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

_____ _____ ___ / ___ / ___

ลายมือชื่อนิสิต ลายมือชื่ออาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก