ปัจจุบันข้อมูลบนเครือข่ายมีจำนวนมากขึ้นเรื่อยๆ ทำให้การเก็บข้อมูลสำหรับการวิเคราะห์ต้องใช้เนื้อที่มากและต้องมีการบริหารจัดการที่ดี วิธีการสุ่มตัวอย่างแพ็กเก็ตสามารถนำมาใช้กับสนิฟเฟอร์ ทำให้สามารถเก็บข้อมูลเป็นระยะเวลานานขึ้น แต่การสุ่มตัวอย่างแพ็กเก็ตทำให้ประสิทธิภาพในการตรวจจับหนอนลดน้อยลง เพราะอัตราการกราดตรวจของหนอนหลังจากถูกสุ่มตัวอย่างจะลดน้อยลงด้วย จึงต้องเลือกอัตราการสุ่มตัวอย่างให้เหมาะสม งานวิจัยนี้ได้เสนอวิธีการสุ่มตัวอย่างสำหรับลดข้อมูล พร้อมทั้งการหาขอบเขตขั้นต่ำของการสุ่มตัวอย่างและอัตราการกราดตรวจของหนอนที่สามารถตรวจถูกจับได้อย่างมีประสิทธิภาพ

224036

At present, data volume in the network is increasing dramatically. To keep traffic log for analysis, huge storage and extensive administration are needed. Packet sampling technique applied to sniffer is an interesting method for lengthening logging period. But packet sampling may cause some problems in worm detection performance, since some traffic log are lost and may not be adequate in capturing worm characteristics. Sampling rate needs to be chosen by considering worm scanning characteristic. This research proposes a packet sampling procedure for sniffer to increase duration of traffic logging, as well as establishing lower limit of sampling rate and minimum scanning rate for detecting scanning worm.