

มุนินทร์ เอี่ยมโอภาส 2554: การเข้ารหัสเครือข่ายเชิงเส้นสำหรับปัญหาการสื่อสาร
ระหว่างต้นทางปลายทางแบบหลายคู่ ปรินญาวิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรม
คอมพิวเตอร์) สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ อาจารย์ที่
ปรึกษาวิทยานิพนธ์หลัก: ผู้ช่วยศาสตราจารย์จิตรีทัศน์ ฝึกเจริญผล, Ph.D. 28 หน้า

การเข้ารหัสเครือข่ายเป็นอีกวิธีที่สามารถใช้เพิ่มประสิทธิภาพในการส่งข้อมูลภายใน
เครือข่ายได้ งานวิจัยนี้มีจุดประสงค์เพื่อศึกษาและพัฒนาการเข้ารหัสเครือข่ายเพื่อให้ทำงานได้ดี
ยิ่งขึ้น โดยสนใจในการเข้ารหัสเครือข่ายเชิงเส้นสำหรับปัญหาการสื่อสารระหว่างต้นทาง
ปลายทางแบบหลายคู่

ไม่นานมานี้ Iwama *et al.* ได้เสนออัลกอริทึมสำหรับคำนวณการเข้ารหัสเครือข่ายใน
เครือข่ายที่มีคู่รับส่ง k คู่ ที่ทำงานในเวลาเป็นพหุนามในขนาดของเครือข่าย ในกรณีที่ k เป็น
ค่าคงที่ เวลาการทำงานของอัลกอริทึมนี้ขึ้นอยู่กับขีดจำกัดบนของจำนวนโหนดที่ทำการเข้ารหัส
เครือข่ายในคำตอบ Iwama *et al.* ได้พิสูจน์ขีดจำกัดบนของจำนวนโหนดเข้ารหัสว่าจำเป็นต้องใช้
ไม่เกิน $|\mathcal{V}|^{3k}$ โหนด ถ้าการเข้ารหัสกระทำบนฟิลด์ \mathbb{F} งานวิจัยนี้เสนอว่าโหนดเข้ารหัสจำนวน
ไม่เกิน $k^2|\mathcal{V}|^{2k}$ โหนดนั้นเพียงพอต่อการหาการเข้ารหัสเครือข่าย ในกรณีที่คู่รับส่ง k คู่
ขีดจำกัดบนที่แน่นขึ้นดังกล่าว ทำให้เวลาในการทำงานของอัลกอริทึมที่เสนอ โดย Iwama *et al.*
ลดลงอย่างมาก การพิสูจน์ขีดจำกัดบนใหม่นี้ใช้หลักทางพีชคณิตเชิงเส้นและทฤษฎีบทของ
Dilworth