เกรียงไกร ลิ่มทอง 2552: การตรวจการโจมตีแบบฟลัดดิ้งที่แหล่งต้นทางโดยวิธีเชิงเวฟเล็ต ปริญญาวิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมคอมพิวเตอร์) สาขาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก: ผู้ช่วยศาสตราจารย์พีรวัฒน์ วัฒนพงศ์, Ph.D. 94 หน้า

วิทยานิพนธ์ฉบับนี้ได้นำเสนอวิธีตรวจจับการโจมตีแบบฟลัดดิ้งที่แหล่งต้นทางโดยวิธีเชิงเวฟเล็ต โดยการเปลี่ยนข้อมูลที่ได้รับจากระบบเครือข่ายคอมพิวเตอร์ให้อยู่ในรูปสัญญาณที่มีความสัมพันธ์ระหว่างจำนวนชุดข้อมูลที่ส่งกับช่วงเวลา จากนั้นจึงแยกส่วนประกอบความถี่จากสัญญาณดังกล่าวเป็นส่วนประกอบความถี่สูงและส่วนประกอบความถี่ต่ำแต่ละระดับ และวิเคราะห์ความผิดปกติในระบบเครือข่ายคอมพิวเตอร์จากส่วนประกอบความถี่ในแต่ระดับ ถ้าไม่เกิดความผิดปกติในระบบเครือข่ายคอมพิวเตอร์ก็ให้นำรูปสัญญาณดังกล่าวไปคำนวณทางสถิติเพื่อสร้างค่าฐานสำหรับนำมาใช้ในการตรวจจับความผิดปกติต่อไป

งานวิจัยนี้ได้ทำการศึกษาโปรโตคอลมาตรฐานที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ ได้แก่ ICMP, TCP SYN, TCP SYN/ACK และ UDP โดยกำหนดช่วงเวลาในการจัดเก็บข้อมูลเท่ากับ 1 วินาที และใช้เวฟเล็ตแม่แบบ Haar ในการแยกส่วนประกอบความถี่ของสัญญาณที่ได้รับจากระบบเครือข่ายคอมพิวเตอร์ ข้อมูลที่นำมาทดลองจัดเก็บจากห้องปฏิบัติการคอมพิวเตอร์และอินเตอร์เน็ต มหาวิทยาลัยเกษตรศาสตร์ บางเขน ระหว่างเดือน มิถุนายน ถึง สิงหาคม 2551

ผลจากงานวิจัยนี้แสดงให้เห็นว่าเราสามารถใช้การแยกส่วนประกอบความถี่ด้วยเวฟเล็ตและการวิเคราะห์ส่วนประกอบความถี่ดังกล่าวเพื่อตรวจจับความผิดปกติที่เกิดจากการโจมตีแบบฟลัดดิ้งที่แหล่งต้นทางได้ โดยมีปัจจัยหลักที่มีผลต่อความเที่ยงตรงและแม่นยำในการตรวจจับการส่งชุดข้อมูลจำนวนมากที่เครือข่ายต้นทางคือระดับของส่วนประกอบความถี่ที่นำมาใช้ในการตรวจจับ

Kriangkrai Limthong 2009: Wavelet-Based Detection of Source-Network Packet Flooding. Master of Engineering (Computer Engineering), Major Field: Computer Engineering, Department of Computer Engineering. Thesis Advisor: Associate Professor Pirawat Watanapongse, Ph.D. 94 pages.

In this thesis, we proposed wavelet-based flooding detection method at source of a computer network. We changed the data which received from the computer network to signal that have a relationship between number of packet and time interval. After that, we decomposed the original signal into high frequency part and low frequency part for each level. Moreover, we analyze each level of the composite parts in order to detect anomaly behavior in computer network. If it is not have an abnormality in computer network, we will combine the original signal with normal signal which store in database so as to use for next detection.

In this work, we studied on the standard protocols that using in computer network such as, ICMP, TCP SYN, TCP SYN/ACK and UDP. The interval time in this work is 1 second and we use Haar mother of wavelet to decomposed original signal. The data set, we collected from Kasetsart IT Square laboratory rooms between June and August 2008.

The results from this work indicated that we can use wavelet-based decomposition and analysis of high frequency part and low frequency part in order to detect anomaly at source of computer network. The main of parameters for accurate and precisely detection of source network packet flooding is level of decomposition that use for this detection method.