



รายงานฉบับสมบูรณ์

Final Report

รหัสโปรดักต์โดยใช้โครงสร้างรหัสบล็อกเทอร์โบสำหรับช่องสัญญาณซินทิเลชัน

Product Codes: Block Turbo Codes for Scintillation Channel

- รศ. นิภา ตีลาจจิ
- รศ. ณรงค์ เหมกรณ์
- ผศ.ดร. พรชัย ทรัพย์นิต
- ผศ.ดร. สุทธิชัย นพนาดีพงษ์
- นาย อำนาจ ขาวเน
- นาย กุสิทธิ์ สุวรรณแสง

ห้องปฏิบัติการวิจัย การสื่อสารดาวเทียม
 โครงการสำนักวิจัยการสื่อสารและเทคโนโลยีสารสนเทศ
 สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
 กันยายน พ.ศ. 2549

Satellite Communication Laboratory
 Research Center for Communications and Information Technology
 King Mongkut's Institute of Technology Ladkrabang
 September 2006

RCH
 TK
 ๕๐๒.๑๒
 ๖๑๗๑

เลขหมู่.....
 เลขทะเบียน..... 83637
 วัน,เดือน,ปี..... 1๐ ก.ย. 2551

b. ๖๑๗๑๖๕
 i.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
 ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กิตติกรรมประกาศ

โครงการวิจัยนี้ได้รับทุนอุดหนุนจาก โครงการสำนักวิจัยการสื่อสารและเทคโนโลยีสารสนเทศ (Research Center for Communications and Information Technology : ReCCIT) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ประจำปีงบประมาณ พ.ศ. 2549 วงเงินงบประมาณ 55,171 บาท และขอขอบพระคุณอาจารย์ที่ปรึกษาและอาจารย์ประจำห้องปฏิบัติการวิจัยทุกท่านที่คอยให้คำปรึกษาและคำแนะนำในการทำงานวิจัยชิ้นนี้



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทสรุปย่อ

ในโครงการวิจัยนี้จะพูดถึงปัญหาที่เกิดจากการเปลี่ยนแปลงแอมพลิจูดอย่างกะทันหัน (Amplitude Scintillation) โดยผลกระทบของปรากฏการณ์นี้จะส่งผลให้ระดับกำลังงานของสัญญาณที่รับได้เพิ่มขึ้นและลดลงอย่างรวดเร็วซึ่งส่งผลเสียต่อระบบการสื่อสารทั้งทางด้านความถูกต้องของข้อมูล หรือทำให้เกิดการเสียหายแก่ระบบและอุปกรณ์ที่สถานีภาคพื้นดินในกรณีที่เกิดการเปลี่ยนแปลงอย่างรุนแรงขึ้นในงานวิจัยนี้พยายามจะลดปัญหาที่เกิดขึ้นนี้ โดยใช้รหัสบล็อกเทอร์โบในการลดอัตราบิดผิดพลาดของข้อมูลและปรับปรุงสมรรถนะของระบบให้ดีขึ้น

โครงการวิจัยนี้ได้แบ่งขั้นตอนการดำเนินการออกเป็น 7 ขั้นตอน

1. ศึกษาโครงสร้างรหัสบล็อกเทอร์โบ
2. ศึกษาการเข้ารหัส/ถอดรหัส BCH
3. ศึกษาการเข้ารหัส/ถอดรหัส SISO
4. ศึกษาช่องสัญญาณซินทิเลชัน
5. ทำการจำลองแบบระบบผ่านช่องสัญญาณ AWGN
6. ทำการจำลองแบบระบบผ่านช่องสัญญาณซินทิเลชัน
7. สรุปและเขียนบทความวิจัย

บทคัดย่อ

บทความนี้นำเสนอหลักการเข้ารหัสและถอดรหัสโพรค ในช่องสัญญาณแบบเกาส์ โดยใช้หลักการถอดรหัสแบบฮาร์ด ทำการถอดรหัสในลักษณะของแถวและหลัก เพื่อศึกษาสมรรถนะของระบบ โดยทำการเปรียบเทียบสมรรถนะของระบบที่เข้ารหัสแตกต่างกันและเข้ารหัสที่มีความยาวเข้ารหัสเท่ากันแต่อัตราหัสต่างกัน ในบทความนี้ได้เพิ่มในส่วนของการถอดรหัสแบบวนซ้ำในส่วนของภาคถอดรหัสซึ่งผลที่ได้จากการจำลองแบบคือ การรหัสที่มีอัตราหัสสูงจะให้ค่าสมรรถนะที่สูงกว่าการรหัสที่มีอัตราหัสต่ำ

Abstract

This paper presents a study encoding and decoding of product codes in the additive white gaussian channel by using the hard decoder to decode rows and columns. The performance of the system is investigated by comparing different codes and different code rates. In this paper, the iterative decoding is added in the decoding part to achieve power bit error rate.

สารบัญ

	หน้า
กิตติกรรมประกาศ	I
บทสรุปย่อ	II
บทคัดย่อ	III
บทที่ 1 บทนำ	1
1.1 บทนำและความเป็นมา	1
1.2 ความมุ่งหมายและวัตถุประสงค์	1
1.3 รายละเอียดของโครงการขอบเขตของการศึกษา	2
บทที่ 2 ทฤษฎีที่เกี่ยวข้อง	3
2.1 การเปลี่ยนแปลงแอมพลิจูดอย่างกะทันหัน	3
2.2 รหัส BCH	8
2.3 การถอดรหัส BCH	10
2.4 ช่องสัญญาณที่มีการรบกวนแบบบวก(additive noise channel)	15
บทที่ 3 การออกแบบระบบ	17
บทที่ 4 ผลการจำลองแบบ	20
บทที่ 5 ข้อวิจารณ์	22
บทที่ 6 บทสรุปและข้อเสนอแนะ	23
เอกสารอ้างอิง	24

บทที่ 1

บทนำ

1.1 บทนำและความเป็นมา

ในปัจจุบันเทคโนโลยีทางด้านดาวเทียมเติบโตขึ้นอย่างรวดเร็วเพื่อตอบสนองความต้องการใช้งานที่เพิ่มขึ้นทั้งในด้านการสื่อสารทั่วไปไม่ว่าจะเป็นการส่งสัญญาณภาพและเสียงหรือการให้บริการอินเทอร์เน็ตผ่านดาวเทียม แม้กระทั่งใช้งานทางการทหารซึ่งการพิจารณาความถี่ที่เหมาะสมต่อการใช้งานนั้นอาจประกอบจากหลายปัจจัย เช่น ขนาดของข้อมูล ความเร็วในการส่งข้อมูล รวมไปถึงความถูกต้องของข้อมูล ซึ่งการใช้งานในแต่ละความถี่ก็มีปัญหาที่แตกต่างกัน อย่างเช่นสัญญาณดาวเทียมที่ใช้ความถี่สูง(Ku-Band หรือ Ka-Band) นั้นจะเกิดปัญหาจากการลดทอนของสัญญาณในขณะที่ฝนตก(Rain Attenuation) ผ่านเส้นทางการแพร่กระจายคลื่น ส่วนสัญญาณดาวเทียมที่ใช้ความถี่ต่ำจะได้รับผลกระทบจากชั้นบรรยากาศไอโอโนสเฟียร์(Ionosphere) ซึ่งทำให้เกิดปัญหาหลายรูปแบบเช่น ความคลาดเคลื่อนของการบอกตำแหน่งในระบบนำร่อง(Navigation Satellites) หรือการแทรกสอด(Interference) ของสัญญาณวิทยุภาคพื้นดิน ในรายงานฉบับนี้จะพูดถึงปัญหาที่เกิดจากการเปลี่ยนแปลงแอมพลิจูดอย่างกะทันหัน(Amplitude Scintillation) โดยผลกระทบของปรากฏการณ์นี้จะส่งผลให้ระดับกำลังงานของสัญญาณที่รับได้เพิ่มขึ้นและลดลงอย่างรวดเร็วซึ่งส่งผลเสียต่อระบบการสื่อสารทั้งทางด้านความถูกต้องของข้อมูล หรือทำให้เกิดการเสียหายแก่ระบบและอุปกรณ์ที่สถานีภาคพื้นดิน ในกรณีที่เกิดการเปลี่ยนแปลงอย่างรุนแรงขึ้นในงานวิจัยนี้พยายามจะลดปัญหาที่เกิดขึ้นนี้โดยใช้รหัสบล็อกเทอร์โบเข้ามาแก้ปัญหาในส่วนของภาคส่งและภาครับของสัญญาณดาวเทียมโดยทำการเข้ารหัสบล็อกเทอร์โบที่ภาคส่งและทำการถอดรหัสในส่วนของภาครับเพื่อลดปัญหาการเกิดอัตราบิดผิดพลาดของข้อมูลและปรับปรุงสมรรถนะของระบบให้ดีขึ้น

1.2 ความมุ่งหมายและวัตถุประสงค์

ในการทำวิจัยหัวข้อรหัสโพรคโดยใช้โครงสร้างรหัสบล็อกเทอร์โบสำหรับช่องสัญญาณซินทิเลชันวัตถุประสงค์เพื่อ

1. ศึกษาปัญหาที่เกิดจากการเปลี่ยนแปลงแอมพลิจูดอย่างกะทันหัน(Amplitude Scintillation)
2. ศึกษาโครงสร้างการเข้ารหัสและถอดรหัสของรหัสบล็อกเทอร์โบ
3. ศึกษาวิธีการในการแก้ปัญหาสัญญาณรบกวนที่เกิดจากซินทิเลชัน

1.3 รายละเอียดของโครงการขอบเขตของการศึกษา

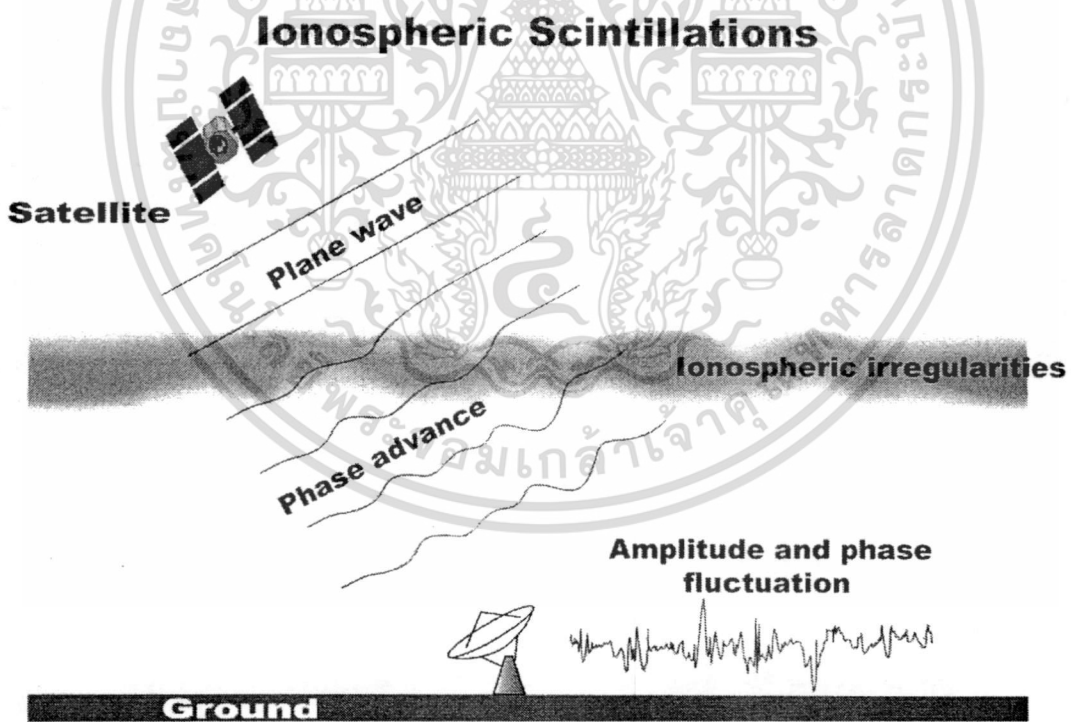
- ในรายงานฉบับนี้จะแบ่งออกเป็น 7 ส่วน โดยมีรายละเอียดของแต่ละส่วนดังนี้
- ส่วนที่ 1 บทนำและความเป็นมา ความมุ่งหมายและวัตถุประสงค์
 - ส่วนที่ 2 ทฤษฎีที่เกี่ยวข้อง การเปลี่ยนแปลงแอมพลิจูดอย่างกะทันหัน, รหัส BCH
 - ส่วนที่ 3 การออกแบบระบบ
 - ส่วนที่ 4 ผลการจำลองแบบ
 - ส่วนที่ 5 ข้อวิจารณ์
 - ส่วนที่ 6 สรุปและข้อเสนอแนะ
 - ส่วนที่ 7 เอกสารอ้างอิง



บทที่ 2 ทฤษฎีที่เกี่ยวข้อง

2.1 การเปลี่ยนแปลงแอมพลิจูดอย่างกะทันหัน

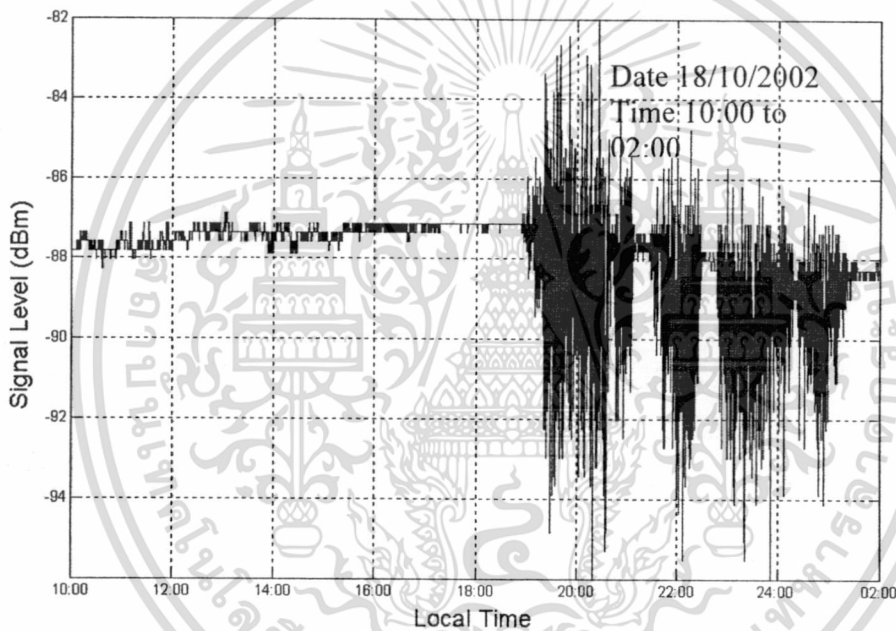
การเปลี่ยนแปลงระดับกำลังงานของสัญญาณดาวเทียมในช่วงเวลาที่เกิดปรากฏการณ์นี้ เรียกว่า การเปลี่ยนแปลงแอมพลิจูดอย่างกะทันหัน (Amplitude Scintillation) ซึ่งมีสาเหตุหลักมาจากการแทรกสอดกันของสัญญาณ (Interference Effects) โดยถ้าเป็นการสื่อสารภาคพื้นเช่นระบบสัญญาณเอฟเอ็มสาเหตุของการแทรกสอดอาจมาจากสถานีวิทยุข้างเคียงที่ใช้ค่าความถี่ของคลื่นพาห์ (Carrier) ที่ใกล้เคียงหรือใช้ความถี่ที่ทับกัน [3] แต่ในปรากฏการณ์นี้สัญญาณที่มาแทรกสอดก็คือสัญญาณของตัวเองโดยเกิดจากการเดินทางผ่านชั้นบรรยากาศที่มีค่าความหนาแน่นไม่เท่ากันดังรูปที่ 2.1 ทำให้เกิดปรากฏการณ์ที่เรียกว่า Phase Advance ซึ่งจะทำความเร็วของคลื่นระนาบ (Plane Wave) เพิ่มขึ้น ดังนั้นสัญญาณดาวเทียมที่รับได้จะมีเฟสแตกต่างกันซึ่งเป็นผลให้เกิดการเปลี่ยนแปลงของระดับแอมพลิจูดและเฟสอย่างกะทันหัน



รูปที่ 2.1 ลักษณะสัญญาณดาวเทียมเมื่อเดินทางผ่านกลุ่มความไม่สม่ำเสมอของอิเล็กตรอน

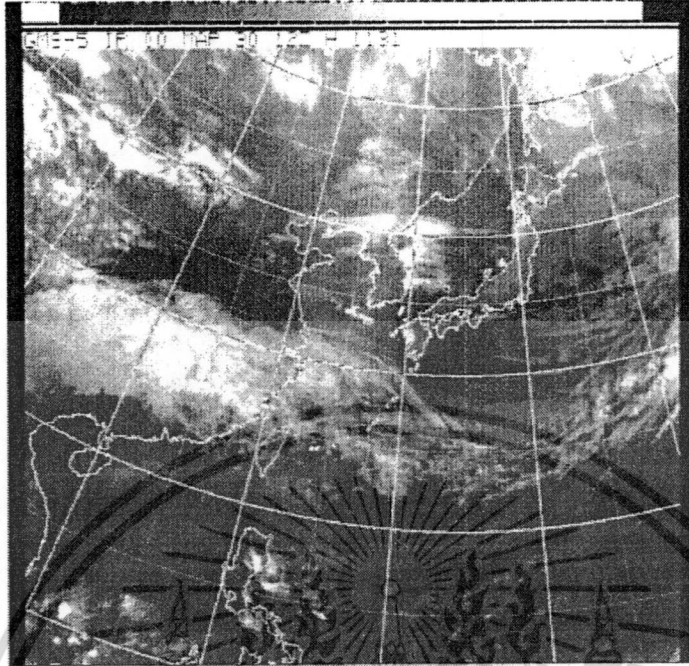
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การเปลี่ยนแปลงระดับสัญญาณดาวเทียมในขณะที่เกิดปรากฏการณ์นี้แสดงในรูปที่ 2.2 เป็นระดับสัญญาณดาวเทียมของวันที่ 18 ตุลาคม พ.ศ. 2545 โดยมีพิจารณาช่วงเวลา 10:00 – 18:00 น. ระดับสัญญาณ (Signal Level) มีการเปลี่ยนแปลงเพียงเล็กน้อยในระดับที่ไม่เกิน 0.5 – 1 dBp-p โดยถือว่าเป็นระดับสัญญาณปกติซึ่งการเปลี่ยนแปลงนี้อาจเกิดจากคลื่นเดินทางผ่านตัวกลางที่เป็นชั้นบรรยากาศที่แตกต่างกันหลายชั้น รวมถึงการเปลี่ยนแปลงเนื่องจากการเคลื่อนตัวของดาวเทียม [4] แต่หลังจากเวลา 19:00 น. ระดับสัญญาณเริ่มมีการเปลี่ยนแปลงเพิ่มขึ้นและลดลงอย่างรวดเร็ว ซึ่งเกิดอย่างต่อเนื่องจนถึงเวลา 01:30 น. ช่วงเวลานี้คือช่วงที่สัญญาณดาวเทียมได้รับอิทธิพลจากปรากฏการณ์การเปลี่ยนแปลงแอมพลิจูดอย่างกะทันหันที่ส่งผลให้ระดับกำลังงานเปลี่ยนไปจากระดับปกติถึง 15 dBp-p หลังจากนั้นระดับสัญญาณก็กลับสู่สภาวะปกติในเวลาประมาณ 02:00 น.

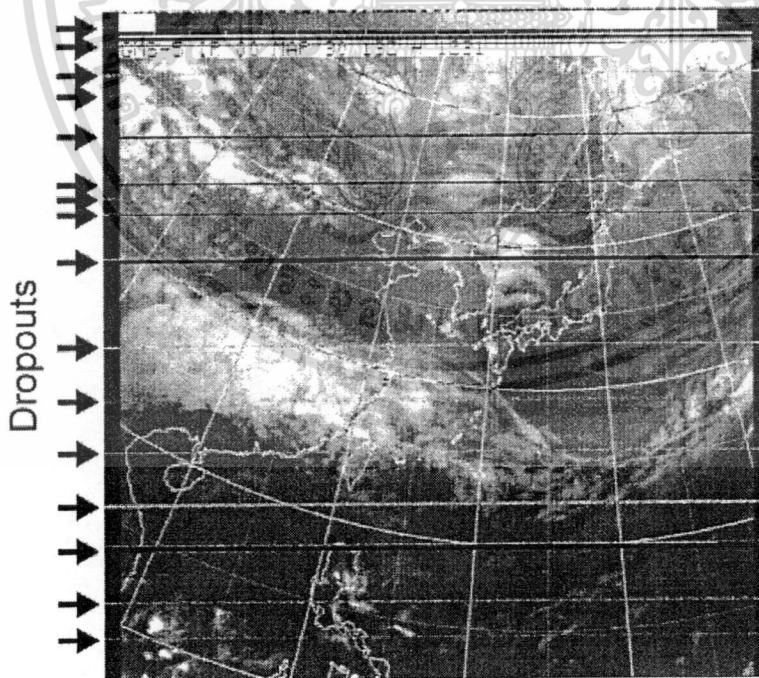


รูปที่ 2.2 สัญญาณดาวเทียมภายใต้อิทธิพลของการเปลี่ยนแปลงแอมพลิจูดอย่างกะทันหัน

เพื่อแสดงให้เห็นถึงคุณภาพที่ลดลงในการใช้งานจริงของสัญญาณดาวเทียมเนื่องจากปรากฏการณ์นี้ วิทยานิพนธ์นี้จึงนำรูปที่เป็นภาพถ่ายจากดาวเทียม GSM-5 (Geostationary Meteorological Satellite-5 or Himawari-5) ซึ่งเป็นดาวเทียมสำรวจสภาพอากาศ โดยในรูปที่ 2.3 แสดงภาพถ่ายจากดาวเทียมที่รับได้ในสภาวะปกติ ส่วนในรูปที่ 2.4 แสดงภาพถ่ายจากดาวเทียมที่รับได้ในขณะที่เกิดการเปลี่ยนแปลงแอมพลิจูดอย่างกะทันหันของวันที่ 30 มีนาคม พ.ศ. 2545 ซึ่งจะเห็นได้ว่าภาพที่รับได้นั้นหายไปเป็นช่วง (Dropouts) ซึ่งเกิดจากการที่แอมพลิจูดของสัญญาณเพิ่มขึ้นหรือลดลงจนเกินความสามารถของเครื่องรับจึงทำให้เราสูญเสียสัญญาณภาพในช่วงเวลาดังกล่าว



รูปที่ 2.3 แสดงภาพถ่ายจากดาวเทียมสำรวจสภาพอากาศ GMS-5 ในสภาวะปกติ



รูปที่ 2.4 แสดงภาพถ่ายจากดาวเทียมในขณะที่เกิดการเปลี่ยนแปลงแอมพลิจูดอย่างกะทันหัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านกา⁵ค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.1.1 ธรรมชาติการเปลี่ยนแปลงแอมพลิจูดอย่างกะทันหัน (S4 Index)

ค่าที่แสดงถึงระดับความรุนแรงของการเปลี่ยนแปลงแอมพลิจูดอย่างกะทันหันที่นิยมใช้กันมาก คือ การอ่านค่าสูงสุดและค่าต่ำสุดของระดับสัญญาณที่รับได้ (Peak-to-peak) แต่เนื่องจากค่านี้ไม่เหมาะกับการอธิบายความรุนแรงที่เกิดเป็นช่วงเวลาและเป็นตัวแปรสุ่มจึงมีการกำหนดวิธีการหาที่ละเอียดยิ่งขึ้นที่เรียกว่า ธรรมชาติการเปลี่ยนแปลงแอมพลิจูดอย่างกะทันหัน (Scintillation Index) สามารถแสดงได้ดังต่อไปนี้ คือ

2.1.1.1 ธรรมชาติ SI (SI Index)

ค่าธรรมชาติ SI เป็นการประมาณค่าความเข้มของการเปลี่ยนแปลงแอมพลิจูดที่ง่าย ๆ โดยมักใช้สำหรับการวิเคราะห์ข้อมูลการเกิดการเปลี่ยนแปลงแอมพลิจูดอย่างกะทันหันอันดับหนึ่ง (First-Order Analysis) กำหนดโดยสมการที่ (2.1) [5]

$$SI = \frac{P_{\max} - P_{\min}}{P_{\max} + P_{\min}} \quad (1)$$

โดยที่ P แทนค่ากำลังของสัญญาณในหน่วยเดซิเบล(dB)และเพื่อหลีกเลี่ยงสถานะปรากฏการณ์ที่เกินจริง จึงพิจารณาค่ายอดที่สามจากค่าสูงสุดและต่ำสุด

P_{\max} คือ ระดับกำลังของค่ายอดที่สามจากค่ายอดที่สูงสุดในช่วงเวลาหนึ่งที่กำหนด

P_{\min} คือ ระดับกำลังของค่ายอดที่สามจากค่ายอดที่ต่ำสุดในช่วงเวลาหนึ่งที่กำหนด

2.1.1.2 ธรรมชาติ S_4

Briggs และ Parkin (1963) ได้นำเสนอชุดของธรรมชาติในเทอมของ S_1, S_2, S_3 และ S_4 โดยเฉพาะ ธรรมชาติ S_4 เป็นธรรมชาติซึ่งมีความสัมพันธ์กับช่วงเวลาโดยสามารถหาได้จากค่าเบี่ยงเบนมาตรฐาน (Standard Deviation) ของกำลังสัญญาณที่รับได้หารด้วยค่าเฉลี่ย (Mean) ของกำลังสัญญาณนั้นในหน่วยวัตต์ดังแสดงในสมการ (3)

$$S_4 = \frac{\sigma_x}{m_x} \quad (2)$$

โดยที่ σ_x คือ ค่าเบี่ยงเบนมาตรฐาน (Standard Deviation)

m_x คือ ค่าเฉลี่ยของข้อมูล (Mean Value)

โดยค่าเฉลี่ยของข้อมูลและค่าเบี่ยงเบนมาตรฐานสามารถหาได้จากสมการ (3) และ สมการ (4)

ตามลำดับ

$$m_x = \bar{x} = \frac{1}{N} \sum_{i=1}^N x_i \quad (3)$$

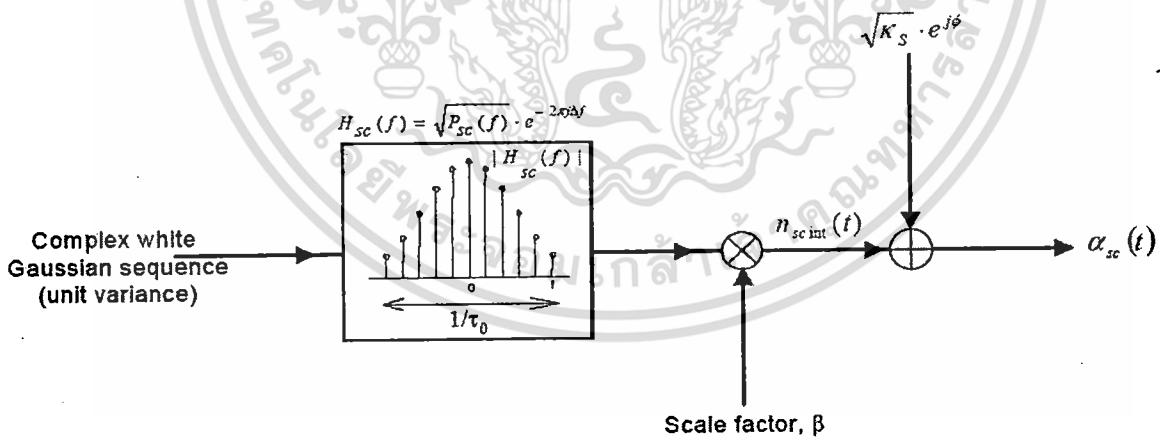
$$\sigma_x = \sqrt{\frac{1}{N} \sum_{i=1}^N (x_i - \bar{x})^2} \quad (4)$$

โดยที่ x_i คือ ระดับสัญญาณที่รับ ได้ (Receive Signal)

N คือ จำนวนข้อมูลทั้งหมด (Whole Number)

การคำนวณหาค่าพารามิเตอร์ในครรชนี S_4 สามารถคำนวณได้โดยทำการเฉลี่ยสัญญาณในช่วงเวลาที่กำหนด ซึ่งค่าครรชนี S_4 ที่เท่ากับ 0.5 [5] จะเป็นตัวแบ่งระหว่างเกิดการเปลี่ยนแปลงแอมพลิจูดอย่างกะทันหันที่ไม่รุนแรง (Weak Scintillation) กับการเปลี่ยนแปลงที่รุนแรง (Strong Scintillation) ซึ่งบางครั้งค่าครรชนี S_4 อาจมากกว่า 1 ก็ได้

2.1.1.3 แบบจำลองช่องสัญญาณซินทิเลชัน



รูปที่ 2.5 แบบจำลองช่องสัญญาณซินทิเลชัน

$$\alpha_{sc}(t) = \sqrt{K_s} \cdot e^{j\phi} + n_{scint}(t) \quad (5)$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านก7รค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แบบจำลองช่องสัญญาณซินทิลเลขันจากแบบจำลองดังรูปสามารถสร้างได้จากการนำลำดับข้อมูลเกาส์เซียนเชิงซ้อนมาผ่านฟิลเตอร์จากนั้นนำมาคูณด้วยสเกลแฟกเตอร์เพื่อให้ค่าที่ได้มีคุณลักษณะตามช่องสัญญาณที่ต้องการ ก็จะทำได้ค่าสัญญาณในทิศทางสุมที่เกิดจากการเปลี่ยนแปลงของชั้นบรรยากาศไอโอโนสเฟียร์ จากนั้นนำมารวมกับสัญญาณที่รับได้ในทิศทางตรงก็จะทำให้ได้ค่าสัมประสิทธิ์ซินทิลเลขันตามที่ต้องการ

2.2 รหัส BCH

สำหรับจำนวนเต็มบวก m ใดๆ ที่มีค่ามากกว่าหรือเท่ากับ 3 ($m \geq 3$) และจำนวนเต็ม t ที่เล็กกว่า 2^{m-1} ($t \leq 2^{m-1}$) จะมีรหัสโบนารี BCH ที่มีคุณลักษณะต่อไปนี้

ความยาวของรหัส	$n = 2^m - 1$
ความยาวของบิตข้อมูล	$k \geq n - mt$
ความยาวของบิตเช็ก	$n - k \leq mt$
ระยะแฮมมิงต่ำสุด	$d_{\min} \geq 2t + 1$

ตัวอย่างรหัส BCH ที่มีความยาวไม่เกิน $2^5 - 1$ แสดงในตารางที่ 1 เนื่องจากระยะแฮมมิงต่ำสุดของชุดรหัสมีค่ามากกว่าหรือเท่ากับ $2t + 1$ เสมอ ฉะนั้นชุดรหัสดังกล่าวจึงมีขีดความสามารถในการแก้ไขความผิดพลาดได้มากถึง t บิต

ตารางที่ 1 ตัวอย่างรหัส BCH

m	n	t	(n, k)	$n - k$
3	7	1	(7, 4)	3
4	15	1	(15, 11)	4
		2	(15, 7)	8
		3	(15, 5)	10
		1	(31, 26)	5
		2	(31, 21)	10

5	31	3	(31, 16)	15
		5	(31, 11)	20
		7	(31, 6)	25

2.2.1 พหุนามตัวกำเนิดของรหัส BCH

การกำหนดพหุนามตัวกำเนิด $g(x)$ ให้กับขุรหัส BCH สามารถพิจารณาในรูปของรากจากฟิลด์กาลัว $GF(2^m)$ ดังนี้คือให้ α เป็นพหุมีที่พีลิมেন্টในฟิลด์ $GF(2^m)$ พหุนามตัวกำเนิด $g(x)$ ของรหัส BCH ขนาดความยาว $n = 2^m - 1$ ที่สามารถแก้ไขความผิดพลาดได้ t บิต จะเป็นพหุนามที่มีดีกรีต่ำสุดโดยมี

$$\alpha, \alpha^2, \alpha^3, \dots, \alpha^{2t} \quad (6)$$

เป็นรากกล่าวคือ $g(\alpha^i) = 0$ สำหรับ $1 \leq i \leq 2t$ จากความรู้พื้นฐานของพหุนามต่ำสุด (minimal polynomial) ที่กล่าวว่ามีอิลิมেন্ট $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{2t}$ เป็นรากของพหุนามต่ำสุด $\Phi_1(x), \Phi_2(x), \Phi_3(x), \dots, \Phi_{2t}(x)$ ฉะนั้นการหาพหุนามที่มีอิลิมেন্টทั้งหมดนี้เป็นรากก็สามารถทำได้โดยการคูณพหุนามต่ำสุดทั้งหมดเข้าด้วยกัน แต่เนื่องจากอิลิมেন্টบางส่วนเป็นคอนจูเกตของกันและกัน ซึ่งหมายความว่าอิลิมেন্টเหล่านั้นจะเป็นรากของพหุนามต่ำสุดชุดเดียวกัน ด้วยเหตุนี้พหุนามที่มีดีกรีต่ำสุดและมีอิลิมেন্ট $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{2t}$ เป็นรากจะมีค่าเท่ากับค่าคูณร่วมน้อย (LCM: Least Common Multiplier) ของพหุนามต่ำสุดที่เกี่ยวข้องทั้งหมด

$$g(x) = LCM\{\Phi_1(x), \Phi_2(x), \Phi_3(x), \dots, \Phi_{2t}(x)\} \quad (7)$$

ความสัมพันธ์นี้สามารถลดรูปลงอีกได้เป็น

$$g(x) = LCM\{\Phi_1(x), \Phi_3(x), \Phi_5(x), \dots, \Phi_{2t-1}(x)\} \quad (8)$$

เหตุที่สามารถลดจำนวนพหุนามต่ำสุดที่เหลือเฉพาะชุดที่เป็นตัวเลขจำนวนคี่ได้เพราะตัวเลขจำนวนคู่ a ใด ๆ สามารถเขียนอยู่ในรูปของตัวเลขจำนวนคี่ b ไปคูณกับค่า 2^j ที่เหมาะสมโดย $j \geq 1$ กล่าวคือ

$$a = b \cdot 2^j \quad (9)$$

ยกตัวอย่างเช่น

$$2 = 1 \cdot 2^1, 4 = 1 \cdot 2^2, 6 = 3 \cdot 2, 8 = 1 \cdot 2^3, 10 = 5 \cdot 2, 12 = 3 \cdot 2^2 \\ 14 = 7 \cdot 2, 16 = 1 \cdot 2^4, 18 = 9 \cdot 2, 20 = 5 \cdot 2^2, 22 = 11 \cdot 2$$

จากความสัมพันธ์ตามสมการที่ (9) จะได้ว่า

$$\alpha^a = (\alpha^b)^{2^j} \quad (10)$$

สมการนี้มีความหมายว่า α^a เป็นคอนจูเกตของ α^b ฉะนั้นทั้งคู่จึงเป็นพหุนามต่ำสุดตัวเดียวกันคือ

$$\Phi_a(x) = \Phi_b(x) \quad (11)$$

ด้วยเหตุนี้เราจึงสามารถสรุปได้ว่าอีลิเมนต์ที่มีค่ายกกำลังของ α เป็นเลขคู่ภายในลำดับของอีลิเมนต์ตามสมการที่ (6) จะมีพหุนามต่ำสุดตัวเดียวกับอีลิเมนต์ที่มีค่ายกกำลังของ α เป็นเลขคี่บางตัวที่อยู่ในลำดับก่อนหน้าเสมอ ฉะนั้นสมการที่ (7) จึงสามารถลดรูปลงได้เป็นความสัมพันธ์ตามสมการที่ (8)

เนื่องจากพหุนามต่ำสุดทุกตัวจะมีดีกรีได้ไม่เกิน m ฉะนั้นผลคูณของพหุนามต่ำสุดทั้ง t ตัวจึงมีดีกรีไม่เกิน mt เสมอ ซึ่งหมายความว่าจำนวนบิตพริตตีเช็ก $n-k$ ของคำรหัสย่อจะมีไม่เกิน mt ด้วย จากการศึกษาที่ผ่านมาเรายังไม่สามารถระบุได้แน่นอนว่าจะมีจำนวนบิตพริตตีเช็กกี่บิต แต่อย่างไรก็ตามโดยทั่วไปเราพบว่าถ้า t มีขนาดเล็กจำนวนบิตพริตตีเช็ก $n-k$ จะมีค่าเท่ากับ mt พอดี

2.3 การถอดรหัส BCH

สมมติว่าภาคส่งได้ให้กำเนิดคำรหัส $c(x) = c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1}$ ขึ้น และได้ส่งคำรหัสดังกล่าวผ่านช่องสัญญาณที่มีสัญญาณรบกวน เมื่อชุดบิตของคำรหัสดังกล่าวถึงภาครับได้มีความผิดพลาดเกิดขึ้นกับบางบิต ให้ชุดบิตที่รับได้มีค่าเท่ากับ $r(x) = r_0 + r_1x + r_2x^2 + \dots + r_{n-1}x^{n-1}$ และให้รูปแบบของความผิดพลาดบิตแสดงในรูปของ $e(x) = e_0 + e_1x + e_2x^2 + \dots + e_{n-1}x^{n-1}$ จะได้ว่า

$$r(x) = c(x) + e(x) \quad (12)$$

ในกระบวนการถอดรหัสชุดบิตที่ได้รับของวงจรภาครับ จะเริ่มจากการคำนวณหาค่าซินโดรมจากชุดบิต $r(x)$ ที่ได้รับ สำหรับรหัส BCH ที่สามารถแก้ไขความผิดพลาดได้ t บิต จะมีซินโดรมอยู่ทั้งสิ้น $2t$ ค่าดังนี้

$$s = (s_1, s_2, s_3, \dots, s_{2t}) = rH^T \quad (13)$$

โดย H เป็นเมตริกซ์พาริตีเช็ก เมื่อพิจารณาความสัมพันธ์ตามสมการ (13) จะเห็นว่าซินโดรมแต่ละตัวสามารถหาได้ดังนี้

$$s_i = r(\alpha^i) = r_0 + r_1\alpha^i + r_2\alpha^{2i} + \dots + r_{n-1}\alpha^{(n-1)i} \quad (14)$$

สำหรับ $1 \leq i \leq 2t$ นอกจากวิธีการที่แสดงนี้ เรายังสามารถคำนวณค่าซินโดรม s_i แต่ละตัวได้โดยการนำพหุนามต่ำสุด $\Phi_i(x)$ ของอีลิเมนต์ α^i ไปหารพหุนาม $r(x)$ ซึ่งการทำเช่นนี้จะได้สมการความสัมพันธ์ดังนี้

$$r(x) = a_i(x)\Phi_i(x) + b_i(x) \quad (15)$$

โดย $a_i(x)$ คือผลหารหารและ $b_i(x)$ คือเศษที่ได้จากการหาร ทั้งนี้ $b_i(x)$ จะมีดีกรีน้อยกว่าพหุนามต่ำสุด $\Phi_i(x)$ เสมอเนื่องจาก $\Phi_i(\alpha^i) = 0$ เพราะตามนิยาม α^i เป็นรากของพหุนาม $\Phi_i(x)$ ฉะนั้น

$$s_i = r(\alpha^i) = b_i(\alpha^i) \quad (16)$$

สมการนี้คำนวณหาซินโดรมตัวที่ i ได้จากการคำนวณหาเศษ $b_i(x)$ และแทนค่า x ด้วย α^i เนื่องจาก $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{2t}$ เป็นรากของพหุนามค้ำรหัสทุกค่า ฉะนั้น $c(\alpha^i) = 0$ สำหรับ $1 \leq i \leq 2t$ เมื่อพิจารณาสมการที่ (7) อีกครั้งและแทนค่า x ด้วย α^i จะได้ว่า

$$r(\alpha^i) = c(\alpha^i) + e(\alpha^i) = e(\alpha^i) \quad (17)$$

และจากสมการที่ (14) เราสามารถสรุปได้ว่า

$$s_i = e(\alpha^i) \quad (18)$$

ความสัมพันธ์นี้แสดงให้เห็นว่าค่าซินโดรมสามารถคำนวณได้จากรูปแบบของความผิดพลาด $e(x)$ ได้เช่นกัน

สมมติว่ารูปแบบของความผิดพลาด $e(x)$ หนึ่งมีบิตที่เกิดความผิดพลาดทั้งหมด v ตำแหน่ง ได้แก่ $x^{j_1}, x^{j_2}, \dots, x^{j_v}$ นั่นคือ

$$e(x) = x^{j_1} + x^{j_2} + \dots + x^{j_v} \quad (19)$$

โดย $0 \leq j_1 < j_2 < \dots < j_v < n$ จากความสัมพันธ์ตามสมการ (18) และ (19) เมื่อนำมาแจกแจงเป็นเซตของสมการจะได้ดังนี้

$$\begin{aligned} s_1 &= \alpha^{j_1} + \alpha^{j_2} + \dots + \alpha^{j_v} \\ s_2 &= (\alpha^{j_1})^2 + (\alpha^{j_2})^2 + \dots + (\alpha^{j_v})^2 \\ s_3 &= (\alpha^{j_1})^3 + (\alpha^{j_2})^3 + \dots + (\alpha^{j_v})^3 \\ &\vdots \\ s_{2^k} &= (\alpha^{j_1})^{2^k} + (\alpha^{j_2})^{2^k} + \dots + (\alpha^{j_v})^{2^k} \end{aligned} \quad (20)$$

โดย $\alpha^{j_1} + \alpha^{j_2} + \dots + \alpha^{j_v}$ เป็นตัวแปรที่ไม่ทราบค่า และเราสามารถแก้เซตของสมการเหล่านี้เพื่อหาค่าของตัวแปรเหล่านี้ เมื่อเราทราบค่าของตัวแปรทั้งหมดแล้ว ค่ายกกำลัง j_1, j_2, \dots, j_v จะบ่งถึงตำแหน่งที่มีความผิดพลาดของบิต อย่างไรก็ตามเมื่อพิจารณาเซตของสมการให้ดีๆจะพบว่าสมการเหล่านี้มีผลเฉลยได้มากกว่าหนึ่งรูปแบบ นั่นคือให้ผลเฉลยที่ต่างกันได้ถึง 2^v รูปแบบโดยที่ผลเฉลยแต่ละแบบจะแทนรูปแบบความผิดพลาดที่ไม่เหมือนกัน ฉะนั้นจึงเป็นเรื่องของวงจรถอดรหัสที่จะต้องตัดสินใจว่าชุดบิตที่รับได้มีความผิดพลาดตามรูปแบบใด และโดยทั่วไปเรามักจะเลือกรูปแบบความผิดพลาดที่มีจำนวนบิตผิดพลาดน้อยที่สุดเป็นคำตอบที่ถูกต้อง

โดยทั่วไปการแก้สมการข้างต้นโดยวิธีตรงไปตรงมาจะค่อนข้างยุ่งยากและให้ประสิทธิภาพที่ไม่ดีนัก โดยเฉพาะอย่างยิ่งในกรณีที่ t มีขนาดใหญ่ คือมีสมการจำนวนมากนั่นเอง ฉะนั้นในส่วนต่อไปนี้จะอธิบายถึงวิธีหาผลเฉลยที่แตกต่างไป ชั้นแรกเพื่อความสะดวกนิยามให้

$$\beta_\lambda = \alpha^{j_\lambda} \quad (21)$$

โดย $1 \leq \lambda \leq v$ และเราเรียก β_λ ว่าเป็นหมายเลขระบุตำแหน่งของความผิดพลาด (error location numbers) เมื่อแทนค่า β_λ ลงในสมการ(15) จะได้

$$\begin{aligned} s_1 &= \beta_1 + \beta_2 + \dots + \beta_v \\ s_2 &= \beta_1^2 + \beta_2^2 + \dots + \beta_v^2 \\ s_3 &= \beta_1^3 + \beta_2^3 + \dots + \beta_v^3 \\ &\quad \text{M} \\ s_{2l} &= \beta_1^{2l} + \beta_2^{2l} + \dots + \beta_v^{2l} \end{aligned} \tag{22}$$

ชุดของสมการทั้ง $2l$ สมการที่ได้นี้มีชื่อเรียกว่า สมการซินโดรม (syndrome equations) หรือฟังก์ชันผลรวมยกกำลังแบบสมมาตร(power-sum symmetric functions) ในลำดับถัดไปจะนิยามพหุนามเฉพาะขึ้นมาใหม่ดังนี้

$$\begin{aligned} \sigma(x) &= (1 + \beta_1 x)(1 + \beta_2 x) \dots (1 + \beta_v x) \\ &= \sigma_0 + \sigma_1 x + \sigma_2 x^2 + \dots + \sigma_v x^v \end{aligned} \tag{23}$$

และเรียกพหุนามนี้ว่า พหุนามระบุตำแหน่งความผิดพลาด(error – location polynomial) ทั้งนี้สัมประสิทธิ์ของพหุนาม $\sigma(x)$ มีความสัมพันธ์กับตัวแปร β_i ดังนี้

$$\begin{aligned} \sigma_0 &= 1 \\ \sigma_1 &= \beta_1 + \beta_2 + \dots + \beta_v \\ \sigma_2 &= \beta_1 \beta_2 + \beta_2 \beta_3 + \dots + \beta_{v-1} \beta_v \\ &\quad \text{M} \\ \sigma_v &= \beta_1 \beta_2 \beta_3 \beta_{v-1} \beta_v \end{aligned} \tag{24}$$

และจากที่ได้อธิบายมาทั้งหมดสามารถสรุปขั้นตอนการถอดรหัสออกได้ดังนี้

ขั้นที่ 1 คำนวณหาค่าซินโดรม $\{s_1, s_2, s_3, \dots, s_l\}$ จากสัญญาณที่รับได้ $r(x)$

ขั้นที่ 2 คำนวณหาพหุนามระบุตำแหน่งความผิดพลาด $\sigma(x)$ จากเซตของซินโดรมที่ได้จากขั้นที่ 1

ขั้นที่ 3 หาค่าตำแหน่งที่เกิดความผิดพลาด $\beta_1, \beta_2, \dots, \beta_v$ จากรากของพหุนาม $\sigma(x)$

โดยปกติการคำนวณในขั้นตอนที่ 1 และ 3 ค่อนข้างจะง่าย ความซับซ้อนของกระบวนการถอดรหัสส่วนใหญ่จึงอยู่ที่ขั้นตอนที่ 2 และที่ผ่านมามีผู้เสนอแนวทางในการคำนวณของขั้นที่ 2 ไว้หลายวิธี ในที่นี้จะขอกล่าวถึงเฉพาะวิธีการของ Peterson – Gorenstein – Zierler

2.3.1 วิธีิการของ Peterson – Gorenstein – Zierler

พิจารณาสมการที่ (23)

$$\begin{aligned}\sigma(x) &= (1 + \beta_1 x)(1 + \beta_2 x) \dots (1 + \beta_v x) \\ &= 1 + \sigma_1 x + \sigma_2 x^2 + \dots + \sigma_v x^v\end{aligned}$$

จะเห็นว่าสมการดังกล่าวนี้มี β_γ^{-1} เป็นรากเสมอสำหรับ $1 \leq \gamma \leq v$ ฉะนั้นถ้าแทน $x = \beta_\gamma^{-1}$ ลงในความสัมพันธ์นี้จะได้ $\sigma(\beta_\gamma^{-1}) = 0$ กล่าวคือ

$$1 + \sigma_1 \beta_\gamma^{-1} + \sigma_2 \beta_\gamma^{-2} + \dots + \sigma_v \beta_\gamma^{-v} = 0 \quad (25)$$

คูณสมการทั้งสองด้านด้วย β_γ^{k+v} ผลที่ได้คือ

$$\beta_\gamma^{k+v} + \sigma_1 \beta_\gamma^{k+v-1} + \sigma_2 \beta_\gamma^{k+v-2} + \dots + \sigma_v \beta_\gamma^k = 0 \quad (26)$$

ถ้ากำหนดค่าของ k ขึ้นมาค่าหนึ่ง ที่อยู่ระหว่าง $1 \leq k \leq v$ แล้วทำการสร้างสมการตามรูปแบบของสมการ (26) ขึ้นมาทั้งหมด v สมการ สำหรับ γ ที่ค่าต่างๆ ตั้งแต่ $1 \leq \gamma \leq v$ จากนั้นนำสมการทั้งหมดมาบวกรวมกัน จะได้เป็น

$$\sum_{\gamma=1}^v \beta_\gamma^{k+v} + \sigma_1 \sum_{\gamma=1}^v \beta_\gamma^{k+v-1} + \sigma_2 \sum_{\gamma=1}^v \beta_\gamma^{k+v-2} + \dots + \sigma_v \sum_{\gamma=1}^v \beta_\gamma^k = 0 \quad (27)$$

อาศัยความสัมพันธ์ในสมการ(22) จะสังเกตเห็นว่าผลบวกของแต่ละพจน์ก็คือ ค่าของซินโดรม $s_1, s_2, s_3, \dots, s_v$ ด้วยเหตุนี้สมการ (27) จึงเขียนใหม่ได้เป็น

$$s_{k+v} + \sigma_1 s_{k+v-1} + \sigma_2 s_{k+v-2} + \dots + \sigma_v s_k = 0 \quad (28)$$

หรือถ้าย้ายข้างพจน์แรกไปทางด้านขวามือของสมการจะได้

$$\sigma_1 s_{k+v-1} + \sigma_2 s_{k+v-2} + \dots + \sigma_v s_k = -s_{k+v} \quad (29)$$

เนื่องจาก k มีค่าอยู่ระหว่าง $1 \leq k \leq v$ ฉะนั้นสมการ (29) จึงให้กำเนิดสมการสำหรับ k แต่ละค่า ได้มากถึง v สมการดังนี้

$$\begin{aligned}
 \sigma_1 s_v + \sigma_2 s_{v-1} + \dots + \sigma_v s_1 &= -s_{v+1} \\
 \sigma_1 s_{v+1} + \sigma_2 s_v + \dots + \sigma_v s_2 &= -s_{v+2} \\
 \sigma_1 s_{v+2} + \sigma_2 s_{v+1} + \dots + \sigma_v s_3 &= -s_{v+3} \\
 &\vdots \\
 \sigma_1 s_{2v-2} + \sigma_2 s_{2v-3} + \dots + \sigma_v s_{v-1} &= -s_{2v-1} \\
 \sigma_1 s_{2v-1} + \sigma_2 s_{2v-2} + \dots + \sigma_v s_v &= -s_{2v}
 \end{aligned} \tag{30}$$

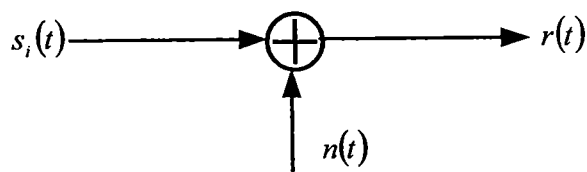
สามารถแก้เซตของสมการ(30) เพื่อหาค่าของ $\sigma_1, \sigma_2, \dots, \sigma_v$ ได้นอกจากนี้ยังสามารถแสดงเซตของสมการเหล่านี้ในรูปของเมตริกซ์ได้เป็น

$$\begin{bmatrix} s_1 & s_2 & s_3 & L & s_{v-1} & s_v \\ s_2 & s_3 & s_4 & L & s_v & s_{v+1} \\ M & M & M & M & M & M \\ s_{v-1} & s_v & s_{v+1} & L & s_{2v-3} & s_{2v-2} \\ s_v & s_{v+1} & s_{v+2} & L & s_{2v-2} & s_{2v-1} \end{bmatrix} = \begin{bmatrix} \sigma_v \\ \sigma_{v-1} \\ M \\ \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} -s_{v+1} \\ -s_{v+2} \\ M \\ -s_{2v-1} \\ -s_{2v} \end{bmatrix} \tag{31}$$

และก็อาศัยกรรมวิธีของเมตริกซ์เพื่อหาค่า $\sigma_1, \sigma_2, \dots, \sigma_v$ ได้เช่นกัน จากผลการคำนวณให้นำค่าที่ได้ไปแทนลงในพหุนาม $\sigma(x)$ ตามสมการที่ (18) จากนั้นให้แก้สมการ $\sigma(x) = 0$ เพื่อหารากทั้งหมด ซึ่งค่าของรากที่ได้จะใช้ระบุถึงตำแหน่งของบิตที่มีความผิดพลาดเกิดขึ้น ในขั้นตอนการหารากของสมการมักจะใช้วิธีการแทนค่าอีลิเมนต์ที่เป็นสมาชิก α^k ของฟิลด์กาลัวแต่ละตัวเพื่อทดสอบว่า $\sigma(\alpha^k) = 0$ หรือไม่

2.4 ช่องสัญญาณที่มีการรบกวนแบบบวก(additive noise channel)

ช่องสัญญาณที่มีสัญญาณรบกวนแบบบวกเป็นการโมเดลแบบที่ง่ายที่สุด แหล่งที่มาของสัญญาณรบกวนเกิดจากอุณหภูมิได้แก่ องค์ประกอบอิเล็กทรอนิกส์ ตัวขยายสัญญาณที่ฝั่งรับ



รูปที่ 2.6 ช่องสัญญาณ AWGN

และการแทรกสอดของสัญญาณผู้อื่น เป็นต้น สัญญาณ $r(t)$ ที่ได้รับสามารถหาได้จากสัญญาณที่ส่ง $s_i(t)$ บวกกับสัญญาณรบกวน $n(t)$ คือ

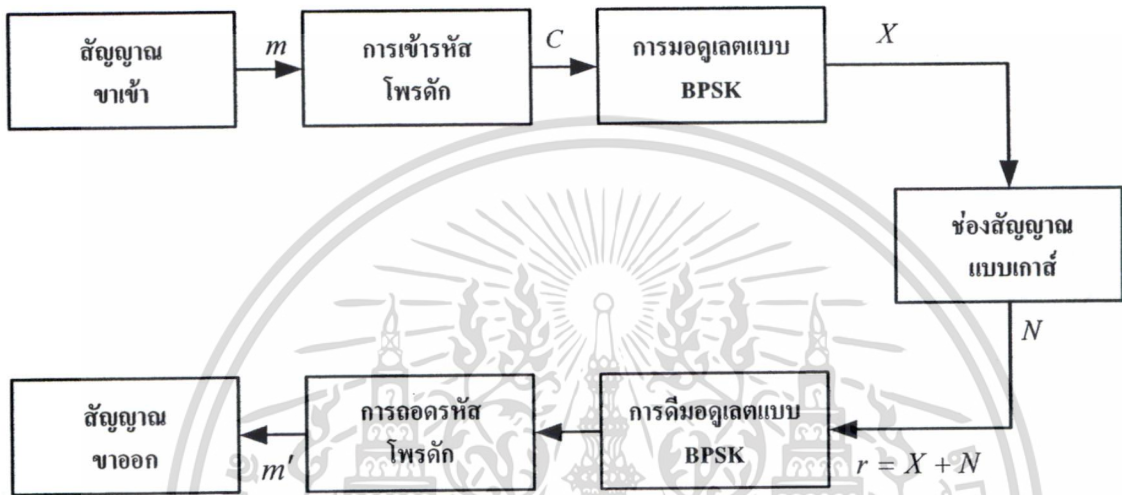
$$r(t) = s_i(t) + n(t) \quad (32)$$

โดยที่ $i=1,2,\dots,M$ ในส่วนบทความนี้จะสนใจสัญญาณรบกวนแบบเกาส์เป็นหลักและเรียกช่องสัญญาณชนิดนี้ว่าช่องสัญญาณแบบเกาส์สีขาวบวก (Additive White Gaussian Noise Channel) หรือช่องสัญญาณ AWGN สัญญาณรบกวนแบบเกาส์มีผลกระทบอย่างสูงและพบในระบบสื่อสารต่างๆ ข้อดีอย่างหนึ่งของการโมเดลแบบเกาส์ คือในการวิเคราะห์สามารถใช้คณิตศาสตร์และการคำนวณค่าสมรรถนะของระบบสามารถเขียนได้ในสูตรที่ชัดเจน

บทที่ 3

การออกแบบระบบ

3.1 โครงสร้างของการเข้ารหัส/ถอดรหัสโพรตัก



รูปที่ 3.1 บล็อกไดอะแกรมของการเข้ารหัส/ถอดรหัสโพรตัก

จากโครงสร้างของบล็อกไดอะแกรมถ้าข้อมูลที่เข้ามาเป็นสัญญาณแอนะล็อกต้องทำให้เป็นสัญญาณดิจิทัลก่อนในส่วนของการออกแบบ จะเริ่มโดยการนำบิตข้อมูล m ไปทำการเข้ารหัสโพรตักได้เป็นคำรหัส C แล้วทำการมอดูเลตแบบ BPSK ได้เป็นคำรหัส X ออกมาแล้วทำการส่งผ่านช่องสัญญาณแบบเกาส์ ทางภาครับ $r = X + N$ นำข้อมูล r ที่รับได้ไปทำการดีมอดูเลเตอร์แล้วส่งผ่านไปเข้าภาคถอดรหัสโพรตัก ได้เป็นบิตข้อมูล m' แล้วทำการแปลงบิตข้อมูลกลับเป็นข่าวสารต่อไป

3.2 โครงสร้างการเข้ารหัสโพรตัก

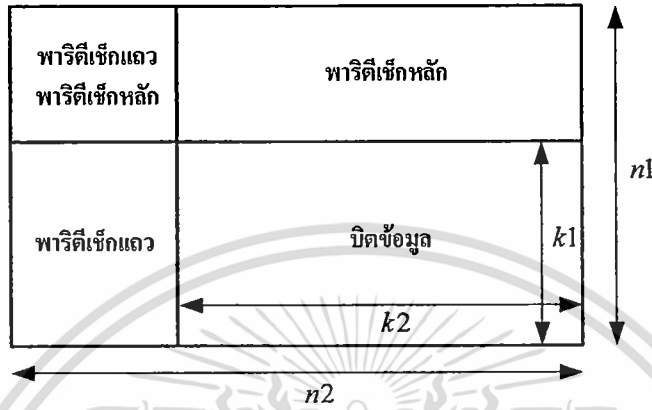
การออกแบบการเข้ารหัสโพรตัก นั้นเราจะทำการ random ข้อมูลแบบ 2 มิติ ขนาด $(k \times k)$ ขึ้นมาแล้วทำการเข้ารหัสแบบ 2 มิติ ได้คำรหัสที่มีขนาด $(n \times n)$ พารามิเตอร์ของรหัสโพรตักมีดังนี้

$$n = n_1 \times n_2 \quad , \quad k = k_1 \times k_2$$

$$d = d_1 \times d_2 \quad , \quad R = R_1 \times R_2$$

$$R = (k_1 \times k_2) / (n_1 \times n_2) \quad C^1 = (n_1, k_1, d_1) \quad , \quad C^2 = (n_2, k_2, d_2)$$

จากพารามิเตอร์ของรหัสโพรตัก n คือความยาวของคำรหัส k คือ บิตข่าวสารข้อมูล d คือระยะแรมมิ่งต่ำสุด R คือ อัตราคำรหัส C^1 คือคำรหัสในแนวหลัก C^2 คือคำรหัสในแนวแถว

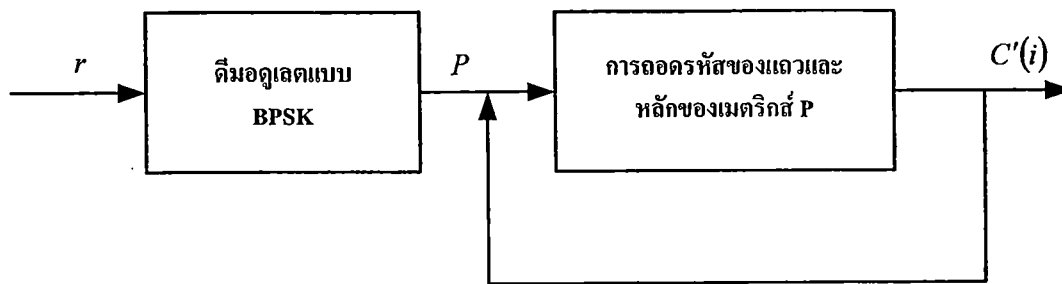


รูปที่ 3.2 โครงสร้างของรหัสโพรตัก

จากรูปที่ 3.2 จะเห็นว่า $(k_1 \times k_2)$ คือพื้นที่ของบิตข้อมูล เมื่อทำการเข้ารหัสแล้วจะได้เป็นคำรหัส $(n_1 \times n_2)$ checks on rows เป็นพาริตีเช็กละหวในแนวแถว checks on columns เป็นพาริตีเช็กลักในแนวหลัก สมมติทำการเข้ารหัสโพรตักโดยใช้คำรหัส $(7, 4, 1)$ n, k และ t ตามลำดับ t คือความสามารถในการแก้ไขบิตพลาด ทำการ random บิตข้อมูล (4×4) 4 แถว 4 หลักพื้นที่บิตข้อมูลเท่ากับ 16 บิต แล้วทำการเข้ารหัสจะได้คำรหัสเป็น (7×7) 7 แถว 7 หลัก ทำให้ได้พื้นที่คำรหัสเป็น 49 บิต

3.3 โครงสร้างการถอดรหัสโพรตัก

เมื่อภาคส่งได้ทำการส่งข้อมูลผ่านช่องสัญญาณแบบเกาส์ ในส่วนของภาครับ $r = X + N$ เมื่อได้รับสัญญาณ r มาแล้วทำการตีมอดูเลเตอร์แบบ BPSK ได้เป็นเมตริกซ์ P ออกมา แล้วนำข้อมูลใน เมตริกซ์ P ไปถอดรหัสโดยทำการถอดรหัสในแนวแถวและหลักจะได้คำรหัสแบบ 2 มิติออกมา



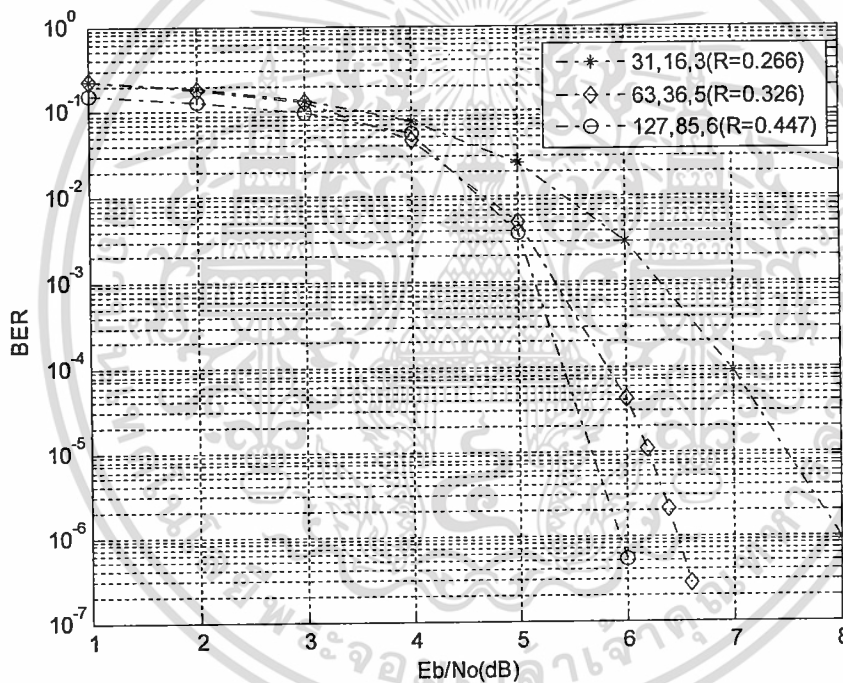
รูปที่ 3.3 บล็อกไดอะแกรมการถอดรหัสโพรตัก

จากรูปที่ 3.3 เมื่อภาครับได้รับข้อมูลจากภาคส่ง r มาแล้วจะทำการส่งผ่านไปยังการคิมอดูเลตแบบ BPSK เพื่อทำการตัดสินใจว่าข้อมูลที่ส่งมาเป็น 0 หรือ 1 โดยถ้าข้อมูลที่ส่งมามีค่ามากกว่า 0 จะตัดสินใจให้เป็น 1 แต่ถ้าข้อมูล r ที่รับมามีค่าน้อยกว่า 0 จะตัดสินใจให้เป็น 0 เมื่อผ่านการคิมอดูเลตจะได้ข้อมูลในรูปแบบของเมตริกส์ P ทำการส่งผ่านเข้าภาคถอดรหัสทำการถอดรหัสในลักษณะของแฉวและหลักจะได้ค่ารหัส $C'(i)$ i คือจำนวนรอบของการวนซ้ำของข้อมูล(iteration) หากต้องการให้ค่ารหัสถูกต้องมากขึ้นหรือ อัตราบิตผิดพลาด ต่ำลงสามารถทำได้โดยการนำค่ารหัสที่ถอดได้ในรอบแรกมาทำการวนซ้ำในภาคถอดรหัสในลักษณะเดิมคือถอดรหัสในแฉวแฉวและหลักอีกครั้งและถ้าต้องการให้สมรรถนะของระบบดีขึ้นก็สามารถทำได้โดยเพิ่มจำนวนรอบของการวนซ้ำ

บทที่ 4

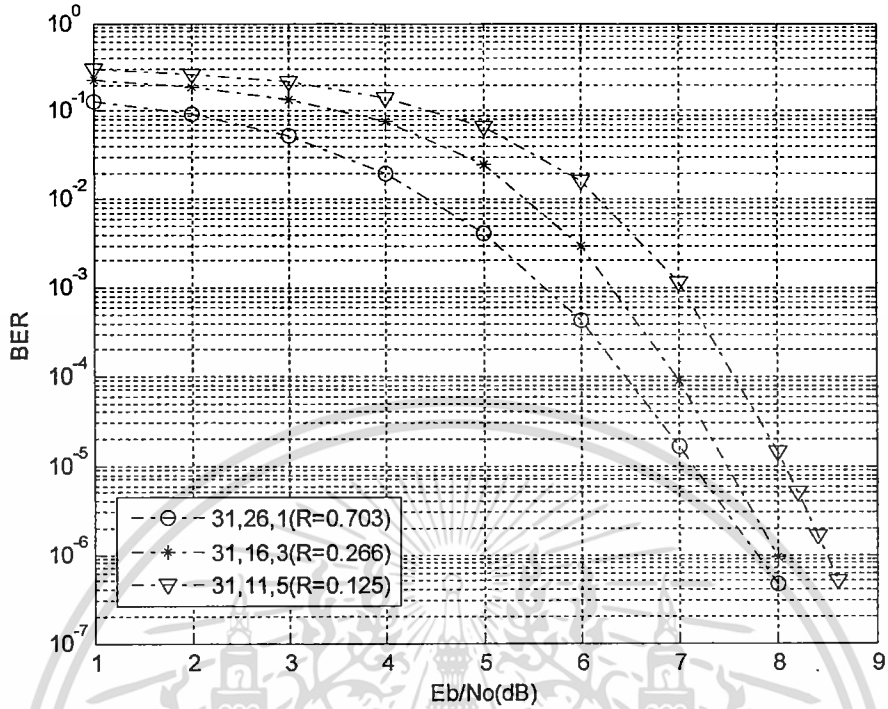
ผลการจำลองแบบ

ในบทที่ 3 ได้นำเสนอการออกแบบรหัสโพรตักโดยนำเสนอในส่วนของโครงสร้างของทั้งระบบ โครงสร้างของการเข้ารหัสและโครงสร้างของการถอดรหัสของรหัสโพรตักในส่วนต่อไปนี้จะนำเสนอใน ส่วนของการจำลองแบบและวิเคราะห์ผลที่ได้ จากการทดลองได้ทำการจำลองแบบการถอดโพรตัก ที่เข้ารหัส ที่มีค่าพารามิเตอร์ต่างกัน โดยทำการเปรียบเทียบสมรรถนะของรหัสที่แตกต่างกัน โดยใช้รหัส (31,16, 3) , (63 , 36 , 5) และ (127 , 85, 6) ทำการเปรียบเทียบ BER กับ E_b / N_0 และได้ทำการเปรียบเทียบสมรรถนะที่ค่า รหัสเดียวกันคือ ใช้ n ค่าเดียวกันแต่ค่า k และ t ต่างกันหรือ อัตรารหัสต่างกันนั่นเอง



รูปที่ 4.1 การเปรียบเทียบสมรรถนะของรหัสโพรตักที่ค่าพารามิเตอร์ต่างกัน

จากรูปที่ 4.1 เป็นการเปรียบเทียบสมรรถนะของรหัสโพรตักที่เข้ารหัสต่างกันจากผลแสดงให้เห็นว่า รหัส (127, 85, 6) แบบ 2 มิติ มีสมรรถนะดีที่สุดในเมื่อเทียบกับรหัสตัวอื่น สังเกตได้จากที่ค่า BER เท่ากับ 1×10^{-5} E_b / N_0 เท่ากับ 5.7 dB และที่เข้ารหัส (63, 36, 5) , (31, 16, 3) E_b / N_0 เท่ากับ 6.2 dB และ 7.5 dB ตามลำดับ



รูปที่ 4.2 การเปรียบเทียบสมรรถนะของรหัสไทรคิกที่ n เท่ากันแต่อัตราหัสต่างกัน

จากรูปที่ 4.2 แสดงให้เห็นว่าที่ความยาวรหัสเท่ากันแต่อัตราหัสต่างกันจะพบว่า รหัสที่มีอัตราหัสสูง สมรรถนะของระบบจะดีกว่ารหัสที่มีอัตราหัสต่ำ สังเกตได้จากที่ BER เท่ากับ 10^{-5} รหัส (31, 26, 1) จะมีสมรรถนะดีที่สุด E_b/N_0 เท่ากับ 7.1dB เมื่อเทียบกับรหัส (31, 16, 3), (31, 11, 5) โดยค่า E_b/N_0 อยู่ที่ 7.5 dB และ 8 dB ตามลำดับ

บทที่ 5 ข้อวิจารณ์

งานวิจัยนี้ได้นำเสนอหัวข้อ รหัสโปรคักโดยใช้โครงสร้างรหัสบล็อกเทอร์โบสำหรับช่องสัญญาณ
ซินทิเลชัน แต่ส่วนของงานวิจัยที่ได้นำเสนอนี้สามารถดำเนินการไปได้เพียงส่วนหนึ่งของงานวิจัยคือสามารถทำ
ได้ในส่วนของการเข้ารหัสและถอดรหัสโปรคักผ่านช่องสัญญาณแบบเกาส์ แต่ในส่วนของการจำลองแบบ
ผ่านช่องสัญญาณแบบซินทิเลชันยังอยู่ระหว่างดำเนินการแต่ยังไม่ได้ผลเป็นที่น่าพอใจเนื่องจากเกิดปัญหา
ทางด้านเทคนิคของงานวิจัยที่ดำเนินการ



บทที่ 6

บทสรุปและข้อเสนอแนะ

ในบทความนี้ได้ทบทวนการออกแบบการเข้าและถอดรหัสโพรต็อก เพื่อทำการศึกษสมรรถนะของระบบ จากผลการจำลองจะเห็นได้ว่าอัตรารหัส (R) หรืออัตราส่วนของ k/n มีผลต่อสมรรถนะ นอกจากนี้ความยาวคำรหัสค่าเดียวกันแต่ค่าอัตรารหัสต่างกันจะ พบว่าที่อัตรารหัสสูงสมรรถนะของระบบจะดีขึ้น อัตราบิดผิดพลาดลดลง เมื่อเทียบกับคำรหัสที่ (R) ต่ำ และในส่วนของงานที่จะทำต่อไปคือ การจำลองแบบผ่านช่องสัญญาณแบบซินทิเลชัน



เอกสารอ้างอิง

- [1] ตัญจนกร วุฒิสิตธิกุลกิจ, เทคโนโลยีโทรคมนาคมทฤษฎีข่าวสารและการเข้ารหัส, สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, 2546.
- [2] ศศ.ดร. พรชัย ทรัพย์นิธิ, ระบบสื่อสารดิจิทัล, วศ.สจล. 198 : ISBN 974-15-0035-1, 2549.
- [3] วิวัฒน์ กิรานนท์, วิศวกรรมการสื่อสาร, พิมพ์ครั้งที่ 1, กรุงเทพมหานคร : อักษรสยามการพิมพ์, 2540
- [4] วิสุทธิ์ อธิพรธรรม, “การเปลี่ยนแปลงแอมพลิจูดอย่างกะทันหันของสัญญาณดาวเทียม”, วิทยานิพนธ์วิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมไฟฟ้า บัณฑิตวิทยาลัย, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง, 2536
- [5] Allnutt J. E., Satellite to Ground Radiowave Propagation Theory, Practice and System Impact at Frequencies above 1 GHz, London: Peter Peregrinus Ltd. 1989.
- [6] Tadanori Ondoh & Katsuhide Marubashi eds., “Science of Space Environment”, Japan: IOS Press, 2000
- [7] Kenneth Davies, Ionospheric Radio, Peter Peregrinus Ltd. 1990, London, United Kingdom.
- [8] R. Pyndiah, “Near-Optimum Decoding of Product Codes: Block Turbo Codes”, IEEE Trans. On Commun. Vol. 46, pp. 1003-1010, August 1998.
- [9] Z. Ye and E. Satorius, “Channel Modeling and Simulation for Mobile User Objective System (MUOS)¹—Part I: Flat Scintillation and Fading”, IEEE, pp. 3503-3510, 2003.
- [10] กิตติชัย วิเศษศิริ, “การวิเคราะห์ผลกระทบของการเปลี่ยนแปลงแอมพลิจูดอย่างกะทันหันที่มีผลต่อสัญญาณดาวเทียมย่านความถี่ VHF”, วิทยานิพนธ์วิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมไฟฟ้า บัณฑิตวิทยาลัย, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง, 2547