การถอดรหัสแบบวนซ้ำโดยอาศัยการตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์สำหรับสัญญาณคิวพีเอสเคที่เกิดเรย์ลีเฟดดิงที่มีสหสัมพันธ์กัน

นางสาวจันทิมา ศรีเตียเพ็ชร

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า ภาควิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2545
ISBN 974-17-1653-2

ITERATIVE DECODING USING MULTIPLE SYMBOL DIFFERENTIAL DETECTION OF CORRELATED RAYLEIGH FADING QPSK

Miss Chantima Sritiapetch

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Engineering in Electrical Engineering

Department of Electrical Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2002

ISBN 974-17-1653-2

หัวข้อวิทยานิพนธ์	การถอดรหัสแบบวนซ้ำโดยอาศัยการตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์สำหรับสัญญาณคิวพีเอสเคที่เกิดเรย์ลีเฟดดิงที่มีสหสัมพันธ์กัน
โดย	นางสาวจันทิมา ศรีเตียเพ็ชร
สาขาวิชา	วิศวกรรมไฟฟ้า
อาจารย์ที่ปรึกษา	อาจารย์ สุวิทย์ นาคพีระยุทธ

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร.สมศักดิ์ ปัญญาแก้ว)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(ศาสตราจารย์ ดร.ประสิทธิ์ ประพิณมงคลการ)

..... อาจารย์ที่ปรึกษา
(อาจารย์ สุวิทย์ นาคพีระยุทธ)

..... กรรมการ
(รองศาสตราจารย์ ดร.วาทิต เบญจพลกุล)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ลัญฉกร วุฒิสิทธิกุลกิจ)

จันทิมา ศรีเตียเพ็ชร : การถอดรหัสแบบวนซ้ำโดยอาศัยการตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์สำหรับสัญญาณคิวพีเอสเคที่เกิดเรย์ลีเฟดดิงที่มีสหสัมพันธ์กัน. (ITERATIVE DECODING USING MULTIPLE SYMBOL DIFFERENTIAL DETECTION OF CORRELATED RAYLEIGH FADING QPSK) อาจารย์ที่ปรึกษา : อ. สุวิทย์ นาคพีระยุทธ, 87 หน้า. ISBN 974-17-1653-2.

วิทยานิพนธ์ฉบับนี้เสนอวิธีการปรับปรุงสมรรถนะของระบบถอดรหัสเทอร์โบ ที่ใช้ตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์สำหรับสัญญาณคิวพีเอสเคที่เกิดเรย์ลีเฟดดิงที่มีสหสัมพันธ์กัน ตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ทำหน้าที่ประมาณข่าวสารช่องสัญญาณ และส่งข่าวสารนี้ให้กับเครื่องถอดรหัสเทอร์โบเพื่อใช้ในกระบวนการถอดรหัส นอกจากนี้เครื่องถอดรหัสเทอร์โบยังถูกออกแบบให้ส่งข่าวสารกลับไปให้ตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ ทำให้การประมาณช่องสัญญาณแม่นยำขึ้นในแต่ละรอบของการถอดรหัสและส่งผลให้กระบวนการถอดรหัสมีประสิทธิภาพดีขึ้น แนวความคิดหลักที่ใช้ในการปรับปรุงสมรรถนะของระบบถอดรหัสเทอร์โบที่ใช้ตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ คือ การเสนอให้ภาคส่งแยกส่งบิตข้อมูลและบิตรหัสที่คู่กันไปในสัญญาณคิวพีเอสเคต่างสัญลักษณ์กัน เพื่อหลีกเลี่ยงกรณีที่บิตข้อมูลและบิตรหัสจะเสียหายไปพร้อมกันเมื่อผ่านช่องสัญญาณแบบเฟดดิง ทั้งนี้ระบบที่เสนอนี้จำเป็นจะต้องวิเคราะห์วิธีการถอดรหัสขึ้นใหม่เพื่อให้สอดคล้องกัน โดยที่เครื่องถอดรหัสเทอร์โบยังคงสามารถใช้ข่าวสารช่องสัญญาณที่คำนวณมาจากตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ได้ ผลจากการจำลองระบบแสดงให้เห็นว่า ระบบถอดรหัสที่เสนอสามารถปรับปรุงสมรรถนะของระบบถอดรหัสแบบเดิมให้ดีขึ้นได้ ทั้งในกรณีที่อัตราเร็วเฟดดิงเท่ากับ 0.01 0.125 และ 0.200 โดยเฉพาะอย่างยิ่งเมื่อเฟดดิงมีการเปลี่ยนแปลงช้า ๆ ที่อัตราเร็วเฟดดิงเท่ากับ 0.01 ระบบถอดรหัสที่เสนอสามารถลดอัตราความผิดพลาดของบิตลงได้ถึง 3 ระดับขนาด

ภาควิชา วิศวกรรมไฟฟ้า ลายมือชื่อนิสิต .....

สาขาวิชา วิศวกรรมไฟฟ้า ลายมือชื่ออาจารย์ที่ปรึกษา .....

ปีการศึกษา 2545

4370246021 : MAJOR ELECTRICAL ENGINEERING

KEY WORD: ITERATIVE DECODING / MULTIPLE SYMBOL DIFFERENTIAL DETECTION / RAYLEIGH FADING

CHANTIMA SRITIAPETCH : ITERATIVE DECODING USING MULTIPLE SYMBOL DIFFERENTIAL DETECTION OF CORRELATED RAYLEIGH FADING QPSK. THESIS ADVISOR : SUVIT NAKPEERAYUTH, 87 pp. ISBN 974-17-1653-2.

In this thesis, an improvement strategy of a turbo decoding system with Multiple Symbol Differential Detector (MSDD) of correlated Rayleigh fading QPSK is proposed. The main task of MSDD is to estimate the channel states and send to turbo decoder. In addition, MSDD can also utilize the information output from turbo decoder. Due to the information exchange between MSDD and turbo decoder, the channel estimation can be improved with each decoding iteration resulting in better performance of decoding process. The main idea in improving the performace of turbo decoding system with MSDD is to transmit data bit and associated coded bit into different QPSK symbols in order to avoid the case that both bits are corrupted over fading channel. With this proposed system, the new decoding scheme has to be derived accordingly. However, the channel information calculated from MSDD can still be used by turbo decoder. Based on the results from computer simulations, it is found that the performance of the proposed decoding system is better than that of the original decoding system for fading rate of 0.01 0.125 and 0.200. Especially for slow fading at fading rate equals to 0.01, the proposed decoding system can lower the bit error rate down by 3 orders of magnitude.

Department Electrical Engineering Student's signature

Field of study Electrical Engineering Advisor's signature

Academic year 2002

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปด้วยดี ด้วยความช่วยเหลือของอาจารย์สุวิทย์ นาคพีระยุทธ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งท่านได้ให้คำแนะนำและข้อคิดเห็นต่าง ๆ อันเป็นประโยชน์อย่างยิ่งในการทำวิจัย อีกทั้งยังช่วยแก้ปัญหาต่าง ๆ ที่เกิดขึ้นระหว่างการดำเนินงานอีกด้วย ขอขอบคุณ นายพิสิฐ วนิชชานันท์ สำหรับข้อแนะนำและความช่วยเหลือในทุก ๆ ด้านในการทำวิจัย นอกจากนี้ ขอขอบคุณเพื่อน ๆ ในห้องปฏิบัติการไฟฟ้าสื่อสารทุกคนที่เป็นกำลังใจ และให้ความช่วยเหลือในการทำวิทยานิพนธ์เรื่องนี้

สุดท้ายนี้ ผู้วิจัยขอขอบพระคุณบิดามารดา และครอบครัว ซึ่งเปิดโอกาสให้ได้รับการศึกษาเล่าเรียน ตลอดจนคอยช่วยเหลือและให้กำลังใจผู้วิจัยเสมอมาจนสำเร็จการศึกษา

จันทิมา ศรีเตียเพ็ชร

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญตาราง

หน้า

สารบัญรูป

หน้า

สารบัญรูป (ต่อ)

หน้า

สารบัญรูป (ต่อ)

หน้า

บัญชีคำศัพท์

การเข้ารหัสช่องสัญญาณ	channel coding
การซิงโครไนซ์	synchronization
การตรวจจับแบบไม่ร่วมนัย	noncoherent detection
การตรวจจับแบบร่วมนัย	coherent detection
การถอดรหัสแบบวนซ้ำ	iterative decoding
การแทรกสอดระหว่างสัญลักษณ์	intersymbol interference (ISI)
การแผ่แบบดอปเปลอร์	Doppler spread
การแผ่แบบประวิงเวลา	delay spread
ขนาดหน่วยความจำ	memory size
ข้อด้อยของการตรวจจับแบบไม่ร่วมนัย	noncoherence penalty
ข่าวสารช่องสัญญาณ	channel information
ข่าวสารเอ็กซ์ทรินซิก	extrinsic information
ความเชื่อถือได้	reliability
ความน่าจะเป็นเบื้องแรก	*a priori* probability
ความน่าจะเป็นหลัง	*a posteriori* probability (APP)
ความยาวของบล็อก	block length
ความยาวคอนสเตรนต์	constraint length
ค่าความน่าจะเป็นหลังสูงสุด	maximum *a posteriori* (MAP)
คาบของสัญลักษณ์	symbol period
ค่าพื้นของความผิดพลาด	error floor
คำรหัส	code word
เครื่องเข้ารหัสคอนโวลูชันแบบมีระบบที่มีการป้อนกลับ	recursive systematic convolutional encoder (RSC)
เครื่องเข้ารหัสคอนโวลูชันแบบไม่มีระบบ	non systematic convolutional encoder (NSC)
เครื่องเข้ารหัสเทอร์โบ	turbo encoder
เครื่องถอดรหัสย่อย	constituent decoder (CD)
ช่วงสังเกตการณ์	observation interval
ช่องสัญญาณที่เกิดเรย์ลีเฟดดิงที่มีสหสัมพันธ์กัน	correlated Rayleigh fading channel

บัญชีคำศัพท์ (ต่อ)

ดิจิตอล	digital
ตัวกำเนิดโพลิโนเมียล	polynomial generator
ตัวเข้ารหัสเชิงผลต่าง	differential encoder (DE)
ตัวจับคู่สัญลักษณ์	symbol mapper (SM)
ตัวตรวจจับเชิงผลต่าง	differential detecter (DD)
ตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์	multiple symbol differential detector (MSDD)
ตัวสลับลำดับกลับการเข้ารหัส	coding deinterleaver
ตัวสลับลำดับการเข้ารหัส	coding interleaver
ตัวสลับลำดับช่องสัญญาณ	channel interleaver (CI)
ตัวสลับลำดับบิตรหัส	coded bit interleaver (CBI)
ตัวสลับลำดับแบบคี่-คู่	odd-even interleaver
ตัวสลับลำดับแบบบล็อก	block interleaver
ตัวสลับลำดับแบบสุ่ม	random interleaver
บล็อกข้อมูล	data block
บิตข้อมูล	data bit
บิตรหัส	coded bit
บิตหาง	tail bit
เบิรสต์	burst
แบนด์วิดท์	bandwidth
พหุนามป้อนกลับ	feedback polynomial
พหุนามป้อนไปข้างหน้า	feedforward polynomial
พหุวิถี	multipath
ฟังก์ชันความน่าเป็นจริง	likelihood function
ฟังก์ชันเมตริกสาขา	branch metric function
เฟดดิง	fading
เฟดดิงแบบช้า	slow fading
เฟดดิงแบบเร็ว	fast fading
เฟดดิงแบบเรียบ	flat fading

บัญชีคำศัพท์ (ต่อ)

เฟดดิงแบบเลือกความถี่	frequency-selective fading
เฟส	phase
เมตริก	metric
เมตริกช่องสัญญาณ	channel metric
เมตริกทุติยภูมิ	secondary metric
เมตริกปฐมภูมิ	primary metric
รหัสเทอร์โบ	Turbo code
ระดับขนาด	order of magnitude
เรย์ลีเฟดดิง	Rayleigh fading
สัญญาณเชิงซ้อน	complex signal
สัญญาณเบสแบนด์	baseband signal
สัญญาณพาห์	carrier signal
สัญญาณรบกวนเกาส์เซียนสีขาวแบบบวก	additive white Gaussian noise (AWGN)
หน่วยคำนวณเมตริกทุติยภูมิ	secondary metric calculation unit (secondary MCU)
หน่วยคำนวณเมตริกปฐมภูมิ	primary metric calculation unit (primary MCU)
ออสซิลเลเตอร์	oscillator
อัตราการเข้ารหัส	coding rate
อัตราการส่ง	transmission rate
อัตราความผิดพลาดของบล็อก	block error rate (BKER)
อัตราความผิดพลาดของบิต	bit error rate (BER)
อัตราเร็วเฟดดิง	fading rate
อัตราส่วนสัญญาณต่อสัญญาณรบกวน	signal-to-noise ratio (SNR)
อัตสหสัมพันธ์	autocorrelation
แอมพลิจูด	amplitude

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

การสื่อสารแบบไร้สายเข้ามามีบทบาทในโลกยุคปัจจุบันมากขึ้น ระบบโทรศัพท์เคลื่อนที่ถูกพัฒนาให้สามารถส่งสัญญาณเสียง สัญญาณภาพ รวมไปถึงรองรับบริการต่าง ๆ ที่จะมีขึ้นในอนาคต ปัญหาสำคัญสำหรับการสื่อสารในระบบโทรคมนาคมคือสภาพแวดล้อมของตัวกลางที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา ส่งผลให้สัญญาณที่ปลายทางได้รับผิดเพี้ยนไปจากสัญญาณจริงที่ถูกส่งและทำให้การรับส่งข้อมูลเกิดความผิดพลาดขึ้น ด้วยเหตุนี้จึงมีการนำข้อมูลดิจิตอลไปผ่านกระบวนการเข้ารหัสช่องสัญญาณ (channel coding) ก่อนที่จะส่งออก เพื่อให้การรับส่งข้อมูลมีความผิดพลาดน้อยลงและอยู่ในระดับที่ยอมรับได้

การเข้ารหัสช่องสัญญาณเป็นกระบวนการที่ภาคส่งเพิ่มบิตพิเศษเข้าไปกับบิตข้อมูล เพื่อช่วยให้ภาครับสามารถตรวจจับหรือแก้ไขบิตบางบิตที่ผิดพลาดระหว่างการส่งผ่านช่องสัญญาณได้ ทั้งนี้ความสามารถในการแก้ไขบิตที่ผิดพลาดขึ้นอยู่กับขนาดของบิตรหัสที่เพิ่มเข้าไป อย่างไรก็ตาม เมื่อจำนวนบิตรหัสเพิ่มขึ้น ความซับซ้อนและเวลาที่ใช้ในการถอดรหัสก็จะสูงขึ้นตามไปด้วยจนไม่สามารถกระทำได้ในทางปฏิบัติ การศึกษาและค้นคว้ารหัสที่มีสมรรถนะสูงแต่มีความซับซ้อนในกระบวนการถอดรหัสต่ำจึงเกิดขึ้น

รหัสเทอร์โบ (Turbo code) เป็นกรรมวิธีการเข้าและถอดรหัสช่องสัญญาณที่ถูกพัฒนาขึ้นในปี ค.ศ. 1993 โดย Claude Berrou, Alain Glavieux และ Punya Thitimajshima [1] และได้รับความสนใจจากนักวิจัยเป็นอย่างมาก เนื่องจากสามารถจัดการกับปัญหาความผิดพลาดได้อย่างมีประสิทธิภาพในขณะที่มีกระบวนการเข้าและถอดรหัสที่ไม่ซับซ้อน งานวิจัยในช่วงหลายปีที่ผ่านมาชี้ให้เห็นถึงประสิทธิภาพของรหัสเทอร์โบในการส่งสัญญาณผ่านช่องสัญญาณที่มีสัญญาณรบกวนแบบเกาส์ (Gaussian channel) [1-2] โดยรหัสเทอร์โบสามารถให้อัตราความผิดพลาดของบิต (bit error rate : BER) ที่ต่ำ แม้ว่าจะอยู่ในสถานะที่อัตราส่วนสัญญาณต่อสัญญาณรบกวน (signal-to-noise ratio : SNR) มีค่าน้อยก็ตาม นักวิจัยจึงสนใจถึงการนำรหัสเทอร์โบมาประยุกต์ใช้ในงานต่าง ๆ โดยเฉพาะอย่างยิ่งการสื่อสารระบบดิจิตอลในช่องสัญญาณแบบเฟดดิง (fading channel) งานวิจัยในช่วงแรกศึกษาโดยจำกัดให้ช่องสัญญาณเป็นไปตามสมมติฐานที่กำหนดไว้ กล่าวคือ กำหนดให้ระบบรับทราบแอมพลิจูด (amplitude) และเฟส (phase) ของ เฟดดิงอย่างถูกต้อง หรือกำหนดให้ช่องสัญญาณเกิดเฟดดิงที่ไม่มีสหสัมพันธ์กัน (uncorrelated

fading) ต่อมาการศึกษาได้ขยายออกไปในกรณีช่องสัญญาณที่เกิดเรย์ลีเฟดดิงที่มีสหสัมพันธ์กัน (correlated Rayleigh fading channel) เช่น ในงานวิจัยอ้างอิง [3] ซึ่งพิจารณาทั้งในกรณีที่รู้ และไม่รู้แอมพลิจูดของเฟดดิง แต่ยังคงสมมติให้เฟสเป็นค่าที่รับทราบและมีค่าคงที่ในช่วงสัญลักษณ์ช่วงหนึ่ง ๆ สมมติฐานดังกล่าวนำมาใช้ได้เฉพาะในกรณีเฟดดิงแบบช้า (slow fading) เท่านั้น สำหรับกรณีเฟดดิงแบบเร็ว (fast fading) เฟสจะเปลี่ยนแปลงเร็วมากดังนั้นจึงยากที่จะตรวจจับได้

เป็นที่ทราบกันดีว่าเฟดดิงทำให้การส่งสัญญาณในระบบดิจิตอลมีประสิทธิภาพด้อยลงไป ถึงแม้จะเพิ่มอัตราส่วนสัญญาณต่อสัญญาณรบกวน ก็ไม่ทำให้อัตราความผิดพลาดของบิตลดลงได้ เกิดเป็นค่าพื้นของความผิดพลาดขึ้น (error floor) [4] และเมื่อเฟดดิงมีความเร็วเพิ่มขึ้น ค่าพื้นของความผิดพลาดก็จะสูงขึ้นตามไปด้วยเนื่องจากเฟดดิงมีผลทำให้สัญญาณที่ภาครับได้รับมีความผิดเพี้ยนไป ทั้งในแง่ของแอมพลิจูดที่ถูกลดทอนและเฟสที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา โดยเฉพาะอย่างยิ่งสัญญาณที่ถูกมอดูเลตทางเฟส หรือที่เรียกว่า สัญญาณ M-PSK (M-ary Phase Shift Keying) ข่าวสารของสัญญาณจะถูกเข้ารหัสให้อยู่ในรูปของเฟสของสัญญาณพาห์ (carrier signal) ดังนั้นเพื่อให้ได้สมรรถนะที่ดีที่สุด ภาครับจำเป็นจะต้องมีการซิงโครไนซ์เฟส (phase synchronization) ที่แม่นยำ เพื่อใช้ตรวจหาสัญญาณที่ถูกต้องที่ถูกส่งมา วิธีการเช่นนี้เรียกว่า การตรวจจับแบบร่วมนัย (coherent detection) ซึ่งมีความซับซ้อนสูง เนื่องจากภาครับต้องมีความสามารถในการติดตามเฟสของสัญญาณพาห์ที่เปลี่ยนแปลงอย่างรวดเร็วได้ ทั้งนี้ในระบบสื่อสารไร้สายส่วนใหญ่ ภาครับไม่สามารถจะรับทราบเฟสที่ถูกต้องของสัญญาณพาห์ได้เลย วิธีการนี้จึงไม่สามารถนำมาใช้ได้ในทางปฏิบัติ เทคนิคการแทรกสัญลักษณ์ไพลอต (pilot symbol insertion) เข้าไปในชุดลำดับข้อมูลอาจช่วยลดปัญหาข้างต้นได้บ้าง แต่ระบบก็ต้องสูญเสียพลังงานและแบนด์วิดท์ (bandwidth) บางส่วนไป

วิธีการที่นำมาใช้แทนการตรวจจับแบบร่วมนัย (coherent detection) คือ การตรวจจับแบบไม่ร่วมนัย (noncoherent detection) ขั้นตอนหนึ่งที่นิยมใช้คือการเข้ารหัสเชิงผลต่าง (differential encoding) ที่ภาคส่งหลังจากที่สัญญาณถูกมอดูเลตทางเฟสแล้ว วิธีนี้ทำให้ข่าวสารของสัญญาณถูกเข้ารหัสอยู่ในผลต่างระหว่างเฟสของสัญลักษณ์ที่อยู่ติดกัน ทางภาครับสามารถตรวจจับข่าวสาร โดยการหาผลต่างระหว่างเฟสของสัญลักษณ์ก่อนหน้าและสัญลักษณ์ปัจจุบันที่รับได้ เรียกวิธีการนี้ว่า การตรวจจับเชิงผลต่าง (differential detection) จะเห็นว่าการตรวจจับเชิงผลต่างอาศัยช่วงสังเกตการณ์ (observation interval) เพียงสองสัญลักษณ์เท่านั้น และไม่ต้องการการซิงโครไนซ์สัญญาณพาห์อีกต่อไป การตรวจจับเชิงผลต่างจึงมีความซับซ้อนต่ำกว่าการตรวจจับแบบร่วมนัยมาก งานวิจัยเกี่ยวกับการตรวจจับเชิงผลต่างได้แก่ งานวิจัยอ้างอิง [5] ซึ่งนำตัวตรวจจับเชิงผลต่างมาใช้ร่วมกับการถอดรหัสเทอร์โบ ในช่องสัญญาณที่เกิดเรย์ลีเฟดดิงแบบเร็วที่มีสหสัมพันธ์กัน (correlated fast Rayleigh fading channel) เทคนิคดังกล่าวทำให้อัตรา

ความผิดพลาดของบิต (bit error rate : BER) และอัตราความผิดพลาดของบล็อก (block error rate :BKER) ต่ำกว่าการใช้รหัสคอนโวลูชัน (convolutional code) อย่างไรก็ดี เนื่องจากการตรวจจับเชิงผลต่างอาศัยช่วงสังเกตการณ์เพียง 2 สัญลักษณ์ในการประมาณเฟสที่ผิดพลาด ผลที่ได้จึงแย่กว่าการตรวจจับแบบร่วมนัย ทำให้เกิดเป็นข้อด้อยของการตรวจจับแบบไม่ร่วมนัยขึ้น (noncoherence penalty) นอกจากนี้เมื่ออัตราเร็วเฟดดิง (fading rate) เพิ่มขึ้น ตัวตรวจจับเชิงผลต่างก็ไม่สามารถตรวจจับการเปลี่ยนแปลงของเฟสที่เกิดขึ้นอย่างรวดเร็วได้อีกต่อไป ถึงแม้จะเพิ่มจำนวนรอบของการถอดรหัสเทอร์โบก็ไม่ทำให้สมรรถนะดีขึ้นได้

การตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ (multiple symbol differential detection : MSDD) จึงถูกเสนอขึ้นเพื่อปรับปรุงสมรรถนะของการตรวจจับเชิงผลต่างแบบเดิม โดยการเพิ่มช่วงสังเกตการณ์ของสัญลักษณ์ที่รับได้ที่ภาครับเป็นมากกว่า 2 สัญลักษณ์ ทำให้เครื่องรับสามารถประมาณช่องสัญญาณได้แม่นยำมากขึ้น งานวิจัยที่ผ่านมา [6-12] ชี้ให้เห็นว่าการตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ มีผลทำให้ค่าพื้นของความผิดพลาดลดลง เนื่องจากการตรวจจับการเปลี่ยนแปลงของเฟสดีขึ้น พร้อมทั้งยังช่วยลดจุดด้อยของเครื่องรับแบบไม่ร่วมนัยที่จำเป็นต้องใช้อัตราส่วนสัญญาณต่อสัญญาณรบกวนสูงกว่าเครื่องรับแบบร่วมนัยได้อีกด้วย

งานวิจัยอ้างอิง [13] เสนอให้นำตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์มาใช้ร่วมกับการถอดรหัสเทอร์โบ โดยประยุกต์ให้ตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์แบบเดิมสามารถทำงานร่วมกับตัวสลับลำดับช่องสัญญาณ (channel interleaver) และตัวถอดรหัสเทอร์โบซึ่งมีการส่งผ่านข่าวสารแบบซอฟต์ (soft information) ได้ นอกจากนี้ในงานวิจัยดังกล่าวยังออกแบบให้มีการแลกเปลี่ยนข่าวสารที่เรียกว่าข่าวสารเอ็กซ์ทรินซิก (extrinsic information) ระหว่างตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์และตัวถอดรหัสเทอร์โบอีกด้วย ทำให้การประมาณข่าวสารช่องสัญญาณดีขึ้นในแต่ละรอบของการถอดรหัสเทอร์โบ ผลที่แสดงในงานวิจัยนี้ชี้ให้เห็นว่าตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์มีสมรรถนะที่ดีกว่าตัวตรวจจับเชิงผลต่างแบบเดิมมาก โดยเฉพาะอย่างยิ่งเมื่ออัตราเร็วเฟดดิงมีค่าสูง ซึ่งเฟดดิงจะมีการเปลี่ยนแปลงทั้งแอมพลิจูดและเฟสอย่างรวดเร็ว อย่างไรก็ตามวิธีการวิเคราะห์ในงานวิจัยดังกล่าวได้จัดให้บิตข้อมูล (data bit) และบิตรหัส (coded bit) ที่ได้จากการเข้ารหัสเทอร์โบของบิตข้อมูลนั้น ถูกจับคู่อยู่ในสัญลักษณ์ QPSK เดียวกัน แล้วส่งออกไปทางภาคส่ง เมื่อไปผ่านช่องสัญญาณแบบเฟดดิง บิตข้อมูลและบิตรหัสก็จะเสียหายไปพร้อมกันด้วยทำให้ภาครับไม่ได้รับทราบข่าวสารของบิตนั้นเลย

ดังนั้นในงานวิจัยนี้จึงเสนอวิธีการวิเคราะห์ที่สามารถแยกคิดบิตข้อมูล และบิตรหัสของบิตข้อมูลนั้นออกจากกัน โดยที่ตัวถอดรหัสเทอร์โบยังคงสามารถใช้ข่าวสารช่องสัญญาณ ซึ่งมาจากสัญลักษณ์ที่บิตข้อมูลและบิตรหัสถูกจับแยกออกจากกันได้

1.2 แนวทางของงานวิจัย

งานวิจัยนี้จะใช้การถอดรหัสแบบวนซ้ำของรหัสเทอร์โบ ร่วมกับโครงสร้างของภาครับที่ประกอบด้วยตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ซึ่งอาศัยข้อมูลทางสถิติของเฟดดิงในการประมาณค่าแอมพลิจูดและเฟสที่เปลี่ยนแปลงอย่างรวดเร็ว โดยพิจารณาในกรณีช่องสัญญาณที่เกิดเรย์ลีเฟดดิงที่มีสหสัมพันธ์กัน เฟดดิงที่เกิดขึ้นจะมีความสัมพันธ์กันทางเวลา ทำให้ความผิดพลาดที่เกิดจากเฟดดิงมีแนวโน้มที่จะเกิดเป็นเบิรสต์ (burst) คือมีความผิดพลาดที่ติดกันเป็นช่วงยาวซึ่งแก้ไขได้ยาก งานวิจัยนี้เสนอให้ภาคส่งแยกส่งบิตข้อมูลและบิตรหัสของบิตข้อมูลนั้นออกจากกัน กล่าวคือ ไม่ส่งไปในสัญลักษณ์ QPSK เดียวกัน เพื่อหลีกเลี่ยงการสูญหายของข่าวสารของบิตนั้นเมื่อผ่านเฟดดิง โดยเฉพาะอย่างยิ่งเมื่อช่องสัญญาณอยู่ในสถานะเลวร้าย คือ เกิดเบิรสต์เป็นช่วงยาว การที่ภาครับไม่ได้รับทราบข่าวสารของบิตทั้งที่มาจากบิตข้อมูลเองหรือจากบิตรหัสของบิตข้อมูลนั้นจะทำให้ตัวถอดรหัสเทอร์โบไม่สามารถถอดรหัสได้อย่างถูกต้อง การแยกส่งบิตข้อมูลและบิตรหัสของบิตข้อมูลนั้นออกจากกัน จึงเป็นการช่วยเพิ่มโอกาสที่ภาครับจะได้ รับทราบข่าวสารของบิตนั้นจากทางใดทางหนึ่งนั่นเอง ทั้งนี้ที่ภาครับก็จำเป็นจะต้องวิเคราะห์ให้ตัวถอดรหัสเทอร์โบสามารถใช้ข่าวสารช่องสัญญาณ ซึ่งสัญลักษณ์ที่ถูกส่งมาจากการแยกบิตข้อมูลกับบิตรหัสออกจากกันได้ นอกจากนี้งานวิจัยที่เสนอยังคำนึงถึงการใช้ข่าวสารเอ็กซ์ทรินซิกให้เกิดประโยชน์สูงสุด โดยออกแบบให้ตัวถอดรหัสเทอร์โบคำนวณข่าวสารเอ็กซ์ทรินซิกของสัญลักษณ์ที่ถูกส่งมาอีกด้วย ข่าวสารนี้เป็นค่าที่บอกว่าสัญลักษณ์ที่ถูกส่งมาคือสัญลักษณ์ใดด้วยความน่าจะเป็นเท่าไร ซึ่งข่าวสารดังกล่าวจะถูกส่งกลับไปให้ตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์อีกครั้งหนึ่งเพื่อใช้ปรับปรุงข่าวสารช่องสัญญาณ ทำให้การประมาณช่องสัญญาณดีขึ้นในแต่ละรอบของการถอดรหัส เป็นผลให้ตัวถอดรหัสเทอร์โบสามารถทำงานได้อย่างมีประสิทธิภาพมากขึ้น

1.3 วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาการตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์และนำมาประยุกต์ใช้ร่วมกับการถอดรหัสแบบวนซ้ำ สำหรับช่องสัญญาณที่เกิดเรย์ลีเฟดดิงที่มีสหสัมพันธ์กัน
2. วิเคราะห์สมรรถนะของตัวถอดรหัสแบบวนซ้ำที่ทำงานร่วมกับตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ และปรับปรุงอัลกอริทึมเดิมให้มีสมรรถนะสูงขึ้น

1.4 ขอบเขตของวิทยานิพนธ์

1. เขียนโปรแกรมจำลองการถอดรหัสแบบวนซ้ำ ที่นำมาประยุกต์ใช้ร่วมกับการตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ตามอัลกอริทึมในงานวิจัยที่ผ่านมา พร้อมทั้งทดสอบสมรรถนะและตรวจสอบผลที่ได้กับงานวิจัยดังกล่าว
2. ปรับปรุงระบบเดิมโดยใช้อัลกอริทึมตามที่เสนอในแนวทางของงานวิจัยและทดสอบสมรรถนะของวิธีที่นำเสนอ ร่วมกับการวิเคราะห์ผลเปรียบเทียบกับอัลกอริทึมเดิม

1.5 ขั้นตอนและวิธีการดำเนินงาน

1. ศึกษาความรู้พื้นฐานของการถอดรหัสแบบวนซ้ำ
2. ศึกษาการเข้ารหัสและถอดรหัสสัญญาณผ่านช่องสัญญาณที่เกิดเรย์ลีเฟดดิง
3. ศึกษาและวิเคราะห์การประยุกต์ใช้ตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ในการ ถอดรหัสแบบวนซ้ำสำหรับช่องสัญญาณที่เกิดเรย์ลีเฟดดิงที่มีสหสัมพันธ์กัน
4. จำลองการถอดรหัสแบบวนซ้ำร่วมกับการตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ตามอัลกอริทึมในงานวิจัยที่ผ่านมา พร้อมทั้งตรวจสอบผลที่ได้กับงานวิจัยดังกล่าว
5. หาอัลกอริทึมเพื่อปรับปรุงให้ระบบมีสมรรถนะที่ดีขึ้น
6. จำลองการถอดรหัสแบบวนซ้ำร่วมกับการตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ด้วยอัลกอริทึมที่พัฒนาขึ้น
7. เปรียบเทียบและวิเคราะห์ผลจากการจำลองการถอดรหัส
8. สรุป วิจารณ์ และจัดทำวิทยานิพนธ์

1.6 ประโยชน์ที่คาดว่าจะได้รับ

สามารถพัฒนาอัลกอริทึมในการถอดรหัสแบบวนซ้ำ ร่วมกับการตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ เพื่อลดความผิดพลาดในการส่งสัญญาณผ่านช่องสัญญาณที่เกิดเรย์ลีเฟดดิงที่มีสหสัมพันธ์กัน ทำให้ระบบมีสมรรถนะที่ดีขึ้น

บทที่ 2

โครงสร้างของภาคส่ง

เนื้อหาในบทนี้และบทต่อจากนี้ไปอีกสองบท คือ บทที่ 3 และบทที่ 4 จะกล่าวถึงแบบจำลองการรับส่งสัญญาณดิจิตอลในระบบสื่อสาร โดยแบ่งเนื้อหาออกเป็น 3 ส่วน คือ โครงสร้างของภาคส่ง ช่องสัญญาณ และโครงสร้างของภาครับ สำหรับในบทนี้จะอธิบายถึงโครงสร้างของภาคส่ง ซึ่งประกอบด้วยการเข้ารหัสเทอร์โบ การจับคู่สัญลักษณ์ การสลับลำดับช่องสัญญาณ และการเข้ารหัสเชิงผลต่าง

2.1 การเข้ารหัสเทอร์โบ

การเข้ารหัสเทอร์โบนั้นอาศัยการเข้ารหัสของเครื่องเข้ารหัสคอนโวลูชันแบบมีระบบที่มีการป้อนกลับ (recursive systematic convolutional encoder : RSC) ตั้งแต่ 2 ตัวขึ้นไป นำมาต่อขนานกันและมีตัวสลับลำดับการเข้ารหัส (coding interleaver) ต่ออยู่ด้านหน้า เครื่องเข้ารหัสคอนโวลูชันย่อยแต่ละตัวไม่จำเป็นต้องเหมือนกัน ทั้งนี้ชุดของบิตข้อมูลที่ป้อนให้กับเครื่องเข้ารหัสย่อยแต่ละตัวนั้นเป็นชุดของบิตข้อมูลเดียวกันเพียงแต่ถูกสลับลำดับในการป้อนเข้าสู่เครื่องเข้ารหัสด้วยตัวสลับลำดับการเข้ารหัสนั่นเอง

เครื่องเข้ารหัสเทอร์โบที่มีอัตราการเข้ารหัส (coding rate) เท่ากับ $\frac{1}{2}$ แสดงอยู่ในรูปที่ 2.1 เครื่องเข้ารหัสนี้ถูกดัดแปลงจากเครื่องเข้ารหัสแบบดั้งเดิมที่ Berrou [1] ได้เสนอขึ้น โดยที่เครื่องเข้ารหัสย่อยทั้งสองตัวเป็นเครื่องเข้ารหัสคอนโวลูชันแบบมีระบบที่มีการป้อนกลับชนิดเดียวกัน ซึ่งมีพหุนามป้อนไปข้างหน้า (feedforward polynomial) เป็น $1+D^4$ และมีพหุนามป้อนกลับ (feedback polynomial) เป็น $1+D+D^2+D^3+D^4$ หรือเขียนให้อยู่ในระบบเลขฐานแปดได้เป็น $(1, \frac{21}{37})_8$ บิตข้อมูลที่ป้อนเข้าสู่เครื่องเข้ารหัสเทอร์โบจะถูกแบ่งออกเป็นชุด ๆ แต่ละชุดเรียกว่า บล็อกข้อมูล (data block) ชุดของลำดับข้อมูล $a_1, a_2, ..., a_n, ..., a_{N_b}$ ซึ่งเขียนแทนด้วย $\underline{a}_1^{N_b}$ เป็นบล็อกข้อมูลที่มีขนาด N_b บิต โดยที่ N_b คือความยาวของบล็อก (block length) a_n คือบิตข้อมูล (data bit) ลำดับที่ n ที่ถูกป้อนเข้าสู่เครื่องเข้ารหัสเทอร์โบ เอาต์พุตของเครื่องเข้ารหัสเทอร์โบจะประกอบด้วยสองส่วน ส่วนแรกคือบิตข้อมูล a_n ที่ไม่มีการเข้ารหัสแต่อย่างใด และส่วนที่สองคือบิตรหัส (coded bit) หรือ บิตพาริตี (parity bit) ซึ่งเป็นบิตที่ได้จากการเข้ารหัสบิตข้อมูลที่เครื่องเข้ารหัสคอนโวลูชันย่อย บิตรหัสที่ได้นี้จะเขียนแทนด้วยสัญลักษณ์ p_n ดังแสดงในรูปที่ 2.1

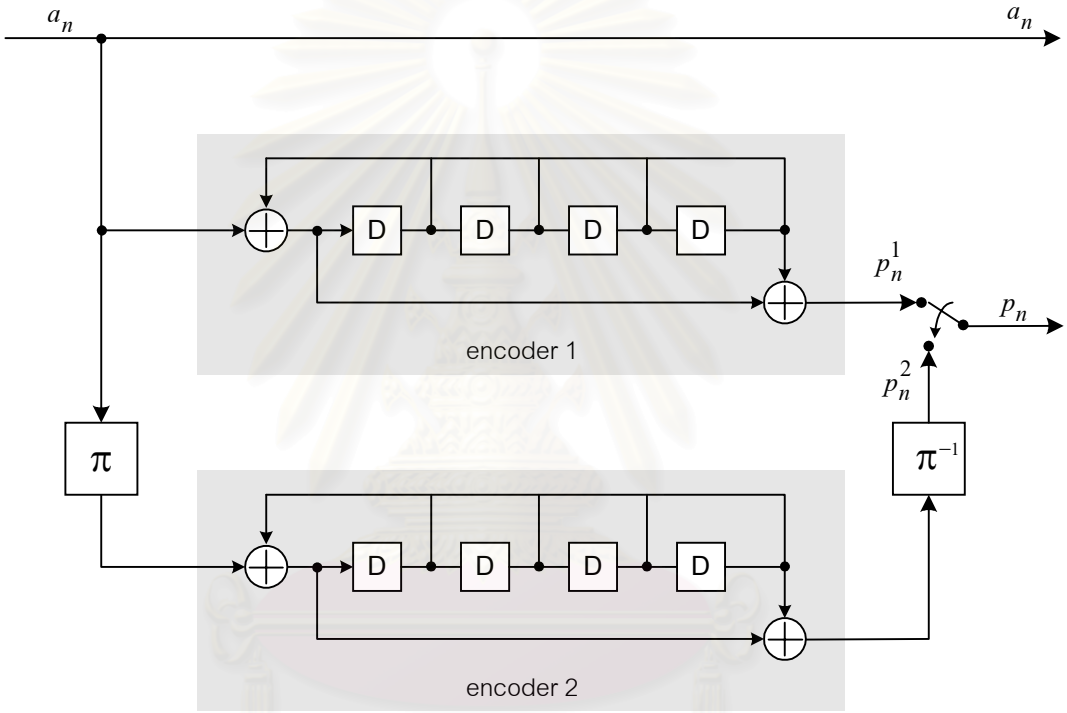
อย่างไรก็ตาม บิตรหัส p_n ที่ได้นี้จะมาจากเครื่องเข้ารหัสย่อยตัวใดตัวหนึ่งเท่านั้น เนื่องจากที่ส่วนท้ายของเครื่องเข้ารหัสเทอร์โบมีวงจรพังเจอร์ (puncture) ต่ออยู่ด้วย วงจรพังเจอร์ทำหน้าที่เลือกบิตรหัสที่จะถูกส่งออกไปเป็นเอาต์พุตของเครื่องเข้ารหัสเทอร์โบ โดยการเลือกสลับไปมาระหว่างเครื่องเข้ารหัสย่อยทั้งสองตัวทีละบิต กล่าวคือ ถ้าลำดับที่ n บิตรหัส p_n มาจากเครื่องเข้ารหัสย่อยตัวที่หนึ่ง (p_n^1) ที่ลำดับถัดไปคือ n+1 บิตรหัส p_{n+1} จะได้มาจากเครื่องเข้ารหัสย่อยตัวที่สอง (p_n^2) การพังเจอร์ตามที่กล่าวนี้จะทำให้อัตราการเข้ารหัสมีค่าสูงขึ้น ในที่นี้คือ เพิ่มขึ้นจาก $\frac{1}{3}$ เป็น $\frac{1}{2}$ แต่ก็ทำให้สูญเสียข้อมูลส่วนที่ถูกเข้ารหัสไปถึงครึ่งหนึ่ง

ตัวสลับลำดับการเข้ารหัส (coding interleaver : π) ที่ต่ออยู่กับเครื่องเข้ารหัสย่อยตัวที่สอง ทำหน้าที่สลับลำดับบิตข้อมูลในบล็อกข้อมูล $\underline{a}_1^{N_b}$ ก่อนที่จะป้อนเข้าสู่เครื่องเข้ารหัสย่อย ดังนั้นลำดับในการเข้ารหัสบิตข้อมูลของเครื่องเข้ารหัสย่อยทั้งสองตัวจึงแตกต่างกัน ที่ทำเช่นนี้เนื่องจากต้องการให้ชุดของบิตรหัสที่ได้มีค่าแตกต่างกัน ทั้งที่เกิดจากการเข้ารหัสชุดของบิตข้อมูลชุดเดียวกัน ทำให้ภาครับได้รับทราบข่าวสารของบิตข้อมูลแต่ละบิตเพิ่มขึ้น โดยหวังว่าบิตรหัสที่แตกต่างกันนี้จะช่วยให้การถอดรหัสเทอร์โบทำงานได้อย่างมีประสิทธิภาพมากขึ้น กล่าวคือถ้าเครื่องถอดรหัสเทอร์โบไม่สามารถตัดสินบิตได้ถูกต้อง เมื่อทราบเพียงบิตข้อมูลกับบิตรหัสที่มาจากเครื่องเข้ารหัสย่อยตัวที่หนึ่ง บิตรหัสที่ได้จากเครื่องเข้ารหัสย่อยตัวที่สองควรจะทำให้การถอดรหัสมีความถูกต้องมากขึ้นได้ เพราะฉะนั้นการเลือกใช้ตัวสลับลำดับการเข้ารหัสจึงมีผลกับสมรรถนะของรหัสเทอร์โบเป็นอย่างมาก

หลังจากเข้ารหัสบิตข้อมูลที่เครื่องเข้ารหัสย่อยตัวที่สองแล้ว ชุดของบิตรหัสที่ได้จะถูกสลับลำดับกลับไปอยู่ในลำดับเดียวกับชุดของบิตข้อมูล $\underline{a}_1^{N_b}$ อีกครั้งโดยตัวสลับลำดับกลับการเข้ารหัส (coding deinterleaver : π^{-1}) ที่ทำเช่นนี้ก็เพื่อให้ลำดับของบิตรหัสที่ได้จากเครื่องถอดรหัสย่อยตัวที่สองตรงกันกับลำดับของบิตข้อมูลและบิตรหัสที่ได้จากเครื่องเข้ารหัสย่อยตัวแรก เนื่องจากบิตรหัสที่ได้จากเครื่องเข้ารหัสย่อยทั้งสองตัวจะถูกส่งไปที่วงจรพังเจอร์ เพื่อทำให้อัตราการเข้ารหัสเป็น $\frac{1}{2}$ ดังนั้นการทำให้ลำดับของบิตรหัสทั้งสองบิตตรงกันจึงเป็นการรับประกันว่าบิตข้อมูลทุกตัวจะถูกส่งออกไปพร้อมกับบิตรหัสที่ได้จากการเข้ารหัสบิตข้อมูลนั้น ถ้าไม่สลับลำดับบิตรหัสชุดที่สองกลับให้ตรงกันกับลำดับของบิตรหัสชุดแรกจะทำให้บิตข้อมูลบางบิตมีบิตรหัสของบิตข้อมูลนั้นถูกส่งออกไปถึงสองบิต ในขณะที่บิตข้อมูลบางบิตก็ไม่มีบิตรหัสถูกส่งออกไปด้วยเลย เป็นผลให้สมรรถนะของเครื่องถอดรหัสเทอร์โบแย่ลงไป

หลังจากเข้ารหัสบล็อกข้อมูลเสร็จแล้ว จะต้องส่งบิตข้อมูลส่วนท้าย ที่เรียกว่า บิตหาง (tail bit) เพิ่มเข้าไป เพื่อทำให้สถานะของเครื่องเข้ารหัสย่อยแต่ละตัวเป็นศูนย์ และเนื่องจากเครื่องเข้ารหัสย่อยแต่ละตัวที่นำมาใช้ในเครื่องเข้ารหัสเทอร์โบ เป็นเครื่องเข้ารหัสคอนโวลูชันแบบมีระบบที่มี

การป้อนกลับ ซึ่งโดยทั่วไปแล้วจะไม่สามารถทำให้สถานะของเครื่องเข้ารหัสย่อยทุกตัวเป็นศูนย์พร้อมกันด้วยบิตหางเพียงชุดเดียวได้ อย่างไรก็ตาม หากพิจารณาถึงลักษณะการเปลี่ยนสถานะในกระบวนการเข้ารหัสของเครื่องเข้ารหัสคอนโวลูชันแบบมีระบบที่มีการป้อนกลับ โดยคำนึงถึงความสัมพันธ์กับการออกแบบตัวสลับลำดับการเข้ารหัสแล้ว จะสามารถทำให้สถานะสุดท้ายของเครื่องเข้ารหัสย่อยทั้งสองตัวเป็นศูนย์พร้อมกันได้โดยใช้บิตหางที่เหมือนกันเพียงชุดเดียวเท่านั้น การทำงานของเครื่องเข้ารหัสย่อย และรายละเอียดของตัวสลับลำดับการเข้ารหัสจะอธิบายในหัวข้อต่อไป

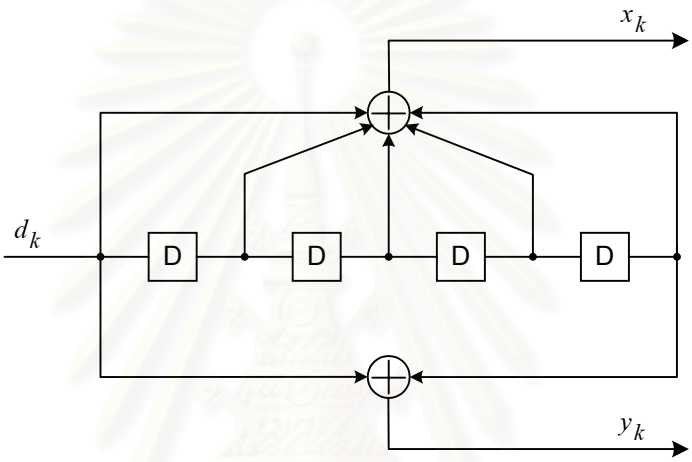


รูปที่ 2.1 เครื่องเข้ารหัสเทอร์โบ

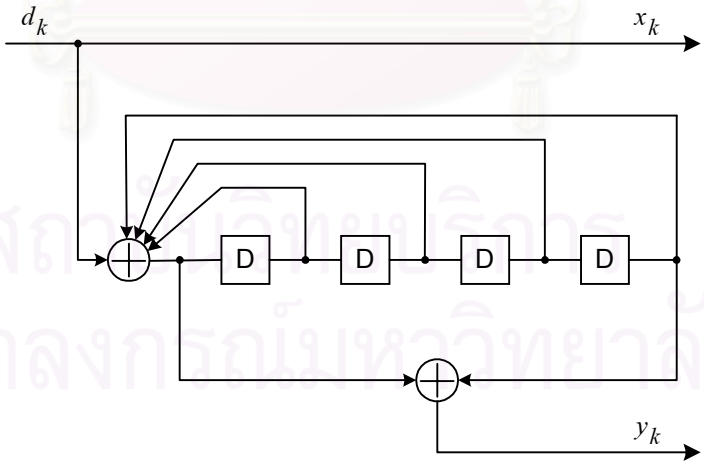
2.1.1 เครื่องเข้ารหัสย่อย

ตามที่ได้กล่าวไปแล้วว่า เครื่องเข้ารหัสย่อยแต่ละตัวของเครื่องเข้ารหัสเทอร์โบ เป็นเครื่องเข้ารหัสคอนโวลูชันแบบมีระบบที่มีการป้อนกลับ (recursive systematic convolutional encoder : RSC) ซึ่งได้มาจากการดัดแปลงเครื่องเข้ารหัสคอนโวลูชันแบบเดิม หรือที่เรียกว่า เครื่องเข้ารหัสคอนโวลูชันแบบไม่มีระบบ (non systematic convolutional encoder : NSC) โดยการใช้ลูปป้อนกลับ (feedback loop) ส่งบิตที่อยู่ในวงจรเข้ารหัสกลับไปยังขาเข้าของเครื่องเข้ารหัสอีกครั้งหนึ่ง นอกจากนี้ยังกำหนดให้เอาต์พุตด้านหนึ่งของเครื่องเข้ารหัส มีค่าเท่ากับอินพุตที่ป้อนเข้าสู่เครื่อง

เข้ารหัสอีกด้วย รูปที่ 2.2 แสดงเครื่องเข้ารหัส NSC เปรียบเทียบกับเครื่องเข้ารหัส RSC ที่มีอัตราการเข้ารหัสเท่ากับ $\frac{1}{2}$ ความยาวคอนสเตรนต์ (constraint length) เท่ากับ 5 บิต และมีขนาดหน่วยความจำ (memory size : m) เท่ากับ 4 บิต อินพุตของเครื่องเข้ารหัสที่เวลา k คือ บิตข้อมูล d_k และได้เอาต์พุตคือ คำรหัส (code word) ที่ประกอบด้วยคู่บิต (x_k, y_k) และในกรณีที่เป็นเครื่องเข้ารหัส RSC จะได้ว่า x_k มีค่าเท่ากับบิตข้อมูล d_k ตัวกำเนิดโพลิโนเมียล (polynomial generator) ของเครื่องเข้ารหัส NSC และเครื่องเข้ารหัส RSC คือ (37,21) และ $(1, \frac{21}{37})$ ตามลำดับ



(ก)



(ข)

รูปที่ 2.2 เครื่องเข้ารหัสคอนโวลูชัน

() เครื่องเข้ารหัส NSC

() เครื่องเข้ารหัส RSC

2.1.2 ตัวสลับลำดับการเข้ารหัส

สมรรถนะของรหัสเทอร์โบนั้นขึ้นอยู่กับปัจจัยหลายอย่าง หนึ่งในนั้นก็คือ ชนิดและขนาดของตัวสลับลำดับการเข้ารหัส เนื่องจากโครงสร้างของตัวสลับลำดับการเข้ารหัส จะส่งผลต่อลักษณะการกระจายบิตของรหัสเทอร์โบ ซึ่งมีกระบวนการถอดรหัสแบบวนซ้ำของเครื่องถอดรหัสย่อยมากกว่าหนึ่งตัว จุดประสงค์หลักของตัวสลับลำดับการเข้ารหัส ก็คือการเพิ่มระยะห่างน้อยที่สุด (minimum distance) ของรหัสเทอร์โบ ทั้งนี้เพื่อให้บิตที่ยังคงผิดพลาดอยู่หลังจากการถอดรหัสที่เครื่องถอดรหัสย่อยตัวแรก ถูกแก้ไขให้ถูกต้องได้ที่เครื่องถอดรหัสย่อยตัวอื่น นอกจากนี้ตัวสลับลำดับการเข้ารหัส ยังส่งผลต่อรูปแบบของบิตหางที่จะป้อนเข้าสู่เครื่องเข้ารหัสย่อยอีกด้วย งานวิจัยอ้างอิง [14] ได้ออกแบบตัวสลับลำดับการเข้ารหัสแบบพิเศษ ที่ทำให้สถานะของเครื่องเข้ารหัสย่อยทั้งสองตัวหลังการเข้ารหัสบิตข้อมูลทั้งหมดมีสถานะเหมือนกัน ดังนั้นจึงสามารถใช้บิตหางเพียงชุดเดียวเท่านั้นในการขับให้สถานะสุดท้ายของเครื่องเข้ารหัสย่อยทั้งสองตัวเป็นศูนย์ ตัวสลับลำดับการเข้ารหัสนี้ เรียกว่า ตัวสลับลำดับแบบ simile (simile interleaver)

ตัวสลับลำดับแบบ simile ได้มาจากการประยุกต์ใช้ตัวสลับลำดับแบบ helical block ชนิดหนึ่ง (helical block interleaver) [15] นอกเหนือจากนั้น ถ้านำคุณสมบัติของการสลับลำดับแบบคี่-คู่ (odd-even interleaving) [16] มาใช้ร่วมด้วย ก็จะทำให้ความสามารถในการแก้ไขความผิดพลาดมีการกระจายแบบสม่ำเสมอในบิตข้อมูลทุกบิต ตัวสลับลำดับการเข้ารหัสที่กล่าวถึงนี้คือ ตัวสลับลำดับแบบ simile odd-even helical block ซึ่งได้มาจากการออกแบบตัวสลับลำดับแบบ helical block ให้สอดคล้องกับเงื่อนไขบางประการ ได้แก่ ความกว้าง (width) ของตัวสลับลำดับต้องเป็นเลขคู่ และมีค่าเป็นพหุคูณของ m+1 โดยที่ m คือขนาดหน่วยความจำของเครื่องเข้ารหัสย่อย ทั้งนี้ความกว้างและความลึก (depth) ของตัวสลับลำดับ จะต้องเป็นตัวเลขที่หารกันไม่ลงตัวอีกด้วย [15] ตัวอย่างของตัวสลับลำดับแบบ simile odd-even helical block อยู่ในตารางที่ 2.1

ตารางที่ 2.1 ตัวสลับลำดับแบบ simile odd-even helical block ขนาด 5×6 บิต

() อินพุตของตัวสลับลำดับ

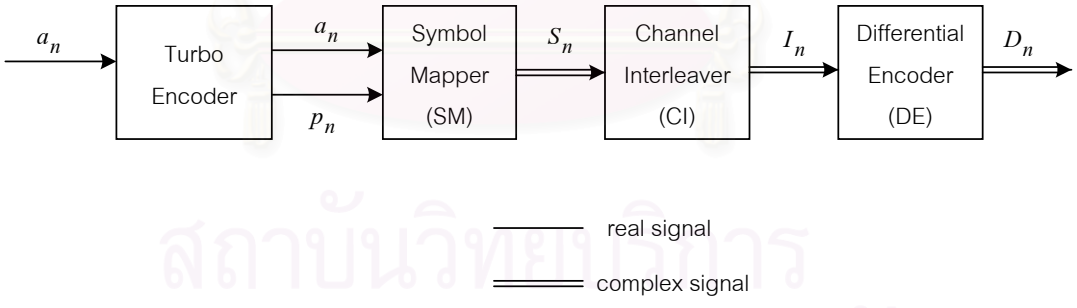
1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30

() เอาต์พุตที่ได้จากตัวสลับลำดับ

25	20	15	10	5	30	19	14	9	4	29	24	13	8	3
28	23	18	7	2	27	22	17	12	1	26	21	16	11	6

ตัวสลับลำดับในตารางที่ 2.1 มีขนาดหน่วยความจำเท่ากับ 2 ความกว้างเท่ากับ 6 (6 เป็นเลขคู่และมีค่าเป็น 2 เท่าของ 3) และมีความลึกเท่ากับ 5 ในงานวิจัยนี้จะใช้ตัวสลับลำดับการเข้ารหัสที่มีขนาดต่าง ๆ กัน คือ 420 บิต 930 บิต และ 2550 บิต ซึ่งเป็นตัวสลับลำดับที่มีความลึกและความกว้างเป็น 21×20 31×30 และ 51×50 ตามลำดับ

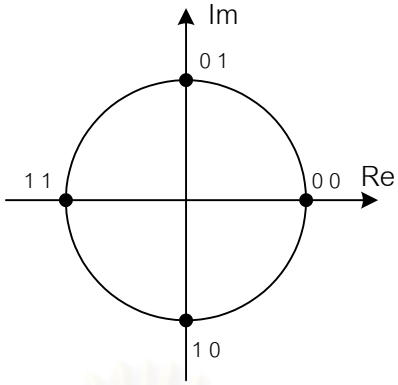
หลังจากบิตข้อมูล a_n ถูกเข้ารหัสที่เครื่องเข้ารหัสเทอร์โบแล้ว จะได้เอาต์พุตเป็นคำรหัส (a_n, p_n) ซึ่งยังไม่สามารถส่งออกไปที่ภาคส่งได้ คำรหัส (a_n, p_n) จะถูกนำไปผ่านกระบวนการจับคู่สัญลักษณ์ การสลับลำดับช่องสัญญาณ และการเข้ารหัสเชิงผลต่าง โครงสร้างของภาคส่งที่กล่าวนี้แสดงอยู่ในรูปที่ 2.3



รูปที่ 2.3 โครงสร้างของภาคส่ง

2.2 การจับคู่สัญลักษณ์

ตัวจับคู่สัญลักษณ์ (symbol mapper : SM) จะจับคู่คำรหัส (a_n, p_n) ไปเป็นสัญลักษณ์ QPSK S_n โดยใช้การจับคู่แบบเกรย์ (Gray mapping) [17] ซึ่งเป็นไปตามรูปที่ 2.4 สัญลักษณ์ QPSK ที่ได้จะอยู่ในรูปของสัญญาณเชิงซ้อน (complex signal) ดังแสดงในตารางที่ 2.2



รูปที่ 2.4 การจัดตำแหน่งของสัญลักษณ์ QPSK

ตารางที่ 2.2 การจับคู่คำรหัส (a_n, p_n) ไปเป็นสัญลักษณ์ QPSK

คำรหัส (a_n, p_n)	สัญลักษณ์ QPSK (จำนวนเชิงซ้อน)
0 0	1 + j 0
0 1	0 + j 1
1 0	-1+ j 0
1 1	-1 – j 1

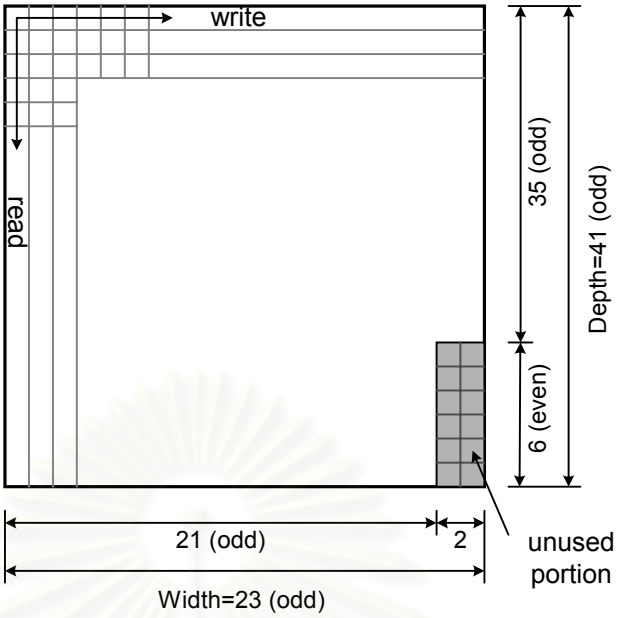
2.3 การสลับลำดับช่องสัญญาณ

การสลับลำดับของสัญลักษณ์ก่อนที่จะส่ง เป็นวิธีหนึ่งที่จะช่วยป้องกันผลของเฟดดิงที่เกิดขึ้นในช่องสัญญาณได้ โดยตัวสลับลำดับช่องสัญญาณ (channel interleaver : CI) จะช่วยให้ผลกระทบที่เกิดจากความสัมพันธ์กันทางเวลาของเฟดดิงลดลง ทำให้ช่องสัญญาณที่แต่ละเวลาเสมือนไร้สหสัมพันธ์กันเมื่อปรากฏต่อภาคถอดรหัส ทั้งนี้ก็ขึ้นอยู่กับประเภทและขนาดของตัวสลับลำดับด้วย ตัวสลับลำดับแบบบล็อก (block interleaver) เป็นอีกชนิดหนึ่งที่มักถูกนำมาใช้เป็นตัวสลับลำดับช่องสัญญาณ เนื่องจากมีโครงสร้างที่ไม่ซับซ้อน และมีความสามารถในการกระจายความสัมพันธ์ได้ดี [18] อีกทั้งยังมีลักษณะการจัดเรียงข้อมูลแตกต่างไปจากตัวสลับลำดับแบบ simile odd-even helical block ที่ใช้ในการสลับลำดับการเข้ารหัสอีกด้วย จึงสามารถนำมาใช้ในการสลับลำดับช่องสัญญาณได้

สัญลักษณ์ที่ได้หลังจากถูกสลับลำดับด้วยตัวสลับลำดับช่องสัญญาณแล้ว จะเขียนแทนด้วย I โดยที่ I_n คือสัญลักษณ์ลำดับที่ n ที่ได้จากการสลับลำดับช่องสัญญาณ และ $\underline{I}_1^N$ คือชุดของลำดับสัญลักษณ์ $I_1, I_2, ..., I_n, ..., I_N$ เมื่อ N คือความยาวของสัญลักษณ์ที่ถูกส่งในหนึ่งบล็อก และมีค่าเท่ากับ $N_b + L$ โดยที่ L แทนจำนวนของบิตหางที่ป้อนให้กับเครื่องเข้ารหัสย่อยเพื่อทำให้สถานะสุดท้ายเป็นศูนย์ และเนื่องจากตัวสลับลำดับการเข้ารหัสที่ใช้เป็นแบบ simile ซึ่งสามารถทำให้สถานะสุดท้ายของเครื่องเข้ารหัสย่อยเป็นศูนย์พร้อมกันได้โดยใช้บิตหางที่เหมือนกันเพียงชุดเดียว ดังนั้น L จึงมีค่าเท่ากับขนาดหน่วยความจำของเครื่องเข้ารหัสย่อย

ขนาดของตัวสลับลำดับแบบบล็อก มีค่าเท่ากับขนาดของความลึก (depth : D) คูณกับความกว้าง (width : W) ของตัวสลับลำดับ ซึ่งตัวสลับลำดับที่มีขนาดของความลึกสูง จะมีความสามารถในการกระจายความสัมพันธ์ของเฟดดิงที่มีขนาดยาว ๆ ได้ ทั้งนี้ความกว้างก็จำเป็นจะต้องมีค่ามากพออีกด้วย อย่างน้อยที่สุดก็ไม่ควรน้อยกว่าความยาวคอนสเตรนต์ของเครื่องเข้า รหัสย่อย ยิ่งกว่านั้นการเลือกใช้ตัวสลับลำดับแบบคี่-คู่ ที่มีการสลับสัญลักษณ์ที่อยู่ในตำแหน่งคี่ก่อนการสลับลำดับ ไปยังตำแหน่งคี่หลังการสลับลำดับ และสลับสัญลักษณ์ที่อยู่ในตำแหน่งคู่ ไปยังตำแหน่งคู่ จะทำให้สัญลักษณ์ 2 สัญลักษณ์ที่ถูกส่งติดกันที่ภาคส่ง ประกอบด้วยบิตรหัสที่มาจากเครื่องเข้ารหัสย่อยคนละตัวกัน ส่งผลให้เครื่องถอดรหัสมีสมรรถนะที่ดีขึ้น

การออกแบบตัวสลับลำดับให้เป็นแบบคี่-คู่นั้น ทำได้โดยการบังคับให้ความลึกและความกว้างของตัวสลับลำดับแบบบล็อกมีขนาดเป็นเลขคี่ แต่การทำเช่นนี้ทำให้ตัวสลับลำดับมีขนาดไม่พอดีกับขนาดของสัญลักษณ์ที่จะนำมาสลับลำดับ ดังนั้นจึงต้องออกแบบให้บางส่วนของตัวสลับลำดับไม่ถูกใช้งาน ตัวอย่างของตัวสลับลำดับช่องสัญญาณแบบบล็อกที่มีคุณสมบัติการสลับแบบคี่-คู่ (odd-even block channel interleaver) แสดงอยู่ในรูปที่ 2.5 ความลึกของตัวสลับลำดับมีค่าเท่ากับ 41 และความกว้างมีค่าเท่ากับ 23 ตัวสลับลำดับในตัวอย่างนี้ใช้สำหรับสลับลำดับบล็อกของสัญลักษณ์ที่มีขนาด 934 สัญลักษณ์ ซึ่งประกอบไปด้วยสัญลักษณ์ของบิตข้อมูล 930 สัญลักษณ์ และสัญลักษณ์ของบิตหางอีก 4 สัญลักษณ์ (ขนาดของหน่วยความจำมีค่าเท่ากับ 4) แต่เนื่องจากตัวสลับลำดับมีขนาดเท่ากับ $41 \times 23 = 943$ สัญลักษณ์ ซึ่งมากกว่าขนาดของสัญลักษณ์ที่จะนำมาสลับลำดับ ดังนั้นจึงต้องออกแบบให้ตำแหน่งทางด้านขวาล่างของตัวสลับลำดับจำนวน 12 ตำแหน่งไม่ถูกใช้งาน เหตุผลที่เป็น 12 ตำแหน่งก็เพราะ ส่วนที่ไม่ถูกใช้งานจะต้องมีจำนวนคอลัมน์ (column) เท่ากับ 2 และมีจำนวนแถวเป็นเลขคู่ ซึ่งในที่นี้คือ 6 เพื่อให้ตัวสลับลำดับยังคงมีคุณสมบัติของการสลับลำดับแบบคี่-คู่อยู่ ทั้งนี้ขนาดที่ตัวสลับลำดับทำงานได้จะมีค่าเท่ากับ 931 สัญลักษณ์เท่านั้น สัญลักษณ์ที่เหลืออีก 3 สัญลักษณ์จึงไม่ถูกนำไปสลับลำดับด้วย แต่จะถูกส่งรวมไปกับบล็อกของสัญลักษณ์ที่ถูกสลับลำดับแล้ว



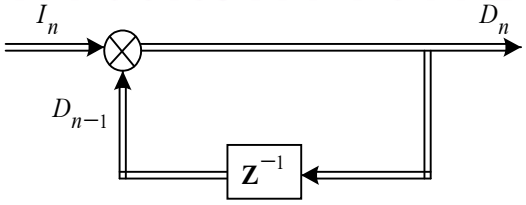
รูปที่ 2.5 ตัวสลับลำดับช่องสัญญาณแบบบล็อกที่มีคุณสมบัติการสลับแบบคี่-คู่ ขนาด 41×23 สัญลักษณ์

2.4 การเข้ารหัสเชิงผลต่าง

ขั้นตอนสุดท้ายก่อนที่สัญญาณจะถูกส่งออกไปที่ภาคส่ง คือ การเข้ารหัสเชิงผลต่าง ชุดของสัญลักษณ์ $\underline{I}_1^N$ จะถูกส่งไปที่ตัวเข้ารหัสเชิงผลต่าง (differential encoder : DE) และได้เอาต์พุตออกมาเป็นสัญลักษณ์ DQPSK (differential QPSK) $\underline{D}_0^N$ ซึ่งมีความสัมพันธ์กันดังนี้

$$D_n = D_{n-1} I_n \tag{1}$$

โดยที่ D_0 แทนสัญลักษณ์อ้างอิง (reference symbol) และมีค่าเท่ากับ 1



รูปที่ 2.6 ตัวเข้ารหัสเชิงผลต่าง

การเข้ารหัสเชิงผลต่างทำให้ข่าวสารของสัญญาณถูกเข้ารหัสอยู่ในผลต่างระหว่างเฟสของสัญลักษณ์ที่อยู่ติดกัน ภาครับจึงไม่จำเป็นต้องทราบค่าประมาณเฟสของสัญญาณพาห์ แต่สามารถนำเทคนิคการตรวจจับสัญญาณที่เรียกว่า การตรวจจับแบบไม่ร่วมนัย มาใช้ประมาณสัญญาณที่ถูกส่งมาได้ รายละเอียดของการตรวจจับแบบไม่ร่วมนัยจะกล่าวถึงต่อไปในบทที่ 4

บทที่ 3

ช่องสัญญาณ

หลังจากที่สัญญาณผ่านกระบวนการเข้ารหัสที่ภาคส่งแล้ว จะถูกส่งไปที่ภาครับผ่านทางช่องสัญญาณ สัญญาณที่ภาครับรับได้จะแตกต่างไปจากสัญญาณที่ถูกส่งมา เนื่องจากผลของช่องสัญญาณที่ไม่เป็นอุดมคติ ทั้งนี้ลักษณะการลดทอนหรือความผิดเพี้ยนของสัญญาณขึ้นอยู่กับรูปแบบของช่องสัญญาณที่ส่งผ่าน ซึ่งในงานวิจัยนี้จะพิจารณาผลกระทบที่เกิดจากช่องสัญญาณแบบเรย์ลีเฟดดิง ลักษณะการลดทอนสัญญาณของช่องสัญญาณแบบเฟดดิงจะกล่าวไว้ในหัวข้อที่ 3.1 เนื้อหาส่วนที่เหลือจะอธิบายถึงแบบจำลองของช่องสัญญาณ การจำลองช่องสัญญาณโดยใช้แบบจำลองของ Jakes รวมไปถึงผลที่ได้จากการจำลองช่องสัญญาณ

3.1 ช่องสัญญาณแบบเฟดดิง

ในระบบการสื่อสารแบบไร้สาย โดยเฉพาะอย่างยิ่งในระบบโทรศัพท์เคลื่อนที่ คุณลักษณะของช่องสัญญาณจะไม่อยู่ในสภาพคงที่ (stationary) และสามารถคาดเดาได้เหมือนช่องสัญญาณในระบบที่เชื่อมต่อด้วยสาย (wired channel) แต่ช่องสัญญาณที่เกิดขึ้นจะมีลักษณะสุ่ม (random) และเปลี่ยนแปลงไปตามเวลา ทั้งนี้เนื่องจากการส่งสัญญาณระหว่างสายอากาศของโทรศัพท์เคลื่อนที่กับสถานีฐานเกิดขึ้นสูงจากพื้นดินไม่มากนัก สัญญาณที่ถูกส่งอาจจะไปสะท้อนสิ่งกีดขวางต่าง ๆ เช่น อาคาร ต้นไม้ หรือ พื้นดิน ทำให้สัญญาณที่ปลายทางได้รับ ประกอบด้วยสัญญาณที่สะท้อนมาจากหลายเส้นทาง ซึ่งสัญญาณในแต่ละเส้นทางก็จะมีขนาด และ เฟสที่แตกต่างกัน นอกจากนี้การเคลื่อนที่ของเครื่องโทรศัพท์ขณะที่มีการส่งสัญญาณ หรือการที่สภาพแวดล้อมที่อยู่ระหว่างภาคส่งและภาครับมีการเปลี่ยนแปลงตามเวลา เช่น การเคลื่อนที่ของรถยนต์ที่อยู่รอบ ๆ โทรศัพท์เคลื่อนที่ก็มีผลต่อสัญญาณที่ปลายทางจะได้รับด้วยเช่นกัน ผลกระทบต่าง ๆ ที่เกิดขึ้นนี้ทำให้สัญญาณที่ปลายทางได้รับมีการเปลี่ยนแปลงขึ้นลงอย่างรวดเร็ว ทั้งในแง่ของแอมพลิจูดและเฟสของสัญญาณ ปรากฏการณ์ดังกล่าวนี้เรียกว่า small-scale fading หรือ เฟดดิง (fading) [19-20] ทั้งนี้ถ้าสัญญาณที่สะท้อนจากทิศทางต่าง ๆ มีจำนวนมาก และไม่มีสัญญาณที่มาจากเส้นทางตรงระหว่างภาคส่งกับภาครับที่เรียกว่า line-of-sight (LOS) เลย เฟดดิงที่เกิดขึ้นจะถูกเรียกว่า เรย์ลีเฟดดิง (Rayleigh fading) เนื่องจากเอนเวโลป (envelope) ของสัญญาณที่รับได้จะมีการกระจายตัวทางสถิติเป็นแบบเรย์ลี

3.1.1 ปัจจัยหลักที่ส่งผลต่อการเกิดเฟดดิง

ปัจจัยที่ก่อให้เกิดเฟดดิงประกอบด้วย 2 ประการ คือ

1) การแผ่แบบประวิงเวลา (delay spread)

เนื่องจากสัญญาณที่ถูกส่งมาจากต้นทางมักจะเกิดการสะท้อนและหักเห เมื่อไปกระทบกับสิ่งแวดล้อมต่าง ๆ ที่กีดขวางอยู่ระหว่างภาคส่งกับภาครับ ทำให้สัญญาณที่ปลายทางรับได้ประกอบด้วยสัญญาณที่สะท้อนมาจากเส้นทางที่ต่างกัน และมาถึงปลายทางในเวลาที่ต่างกันด้วย ดังนั้นสัญญาณรวมที่ปลายทางรับได้ จึงเป็นสัญญาณที่มีการประวิงเวลาไป หรืออาจเรียกว่าสัญญาณเกิดการแผ่ทางเวลา (time spread) ผลของการแผ่ทางเวลาจะทำให้สัญญาณเดินทางไปถึงปลายทางด้วยเวลานานกว่าปกติ ก่อให้เกิดการรบกวนกันของสัญญาณในแต่ละสัญลักษณ์ หรือที่เรียกว่า การแทรกสอดระหว่างสัญลักษณ์ (intersymbol interference : ISI) ทั้งนี้การประวิงเวลาของสัญญาณจะเกิดขึ้นมากหรือน้อยก็ขึ้นอยู่กับคุณลักษณะของช่องสัญญาณ

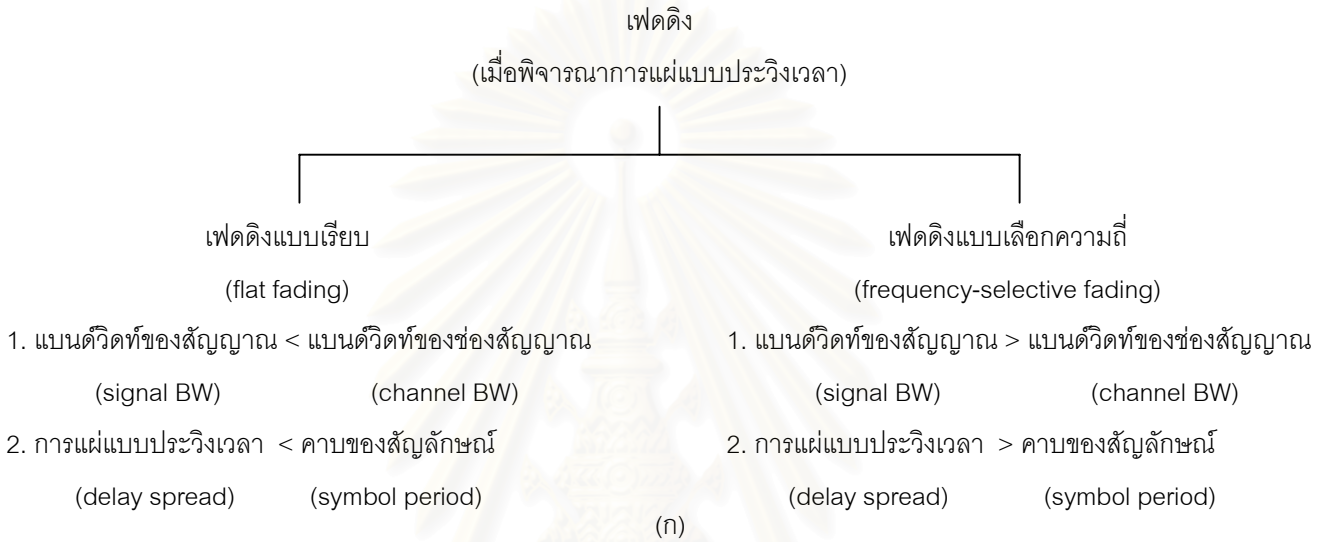
2) การแผ่แบบดอปเปลอร์ (Doppler spread)

การเคลื่อนที่ที่เกิดขึ้นระหว่างเครื่องรับกับเครื่องส่ง มีผลทำให้คลื่นที่เดินทางมาในแต่ละเส้นทางเกิดการเลื่อนทางความถี่ขึ้น เรียกว่า ดอปเปลอร์ชิฟต์ (Doppler shift) ความถี่ที่เลื่อนไปจะมีค่ามากหรือน้อย ก็ขึ้นอยู่กับความเร็วและทิศทางการเคลื่อนที่ของโทรศัพท์เคลื่อนที่ นอกจากนี้การเคลื่อนที่ของวัตถุที่อยู่บริเวณรอบ ๆ ยังส่งผลให้ดอปเปลอร์ชิฟต์มีการเปลี่ยนแปลงไปตามเวลาอีกด้วย ดังนั้นจึงอาจกล่าวได้ว่า การแผ่แบบดอปเปลอร์ทำให้ช่องสัญญาณมีพฤติกรรมที่เปลี่ยนแปลงไปตามเวลา (time-varying channel) และอัตราการเปลี่ยนแปลงที่เกิดขึ้นก็ส่งผลโดยตรงต่อความเร็วของเฟดดิงด้วย

3.1.2 รูปแบบของเฟดดิง

เฟดดิงที่เกิดขึ้นระหว่างการส่งสัญญาณผ่านช่องสัญญาณแบบไร้สาย มีอยู่หลายประเภท ทั้งนี้การจะพิจารณาว่าเฟดดิงเป็นแบบไหนนั้นขึ้นอยู่กับลักษณะของสัญญาณที่ส่งเปรียบเทียบกับลักษณะเฉพาะ (characteristic) ของช่องสัญญาณเป็นหลัก พารามิเตอร์ของสัญญาณที่พิจารณา ได้แก่ แบนด์วิดท์ (bandwidth) คาบของสัญลักษณ์ (symbol period) หรือ อัตราการส่งสัญญาณ (transmission rate) ส่วนปัจจัยของช่องสัญญาณที่ส่งผลต่อลักษณะของเฟดดิงที่เกิดขึ้นได้แก่ การแผ่แบบประวิงเวลา และ การแผ่แบบดอปเปลอร์ เมื่อพิจารณาการแผ่แบบประวิง

เวลาเปรียบเทียบกับลักษณะของสัญญาณที่ส่ง เฟดดิงจะมีลักษณะแตกต่างกัน 2 รูปแบบ คือ เฟดดิงแบบเรียบ (flat fading) และ เฟดดิงแบบเลือกความถี่ (frequency-selective fading) ในขณะที่การแผ่แบบดอปเปลอร์จะส่งผลกระทบต่อเฟดดิงในอีก 2 รูปแบบ คือ เฟดดิงแบบเร็ว (fast fading) และเฟดดิงแบบช้า (slow fading) รูปแบบของเฟดดิงเมื่อพิจารณาในแง่ของการแผ่แบบประวิงเวลา และ การแผ่แบบดอปเปลอร์นี้เกิดขึ้นอย่างเป็นอิสระต่อกัน ดังแสดงในรูปที่ 3.1



รูปที่ 3.1 รูปแบบของเฟดดิง
(ก) เมื่อพิจารณาการแผ่แบบประวิงเวลา
(ข) เมื่อพิจารณาการแผ่แบบดอปเปลอร์

3.1.1.1 ผลของเฟดดิงเนื่องจากการแผ่แบบประวิงเวลา

การแผ่ทางเวลาเนื่องมาจากพหุวิถี (multipath) ทำให้เกิดเฟดดิงใน 2 รูปแบบ คือ เฟดดิงแบบเรียบและเฟดดิงแบบเลือกความถี่

. *เฟดดิงแบบเรียบ*

ถ้าช่องสัญญาณมีผลตอบสนองอัตราขยายที่คงที่ และเฟสที่เป็นเชิงเส้นในช่วงแบนด์วิดท์ที่กว้างกว่าแบนด์วิดท์ของสัญญาณแล้ว เฟดดิงที่เกิดขึ้นจะเป็นเฟดดิงแบบเรียบ สัญญาณที่ปลายทางรับได้จะมีคุณลักษณะเชิงสเปกตรัม (spectrum characteristic) เหมือนเดิม แต่กำลังของสัญญาณจะเปลี่ยนแปลงไปตามเวลาเนื่องจากผลของพหุวิถีที่เกิดขึ้นในช่องสัญญาณ ดังนั้น ช่องสัญญาณที่เกิดเฟดดิงแบบเรียบนี้จึงเรียกอีกอย่างหนึ่งได้ว่า ช่องสัญญาณที่เปลี่ยนแปลงทางแอมพลิจูด (amplitude varying channel) การแจกแจงของแอมพลิจูดที่มักพบโดยทั่วไปจะเป็นการแจกแจงแบบเรย์ลี (Rayleigh distribution)

. *เฟดดิงแบบเลือกความถี่*

ถ้าช่วงแบนด์วิดท์ที่ช่องสัญญาณมีผลตอบสนองอัตราขยายที่คงที่ และ เฟสที่เป็นเชิงเส้นมีขนาดแคบกว่าแบนด์วิดท์ของสัญญาณแล้ว ช่องสัญญาณจะเกิดเฟดดิงแบบเลือกความถี่ขึ้น สเปกตรัมของสัญญาณจะถูกกระทบจากช่องสัญญาณไม่เท่ากันทั้งหมด โดยส่วนประกอบสเปก-ตรัมที่อยู่นอกช่วงแบนด์วิดท์ของช่องสัญญาณจะได้รับผลกระทบที่แตกต่างออกไป ช่วงพิสัยของความถี่ที่ช่องสัญญาณมีผลกระทบกับส่วนประกอบสเปกตรัมโดยเท่าเทียมกัน เรียกว่า แบนด์วิดท์โคฮีเรนซ์ (coherence BW) เมื่อช่องสัญญาณเกิดเฟดดิงแบบเลือกความถี่ ผลตอบสนองช่องสัญญาณจะเกิดการแผ่ออกทางเวลา ซึ่งมีขนาดยาวกว่าคาบของสัญลักษณ์ ทำให้สัญญาณ ที่รับได้ถูกลดทอนทางขนาด และมีการประวิงทางเวลา เป็นผลให้เกิดการแทรกสอดระหว่างสัญลักษณ์ขึ้น (intersymbol interference)

3.1.1.2 ผลของเฟดดิงเนื่องจากการแผ่แบบดอปเปลอร์

การเลื่อนความถี่แบบดอปเปลอร์อันเนื่องมาจากการเคลื่อนที่ระหว่างเครื่องส่งกับเครื่องรับมีผลกับความเร็วของเฟดดิง เกิดเป็น เฟดดิงแบบเร็ว และ เฟดดิงแบบช้า

ก. เฟดดิงแบบเร็ว

การแผ่แบบดอปเปลอร์ และ เวลาโคฮีเรนซ์ (coherence time) เป็นพารามิเตอร์ที่ใช้บ่งบอกถึงคุณสมบัติการเปลี่ยนแปลงไปตามเวลาของช่องสัญญาณที่มีผลมาจากการเคลื่อนที่ของเครื่องส่งหรือการเคลื่อนที่ของวัตถุที่อยู่ในช่องสัญญาณ เวลาโคฮีเรนซ์คือช่วงเวลาทางสถิติที่ผลตอบสนองช่องสัญญาณมีค่าไม่เปลี่ยนแปลง ทั้งนี้ยังเป็นค่าที่แสดงถึงความคล้ายคลึงกันของผลตอบสนองช่องสัญญาณในช่วงเวลาหนึ่งอีกด้วย กล่าวคือ สัญญาณที่มาถึงภาครับที่เวลาต่างกันแต่ไม่เกินเวลาโคฮีเรนซ์ จะได้รับผลกระทบจากช่องสัญญาณใกล้เคียงกัน หรืออาจกล่าวได้ว่าสัญญาณที่ถูกส่งมาภายในช่วงเวลาโคฮีเรนซ์ จะมีแอมพลิจูดที่สัมพันธ์กันทางเวลา เนื่องจากได้รับผลกระทบจากช่องสัญญาณคล้ายคลึงกัน

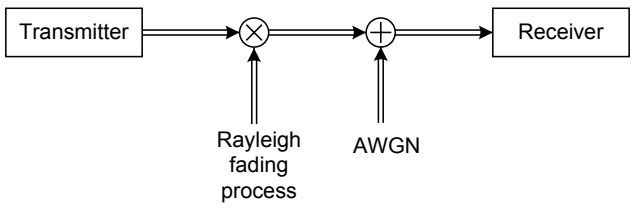
ในกรณีเฟดดิงแบบเร็ว ผลตอบสนองของช่องสัญญาณจะมีการเปลี่ยนแปลงอย่างรวดเร็วภายในช่วงเวลาที่ส่งสัญญาณ ดังนั้นเวลาโคฮีเรนซ์ของช่องสัญญาณจะมีค่าน้อยกว่าคาบของสัญลักษณ์ และคุณลักษณะของเฟดดิงจะเปลี่ยนแปลงไปมาหลายครั้งในขณะที่สัญลักษณ์หนึ่ง ๆ ถูกส่งไป เป็นผลให้รูปร่างของสัญญาณเบสแบนด์ผิดเพี้ยนไป

ก. เฟดดิงแบบช้า

เฟดดิงแบบช้า เกิดขึ้นเมื่ออัตราการเปลี่ยนแปลงของผลตอบสนองของช่องสัญญาณมีค่าน้อยกว่าการเปลี่ยนแปลงของสัญญาณ หรือ เวลาโคฮีเรนซ์มีค่ามากกว่าคาบของสัญลักษณ์ ในกรณีนี้ช่องสัญญาณจะมีผลตอบสนองคงที่ภายในช่วงเวลาหลายสัญลักษณ์ ทำให้ผลกระทบที่เกิดจากช่องสัญญาณติดกันเป็นช่วงยาว

3.2 แบบจำลองของช่องสัญญาณ

ช่องสัญญาณที่พิจารณาในงานวิจัยนี้ เป็นช่องสัญญาณแบบเรย์ลีเฟดดิงชนิดเรียบที่มีสหสัมพันธ์กัน (correlated flat Rayleigh fading channel) และมีสัญญาณรบกวนเกาส์เซียน สีขาวแบบบวก (additive white Gaussian noise : AWGN) ดังรูปที่ 3.2



รูปที่ 3.2 ช่องสัญญาณ

แบบจำลองของช่องสัญญาณที่อยู่ในรูปดีสครีตทางเวลา เป็นไปตามสมการดังนี้

$$R_n = F_n D_n + N_n \tag{3.1}$$

โดยที่ (1) D_n เป็น สัญลักษณ์ที่ถูกส่งมาจากภาคส่ง

(2) R_n เป็น สัญลักษณ์ที่รับได้ที่ภาครับ

(3) $\underline{F}_0^N$ แทนกระบวนการเฟดดิง (fading process) ที่มีค่าเฉลี่ยเป็นศูนย์ และมีฟังก์ชันอัตสหสัมพันธ์ (autocorrelation function) เป็นไปตามสมการดังนี้

$$\phi_F(m) \triangleq \mathbf{E}[\, F_n \, F_{n-m}^{*} \,] = J_0(2\pi B_d T m) \tag{3.2}$$

$\mathbf{E}[\bullet]$ คือ ค่าคาดหวัง (expected value) ของ $\bullet$

* แทน สังยุคเชิงซ้อน (complex conjugate)

$J_0(\cdot)$ คือ ฟังก์ชัน Bessel ลำดับศูนย์ชนิดที่หนึ่ง (zero-order Bessel function of the first kind)

B_d คือ การแผ่แบบดอปเปลอร์ของช่องสัญญาณ ซึ่งเป็นค่าที่ใช้วัดอัตราการเปลี่ยนแปลงของช่องสัญญาณ

T คือ คาบของสัญลักษณ์ (symbol duration)

(4) $\underline{N}_0^N$ แทนกระบวนการของสัญญาณรบกวน (noise process) ที่มีค่าเฉลี่ยเป็นศูนย์ และมีค่าอัตสหสัมพันธ์เท่ากับ

$$\phi_N(m) \triangleq \mathbf{E}[\, N_n N_{n-m}^{*} \,] = N_o \delta(m) \qquad n \in [0, N] \tag{3.3}$$

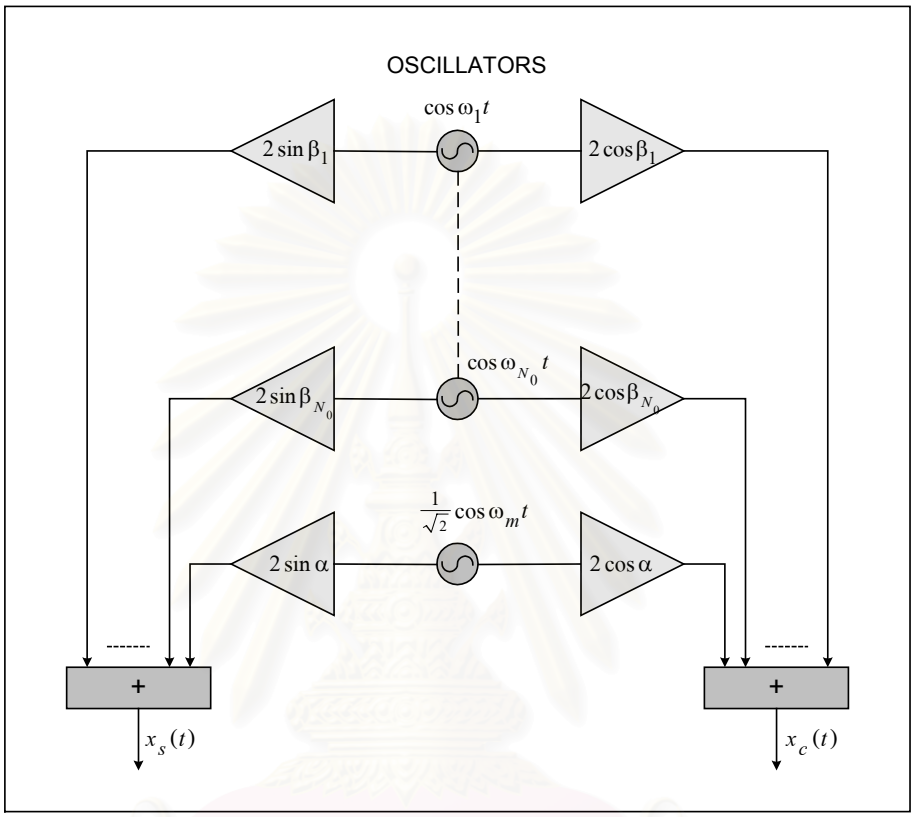
N_o คือ ความหนาแน่นสเปกตรัมของกำลังงานของสัญญาณรบกวนแบบความถี่ข้างเดียว (single-sided noise power spectral density)

$\delta(\cdot)$ คือ เดลตาฟังก์ชัน (delta function)

จากแบบจำลองข้างต้น เฟดดิงที่ได้จะมีสหสัมพันธ์กันทางเวลาและมีผลทำให้แอมพลิจูดและเฟสของสัญญาณเพี้ยนไป โดยที่แอมพลิจูดมีการแจกแจงแบบเรย์ลี (Rayleigh distribution) และเฟสมีการแจกแจงแบบยูนิฟอร์ม (uniform distribution) ตั้งแต่ $[0, 2\pi)$

3.3 การจำลองช่องสัญญาณโดยใช้แบบจำลองของ Jakes

การกำเนิดอัตราขยายของช่องสัญญาณแบบเรย์ลีเฟดดิงที่มีสหสัมพันธ์กัน โดยใช้เครื่องจำลองของ Jakes แสดงอยู่ในรูปที่ 3.3



รูปที่ 3.3 เครื่องจำลองช่องสัญญาณแบบ Jakes

เครื่องจำลองช่องสัญญาณในรูปที่ 3.3 ประกอบด้วยออสซิลเลเตอร์ความถี่ต่ำ (low frequency oscillator) จำนวน N_0 ตัว แต่ละตัวมีความถี่เท่ากับ $\omega_n = \omega_m \cos(2\pi n / N)$ โดยที่ $n = 1,2,\ldots,N_0$ และมีออสซิลเลเตอร์อีกหนึ่งตัวที่มีความถี่เท่ากับความถี่ดอปเปลอร์ ω_m เอาต์พุตที่ได้จากออสซิลเลเตอร์แต่ละตัวจะถูกนำมารวมกัน ได้เป็นอัตราขยายของช่องสัญญาณในแกน in-phase (x_c) และแกน quadrature-phase (x_s) ดังต่อไปนี้

$$x_c(t) = 2\sum_{n=1}^{N_0} \cos\beta_n \cos\omega_n t + \sqrt{2}\cos\alpha\cos\omega_m t \tag{3.4}$$

$$x_s(t) = 2\sum_{n=1}^{N_0} \sin\beta_n \cos\omega_n t + \sqrt{2}\sin\alpha\cos\omega_m t \tag{3.5}$$

และจะได้อัตราขยายของช่องสัญญาณแบบเฟดดิงเป็น

$$y(t) = x_c(t) + jx_s(t) \tag{3.6}$$

โดยที่ $\alpha = \frac{\pi}{4}$, $\beta = \frac{\pi n}{N_0}$, $\omega_n = \omega_m \cos(\frac{2\pi n}{N})$

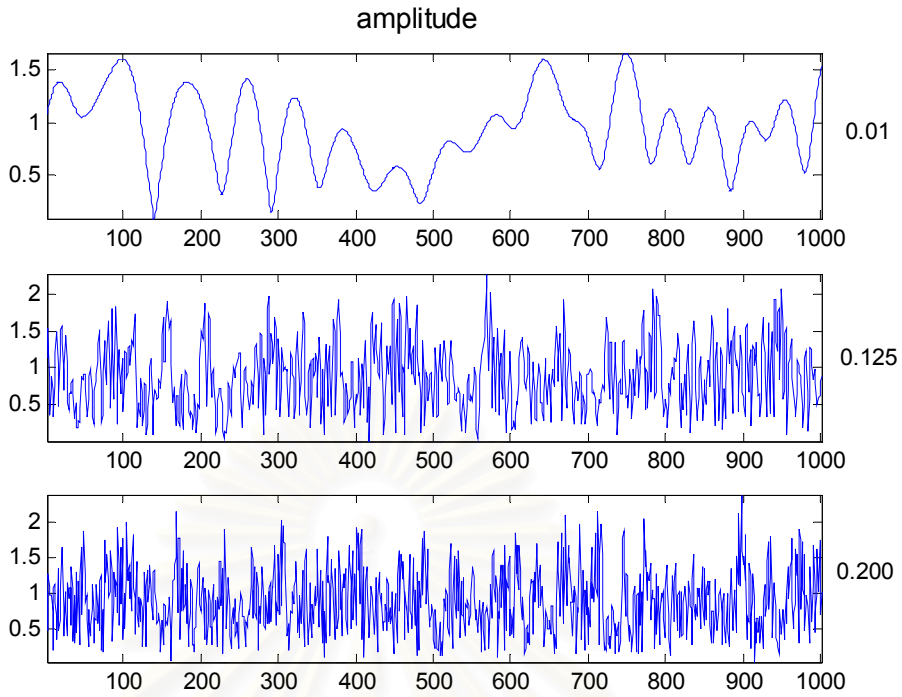
$N_0 = \frac{1}{2}(\frac{N}{2} - 1)$ ซึ่งในงานวิจัยนี้จะใช้ $N_0 = 8$

$x_c(t)$ และ $x_s(t)$ ต่างก็เป็นการประมาณของกระบวนการสุ่มแบบเกาส์เซียน (Gaussian random process) ซึ่งมีค่าเฉลี่ยเท่ากับศูนย์ และค่าความแปรปรวนเท่ากับหนึ่ง ส่วน $y(t)$ ที่ได้จะเป็นสัญญาณเชิงซ้อนแบบสุ่ม ซึ่งขนาด $|y|$ มีการแจกแจงแบบเรย์ลี และเฟสมีการแจกแจงแบบยูนิฟอร์มตั้งแต่ 0 ถึง 2π นอกจากนี้ค่าอัตสหสัมพันธ์ของสัญญาณ $y(t)$ ที่ได้จากแบบจำลองนี้จะมีค่าเท่ากับ $J_0(\omega_m \tau)$

3.4 ผลที่ได้จากการจำลองช่องสัญญาณ

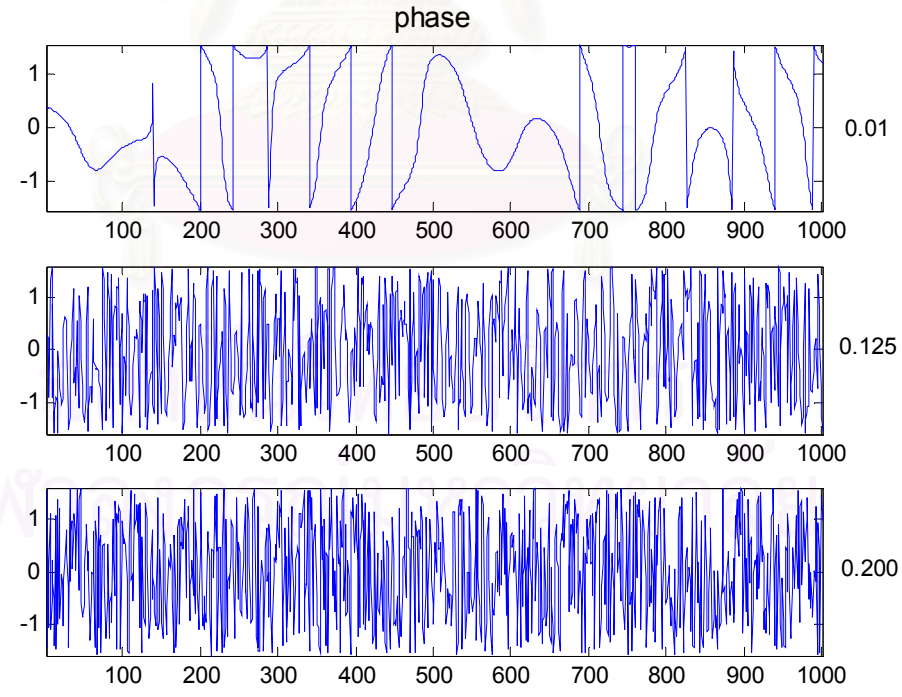
งานวิจัยนี้จะจำลองช่องสัญญาณที่เกิดเรย์ลีเฟดดิงที่มีสหสัมพันธ์กัน โดยใช้แบบจำลองของ Jakes ที่ได้กล่าวไว้ในหัวข้อที่ 3.3 เฟดดิงที่ได้จะมีขนาดและเฟสเปลี่ยนแปลงไปตามเวลา ทั้งนี้อัตราการเปลี่ยนแปลง หรืออัตราเร็วเฟดดิง ขึ้นอยู่กับค่าผลคูณ B_dT หรือที่เรียกว่า ค่าดอปเปลอร์สเปรดแบบนอร์มอลไลซ์ (normalized Doppler spread) เมื่อ B_dT มีค่าสูง เฟดดิงจะมีการเปลี่ยนแปลงทั้งแอมพลิจูดและเฟสอย่างรวดเร็ว ในทางกลับกันถ้า B_dT มีค่าต่ำ การเปลี่ยนแปลงจะเป็นไปอย่างช้า ๆ แต่เฟดดิงที่เกิดขึ้นในแต่ละเวลาจะมีความสัมพันธ์กันมากขึ้น เป็นผลให้เฟดดิงเกิดติดกันเป็นช่วงยาว

การเปลี่ยนแปลงของแอมพลิจูดและเฟสของเฟดดิงที่ B_dT เท่ากับ 0.01 0.125 และ 0.200 แสดงอยู่ในรูปที่ 3.4 และ 3.5 เมื่อพิจารณาค่าทางสถิติของเฟดดิงที่จำลองได้ จะพบว่าแอมพลิจูดมีการแจกแจงแบบเรย์ลี และเฟสมีการแจกแจงแบบยูนิฟอร์มตั้งแต่ 0 ถึง 2π ดังรูปที่ 3.6 และ 3.7 นอกจากนี้ค่าอัตสหสัมพันธ์ของเฟดดิงยังมีค่าใกล้เคียงกับฟังก์ชัน Bessel (Bessel function) ซึ่งสอดคล้องกับแบบจำลองที่ได้กล่าวไว้ข้างต้น



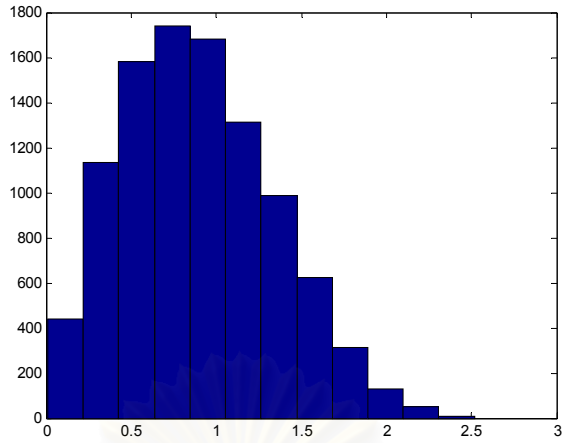
รูปที่ 3.4 แอมพลิจูดของเฟดดิงที่ B_dT เท่ากับ

(ก) 0.01 (ข) 0.125 (ค) 0.200

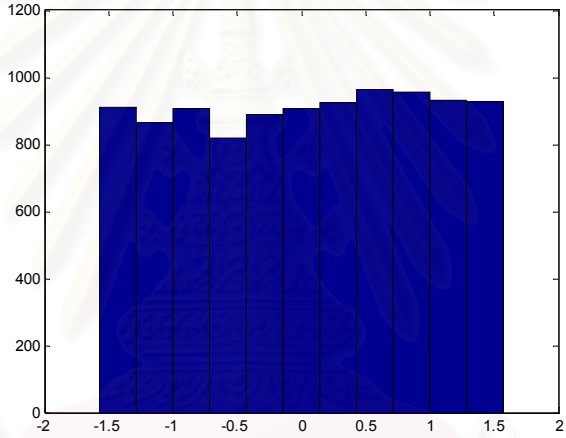


รูปที่ 3.5 เฟสของเฟดดิงที่ B_dT เท่ากับ

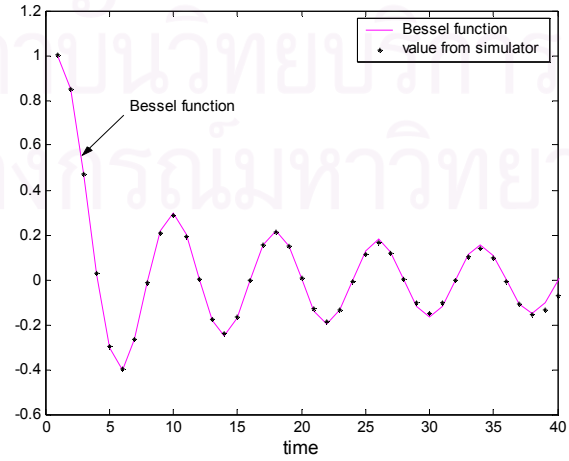
(ก) 0.01 (ข) 0.125 (ค) 0.200



รูปที่ 3.6 ฮีสโตแกรมของแอมพลิจูดของเฟดดิงที่ B_dT เท่ากับ 0.125



รูปที่ 3.7 ฮีสโตแกรมของเฟสของเฟดดิงที่ B_dT เท่ากับ 0.125



รูปที่ 3.8 ค่าอัตสหสัมพันธ์ของเฟดดิงที่ B_dT เท่ากับ 0.125

บทที่ 4

โครงสร้างของภาครับ

ภาครับจะทำหน้าที่ตรวจสอบและตัดสินว่าข้อมูลที่ถูกส่งมาคือข้อมูลใด โดยอาศัยข่าวสารจากชุดข้อมูลที่รับได้ ซึ่งถูกเข้ารหัสมาแล้วที่ภาคส่ง แต่เนื่องจากข้อมูลถูกส่งผ่านทางช่องสัญญาณทำให้ภาครับต้องถอดรหัสสัญญาณ โดยคำนึงถึงผลกระทบของช่องสัญญาณที่เกิดขึ้นด้วย การทำงานของภาครับจะประกอบด้วยส่วนหลัก ๆ สองส่วน คือ การประมาณข่าวสารช่องสัญญาณ และ การถอดรหัสเทอร์โบ

4.1 การประมาณข่าวสารช่องสัญญาณ

ข่าวสารช่องสัญญาณ (channel information) เป็นค่าที่ขึ้นอยู่กับคุณลักษณะของช่องสัญญาณแต่ละประเภท การประมาณข่าวสารช่องสัญญาณ ก็คือ การหาค่าความน่าจะเป็นของสัญญาณที่รับได้เมื่อกำหนดให้สัญญาณที่ถูกส่งมาเป็นค่าใดค่าหนึ่ง ฟังก์ชันความน่าจะเป็นนี้เรียกอีกอย่างหนึ่งว่า ฟังก์ชันความน่าเป็นจริงของช่องสัญญาณ (channel likelihood function) หรือ เมตริกช่องสัญญาณ (channel metric) ซึ่งจะถูกส่งไปให้กับเครื่องถอดรหัสเทอร์โบเพื่อช่วยในการตัดสินบิตที่ถูกส่งมา โดยข่าวสารจากช่องสัญญาณจะแสดงถึงความเชื่อถือได้ (reliability) ของช่องสัญญาณในขณะนั้น สำหรับช่องสัญญาณที่มีสัญญาณรบกวนแบบเกาส์ ฟังก์ชันความน่าเป็นจริงของช่องสัญญาณ จะถูกแทนค่าด้วยฟังก์ชันความน่าจะเป็นที่มีการแจกแจงแบบเกาส์ แต่สำหรับช่องสัญญาณแบบเรย์ลีเฟดดิง การคำนวณฟังก์ชันความน่าเป็นจริงของช่องสัญญาณจะต้องมีการประมาณเฟดดิงที่เกิดขึ้นบนช่องสัญญาณร่วมด้วย โดยอาศัยเทคนิคการตรวจจับสัญญาณแบบต่าง ๆ ซึ่งมีทั้งกรณีที่เป็นการตรวจจับแบบร่วมนัย และการตรวจจับแบบไม่ร่วมนัย

4.1.1 การตรวจจับแบบร่วมนัย

ในกรณีที่เป็นการตรวจจับแบบร่วมนัย (coherent detection) ทางภาครับจะทราบกระบวนการของเฟดดิงอย่างถูกต้อง กล่าวคือ ตัวตรวจจับสามารถติดตามทั้งเฟสและแอมพลิจูดของเฟดดิงได้อย่างสมบูรณ์และส่งข่าวสารนี้ไปให้เครื่องถอดรหัส เพราะฉะนั้นในกรณีนี้ทางภาคส่งจึงไม่จำเป็นต้องมีขั้นตอนการเข้ารหัสเชิงผลต่างของสัญญาณก่อนส่ง

ฟังก์ชันความน่าเป็นจริงของช่องสัญญาณสามารถคำนวณได้จากความสัมพันธ์ระหว่างสัญลักษณ์ที่รับได้และสัญลักษณ์ที่ถูกส่ง ดังสมการต่อไปนี้

$$M_n(I_n) = \Pr\{R_n \mid I_n\}$$

$$= \frac{1}{\pi N_0} \exp\left\{-\frac{1}{N_0}\left|R_n - F_n I_n\right|^2\right\} \quad (4.1)$$

เมื่อ $\Pr\{R_n \mid I_n\}$ คือ ฟังก์ชันความน่าจะเป็นแบบมีเงื่อนไข (conditional probability density function) ของสัญลักษณ์ที่รับได้ที่เวลา n เมื่อมีเงื่อนไขว่าสัญลักษณ์ที่ถูกส่งมาคือ I_n

เมตริก $M_n(I_n)$ นี้เป็นข่าวสารที่มาจากช่องสัญญาณ ซึ่งจะถูกส่งไปให้เครื่องถอดรหัสเทอร์โบต่อไป

4.1.2 การตรวจจับแบบไม่ร่วมนัย

สำหรับการตรวจจับแบบไม่ร่วมนัย (noncoherent detection) จะไม่มีสมมติฐานว่าภาครับสามารถทราบกระบวนการของเฟดดิงที่เกิดขึ้นได้อย่างถูกต้อง เนื่องจากการติดตามเฟสและแอมพลิจูดที่เปลี่ยนแปลงไปตามเวลานั้นไม่สามารถกระทำได้ในทางปฏิบัติ การตรวจจับแบบไม่ร่วมนัยจะใช้กระบวนการตรวจจับสัญญาณ โดยอาศัยขั้นตอนการเข้ารหัสเชิงผลต่างที่ภาคส่ง ซึ่งจะทำให้สัญญาณถูกเข้ารหัสอยู่ในผลต่างระหว่างเฟสของสัญลักษณ์ที่อยู่ติดกัน ภาครับจึงสามารถใช้กระบวนการตรวจจับเชิงผลต่างเพื่อประมาณข่าวสารจากช่องสัญญาณได้

4.1.2.1 การตรวจจับเชิงผลต่าง

การตรวจจับเชิงผลต่าง (differential detection : DD) จะใช้ประโยชน์จากกระบวนการเข้ารหัสเชิงผลต่างที่ภาคส่งในการตรวจหาสัญญาณที่ถูกส่งมา โดยข่าวสารของสัญญาณที่ถูกส่งจะถูกประมาณจากผลต่างระหว่างเฟสของสัญลักษณ์ปัจจุบันที่รับได้ กับสัญลักษณ์ก่อนหน้าหนึ่งสัญลักษณ์

สัญลักษณ์ DQPSK D_n ที่ได้จากกระบวนการเข้ารหัสเชิงผลต่าง เป็นไปตามสมการ (2.1) ที่กล่าวไว้ในบทที่ 2 จากความสัมพันธ์ดังกล่าว จะได้ว่าสัญลักษณ์ $\hat{I}_n$ ซึ่งใช้ประมาณสัญลักษณ์ I_n ที่ถูกส่ง สามารถคำนวณได้จากสัญลักษณ์ที่รับได้ ดังนี้

$$\hat{I}_n = R_n R_{n-1}^* \quad (4.2)$$

และฟังก์ชันความน่าเป็นจริง หรือเมตริกช่องสัญญาณที่เป็นค่าประมาณข่าวสารจากช่องสัญญาณมีค่าเป็น

$$M_n(I_n) = \Pr\{R_n \mid I_n, R_{n-1}\}$$

$$= \frac{1}{\pi N_0} \exp\left\{-\frac{1}{2N_0}\left|\hat{I}_n - I_n\right|^2\right\} \qquad (4.3)$$

จากสมการ (4.2) และ (4.3) จะสังเกตเห็นว่า การตรวจจับเชิงผลต่างมีการประมาณข่าวสารช่องสัญญาณจากสัญลักษณ์ที่รับได้จำนวน 2 สัญลักษณ์ คือ สัญลักษณ์ที่รับได้ที่เวลาปัจจุบัน R_n และสัญลักษณ์ที่รับได้ที่เวลาก่อนหน้าหนึ่งสัญลักษณ์ R_{n-1} การตรวจจับสัญญาณด้วยวิธีนี้สามารถทำได้ง่าย และมีโครงสร้างที่ไม่ซับซ้อน อาศัยช่วงสังเกตการณ์ของสัญลักษณ์ที่รับได้เพียง 2 สัญลักษณ์เท่านั้น แต่ถ้าเฟดดิงมีการเปลี่ยนแปลงอย่างรวดเร็ว อย่างในกรณีที่ เฟดดิงมีค่าผลคูณ B_dT สูง ๆ การตรวจจับเชิงผลต่างจะไม่สามารถติดตามการเปลี่ยนแปลงของเฟดดิงได้ทัน ทำให้การทำงานของเครื่องถอดรหัสมีประสิทธิภาพแย่ลง และส่งผลให้อัตราความผิดพลาดของสัญญาณไม่ลดลง ถึงแม้จะเพิ่มอัตราส่วนสัญญาณต่อสัญญาณรบกวนแล้วก็ตาม ลักษณะความผิดพลาดที่เกิดขึ้นนี้เรียกว่า ค่าพื้นของความผิดพลาด (error floor) ดังนั้นวิธีการตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์จึงถูกพัฒนาขึ้น เพื่อใช้ปรับปรุงประสิทธิภาพของการตรวจจับเชิงผลต่างแบบเดิม

4.1.2.2 การตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์

การตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ (multiple symbol differential detection : MSDD) จะประมาณข่าวสารช่องสัญญาณโดยใช้ช่วงสังเกตการณ์ของสัญลักษณ์ที่รับได้มากกว่า 2 สัญลักษณ์ คือใช้สัญลักษณ์ที่รับได้ที่เวลาก่อนหน้ามากกว่าหนึ่งสัญลักษณ์มาช่วยประมาณข่าวสารจากช่องสัญญาณ ณ เวลาปัจจุบัน ทำให้การประมาณข่าวสารช่องสัญญาณแม่นยำกว่าวิธีการตรวจจับเชิงผลต่างแบบเดิม

เมตริกที่เป็นค่าประมาณความน่าเป็นจริงสูงสุดที่เหมาะสมที่สุด (optimal maximum likelihood : optimal ML) ของสัญลักษณ์ที่รับได้ที่เวลา n มีค่าเป็นไปตามสมการดังนี้

$$M_n(\underline{I}_1^n) = \Pr\{R_n \mid \underline{I}_1^n, \underline{R}_0^{n-1}\}$$

$$= \frac{1}{\pi\sigma_n^2}\exp\left\{-\frac{1}{\sigma_n^2}\left|R_n - \left(\sum_{z=1}^{n} P_{n,z} R_{n-z} \prod_{k=1}^{z-1} I_{n-k}\right) I_n\right|^2\right\} \qquad (4.4)$$

โดยที่

$P_{n,z}$ คือ สัมประสิทธิ์การทำนายเชิงเส้น (linear prediction coefficient) ลำดับที่ n ของ $F_n D_{n-1}$

σ_n^2 คือ ค่าเฉลี่ยกำลังสองของค่าผิดพลาดจากการทำนายต่ำที่สุด (minimum mean-squared prediction error : MMSPE)

พจน์ $\left(\sum_{z=1}^{n} P_{n,z} R_{n-z} \prod_{k=1}^{z-1} I_{n-k} \right)$ ในสมการ (4.4) จะใช้เป็นค่าประมาณของ $F_n D_{n-1}$ ซึ่งมีค่าขึ้นอยู่กับสัญลักษณ์ที่รับได้ก่อนหน้านี้ $\underline{R}_0^{n-1}$ และลำดับของสัญลักษณ์ที่ถูกส่งมา $\underline{I}_1^{n-1}$

ถึงแม้ว่าเมตริกที่คำนวณได้นี้เป็นการประมาณค่าเฟดดิงที่แม่นยำมากก็ตาม แต่จะเห็นว่าถ้า n มีค่ามาก การคำนวณก็จะมากขึ้นด้วย เนื่องจากต้องคำนวณทุกกรณีที่เป็นไปได้ของลำดับ $\underline{I}_1^n$ ดังนั้นเพื่อลดความซับซ้อนในการคำนวณ เมตริกในสมการ (4.4) จะถูกตัดทอนให้สัมพันธ์กับลำดับของสัญลักษณ์ $\underline{I}$ ที่มีความยาวเพียงแค่ Z สัญลักษณ์เท่านั้น (Z มีค่าไม่เกิน 5) เมตริกความน่าเป็นจริงสูงสุดที่ถูกตัดทอนนี้ (truncated maximum likelihood metric) จะถูกคำนวณที่หน่วยคำนวณเมตริกปฐมภูมิ (primary metric calculation unit : primary MCU) จากนั้นเมตริกที่คำนวณได้จะถูกส่งต่อไปยังหน่วยคำนวณเมตริกทุติยภูมิ (secondary MCU) เพื่อแปลงให้อยู่ในรูปที่เหมาะสมกับการถอดรหัสแบบวนซ้ำต่อไป

. *หน่วยคำนวณเมตริกปฐมภูมิ*

ถ้ามีสมมติฐานให้เฟดดิงมีความสัมพันธ์กันเพียงแค่ Z สัญลักษณ์ที่ติดกันเท่านั้น จะได้ว่า $\phi_F(m) = 0$ เมื่อ $|m| > Z$ และเมตริกในสมการ (4.4) สามารถเขียนใหม่ได้เป็น

$$\begin{aligned}
\Pr\{R_n \mid \underline{I}_1^n, \underline{R}_0^{n-1}\} &= \Pr\{R_n \mid \underline{I}_1^n, \underline{R}_{n-Z}^{n-1}\} \\
&= \frac{1}{\pi\sigma_Z^2} \exp\left\{ -\frac{1}{\sigma_Z^2} \left| R_n - \left(\sum_{z=1}^{Z} P_z R_{n-z} \prod_{k=1}^{z-1} I_{n-k} \right) I_n \right|^2 \right\} \\
&= \Pr\{R_n \mid \underline{I}_{n-Z+1}^n, \underline{R}_0^{n-1}\} \\
&== M_n(\underline{I}_{n-Z+1}^n) \qquad (4.5)
\end{aligned}$$

โดยค่าสัมประสิทธิ์การทำนายเชิงเส้น $\underline{P}_1^Z$ หาได้จากการแก้สมการดังต่อไปนี้

$$\begin{bmatrix} N_o+\phi_F(0) & \phi_F(1) & \cdots & \phi_F(Z-1) \\ \phi_F(1) & N_o+\phi_F(0) & \cdots & \phi_F(Z-2) \\ \vdots & \vdots & \ddots & \vdots \\ \phi_F(Z-1) & \phi_F(Z-2) & \cdots & N_o+\phi_F(0) \end{bmatrix} \times \begin{bmatrix} P_1 \\ P_2 \\ \vdots \\ P_Z \end{bmatrix} = \begin{bmatrix} \phi_F(1) \\ \phi_F(2) \\ \vdots \\ \phi_F(Z) \end{bmatrix} \tag{4.6}$$

และค่า σ_Z^2 สอดคล้องกับสมการ

$$\sigma_Z^2 = N_o + \phi_F(0) - \sum_{z=1}^{Z} P_z \phi_F(z) \tag{4.7}$$

เมตริกในสมการ (4.5) จะสัมพันธ์กับลำดับของสัญลักษณ์ $\underline{I}_{n-z+1}^n$ ซึ่งมีความยาวเพียง Z สัญลักษณ์เท่านั้น ทำให้ความซับซ้อนในการคำนวณน้อยกว่าเมตริกในสมการ (4.4) เมตริกนี้จะถูกคำนวณที่หน่วยคำนวณเมตริกปฐมภูมิ และถูกเรียกว่า เมตริกปฐมภูมิ

. *หน่วยคำนวณเมตริกทุติยภูมิ*

เมตริกปฐมภูมิที่คำนวณได้จากหน่วยคำนวณเมตริกปฐมภูมิ ยังไม่สามารถส่งไปให้เครื่องถอดรหัสเทอร์โบได้ เนื่องจากขั้นตอนในการคำนวณเมตริกดังกล่าวไม่เหมาะสมกับกรรมวิธีการถอดรหัสแบบวนซ้ำซึ่งใช้ประโยชน์จากเทคนิคการสลับลำดับของสัญญาณในการเข้าและถอดรหัส เพราะฉะนั้นหน่วยคำนวณเมตริกทุติยภูมิจึงมีหน้าที่ดัดแปลงเมตริกปฐมภูมิในสมการ (4.5) ให้ขึ้นอยู่กับสัญลักษณ์ I_n เพียงสัญลักษณ์เดียว เพื่อให้เมตริกที่ถูกสร้างขึ้นใหม่เข้ากันได้กับตัวสลับลำดับและเครื่องถอดรหัสเทอร์โบ เรียกเมตริกใหม่นี้ว่า เมตริกทุติยภูมิ ซึ่งสามารถคำนวณได้จากเมตริกปฐมภูมิ ดังสมการต่อไปนี้ (รายละเอียดในการคำนวณแสดงอยู่ในภาคผนวก ก)

$$\begin{aligned} \Gamma_n(I_n) &\quad \Pr\{R_n \mid I_n, \underline{R}_0^{n-1}\} \\ &= \sum_{\underline{I}_{n-Z+1}^{n-1}} M_n(\underline{I}_{n-Z+1}^n)\Psi_{n-1}(\underline{I}_{n-Z+1}^{n-1}) \end{aligned} \tag{4.8}$$

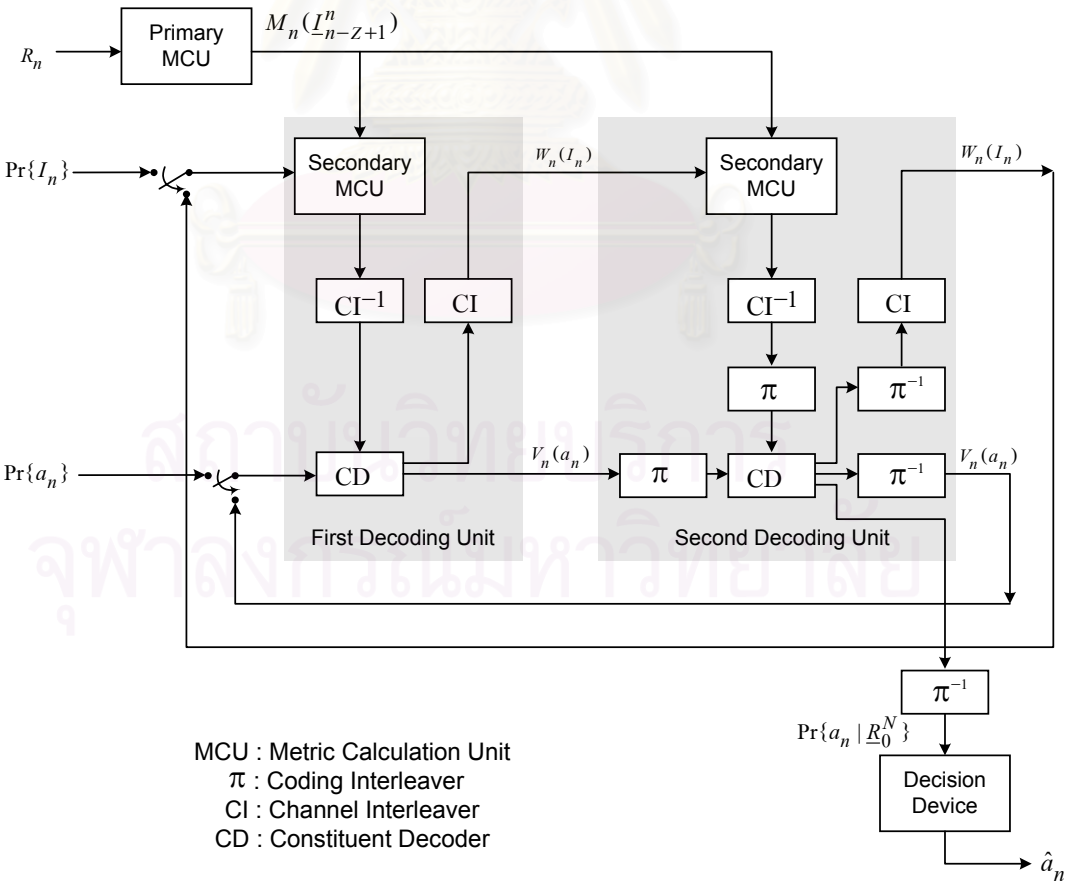
โดยที่

$$\Psi_{n-1}(\underline{I}_{n-Z+1}^{n-1}) = \frac{\sum_{I_{n-Z}} M_{n-1}(\underline{I}_{n-Z}^{n-1})\Psi_{n-2}(\underline{I}_{n-Z}^{n-2})\Pr\{I_{n-1}\}}{\sum_{\underline{I}_{n-Z+1}^{n-1}} \sum_{I_{n-Z}} M_{n-1}(\underline{I}_{n-Z}^{n-1})\Psi_{n-2}(\underline{I}_{n-Z}^{n-2})\Pr\{I_{n-1}\}} \tag{4.9}$$

เมตริกทุติยภูมินี้จะถูกส่งไปให้เครื่องถอดรหัสเทอร์โบเพื่อใช้เป็นค่าประมาณข่าวสารจากช่องสัญญาณ หลักการทำงานของเครื่องถอดรหัสเทอร์โบจะกล่าวถึงในหัวข้อต่อไป

4.2 การถอดรหัสเทอร์โบ

หลักการถอดรหัสเทอร์โบโดยทั่วไปนั้นอาศัยการถอดรหัสแบบวนซ้ำ (iterative decoding) ของเครื่องถอดรหัสย่อยจำนวนเท่ากับจำนวนเครื่องเข้ารหัสย่อยที่ใช้ในการเข้ารหัส ในที่นี้คือสองตัว คำรหัสที่ไม่ถูกสลับลำดับจะถูกถอดรหัสก่อนที่เครื่องถอดรหัสย่อยตัวที่หนึ่ง จากนั้นข่าวสารที่ได้จากการถอดรหัสจะถูกส่งผ่านไปให้เครื่องถอดรหัสย่อยตัวที่สอง ซึ่งจะทำหน้าที่ถอดรหัสคำรหัสที่ถูกสลับลำดับให้ตรงกับลำดับที่ป้อนเข้าสู่เครื่องเข้ารหัสย่อยตัวที่สอง นอกจากนี้ยังส่งข่าวสารส่วนหนึ่งกลับไปให้เครื่องถอดรหัสย่อยตัวแรกอีกด้วย ข่าวสารนั้นเรียกว่า ข่าวสารเอ็กซ์ทรินซิก (extrinsic information) การส่งผ่านข่าวสารเอ็กซ์ทรินซิกระหว่างกันของเครื่องถอดรหัสย่อยทั้งสองตัวนั้นทำให้ความเชื่อถือได้ (reliability) ของการถอดรหัสในแต่ละรอบมีค่าดีขึ้น การถอดรหัสจะดำเนินซ้ำไปซ้ำมาจนกระทั่งจำนวนรอบของการถอดรหัสมีค่ามากพอ จากนั้นจะนำค่าความน่าจะเป็นหลัง (*a posteriori* probability : APP) $\Pr\{a_n \mid \underline{R}_0^N\}$ ที่คำนวณได้ไปใช้ในการตัดสินว่าบิตใดถูกส่งมา หลักการที่กล่าวมาข้างต้นนี้ถูกนำมาประยุกต์เพื่อให้สอดคล้องกับเครื่องเข้ารหัสที่กล่าวไว้ในบทที่ 2 โครงสร้างของเครื่องถอดรหัสจะเป็นดังรูปที่ 4.1



รูปที่ 4.1 โครงสร้างของเครื่องถอดรหัส

จากรูปจะเห็นว่า โครงสร้างของเครื่องถอดรหัสประกอบด้วย หน่วยคำนวณเมตริกปฐมภูมิ (primary MCU) หน่วยคำนวณเมตริกทุติยภูมิ (secondary MCU) และเครื่องถอดรหัสย่อย (constituent decoder : CD) สัญลักษณ์ที่รับได้จะถูกป้อนให้กับหน่วยคำนวณเมตริกปฐมภูมิ ซึ่งจะทำหน้าที่คำนวณเมตริกที่เป็นค่าประมาณข่าวสารช่องสัญญาณ โดยอาศัยวิธีการตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ ให้ผลออกมาเป็นเมตริกปฐมภูมิ ซึ่งเป็นค่าที่แสดงถึงความน่าเป็นจริงของสัญญาณที่รับได้เมื่อกำหนดให้ชุดข้อมูลที่ถูกส่งมาเป็นค่าหนึ่ง ๆ จากนั้นหน่วยคำนวณเมตริกทุติยภูมิจะนำเมตริกเหล่านี้ไปแปลงให้เป็นเมตริกทุติยภูมิ เพื่อให้เหมาะสำหรับการถอดรหัสแบบวนซ้ำดังที่ได้อธิบายไว้ในหัวข้อที่ผ่านมา สำหรับเครื่องถอดรหัสย่อยแต่ละตัวจะทำหน้าที่คำนวณค่าความน่าจะเป็นหลัง (*a posteriori* probability : APP) โดยอาศัยขั้นตอนวิธีที่พัฒนาขึ้นโดย Bahl, Cocke, Jelinek และ Raviv [22] เรียกว่าขั้นตอนวิธี BCJR หรือ ขั้นตอนวิธี MAP ค่าความน่าจะเป็นหลังนี้เองที่เครื่องถอดรหัสใช้เป็นตัวตัดสินว่าบิตที่ถูกส่งมาคือบิตใด นอกจากนี้เครื่องถอดรหัสย่อยยังถูกออกแบบให้ส่งข่าวสารเอ็กซ์ทรินซิกของสัญลักษณ์ที่ถูกส่งมา กลับไปให้หน่วยคำนวณเมตริกทุติยภูมิเพื่อใช้ในการคำนวณข่าวสารช่องสัญญาณอีกด้วย เพราะฉะนั้นการประมาณช่องสัญญาณจึงแม่นยำขึ้นในแต่ละรอบของการถอดรหัสเทอร์โบ

4.2.1 การถอดรหัสโดยใช้ขั้นตอนวิธี BCJR

เครื่องถอดรหัสย่อยแต่ละตัวจะถอดรหัสโดยอาศัยขั้นตอนวิธีของ BCJR ซึ่งถูกดัดแปลงเพื่อให้เหมาะสมกับวิธีการตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ ในช่องสัญญาณแบบเฟดดิง ค่าความน่าจะเป็นหลัง (*a posteriori* probability : APP) ของบิตข้อมูล a_n สามารถคำนวณได้จากสมการต่อไปนี้

$$\Pr\{a_n \mid \underline{R}_0^N\} = \sum_{(S_n, S_{n+1}):a_n} \Pr\{S_n, S_{n+1} \mid \underline{R}_0^N\} \qquad (4.10)$$

เมื่อ a_n คือบิตข้อมูล ณ เวลา n ซึ่งต้องการจะถอดรหัส โดยที่ a_n เป็นบิตข้อมูลในชุดของลำดับบิตข้อมูล $\underline{a}_1^N$ ที่ถูกป้อนให้กับเครื่องเข้ารหัสย่อยเรียงตามลำดับตั้งแต่ 1 ถึง N

$\underline{R}_0^N$ คือชุดของลำดับสัญลักษณ์ที่รับได้ที่เครื่องถอดรหัสย่อย มีลำดับตรงกันกับลำดับของ $\underline{a}_1^N$ ซึ่งหมายความว่า บิตข้อมูล a_n ถูกรับได้อยู่ในสัญลักษณ์ R_n

S_n คือ สถานะ (state) ของเครื่องเข้ารหัสย่อยก่อนที่ a_n จะถูกเข้ารหัส

S_{n+1} คือ สถานะของเครื่องเข้ารหัสย่อยหลังจากที่ a_n ถูกเข้ารหัสแล้ว

$(S_n, S_{n+1}) : a_n$ หมายถึง เหตุการณ์ที่เครื่องเข้ารหัสย่อยเปลี่ยนสถานะจาก S_n ไปเป็น S_{n+1} เมื่อบิตข้อมูล a_n ถูกป้อนเข้าสู่เครื่องเข้ารหัสย่อย

ค่าความน่าจะเป็นหลังที่คำนวณได้นี้จะนำมาใช้ในการตัดสินใจว่าบิตข้อมูล a_n น่าจะเป็นบิตใดระหว่างบิต 0 กับบิต 1 โดยกระบวนการตัดสินใจเป็นไปดังนี้

$$\Pr\{a_n = 0 \mid \underline{R}_0^N\} \underset{a_n = 1}{\overset{a_n = 0}{\gtrless}} \Pr\{a_n = 1 \mid \underline{R}_0^N\} \tag{4.11}$$

กฎการตัดสินใจแบบนี้ เรียกว่า การหาค่าความน่าจะเป็นหลังสูงสุด (maximum *a posteriori* : MAP) โดยจะตัดสินให้บิต a_n มีค่าเป็น 0 เมื่อค่าความน่าจะเป็นหลังที่กำหนดให้ $a_n = 0$ มีค่ามากกว่าค่าความน่าจะเป็นหลังที่กำหนดให้ $a_n = 1$ และตัดสินให้ a_n มีค่าเป็น 1 ในกรณีตรงกันข้ามกับกรณีแรก

ในการคำนวณค่าความน่าจะเป็นหลังมักจะมีการแปลงรูปความสัมพันธ์ และจัดให้อยู่ในรูปแบบที่คำนวณได้ง่ายโดยใช้วิธีรีเคอร์ซีฟ ดังต่อไปนี้ (ดูภาคผนวก ข ประกอบ)

$$\Pr\{a_n \mid \underline{R}_0^N\} = \frac{\sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1})}{\sum_{a_n} \sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1})} \tag{4.12}$$

โดยที่

$$\alpha_n(S_n) = \Pr(S_n \mid \underline{R}_0^{n-1}) \tag{4.13}$$

$$\beta_n(S_n) = \frac{\Pr\{\underline{R}_n^N \mid S_n, \underline{R}_0^{n-1}\}}{\Pr\{\underline{R}_n^N \mid \underline{R}_0^{n-1}\}} \tag{4.14}$$

และ

$$\gamma_n(S_n, S_{n+1}) = \Pr\{R_n, S_{n+1} \mid S_n, \underline{R}_0^{n-1}\} \tag{4.15}$$

$\alpha_n(S_n)$ และ $\beta_n(S_n)$ คือ ความน่าจะเป็นของสถานะของเครื่องเข้ารหัสย่อยเมื่อกวาดแผนภาพเทรลลิส (Trellis diagram) ไปข้างหน้าและข้างหลัง ซึ่งสามารถคำนวณในลักษณะรีเคอร์ซีฟแบบไปข้างหน้า (forward recursive) และรีเคอร์ซีฟแบบย้อนไปข้างหลัง (backward recursive) ได้ดังนี้

$$\alpha_{n+1}(S_{n+1}) = \frac{\sum_{S_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})}{\sum_{S_{n+1}} \sum_{S_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})} \tag{4.16}$$

$$\beta_n(S_n) = \frac{\sum_{S_{n+1}} \gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1})}{\sum_{S_n} \sum_{S_{n+1}} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})} \tag{4.17}$$

$\gamma_n(S_n, S_{n+1})$ คือ ฟังก์ชันเมตริกสาขา (branch metric function) ซึ่งคำนวณได้ดังนี้

$$\gamma_n(S_n, S_{n+1}) = \Pr\{S_{n+1} \mid S_n\} \Pr\{R_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}\} \tag{4.18}$$

ถ้าวงจรเข้ารหัสไม่สามารถเปลี่ยนสถานะจาก S_n ไปเป็นสถานะ S_{n+1} ได้ $\gamma_n(S_n, S_{n+1})$ จะมีค่าเท่ากับ 0 แต่สำหรับกรณีที่การเปลี่ยนสถานะมีความเป็นไปได้ จะได้ว่า

$$\gamma_n(S_n, S_{n+1}) = \Pr\{a_n\} \Pr\{R_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}\} \tag{4.19}$$

โดยที่

$$\Pr\{R_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}\} = \sum_{p_n} \Gamma_n(a_n, p_n) \Pr\{p_n \mid S_n, S_{n+1}\} \tag{4.20}$$

$\Pr\{p_n \mid S_n, S_{n+1}\}$ จะมีค่าเท่ากับ 1 ก็ต่อเมื่อ การเปลี่ยนสถานะจาก S_n ไปเป็น S_{n+1} มีความเป็นไปได้ และการเปลี่ยนสถานะนั้นได้บิตรหัสเป็น p_n แต่สำหรับกรณีที่ p_n ถูกพังก์เจอร์ จะกำหนดให้ $\Pr\{p_n \mid S_n, S_{n+1}\}$ มีค่าเท่ากับ 0.5

จากสมการ (4.19) และ (4.20) จะได้ว่าฟังก์ชันเมตริกสาขามีค่าเท่ากับ

$$\gamma_n(S_n, S_{n+1}) = \Pr\{a_n\} \sum_{p_n} \Gamma_n(a_n, p_n) \Pr\{p_n \mid S_n, S_{n+1}\} \tag{4.21}$$

ฟังก์ชันเมตริกสาขาตามสมการ (4.21) ประกอบด้วยความน่าจะเป็นเบื้องแรก (*a priori* probability) $\Pr\{a_n\}$ และ ฟังก์ชันเมตริกช่องสัญญาณ $\Gamma_n(a_n, p_n)$ ซึ่งคำนวณได้จากหน่วยคำนวณเมตริกทุติยภูมิ สำหรับการถอดรหัสแบบวนซ้ำในรอบแรก จะกำหนดให้ $\Pr\{a_n\}$ มีค่าเท่ากับ 0.5 ส่วนในรอบถัดไปค่าความน่าจะเป็นเบื้องแรกจะคำนวณได้จากข่าวสารเอ็กซ์ทรินซิกของบิตข้อมูลนั้นซึ่งได้มาจากเครื่องถอดรหัสย่อยตัวอื่น วิธีการคำนวณข่าวสารเอ็กซ์ทรินซิกของเครื่องถอดรหัสย่อยจะกล่าวถึงในหัวข้อต่อไป

4.2.2 ข่าวสารเอ็กซ์ทรินซิก

การที่เครื่องถอดรหัสเทอร์โบมีประสิทธิภาพสูง ก็เนื่องมาจากความสามารถในการส่งผ่านข่าวสารจากเครื่องถอดรหัสย่อยตัวหนึ่งไปยังอีกตัวหนึ่ง ทำให้ความเชื่อถือได้ (reliability) เพิ่มขึ้นในแต่ละรอบของการถอดรหัส โดยทั่วไปแล้วข่าวสารเกี่ยวกับบิตข้อมูล a_n พิจารณาได้จาก 3 ทาง คือ 1) ฟังก์ชันความน่าจะเป็นเบื้องแรก (*a priori* pdf) ของ a_n 2) ข่าวสารซิสเต็มมาติก (systematic information) จากสัญลักษณ์ที่รับได้ซึ่งมีข้อมูล a_n อยู่ และ 3) ข่าวสารเกี่ยวกับ a_n ที่ได้รับรู้ผ่านทางสัญลักษณ์ที่รับได้ตัวอื่น ๆ ข่าวสารในข้อ 3) นี้เอง ที่เรียกว่า ข่าวสารเอ็กซ์ทรินซิก (extrinsic information) ซึ่งจะถูกส่งจากเครื่องถอดรหัสย่อยตัวหนึ่งไปยังอีกตัวหนึ่งในรูปของข่าวสารเบื้องแรก (*a priori* information) $\Pr\{a_n\}$

การจะคำนวณข่าวสารเอ็กซ์ทรินซิกจากความน่าจะเป็นหลัง $\Pr\{a_n \mid \underline{R}_0^N\}$ จำเป็นจะต้องกำจัดข่าวสารเบื้องแรกและข่าวสารซิสเต็มมาติกออกก่อนเพื่อไม่ให้เกิดความซ้ำซ้อนของข่าวสารที่จะส่งไปให้เครื่องถอดรหัสย่อยอีกตัวหนึ่ง ข่าวสารซิสเต็มมาติกในที่นี้มีค่าเท่ากับ $\frac{1}{2}\sum_{p_n}\Gamma_n(a_n, p_n)$ ดังนั้นจะได้ว่า ข่าวสารเอ็กซ์ทรินซิกมีค่าดังนี้ (ดูภาคผนวก ข ประกอบ)

$$V_n(a_n) = \frac{\Pr\{a_n \mid \underline{R}_0^N\}}{\Pr\{a_n\} \bullet \frac{1}{2}\sum_{p_n}\Gamma_n(a_n, p_n)}$$

$$= \frac{\sum_{(S_n, S_{n+1}):a_n} \frac{\sum_{p_n}\Gamma_n(a_n, p_n)\Pr\{p_n \mid S_n, S_{n+1}\}}{\sum_{p_n}\Gamma_n(a_n, p_n)} \alpha_n(S_n)\beta_{n+1}(S_{n+1})}{\sum_{a_n}\sum_{(S_n, S_{n+1}):a_n} \frac{\sum_{p_n}\Gamma_n(a_n, p_n)\Pr\{p_n \mid S_n, S_{n+1}\}}{\sum_{p_n}\Gamma_n(a_n, p_n)} \alpha_n(S_n)\beta_{n+1}(S_{n+1})} \qquad (4.22)$$

ในทำนองเดียวกันเราสามารถดึงข่าวสารเอ็กซ์ทรินซิกของสัญลักษณ์ I_n ออกจากความน่าจะเป็นหลัง $\Pr\{a_n, p_n \mid \underline{R}_0^N\}$ ได้เช่นกันโดยนำข่าวสารเบื้องแรก $\Pr\{a_n\}$ และข่าวสารซิสเต็มมาติก $\Gamma_n(a_n, p_n)$ ไปหารออกจาก $\Pr\{a_n, p_n \mid \underline{R}_0^N\}$ ดังสมการต่อไปนี้

$$W_n(I_n) = W_n(a_n, p_n) = \frac{\Pr\{a_n, p_n \mid \underline{R}_0^N\}}{\Pr\{a_n\}\Gamma_n(a_n, p_n)}$$

$$= \frac{\sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\beta_{n+1}(S_{n+1})\Pr\{p_n \mid S_n, S_{n+1}\}}{\sum_{a_n}\sum_{p_n}\sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\beta_{n+1}(S_{n+1})\Pr\{p_n \mid S_n, S_{n+1}\}} \quad (4.23)$$

ข่าวสารเอ็กซ์ทรินซิกของสัญลักษณ์ I_n ที่คำนวณได้จากสมการ (4.23) จะถูกส่งไปให้กับหน่วยคำนวณเมตริกทุติยภูมิ เพื่อใช้เป็นข่าวสารเบื้องแรกของสัญลักษณ์ I_n $\Pr\{I_n\}$ ดังนั้นข่าวสารจากช่องสัญญาณจะถูกปรับปรุงให้มีค่าถูกต้องยิ่งขึ้นในทุกรอบของการถอดรหัสเทอร์โบ

บทที่ 5

ระบบที่เสนอ

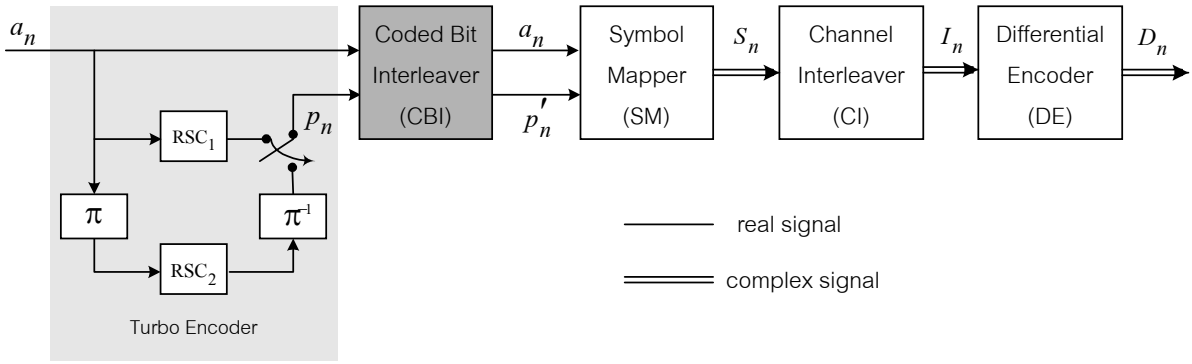
บทนี้จะอธิบายถึงโครงสร้างของระบบที่เสนอ โดยมีวัตถุประสงค์เพื่อปรับปรุงสมรรถนะของระบบเดิมให้สามารถทนทานต่อเฟดดิงที่เกิดในช่องสัญญาณได้มากขึ้น หัวข้อที่จะกล่าวถึงประกอบด้วย ส่วนของการเข้ารหัสที่ภาคส่งและส่วนของการถอดรหัสที่ภาครับ ซึ่งดัดแปลงให้สอดคล้องกับภาคเข้ารหัส และสัมพันธ์กับการประมาณข่าวสารช่องสัญญาณของตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์

5.1 ภาคเข้ารหัสที่เสนอ

เนื่องจากช่องสัญญาณแบบเฟดดิง มีผลทำให้สัญลักษณ์ที่รับได้มีขนาดและเฟสผิดเพี้ยนไปจากสัญลักษณ์ที่ถูกส่งมา โดยเฉพาะกรณีช่องสัญญาณที่เกิดเรย์ลีเฟดดิงที่มีสหสัมพันธ์กัน ซึ่งเฟดดิงจะมีความสัมพันธ์กันทางเวลา ทำให้ความผิดพลาดที่เกิดจากเฟดดิงมีแนวโน้มที่จะเกิดเป็นเบิรสต์ คือ มีความผิดพลาดที่ติดกันเป็นช่วงยาวและแก้ไขได้ยาก

เมื่อพิจารณาระบบเข้ารหัสที่กล่าวไว้ในบทที่ 2 จะพบว่า บิตข้อมูล a_n และบิตรหัส p_n ถูกจับคู่อยู่ในสัญลักษณ์ QPSK เดียวกัน ทำให้คู่บิต (a_n, p_n) เกิดความเสียหายขึ้นพร้อมกันเมื่อถูกส่งผ่านช่องสัญญาณแบบเฟดดิง ส่งผลให้ภาครับไม่ได้รับข่าวสารของบิตนั้นเลย ทั้งจากบิตข้อมูล a_n และบิตรหัส p_n ยิ่งไปกว่านั้นหากเฟดดิงที่เกิดขึ้นมีลักษณะเป็นเบิรสต์ ทางภาครับจะไม่ได้รับข่าวสารที่ถูกต้องติดกันเป็นช่วงยาว เป็นผลให้เครื่องถอดรหัสเทอร์โบไม่สามารถทำงานได้อย่างมีประสิทธิภาพ งานวิจัยนี้จึงเสนอให้ภาคส่งแยกส่งบิตข้อมูล a_n กับบิตรหัส p_n ไปในสัญลักษณ์ QPSK ต่างสัญลักษณ์กัน เพื่อหลีกเลี่ยงกรณีที่บิตข้อมูล a_n กับบิตรหัส p_n จะ เสียหายไปพร้อมกัน โดยคาดหวังว่าระบบที่เสนอนี้จะช่วยให้ความผิดพลาดที่เกิดขึ้นจากเฟดดิง โดยเฉพาะอย่างยิ่งเฟดดิงแบบเบิรสต์มีค่าลดลง ภาคเข้ารหัสที่เสนอแสดงอยู่ในรูปที่ 5.1

ส่วนประกอบของภาคเข้ารหัสที่เพิ่มขึ้นมาก็คือ ตัวสลับลำดับบิตรหัส (coded bit interleaver : CBI) ซึ่งต่ออยู่ก่อนหน้าตัวจับคู่สัญลักษณ์ (SM) ตัวสลับลำดับบิตรหัสจะทำหน้าที่จัดลำดับของบิตรหัส p_n ไม่ให้ตรงกันกับลำดับของบิตข้อมูล a_n เพราะฉะนั้นสัญลักษณ์ S_n จะไม่ได้ประกอบด้วยคู่บิต (a_n, p_n) แต่ประกอบด้วยคู่บิต (a_n, p'_n) เมื่อ p'_n คือ บิตรหัสหลังจากถูกสลับลำดับด้วยตัวสลับลำดับบิตรหัส โดยที่ $p'_n \neq p_n$ กล่าวคือ p'_n ต้องไม่ใช่บิตรหัสที่เกิดจากการเข้ารหัสบิตข้อมูล a_n



รูปที่ 5.1 ภาคเข้ารหัสที่เสนอ

5.2 ภาคถอดรหัสที่เสนอ

โครงสร้างของภาคถอดรหัสได้ถูกดัดแปลงเพื่อให้สอดคล้องกับภาคเข้ารหัสที่เสนอ ดังรูปที่ 5.2 ส่วนที่แตกต่างจากภาคถอดรหัสแบบเดิมก็คือ ตัวสลับลำดับกลับบิตรหัส (coded bit deinterleaver : CBI^{-1}) ที่เรียงต่อจากตัวสลับลำดับกลับช่องสัญญาณ (CI^{-1}) ตัวสลับลำดับกลับบิตรหัสที่เพิ่มขึ้นมานี้มีหน้าที่สลับลำดับเมตริกทุติยภูมิ $\Gamma_n(I_n)$ เพื่อให้ตัวถอดรหัสย่อยนำไปใช้ในสองรูปแบบคือ $\Gamma_n(a_n, p_n')$ และ $\tilde{\Gamma}_n(a_n', p_n)$ ทั้งนี้การคำนวณค่าความน่าจะเป็นหลัง และ ข่าวสารเอ็กซ์ทรินซิกของเครื่องถอดรหัสย่อย จะแตกต่างจากขั้นตอนการคำนวณที่ได้กล่าวไว้ในบทที่แล้ว เนื่องจากบิตข้อมูล a_n และบิตรหัส p_n ไม่ได้ถูกส่งมาในสัญลักษณ์ QPSK เดียวกัน นอกจากนี้ข่าวสารช่องสัญญาณที่คำนวณได้จากหน่วยคำนวณเมตริกทุติยภูมิ ยังไม่สามารถนำมาใช้ที่เครื่องถอดรหัสย่อยได้โดยตรง แต่ต้องมีการปรับเปลี่ยนเพื่อให้สัมพันธ์กับขั้นตอนการถอดรหัสของเครื่องถอดรหัสย่อยที่เสนอ

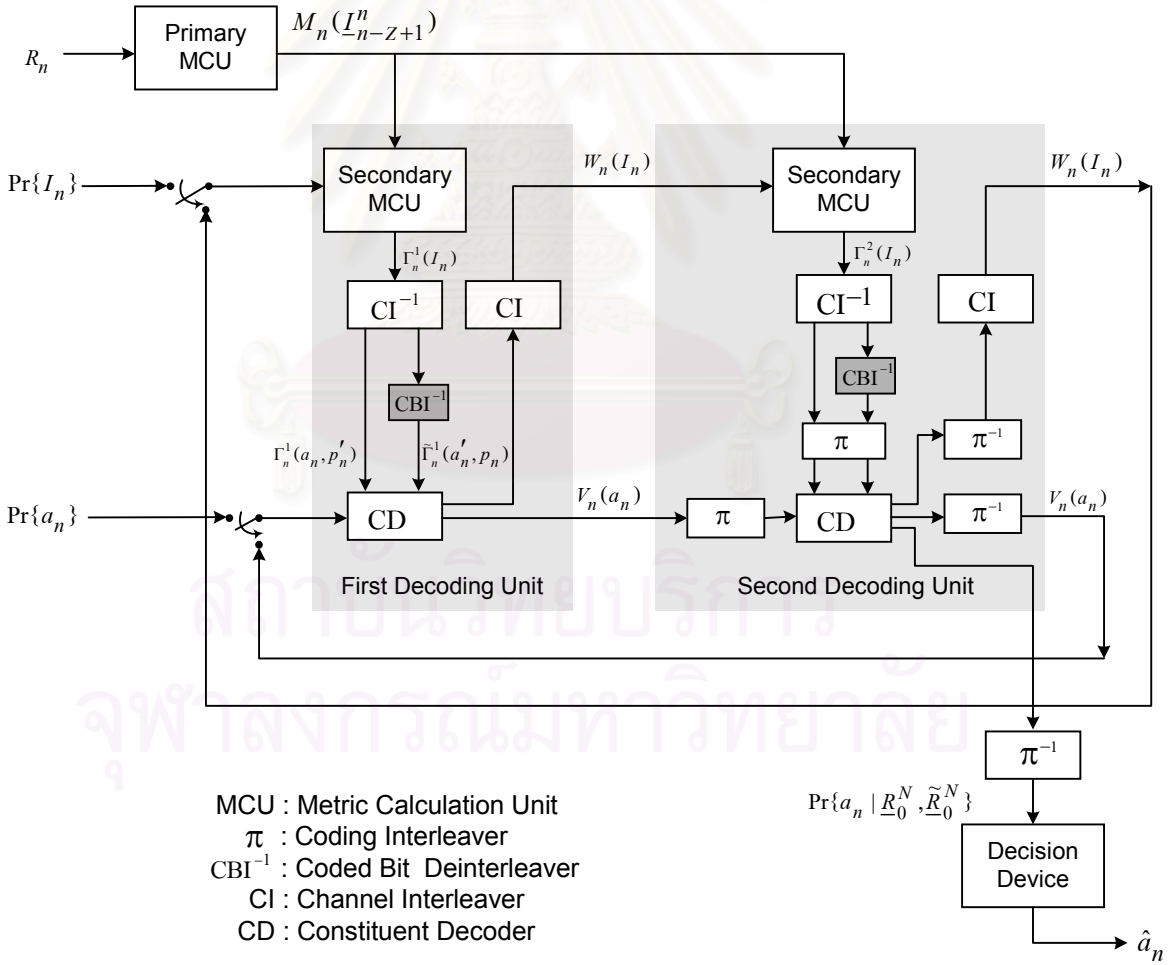
หัวข้อนี้จะวิเคราะห์การทำงานของเครื่องถอดรหัสย่อย ทั้งการคำนวณค่าความน่าจะเป็นหลังและข่าวสารเอ็กซ์ทรินซิก รวมถึงการประยุกต์ใช้ข่าวสารช่องสัญญาณที่มาจากหน่วยคำนวณเมตริกทุติยภูมิ

5.2.1 การคำนวณค่าความน่าจะเป็นหลัง

สำหรับระบบที่เสนอ ซึ่งบิตข้อมูล a_n และบิตรหัส p_n ถูกแยกส่งมาในสัญลักษณ์ QPSK ต่างสัญลักษณ์กัน ในกระบวนการถอดรหัสของเครื่องถอดรหัสย่อย สัญลักษณ์ที่รับได้ R_n จะถูกนำมาใช้ในสองรูปแบบ คือ $\underline{R}_0^N$ และ $\underline{\tilde{R}}_0^N$ โดยที่แต่ละแบบจะมีการเรียงลำดับของสัญลักษณ์แตกต่างกัน ในรูปแบบแรก ชุดของลำดับสัญลักษณ์ที่รับได้จะมีลำดับตรงกับลำดับของบิตข้อมูลที่ถูกป้อนให้กับเครื่องเข้ารหัสย่อย เขียนแทนด้วย $\underline{R}_0^N$ ส่วนรูปแบบที่สอง ลำดับของสัญลักษณ์ที่รับได้จะถูกเรียงให้ตรงกับลำดับของบิตรหัสที่ออกมาจากเครื่องเข้ารหัสย่อย เขียนแทนด้วย $\underline{\tilde{R}}_0^N$

นอกจากนี้เมตริกทุติยภูมิ $\Gamma_n(I_n)$ ที่นำมาใช้ในการคำนวณค่าความน่าจะเป็นหลัง ก็ถูกนำมาใช้ในสองรูปแบบด้วยเช่นกัน คือ $\Gamma_n(a_n, p'_n)$ และ $\tilde{\Gamma}_n(a'_n, p_n)$ เมตริกแรกเป็นเมตริกที่ได้มาจากหน่วยคำนวณเมตริกทุติยภูมิที่ผ่านการสลับลำดับกลับช่องสัญญาณเพียงอย่างเดียว ดังนั้นเมตริกนี้จะมีลำดับตรงกับลำดับของบิตข้อมูลที่ถูกป้อนให้กับเครื่องเข้ารหัสย่อย ส่วนเมตริกที่สองจะเป็นเมตริกที่ถูกเรียงลำดับด้วยตัวสลับลำดับกลับบิตรหัสอีกทีหนึ่ง เพื่อให้มีลำดับตรงกับลำดับของบิตรหัสที่ออกมาจากเครื่องเข้ารหัสย่อย

เครื่องถอดรหัสย่อยในระบบที่เสนอนี้ นอกจากจะมีหน้าที่คำนวณค่าความน่าจะเป็นหลังและข่าวสารเอ็กซ์ทรินซิกของบิตข้อมูล a_n แล้ว ยังถูกออกแบบให้คำนวณค่าความน่าจะเป็นหลังและข่าวสารเอ็กซ์ทรินซิกของบิตรหัส p_n อีกด้วย ข่าวสารเอ็กซ์ทรินซิกของบิตรหัส p_n จะถูกนำมาใช้ในรูปของข่าวสารเบื้องแรกของบิตรหัส p_n เพื่อนำไปคำนวณค่าความน่าจะเป็นหลังที่เครื่องถอดรหัสย่อยอีกตัวหนึ่ง



รูปที่ 5.2 ภาคถอดรหัสที่เสนอ

5.2.1.1 ค่าความน่าจะเป็นหลังของบิตข้อมูล a_n

ก่อนจะกล่าวถึงสมการที่ใช้คำนวณค่าความน่าจะเป็นหลังของบิตข้อมูล a_n เขียนแทนด้วย $\Pr\{a_n \mid \underline{R}_0^N, \underline{\widetilde{R}}_0^N\}$ จะขอนิยามสัญลักษณ์ต่าง ๆ ดังต่อไปนี้

$\underline{a}_1^N$ คือ ชุดของลำดับบิตข้อมูลเรียงตามลำดับที่ถูกป้อนเข้าสู่เครื่องเข้ารหัสเทอร์โบ

$\underline{p}_1^N$ คือ ชุดของลำดับบิตรหัสเรียงตามลำดับที่ออกมาจากเครื่องเข้ารหัสเทอร์โบ ซึ่งบิตรหัส p_n เกิดจากการเข้ารหัสบิตข้อมูล a_n ที่เครื่องเข้ารหัสเทอร์โบนั่นเอง

$\underline{R}_0^N$ คือ ชุดของลำดับสัญลักษณ์ที่รับได้ที่เครื่องถอดรหัสย่อย มีลำดับตรงกันกับลำดับของ $\underline{a}_1^N$ ซึ่งหมายความว่าสัญลักษณ์ R_n ประกอบไปด้วยข่าวสารจากคู่บิต (a_n, p_n')

$\underline{\widetilde{R}}_0^N$ คือ ชุดของลำดับสัญลักษณ์ที่รับได้ที่เครื่องถอดรหัสย่อย มีลำดับตรงกันกับลำดับของ $\underline{p}_1^N$ ซึ่งหมายความว่าสัญลักษณ์ $\widetilde{R}_n$ ประกอบไปด้วยข่าวสารจากคู่บิต (a_n', p_n)

a_n' คือ บิตข้อมูลที่ถูกสลับลำดับด้วยตัวสลับลำดับกลับบิตรหัส (CBI^{-1})

p_n' คือ บิตรหัสที่ถูกสลับลำดับด้วยตัวสลับลำดับบิตรหัส (CBI)

S_n คือ สถานะของเครื่องเข้ารหัสย่อยก่อนที่ a_n จะถูกเข้ารหัส

S_{n+1} คือ สถานะของเครื่องเข้ารหัสย่อยหลังจากที่ a_n ถูกเข้ารหัสแล้ว

$(S_n, S_{n+1}) : a_n$ หมายถึง เหตุการณ์ที่เครื่องเข้ารหัสย่อยเปลี่ยนสถานะจาก S_n ไปเป็น S_{n+1} เมื่อบิตข้อมูล a_n ถูกป้อนเข้าสู่เครื่องเข้ารหัสย่อย

ค่าความน่าจะเป็นหลัง (*a posteriori* probability : APP) ของบิตข้อมูล a_n คำนวณได้จากสมการต่อไปนี้ (ดูภาคผนวก ค ประกอบ)

$$\Pr\{a_n \mid \underline{R}_0^N, \underline{\widetilde{R}}_0^N\} = \sum_{(S_n, S_{n+1}):a_n} \Pr\{S_n, S_{n+1} \mid \underline{R}_0^N, \underline{\widetilde{R}}_0^N\}$$

$$= \frac{\sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1})}{\sum_{a_n}\sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1})} \qquad (5.1)$$

เมื่อ

$$\alpha_n(S_n) = \Pr(S_n \mid \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}) \tag{5.2}$$

$$\beta_n(S_n) = \frac{\Pr\{\underline{R}_n^N, \underline{\widetilde{R}}_n^N \mid S_n, \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\}}{\Pr\{\underline{R}_n^N, \underline{\widetilde{R}}_n^N \mid \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\}} \tag{5.3}$$

และ

$$\gamma_n(S_n, S_{n+1}) = \Pr\{R_n, \widetilde{R}_n, S_{n+1} \mid S_n, \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\} \tag{5.4}$$

$\alpha_n(S_n)$ และ $\beta_n(S_n)$ สามารถคำนวณในลักษณะรีเคอร์ซีฟได้ดังนี้

$$\alpha_{n+1}(S_{n+1}) = \frac{\sum_{S_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})}{\sum_{S_{n+1}} \sum_{S_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})} \tag{5.5}$$

$$\beta_n(S_n) = \frac{\sum_{S_{n+1}} \gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1})}{\sum_{S_n} \sum_{S_{n+1}} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})} \tag{5.6}$$

และฟังก์ชันเมตริกสาขา $\gamma_n(S_n, S_{n+1})$ คำนวณได้จากสมการต่อไปนี้

$$\gamma_n(S_n, S_{n+1}) = \Pr\{a_n\}\Pr\{R_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}\}\Pr\{\widetilde{R}_n \mid S_n, S_{n+1}, \underline{\widetilde{R}}_0^{n-1}\} \tag{5.7}$$

โดยที่

$$\Pr\{R_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}\} = \sum_{p_n'} \Gamma_n(a_n, p_n')\Pr\{p_n'\} \tag{5.8}$$

และ

$$\Pr\{\widetilde{R}_n \mid S_n, S_{n+1}, \underline{\widetilde{R}}_0^{n-1}\} = \sum_{a_n'} \widetilde{\Gamma}_n(a_n', p_n)\Pr\{a_n'\} \tag{5.9}$$

จากสมการ (5.7) ถึง (5.9) จะเห็นว่าฟังก์ชันเมตริกสาขาประกอบด้วย ข่าวสารเบื้องแรก $\Pr\{a_n\}$ และฟังก์ชันเมตริกช่องสัญญาณของสัญลักษณ์ที่รับได้ R_n และ $\widetilde{R}_n$ ซึ่งได้จากเมตริกทุติยภูมิ $\Gamma_n(I_n)$ เมื่อ I_n แทนคู่บิต (a_n, p_n') และ เมตริก $\widetilde{\Gamma}_n(\widetilde{I}_n)$ เมื่อ $\widetilde{I}_n$ แทนคู่บิต (a_n', p_n) ซึ่งคำนวณได้จากหน่วยคำนวณเมตริกทุติยภูมิ

5.2.1.2 ค่าความน่าจะเป็นหลังของบิตรหัส p_n

ค่าความน่าจะเป็นหลังของบิตข้อมูล a_n จะถูกนำไปใช้ตัดสินว่าบิตใดถูกส่งมา สำหรับค่าความน่าจะเป็นหลังของบิตรหัส p_n นั้น เป็นค่าที่จะนำไปใช้คำนวณข่าวสารเอ็กซ์ทรินซิกของบิตรหัส p_n โดยวิธีการคำนวณจะคล้ายกับการคำนวณค่าความน่าจะเป็นหลังของบิตข้อมูล a_n ดังสมการต่อไปนี้ (ดูภาคผนวก ค ประกอบ)

$$\Pr\{p_n \mid \underline{R}_0^N, \underline{\widetilde{R}}_0^N\} = \sum_{(S_n, S_{n+1}):p_n} \Pr\{S_n, S_{n+1} \mid \underline{R}_0^N, \underline{\widetilde{R}}_0^N\}$$

$$= \frac{\sum_{(S_n, S_{n+1}):p_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1})}{\sum_{p_n}\sum_{(S_n, S_{n+1}):p_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1})} \quad (5.10)$$

เมื่อ $(S_n, S_{n+1}) : p_n$ หมายถึง เหตุการณ์ที่เครื่องเข้ารหัสย่อยเปลี่ยนสถานะจาก S_n ไปเป็น S_{n+1} แล้วได้บิตรหัส p_n ออกมาจากการเข้ารหัสที่เครื่องเข้ารหัสย่อยนั้น

ค่า $\alpha_n(S_n)$ $\beta_n(S_n)$ และ $\gamma_n(S_n, S_{n+1})$ คำนวณในลักษณะเดียวกับการคำนวณค่าความน่าจะเป็นหลังของบิตข้อมูล a_n ที่อธิบายไปแล้วในหัวข้อที่ผ่านมา

5.2.2 ข่าวสารเอ็กซ์ทรินซิก

ข่าวสารเอ็กซ์ทรินซิกของบิตข้อมูล a_n มีค่าเป็นไปตามสมการดังนี้ (รายละเอียดในการคำนวณอยู่ในภาคผนวก ค)

$$V_n(a_n) = \frac{\Pr\{a_n \mid \underline{R}_0^N, \underline{\widetilde{R}}_0^N\}}{\Pr\{a_n\}\left(\sum_{p_n'} \Gamma_n(a_n, p_n')\Pr\{p_n'\}\right)}$$

$$= \frac{\sum_{(S_n, S_{n+1}):a_n}\left(\sum_{a_n'} \tilde{\Gamma}_n(a_n', p_n)\Pr\{a_n'\}\right)\alpha_n(S_n)\beta_{n+1}(S_{n+1})}{\sum_{a_n}\sum_{(S_n, S_{n+1}):a_n}\left(\sum_{a_n'} \tilde{\Gamma}_n(a_n', p_n)\Pr\{a_n'\}\right)\alpha_n(S_n)\beta_{n+1}(S_{n+1})} \quad (5.11)$$

และข่าวสารเอ็กทรินซิกของบิตรหัส p_n คำนวณได้จากค่าความน่าจะเป็นหลังของบิตรหัส p_n ดังนี้ (ดูภาคผนวก ค ประกอบ)

$$V_n(p_n) = \frac{\Pr\{p_n \mid \underline{R}_0^N, \underline{\tilde{R}}_0^N\}}{\left(\sum_{a_n'} \tilde{\Gamma}_n(a_n', p_n)\Pr\{a_n'\}\right)}$$

$$= \frac{\sum_{(S_n, S_{n+1}):p_n} \Pr\{a_n\}\left(\sum_{p_n'} \Gamma_n(a_n, p_n')\Pr\{p_n'\}\right)\alpha_n(S_n)\beta_{n+1}(S_{n+1})}{\sum_{p_n}\sum_{(S_n, S_{n+1}):p_n} \Pr\{a_n\}\left(\sum_{p_n'} \Gamma_n(a_n, p_n')\Pr\{p_n'\}\right)\alpha_n(S_n)\beta_{n+1}(S_{n+1})} \quad (5.12)$$

เนื่องจากบิตข้อมูล a_n และบิตรหัส p_n ไม่ได้ถูกส่งมาในสัญลักษณ์ QPSK เดียวกัน เป็นผลให้สัญลักษณ์ I_n ประกอบไปด้วยข่าวสารจากคู่บิต (a_n, p_n') ซึ่งบิตข้อมูล a_n และบิตรหัส p_n' เป็นอิสระทางสถิติต่อกัน เพราะฉะนั้นข่าวสารเอ็กซ์ทรินซิกของสัญลักษณ์ I_n จึงสามารถคำนวณได้จากผลคูณของข่าวสารเอ็กซ์ทรินซิกของบิตข้อมูล a_n และข่าวสารเอ็กซ์ทรินซิกของบิตรหัส p_n' ดังต่อไปนี้

$$W_n(I_n) = W_n(a_n, p_n') = V_n(a_n) \cdot V_n(p_n') \quad (5.13)$$

$V_n(a_n)$ คำนวณได้จากสมการ (5.11) และ $V_n(p_n')$ ได้จากการนำค่า $V_n(p_n)$ ที่คำนวณได้จากสมการ (5.12) ไปสลับลำดับด้วยตัวสลับลำดับบิตรหัส

บทที่ 6

ผลการทดสอบ

บทนี้จะกล่าวถึงผลจากการจำลองระบบ เพื่อทดสอบสมรรถนะของระบบที่เสนอ เมื่อช่องสัญญาณเป็นแบบเรย์ลีเฟดดิงที่มีอัตราเร็วเฟดดิงต่าง ๆ กัน โดยจะพิจารณาทั้งในกรณีที่ภาครับมีการตรวจจับแบบร่วมนัยและการตรวจจับแบบไม่ร่วมนัย สำหรับกรณีการตรวจจับแบบไม่ร่วมนัยจะเปรียบเทียบสมรรถนะของระบบเมื่อภาครับใช้ตัวตรวจจับเชิงผลต่างแบบธรรมดา และตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ นอกจากนี้ยังทดสอบผลกระทบจากการเปลี่ยนค่าพารามิเตอร์ ได้แก่ จำนวนรอบในการถอดรหัสแบบวนซ้ำ ขนาดของบล็อกข้อมูล และผลของตัวสลับลำดับบิตรหัสประเภทต่าง ๆ ที่มีต่อสมรรถนะของระบบถอดรหัสที่เสนอ

6.1 การจำลองระบบ

สำหรับเงื่อนไขในการจำลองระบบ เครื่องเข้ารหัสเทอร์โบประกอบด้วยเครื่องเข้ารหัสย่อยแบบ RSC จำนวนสองตัว แต่ละตัวมีขนาดหน่วยความจำเท่ากับ 4 บิต ซึ่งมีพหุนามป้อนไปข้างหน้าเป็น $1+D^4$ และพหุนามป้อนกลับเป็น $1+D+D^2+D^3+D^4$ ดังรูปที่ 2.1 ขนาดของบล็อกข้อมูลที่ใช้ในการทดสอบหลักคือ 930 บิต และจำนวนบล็อกข้อมูลที่ใช้คือ 10000 บล็อก ตัวสลับลำดับการเข้ารหัสเป็นแบบ simile odd-even helical block ที่มีขนาด 31×30 บิต ส่วนตัวสลับลำดับช่องสัญญาณเป็นตัวสลับลำดับแบบบล็อกขนาด 41×23 บิต เครื่องถอดรหัสเทอร์โบประกอบด้วยเครื่องถอดรหัสย่อยจำนวนสองตัว ทำหน้าที่ถอดรหัสแบบวนซ้ำโดยใช้ขั้นตอนวิธีของ BCJR จำนวนรอบของการถอดรหัสแบบวนซ้ำคือ 5 รอบ (ดูรายละเอียดในหัวข้อ 6.3.1)

การจำลองช่องสัญญาณเป็นไปตามแบบจำลองของ Jakes ที่กล่าวไว้ในบทที่ 3 ช่องสัญญาณที่จำลองได้เป็นช่องสัญญาณที่เกิดเรย์ลีเฟดดิงที่มีสหสัมพันธ์กัน โดยจะพิจารณาที่อัตราการเปลี่ยนแปลงสถานะของเฟดดิงต่าง ๆ กัน ทั้งนี้อัตราการเปลี่ยนแปลงหรืออัตราเร็วเฟดดิงจะสัมพันธ์กับค่า B_dT ซึ่งเป็นค่าผลคูณระหว่างความถี่ดอปเปลอร์ และ คาบของสัญลักษณ์ที่ใช้ส่งข้อมูล ถ้า B_dT มีค่ามาก หมายความว่าสถานะของช่องสัญญาณมีการเปลี่ยนแปลงอย่างรวดเร็ว ในทางกลับกัน ถ้า B_dT มีค่าน้อย ก็แสดงว่าสถานะของช่องสัญญาณมีการเปลี่ยนแปลงอย่างช้า ๆ ซึ่งจะส่งผลให้เฟดดิงเกิดติดกันเป็นช่วงยาว การนิยามว่าเฟดดิงเป็นแบบเร็วหรือแบบช้านั้น ไม่มีคำจำกัดความที่แน่นอน แต่จากงานวิจัยอ้างอิง [7] และ [13] กำหนดให้เฟดดิงเป็นแบบเร็ว เมื่อ B_dT มีค่ามากกว่า 0.1

ในงานวิจัยนี้จะทดสอบสมรรถนะของระบบบนช่องสัญญาณแบบเรย์ลีเฟดดิง ทั้งที่มีการเปลี่ยนแปลงช้า เร็ว และเร็วมาก กล่าวคือ เมื่อ B_dT มีค่าเท่ากับ 0.01 0.125 และ 0.200 ที่ B_dT เท่ากับ 0.01 สถานะของช่องสัญญาณจะเปลี่ยนแปลงอย่างช้า ๆ ช่วงเวลาที่เฟดดิงเกิดติดกันมีค่าประมาณ 50 สัญลักษณ์ [20] ซึ่งถือว่าเป็นช่วงยาวเมื่อเทียบกับบล็อกข้อมูลขนาด 930 สัญลักษณ์ เมื่อ B_dT มีค่าเท่ากับ 0.125 เฟดดิงจะเกิดติดกันในช่วงประมาณ 4 สัญลักษณ์ เพราะฉะนั้นจึงกล่าวได้ว่าเฟดดิงมีการเปลี่ยนแปลงอย่างรวดเร็ว สำหรับกรณีที่ B_dT เท่ากับ 0.200 เฟดดิงจะมีความสัมพันธ์กันเพียงแค่ 2 ถึง 3 สัญลักษณ์เท่านั้น ดังนั้นในช่วงเวลาที่ส่งข้อมูลหนึ่งบล็อก เฟดดิงจะเปลี่ยนแปลงไปมาหลายครั้ง ซึ่งถือว่าเฟดดิงมีการเปลี่ยนแปลงรวดเร็วมาก

6.2 ผลการทดสอบสมรรถนะของระบบ

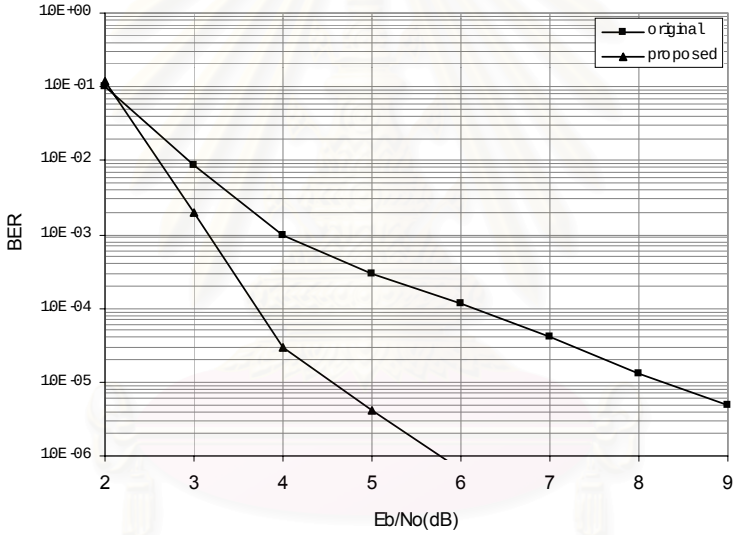
สมรรถนะของระบบที่เสนอจะถูกวัดอยู่ในรูปของอัตราความผิดพลาดของบิต (bit error rate : BER) ที่อัตราส่วนสัญญาณต่อสัญญาณรบกวน (signal-to-noise ratio : SNR หรือ Eb/No) ค่าต่าง ๆ โดยจะเปรียบเทียบกับสมรรถนะของระบบเดิมที่ไม่มีการแยกบิตข้อมูลกับบิตรหัสออกจากกัน [13] ทั้งนี้จะเริ่มพิจารณาในกรณีการตรวจจับแบบร่วมนัยก่อน เพื่อวิเคราะห์สมรรถนะของระบบถอดรหัสเมื่อไม่คำนึงถึงผลจากการประมาณเฟดดิง และเพื่อนำผลที่ได้ไปเปรียบเทียบกับกรณีการตรวจจับแบบไม่ร่วมนัย ซึ่งอาศัยตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ในการประมาณช่องสัญญาณ ร่วมกับการถอดรหัสเทอร์โบ

6.2.1 สมรรถนะของระบบถอดรหัสสำหรับกรณีการตรวจจับแบบร่วมนัย

การตรวจจับแบบร่วมนัยมีสมมติฐานว่า ทางภาครับสามารถทราบกระบวนการของเฟดดิงอย่างถูกต้องซึ่งหมายความว่าภาครับไม่จำเป็นต้องประมาณข่าวสารจากช่องสัญญาณแต่อย่างใด การทดสอบสมรรถนะของระบบสำหรับกรณีการตรวจจับแบบร่วมนัย จึงเป็นการทดสอบสมรรถนะของขั้นตอนวิธีการเข้ารหัสและถอดรหัส โดยไม่คำนึงถึงผลของการประมาณเฟดดิง ทั้งนี้การทดสอบสมรรถนะของระบบในกรณีนี้ ก็เพื่อเป็นแนวทางสำหรับการวิเคราะห์สมรรถนะของระบบสำหรับกรณีการตรวจจับแบบไม่ร่วมนัยต่อไป นอกจากนี้สมรรถนะของระบบในกรณีการตรวจจับแบบร่วมนัยยังถูกใช้เพื่อเปรียบเทียบกับสมรรถนะในกรณีการตรวจจับแบบไม่ร่วมนัย โดยถือว่าเป็นกรณีที่ดีที่สุดที่สามารถเกิดขึ้นได้

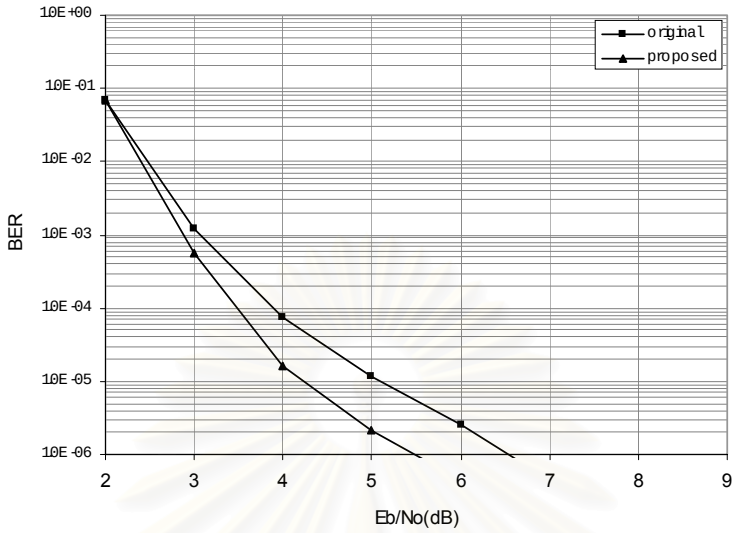
การทดสอบสมรรถนะของระบบที่เสนอ บนช่องสัญญาณที่เกิดเรย์ลีเฟดดิงที่มีสหสัมพันธ์กัน จะพิจารณาเมื่ออัตราเร็วเฟดดิงต่างกัน 3 กรณีคือ 1) เฟดดิงแบบช้า ที่ B_dT เท่ากับ 0.01 2) เฟดดิงแบบเร็ว ที่ B_dT เท่ากับ 0.125 และ 3) เฟดดิงแบบเร็วมาก ที่ B_dT เท่ากับ 0.200 โดยจะเปรียบเทียบกับสมรรถนะของระบบเดิมที่ไม่มีการแยกบิตข้อมูลกับบิตรหัสออกจากกัน

สมรรถนะของระบบถอดรหัสสำหรับกรณีการตรวจจับแบบร่วมนัย เมื่อ B_dT เท่ากับ 0.01 0.125 และ 0.200 แสดงอยู่ในรูปที่ 6.1 ถึง 6.3 สำหรับกรณีเฟดดิงแบบช้าที่ B_dT เท่ากับ 0.01 ระบบที่เสนอมีสมรรถนะดีกว่าระบบเดิมมาก ดังรูปที่ 6.1 เมื่อพิจารณาที่ระดับ BER เท่ากับ 10^{-5} จะพบว่า ระบบที่เสนอต้องการ Eb/No ต่ำกว่าระบบเดิมถึง 3.7 dB ผลที่ได้แสดงให้เห็นว่าการเสนอให้แยกส่งบิตข้อมูลกับบิตรหัสไปในสัญลักษณ์ QPSK ต่างสัญลักษณ์กัน ช่วยทำให้กระบวนการถอดรหัสแบบวนซ้ำมีประสิทธิภาพดีขึ้น

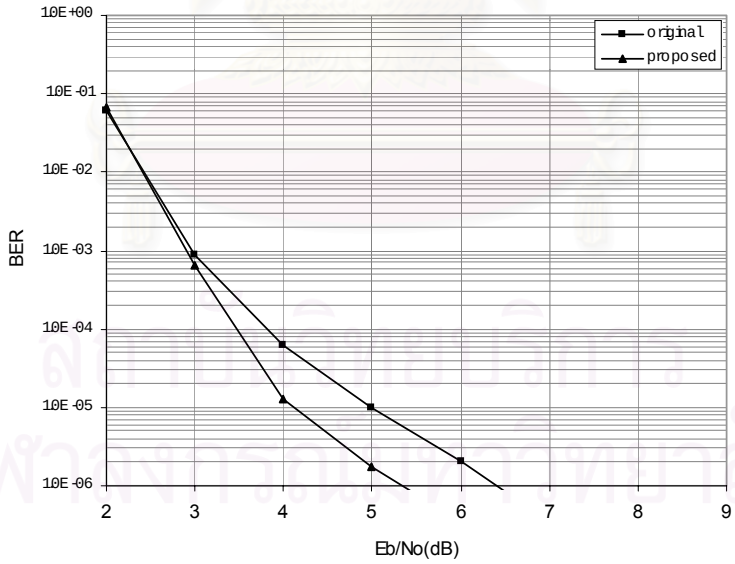


รูปที่ 6.1 สมรรถนะของระบบถอดรหัส (สำหรับกรณีการตรวจจับแบบร่วมนัย) เมื่อ B_dT เท่ากับ 0.01

เมื่ออัตราเร็วเฟดดิงมีค่าเพิ่มขึ้นเป็น 0.125 และ 0.200 เฟดดิงจะมีการเปลี่ยนแปลงอย่างรวดเร็ว ในกรณีนี้พบว่าสมรรถนะของระบบที่เสนอก็ยังคงดีกว่าสมรรถนะของระบบเดิม ดังรูปที่ 6.2 และ 6.3 จากรูปจะเห็นว่าที่ระดับ BER เท่ากับ 10^{-5} ระบบที่เสนอต้องการ Eb/No ต่ำกว่าระบบเดิมอยู่ประมาณ 0.8 dB ทั้งที่ B_dT เท่ากับ 0.125 และ 0.200 ผลที่ได้เป็นการยืนยันว่าระบบที่เสนอช่วยให้การถอดรหัสแบบวนซ้ำมีประสิทธิภาพดีขึ้น ทั้งในกรณีเฟดดิงแบบช้า และเฟดดิงแบบเร็ว



รูปที่ 6.2 สมรรถนะของระบบถอดรหัส (สำหรับกรณีการตรวจจับแบบร่วมนัย)
เมื่อ B_dT เท่ากับ 0.125



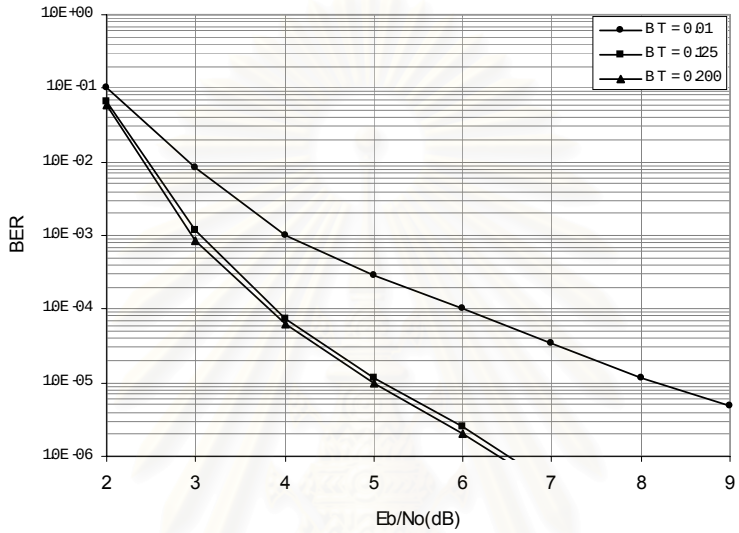
รูปที่ 6.3 สมรรถนะของระบบถอดรหัส (สำหรับกรณีการตรวจจับแบบร่วมนัย)
เมื่อ B_dT เท่ากับ 0.200

เมื่อพิจารณาสมรรถนะของระบบถอดรหัสแบบเดิมที่อัตราเร็วเฟดดิงต่าง ๆ กัน สำหรับกรณีการตรวจจับแบบร่วมนัย ดังรูปที่ 6.4 พบว่า สมรรถนะของระบบที่ B_dT เท่ากับ 0.01 ด้อยกว่าสมรรถนะของระบบที่ B_dT เท่ากับ 0.125 และ 0.200 มาก ในขณะที่สมรรถนะของระบบที่ B_dT เท่ากับ 0.125 และ 0.200 กลับไม่แตกต่างกันมากนัก สาเหตุที่เป็นเช่นนี้เนื่องจากเฟดดิงที่อัตราเร็วต่ำ จะมีการเปลี่ยนแปลงช้า ทำให้ผลกระทบของเฟดดิงที่มีต่อสัญลักษณ์ที่ถูกส่ง เกิดติดกันหลายสัญลักษณ์ ซึ่งจะส่งผลเสียหายเป็นอย่างมากกับกระบวนการถอดรหัสเทอร์โบ แต่เมื่อเฟดดิงมีอัตราเร็วเพิ่มขึ้น ช่วงเวลาที่เฟดดิงเกิดติดกันก็จะลดลง และความเป็นไปได้ที่สัญลักษณ์ที่ถูกส่งจะเสียหายไปพร้อมกันทั้งบล็อกก็ลดลงตามไปด้วย กระบวนการถอดรหัสเทอร์โบจึงสามารถทำงานได้อย่างมีประสิทธิภาพ จากผลการทดสอบนี้เห็นได้ชัดว่า เฟดดิงที่ติดกันเป็นช่วงยาวสร้างความเสียหายให้กับข้อมูลที่ถูกส่ง และกระบวนการถอดรหัสเทอร์โบมากกว่าเฟดดิงที่ติดกันเป็นช่วงสั้น ๆ อย่างไรก็ตาม หากพิจารณาสมรรถนะของระบบถอดรหัสที่เสนอที่อัตราเร็วเฟดดิงต่าง ๆ กันในรูปที่ 6.5 จะเห็นว่า สมรรถนะของระบบที่ B_dT เท่ากับ 0.01 ด้อยกว่าสมรรถนะของระบบที่ B_dT เท่ากับ 0.125 และ 0.200 ไม่มากนัก ซึ่งหมายความว่าระบบที่เสนอสามารถทำงานได้อย่างมีประสิทธิภาพทั้งในกรณีเฟดดิงแบบเร็ว และเฟดดิงแบบช้าที่ความเสียหายจากเฟดดิงเกิดติดกันเป็นช่วงยาว

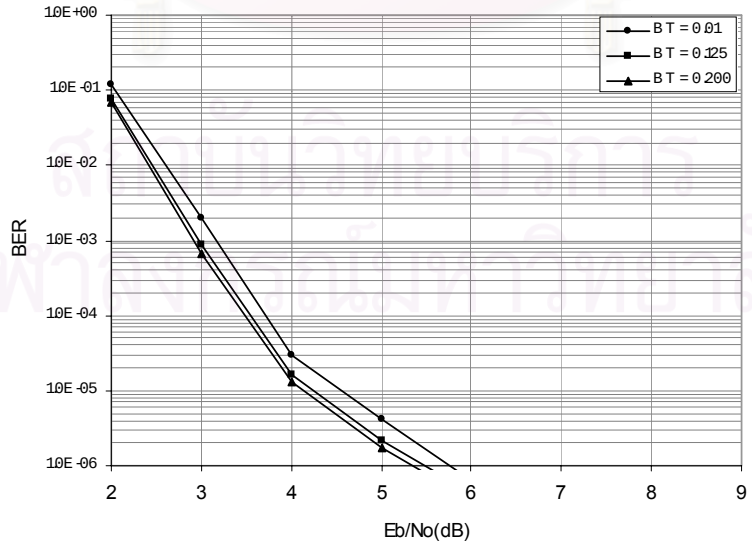
จากผลการทดสอบระบบกรณีการตรวจจับแบบร่วมนัย ซึ่งไม่คำนึงถึงผลจากการประมาณช่องสัญญาณของภาครับ เนื่องจากมีสมมติฐานว่าภาครับทราบกระบวนการเฟดดิงอย่างสมบูรณ์ สรุปได้ว่า สมรรถนะของระบบที่เสนอดีกว่าสมรรถนะของระบบเดิม ทั้งในกรณีที่ B_dT เท่ากับ 0.01 0.125 และ 0.200 โดยเฉพาะอย่างยิ่งที่ B_dT เท่ากับ 0.01 เฟดดิงจะเกิดติดกันเป็นช่วงยาว เป็นผลให้สมรรถนะของระบบเดิมด้อยลงอย่างมาก เนื่องจากเฟดดิงที่ติดกันเป็นช่วงยาว ทำให้ความเสียหายที่เกิดขึ้นมีลักษณะเป็นเบริสต์ ซึ่งจะส่งผลให้เครื่องถอดรหัสเทอร์โบไม่สามารถตัดสินบิตได้ถูกต้อง เมื่อพิจารณาระบบที่เสนอพบว่า สมรรถนะของระบบที่ B_dT เท่ากับ 0.01 ยังคงมีค่าใกล้เคียงกับสมรรถนะของระบบที่ B_dT เท่ากับ 0.125 และ 0.200 ซึ่งแสดงให้เห็นว่า การแยกส่งบิตข้อมูลกับบิตรหัสออกจากกันช่วยเสริมการทำงานของกระบวนการถอดรหัสเทอร์โบ และทำให้ระบบถอดรหัสมีประสิทธิภาพดีขึ้น

<u>หมายเหตุ</u> สำหรับกรณีการตรวจจับแบบร่วมนัย เป็นที่สังเกตว่า สมรรถนะของระบบที่เฟดดิงแบบเร็วดีกว่าที่เฟดดิงแบบช้า ทั้งนี้เนื่องจากการทดสอบในกรณีการตรวจจับแบบร่วมนัย จะกำหนดให้ภาครับรู้กระบวนการเฟดดิงอย่างถูกต้องเพราะฉะนั้นจึงถือว่าภาครับมีการประมาณช่องสัญญาณแบบสมบูรณ์ (perfect channel estimation) ในกรณีนี้เฟดดิงแบบช้าจะส่งผลกระทบต่อระบบมากกว่าเฟดดิงแบบเร็ว แต่ถ้าพิจารณากรณีการตรวจจับแบบไม่ร่วมนัย (จะกล่าวถึงในหัวข้อต่อ

ไป) ทางภาครับต้องมีการประมาณเฟดดิงที่เกิดขึ้นบนช่องสัญญาณ ทำให้เฟดดิงแบบเร็วส่งผลกระทบต่อระบบมากกว่าเฟดดิงแบบช้า เนื่องจากการประมาณช่องสัญญาณเมื่อเฟดดิงมีการเปลี่ยนแปลงอย่างรวดเร็วกระทำได้ยากกว่าเมื่อเฟดดิงเปลี่ยนแปลงอย่างช้า ๆ เพราะฉะนั้นในกรณีการตรวจจับแบบไม่ร่วมนัย สมรรถนะของระบบที่เฟดดิงแบบเร็วจึงด้อยกว่าที่เฟดดิงแบบช้า



รูปที่ 6.4 การเปรียบเทียบสมรรถนะของระบบถอดรหัสแบบเดิม (กรณีการตรวจจับแบบร่วมนัย) เมื่อ B_dT เท่ากับ 0.01 0.125 และ 0.200



รูปที่ 6.5 การเปรียบเทียบสมรรถนะของระบบถอดรหัสที่เสนอ (กรณีการตรวจจับแบบร่วมนัย) เมื่อ B_dT เท่ากับ 0.01 0.125 และ 0.200

6.2.2 **สมรรถนะของระบบถอดรหัสสำหรับกรณีการตรวจจับแบบไม่ร่วมนัย**

ถึงแม้สมรรถนะของระบบที่เสนอจะดีกว่าสมรรถนะของระบบเดิม เมื่อพิจารณาในกรณีการตรวจจับแบบร่วมนัย แต่อย่างไรก็ตามการทดสอบในกรณีการตรวจจับแบบร่วมนัยเป็นเพียงแค่การทดสอบเพื่อดูแนวโน้มของประสิทธิภาพของระบบเท่านั้น ในหัวข้อนี้จะเป็นการทดสอบสมรรถนะของระบบสำหรับกรณีการตรวจจับแบบไม่ร่วมนัย ซึ่งจะคำนึงถึงผลจากการประมาณช่องสัญญาณของภาครับร่วมด้วย การทดสอบสมรรถนะของระบบในกรณีนี้จึงเป็นการทดสอบประสิทธิภาพในการทำงานร่วมกันระหว่างตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ ที่ทำหน้าที่ประมาณข่าวสารจากช่องสัญญาณ และการถอดรหัสแบบวนซ้ำ

การทดสอบสมรรถนะของระบบถอดรหัสจะพิจารณาทั้งในกรณีที่ใช้ตัวตรวจจับเชิงผลต่างแบบธรรมดา (differential detector : DD) และกรณีที่ใช้ตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ (multiple symbol differential detecter : MSDD) เมื่อจำนวนสัญลักษณ์ (Z) มีค่าเป็น 2 3 และ 4 สัญลักษณ์ ทั้งนี้เพื่อจะวิเคราะห์ว่าจำนวนสัญลักษณ์ที่เพิ่มขึ้นช่วยปรับปรุงสมรรถนะของระบบถอดรหัสให้ดีขึ้นหรือไม่ อย่างไร นอกจากนี้ยังได้เปรียบเทียบกับกรณีที่ใช้การตรวจจับแบบร่วมนัย (coherent) เพื่อจะวัดค่าแตกต่างระหว่างการตรวจจับแบบร่วมนัย และการตรวจจับแบบไม่ร่วมนัย ที่เรียกว่า ข้อด้อยของการตรวจจับแบบไม่ร่วมนัย (noncoherence penalty)

การวิเคราะห์สมรรถนะของระบบถอดรหัสจะแยกพิจารณาเมื่ออัตราเร็วเฟดดิงต่างกัน 3 กรณี คือ ก) เฟดดิงแบบช้า เมื่อ B_dT เท่ากับ 0.01 ข) เฟดดิงแบบเร็ว เมื่อ B_dT เท่ากับ 0.125 และ ค) เฟดดิงแบบเร็วมาก เมื่อ B_dT เท่ากับ 0.200

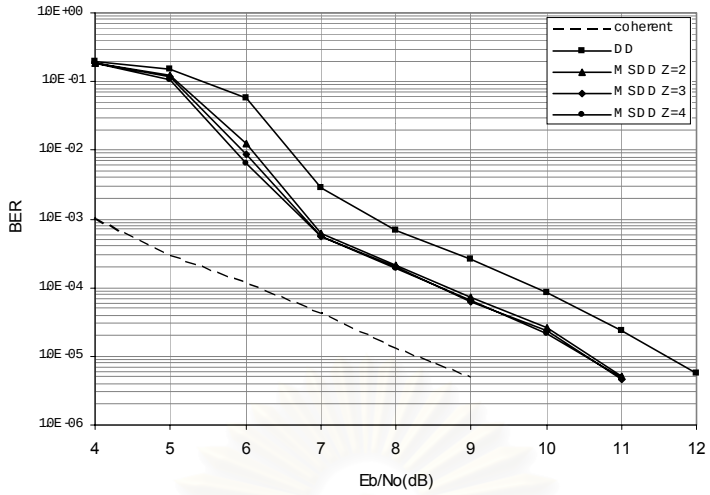
. *กรณีที่ B_dT เท่ากับ 0.01*

สมรรถนะของระบบถอดรหัสเปรียบเทียบในกรณีที่ใช้การตรวจจับแบบต่าง ๆ ที่ B_dT มีค่าเท่ากับ 0.01 แสดงอยู่ในรูปที่ 6.6 และ 6.7 รูปที่ 6.6 เป็นสมรรถนะของระบบถอดรหัสแบบเดิม ส่วนรูปที่ 6.7 เป็นสมรรถนะของระบบถอดรหัสที่เสนอ พิจารณารูปที่ 6.6 จะพบว่าระบบถอดรหัสในกรณี MSDD มีสมรรถนะดีกว่ากรณี DD ซึ่งแสดงให้เห็นว่า MSDD สามารถปรับปรุงสมรรถนะของระบบที่ใช้ DD หรือตัวตรวจจับเชิงผลต่างแบบธรรมดาได้ ทั้งนี้เป็นเพราะ DD ใช้สัญลักษณ์ที่รับได้ที่เวลาก่อนหน้าเพียงหนึ่งสัญลักษณ์ในการประมาณเฟดดิง ทำให้ข่าวสารของช่องสัญญาณที่ประมาณได้ไม่ถูกต้องนัก ในขณะที่ MSDD ใช้ประโยชน์จากสัญลักษณ์ที่รับได้ก่อนหน้าจำนวนมากกว่าหนึ่งสัญลักษณ์ จึงประมาณเฟดดิงได้แม่นยำกว่า DD เป็นผลให้สมรรถนะของระบบถอด

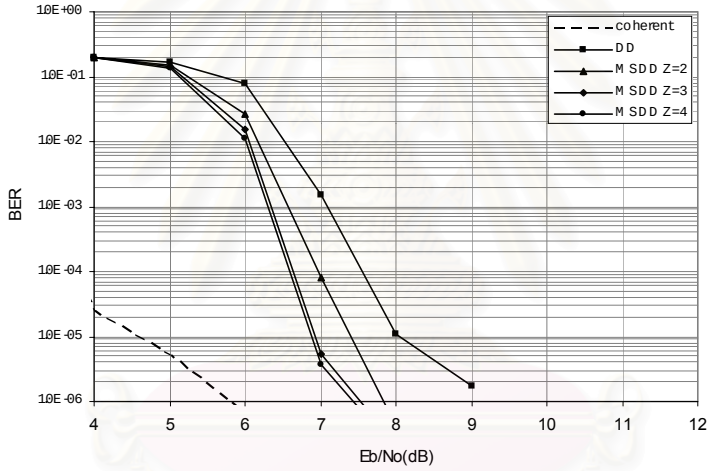
รหัสดีขึ้น อย่างไรก็ตาม การเพิ่มจำนวนสัญลักษณ์ที่สังเกตการณ์ของ MSDD จาก Z=2 เป็น Z=3 และ Z=4 สำหรับระบบถอดรหัสแบบเดิมในรูปที่ 6.6 ไม่ได้ช่วยให้สมรรถนะของระบบ ดีขึ้นเลย แต่เมื่อพิจารณาระบบถอดรหัสที่เสนอในรูปที่ 6.7 จะเห็นว่าสมรรถนะของระบบดีขึ้น เมื่อจำนวนสัญลักษณ์ Z เพิ่มขึ้น ที่ BER เท่ากับ 10^{-5} สมรรถนะของระบบดีขึ้น 0.6 dB เมื่อ Z เพิ่มจาก 2 เป็น 3 สัญลักษณ์ ที่เป็นเช่นนี้เนื่องจากการเพิ่มจำนวนสัญลักษณ์ที่สังเกตการณ์ของ MSDD ทำให้การติดตามเฟดดิงของภาครับดีขึ้น ถึงแม้ว่า MSDD ที่ Z=3 จะปรับปรุงสมรรถนะของระบบให้ดีขึ้นได้ แต่เมื่อเพิ่มจำนวนสัญลักษณ์ขึ้นอีกเป็น Z=4 สมรรถนะของระบบก็ไม่ดีขึ้นแต่อย่างใด นอกจากนี้ระบบถอดรหัสยังมีสมรรถนะด้อยกว่าสมรรถนะของระบบกรณีการตรวจจับแบบร่วมนัยอยู่ถึง 2.2 dB ทั้งนี้เกิดจากข้อจำกัดของการตรวจจับแบบไม่ร่วมนัยเมื่อเทียบกับการตรวจจับแบบร่วมนัยซึ่งมีสมมติฐานว่าภาครับทราบกระบวนการเฟดดิงอย่างถูกต้อง

การเปรียบเทียบสมรรถนะของระบบถอดรหัสแบบเดิมกับระบบถอดรหัสที่เสนอ จะแสดงอยู่ในรูปของอัตราส่วน BER ของระบบถอดรหัสแบบเดิม ต่อ BER ของระบบถอดรหัสที่เสนอ ที่ Eb/No ค่าต่าง ๆ ถ้าอัตราส่วนดังกล่าวมีค่าน้อยกว่าหนึ่ง แสดงว่าระบบถอดรหัสแบบเดิมมี BER ต่ำกว่าระบบถอดรหัสที่เสนอ ซึ่งก็หมายความว่าระบบถอดรหัสแบบเดิมมีสมรรถนะดีกว่าระบบถอดรหัสที่เสนอ ในทางกลับกันถ้าอัตราส่วนมีค่ามากกว่าหนึ่ง แสดงว่าระบบถอดรหัสที่เสนอมีสมรรถนะดีกว่าระบบถอดรหัสแบบเดิม

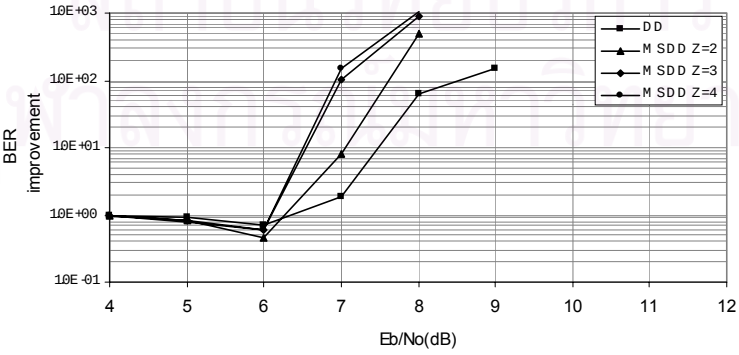
รูปที่ 6.8 เป็นการเปรียบเทียบสมรรถนะของระบบถอดรหัสแบบเดิมกับระบบถอดรหัสที่เสนอ สำหรับกรณีที่ใช้การตรวจจับแบบต่าง ๆ เมื่อ B_dT มีค่าเท่ากับ 0.01 จากรูปจะเห็นว่าเมื่อ Eb/No มากกว่า 6.2 dB ระบบถอดรหัสที่เสนอมีสมรรถนะดีกว่าระบบถอดรหัสแบบเดิม ทั้งในกรณีที่ใช้ตัวตรวจจับเชิงผลต่างแบบธรรมดาและตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ นอกจากนี้ถ้าตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ เพิ่มจำนวนสัญลักษณ์ที่สังเกตการณ์จาก 2 สัญลักษณ์ เป็น 3 และ 4 สัญลักษณ์ ระบบถอดรหัสที่เสนอจะสามารถปรับปรุงสมรรถนะของระบบถอดรหัสแบบเดิมได้มากขึ้นตามลำดับ พิจารณาที่ Eb/No เท่ากับ 8 dB จะเห็นว่าสมรรถนะของระบบถอดรหัสที่เสนอสำหรับกรณี MSDD ที่ Z=4 ดีกว่าสมรรถนะของระบบถอดรหัสแบบเดิมถึง 10^3 เท่า หรือ 3 ระดับขนาด (order of magnitude)



รูปที่ 6.6 การเปรียบเทียบสมรรถนะของระบบถอดรหัสแบบเดิม สำหรับกรณีที่ใช้การตรวจจับแบบต่าง ๆ เมื่อ B_dT เท่ากับ 0.01



รูปที่ 6.7 การเปรียบเทียบสมรรถนะของระบบถอดรหัสที่เสนอ สำหรับกรณีที่ใช้การตรวจจับแบบต่าง ๆ เมื่อ B_dT เท่ากับ 0.01

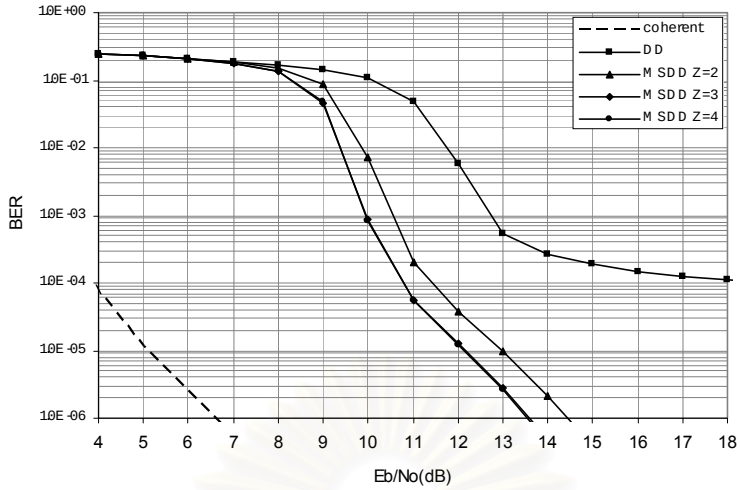


รูปที่ 6.8 อัตราส่วน BER ของระบบถอดรหัสแบบเดิมต่อ BER ของระบบถอดรหัสที่เสนอ สำหรับกรณีที่ใช้การตรวจจับแบบต่าง ๆ เมื่อ B_dT เท่ากับ 0.01

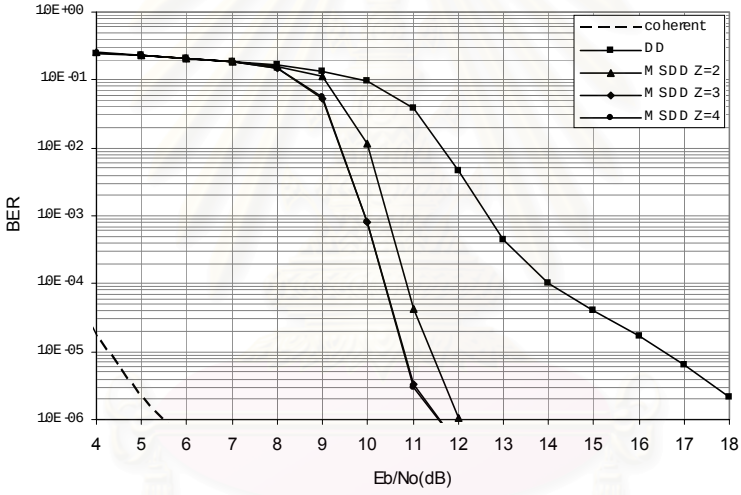
. *กรณีที่ B_dT เท่ากับ 0.125*

เมื่อเฟดดิงมีการเปลี่ยนแปลงเร็วขึ้น ที่ B_dT เท่ากับ 0.125 ระบบถอดรหัสแบบเดิมและแบบที่เสนอให้ผลการทดสอบออกมาในลักษณะเดียวกัน ดังรูปที่ 6.9 และ 6.10 เมื่อพิจารณาสมรรถนะของระบบในกรณี MSDD ที่ Z = 2 เปรียบเทียบกับกรณี DD จะเห็นว่า MSDD มีสมรรถนะดีกว่า DD อย่างเห็นได้ชัด และเมื่อเปรียบเทียบกับสมรรถนะที่ B_dT เท่ากับ 0.01 พบว่าเมื่อเฟดดิงมีอัตราเร็วสูงขึ้น ความแตกต่างของสมรรถนะระหว่าง MSDD กับ DD ก็มากขึ้นด้วย จากรูปที่ 6.7 เมื่อ B_dT เท่ากับ 0.01 พิจารณาที่ระดับ BER เท่ากับ 10^{-5} จะเห็นว่าสมรรถนะของระบบถอดรหัสกรณี MSDD ที่ Z = 2 ดีกว่ากรณี DD อยู่ 0.6 dB ในขณะที่ B_dT เพิ่มขึ้นเป็น 0.125 ในรูปที่ 6.10 พบว่า ที่ระดับ BER เท่ากับ 10^{-5} สมรรถนะของระบบกรณี MSDD ดีกว่ากรณี DD ถึง 5 dB ผลที่ได้ชี้ให้เห็นว่า การนำ MSDD มาใช้แทน DD เมื่อเฟดดิงมีการเปลี่ยนแปลงอย่างรวดเร็วช่วยเพิ่มสมรรถนะของระบบถอดรหัสให้ดีขึ้น เนื่องจาก MSDD ทำให้ภาครับสามารถประมาณช่องสัญญาณได้แม่นกว่า DD นอกจากนี้ MSDD ยังช่วยลดค่าพื้นของความผิดพลาดที่เกิดขึ้นกับกรณี DD ได้อีกด้วย อย่างไรก็ตาม การเพิ่มจำนวนสัญลักษณ์ Z ของ MSDD ขึ้นไปเป็น 4 สัญลักษณ์ ก็ไม่ทำให้สมรรถนะของระบบถอดรหัสดีขึ้นกว่ากรณี Z เท่ากับ 3 สัญลักษณ์ ยิ่งไปกว่านั้น ผลที่ได้ยังด้อยกว่ากรณีการตรวจจับแบบร่วมนัยอยู่ถึง 6.5 dB สาเหตุที่ข้อด้อยของการตรวจจับแบบไม่ร่วมนัยที่ B_dT เท่ากับ 0.125 สูงกว่าที่ B_dT เท่ากับ 0.01 เนื่องจากการติดตามการเปลี่ยนแปลงของเฟดดิงจะยากขึ้นเมื่อเฟดดิงมีอัตราเร็วสูงขึ้น

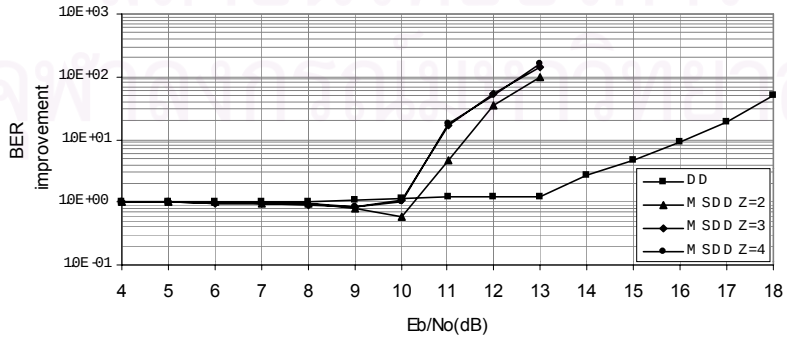
ถ้าพิจารณาสมรรถนะของระบบถอดรหัสแบบเดิม กรณี DD ในรูปที่ 6.9 จะสังเกตเห็นว่าเมื่อเฟดดิงมีอัตราเร็วเพิ่มขึ้น ระบบถอดรหัสแบบเดิมเริ่มเกิดค่าพื้นของความผิดพลาดขึ้น ในขณะที่ BER ของระบบถอดรหัสที่เสนอ มีค่าลดลง เมื่อ Eb/No เพิ่มขึ้น ความแตกต่างนี้จะเห็นได้อย่างชัดเจน เมื่อพิจารณาอัตราส่วน BER ของระบบถอดรหัสแบบเดิม ต่อ BER ของระบบถอดรหัสที่เสนอ ดังแสดงในรูปที่ 6.11 สำหรับกรณี MSDD ที่ Z = 2 3 และ 4 สัญลักษณ์ ระบบถอดรหัสที่เสนอก็มีสมรรถนะดีกว่าระบบถอดรหัสแบบเดิมเช่นเดียวกัน



รูปที่ 6.9 การเปรียบเทียบสมรรถนะของระบบถอดรหัสแบบเดิม สำหรับกรณีที่ใช้การตรวจจับแบบต่าง ๆ เมื่อ B_dT เท่ากับ 0.125



รูปที่ 6.10 การเปรียบเทียบสมรรถนะของระบบถอดรหัสที่เสนอ สำหรับกรณีที่ใช้การตรวจจับแบบต่าง ๆ เมื่อ B_dT เท่ากับ 0.125



รูปที่ 6.11 อัตราส่วน BER ของระบบถอดรหัสแบบเดิมต่อ BER ของระบบถอดรหัสที่เสนอ สำหรับกรณีที่ใช้การตรวจจับแบบต่าง ๆ เมื่อ B_dT เท่ากับ 0.125

. *กรณีที่* B_dT *เท่ากับ 0.200*

การเปรียบเทียบสมรรถนะของระบบถอดรหัสสำหรับกรณีที่ใช้การตรวจจับแบบต่าง ๆ จะเห็นได้ชัดเจนยิ่งขึ้นเมื่อเฟดดิงมีอัตราเร็วสูงขึ้น รูปที่ 6.12 และ 6.13 เป็นสมรรถนะของระบบถอดรหัสแบบเดิมและระบบถอดรหัสแบบที่เสนอเมื่อ B_dT เท่ากับ 0.200 ตามลำดับ จากรูปจะเห็นว่า DD มีสมรรถนะด้อยลงอย่างมาก เนื่องจาก DD ไม่สามารถตรวจจับการเปลี่ยนแปลงของ เฟดดิงได้เลย ในขณะที่ MSDD ที่ Z = 2 สามารถติดตามเฟดดิงซึ่งเปลี่ยนแปลงอย่างรวดเร็วได้ และเมื่อเพิ่มจำนวนสัญลักษณ์จาก Z = 2 เป็น Z = 3 สมรรถนะของระบบจะดีขึ้นอย่างเห็นได้ชัด ความแตกต่างของสมรรถนะระหว่าง Z = 2 และ Z = 3 เมื่อ B_dT เท่ากับ 0.200 มีค่ามากกว่าในกรณีที่ B_dT เท่ากับ 0.125 และ 0.01 นอกจากนี้ถ้าเพิ่มจำนวนสัญลักษณ์เป็น Z = 4 สมรรถนะของระบบก็จะดีขึ้นอีก ในขณะที่สมรรถนะของระบบถอดรหัสที่ Z = 3 และ Z = 4 เมื่อ B_dT เท่ากับ 0.125 และ 0.01 มีค่าไม่แตกต่างกัน ผลการทดสอบนี้ชี้ให้เห็นว่า การเพิ่มจำนวนสัญลักษณ์ของตัวตรวจจับเชิงผลต่างมีนัยสำคัญมากขึ้น เมื่ออัตราเร็วเฟดดิงสูงขึ้น แต่กระนั้นก็ตาม ความแตกต่างของสมรรถนะระหว่าง MSDD ที่ Z = 4 กับกรณีการตรวจจับแบบร่วมนัย ในรูปที่ 6.13 มีค่าสูงถึง 12 dB เมื่อพิจารณาที่ระดับ BER เท่ากับ 10^{-5} ความแตกต่างนี้เป็นผลมาจากการเปลี่ยนแปลงที่รวดเร็วของเฟดดิง ทำให้การประมาณเฟดดิงที่ถูกต้องกระทำได้ยาก

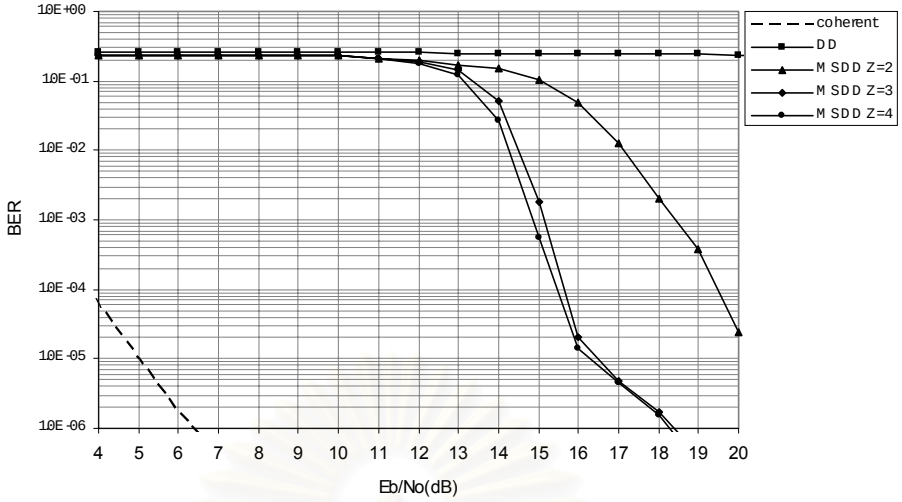
เนื่องจาก DD ทำงานได้ดีเฉพาะกรณีที่เฟดดิงเปลี่ยนแปลงอย่างช้า ๆ เท่านั้น เมื่อ B_dT เพิ่มขึ้นเป็น 0.200 DD จะไม่สามารถตรวจจับการเปลี่ยนแปลงของเฟดดิงได้อีกต่อไป เป็นผลให้ระบบถอดรหัสทั้งแบบเดิมและแบบที่เสนอมีสมรรถนะด้อยลงอย่างมาก ดังนั้นจึงไม่สามารถนำผลมาเปรียบเทียบกันได้ แต่เมื่อพิจารณากรณี MSDD ที่ Z = 2 จะพบว่าสมรรถนะของระบบถอดรหัสที่เสนอด้อยกว่าสมรรถนะของระบบถอดรหัสแบบเดิม ดังแสดงในรูปที่ 6.14 ผลการทดสอบที่ Z = 2 นี้ แตกต่างจากกรณีที่ B_dT เท่ากับ 0.01 และ 0.125 ที่เป็นเช่นนี้เนื่องจากเมื่อเฟดดิงมีการเปลี่ยนแปลงอย่างรวดเร็ว กระบวนการถอดรหัสเทอร์โบจะทำงานได้อย่างมีประสิทธิภาพหรือไม่ก็ขึ้นอยู่กับการประมาณข่าวสารจากช่องสัญญาณของภาครับเป็นส่วนสำคัญ ถ้าพิจารณาขั้นตอนการคำนวณค่าความน่าจะเป็นหลังของเครื่องถอดรหัสย่อย จะพบว่าการคำนวณฟังก์ชันเมตริกสาขาของระบบถอดรหัสที่เสนอ ต้องอาศัยข่าวสารจากช่องสัญญาณที่ถูกส่งมาจากหน่วยคำนวณเมตริกทุติยภูมิถึงสองเมตริก คือ เมตริกช่องสัญญาณที่มีข่าวสารของบิตข้อมูล และ เมตริกช่องสัญญาณที่มีข่าวสารของบิตรหัส ในกรณีนี้ถ้าข่าวสารจากเมตริกใดเมตริกหนึ่งมีความไม่แน่นอนจะส่งผลให้ฟังก์ชันเมตริกสาขาที่คำนวณได้มีค่าความน่าเชื่อถือต่ำ และการตัดสินบิตเกิดความผิดพลาดสูง ในขณะที่ฟังก์ชันเมตริกสาขาของระบบถอดรหัสแบบเดิม ที่ไม่มีการแยกบิตข้อมูลกับบิตรหัสออกจากกัน สามารถคำนวณได้จากเมตริกช่องสัญญาณที่ประกอบด้วยบิตข้อมูลและบิตรหัส

พร้อมกันทั้งสองบิตได้โดยตรง ทำให้ฟังก์ชันเมตริกสาขามีค่าความน่าเชื่อถือสูงกว่าการส่งบิตข้อมูลกับบิตรหัสไปในสัญลักษณ์ QPSK ต่างสัญลักษณ์กัน เพราะฉะนั้นในกรณีที่ เฟดดิงเปลี่ยนแปลงอย่างรวดเร็ว และการประมาณข่าวสารจากช่องสัญญาณไม่แม่นยำเพียงพอ สมรรถนะของระบบถอดรหัสที่เสนอจะด้อยกว่าสมรรถนะของระบบถอดรหัสแบบเดิม

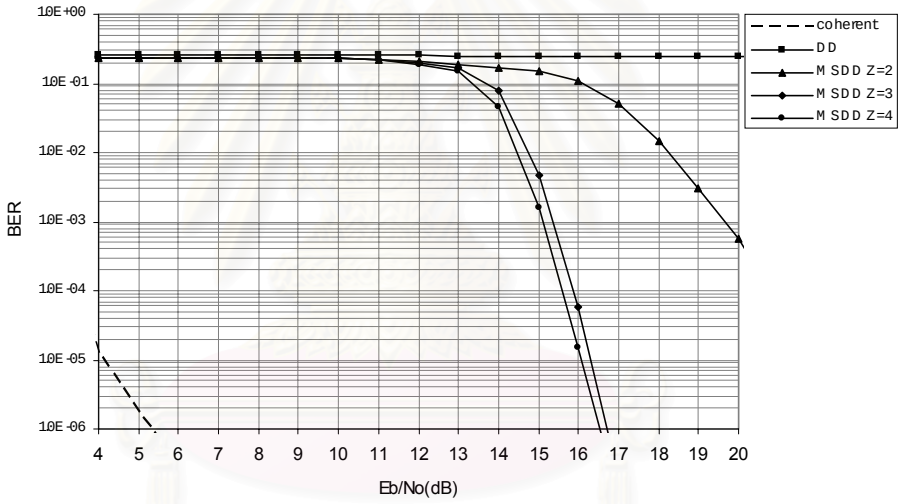
อย่างไรก็ตาม เมื่อตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ เพิ่มจำนวนสัญลักษณ์ที่สังเกตการณ์เป็น 3 และ 4 สัญลักษณ์ การประมาณช่องสัญญาณก็จะแม่นยำมากยิ่งขึ้น ส่งผลให้สมรรถนะของระบบถอดรหัสที่เสนอดีกว่าสมรรถนะของระบบถอดรหัสแบบเดิม ซึ่งนั่นหมายความว่า ในกรณีที่เฟดดิงเปลี่ยนแปลงอย่างรวดเร็ว สมรรถนะของระบบที่เสนอสามารถถูกปรับปรุงให้ดีขึ้นได้ ถ้าภาครับมีการประมาณเฟดดิงที่แม่นยำเพียงพอ

จากผลการทดสอบสมรรถนะของระบบถอดรหัสที่แสดงข้างต้น สรุปได้ว่า ตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ สามารถทำงานร่วมกับระบบถอดรหัสที่เสนอ บนช่องสัญญาณแบบเฟดดิงได้เป็นอย่างดี สมรรถนะของระบบถอดรหัสที่อัตราเร็วเฟดดิงต่าง ๆ กัน ดีกว่ากรณีตัวตรวจจับเชิงผลต่างแบบธรรมดาอย่างเห็นได้ชัด และเมื่อเพิ่มจำนวนสัญลักษณ์ของตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ให้มากขึ้น สมรรถนะของระบบถอดรหัสก็จะดีขึ้นตามไปด้วย ผลที่ดีขึ้นพบทั้งในกรณีที่ B_dT เท่ากับ 0.01 0.125 และ 0.200 ในขณะที่เมื่อพิจารณาสมรรถนะของระบบถอดรหัสแบบเดิม พบว่าเมื่อเพิ่มจำนวนสัญลักษณ์ของตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ ผลที่ได้จะดีขึ้นเฉพาะเมื่อ B_dT เท่ากับ 0.125 และ 0.200 เท่านั้น ที่ B_dT เท่ากับ 0.01 ระบบถอดรหัสแบบเดิมไม่สามารถปรับปรุงให้มีสมรรถนะที่ดีขึ้นได้

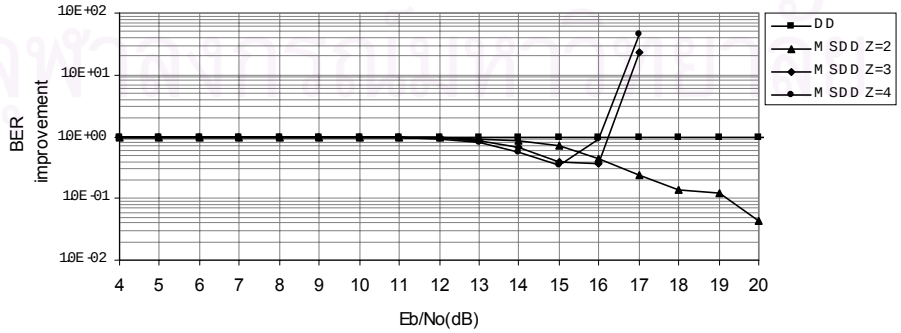
เมื่อพิจารณาสมรรถนะของระบบถอดรหัสที่เสนอ สำหรับกรณีที่ใช้ตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ เปรียบเทียบกับสมรรถนะของระบบถอดรหัสแบบเดิม พบว่า ระบบถอดรหัสที่เสนอมีสมรรถนะดีกว่าระบบถอดรหัสแบบเดิม เมื่อ B_dT เท่ากับ 0.01 และ 0.125 ที่ B_dT เท่ากับ 0.200 และ จำนวนสัญลักษณ์ที่สังเกตการณ์ (Z) ของตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์เท่ากับ 2 สัญลักษณ์ สมรรถนะของระบบถอดรหัสที่เสนอจะด้อยกว่าสมรรถนะของระบบถอดรหัสแบบเดิม อย่างไรก็ตาม สมรรถนะของระบบถอดรหัสที่เสนอจะดีกว่าสมรรถนะของระบบถอดรหัสแบบเดิม ถ้าจำนวนสัญลักษณ์ที่สังเกตการณ์ของตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์เพิ่มขึ้น หรือ เมื่อภาครับมีการประมาณช่องสัญญาณที่แม่นยำยิ่งขึ้น



รูปที่ 6.12 การเปรียบเทียบสมรรถนะของระบบถอดรหัสแบบเดิม สำหรับกรณีที่ใช้การตรวจจับแบบต่าง ๆ เมื่อ B_dT เท่ากับ 0.200



รูปที่ 6.13 การเปรียบเทียบสมรรถนะของระบบถอดรหัสที่เสนอ สำหรับกรณีที่ใช้การตรวจจับแบบต่าง ๆ เมื่อ B_dT เท่ากับ 0.200



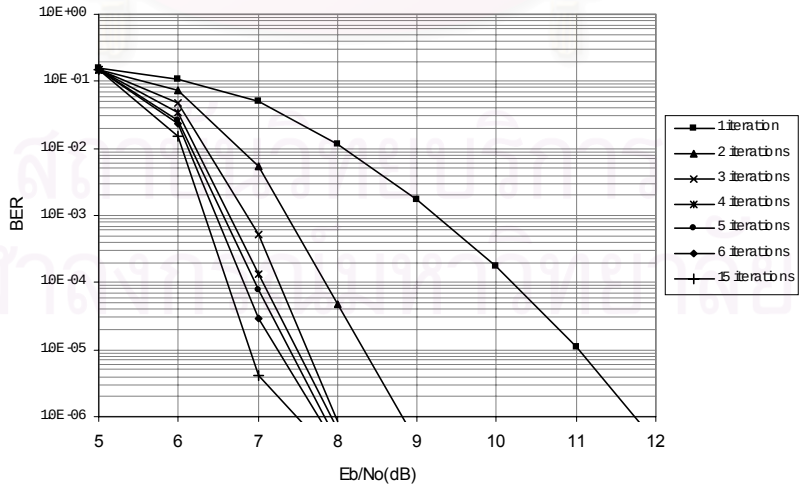
รูปที่ 6.14 อัตราส่วน BER ของระบบถอดรหัสแบบเดิมต่อ BER ของระบบถอดรหัสที่เสนอ สำหรับกรณีที่ใช้การตรวจจับแบบต่าง ๆ เมื่อ B_dT เท่ากับ 0.200

6.3 ผลการทดสอบผลกระทบจากการเปลี่ยนค่าพารามิเตอร์

ในหัวข้อนี้จะเป็นการศึกษาถึงผลกระทบจากการเปลี่ยนแปลงค่าพารามิเตอร์ต่าง ๆ ของระบบถอดรหัสที่เสนอ ซึ่งประกอบด้วย ผลของจำนวนรอบในการถอดรหัสแบบวนซ้ำ ผลของขนาดของบล็อกข้อมูล และ ผลของตัวสลับลำดับบิตรหัสที่มีต่อสมรรถนะของระบบถอดรหัส พร้อมกันนี้ยังได้วิเคราะห์ถึงผลกระทบของจำนวนสัญลักษณ์ของตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ที่มีต่อความซับซ้อนในกระบวนการถอดรหัส

6.3.1 ผลของจำนวนรอบในการถอดรหัสแบบวนซ้ำที่มีต่อสมรรถนะของระบบถอดรหัส

สมรรถนะของการถอดรหัสเทอร์โบจะดีขึ้นเมื่อจำนวนรอบในการถอดรหัสเพิ่มขึ้น ดังรูปที่ 6.15 ซึ่งแสดงสมรรถนะของระบบถอดรหัสที่เสนอ ที่ B_dT เท่ากับ 0.01 สำหรับกรณีการตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ ที่ Z = 2 เมื่อจำนวนรอบในการถอดรหัสเท่ากับ 1 ถึง 6 รอบ พร้อมทั้งเปรียบเทียบกับกรณีที่จำนวนรอบในการถอดรหัสเท่ากับ 15 รอบ ซึ่งถือว่าเข้าใกล้สมรรถนะของระบบที่ระดับคอนเวอร์เจนซ์ (convergence) จากรูปจะเห็นว่า ที่ระดับ BER เท่ากับ 10^{-5} สมรรถนะของระบบเมื่อจำนวนรอบในการถอดรหัสเท่ากับ 2 รอบดีกว่าที่ 1 รอบถึง 2.7 dB และดีขึ้นอีก 0.7 dB เมื่อจำนวนรอบในการถอดรหัสเป็น 3 รอบ หลังจากนั้นสมรรถนะของระบบจะดีขึ้นอีกเพียงเล็กน้อยเท่านั้น และสมรรถนะของระบบที่ 5 รอบและ 6 รอบมีค่าใกล้เคียงกับสมรรถนะของระบบที่ 15 รอบมาก งานวิจัยนี้จึงเลือกทดสอบสมรรถนะของระบบถอดรหัสเมื่อจำนวนรอบในการถอดรหัสแบบวนซ้ำมีค่าเท่ากับ 5 รอบ



รูปที่ 6.15 การเปรียบเทียบสมรรถนะของระบบถอดรหัสที่เสนอ (สำหรับกรณีการตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ ที่ Z = 2) เมื่อจำนวนรอบในการถอดรหัสแบบวนซ้ำต่างกัน พิจารณากรณีที่ B_dT เท่ากับ 0.01

6.3.2 ผลของขนาดของบล็อกข้อมูลที่มีต่อสมรรถนะของระบบถอดรหัส

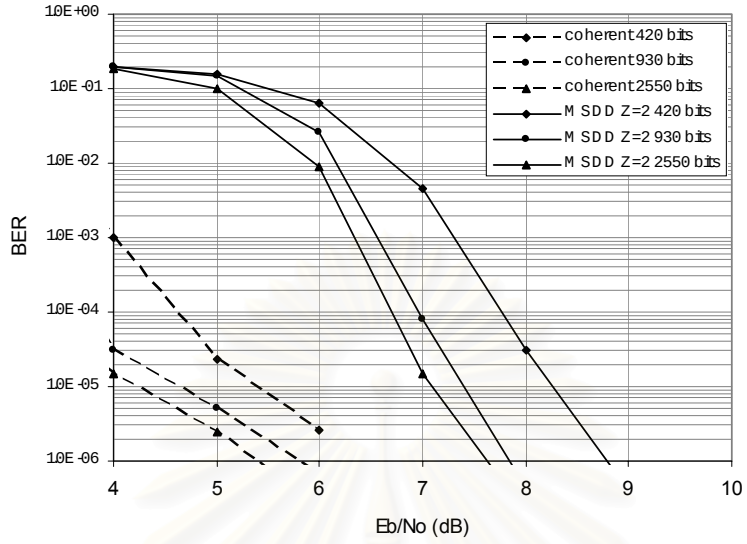
เมื่อเพิ่มขนาดของบล็อกข้อมูล ระบบถอดรหัสจะมีสมรรถนะดีขึ้น เนื่องจากขนาดของบล็อกข้อมูลที่เพิ่มขึ้น หมายความถึงขนาดของตัวสลับลำดับที่ใหญ่ขึ้นด้วย ในช่องสัญญาณแบบเฟดดิง ตัวสลับลำดับที่มีขนาดใหญ่จะมีความสามารถในการกระจายความผิดพลาดที่เกิดจากเฟดดิงได้ดี ส่งผลให้กระบวนการถอดรหัสมีประสิทธิภาพดีขึ้น สมรรถนะของระบบถอดรหัสที่เสนอสำหรับกรณีการตรวจจับแบบร่วมนัย และการตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ ที่ Z = 2 เมื่อบล็อกข้อมูลมีขนาดเท่ากับ 420 บิต 930 บิต และ 2550 บิต ที่ B_dT เท่ากับ 0.01 แสดงอยู่ในรูปที่ 6.16 สมรรถนะของระบบถอดรหัสสำหรับกรณีการตรวจจับแบบร่วมนัยเมื่อบล็อกข้อมูลมีขนาด 2550 บิต ดีกว่าสมรรถนะของระบบเมื่อบล็อกข้อมูลมีขนาด 420 บิตอยู่ 1.2 dB เมื่อพิจารณากรณี MSDD ที่ Z = 2 พบว่าขนาดของบล็อกข้อมูลที่เพิ่มขึ้น ช่วยให้ระบบถอดรหัสมีสมรรถนะดีขึ้นเช่นเดียวกัน อย่างไรก็ตาม สัดส่วนของสมรรถนะที่ดีขึ้นยังคงน้อยกว่ากรณีการตรวจจับแบบร่วมนัย ซึ่งสังเกตได้จากข้อด้อยของการตรวจจับแบบไม่ร่วมนัยที่เพิ่มขึ้นเมื่อบล็อกข้อมูลมีขนาดใหญ่ขึ้น ดังแสดงในตารางที่ 6.1

ตารางที่ 6.1 ข้อด้อยของการตรวจจับแบบไม่ร่วมนัยที่ระดับ BER เท่ากับ 10^{-5} เมื่อบล็อกข้อมูลมีขนาด 420 930 และ 2550 บิต

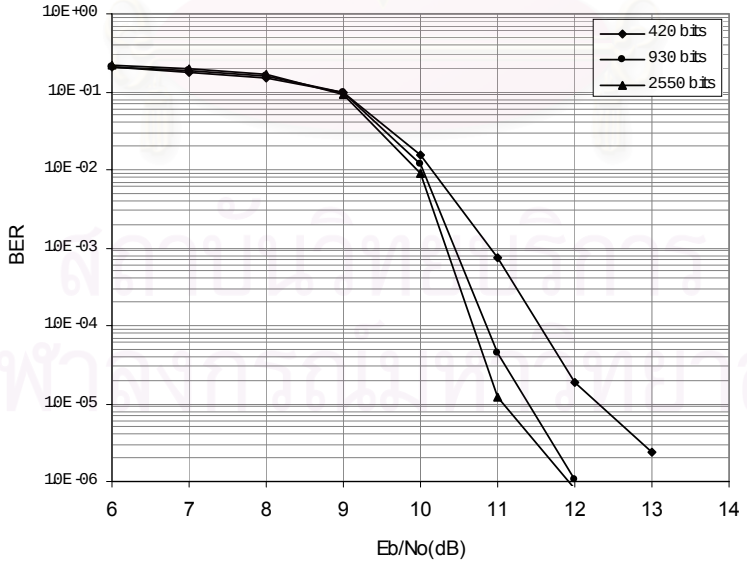
ขนาดของบล็อกข้อมูล (บิต)	ข้อด้อยของการตรวจจับแบบไม่ร่วมนัย (dB)
420	2.6
930	2.8
2550	2.9

สำหรับกรณีที่ B_dT เท่ากับ 0.125 และ 0.200 ผลของขนาดของบล็อกข้อมูลที่มีต่อสมรรถนะของระบบถอดรหัสก็เป็นไปในลักษณะเดียวกันกับกรณีที่ B_dT เท่ากับ 0.01 ดังรูปที่ 6.17 และ 6.18

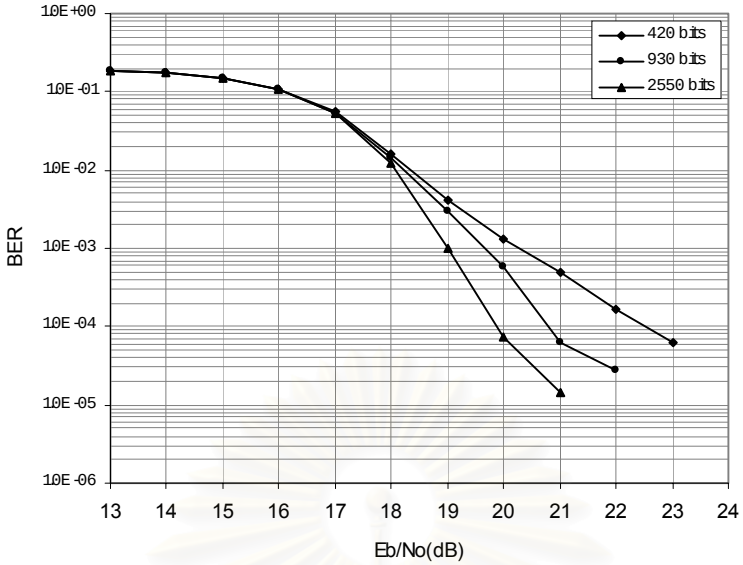
<u>หมายเหตุ</u> ข้อด้อยของการตรวจจับแบบไม่ร่วมนัย (noncoherence penalty) คือ ค่าผลต่างของ Eb/No ระหว่างกรณีการตรวจจับแบบร่วมนัยและการตรวจจับแบบไม่ร่วมนัย เมื่อพิจารณาที่ระดับ BER ค่าหนึ่ง ๆ ซึ่งเป็นค่าที่แสดงถึงข้อเสียเปรียบของการตรวจจับแบบไม่ร่วมนัยเมื่อเปรียบเทียบกับการตรวจจับแบบร่วมนัย



รูปที่ 6.16 การเปรียบเทียบสมรรถนะของระบบถอดรหัสที่เสนอ สำหรับกรณีการตรวจจับแบบร่วมนัยและการตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ ที่ Z = 2 เมื่อ B_dT เท่ากับ 0.01 และบล็อกข้อมูลมีขนาดเท่ากับ 420 930 และ 2550 บิต



รูปที่ 6.17 การเปรียบเทียบสมรรถนะของระบบถอดรหัสที่เสนอ (สำหรับกรณีการตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ ที่ Z = 2) เมื่อ B_dT เท่ากับ 0.125 และบล็อกข้อมูลมีขนาดเท่ากับ 420 930 และ 2550 บิต



รูปที่ 6.18 การเปรียบเทียบสมรรถนะของระบบถอดรหัสที่เสนอ (สำหรับกรณีการตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ ที่ Z = 2) เมื่อ B_dT เท่ากับ 0.200 และบล็อกข้อมูลมีขนาดเท่ากับ 420 930 และ 2550 บิต

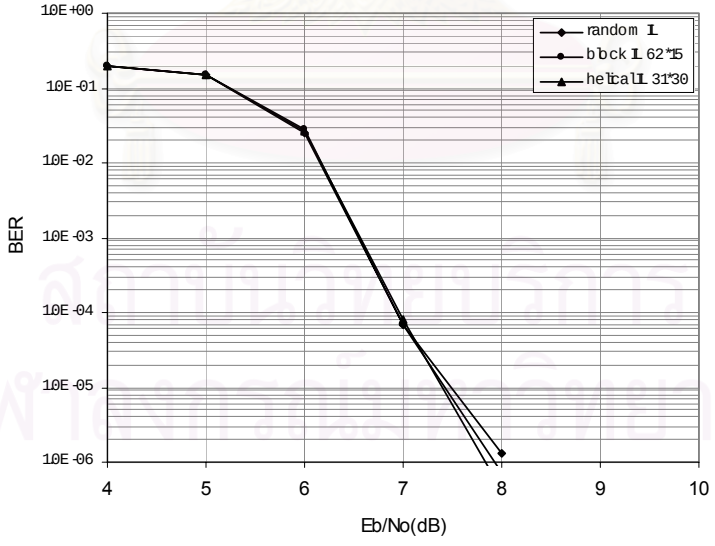
6.3.3 ผลของตัวสลับลำดับบิตรหัสที่มีต่อสมรรถนะของระบบถอดรหัส

การทดสอบสมรรถนะของระบบถอดรหัสที่ผ่านมา ตัวสลับลำดับบิตรหัสที่ใช้เป็นตัวสลับลำดับแบบ helical block ขนาด 31×30 บิต สำหรับหัวข้อนี้จะทดสอบสมรรถนะของระบบถอดรหัสเมื่อตัวสลับลำดับบิตรหัสมีรูปแบบแตกต่างกัน เพื่อศึกษาว่า ตัวสลับลำดับแต่ละแบบส่งผลต่อสมรรถนะของระบบถอดรหัสอย่างไร ตัวสลับลำดับที่นำมาใช้เปรียบเทียบสมรรถนะของระบบถอดรหัสได้แก่ 1) ตัวสลับลำดับแบบสุ่ม (random IL) 2) ตัวสลับลำดับแบบบล็อก ขนาด 62×15 บิต (block IL 62*15) และ 3) ตัวสลับลำดับแบบ helical block ขนาด 31×30 บิต (helical IL 31*30) โดยจะพิจารณาระบบสำหรับกรณีตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ที่ Z = 2

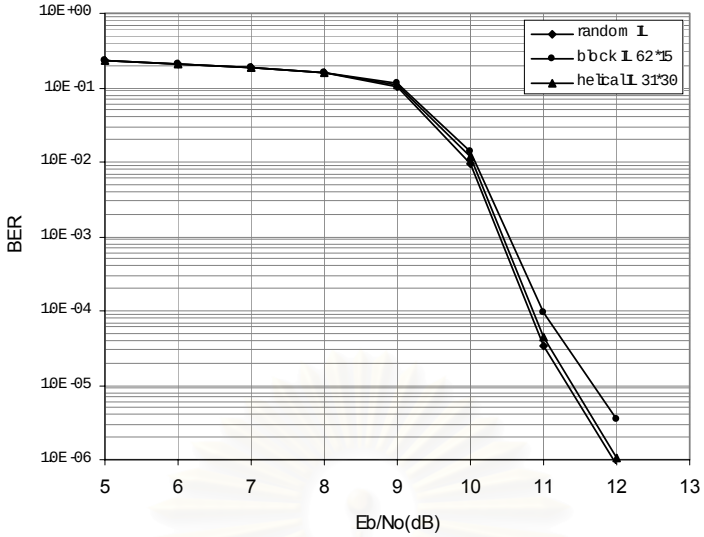
รูปที่ 6.19 เป็นสมรรถนะของระบบถอดรหัสที่เสนอ เมื่อ B_dT เท่ากับ 0.01 จากรูปจะเห็นว่า สมรรถนะของระบบถอดรหัสเมื่อใช้ตัวสลับลำดับทั้งสามแบบมีค่าใกล้เคียงกันมาก ซึ่งแสดงว่ารูปแบบของตัวสลับลำดับบิตรหัสที่แตกต่างกัน ไม่ได้ส่งผลกระทบต่อสมรรถนะของระบบถอดรหัสเท่าใดนัก เมื่อพิจารณาสมรรถนะของระบบที่ B_dT เท่ากับ 0.125 ในรูปที่ 6.20 พบว่า สมรรถนะของระบบถอดรหัสเมื่อใช้ตัวสลับลำดับแบบสุ่ม และแบบ helical block มีค่าใกล้เคียงกัน และสมรรถนะของระบบถอดรหัสเมื่อใช้ตัวสลับลำดับแบบบล็อก ด้อยกว่าสมรรถนะในสองกรณีแรกเล็กน้อย ทั้งนี้อาจเนื่องมาจากตัวสลับลำดับแบบสุ่ม และแบบ helical block มีรูปแบบการกระจายบิตที่ดีกว่าตัวสลับลำดับแบบบล็อก อย่างไรก็ตามความแตกต่างของสมรรถนะที่พบถือว่า

ไม่มากนัก และอาจกล่าวได้ว่า สมรรถนะของระบบถอดรหัสเมื่อใช้ตัวสลับลำดับทั้งสามแบบมีค่าใกล้เคียงกัน

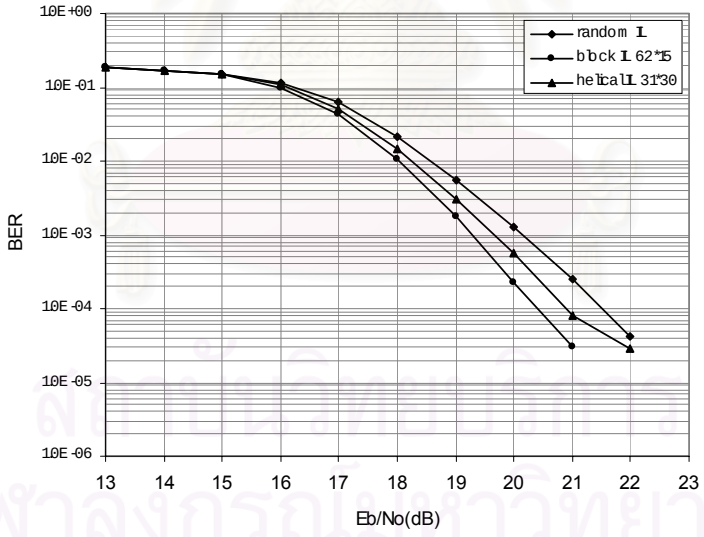
สำหรับสมรรถนะของระบบถอดรหัส เมื่อ B_dT เท่ากับ 0.200 แสดงอยู่ในรูปที่ 6.21 ในกรณีนี้พบว่า สมรรถนะของระบบแตกต่างจากกรณีที่ B_dT เท่ากับ 0.01 และ 0.125 จากรูปจะเห็นว่าตัวสลับลำดับแบบบล็อกให้สมรรถนะดีที่สุด รองลงมาคือ ตัวสลับลำดับแบบ helical block ส่วนตัวสลับลำดับแบบสุ่มให้สมรรถนะด้อยที่สุด ผลการทดสอบที่เกิดขึ้นไม่สามารถชี้ชัดลงไปได้ว่าเหตุใดตัวสลับลำดับแบบบล็อกซึ่งมีรูปแบบการกระจายบิตแบบหยาบ ๆ จึงให้สมรรถนะดีกว่าตัวสลับลำดับแบบสุ่ม และแบบ helical block แต่มีข้อที่น่าสังเกตคือ ระบบถอดรหัสที่เสนอสำหรับกรณี MSDD ที่ Z=2 เมื่อ B_dT เท่ากับ 0.200 ซึ่งกำลังพิจารณาอยู่นี้ มีสมรรถนะด้อยกว่าระบบถอดรหัสแบบเดิม ดังที่ได้กล่าวไปแล้วในหัวข้อ 6.2.2 นั่นก็หมายความว่า สำหรับกรณีดังกล่าว การแยกบิตข้อมูลกับบิตรหัสออกจากกันจะส่งผลให้สมรรถนะของระบบถอดรหัสด้อยลง เพราะฉะนั้นจึงอาจเป็นไปได้ว่า การกระจายบิตรหัสออกจากกันจะยิ่งส่งผลให้สมรรถนะของระบบถอดรหัสด้อยลงไปอีก ตัวสลับลำดับแบบบล็อกที่มีการกระจายบิตไม่ดีเท่ากับตัวสลับลำดับแบบสุ่มจึงให้สมรรถนะดีกว่าตัวสลับลำดับแบบสุ่ม อย่างไรก็ตาม ข้อน่าสังเกตที่กล่าวมาเป็นเพียงแค่สมมติฐานส่วนหนึ่งเท่านั้น ข้อสรุปที่แท้จริงยังต้องอาศัยการศึกษาและวิเคราะห์ จากผลการทดสอบผลกระทบของตัวสลับลำดับอย่างละเอียดต่อไป



รูปที่ 6.19 การเปรียบเทียบสมรรถนะของระบบถอดรหัสที่เสนอ (สำหรับกรณีตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ ที่ Z=2) เมื่อตัวสลับลำดับบิตรหัสมีรูปแบบแตกต่างกัน พิจารณาที่ B_dT เท่ากับ 0.01



รูปที่ 6.20 การเปรียบเทียบสมรรถนะของระบบถอดรหัสที่เสนอ (สำหรับกรณีตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ ที่ Z=2) เมื่อตัวสลับลำดับบิตรหัสมีรูปแบบแตกต่างกัน พิจารณาที่ B_dT เท่ากับ 0.125



รูปที่ 6.21 การเปรียบเทียบสมรรถนะของระบบถอดรหัสที่เสนอ (สำหรับกรณีตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ ที่ Z=2) เมื่อตัวสลับลำดับบิตรหัสมีรูปแบบแตกต่างกัน พิจารณาที่ B_dT เท่ากับ 0.200

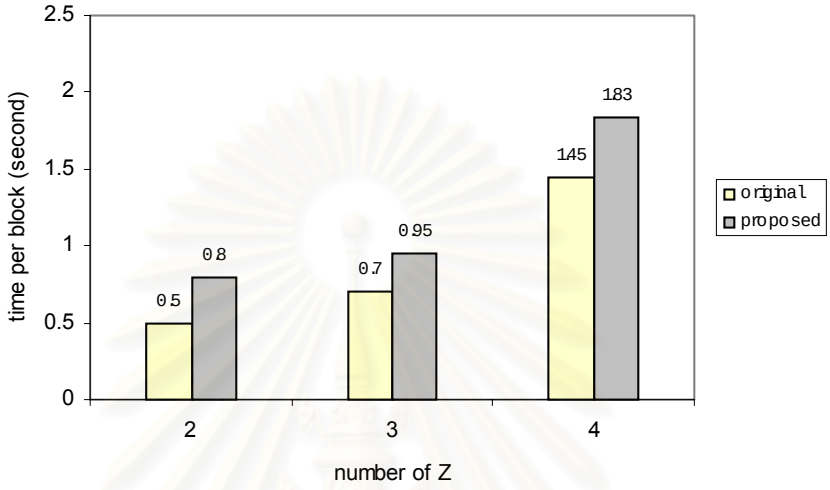
6.3.4 ผลของจำนวนสัญลักษณ์ของตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ที่มีต่อความซับซ้อนของระบบถอดรหัส

หัวข้อนี้เป็นการทดสอบสมรรถนะของระบบถอดรหัส เมื่อจำนวนสัญลักษณ์ของตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์เพิ่มขึ้น โดยจะวิเคราะห์ว่าจำนวนสัญลักษณ์ที่เพิ่มขึ้น ส่งผลให้ความซับซ้อนในกระบวนการถอดรหัสสูงขึ้นมากน้อยเพียงใด ทั้งนี้เพื่อใช้ประกอบกับการศึกษาผลกระทบของจำนวนสัญลักษณ์ที่มีต่อสมรรถนะของระบบถอดรหัส ที่กล่าวไว้ในหัวข้อ 6.2.2 ซึ่งชี้ให้เห็นว่า การเพิ่มจำนวนสัญลักษณ์ช่วยทำให้สมรรถนะของระบบถอดรหัสดีขึ้น เพราะฉะนั้นการคำนึงถึงความซับซ้อนในกระบวนการถอดรหัส จะเป็นเครื่องบ่งชี้ว่าควรเพิ่มจำนวนสัญลักษณ์ขึ้นเป็นเท่าใด ระบบถอดรหัสจึงจะมีประสิทธิภาพสูงสุด ในขณะที่ความซับซ้อนยังอยู่ในระดับที่ยอมรับได้

การวัดค่าความซับซ้อนของระบบถอดรหัส จะพิจารณาจากระยะเวลาที่ใช้ในการจำลองระบบด้วยโปรแกรมคอมพิวเตอร์ โดยจะวัดอยู่ในรูปของระยะเวลาเป็นวินาที ต่อ จำนวนบล็อกข้อมูลที่ถอดรหัสหนึ่งบล็อก (930 บิต) คอมพิวเตอร์ที่นำมาใช้ประมวณผลมี CPU Pentium III 700 MHz และ RAM ขนาด 256 MB ผลการทดสอบแสดงอยู่ในรูปที่ 6.22 ทั้งนี้ระยะเวลาที่วัดได้จะไม่ขึ้นอยู่กับค่า Eb/No หรือ B_dT ที่พิจารณา เนื่องจากระยะเวลาที่ใช้ประมวลผลที่แต่ละ Eb/No และที่ B_dT ค่าต่าง ๆ มีค่าเท่ากันทุกกรณี เพราะฉะนั้นเวลาที่ใช้ในการจำลองระบบจะแปรผันตามจำนวนสัญลักษณ์ของตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์เท่านั้น จากรูปจะเห็นว่าเมื่อจำนวนสัญลักษณ์เพิ่มขึ้น ระยะเวลาที่ใช้ในกระบวนการถอดรหัสก็จะเพิ่มขึ้นตามไปด้วย อย่างไรก็ตามความซับซ้อนที่ระดับ Z=3 มากกว่าที่ระดับ Z=2 เพียงเล็กน้อย และความซับซ้อนที่ระดับ Z=4 เพิ่มสูงขึ้นจากระดับ Z=3 ประมาณสองเท่าเท่านั้น ซึ่งถือว่าไม่มากนักเมื่อคำนึงถึงสมรรถนะของระบบถอดรหัสที่ถูกปรับปรุงให้ดีขึ้น โดยเฉพาะอย่างยิ่งในกรณีเฟดดิงแบบเร็วที่ B_dT เท่ากับ 0.200 การเพิ่ม Z จาก 2 เป็น 3 สัญลักษณ์ช่วยให้ Eb/No ลดลงได้ถึง 4.2 dB และการเพิ่ม Z จาก 3 เป็น 4 สัญลักษณ์ จะช่วยลด Eb/No ลงได้อีกประมาณ 0.5 dB (พิจารณาที่ระดับ BER เท่ากับ 10^{-3})

เมื่อพิจารณาความซับซ้อนของระบบเดิมเปรียบเทียบกับระบบที่เสนอ พบว่าระบบที่เสนอมีความซับซ้อนสูงกว่าระบบเดิม ดังรูปที่ 6.22 ความซับซ้อนที่เพิ่มขึ้นนี้เป็นผลมาจากขั้นตอนการสลับลำดับบิตรหัสที่ภาคส่ง และขั้นตอนการสลับลำดับกลับที่ภาคถอดรหัส รวมไปถึงความซับซ้อนในการคำนวณค่าความน่าจะเป็นหลังของกระบวนการถอดรหัสเทอร์โบ ซึ่งมีขั้นตอนการทำงานที่ยุ่งยากกว่าระบบถอดรหัสแบบเดิม ดังนั้นระยะเวลาที่ใช้ในการประมวลผลของระบบที่

เสนอจึงมากกว่าระบบเดิม อย่างไรก็ดีความซับซ้อนของระบบที่เสนอนี้สูงกว่าระบบเดิมเพียงเล็กน้อยเท่านั้น ในขณะที่ระบบที่เสนอสามารถลด BER ลงได้มากที่สุดถึง 3 ระดับขนาด (พิจารณาที่ B_dT เท่ากับ 0.01 และ Z เท่ากับ 3 หรือ 4 สัญลักษณ์)



รูปที่ 6.22 การเปรียบเทียบระยะเวลาที่ใช้ในการถอดรหัสบล็อกข้อมูลหนึ่งบล็อก เมื่อจำนวนสัญลักษณ์ (Z) เท่ากับ 2 3 และ 4 สัญลักษณ์

บทที่ 7

บทสรุปและข้อเสนอแนะ

7.1 บทสรุป

งานวิจัยนี้ได้ศึกษาและปรับปรุงสมรรถนะของการถอดรหัสแบบวนซ้ำ หรือ การถอดรหัสเทอร์โบ ที่ทำงานร่วมกับตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ (multiple symbol differential detector : MSDD) บนช่องสัญญาณที่เกิดเรย์ลีเฟดดิงที่มีสหสัมพันธ์กัน ตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์จะทำหน้าที่ประมาณข่าวสารช่องสัญญาณและส่งข่าวสารนี้ให้กับเครื่องถอดรหัสเทอร์โบ เพื่อนำไปใช้คำนวณค่าความน่าจะเป็นหลังของบิตข้อมูลในกระบวนการถอดรหัส แนวความคิดหลักที่ใช้ในการปรับปรุงสมรรถนะของระบบถอดรหัส คือ การเสนอให้ภาคส่งแยกส่งบิตข้อมูลกับบิตรหัสที่เกิดจากบิตข้อมูลนั้นไปในสัญลักษณ์ QPSK ต่างสัญลักษณ์กัน ทั้งนี้เพื่อหลีกเลี่ยงกรณีที่บิตข้อมูลและบิตรหัสจะเสียหายไปพร้อมกันเมื่อผ่านเฟดดิง ดังนั้นการแยกส่งบิตข้อมูลกับบิตรหัสออกจากกัน จึงเป็นการช่วยเพิ่มโอกาสที่ภาครับจะได้รับรู้ข่าวสารของบิตข้อมูลนั้นจากทางใดทางหนึ่ง เป็นผลให้กระบวนการถอดรหัสเทอร์โบทำงานได้อย่างมีประสิทธิภาพมากขึ้น เนื่องจากขั้นตอนวิธีการถอดรหัสที่ใช้ MSDD แบบเดิมซึ่งไม่มีการแยกบิต [13] ไม่สามารถนำมาใช้กับระบบถอดรหัสที่เสนอได้ งานวิจัยนี้จึงได้วิเคราะห์ขั้นตอนวิธีการถอดรหัสขึ้นใหม่เพื่อให้สอดคล้องกับระบบถอดรหัสที่เสนอ โดยที่เครื่องถอดรหัสเทอร์โบยังคงสามารถใช้ข่าวสารช่องสัญญาณ ที่คำนวณมาจากตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ได้นอกจากนี้เครื่องถอดรหัสเทอร์โบยังถูกออกแบบให้ส่งข่าวสารเอ็กซ์ทรินซิกกลับไปให้ตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ เพื่อใช้ประมาณข่าวสารช่องสัญญาณใหม่อีกครั้ง ทำให้การประมาณช่องสัญญาณแม่นยำขึ้นในแต่ละรอบของการถอดรหัส ซึ่งจะส่งผลให้กระบวนการตัดสินบิตของเครื่องถอดรหัสเทอร์โบถูกต้องยิ่งขึ้นด้วย

จากผลการทดสอบพบว่า ตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์สามารถทำงานร่วมกับระบบถอดรหัสที่เสนอบนช่องสัญญาณแบบเฟดดิงได้เป็นอย่างดี การทดสอบสมรรถนะของระบบถอดรหัสที่เสนอสำหรับกรณีการตรวจจับแบบไม่ร่วมนัย ซึ่งใช้ตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ แสดงให้เห็นว่า สมรรถนะของระบบถอดรหัสที่อัตราเร็วเฟดดิงต่าง ๆ ดีกว่าสมรรถนะของระบบกรณีที่ใช้ตัวตรวจจับเชิงผลต่างแบบธรรมดา (differential detector : DD) อย่างเห็นได้ชัด และเมื่อเพิ่มจำนวนสัญลักษณ์ของตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์จาก $Z=2$ เป็น $Z=3$ และ $Z=4$ สมรรถนะของระบบถอดรหัสก็จะดีขึ้นตามลำดับ ผลที่ดีขึ้นพบทั้งใน

กรณีที่ B_dT เท่ากับ 0.01 0.125 และ 0.200 แต่เมื่อพิจารณาสมรรถนะของระบบถอดรหัสที่ใช้ MSDD แบบเดิม พบว่าเมื่อเพิ่มจำนวนสัญลักษณ์ของตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ สมรรถนะของระบบจะดีขึ้นเฉพาะกรณีที่ B_dT เท่ากับ 0.125 และ 0.200 เท่านั้น ที่ B_dT เท่ากับ 0.01 การเพิ่มจำนวนสัญลักษณ์ของตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ไม่สามารถปรับปรุงสมรรถนะของระบบถอดรหัสที่ใช้ MSDD แบบเดิมให้ดีขึ้นได้

เมื่อพิจารณาสมรรถนะของระบบถอดรหัสที่เสนอ เปรียบเทียบกับสมรรถนะของระบบถอดรหัสที่ใช้ MSDD แบบเดิม พบว่าที่ B_dT เท่ากับ 0.01 และ 0.125 สมรรถนะของระบบถอดรหัสที่เสนอดีกว่าระบบเดิม โดยเฉพาะอย่างยิ่งเมื่อเฟดดิงมีการเปลี่ยนแปลงอย่างช้า ๆ ซึ่งจะส่งผลให้ความผิดพลาดเกิดติดกันเป็นช่วงยาวและแก้ไขได้ยาก ในกรณีนี้สมรรถนะของระบบเดิมจะด้อยลงอย่างมาก ขณะที่สมรรถนะในแง่ของอัตราความผิดพลาดของบิตของระบบถอดรหัสที่เสนอดีกว่าสมรรถนะของระบบถอดรหัสแบบเดิมถึง 10^3 เท่า หรือ 3 ระดับขนาด สำหรับผลการทดสอบระบบที่ B_dT เท่ากับ 0.200 พบว่า สมรรถนะของระบบถอดรหัสที่เสนอกรณีตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ ที่ Z=2 ด้อยกว่าสมรรถนะของระบบถอดรหัสแบบเดิม ที่เป็นเช่นนี้เนื่องจากเฟดดิงมีการเปลี่ยนแปลงอย่างรวดเร็ว และการประมาณข่าวสารช่องสัญญาณของตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ที่ Z=2 ไม่แม่นยำเพียงพอ ทำให้กระบวนการตัดสินบิตของระบบถอดรหัสที่เสนอเกิดความไม่แน่นอนขึ้น ส่งผลให้การถอดรหัสเทอร์โบมีประสิทธิภาพด้อยลง อย่างไรก็ตามเมื่อจำนวนสัญลักษณ์ของตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์เพิ่มขึ้นเป็น 3 และ 4 สัญลักษณ์ การประมาณช่องสัญญาณของภาครับก็จะแม่นยำมากยิ่งขึ้น ส่งผลให้สมรรถนะของระบบถอดรหัสที่เสนอดีกว่าสมรรถนะของระบบถอดรหัสแบบเดิม ในส่วนของการทดสอบความซับซ้อนของระบบถอดรหัส เมื่อจำนวนสัญลักษณ์ของตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์เพิ่มขึ้น แสดงให้เห็นว่า ความซับซ้อนที่ระดับ Z=4 สูงกว่าระดับ Z=3 และ Z=2 ประมาณสองเท่าเท่านั้น เพราะฉะนั้นการเลือกใช้ตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์ที่ Z=4 จึงสมเหตุสมผลเมื่อคำนึงถึงสมรรถนะของระบบถอดรหัสที่ถูกปรับปรุงให้ดีขึ้น

จากผลการทดสอบข้างต้น สรุปได้ว่าการเสนอให้แยกส่งบิตข้อมูลกับบิตรหัสออกจากกัน ช่วยเสริมการทำงานของกระบวนการถอดรหัสเทอร์โบ และสามารถปรับปรุงสมรรถนะของระบบถอดรหัสที่ใช้ตัวตรวจจับเชิงผลต่างแบบหลายสัญลักษณ์แบบเดิมให้ดีขึ้นได้

7.2 ข้อเสนอแนะ

หัวข้อที่ควรศึกษาและวิจัยต่อไปในอนาคตคือ

1. การเลือกใช้ตัวสลับลำดับบิตรหัส

การศึกษาว่าตัวสลับลำดับบิตรหัสที่แตกต่างกัน ส่งผลต่อรูปแบบการกระจายบิตรหัสอย่างไร และมีผลกระทบกับสมรรถนะของระบบถอดรหัสหรือไม่ ทั้งนี้เพื่อวิเคราะห์ว่าตัวสลับลำดับบิตรหัสแบบใดสามารถปรับปรุงสมรรถนะของระบบถอดรหัสให้ดีขึ้นได้

2. การประยุกต์ใช้กับช่องสัญญาณแบบอื่น

งานวิจัยนี้พิจารณาเฉพาะกรณีช่องสัญญาณที่เกิดเรย์ลีเฟดดิงชนิดเรียบที่มีสหสัมพันธ์กันเท่านั้น งานวิจัยในอนาคตจึงควรประยุกต์ใช้ระบบถอดรหัสที่เสนอบนช่องสัญญาณแบบอื่น ยกตัวอย่างเช่น ช่องสัญญาณที่เกิดเรย์ลีเฟดดิงชนิดเลือกความถี่ (Rayleigh frequency-selective fading) หรือ ช่องสัญญาณที่มีการแจกแจงทางแอมพลิจูดรูปแบบอื่น ได้แก่ การแจกแจงแบบนาคากามิ (Nakagami distribution) แทนการแจกแจงแบบเรย์ลี

รายการอ้างอิง

1. Berrou, C., Glavieux, A., and Thitimajshima, P. Near Shannon Limit Error-Correcting Coding and Decoding: Turbo Codes (1). IEEE International Conference on Communications (May 1993): 1064-1070.
2. Divsalar, D., and Pollara, F. Turbo Codes for PCS Applications. IEEE International Conference on Communications (June 1995): 54-59.
3. Hall, E. K., and Wilson, S. G. Design and Performance Analysis of Turbo Codes on Rayleigh Fading Channels. IEEE Proceedings (March 1996): 16-20.
4. Lee, W. C. Y. Mobile Communications Engineering. New York: McGraw Hill, 1982.
5. Marsland, I. D., and Mathiopoulos, P. T. Differential Detection of Turbo Codes for Rayleigh fast Fading Channels. IEEE Communications Letters Vol.2 (February 1998): 42-44.
6. Makrakis, D., and Feher, K. Multiple Differential Detection of Continuous Phase Modulation Signals. IEEE Transactions on Vehicular Technology Vol.42 (May 1993): 186-196.
7. Makrakis, D., Mathiopoulos, P. T., and Bouras, D. P. Optimal decoding of coded PSK and QAM signals in correlated fast fading channels and AWGN: A combined envelope, multiple differential and coherent approach. IEEE Transactions on Communications Vol.42 (January 1994): 63-75.
8. Ho, P., and Fung, D. Error Performance of Multiple Symbol Differential Detection of PSK Signals Transmitted over Correlated Rayleigh Fading Channels. IEEE Transactions on Communications Vol.40 (October 1992): 1556-1569.
9. Peleg, M., and Shamai, S. Iterative decoding of coded and interleaved noncoherent multiple symbol detected DPSK. IEEE Electronics Letters Vol.33 (June 1997): 1018-1020.
10. Abrardo, A., Benelli, G., and Cau, G. R. Multiple-Symbol Differential Detection of GMSK for Mobile Communications. IEEE Transactions on Vehicular Technology Vol.44 (August 1995): 379-389.
11. Hoeher, P. "Turbo DPSK": Iterative differntial PSK demodulation and channel decoding. IEEE Transactions on Communications Vol.47 (June 1999): 837-843.

12. Qin, G. F., Zhou, S. D., Xiao, L. M., and Yao, Y. Iterative decoding of GMSK modulated convolutional code with multiple differential detection. IEEE Electronics Letters Vol.36 (February 2000): 258-259.
13. Marsland, I. D., and Mathiopoulos, P. T. Multiple Differential Detection of Parallel Concatenated Convolutional (Turbo) Codes in Correlated Fast Rayleigh Fading. IEEE Journal on Selected Areas in Communications Vol.16 (February 1998): 265-275.
14. Barbulescu, A. S., and Pietrobon, S. S. Terminating the trellis of turbo-codes in the same state. IEEE Electronics Letters Vol.31 (January 1995): 22-23.
15. Chi, D. T. A new block helical interleaver. IEEE MILCOM (1992): 799-804.
16. Barbulescu, A. S., and Pietrobon, S. S. Interleaver design for turbo codes. IEEE Electronics Letters Vol.30 (December 1994): 2107-2108.
17. Proakis, J. G. Digital Communications. Fourth Edition. Singapore: McGraw Hill, 2001.
18. Hall, E. K., and Wilson, S. G. Design and Analysis of Turbo Codes on Rayleigh Fading Channels. Proceedings of IEEE Global Telecommunications Conference (GLOBECOM'96) (November 1996): 16-20.
19. Rappaport, T. S. Wireless Communications. New York: Prentice Hall, 1996.
20. Sklar, B. Rayleigh Fading Channels in Mobile Digital Communication Systems Part I: Characterization. IEEE Communications Magazine (July 1997): 90-100.
21. Jakes, W. C. Microwave Mobile Communications. New York: Wiley, 1974.
22. Bahl, L. R., Cocke, J., Jelinek, F., and Raviv, J. Optimal decoding of linear codes for minimizing symbol error rate. IEEE Transactions on Information Theory Vol.20 (March 1974): 284-287.

ภาคผนวก

ภาคผนวก ก
การคำนวณเมตริกทุติยภูมิ

เมตริกทุติยภูมิสามารถคำนวณจากเมตริกปฐมภูมิ ได้ดังนี้

$$\begin{aligned}
\Gamma_n(I_n) \quad & \Pr\{R_n \mid I_n, \underline{R}_0^{n-1}\} \\
&= \sum_{\underline{I}_{n-Z+1}^{n-1}} \Pr\{R_n, \underline{I}_{n-Z+1}^{n} \mid I_n, \underline{R}_0^{n-1}\} \\
&= \sum_{\underline{I}_{n-Z+1}^{n-1}} \Pr\{R_n \mid \underline{I}_{n-Z+1}^{n}, \underline{R}_0^{n-1}\} \Pr\{\underline{I}_{n-Z+1}^{n-1} \mid I_n, \underline{R}_0^{n-1}\} \\
&= \sum_{\underline{I}_{n-Z+1}^{n-1}} M_n(\underline{I}_{n-Z+1}^{n}) \Pr\{\underline{I}_{n-Z+1}^{n-1} \mid I_n, \underline{R}_0^{n-1}\} \qquad \text{(ก.1)}
\end{aligned}$$

ถ้าความกว้างของตัวสลับลำดับช่องสัญญาณ มีขนาดมากกว่าขนาดหน่วยความจำของเครื่องเข้ารหัสย่อยแล้ว สัญลักษณ์ที่ถูกส่งมาในอดีตจะไม่มีความสัมพันธ์กับสัญลักษณ์ที่ถูกส่งมาณ เวลาปัจจุบัน เพราะฉะนั้น $\underline{I}_{n-Z+1}^{n-1}$ จะเป็นอิสระทางสถิติกับ I_n และจะได้ว่า

$$\begin{aligned}
\Pr\{\underline{I}_{n-Z+1}^{n-1} \mid I_n, \underline{R}_0^{n-1}\} &= \Pr\{\underline{I}_{n-Z+1}^{n-1} \mid \underline{R}_0^{n-1}\} \\
&\quad \Psi_{n-1}(\underline{I}_{n-Z+1}^{n-1}) \qquad \text{(ก.2)}
\end{aligned}$$

โดยที่ $\Psi_{n-1}(\underline{I}_{n-Z+1}^{n-1})$ สามารถคำนวณในลักษณะรีเคอร์ซีฟ (recursive) ได้ดังนี้

$$\begin{aligned}
\Psi_{n-1}(\underline{I}_{n-Z+1}^{n-1}) \quad & \Pr\{\underline{I}_{n-Z+1}^{n-1} \mid \underline{R}_0^{n-1}\} \\
&= \sum_{I_{n-Z}} \Pr\{\underline{I}_{n-Z}^{n-1} \mid \underline{R}_0^{n-1}\} \\
&= \sum_{I_{n-Z}} \frac{\Pr\{R_{n-1}, \underline{I}_{n-Z}^{n-1} \mid \underline{R}_0^{n-2}\}}{\Pr\{R_{n-1} \mid \underline{R}_0^{n-2}\}} \\
&= \sum_{I_{n-Z}} \frac{\Pr\{R_{n-1} \mid \underline{I}_{n-Z}^{n-1}, \underline{R}_0^{n-2}\}}{\Pr\{R_{n-1} \mid \underline{R}_0^{n-2}\}} \Pr\{\underline{I}_{n-Z}^{n-1} \mid \underline{R}_0^{n-2}\} \\
&= \sum_{I_{n-Z}} \frac{\Pr\{R_{n-1} \mid \underline{I}_{n-Z}^{n-1}, \underline{R}_0^{n-2}\}}{\Pr\{R_{n-1} \mid \underline{R}_0^{n-2}\}} \Pr\{\underline{I}_{n-Z}^{n-2} \mid I_{n-1}, \underline{R}_0^{n-2}\} \Pr\{I_{n-1} \mid \underline{R}_0^{n-2}\} \qquad \text{(ก.3)}
\end{aligned}$$

เมื่อ $\Pr\{R_{n-1} \mid \underline{I}_{n-Z}^{n-1}, \underline{R}_0^{n-2}\} = M_{n-1}(\underline{I}_{n-Z}^{n-1})$ คำนวณได้จากหน่วยคำนวณเมตริกปฐมภูมิ

$\Pr\{\underline{I}_{n-Z}^{n-2} \mid I_{n-1}, \underline{R}_0^{n-2}\} = \Psi_{n-2}(\underline{I}_{n-Z}^{n-2})$ ได้จากการคำนวณแบบรีเคอร์ซีฟรอบก่อนหน้านี้

นอกจากนี้การสลับลำดับของตัวสลับลำดับช่องสัญญาณยังส่งผลให้ I_{n-1} เป็นอิสระทางสถิติกับ $\underline{R}_0^{n-2}$ อีกด้วย ดังนั้น $\Pr\{I_{n-1} \mid \underline{R}_0^{n-2}\} = \Pr\{I_{n-1}\}$ และสมการ (ก.3) สามารถเขียนใหม่ได้ดังนี้

$$\Psi_{n-1}(\underline{I}_{n-Z+1}^{n-1}) = \frac{\sum_{I_{n-Z}} M_{n-1}(\underline{I}_{n-Z}^{n-1})\Psi_{n-2}(\underline{I}_{n-Z}^{n-2})\Pr\{I_{n-1}\}}{\Pr\{R_{n-1} \mid \underline{R}_0^{n-2}\}} \qquad (ก.4)$$

เนื่องจากว่า $\sum_{\underline{I}_{n-Z+1}^{n-1}} \Pr\{\underline{I}_{n-Z+1}^{n-1} \mid \underline{R}_0^{n-1}\} = 1$ เพราะฉะนั้นจะได้ว่า

$$\Pr\{R_{n-1} \mid \underline{R}_0^{n-2}\} = \sum_{\underline{I}_{n-Z+1}^{n-1}} \sum_{I_{n-Z}} M_{n-1}(\underline{I}_{n-Z}^{n-1})\Psi_{n-2}(\underline{I}_{n-Z}^{n-2})\Pr\{I_{n-1}\} \qquad (ก.5)$$

และ

$$\Psi_{n-1}(\underline{I}_{n-Z+1}^{n-1}) = \frac{\sum_{I_{n-Z}} M_{n-1}(\underline{I}_{n-Z}^{n-1})\Psi_{n-2}(\underline{I}_{n-Z}^{n-2})\Pr\{I_{n-1}\}}{\sum_{\underline{I}_{n-Z+1}^{n-1}} \sum_{I_{n-Z}} M_{n-1}(\underline{I}_{n-Z}^{n-1})\Psi_{n-2}(\underline{I}_{n-Z}^{n-2})\Pr\{I_{n-1}\}} \qquad (ก.6)$$

จากสมการ (ก.1) และ (ก.2) จะได้ว่าเมตริกทุติยภูมิสามารถคำนวณได้จาก

$$\Gamma_n(I_n) = \sum_{\underline{I}_{n-Z+1}^{n-1}} M_n(\underline{I}_{n-Z+1}^{n})\Psi_{n-1}(\underline{I}_{n-Z+1}^{n-1}) \qquad (ก.7)$$

ภาคผนวก ข
การวิเคราะห์เครื่องถอดรหัสย่อย

1. การคำนวณค่าความน่าจะเป็นหลัง

ความน่าจะเป็นหลัง (*a posteriori* probability : APP) จะถูกคำนวณที่เครื่องถอดรหัสย่อยแต่ละตัว โดยอาศัยขั้นตอนวิธีของ BCJR ซึ่งมีวิธีการวิเคราะห์ดังต่อไปนี้

$$\begin{aligned}
\Pr\{a_n \mid \underline{R}_0^N\} &= \sum_{(S_n,S_{n+1}):a_n} \Pr\{S_n, S_{n+1} \mid \underline{R}_0^N\} \\
&= \sum_{(S_n,S_{n+1}):a_n} \frac{\Pr\{\underline{R}_n^N, S_n, S_{n+1} \mid \underline{R}_0^{n-1}\}}{\Pr\{\underline{R}_n^N \mid \underline{R}_0^{n-1}\}} \\
&= \sum_{(S_n,S_{n+1}):a_n} \Pr\{S_n \mid \underline{R}_0^{n-1}\} \frac{\Pr\{\underline{R}_n^N, S_{n+1} \mid S_n, \underline{R}_0^{n-1}\}}{\Pr\{\underline{R}_n^N \mid \underline{R}_0^{n-1}\}} \\
&= \sum_{(S_n,S_{n+1}):a_n} \Pr\{S_n \mid \underline{R}_0^{n-1}\} \frac{\Pr\{R_n, S_{n+1} \mid S_n, \underline{R}_0^{n-1}\}}{\Pr\{R_n \mid \underline{R}_0^{n-1}\}} \frac{\Pr\{\underline{R}_{n+1}^N \mid S_{n+1}, S_n, \underline{R}_0^n\}}{\Pr\{\underline{R}_{n+1}^N \mid \underline{R}_0^n\}} \\
&= \sum_{(S_n,S_{n+1}):a_n} \Pr\{S_n \mid \underline{R}_0^{n-1}\} \frac{\Pr\{R_n, S_{n+1} \mid S_n, \underline{R}_0^{n-1}\}}{\Pr\{R_n \mid \underline{R}_0^{n-1}\}} \frac{\Pr\{\underline{R}_{n+1}^N \mid S_{n+1}, \underline{R}_0^n\}}{\Pr\{\underline{R}_{n+1}^N \mid \underline{R}_0^n\}} \qquad \text{(ข.1)}
\end{aligned}$$

พจน์ $\Pr\{\underline{R}_{n+1}^N \mid S_{n+1}, S_n, \underline{R}_0^n\}$ ในบรรทัดที่สี่ สามารถลดรูปมาเป็น $\Pr\{\underline{R}_{n+1}^N \mid S_{n+1}, \underline{R}_0^n\}$ ในบรรทัดที่ห้า เนื่องมาจากคุณสมบัติมาคอฟของวงจรเข้ารหัส กล่าวคือ ถ้าทราบสถานะของวงจรเข้ารหัสที่เวลา n+1 คือ S_{n+1} แล้ว สถานะ S_n ที่เกิดขึ้นที่เวลา n จะไม่ส่งผลต่อเหตุการณ์ที่เกิดขึ้นหลังจากเวลา n อีกต่อไป

กำหนดให้

$$\alpha_n(S_n) = \Pr(S_n \mid \underline{R}_0^{n-1}) \qquad \text{(ข.2)}$$

$$\beta_n(S_n) = \frac{\Pr\{\underline{R}_n^N \mid S_n, \underline{R}_0^{n-1}\}}{\Pr\{\underline{R}_n^N \mid \underline{R}_0^{n-1}\}} \qquad \text{(ข.3)}$$

$$\gamma_n(S_n, S_{n+1}) = \Pr\{R_n, S_{n+1} \mid S_n, \underline{R}_0^{n-1}\} \qquad \text{(ข.4)}$$

แทนสมการ (ข.2) (ข.3) และ (ข.4) ลงในสมการ (ข.1) จะได้ว่า

$$\Pr\{a_n \mid \underline{R}_0^N\} = \frac{\sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1})}{\Pr\{R_n \mid \underline{R}_0^{n-1}\}} \qquad \text{(ข.5)}$$

เนื่องจาก $\sum_{a_n} \Pr\{a_n \mid \underline{R}_0^N\} = 1$ เพราะฉะนั้นจะได้ว่า

$$\Pr\{R_n \mid \underline{R}_0^{n-1}\} = \sum_{a_n} \sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1}) \qquad \text{(ข.6)}$$

จากสมการ (ข.5) และ(ข.6) จะได้ว่าค่าความน่าจะเป็นหลังมีค่าดังนี้

$$\Pr\{a_n \mid \underline{R}_0^N\} = \frac{\sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1})}{\sum_{a_n} \sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1})} \qquad \text{(ข.7)}$$

$\alpha_{n+1}(S_{n+1})$ เมื่อ $n = 1,2,...,N$ สามารถคำนวณในลักษณะรีเคอร์ซีฟได้จากสมการต่อไปนี้

$$\begin{aligned}
\alpha_{n+1}(S_{n+1}) &= \Pr\{S_{n+1} \mid \underline{R}_0^n\} \\
&= \sum_{S_n} \Pr(S_{n+1}, S_n \mid \underline{R}_0^n) \\
&= \sum_{S_n} \frac{\Pr\{R_n, S_{n+1}, S_n \mid \underline{R}_0^{n-1}\}}{\Pr\{R_n \mid \underline{R}_0^{n-1}\}} \\
&= \sum_{S_n} \Pr(S_n \mid \underline{R}_0^{n-1}) \frac{\Pr\{R_n, S_{n+1} \mid S_n, \underline{R}_0^{n-1}\}}{\Pr\{R_n \mid \underline{R}_0^{n-1}\}} \\
&= \frac{\sum_{S_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})}{\Pr\{R_n \mid \underline{R}_0^{n-1}\}}
\end{aligned} \qquad \text{(ข.8)}$$

และเนื่องจาก $\sum_{S_{n+1}} \Pr(S_{n+1} \mid \underline{R}_0^n) = 1$ ดังนั้น

$$\Pr\{R_n \mid \underline{R}_0^{n-1}\} = \sum_{S_{n+1}} \sum_{S_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1}) \qquad \text{(ข.9)}$$

แทนสมการ (ข.9) ลงในสมการ (ข.8) จะได้ว่า

$$\alpha_{n+1}(S_{n+1}) = \frac{\sum_{S_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})}{\sum_{S_{n+1}} \sum_{S_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})} \qquad \text{(ข.10)}$$

ในทำนองเดียวกัน $\beta_n(S_n)$ เมื่อ $n = N, N-1, ..., 1$ ก็สามารถคำนวณในลักษณะรีเคอร์ซีฟได้ดังนี้

$$\begin{aligned}
\beta_n(S_n) &= \frac{\Pr\{\underline{R}_n^N \mid S_n, \underline{R}_0^{n-1}\}}{\Pr\{\underline{R}_n^N \mid \underline{R}_0^{n-1}\}} \\
&= \sum_{S_{n+1}} \frac{\Pr\{\underline{R}_n^N, S_{n+1} \mid S_n, \underline{R}_0^{n-1}\}}{\Pr\{\underline{R}_n^N \mid \underline{R}_0^{n-1}\}} \\
&= \sum_{S_{n+1}} \frac{\Pr\{\underline{R}_n, S_{n+1} \mid S_n, \underline{R}_0^{n-1}\}}{\Pr\{R_n \mid \underline{R}_0^{n-1}\}} \frac{\Pr\{\underline{R}_{n+1}^N \mid S_n, S_{n+1}, \underline{R}_0^n\}}{\Pr\{\underline{R}_{n+1}^N \mid \underline{R}_0^n\}} \\
&= \frac{\sum_{S_{n+1}} \gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1})}{\Pr\{R_n \mid \underline{R}_0^{n-1}\}}
\end{aligned} \qquad \text{(ข.11)}$$

แทนสมการ (ข.9) ลงในสมการ (ข.11) จะได้ว่า

$$\beta_n(S_n) = \frac{\sum_{S_{n+1}} \gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1})}{\sum_{S_n} \sum_{S_{n+1}} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})} \qquad \text{(ข.12)}$$

สำหรับเงื่อนไขขอบเขตของสมการความสัมพันธ์ของ $\alpha_n(S_n)$ และ $\beta_n(S_n)$ คือ

$$\alpha_1(S_1 = 0) = 1$$

$$\alpha_1(S_1 \neq 0) = 0$$

และ

$$\beta_{N+1}(S_{N+1} = 0) = 1$$

$$\beta_{N+1}(S_{N+1} \neq 0) = 0$$

เงื่อนไขขอบเขตเหล่านี้พิจารณาจากกลไกการทำงานของวงจรเข้ารหัส ที่กำหนดให้ชิฟท์รีจิสเตอร์ทุกตัว เริ่มต้นและสิ้นสุดการเข้ารหัสที่สถานะเป็นศูนย์เสมอ

พิจารณาการคำนวณ $\gamma_n(S_n, S_{n+1})$

$$\begin{aligned}\gamma_n(S_n, S_{n+1}) &= \Pr\{R_n, S_{n+1} \mid S_n, \underline{R}_0^{n-1}\} \\ &= \Pr\{S_{n+1} \mid S_n, \underline{R}_0^{n-1}\}\Pr\{R_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}\} \\ &= \Pr\{S_{n+1} \mid S_n\}\Pr\{R_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}\} \qquad \text{(ข.13)}\end{aligned}$$

การเปลี่ยนรูปสมการจากบรรทัดแรกเป็นบรรทัดที่สองในสมการ (ข.13) อาศัยกฎของเบย์ (Baye's Rules) ส่วนการลดรูปพจน์ $\Pr\{S_{n+1} \mid S_n, \underline{R}_0^{n-1}\}$ มาเป็น $\Pr\{S_{n+1} \mid S_n\}$ ในบรรทัดที่สามได้เพราะอาศัยคุณสมบัติมาร์คอฟของวงจรเข้ารหัส

ถ้าการเปลี่ยนสถานะจาก S_n ไปเป็นสถานะ S_{n+1} มีความเป็นไปได้

$$\Pr\{S_{n+1} \mid S_n\} = \Pr\{a_n\} \qquad \text{(ข.14)}$$

และ

$$\begin{aligned}\Pr\{R_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}\} &= \sum_{p_n} \Pr\{R_n, p_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}\} \\ &= \sum_{p_n} \Pr\{R_n \mid S_n, S_{n+1}, p_n, \underline{R}_0^{n-1}\}\Pr\{p_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}\} \\ &= \sum_{p_n} \Pr\{R_n \mid a_n, p_n, \underline{R}_0^{n-1}\}\Pr\{p_n \mid S_n, S_{n+1}\} \qquad \text{(ข.15)}\end{aligned}$$

พจน์ $\Pr\{R_n \mid a_n, p_n, \underline{R}_0^{n-1}\}$ ก็คือ เมตริกทุติยภูมิ $\Gamma_n(I_n)$ เมื่อ I_n แทนคู่บิต (a_n, p_n) เพราะฉะนั้นจะได้ว่า

$$\gamma_n(S_n, S_{n+1}) = \Pr\{a_n\}\sum_{p_n}\Gamma_n(a_n, p_n)\Pr\{p_n \mid S_n, S_{n+1}\} \qquad \text{(ข.16)}$$

2. การคำนวณข่าวสารเอ็กซ์ทรินซิก

2.1 ข่าวสารเอ็กซ์ทรินซิกของบิตข้อมูล a_n คำนวณได้จากสมการต่อไปนี้

$$V_n(a_n) = \frac{\Pr\{a_n \mid \underline{R}_0^N\}}{\Pr\{a_n\} \bullet \frac{1}{2}\sum_{p_n} \Gamma_n(a_n, p_n)} \qquad \text{(ข.17)}$$

จากสมการ (ข.5) และ (ข.16) จะได้ว่าค่า $\Pr\{a_n \mid \underline{R}_0^N\}$ มีค่าเท่ากับ

$$\Pr\{a_n \mid \underline{R}_0^N\} = \frac{\sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\left(\Pr\{a_n\}\sum_{p_n}\Gamma_n(a_n, p_n)\Pr\{p_n \mid S_n, S_{n+1}\}\right)\beta_{n+1}(S_{n+1})}{\Pr\{R_n \mid \underline{R}_0^{n-1}\}} \qquad \text{(ข.18)}$$

ดังนั้นจะได้ว่า

$$V_n(a_n) = \frac{\sum_{(S_n, S_{n+1}):a_n} \frac{\sum_{p_n}\Gamma_n(a_n, p_n)\Pr\{p_n \mid S_n, S_{n+1}\}}{\frac{1}{2}\sum_{p_n}\Gamma_n(a_n, p_n)} \alpha_n(S_n)\beta_{n+1}(S_{n+1})}{\Pr\{R_n \mid \underline{R}_0^{n-1}\}} \qquad \text{(ข.19)}$$

เนื่องจาก $V_n(a_n)$ เป็นค่าที่จะใช้แทนข่าวสารเบื้องแรก $\Pr\{a_n\}$ ของเครื่องถอดรหัสย่อยตัวถัดไป ดังนั้นจำเป็นจะต้อง normalize ให้ $\sum_{a_n} V_n(a_n) = 1$ ซึ่งจะทำให้ $V_n(a_n)$ ในสมการ (ข.19) มีค่าเป็น

$$V_n(a_n) = \frac{\sum_{(S_n, S_{n+1}):a_n} \frac{\sum_{p_n}\Gamma_n(a_n, p_n)\Pr\{p_n \mid S_n, S_{n+1}\}}{\sum_{p_n}\Gamma_n(a_n, p_n)} \alpha_n(S_n)\beta_{n+1}(S_{n+1})}{\sum_{a_n}\sum_{(S_n, S_{n+1}):a_n} \frac{\sum_{p_n}\Gamma_n(a_n, p_n)\Pr\{p_n \mid S_n, S_{n+1}\}}{\sum_{p_n}\Gamma_n(a_n, p_n)} \alpha_n(S_n)\beta_{n+1}(S_{n+1})} \qquad \text{(ข.20)}$$

2.2 ข่าวสารเอ็กซ์ทรินซิกของสัญลักษณ์ I_n นิยามได้ดังนี้

$$W_n(I_n) = W_n(a_n, p_n) = \frac{\Pr\{a_n, p_n \mid \underline{R}_0^N\}}{\Pr\{a_n\}\Gamma_n(a_n, p_n)} \qquad \text{(ข.21)}$$

โดยที่

$$\Pr\{a_n, p_n \mid \underline{R}_0^N\} = \sum_{(S_n, S_{n+1}):a_n} \Pr\{S_n, S_{n+1}, p_n \mid \underline{R}_0^N\}$$

$$= \sum_{(S_n, S_{n+1}):a_n} \frac{\Pr\{\underline{R}_n^N, S_n, S_{n+1}, p_n \mid \underline{R}_0^{n-1}\}}{\Pr\{\underline{R}_n^N \mid \underline{R}_0^{n-1}\}}$$

$$= \sum_{(S_n, S_{n+1}):a_n} \frac{\Pr\{R_n, S_n, S_{n+1}, p_n \mid \underline{R}_0^{n-1}\}}{\Pr\{R_n \mid \underline{R}_0^{n-1}\}} \frac{\Pr\{\underline{R}_{n+1}^N \mid S_n, S_{n+1}, p_n, \underline{R}_0^n\}}{\Pr\{\underline{R}_{n+1}^N \mid \underline{R}_0^n\}}$$

$$= \sum_{(S_n, S_{n+1}):a_n} \frac{\Pr\{S_n \mid \underline{R}_0^{n-1}\}\Pr\{S_{n+1} \mid S_n, \underline{R}_0^{n-1}\}\Pr\{p_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}\}\Pr\{R_n \mid S_n, S_{n+1}, p_n, \underline{R}_0^{n-1}\}}{\Pr\{R_n \mid \underline{R}_0^{n-1}\}} \times \frac{\Pr\{\underline{R}_{n+1}^N \mid S_n, S_{n+1}, p_n, \underline{R}_0^n\}}{\Pr\{\underline{R}_{n+1}^N \mid \underline{R}_0^n\}}$$

$$= \sum_{(S_n, S_{n+1}):a_n} \frac{\Pr\{S_n \mid \underline{R}_0^{n-1}\}\Pr\{S_{n+1} \mid S_n\}\Pr\{p_n \mid S_n, S_{n+1}\}\Pr\{R_n \mid S_n, S_{n+1}, p_n\}}{\Pr\{R_n \mid \underline{R}_0^{n-1}\}} \times \frac{\Pr\{\underline{R}_{n+1}^N \mid S_n, S_{n+1}, p_n, \underline{R}_0^n\}}{\Pr\{\underline{R}_{n+1}^N \mid \underline{R}_0^n\}}$$

$$= \frac{\sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\Pr\{a_n\}\Pr\{p_n \mid S_n, S_{n+1}\}\Gamma_n(a_n, p_n)\beta_{n+1}(S_{n+1})}{\Pr\{R_n \mid \underline{R}_0^{n-1}\}} \qquad \text{(ข.22)}$$

ดังนั้น $W_n(a_n, p_n)$ ที่ normalize แล้วจะมีค่าเท่ากับ

$$W_n(a_n, p_n) = \frac{\sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\beta_{n+1}(S_{n+1})\Pr\{p_n \mid S_n, S_{n+1}\}}{\sum_{a_n}\sum_{p_n}\sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\beta_{n+1}(S_{n+1})\Pr\{p_n \mid S_n, S_{n+1}\}} \qquad \text{(ข.23)}$$

ภาคผนวก ค
การวิเคราะห์เครื่องถอดรหัสย่อยที่เสนอ

1. การคำนวณค่าความน่าจะเป็นหลัง

1.1 ความน่าจะเป็นหลังของบิตข้อมูล a_n มีขั้นตอนในการคำนวณดังนี้

$$
\begin{aligned}
\Pr\{a_n \mid \underline{R}_0^N, \underline{\widetilde{R}}_0^N\} &= \sum_{(S_n, S_{n+1}):a_n} \Pr\{S_n, S_{n+1} \mid \underline{R}_0^N, \underline{\widetilde{R}}_0^N\} \\
&= \sum_{(S_n, S_{n+1}):a_n} \frac{\Pr\{\underline{R}_n^N, \underline{\widetilde{R}}_n^N, S_n, S_{n+1} \mid \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\}}{\Pr\{\underline{R}_n^N, \underline{\widetilde{R}}_n^N \mid \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\}} \\
&= \sum_{(S_n, S_{n+1}):a_n} \Pr\{S_n \mid \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\} \frac{\Pr\{\underline{R}_n^N, \underline{\widetilde{R}}_n^N, S_{n+1} \mid S_n, \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\}}{\Pr\{\underline{R}_n^N, \underline{\widetilde{R}}_n^N \mid \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\}} \\
&= \sum_{(S_n, S_{n+1}):a_n} \Pr\{S_n \mid \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\} \frac{\Pr\{\underline{R}_n, \underline{\widetilde{R}}_n, S_{n+1} \mid S_n, \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\}}{\Pr\{\underline{R}_n, \underline{\widetilde{R}}_n \mid \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\}} \\
&\qquad \times \frac{\Pr\{\underline{R}_{n+1}^N, \underline{\widetilde{R}}_{n+1}^N \mid S_{n+1}, S_n, \underline{R}_0^n, \underline{\widetilde{R}}_0^n\}}{\Pr\{\underline{R}_{n+1}^N, \underline{\widetilde{R}}_{n+1}^N \mid \underline{R}_0^n, \underline{\widetilde{R}}_0^n\}} \\
&= \sum_{(S_n, S_{n+1}):a_n} \Pr\{S_n \mid \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\} \frac{\Pr\{\underline{R}_n, \underline{\widetilde{R}}_n, S_{n+1} \mid S_n, \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\}}{\Pr\{\underline{R}_n, \underline{\widetilde{R}}_n \mid \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\}} \\
&\qquad \times \frac{\Pr\{\underline{R}_{n+1}^N, \underline{\widetilde{R}}_{n+1}^N \mid S_{n+1}, \underline{R}_0^n, \underline{\widetilde{R}}_0^n\}}{\Pr\{\underline{R}_{n+1}^N, \underline{\widetilde{R}}_{n+1}^N \mid \underline{R}_0^n, \underline{\widetilde{R}}_0^n\}}
\end{aligned}
\qquad \text{(ค.1)}
$$

การลดรูป $\Pr\{\underline{R}_{n+1}^N, \underline{\widetilde{R}}_{n+1}^N \mid S_{n+1}, S_n, \underline{R}_0^n, \underline{\widetilde{R}}_0^n\}$ มาเป็น $\Pr\{\underline{R}_{n+1}^N, \underline{\widetilde{R}}_{n+1}^N \mid S_{n+1}, \underline{R}_0^n, \underline{\widetilde{R}}_0^n\}$ อาศัยคุณสมบัติมาร์คอฟของวงจรเข้ารหัส

กำหนดให้

$$\alpha_n(S_n) = \Pr(S_n \mid \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}) \qquad \text{(ค.2)}$$

$$\beta_n(S_n) = \frac{\Pr\{\underline{R}_n^N, \underline{\tilde{R}}_n^N \mid S_n, \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}\}}{\Pr\{\underline{R}_n^N, \underline{\tilde{R}}_n^N \mid \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}\}} \quad (ค.3)$$

และ

$$\gamma_n(S_n, S_{n+1}) = \Pr\{R_n, \tilde{R}_n, S_{n+1} \mid S_n, \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}\} \quad (ค.4)$$

แทนสมการ (ค.2) (ค.3) และ (ค.4) ลงในสมการ (ค.1) จะได้ว่า

$$\Pr\{a_n \mid \underline{R}_0^N, \underline{\tilde{R}}_0^N\} = \frac{\sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1})}{\Pr\{\underline{R}_n^N, \underline{\tilde{R}}_n^N \mid \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}\}} \quad (ค.5)$$

เนื่องจาก $\sum_{a_n} \Pr\{a_n \mid \underline{R}_0^N, \underline{\tilde{R}}_0^N\} = 1$ เพราะฉะนั้นจะได้ว่า

$$\Pr\{\underline{R}_n^N, \underline{\tilde{R}}_n^N \mid \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}\} = \sum_{a_n} \sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1}) \quad (ค.6)$$

และค่าความน่าจะเป็นหลังของบิตข้อมูล a_n จะมีค่าดังนี้

$$\Pr\{a_n \mid \underline{R}_0^N, \underline{\tilde{R}}_0^N\} = \frac{\sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1})}{\sum_{a_n} \sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1})} \quad (ค.7)$$

$\alpha_n(S_n)$ และ $\beta_n(S_n)$ สามารถคำนวณในลักษณะรีเคอร์ซีฟได้ดังนี้

$$\begin{aligned}
\alpha_{n+1}(S_{n+1}) &= \Pr(S_{n+1} \mid \underline{R}_0^n, \underline{\tilde{R}}_0^n) \\
&= \sum_{S_n} \Pr(S_{n+1}, S_n \mid \underline{R}_0^n, \underline{\tilde{R}}_0^n) \\
&= \sum_{S_n} \frac{\Pr\{R_n, \tilde{R}_n, S_n, S_{n+1} \mid \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}\}}{\Pr\{R_n, \tilde{R}_n \mid \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}\}} \\
&= \sum_{S_n} \Pr(S_n \mid \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}) \frac{\Pr\{R_n, \tilde{R}_n, S_{n+1} \mid S_n, \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}\}}{\Pr\{R_n, \tilde{R}_n \mid \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}\}}
\end{aligned}$$

$$= \frac{\sum_{S_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})}{\Pr\{R_n, \tilde{R}_n \mid \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}\}} \qquad \text{(ค.8)}$$

และเนื่องจาก $\sum_{S_{n+1}} \Pr(S_{n+1} \mid \underline{R}_0^n, \underline{\tilde{R}}_0^n) = 1$ ดังนั้น

$$\Pr\{R_n, \tilde{R}_n \mid \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}\} = \sum_{S_{n+1}} \sum_{S_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1}) \qquad \text{(ค.9)}$$

แทนสมการ (ค.9) ลงในสมการ (ค.8) จะได้ว่า

$$\alpha_{n+1}(S_{n+1}) = \frac{\sum_{S_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})}{\sum_{S_{n+1}} \sum_{S_n} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})} \qquad \text{(ค.10)}$$

ในทำนองเดียวกัน $\beta_n(S_n)$ เมื่อ $n = N, N-1, ..., 1$ ก็สามารถคำนวณในลักษณะรีเคอร์ซีฟได้ดังนี้

$$\beta_n(S_n) = \frac{\Pr\{\underline{R}_n^N, \underline{\tilde{R}}_n^N \mid S_n, \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}\}}{\Pr\{\underline{R}_n^N, \underline{\tilde{R}}_n^N \mid \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}\}}$$

$$= \sum_{S_{n+1}} \frac{\Pr\{\underline{R}_n^N, \underline{\tilde{R}}_n^N, S_{n+1} \mid S_n, \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}\}}{\Pr\{\underline{R}_n^N, \underline{\tilde{R}}_n^N \mid \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}\}}$$

$$= \sum_{S_{n+1}} \frac{\Pr\{R_n, \tilde{R}_n, S_{n+1} \mid S_n, \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}\}}{\Pr\{R_n, \tilde{R}_n \mid \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}\}} \frac{\Pr\{\underline{R}_{n+1}^N, \underline{\tilde{R}}_{n+1}^N \mid S_n, S_{n+1}, \underline{R}_0^n, \underline{\tilde{R}}_0^n\}}{\Pr\{\underline{R}_{n+1}^N, \underline{\tilde{R}}_{n+1}^N \mid \underline{R}_0^n, \underline{\tilde{R}}_0^n\}}$$

$$= \frac{\sum_{S_{n+1}} \gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1})}{\Pr\{R_n, \tilde{R}_n \mid \underline{R}_0^{n-1}, \underline{\tilde{R}}_0^{n-1}\}} \qquad \text{(ค.11)}$$

แทนสมการ (ค.9) ลงในสมการ (ค.11) จะได้ว่า

$$\beta_n(S_n) = \frac{\sum_{S_{n+1}} \gamma_n(S_n, S_{n+1})\beta_{n+1}(S_{n+1})}{\sum_{S_n} \sum_{S_{n+1}} \alpha_n(S_n)\gamma_n(S_n, S_{n+1})} \qquad \text{(ค.12)}$$

ค่า $\gamma_n(S_n, S_{n+1})$ คำนวณได้จากสมการต่อไปนี้

$$\begin{aligned}
\gamma_n(S_n, S_{n+1}) &= \Pr\{R_n, \widetilde{R}_n, S_{n+1} \mid S_n, \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\} \\
&= \Pr\{S_{n+1} \mid S_n, \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\} \Pr\{R_n, \widetilde{R}_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\} \\
&= \Pr\{S_{n+1} \mid S_n\} \Pr\{R_n, \widetilde{R}_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\} \\
&= \Pr\{S_{n+1} \mid S_n\} \Pr\{R_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\} \Pr\{\underline{\widetilde{R}}_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\} \\
&= \Pr\{S_{n+1} \mid S_n\} \Pr\{R_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}\} \Pr\{\underline{\widetilde{R}}_n \mid S_n, S_{n+1}, \underline{\widetilde{R}}_0^{n-1}\} \qquad \text{(ค.13)}
\end{aligned}$$

การลดรูปสมการจากบรรทัดที่สองเป็นบรรทัดที่สามในสมการ (ค.13) อาศัยคุณสมบัติมาร์คอฟของวงจรเข้ารหัส และการที่พจน์ $\Pr\{R_n, \widetilde{R}_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\}$ ในบรรทัดที่สามสามารถแยกออกเป็นผลคูณของพจน์ $\Pr\{R_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\}$ กับพจน์ $\Pr\{\underline{\widetilde{R}}_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}, \underline{\widetilde{R}}_0^{n-1}\}$ ในบรรทัดที่สี่ได้ เนื่องจากสัญลักษณ์ที่รับได้ R_n และ $\widetilde{R}_n$ เป็นอิสระต่อกัน นอกจากนี้ R_n ยังเป็นอิสระกับ $\underline{\widetilde{R}}_0^{n-1}$ และ $\widetilde{R}_n$ ก็เป็นอิสระกับ $\underline{R}_0^{n-1}$ อีกด้วย เพราะฉะนั้นสมการในบรรทัดที่สี่จึงลดรูปลงมาเป็นสมการในบรรทัดที่ห้า

ถ้าการเปลี่ยนสถานะของเครื่องเข้ารหัสย่อยจาก S_n เป็น S_{n+1} มีความเป็นไปได้ จะได้ว่า

$$\Pr\{S_{n+1} \mid S_n\} = \Pr\{a_n\} \qquad \text{(ค.14)}$$

ส่วนพจน์ที่เหลือทางขวามือของสมการ (ค.13) คำนวณได้ดังนี้

$$\begin{aligned}
\Pr\{R_n \mid S_n, S_{n+1}, \underline{R}_0^{n-1}\} &= \sum_{p_n'} \Pr\{R_n, p_n' \mid S_n, S_{n+1}, \underline{R}_0^{n-1}\} \\
&= \sum_{p_n'} \Pr\{R_n \mid S_n, S_{n+1}, p_n', \underline{R}_0^{n-1}\} \Pr\{p_n' \mid S_n, S_{n+1}, \underline{R}_0^{n-1}\} \\
&= \sum_{p_n'} \Pr\{R_n \mid a_n, p_n', \underline{R}_0^{n-1}\} \Pr\{p_n'\} \\
&= \sum_{p_n'} \Gamma_n(a_n, p_n') \Pr\{p_n'\} \qquad \text{(ค.15)}
\end{aligned}$$

และ

$$\Pr\{\tilde{R}_n \mid S_n, S_{n+1}, \underline{\tilde{R}}_0^{n-1}\} = \sum_{a_n'} \Pr\{\tilde{R}_n, a_n' \mid S_n, S_{n+1}, \underline{\tilde{R}}_0^{n-1}\}$$

$$= \sum_{a_n'} \Pr\{\tilde{R}_n \mid a_n', S_n, S_{n+1}, \underline{\tilde{R}}_0^{n-1}\} \Pr\{a_n' \mid S_n, S_{n+1}, \underline{\tilde{R}}_0^{n-1}\}$$

$$= \sum_{a_n'} \Pr\{\tilde{R}_n \mid a_n', p_n, \underline{\tilde{R}}_0^{n-1}\} \Pr\{a_n'\}$$

$$= \sum_{a_n'} \tilde{\Gamma}_n(a_n', p_n) \Pr\{a_n'\} \qquad \text{(ค.16)}$$

แทนสมการ (ค.14) ถึง (ค.16) ลงในสมการ (ค.13) จะได้ว่า

$$\gamma_n(S_n, S_{n+1}) = \Pr\{a_n\} \left(\sum_{p_n'} \Gamma_n(a_n, p_n') \Pr\{p_n'\} \right) \left(\sum_{a_n'} \tilde{\Gamma}_n(a_n', p_n) \Pr\{a_n'\} \right) \qquad \text{(ค.17)}$$

1.2 ความน่าจะเป็นหลังของบิตรหัส p_n นิยามได้ดังนี้

$$\Pr\{p_n \mid \underline{R}_0^N, \underline{\tilde{R}}_0^N\} = \sum_{(S_n, S_{n+1}):p_n} \Pr\{S_n, S_{n+1} \mid \underline{R}_0^N, \underline{\tilde{R}}_0^N\} \qquad \text{(ค.18)}$$

วิธีการคำนวณ $\Pr\{p_n \mid \underline{R}_0^N, \underline{\tilde{R}}_0^N\}$ จะคล้ายกับการคำนวณ $\Pr\{a_n \mid \underline{R}_0^N, \underline{\tilde{R}}_0^N\}$ ที่ได้แสดงไปแล้ว ดังนั้นความน่าจะเป็นหลังของบิตรหัส p_n จึงมีค่าเท่ากับ

$$\Pr\{p_n \mid \underline{R}_0^N, \underline{\tilde{R}}_0^N\} = \frac{\sum_{(S_n, S_{n+1}):p_n} \alpha_n(S_n) \gamma_n(S_n, S_{n+1}) \beta_{n+1}(S_{n+1})}{\sum_{p_n} \sum_{(S_n, S_{n+1}):p_n} \alpha_n(S_n) \gamma_n(S_n, S_{n+1}) \beta_{n+1}(S_{n+1})} \qquad \text{(ค.19)}$$

2. การคำนวณข่าวสารเอ็กซ์ทรินซิก

2.1 ข่าวสารเอ็กซ์ทรินซิกของบิตข้อมูล a_n มีค่าดังนี้

$$V_n(a_n) = \frac{\Pr\{a_n \mid \underline{R}_0^N, \underline{\widetilde{R}}_0^N\}}{\Pr\{a_n\}\left(\sum_{p_n'} \Gamma_n(a_n, p_n')\Pr\{p_n'\}\right)} \qquad \text{(ค.20)}$$

จากสมการ (ค.7) และ (ค.17) จะได้ว่าค่า $\Pr\{a_n \mid \underline{R}_0^N, \underline{\widetilde{R}}_0^N\}$ มีค่าเท่ากับ

$$\Pr\{a_n \mid \underline{R}_0^N, \underline{\widetilde{R}}_0^N\} = \frac{\sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\left[\Pr\{a_n\}\left(\sum_{p_n'} \Gamma_n(a_n, p_n')\Pr\{p_n'\}\right)\left(\sum_{a_n'} \tilde{\Gamma}_n(a_n', p_n)\Pr\{a_n'\}\right)\right]\beta_{n+1}(S_{n+1})}{\sum_{a_n}\sum_{(S_n, S_{n+1}):a_n} \alpha_n(S_n)\left[\Pr\{a_n\}\left(\sum_{p_n'} \Gamma_n(a_n, p_n')\Pr\{p_n'\}\right)\left(\sum_{a_n'} \tilde{\Gamma}_n(a_n', p_n)\Pr\{a_n'\}\right)\right]\beta_{n+1}(S_{n+1})} \qquad \text{(ค.21)}$$

เพราะฉะนั้นข่าวสารเอ็กซ์ทรินซิกของบิตข้อมูล a_n จะมีค่าเท่ากับ

$$V_n(a_n) = \frac{\sum_{(S_n, S_{n+1}):a_n}\left(\sum_{a_n'} \tilde{\Gamma}_n(a_n', p_n)\Pr\{a_n'\}\right)\alpha_n(S_n)\beta_{n+1}(S_{n+1})}{\sum_{a_n}\sum_{(S_n, S_{n+1}):a_n}\left(\sum_{a_n'} \tilde{\Gamma}_n(a_n', p_n)\Pr\{a_n'\}\right)\alpha_n(S_n)\beta_{n+1}(S_{n+1})} \qquad \text{(ค.22)}$$

2.2 ข่าวสารเอ็กซ์ทรินซิกของบิตรหัส p_n มีค่าดังนี้

$$V_n(p_n) = \frac{\Pr\{p_n \mid \underline{R}_0^N, \underline{\widetilde{R}}_0^N\}}{\left(\sum_{a_n'} \tilde{\Gamma}_n(a_n', p_n)\Pr\{a_n'\}\right)} \qquad \text{(ค.23)}$$

จากสมการ (ค.17) และ (ค.19) จะได้ว่า

$$\Pr\{p_n \mid \underline{R}_0^N, \underline{\tilde{R}}_0^N\} = \frac{\sum_{(S_n, S_{n+1}):p_n} \alpha_n(S_n)\left[\Pr\{a_n\}\left(\sum_{p_n'}\Gamma_n(a_n, p_n')\Pr\{p_n'\}\right)\left(\sum_{a_n'}\tilde{\Gamma}_n(a_n', p_n)\Pr\{a_n'\}\right)\right]\beta_{n+1}(S_{n+1})}{\sum_{p_n}\sum_{(S_n, S_{n+1}):p_n} \alpha_n(S_n)\left[\Pr\{a_n\}\left(\sum_{p_n'}\Gamma_n(a_n, p_n')\Pr\{p_n'\}\right)\left(\sum_{a_n'}\tilde{\Gamma}_n(a_n', p_n)\Pr\{a_n'\}\right)\right]\beta_{n+1}(S_{n+1})}$$

(ค.24)

ดังนั้นข่าวสารเอ็กซ์ทรินซิกของบิตรหัส p_n จะมีค่าเท่ากับ

$$V_n(p_n) = \frac{\sum_{(S_n, S_{n+1}):p_n} \Pr\{a_n\}\left(\sum_{p_n'}\Gamma_n(a_n, p_n')\Pr\{p_n'\}\right)\alpha_n(S_n)\beta_{n+1}(S_{n+1})}{\sum_{p_n}\sum_{(S_n, S_{n+1}):p_n} \Pr\{a_n\}\left(\sum_{p_n'}\Gamma_n(a_n, p_n')\Pr\{p_n'\}\right)\alpha_n(S_n)\beta_{n+1}(S_{n+1})} \quad \text{(ค.25)}$$

2.3 ข่าวสารเอ็กซ์ทรินซิกของสัญลักษณ์ I_n คำนวณได้ดังนี้

$$W_n(I_n) \;=\; W_n(a_n, p_n') \;=\; V_n(a_n)\cdot V_n(p_n') \quad \text{(ค.26)}$$

เมื่อ $V_n(a_n)$ คำนวณได้จากสมการ (ค.22) และ $V_n(p_n')$ คือ $V_n(p_n)$ ที่ถูกสลับลำดับด้วยตัวสลับลำดับบิตรหัส ซึ่ง $V_n(p_n)$ คำนวณได้จากสมการ (ค.25)

ประวัติผู้เขียนวิทยานิพนธ์

นางสาวจันทิมา ศรีเตียเพ็ชร เกิดเมื่อวันที่ 19 มิถุนายน พ.ศ. 2522 ที่กรุงเทพมหานคร เข้ารับการศึกษาในหลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์ ในปีการศึกษา 2539 และเข้าศึกษาต่อในหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2543