การลดความผิดพลาดของการบ่งชี้ถึงความผิดปกติในโนดโครงข่าย

นาย พิชัย วัฒนะภราดร

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า ภาควิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2548
ISBN 974-53-2648-8

ALLEVIATION OF ERRONEOUS ANOMALY INDICATION IN A NETWORK NODE

Mr. Pichai Wattanaparadorn

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Engineering Program in Electrical Engineering

Department of Electrical Engineering
Faculty of Engineering
Chulalongkorn University

Academic Year 2005
ISBN 974-53-2648-8

หัวข้อวิทยานิพนธ์	การลดความผิดพลาดของการบ่งชี้ถึงความผิดปกติในโนดโครงข่าย
โดย	นายพิชัย วัฒนะภราดร
สาขาวิชา	วิศวกรรมไฟฟ้า
อาจารย์ที่ปรึกษา	ผู้ช่วยศาสตราจารย์ ดร.ชัยเชษฐ์ สายวิจิตร

คณะวิศวกรรมศาสตร์จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์

(ศาสตราจารย์ ดร. ดิเรก ลาวัณย์ศิริ)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ

(รองศาสตราจารย์ ดร.วาทิต เบญจพลกุล)

..... อาจารย์ที่ปรึกษา

(ผู้ช่วยศาสตราจารย์ ดร.ชัยเชษฐ์ สายวิจิตร)

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.เชาวน์ดิศ อัศวกุล)

..... กรรมการ

(อาจารย์ ดร.ชาญชัย ปลื้มปิติวิริยะเวช)

นาย พิชัย วัฒนะภราดร :การลดความผิดพลาดของการบ่งชี้ถึงความผิดปกติในโนด (ALLEVIATION OF ERRONEOUS ANOMALY INDICATION IN A NETWORK NODE) อ. ที่ปรึกษา: ผศ.ดร.ชัยเชษฐ์ สายวิจิตร, 101 หน้า. ISBN 974-53-2648-8.

วิทยานิพนธ์ฉบับนี้นำเสนอการปรับปรุงวิธีการตรวจจับความผิดปกติของระบบโครงข่าย 3 ส่วนคือ ในส่วนแรกเป็นการปรับปรุงวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก ด้วยกัน 4 วิธีคือ การเสนอการหาค่าถ่วงน้ำหนักแบบใหม่ การปรับค่าถ่วงน้ำหนักให้เปลี่ยนตามเวลา การใช้ข้อมูลมากกว่าหนึ่งชนิดข้อมูลร่วมกันในการตรวจจับความผิดปกติ และการใช้ค่าถ่วงน้ำหนักที่เปลี่ยนแปลงตามเวลาร่วมกับการใช้ข้อมูลมากกว่าหนึ่งชนิดข้อมูลในการตรวจจับความผิดปกติ อีกทั้งยังวิเคราะห์ถึงผลของขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติที่มีผลต่อความแน่นอนในการตรวจจับความผิดปกติที่อาจจะเกิดขึ้นในอนาคต โดยการใช้โปรแกรม *NS (Network Simulator)* ในการก่อเกิดทราฟฟิกและทดลองในการตรวจจับความผิดปกติ ในส่วนที่สองทำการวิเคราะห์ผลของวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบทันทีทันใด โดยใช้ทราฟฟิกที่ได้จากโครงข่ายของจุฬาลงกรณ์มหาวิทยาลัย ที่รูทเทอร์ 7513 และนำเสนอการเลือกใช้เกณฑ์ในการบอกว่าระบบโครงข่ายเกิดความผิดปกติหรือไม่ด้วยกัน 2 วิธี คือ การเลือกใช้ค่ากลางของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด และ การเลือกใช้ค่าเฉลี่ยของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด ในส่วนที่สามใช้วิธีการตรวจจับความผิดปกติของการเปรียบเทียบรูปแบบทราฟฟิก และเปลี่ยนแปลงทันทีทันใด ร่วมกันโดยใช้กรรมวิธีการของฟัซซี ในการตัดสินใจว่าในขณะนั้นเกิดความผิดปกติหรือไม่โดยใช้ทราฟฟิกที่ได้จากโครงข่ายของจุฬาลงกรณ์มหาวิทยาลัย ที่รูทเทอร์ 7513

ซึ่งจะเห็นได้ว่าวิธีการที่นำเสนอการปรับปรุงวิธีการตรวจจับความผิดปกติของระบบโครงข่ายนั้นจะให้ผลดีกว่าวิธีการเดิมในบางขนาดหน้าต่าง

ภาควิชา วิศวกรรมไฟฟ้า ลายมือชื่อนิสิต พิชัย วัฒนะภราดร

สาขาวิชา วิศวกรรมไฟฟ้า ลายมือชื่ออาจารย์ที่ปรึกษา

ปีการศึกษา 2548

4670410821 : MAJOR ELECTRICAL ENGINEERING

KEY WORDS: NETWORK ANOMALY / PATTERN MATCHING / ABRUPT CHANGE DETECTION

PICHAI WATTANAPARADORN : ALLEVIATION OF ERRONEOUS ANOMALY INDICATION IN A NETWORK NODE. THESIS ADVISOR : ASST. PROF. CHAIYACHET SAIVICHIT. Ph.D., 101 pp. ISBN 974-53-2648-8.

In this thesis, improving methods in detecting network anomaly have been proposed. The thesis was organized into three parts . To start with, four criterion to improve performance of network anomaly detection by Pattern Matching method are proposed; namely, finding new weighted value, time varying weighted value, multiple sets of data, and combining both techniques, respectively. Furthermore, the work also discusses on the effect of windows size in network anomaly detection process. Next, Abrupt Change Detection technique has been analyzed on its advantages and disadvantages by implementing on CUNET traffic at Router7513 and the work also proposes two methods to select appropriate threshold for anomaly detection. Two proposed methods consist of using average of fault value and using middle fault value. Finally, Pattern Matching and Abrupt Change Detection methods are used together by applying Fuzzy Logic method for proper decision on network situation. This leads to an improvement of performance in network anomaly detection which could be seen from the test with CUNET traffic at Router7513. The simulated results show that proposed methods generally give better results than the conventional methods.

Department Electrical Engineering Student's signature พิชัย วัฒนาปรดร

Field of study Electrical Engineering Advisor's signature

Academic year 2005

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปด้วยคำแนะนำและความช่วยเหลืออย่างดียิ่งจากอาจารย์ที่ปรึกษาวิทยานิพนธ์ คือ ผศ. ดร. ชัยเชษฐ์ สายวิจิตร และคำปรึกษาที่ดีจาก ผศ. ดร. เชาวน์ดิศ อัศวกุล ผู้วิจัยจึงขอกราบขอบพระคุณมา ณ ที่นี้

ขอขอบคุณพี่กำพล ที่ให้คำปรึกษาที่ดีเสมอ ขอขอบคุณ พี่ขวัญตา พี่จันทร์จิรา นางสาวพนิดา นายจิระศักดิ์ และ พี่ๆเพื่อนๆน้องๆและคนรอบตัวของผู้วิจัยทุกคน ไม่ว่าจะเป็นที่อยู่ภายในศูนย์เชี่ยวชาญเทคโนโลยีระบบโทรคมนาคม (Center of Excellence in Telecommunication System) หรือที่ใดก็ตาม สำหรับความช่วยเหลือและกำลังใจ ขอขอบคุณทุนโครงการวิจัยร่วมภาครัฐและเอกชนที่ให้การสนับสนุนเงินทุนในการทำวิจัย

สุดท้ายนี้ ผู้วิจัยขอกราบขอบพระคุณบิดามารดาและทุกคนในครอบครัวของข้าพเจ้า ซึ่งให้การสนับสนุนด้านการศึกษา รวมถึงกำลังใจและความเข้าใจที่มีให้ข้าพเจ้าเสมอมา

สารบัญ

บทที่ หน้า

บทที่ หน้า

สารบัญภาพ

ภาพประกอบ หน้า

ภาพประกอบ หน้า

ภาพประกอบ หน้า

ภาพประกอบ หน้า

ภาพประกอบ หน้า

ภาพประกอบ หน้า

สารบัญตาราง

ภาพประกอบ หน้า

บทที่ 1

บทนำ

เทคโนโลยีของระบบสื่อสารในปัจจุบันได้ถูกรวบรวมให้เป็นส่วนหนึ่งในชีวิตประจำวันของมนุษย์ ดังนั้นการพัฒนาศักยภาพของเทคโนโลยีของระบบสื่อสารจึงเป็นหัวข้อที่ได้รับความสนใจทั้งในเชิงปริมาณและเชิงคุณภาพจากนักวิจัยและผู้เชี่ยวชาญมากมาย วิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งที่ได้นำเสนอแนวทางในการพัฒนารูปแบบ และวิธีการซึ่งมีส่วนช่วยพัฒนาเทคโนโลยีของระบบสื่อสารให้มีคุณภาพดีขึ้น โดยเนื้อหาในบทนี้ได้กล่าวถึงความเป็นมาและความสำคัญของปัญหาที่นำมาศึกษา จากนั้นได้เสนอแนวทางของวิทยานิพนธ์ วัตถุประสงค์ของวิทยานิพนธ์ ขอบเขตของวิทยานิพนธ์ รวมไปถึงขั้นตอนดำเนินงาน และประโยชน์ที่คาดว่าจะได้รับ

1.1 ความเป็นมาและความสำคัญของปัญหา

เทคโนโลยีของระบบสื่อสารในปัจจุบันมีความก้าวหน้าอย่างมากเมื่อเปรียบเทียบกับในอดีต เป็นผลให้ระบบโครงข่ายในปัจจุบันมีขนาดใหญ่และมีจำนวนของอุปกรณ์สื่อสารเพิ่มมากขึ้น ซึ่งทำให้ระบบการจัดการภายในโครงข่ายมีความซับซ้อนสูงขึ้น อุปกรณ์ในระบบโครงข่ายประกอบไปด้วย รูทเทอร์ สวิตช์ ซึ่งมีหน้าที่ในการส่งข้อมูลจากต้นทางไปยังปลายทางผ่านเส้นทางที่เหมาะสม พฤติกรรมของแต่ละอุปกรณ์ในโครงข่ายสามารถบ่งบอกถึงพฤติกรรมโดยรวมของระบบโครงข่ายว่า ในขณะนั้นระบบโครงข่ายอยู่ในสถานะใด

ในงานวิจัยการตรวจจับความผิดปกติในระบบโครงข่ายโดยการวิเคราะห์ถึงพฤติกรรมของทราฟฟิกนั้น พฤติกรรมของทราฟฟิกในโครงข่ายอินเทอร์เนตได้รับความนิยมเป็นอย่างมาก เห็นได้จากบทความต่างๆมากมาย พฤติกรรมของทราฟฟิกในโครงข่ายอินเทอร์เนตมีการเปลี่ยนแปลงตลอดเวลาจึงเป็นการยากที่จะเข้าใจพฤติกรรมที่แท้จริงเหล่านี้ โดยที่ Leland et al [1] เป็นผู้แสดงถึงรูปแบบส่วนตัวและความซับซ้อนของทราฟฟิกในโครงข่ายอินเทอร์เนต ข้อมูลการใช้งานของระบบโครงข่ายไม่สามารถนำมาใช้ในการบ่งบอกถึงประสิทธิภาพและพฤติกรรมของโครงข่ายได้โดยตรง ต้องมีการนำข้อมูลที่ได้มาสังเคราะห์และวิเคราะห์ เพื่อที่จะได้เข้าใจถึงพฤติกรรมของระบบโครงข่ายได้ดียิ่งขึ้น

ความผิดปกติที่เกิดขึ้นภายในโครงข่ายและนำมาซึ่งความล้มเหลวของโครงข่ายโดยที่ระบบการจัดการภายในโครงข่ายไม่สามารถตรวจสอบได้ว่าเกิดความผิดปกติเกิดขึ้น จะส่งผลให้เกิดความเสียหายต่อระบบโครงข่ายนั้นทั้งในด้านเวลาที่ต้องสูญเสียไป และค่าใช้จ่ายที่เกิดขึ้นในภายหลัง

ด้วยเหตุดังกล่าวก่อให้เกิดความสนใจเพื่อการค้นคว้าและวิจัยมากมายเกี่ยวกับวิธีในการตรวจจับความผิดปกติของระบบโครงข่ายก่อนที่ระบบโครงข่ายจะเกิดความเสียหาย เพื่อที่จะช่วยเตือนผู้ควบคุมดูแลระบบโครงข่าย ทำการตรวจสอบและแก้ไขได้ทันท่วงที มีวิธีการตรวจจับความผิดปกติของระบบโครงข่ายหลายวิธีได้ถูกพัฒนาขึ้นเพื่อใช้ในการตรวจจับความผิดปกติ เช่น

- วิธี *Rule-Based [3]* จะบันทึกลักษณะความผิดปกติที่เกิดขึ้นของโครงข่ายในอดีตเก็บไว้ในฐานข้อมูล และนำข้อมูลในปัจจุบันมาเปรียบเทียบผลกับข้อมูลลักษณะความปกติที่ถูกบันทึกไว้ในฐานข้อมูล ถ้าตรงกันแสดงว่าเกิดความผิดปกติเกิดขึ้นในระบบโครงข่าย ซึ่งวิธีการนี้มีข้อจำกัดคือ การทำงานช้ามากในการนำไปใช้จริง วิธีการนี้ขึ้นอยู่กับข้อมูลความผิดพลาดที่บันทึกในฐานข้อมูล ทำให้เมื่อมีความผิดพลาดในลักษณะใหม่ๆเกิดขึ้นจะทำให้ไม่สามารถตรวจจับได้ ไม่สามารถเรียนรู้จากประสบการณ์ได้และยากในการปรับปรุงการตรวจจับความผิดปกติของระบบโครงข่ายที่มีการเปลี่ยนแปลงอย่างรวดเร็ว เช่น *Heterogeneous Networks*
- วิธี *Case-Base Reasoning [4]* การตรวจจับความผิดปกติของข่ายเชื่อมโยงวิธีนี้จะมีการเก็บลักษณะข้อมูลที่บรรจุพฤติกรรมของความผิดปกติ ที่เกิดขึ้นอยู่ก่อนแล้วเก็บอยู่ใน ฐานข้อมูลเช่นเดียวกับวิธี *Rule-Based* โดยหลักการตรวจจับความผิดปกติจะมีลักษณะคล้ายกับวิธี *Rule-Based* แต่วิธีนี้จะมีการปรับปรุงฐานข้อมูลความผิดปกติคือเมื่อเกิดลักษณะความผิดปกติแบบใหม่ๆ จะมีการเรียนรู้และทำการปรับปรุงฐานข้อมูลลักษณะความผิดปกติเดิมที่มีอยู่ วิธีนี้มีข้อดีคือสามารถเรียนรู้จากประสบการณ์และสามารถตรวจจับความผิดพลาดลักษณะใหม่ๆได้บนพื้นฐานของประสบการณ์ในอดีต
- วิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก [7] *(Pattern Matching)* การตรวจจับความผิดปกติของข่ายเชื่อมโยงวิธีนี้ จะมีการเก็บค่าข้อมูล เช่น การใช้ประโยชน์ของข่ายเชื่อมโยง *(Link Utilization)* การสูญหายของแพ็กเกต *(Packet Loss)* อัตราของจำนวนไบต์ของข้อมูล*(Rate of Byte Counts)* หรือ จำนวนการชนกันของข้อมูล *(Number of Collision)* ซึ่งการเก็บข้อมูลนี้จะเก็บเป็นข้อมูลของแต่ละวัน แล้วนำข้อมูลนี้มาใช้ในการทำนายข้อมูลปัจจุบันเพื่อใช้ในการตรวจจับความผิดปกติในช่วงเวลานั้น ในการทำงานของระบบโครงข่ายจะนำเอาข้อมูลจริงที่ได้มาเทียบกับข้อมูลที่เราได้ทำนายไว้แล้วภายในช่วงเวลาที่กำหนด แล้วพิจารณาว่าเกิดความผิดปกติหรือไม่ โดยมีระดับของช่วงของค่ามากที่สุดและน้อยที่สุดซึ่งยอมรับได้ว่าระบบจะไม่ผิดปกติ เป็นช่วงในการเปรียบเทียบ ถ้าค่าที่ได้ไม่อยู่ในช่วงนี้แสดงว่ามีความผิดปกติเกิดขึ้น เป็นผลให้ระบบการจัดการส่งสัญญาณว่าเกิดความผิดปกติ

เกิดขึ้น ประสิทธิภาพของวิธีนี้ขึ้นกับวิธีที่ใช้ในการทำนายทราฟฟิกปัจจุบัน และเวลาในการเก็บข้อมูลที่เพียงพอ

- วิธีการตรวจจับความผิดปกติแบบเปลี่ยนแปลงทันทีทันใด [3, 9, 10] *(Abrupt Change Detection)* การตรวจจับของข่ายเชื่อมโยงวิธีนี้ จะใช้ชุดข้อมูลของ 2 หน้าต่างมาเปรียบเทียบกัน ซึ่งประกอบด้วย *Learning Window* และ *Test Window* โดยใช้สมมุติฐานว่าถ้าการกระจายของความผิดพลาดของ 2 หน้าต่างมีลักษณะที่คล้ายกัน แสดงว่าไม่เกิดความผิดปกติของระบบโครงข่าย แต่ถ้าการกระจายของความผิดพลาดมีลักษณะที่แตกต่างกันถึงระดับหนึ่ง แสดงว่าเกิดความผิดปกติเกิดขึ้นในระบบโครงข่าย

โดยที่แต่ละวิธีของการตรวจจับความผิดปกติของระบบโครงข่ายนั้นมีข้อจำกัดหลายประการเช่น การไม่สามารถตรวจจับความผิดปกติของระบบโครงข่ายที่มีลักษณะใหม่ๆได้ หรือที่เรียกว่า *False Negative Rate* และ อีกทั้งยังมีกรณีที่มีการส่งสัญญาณเตือนที่ผิดพลาดว่ามีความผิดปกติของระบบโครงข่ายเกิดขึ้นทั้งที่ระบบโครงข่ายยังอยู่ในสภาวะที่ปกติ หรือที่เรียกว่า *False Positive Rate*

ดังนั้นปัญหาที่กล่าวมาทั้งสองประการนี้จึงเป็นสิ่งที่น่าสนใจในการนำไปสู่การปรับปรุงวิธีการแก้ไขปัญหา เพื่อประสิทธิภาพและความสามารถในการเฝ้าระวังและการตรวจสอบที่ถูกต้องของโครงข่าย

จากเหตุผลที่ได้กล่าวมาข้างต้นนี้ เราจึงได้มีการทำการศึกษาและพัฒนาวิธีการตรวจจับความผิดปกติของระบบโครงข่ายให้มีประสิทธิภาพที่ดียิ่งขึ้นโดยใช้ข้อมูลหลายๆส่วนร่วมกัน โดยใช้วิธีการของการตรวจจับความผิดปกติแบบแปรียบเทียบเทียบรูปแบบทราฟฟิก และ แบบทันทีทันใด ร่วมกันในการตรวจจับความผิดปกติ โดยใช้กรรมวิธีของฟัซซีในการตัดสินใจว่าโนดในระบบโครงข่ายเกิดความผิดปกติหรือไม่ ข้อมูลที่จะใช้ในการพิจารณาความผิดปกติของระบบโครงข่ายนั้นเราจะใช้ข้อมูลของ *MIB (Management Information Base)* ในโพโทรคอลของ *SNMP* ในการพิจารณาความผิดปกติของระบบโครงข่าย

1.2 แนวทางของวิทยานิพนธ์

ในวิทยานิพนธ์ฉบับนี้นำเสนอการปรับปรุงวิธีการตรวจจับความผิดปกติของระบบโครงข่าย 3 ส่วนคือ ในส่วนแรกเป็นการปรับปรุงวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกด้วยกัน 4 วิธีคือ การหาค่าถ่วงน้ำหนักแบบใหม่ การปรับค่าถ่วงน้ำหนักให้เปลี่ยนตามเวลา การใช้ข้อมูลมากกว่าหนึ่งชนิดข้อมูลร่วมกันในการตรวจจับความผิดปกติ และการใช้ค่า

ถ่วงน้ำหนักที่เปลี่ยนแปลงตามเวลาร่วมกับการใช้ข้อมูลมากกว่าหนึ่งชนิดข้อมูลในการตรวจจับความผิดปกติ โดยการใช้โปรแกรม *NS (Network Simulator)* ก่อเกิดทราฟฟิกและทดลองในการตรวจจับความผิดปกติ ในส่วนที่สองได้ทำการเสนอการใช้ค่าเกณฑ์แบบใหม่ในวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบทันทีทันใด ในส่วนที่สามเป็นการเสนอการใช้วิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก กับการเปลี่ยนแปลงทันทีทันใด ร่วมกันโดยใช้กรรมวิธีการของฟัซซี ในการตัดสินใจว่าในขณะนั้นเกิดความผิดปกติหรือไม่ โดยใช้ทราฟฟิกที่ได้จากโครงข่าย *CUNET* ที่รูทเทอร์หมายเลข 7513 อีกทั้งยังวิเคราะห์ถึงผลกระทบของขนาดหน้าต่างที่ใช้ในการจับความผิดปกติที่มีผลต่อความแน่นอนในการตรวจจับความผิดปกติที่อาจจะเกิดขึ้นในอนาคต

1.3 วัตถุประสงค์ของงานวิทยานิพนธ์

เพื่อศึกษาและพัฒนาวิธีการตรวจจับความผิดปกติของระบบโครงข่าย *(Network Anomaly)* ก่อนที่ระบบโครงข่ายจะเกิดความเสียหาย และ นำเสนอวิธีลดจำนวนสัญญาณเตือนที่ผิดพลาด *(False Alarm)* ในโนด วิธีการตรวจจับความผิดปกติของระบบโครงข่ายที่นำเสนอนี้ จะใช้ข้อมูลร่วมจากหลายๆส่วนมาใช้พิจารณาร่วมกันเพื่อใช้ลดความผิดพลาดของสัญญาณเตือน และสามารถรู้ได้ว่าความผิดปกติของระบบโครงข่ายเกิดมาจากตำแหน่งใด โดยจะส่งผลให้ผู้ดูแลระบบโครงข่าย *(Network Administrator)* รีบตรวจสอบและแก้ไขปัญหาของระบบโครงข่ายที่เกิดขึ้นก่อนที่ความเสียหายจะเกิดขึ้น

1.4 ขอบเขตวิทยานิพนธ์

วิทยานิพนธ์ฉบับนี้เสนอการปรับปรุงวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก *(Pattern Matching)* โดยใช้ทราฟฟิคที่ก่อกำเนิดจากโปรแกรม *NS(Network Simulator)* ในการทดสอบ เสนอวิธีการใช้ค่าเกณฑ์แบบใหม่ในการตรวจจับความผิดปกติในระบบโครงข่ายแบบทันทีทันใด *(Abrupt Change)* และ เสนอการใช้การตรวจจับความผิดปกติของระบบโครงข่ายแบบเปรียบเทียบรูปแบบทราฟฟิก กับวิธีการตรวจจับแบบทันทีทันใดร่วมกัน โดยใช้กรมมวิธีของฟัซซี ในการตัดสินใจว่าเกิดความผิดปกติหรือไม่ในระบบโครงข่าย โดยใช้ทราฟฟิกที่ได้จากโครงข่าย *CUNET* ที่รูทเทอร์ 7513 ในการตรวจจับความผิดปกติในระบบโครงข่าย

1.5 ขั้นตอนการทำงาน

1. ศึกษางานวิจัยที่เกี่ยวข้อง พร้อมทั้งความรู้และทฤษฎีพื้นฐานที่ต้องใช้ในงานวิจัย

2. ศึกษาวิธีการของการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก การเปลี่ยนแปลงทันทีทันใด และฟัซซี ในการตรวจจับความผิดปกติในระบบโครงข่าย

3. กำหนดแบบจำลองที่ต้องการศึกษา

4. เขียนโปรแกรมทดสอบวิธีที่เสนอ

5.วิเคราะห์และประเมินผลการทดลองและเปรียบเทียบผลกับวิธีที่มีอยู่

6.สรุป วิจารณ์ และรวบรวมข้อมูลทั้งหมด พร้อมทั้งจัดทำรูปเล่มวิทยานิพนธ์

1.6 ประโยชน์ที่คาดว่าจะได้รับ

สามารถนำวิธีการตรวจจับความผิดปกติ ของระบบโครงข่ายนี้ ไปใช้ในการช่วยผู้ดูแลระบบโครงข่ายเพื่อเตือนว่าระบบโครงข่ายกำลังมีความผิดปกติเกิดขึ้น ซึ่งจะส่งผลให้ระบบโครงข่ายสามารถตรวจสอบและแก้ไขปัญหาได้ทันท่วงทีก่อนที่ความเสียหายจะเกิดขึ้น

บทที่ 2

ความรู้พื้นฐานและทฤษฎีที่เกี่ยวข้อง

การแยกแยะพฤติกรรมของระบบโครงข่ายประกอบไปด้วย 2 วิธี คือ 1. การศึกษาที่พฤติกรรมของระบบโครงข่ายโดยรวม และ 2. การศึกษาที่พฤติกรรมของแต่ละอุปกรณ์ในระบบโครงข่าย

ข้อมูลที่ใช้ในการวิเคราะห์เพื่อบอกถึงสภาวะของระบบโครงข่ายว่าเกิดความผิดปกติหรือไม่ สามารถได้จากข้อมูลของ *End-User-Based* และ *Network-Based*

ข้อมูล *End-User-Based* เกี่ยวข้องกับข้อมูลของ *Transmission Control Protocol (TCP)* และ *User Datagram Protocol (UDP)* ส่วนข้อมูล *Network-Based* นั้นเกี่ยวข้องกับหน้าที่ของแต่ละอุปกรณ์รวมถึงข้อมูลที่ถูกรวบรวมจากทุกๆการเชื่อมต่อทางกายภาพของรูทเทอร์ การตรวจจับความผิดปกติในระบบโครงข่ายโดยทั่วไปจะใช้ข้อมูลของผลรวมของทราฟฟิกในแต่ละช่วงเวลา อย่างไรก็ตามในบางกรณีเราจะใช้ จำนวนการเชื่อมต่อของ *TCP* คู่ที่อยู่ของต้นทางและปลายทาง และจำนวนพอร์ตในการตรวจจับความผิดปกติในระบบโครงข่าย

ความผิดปกติโครงข่ายทั่วไปจะเป็นสถานการณ์เมื่อการปฏิบัติการของโครงข่ายเบี่ยงเบนไปจากพฤติกรรมที่ปกติ ความผิดปกติของระบบโครงข่ายสามารถเกิดได้เนื่องจากหลายๆสาเหตุ เช่น อุปกรณ์ในโครงข่ายทำงานผิดพลาด การใช้งานที่มากเกินไปในโครงข่าย และการจู่โจมโครงข่ายโดยผู้ที่ไม่ประสงค์ดี เหตุการณ์ที่ผิดปกติเหล่านี้จะรบกวนพฤติกรรมปกติของบางข้อมูลโครงข่ายที่ถูกวัด

ความผิดปกติของระบบโครงข่ายสามารถแบ่งแยกได้ 2 กรณีคือ

1. ความผิดปกติที่เกี่ยวข้องกับความล้มเหลวและปัญหาประสิทธิภาพของระบบโครงข่าย ตัวอย่างเช่น *File Server Failures, Paging Across The Network, Broadcast Storms, Babbling Node* และ *Transient Congestion* โดยที่ *File Server Failures* เช่น *Web Server Failure* ปรากฏเมื่อมีการเพิ่มขึ้นของจำนวนของความต้องการ *FTP* ถึง *Server Broadcast Storm* เป็นสถานะซึ่ง *Broadcast Packet* ถูกส่งเป็นจำนวนมากจนโครงข่ายไม่สามารถทำงานได้ *Babbling Node* เป็นสถานการณ์ที่โนดส่งออกแพ็กเกตเล็กๆออกมาในลูปไม่สิ้นสุด

2. ความผิดปกติที่เกี่ยวข้องกับปัญหาของความปลอดภัย ตัวอย่างเช่น *Denial of Service Attack (DoS)* ปรากฏเมื่อระบบที่ให้บริการถูกใช้งานอย่างหนักโดยผู้ประสงค์ร้าย จนการให้บริการไม่สามารถทำงานได้ เช่น การจู่โจม *DNS (Domain Name Server)* โดยผู้ประสงค์ร้ายจนทำให้ผู้ต้องการใช้บริการจริงๆไม่สามารถได้รับ ไอพี ที่แสดงที่อยู่ของเวปที่ต้องการใช้งานได้

แหล่งข้อมูลโครงข่ายที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่ายประกอบไปด้วย

- *Network Probe* เป็นเครื่องมือที่ใช้กันอย่างกว้างขวางในการบอกสถานะของระบบโครงข่ายอย่างคร่าวๆเช่น *Ping* และ *Traceroute* ซึ่งสามารถบอกถึงสถานะของโครงข่ายในขณะนั้นว่ามี ค่าหน่วงเวลาระหว่างต้นทางและปลายทาง และจำนวนแพ็กเกตที่สูญหายเป็นเท่าใด

- *Packet Filtering For Flow-Based Statistics* เป็นการกรองแพ็กเกตโดยการสุ่ม *IP Header* ของแพ็กเกตที่จุดแตกต่างกันในโครงข่าย ข้อมูลที่ถูกรวบรวมจาก *IP Header* บอกถึงประสิทธิภาพโครงข่าย สำหรับการวัดนั้นจะถูกจำแนกโดยที่อยู่ของต้นทางและปลายทาง หมายเลขพอร์ตของต้นทางและปลายทาง วิธีการกรองแพ็กเกตต้องการเทคนิคการสุ่มที่ซับซ้อนเช่นเดียวกับฮาร์ดแวร์ที่มีประสิทธิภาพ

- *Data From Routing Protocols*

เป็นข้อมูลเกี่ยวกับเหตุการณ์ที่เกิดขึ้นในโครงข่ายจากการใช้ข้อมูลของ *Routing Protocol* ตัวอย่างเช่นการใช้ *Open Shortest Path First (OSPF)* จะรวมการปรับปรุงตารางเส้นทางทั้งหมด ซึ่งเป็นการถูกส่งโดยรูทเทอร์ ข้อมูลที่ถูกสะสมนี้สามารถถูกใช้ในการบอกถึงสถานการณ์เชื่อมต่อของโครงข่ายและใช้ในการจัดสรรการปรับปรุงสถานะข่ายเชื่อมโยง

- *Data from Network Management Protocol*

เป็นโปรโตคอลการจัดการโครงข่ายทางสถิติของทราฟฟิกในโครงข่าย โปรโตคอลเหล่านี้จะเก็บค่าตัวแปรหลายๆค่าที่เกี่ยวข้องกับการนับทราฟฟิกที่วิ่งผ่านอุปกรณ์ ซึ่งข้อมูลที่ได้อาจจะไม่สามารถนำไปใช้อย่างตรงไปตรงมา แต่เราสามารถนำข้อมูลนั้นมาวิเคราะห์ และจำแนกพฤติกรรมของโครงข่าย ซึ่งต้องอาศัยซอฟท์แวร์การจัดการโครงข่าย อย่างไรก็ตามโปรโตคอลเหล่านี้สามารถบอกคุณสมบัติของข้อมูลได้ทุกๆระดับความละเอียด

- *Simple Network Management Protocol (SNMP)*

SNMP ทำงานในแบบแม่ข่ายลูกข่าย ซึ่งโปรโตคอลนี้จะจัดสรรการสื่อสารระหว่าง *SNMP MANAGER* และ *SNMP AGENT* โดยที่ *SNMP MANAGER* 1 ตัว สามารถรับข้อมูลการใช้บริการจาก *SNMP AGENT* ที่เป็นลูกข่ายได้ถึง 100 ตัว *SNMP MANAGER* มีความสามารถในการสะสมข้อมูลการจัดการซึ่งถูกส่งโดย *SNMP AGENT* แต่ไม่มีความสามารถในการประมวลผลข้อมูลการจัดการ ข้อมูลที่เก็บใน *SNMP MANAGER* นี้จะถูกเรียกว่า *Management Information Base (MIB)* ซึ่งบรรจุชนิดข้อมูลที่แตกต่างกันขึ้นอยู่กับชนิดของ *MIB* ตัวอย่างเช่น *Bridges* ซึ่งเป็นอุปกรณ์ที่อยู่ในชั้น *Data Link Layer* จะวัดข้อมูลทราฟฟิกระดับข่ายเชื่อมโยง รูทเทอร์ซึ่งเป็นอุปกรณ์ในชั้น *Network Layer* จะวัดข้อมูลในชั้น *Network Layer* ข้อได้เปรียบของการใช้ *SNMP* คือเป็นโปรโตคอลที่ใช้กัน

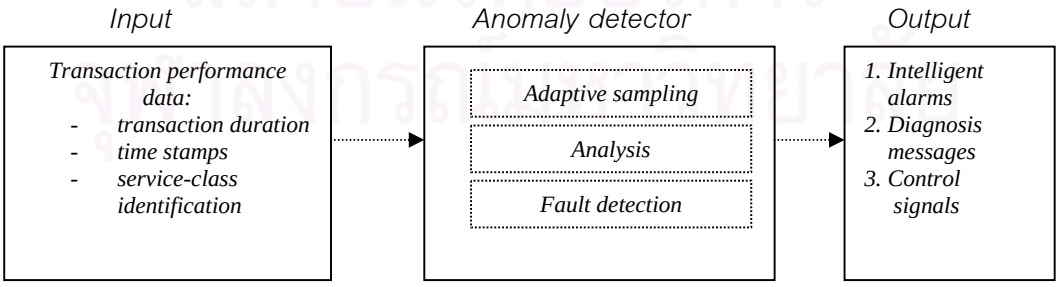
อย่างกว้างขวางและเป็นมาตรฐานสำหรับทุกๆอุปกรณ์โครงข่ายที่แตกต่างกัน เนื่องจากเราสามารถได้ข้อมูลที่ละเอียดจาก *SNMP* ดังนั้น *SNMP* จึงเป็นแหล่งข้อมูลเชิงอุดมคติสำหรับการตรวจจับความผิดปกติในระบบโครงข่าย

- *SNMP-MIB Variables*

MIB ประกอบอยู่ในโปรโตคอลเหล่านี้คือ *System, Interfaces (If), Address Translation (AT), Internet Protocol (IP), Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Exterior Gateway Protocol (EGP)* และ *Simple Network Management Protocol (SNMP)* อุปกรณ์ในระบบโครงข่ายจะมีชนิดของข้อมูลที่เหมาะ เช่น ถ้าโนดที่ถูกวัดเป็นรูทเทอร์ เมื่อนั้น *IP GROUP* ของตัวแปร *MIB* จะถูกนำมาใช้ ตัวแปร *IP* อธิบายลักษณะทราฟฟิกในชั้น *Network Layer*

2.1 ทฤษฎีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก*(Pattern Matching)*

หลักการการตรวจจับความผิดปกติของข่ายเชื่อมโยงโดยวิธีนี้ จะมีการเก็บค่าข้อมูล เช่น การใช้ประโยชน์ของข่ายเชื่อมโยง *(Link Utilization)* การสูญหายของแพ็กเกต *(Packet Loss)* อัตราของจำนวนไบต์ของข้อมูล*(Rate of Byte Counts)* หรือ จำนวนการชนกันของข้อมูล *(Number of Collision)* ซึ่งการเก็บข้อมูลนี้จะเก็บเป็นข้อมูลของแต่ละวัน แล้วนำข้อมูลนี้มาใช้ในการทำนายข้อมูลปัจจุบันเพื่อใช้ในการตรวจจับความผิดปกติในช่วงเวลานั้น ในการทำงานจริงระบบโครงข่ายจะนำเอาข้อมูลจริงที่ได้มาเทียบกับข้อมูลที่เราได้ทำนายไว้แล้วภายในช่วงเวลาที่กำหนด แล้วพิจารณาว่าเกิดความผิดปกติหรือไม่ โดยมีช่วงของค่ามากที่สุดและน้อยที่สุดซึ่งยอมรับได้ว่าระบบไม่มีความผิดปกติเป็นช่วงที่ใช้ในการเปรียบเทียบ ถ้าค่าที่ได้ไม่อยู่ในช่วงนี้ แสดงว่ามีความผิดปกติเกิดขึ้น เป็นผลให้ระบบการจัดการส่งสัญญาณว่าเกิดความผิดปกติเกิดขึ้น ประสิทธิภาพของวิธีนี้ขึ้นกับวิธีที่ใช้ในการทำนายทราฟฟิกปัจจุบัน และเวลาในการเก็บข้อมูลที่เพียงพอ ดังรูปที่ 2.1



รูปที่ 2.1 แบบจำลองของ *pattern matching [5]*

กำหนดให้ $I(t)$ คือ ค่าเฉลี่ยของทราฟฟิกที่ใช้ในการทำนายลักษณะทราฟฟิกในปัจจุบันเพื่อใช้ในการเปรียบเทียบกับทราฟฟิกทางปฏิบัติ

โดยที่ $$I(t) = \alpha(t) + \beta(t) + \varepsilon(t) \quad (2.1)$$

ซึ่ง $\alpha(t)$ คือ ค่าเฉลี่ยของทราฟฟิกของช่วงเวลาในแต่ละวัน

$\beta(t)$ คือ ค่าเฉลี่ยของทราฟฟิกของช่วงเวลาในวันเสาร์ วันอาทิตย์ หรือ วันหยุดพิเศษ เช่น วันปีใหม่ วันสงกรานต์ วันลงทะเบียน ฯลฯ

$\varepsilon(t)$ คือ เป็นค่าเบี่ยงเบนเฉลี่ยของทราฟฟิกของ $\alpha(t)$ และ $\beta(t)$

โดยที่ $\alpha_j(t)$ นั้นสามารถหาค่าได้จากการถ่วงน้ำหนักของข้อมูลทราฟฟิกของวันจันทร์ถึงวันศุกร์ในสัปดาห์ที่แล้วโดยไม่รวมวันที่เราสนใจ ดังสมการที่ (2.2)

$$\alpha_j(t) = \sum_{k \in \{1,\ldots,5\} - \{j\}} c_{j,k}{}' \alpha_k(t) \quad (2.2)$$

ซึ่ง $j = \{1,2,3,4,5\}$ โดยที่ 1 แทนวันจันทร์ 2 แทนวันอังคาร และ อื่นๆ

$k \in \{1,\ldots,5\} - \{j\}$ โดยที่ 1 แทนวันจันทร์ 2 แทนวันอังคาร และ อื่นๆ

$c_{j,k}{}'$ คือค่าถ่วงน้ำหนักของวันที่ j เทียบกับวันที่ k

และ $$\sum_k c_{j,k}{}' = 1 \quad (2.3)$$

$\beta_j(t)$ นั้นสามารถหาค่าได้จากการถ่วงน้ำหนักของข้อมูลทราฟฟิกของวันเสาร์ วันอาทิตย์ หรือ วันหยุดพิเศษ ใน 4 สัปดาห์ที่แล้ว โดยไม่รวมสัปดาห์ที่สนใจ

$$\beta_j(t) = \sum_{k \in \{1,\ldots,4\} - \{j\}} d_{j,k}{}' \beta_k(t) \quad (2.4)$$

ซึ่ง $j = \{1,2,3,4\}$ โดยที่ 1 แทน หลังจากสัปดาห์ปัจจุบัน 1 สัปดาห์ 2 แทน หลังจากสัปดาห์ปัจจุบัน 2 สัปดาห์ เป็นต้น

$k \in \{1,\ldots,4\} - \{j\}$ โดยที่ 1 แทน หลังจากสัปดาห์ปัจจุบัน 1 สัปดาห์ 2 แทน หลังจากสัปดาห์ปัจจุบัน 2 สัปดาห์ เป็นต้น

$d_{j,k}$ คือค่าถ่วงน้ำหนักของสัปดาห์ที่ j เทียบกับสัปดาห์ที่ k

และ $$\sum_k d_{j,k}{}' = 1 \quad (2.5)$$

ค่าของ $c_{m,n}$ หาได้จากค่าเฉลี่ยของอัตราส่วนของทราฟฟิกในแต่ละเวลาของทราฟฟิกของวันที่ m กับทราฟฟิกรวมของวันที่ n ส่วนค่าของ $d_{m,n}$ หาได้จากค่าเฉลี่ยของอัตราส่วนของทราฟฟิกในแต่ละเวลาของทราฟฟิกของวันหยุดสุดสัปดาห์ของสัปดาห์ที่ m กับทราฟฟิกรวมของวันหยุดสุดสัปดาห์ของสัปดาห์ที่ n ดังสมการที่ (2.6) และ (2.7) ตามลำดับ

$$c_{m,n}{}' = \sum_{\forall t} \alpha_m(t) / \alpha_n(t) \quad (2.6)$$

$$d_{m,n}{}' = \sum_{\forall t} \beta_m(t) / \beta_n(t) \quad (2.7)$$

ค่าของ $\varepsilon_{wk,j}(t), \varepsilon_{wked,j}(t)$ สามารถหาได้จากสมการที่ (2.8) และ (2.9) ตามลำดับ

$$\{<[\varepsilon_{wk,j}(t)]^2>_t\}^{\frac{1}{2}} = \sum_{k\in\{1,\ldots,5\}-\{j\}} c_{j,k}{}'\{<[\varepsilon_{wk,k}(t)]^2>_t\}^{\frac{1}{2}} \quad (2.8)$$

$$\{<[\varepsilon_{wked,j}(t)]^2>_t\}^{\frac{1}{2}} = \sum_{k\in\{1,\ldots,4\}-\{j\}} d_{j,k}{}'\{<[\varepsilon_{wked,k}(t)]^2>_t\}^{\frac{1}{2}} \quad (2.9)$$

โดยที่ $\varepsilon_{wk,j}(t)$ คือ ค่าการเบี่ยงเบนของทราฟฟิกของวันที่ j ของวันธรรมดา

$\varepsilon_{wked,j}(t)$ คือค่าการเบี่ยงเบนของทราฟฟิกของเสัปดาห์ที่ j ของวันหยุดสุดสัปดาห์

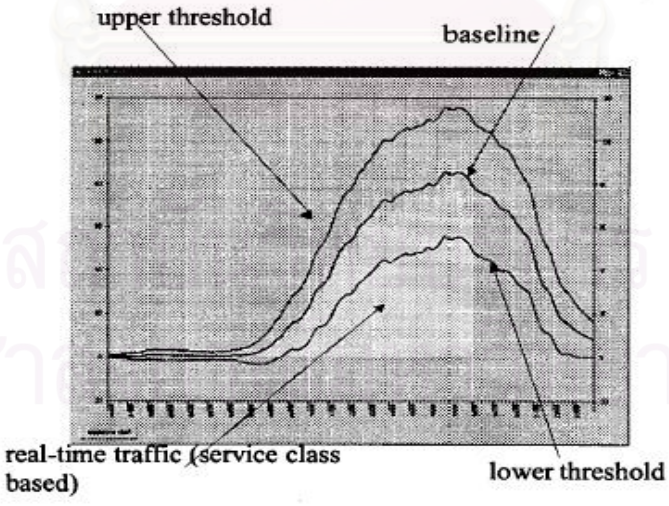
ค่าขอบเขตบนและขอบเขตล่างที่ได้จาการทำนายเพื่อใช้ในการตรวจจับความผิดปกติของระบบโครงข่าย แสดงในสมการที่ (2.10) (2.11) และ (2.12) ตามลำดับ

ค่าขอบเขตบน = $I(T_n) + 2\bar{\sigma}(T_n)$ (2.10)

ค่ากลาง = $I(T_n)$ (2.11)

ค่าขอบเขตล่าง = $I(T_n) - 2\bar{\sigma}(T_n)$ (2.12)

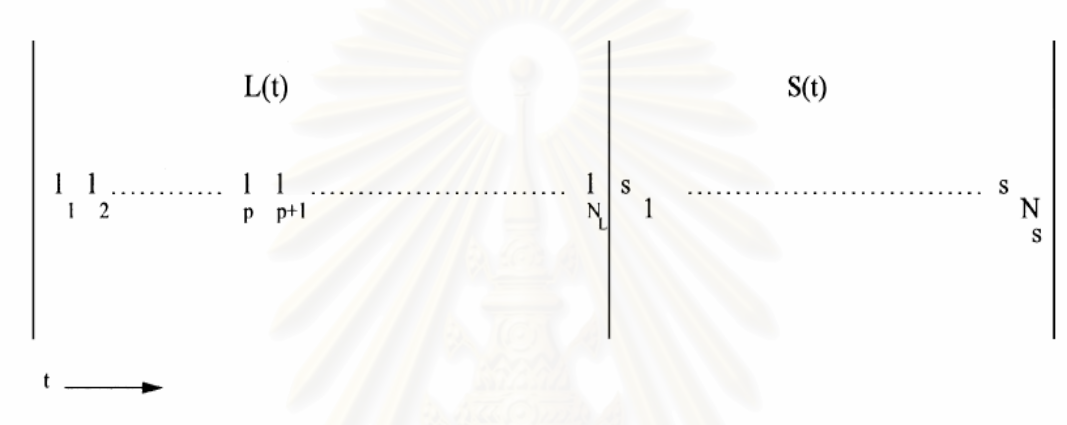
ความผิดปกติของระบบโครงข่ายจะเกิดขึ้นเมื่อค่าเฉลี่ยของทราฟฟิกจริงที่วัดได้ไม่อยู่ภายในขอบเขตบนและขอบเขตล่างของทราฟฟิคที่ทำนายได้แสดงดังรูปที่ 2.2



รูปที่ 2.2 การเปรียบผลของทราฟฟิคว่าระบบโครงข่ายนั้นมีลักษณะผิดปกติหรือไม่ [7]

2.2 ทฤษฎีการตรวจจับความผิดปกติแบบทันทีทันใด *(Abrupt Change Detection)*

การตรวจจับความผิดปกติแบบทันทีทันใดนั้น จะใช้การทดสอบสมมติฐานบน *Generalized Likelihood Ratio (GLR)* โดยที่การตรวจจับการเปลี่ยนแปลงทันทีทันใดนั้นจะใช้ค่าเบี่ยงเบนมาตรฐาน *(Standard Deviation) [6]* ของหน้าต่าง *(Window)* 2 ชุดเปรียบเทียบกันคือในช่วง *Learning Window (L(t))* และ *Test Window (S(t))* ดังรูปที่ 2.3



รูปที่ 2.3 *Learning Window (L(t))* และ *Test Window (S(t)) [3]*

โดยที่ภายในหน้าต่างของ *Learning Window* และ *Test Window* นั้นประกอบด้วย ข้อมูลที่เรียงกันตามเวลาจำนวน N_L ค่า และ N_S ค่าตามลำดับ

เรากำหนดให้ $\tilde{r}_i(t)$ คือ ความผิดพลาดของจุดข้อมูลที่ตำแหน่งที่ i จากค่าเฉลี่ยของข้อมูลทั้งหมด ดังสมการที่ (2.13)

$$\tilde{r}_i(t) = r_i(t) - \mu \tag{2.13}$$

โดยที่ $r_i(t)$ คือ ค่าของข้อมูลที่ตำแหน่งที่ i

μ คือ ค่าเฉลี่ยของข้อมูลทั้งหมดในช่วงเวลา t

ดังนั้นความผิดพลาดของจุดของข้อมูลที่ปรากฏนั้นเราสามารถที่จะประมาณด้วยวิธีการของ *Auto Regressive (AR)* ดังสมการที่ (2.14)

$$\varepsilon_i(t) = \sum_{k=0}^{p} \alpha_k \tilde{r}_i(t-k) \tag{2.14}$$

ซึ่ง $\varepsilon_i(t)$ คือ ความผิดพลาดของข้อมูลที่ตำแหน่งที่ i ส่วน α_k นั้นเป็นค่าตัวแปรที่ใช้ในการ

ถ่วงน้ำหนักในการประมาณค่า $\varepsilon_i(t)$ และ p เป็นจำนวนข้อมูลในอดีตที่เราจะใช้ในการประมาณค่า $\varepsilon_i(t)$ ของวิธี *Auto Regressive*

ถ้าเราใช้วิธีการทดสอบสมมติฐาน *(Hypothesis Testing)* ในการบอกถึงความผิดปกติที่เกิดขึ้นระหว่าง 2 หน้าต่าง คือ *Test Window* และ *Learning Window* โดยที่ กำหนดให้ H_0 แสดงถึงสมมติฐานซึ่งไม่มีการเปลี่ยนแปลงเกิดขึ้นระหว่าง 2 หน้าต่าง เราจะได้ *Likelihood,* LI_0 มีค่าเท่ากับ

$$LI_0 = \left(\frac{1}{\sqrt{2\pi\sigma_P{}^2}} \right)^{N_L{}' + N_S{}'} \exp\left(\frac{-(N_L{}' + N_S{}')\hat{\sigma}_P{}^2}{2\sigma_P{}^2} \right) \tag{2.15}$$

และกำหนดให้ H_1 แสดงถึงสมมติฐานซึ่งมีความเปลี่ยนแปลงเกิดขึ้นระหว่าง 2 หน้าต่าง เราจะได้ *Likelihood,* LI_1 มีค่าเท่ากับ

$$LI_1 = \left(\frac{1}{\sqrt{2\pi\sigma_L{}^2}} \right)^{N_L{}'} \left(\frac{1}{\sqrt{2\pi\sigma_S{}^2}} \right)^{N_S{}'} \exp\left(\frac{-N_L{}'\hat{\sigma}_L{}^2}{2\sigma_L{}^2} \right) \exp\left(\frac{-N_S{}'\hat{\sigma}_S{}^2}{2\sigma_S{}^2} \right) \tag{2.16}$$

โดยที่ σ_L คือ ค่าเบี่ยงเบนมาตรฐานของข้อมูลที่ปรากฏใน *Learning Window*

σ_S คือ ค่าเบี่ยงเบนมาตรฐานของข้อมูลที่ปรากฏใน *Test Window*

σ_P คือ ค่าเบี่ยงเบนมาตรฐานรวมของข้อมูลที่ปรากฏใน *Learning* และ *Test Window*

$\hat{\sigma}_L$ คือ ค่าเบี่ยงเบนมาตรฐานของค่าความผิดพลาดของจุดข้อมูลที่ปรากฏใน *Learning Window*

$\hat{\sigma}_S$ คือ ค่าเบี่ยงเบนมาตรฐานของค่าความผิดพลาดของจุดข้อมูลที่ปรากฏใน *Test Window*

$\hat{\sigma}_P$ คือ ค่าเบี่ยงเบนมาตรฐานรวมของค่าความผิดพลาดของจุดข้อมูลที่ปรากฏใน *Learning* และ *Test Window*

ซึ่ง
$$N_L{}' = N_L - p \tag{2.17}$$

$$N_S{}' = N_S - p \tag{2.18}$$

ดังนั้นเราจะกำหนดให้ *Likelihood Ratio* η *[7],[8]* ซึ่งมีค่าอยู่ในช่วง (0,1) ซึ่ง 0 หมายถึงปกติ ในขณะที่ 1 หมายถึง ผิดปกติ โดยที่ η นั้นเป็นตัวบ่งชี้ความผิดปกติของข้อมูลที่ใช้วิเคราะห์ ดังสมการที่ (2.19)

$$\eta = \frac{LI_1}{LI_1 + LI_0} \tag{2.19}$$

โดยการใช้วิธีของ *Maximum Likelihood Estimate* เพื่อประมาณค่าของความแปรปรวนของข้อมูลในสมการที่ (2.15) และ สมการที่ (2.16) เราจะได้ว่า $\sigma_L^{\,2} = \hat{\sigma}_L^{\,2}$ $\sigma_P^{\,2} = \hat{\sigma}_P^{\,2}$ และ $\sigma_S^{\,2} = \hat{\sigma}_S^{\,2}$ ดังนั้นเราจะได้

$$\eta = \frac{\hat{\sigma}_L^{\,-N_L'} \hat{\sigma}_S^{\,-N_S'}}{\hat{\sigma}_L^{\,-N_L'} \hat{\sigma}_S^{\,-N_S'} + \hat{\sigma}_P^{\,-(N_L'+N_S')}} \tag{2.20}$$

ในกรณีที่เรามีการใช้ข้อมูลหลายระดับในการตรวจจับความผิดปกตินั้น เราจะมีการกำหนดถึง $\vec{\psi}(t)$ เป็นเวกเตอร์ความผิดปกติ โดยที่ความผิดปกติของข้อมูลหลายระดับจะถูกจัดเก็บ ในเวกเตอร์ความผิดปกตินี้ ดังสมการที่ (2.21)

$$\vec{\psi}(t) = [\eta_1(t).....\eta_m(t)] \tag{2.21}$$

จากผลของเวกเตอร์ความผิดปกติที่ได้จากความผิดปกติของชนิดข้อมูลหลายระดับ เราจะมีการนิยามฟังก์ชันสุขภาพของโครงข่าย *(Network Health Function)* เป็น $(f(\vec{\psi}(t))$ ดังสมการที่ (2.22)

$$f(\vec{\psi}(t)) = \vec{\psi}(t) A \vec{\psi}^{T}(t) \tag{2.22}$$

โดยที่ฟังก์ชันสุขภาพของโครงข่ายนั้น เป็นตัวบ่งชี้ถึงความผิดปกติของระบบโครงข่าย ซึ่ง 0 แสดงว่าระบบโครงข่ายเป็นปกติ และ 1 แสดงถึงระบบโครงข่ายเกิดความผิดปกติแน่นอน

โดยเมตริกซ์ A เป็นเมตริกซ์ที่แสดงถึงความสัมพันธ์กันของความผิดปกติของข้อมูลหลายระดับ มีขนาด $M \times M$ โดยที่ M เป็นจำนวนของข้อมูลที่ใช้ในการตรวจจับความผิดปกติ ดังสมการที่ (2.23)

$$A = \begin{bmatrix} a_{11} & a_{12} & . & . & a_{1(M-1)} & a_{1M} \\ a_{21} & a_{22} & . & . & a_{2(M-1)} & a_{2M} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ a_{M1} & a_{M2} & a_{M3} & a_{M.} & a_{M(M-1)} & a_{MM} \end{bmatrix} \tag{2.23}$$

การหาค่าของเมตริกซ์ A เราสามารถแบ่งได้เป็น 2 กรณีคือ

กรณีที่ $i \neq j$

$$\begin{aligned} A(i,j) &= |< \eta_i(t), \eta_j(t) >| \\ &= \frac{1}{T} \left| \sum_{t=1}^{T} \eta_i(t) \eta_j(t) \right| \end{aligned} \tag{2.24}$$

กรณีที่ $i = j$

$$A(i,i) = 1 - \sum_{j \neq i} A(i,j) \tag{2.25}$$

ซึ่งเมตริกซ์ A นั้นสามารถหาค่าจำนวน M ค่าของ *Orthogonal Eigenvectors* และจำนวน M ค่าของ *Eigenvalues* ที่เป็นค่าจริง ดังสมการที่ (2.26) โดยที่ A นั้นเป็นเมตริกซ์ที่สมมาตร *(Symmetric)*

$$A\bar{\phi} = \lambda\bar{\phi} \tag{2.26}$$

ในกรณีที่เวกเตอร์ความผิดปกติ $\vec{\psi}(t)$ ขึ้นอยู่กับค่า *Orthogonal Eigenvectors,* $\vec{\phi}$ ตั้งแต่เวกเตอร์ที่ N ถึง M ดังสมการที่ (2.27)

$$\vec{\psi}^T(t) = \sum_{i=N}^{M} c_i \vec{\phi}_i \tag{2.27}$$

Orthogonal Eigenvector ในกรณีนี้จะถูกเรียกว่า เวกเตอร์ความผิดพลาด *(Fault vector)* และค่า *Eigenvalues* ของเวกเตอร์ความผิดพลาดจะถูกเรียกว่า ค่าความผิดพลาด *(Fault value)* ซึ่งเวกเตอร์ความผิดพลาดและค่าความผิดพลาดนี้จะเป็นตัวบอกถึงขอบเขตของความผิดพลาดของระบบโครงข่าย โดยที่

$$\sum_{i=1}^{M} {c_i}^2 = 1 \tag{2.28}$$

c_i คือ ขนาดของระดับซึ่งเวกเตอร์ความผิดปกติตกอยู่ใน *Eigenvector* ที่ *i*

c_i^2 คือ ความน่าจะเป็นของการอยู่ใน *Eigenstate* ที่ *i*

กำหนดให้ λ_N และ λ_M คือค่าน้อยที่สุดและค่ามากที่สุดของค่าความผิดพลาด โดยที่ค่าความผิดพลาด λ_N ถึง λ_M มีค่าเวกเตอร์ความผิดพลาดที่อยู่ใกล้กับเวกเตอร์ความผิดปกติ[1 1 1] มากกว่าค่าความผิดพลาด λ_1

ในการพิจารณาค่าของฟังก์ชันสุขภาพของโครงข่ายนั้นจะมีค่า α เป็น *Normalization Constant* เพื่อที่จะทำให้ค่าของฟังก์ชันสุขภาพของโครงข่ายมีค่าอยู่ในช่วง (0,1) ดังสมการที่ (2.29)

$$\vec{\psi}(t) = \alpha[\eta_1(t).....\eta_m(t)] \tag{2.29}$$

จากคุณสมบัติของค่า *Eigenvalues* และ *Eigenvector* เราจะเห็นได้ว่าค่าของฟังก์ชันสุขภาพของโครงข่ายมีค่าเท่ากับค่าเฉลี่ยของค่าความผิดพลาดดังสมการที่ (2.30)

$$\begin{aligned} \vec{\psi}(t) A \vec{\psi}^T(t) &= \sum_{i=N}^{M} {c_i}^2 \lambda_i \\ &= E(\lambda) \end{aligned} \tag{2.30}$$

โดยที่ $E(\lambda)$ คือตัวบอกถึงค่าเฉลี่ยความผิดปกติของโครงข่าย และจะได้

$$\lambda_i \in \{\lambda_N, \lambda_{N+1}, ..., \lambda_M\} \min(\lambda_i) \leq E(\lambda) \leq \lambda_i \in \{\lambda_N, \lambda_{N+1}, ..., \lambda_M\} \max(\lambda_i) \quad (2.31)$$

เพราะฉะนั้นการตรวจจับความผิดปกติของโครงข่ายนี้จะเกิดสัญญาณเตือนโดยเงื่อนไขคือ

$$E(\lambda) > \lambda_i \in \{\lambda_N, \lambda_{N+1}, ..., \lambda_M\} \min(\lambda_i) \quad (2.32)$$

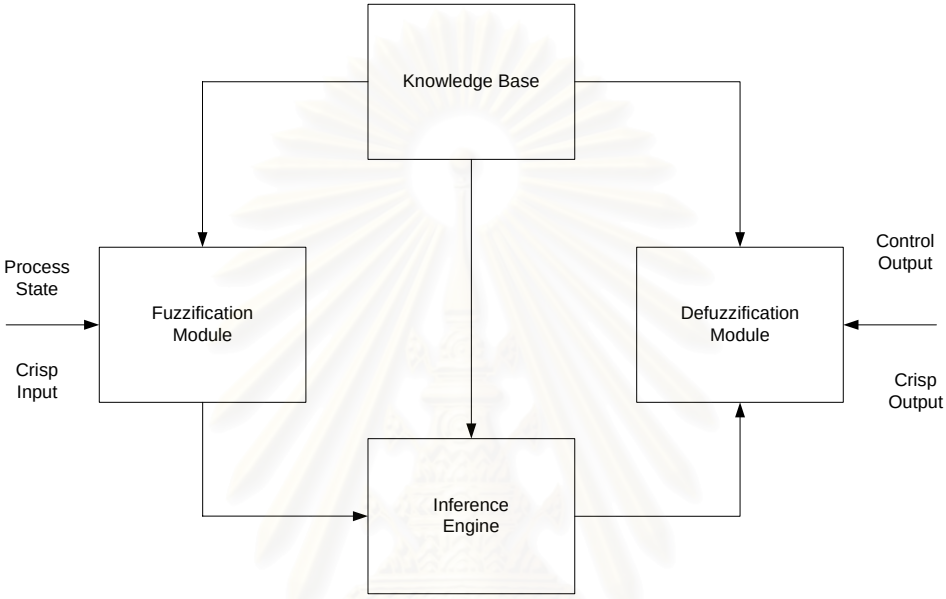
2.3 **ทฤษฎีของ** *Fuzzy Logic*

ในปี 1965 *L.A.Zadeh* ได้เสนอบทความเรื่องฟัซซีเซต *(Fuzzy Sets)* โดยให้เหตุผลว่ามนุษย์ทำการตัดสินใจและแก้ปัญหาได้ดีกว่าเครื่องจักร เพราะการตัดสินใจสามารถกระทำอย่างมีประสิทธิภาพบนพื้นฐานของสารสนเทศเชิงบรรยายที่ไม่เที่ยงตรง และการแก้ไขปัญหาก็จะกระทำโดยอาศัยความรู้และประสบการณ์ ซึ่งแนวทางการตัดสินใจและวิเคราะห์ปัญหาจะอยู่ในรูปแบบตรรกที่คลุมเคลือ *(Fuzzy)*

ตัวควบคุมแบบฟัซซีถูกตีพิมพ์ครั้งแรกในปี 1974 โดย *E.H.Mamdani* แทนการใช้ตัวควบคุมพีไอแบบดั้งเดิม โดยตัวควบคุมแบบฟัซซีจะทำงานบนพื้นฐานของแบบจำลองเชิงตรรกที่แสดงกระบวนการทางความคิดของผู้ปฏิบัติการ และถูกอธิบายเป็นชุดกฎการอนุมานที่อยู่ในรูปของ “ถ้าตัวแปรเชิงพฤติกรรม *B* (สัญญาณเข้าตัวควบคุม) ถูกสังเกตว่าอยู่ในสถานะ *x* ดังนั้นเปลี่ยนพารามิเตอร์ควบคุม *C* (สัญญาณออกจากตัวควบคุม) ด้วยจำนวน *y* แบบจำลองดังกล่าวเป็นฟัซซีเนื่องจากมีการกำหนดจำนวน *x* และ *y* ให้อยู่ในเทอมของภาษาเช่น ใหญ่บวก ปานกลางบวก เล็กบวก ไม่มีการเปลี่ยนแปลง เล็กลบ ฯลฯ โดยพจน์แต่ละพจน์เป็นเซตย่อยของฟัซซีโดเมนของการวัดที่เกี่ยวข้อง การควบคุมจะกระทำโดยการนำฐานกฎมาผ่านการอนุมานผลประกอบ*(Compositional rule of inference)* โดยผลลัพธ์ที่ได้จะเป็นเซตย่อยของฟัซซีเซตของสัญญาณควบคุมในช่วงที่พิจารณา จากนั้นจึงทำการพิจารณาผลที่ได้จากการอนุมานว่าค่าใดสอดคล้องกับกฎการควบคุมที่ตั้งไว้มากที่สุดให้สรุปค่าสัญญาณออกว่าเป็นค่านั้น แต่ถ้ามีค่าสัญญาณออกที่สอดคล้องกับกฎที่กำหนดสูงสุดหลายค่าให้ทำการหาค่าเฉลี่ย ซึ่งค่าสัญญาณออกจากตัวควบคุมจะเป็นค่าคงที่ค่าหนึ่งไม่ใช่ค่าฟัซซี ส่วนของการปรับปรุงการทำงานของระบบควบคุมแบบฟัซซีนั้นสามารถกระทำได้โดยการตรวจสอบและปรับปรุงกฎต่างๆ รวมทั้งจัดการกับกฎที่มีความน่าจะเป็นการเกิดความขัดแย้งกันเองระหว่างกฎที่ตั้งขึ้น

2.3.1 โครงสร้างพื้นฐานของตัวควบคุมแบบฟัซซี

โครงสร้างพื้นฐานของตัวควบคุมแบบฟัซซีประกอบด้วย ฟัซซิฟิเคชันมอดูล *(Fuzzification Module)*, ฐานความรู้ *(Knowledge Base)*, เครื่องอนุมาน *(Inference Engine)* และดีฟัซซิฟิเคชันมอดูล *(Defuzzification Module)* โครงสร้างหลักของตัวควบคุมแบบฟัซซีแสดงในรูปที่ 2.4



รูปที่ 2.4 โครงสร้างหลักของตัวควบคุมแบบฟัซซี

2.3.1.1 **ฟัซซิฟิเคชันมอดูล** *(Fuzzification Module)* มีหน้าที่ดังต่อไปนี้

1. ทำการนอมอลไลซ์ค่าทางกายภาพของตัวแปรสเตตของกระบวนการ ให้อยู่ในช่วงพิจารณา

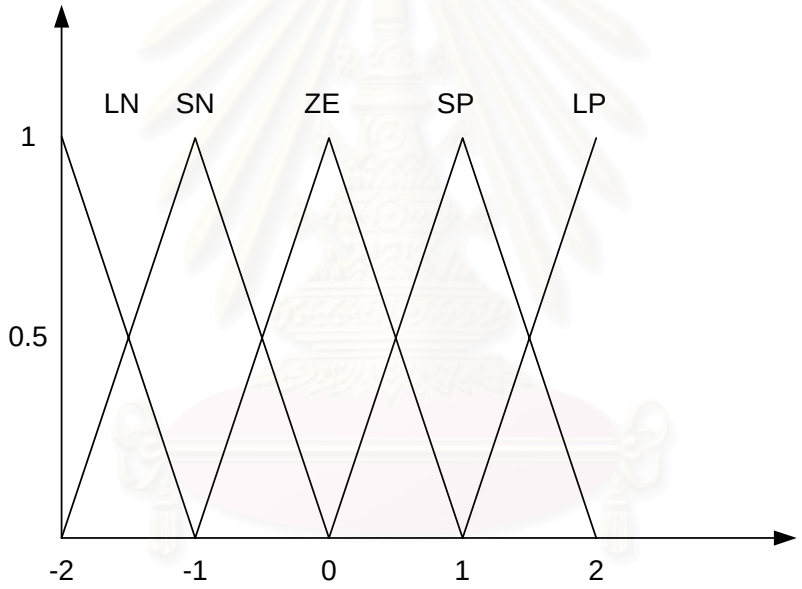
2. แปลงค่าจุด *(Crisp)* แต่ละจุดของข้อมูลขาเข้าที่เป็นตัวแปรสเตตของกระบวนการให้เป็นฟัซซีเซต เพื่อให้เข้ากันได้กับการแสดงฟัซซีเซตของตัวแปรสเตตของกระบวนการแล้วส่งต่อไปยังเครื่องอนุมาน

2.3.1.2 **ฐานความรู้** *(Knowledge Base)* ประกอบด้วย

1. ฐานข้อมูล *(Data Base)* เป็นสารสนเทศที่จำเป็นที่ทำให้ฟัซซิฟิเคชันมอดูล, เครื่องอนุมาน และดีฟัซซิฟิเคชันมอดูลทำงานได้ถูกต้อง ในการออกแบบฐานข้อมูลต้องคำนึงถึง

- การเลือกฟังก์ชันการเป็นสมาชิก *(Membership Function)*

รูปร่างของฟังก์ชันการเป็นสมาชิกที่นิยมมากได้แก่ รูปสามเหลี่ยม รูปสี่เหลี่ยมคางหมู และรูประฆัง เนื่องจากสามารถอธิบายได้ในรูปของฟังก์ชันและพารามิเตอร์ได้ง่าย ทั้งยังใช้หน่วยความจำในการเก็บข้อมูลและประมวลผลน้อย ฟังก์ชันการเป็นสมาชิกจะถูกใช้ในการแปลงค่าจุดของข้อมูลขาเข้าให้เป็นตัวแปรเชิงภาษาดังรูปที่ 2.5



รูปที่ 2.5 ฟังก์ชันการเป็นสมาชิกแบบสามเหลี่ยม ที่ใช้ในการแปลงค่าจุดของข้อมูลขาเข้าในโดเมน [-2, 2] ให้เป็นตัวแปรเชิงภาษา

-การเลือกตัวประกอบมาตราส่วน

ตัวประกอบมาตราส่วน เป็นตัวกำหนดมาตราส่วนในการแปลงค่าตัวแปรกระบวนการให้อยู่ในนอมอลไลซ์โดเมน และทำการแปลงค่าในนอมอลไลซ์โดเมนของตัวแปรควบคุมเป็นค่าทางกายภาพ นั่นคือทำหน้าที่คล้ายอัตราขยายในเครื่องควบคุมแบบดั้งเดิม ดังนั้นการกำหนด

ตัวประกอบมาตราส่วนจึงมีความสำคัญต่อสมรรถนะของเครื่องควบคุม และเสถียรภาพของระบบ เพราะเป็นสาเหตุที่ทำให้เกิดการเสียเสถียรภาพ การแกว่ง และการหน่วงของระบบควบคุม

การกำหนดตัวประกอบมาตราส่วนสามารถกระทำได้ 2 วิธีคือ การลองผิดลองถูก และการหาความสัมพันธ์ระหว่างตัวประกอบมาตราส่วนและพฤติกรรมของกระบวนการซึ่งการกำหนดตัวประกอบมาตราส่วนด้วยวิธีหลังในบางกรณีกระทำได้ค่อนข้างยาก

2. ฐานกฎ *(Rule Base)* มีหน้าที่ควบคุมกระบวนการที่เกี่ยวกับความชำนาญในรูปของ *Production Rule* เช่นกรณีที่ระบบหนึ่งมีฐานกฎ *m* กฎ ที่กฎที่ *k* ใดๆ แสดงในรูปของ *IF* (สภาวะของกระบวนการ)$^{(k)}$ *THEN* (กริยาควบคุม)$^{(k)}$

โดยในส่วนของสภาวะของกระบวนการแสดงด้วย $x_1^{(k)}$เป็น $A_1^{(*k)}$และ...และ $x_n^{(k)}$ เป็น $A_n^{(*k)}$ส่วนของกริยาควบคุมแสดงด้วย $u^{(k)}$เป็น $B^{(k)}$ โดยที่ $A_1^{(*k)}$และ $B^{(k)}$ เป็นค่าเชิงภาษาที่กำหนดไว้สำหรับตัวแปรเชิงภาษา $x_i^{(k)}$ และ $u^{(k)}$ ตามลำดับ หรืออาจเขียนกริยาควบคุมในรูปของฟังก์ชัน $u^{(k)}=f^{(k)}(x_1^{(k)},\ldots,x_n^{(k)})$ และในการสร้างฐานกฎจะต้องทำการเลือกพารามิเตอร์ต่างๆต่อไปนี้

- การเลือกตัวแปรกระบวนการ และตัวแปรควบคุม

ตัวควบคุมแบบฟัซซีพีไอ *(Proportion-plus –Integral Fuzzy Controller)* จะมีตัวแปรกระบวนการคือ ความผิดพลาด *(Error: e)* และการเปลี่ยนแปลงความผิดพลาด *(Δe)* ตัวแปรควบคุม *(u)* ที่เป็นข้อมูลขาออกของตัวควบคุม เมื่อ *k* เป็นเวลาของการชักตัวอย่าง *e* และ Δe

$$e(k) = \text{ค่าสัญญาณออกที่ต้องการ-ค่าสัญญาณออกที่วัด} \quad (2.33)$$

$$\Delta e(k) = (e\text{ในรอบการชักตัวอย่างที่ } k)-(e\text{ในรอบการชักตัวอย่างที่}(k-1)) \quad (2.34)$$

- การเลือกเนื้อหาของกฎ

ถ้าตัวควบคุมเป็นแบบฟัซซีพีไอ การแสดงกฎจะอยู่ในรูป *IF* (*e* เป็น A_i และ Δe เป็น B_i) *THEN* (*u* เป็น C_i) โดย *A, B* และ *C* เป็นเทอมเซตใดๆของฟัซซี

- การเลือกเทอมเซต

เทอมเซตของตัวแปรเชิงภาษา x ประกอบด้วยจำนวนจำกัดของค่าที่แสดงด้วยอักษรซึ่ง *x* เป็นไปได้ เช่นการกรณีที่ตัวแปรสเตตเป็นค่าความผิดพลาด เทอมเซตที่เลือกใช้มักเป็นเทอมเซตที่แสดงเครื่องหมายบวก-ลบ และขนาดได้ เช่น ใหญ่บวก เล็กบวก ไม่มีความผิดพลาด เล็กลบ ใหญ่ลบ เป็นต้น โดยขนาดของเทอมเซตจะเป็นตัวกำหนดความละเอียดของตัวควบคุมแบบฟัซซี แต่การเพิ่มจำนวนของเทอมเซตก็จะส่งผลให้การออกแบบกฎต้องกระทำเพิ่มขึ้นตามไปด้วย

2.3.1.3 **เครื่องอนุมาน** *(Inference Engine)*

เป็นกลไลสำคัญที่นำสภาวะของระบบที่ตรวจวัดได้มาเทียบกับกฎการควบคุมที่กำหนดเพื่อสรุปกริยาควบคุมที่ทำให้กระบวนการดำเนินไปในลักษณะที่ต้องการ เครื่องอนุมานสำหรับฟัซซีแบ่งได้ 2 ประเภท คือ

1. การอนุมานแบบพิจารณาทุกกฎพร้อมกัน *(Composition Based Inference)* เป็นการอนุมานโดยรวมความสัมพันธ์ของฟัซซีทั้งหมดในแต่ละกฎเข้าไว้ด้วยกัน แล้วทำการหากริยาควบคุมที่เหมาะสมกับสภาวะของกระบวนการจากความสัมพันธ์รวมนั้น ผลลัพธ์ที่ได้จะเป็นฟัซซีเซตที่บอกค่าฟัซซีของตัวแปรควบคุมทั้งหมด

2. การอนุมานแบบพิจารณาทีละกฎ *(Individual Rule Based Inference)* เป็นกาอนุมานกฎทีละกฎเพื่อให้ได้ฟัซซีเซตที่อธิบายความหมายของส่วนกริยาควบคุมของกฎนั้นๆแล้ว นำค่าฟัซซีเซตที่ได้จากแต่ละกฎมาทำการรวมกันเป็นค่าตัวแปรควบคุมทั้งหมด โดยการอนุมานแบบนี้จะมีประสิทธิภาพในการคำนวณดีกว่า และประหยัดหน่วยความจำกว่าวิธีการอนุมานแบบพิจารณาทุกกฎพร้อมกัน

วิธีการอนุมานของตัวควบคุมฟัซซีนั้น ได้มีการวิจัยสรุปออกมาเป็นวิธีการทำงานหลายรูปแบบดังนี้เช่น วิธีของ *Mamdami, Sugeno* และ Tsukamoto โดยทั้งสามวิธีนี้เป็นที่นิยมใช้งานอย่างแพร่หลาย ในแต่ละวิธีก็จะมีการทำงานที่แตกต่างกัน ในที่นี้จะกล่าวถึงการอนุมานตามระเบียบวิธีการอนุมานของ *Mamdani* ซึ่งมีชื่อเรียกว่าวิธีอนุมานแบบค่าสูงสุด-ต่ำสุด *(Max-Min Inference)* ซึ่งเป็นวิธีการอนุมานที่เลือกใช้ในวิธีการควบคุมกำลังที่เสนอ การทำงานของวิธีอนุมานแบบค่าสูงสุด-ต่ำสุดจะประกอบด้วย 2 ส่วนคือ

- *Aggregation*

ทำหน้าที่ประมวลผลในส่วนของ *"If"* ในฐานกฎที่อยู่ในรูป *If-Then Rule* ซึ่งก็คือการหาค่าผลลัพธ์ในส่วนของเงื่อนไข *If* ที่แทนสภาวะของระบบ ที่อยู่ในฐานกฎข้อเดียวกัน มีวิธีกระทำโดยใช้ตัวดำเนินการ *min (Intersection, AND)* เขียนได้ในรูปของสมการที่ 2.35

$$\mu_{A\cap B}(u) = \min\{\mu_A(u), \mu_B(u)\} \qquad (2.35)$$

โดยที่ *A* และ *B* เป็นฟัซซีเซตใน U และ $u \in U$ *(Universe of Discourse)*

- *Composition*

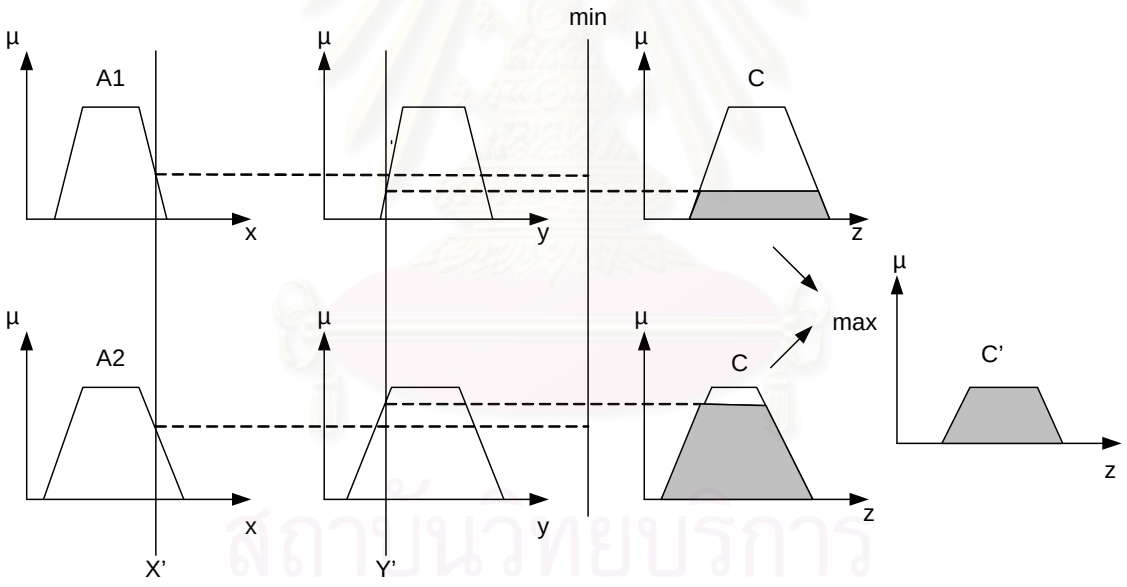
ทำหน้าที่ประมวลผลในส่วนของ *"Then"* ในฐานกฎที่อยู่ในรูป *If-Then Rule* ซึ่งก็คือการหาค่าผลลัพธ์ในส่วนของเงื่อนไข *Then* ที่แทนกริยาควบคุม ที่อยู่ในเทอมเซตเดียวกันของตัวแปรภาษา

ของข้อมูลขาออก มีวิธีกระทำโดยใช้ตัวดำเนินการ *max (Union, OR)* เขียนได้ในรูปของสมการที่ (2.36)

$$\mu_{A\cap B}(u) = \max\{\mu_A(u), \mu_B(u)\} \qquad (2.36)$$

โดยที่ *A* และ *B* เป็นฟัซซีเซตใน U และ $u \in U$ *(Universe of Discourse)*

จากการทำงานของวิธีการอนุมานทั้งสองส่วน จะได้ข้อมูลขาออกที่เป็นค่าทางฟัซซีที่อยู่ในรูปของเทอมเซตต่างๆ ของตัวแปรภาษาของข้อมูลขาออก ซึ่งเครื่องอนุมานจะส่งค่าเหล่านี้ไปยังกระบวนการ *Defuzzification* เพื่อแปลงค่าทางฟัซซีให้เป็นค่าจริงที่สามารถนำไปใช้ในการควบคุมระบบได้ รูปที่ 6 แสดงตัวอย่างการอนุมานตามระเบียบวิธีการอนุมานแบบค่าสูงสุด-ต่ำสุด เทียบกับฐานกฎสองข้อ โดยมีค่าจุดของข้อมูลขาเข้าเป็นค่า *x'* และ *y'* ส่วนข้อมูลขาออกเป็นค่า *C'* ที่เป็นค่าทางฟัซซี เมื่อกำหนดให้ *A1, A2* และ *B1, B2* เป็นเทอมเซตของตัวแปรเชิงภาษาของข้อมูลขาเข้า *A* และ *B* ตามลำดับ และ *C* เป็นเทอมเซตของตัวแปรเชิงภาษาของข้อมูลขาออก



รูปที่ 2.6 วิธีการอนุมานตามระเบียบวิธีการอนุมานแบบค่าสูงสุด-ต่ำสุด

2.3.1.4 **ดีฟัซซิฟิเคชันมอดูล** *(Defuzzification Module)* มีหน้าที่คือ

1. แปลงฟัซซีเซตของค่าตัวแปรควบคุมที่ได้จากการอนุมานตามกฎต่างๆ ให้เป็นค่าคงตัวค่าหนึ่ง

2. แปลงค่าจุดของตัวแปรควบคุมเป็นค่าทางกายภาพ

ตัวอย่างของวิธีดีฟัซซิฟิเคชัน เช่น

- วิธีการหาค่าเฉลี่ยของค่าสูงสุดของค่าสนับสนุน *(Mean of Maximum Method: MOM)* กระทำโดยการหาค่าเฉลี่ยของค่าสนับสนุน *(Support Value)* ที่ทำให้ฟังก์ชันการเป็นสมาชิกมีค่ามากที่สุดในฟัซซีเซตแต่ละเซตของตัวแปรกริยาหรือข้อมูลขาออกของตัวควบคุม ซึ่งสามารถคำนวณได้จากสมการที่ (2.37)

$$u^* = \sum_{i=1}^{r} \frac{u_i}{r} \tag{2.37}$$

โดย $\{u_1, \ldots, u_r\}$ เป็นค่าสนับสนุน ที่ทำให้ฟังก์ชันการเป็นสมาชิกมีค่ามากที่สุดในฟัซซีเซตแต่ละเซตของตัวแปรกริยาหรือข้อมูลขาออกของตัวควบคุม และ r คือจำนวนฟัซซีเซตของตัวแปรกริยาหรือข้อมูลขาออกของตัวควบคุม

- วิธีจุดศูนย์ถ่วง *(Central of Gravity)* เป็นวิธีการเฉลี่ยผลที่ได้จากเครื่องอนุมานวิธีหนึ่งที่นิยมใช้ในปัจจุบัน โดยคำนวณจากสมการที่ (2.38)

$$u^* = \frac{\sum_{i=1}^{r} \mu_i \bullet u_i}{\sum_{i=1}^{r} \mu_i} \tag{2.38}$$

โดย μ_i เป็นระดับการเป็นสมาชิกของฟัซซีเซตที่ i และ $\{u_1, \ldots, u_r\}$ เป็นค่าสนับสนุน *(Support Value)* ที่ทำให้ฟังก์ชันการเป็นสมาชิกมีค่ามากที่สุดในฟัซซีเซตแต่ละเซตของตัวแปรกริยา หรือข้อมูลขาออกของตัวแปรควบคุม และ r คือ จำนวนฟัซซีเซตของตัวแปรกริยาหรือข้อมูลขาออกของตัวแปรควบคุม

บทที่ 3

การปรับปรุงวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก

ในบทที่ผ่านมานั้นเราได้มีการนำเสนอเนื้อหาทางทฤษฎีของการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก ซึ่งจะเห็นได้ว่าวิธีการนี้นั้นค่าถ่วงน้ำหนักมีค่าคงที่ตลอดเวลาและใช้ข้อมูลเพียง 1 ชนิด ในการตรวจจับความผิดปกติ ถ้าเราทำการเปลี่ยนให้วิธีการตรวจจับความผิดปกตินี้มีการเปลี่ยนแปลงค่าถ่วงน้ำหนักตามเวลา และใช้ชนิดข้อมูลมากชนิดขึ้นในการตรวจจับความผิดปกติ น่าจะให้ผลที่ดีกว่าวิธีการดั้งเดิม ดังนั้นเราจึงเสนอการปรับปรุงการหาค่าถ่วงน้ำหนักแบบใหม่โดยใช้ผลรวมของค่าสมบูรณ์ของความแตกต่างของข้อมูล 2 วัน และนำวิธีการหาค่าถ่วงน้ำหนักแบบเดิมและการหาค่าถ่วงน้ำหนักแบบใหม่มาปรับปรุงใช้กับวิธีการที่เรานำเสนอ 3 วิธีคือ

1. การปรับค่าถ่วงน้ำหนักให้เปลี่ยนตามเวลา
2. การใช้ข้อมูลมากกว่าหนึ่งชนิดข้อมูลร่วมกันในการตรวจจับความผิดปกติ
3. การใช้ค่าถ่วงน้ำหนักที่เปลี่ยนแปลงตามเวลาร่วมกับการใช้ข้อมูลมากกว่าหนึ่งชนิดข้อมูลในการตรวจจับความผิดปกติ

อีกทั้งยังวิเคราะห์ถึงผลกระทบของขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติซึ่งมีผลต่อความแน่นอนในการตรวจจับความผิดปกติที่อาจจะเกิดขึ้นในอนาคต

เนื้อหาในบทที่ 3 นี้จะแบ่งเป็น 3 ส่วน ในส่วนที่ 1 เกี่ยวข้องกับวิธีการที่เรานำเสนอในการปรับปรุงวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก ส่วนที่ 2 แสดงถึงดัชนีชี้วัดที่ใช้ในการประเมินประสิทธิภาพของวิธีตรวจจับความผิดปกติของระบบโครงข่าย ส่วนที่ 3 จะแสดงถึงผลการทดลองและสรุปผลการทดลอง

3.1 วิธีการที่เรานำเสนอในการปรับปรุงวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก

จากวิธีการเปรียบเทียบรูปแบบทราฟฟิก ที่กล่าวมานั้นเราจึงได้มีการเสนอการปรับปรุงการตรวจจับความผิดปกติของวิธีการนี้ดังนี้

3.1.1 การปรับเปลี่ยนการหาค่าถ่วงน้ำหนักแบบใหม่

วิธีการหาค่าถ่วงน้ำหนักแบบใหม่นั้นจะใช้สมมุติฐานที่ว่าถ้าผลรวมของผลต่างของค่าเฉลี่ยทราฟฟิกของวันที่ *I* และ ทราฟฟิกวันที่ *j* ภายในช่วงเวลาหนึ่งมีค่าน้อยแสดงว่าลักษณะของทราฟฟิกระหว่างสองวันนี้มีลักษณะคล้ายกันมาก ดังนั้นค่าถ่วงน้ำหนักระหว่างวันทั้งสองนี้จะมีค่ามาก ซึ่งการหาค่าถ่วงน้ำหนักแบบใหม่แสดงดังสมการที่ (3.1) และ (3.2)

$$c_{m,n} = \sum_{t=1}^{T} | \alpha_m(t) - \alpha_n(t) | \tag{3.1}$$

$$c_{m,n}{}' = \frac{1 / c_{m,n}}{\sum_{i \neq m} 1 / c_{m,i}} \tag{3.2}$$

โดยที่ $c_{m,n}{}'$ คือ ค่าถ่วงน้ำหนักของวันที่ *m* กับวันที่ *n*

$\alpha_m(t)$ คือ ค่าเฉลี่ยของทราฟฟิกของวันที่ *m* ที่เวลาที่ *t*

$\alpha_n(t)$ คือ ค่าเฉลี่ยของทราฟฟิกของวันที่ *n* ที่เวลาที่ *t*

T คือ เวลาทั้งหมดของข้อมูลในแต่ละวัน

N คือ จำนวนข้อมูลทั้งหมดใน 1 หน้าต่างที่ใช้ในการตรวจจับความผิดปกติ

D คือ จำนวนข้อมูลทั้งหมดใน 1 วัน

ซึ่งค่า *T* นั้นสามารถหาค่าได้จากสมการที่ (3.3)

$$T = \frac{D}{N} \tag{3.3}$$

ซึ่งค่าถ่วงน้ำหนักแบบใหม่ที่นำเสนอน่าจะให้ผลของประสิทธิภาพในการตรวจจับความผิดปกติดีกว่าค่าถ่วงน้ำหนักแบบเดิม เนื่องจากค่าถ่วงน้ำหนักแบบเดิมมีความคลาดเคลื่อนที่มากถ้าทราฟฟิกของวันที่ต้องการทำนายมีค่ามากกว่าวันที่ต้องการใช้เทียบ แต่วิธีการของการหาค่าถ่วงน้ำหนักแบบใหม่สามารถแก้ปัญหาในกรณีนี้ได้

3.1.2 การปรับเปลี่ยนค่าถ่วงหนักแบบเดิมและแบบใหม่ให้เปลี่ยนแปลงตามเวลา

เนื่องจากค่าถ่วงน้ำหนักแบบเดิมและแบบใหม่ของวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบเปรียบเทียบรูปแบบทราฟฟิกมีค่าคงที่ ดังนั้นเราจึงมีแนวคิดที่ว่าถ้าเราทำให้ค่าถ่วงน้ำหนักทั้งแบบเดิมและแบบใหม่สามารถเปลี่ยนแปลงตามเวลาของหน้าต่างในการตรวจจับความผิดปกติที่เปลี่ยนไป น่าจะให้ผลของประสิทธิภาพการตรวจจับความผิดปกติที่ดีกว่า ดังนั้นการหาค่าถ่วงน้ำหนักแบบเดิมเปลี่ยนตามเวลาแสดงดังสมการ (3.4) และ (3.5)

$$c_{m,n}(t) = \sum_{i=1}^{N} \frac{\alpha_{m,i}(t)}{\alpha_{n,i}(t)} \tag{3.4}$$

$$c_{m,n}{}'(t) = \frac{c_{m,n}(t)}{\sum_{i \neq m} c_{m,i}(t)} \tag{3.5}$$

ส่วนการหาค่าถ่วงน้ำหนักแบบใหม่เปลี่ยนแปลงตามเวลาแสดงดังสมการที่ (3.6) และ (3.7)

$$c_{m,n}(t) = \sum_{i=1}^{N} | \alpha_{m,i}(t) - \alpha_{n,i}(t) | \tag{3.6}$$

$$c_{m,n}'(t) = \frac{1/c_{m,n}(t)}{\sum_{i \neq m} 1/c_{m,i}(t)} \tag{3.7}$$

โดยที่ $c_{m,n}'(t)$ คือ ค่าถ่วงน้ำหนักของวันที่ *m* กับวันที่ *n* ที่เวลา *t*

$\alpha_{m,i}'(t)$ คือ ค่าเฉลี่ยของทราฟฟิกของวันที่ *m* ของชุดข้อมูลตำแหน่งที่ *i* ที่เวลาที่ *t*

$\alpha_{n,i}'(t)$ คือ ค่าเฉลี่ยของทราฟฟิกของวันที่ *n* ของชุดข้อมูลตำแหน่งที่ *i* ที่เวลาที่ *t*

3.1.3 การใช้ข้อมูล 3 ระดับในการตรวจจับความผิดปกติของระบบโครงข่าย

การใช้ข้อมูลเพียง 1 ชนิดในการตรวจจับความผิดปกติของระบบโครงข่ายนั้นอาจให้ผลที่ไม่ดีนัก ถ้าความผิดปกติในระบบโครงข่ายเกิดขึ้นที่ตำแหน่งที่ข้อมูลที่เราใช้ในการตรวจจับความผิดปกติของระบบโครงข่ายไม่สามารถตรวจจับได้ ดังนั้นจึงมีแนวคิดที่ว่าถ้าใช้ข้อมูลหลากหลายชนิดมากขึ้นพร้อมกันในการตรวจจับความผิดปกติน่าที่จำทำให้ประสิทธิภาพในการตรวจจับความผิดปกติในระบบโครงข่ายดีขึ้น ในที่นี้จึงนำเสนอการใช้ข้อมูล 3 ระดับประกอบไปด้วย *ipIDE*, *ipOR* และ *ipIR* ในการตรวจจับความผิดปกติของระบบโครงข่าย

ซึ่ง *ipIR* คือ จำนวนไบต์ของทราฟฟิกทั้งหมดที่เข้าสู่รูทเทอร์ในช่วงเวลาหนึ่ง

ipOR คือ จำนวนไบต์ของทราฟฟิกที่ผ่านจากอุปกรณ์ที่ต่อกับรูทเทอร์ เข้าสู่รูทเทอร์เพื่อส่งออกไปในช่วงเวลาหนึ่ง

ipIDE คือ จำนวนไบต์ของทราฟฟิกที่ผ่านจากรูทเทอร์เพื่อเข้าสู่อุปกรณ์ที่ต่อกับรูทเทอร์ในช่วงเวลาหนึ่ง

โดยเงื่อนไขที่ระบบโครงข่ายจะไม่ผิดปกติเป็นดังสมการที่ (3.8)

$$\sum_{i=1}^{3}(\bar{I}_i - 2\bar{\sigma}_i) \leq \sum_{i=1}^{3} I_i \leq \sum_{i=1}^{3}(\bar{I}_i + 2\bar{\sigma}_i) \tag{3.8}$$

i คือ จำนวนชนิดข้อมูลที่ใช้ในการตรวจจับความผิดปกติในระบบโครงข่าย

$\bar{I}$ คือ ค่าเฉลี่ยของทราฟฟิกที่ถูกทำนายโดยข้อมูลในอดีตที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่าย

$\bar{\sigma}$ คือ ค่าเบี่ยงเบนมาตรฐานของทราฟฟิกที่ถูกทำนายโดยข้อมูลในอดีตที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่าย

I คือ ค่าเฉลี่ยของทราฟฟิกจริงที่วัดได้ที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่าย

3.1.4 การใช้การปรับเปลี่ยนค่าถ่วงน้ำหนักให้เปลี่ยนแปลงตามเวลาร่วมกับการใช้ข้อมูล 3 ระดับในการตรวจจับความผิดปกติของระบบโครงข่าย

ในส่วนนี้จะเป็นการนำวิธีการเปลี่ยนค่าถ่วงน้ำหนักตามเวลามาใช้ร่วมกับการใช้ข้อมูล 3 ระดับ ซึ่งประกอบไปด้วย *ipOR ipIR* และ *ipIDE* ในการตรวจจับความผิดปกติ โดยมีแนวคิดที่ว่าถ้าเราใช้วิธีการทั้งสองพร้อมกันน่าจะทำให้ประสิทธิภาพในการตรวจจับความผิดปกติของระบบโครงข่ายดีขึ้น

3.2 ดัชนีชี้วัดที่ใช้ในการประเมินประสิทธิภาพของวิธีตรวจจับความผิดปกติของระบบโครงข่าย

ดัชนีที่ใช้วัดประสิทธิภาพในวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบเปรียบเทียบรูปแบบทราฟฟิกประกอบด้วย 4 ดัชนีชี้วัด ดังต่อไปนี้

ความน่าจะเป็นที่จะเกิดสัญญาณเตือนที่ผิดพลาด (P_f) โดย

$$P_f = \frac{Total\ number\ of\ false\ alarms}{Total\ number\ of\ data\ samples} \tag{3.9}$$

ความน่าจะเป็นที่สามารถตรวจจับความผิดปกติได้ถูกต้อง (P_p) โดย

$$P_p = \frac{Total\ number\ of\ true\ alarms}{Total\ number\ of\ know\ faults} \tag{3.10}$$

นอกจากนี้ยังมีการตรวจจับที่ผิดพลาด 2 รูปแบบคือ

- *False positive rate* คือ อัตราที่ระบบตรวจจับความผิดปกติจะตรวจจับทราฟฟิกที่ปกติว่าผิดปกติ โดยที่

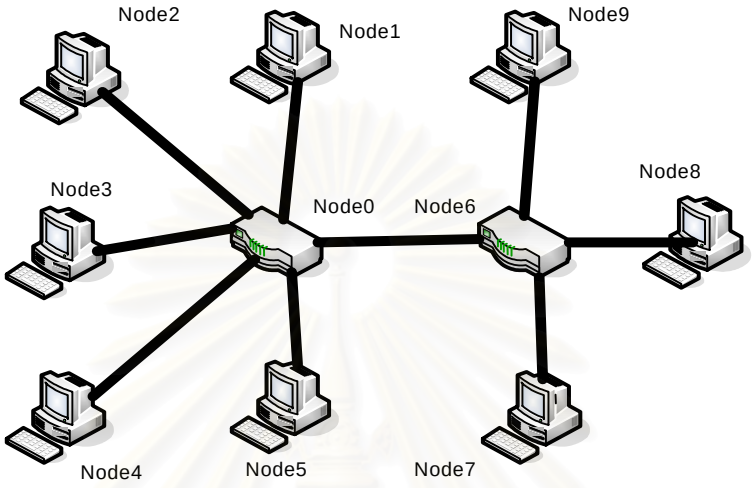
$$False\ positive\ rate = \frac{Total\ number\ of\ false\ alarms}{Total\ number\ of\ alarms} \tag{3.11}$$

- *False negative rate* คือ อัตราที่ระบบตรวจจับความผิดปกติจะตรวจจับทราฟฟิกที่ผิดปกติว่าปกติ โดยที่

$$False\ negative\ rate = \frac{Number\ of\ undetected\ alarms}{Number\ of\ errors} \tag{3.12}$$

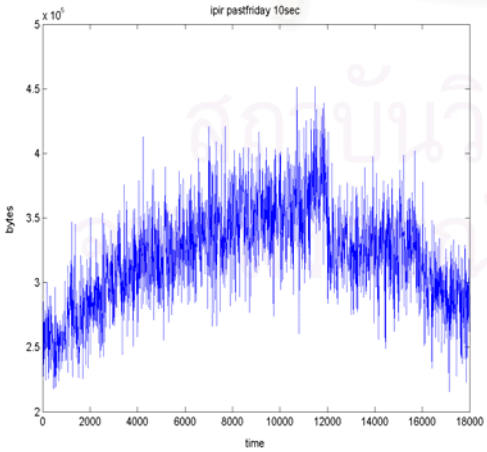
3.3 ผลการทดลองและสรุปผลการทดลอง

ในการทดลองนี้เราจะใช้ระบบโครงข่ายที่ประกอบไปด้วย 10 โนด 9 ข่ายเชื่อมโยง เป็นโครงข่ายที่ใช้ในการทดลองดังรูปที่ 3.1

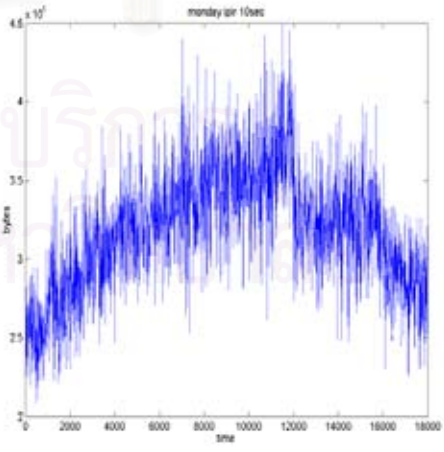


รูปที่ 3.1 ระบบโครงข่ายที่ใช้ในการทดลอง

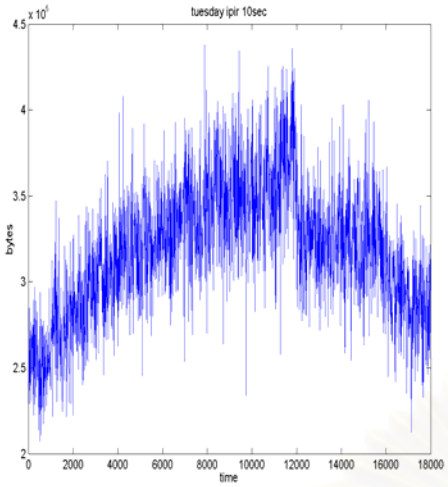
ในการทดลองนี้เราจะทำการกำเนิดทราฟฟิกในระบบโครงข่ายนี้โดยใช้โปรแกรม *NS(Network Simulator)* โดยใช้การส่งข้อมูลแบบ *UDP (User Datagram Protocol)* ด้วยแบบจำลอง *On-Off* โดยที่การกระจายของการส่งข้อมูลเป็นแบบ *Exponential* จำนวนทั้งสิ้น 6 วัน จากช่วงเวลาที่ 0 วินาทีถึงช่วงเวลาที่ 18,000 วินาที ดังรูปที่ 3.2-3.19 ตามลำดับ



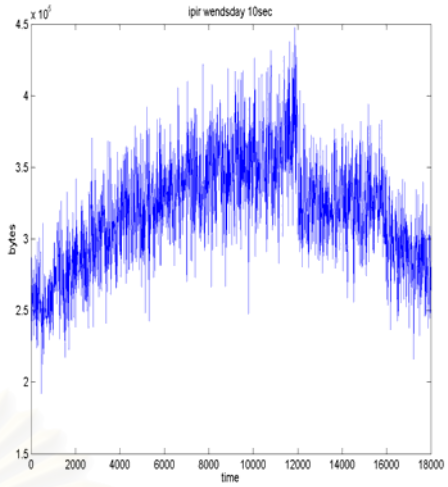
รูปที่ 3.2 *ipIR PastFriday*



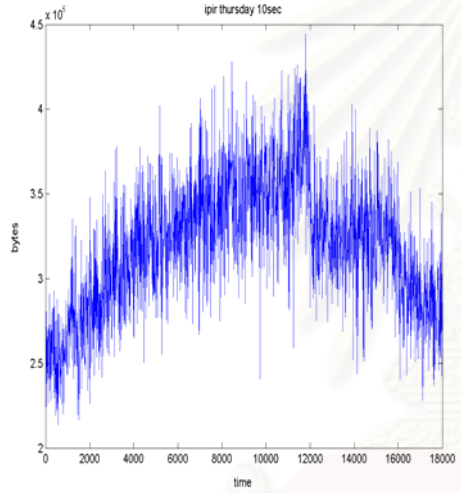
รูปที่ 3.3 *ipIR Monday*



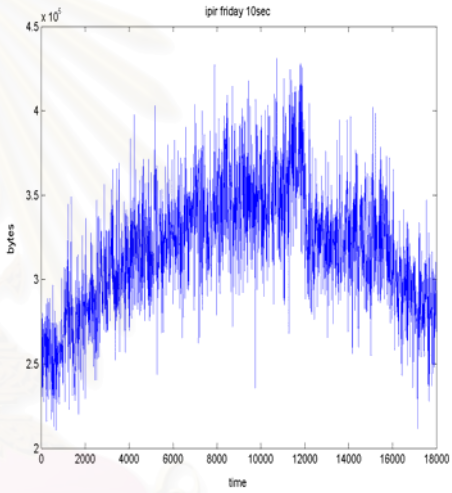
รูปที่ 3.4 *ipIR Tuesday*



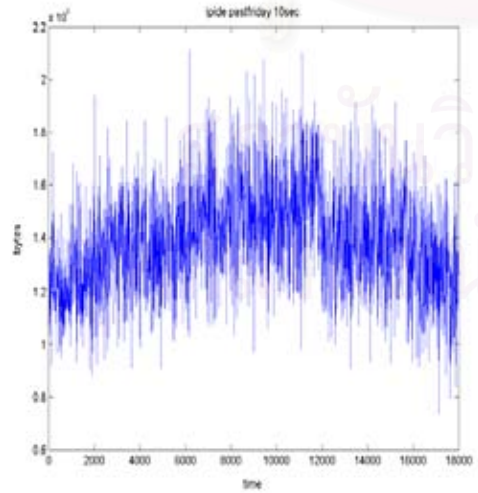
รูปที่ 3.5 *ipIR Wednesday*



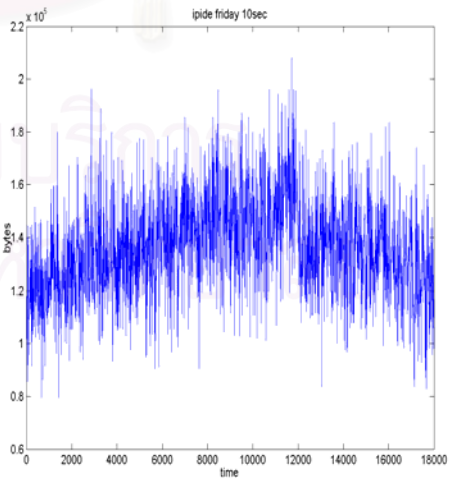
รูปที่ 3.6 *ipIR Thursday*



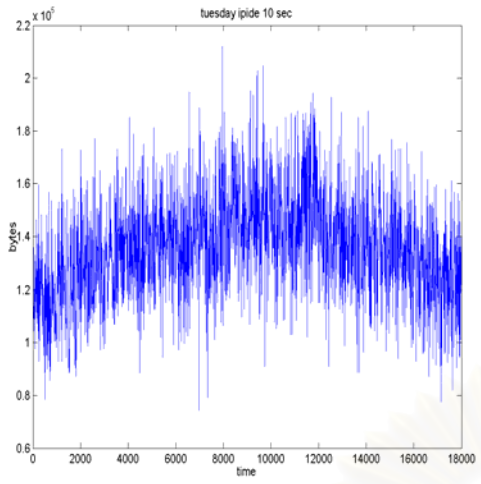
รูปที่ 3.7 *ipIR Friday*



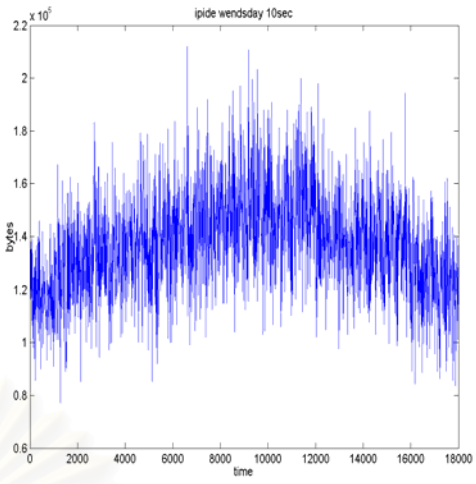
รูปที่ 3.8 *ipIDE Pastfriday*



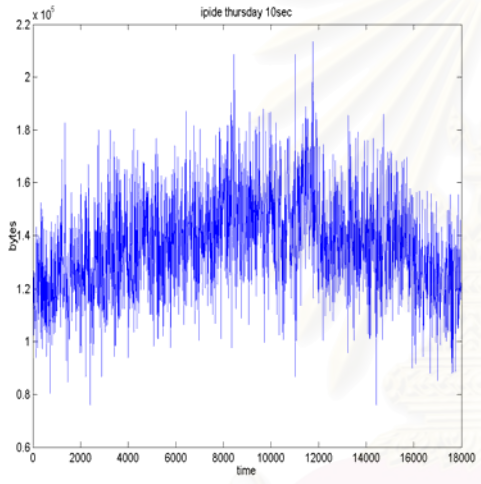
รูปที่ 3.9 *ipIDE Monday*



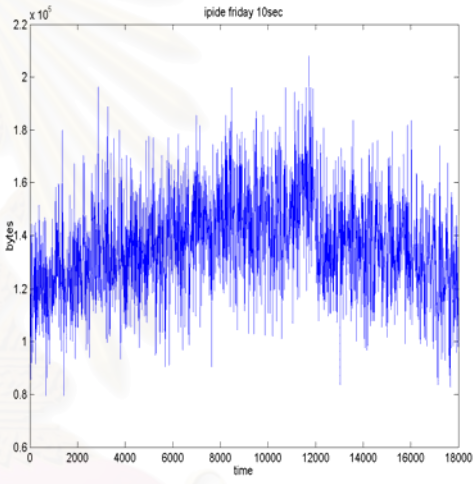
รูปที่ 3.10 *ipIDE Tuesday*



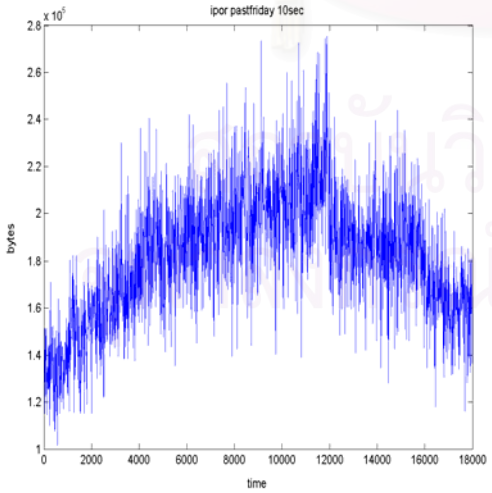
รูปที่ 3.11 *ipIDE Wenesday*



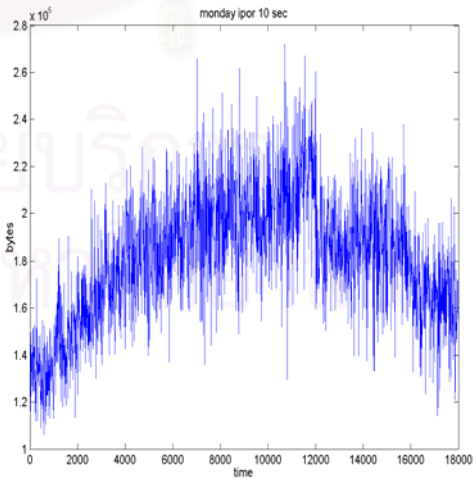
รูปที่ 3.12 *ipIDE Thursday*



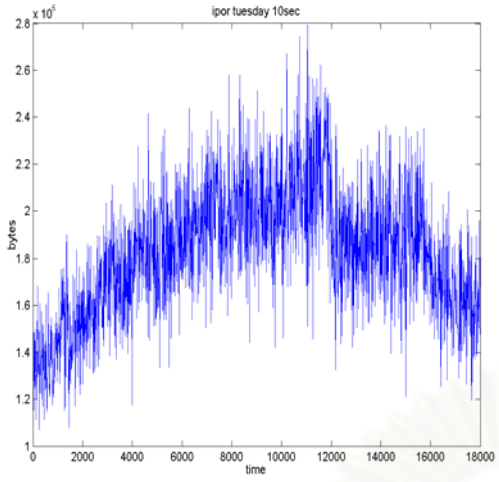
รูปที่ 3.13 *ipIDE Friday*



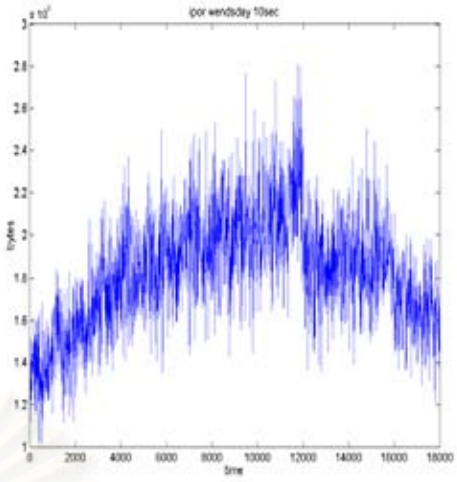
รูปที่ 3.14 *ipOR PastFriday*



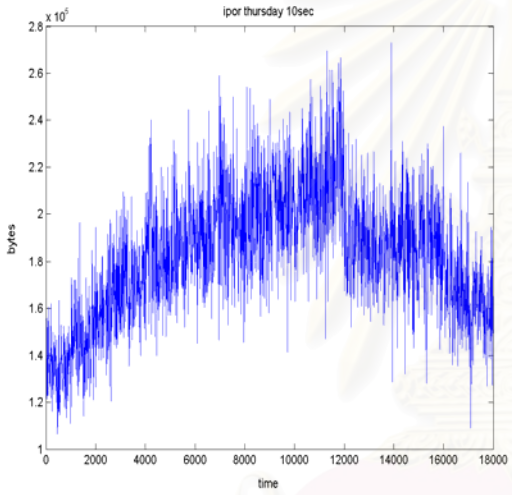
รูปที่ 3.15 *ipOR Monday*



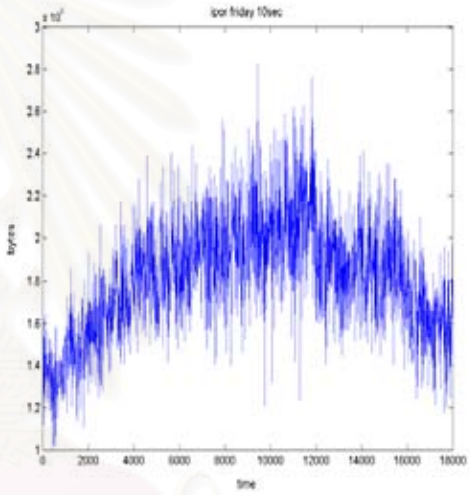
รูปที่ 3.16 *ipOR Tuesday*



รูปที่ 3.17 *ipOR Wendsday*



รูปที่ 3.18 *ipOR Thursday*



รูปที่ 3.19 *ipOR Friday*

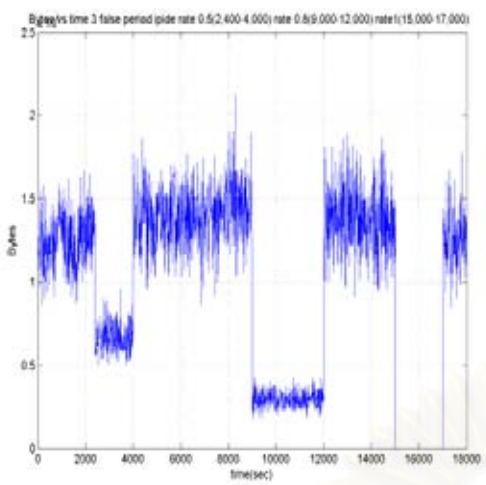
วิธีการตรวจจับทั้งหลายที่ได้นำเสนอมานั้นได้นำมาทดสอบใน 3 สถานการณ์ดังนี้

สถานการณ์ที่ 1. ไม่มีความผิดปกติเกิดขึ้นในระบบโครงข่าย

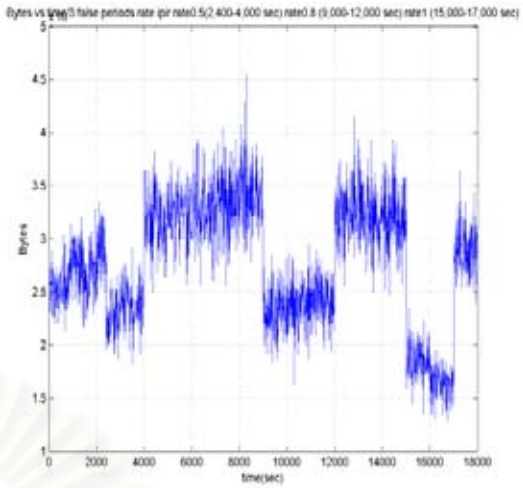
สถานการณ์ที่ 2. มีความผิดปกติเกิดขึ้นที่ข่ายเชื่อมโยงระหว่าง โนด 0 และ โนด 6 ซึ่งแพ็กเกตที่ผ่านข่ายเชื่อมโยงคู่นี้จะสูญหาย 50 เปอร์เซ็นต์ ในช่วงเวลา(2,400-4,000) 80 เปอร์เซนต์ในช่วงเวลา (9,000-12,000) และ 100 เปอร์เซนต์ในช่วงเวลา (15,000-17,000)

สถานการณ์ที่ 3. มีความผิดปกติเกิดขึ้นที่โนด 0 และ โนด 1 ที่เวลา (3,000-3,100) โดยที่โนด 1 ส่งข้อมูลไปยังโนด 0 มากผิดปกติในช่วงเวลานี้ และความผิดปกติเกิดขึ้นที่ทุกโนดในกรณีที่อัตราส่วนระหว่างช่วงเวลาการส่งและหยุดส่งคงที่ แต่ค่าของสองค่านี้เปลี่ยนไปในช่วงเวลา(7,000-8,000)

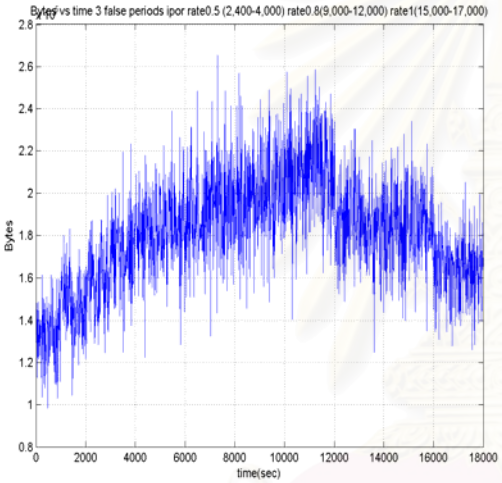
โดยที่ลักษณะของทราฟฟิกที่ผิดปกติของการทดลองในสถานการณ์ที่ 2 และสถานการณ์ที่ 3 แสดงดังรูปที่ 3.20-3.25 ตามลำดับ



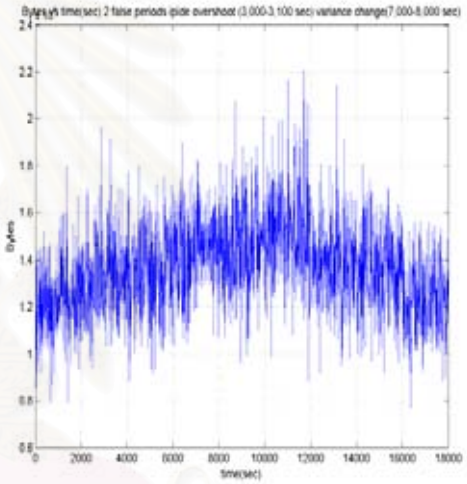
รูปที่ 3.20 ทราฟฟิก *ipIDE* ในสถานการณ์ที่ 2



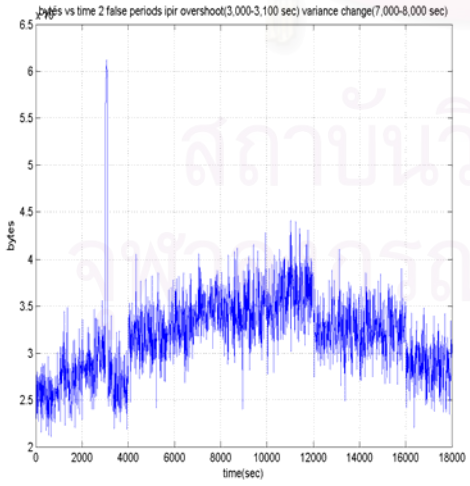
รูปที่ 3.21 ทราฟฟิก *ipIR* ในสถานการณ์ที่ 2



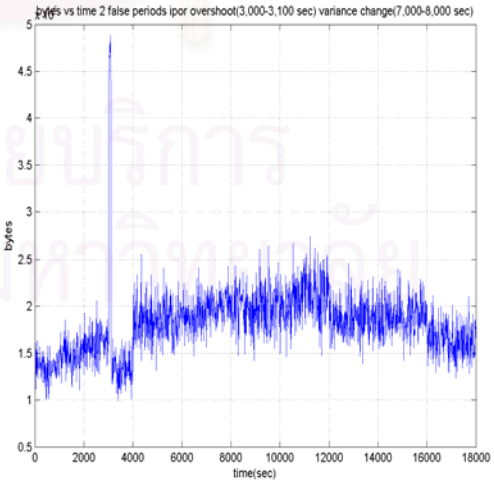
รูปที่ 3.22 ทราฟฟิก *ipOR* ในสถานการณ์ที่ 2



รูปที่ 3.23 ทราฟฟิก *ipIDE*ในสถานการณ์ที่ 3



รูปที่ 3.24 ทราฟฟิก *ipIR*ในสถานการณ์ที่ 3



รูปที่ 3.25 ทราฟฟิก *ipOR* ในสถานการณ์ที่ 3

ในการทดลองนั้นเราได้มีการกำหนดตัวแปรในการแสดงผลของแต่ละวิธีในการตรวจจับความผิดปกติของระบบโครงข่ายดังนี้

method1ide หมายถึง การใช้ค่าถ่วงน้ำหนักแบบเดิมไม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูลชนิด *ipIDE*

method1ir หมายถึง การใช้ค่าถ่วงน้ำหนักแบบเดิมไม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูลชนิด *ipIR*

method1or หมายถึง การใช้ค่าถ่วงน้ำหนักแบบเดิมไม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูลชนิด *ipOR*

method2ide หมายถึง การใช้ค่าถ่วงน้ำหนักแบบเดิมเปลี่ยนแปลงตามเวลาโดยใช้ข้อมูลชนิด *ipIDE*

method2ir หมายถึง การใช้ค่าถ่วงน้ำหนักแบบเดิมเปลี่ยนแปลงตามเวลาโดยใช้ข้อมูลชนิด *ipIR*

method2or หมายถึง การใช้ค่าถ่วงน้ำหนักแบบเดิมเปลี่ยนแปลงตามเวลาโดยใช้ข้อมูลชนิด *ipOR*

method3 หมายถึง การใช้ค่าถ่วงน้ำหนักแบบเดิมไม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูล 3 ชนิดพร้อมกันคือ i*pIR ipOR* และ *ipIDE*

method4 หมายถึง การใช้ค่าถ่วงน้ำหนักแบบเดิมเปลี่ยนแปลงตามเวลาโดยใช้ข้อมูล 3 ชนิดพร้อมกันคือ i*pIR ipOR* และ *ipIDE*

*method1ide*newidea หมายถึง การใช้ค่าถ่วงน้ำหนักแบบใหม่ไม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูลชนิด *ipIDE*

method1irnewidea หมายถึง การใช้ค่าถ่วงน้ำหนักแบบใหม่ไม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูลชนิด *ipIR*

method1ornewidea หมายถึง การใช้ค่าถ่วงน้ำหนักแบบใหม่ไม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูลชนิด *ipOR*

*method2ide*newidea หมายถึง การใช้ค่าถ่วงน้ำหนักแบบใหม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูลชนิด *ipIDE*

method2irnewidea หมายถึง การใช้ค่าถ่วงน้ำหนักแบบใหม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูลชนิด *ipIR*

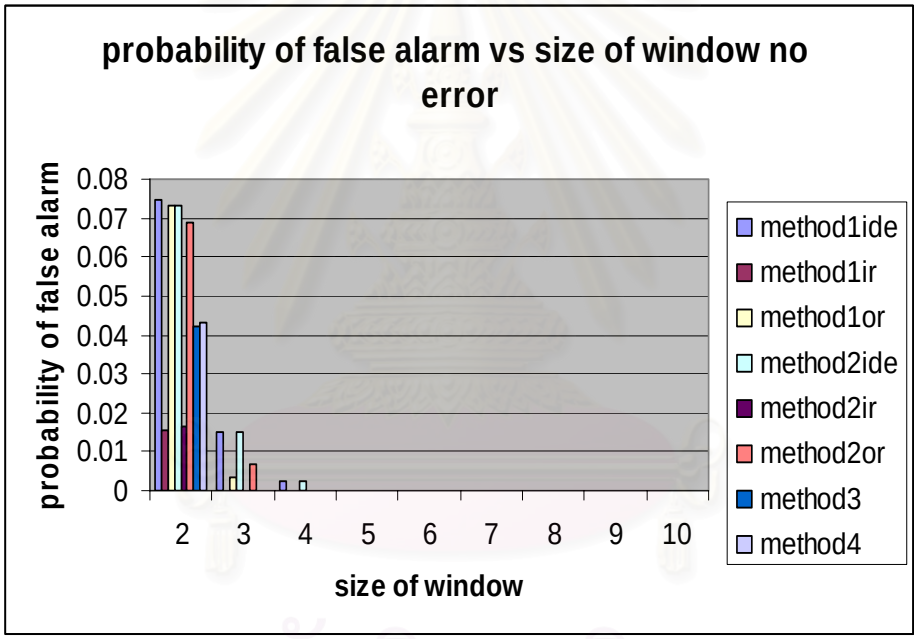
method2ornewidea หมายถึง การใช้ค่าถ่วงน้ำหนักแบบใหม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูลชนิด *ipOR*

method3newidea หมายถึง การใช้ค่าถ่วงน้ำหนักแบบใหม่ไม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูล 3 ชนิดพร้อมกันคือ i*pIR ipOR* และ *ipIDE*

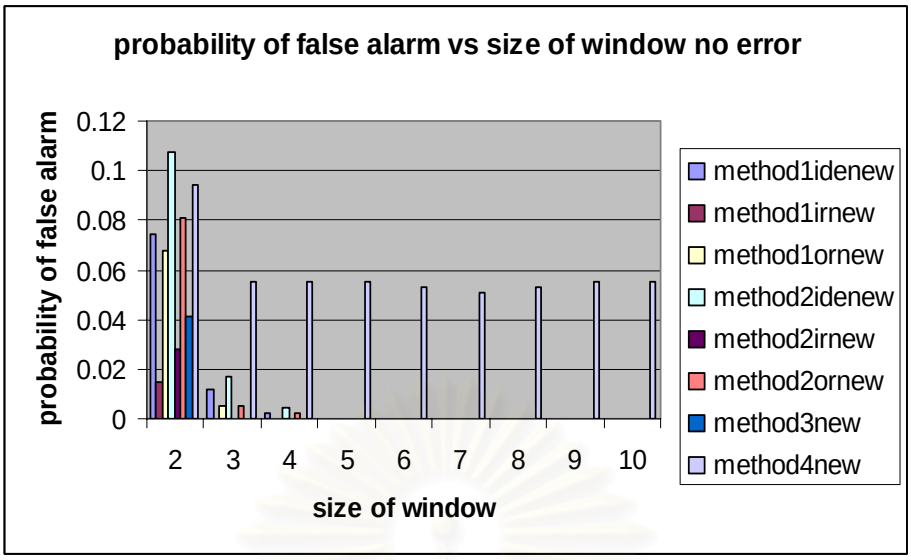
method4newidea หมายถึง การใช้ค่าถ่วงน้ำหนักแบบใหม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูล 3 ชนิดพร้อมกันคือ i*pIR ipOR* และ *ipIDE*

3.3.1 การทดลองการตรวจจับความผิดปกติของระบบโครงข่ายในสถานการณ์ที่ 1

ในการทดลองเพื่อทดสอบประสิทธิภาพของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกที่นำเสนอทั้งสิ้น 16 วิธี ในสถานการณ์ที่ 1 นั้นได้ผลการทดลองดังรูปที่ 3.26 และ 3.27



รูปที่ 3.26 ความสัมพันธ์ระหว่างความน่าจะเป็นของการเกิดสัญญาณเตือนที่ผิดพลาดและขนาดของหน้าต่าง เมื่อไม่เกิดความผิดปกติในระบบโครงข่าย



รูปที่ 3.27 ความสัมพันธ์ระหว่างความน่าจะเป็นของการเกิดสัญญาณเตือนที่ผิดพลาดและขนาดของหน้าต่าง เมื่อไม่เกิดความผิดปกติในระบบโครงข่าย

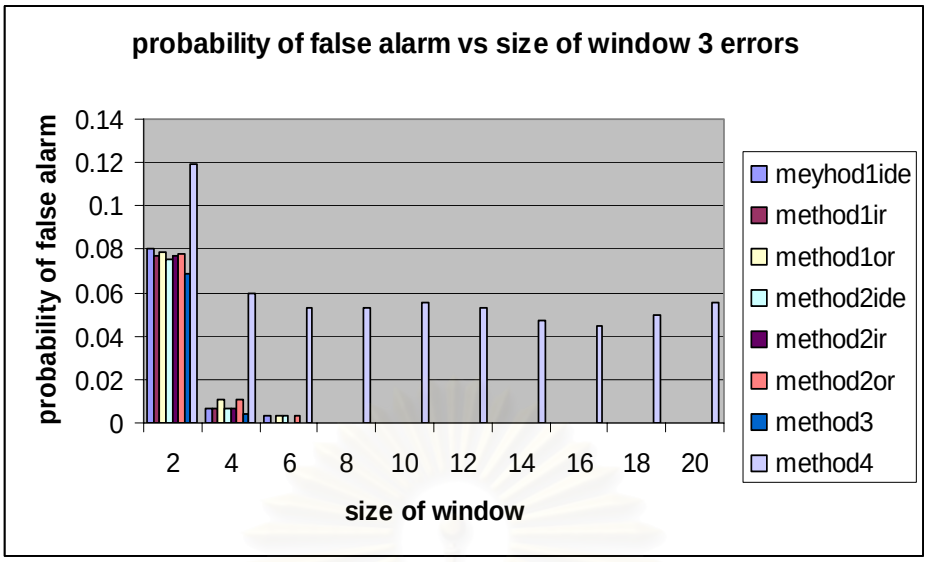
m1ide	*m1idenew*	*m1ir*	***m1irnew***	*m1or*	*m1ornew*	*m2ide*	*m2idenew*
0.0032	0.003	5.36E-04	4.98E-04	0.0026	0.0025	0.0031	0.0044
m2ir	*m2irnew*	*m2or*	*m2ornew*	*m3*	*m3new*	*m4*	*m4new*
5.75E-04	9.58E-04	0.0026	0.003	0.0015	0.0014	0.0015	0.0509

ตารางที่ 3.1 ค่าเฉลี่ยของความน่าจะเป็นของการเกิดสัญญาณเตือนที่ผิดพลาด เมื่อไม่เกิดความผิดปกติในระบบโครงข่าย

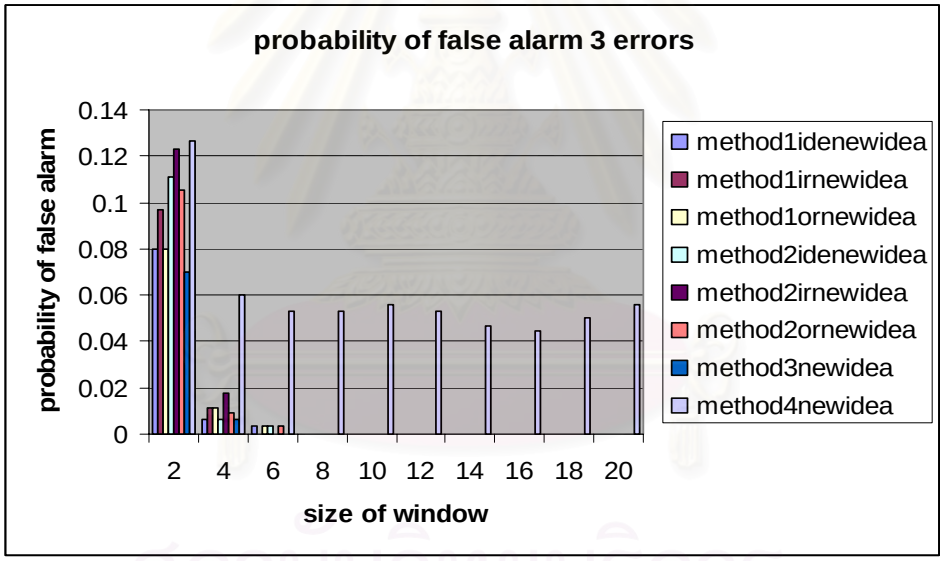
จากผลการทดลองในรูปที่ 3.26 และ 3.27 จะเห็นว่าการใช้ค่าถ่วงน้ำหนักแบบเดิมและค่าถ่วงน้ำหนักแบบใหม่นั้น ขนาดหน้าต่างที่สั้นลงจะมีผลให้ความน่าจะเป็นที่จะเกิดสัญญาณเตือนที่ผิดพลาดสูงขึ้น เช่นขนาดหน้าต่างที่เท่ากับ 2 และ 3 ที่เป็นเช่นนี้เนื่องจากจำนวนจุดข้อมูลที่ใช้ในการทำนายค่าเฉลี่ยและความแปรปรวนมีน้อยเกินไปทำให้เกิดความผิดพลาด และแต่ละชนิดข้อมูลที่ใช้ในการตรวจจับความผิดปกติให้ผลของประสิทธิภาพในการตรวจจับความผิดปกติไม่เท่ากัน ที่เป็นเช่นนี้เนื่องจากบางชนิดข้อมูลการกระจายของทราฟฟิกไม่สอดคล้องกับการทำนายทราฟฟิก ในกรณีนี้วิธีการตรวจจับความผิดปกติแบบการใช้ค่าถ่วงน้ำหนักแบบใหม่ไม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูลชนิด *ipIR* ให้ผลที่ดีที่สุด

3.3.2 การทดลองการตรวจจับความผิดปกติของระบบโครงข่ายในสถานการณ์ที่ 2

ในการทดลองเพื่อทดสอบประสิทธิภาพของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกที่นำเสนอทั้งสิ้น 16 วิธี ในสถานการณ์ที่ 2 นั้นได้ผลการทดลองดังรูปที่ 3.28-3.36



รูปที่ 3.28 ความสัมพันธ์ระหว่างความน่าจะเป็นของการเกิดสัญญาณเตือนที่ผิดพลาดและขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 2

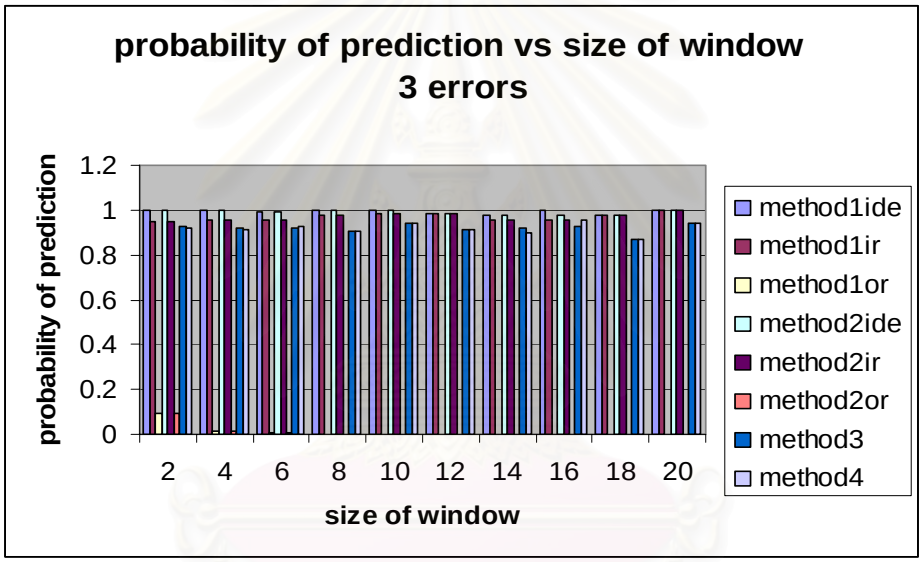


รูปที่ 3.29 ความสัมพันธ์ระหว่างความน่าจะเป็นของการเกิดสัญญาณเตือนที่ผิดพลาดและขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 2

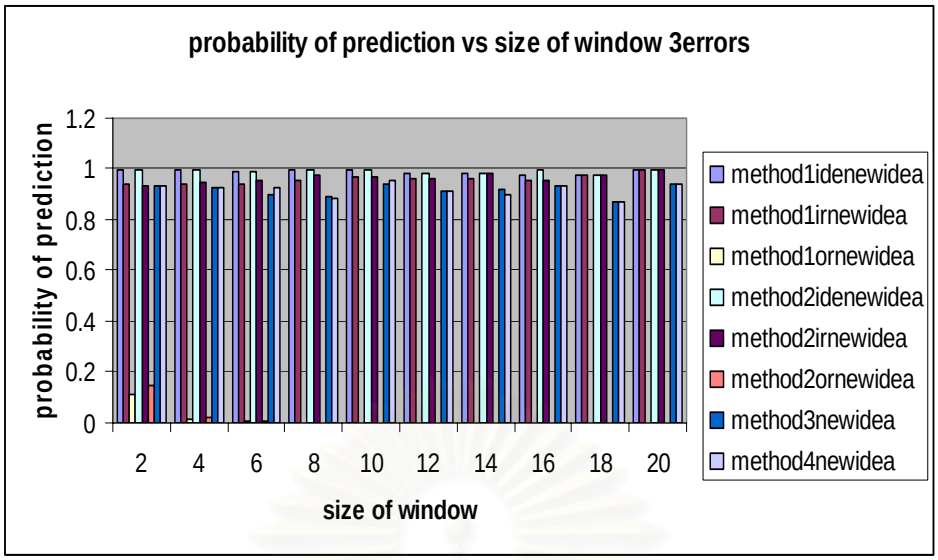
m1ide	*m1idenew*	*m1ir*	*m1irnew*	*m1or*	*m1ornew*	*m2ide*	*m2idenew*
0.004	0.004	4.00E-03	5.10E-03	0.0039	0.0041	0.0037	0.0054
m2ir	*m2irnew*	*m2or*	*m2ornew*	***m3***	*m3new*	*m4*	*m4new*
4.00E-03	6.60E-03	0.0038	0.005	**0.0028**	0.003	0.053	0.0526

ตารางที่ 3.2 ค่าเฉลี่ยของความน่าจะเป็นของการเกิดสัญญาณเตือนที่ผิดพลาด เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 2

จากผลการทดลองขนาดหน้าต่างที่สั้นลงของการหาค่าถ่วงน้ำหนักแบบเดิมและการหาค่าถ่วงน้ำหนักแบบใหม่ จากผลการทดลองในรูปที่ 3.28 และ 3.29 จะเห็นว่าการใช้ค่าถ่วงน้ำหนักแบบเดิมและค่าถ่วงน้ำหนักแบบใหม่นั้น ขนาดหน้าต่างที่สั้นลงจะมีผลให้ความน่าจะเป็นที่จะเกิดสัญญาณเตือนที่ผิดพลาดสูงขึ้น เช่นขนาดหน้าต่างที่เท่ากับ 2 และ 3 ที่เป็นเช่นนี้เนื่องจากจำนวนจุดข้อมูลที่ใช้ในการทำนายค่าเฉลี่ยและความแปรปรวนมีน้อยเกินไปทำให้เกิดความผิดพลาด และแต่ละชนิดข้อมูลที่ใช้ในการตรวจจับความผิดปกติให้ผลของประสิทธิภาพในการตรวจจับความผิดปกติไม่เท่ากัน ที่เป็นเช่นนี้เนื่องจากบางชนิดข้อมูลการกระจายของทราฟฟิกไม่สอดคล้องกับการทำนายทราฟฟิก ในกรณีนี้วิธีการตรวจจับความผิดปกติแบบการใช้ค่าถ่วงน้ำหนักแบบเดิมไม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูล 3 ชนิดพร้อมกันคือ *ipIR ipOR* และ *ipIDE* ให้ผลดีที่สุด



รูปที่ 3.30 ความสัมพันธ์ระหว่างความน่าจะเป็นที่สามารถตรวจจับความผิดปกติได้และขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 2

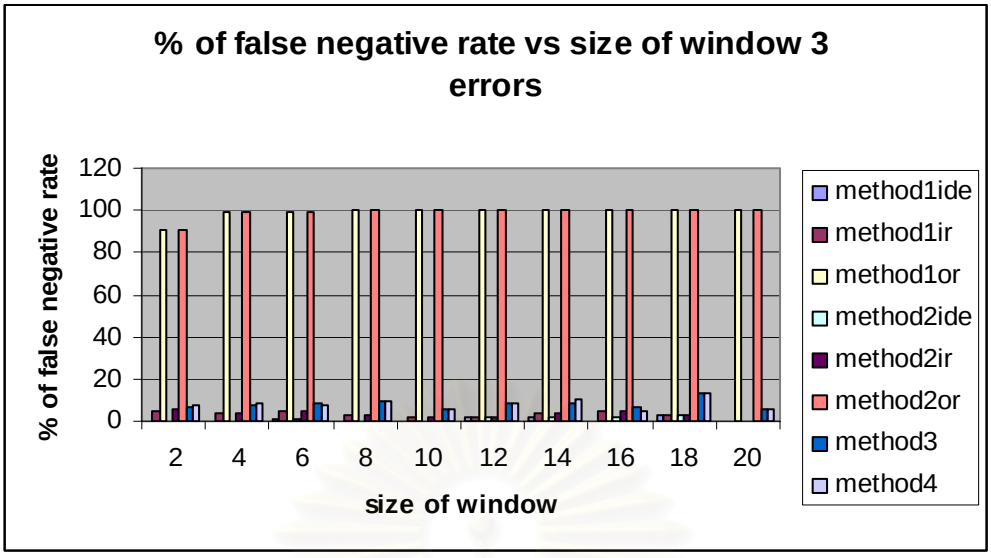


รูปที่ 3.31 ความสัมพันธ์ระหว่างความน่าจะเป็นที่สามารถตรวจจับความผิดปกติได้และขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 2

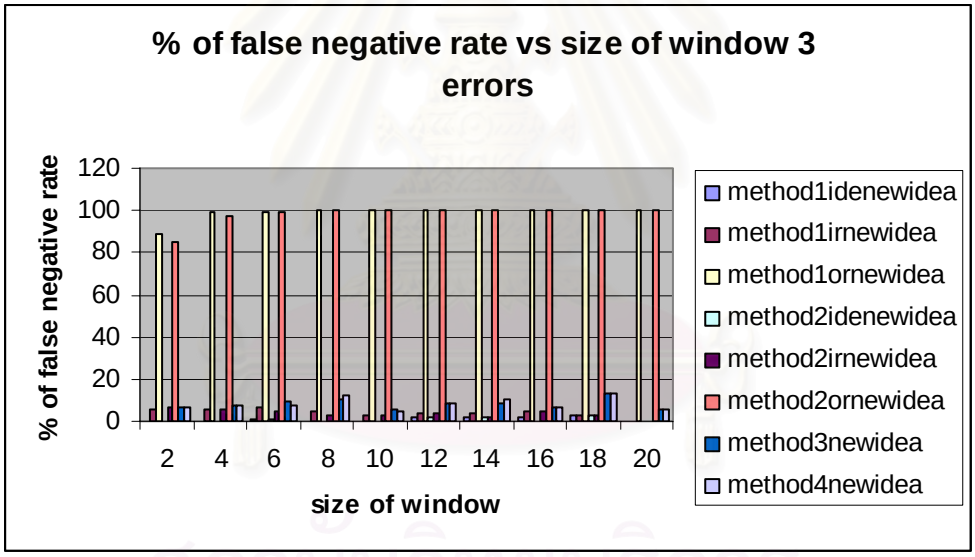
m1ide	*m1idenew*	*m1ir*	*m1irnew*	*m1or*	*m1ornew*	*m2ide*	***m2idenew***
0.9671	0.9663	9.34E-01	9.31E-01	0.006	0.0071	0.9663	0.9671
m2ir	*m2irnew*	*m2or*	*m2ornew*	*m3*	*m3new*	*m4*	*m4new*
9.34E-01	9.31E-01	0.0063	0.0094	0.8852	0.8828	0.8848	0.8831

ตารางที่ 3.3 ค่าเฉลี่ยของความน่าจะเป็นที่สามารถตรวจจับความผิดปกติได้ เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 2

จากผลการทดลองจะเห็นว่าการหาค่าถ่วงน้ำหนักแบบเดิมและแบบใหม่นั้น ความน่าจะเป็นที่จะตรวจจับความผิดปกติได้ ดังรูปที่ 3.30 และ 3.31 ข้อมูลชนิด *ipOR* นั้นจะให้ความน่าจะเป็นที่จะตรวจจับความผิดปกติได้มีค่าต่ำมากเนื่องจากว่าความผิดปกติของระบบโครงข่ายเกิดขึ้นที่ข่ายเชื่อมโยงระหว่างโนด 0 และ โนด 6 ซึ่งข้อมูลของ *ipOR* นั้นจะเก็บค่าทราฟฟิกที่ไหลจากโนด 1, 2, 3, 4, 5 ไปยังโนด 0 ในกรณีนี้นั้น วิธีการตรวจจับความผิดปกติซึ่งใช้ค่าถ่วงน้ำหนักแบบใหม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูลชนิด *ipIDE* ให้ผลดีที่สุด



รูปที่ 3.32 ความสัมพันธ์ระหว่างปริมาณของ *false negative rate* และขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 2

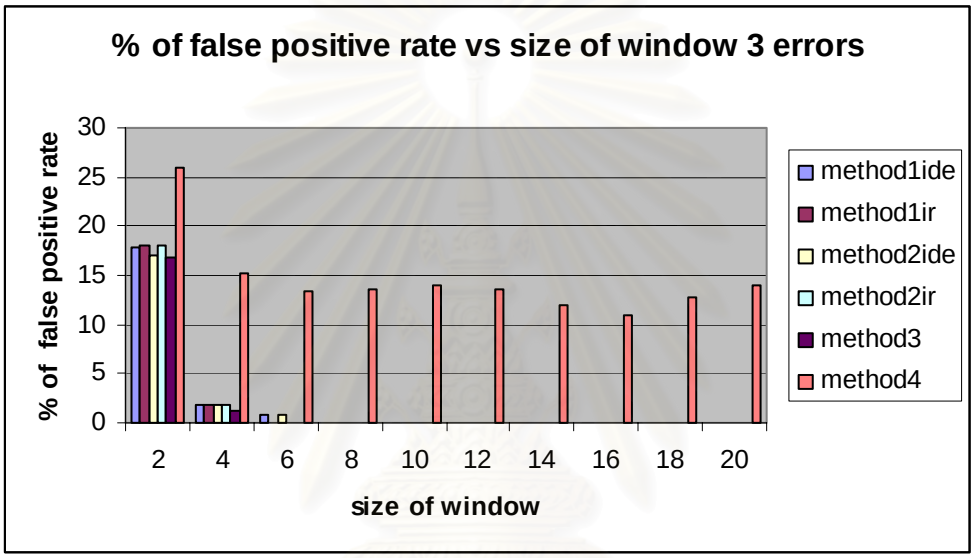


รูปที่ 3.33 ความสัมพันธ์ระหว่างปริมาณของ *false negative rate* และขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 2

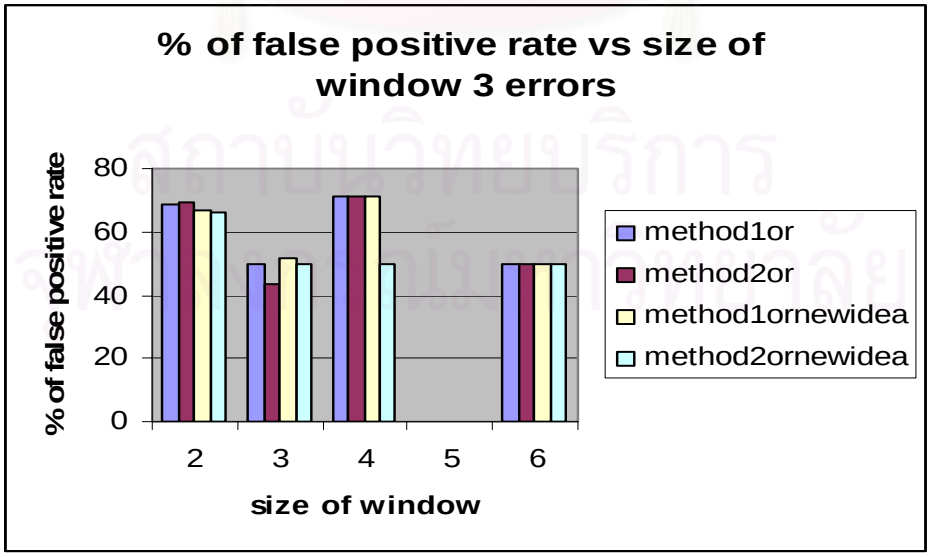
m1ide	*m1idenew*	*m1ir*	*m1irnew*	*m1or*	*m1ornew*	*m2ide*	***m2idenew***
3.2861	3.3663	6.61E+00	6.87E+00	99.395	99.2864	3.3663	3.2861
m2ir	*m2irnew*	*m2or*	*m2ornew*	*m3*	*m3new*	*m4*	*m4new*
6.62E+00	6.91E+00	99.3742	99.0568	11.48	11.7158	11.522	11.6876

ตารางที่ 3.4 ค่าเฉลี่ยของปริมาณของ *false negative rate* เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 2

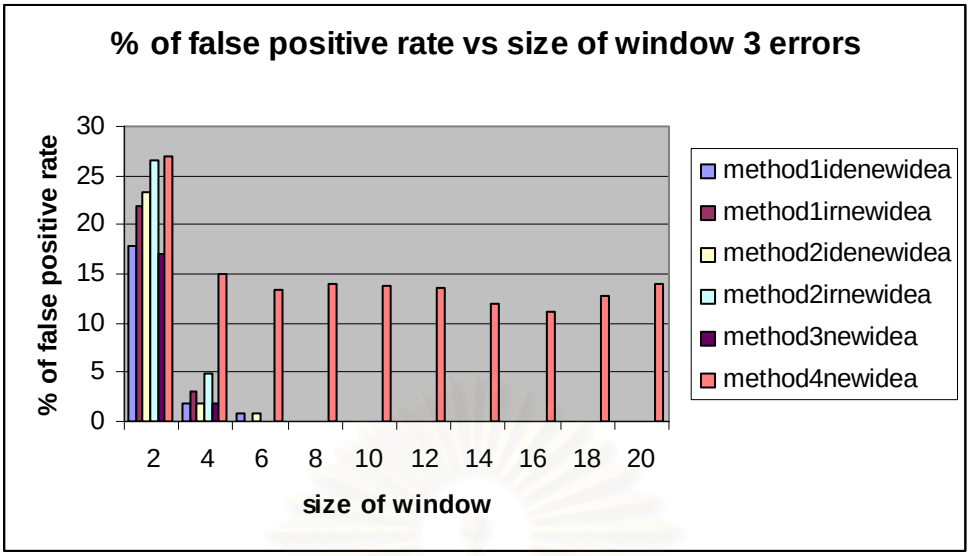
ในส่วนของปริมาณของ *false negative rate* ของการหาค่าถ่วงน้ำหนักแบบเดิมและแบบใหม่ ในรูปที่ 3.32 และ 3.33 นั้น จะเห็นได้ว่าข้อมูลชนิด *ipOR* นั้นจะให้ความผิดพลาดที่สูงมาก เนื่องจากว่าความผิดปกติของระบบโครงข่ายเกิดขึ้นที่ข่ายเชื่อมโยงระหว่างโนด 0 และ โนด 6 ซึ่งข้อมูลของ *ipOR* นั้นจะเก็บค่าทราฟฟิกที่ไหลจากโนด 1, 2, 3, 4, 5 ไปยังโนด 0 ซึ่งไม่มีความเกี่ยวข้องกัน ซึ่งถ้านำข้อมูลชนิดนี้มาตรวจจับจะเกิดความผิดพลาดอย่างมาก ในกรณีนี้นั้น วิธีการตรวจจับความผิดปกติซึ่งใช้ค่าถ่วงน้ำหนักแบบใหม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูลชนิด *ipIDE* ให้ผลดีที่สุด



รูปที่ 3.34 ความสัมพันธ์ระหว่างปริมาณของ *false positive rate* และขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 2



รูปที่ 3.35 ความสัมพันธ์ระหว่างปริมาณของ *false positive rate* และขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 2



รูปที่ 3.36 ความสัมพันธ์ระหว่างปริมาณของ *false positive rate* และขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 2

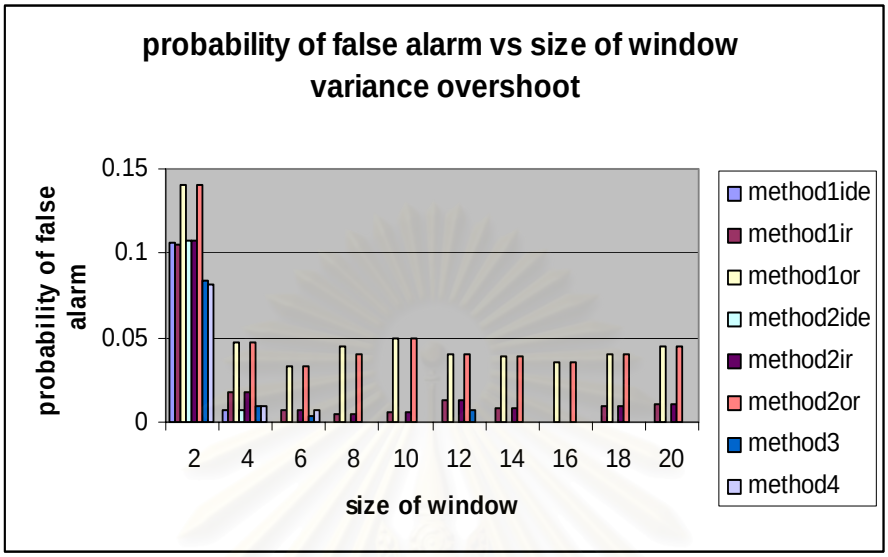
m1ide	*m1idenew*	*m1ir*	*m1irnew*	*m1or*	*m1ornew*	*m2ide*	*m2idenew*
0.9501	0.9359	9.84E-01	1.22E+00	48.072	39.9912	0.8788	1.2034
m2ir	*m2irnew*	*m2or*	*m2ornew*	*m3*	*m3new*	*m4*	*m4new*
9.86E-01	1.53E+00	46.8428	36.0723	0.6902	0.7529	13.37	13.2639

ตารางที่ 3.5 ค่าเฉลี่ยของปริมาณของ *false positive rate* เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 2

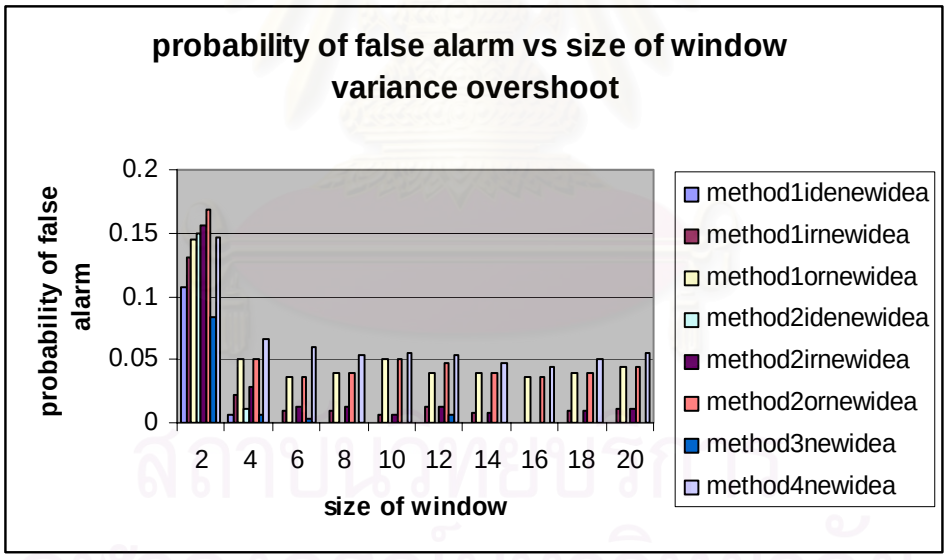
จากผลการทดลอง ขนาดหน้าต่างที่สั้นลงของการหาค่าถ่วงน้ำหนักแบบเดิมและการหาค่าถ่วงน้ำหนักแบบใหม่ จะมีผลให้ปริมาณของ *false positive rate* สูงขึ้น เช่นขนาดหน้าต่างที่เท่ากับ 2 และ 3 ดังรูปที่ 3.34-3.36 ที่เป็นเช่นนี้เนื่องจากจำนวนจุดข้อมูลที่ใช้ในการทำนายค่าเฉลี่ยและความแปรปรวนมีน้อยเกินไปส่งผลให้เกิดความผิดพลาด ในกรณีนี้นั้นการตรวจจับความผิดปกติซึ่งใช้ค่าถ่วงน้ำหนักแบบเดิมไม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูล 3 ชนิดพร้อมกัน คือ i*pIR ipOR* และ *ipIDE* ให้ผลดีที่สุด

3.3.3 การทดลองการตรวจจับความผิดปกติของระบบโครงข่ายในสถานการณ์ที่ 3

ในการทดลองเพื่อทดสอบประสิทธิภาพของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกที่นำเสนอทั้งสิ้น 16 วิธี ในสถานการณ์ที่ 3 นั้นได้ผลการทดลองดังรูปที่ 3.37-3.45



รูปที่ 3.37 ความสัมพันธ์ระหว่างความน่าจะเป็นของการเกิดสัญญาณเตือนที่ผิดพลาดและขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 3

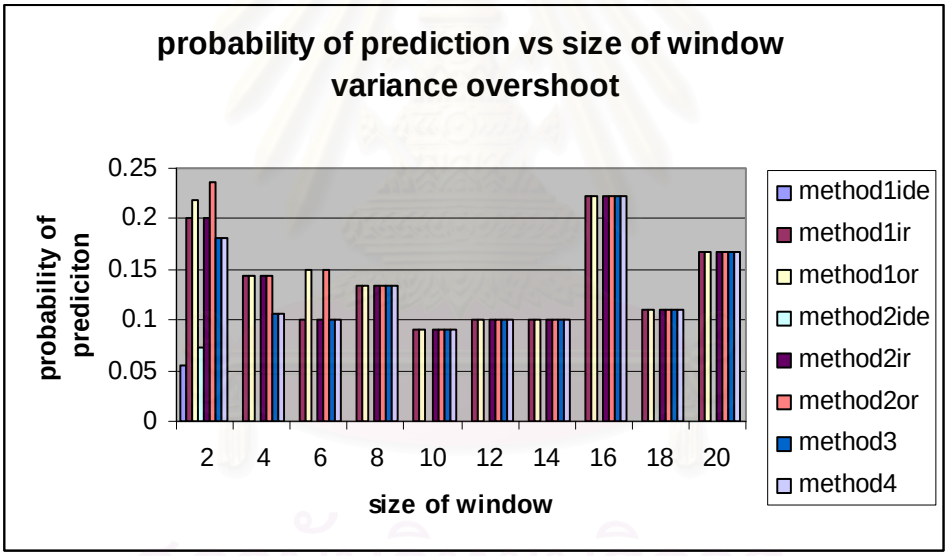


รูปที่ 3.38 ความสัมพันธ์ระหว่างความน่าจะเป็นของการเกิดสัญญาณเตือนที่ผิดพลาดและขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 3

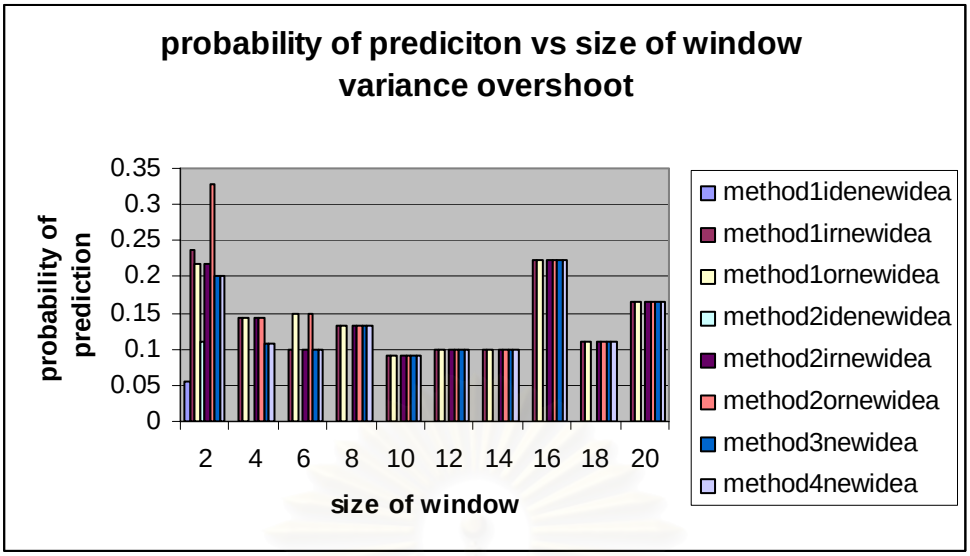
m1ide	*m1idenew*	*m1ir*	*m1irnew*	*m1or*	*m1ornew*	*m2ide*	*m2idenew*
0.0053	0.0053	1.02E-02	1.02E-02	0.0429	0.0433	0.0052	0.007
m2ir	*m2irnew*	*m2or*	*m2ornew*	*m3*	*m3new*	***m4***	*m4new*
1.03E-02	1.51E-02	0.0427	0.0446	0.0052	0.0052	0.005	0.0552

ตารางที่ 3.6 ค่าเฉลี่ยของความน่าจะเป็นของการเกิดสัญญาณเตือนที่ผิดพลาด เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 3

จากผลของการหาค่าถ่วงน้ำหนักแบบเดิมและแบบใหม่ ซึ่งขนาดหน้าต่างที่สั้นลงจะมีผลให้ความน่าจะเป็นของสัญญาณเตือนที่ผิดพลาดสูงขึ้น เช่นขนาดหน้าต่างที่เท่ากับ 2 และ 3 ดังรูปที่ 3.37 และ 3.38 ที่เป็นเช่นนี้เนื่องจากจำนวนจุดข้อมูลที่ใช้ในการทำนายค่าเฉลี่ยและความแปรปรวนมีน้อยเกินไปทำให้เกิดความผิดพลาด ในกรณีนี้นั้น การตรวจจับความผิดปกติซึ่งใช้ค่าถ่วงน้ำหนักแบบเดิมเปลี่ยนแปลงตามเวลาโดยใช้ข้อมูล 3 ชนิดพร้อมกันคือ i*pIR* *ipOR* และ *ipIDE* ให้ผลดีที่สุด



รูปที่ 3.39 ความสัมพันธ์ระหว่างความน่าจะเป็นที่สามารถตรวจจับความผิดปกติได้และขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 3

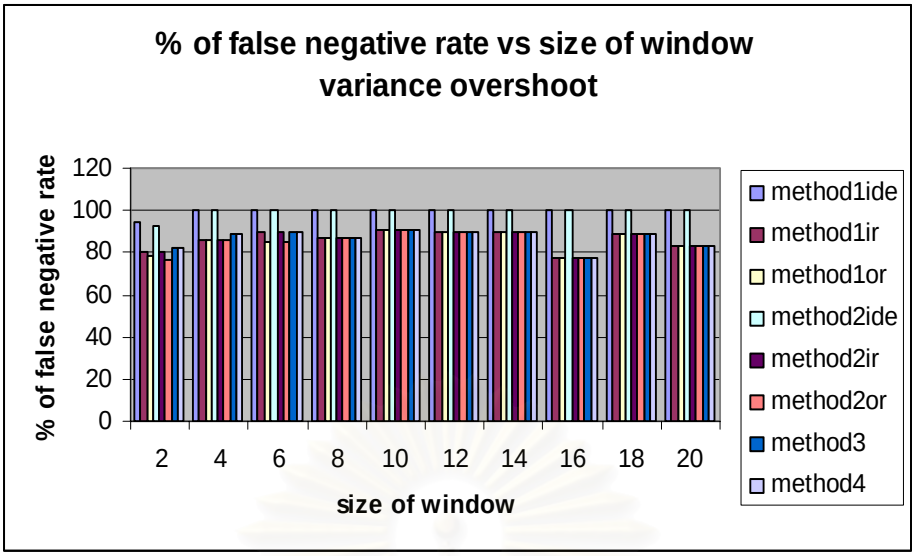


รูปที่ 3.40 ความสัมพันธ์ระหว่างความน่าจะเป็นที่สามารถตรวจจับความผิดปกติได้และขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 3

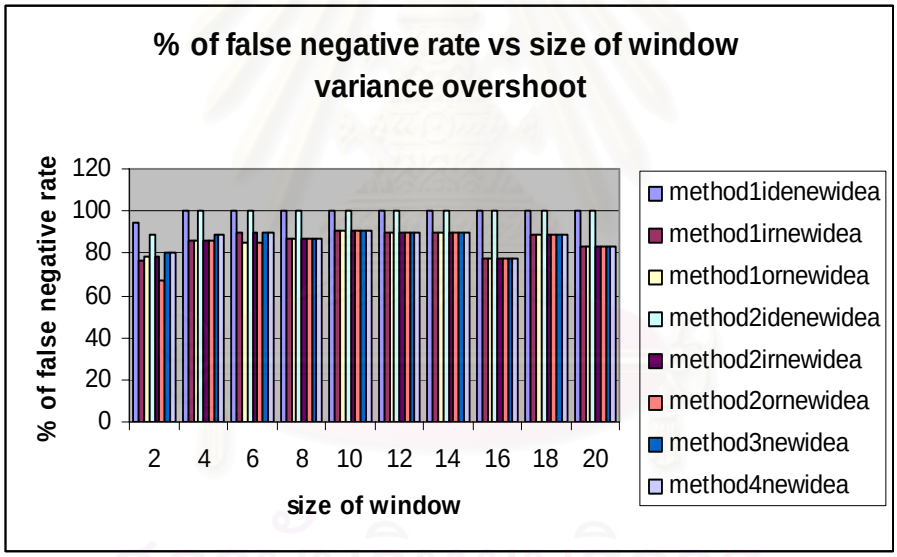
m1ide	*m1idenew*	*m1ir*	*m1irnew*	*m1or*	*m1ornew*	*m2ide*	*m2idenew*
0.0028	0.0028	1.44E-01	1.45E-01	0.1497	0.1497	0.1497	0.0056
m2ir	*m2irnew*	*m2or*	***m2ornew***	*m3*	*m3new*	*m4*	*m4new*
1.44E-01	1.44E-01	0.1503	0.1544	0.1401	0.1407	0.1401	0.1407

ตารางที่ 3.7 ค่าเฉลี่ยของความน่าจะเป็นที่สามารถตรวจจับความผิดปกติได้ เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 3

ในส่วนของความน่าจะเป็นที่จะตรวจจับความผิดปกติได้ นั้นมีค่าต่ำมากเนื่องจากวิธีการเปรียบเทียบรูปแบบทราฟฟิก ไม่สามารถที่จะตรวจจับความปกติเนื่องจากค่าความแปรปรวนที่เปลี่ยนไปได้ ในกรณีนี้นั้น การใช้ค่าถ่วงน้ำหนักแบบใหม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูลชนิด *ipOR* ให้ผลดีที่สุด



รูปที่ 3.41 ความสัมพันธ์ระหว่างปริมาณของ *false negative rate* และขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 3

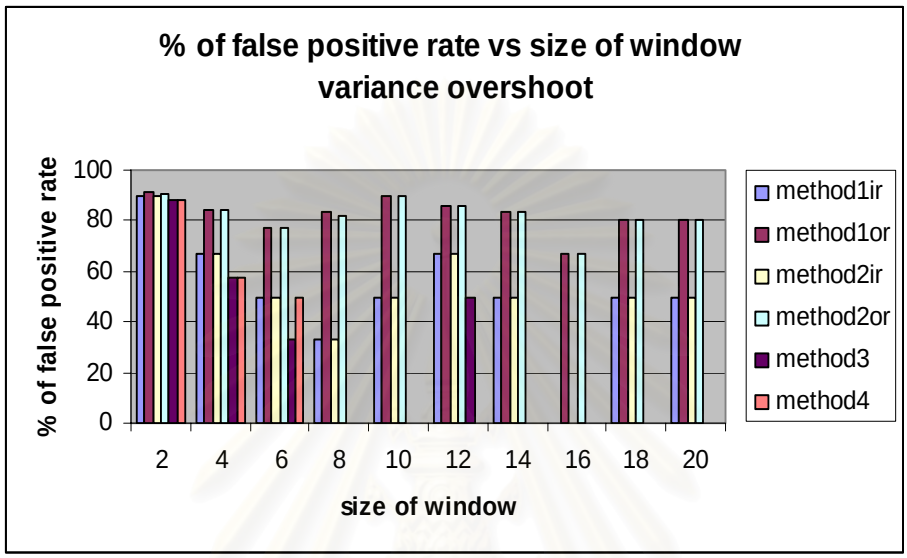


รูปที่ 3.42 ความสัมพันธ์ระหว่างปริมาณของ *false negative rate* และขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 3

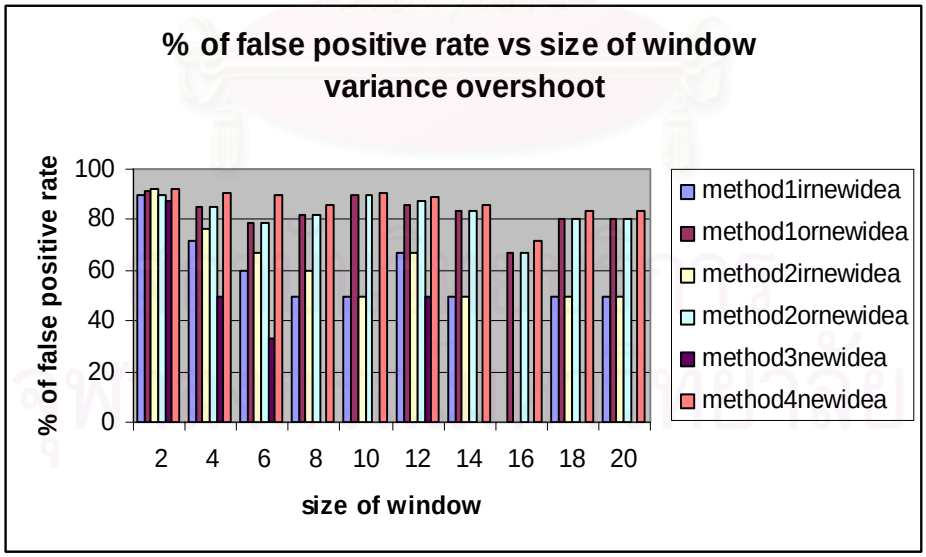
m1ide	*m1idenew*	*m1ir*	*m1irnew*	*m1or*	*m1ornew*	*m2ide*	*m2idenew*
99.7212	99.7212	8.56E+01	8.55E+01	85.029	85.0286	99.659	99.4423
m2ir	*m2irnew*	*m2or*	***m2ornew***	*m3*	*m3new*	*m4*	*m4new*
8.56E+01	8.56E+01	84.9659	**84.5616**	85.989	85.9267	85.989	85.9267

ตารางที่ 3.8 ค่าเฉลี่ยของปริมาณของ *false negative rate* เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 3

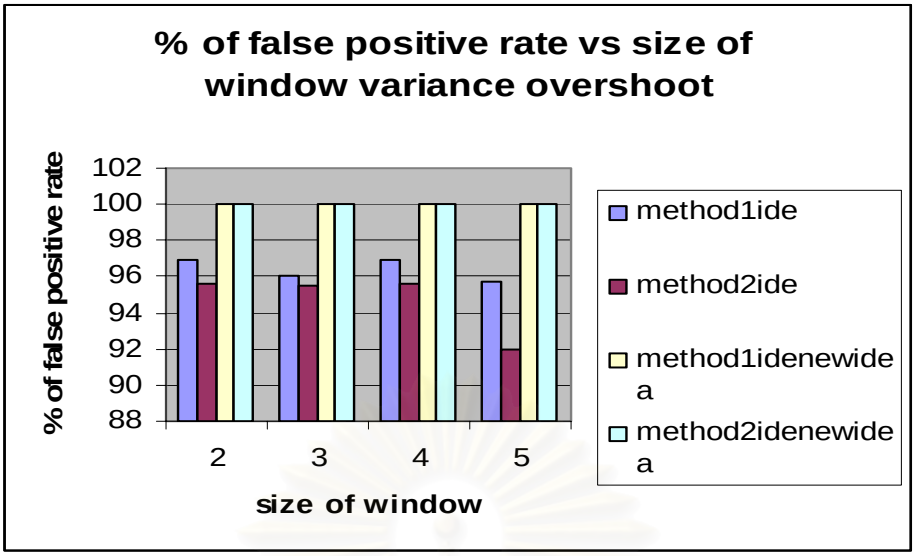
ในส่วนของปริมาณของ *false negative rate* มีค่าของความผิดพลาดในการตรวจจับความผิดปกติของระบบโครงข่ายที่สูงมาก เนื่องจากวิธีการเปรียบเทียบรูปแบบทราฟฟิก ไม่สามารถที่จะตรวจจับความปกติเนื่องจากค่าความแปรปรวนที่เปลี่ยนไปได้ ในกรณีนี้นั้น การใช้ค่าถ่วงน้ำหนักแบบใหม่เปลี่ยนแปลงตามเวลาโดยใช้ข้อมูลชนิด *ipOR* ให้ผลดีที่สุด



รูปที่ 3.43 ความสัมพันธ์ระหว่างปริมาณของ *false positive rate* และขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 3



รูปที่ 3.44 ความสัมพันธ์ระหว่างปริมาณของ *false positive rate* และขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 3



รูปที่ 3.45 ความสัมพันธ์ระหว่างปริมาณของ *false positive rate* และขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 3

m1ide	*m1idenew*	*m1ir*	*m1irnew*	*m1or*	*m1ornew*	*m2ide*	*m2idenew*
98.1555	98.1555	3.35E+01	3.54E+01	78.028	78.028	97.874	96.9362
m2ir	*m2irnew*	*m2or*	*m2ornew*	*m3*	*m3new*	*m4*	*m4new*
3.35E+01	3.83E+01	77.9412	78.0467	17.729	17.5103	16.76	82.6364

ตารางที่ 3.9 ค่าเฉลี่ยของปริมาณของ *false positive rate* เมื่อเกิดความผิดปกติในระบบโครงข่ายในสถานการณ์ที่ 3

ในส่วนของปริมาณของ *false positive rate* มีค่าของความผิดพลาดในการตรวจจับความผิดปกติของระบบโครงข่ายที่สูงมาก เนื่องจากวิธีการเปรียบเทียบรูปแบบทราฟฟิก ไม่สามารถที่จะตรวจจับความปกติเนื่องจากค่าความแปรปรวนที่เปลี่ยนไปได้ ในกรณีนี้นั้น วิธีการตรวจจับความผิดปกติโดยใช้ค่าถ่วงน้ำหนักแบบเดิมเปลี่ยนแปลงตามเวลาโดยใช้ข้อมูล 3 ชนิดพร้อมกันคือ i*pIR ipOR* และ *ipIDE* ให้ผลดีที่สุด

3.3.4 **สรุปผลการทดลอง**

การใช้ขนาดหน้าต่างที่สั้นเกินไปในการตรวจจับความผิดปกติของระบบโครงข่าย จะมีผลให้ประสิทธิภาพในการตรวจจับความผิดปกติลดลง ที่เป็นเช่นนี้เนื่องจากจำนวนจุดข้อมูลที่ใช้ในการทำนายค่าเฉลี่ยและความแปรปรวนมีน้อยเกินไปส่งผลให้เกิดความผิดพลาด และชนิดของข้อมูลที่ใช้ในการตรวจจับความผิดปกติที่แตกต่างกันให้ผลของประสิทธิภาพในการตรวจจับความ

ผิดปกติที่แตกต่างกันที่เป็นเช่นนี้เนื่องจากแต่ละชนิดข้อมูลมีความคล้ายคลึงกันระหว่างข้อมูลในอดีตและปัจจุบันที่แตกต่างกัน วิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบเปรียบเทียบรูปแบบทราฟฟิกนั้นเหมาะสำหรับตรวจจับความผิดปกติที่เป็นแบบค่าเฉลี่ยของทราฟฟิกเกิดการเปลี่ยนแปลง ซึ่งเกิดในกรณีของ ข่ายเชื่อมโยงเกิดความเสียหาย แต่ไม่เหมาะสำหรับความผิดปกติที่ทราฟฟิกมีลักษณะค่าเบี่ยงเบนทราฟฟิกเฉลี่ยเปลี่ยนแปลง เนื่องจากวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกใช้ข้อมูลค่าเฉลี่ยของทราฟฟิกในการตรวจจับ และวิธีการที่นำเสนอในการปรับปรุงวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกให้ประสิทธิภาพในการตรวจจับความผิดปกติที่ดีขึ้นกว่าวิธีการเดิม

บทที่4

การปรับปรุงวิธีการตรวจจับความผิดปกติแบบการเปลี่ยนแปลงทันทีทันใด *(Abrupt Change)*

ในบทที่ผ่านมานั้น เราได้มีการนำเสนอเนื้อหาทางทฤษฎีของการตรวจจับความผิดปกติแบบการเปลี่ยนแปลงทันทีทันใด *(Abrupt Change)* ซึ่งจะเห็นได้ว่าวิธีการนี้นั้นจะใช้ข้อมูล 3 ชนิดพร้อมกัน ในการตรวจจับความผิดปกติของระบบโครงข่าย ซึ่งประกอบไปด้วยข้อมูลจาก *ipIR*, *ipOR* และ *ipIDE* ซึ่งค่าที่ใช้ในการตัดสินใจว่าระบบโครงข่ายเกิดความผิดปกติหรือไม่นั้นหาได้จากค่าความผิดพลาดของเวกเตอร์ความผิดพลาดของข้อมูล *[ipIR ipOR ipIDE]* ที่มีทิศทางที่ใกล้กับเวกเตอร์ความผิดปกติ [1 1 1] มากที่สุด ซึ่งหมายความว่า เวกเตอร์นั้นให้ผลที่ค่าความผิดพลาดของ 3 ชนิดข้อมูลมีการแปรผันตรงกันมากที่สุด โดยวิธีการนี้ จะเลือกค่าความผิดพลาดของเวกเตอร์ความผิดพลาดที่มีทิศทางใกล้กับเวกเตอร์ [1 1 1] มา 2 ค่า แล้วเลือกค่าที่ต่ำที่สุดเป็นค่าที่ใช้เป็นเกณฑ์สำหรับใช้ในการบ่งชี้ว่าขณะนี้ระบบโครงข่ายของเราเกิดความผิดปกติหรือไม่ ดังนั้นเราจึงเสนอวิธีการเลือกค่าที่ใช้เป็นเกณฑ์ในการบ่งชี้ถึงความผิดปกติในโครงข่ายของวิธีการตรวจจับความผิดปกติแบบทันทีทันใด ด้วยกัน 2 วิธีคือ 1) การเลือกใช้ค่ากลางของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด และ 2) การเลือกใช้ค่าเฉลี่ยของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด นอกจากนี้ในบทนี้จะวิเคราะห์ถึงผลของขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติที่มีผลต่อความแน่นอนในการตรวจจับความผิดปกติที่อาจจะเกิดขึ้นในอนาคต ผลของจำนวนรอบที่ใช้ในการหาค่าเมตริกซ์ที่แสดงถึงความสัมพันธ์กันของความผิดปกติของข้อมูลหลายระดับต่อผลของการตรวจจับความผิดปกติของระบบโครงข่าย และผลของค่า *Threshold* ของแต่ละวิธีที่มีความสัมพันธ์ถึงขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่าย

เนื้อหาในบทที่ 4 นี้จะแบ่งเป็น 3 ส่วน ซึ่งส่วนที่ 1 จะเกี่ยวข้องกับวิธีการที่เรานำเสนอในการปรับปรุงวิธีการตรวจจับความผิดปกติแบบเปลี่ยนแปลงทันทีทันใด ส่วนที่ 2 แสดงถึงดัชนีชี้วัดที่ใช้ในการประเมินประสิทธิภาพของวิธีตรวจจับความผิดปกติของระบบโครงข่าย และส่วนที่ 3 จะกล่าวถึงผลการทดลองและสรุปผลการทดลอง

4.1 วิธีการที่นำเสนอในการปรับปรุงวิธีการตรวจจับความผิดปกติแบบเปลี่ยนแปลงทันทีทันใด

ในที่นี้เราจะอธิบายถึงวิธีที่ใช้การหาค่าเกณฑ์ในการตัดสินใจว่าเกิดความผิดปกติในระบบโครงข่ายหรือไม่ด้วยกัน 3 วิธี คือ 1) การใช้ค่าน้อยสุดของความผิดพลาด 2 ตัว ที่ใกล้กับเวกเตอร์ความผิดปกติ [1 1 1] มากที่สุด 2) การเลือกใช้ค่ากลางของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด และ 3) การเลือกใช้ค่าเฉลี่ยของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด

4.1.1 การใช้ค่าน้อยสุดของความผิดพลาด 2 ตัว ที่ใกล้กับเวกเตอร์ความผิดปกติ [1 1 1] มากที่สุด

ในวิธีการของการตรวจจับความผิดปกติของระบบโครงข่ายแบบเปลี่ยนแปลงทันทีทันใดนั้นในกรณีที่เราใช้ชนิดข้อมูลในการตรวจจับความผิดปกติของระบบโครงข่ายเป็น 3 ชนิด จะได้ค่า *Eigenvalue* และ *Eigenvector* อย่างละ 3 ค่า ซึ่ง จะนำค่า *Eigenvector* แต่ละค่านี้มาตรวจสอบว่า *Eigenvector* 2 ค่าไหนที่มีทิศทางไปทางเดียวกับเวกเตอร์ความผิดปกติ [1 1 1] มากที่สุด แล้วนำค่า *Eigenvalue* ของ *Eigenvector* 2 ค่านั้นมาพิจารณาหาค่าที่ใช้ในการบอกว่าระบบโครงข่ายของเราตอนนี้เกิดความผิดปกติหรือไม่ ดังสมการที่ (4.1)

$$Th = \min_{i=1}^{2}(\lambda_i(\max(\frac{[111]*\vec{\phi}}{|\vec{\phi}|}))) \tag{4.1}$$

ซึ่ง $1 < N < M$ โดยที่ M เป็นจำนวนชนิดข้อมูลที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่าย ซึ่งถ้าค่าความผิดปกติของระบบโครงข่ายเกินค่าเกณฑ์ จะถือว่าระบบโครงเกิดความผิดปกติขึ้น

4.1.2 การเลือกใช้ค่ากลางของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด

ในวิธีการของการตรวจจับความผิดปกติของระบบโครงข่ายแบบเปลี่ยนแปลงทันทีทันใดนั้น ในกรณีที่เราใช้ชนิดข้อมูลในการตรวจจับความผิดปกติของระบบโครงข่าย 3 ชนิด จะได้ *Eigenvalue* และ *Eigenvector* อย่างละ 3 ค่า ซึ่งค่าที่ใช้เป็นเกณฑ์ในการบอกว่าระบบเกิดความผิดปกติหรือไม่ เราจะเลือกใช้ค่าความผิดพลาดค่ากลาง ซึ่ง $\lambda_1 < \lambda_2 < \lambda_3$ ดังสมการที่ (4.2)

$$Th = \lambda_2 \tag{4.2}$$

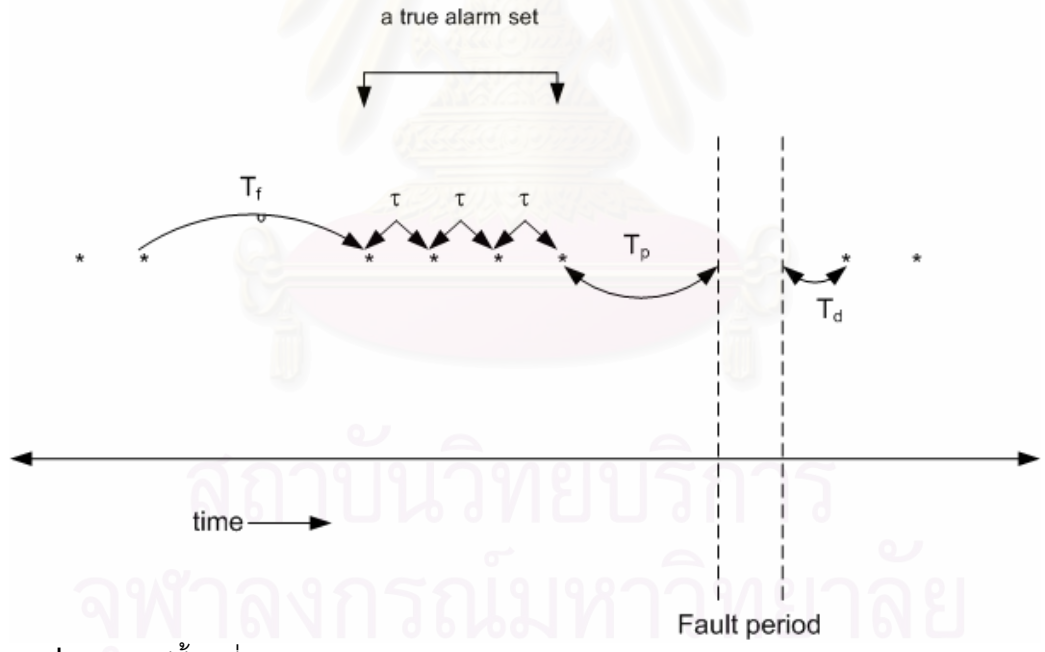
4.1.3 การเลือกใช้ค่าเฉลี่ยของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด

ในวิธีการของการตรวจจับความผิดปกติของระบบโครงข่ายแบบเปลี่ยนแปลงทันทีทันใดนั้น ในกรณีที่เราใช้ชนิดข้อมูลในการตรวจจับความผิดปกติของระบบโครงข่ายเป็น 3 ชนิด จะได้ค่า *Eigenvalue* และ *Eigenvector* อย่างละ 3 ค่า ซึ่งค่าที่ใช้เป็นเกณฑ์ในการบอกว่าระบบเกิดความผิดปกติหรือไม่เราจะเลือกใช้เฉลี่ยเลขคณิตของค่าความผิดพลาดของ $\lambda_1, \lambda_2, \lambda_3$ ซึ่ง $\lambda_1 < \lambda_2 < \lambda_3$ ดังสมการที่ (4.3)

$$Th = \frac{\lambda_1 + \lambda_2 + \lambda_3}{3} \tag{4.3}$$

4.2 ดัชนีชี้วัดที่ใช้ในการประเมินประสิทธิภาพของวิธีตรวจจับความผิดปกติของระบบโครงข่าย

ในการประเมินว่าวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบเปลี่ยนแปลงทันทีทันใดมีประสิทธิภาพหรือไม่นั้น เราจะใช้ดัชนีชี้วัดที่ประกอบไปด้วย T_f, T_p, T_d, τ ดังรูปที่ 4.1



รูปที่ 4.1 ดัชนีชี้วัดที่ใช้ในการประเมินประสิทธิภาพของการตรวจจับความผิดปกติของระบบโครงข่าย

ซึ่ง N_f คือ จำนวนสัญญาณเตือนที่ผิดพลาดต่อจำนวนหน้าต่างข้อมูล

T_f คือ ช่วงเวลาที่เกิดความผิดพลาดในการทำนายความผิดปกติของระบบโครงข่าย

T_p คือ ช่วงเวลาที่สามารถทำนายความผิดปกติได้ก่อนเกิดความผิดปกติในระบบโครงข่าย

T_d คือ เวลาที่สามารถตรวจจับความผิดปกติได้หลังจากเกิดความผิดปกติในระบบโครงข่ายไปแล้ว

τ คือ ช่วงเวลาที่สัญญาณเตือนความผิดปกติยังคงเป็นสัญญาณเตือนที่ถูกต้องในการตรวจจับความผิดปกติในระบบโครงข่าย

โดยที่มีเงื่อนไขที่ว่า $\tau < 15\,\text{min}$ (4.4)

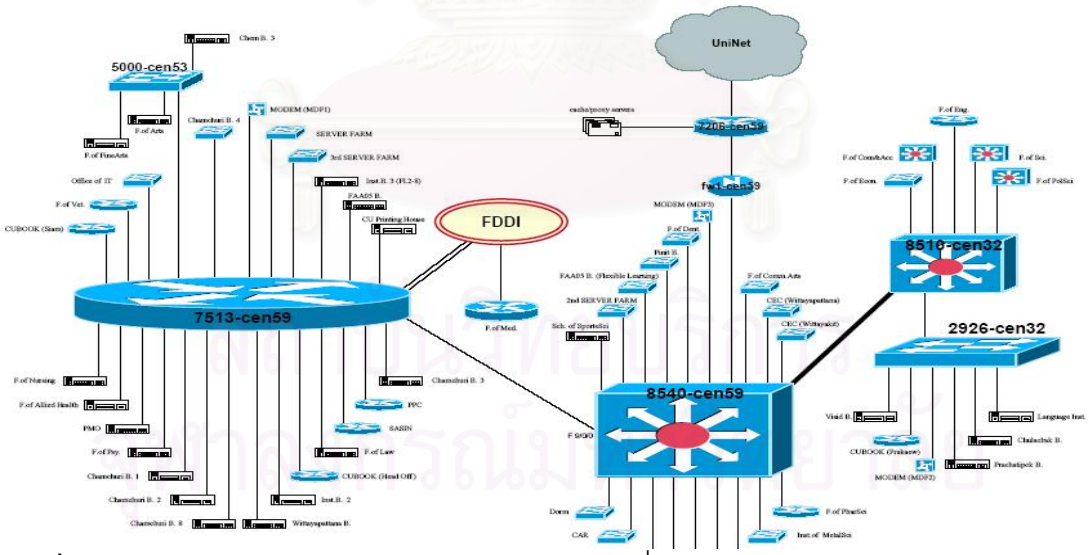
ในที่นี้เราได้นิยามตัวแปร S ซึ่งใช้เป็นตัวบอกว่าระบบโครงข่ายของเราควรเลือกใช้ค่าขนาดหน้าต่างเท่าใดในการตรวจจับความผิดปกติของระบบโครงข่าย โดยที่ ค่าตัวแปร S มีค่าดังสมการที่ (4.5)

$$S = T_f * N_f \quad (4.5)$$

ซึ่งถ้าค่า S ยิ่งมีค่ามากแสดงว่าขนาดหน้าต่างนั้นให้ค่าการตรวจจับความผิดปกติโครงข่ายที่มีประสิทธิภาพสูงขึ้น

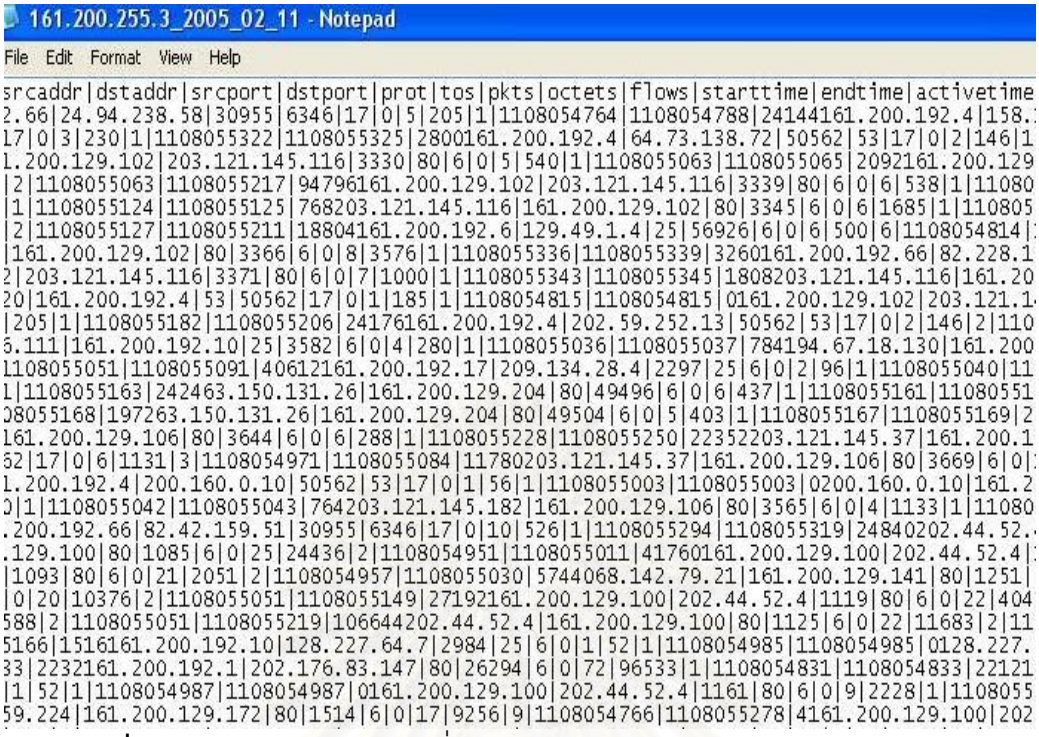
4.3 ผลการทดลองและสรุปผลการทดลอง

ในการทดลองเพื่อทดสอบประสิทธิภาพของวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบทันทีทันใดที่นำเสนอนั้น จะใช้ข้อมูลทราฟฟิกที่ได้จากโครงข่ายของจุฬาลงกรณ์มหาวิทยาลัยที่รูทเทอร์ 7513 ซึ่งแสดงดังรูปที่ 4.2



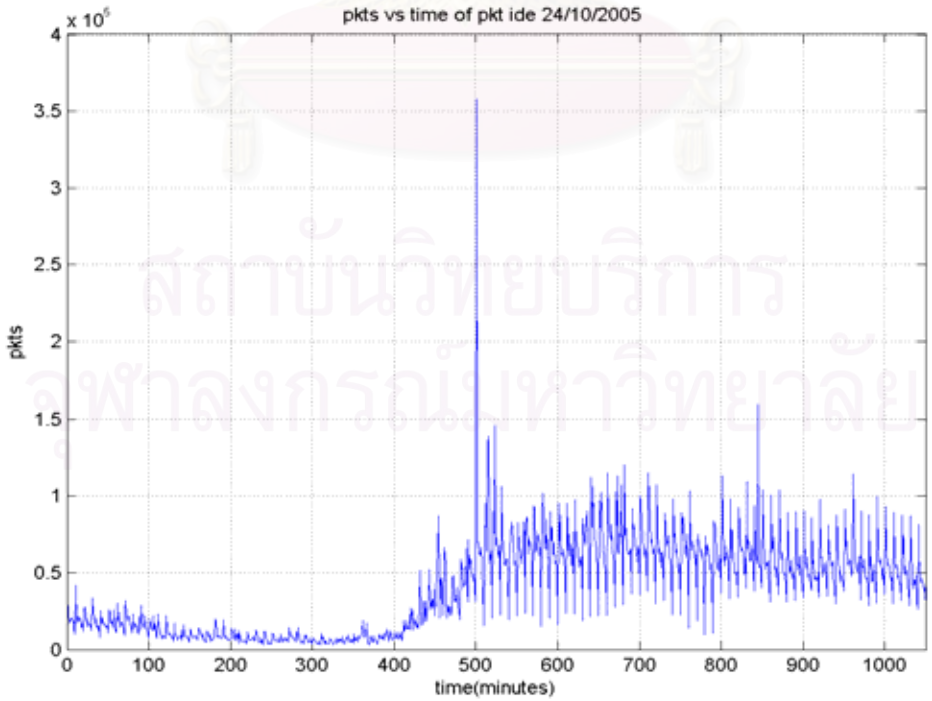
รูปที่ 4.2 ระบบโครงข่ายของจุฬาลงกรณ์มหาวิทยาลัย ที่รูทเทอร์ หมายเลข 7513 และ รูทเทอร์ หมายเลข 7206

ข้อมูลของการส่งข้อมูลที่ได้จากรูทเทอร์ 7513 นั้นถูกเก็บโดยใช้โปรแกรม *NETFLOW* ซึ่งการเก็บข้อมูลของโปรแกรม *NETFLOW* นี้แสดงดังรูปที่ 4.3

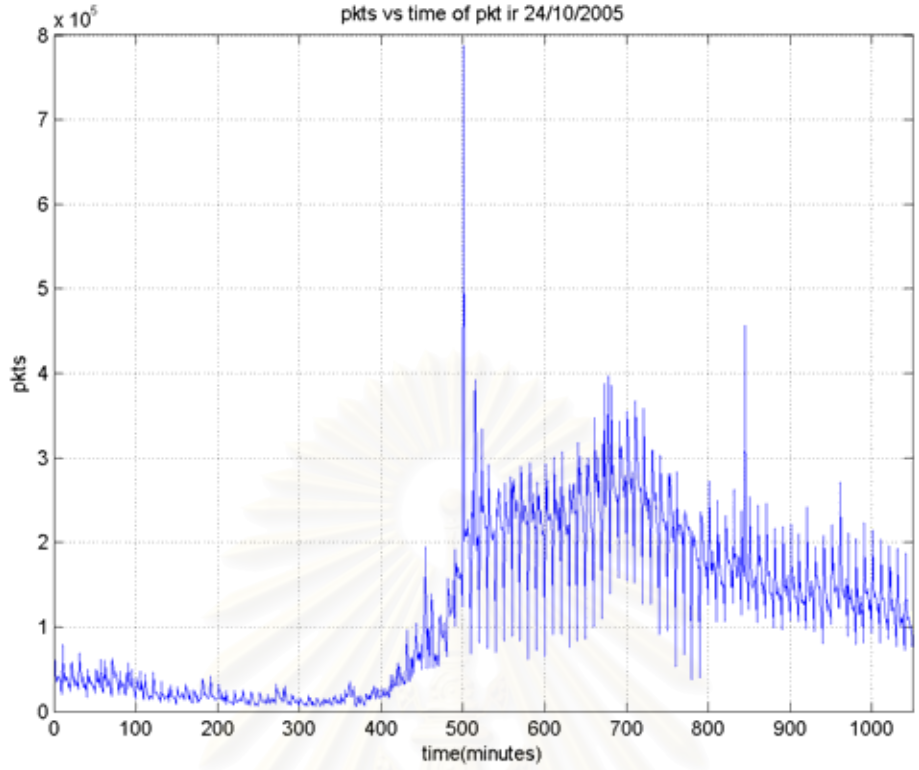


รูปที่ 4.3 ลักษณะของทราฟฟิกที่โปรแกรม *NETFLOW* บันทึกในรูทเทอร์ 7513

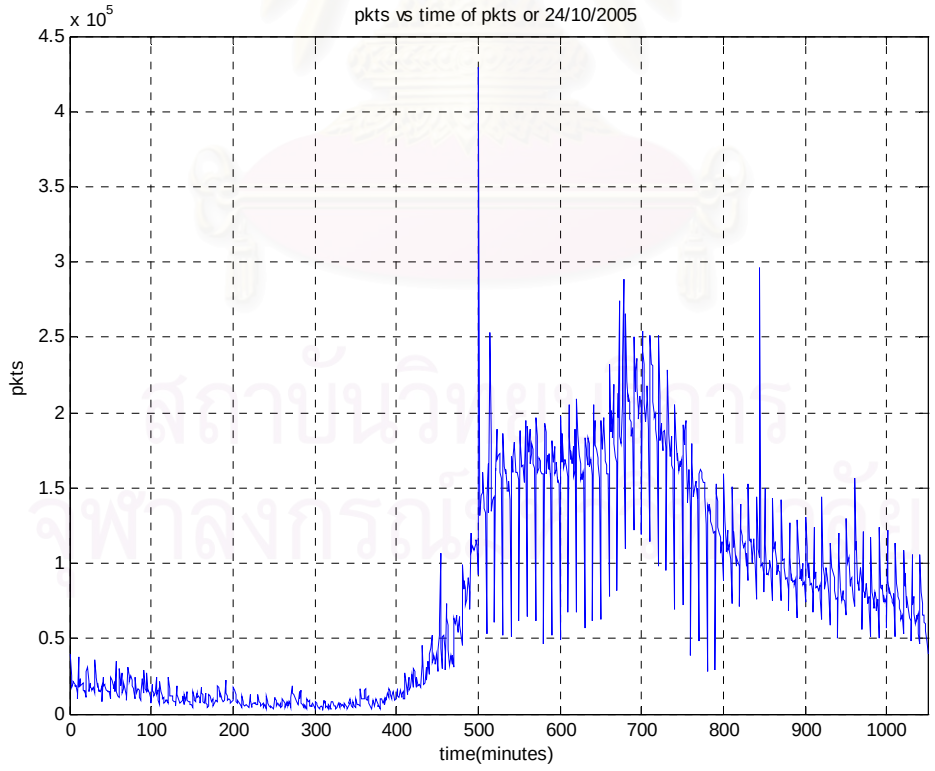
จากผลของข้อมูลที่ได้จากโปรแกรม *NETFLOW* นี้เราจึงต้องนำข้อมูลนี้มาทำการแบ่งแยกเป็นชนิดของข้อมูล *ipIR*, *ipIDE* และ *ipOR* โดยใช้โปรแกรม *PERL* ในการแบ่งแยกชนิดข้อมูล ซึ่งในการทดลองนี้เราจะใช้ข้อมูลของวันที่ 24 ตุลาคม 2548 ในการตรวจจับความผิดปกติของระบบโครงข่าย แสดงดังรูปที่ 4.4-4.6



รูปที่ 4.4 ข้อมูล *ipIDE* ของรูทเทอร์ 7513 ในวันที่ 24/10/2005



รูปที่ 4.5 ข้อมูล *ipIR* ของรูทเทอร์ 7513 ในวันที่ 24/10/2005



รูปที่ 4.6 ข้อมูล *ipOR* ของรูทเทอร์ 7513 ในวันที่ 24/10/2005

เราได้แบ่งการทดลองออกเป็น 2 ส่วนคือ ส่วนแรก เราได้ศึกษาถึงผลของการเปลี่ยนขนาดหน้าต่างและจำนวนรอบในการคำนวณเมตริกซ์ A ที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่ายต่อค่า *Threshold* ส่วนที่สอง เรากำหนดให้จำนวนรอบที่ใช้ในการหาค่าเมตริกซ์ A มีค่าคงที่เท่ากับ 14 รอบ แต่ปรับเปลี่ยนค่าความกว้างของหน้าต่างในการตรวจจับความผิดปกติของระบบโครงข่าย

เนื่องจากข้อมูลทราฟฟิกที่บันทึกได้จากโปรแกรม *NETFLOW* ที่ได้จากโครงข่ายจุฬาลงกรณ์มหาวิทยาลัยนั้น ไม่ได้มีการบันทึกว่าในช่วงเวลาที่ผ่านมาเกิดความผิดปกติขึ้นเมื่อใด ด้วยสาเหตุใด เป็นเวลานานเท่าใด ดังนั้นจากรูปที่ 4.4-4.6 ของทราฟฟิกวันที่ 24 ตุลาคม 2548 เราจึงได้กำหนดให้มีความผิดปกติเกิดขึ้นที่ระบบโครงข่ายที่เวลา 500 นาที ด้วยเหตุผลที่ว่าที่เวลานี้จำนวนแพ็กเก็ตมีความเปลี่ยนแปลงอย่างมากเมื่อเทียบกับช่วงเวลาที่ติดกัน

ในการทดลองนั้นเราได้มีการกำหนดตัวแปรในการแสดงผลของแต่ละวิธีในการตรวจจับความผิดปกติของระบบโครงข่ายดังนี้

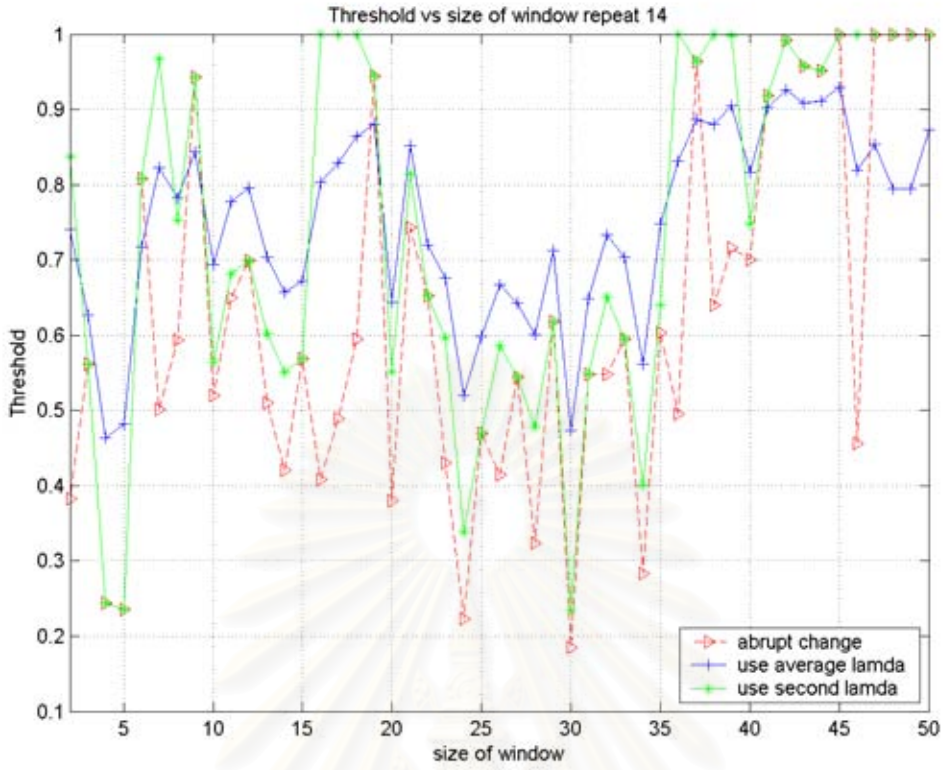
useabruptchange หมายถึง การใช้ค่าน้อยสุดของความผิดพลาด 2 ตัว ที่ใกล้กับเวกเตอร์ความผิดปกติ [1 1 1] มากที่สุด เป็นค่า *Threshold*

useaveragelamda หมายถึง การเลือกใช้ค่าเฉลี่ยของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด เป็นค่า *Threshold*

usesecondlamda หมายถึง การเลือกใช้ค่ากลางของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด เป็นค่า *Threshold*

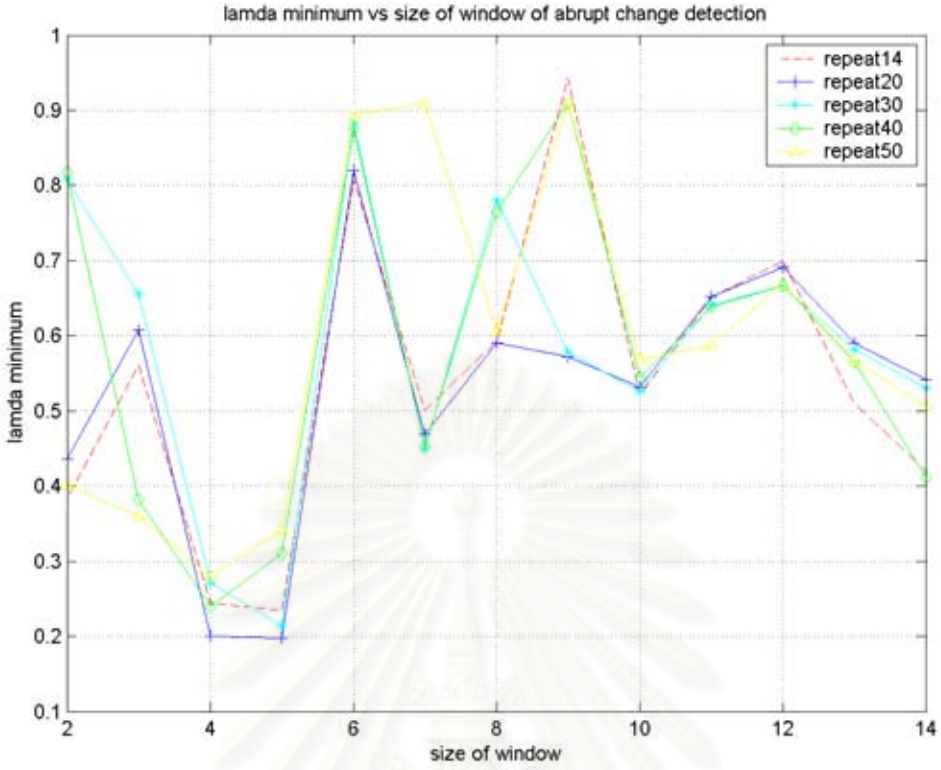
4.3.1 ผลของการแปรเปลี่ยนขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่ายต่อค่า *Threshold*

ในการทดลองเพื่อทดสอบประสิทธิภาพของวิธีการตรวจจับความผิดปกติแบบทันทีทันใดที่นำเสนอทั้งสิ้น 3 วิธี ในส่วนแรกนั้นได้ผลการทดลองดังรูปที่ 4.7-4.10

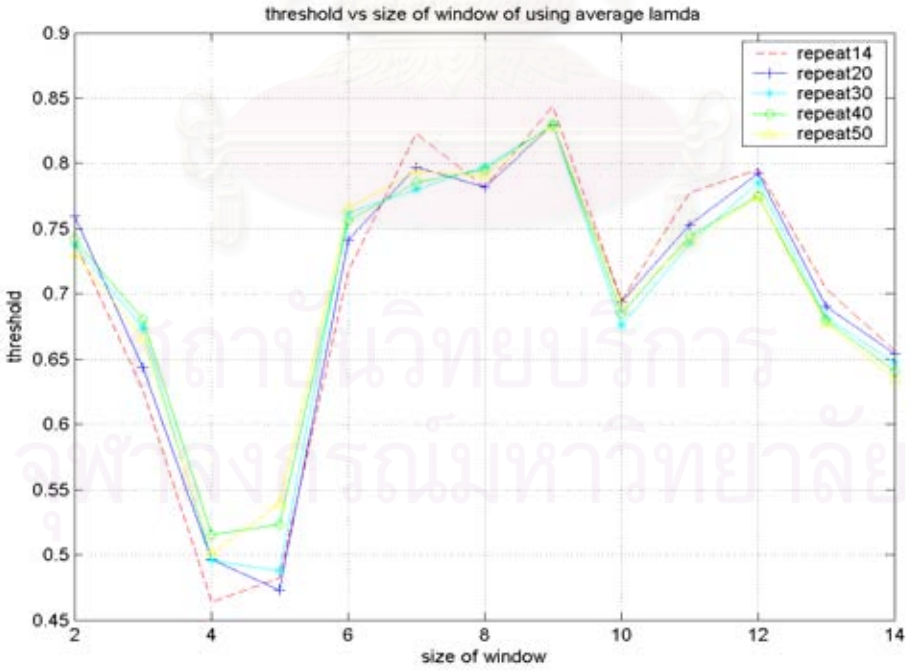


รูปที่ 4.7 ความสัมพันธ์ระหว่างค่า *Threshold* และขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่าย

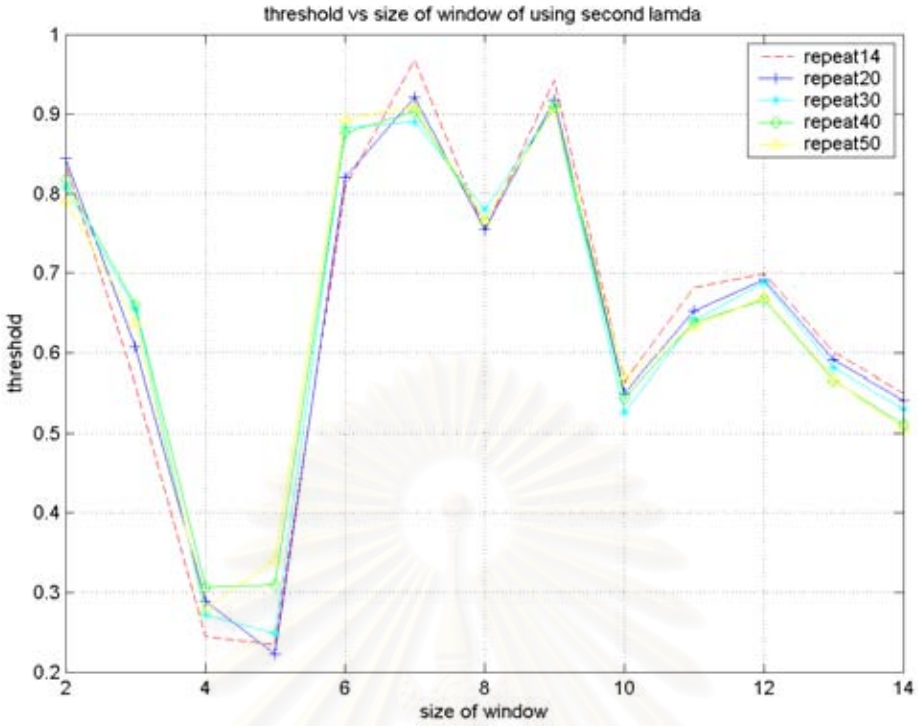
จากผลการทดลองจะเห็นได้ว่าค่าเกณฑ์ในการตัดสินใจว่าระบบโครงข่ายเกิดความผิดปกติหรือไม่ของวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบทันทีทันใด วิธีการที่เรานำเสนอโดยการเลือกใช้ค่ากลางของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด และการเลือกใช้ค่าเฉลี่ยของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด เมื่อมีการเปลี่ยนขนาดหน้าต่างในการตรวจจับความผิดปกติของระบบโครงข่ายไปเรื่อยๆ มีค่าเปลี่ยนไปตามขนาดหน้าต่างที่เปลี่ยนไป และไม่มีแนวโน้ม ดังนั้นการตรวจจับความผิดปกติของโครงข่ายโดยใช้วิธีการทั้ง 3 วิธีนี้จะต้องมีการทดสอบและเลือกค่าขนาดหน้าต่างที่เหมาะสมเพื่อที่จะทำให้ระบบการตรวจจับความผิดปกติมีประสิทธิภาพที่ดี ซึ่งขนาดหน้าต่างในทางปฏิบัติที่ควรใช้ควรอยู่ในช่วง 5 ถึง 20 นาที เนื่องจากถ้าใช้ขนาดหน้าต่างที่ยาวเกินไป จะทำให้ระบบการตรวจจับความผิดปกติไม่สามารถตรวจจับความผิดปกติได้ทันท่วงที



รูปที่ 4.8 ความสัมพันธ์ระหว่างค่า *Threshold* และขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่ายโดยการเลือกค่า *Threshold* จากวิธีการเปลี่ยนแปลงทันทีทันใด



รูปที่ 4.9 ความสัมพันธ์ระหว่างค่า *Threshold* และขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่ายโดยการเลือกค่า *Threshold* จากค่าเฉลี่ยของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด

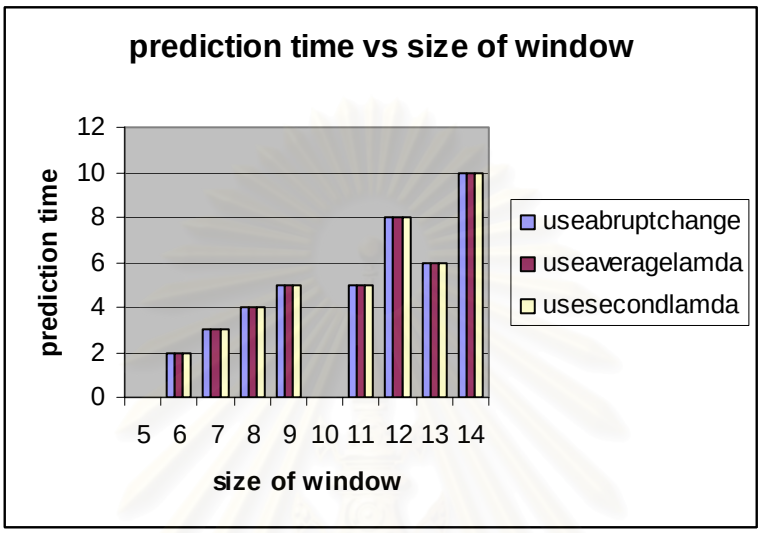


รูปที่ 4.10 ความสัมพันธ์ระหว่างค่า *Threshold* และขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่ายโดยการเลือกค่า *Threshold* จากค่ากลางของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด

จากผลการทดลองจะเห็นได้ว่าค่าเกณฑ์ในการตัดสินใจว่าระบบโครงข่ายเกิดความผิดปกติหรือไม่ของวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบทันทีทันใด วิธีการที่เรานำเสนอโดยการเลือกใช้ค่ากลางของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด และการเลือกใช้ค่าเฉลี่ยของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด จะมีค่าแปรเปลี่ยนไปตามจำนวนรอบที่ใช้ในการคำนวณหาค่าเมตริกซ์ *A* ซึ่งค่าเกณฑ์ในการตัดสินใจว่าระบบโครงข่ายเกิดความผิดปกติของวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบทันทีทันใดในแต่ละรอบของการคำนวณหาค่าเมตริกซ์ *A* นั้นมีค่าที่ต่างกันอย่างมาก เพราะฉะนั้นจำนวนรอบที่ใช้ในการคำนวณหาเมตริกซ์ *A* มีผลอย่างมาก ในกรณีที่จำนวนรอบในการคำนวณหาเมตริกซ์ *A* ถูกเลือกไม่เหมาะสม จะส่งผลให้ระบบโครงข่ายของเราเกิดสัญญาณเตือนที่ผิดพลาดบ่อยครั้ง ในส่วนของการเลือกใช้ค่ากลางของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด การเลือกใช้ค่าเฉลี่ยของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด จำนวนรอบในการคำนวณหาเมตริกซ์ A ไม่ค่อยมีผลมากนักต่อค่าเกณฑ์ในการตัดสินใจว่าระบบโครงข่ายเกิดความผิดปกติ

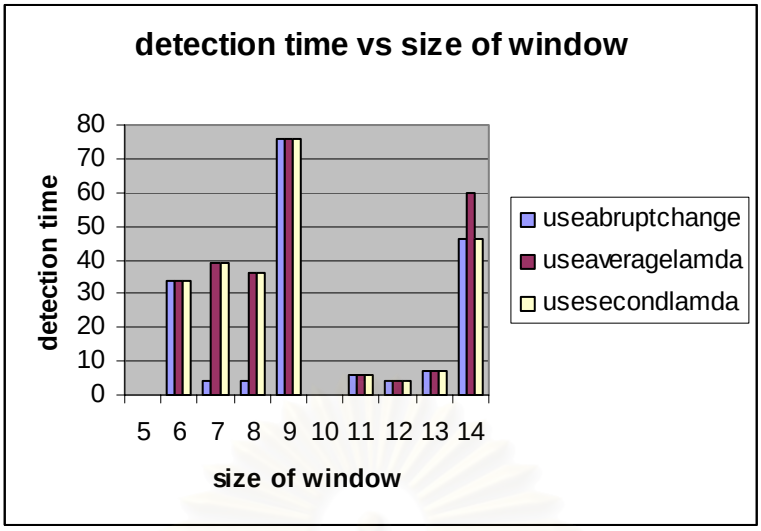
4.3.2 จำนวนรอบที่ใช้ในการหาค่าเมตริกซ์ A มีค่าคงที่เท่ากับ 14 รอบ แต่ปรับเปลี่ยนค่าความกว้างของหน้าต่างในการตรวจจับความผิดปกติของระบบโครงข่าย

ในการทดลองเพื่อทดสอบประสิทธิภาพของวิธีการตรวจจับความผิดปกติแบบทันทีทันใดที่นำเสนอทั้งสิ้น 3 วิธี ในส่วนแรกนั้นได้ผลการทดลองดังรูปที่ 4.11-4.15



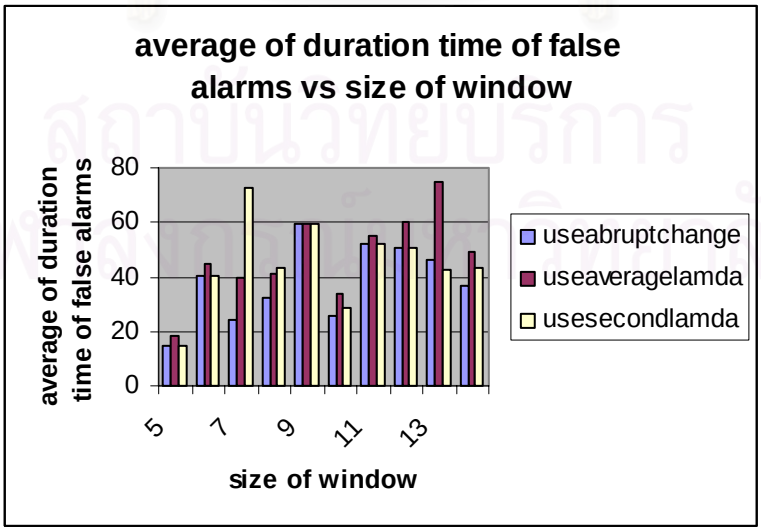
รูปที่ 4.11 ความสัมพันธ์ระหว่างเวลาที่สามารถตรวจจับความผิดปกติก่อนเกิดความเสียหายและขนาดความกว้างของหน้าต่างที่ใช้ในการตรวจจับความผิดปกติ

จากผลการทดลองดังรูปที่ 4.11 ขนาดของหน้าต่างที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่ายที่แตกต่างกันจะให้ผลของเวลาที่สามารถตรวจจับความผิดปกติก่อนเกิดความเสียหายที่แตกต่างกัน โดยที่ทั้ง 3 วิธีที่ทดสอบนั้นให้ผลของเวลาที่สามารถตรวจจับความผิดปกติก่อนเกิดความเสียหายเท่ากันทุกขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติ ที่เป็นเช่นนี้เนื่องจากทราฟฟิกที่ใกล้กับช่วงเวลาที่ 500 มีการเกิดการเปลี่ยนแปลงเป็นอย่างมากเป็นผลให้ค่าความผิดปกติในช่วงนี้มีค่าที่สูงมาก ดังนั้นค่าเกณฑ์ของทั้ง 3 วิธีซึ่งให้ค่าเกณฑ์ที่แตกต่างกัน ไม่มีผลเพราะ ค่าความผิดปกติของโนดเกินค่าเกณฑ์ของทั้ง 3 วิธี



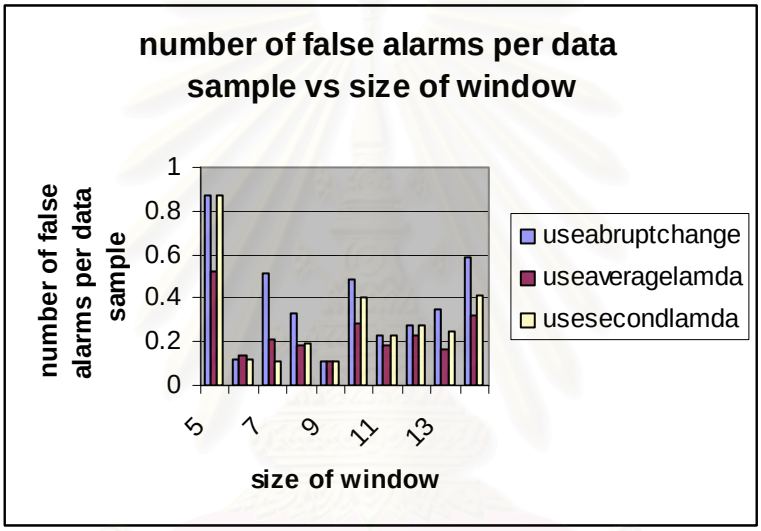
รูปที่ 4.12 ความสัมพันธ์ระหว่างค่าเฉลี่ยของเวลาที่สามารถตรวจจับความผิดปกติหลังเกิดความเสียหายและขนาดความกว้างของหน้าต่างที่ใช้ในการตรวจจับความผิดปกติ

จากผลการทดลองดังรูปที่ 4.12 จะเห็นได้ว่าขนาดของหน้าต่างที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่ายที่แตกต่างกันและการเลือกใช้วิธีที่หาค่าเกณฑ์แตกต่างกัน จะให้ผลของเวลาที่สามารถตรวจจับความผิดปกติหลังเกิดความเสียหายที่แตกต่างกัน ซึ่งเป็นผลมาจากค่าเกณฑ์ที่เลือกใช้เพื่อระบุว่าระบบโครงข่ายเกิดความผิดปกติหรือไม่มีค่าที่ต่างกัน และที่ขนาดหน้าต่างเท่ากันนั้น บางขนาดหน้าต่างเวลาที่สามารถตรวจจับความผิดปกติหลังเกิดความเสียหายมีค่าต่างกัน ที่เป็นเช่นนี้เนื่องจากค่าความผิดปกติของโนดอาจไม่มากเกินค่าเกณฑ์ของบางวิธีทำให้เวลาที่สามารถตรวจจับความผิดปกติหลังเกิดความเสียหายที่แตกต่างกัน



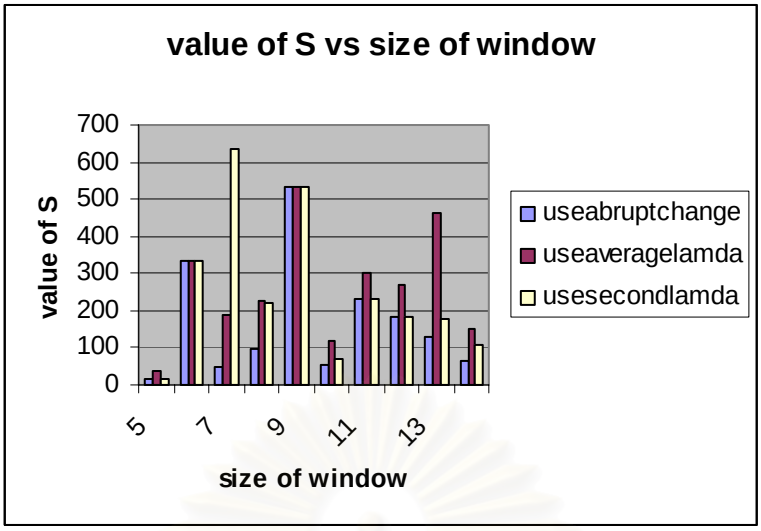
รูปที่ 4.13 ความสัมพันธ์ระหว่างค่าเฉลี่ยของช่วงเวลาที่เกิดสัญญาณเตือนที่ผิดพลาดและขนาดความกว้างของหน้าต่างที่ใช้ในการตรวจจับความผิดปกติ

จากผลการทดลองดังรูปที่ 4.13 จะเห็นได้ว่า ขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่ายที่แตกต่างกันจะให้ผลของค่าเฉลี่ยของช่วงสัญญาณเตือนที่ผิดพลาดที่แตกต่างกัน ซึ่งเป็นผลมาจากค่าเกณฑ์ที่เลือกใช้เพื่อระบุว่าระบบโครงข่ายเกิดความผิดปกติหรือไม่มีค่าที่ต่างกัน และวิธีที่นำเสนอทั้ง 2 วิธีคือ การเลือกใช้ค่ากลางของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด และการเลือกใช้ค่าเฉลี่ยของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด ให้ผลของค่าเฉลี่ยของช่วงสัญญาณเตือนที่ผิดพลาดที่สูงกว่าวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบทันทีทันใด ที่เป็นเช่นนี้เนื่องจากค่าเกณฑ์ของทั้ง 2 วิธีมีค่าที่สูงกว่า



รูปที่ 4.14 ความสัมพันธ์ระหว่างจำนวนสัญญาณเตือนที่ผิดพลาดต่อจำนวนหน้าต่างข้อมูลและขนาดความกว้างของหน้าต่างที่ใช้ในการตรวจจับความผิดปกติ

จากผลการทดลองดังรูปที่ 4.14 จะเห็นได้ว่าขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่ายที่แตกต่างกันจะให้ผลของจำนวนสัญญาณเตือนที่ผิดพลาดต่อจำนวนหน้าต่างข้อมูลที่แตกต่างกัน ซึ่งเป็นผลมาจากค่าเกณฑ์ที่เลือกใช้เพื่อระบุว่าระบบโครงข่ายเกิดความผิดปกติหรือไม่มีค่าที่ต่างกัน และวิธีที่นำเสนอทั้ง 2 วิธีคือ การเลือกใช้ค่ากลางของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด และการเลือกใช้ค่าเฉลี่ยของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด ให้ผลของจำนวนสัญญาณเตือนที่ผิดพลาดต่อจำนวนหน้าต่างข้อมูลที่ต่ำกว่าวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบทันทีทันใด ที่เป็นเช่นนี้เนื่องจากค่าเกณฑ์ของทั้ง 2 วิธีมีค่าที่สูงกว่า



รูปที่ 4.15 ความสัมพันธ์ระหว่าง *value of S* และขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่าย

จากผลการทดลองในกรณีนี้จะเห็นได้ว่า ขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติที่เปลี่ยนไป จะให้ผลของค่า *S* ที่แตกต่างกัน และวิธีที่นำเสนอทั้ง 2 วิธีคือ การเลือกใช้ค่ากลางของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด และการเลือกใช้ค่าเฉลี่ยของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด ให้ผลของค่า *S* ที่สูงกว่าวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบทันทีทันใด ในทุกขนาดหน้าต่าง ที่เป็นเช่นนี้เนื่องจากค่าเกณฑ์ของทั้ง 2 วิธีมีค่าที่สูงกว่า

4.3.3 **สรุปผลการทดลอง**

จากผลการทดลองจะเห็นได้ว่าจำนวนหน้าต่างที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่าย จำนวนรอบที่ใช้ในการคำนวณเมตริกซ์ *A* และวิธีการที่เราเลือกใช้ในการหาค่าเกณฑ์ในการระบุว่าเกิดความผิดปกติในโครงข่ายหรือไม่ มีผลต่อประสิทธิภาพในการตรวจจับความผิดปกติของระบบโครงข่าย ดังนั้นเราควรที่จะทดสอบเพื่อหาขนาดความกว้างหน้าต่างที่เหมาะสมที่สุดและจำนวนรอบที่ใช้ในการคำนวณเมตริกซ์ *A* ที่เหมาะสมที่สุดเช่นเดียวกัน เพื่อที่จะได้ประสิทธิภาพที่ดีที่สุดในการตรวจจับความผิดปกติของระบบโครงข่าย

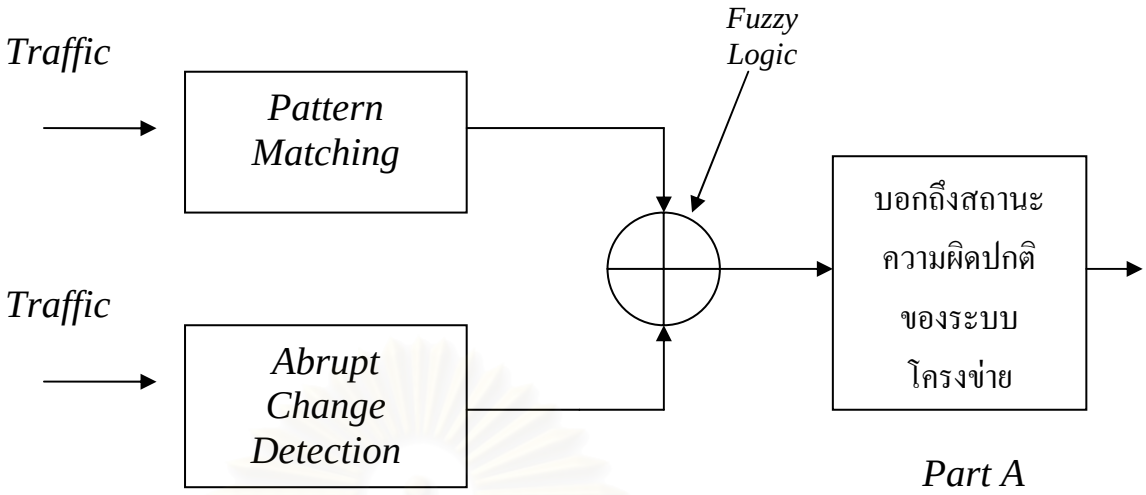
บทที่ 5
วิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกร่วมกับการเปลี่ยนแปลงทันทีทันใดโดยใช้กรรมวิธีของฟัซซีในการตัดสินใจ

ในบทที่ผ่านมาเราได้มีการนำเสนอเนื้อหาทางทฤษฎีของวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบเปรียบเทียบรูปแบบทราฟฟิก *(Pattern Matching)* และการเปลี่ยนแปลงทันทีทันใด *(Abrupt Change)* ซึ่งได้เห็นถึงข้อดีข้อเสียของวิธีการทั้งสองในการตรวจจับความผิดปกติของระบบโครงข่าย ดังนั้นในบทนี้เราจะนำเสนอวิธีการตรวจจับความผิดปกติของระบบโครงข่ายโดยใช้วิธีการเปรียบเทียบรูปแบบทราฟฟิกร่วมกับการเปลี่ยนแปลงทันทีทันใดโดยใช้กรรมวิธีของฟัซซี *(Fuzzy)*ในการตัดสินใจ โดยที่ฟังก์ชันการเป็นสมาชิกของวิธีการตรวจจับความผิดปกติของระบบโครงข่ายของวิธีการเปรียบเทียบรูปแบบทราฟฟิกและการเปลี่ยนแปลงทันทีทันใดของค่าที่ผิดปกติและไม่ผิดปกติจะเป็นแบบรูปสามเหลี่ยมและสี่เหลี่ยมคางหมู อีกทั้งยังวิเคราะห์ถึงผลของขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติที่มีผลต่อความแน่นอนในการตรวจจับความผิดปกติที่อาจจะเกิดขึ้นในอนาคต

เนื้อหาในบทที่ 5 นี้จะแบ่งเป็น 3 ส่วน โดยส่วนที่ 1 จะเกี่ยวข้องกับวิธีการที่เรานำเสนอในการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกร่วมกับการเปลี่ยนแปลงทันทีทันใด ส่วนที่ 2 แสดงถึงดัชนีชี้วัดที่ใช้ในการประเมินประสิทธิภาพของวิธีตรวจจับความผิดปกติของระบบโครงข่าย ส่วนที่ 3 จะแสดงถึงผลการทดลองและสรุปผลการทดลอง

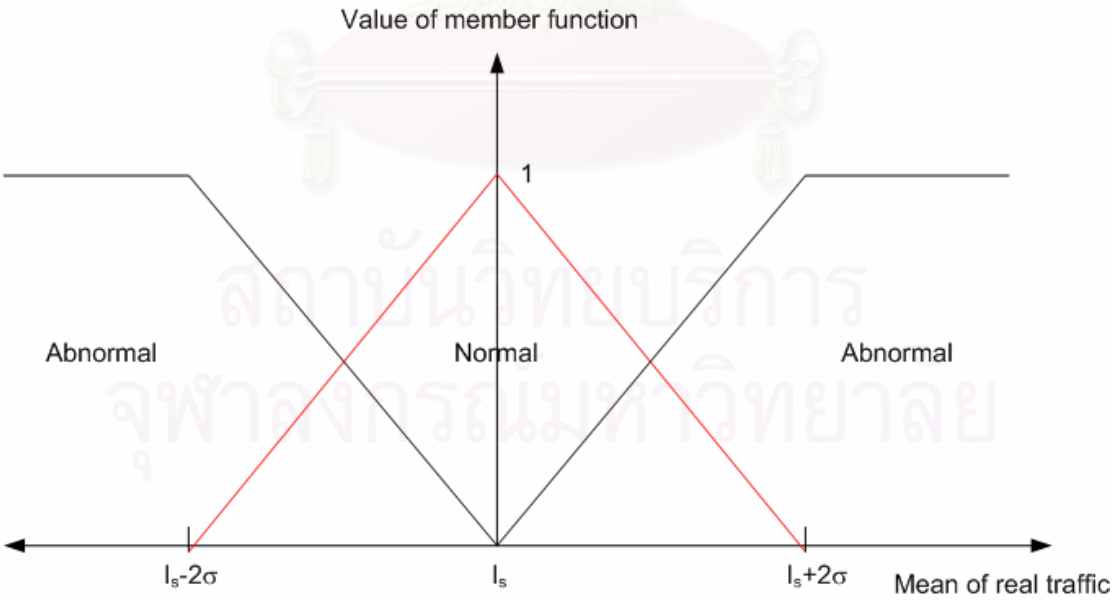
5.1 วิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกร่วมกับการเปลี่ยนแปลงทันทีทันใดโดยใช้กรรมวิธีของฟัซซีในการตัดสินใจ

โดยการตรวจจับความผิดปกติของทราฟฟิกนี้ เราจะใช้ 2 วิธี ร่วมกันในการตรวจจับความผิดปกติของระบบโครงข่ายเบื้องต้น ในการบอกว่าข้อมูลในช่วงนั้นมีความผิดปกติมากน้อยเพียงใด เราจะนำวิธีการของการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก และ แบบเปลี่ยนแปลงทันทีทันใด ร่วมกันในการตรวจจับความผิดปกติ โดยที่ใช้กรรมของฟัซซี มาใช้เป็นหลักในการตัดสินใจว่าโนดในระบบโครงข่ายเกิดความผิดปกติหรือไม่ แสดงดังรูปที่ 5.1

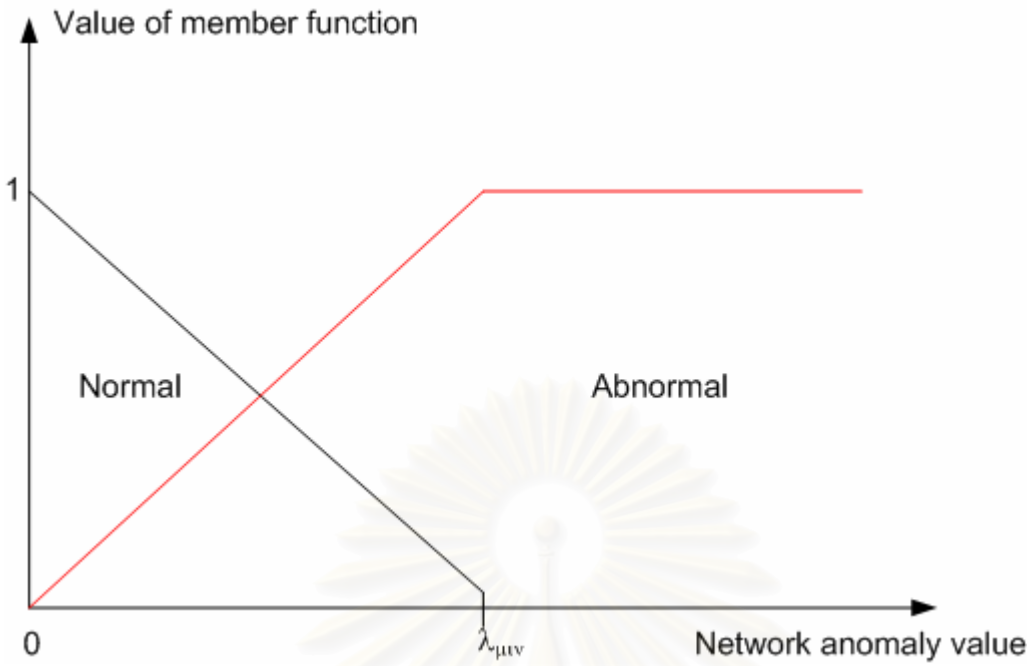


รูปที่ 5.1 การตรวจจับความผิดปกติของระบบโครงข่ายโดยใช้วิธีการเปรียบเทียบรูปแบบทราฟฟิกร่วมกับการเปลี่ยนแปลงทันทีทันใดโดยใช้กรรมวิธีฟัซซีในการตัดสินใจ

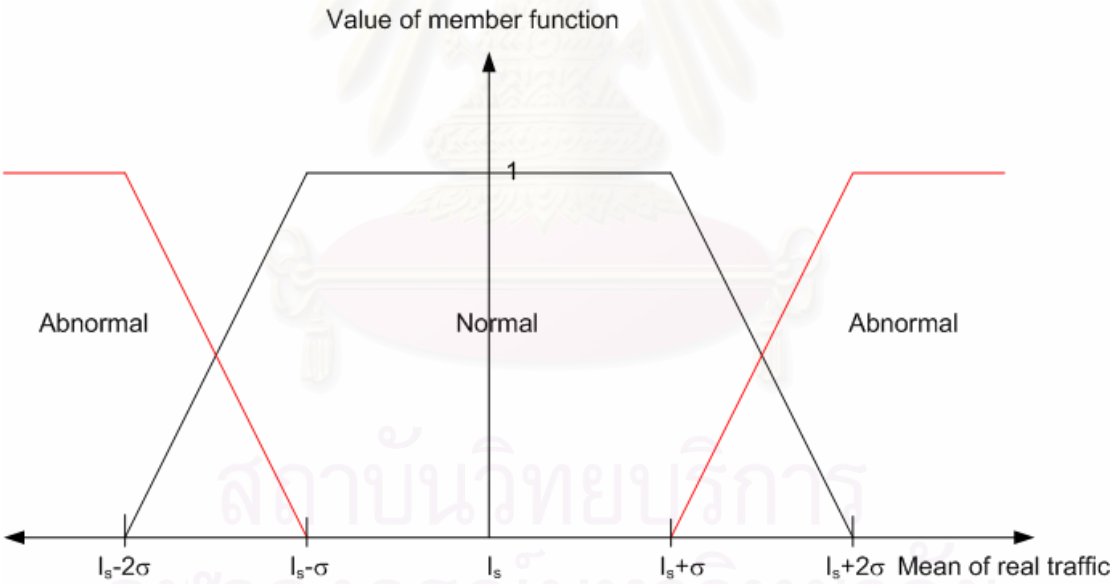
ในการใช้วิธีฟัซซีต้องมีการกำหนดฟังก์ชันการเป็นสมาชิกขึ้นมา ซึ่งในที่นี้เรามีการกำหนดให้ฟังก์ชันการเป็นสมาชิกของวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบเปรียบเทียบรูปแบบทราฟฟิกและเปลี่ยนแปลงทันทีทันใด เป็นแบบรูปสามเหลี่ยมและสี่เหลี่ยมคางหมู ประกอบไปด้วย แบบ *A* และ แบบ *B* แสดงดังรูปที่ 5.2-5.9



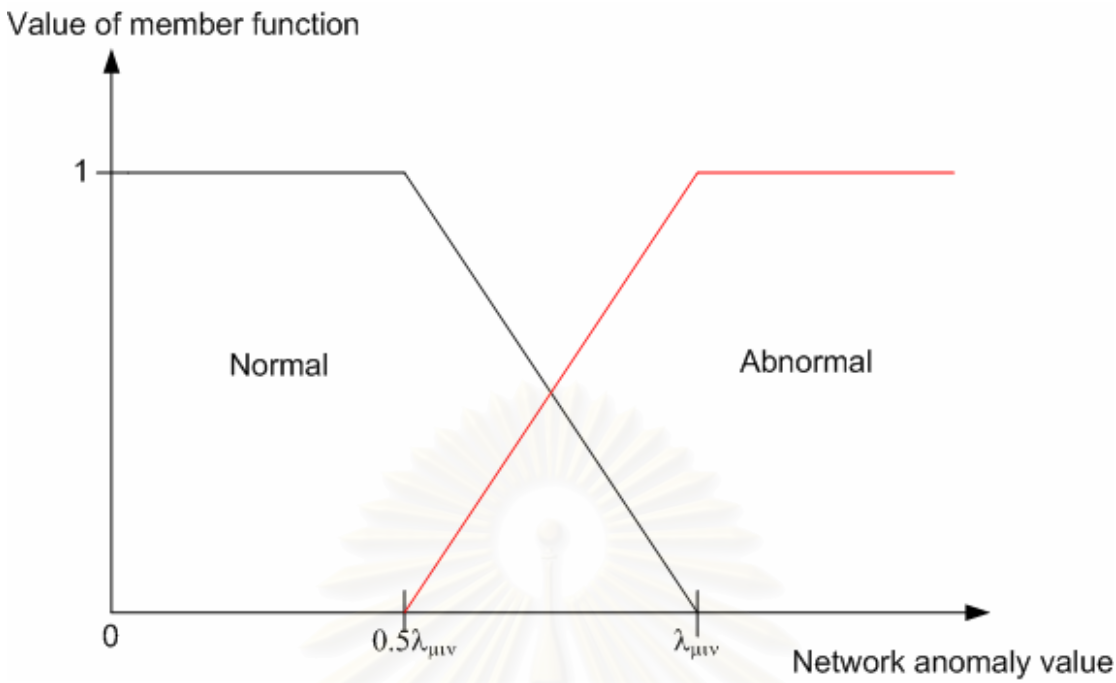
รูปที่ 5.2 ฟังก์ชันการเป็นสมาชิกของ วิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบเปรียบเทียบรูปแบบทราฟฟิกแบบสามเหลี่ยม แบบ *A*



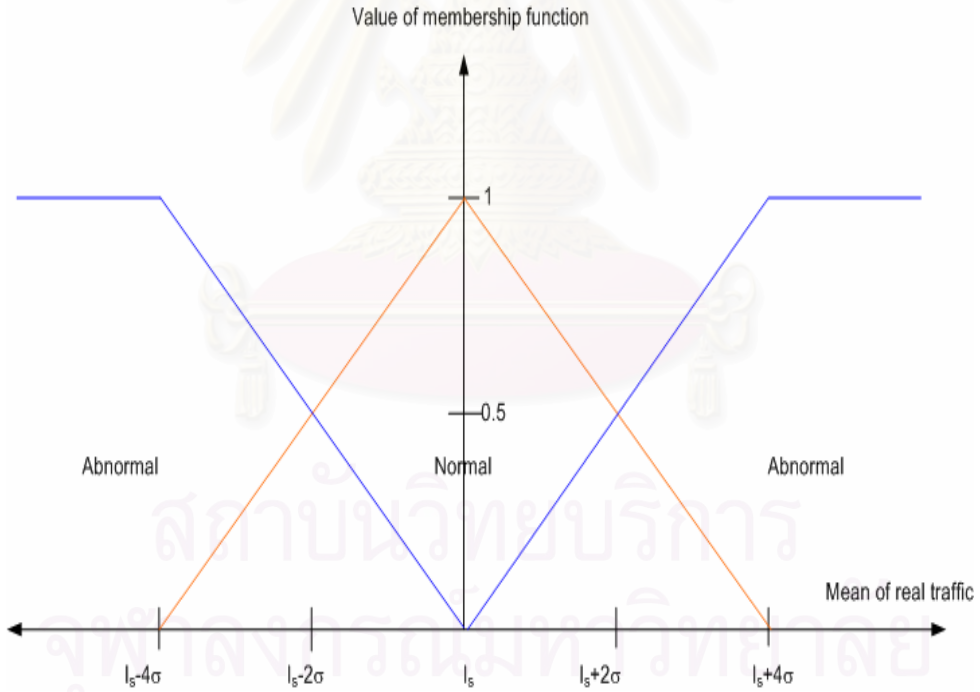
รูปที่ 5.3 ฟังก์ชันการเป็นสมาชิกของวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบเปลี่ยนแปลงทันทีทันใดแบบสามเหลี่ยม แบบ *A*



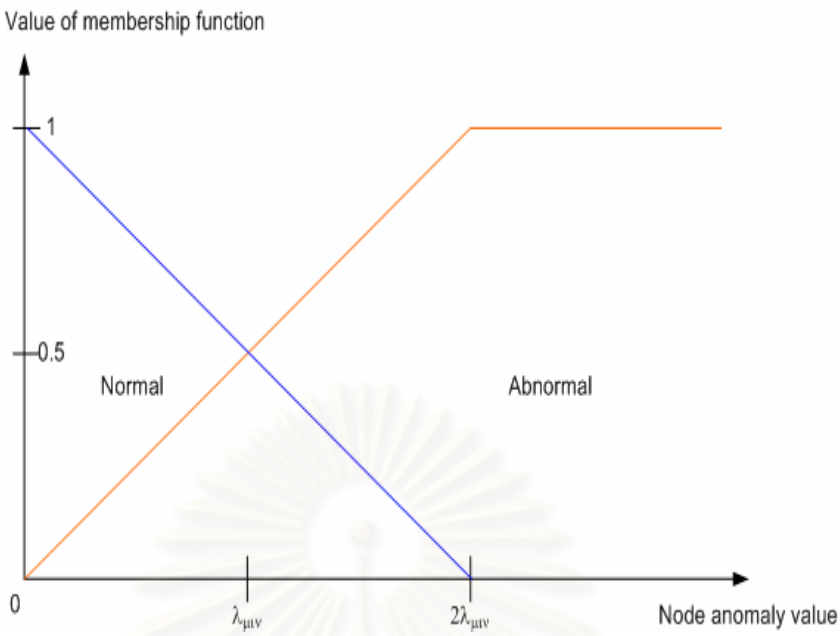
รูปที่ 5.4 ฟังก์ชันการเป็นสมาชิกของวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบเปรียบเทียบรูปแบบทราฟฟิค แบบสี่เหลี่ยมคางหมู แบบ *A*



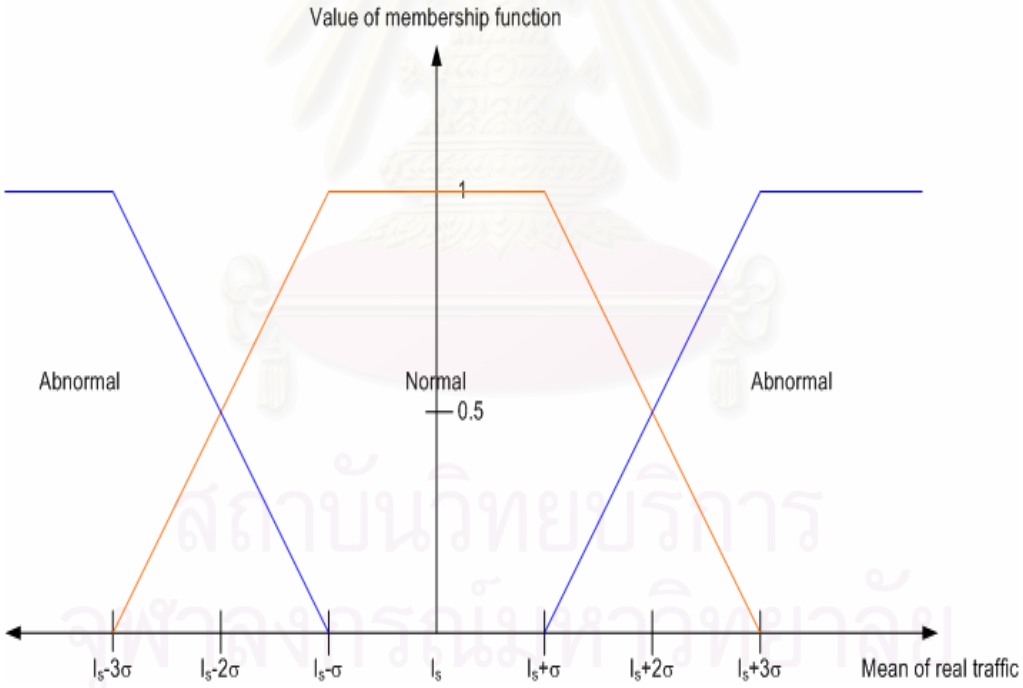
รูปที่ 5.5 ฟังก์ชันการเป็นสมาชิกของวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบเปลี่ยนแปลงทันทีทันใด แบบสี่เหลี่ยมคางหมู แบบ *A*



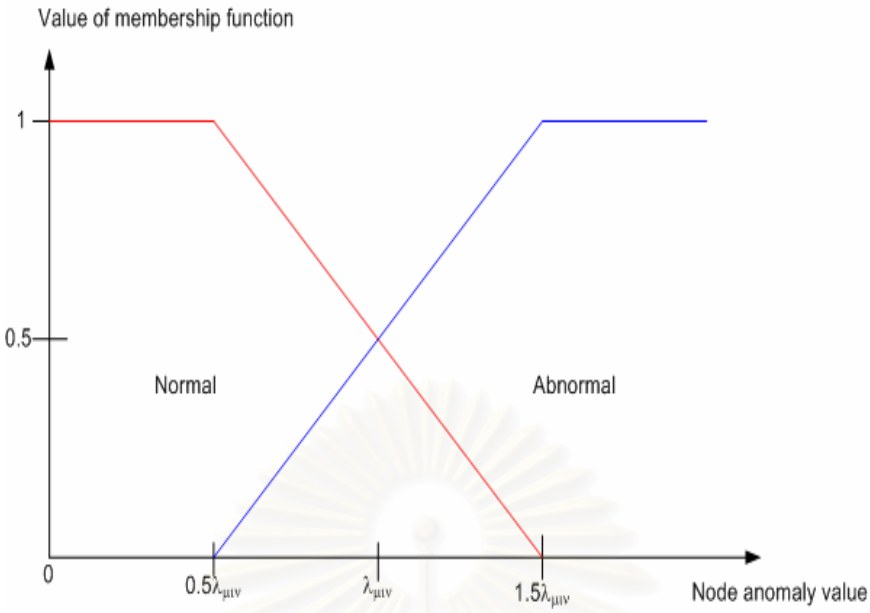
รูปที่ 5.6 ฟังก์ชันการเป็นสมาชิกของ วิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบเปรียบเทียบรูปแบบทราฟฟิกแบบสามเหลี่ยม แบบ *B*



รูปที่ 5.7 ฟังก์ชันการเป็นสมาชิกของวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบเปลี่ยนแปลงทันทีทันใดแบบสามเหลี่ยม แบบ *B*



รูปที่ 5.8 ฟังก์ชันการเป็นสมาชิกของวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบเปรียบเทียบรูปแบบทราฟฟิค แบบสี่เหลี่ยมคางหมู แบบ *B*



รูปที่ 5.9ฟังก์ชันการเป็นสมาชิกของวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบเปลี่ยนแปลงทันทีทันใด แบบสี่เหลี่ยมคางหมู แบบ *B*

โดยที่ แบบ *A* นั้นเป็นการกำหนดฟังก์ชันการเป็นสมาชิกแบบโอนเอียงไปทางทางด้านความผิดปกติ แต่แบบ *B* นั้นเป็นการกำหนดฟังก์ชันการเป็นสมาชิกแบบมีความยุติธรรม เนื่องจากวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกและแบบทันทีทันใดมีค่าเกณฑ์ของความผิดปกติอยู่ที่ $I_s \pm 2\sigma$ และ $\lambda_{\min}$ ตามลำดับ ดังนั้นที่ค่านี้จึงกำหนดให้ค่าฟังก์ชันการเป็นสมาชิกของสถานะปกติและสถานะผิดปกติของแต่ละวิธี มีค่าฟังก์ชันการเป็นสมาชิกเป็น 0.5

ในที่นี้กำหนดให้ทั้งวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกและแบบทันทีทันใด มีสถานะของโนดทั้งสิ้น 2 สถานะ คือ 0 แทนสถานะที่ไม่เกิดความผิดปกติ และ 1 แทนสถานะที่เกิดความผิดปกติ หลังจากนั้นต้องมีการกำหนดสถานะของโนดเมื่อสถานะของแต่ละวิธีในการตรวจจับความผิดปกติแสดงขึ้น แสดงดังตารางที่ 5.1-5.4

	Pattern Matching	
	Normal(0)	*Alarm(1)*
Normal(0)	0	0
Alarm(1)	1	1

Abrupt Change Detection

ตารางที่ 5.1 การเปลี่ยนสถานะของโนดเมื่อมีการใช้ข้อมูลแสดงสถานะความผิดปกติของวิธีตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก และ เปลี่ยนแปลงทันทีทันใดในกรณีที่เชื่อในวิธีของการเปลี่ยนแปลงทันทีทันใด

	Pattern Matching		
	Normal(0)	*Alarm(1)*	
Normal(0)	0	1	*Abrupt Change Detection*
Alarm(1)	0	1	

ตารางที 5.2 การเปลี่ยนสถานะของโนดเมื่อมีการใช้ข้อมูลแสดงสถานะความผิดปกติของวิธีตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก และ เปลี่ยนแปลงทันทีทันใดในกรณีที่เชื่อในวิธีของการเปรียบเทียบรูปแบบทราฟฟิก

	Pattern Matching		
	Normal(0)	*Alarm(1)*	
Normal(0)	0	1	*Abrupt Change Detection*
Alarm(1)	1	1	

ตารางที 5.3 การเปลี่ยนสถานะของโนดเมื่อมีการใช้ข้อมูลแสดงสถานะความผิดปกติของวิธีตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก และ เปลี่ยนแปลงทันทีทันใด ในกรณีที่เชื่อในวิธีของการเปรียบเทียบรูปแบบทราฟฟิกและ เปลี่ยนแปลงทันทีทันใด

	Pattern Matching		
	Normal(0)	*Alarm(1)*	
Normal(0)	0	0	*Abrupt Change Detection*
Alarm(1)	0	1	

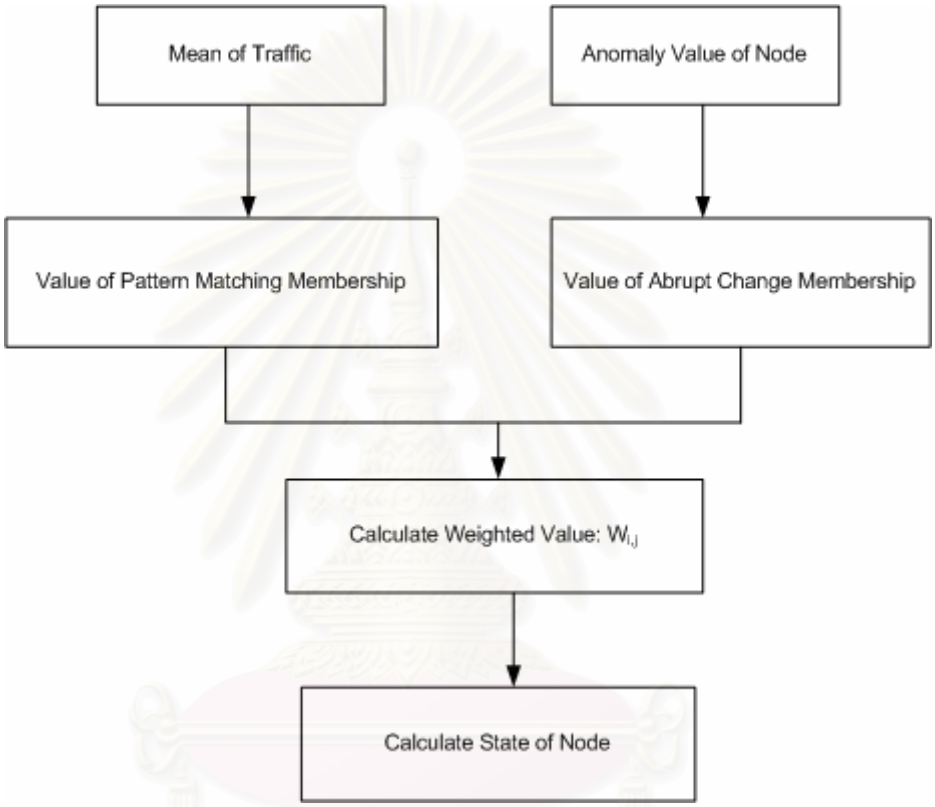
ตารางที 5.4 การเปลี่ยนสถานะของโนดเมื่อมีการใช้ข้อมูลแสดงสถานะความผิดปกติของวิธีตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก และ เปลี่ยนแปลงทันทีทันใดในกรณีที่เชื่อว่าจะเกิดความผิดปกติขึ้นถ้าสถานะความผิดปกติของวิธีของการเปรียบเทียบรูปแบบทราฟฟิกและเปลี่ยนแปลงทันทีทันใดมีสถานะผิดปกติ

โดยที่ $w_{i,j}$ คือ ค่าถ่วงน้ำหนักของ สถานะที่ i ของวิธีตรวจจับความผิดปกติแบบเปลี่ยนแปลงทันทีทันใดและ สถานะที่ j ของวิธีเปรียบเทียบรูปแบบทราฟฟิก และผลของสถานะของโนดในระบบโครงข่ายหาได้จากสมการที่ (5.1) และ (5.2) ตามลำดับ

$$w_{i,j} = \min\{F_{state}(Abruptchange), F_{state}(Patternmatch)\} \quad (5.1)$$

$$State\_of\_node = \frac{\sum w_{i,j} * state}{\sum w_{i,j}} \quad (5.2)$$

หลักการในการดำเนินงานของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกร่วมกับการเปลี่ยนแปลงทันทีทันใดโดยกรรมวิธีการของฟัซซีในการตัดสินใจแสดงดังรูปที่ 5.10



รูปที่ 5.10 การดำเนินงานของการตรวจจับความผิดปกติโดยใช้ฟัซซี

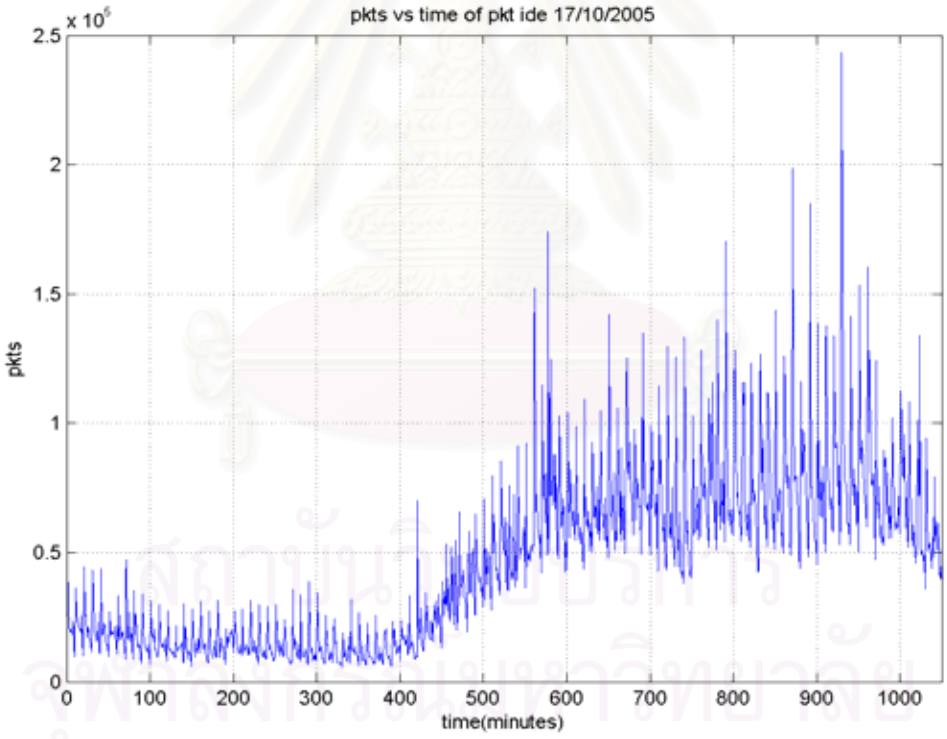
จากรูป 5.10 จะเห็นว่าขั้นตอนการดำเนินงานของวิธีฟัซซีเริ่มจาก วิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกคำนวณหาค่าเฉลี่ยของทราฟฟิก เช่นเดียวกับวิธีการตรวจจับความผิดปกติแบบทันทีทันใดคำนวณหาค่าความผิดปกติของโนด หลังจากนั้นนำค่าทั้งสองไปหาฟังก์ชันการเป็นสมาชิกของแต่ละวิธีจากรูปที่ 5.2-5.9 เมื่อคำนวณหาค่าฟังก์ชันการเป็นสมาชิกแล้ว ทำการคำนวณหาค่าถ่วงน้ำหนักของสถานะที่ i ของวิธีตรวจจับความผิดปกติแบบเปลี่ยนแปลงทันทีทันใดและ สถานะที่ j ของวิธีเปรียบเทียบรูปแบบทราฟฟิก ตามสมการที่ (5.1) หลังจากนั้นจะทำการคำนวณสถานะของโดยสมการที่ (5.2) โดยถ้าค่าสถานะของโนดมีค่าใกล้เคียง 0 (สถานะปกติ) มากกว่า 1 (สถานะผิดปกติ) แสดงว่าในขณะนั้นโนดที่ถูกตรวจจับความผิดปกติอยู่ในสถานะปกติ ในทางตรงกันข้าม โนดจะอยู่ในสถานะผิดปกติ

5.2 ดัชนีชี้วัดที่ใช้ในการประเมินประสิทธิภาพของวิธีตรวจจับความผิดปกติของระบบโครงข่าย

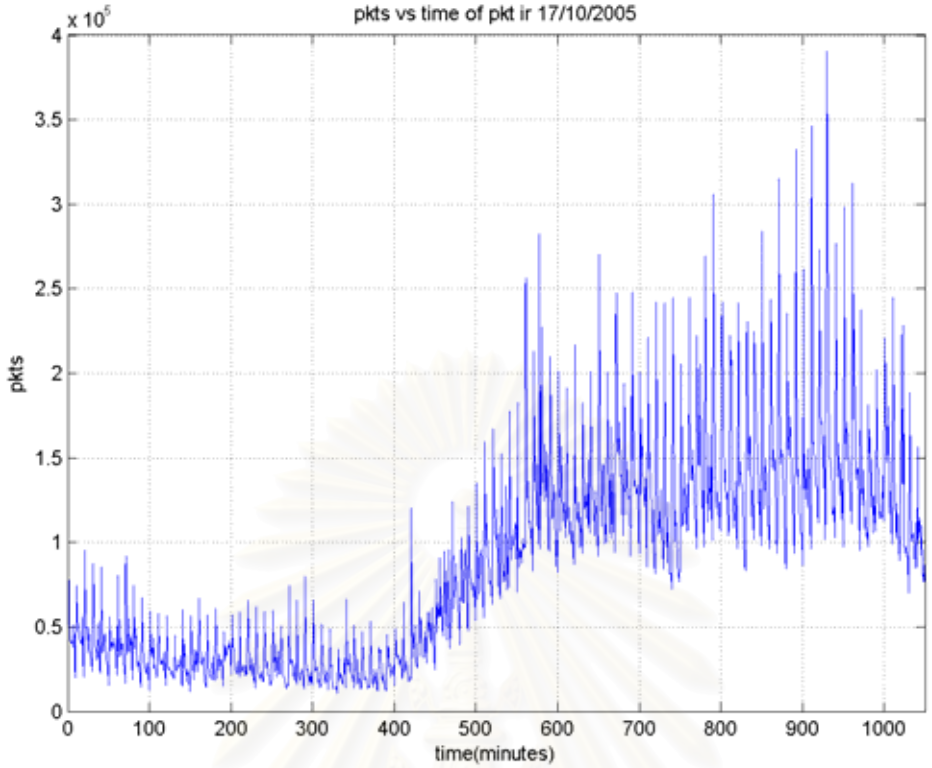
ดัชนีชี้วัดในการประเมินประสิทธิภาพของวิธีตรวจจับความผิดปกติของระบบโครงข่ายในบทนี้จะใช้ดัชนีชี้วัดเหมือนกับดัชนีชี้วัดในบทที่ 4 (หน้าที่ 47-48)

5.3 ผลการทดลองและสรุปผลการทดลอง

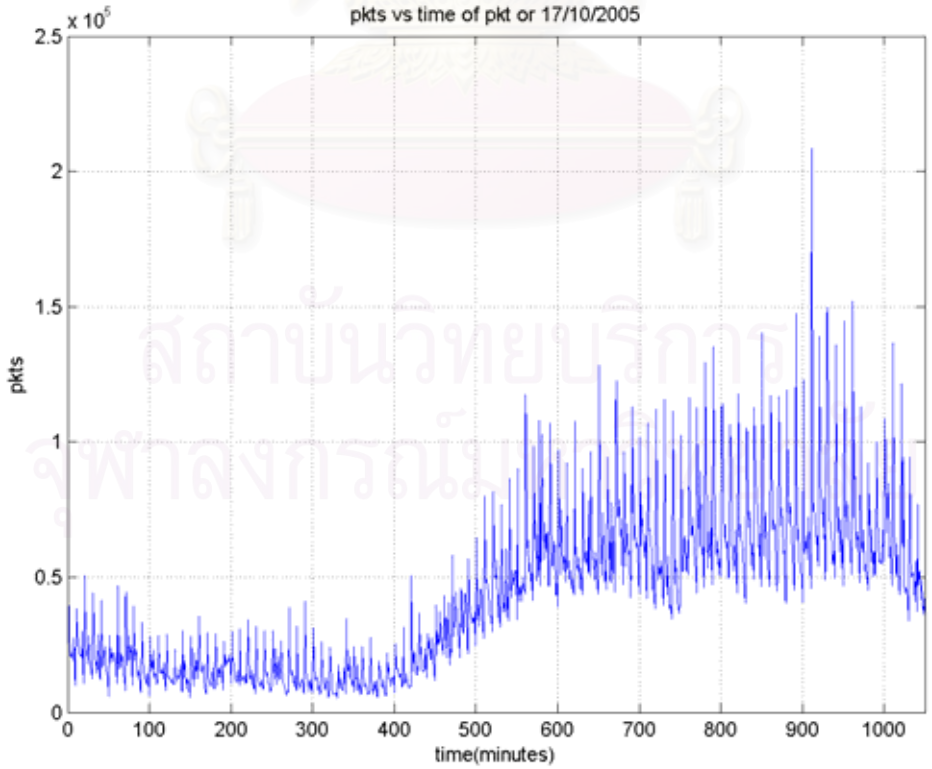
โดยการทดลองนี้เราจะใช้ข้อมูลทราฟฟิกจากโครงข่ายของจุฬาลงกรณ์มหาวิทยาลัย จำนวนทั้งสิ้น 6 วัน ในการตรวจจับความผิดปกติของระบบโครงข่าย ซึ่งประกอบไปด้วย วันที่ 17, 18, 19, 20, 21 และ 24 ของเดือนตุลาคม พ.ศ.2548 ซึ่งแสดงดังรูปที่ 5.11-5.28



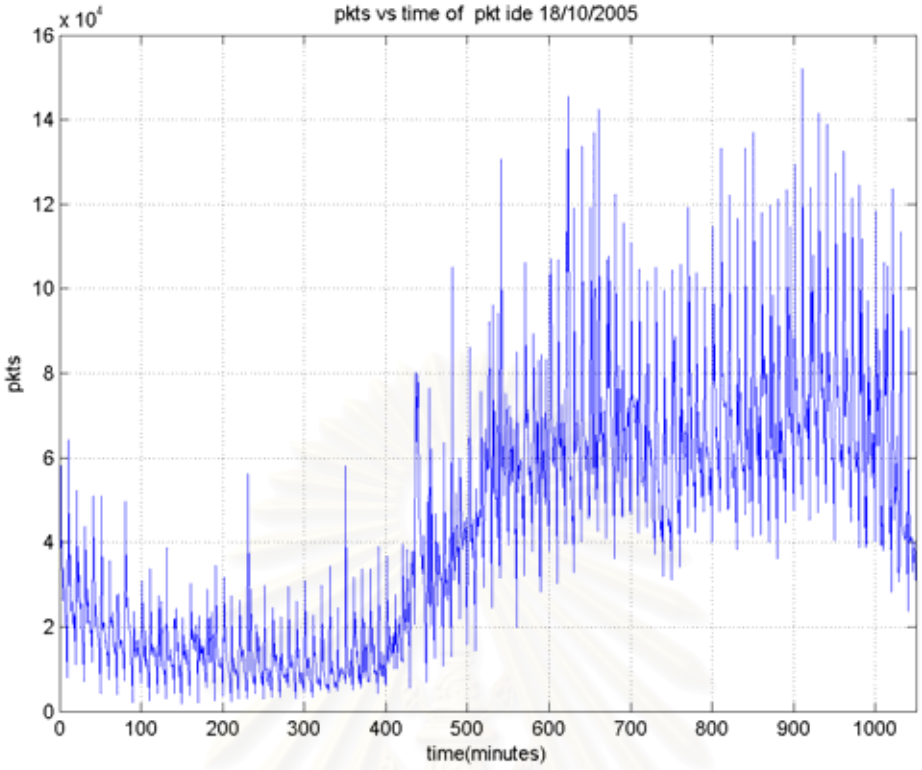
รูปที่ 5.11 ข้อมูล *ipIDE* ของรูทเทอร์ 7513 ในวันที่ 17/10/2005



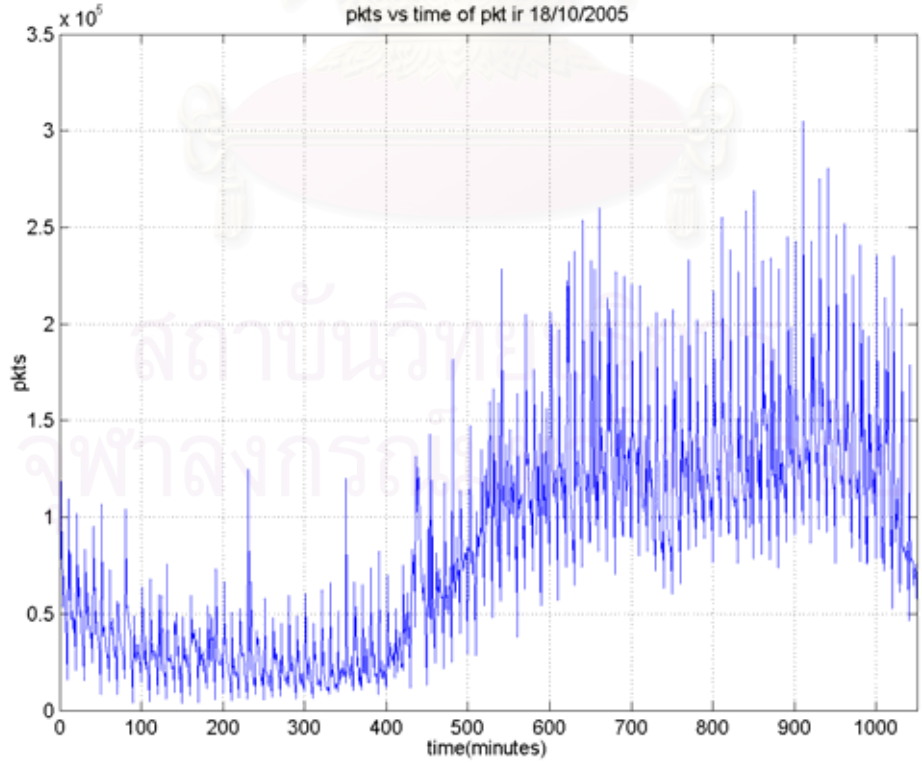
รูปที่ 5.12 ข้อมูล *ipIR* ของรูทเทอร์ 7513 ในวันที่ 17/10/2005



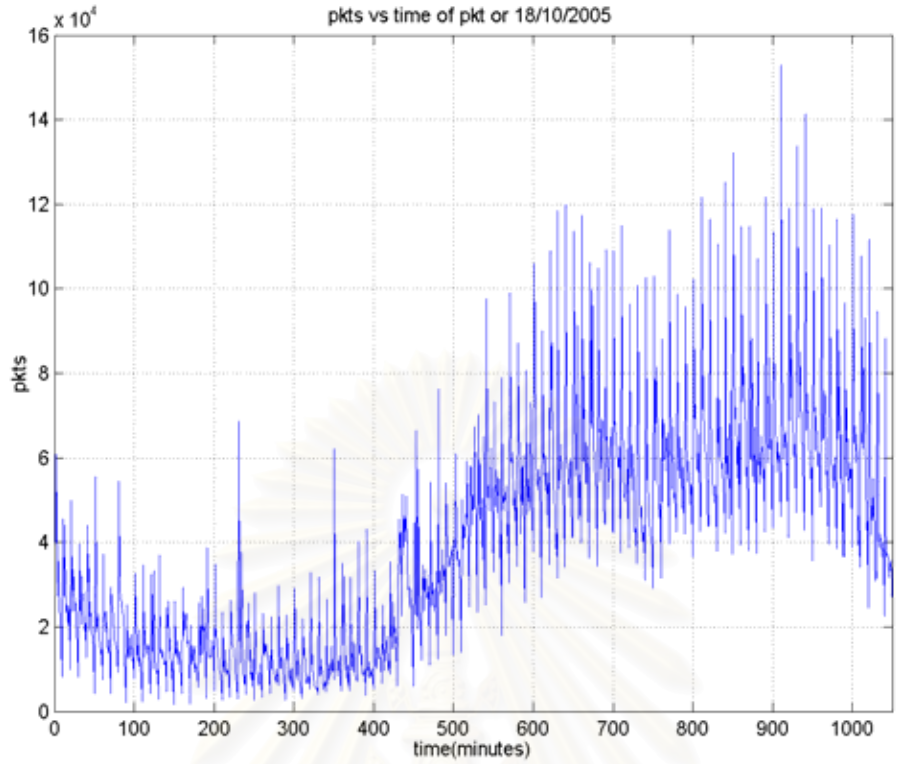
รูปที่ 5.13 ข้อมูล *ipOR* ของรูทเทอร์ 7513 ในวันที่ 17/10/2005



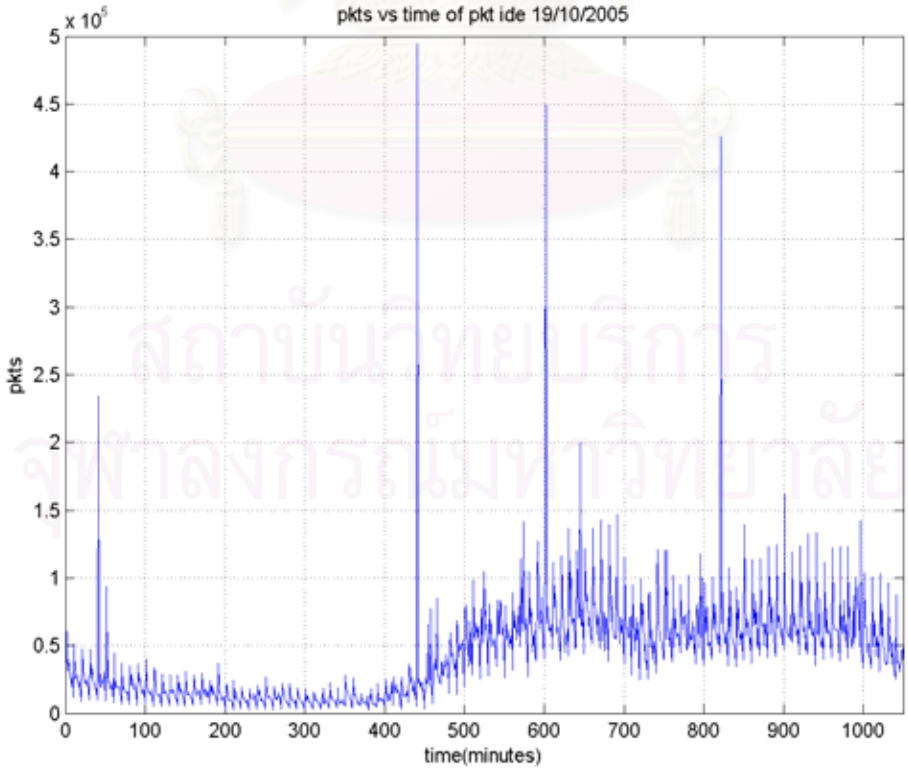
รูปที่ 5.14 ข้อมูล *ipIDE* ของรูทเทอร์ 7513 ในวันที่ 18/10/2005



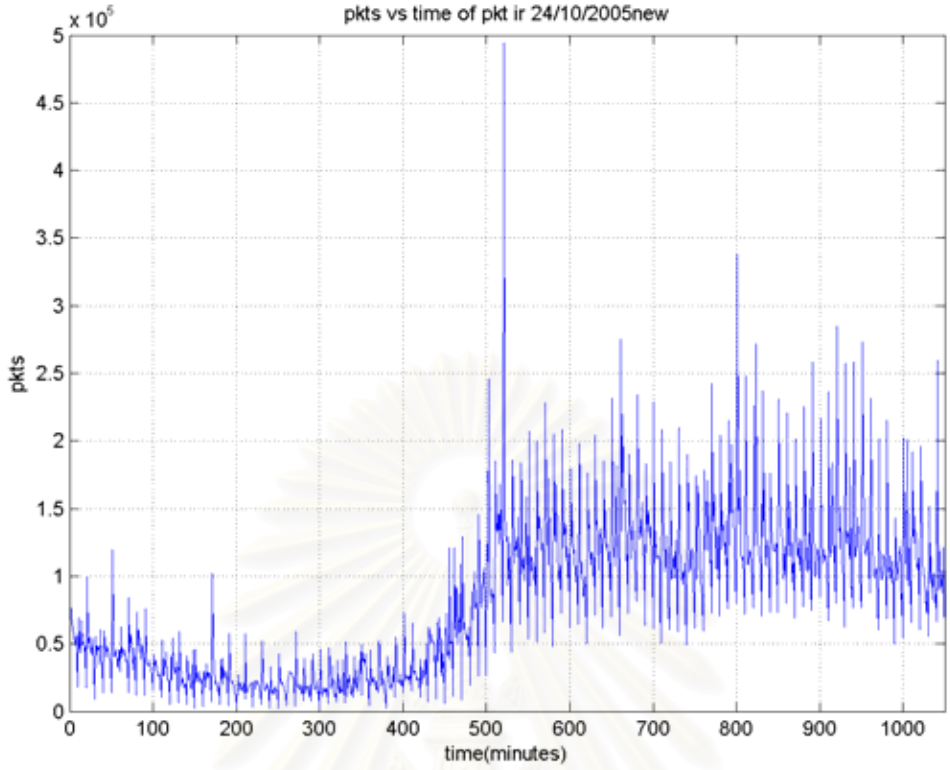
รูปที่ 5.15 ข้อมูล *ipIR* ของรูทเทอร์ 7513 ในวันที่ 18/10/2005



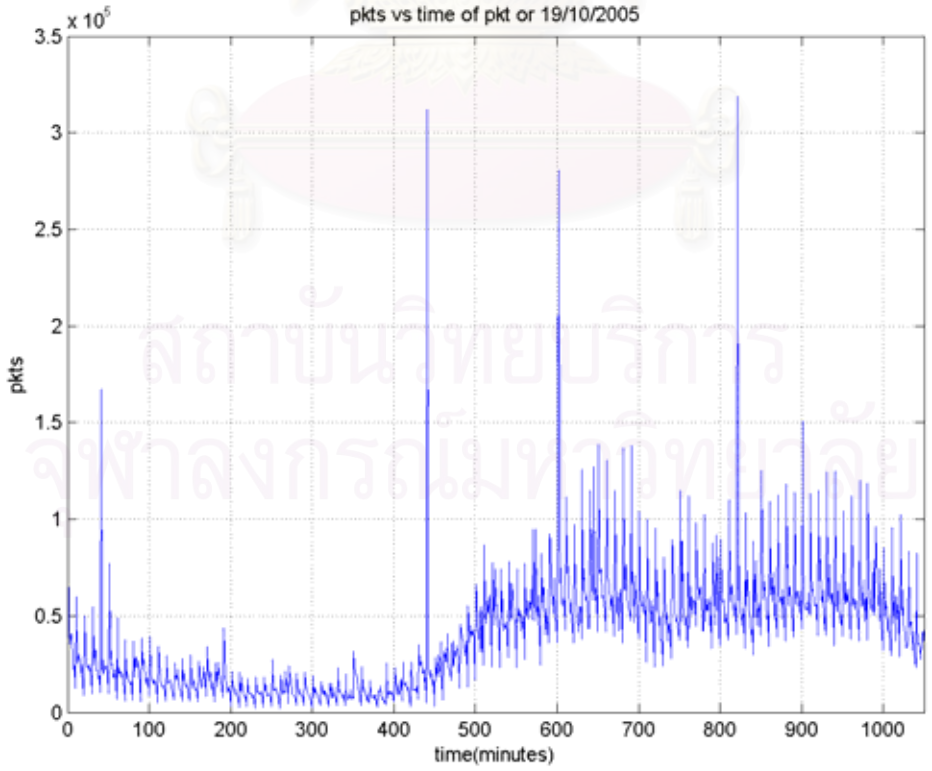
รูปที่ 5.16 ข้อมูล *ipOR* ของรูทเทอร์ 7513 ในวันที่ 18/10/2005



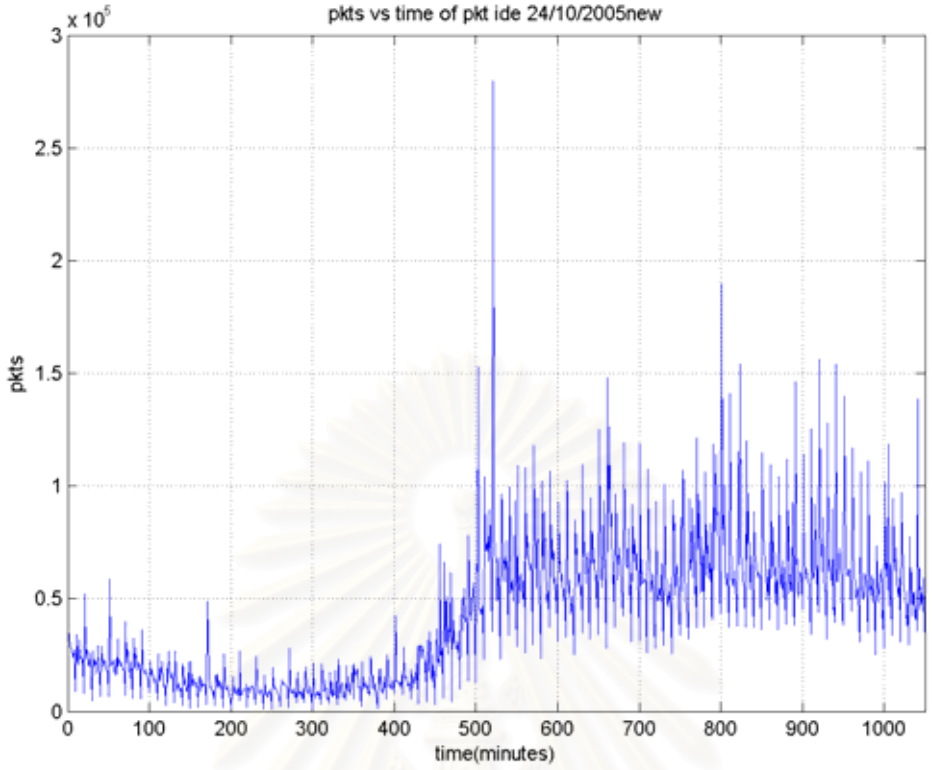
รูปที่ 5.17 ข้อมูล *ipIDE* ของรูทเทอร์ 7513 ในวันที่ 19/10/2005



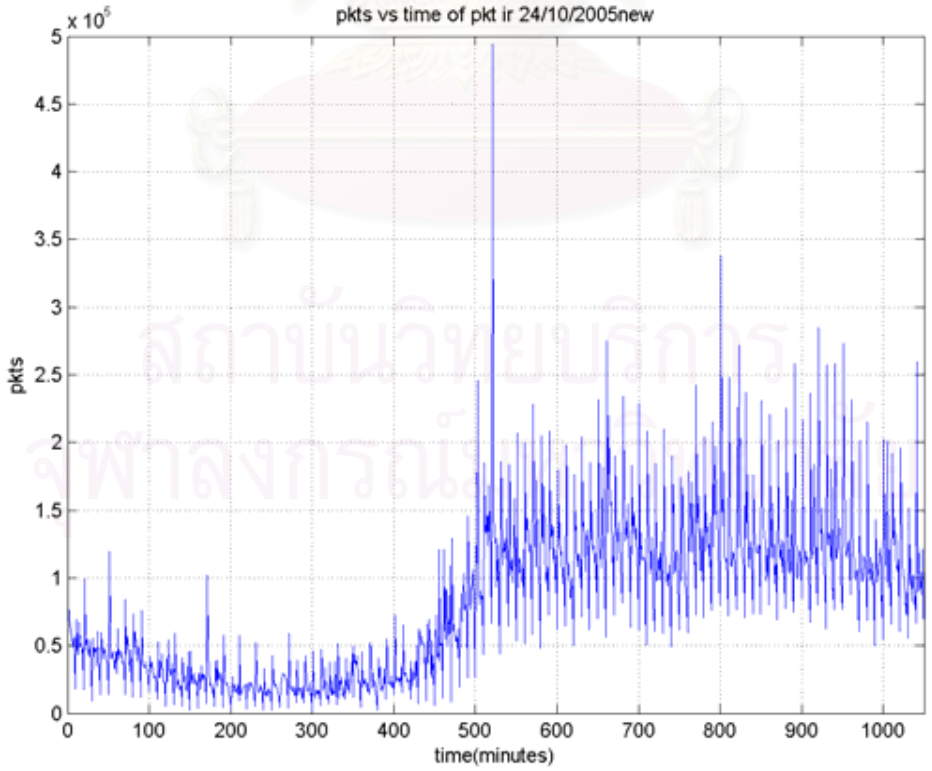
รูปที่ 5.18 ข้อมูล *ipIR* ของรูทเทอร์ 7513 ในวันที่ 19/10/2005



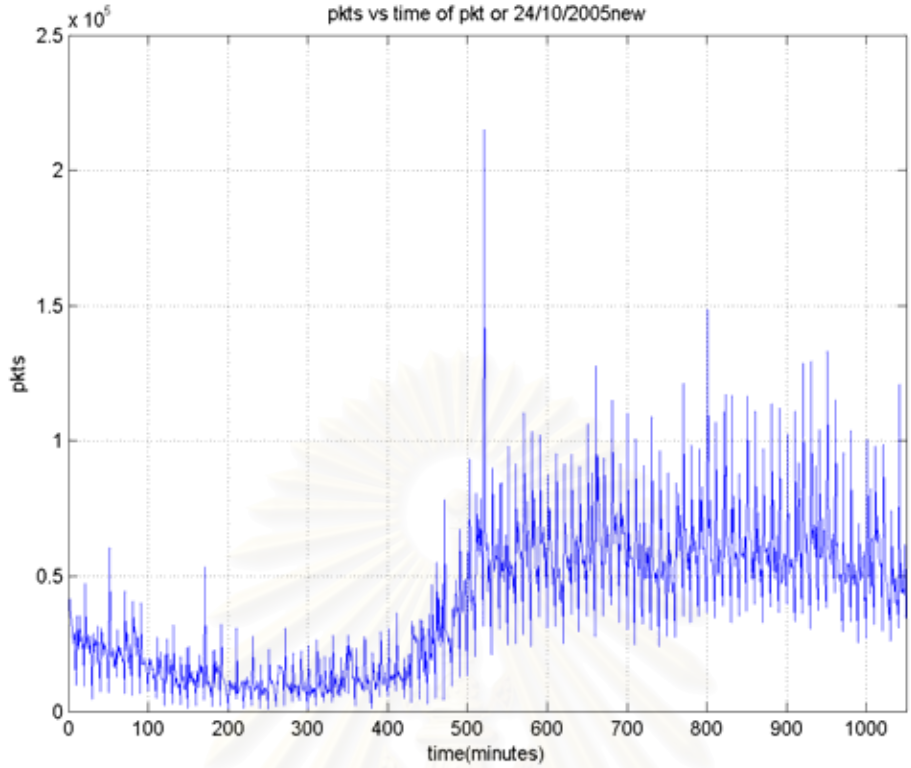
รูปที่ 5.19 ข้อมูล *ipOR* ของรูทเทอร์ 7513 ในวันที่ 19/10/2005



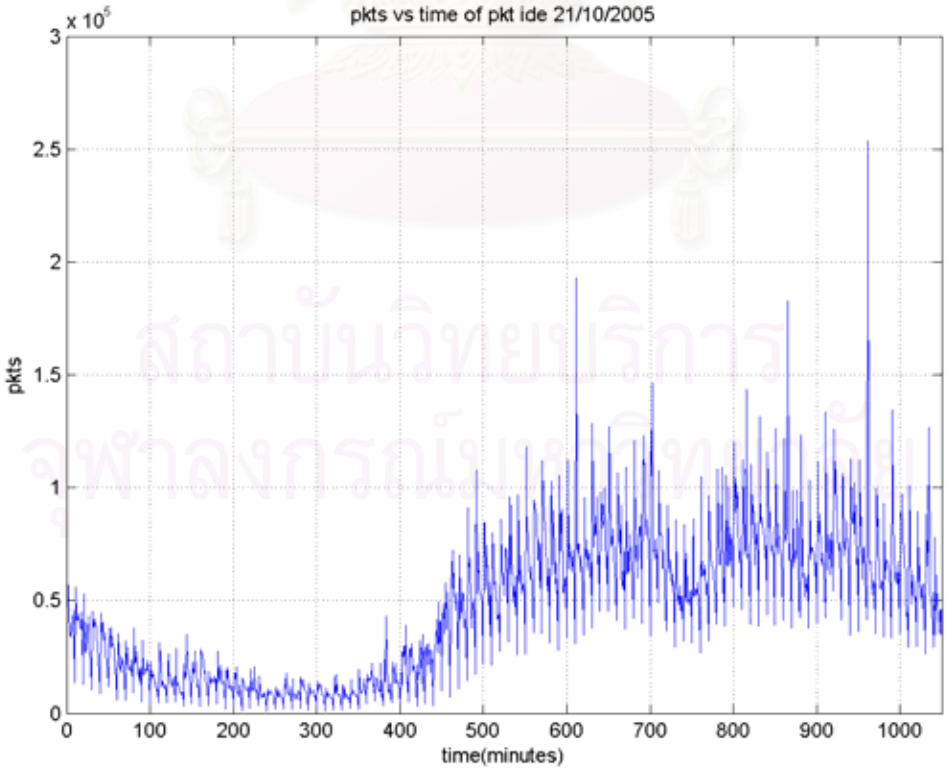
รูปที่ 5.20 ข้อมูล *ipIDE* ของรูทเทอร์ 7513 ในวันที่ 20/10/2005



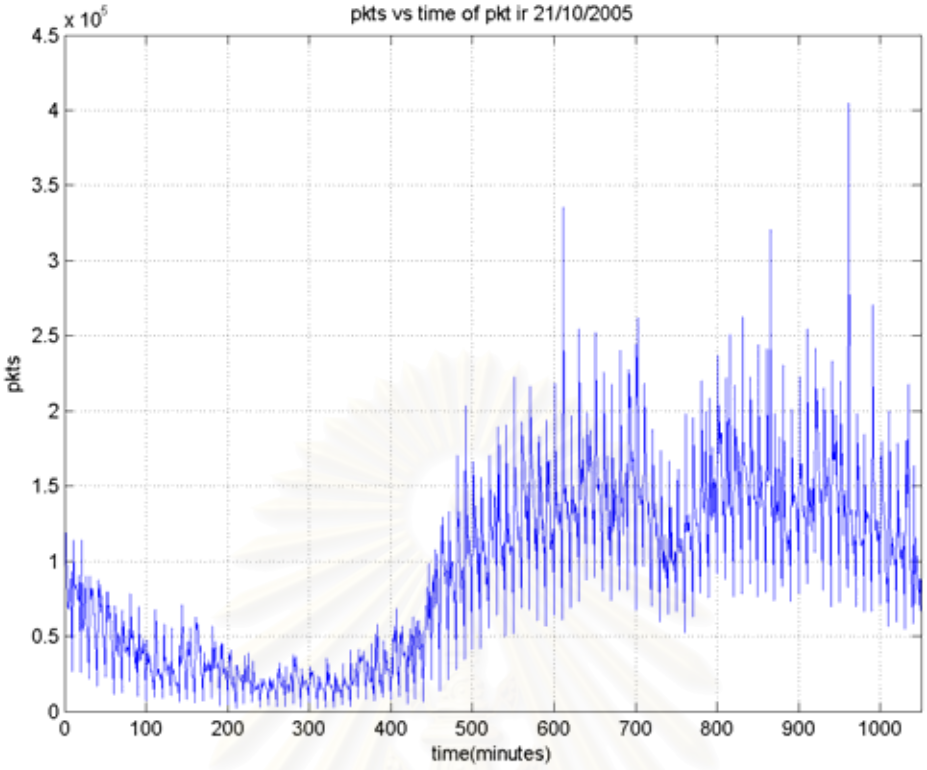
รูปที่ 5.21 ข้อมูล *ipIR* ของรูทเทอร์ 7513 ในวันที่ 20/10/2005



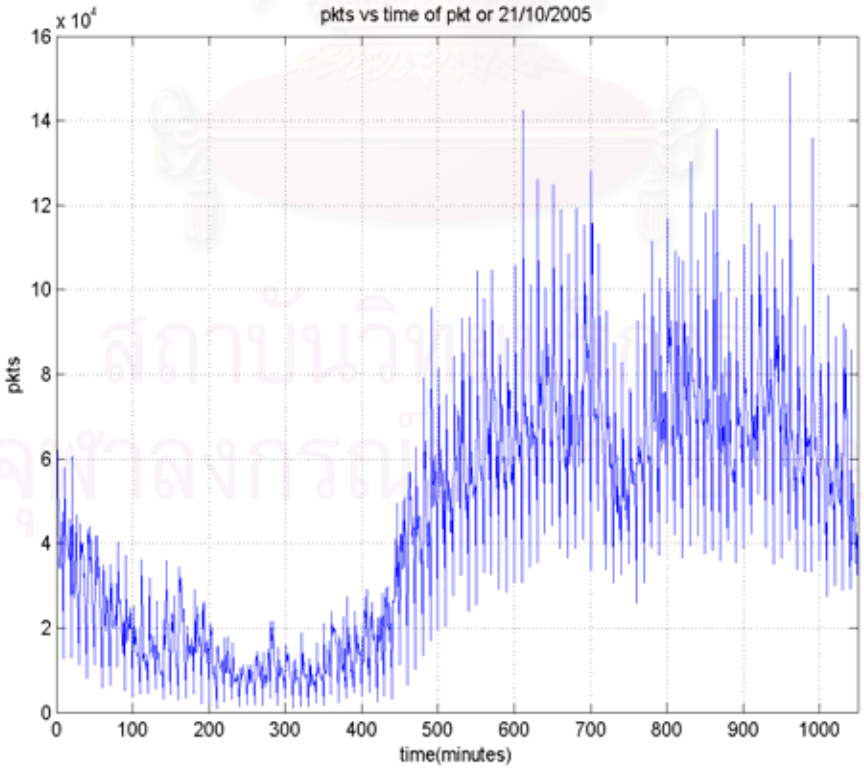
รูปที่ 5.22 ข้อมูล *ipOR* ของรูทเทอร์ 7513 ในวันที่ 20/10/2005



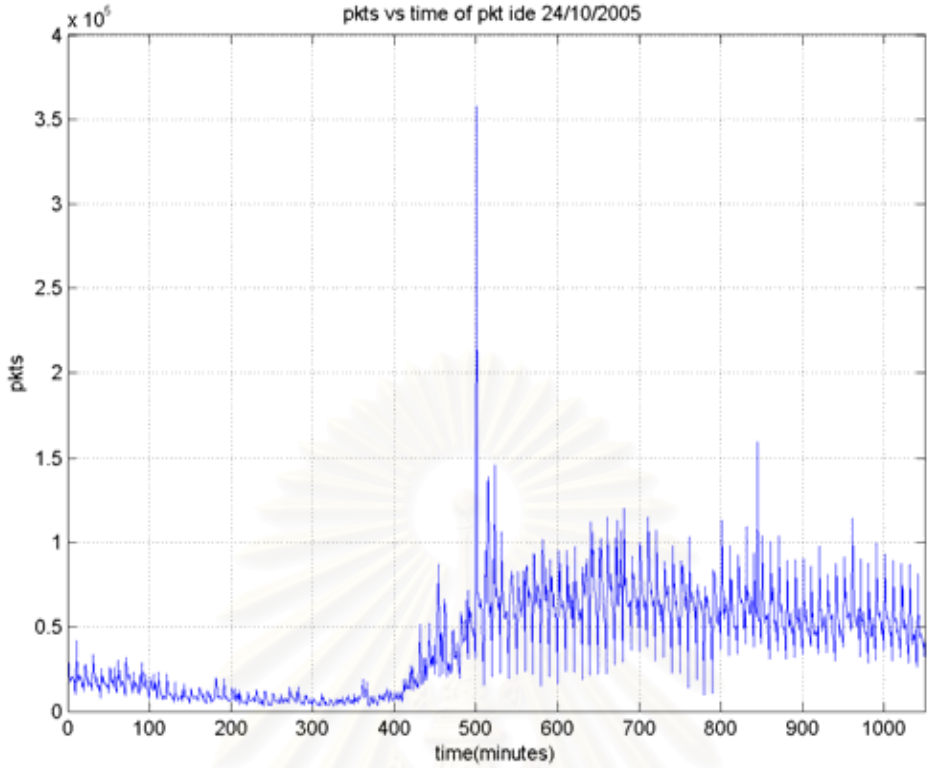
รูปที่ 5.23 ข้อมูล *ipIDE* ของรูทเทอร์ 7513 ในวันที่ 21/10/2005



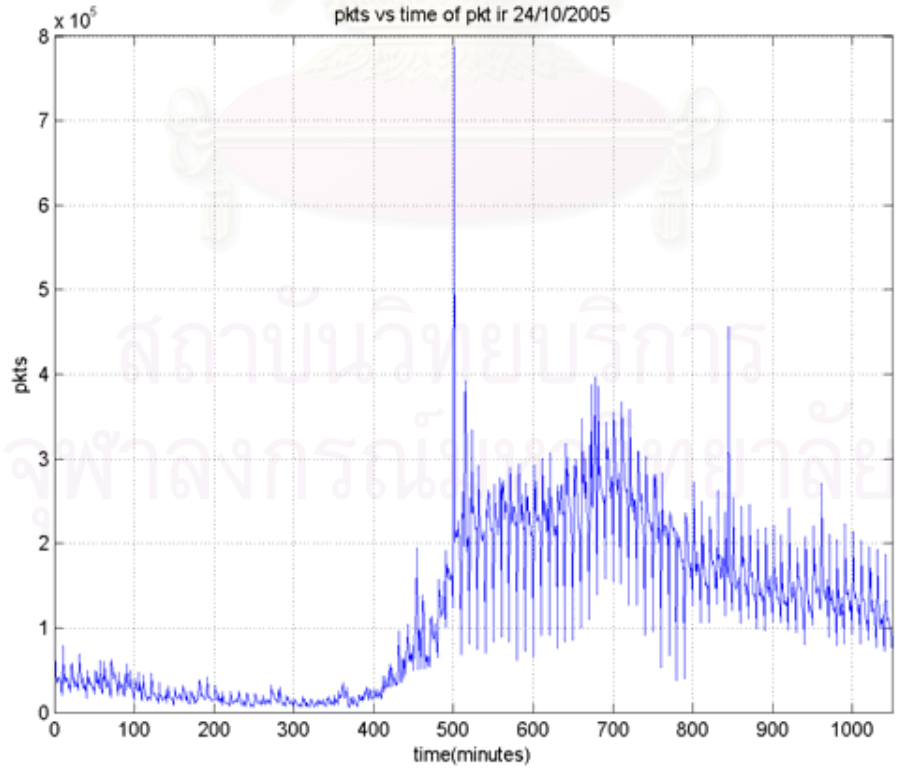
รูปที่ 5.24 ข้อมูล *ipIR* ของรูทเทอร์ 7513 ในวันที่ 21/10/2005



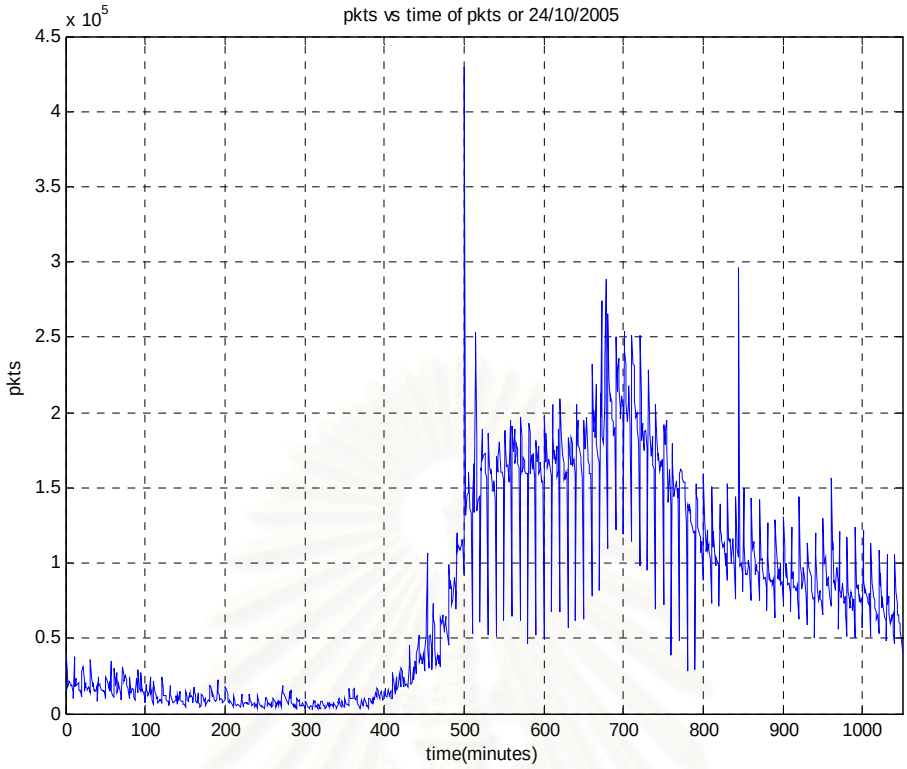
รูปที่ 5.25 ข้อมูล *ipOR* ของรูทเทอร์ 7513 ในวันที่ 21/10/2005



รูปที่ 5.26 ข้อมูล *ipIDE* ของรูทเทอร์ 7513 ในวันที่ 24/10/2005



รูปที่ 5.27 ข้อมูล *ipIR* ของรูทเทอร์ 7513 ในวันที่ 24/10/2005



รูปที่ 5.28 ข้อมูล *ipOR* ของรูทเทอร์ 7513 ในวันที่ 24/10/2005

ในการทดลองเพื่อทดสอบประสิทธิภาพในการตรวจจับความผิดปกติของวิธีการฟัซซี เราจะทำการตรวจจับความผิดปกติของระบบโครงข่ายของจุฬาลงกรณ์มหาวิทยาลัยที่วันที่ 24 ตุลาคม 2548 และใช้ข้อมูลของวันที่ 17-24 ตุลาคม 2548 สำหรับเป็นฐานข้อมูลในอดีตในการใช้วิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก เราได้แบ่งการทดลองออกเป็น 1 ส่วน คือ กำหนดให้จำนวนรอบที่ใช้ในการหาค่าเมตริกซ์ A มีค่าคงที่เท่ากับ 14 รอบ แต่ปรับเปลี่ยนค่าความกว้างของหน้าต่างในการตรวจจับความผิดปกติของระบบโครงข่าย

เนื่องจากข้อมูลทราฟฟิกที่บันทึกได้จากโปรแกรม *NETFLOW* ที่ได้จากโครงข่ายจุฬาลงกรณ์มหาวิทยาลัยนั้น ไม่ได้มีการบันทึกว่าในช่วงเวลาที่ผ่านมาเกิดความผิดปกติขึ้นเมื่อใด ด้วยสาเหตุใด เป็นเวลานานเท่าใด ดังนั้นจากรูปที่ 5.22-5.24 ของทราฟฟิกวันที่ 24 ตุลาคม 2548 เราจึงได้กำหนดให้มีความผิดปกติเกิดขึ้นที่ระบบโครงข่ายที่เวลา 500 นาที ด้วยเหตุผลที่ว่าที่เวลานี้จำนวนแพ็กเก็ตมีความเปลี่ยนแปลงอย่างมากเมื่อเทียบกับช่วงเวลาที่ติดกัน

ในการทดลองนั้นเราได้มีการกำหนดตัวแปรในการแสดงผลของแต่ละวิธีในการตรวจจับความผิดปกติของระบบโครงข่ายดังนี้

patternmatching หมายถึง การตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก

abruptchange หมายถึง การตรวจจับความผิดปกติแบบทันทีทันใด

abruptsquarenew1 หมายถึง การตรวจจับความผิดปกติโดยใช้ฟัซซี โดยเชื่อในวิธีของการตรวจจับความผิดปกติแบบทันทีทันใด โดยใช้รูปร่างของฟังก์ชันการเป็นสมาชิกแบบสี่เหลี่ยมคางหมู และ ใช้การหาค่าถ่วงน้ำหนักแบบใหม่ของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก

abruptsquareold1 หมายถึง การตรวจจับความผิดปกติโดยใช้ฟัซซี โดยเชื่อในวิธีของการตรวจจับความผิดปกติแบบทันทีทันใด โดยใช้รูปร่างของฟังก์ชันการเป็นสมาชิกแบบสี่เหลี่ยมคางหมู และ ใช้การหาค่าถ่วงน้ำหนักแบบเดิมของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก

abrupttrianglenew1 หมายถึง การตรวจจับความผิดปกติโดยใช้ฟัซซี โดยเชื่อในวิธีของการตรวจจับความผิดปกติแบบทันทีทันใด โดยใช้รูปร่างของฟังก์ชันการเป็นสมาชิกแบบสามเหลี่ยม และ ใช้การหาค่าถ่วงน้ำหนักแบบใหม่ของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก

abrupttriangleold1 หมายถึง การตรวจจับความผิดปกติโดยใช้ฟัซซี โดยเชื่อในวิธีของการตรวจจับความผิดปกติแบบทันทีทันใด โดยใช้รูปร่างของฟังก์ชันการเป็นสมาชิกแบบสามเหลี่ยม และ ใช้การหาค่าถ่วงน้ำหนักแบบเดิมของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก

bothsquarenew1 หมายถึง การตรวจจับความผิดปกติโดยใช้ฟัซซี โดยเชื่อในวิธีของการตรวจจับความผิดปกติแบบทันทีทันใด และแบบเปรียบเทียบรูปแบบทราฟฟิก โดยใช้รูปร่างของฟังก์ชันการเป็นสมาชิกแบบสี่เหลี่ยมคางหมูและ ใช้การหาค่าถ่วงน้ำหนักแบบใหม่ของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก

bothsquareold1 หมายถึง การตรวจจับความผิดปกติโดยใช้ฟัซซี โดยเชื่อในวิธีของการตรวจจับความผิดปกติแบบทันทีทันใด และแบบเปรียบเทียบรูปแบบทราฟฟิก โดยใช้รูปร่างของฟังก์ชันการเป็นสมาชิกแบบสี่เหลี่ยมคางหมู และ ใช้การหาค่าถ่วงน้ำหนักแบบเดิมของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก

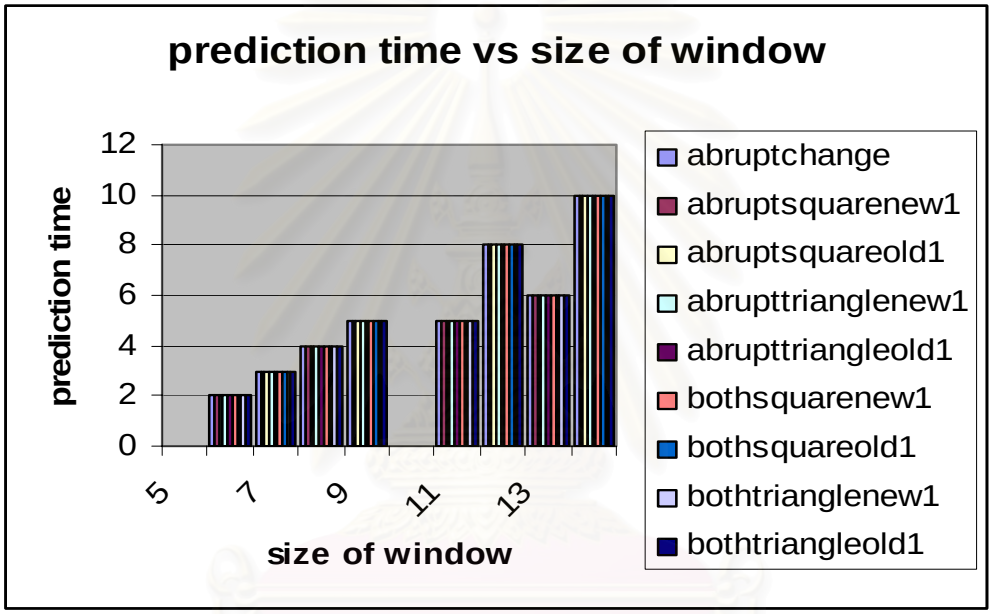
boththrianglenew1 หมายถึง การตรวจจับความผิดปกติโดยใช้ฟัซซี โดยเชื่อในวิธีของการตรวจจับความผิดปกติแบบทันทีทันใด และแบบเปรียบเทียบรูปแบบทราฟฟิก โดยใช้รูปร่างของฟังก์ชันการเป็นสมาชิกแบบสามเหลี่ยม และ ใช้การหาค่าถ่วงน้ำหนักแบบใหม่ของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก

boththriangleold1 หมายถึง การตรวจจับความผิดปกติโดยใช้ฟัซซี โดยเชื่อในวิธีของการตรวจจับความผิดปกติแบบทันทีทันใด และแบบเปรียบเทียบรูปแบบทราฟฟิก โดยใช้รูปร่างของ

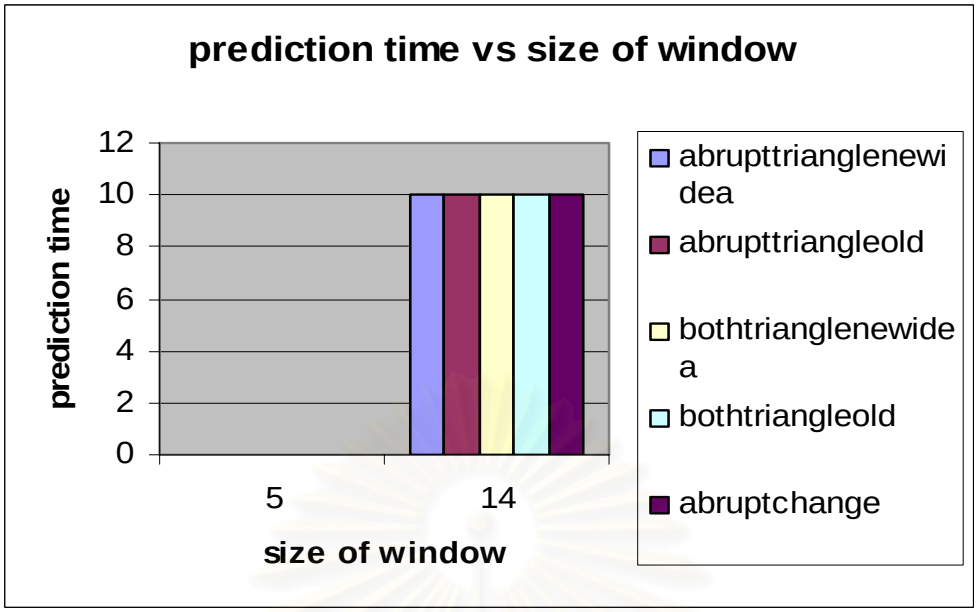
ฟังก์ชันการเป็นสมาชิกแบบสามเหลี่ยม และ ใช้การหาค่าถ่วงน้ำหนักแบบเดิมของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก

5.3.1 จำนวนรอบที่ใช้ในการหาค่าเมตริกซ์ A มีค่าคงที่ 14 รอบ แต่ปรับเปลี่ยนค่าความกว้างของหน้าต่างในการตรวจจับความผิดปกติของระบบโครงข่าย

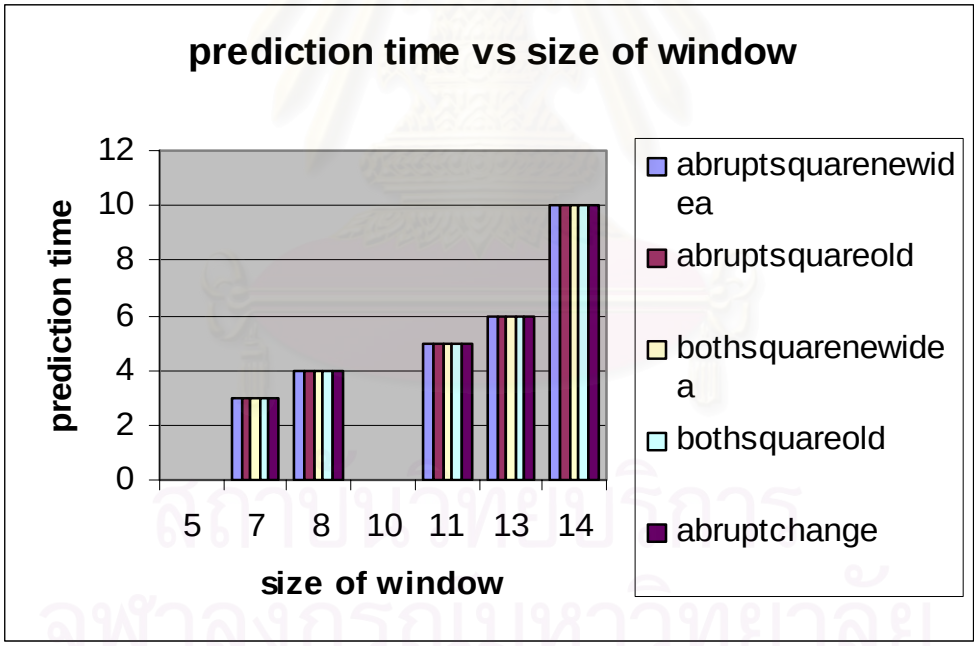
ในการทดลองเพื่อทดสอบประสิทธิภาพของวิธีการตรวจจับความผิดปกติโดยใช้ฟัซซีได้ผลการทดลองดังรูปที่ 5.29-5.31



รูปที่ 5.29 ความสัมพันธ์ระหว่างเวลาที่สามารถตรวจจับความผิดปกติในระบบโครงข่ายก่อนเกิดความเสียหายและขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติในระบบโครงข่าย แบบ *A*



รูปที่ 5.30 ความสัมพันธ์ระหว่างเวลาที่สามารถตรวจจับความผิดปกติในระบบโครงข่ายก่อนเกิดความเสียหายและขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติในระบบโครงข่าย ของฟังก์ชันการเป็นสมาชิกแบบ *B*



รูปที่ 5.31 ความสัมพันธ์ระหว่างเวลาที่สามารถตรวจจับความผิดปกติในระบบโครงข่ายก่อนเกิดความเสียหายและขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติในระบบโครงข่าย ของฟังก์ชันการเป็นสมาชิกแบบ *B*

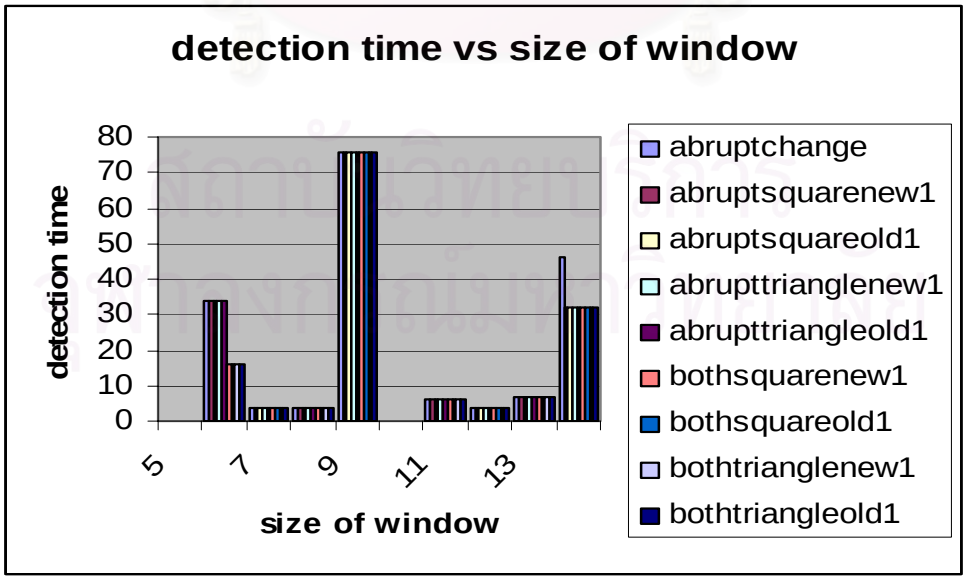
จากผลการทดลองดังรูปที่ 5.29-5.31 จะเห็นได้ว่าขนาดหน้าต่างในการตรวจจับความผิดปกติของระบบโครงข่ายที่แตกต่างกันจะให้ผลของเวลาที่สามารถตรวจจับความผิดปกติใน

ระบบโครงข่ายก่อนเกิดความเสียหายที่แตกต่างกัน จะเห็นได้ว่าเวลาที่สามารถตรวจจับความผิดปกติของระบบโครงข่ายก่อนเกิดความเสียหายมีค่าเท่ากันทุกวิธีเนื่องจาก ลักษณะทราฟฟิกที่เวลาใกล้ช่วงเวลาที่เกิดความผิดปกติให้ค่าความผิดปกติของโนด ของวิธีการตรวจจับความผิดปกติแบบเปลี่ยนแปลงทันทีทันใด ที่มีค่าสูงมาก เกินค่าเกณฑ์ และค่าเฉลี่ยทราฟฟิกจริงที่วัดได้เกินค่าที่ทำนายได้ของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกดังนั้นทำให้เกินสัญญาณเตือนเกิดขึ้น

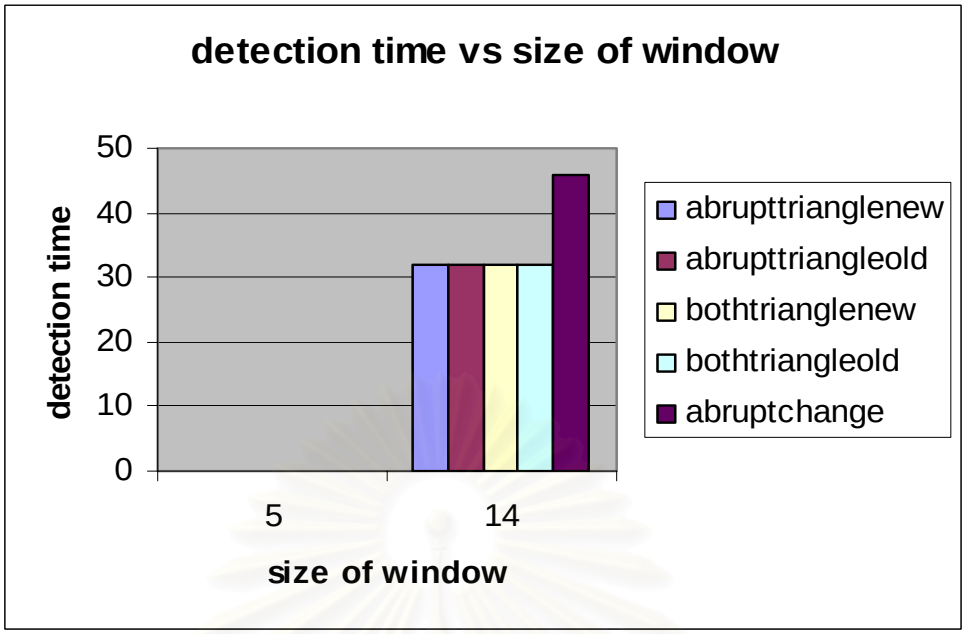
win	$T_p(ipIDE)$
5	230
6	336
7	199

ตารางที่ 5.5 เวลาที่สามารถตรวจจับความผิดปกติก่อนระบบโครงข่ายเกิดความเสียหาย ของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก

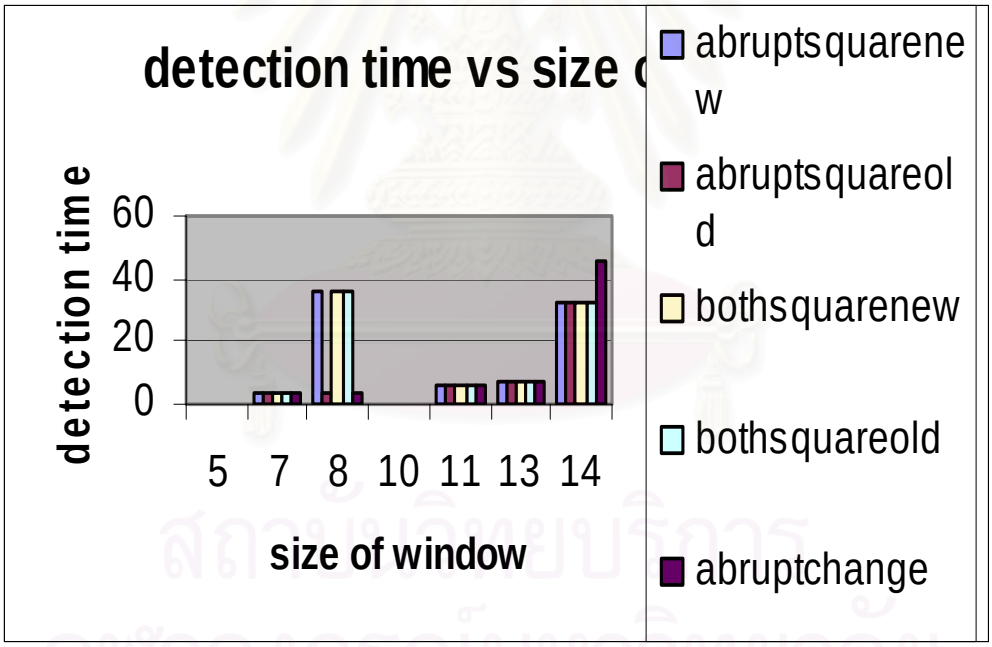
จากผลการทดลองดังตารางที่ 5.5 จะเห็นได้ว่าวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกไม่สามารถตรวจจับความผิดปกติก่อนเกิดความเสียหายได้ในบางขนาดหน้าต่าง และที่ขนาดหน้าต่างที่สามารถตรวจจับความผิดปกติก่อนเกิดความเสียหายได้นั้นค่าเวลาที่สารถตรวจจับความผิดปกติก่อนเกิดความเสียหายมีค่าสูงมาก เมื่อเปรียบเทียบกับวิธีการตรวจจับความผิดปกติแบบทันทีทันใด และวิธีฟัซซี ดังนั้นวิธีการเปรียบเทียบรูปแบบทราฟฟิกจึงให้ไปประสิทธิภาพที่แย่กว่าวิธีการตรวจจับความผิดปกติแบบทันทีทันใด และวิธีฟัซซี



รูปที่ 5.32 ความสัมพันธ์ระหว่างเวลาที่สามารถตรวจจับความผิดปกติในระบบโครงข่ายหลังเกิดความเสียหายและขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติในระบบโครงข่าย แบบ *A*



รูปที่ 5.33 ความสัมพันธ์ระหว่างเวลาที่สามารถตรวจจับความผิดปกติในระบบโครงข่ายหลังเกิดความเสียหายและขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติในระบบโครงข่าย แบบ *B*



รูปที่ 5.34 ความสัมพันธ์ระหว่างเวลาที่สามารถตรวจจับความผิดปกติในระบบโครงข่ายหลังเกิดความเสียหายและขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติในระบบโครงข่าย แบบ *B*

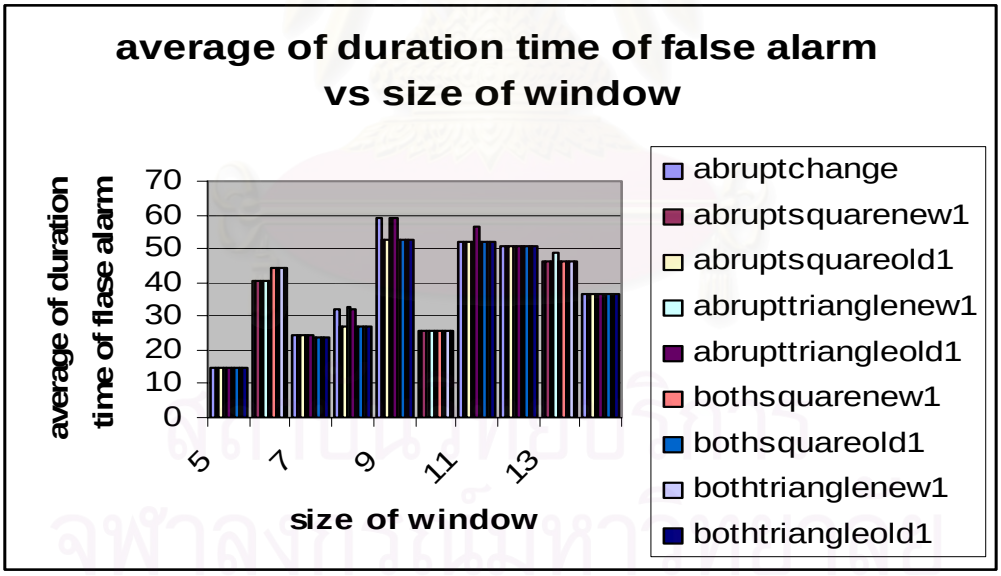
จากผลการทดลองดังรูปที่ 5.32-5.34 จะเห็นได้ว่าขนาดของหน้าต่างในการตรวจจับความผิดปกติของระบบโครงข่ายที่แตกต่างกันจะให้ผลของเวลาที่สามารถตรวจจับความผิดปกติหลังเกิดความเสียหายที่แตกต่างกัน จะเห็นได้ว่าเวลาที่สามารถตรวจจับความผิดปกติของระบบโครงข่ายหลังเกิดความเสียหายมีค่าเท่ากันเกือบทุกขนาดหน้าต่างเนื่องจาก ลักษณะทราฟฟิกที่

เวลาใกล้ช่วงเวลาที่เกิดความผิดปกติให้ค่าความผิดปกติของโนด ของวิธีการตรวจจับความผิดปกติแบบเปลี่ยนแปลงทันทีทันใด ที่มีค่าสูงมาก เกินค่าเกณฑ์ และค่าเฉลี่ยทราฟฟิกจริงที่วัดได้เกินค่าที่ทำนายได้ของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกดังนั้นทำให้เกินสัญญาณเตือนเกิดขึ้น

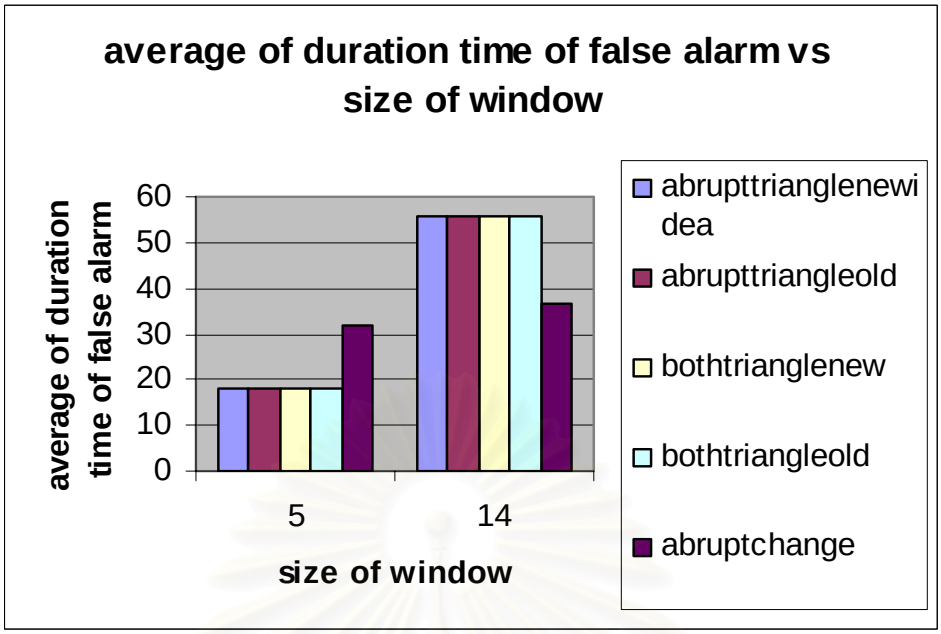
win	$T_d(ipIDE)$
5	5
6	16
7	18

ตารางที่ 5.6 เวลาที่สามารถตรวจจับความผิดปกติหลังระบบโครงข่ายเกิดความเสียหาย ของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก

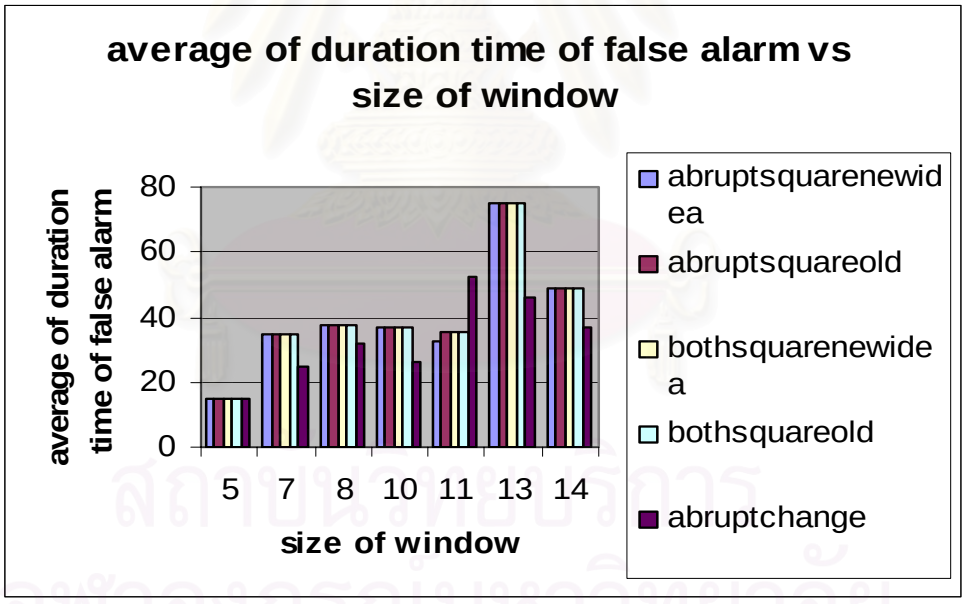
จากผลการทดลองดังตารางที่ 5.6 จะเห็นได้ว่าวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกไม่สามารถตรวจจับความผิดปกติหลังเกิดความเสียหายได้ในบางขนาดหน้าต่าง



รูปที่ 5.35 ความสัมพันธ์ระหว่างค่าเฉลี่ยของช่วงเวลาที่จะเกิดสัญญาณเตือนที่ผิดพลาดและขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติในระบบโครงข่าย แบบ *A*



รูปที่ 5.36 ความสัมพันธ์ระหว่างค่าเฉลี่ยของช่วงเวลาที่จะเกิดสัญญาณเตือนที่ผิดพลาดและขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติในระบบโครงข่าย แบบ *B*



รูปที่ 5.37 ความสัมพันธ์ระหว่างค่าเฉลี่ยของช่วงเวลาที่จะเกิดสัญญาณเตือนที่ผิดพลาดและขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติในระบบโครงข่าย แบบ *B*

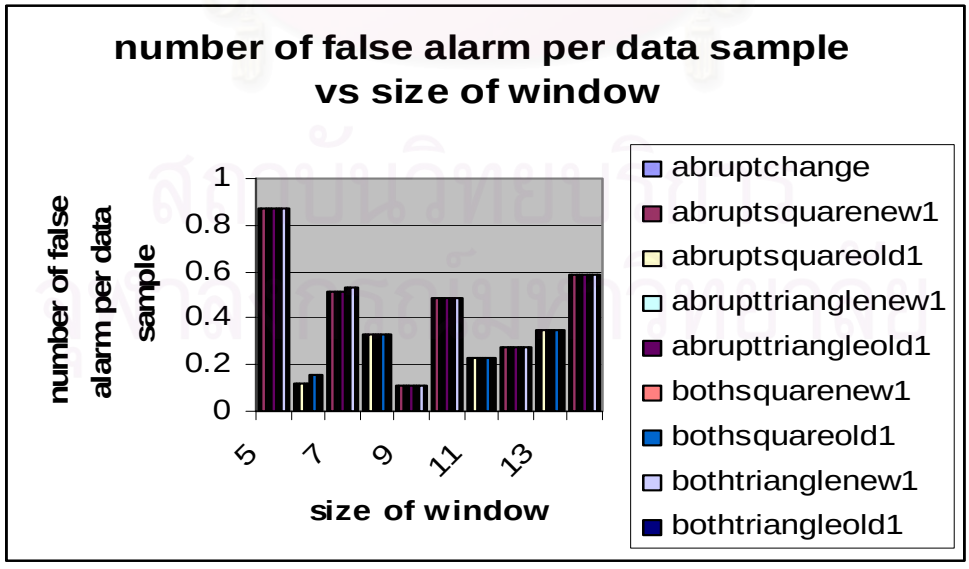
จากผลการทดลองดังรูปที่ 5.35-5.37 จะเห็นได้ว่าการใช้ขนาดหน้าต่างในการตรวจจับความผิดปกติของระบบโครงข่ายที่แตกต่างกันจะให้ผลของค่าเฉลี่ยของช่วงสัญญาณเตือนที่ผิดพลาดที่แตกต่างกัน และการใช้ฟังก์ชันการเป็นสมาชิกของ แบบ *A* และ แบบ *B* ให้ผลของค่าเฉลี่ยของช่วงเวลาที่จะเกิดสัญญาณเตือนที่ผิดพลาดที่แตกต่างกัน โดยที่แบบ *B* นั้นให้ผลของ

ค่าเฉลี่ยของช่วงเวลาที่จะเกิดสัญญาณเตือนที่ผิดพลาดที่สูงกว่าแบบ *A* เนื่องจากแบบ *A* มีฟังก์ชันการเป็นสมาชิกโน้มเอียงไปทางด้านความผิดปกติมากกว่าแบบ *B* ค่าค่าเฉลี่ยของช่วงเวลาที่จะเกิดสัญญาณเตือนที่ผิดพลาดของแบบ *B* มีค่าที่สูงกว่า วิธีการตรวจจับความผิดปกติแบบทันทีทันใดอย่างมาก ซึ่งแสดงถึงประสิทธิภาพที่ดีขึ้น แต่ข้อเสียคือในบางขนาดหน้าต่างนั้นแบบ *B* ไม่สารถตรวจจับความผิดปกติได้เลย

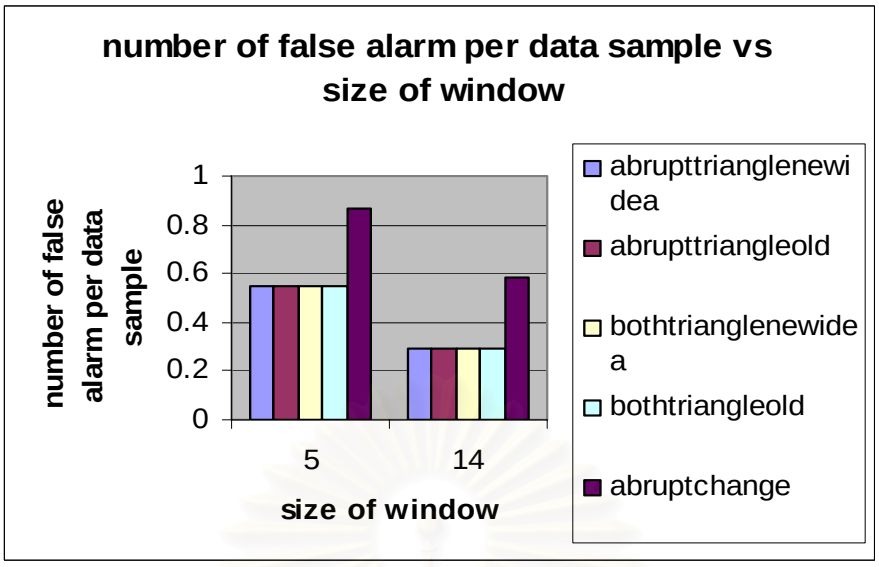
win	$T_f(ipIDE)$
5	-
6	120
7	140

ตารางที่ 5.7 ค่าเฉลี่ยของช่วงเวลาที่จะเกิดสัญญาณเตือนที่ผิดพลาด ของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก

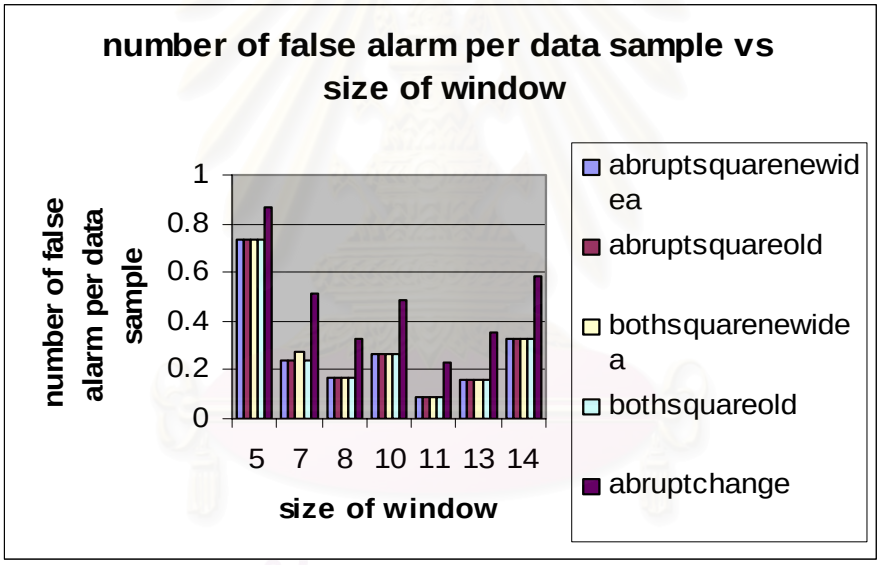
จากผลการทดลองดังตารางที่ 5.7 จะเห็นได้ว่าวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกให้ค่าเฉลี่ยของช่วงเวลาที่จะเกิดสัญญาณเตือนที่ผิดพลาดที่สูงกว่าวิธีการของฟัซซี ในบางขนาดหน้าต่าง แต่ว่าเมื่อย้อนกลับไปดูถึงเวลาที่สามารถตรวจจับความผิดปกติก่อนเกิดความเสียหายนั้น วิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกให้ผลที่แย่มากดังนั้นผลของค่าเฉลี่ยของช่วงเวลาที่จะเกิดสัญญาณเตือนที่ผิดพลาดที่สูงไม่สามารถแสดงถึงประสิทธิภาพที่ดีได้



รูปที่ 5.38 ความสัมพันธ์ระหว่างจำนวนสัญญาณเตือนที่ผิดพลาดต่อจำนวนหน้าต่างข้อมูลและขนาดความกว้างของหน้าต่างที่ใช้ในการตรวจจับความผิดปกติ แบบ *A*



รูปที่ 5.39 ความสัมพันธ์ระหว่างจำนวนสัญญาณเตือนที่ผิดพลาดต่อจำนวนหน้าต่างข้อมูลและขนาดความกว้างของหน้าต่างที่ใช้ในการตรวจจับความผิดปกติ แบบ *B*



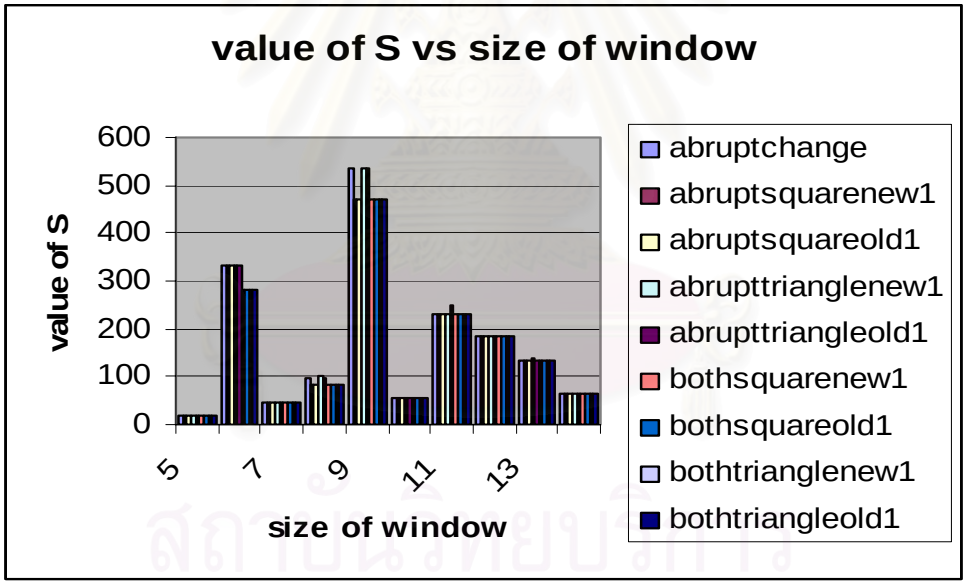
รูปที่ 5.40 ความสัมพันธ์ระหว่างจำนวนสัญญาณเตือนที่ผิดพลาดต่อจำนวนหน้าต่างข้อมูลและขนาดความกว้างของหน้าต่างที่ใช้ในการตรวจจับความผิดปกติ แบบ *B*

จากผลการทดลองดังรูปที่ 5.38-5.40 จะเห็นได้ว่าการใช้ขนาดหน้าต่างในการตรวจจับความผิดปกติของระบบโครงข่ายที่แตกต่างกันจะให้ผลของจำนวนสัญญาณเตือนที่ผิดพลาดต่อจำนวนหน้าต่างข้อมูลที่แตกต่างกัน และการใช้ฟังก์ชันการเป็นสมาชิกแบบ *B* ให้ผลของการปรับปรุงจำนวนสัญญาณเตือนที่ผิดพลาดต่อจำนวนหน้าต่างข้อมูล จากการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก ดีกว่าแบบ *A* ที่เป็นเช่นนี้เนื่องจากแบบ *A* มีฟังก์ชันการเป็นสมาชิกโน้มเอียงไปทางความผิดปกติมากกว่าแบบ *A* เป็นผลให้จำนวนสัญญาณเตือนที่ผิดพลาดมีค่าสูงกว่า แบบ *B*

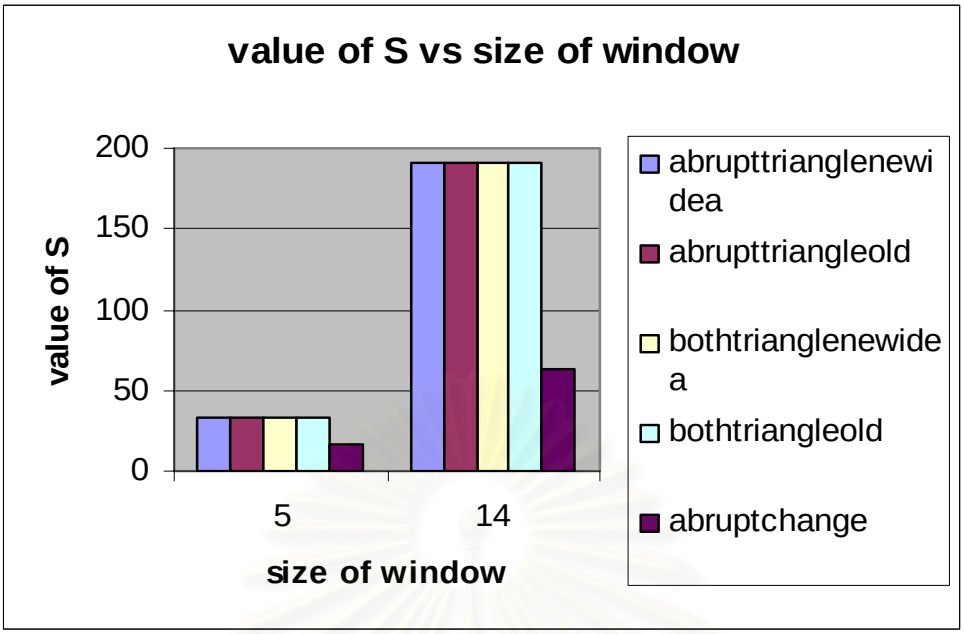
win	$N_f(ipIDE)$
5	0
6	0.0243
7	0.0142

ตารางที่ 5.8 จำนวนสัญญาณเตือนที่ผิดพลาดต่อจำนวนหน้าต่างข้อมูล ของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก

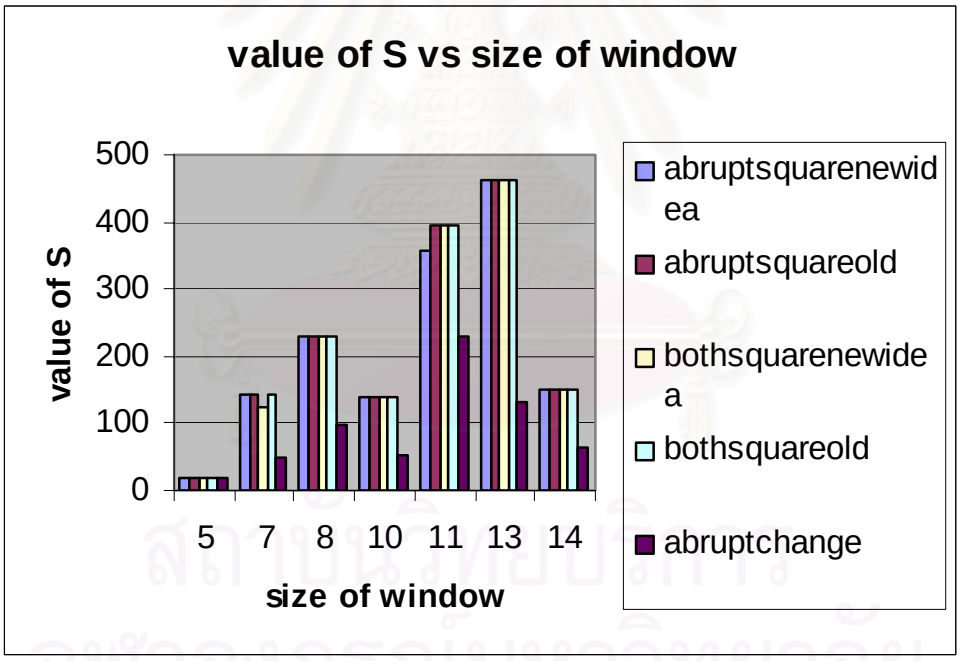
จากผลการทดลองดังตารางที่ 5.8 จะเห็นได้ว่าวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกให้จำนวนสัญญาณเตือนที่ผิดพลาดต่อจำนวนหน้าต่างข้อมูลที่ต่ำกว่าวิธีการของฟัซซี ในบางขนาดหน้าต่าง แต่ว่าเมื่อย้อนกลับไปดูถึงเวลาที่สามารถตรวจจับความผิดปกติก่อนเกิดความเสียหายนั้น วิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกให้ผลที่แย่มากดังนั้นผลของค่าเฉลี่ยของช่วงเวลาที่จะเกิดสัญญาณเตือนที่ผิดพลาดที่สูงไม่สามารถแสดงถึงประสิทธิภาพที่ดีได้



รูปที่ 5.41 ความสัมพันธ์ระหว่าง *value of S* และขนาดความกว้างของหน้าต่างที่ใช้ในการตรวจจับความผิดปกติ แบบ *A*



รูปที่ 5.42 ความสัมพันธ์ระหว่าง *value of S* และขนาดความกว้างของหน้าต่างที่ใช้ในการตรวจจับความผิดปกติ แบบ *B*



รูปที่ 5.43 ความสัมพันธ์ระหว่าง *value of S* และขนาดความกว้างของหน้าต่างที่ใช้ในการตรวจจับความผิดปกติ แบบ *B*

จากผลการทดลองดังรูปที่ 5.41-5.43 จะเห็นได้ว่าวิธีการตรวจจับความผิดปกติแบบใช้ฟัซซี แบบ *B* ให้ผลที่ดีกว่าแบบ *A* อย่างมาก และปรับปรุงประสิทธิภาพการตรวจจับความผิดปกติแบบทันทีทันใดทุกขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติ

win	*S(ipIDE)*
5	-
6	4938.27
7	9859.15

ตารางที่ 5.9 ค่า *S* ของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิก

จากผลการทดลองดังตารางที่ 5.9 จะเห็นได้ว่าวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกให้ผลของค่า *S* ที่สูงมาก เมื่อเปรียบเทียบกับวิธีฟัซซี แต่ว่าในการที่เราจะบอกว่าวิธีการตรวจจับความผิดปกติมีประสิทธิภาพดีหรือไม่ต้องคำนึงถึง เวลาที่สามารถตรวจจับความผิดปกติก่อนระบบโครงข่ายเกิดความเสียหาย ซึ่งวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกให้ผลที่แย่มาก ดังนั้น ประสิทธิภาพโดยรวมของวิธีการนี้จึงแย่กว่าวิธีการตรวจจับความผิดปกติแบบทันทีทันใด และวิธีการตรวจจับความผิดปกติโดยใช้ฟัซซี

5.3.2 **สรุปผลการทดลอง**

จากผลการทดลองจะเห็นได้ว่าประสิทธิภาพในการตรวจจับความผิดปกติของระบบโครงข่ายของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกให้ผลแย่ที่สุด และการตรวจจับความผิดปกติของระบบโครงข่ายโดยใช้ฟัซซี แบบ *B* ปรับปรุงประสิทธิภาพในการตรวจจับความผิดปกติของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกและแบบทันทีทันใด ดีกว่าแบบ *A* เนื่องจากแบบ *A* นั้นฟังก์ชันการเป็นสมาชิกมีความโน้มเอียงไปทางความผิดปกติมาก ทำให้จำนวนสัญญาณเตือนที่ผิดพลาดมีจำนวนมากกว่าแบบ *B*

บทที่ 6

บทสรุปและข้อเสนอแนะ

บทนี้กล่าวถึงบทสรุปของระบบการตรวจจับความผิดปกติในระบบโครงข่ายที่นำเสนอในวิทยานิพนธ์ และข้อเสนอแนะเพิ่มเติม

6.1 บทสรุป

วิทยานิพนธ์ฉบับนี้นำเสนอการปรับปรุงวิธีการตรวจจับความผิดปกติของระบบโครงข่าย 3 ส่วน ในส่วนแรกเป็นการปรับปรุงวิธีการตรวจจับความผิดปกติของการเปรียบเทียบรูปแบบทราฟฟิกด้วยกัน 4 วิธีคือ การเสนอการหาค่าถ่วงน้ำหนักแบบใหม่ การปรับค่าถ่วงน้ำหนักให้เปลี่ยนตามเวลา การใช้ข้อมูลมากกว่าหนึ่งชนิดข้อมูลร่วมกันในการตรวจจับความผิดปกติ และการใช้ค่าถ่วงน้ำหนักที่เปลี่ยนแปลงตามเวลาร่วมกับการใช้ข้อมูลมากกว่าหนึ่งชนิดข้อมูลในการตรวจจับความผิดปกติ อีกทั้งยังวิเคราะห์ถึงผลของขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติที่มีผลต่อความแน่นอนในการตรวจจับความผิดปกติที่อาจจะเกิดขึ้นในอนาคต โดยการใช้โปรแกรม *NS (Network Simulator)* ในการก่อเกิดทราฟฟิกและทดลองในการตรวจจับความผิดปกติ จะเห็นได้ว่าการใช้ขนาดหน้าต่างที่สั้นเกินไปในการตรวจจับความผิดปกติของระบบโครงข่าย จะมีผลให้ประสิทธิภาพในการตรวจจับความผิดปกติลดลง ที่เป็นเช่นนี้เนื่องจากจำนวนจุดข้อมูลที่ใช้ในการทำนายค่าเฉลี่ยและความแปรปรวนมีน้อยเกินไปส่งผลให้เกิดความผิดพลาด และชนิดของข้อมูลที่ใช้ในการตรวจจับความผิดปกติที่แตกต่างกันให้ผลของประสิทธิภาพในการตรวจจับความผิดปกติที่แตกต่างกันที่เป็นเช่นนี้เนื่องจากแต่ละชนิดข้อมูลมีความคล้ายคลึงกันระหว่างข้อมูลในอดีตและปัจจุบันที่แตกต่างกัน วิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบเปรียบเทียบรูปแบบทราฟฟิกนั้นเหมาะสำหรับตรวจจับความผิดปกติที่เป็นแบบค่าเฉลี่ยของทราฟฟิกเกิดการเปลี่ยนแปลง ซึ่งเกิดในกรณีของ ข่ายเชื่อมโยงเกิดความเสียหาย แต่ไม่เหมาะสำหรับความผิดปกติที่ทราฟฟิกมีลักษณะค่าเบี่ยงเบนทราฟฟิกเฉลี่ยเปลี่ยนแปลง เนื่องจากวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกใช้ข้อมูลค่าเฉลี่ยของทราฟฟิกในการตรวจจับ และวิธีการที่นำเสนอในการปรับปรุงวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกให้ประสิทธิภาพในการตรวจจับความผิดปกติที่ดีขึ้นกว่าวิธีการเดิม

ในส่วนที่สองทำการวิเคราะห์ผลของวิธีการตรวจจับความผิดปกติของระบบโครงข่ายแบบทันทีทันใดโดยใช้ทราฟฟิกที่ได้จากโครงข่ายจุฬาลงกรณ์มหาวิทยาลัย ที่รูทเทอร์ 7513 และนำเสนอการเลือกใช้เกณฑ์ในการบอกว่าระบบโครงข่ายเกิดความผิดปกติหรือไม่ด้วยกัน 2 วิธี คือ

การเลือกใช้ค่ากลางของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด และ การเลือกใช้ค่าเฉลี่ยของค่าความผิดพลาดของเวกเตอร์ความผิดพลาด จะเห็นได้ว่าจำนวนหน้าต่างที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่าย จำนวนรอบที่ใช้ในการคำนวณเมตริกซ์ *A* และวิธีการที่เราเลือกใช้ในการหาค่าเกณฑ์ในการระบุว่าเกิดความผิดปกติในโครงข่ายหรือไม่ มีผลต่อประสิทธิภาพในการตรวจจับความผิดปกติของระบบโครงข่าย ดังนั้นเราควรที่จะทดสอบเพื่อหาขนาดความกว้างหน้าต่างที่เหมาะสมที่สุดและจำนวนรอบที่ใช้ในการคำนวณเมตริกซ์ *A* ที่เหมาะสมที่สุดเช่นเดียวกัน เพื่อที่จะได้ประสิทธิภาพที่ดีที่สุดในการตรวจจับความผิดปกติของระบบโครงข่าย

ในส่วนที่สามทำการใช้วิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกและเปลี่ยนแปลงทันทีทันใด ร่วมกันโดยใช้กรรมวิธีการของฟัซซีในการตัดสินใจว่าในขณะนั้นเกิดความผิดปกติหรือไม่โดยใช้ทราฟฟิกที่ได้จากโครงข่ายจุฬาลงกรณ์มหาวิทยาลัย ที่รูทเทอร์ 7513 จากผลการทดสอบจะเห็นได้ว่าประสิทธิภาพในการตรวจจับความผิดปกติของระบบโครงข่ายของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกให้ผลแย่ที่สุด และการตรวจจับความผิดปกติของระบบโครงข่ายโดยใช้ฟัซซี แบบ *B* ปรับปรุงประสิทธิภาพในการตรวจจับความผิดปกติของวิธีการตรวจจับความผิดปกติแบบเปรียบเทียบรูปแบบทราฟฟิกและแบบทันทีทันใดดีกว่าแบบ *A* เนื่องจากแบบ *A* นั้นฟังก์ชันการเป็นสมาชิกมีความโน้มเอียงไปทางความผิดปกติมาก ทำให้จำนวนสัญญาณเตือนที่ผิดพลาดมีจำนวนมากกว่าแบบ *B*

6.2 ข้อเสนอแนะ

1. การใช้ระบบการตรวจจับความผิดปกติในระบบโครงข่ายในวิทยานิพนธ์ที่เสนอนี้ เมื่อนำไปใช้ในโครงข่ายต่างๆนั้นควรที่จะเลือกขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติในระบบโครงข่ายให้เหมาะสมเพื่อประสิทธิภาพที่ดีในการตรวจจับความผิดปกติในระบบโครงข่าย

2. เนื่องจากมีข้อจำกัดทางด้านทราฟฟิกในระบบโครงข่ายของจุฬาลงกรณ์มหาวิทยาลัย คือ ไม่มีการบันทึกข้อมูลการเกิดความเสียหายในระบบโครงข่าย และหน่วยความจำของคอมพิวเตอร์ที่บรรจุข้อมูลทราฟฟิกผ่านโปรแกรม *NETFLOW* มีขนาดไม่ใหญ่นัก เป็นผลให้ทราฟฟิกที่นำมาใช้ในการตรวจจับความผิดปกติของระบบโครงข่ายมีจำนวนน้อย ดังนั้นถ้าสามารถหาทราฟฟิกของระบบโครงข่ายอื่นที่มีการบันทึกข้อมูลการเกิดความเสียหายในระบบโครงข่าย และหน่วยความจำของคอมพิวเตอร์ที่บรรจุข้อมูลทราฟฟิกผ่านโปรแกรม *NETFLOW* มีขนาดใหญ่พอเราสามารถที่จะตรวจสอบประสิทธิภาพของระบบการตรวจจับความผิดปกติของระบบโครงข่ายได้อย่างมีประสิทธิภาพมากขึ้น

รายการอ้างอิง.

1. W.E. Leland, M.S. Taqqu, W. Willinger, and D. V. Wilson. On the Self-Similar Nature of Ethernet Traffic (extended version). IEEE/ACM Trans Networking. (1994) : 1-15.

2. J. L. Vehel, E. Lutton, and C. Tricot. Fractals in Engineering: From Theory to Industrial Applications. New York: Springer-Verlag. (1997) : 185-202.

3. Marina Thottan and Chuanyi Ji. Anomaly Detection in IP Network. IEEE Transactions on Signal Processing. (August 2003) : 2191-2204.

4. L.Lewis. A Case Based Reasoning Approach to the Management of Faults in Communication Networks. in Proc. IEEE INFOCOM. (March 1993) : 1422-1429.

5. A.Lazar, W. Wang, and R. Deng. Models and Algorithms for Network Fault Detection and Identification. in Proc. IEEE Int. Contr. Conf. (November 1992) : 999-1003.

6. C. Hood and C. Ji. Proactive Network Fault Detection. in Proc. IEEE INFOCOM. (April 1997) : 1147-1155

7. S. Papavassiliou, M.Pace, A. Zawadzki, and L.Ho. Implementing Enhanced Network Maintenance for Transaction Access Services: Tools and Applications. Proc. IEEE Int. Contr. Conf. (2000) : 211-215

8. Peter V. de Souza. Statistical Tests and Distance Measures for LPC Coefficients. IEEE Transactions on Acoustics, Speech, and Signal Processing. (December 1997) : 554-559.

9. Yan Qiao and Xie Weixin. A Network IDS with Low False Positive Rate. IEEE Proceedings of the 2002 Congress on Evolutionary Computation. (May 2002) : 1121-1126.

10. Hassan Hajji. Baselining Network Traffic and Online Faults Detection. IEEE International Conference on Communications. (May 2003) : 301-308.

11. Xiaolin Li, Marc Parizeau and Rejean Plamondon. Training Hidden Markov Models with Multiple Observations-A Combinatorial Method. IEEE Transactions on Pattern Analysis and Machine Intelligence. (April 2000) : 371-377

12. Sung-Bae Cho. Incorporating Soft Computing Techniques Into a Probabilistic Intrusion Detection System. IEEE Transactions on Systems, Man, and Cybernetics-Part C: Applications and Reviews. (May 2002) :154-160

13. Ari S. Nissinen and Heikki Hyotyniemi, Evolutionary Training of Behavior-Based Self-Organizing Mao. IEEE. (1998).

14. Daniel Ramot, Menahem Friedman, Gideon Langholz, and Abraham Kandel, Fello, IEEE. Complex Fuzzy Logic. IEEE Transactions on Fuzzy Systems. (August 2003) : 450-461

ภาคผนวก

บทความทางวิชาการที่ได้รับการเผยแพร่

1. ชัยเชษฐ์ สายวิจิตร และ พิชัย วัฒนะภราดร. การเฝ้าระวังโครงข่ายเพื่อตรวจจับความผิดปกติโดยการเปรียบเทียบรูปแบบทราฟฟิก.การประชุมวิชาการทางวิศวกรรมไฟฟ้า ครั้งที่ 28 (ตุลาคม 2548):721-724

การเฝ้าระวังโครงข่ายเพื่อตรวจจับความผิดปกติโดยการเปรียบเทียบรูปแบบทราฟฟิค

Network Monitoring for Anomalies Detection based on Modified Pattern Matching Technique

ชัยเชษฐ์ สายวิจิตร และ พิชัย วัฒนะภราดร
ภาควิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ถนนพญาไท เขตปทุมวัน กรุงเทพฯ 10330
โทร: 0-2218-6907 โทรสาร: 0-2218-6912 E-mail : Chaiyachet.s@chula.ac.th

บทคัดย่อ

จากความสำคัญและความจำเป็นของการใช้งานของโครงข่ายเพื่อการสื่อสารที่ราบรื่นและต่อเนื่อง บทความนี้นำเสนอวิธีการและขั้นตอนการศึกษาวิธีการตรวจจับความผิดปกติของระบบโครงข่ายของการเปรียบเทียบรูปแบบทราฟฟิค (Pattern Matching) และเสนอการปรับปรุงวิธีการตรวจจับความผิดปกติของการเปรียบเทียบรูปแบบทราฟฟิคด้วยกัน 3 วิธีคือ การปรับค่าถ่วงน้ำหนักให้เปลี่ยนตามเวลา การใช้ข้อมูลมากกว่าหนึ่งชนิดข้อมูลร่วมกันในการตรวจจับความผิดปกติ และการใช้ค่าถ่วงน้ำหนักที่เปลี่ยนแปลงตามเวลาร่วมกับการใช้ข้อมูลมากกว่าหนึ่งชนิดข้อมูลในการตรวจจับความผิดปกติ อีกทั้งยังวิเคราะห์ถึงผลของขนาดหน้าต่างที่ใช้ในการตรวจจับความผิดปกติที่มีผลต่อความแน่นอนในการตรวจจับความผิดปกติที่อาจจะเกิดขึ้นในอนาคต

คำสำคัญ : ความผิดปกติของระบบโครงข่าย, ค่าถ่วงน้ำหนัก

Abstract

This paper presents methods on network anomaly detection by using Pattern Matching techniques and proposes three methods to improve performance in detecting network anomaly of Pattern Matching method. Three proposed methods utilize time varying weighted value, multiple sets of data, and combining both techniques, respectively. Furthermore, this paper also discuss on the effect of windows size on network anomaly detection.

Keywords : Network Anomaly, Weighted Value

1. คำนำ

ปัจจุบันนี้ ความต้องการการใช้งานของระบบโครงข่ายภายในองค์กรต่างๆมีแนวโน้มที่จะเพิ่มสูงขึ้นเรื่อยๆ มีผลทำให้เกิดการเพิ่มขึ้นของความซับซ้อนภายในระบบการจัดการภายในโครงข่าย ส่งผลให้มีความล้มเหลวภายในโครงข่ายเกิดเพิ่มขึ้นตามความซับซ้อน ภายในระบบโครงข่ายนั้นจะประกอบไปด้วย เร้าเตอร์ และ สวิตช์ ซึ่งมีหน้าที่ในการส่งข้อมูลจากต้นทางไปยังปลายทางผ่านเส้นทางที่เหมาะสม โดยที่พฤติกรรมของแต่ละอุปกรณ์นั้น สามารถใช้เป็นตัวช่วยในการบ่งชี้ถึงสภาวะภายในโครงข่ายขณะนั้นได้ว่ามีลักษณะอย่างไร และคาดการณ์ถึงความผิดปกติที่จะเกิดขึ้นในระบบโครงข่ายในเวลาอันใกล้ ด้วยเหตุดังกล่าวก่อให้เกิดความสนใจเพื่อการค้นคว้าและวิจัยมากมายเกี่ยวกับวิธีในการตรวจจับความผิดปกติของระบบโครงข่ายก่อนที่ระบบโครงข่ายจะเกิดความเสียหาย เพื่อที่จะช่วยเตือนผู้ควบคุมดูแลระบบโครงข่าย ทำการตรวจสอบและแก้ไขได้ทันท่วงที มีวิธีการตรวจจับความผิดปกติของระบบโครงข่ายหลายวิธีได้ถูกพัฒนาขึ้นเพื่อใช้ในการตรวจจับความผิดปกติ เช่น ปัญญาประดิษฐ์ (Artificial Intelligence) [1] , การเรียนรู้จากเครื่องจักร (Machine Learning) [2], แบบจำลองสถานะของเครื่องจักร (State Machine Modeling) [2] และวิธีการประมวลผลสัญญาณทางสถิติ (Statistical Signal Processing Technique) [3] โดยที่แต่ละวิธีของการตรวจจับความผิดปกติของระบบโครงข่ายนั้นมีข้อจำกัดหลายประการเช่น การไม่สามารถตรวจจับความผิดปกติของระบบโครงข่ายที่มีลักษณะใหม่ๆได้ (False Negative Alarm) และ อีกทั้งยังมีกรณีที่มีการส่งสัญญาณเตือนที่ผิดพลาดว่ามีความผิดปกติของระบบโครงข่ายเกิดขึ้นทั้งที่ระบบโครงข่ายยังอยู่ในสภาวะที่ปกติ (False Positive Alarm)

จากเหตุผลที่ได้กล่าวมาข้างต้นนี้ เราจึงได้มีการทำการศึกษาและพัฒนาวิธีการเปรียบเทียบรูปแบบทราฟฟิคให้มีประสิทธิภาพที่ดียิ่งขึ้นโดยใช้ข้อมูลหลายระดับ และทำการเปลี่ยนแปลงค่าถ่วงน้ำหนักของวิธีการ เปรียบเทียบรูปแบบทราฟฟิค ให้เปลี่ยนแปลงตามเวลา และใช้ 2 วิธีที่นำเสนอข้างต้นร่วมกัน และทำการวิเคราะห์ถึงผลของขนาดหน้าต่างที่ใช้ต่อความแน่นอนในการตรวจจับความผิดปกติ โดยเราจะใช้ข้อมูลของ MIB (Management Information Base) ในโพโทรคอลของ SNMP (Simple Network Management Protocol) ในการพิจารณาความผิดปกติของระบบโครงข่าย

2. ทฤษฎีการเปรียบเทียบรูปแบบทราฟฟิค [4]

หลักการการตรวจจับความผิดปกติของข่ายเชื่อมโยงวิธีนี้ จะมีการเก็บค่าข้อมูล เช่น การใช้ประโยชน์ของข่ายเชื่อมโยง (Link Utilization) การสูญหายของแพ็กเกต (Packet Loss) หรือ อัตราของจำนวนไบต์ของข้อมูล(Rate of Byte Counts) ซึ่งจะเก็บข้อมูลของแต่ละวัน แล้วนำข้อมูลนี้มาใช้ในการทำนายข้อมูลปัจจุบันเพื่อใช้ในการตรวจจับความผิดปกติในช่วงเวลานั้น วิธีการตรวจจับนี้จะนำเอาข้อมูล

จริงที่ได้มาเทียบกับข้อมูลที่เราได้ทำนายไว้ภายในช่วงเวลาที่กำหนดแล้วพิจารณาว่าเกิดความผิดปกติหรือไม่ โดยมีระดับของช่วงค่ามากที่สุดและน้อยที่สุดซึ่งยอมรับได้ว่าระบบจะไม่ผิดปกติ เป็นช่วงในการเปรียบเทียบ ถ้าค่าที่ได้ไม่อยู่ในช่วงนี้แสดงว่ามีความผิดปกติเกิดขึ้น เป็นผลให้ระบบการจัดการจะส่งสัญญาณ (Alarm) ว่าเกิดความผิดปกติเกิดขึ้น

กำหนดให้ $I(t)$ คือ ค่าเฉลี่ยของทราฟฟิคที่ใช้ในการทำนายลักษณะทราฟฟิคในปัจจุบัน

โดยที่ $$I(t) = \alpha(t) + \beta(t) + \varepsilon(t) \quad (1)$$

ซึ่ง $\alpha(t)$ คือ ค่าเฉลี่ยของทราฟฟิคในวันจันทร์ถึงวันศุกร์

$\beta(t)$ คือ ค่าเฉลี่ยของทราฟฟิคในวันเสาร์ วันอาทิตย์ หรือวันหยุดพิเศษ เช่น วันปีใหม่ วันสงกรานต์ วันลงทะเบียน ฯลฯ

$\varepsilon(t)$ คือ ค่าการเบี่ยงเบนของค่าเฉลี่ยของทราฟฟิคของ $\alpha(t)$ และ $\beta(t)$

ซึ่ง $\alpha_j(t)$ หาค่าได้จากการถ่วงน้ำหนักข้อมูลทราฟฟิควันจันทร์ถึงวันศุกร์ในสัปดาห์ที่แล้วโดยไม่รวมวันที่เราสนใจดังสมการที่ 2

$$\alpha_j(t) = \sum_{k\in\{1,\ldots,5\}-\{j\}} c_{j,k}\alpha_k(t) + \varsigma \quad (2)$$

ซึ่ง $j = \{1,2,3,4,5\}$ โดยที่ 1 แทนวันจันทร์ 2 แทนวันอังคาร และอื่นๆ

$k \in \{1,\ldots,5\} - \{j\}$ โดยที่ 1 แทนวันจันทร์ 2 แทนวันอังคาร และ อื่นๆ

ς คือ ค่าที่ช่วยในการปรับให้ทราฟฟิคที่เราพิจารณามีค่าเชื่อถือมากยิ่งขึ้น

$c_{j,k}$ คือ ค่าถ่วงน้ำหนักของวันที่ j เทียบกับวันที่ k

และ $$\sum_k c_{j,k} = 1 \quad (3)$$

$\beta_j(t)$ หาค่าได้จากการถ่วงน้ำหนักข้อมูลทราฟฟิควันเสาร์ วันอาทิตย์ หรือ วันหยุดพิเศษใน 4 สัปดาห์ที่แล้วโดยไม่รวมสัปดาห์ที่สนใจ

$$\beta_j(t) = \sum_{k\in\{1,\ldots,4\}-\{j\}} d_{j,k}\beta_k(t) + \varsigma \quad (4)$$

ซึ่ง $j = \{1,2,3,4\}$ โดยที่ 1 แทน หลังจากสัปดาห์ปัจจุบัน 1 สัปดาห์ 2 แทน หลังจากสัปดาห์ปัจจุบัน 2 สัปดาห์ เป็นต้น

$k \in \{1,\ldots,4\} - \{j\}$ โดยที่ 1 แทน หลังจากสัปดาห์ปัจจุบัน 1 สัปดาห์ 2 แทน หลังจากสัปดาห์ปัจจุบัน 2 สัปดาห์ เป็นต้น

$d_{j,k}$ คือ ค่าถ่วงน้ำหนักของสัปดาห์ที่ j เทียบกับสัปดาห์ที่ k

และ $$\sum_k d_{j,k} = 1 \quad (5)$$

ค่าของ $c_{m,n}$ หาได้จากค่าเฉลี่ยของอัตราส่วนของทราฟฟิคในแต่ละเวลาของทราฟฟิกของวันที่ m กับทราฟฟิคของวันที่ n ส่วนค่าของ $d_{m,n}$ หาได้จากค่าเฉลี่ยของอัตราส่วนของทราฟฟิคในแต่ละเวลาของทราฟฟิคของวันหยุดสุดสัปดาห์ของสัปดาห์ที่ m กับทราฟฟิคของวันหยุดสุดสัปดาห์ของสัปดาห์ที่ n ดังสมการที่ 6 และ 7 ตามลำดับ

$$c_{m,n} = \overline{<\alpha_m(t)>_t / <\alpha_n(t)>} \quad (6)$$

$$d_{m,n} = \overline{<\beta_m(t)>_t / <\beta_n(t)>} \quad (7)$$

ค่าของ $\varepsilon_{wk,j}(t), \varepsilon_{wked,j}(t)$ สามารถหาได้จากสมการที่ 8 และ 9 ตามลำดับ

$$\{<[\varepsilon_{wk,j}(t)]^2>_t\}^{\frac{1}{2}} = \sum_{k\in\{1,\ldots,5\}-\{j\}} c_{j,k}\{<[\varepsilon_{wk,k}(t)]^2>_t\}^{\frac{1}{2}} \quad (8)$$

$$\{<[\varepsilon_{wked,j}(t)]^2>_t\}^{\frac{1}{2}} = \sum_{k\in\{1,\ldots,4\}-\{j\}} d_{j,k}\{<[\varepsilon_{wked,k}(t)]^2>_t\}^{\frac{1}{2}} \quad (9)$$

โดยที่ $\varepsilon_{wk,j}(t)$ คือ ค่าการเบี่ยงเบนของทราฟฟิคของวันที่ j ของวันธรรมดา

$\varepsilon_{wked,j}(t)$ คือ ค่าการเบี่ยงเบนของทราฟฟิคของสัปดาห์ที่ j ของวันหยุดสุดสัปดาห์

ค่าขอบเขตบนและขอบเขตล่างที่ได้จาการทำนายเพื่อใช้ในการตรวจจับความผิดปกติของระบบโครงข่าย แสดงในสมการที่ (10) (11) และ (12) ตามลำดับ

$$\text{Upper Threshold} = I(T_n) + 2\bar{\sigma}(T_n) \quad (10)$$

$$\text{Baseline} = I(T_n) \quad (11)$$

$$\text{Lower Threshold} = I(T_n) - 2\bar{\sigma}(T_n) \quad (12)$$

3. วิธีที่นำเสนอ

จากวิธีการเปรียบเทียบรูปแบบทราฟฟิค ที่กล่าวมานั้นเราจึงได้มีการเสนอการปรับปรุงการตรวจจับความผิดปกติของวิธีการนี้ดังนี้

3.1 การปรับเปลี่ยนค่าถ่วงหนักให้เปลี่ยนแปลงตามเวลา

$$c_{m,n}(t) = \overline{\sum_{i=1}^{N} \frac{\alpha_{m,i}(t)}{\alpha_{n,i}(t)}} \quad (13)$$

3.2 การใช้ข้อมูล 3 ระดับในการตรวจจับความผิดปกติของระบบโครงข่าย ในที่นี่ข้อมูล 3 ระดับประกอบไปด้วย ipIDE, ipOR และ ipIR

ซึ่ง ipIR คือ จำนวนไบต์ของทราฟฟิคทั้งหมดที่เข้าสู่เร้าเตอร์ในช่วงเวลาหนึ่ง

ipOR คือ จำนวนไบต์ของทราฟฟิคที่ผ่านจากอุปกรณ์ที่ต่อกับเร้าเตอร์ เข้าสู่เร้าเตอร์เพื่อส่งออกไปในช่วงเวลาหนึ่ง

ipIDE คือ จำนวนไบต์ของทราฟฟิคที่ผ่านจากเร้าเตอร์เพื่อเข้าสู่อุปกรณ์ที่ต่อกับเร้าเตอร์ในช่วงเวลาหนึ่ง

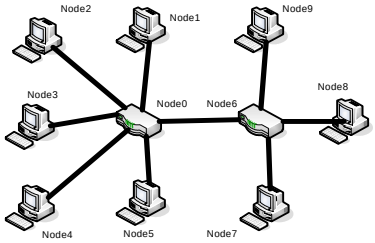
โดยเงื่อนไขที่ระบบโครงข่ายจะไม่ผิดปกติเป็นดังสมการที่ (14)

$$\sum_{i=1}^{3}(\bar{I}_i - 2\bar{\sigma}_i) \le \sum_{i=1}^{3} I_i \le \sum_{i=1}^{3}(\bar{I}_i + 2\bar{\sigma}_i) \quad (14)$$

3.3 การใช้การปรับเปลี่ยนค่าถ่วงน้ำหนักให้เปลี่ยนแปลงตามเวลาร่วมกับการใช้ข้อมูล 3 ระดับในการตรวจจับความผิดปกติของระบบโครงข่าย

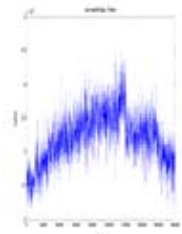
4. ระบบโครงข่ายที่ใช้ในการทดลอง

ระบบโครงข่ายที่ใช้ในการทดลองนี้แสดงดังรูปที่1

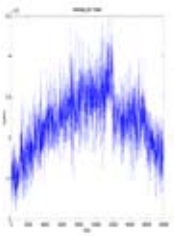


รูปที่. 1 ระบบโครงข่ายที่ใช้ในการทดลอง

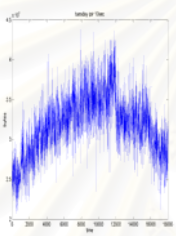
โดยที่เราจะทำการกำเนิดทราฟฟิกในระบบโครงข่ายนี้โดยใช้โปรแกรม NS(Network Simulator)โดยใช้การส่งข้อมูลแบบ UDP (User Datagram Protocol) ด้วยการกระจายของการส่งข้อมูล แบบ Exponential จำนวนทั้งสิ้น 6 วัน จากช่วงเวลาที่ 0 วินาทีถึงช่วงเวลาที่ 18,000 วินาที ดังรูปที่ 2, 3, 4, 5, 6, 7 ตามลำดับ



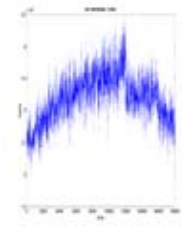
รูปที่.2 ipIR pastfriday



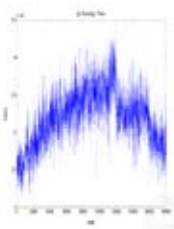
รูปที่.3 ipIR monday



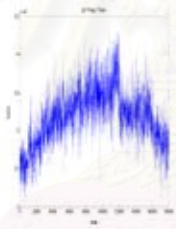
รูปที่.4 ipIR tuesday



รูปที่.5 ipIR wendsday



รูปที่.6 ipIR Thursday



รูปที่.7 ipIR friday

5. ผลการทดลอง

บทความนี้แบ่งการทดลองเป็น 3 ส่วน ซึ่งประกอบไปด้วย

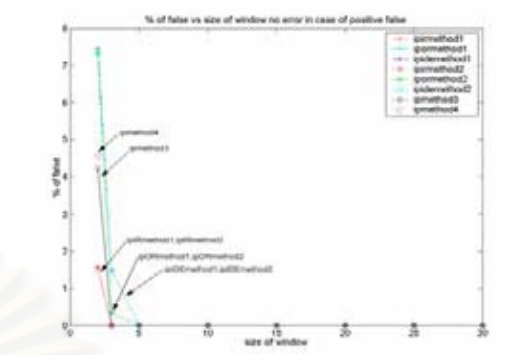
1). ไม่มีความผิดปกติเกิดขึ้นในระบบโครงข่าย

2). มีความผิดปกติเกิดขึ้นที่ข่ายเชื่อมโยงระหว่าง โหนด 0 และโหนด 6 ซึ่งแพ็กเกตที่ผ่านข่ายเชื่อมโยงคู่นี้จะสูญหาย 50 เปอร์เซ็นต์ ในช่วงเวลา(2,400-4,000) 80 เปอร์เซนต์ในช่วงเวลา (9,000-12,000) และ 100 เปอร์เซนต์ในช่วงเวลา (15,000-17,000)

3). มีความผิดปกติเกิดขึ้นที่โหนด 0 และ โหนด 1 ที่เวลา (3,000-3,100) โดยที่โหนด 1 ส่งข้อมูลไปยังโหนด 0 มากผิดปกติในช่วงเวลานี้ และความผิดปกติเกิดขึ้นที่ทุกโนดในกรณีที่ อัตราส่วนระหว่างช่วงเวลาการส่งและหยุดส่งคงที่ แต่ค่าของสองค่านี้เปลี่ยนไปในช่วงเวลา(7,000-8,000)

วิธีการตรวจจับความผิดปกติที่จะใช้ในการศึกษานี้คือ วิธีการดั้งเดิมของการเปรียบเทียบรูปแบบทราฟฟิค และวิธีการที่เรานำเสนออีก3วิธีโดยการเปลี่ยนแปลงคาบของหน้าต่าง(period of window) ในการตรวจจับความผิดปกติของระบบโครงข่าย

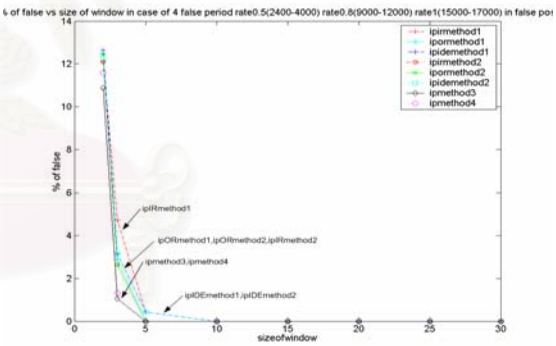
5.1 การทดลองความผิดปกติในระบบโครงข่ายแบบที่ 1



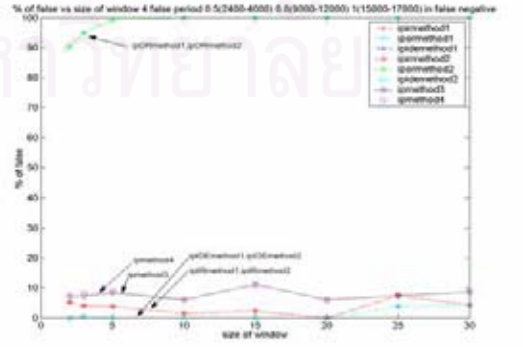
รูปที่.8 ความสัมพันธ์ระหว่างเปอร์เซ็นต์ของfalse positive alarm และขนาดของหน้าต่าง เมื่อไม่เกิดความผิดปกติในระบบโครงข่าย

จากผลการทดลองขนาดหน้าต่างที่สั้นจะมีผลให้เกิดการตรวจจับที่ผิดพลาดเกิดขึ้น เช่นขนาดหน้าต่างที่เท่ากับ 2 และ 3 (ดังรูปที่ 8) ที่เป็นเช่นนี้เนื่องจากจำนวนจุดข้อมูลที่ใช้ในการทำนายค่าเฉลี่ยและความแปรปรวนมีน้อยเกินไปทำให้เกิดความผิดพลาด และการใช้ข้อมูลทั้ง 3 ชนิด ร่วมกันในการตรวจจับจะให้ผลของการผิดพลาดที่น้อยกว่าการใช้ผลของข้อมูลชนิดเดียว

5.2 การทดลองความผิดปกติในระบบโครงข่ายแบบที่ 2



รูปที่.9 ความสัมพันธ์ระหว่างเปอร์เซ็นต์ของfalse positive alarm และขนาดของหน้าต่างเมื่อเกิดความผิดปกติในระบบโครงข่ายแบบที่2

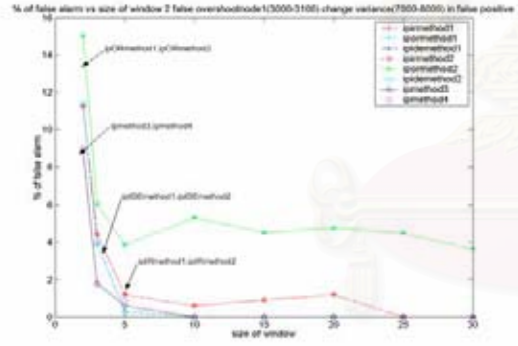


รูปที่.10 ความสัมพันธ์ระหว่างเปอร์เซ็นต์ของfalse negative alarm และขนาดของหน้าต่างเมื่อเกิดความผิดปกติในระบบโครงข่ายแบบที่ 2

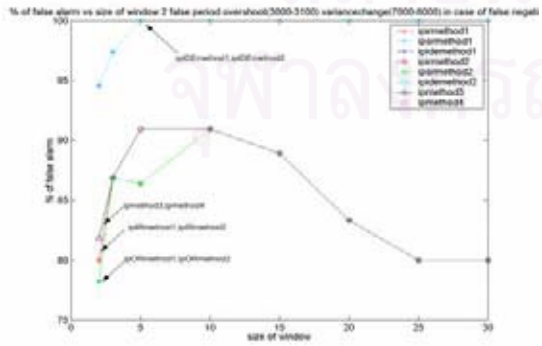
จากผลการทดลองในกรณีของ False Positive Alarm (รูปที่ 9) จะเห็นได้ว่าการลดขนาดของหน้าต่างในการตรวจจับความผิดปกติลง จะมีผลทำให้ความผิดพลาดในการตรวจจับสูงขึ้น และการใช้ข้อมูลทั้ง 3 ชนิดพร้อมกันในการตรวจจับจะให้ความแม่นยำในการตรวจจับที่ดีกว่าการใช้ข้อมูลเพียงชนิดเดียว

ในส่วนของ False Negative Alarm (รูปที่ 10) จะเห็นได้ว่าข้อมูลชนิด ipOR นั้นจะให้ความผิดพลาดที่สูงมากเนื่องจากว่าความผิดปกติของระบบโครงข่ายเกิดขึ้นที่ข่ายเชื่อมโยงระหว่างโหนด 0 และโหนด 6 ซึ่งข้อมูลของ ipOR นั้นจะเก็บค่าทราฟฟิกที่ไหลจากโหนด 1, 2, 3, 4, 5 ไปยังโหนด 0 ซึ่งไม่มีความเกี่ยวข้องกัน ซึ่งถ้านำข้อมูลชนิดนี้มาตรวจจับจะเกิดความผิดพลาดอย่างมาก ส่วนในเรื่องของขนาดของหน้าต่างที่ใช้ในการตรวจจับความผิดปกติของระบบโครงข่ายนั้น ขนาดของหน้าต่างมีผลเป็นอย่างมาก เนื่องจากถ้าขนาดหน้าต่างใหญ่เกินไปและไปคาบเกี่ยวกับช่วงที่เกิดความผิดปกติขึ้นเพียงเล็กน้อย ก็จะทำให้เกิดการตรวจจับที่ผิดพลาดเช่นเดียวกับกรณีที่ขนาดของหน้าต่างเล็กเกินไป จำนวนของข้อมูลน้อยเกินไป ที่ใช้ทำนายทำให้เกิดความผิดพลาดเกิดขึ้น และการใช้ข้อมูลทั้ง 3 ชนิดพร้อมกัน จะให้ผลดีในการตรวจจับมากกว่าการใช้ข้อมูลชนิดเดียวกัน เมื่อเทียบกันโดยใช้ค่าเฉลี่ยเปอร์เซ็นต์ความผิดพลาด

5.3 การทดลองความผิดปกติในระบบโครงข่ายแบบที่ 3



รูปที่.11 ความสัมพันธ์ระหว่างเปอร์เซ็นต์ของfalse positive alarm และขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายแบบที่ 3



รูปที่.12 ความสัมพันธ์ระหว่างเปอร์เซ็นต์ของfalse negative alarm และขนาดของหน้าต่าง เมื่อเกิดความผิดปกติในระบบโครงข่ายแบบที่ 3

ในส่วนของ False Negative Alarm มีค่าของความผิดพลาดในการตรวจจับความผิดปกติของระบบโครงข่ายที่สูงมาก เนื่องจากวิธีการเปรียบเทียบรูปแบบทราฟฟิค ไม่สามารถที่จะตรวจจับความปกติเนื่องจากค่าความแปรปรวนที่เปลี่ยนไปได้ ในส่วนของ False Positive Alarm นั้นการใช้ข้อมูล ทั้ง 3 ชนิดพร้อมกันนั้นจะให้ผลที่ดีกว่าการใช้ข้อมูลเพียงชนิดเดียว

6.สรุปผลการทดลอง

การใช้ข้อมูลทั้ง 3 ชนิดพร้อมกันนั้นจะช่วยให้การตรวจจับความผิดปกติของระบบโครงข่ายโดยรวมมีประสิทธิภาพดีขึ้น และชนิดของความผิดปกติของระบบโครงข่ายมีผลต่อวิธีการตรวจจับและขนาดของหน้าต่าง ซึ่งถ้าเราเลือกหน้าต่างที่ใช้ในการตรวจจับความผิดปกติในระบบโครงข่ายได้ไม่ดี ก็จะมีผลทำให้เกิดความผิดพลาดได้มากในการตรวจจับความผิดปกติในระบบโครงข่าย ในส่วนของวิธีการใช้ค่าถ่วงน้ำหนักแบบแปรตามเวลานั้น จะเห็นได้จากผลการวิเคราะห์ ผลของการใช้ค่าการเปลี่ยนแปลงค่าถ่วงน้ำหนักตามเวลากับค่าถ่วงน้ำหนักคงที่ มีผลใกล้เคียงกันมาก ที่เป็นเช่นนี้เนื่องจากการทดลองของเราให้ลักษณะข้อมูลที่ก่อกำเนิดมีลักษณะที่คล้ายคลึงกัน ซึ่งถ้าเรานำวิธีการนี้ไปใช้กับโครงข่ายที่มีลักษณะของทราฟฟิคของข้อมูลคล้ายกันน้อยกว่าการกำเนิดนี้ ผลของการตรวจจับความผิดปกติของระบบโครงข่ายน่าที่จะมีประสิทธิภาพดียิ่งขึ้น

7.เอกสารอ้างอิง

[1] L. Lewis, “A Case Based Reasoning Approach to The Management of Faults in Communication Networks,” *IEEE INFOCOM*, Vol. 3, San Francisco, CA, pp. 1422-1429, Mar. 1993

[2] A. Lazar, W. Wang, and R. Deng, “Models and Algorithms for Network Fault Detection and Identification: A Review,” *Singapore ICCS/ISITA '92. 'Communications on the Move'.*, Vol. 3, pp. 999-1003, Nov. 1992

[3] M. Thottan and C. Ji, “Anomaly Detection in IP Network,” *IEEE Transactions on Signal Processing*, Vol. 51, pp. 2191-2204 August 2003

[4] S. Papavassiliou, M. Pace, A. Zawadzki, and L. Ho, “Implementing Enhanced Network Maintenance for Transaction Access Services: Tools and Applications,” *IEEE Int. Contr. Conf*, Vol. 1, pp. 211-215, June 2000

[5] C. Hood and C. Ji, “Proactive Network Fault Detection,” *IEEE INFOCOM*, Vol. 3, Kobe, Japan, pp.1147-1155, Apr. 1997

[6] P. V. D. Souza, “Statistical Tests and Distance Measures for LPC Coefficients,” *IEEE Transactions on Acoustics, Speech, and Signal Processing*, Vol. ASSP-25, No.6, pp. 554-559, December 1997

ประวัติผู้เขียนวิทยานิพนธ์

นายพิชัย วัฒนะภราดร เกิดเมื่อวันที่ 9 มิถุนายน พ.ศ. 2524 สำเร็จการศึกษาปริญญาตรีวิศวกรรมศาสตรบัณฑิต ภาควิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2546 จากนั้นได้ศึกษาต่อในหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมไฟฟ้า ภาควิชาวิศวกรรมไฟฟ้า ที่จุฬาลงกรณ์มหาวิทยาลัย เมื่อ พ.ศ. 2546