และรูปที่ 6.29 (c) แสดงสัญญาณจากระดับชั้นย่อย Security โดยที่สัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN1,DE1) เท่ากับ 0.1, 0.5, 0.9 ตามลำดับ จากการจำลองพบว่าวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN1,DE1) พารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_1 ไม่มีผลต่อการสร้างสัญญาณ Optical Key อย่างมีนัยสำคัญ

6.4.14 การจำลองเครือข่ายเพื่อทดสอบสมมติฐานที่ 6.3.3



รูปที่ 6.30 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.3.3



รูปที่ 6.31 เปรียบเทียบผลการจำลองสัญญาณจากระดับชั้นย่อย Security ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.3.3

จากรูปที่ 6.30 เปรียบเทียบผลการจำลองสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.3.3 รูปที่ 6.30 (a) รูปที่ 6.30 (b) และรูปที่ 6.30 (c) แสดงสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ของการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูล โดยที่สัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN1,DE1) เท่ากับ 0.1, 0.5, 0.9 ตามลำดับ รูปที่ 6.31 เปรียบเทียบผลการจำลองสัญญาณจากระดับชั้นย่อย Security ในการส่งข้อมูลของการทดสอบสมมติฐานที่ 6.3.3 รูปที่ 6.31 (a) รูปที่ 6.31 (b) และรูปที่ 6.31 (c) แสดงสัญญาณจากระดับชั้นย่อย Security โดยที่สัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN1,DE1) เท่ากับ 0.1, 0.5, 0.9 ตามลำดับ จากการจำลองพบว่าวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN1,DE1) พารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_2 ไม่มีผลต่อการสร้างสัญญาณ Optical Key อย่างมีนัยสำคัญ

6.5 ข้อจำกัดการทำงานของโปรโตคอลด้านความปลอดภัยในการส่งข้อมูล

6.5.1 การเกิดสัญญาณรูปปาก (LIP Signal)

วิทยานิพนธ์นี้นำเสนอสัญญาณรูปปาก (LIP Signal) ใช้ในการซ่อนกุญแจเชิงแสงและการกู้คืนกุญแจเชิงแสง (Optical Key Suppression and Recovery) เพื่อนำกุญแจเชิงแสง (Optical Key) ไปใช้ในการสร้างเครือข่ายเสมือนเชิงแสง (Optical Private Tunnel) ทำให้การส่งข้อมูลระหว่างผู้ส่งข้อมูลกับผู้รับข้อมูลเป็นไปอย่างปลอดภัย โดยการเกิดสัญญาณรูปปาก (LIP Signal) มีลักษณะสำคัญ ดังนี้

สัญญาณรูปปาก (LIP Signal) เกิดจากการนำสัญญาณ Bright Soliton เข้าทาง Input Port วงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) และนำสัญญาณ Dark Soliton เข้าทาง Control Port วงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) เท่านั้น โดยสัญญาณรูปปาก (LIP Signal) คือสัญญาณที่ออกทาง Through Port ของวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) ซึ่งรูปแบบของสัญญาณ Soliton ทั้งสอง จะส่งผลต่อรูปแบบของสัญญาณรูปปาก (LIP Signal) เท่านั้น ไม่ส่งผลต่อการเกิดสัญญาณรูปปาก (LIP Signal)

จากสมมุติฐานที่ 6.1.1 พบว่า พารามิเตอร์ขนาดวงแหวนกลางของวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) มีผลโดยตรงต่อรูปแบบสัญญาณที่ออกทาง Through Port ของวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) จากการจำลองค่าพารามิเตอร์ขนาดวงแหวนกลางของวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) ที่ทำให้เกิดสัญญาณรูปปาก (LIP Signal) คือ 125 μm ถึง 214 μm

จากสมมุติฐานที่ 6.1.2 พบว่า พารามิเตอร์ขนาดวงแหวนข้างของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator (Ear Rings)) ไม่มีผลอย่างมีนัยสำคัญต่อการเกิดสัญญาณรูปปาก (LIP Signal)

จากสมมุติฐานที่ 6.1.3 พบว่า พารามิเตอร์ค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) ไม่มีผลอย่างมีนัยสำคัญต่อการเกิดสัญญาณรูปปาก (LIP Signal)

จากสมมติฐานที่ 6.1.4 พบว่า พารามิเตอร์ค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) มีผลโดยตรงต่อรูปแบบสัญญาณที่ออกทาง Through

Port ของวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) จากการจำลองค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) ที่ทำให้เกิดสัญญาณรูปปาก (LIP Signal) คือ 0.1 ถึง 0.7

จากสมมติฐานที่ 6.1.5 พบว่า พารามิเตอร์ค่าสัมประสิทธิ์การคัปปลิ้ง κ_3 และ κ_4 ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) มีผลโดยตรงต่อ Noiselike และความเข้มแสงที่ใช้ในการซ่อนข้อมูลที่ถูกส่งไปในสัญญาณรูปปาก (LIP Signal) จากการจำลองค่าสัมประสิทธิ์การคัปปลิ้ง κ_3 และ κ_4 ของวงแหวนสั่นพ้องรูปแพนด้า (PANDA Ring Resonator) ที่ทำให้เกิดสัญญาณรูปปาก (LIP Signal) คือ 0.1 ถึง 0.3

ดังนั้น การเกิดสัญญาณรูปปาก (LIP Signal) สรุปได้ดังนี้

สัญญาณรูปปาก (LIP Signal) คือสัญญาณที่ออกทาง Through Port ของวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) โดยการนำสัญญาณ Bright Soliton เข้าทาง Input Port และนำสัญญาณ Dark Soliton เข้าทาง Control Port และมีค่าพารามิเตอร์ของวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) ดังนี้

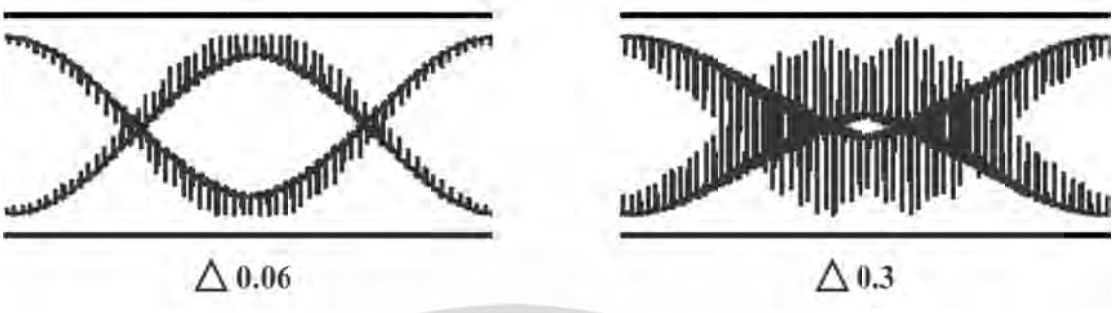
- ค่าพารามิเตอร์ขนาดวงแหวนกลางอยู่ในช่วง 125 μm ถึง 214 μm
- ค่าพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_2 อยู่ในช่วง 0.1 ถึง 0.7
- ค่าพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_3 และ κ_4 อยู่ในช่วง 0.1 ถึง 0.3

6.5.2 ค่าความผิดพลาดของพารามิเตอร์ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณตัวที่ 1 (AD2) ในระดับชั้นย่อย Security ที่สามารถรับข้อมูลได้

รูปที่ 6.32 Eye Diagram กรณีมีค่าความผิดพลาดของพารามิเตอร์ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณตัวที่ 1 (AD2) ในระดับชั้นย่อย Security

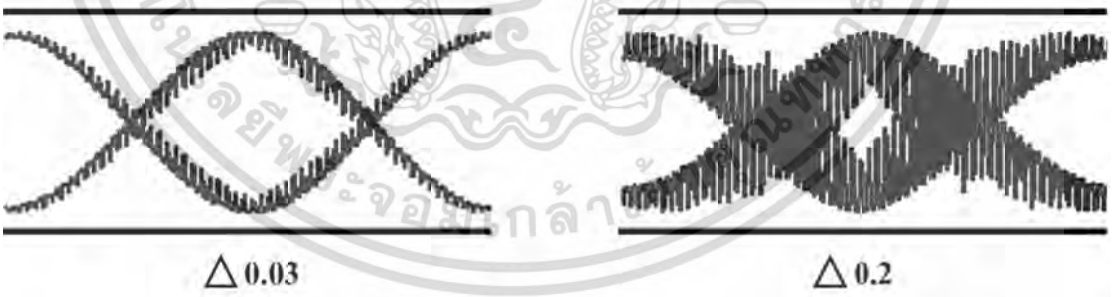
จากหัวข้อ 5.4.1 อธิบายค่าความผิดพลาดของพารามิเตอร์ในฝั่งผู้รับข้อมูลที่สามารถรับข้อมูลได้ และจากรูปที่ 6.32 แสดง Eye Diagram กรณีมีค่าความผิดพลาดของพารามิเตอร์ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณตัวที่ 1 (AD2) (อุปกรณ์ที่ใช้ในการกู้คืนกุญแจเชิงแสง) ในระดับชั้นย่อย Security พบว่า ค่าความผิดพลาดมากที่สุดของพารามิเตอร์ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณตัวที่ 1 (AD2) ที่โปรโตคอลที่นำเสนอสามารถทำงานได้ เท่ากับ 0.0005 % หมายความว่า ผู้ที่ได้รับสัญญาณรูปปาก (LIP Signal) จะสามารถกู้คืนกุญแจเชิงแสงได้ ค่าความ

ผิดพลาดมากที่สุดของพารามิเตอร์ขนาดวงแหวนของอุปกรณ์ที่ใช้ในการกู้คืนกุญแจเชิงแสง เท่ากับ 0.0005 %



รูปที่ 6.33 Eye Diagram กรณีมีค่าความผิดพลาดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณตัวที่ 1 (AD2) ในระดับชั้นย่อย Security

จากหัวข้อ 5.4.1 อธิบายค่าความผิดพลาดของพารามิเตอร์ในฝั่งผู้รับข้อมูลที่สามารถรับข้อมูลได้ และจากรูปที่ 6.33 แสดง Eye Diagram กรณีมีค่าความผิดพลาดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณตัวที่ 1 (AD2) (อุปกรณ์ที่ใช้ในการกู้คืนกุญแจเชิงแสง) ในระดับชั้นย่อย Security พบว่า ค่าความผิดพลาดมากที่สุดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณตัวที่ 1 (AD2) ที่โปรโตคอลที่นำเสนอสามารถทำงานได้ เท่ากับ 0.06 หมายความว่า ผู้ที่ได้รับสัญญาณรูปปาก (LIP Signal) จะสามารถกู้คืนกุญแจเชิงแสงได้ ค่าความผิดพลาดมากที่สุดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_1 ของอุปกรณ์ที่ใช้ในการกู้คืนกุญแจเชิงแสง เท่ากับ 0.06

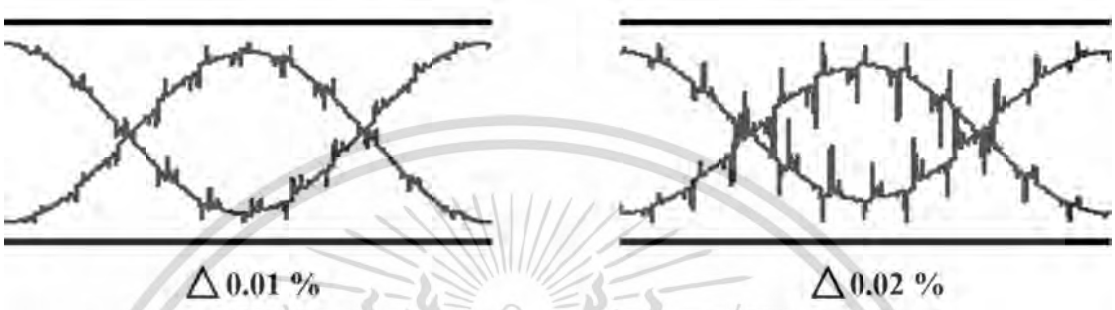


รูปที่ 6.34 Eye Diagram กรณีมีค่าความผิดพลาดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณตัวที่ 1 (AD2) ในระดับชั้นย่อย Security

จากหัวข้อ 5.4.1 อธิบายค่าความผิดพลาดของพารามิเตอร์ในฝั่งผู้รับข้อมูลที่สามารถรับข้อมูลได้ และจากรูปที่ 6.34 แสดง Eye Diagram กรณีมีค่าความผิดพลาดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณตัวที่ 1 (AD2) (อุปกรณ์ที่ใช้ในการกู้คืนกุญแจเชิงแสง) ในระดับชั้นย่อย Security พบว่า ค่าความผิดพลาดมากที่สุดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณตัวที่ 1 (AD2) ที่โปรโตคอลที่นำเสนอ

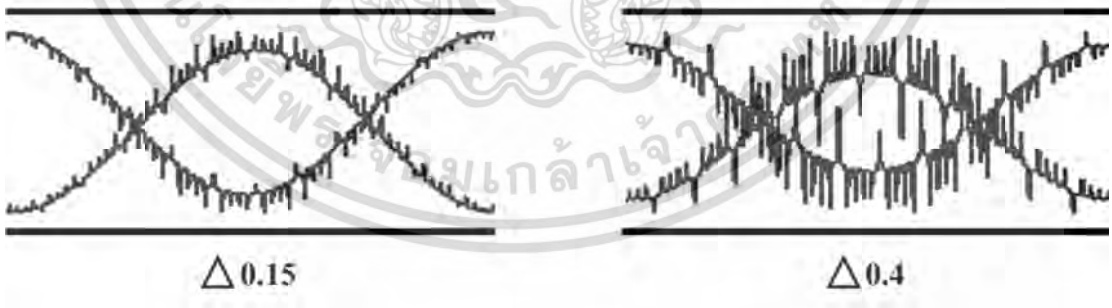
สามารถทำงานได้ เท่ากับ 0.03 หมายความว่า ผู้ที่ได้รับสัญญาณรูปปาก (LIP Signal) จะสามารถกู้คืนกุญแจเชิงแสงได้ ค่าความผิดพลาดมากที่สุดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_2 ของอุปกรณ์ที่ใช้ในการกู้คืนกุญแจเชิงแสง เท่ากับ 0.03

6.5.3 ค่าความผิดพลาดของพารามิเตอร์ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณตัวที่ 2 (ED1 ในระดับชั้นย่อย Security ที่สามารถรับข้อมูลได้



รูปที่ 6.35 Eye Diagram กรณีมีค่าความผิดพลาดของพารามิเตอร์ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณตัวที่ 2 (DE1) ในระดับชั้นย่อย Security

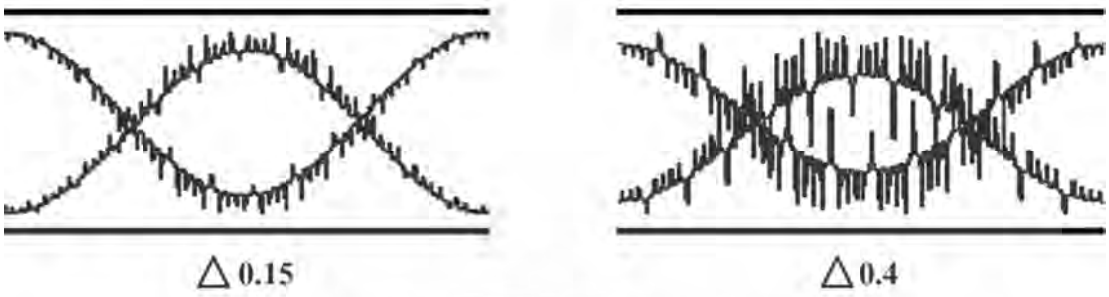
จากหัวข้อ 5.4.1 อธิบายค่าความผิดพลาดของพารามิเตอร์ในฝั่งผู้รับข้อมูลที่สามารถรับข้อมูลได้ และจากรูปที่ 6.35 แสดง Eye Diagram กรณีมีค่าความผิดพลาดของพารามิเตอร์ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณตัวที่ 2 (DE1) ในระดับชั้นย่อย Security พบว่า ค่าความผิดพลาดมากที่สุดของพารามิเตอร์ขนาดวงแหวนของวงแหวนเพิ่มและลดสัญญาณตัวที่ 2 (DE1) ที่โปรโตคอลที่นำเสนอสามารถทำงานได้ เท่ากับ 0.01 %



รูปที่ 6.36 Eye Diagram กรณีมีค่าความผิดพลาดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณตัวที่ 2 (DE1) ในระดับชั้นย่อย Security

จากหัวข้อ 5.4.1 อธิบายค่าความผิดพลาดของพารามิเตอร์ในฝั่งผู้รับข้อมูลที่สามารถรับข้อมูลได้ และจากรูปที่ 6.36 แสดง Eye Diagram กรณีมีค่าความผิดพลาดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณตัวที่ 2 (DE1) ในระดับชั้นย่อย

Security พบว่า ค่าความผิดพลาดมากที่สุดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_1 ของวงแหวนเพิ่มและลดสัญญาณตัวที่ 2 (DE1) ที่โปรโตคอลที่นำเสนอสามารถทำงานได้ เท่ากับ 0.15



รูปที่ 6.37 Eye Diagram กรณีมีค่าความผิดพลาดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณตัวที่ 2 (DE1) ในระดับชั้นย่อย Security

จากหัวข้อ 5.4.1 อธิบายค่าความผิดพลาดของพารามิเตอร์ในฝั่งผู้รับข้อมูลที่สามารถรับข้อมูลได้ และจากรูปที่ 6.37 แสดง Eye Diagram กรณีมีค่าความผิดพลาดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณตัวที่ 2 (DE1) ในระดับชั้นย่อย Security พบว่า ค่าความผิดพลาดมากที่สุดของพารามิเตอร์สัมประสิทธิ์การคัปปลิ้ง κ_2 ของวงแหวนเพิ่มและลดสัญญาณตัวที่ 2 (DE1) ที่โปรโตคอลที่นำเสนอสามารถทำงานได้ เท่ากับ 0.15

6.6 อธิบายการป้องกันการโจมตีของโปรโตคอลที่นำเสนอ

6.6.1 การป้องกันการโจมตีแบบ Interruption

การโจมตีแบบ Interruption เป็นการโจมตีที่ทำให้ทรัพยากรของระบบถูกทำลาย ไม่สามารถให้บริการหรือไม่สามารถใช้งานได้อีก โดยหนึ่งในวิธีการโจมตีแบบ Interruption คือ Denial of Service กล่าวคือ เป็นการปล่อยสัญญาณแสงเข้าไปรบกวนการส่งข้อมูลภายในเครือข่าย เมื่อมีสัญญาณแสงไปรบกวนสัญญาณแสงที่เป็นข้อมูลของการสื่อสาร ทำให้เกิดการแทรกสอดของสัญญาณ เป็นผลให้ผู้รับข้อมูลภายในเครือข่ายไม่สามารถรับข้อมูลที่ถูกต้องจากผู้ส่งข้อมูลได้ โดยโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงที่นำเสนอ ไม่สามารถป้องกันการโจมตีในลักษณะนี้ได้

6.6.2 การป้องกันการโจมตีแบบ Interception

การโจมตีแบบ Interception เป็นการโจมตีที่ไม่ได้ทำให้เกิดการเปลี่ยนแปลงข้อมูลต่าง ๆ ในระบบ แต่ผู้โจมตีสามารถเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต เช่น การแอบดักฟังข้อมูลในสายสัญญาณสื่อสาร เป็นต้น โดยโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงที่นำเสนอ ทำให้เกิดจากโจมตีแบบ Interception ได้ยาก โดยหนึ่งในวิธีการโจมตีแบบ Interception คือ การโจมตีแบบสนิฟเฟอร์ (Sniffer) โดยโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงที่นำเสนอ ทำให้เกิดการป้องกันโจมตีแบบสนิฟเฟอร์ (Sniffer) ดังนี้

1) โปรโตคอลที่นำเสนอ มีการใช้การเข้ารหัสข้อมูลเชิงแสง (Optical Cryptography) ด้วยวิธีการเครือข่ายเสมือนเชิงแสง (Optical Private Tunnel) ซึ่งมีการใช้กุญแจเชิงแสง (Optical Key) ในการสร้างท่อสำหรับการส่งข้อมูล และการแลกเปลี่ยนกุญแจใช้วิธีการซ่อนและการกู้คืนกุญแจ (Key Suppression and Recovery) ทำให้เกิดการโจมตีแบบสนิฟเฟอร์ (Sniffer) ยากมาก ถึงแม้ผู้ไม่หวังดีในเครือข่ายพยายามสุ่มจนได้กุญแจเชิงแสง (Optical Key) ที่ผู้ส่งข้อมูลใช้ในการเข้ารหัสข้อมูลแล้วก็ตาม ผู้ไม่หวังดีในเครือข่ายต้องทราบถึงขั้นตอนของโปรโตคอลที่ถูกต้องถึงจะสามารถถอดข้อมูลที่ผู้ส่งต้องการส่งได้

2) โปรโตคอลที่นำเสนอเป็นการสื่อสารด้วยสัญญาณแสงโดยใช้สื่อเชิงแสง ทำให้การที่จะดักจับข้อมูลภายเครือข่ายทำได้ยากกว่าการสื่อสารด้วยสัญญาณไฟฟ้าโดยใช้สื่อเชิงไฟฟ้า

6.6.3 การป้องกันการโจมตีแบบ Injection

การโจมตีแบบ Injection เป็นการโจมตีที่ทำให้เกิดการสร้างข้อมูลขึ้นมาใหม่โดยการปลอมแปลง เช่น การเพิ่มข้อมูลในไฟล์ในระบบโดยไม่ได้รับอนุญาติ เป็นต้น โดยโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงที่นำเสนอ ทำให้เกิดการโจมตีแบบ Injection ได้ยาก ดังนี้

1) โปรโตคอลที่นำเสนอมีการรองรับงานด้านความปลอดภัย ด้วยวิธีการเครือข่ายเสมือนเชิงแสง (Optical Private Tunnel) ซึ่งมีการใช้กุญแจเชิงแสง (Optical Key) ในการสร้างท่อสำหรับการส่งข้อมูลของเครือข่ายเสมือนเชิงแสง (Optical Private Tunnel) ผู้ที่จะปลอมแปลงข้อมูลภายในเครือข่ายที่ใช้โปรโตคอลที่นำเสนอจะต้องทราบกุญแจเชิงแสง (Optical Key) ในการสร้างท่อสำหรับการส่งข้อมูล ถึงจะปลอมแปลงข้อมูลแล้วทำให้ผู้รับข้อมูลมองเหมือนเป็นข้อมูลที่ส่งมาจากผู้ส่งข้อมูลปกติ ทำให้เกิดจากโจมตีแบบ Injection ได้ยาก

2) โปรโตคอลที่นำเสนอเป็นการสื่อสารด้วยสัญญาณแสงโดยใช้สื่อเชิงแสง ทำให้การจะปลอมแปลงข้อมูลภายเครือข่ายทำได้ยากกว่าการสื่อสารด้วยสัญญาณไฟฟ้าโดยใช้สื่อเชิงไฟฟ้า

6.6.4 การป้องกันการโจมตีแบบ Man in the Middle

การโจมตีแบบ Man in the Middle เป็นการโจมตีที่บุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลและสามารถแก้ไขข้อมูลนั้นได้ด้วย โดยหนึ่งในวิธีการโจมตีของ Man in the Middle คือ การโจมตีรหัสผ่าน (Password Attacks) แบบ Brute Force โดยโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงที่นำเสนอ ทำให้เกิดการโจมตีแบบรหัสผ่าน (Password Attacks) แบบ Brute Force ได้ยาก ดังนี้

1) โปรโตคอลที่นำเสนอมีการใช้กุญแจเชิงแสง (Optical Key) ในการเข้ารหัสข้อมูลที่ส่งระหว่างผู้ส่งข้อมูลกับผู้รับข้อมูล ซึ่งการแลกเปลี่ยนกุญแจระหว่างผู้ส่งข้อมูลและผู้รับข้อมูลใช้วิธีการซ่อนและการกู้คืนกุญแจ (Key Suppression and Recovery) กล่าวคือ ถ้าผู้ไม่หวังดีในเครือข่ายต้องการทราบถึงกุญแจเชิงแสง (Optical Key) จะต้องทราบถึงวิธีการกู้คืนกุญแจ (สุ่มสร้างกุญแจเชิงแสงจากสัญญาณแสงโดยตรงทำไม่ได้ เนื่องจากกุญแจเชิงแสงเกิดจากสัญญาณลักษณะ Noiselike) ซึ่งการกู้คืนกุญแจเชิงแสง (Optical Key) ที่นำเสนอต้องใช้วงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ซึ่งเป็นอุปกรณ์เชิงแสงขนาดเล็ก (เป็นการกู้คืนกุญแจด้วยฮาร์ดแวร์) การที่ผู้ไม่หวังดีในเครือข่ายพยายามสุ่มสร้างอุปกรณ์เชิงแสงขนาดเล็กเพื่อที่จะกู้คืนกุญแจเชิงแสง (Optical Key) ทำได้

ยากมาก เนื่องจากวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) มีพารามิเตอร์ที่เกี่ยวข้องในการสร้างมากมาย วิธีการสร้างก็มีความซับซ้อน อีกทั้งระยะเวลาในการสร้างอุปกรณ์เชิงแสงก็ใช้เวลามาก

2) โปรโตคอลที่นำเสนอมีการใช้กุญแจเชิงแสง (Optical Key) โดยที่สัญญาณแสงที่ส่งไปในเครือข่ายมีมากมาย ทั้งสัญญาณที่เป็นข้อมูล สัญญาณที่เป็นสัญญาณรบกวน รวมถึงสัญญาณแสงที่เป็นกุญแจเชิงแสง (Optical Key) การที่ผู้ไม่หวังดีในเครือข่ายพยายามสุ่มเลือกสัญญาณแสงในช่วงเวลาต่าง ๆ ไปกู้คืนกุญแจเชิงแสงนั้นทำได้ยากมาก จำเป็นต้องมีการ Synchronization สัญญาณที่ส่งภายในเครือข่ายสื่อสาร รวมถึงจำเป็นต้องทราบถึงสถานะของ Reference Port ที่ใช้ในโปรโตคอล

3) ถึงแม้ผู้ไม่หวังดีในเครือข่ายพยายามสุ่มจนได้กุญแจเชิงแสง (Optical Key) ที่ผู้ส่งข้อมูลใช้ในการเข้ารหัสข้อมูลแล้วก็ตาม แต่โปรโตคอลที่นำเสนอมีการใช้การเข้ารหัสข้อมูลเชิงแสง (Optical Cryptography) ซึ่งต้องทราบถึงขั้นตอนของโปรโตคอลที่ถูกต้องถึงจะสามารถถอดข้อมูลที่ผู้ส่งต้องการส่งได้

6.7 อภิปรายสรุปความปลอดภัยในการส่งข้อมูลของโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ

ในบทนี้เป็นการอธิบายความปลอดภัยในการส่งข้อมูลของโปรโตคอลการสื่อสารข้อมูลที่นำเสนอ โดยมีการพัฒนาวิธีการ 2 วิธีการ เรียกว่า การซ่อนกุญแจและการกู้คืนกุญแจ (Key Suppression and Recovery) และเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel)

การซ่อนกุญแจและการกู้คืนกุญแจ (Key Suppression and Recovery) การสื่อสารข้อมูลด้วยโปรโตคอลที่นำเสนอ มีการใช้กุญแจเชิงแสง (Optical Key) สำหรับการเข้ารหัสในการสื่อสารเพื่อสร้างเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) ทำให้การส่งกุญแจเชิงแสง (Optical Key) จากผู้ส่งข้อมูลไปยังผู้รับข้อมูลเป็นส่วนหนึ่งที่มีความสำคัญมาก โดยที่ผู้ส่งข้อมูลจะใช้วิธีการซ่อนกุญแจเชิงแสง (Optical Key) ไปกับสัญญาณรูปปาก (LIP Signal)

เครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) หมายถึง ช่องทางในการสื่อสารเชิงแสงเสมือนจากผู้ส่งข้อมูลไปยังผู้รับข้อมูลโดยตรง โดยเป็นช่องทางที่มีการเข้ารหัสเชิงแสง (Optical Cryptography) ด้วยกุญแจเชิงแสง (Optical Key) โดยกุญแจเชิงแสงที่กู้คืนได้จากสัญญาณรูปปาก เพื่อให้การส่งข้อมูลระหว่างผู้ส่งกับผู้รับข้อมูลมีความปลอดภัยสูง อีกทั้งเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) สามารถเปลี่ยนแปลงกุญแจที่ใช้ในการสร้างเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) ได้ เพื่อให้ความปลอดภัยในการส่งข้อมูลมีสูงมากขึ้น

ผลของพารามิเตอร์ต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ด้านความปลอดภัยในการส่งข้อมูล จากการทดสอบสมมติฐานที่ 6.1 พบว่า วงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) พารามิเตอร์ขนาดวงแหวนกลางและสัมประสิทธิ์การคัปปลิ้งต่าง ๆ ต้องมีความเหมาะสมเพื่อให้เกิดสัญญาณรูปปากที่มีลักษณะ Noiselike ซ่อนกุญแจเชิงแสงตลอดช่วงของสัญญาณที่จะไปใช้งาน เพื่อการแลกกุญแจเชิงแสงระหว่างผู้ส่งข้อมูลกับผู้รับข้อมูลเป็นไปอย่างปลอดภัย จากการทดสอบสมมติฐานที่ 6.2 พบว่าวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ถ้าขนาดของวงแหวนใหญ่ขึ้น จะทำให้ค่าพิสัยสเปกตรัมอิสระ (FSR) น้อยลง ซึ่งค่าพิสัยสเปกตรัมอิสระ (FSR) น้อย

จะทำให้สัญญาณที่ถูกเข้ารหัส (Encrypted Signal) มีค่าพิสัยสเปกตรัมอิสระ (FSR) น้อยตามไปด้วย จะส่งผลให้ความซับซ้อนของสัญญาณสูงมากขึ้น โดยเฉพาะอย่างยิ่งขนาดของวงแหวนของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (AD1,AD2) ซึ่งจะส่งผลต่อการกู้คืนกุญแจเชิงแสงที่ใช้ในการสื่อสารข้อมูลอย่างปลอดภัยภายในเครือข่าย และจากการทดสอบสมมติฐานที่ 6.3 พบว่าวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN1,DE1) พารามิเตอร์ขนาดวงแหวนกลางและสัมประสิทธิ์การคัปปลิ้งต่าง ๆ ต้องมีความเหมาะสม เพื่อให้สัญญาณที่ถูกเข้ารหัส (Encrypted Signal) เหมาะสมแต่จะไม่ส่งผลทำให้การสื่อสารของภายในเครือข่ายผิดพลาด เนื่องจากมีฝั่งผู้ส่งข้อมูลมีการห่อหุ้มเชิงแสง (Optical Encapsulation) และฝั่งผู้รับข้อมูลมีการถอดข้อมูลเชิงแสง (Opical De-Encapsulation) ซึ่งมีผลของการทำงานคล้ายกับตรงข้ามกัน

ข้อจำกัดการทำงานของโปรโตคอลด้านความปลอดภัยในการส่งข้อมูล การเกิดสัญญาณรูปปาก (LIP Signal) ที่ใช้ในการซ่อนกุญแจเชิงแสง (Optical Key) ซึ่งเกิดจากการนำสัญญาณ Bright Soliton เข้าทาง Input Port วงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) และนำสัญญาณ Dark Soliton เข้าทาง Control Port วงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) เท่านั้น และวงแหวนสั่นพ้องแพนด้า (Panda Ring Resonator) มีพารามิเตอร์ดังนี้ ขนาดวงแหวนกลางอยู่ในช่วง 125 μm ถึง 214 μm ค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 อยู่ในช่วง 0.1 ถึง 0.7 และค่าสัมประสิทธิ์การคัปปลิ้ง κ_3 และ κ_4 อยู่ในช่วง 0.1 ถึง 0.3 และค่าความผิดพลาดมากที่สุดของวงแหวนเพิ่มและลดสัญญาณตัวที่ 1 ในระดับชั้นย่อย Security (AD2) โดยที่เป็นอุปกรณ์ที่ใช้ในการกู้คืนกุญแจเชิงแสง (เป็นข้อจำกัดในการกู้คืนกุญแจเชิงแสง) คือพารามิเตอร์ขนาดวงแหวนเท่ากับ 0.0005 % ค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 เท่ากับ 0.06 ค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 เท่ากับ 0.03 รวมถึงค่าความผิดพลาดมากที่สุดของวงแหวนเพิ่มและลดสัญญาณตัวที่ 2 ในระดับชั้นย่อย Security (DE1) ที่ผู้รับข้อมูลสามารถรับข้อมูลได้ คือพารามิเตอร์ขนาดวงแหวนเท่ากับ 0.01 % ค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 เท่ากับ 0.15 ค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 เท่ากับ 0.15

จากการอธิบายการป้องกันการโจมตีของโปรโตคอลที่นำเสนอ พบว่า โปรโตคอลที่นำเสนอสามารถป้องกันการโจมตีแบบ Interception การโจมตีแบบ Injection และการโจมตีแบบ Man in the Middle ได้ แต่จะไม่สามารถป้องกันการโจมตีแบบ Interruption ได้

บทที่ 7
สรุปผลการวิจัยและแนวทางในการศึกษาวิจัยในอนาคต

7.1 สรุปผลการวิจัย

วิทยานิพนธ์นี้นำเสนอโปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมด (Optical Transmission and Addressing Protocol using All Optical Devices) เพื่อให้เครือข่ายสื่อสารที่ใช้โปรโตคอลที่นำเสนอมีความเร็วสูงและมีความปลอดภัยสูง ซึ่งเป็นประโยชน์อย่างมากต่อการใช้งานเฉพาะด้านที่ต้องการความเร็วและความปลอดภัยในคราวเดียวกัน โดยมีข้อจำกัดของงานวิจัยนี้ คือ โปรโตคอลที่นำเสนอไม่รวมถึงการสูญเสียพลังงานระหว่างอุปกรณ์เชิงแสง ไม่รวมถึงการ Synchronization สัญญาณที่ส่งภายในเครือข่ายสื่อสาร และรองรับเฉพาะเครือข่ายแบบวงแหวน (Ring Topology) เครือข่ายแบบบัส (Bus Topology) เท่านั้น

โปรโตคอลที่นำเสนอเทียบได้กับระดับชั้น Physical ของ OSI Model กล่าวคือโปรโตคอลนำเสนอ Physical ที่รองรับการทำงานด้านการระบุที่อยู่และรองรับด้านความปลอดภัยในการสื่อสาร ประกอบด้วย 4 ระดับชั้นย่อย คือ ระดับชั้นย่อย Application ระดับชั้นย่อย Security ระดับชั้นย่อย Network และระดับชั้นย่อย Physical โดยที่การส่งสัญญาณระหว่างระดับชั้นย่อย วิทยานิพนธ์นี้พัฒนาการห่อหุ้มและการถอดข้อมูลเชิงแสง (Optical Encapsulation / Optical De-Encapsulation) ในระดับชั้นย่อย Network มีการพัฒนาที่อยู่เชิงแสง (Optical Address) เพื่อให้สามารถระบุที่อยู่ผู้รับข้อมูลภายในเครือข่ายเชิงแสงได้ ในระดับชั้นย่อย Security มีการพัฒนาการห่อหุ้มและการกู้คืนกุญแจเชิงแสง (Optical Key Suppression and Recovery) เพื่อให้การแลกเปลี่ยนกุญแจเชิงแสงเป็นไปอย่างปลอดภัย อีกทั้งพัฒนาเครือข่ายส่วนตัวเสมือนเชิงแสง (Optical Private Tunnel) โดยการนำกุญแจเชิงแสงจากการห่อหุ้มและการกู้คืนกุญแจเชิงแสงมาสร้างช่องทางการสื่อสารอย่างปลอดภัย รวมถึงมีการใช้งาน Polarizing Beam Splitter (PBS) เพื่อเป็น Reference Port ในการอ้างอิงการส่งข้อมูลภายในเครือข่าย ว่าเป็นการส่งกุญแจเชิงแสง (Optical Key) หรือเป็นการส่งข้อมูลไปยังผู้รับข้อมูล

ด้านการสื่อสารข้อมูล โปรโตคอลสามารถส่งข้อมูลถึงผู้รับข้อมูลได้ โดยที่ผลของพารามิเตอร์ต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ด้านการสื่อสารข้อมูล คือ พารามิเตอร์ความเข้มสัญญาณต่าง ๆ มีผลต่อความเข้มของสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ซึ่งความเข้มของสัญญาณต่าง ๆ มีผลอย่างมากต่อโปรโตคอลที่นำเสนอ เนื่องจากการห่อหุ่มเชิงแสง (Optical Encapsulation) ใช้วิธีการแทรกสอดของสัญญาณ ข้อจำกัดการทำงานของโปรโตคอลด้านการสื่อสารข้อมูล คือ ความเข้มแสงที่เหมาะสมของสัญญาณข้อมูล (Data Signal) คือ น้อยกว่า 200 % ของความเข้มแสงของสัญญาณที่ใช้สร้างกุญแจเชิงแสง (Optical Key) และที่อยู่เชิงแสง (Optical Address) เพราะจะทำให้การห่อหุ้มเชิงแสงของสัญญาณกุญแจเชิงแสงหรือสัญญาณที่อยู่เชิงแสงครอบคลุมสัญญาณข้อมูล (Data Signal)

การระบุที่อยู่ภายในเครือข่าย โปรโตคอลสามารถระบุที่อยู่ผู้รับได้และส่งข้อมูลถึงผู้รับข้อมูลที่ต้องการได้ถูกต้อง อุปกรณ์ที่เกี่ยวข้องด้านการระบุที่อยู่ คือ วงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN2,DE2) พารามิเตอร์ต้องมีความเหมาะสม เพื่อให้ได้สัญญาณที่ถูกเข้ารหัส (Encrypted Signal) เหมาะสม แต่จะไม่ส่งผลทำให้การสื่อสารภายในเครือข่ายผิดพลาด เนื่องจาก

การห่อหุ้มเชิงแสง (Optical Encapsulation) และการถอดข้อมูลเชิงแสง (Optical De-Encapsulation) มีผลของการทำงานคล้ายกับตรงข้ามกัน ข้อจำกัดการทำงานของโปรโตคอลด้านการระบุที่อยู่ภายในเครือข่าย คือ ค่าความผิดพลาดมากที่สุดของวงแหวนเพิ่มและลดสัญญาณในระดับชั้นย่อย Network (DE2) ที่ผู้รับข้อมูลสามารถรับข้อมูลได้ คือพารามิเตอร์ขนาดวงแหวนเท่ากับ 0.0008 % ค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 เท่ากับ 0.25 ค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 เท่ากับ 0.25

ความปลอดภัยในการส่งข้อมูล โปรโตคอลสามารถส่งข้อมูลถึงผู้รับข้อมูลได้อย่างถูกต้อง ถ้าผู้มีผู้ไม่หวังดีในเครือข่ายสื่อสารจะไม่สามารถทราบข้อมูลของผู้ส่งข้อมูลได้ อุปกรณ์ที่เกี่ยวข้องด้านความปลอดภัย คือ วงแหวนสั่นพ้องรูปแพนด้า (Panda Ring Resonator) พารามิเตอร์ขนาดวงแหวนกลางและสัมประสิทธิ์การคัปปลิ้งต่าง ๆ ต้องมีความเหมาะสม เพื่อให้เกิดสัญญาณรูปปากที่มีลักษณะ Noiselike ซ่อนกุญแจเชิงแสงตลอดช่วงของสัญญาณที่จะไปใช้งาน กล่าวคือ ขนาดวงแหวนกลางอยู่ในช่วง 125 μm ถึง 214 μm ค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 อยู่ในช่วง 0.1 ถึง 0.7 และค่าสัมประสิทธิ์การคัปปลิ้ง κ_3 และ κ_4 อยู่ในช่วง 0.1 ถึง 0.3 และวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) ถ้าขนาดของวงแหวนใหญ่ขึ้น จะส่งผลให้ความซับซ้อนของสัญญาณสูงมากขึ้น โดยเฉพาะอย่างยิ่งขนาดของวงแหวนของวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (AD1,AD2) ซึ่งส่งผลต่อการกู้คืนกุญแจเชิงแสง และวงแหวนเพิ่มและลดสัญญาณ (Add Drop Filter) (EN1,DE1) พารามิเตอร์ต้องมีความเหมาะสม เพื่อให้ได้สัญญาณที่ถูกเข้ารหัส (Encrypted Signal) เหมาะสม แต่จะไม่ส่งผลทำให้การสื่อสารภายในเครือข่ายผิดพลาด ข้อจำกัดการทำงานของโปรโตคอลด้านความปลอดภัยในการส่งข้อมูล คือ ค่าความผิดพลาดมากที่สุดของวงแหวนเพิ่มและลดสัญญาณตัวที่ 1 ในระดับชั้นย่อย Security (AD2) โดยที่เป็นอุปกรณ์ที่ใช้ในการกู้คืนกุญแจเชิงแสง (เป็นข้อจำกัดในการกู้คืนกุญแจเชิงแสง) คือพารามิเตอร์ขนาดวงแหวนเท่ากับ 0.0005 % ค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 เท่ากับ 0.06 ค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 เท่ากับ 0.03 รวมถึงค่าความผิดพลาดมากที่สุดของวงแหวนเพิ่มและลดสัญญาณตัวที่ 2 ในระดับชั้นย่อย Security (DE1) ที่ผู้รับข้อมูลสามารถรับข้อมูลได้ คือพารามิเตอร์ขนาดวงแหวนเท่ากับ 0.01 % ค่าสัมประสิทธิ์การคัปปลิ้ง κ_1 เท่ากับ 0.15 ค่าสัมประสิทธิ์การคัปปลิ้ง κ_2 เท่ากับ 0.15 และจากการอธิบายการป้องกันการโจมตี พบว่า โปรโตคอลที่นำเสนอสามารถป้องกันการโจมตีแบบ Interception การโจมตีแบบ Injection และการโจมตีแบบ Man in the Middle ได้ แต่จะไม่สามารถป้องกันการโจมตีแบบ Interruption ได้

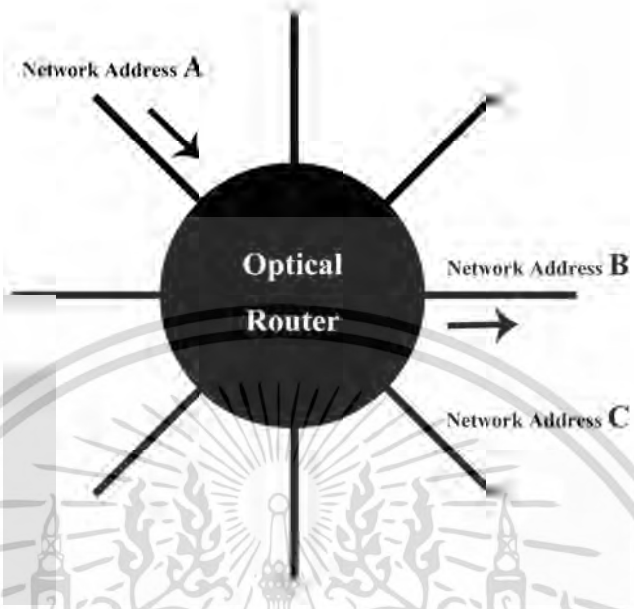
วิทยานิพนธ์นี้สรุปได้ว่า โปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมด สามารถทำการส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูลภายในเครือข่ายเชิงแสงได้อย่างถูกต้อง มีความเร็วในการส่งข้อมูลสูงและมีความปลอดภัยในการส่งข้อมูลสูง

7.2 แนวทางในการศึกษาวิจัยในอนาคต

7.2.1 เราเตอร์เชิงแสง (Optical Router) ที่รองรับโปรโตคอลที่นำเสนอ

โปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง (Optical Transmission and Addressing Protocol) ที่นำเสนอในงานวิจัยนี้ การส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูลต้องใช้ศูนย์กลางช่วงคลื่น (Center Wavelength) เดียวกันในการส่งข้อมูล ถ้าต้องการให้โปรโตคอลที่นำเสนอสามารถส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูลใช้ศูนย์กลางช่วงคลื่น (Center Wavelength)

คนละช่วงกันในการส่งข้อมูล ต้องมีการพัฒนาเราเตอร์เชิงแสง (Optical Router) ที่รองรับโปรโตคอลที่นำเสนอ ตามรูปที่ 7.1

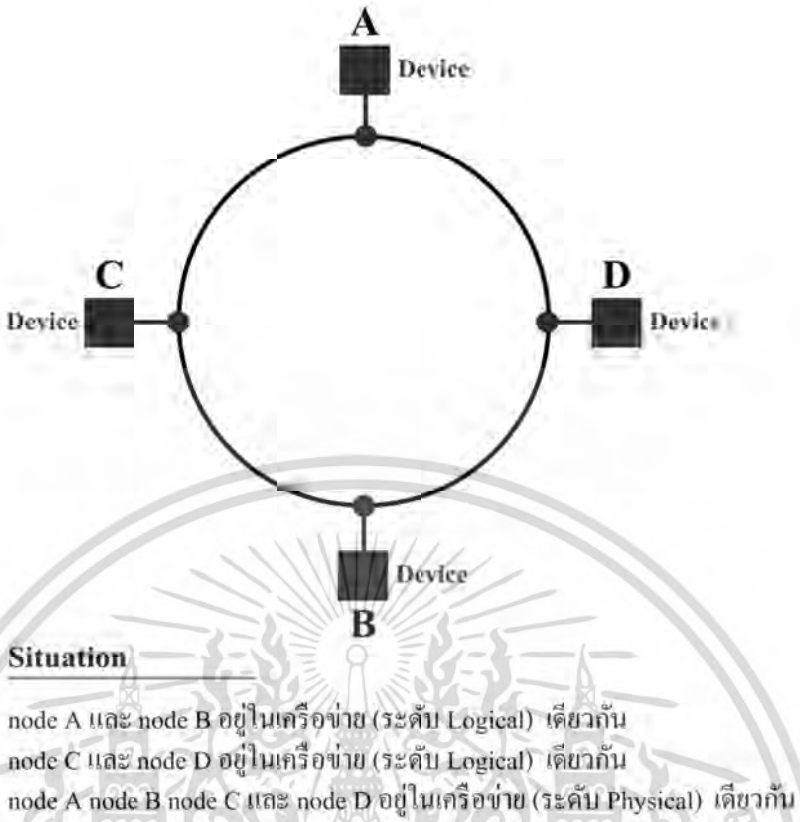


รูปที่ 7.1 เราเตอร์เชิงแสง (Optical Router) ที่รองรับโปรโตคอลที่นำเสนอ

จากรูปที่ 7.1 แสดงเราเตอร์เชิงแสง (Optical Router) ที่รองรับโปรโตคอลที่นำเสนอ อธิบายได้ว่าเราเตอร์เชิงแสง (Optical Router) สามารถส่งต่อสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ออกไปยัง Port ต่าง ๆของเราเตอร์ได้ โดยแต่ละ Port ถูกกำหนดโดยที่อยู่เครือข่ายเชิงแสง (Optical Network Address) โดยที่ในระดับชั้นย่อย Network ของโปรโตคอลที่นำเสนอต้องมีการเพิ่มที่อยู่เครือข่ายเชิงแสง (Optical Network Address)

7.2.2 โปรโตคอลที่รองรับเครือข่ายความยาวคลื่น (Wavelength Network)

โปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสง (Optical Transmission and Addressing Protocol) ที่นำเสนอในงานวิจัยนี้ การส่งข้อมูลจากผู้ส่งข้อมูลไปยังผู้รับข้อมูลต้องใช้ศูนย์กลางช่วงคลื่น (Center Wavelength) เดียวกันในการส่งข้อมูล ทำให้ภายในเครือข่ายจริง (ระดับ Physical) 1 เครือข่าย สามารถที่จะมีเครือข่าย (ระดับ Logical) มากกว่า 1 เครือข่ายได้ โดยการใช้ศูนย์กลางช่วงคลื่น (Center Wavelength) ในการกำหนดเครือข่าย โดยนำเสนอเรียกว่า เครือข่ายความยาวคลื่น (Wavelength Network)



รูปที่ 7.2 เครือข่ายความยาวคลื่น (Wavelength Network)

จากรูปที่ 7.2 เครือข่ายความยาวคลื่น (Wavelength Network) อธิบายว่าโปรโตคอลที่นำเสนอสามารถพัฒนาให้ใช้งานในเครือข่ายลักษณะดังกล่าวได้ โดยต้องมีการพัฒนาโปรโตคอลให้สามารถเปลี่ยนศูนย์กลางช่วงคลื่น (Center Wavelength) ของสัญญาณที่ถูกเข้ารหัส (Encrypted Signal) ได้ เพื่อที่จะสามารถสื่อสารข้อมูลคนละเครือข่าย (ระดับ Logical) ได้ (node A สื่อสารกับ node C ได้)

เอกสารอ้างอิง

[1] C. Yang, Y. Wang, Y. Wang, X. Huang and N. Chi. “Demonstration of high-speed multi-user multi-carrier CDMA visible light communication”, **Optics Communications**, Volume 336, February 2015. pp. 269-272.

[2] S. Kumar, A. Bisht, G. Singh, K. Choudhary and D. Sharma. “Implementation of wavelength selector based on electro-optic effect in Mach–Zehnder interferometers for high speed communications”, **Optics Communications**, Volume 350, September 2015. pp. 108-118.

[3] H. Yeo, J. Chen, Y. Lee and J. Lin. “Half-symbol-rate-carrier PSK modulation for bandwidth-efficient high-speed data communications”, **AEU - International Journal of Electronics and Communications**, Volume 63, Issue 7, July 2009. pp. 609-615.

[4] V. Nazari Talooki, R. Bassoli, D. E. Lucani, J. Rodriguez, F. H.P. Fitzek, H. Marques and R. Tafazolli. “Security concerns and countermeasures in network coding based communication systems: A survey”, **Computer Networks**, Volume 83, 4 June 2015. pp. 422-445.

[5] Y. Liu, S. Zhao, Z. Gong, J. Zhao, X. Li and C. Dong. “Prediction of ionizing radiation effects induced performance degradation in homodyne BPSK based inter-satellite optical communication systems”, **Optics Communications**, Volume 363, 15 March 2016. pp. 97-103.

[6] C. Liu, M. Chen, S. Chen and H. Xian. “Adaptive optics for the free-space coherent optical communications”, **Optics Communications**, Volume 361, 15 February 2016. pp. 21-24.

[7] P. Hua, B.J. Luff, G. R. Quigley, J. S. Wilkinson, K. Kawaguchi, “Integrated optical dual Mach–Zehnder interferometer sensor”, **Sensors and Actuators B**, Volume 87, 2002. pp. 250–257.

[8] R. Levy, A. Peled, S. Ruschin, “Waveguided SPR Sensor Using a Mach–Zehnder Interferometer with Variable Power Splitting Ratio”, **Sens. and Actuat. B**, Volume 119(1), 2006. pp. 20-26.

[9] Q. Xu, B. Schimdt, S. Pradhan, and M, Lipson, “Micrometre-scale silicon electro-optic modulator”, **Nature**, Volume 435, 2005. pp. 325–327.

[10] K. Uomwech, K. Sarapat, and P.P. Yupapin, “Dynamic modulated Gaussian pulse propagation within the double PANDA ring resonator”, **Microw. and Opti. Technol. Lett.**, Volume 52(8), 2010, pp. 1818-1821.

[11] P.P. Yupapin, “Generalized quantum key distribution via micro ring resonator for mobile telephone networks”, **Optik - International Journal for Light and Electron Optics**, Volume 121(5), 2010, pp. 422-425.

[12] B. Knobnob, S. Mitatha, K. Dejhan, S. Chaiyasoonthorn, and P. P. Yupapin, “Dark-bright optical soliton conversion via an optical add/drop filter for signals and network security applications”, **Optik - International Journal for Light and Electron Optics**, Volume 121, 2010. pp. 1743–1747.

[13] P. D. Haye, A. Schliesser, O. Arcizet, T. Wilken, R. Holzwarth, and T. J. Kippenberg, “Optical frequency comb generation from a monolithic microresonator”, **Nature**, Volume 450, 2007. pp. 1214-1217.

[14] T. A. Ibrahim, K. Amarnath, L. C. Kuo, R. Grover, V. Van, and P. –T. Ho, “Photonic logic NOR gate based on two symmetric microring resonators”, **Opt. Lett.**, Volume 29, 2004. pp. 2779–2781.

[15] A. Leinse, M. B. Diemeer, A. Rousseau, and A. Driessen, “A novel high-speed polymeric EO modulator based on a combination of a microring resonator and an MZI”, **IEEE Photon. Technol. Lett.**, Volume 17(10), 2005. pp. 2074–2076.

[16] B. Piyatamrong, K. Kulsirirat, W. Techitdheera, S. Mitatha and P.P. Yupapin, “Multi photons trapping within optical vortices in an add/drop multiplexer”, **Mod. Phys. Lett.**, Volume 24(32), 2010, pp. 3071-3082.

[17] A. Leinse, M. B. Diemeer, A. Rousseau, and A. Driessen, “A Novel High-Speed Polymeric EO Modulator Based on a Combination of a Microring Resonator and an MZI”, **IEEE Photon. Technol. Lett.**, Volume 17, no.10, 2005. pp. 2074–2006.

[18] C. Kochar, A. Kodi, and A. Louri, “Proposed Low-Power High-Speed Microring Resonator-Based Switching Technique for Dynamically Reconfigurable Optical Interconnects”, **IEEE Photon. Technol. Lett.**, Volume 19, no.17, 2007. pp. 1304–1306.

[19] B. Knobnob, S. Mitatha, K. Dejhan, S. Chaiyasoonthorn, and P. P. Yupapin, “Dark-bright optical soliton conversion via an optical add/drop filter for signals and network security applications”, **Optik - International Journal for Light and Electron Optics**, Volume 121, 2010. pp. 1743–1747.

[20] W. Siririth, S. Mitatha, O. Pingern, and P. P. Yupapin, “A novel temporal dark-bright soliton conversion system via an add/drop filter for signal security use”, **Optik - International Journal for Light and Electron Optics**, Volume 121, 2010. pp. 1955–1958.

[21] B. Knobnob, S. Mitatha, K. Dejhan, S. Chaiyasoonthorn, and P. P. Yupapin, “Dark-bright optical soliton conversion via an optical add/drop filter for signals and network security applications”, **Optik - International Journal for Light and Electron Optics**, Volume 121, 2010. pp. 1743–1747.

[22] W. Siririth, S. Mitatha, O. Pingern, P.P. Yupapin, “A Novel Temporal Dark-bright Solitons Conversion System via an Add/drop Filter for Signal Security Use”, **Optik - International Journal for Light and Electron Optics**, Volume 121(21), 2010. pp. 1955-1958.

[23] P. Gallion, F. Mendieta, S. Jiang, “Signal and quantum noise in optical communications and cryptography”, **Progress in Opt.**, Volume 52, 2009. pp. 149-259.

[24] Y. Dumeige, C. Arnaud, P. Féron, “Combining FDTD with coupled mode theories for bistability in micro-ring resonator”, **Opt. Commun.**, Volume 250(4-6), 2005. pp. 376-383.

[25] P. Rabiei, “Calculation of losses in micro-ring resonators with arbitrary refractive index or shape profile and its applications”, **Lightw. Technol.**, Volume 23(3), 2005. pp. 1295-1301.

[26] T. Zhang, X. F. Mo, Z. F. Han, G. C. Guo, “Extensible router for a quantum key distribution network”, **Phys. Lett**. A, Volume 372, 2008. pp. 3957-3959.

[27] ภาควิชาฟิสิกส์. เอกสารประกอบการสอนฟิสิกส์เบื้องต้น, คณะวิทยาศาสตร์ มหาวิทยาลัยนเรศวร.

[28] ภาควิชาฟิสิกส์. ฟิสิกส์2, คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

[29] D.C. Giancoli. Physics Principles with Applications, 3rded., Prentic-Hall, ISBN: 0-13-666769-4, 1991.

[30] D. Halliday, R.Resnick and K.S. Krane. Volume Two extended Version Physics, 4 th ed., John Wiley & Sons, 1992.

[31] C. K. Madsen and J. H. Zhao. Optical Filter Design and Analysis: A Signal Processing Approach. New York: Wiley. 1999.

[32] Somsak Mitatha. 2008. “Signal Processing via Nonlinear Micro Ring Resonator for Optical Communication”, Doctor of Engineering in Electrical Thesis, King Mongkut’s Institute of Technology Ladkrabang.

[33] L. Brzozowski and E. H. Sargent. “Optical signal processing using nonlinear distributed feedback structures”, **IEEE Journal of Quantum Electronics**, Volume 36, 2000. pp. 550-555.

[34] Fan Yi Lin and Meng Chiao Tsai. “Chaotic communication in radio over fiber transmission based on optoelectronic feedback semiconductor laser”, **Optics Express**, Volume 15(2), January 2007. pp. 302-311

[35] Q. Zhou, W. Zhang, S. Zhang, J. Cheng, Y. Huang and J. Peng. “1.5 μm Polarization Entangled Photon Pair Generation Based on Birefringence in Microstructure Fibers”, **Optical Fiber Communication Conference (OFC)**, San Diego, California, March 2009.

[36] R. W. Boyd. Nonlinear Optics. 2nd ed. Academic Press, Inc., 2003.

[37] G.P. Agrawal. Nonlinear Fiber Optics. San Diego, CA: Academic Press. 2001.

[38] S. P. Singh and N. Singh. “Nonlinear Effects Optical Fibers: Origin, Management and Applications,” **Progress In Electromagnetic Research (PIER)**, Volume 73, 2007. pp. 249-275.

[39] S. Blair. “Optical soliton-based logic gates”, Ph.D. dissertation, University of Colorado, 1998.

[40] E. Infeld and G. Rowlands. Nonlinear waves solitons and chaos. Cambridge University Press, 2000.

[41] E. A. J. Marcatili. “Bends in Optical Dielectric Guides”, **Bell System Technical Journal**, Volume 48(7), September 1969. pp. 2103-2132.

[42] K. Sarapat, N. Sangwara, K. Srinuanjan, P.P. Yupapin and N. Pornsuwancharoen, “Novel dark-bright optical solitons conversion system and power amplification”, **Opt. Eng.**, Volume 48, 2009. 045004-1-7.

[43] S.F. Hanim, J. Ali and P.P. Yupapin. “Dark soliton generation using dual Brillouin fiber laser in a fiber optic ring resonator”, **Microwave and Optical Technology Letters**, Volume 52(4), 2010. pp. 881-883.

[44] E. A. J. Marcatili. “Dielectric Rectangular Waveguide and Directional Coupler for Integrated Optics”, **Bell System Technical Journal**, Volume 48(7), September 1969. pp. 2071-2102.

[45] P.P. Yupapin, W. Suwancharoen, “Chaotic signal generation and cancellation using a micro ring resonator incorporating an optical add/drop multiplexer”, **Opt. Commun**. Volume 280(2), 2007. pp. 343-350.

[46] K. Sarapat, N. Sangwara, K. Srinuanjan, P.P. Yupapin and N. Pornsuwancharoen, “Novel dark-bright optical solitons conversion system and power amplification”, **Opt. Eng.**, Volume 48, 2009. 045004-1-7.

[47] T. Phatharaworamet, C. Teeka, R. Jomtarak, S. Mitatha, and P. P. Yupapin, “Random binary code generation using dark-bright soliton conversion control within a PANDA ring resonator”, **Lightw. Technol.**, Volume 28(19), 2010. pp. 2804–2809.

[48] V. Van, T. A. Ibrahim, P. P. Absil, F.G.Johnson, R. Grover, and P.-T. Ho, “Optical signal processing using nonlinear semi-conductor microring resonators”, **Journal of Selected Topics in Quantum Electronics**, Volume 8, No. 3, 2002. pp. 705-713.

[49] Z. Bian, B. Liu, and A. Shakouri, “InP-Based Passive Ring-Resonator-Coupled Lasers”, **IEEE Journal of Quantum Electronics**, Volume 39, No. 7, 2003. pp. 859-865.

[50] T. Barwicz, M. A. Popović , P. T. Rakich, M. R. Watts, H. A. Haus, E. P. Ippen, and Henry I. Smith, "Microring-resonator-based add-drop filters in SiN: fabrication and analysis", **Optics Express**, Volume 12, No. 7, 2004. pp. 1437-1442.

[51] Y. Kokuban, "Vertically Coupled Microring Resonator Filter for Integrated Add/Drop Node", **IEICE Transactions on Electronics**, Volume E88-C, No. 5, 2005. pp. 1458-1464.

[52] T. Barwicz, M. A. Popović , P. T. Rakich, M. R. Watts, H. A. Haus, E. P. Ippen, and Henry I. Smith, "Fabrication of Add–Drop Filters Based on Frequency-Matched Microring Resonators", **Journal of Lightwave Technology**, Volume 24, No. 5, 2006. pp. 2207-2214.

[53] A. Yalçın, K. C. Popat, J. C. Aldridge, T. A. Desai, J. Hryniewicz, N. Chbouki, B. E. Little, O. King, V. Van, S. Chu, D. Gill, M. Anthes-Washburn, and B. B. Goldberg, "Optical sensing of biomolecules using microring resonators", **IEEE Journal of Quantum Electronics**, Volume 12, No. 1, 2006. pp. 148-155.

[54] Q. Xu, D. Fattal, and R. G. Beausoleil, "Silicon microring resonators with 1.5 μm radius", **Optics Express**, Vol. 16, No. 6, 2008. pp. 4309-4315.

[55] X. Xi, L. Yun-Tao, Y. Yu-De, Y. Jin-Zhong, "Silicon-Based Asymmetric Add-Drop Microring Resonators with Ultra-Large Through-Port Extinctions", **Chinese Physics Letters**, Volume 27, No. 5, 2010. pp. 054208.

[56] W. Bogaerts, P. D. Heyn, T. V. Vaerenbergh, K. D. Vos, S. K. Selvaraja, T. Claes, P. Dumon, P. Bienstman, D. V. Thourhout, and R. Baets, "SOI Microring fabrication", **Laser Photonics Review**, Volume 6, No. 1, 2012. pp. 47–73.

[57] P. Rabiei, J. Ma, S. Khan, J. Chiles, and S. Fathpour, "Submicron optical waveguides and microring resonators fabricated by selective oxidation oftantalum", **Optics Express**, Volume 21, No. 6, 2013. pp. 6967-6972.

[58] D. Wu, Y.Wu, Y.Wang, J. An and X. Hu, "reconfigurable optical add-drop multiplexer based on thermally tunable micro-ring resonators", **Optics Communications**, Volume 367, 2016. pp. 44-49.

[59] A. Srivastava and S. Medhekar , "Switching of One Beam by Another in a Kerr Type Nonlinear Mach-Zehnder Interferometer", **Opt. & La. Technol.**, Volume 43(1), 2006. pp. 29-35.

[60] Wiroj Sudatham. "ไมเคิลสันอินเทอร์เฟียร์โรมิเตอร์." [Online]. Available : http://pirun.ku.ac.th/~fsciwrs/optical/optical.html. 2016

[61] Q. Rong, X. Qiao, Y.Du ,H. Sun, D. Feng, R. Wang, M. Hu and Z. Feng, "In-fiber quasi-Michelson interferometer for liquid level measurement with acore-cladding-modes fiber end-face mirror", **Optics and Lasers in Engineering**, Volume 57, January 2014. pp. 53-57.

[62] X Y. Ben-Aryeh. “The use of balanced homodyne and squeezed states for detecting weak optical signals in a Michelson interferometer”, **Physics Letters A**, Volume 375, February 2011. pp. 1300-1303.

[63] S.R.Kachiraju, D. A. Gregory, “Determining the refractive index of liquids using a modified Michelson interferometer”, **Optics & Laser Technology**, Volume 44, May 2012. pp. 2361-2365.

[64] Technical White Paper, The Alcatel-Lucent/NORDUnet Project : Transforming a Legacy Network to an Agile Optical Network, Alcatel-Lucent.

[65] Behrouz A. Forouzan, TCP/IP Protocol Suite, 4 th ed., McGraw-Hill, ISBN: 978-0-07-016678-3.

[66] Payam Rabiei, William H. Steier, Cheng Zhang, Larry R. Dalton, “Polymer Micro Ring Filters and Modulators”, **Journal of Lightwave Technology**, Volume 20, no.11, November 2002.

[67] J.R.R. Sousa, A.F.G.F. Filho, A.C.Ferreira, G.S. Batista, C.S.Sobrinho, A.M. Bastos, M.L. Lyra and A.S.B. Sombra, “Generation of logic gates based on a photonic crystal fiber Michelson interferometer”, **Optics Communications**, Volume 322, February 2014. pp. 143-149.

[68] N. Zhao, H. Fu, M. Shao, X. Yana, H. Li, Q. Liu, H. Gao, Y. Liu and X. Qiao, “High temperature probe sensor with high sensitivity based on Michelson interferometer”, **Optics Communications**, Volume 343, December 2015. pp. 131-134.

[69] M.J. Maciela, C.G. Costaa, M.F. Silvaa, A.C. Peixotoa, R.F. Wolffenbuttelb and J.H. Correia, “A wafer-level miniaturized Michelson interferometer on glass substrate for optical coherence tomography applications”, **Sensors and Actuators A: Physical**, Volume 242, March 2016. pp. 210-216.

[70] W. Jin, Y. Gao and M. Liu, “Fabrication of large area two-dimensional nonlinear photonic lattices using improved Michelson interferometer”, **Optics Communications**, Volume 289, October 2012. pp. 140-143.

[71] H. Gao, D. Hua, Y. Tang, X. Cao, H. Liu and W. Jia, “Wide-angle Michelson interferometer based on LCoS”, **Optics Communications**, Volume 292, December 2012. pp. 36-41.

[72] Behrouz A. Forouzan, Data Communication and Networking, 3 th ed., McGraw-Hill, ISBN: 007-251584-8.

[73] B. Knobnob, S. Mitatha, K. Dejhan, S. Chaiyasoonthorn and P.P.Yupapin, “Dark–bright optical solitons conversion via an optical add/drop filter for signals and networks security applications”, **Optik - International Journal for Light and Electron Optics**, Volume 121, 2010. pp. 1743-1747.

[74] P. Yabosdee, K. Srinuanjan and P.P.Yupapin, “Proposal of the nano-sensing device and system using a nano-waveguide transducer for distributed sensors”, **Optik - International Journal for Light and Electron Optics**, Volume 121, 2010. pp. 2117-2121.

[75] N. Pornsuwancharoena, U. Dunmeekaewa and P.P.Yupapin, “Quantum key distribution using the localized soliton pulses via a wavelength router in the optical network”, **Optik - International Journal for Light and Electron Optics**, Volume 121, 2010. pp. 1111-1115.

[76] W. Siririth, S.Mitatha and P.P.Yupapin, “Novel storage and tunable light source generated by a soliton pulse in a micro ring resonator system”, **Optik - International Journal for Light and Electron Optics**, Volume 121, 2010. pp. 2191-2194.

[77] N. Pornsuwancharoena, P. Kittisuta, N. Kitcharoen and P. P. Yupapin, “Quantum Memory using the Multi-single-photons Storage within a Micro-waveguide System for Security Camera Use”, **Procedia Engineering**, Volume 8, 2011. pp. 200-206.

[78] J. P. Gordon and H. Kogelnik. “PMD fundamentals: Polarization mode dispersion in optical fibers”, **PNAS,** Volume 97(9), 2000. pp. 4541-4550.

[79] A. Galtarossa and L. Palmieri. “Relationship between pulse broadening due to polarisation mode dispersion and differential group delay in long singlemode fiber”, **Electronics Letters,** Volume 34(5) 1998. pp. 492-493.

[80] J. M. Fini and H. A. Haus. “Accumulation of polarization-mode dispersion in cascades of compensated optical fibers”, **IEEE Photonics Technology Letters,** Volume 13(2), 2001. pp. 124-126.

[81] L. N. BINH. “MATLAB Simulink Simulation Platform for Photonic Transmission Systems”, **I. J. Communications, Network and System Sciences,** Volume 2(2), 2009. pp. 97-117.

[82] S. A. Derevyanko and J. E. Prilepsky, “Soliton generation from randomly modulated return-to-zero pulses”, **Optics Communications**, Volume 281, July 2008. pp. 5439-5443.

[83] T. Cheng, T. H. Tuan, X. Xue, D. Deng, T. Suzuki and Y. Ohishi, “Optical solitons and supercontinuum generation in a tellurite microstructured optical fiber”, **Optics Communications**, Volume 369, March 2016. pp. 159-163.

[84] P.P. Yupapin, P. Yabosdee and P. Phiphithirankarn, “Entangled photon generation in a nonlinear micro ring resonator for birefringence-based sensing applications”, **Optik - International Journal for Light and Electron Optics**, Volume 121, 2010. pp. 389-393.

[85] N. Sangwara, N.Pornsuwancharoen and P.P.Yupapin, “Soliton pulses generation and filtering using micro-ring resonators for DWDM-based soliton communication”, **Optik - International Journal for Light and Electron Optics**, Volume 121, 2010. pp. 1263-1267.

[86] K. Sarapata, N.Pornsuwancharoen and P.P.Yupapin, “Polarized soliton pulses generation using nonlinear micro ring resonators for multi- and long distance links”, **Optik - International Journal for Light and Electron Optics**, Volume 121, 2010. pp. 553-558.

ภาคผนวก ก
ผลงานวิจัยที่ได้รับการตีพิมพ์

[1] I. Kolawan, P. Juleang, S. Mitatha, and P. P. Yupapin. “Binary Code Suppression and Recovery using a Dark-Bright Soliton Pair within a PANDA Ring Resonator”, **Joint International Conference on Information & Communication Technology Electronic and Electrical Engineering (JICTEE 2010)**, Luangprabang, Lao PDR, December 21-24, 2010.

[2] P. Juleang, P. Phongsanam, S. Mitatha, and P. P. Yupapin. “Public key suppression and recovery using a PANDA ring resonator for high security communication”, **Optical Engineering**, Volume 50, Issue 3, March 2011.

[3] R. Putthacharoen, P. Juleang, S. Mitatha, and P. P. Yupapin. “Novel optical cryptography using PANDA ring resonator for highly secured communication”, **Optical Engineering**, Volume 50, Issue 7, March 2011.

[4] S. Chaiyasoonthorn, P. Juleang, S. Mitatha, and P. P. Yupapin. “Optical Cryptography Solution by Combined Key for High Security using a Ring Resonator System”, **30th JSST Annual Conference - International Conference on Modeling and Simulation Technology (JSST 2011)**, Tokai University Takanawa Campus, Tokyo, Japan, October 22-23, 2011.

[5] P. Juleang, S. Mitatha, S. Punthawanunt, K. Thananunsophon and P. P. Yupapin. “Optical IP Address for High Security Communication using a Ring Resonator System”, **30th JSST Annual Conference - International Conference on Modeling and Simulation Technology (JSST 2011)**, Tokai University Takanawa Campus, Tokyo, Japan, October 22-23, 2011.

[6] P. Pongsanam, P. Juleang, S. Mitatha, and P. P. Yupapin, “Novel Optical Cryptography using Lip Signals Generated by a PANDA Ring Resonator”, **Microwave and Optical Technology Letters**, Volume 53, No. 11, November 2011. pp. 2575–2580.

[7] P. Juleang, S. Chaiyasoonthorn, S. Mitatha, and P. P. Yupapin. “Optical Encapsulation of Data Signal with Secret key for High Security Communication”, **International Conference on Embedded Systems and Intelligent Technology (ICESIT 2013)**, Nong Khai, Thailand, January 13-15, 2013.

[8] P. Juleang, S. Chaiyasoonthorn, S. Mitatha, and P. P. Yupapin. “A Novel Network Model support Optical Address and Optical Cryptography using All optical Devices”, **International Conference on Embedded Systems and Intelligent Technology (ICESIT 2013)**, Nong Khai, Thailand, January 13-15, 2013.

[9] P. Juleang, R. Putthacharoen, S. Mitatha, and P. P. Yupapin. “Highly Secured Optical Communication by Optical Key and Identification Address”, **Optik - International Journal for Light and Electron Optics**, Volume 124, Issue 9, May 2013. pp. 834–839.

[10] P. Juleang, S. Chaiyasoonthorn, S. Mitatha, and P. P. Yupapin. “Optical Private Tunnel using a Ring Resonator System for Security Communication”, **The 13th International Symposium on Communications and Information Technologies (ISCIT 2013)**, Samui Island, Thailand, 4-6 September, 2013.

ประวัติผู้เขียน

ชื่อ-นามสกุล	นายภากร จูเหล็ง
วัน เดือน ปีเกิด	12 พฤษภาคม 2528 ณ จังหวัดชลบุรี
ที่อยู่	113 หมู่ 9 ตำบล บางปะกง อำเภอ บางปะกง จังหวัด ฉะเชิงเทรา 24130 โทร. 083-7868687
ประวัติการศึกษา	2551 วิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้า เจ้าคุณทหารลาดกระบัง จังหวัดกรุงเทพมหานคร 2553 บริหารธุรกิจมหาบัณฑิต มหาวิทยาลัยกรุงเทพ จังหวัดกรุงเทพมหานคร 2553 วิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้า เจ้าคุณทหารลาดกระบัง จังหวัดกรุงเทพมหานคร
ความชำนาญเฉพาะด้าน	1. การออกแบบระบบเครือข่ายสื่อสารองค์กร 2. การวิเคราะห์ระบบเครือข่ายสื่อสารองค์กร 3. การวิเคราะห์มาตรฐาน ISO 27001 4. การจำลองการทำงานด้วยโปรแกรม MATLAB/Simulink 5. การวิเคราะห์วงแหวนสั่นพ้องทางแสง 6. โปรโตคอลการส่งข้อมูลและการระบุที่อยู่เชิงแสงโดยใช้อุปกรณ์เชิงแสงทั้งหมด
ประสบการณ์การทำงาน	
พ.ศ. 2553-2558	วิศวกร ระดับ 6 หน่วยบริหารเครือข่ายสื่อสาร ส่วนเครือข่ายสื่อสาร ฝ่ายปฏิบัติการศูนย์สารสนเทศ ธนาคารออมสิน จังหวัดกรุงเทพมหานคร