

บทคัดย่อ

โครงการนี้มีเป้าหมายเพื่อพัฒนาความปลอดภัยในระบบไวร์เลสเซ็นเซอร์เน็ตเวิร์คโดยใช้การเข้ารหัสแบบRSA เพื่อป้องกันการโจมตีจากผู้ไม่ประสงค์ดีและการดักจับคีย์หรือข้อมูลต่างๆ จากบุคคลอื่นที่ไม่มีสิทธิ์ เรายำเสนอตัวให้บริการการเข้ารหัสแบบRSA สำหรับเครือข่ายเซ็นเซอร์แบบไร้สาย (RSA Encryption Server for Wireless Sensor Network) โดยเครื่องให้บริการการเข้ารหัสแบบRSA นี้จะเป็นตัวสร้างคีย์แล้วส่งคีย์ที่มีการคำนวณตามกระบวนการสร้างคีย์แบบRSA ที่เสร็จแล้วไปยังโหนดที่ร้องขอ เนื่องจากขั้นตอนในการสร้างคีย์ในรูปแบบของRSA นั้นเป็นการใช้สูตรทางคณิตศาสตร์แบบมอดูล่าซึ่งมีขั้นตอนที่มีความซับซ้อนและมีหลายขั้นตอน การสร้างคีย์นั้นจึงใช้ทรัพยากรในการประมวลผลที่สูง ทำให้ในอดีตที่ผ่านมาการเข้ารหัสแบบRSA ในเครือข่ายเซ็นเซอร์แบบไร้สายจึงไม่สามารถทำได้ในทางปฏิบัติ