การตรวจจับความผิดปกติข้อมูลจราจรทางคอมพิวเตอร์ด้วยวิธีเชิงเวฟเล็ต

Wavelet-Based Anomaly Detection of Computer Network Traffic

เกรียงไกร ลิ่มทอง[1] พีรวัฒน์ วัฒนพงศ์[2] พันธุ์ปิติ เปี่ยมสง่า[2] และ ศิวรักษ์ ศิวโมกษธรรม[3]

[1]ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยกรุงเทพ

9/1 ถ.พหลโยธิน ต.คลองหนึ่ง อ.คลองหลวง จ.ปทุมธานี 12120 โทรศัพท์ : 0-2902-0299 ต่อ 2620 E-mail: kriangkrai.l@bu.ac.th

[2]ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

50 ถ.พหลโยธิน แขวงลาดยาว เขตจตุจักร กรุงเทพฯ 10900 โทรศัพท์ : 0-2942-8555 ต่อ 1402 E-mail: {pw,pp}@ku.ac.th

[3]หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

112 ถ.พหลโยธิน ต.คลองหนึ่ง อ.คลองหลวง จ.ปทุมธานี 12120 โทรศัพท์ : 0-2564-6900 E-mail: siwaruk.siwamogsatham@nectec.or.th

บทคัดย่อ

การเฝ้าระวังและการตรวจจับความผิดปกติภายในระบบเครือข่ายคอมพิวเตอร์เป็นงานที่มีความสำคัญอย่างยิ่งต่อผู้ดูแลระบบ เครื่องมือที่สามารถตรวจจับความผิดปกติได้ถูกต้องและแม่นยำช่วยให้ผู้ดูแลระบบเครือข่ายสามารถแก้ไขปัญหาได้ทันท่วงทีก่อนที่จะเกิดผลกระทบอื่นตามมาจากสิ่งผิดปกติดังกล่าว งานวิจัยนี้จึงได้เสนอวิธีตรวจจับความผิดปกติในระบบเครือข่ายคอมพิวเตอร์โดยการเปลี่ยนข้อมูลจราจรทางคอมพิวเตอร์ให้อยู่ในรูปของสัญญาณทางเวลาและแยกส่วนประกอบความถี่ของสัญญาณดังกล่าวด้วยวิธีเชิงเวฟเล็ตแบบเต็มหน่วย หลังจากนั้นจึงนำข้อมูลของส่วนประกอบความถี่มาวิเคราะห์ทางสถิติเพื่อตัดสินใจว่าเกิดความผิดปกติในระบบเครือข่ายคอมพิวเตอร์หรือไม่ ผลการทดสอบเบื้องต้นจากงานวิจัยนี้พบว่าวิธีดังกล่าวสามารถตรวจจับความผิดปกติที่เกิดขึ้นจากหลาย ๆ สาเหตุได้ เช่น เกิดจากการโจมตี, เกิดจากอุปกรณ์เสียหาย, เกิดจากการเปลี่ยนแปลงโครงสร้างระบบเครือข่ายและเกิดจากการใช้งานของผู้ใช้ที่มากผิดปกติ เป็นต้น

คำสำคัญ: เวฟเล็ต, ข้อมูลจราจรทางคอมพิวเตอร์, สัญญาณทางเวลา, การตรวจจับความผิดปกติ

Abstract

Monitoring and detecting of anomalous in computer network traffic are important tasks for network administrators. The tools can detect anomalies accurately and instantly which help network administrators to solve the problems before the other effects are following up. In this research propose the anomaly detection method by changed the computer network traffic to a signal and then we decomposed the signal with discrete wavelet decomposition. After that we analyzed all of the decomposition signal by statistical method in order to decide that anomalies occur in computer network or not. The primary results from this research showed that we can detected various anomalies. We founded the cause of anomalies that are several things such as attacks, outage, misconfiguration and flash crowd etc.

Keywords: wavelet, network traffic, time series, anomaly detection

1. บทนำ

ความผิดปกติที่เกิดขึ้นในระบบเครือข่ายคอมพิวเตอร์อาจเกิดได้จากหลายสาเหตุ เช่น เกิดจากการโจมตี เกิดจากอุปกรณ์ทำงานผิดพลาดหรือเกิดจากการใช้งานของผู้ใช้ที่มากเกินกว่าปกติ เป็นต้น ดังนั้นถ้าสามารถตรวจจับความผิดปกติที่เกิดขึ้นได้อย่างถูกต้องและรวดเร็วแล้ว ผู้ดูแลระบบก็สามารถแก้ไขปัญหาและป้องกันผลกระทบที่จะเกิดขึ้นตามมาได้อย่างทันท่วงที มีงานวิจัยจำนวนมากได้นำเสนอแนวทางในการตรวจจับความผิดปกติ ซึ่งสามารถแบ่งออกตามวิธีการตรวจจับได้เป็น 2 ประเภท คือ การตรวจจับการใช้งานที่ผิด (Misuse Detection) และการตรวจจับการใช้งานที่ผิดปกติ (Anomaly Detection)

การตรวจจับการใช้งานที่ผิดจะมีการกำหนดกฎ (Rule) หรือรูปแบบ (Signature) สำหรับตรวจสอบการใช้งานที่ผิด ถ้าตรวจจับได้ว่ามีข้อมูลหรือพฤติกรรมที่ตรงตามกฎหรือรูปแบบที่กำหนดไว้ก็จะส่งสัญญาณเตือนว่ามีการใช้งานที่ผิด ถ้าไม่ตรงกับกฎหรือรูปแบบที่กำหนดไว้จะมองว่าเป็นข้อมูลหรือพฤติกรรมที่ปกติ ซึ่งแตกต่างจากการตรวจจับการใช้งานที่ผิดปกติ โดยจะมีการเก็บข้อมูลระบบเครือข่ายเป็นระยะเวลาหนึ่งเพื่อกำหนดว่าข้อมูลหรือพฤติกรรมใดที่เป็นการใช้งานปกติ ถ้าตรวจจับได้ว่ามีข้อมูลหรือพฤติกรรมที่แตกต่างจากข้อมูลที่เก็บไว้ก็จะส่งสัญญาณเตือนว่ามีสิ่งผิดปกติเกิดขึ้น ดังนั้นจึงทำให้การตรวจจับการใช้งานที่ผิดปกตินี้สามารถตรวจจับข้อมูลหรือพฤติกรรมผิดปกติที่ยังไม่เคยเกิดขึ้นมา

ก่อนได้ ต่างจากการตรวจจับการใช้งานที่ผิดที่สามารถตรวจจับได้เฉพาะข้อมูลหรือพฤติกรรมผิดปกติที่เคยเกิดขึ้นมาแล้วเท่านั้น

งานวิจัยนี้จึงได้นำเสนอแนวทางการตรวจจับความผิดปกติในระบบเครือข่ายจากการเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่ขาออกของระบบเครือข่าย (Outgoing Traffic) โดยมีจุดประสงค์เพื่อตรวจจับความผิดปกติในระบบเครือข่ายที่อาจมีผลกระทบกับระบบเครือข่ายภายนอกได้ วิธีนี้ใช้การเปลี่ยนข้อมูลจราจรทางคอมพิวเตอร์ให้อยู่ในรูปสัญญาณทางเวลา และนำสัญญาณดังกล่าวไปแยกส่วนประกอบความถี่ด้วยวิธีเชิงเวฟเล็ตเพื่อนำไปใช้กำหนดข้อมูลหรือพฤติกรรมที่เป็นการใช้งานปกติ นอกจากนั้นได้นำวิธีการประมวลผลทางสถิติมาช่วยวิเคราะห์ตรวจสอบว่ามีข้อมูลหรือพฤติกรรมใหม่ที่แตกต่างจากข้อมูลที่เป็นปกติหรือไม่ ถ้าแตกต่างก็จะส่งสัญญาณเตือนว่ามีสิ่งผิดปกติเกิดขึ้น ถ้าไม่แตกต่างก็จะนำข้อมูลดังกล่าวไปประมวลผลเพื่อรวมกับข้อมูลเดิมที่เป็นการใช้งานปกติต่อไป

บทความนี้ประกอบด้วยส่วนต่าง ๆ ตามลำดับต่อไปนี้ คือ งานวิจัยที่เกี่ยวข้อง ขั้นตอนและหลักการทำงาน การทดลองและผลการทดลอง สรุปและแนวทางในการพัฒนาต่อไป

2. งานวิจัยที่เกี่ยวข้อง

ผู้วิจัยได้ศึกษาแนวทางในการตรวจจับความผิดปกติในระบบเครือข่ายคอมพิวเตอร์จากงานของ Peng และคณะ [1] พบว่าสามารถแบ่งวิธีตรวจจับความผิดปกติได้เป็น 2 ประเภท คือ การตรวจจับการใช้งานที่ผิด (Misuse Detection) และ การตรวจจับการใช้งานที่ผิดปกติ (Anomaly Detection) มีงานวิจัยจำนวนมากได้เสนอวิธีต่าง ๆ ซึ่งเป็นการตรวจจับการใช้งานที่ผิดปกติ เช่น การใช้เหมืองข้อมูล (Data Mining) การใช้วิธีวิเคราะห์เชิงสถิติ (Statistic) หรือแม้แต่การวิเคราะห์ด้วยการประมวลสัญญาณ (Signal Processing) เป็นต้น โดยจุดเด่นของวิธีตรวจจับการใช้งานที่ผิดปกติคือสามารถตรวจจับการโจมตีรูปแบบใหม่ที่ยังไม่เคยเกิดขึ้นมาก่อนได้ การโจมตีดังกล่าวเรียกว่า Zero-Day Attack

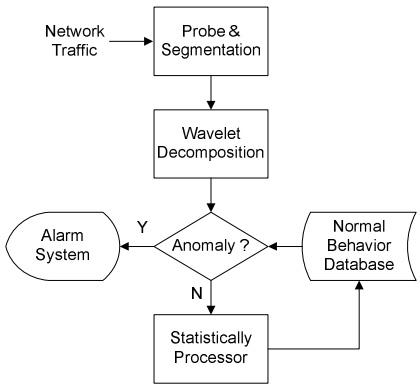
งานวิจัยของ Blazek และคณะ [2] ได้เสนอวิธีในการตรวจจับความผิดปกติในระบบเครือข่ายด้วยการประยุกต์ใช้กระบวนการทางสถิติมาวิเคราะห์ข้อมูลโปรโตคอลแบบหลายระดับในระบบเครือข่าย เพื่อตรวจจับการเปลี่ยนแปลงของจำนวนแพ็คเกจต่อช่วงเวลาที่เกิดขึ้นจากการโจมตี แต่วิธีการดังกล่าวยังมีบางกรณีที่ไม่สามารถตรวจจับการโจมตีที่เกิดขึ้นได้ (False Negative) งานวิจัยของ Glenn และคณะ [3] จึงเสนอการปรับปรุงวิธีของ Blazek และคณะ [2] โดยใช้เวฟเล็ตเข้ามาช่วยในการกรองสัญญาณซึ่งทำให้ False Negative มีจำนวนลดลง งานวิจัยข้างต้นเป็นตัวอย่างการประยุกต์ใช้กระบวนการทางสถิติมาวิเคราะห์เพื่อหาความผิดปกติในระบบเครือข่าย

นอกเหนือจากการประยุกต์ใช้วิธีการทางสถิติแล้วยังมีงานวิจัยที่เสนอการใช้วิธีเชิงเวฟเล็ตนำมาวิเคราะห์เพื่อหาความผิดปกติในระบบเครือข่าย งานวิจัยของ Barford และคณะ [4] ได้เสนอแนวทางในการตรวจจับความผิดปกติในระบบเครือข่ายด้วยการแยกส่วนประกอบความถี่ด้วยเวฟเล็ตออกเป็น 3 ความถี่ ความถี่สูง ความถี่กลางและความถี่ต่ำ ซึ่งวิธีการดังกล่าวสามารถตรวจจับความผิดปกติที่เกิดแบบทันทีทันใด (Abrupt Change) ได้ แต่ยังไม่สามารถตรวจจับความผิดปกติที่เกิดแบบค่อยเป็นค่อยไป (Long Time Change) ได้ งานวิจัยของ Lu และคณะ [5] ได้ศึกษาผลกระทบของเวฟเล็ตแม่ต่อการตรวจจับความผิดปกติและได้เสนอวิธีตรวจจับความผิดปกติโดยวิธีเชิงเวฟเล็ตและการประมาณค่าแบบถดถอย นอกจากนั้นงานวิจัยของ Kriangkrai และคณะ [6] ได้เสนอวิธีวิเคราะห์ข้อมูลที่จัดเก็บใน Darknet ด้วยวิธีเชิงเวฟเล็ตเพื่อแยกความผิดปกติที่เกิดจากการโจมตีออกจากข้อมูลหรือพฤติกรรมผิดปกติที่เกิดจากสาเหตุอื่น

ในงานวิจัยนี้ได้เสนอวิธีการตรวจจับความผิดปกติในระบบเครือข่ายซึ่งแตกต่างจากงานวิจัยที่กล่าวมาข้างต้น เนื่องจากวิธีที่นำเสนอเป็นการประยุกต์วิธีการทางสถิติและการประมวลผลสัญญาณโดยใช้เวฟเล็ตในการแยกส่วนประกอบความถี่ของสัญญาณโดยมีจุดประสงค์เพื่อตรวจจับความผิดปกติที่เกิดแบบทันทีทันใดและแบบค่อยเป็นค่อยไป

3. ขั้นตอนและหลักการทำงาน

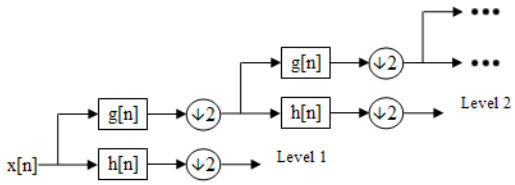
ในงานวิจัยนี้ได้แบ่งขั้นตอนการตรวจจับความผิดปกติข้อมูลจราจรทางคอมพิวเตอร์ดังแสดงในรูปที่ 1



รูปที่ 1 ขั้นตอนการตรวจจับความผิดปกติ

เริ่มจากขั้นตอน Probe & Segmentation ทำหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์และคัดแยกข้อมูลส่วนที่ต้องการ นอกจากนั้นยังทำการแปลงข้อมูลจราจรดังกล่าวให้อยู่ในรูปของสัญญาณทางเวลาที่แสดงถึงจำนวนแพ็คเกจต่อวินาที สัญญาณดังกล่าวถูกส่งต่อไปเพื่อแยกส่วนประกอบความถี่ของสัญญาณออกมาเป็นสัญญาณแต่ละระดับที่ขั้นตอน Wavelet Decomposition หลังจากนั้นที่ขั้นตอนการตรวจสอบ Anomaly จะนำสัญญาณที่ได้จากการแยกส่วนประกอบในแต่ละระดับไปทำการเปรียบเทียบกับข้อมูลหรือพฤติกรรมที่ปกติซึ่งได้มีการจัดเก็บเอาไว้ใน Normal Behavior Database ถ้ามีจำนวนแพ็คเกจต่อวินาทีแตกต่างจากค่าฐาน (Threshold) ที่กำหนดนั่นหมายความว่ามีสิ่งผิดปกติในระบบเครือข่าย ก็จะทำการส่งสัญญาณเตือนไปยัง Alarm System ว่ามีข้อมูลหรือพฤติกรรมที่ผิดปกติเกิดขึ้น แต่ถ้าข้อมูลไม่แตกต่างจากค่าฐานที่กำหนดนั่นหมายความว่าไม่มีสิ่งผิดปกติในระบบเครือข่าย ก็จะทำการประมวลผลทางสถิติที่ขั้นตอน Statistically Processor เพื่อรวมข้อมูลใหม่เข้ากับข้อมูลเก่าและนำไปเก็บเพื่อใช้ในการตรวจจับข้อมูลชุดต่อไป

ที่ขั้นตอน Wavelet Decomposition งานวิจัยนี้ใช้เวฟเล็ตแม่แบบ Harr และวิธีการแปลงเวฟเล็ตแบบเต็มหน่วยในการแยกส่วนประกอบความถี่ของสัญญาณ ซึ่งสามารถแยกส่วนประกอบความถี่ออกมาเป็นสัญญาณในแต่ละระดับดังแสดงในรูปที่ 2



รูปที่ 2 แผนภูมิต้นไม้สำหรับการแยกส่วนประกอบความถี่

สัญญาณ x[n] เป็นสัญญาณที่ได้มาจากขั้นตอน Probe and Segmentation เมื่อทำการแยกส่วนประกอบความถี่ด้วยวิธีเวฟเล็ตจะได้ส่วนประกอบสัญญาณความถี่สูง h[n] และส่วนประกอบสัญญาณความถี่ต่ำ g[n] โดยมีอัตราสุ่ม (Sampling Rate) ของสัญญาณลดลงเหลือครึ่งหนึ่งของอัตราสุ่มเดิม หลังจากนั้นจึงนำส่วนประกอบสัญญาณความถี่ต่ำไปแยกส่วนประกอบความถี่ของสัญญาณในระดับต่อไป

ข้อมูลหรือพฤติกรรมปกติที่เก็บอยู่ใน Normal Behavior Database จะเก็บอยู่ในรูปค่าเฉลี่ยของส่วนประกอบความถี่ระดับต่าง ๆ ดังสมการที่ (1) และค่าความแปรปรวนดังสมการที่ (2)

$$\bar{x}_{(j,t)} = \frac{\sum_{i=1}^{n} x_{(i,j,t)}}{n} \quad (1)$$

$$\sigma^2_{(j,t)} = \frac{1}{n}\sum_{i=1}^{n}\left(x_{(i,j,t)} - \bar{x}^2_{(j,t)}\right) \quad (2)$$

โดย i คือวันที่เก็บข้อมูล โดยทำการเก็บข้อมูลตั้งแต่วันที่ 1 จนถึงวันที่ n, j คือระดับของส่วนประกอบความถี่และ t คือช่วงเวลาในแต่ละวัน ในขั้นตอนการตรวจสอบ Anomaly จะทำการเปรียบเทียบข้อมูลที่เข้ามาใหม่กับค่าฐาน ซึ่งค่าฐานถูกกำหนดโดยสมการที่ 3

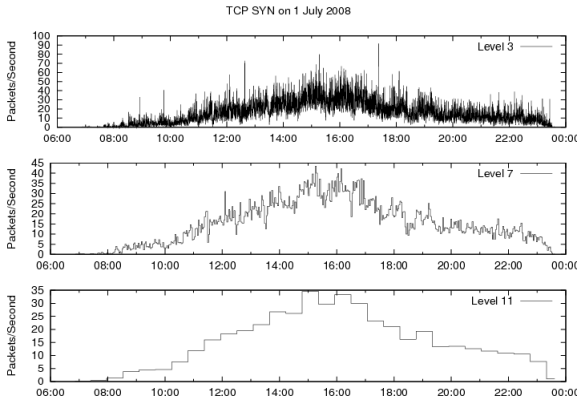
$$b_j = \bar{x}_{(j,t)} \pm c\sigma_{(j,t)} \quad (3)$$

โดย c คือค่าคงที่สำหรับการกำหนดค่าความมั่นใจ (Confidence Interval) ในงานวิจัยนี้ใช้ค่าความมั่นใจเท่ากับ 0.95 และ σ คือค่าเบี่ยงเบนมาตรฐาน ดังนั้นถ้าข้อมูลจราจรคอมพิวเตอร์ที่เข้ามาใหม่มีส่วนประกอบความถี่ j ตกนอกพื้นที่ระหว่างค่า b ก็ตัดสินใจว่ามีความผิดปกติในระบบเครือข่าย

4. การทดลองและผลการทดลอง

งานวิจัยนี้ได้ทำการเก็บข้อมูลจากห้องปฏิบัติการคอมพิวเตอร์และอินเตอร์เน็ต มหาวิทยาลัยเกษตรศาสตร์ บางเขน ระหว่างเดือนมิถุนายนถึงสิงหาคม 2551 ซึ่งห้องปฏิบัติการดังกล่าวมีเครื่องคอมพิวเตอร์ลูกข่ายประมาณ 175 เครื่องและมีนักศึกษาเข้ามาใช้งานประมาณ 1,300 คนต่อวัน โดยเครื่องคอมพิวเตอร์ลูกข่ายมีการติดตั้งโปรแกรมป้องกันไวรัสและมีการปรับปรุงฐานข้อมูลไวรัสอย่างสม่ำเสมอ อีกทั้งยังติดตั้งโปรแกรมที่จำเป็นต่อการใช้งานทั่วไป ซึ่งนักศึกษาไม่สามารถติดตั้งโปรแกรมอื่นเพิ่มเติมได้

ในการทดลองได้ทำการจัดเก็บข้อมูลโปรโตคอล ICMP, TCP SYN, TCP SYN/ACK และ UDP ที่เป็นข้อมูลจราจรทางคอมพิวเตอร์ขาออก นำข้อมูลดังกล่าวไปสร้างสัญญาณทางเวลาและนำไปแยกส่วนประกอบความถี่ต่าง ๆ ดังแสดงในรูปที่ 3 เพื่อนำไปคำนวณหาค่าเฉลี่ยและค่าความแปรปรวนของส่วนประกอบความถี่ในแต่ละระดับ หลังจากนั้นจึงนำไปจัดเก็บใน Normal Behavior Database เพื่อนำไปใช้เป็นค่าฐานในการตรวจหาความผิดปกติในระบบเครือข่ายคอมพิวเตอร์ต่อไป



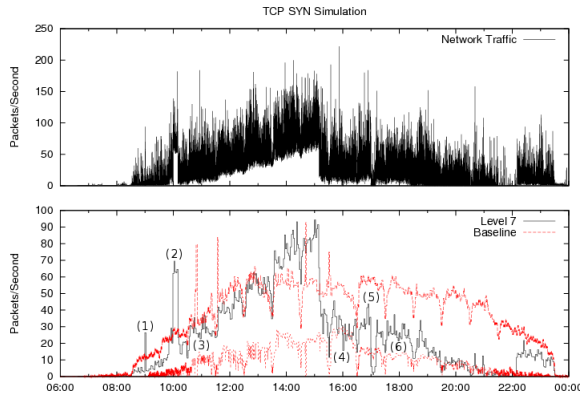
รูปที่ 3 ส่วนประกอบสัญญาณความถี่ต่ำในระดับ 3, 7 และ 11

รูปที่ 3 แสดงถึงตัวอย่างส่วนประกอบสัญญาณความถี่ต่ำในระดับที่ 3 (บน), 7 (กลาง) และ 11 (ล่าง) ของโปรโตคอล TCP SYN ที่จัดเก็บในวันที่ 1 ก.ค. 2551 ซึ่งโปรโตคอล TCP SYN เป็นโปรโตคอลที่มีการใช้งานมากที่สุดในการจัดเก็บข้อมูลครั้งนี้

เมื่อจัดเก็บข้อมูลและพฤติกรรมที่เป็นปกติแล้วจึงทำการจำลองความผิดปกติในระบบเครือข่ายคอมพิวเตอร์ ซึ่งในการทดลองได้จำลองความผิดปกติทั้งสิ้น 6 แบบด้วยกันดังแสดงในรูปที่ 4 ได้แก่

1. ความผิดปกติที่เกิดจากการ Scan Port โดยจำลองว่ามีเครื่องคอมพิวเตอร์ลูกข่ายในระบบเครือข่ายทำการ Scan Port ไปยังเครื่องคอมพิวเตอร์แม่ข่ายภายนอกด้วยอัตรา 50 แพ็คเกจต่อวินาทีเป็นระยะเวลา 1 นาที
2. ความผิดปกติที่เกิดจาก Denial of Service โดยจำลองว่ามีเครื่องคอมพิวเตอร์ลูกข่ายในระบบเครือข่ายทำการส่ง TCP SYN Flood ไปยังเครื่องคอมพิวเตอร์แม่ข่ายภายนอกด้วยอัตรา 50 แพ็คเกจต่อวินาทีเป็นระยะเวลา 10 นาที
3. ความผิดปกติที่เกิดจาก Flash Crowd โดยจำลองว่ามีเครื่องคอมพิวเตอร์ลูกข่ายในระบบเครือข่ายทำการ Download File จากเครื่องคอมพิวเตอร์แม่ข่ายภายนอกโดยเริ่มต้นที่อัตรา 1 แพ็คเกจต่อวินาทีเป็นระยะเวลา 5 นาทีแล้วเพิ่มเป็น 2 แพ็คเกจต่อวินาทีเป็นระยะเวลา 5 นาที และเพิ่มเช่นนี้เรื่อยไปจนกระทั่งเป็นอัตรา 50 แพ็คเกจต่อวินาที

4. ความผิดปกติที่เกิดจาก Outage โดยจำลองว่ามีอุปกรณ์ภายในระบบเครือข่ายเกิดความเสียหายทำให้เครื่องคอมพิวเตอร์ลูกข่ายจำนวน 50 เครื่องไม่สามารถใช้งานได้เป็นระยะเวลา 1 นาที
5. ความผิดปกติที่เกิดจาก Misconfiguration โดยจำลองว่ามีการเปลี่ยนแปลงค่าของอุปกรณ์ภายในระบบเครือข่ายทำให้เครื่องคอมพิวเตอร์ลูกข่ายจำนวน 50 เครื่องไม่สามารถใช้งานได้เป็นระยะเวลา 10 นาที
6. ความผิดปกติที่เกิดจาก Virus โดยจำลองว่าเครื่องคอมพิวเตอร์ลูกข่ายในระบบเครือข่ายติดไวรัสและไม่สามารถใช้งานได้ เริ่มต้นที่ 1 เครื่องเป็นระยะเวลา 5 นาทีแล้วเพิ่มเป็น 2 เครื่องเป็นระยะเวลา 5 นาที และเพิ่มเช่นนี้เรื่อยไปจนกระทั่งเป็น 50 เครื่อง



รูปที่ 4 ตัวอย่างการจำลองความผิดปกติในระบบเครือข่าย

รูปที่ 4 รูปบนแสดงให้เห็นถึงข้อมูลจราจรทางคอมพิวเตอร์ของโปรโตคอล TCP SYN ที่มีการจำลองความผิดปกติซึ่งยังไม่มีการแยกส่วนประกอบความถี่ของสัญญาณ รูปล่างแสดงถึงตัวอย่างส่วนประกอบสัญญาณความถี่ต่ำในระดับที่ 7 (เส้นทึบ) เปรียบเทียบกับเส้นฐาน (เส้นประ) โดยการจำลองความผิดปกติทั้ง 6 แบบแสดงในภาพด้วยตัวเลข (1)-(6) ซึ่งการจำลองเริ่มต้นที่เวลา 9.00, 10.00, 11.00, 16.00, 17.00 และ 18.00 น.ตามลำดับ จากรูปแสดงให้เห็นว่าขณะที่เกิดความผิดปกติในระบบเครือข่าย ข้อมูลของส่วนประกอบสัญญาณความถี่ที่เกิดจากการจำลองความผิดปกติแบบที่ 1, 2, 4 และ 5 จะมีค่าตกอยู่นอกพื้นที่ระหว่างค่าฐานอย่างเห็นได้ชัด ส่วนการจำลองความผิดปกติแบบที่ 3 และ 6 ข้อมูลของส่วนประกอบสัญญาณความถี่มีค่าตกอยู่นอกพื้นที่ระหว่างค่าฐานหลังจากเกิดความผิดปกติไปแล้วประมาณ 3 ชั่วโมง

5. สรุปและแนวทางในการพัฒนาต่อไป

จากการทดลองในงานวิจัยนี้พบว่าส่วนประกอบความถี่ในระดับต่าง ๆ มีผลต่อความสามารถในการตรวจจับความผิดปกติที่เกิดขึ้นในระบบเครือข่าย กล่าวคือส่วนประกอบความถี่ในระดับต่ำ เช่น ระดับที่ 1-3 ระบบสามารถตรวจจับความผิดปกติที่เกิดในระยะเวลาสั้น ๆ ได้ แต่ไม่สามารถตรวจจับความผิดปกติที่เกิดการเปลี่ยนแปลงของจำนวนแพ็คเกจต่อวินาทีที่มีจำนวนเพียงเล็กน้อยได้ ในทางกลับกันส่วนประกอบความถี่ในระดับสูง เช่น ระดับ 9-11 ระบบไม่สามารถตรวจจับความผิดปกติที่เกิดในระยะเวลาสั้น ๆ ได้ แต่สามารถตรวจจับความผิดปกติที่เกิดการเปลี่ยนแปลงของจำนวนแพ็คเกจต่อวินาทีที่มีจำนวนเพียงเล็กน้อยได้ จากข้อมูลจราจรทางคอมพิวเตอร์ที่ได้จัดเก็บและวิเคราะห์ในงานวิจัยนี้ ผู้วิจัยพบว่าส่วนประกอบความถี่ในระดับที่ 6-8 เป็นระดับที่มีความเหมาะสมและสามารถนำไปใช้ในการตรวจจับความผิดปกติในระบบเครือข่ายได้

เนื่องจากในงานวิจัยนี้ผู้วิจัยได้ทำการเก็บข้อมูล ทดลองการทำงานและจำลองการทำงานของระบบเป็นแบบออฟไลน์ ดังนั้นแนวทางในการพัฒนาต่อไปนั้นผู้วิจัยต้องการให้ระบบดังกล่าวสามารถใช้งานและตรวจจับความผิดปกติแบบออนไลน์ได้ เพื่อนำระบบดังกล่าวไปประยุกต์ใช้งานในระบบเครือข่ายคอมพิวเตอร์ที่มีการใช้งานจริง อีกทั้งข้อมูลที่ใช้ในงานวิจัยเป็นข้อมูลที่ได้มาจากขอบของระบบเครือข่าย (Access Network) ซึ่งลักษณะพฤติกรรมการใช้งานอาจแตกต่างจากข้อมูลที่ได้จากแกนของระบบเครือข่าย (Core Network) ดังนั้นจึงต้องมีการเก็บข้อมูลจากแกนของระบบเครือข่ายและนำมาทดสอบกับวิธีการที่ได้นำเสนอ เพื่อศึกษาว่าวิธีการดังกล่าวสามารถนำไปประยุกต์ใช้ที่แกนของระบบเครือข่ายได้หรือไม่

6. กิตติกรรมประกาศ

งานวิจัยนี้ได้รับทุนสนับสนุนจาก สถาบันบัณฑิตวิทยาศาสตร์และเทคโนโลยีไทย (TGIST) สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ สัญญารับทุนเลขที่ TGIST 01-51-092 และขอขอบคุณ คุณสุรชัย จิตพินิตยล ที่อำนวยความสะดวกในการจัดเก็บข้อมูลสำหรับการทดลองครั้งนี้

เอกสารอ้างอิง

[1] P. Tao, et al., "Survey of network-based defense mechanisms countering the DoS and DDoS problems," ACM Comput. Surv., vol. 39, p. 3, 2007.

[2] B. Rudolf, et al., "A Novel Approach to Detection of Denial-of-Service Attacks via Adaptive Sequential and Batch-Sequential Change-Point Detection Methods." Proc. IEEE Workshop Information Assurance and Security. IEEE CS Press, pp. 220 226, 2001.

[3] G. Carl, et al., "Wavelet based Denial-of-Service detection," Computers & Security, vol. 25, pp. 600-615, 2006.

[4] B. Paul, et al., "A signal analysis of network traffic anomalies," presented at the Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment, Marseille, France, 2002.

[5] L. Wei, et al., "Detecting Network Anomalies Using Different Wavelet Basis Functions," 2008, p. 149.

[6] K. Limthong, et al., "Wavelet-Based Unwanted Traffic Time Series Analysis," in Computer and Electrical Engineering, 2008. ICCEE 2008. International Conference on, 2008, pp. 445-449.