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

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.