ปัจจุบันการปิดบังหมายเลขไอพีเป็นวิธีการหนึ่งที่สำคัญสำหรับการวิเคราะห์เครือข่ายและการวิจัยเครือข่าย โดยขั้นตอนการปิดบังของหมายเลขไอพีคือการเปลี่ยนรูปหมายเลขไอพีดั้งเดิมให้เป็นหมายเลขไอพีนิรนาม ทั้งนี้เพื่อต้องการรักษาความลับของข้อมูลส่วนบุคคลของผู้ใช้ในเครือข่ายไม่ให้ถูกล่วงละเมิดความเป็นส่วนตัวได้ กระบวนการปิดบังหมายเลขไอพีที่มีชื่อเสียงได้แก่ ทีซีพีดีไพรว์ คริปโตแพน การเข้าถึงแบบหลายชั้น และทีเอสเอ แต่กระบวนการเหล่านี้ยังใช้งานได้ไม่เหมาะสมกับหน้าที่งานของการวิเคราะห์เครือข่ายที่แท้จริง และปิดบังทั้ง 32 บิตของหมายเลขไอพีอย่างไม่จำเป็น ในความเป็นจริงแล้วสามารถปิดบังเพียงบางบิตหรือบางส่วนที่จำเป็นของหมายเลขไอพีได้ตามความเหมาะสมและตามระดับความเป็นส่วนตัวที่แตกต่างกันได้ งานวิจัยเรื่องนี้จึงได้นำเสนอระดับความเป็นส่วนตัว 5 ระดับเพื่อใช้ในกระบวนการปิดบังหมายเลขไอพีอันได้แก่ ระดับที่ไม่มีการปิดบัง ระดับการปิดบังส่วน n บิตซ้าย ระดับการปิดบังส่วน n บิตขวา ระดับการปิดบังทั้ง 32 บิต และระดับการปิดบังทั้ง 32 บิตแบบสุ่ม งานวิจัยได้ประยุกต์ใช้ระดับความเป็นส่วนตัวเหล่านี้กับวิธีการปิดบังที่คงไว้ซึ่งกลุ่มเครือข่ายโดยเลือกใช้วิธีคริปโตแพน นอกจากนี้งานวิจัยเรื่องนี้ยังได้นำเสนอปัจจัยการปิดบัง 3 ปัจจัยเพื่อใช้สำหรับพิจารณาเลือกระดับความเป็นส่วนตัวที่เหมาะสมที่สุดในการปิดบังหมายเลขไอพี ได้แก่ โครงสร้างต้นไม้ของความเป็นส่วนตัว รายการวิเคราะห์เครือข่าย และกฎหมายคอมพิวเตอร์ ซึ่งปัจจัยการปิดบังทั้ง 3 ปัจจัยถูกผนวกเข้าด้วยกันโดยใช้วิธีการแบบกฎ หลักการทั้งหมดนี้ได้มาซึ่งแบบแผนการปิดบังหมายเลขไอพีใหม่บนพื้นฐานของระดับความเป็นส่วนตัว ซึ่งเหมาะสำหรับการใช้งานตามหน้าที่การวิเคราะห์เครือข่ายต่างๆ อย่างเหมาะสม และเป็นประโยชน์สำหรับองค์กรใดองค์กรหนึ่งที่ต้องการแลกเปลี่ยนข้อมูลระหว่างกัน ทั้งยังเหมาะสำหรับการสูบจับแพ็คเก็ตขนาดมหาศาล

Nowadays, an IP address anonymization is an important technique for network analysis and Internet research. The method of anonymization is the changing of original IP address to anonymized IP address to keep the private information of users in network and to prevent suitable a disclosure and violation of user privacy. The well-known anonymization techniques are TCPdpriv, Crypto-PAn, Multiple Access Level, and TSA; however, they are unsuitable for network analysis functions. The current techniques anonymize all 32 bits of IP address unnecessarily. In fact, we can anonymize the necessary bits or parts of IP address for different privacy levels. In this research, we propose 5 privacy levels for anonymization scheme as follows; non-anonymization, n-left anonymization, n-right anonymization, full anonymization, and randomly full anonymization. We apply these privacy levels to prefix-preserving IP address anonymization, the technique which can preserve network relationship among the same network group from original IP addresses, specifically to Crypto-PAn. Moreover, we present 3 anonymization factors used in considering and selecting appropriate privacy level. The 3 anonymization factors are as follows; privacy tree structures, network analysis functions, and computer law. We combine these factors by using rule-based method. Our anonymization scheme is applicable to an administrator who analyzes packet data in different functions. The scheme benefits any organizations in exchanging network data, and also appropriates for heavy-duty packet tracers and sniffers.