บทคัดย่อ

ในเวลาไม่กี่ปีที่ผ่านมานี้ความต้องการสำหรับบริการไร้สายกำลังเพิ่มขึ้นอย่างรวดเร็ว GSM เป็นหนึ่งในอุตสาหกรรมการสื่อสารโทรคมนาคมที่มีการเจริญเติบโตรวดเร็วที่สุด อย่างไรก็ตาม ระบบการสื่อสารเคลื่อนที่ไร้สายมีความไม่มั่นคงมากกว่าในการถูกลักลอบดักฟังและเข้าถึงระบบอย่างไม่ถูกต้อง งานวิจัยนี้เสนอวิธีการรักษาความปลอดภัยแบบใหม่บนพื้นฐานของการเข้ารหัสลับแบบ Secret Key สำหรับเครือข่าย GSM ด้วยการรักษาความลับ Identity ของผู้ใช้ที่เข้มแข็ง ในระดับที่ลดการจราจรของเครือข่ายและเวลาในการทำ Call Setup ที่ดีกว่า การเข้ารหัสลับที่นำเสนอนั้นถูกพัฒนาจากอัลกอริทึม RC4 ซึ่งสามารถที่จะผลิตลำดับของบิตที่มีการกระจายของบิตศูนย์และบิตหนึ่งอย่างเท่าเทียมกัน ยิ่งไปกว่านั้นข้อมูลที่ถูกเข้ารหัสอย่างต่อเนื่องโดยใช้การเข้ารหัสลับที่นำเสนอยังมีจำนวนบิตที่เปลี่ยนไปจากข้อมูลก่อนที่จะเข้ารหัสลับมากกว่าการเข้ารหัสลับของเครือข่าย GSM แต่ใช้เวลาในการคำนวณน้อยกว่าอีกด้วย วิธีการที่ถูกนำเสนอไม่ยุ่งยากและเป็นประโยชน์มากสำหรับการสื่อสารไร้สายในปัจจุบันและอนาคต

ABSTRACT

In the recent years, the demands for wireless services are increasing rapidly. The Global System for Mobile Communication (GSM) is one of the fastest growing of telecommunication industry. However, wireless mobile systems are more vulnerable to fraudulent access and eavesdropping. This research proposes new security method based on secret key encryption for GSM networks with strongly subscriber identity confidentiality. In order to reduce network traffic and better call setup time. The proposed encryption is developed from RC4 algorithm always produces bit sequence of evenly distributed 0's and 1's. Furthermore, The proposed stream cipher has more the number of bits that differ in the plaintext than the GSM stream cipher, but also has less computational time. The proposed approach is simple and it can be very useful for present and future wireless communications.