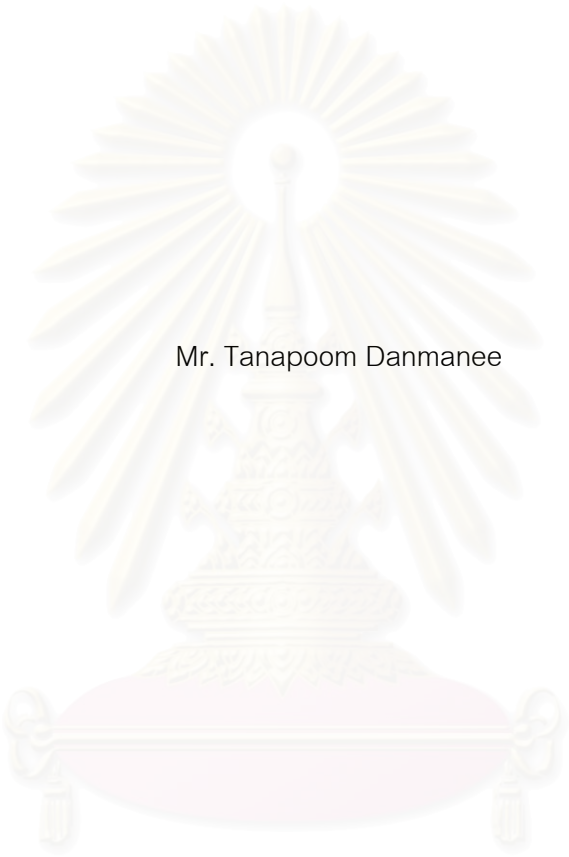
การเพิ่มความถูกต้องวิธีการนับจำนวนเครื่องที่ผ่านการแปลงที่อยู่เครือข่ายบนเครือข่ายขนาดกลาง โดยใช้ข้อมูลสารสนเทศของชั้นการรับส่งข้อมูล

นายธนาภูมิ แดนมณี

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2551

A REFINED TECHNIQUE FOR COUNTING NATTED HOSTS ON MEDIUM-SIZED NETWORKS USING TRANSPORT-LAYER INFORMATION

Mr. Tanapoom Danmanee



A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science Program in Computer Science

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2008

หัวข้อวิทยานิพนธ์	การเพิ่มความถูกต้องวิธีการนับจำนวนเครื่องที่ผ่านการแปลงที่อยู่เครือข่ายบนเครือข่ายขนาดกลางโดยใช้ข้อมูลสารสนเทศของชั้นการรับส่งข้อมูล
โดย	นายธนาภูมิ แดนมณี
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์ ดร.เฉลิมเอก อินทนากรวิวัฒน์

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดี คณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร. บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ผู้ช่วยศาสตราจารย์ ดร.เฉลิมเอก อินทนากรวิวัฒน์)

..... กรรมการภายนอกมหาวิทยาลัย
(รองศาสตราจารย์ ดร.อนันต์ ผลเพิ่ม)

..... กรรมการ
(อาจารย์ ดร.เกริก ภิรมย์โสภา)

ธนาภูมิ แดนมณี : การเพิ่มความถูกต้องวิธีการนับจำนวนเครื่องที่ผ่านการแปลงที่อยู่เครือข่ายบนเครือข่ายขนาดกลางโดยใช้ข้อมูลสารสนเทศของชั้นการรับส่งข้อมูล(A REFINED TECHNIQUE FOR COUNTING NATTED HOSTS ON MEDIUM-SIZED NETWORKS USING TRANSPORT-LAYER INFORMATION) อ. ที่ปรึกษาวิทยานิพนธ์หลัก : ผศ.ดร.เฉลิมเอก อินทนากรวิวัฒน์, 54 หน้า.

การแปลงที่อยู่เครือข่ายคือวิธีการใช้หมายเลขที่อยู่ไอพีสาธารณะร่วมกันของกลุ่มเครื่องลูกข่ายในเครือข่ายส่วนบุคคล ถึงแม้ว่าวิธีนี้จะเป็นที่นิยมก็ตาม วิธีนี้ได้สร้างความยากลำบากต่อการบริหารจัดการเครือข่ายของผู้ให้บริการเชื่อมต่อเครือข่ายจำนวนมาก เนื่องจากเครื่องลูกข่ายจำนวนมากที่เชื่อมต่อเครือข่ายจะเสมือนว่าเป็นเครื่องเดียวกัน เพื่อแก้ไขปัญหานี้ ผู้วิจัยจึงได้นำเสนอขั้นตอนวิธีการนับจำนวนเครื่องที่ผ่านการแปลงที่อยู่เครือข่าย โดยขั้นตอนวิธีที่เสนอเป็นขั้นตอนวิธีที่เพิ่มความถูกต้องของวิธีการนับจำนวนเครื่องที่ผ่านการแปลงที่อยู่เครือข่าย บนเครือข่ายขนาดกลางโดยใช้ข้อมูลสารสนเทศของชั้นการรับส่งข้อมูล มาเพิ่มเติมจากขั้นตอนวิธีการเดิมที่มีอยู่แล้ว ขั้นตอนวิธีที่เสนอได้รับการพัฒนาและทดสอบบนเครือข่ายจริง ผลการทดสอบของงานวิจัยระบุว่า ขั้นตอนวิธีที่เสนอนั้นใช้ได้จริงภายใต้สภาวะแวดล้อมที่ใช้ในการทดลอง

ภาควิชา...วิศวกรรมคอมพิวเตอร์... ลายมือชื่อนิสิต...ธนาภูมิ แดนมณี...
สาขาวิชา...วิทยาศาสตร์คอมพิวเตอร์... ลายมือชื่ออ.ที่ปรึกษาวิทยานิพนพนธ์...
ปีการศึกษา...2551...

4971429221 : MAJOR COMPUTER SCIENCE

KEY WORD: NETWORK ADDRESS TRANSLATION / NAT / TECHNIQUE

TANAPOOM DANMANEE : A REFINED TECHNIQUE FOR COUNTING NATTED HOSTS ON MEDIUM-SIZED NETWORKS USING TRANSPORT-LAYER INFORMATION. THESIS PRINCIPAL ADVISOR : ASST. PROF. CHALERMEK INTANAGORWIWAT, Ph.D., 54 pp.

Network Address Translation (NAT) is a popular technique for sharing a public IP address among several hosts in a private network. Despite its popularity, NAT leads to difficulty in network management for several network adminisatrator as several hosts appear as one host in the network. To address this problem, we propose a refined technique for counting natted hosts on medium-sized networks using transport-layer information. Our technique has been implemented and tested on real networks. Our preliminary result indicates that our technique is viable under environments used in our experiment.

Department: Computer Engineering ..... Student's Signature: .....

Field of Study: Computer Science ..... Principal Advisor's Signature: .....

Academic Year: 2008 .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยความอนุเคราะห์อย่างดียิ่งของท่านผู้ช่วยศาสตราจารย์ ดร.เฉลิมเอก อินทนากรวิวัฒน์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งท่านได้สละเวลาให้ความรู้ ให้คำปรึกษา ตรวจสอบ ให้คำแนะนำแนวทางการวิจัย และสนับสนุนเป็นอย่างดี จนทำให้การวิจัยในครั้งนี้สำเร็จออกมาด้วยดี

ขอขอบพระคุณ อาจารย์ ดร.ยรรยง เต็งอำนวย อาจารย์ ดร.เกริก ภิรมย์โสภา และรองศาสตราจารย์ ดร.อนันต์ ผลเพิ่ม กรรมการสอบวิทยานิพนธ์ ที่กรุณาเสียสละเวลา ให้คำแนะนำตรวจสอบ และแก้ไขวิทยานิพนธ์ฉบับนี้

ขอกราบขอบพระคุณ คุณพ่อ-คุณแม่ ที่ให้การสนับสนุนและเป็นกำลังใจที่ดีเสมอมา

ท้ายที่สุด ผู้วิจัยขอขอบคุณเพื่อนๆ ทุกๆ คน ที่คอยติดตามและให้กำลังใจ รวมถึงท่านอื่นๆ ที่มิได้กล่าวชื่อไว้ ณ ที่นี้ที่มีส่วนทำให้วิทยานิพนธ์สำเร็จได้ด้วยดี

สารบัญ

หน้า

สารบัญตาราง

หน้า

สารบัญภาพ

หน้า

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

การสื่อสารผ่านเครือข่ายคอมพิวเตอร์ในปัจุบัน เป็นที่ยอมรับแล้วว่า ต้องใช้อินเทอร์เน็ตโพรโทคอล[1] เป็นมาตรฐาน ซึ่งการสื่อสารในวิธีการนี้จำเป็นต้องใช้เลขที่อยู่ไอพีเป็นหมายเลขประจำเครื่องคอมพิวเตอร์ อีกทั้งปัจุบันนี้อินเทอร์เน็ตเข้ามาบทบาทในการสื่อสารผ่านเครือข่ายอย่างมาก และจากหมายเลขที่อยู่ไอพีนั้นมีจำนวนจำกัด จึงต้องมีวิธีการเพื่อช่วยไม่ให้หมายเลขที่อยู่ไอพีถูกใช้จนหมด

จากการใช้งานระบบเครือข่ายโดยทั่วไปนั้น ในบางครั้งก็ไม่จำเป็นที่จะต้องเชื่อมต่อกับเครือข่ายอื่นๆ เลย ดังตัวอย่างเช่นเครือข่ายภายในบริษัท ซึ่งจะติดต่อสื่อสารกันเฉพาะภายในบริษัทเท่านั้น จึงไม่มีความจำเป็นต้องติดต่อกับบริษัทอื่นๆ หรือเครือข่ายภายนอก แต่การติดต่อสื่อสารเพื่อใช้งานโปรแกรมประยุกต์ต่างๆ ก็ยังจำเป็นต้องใช้หมายเลขที่อยู่ไอพีอยู่ ปัญหาที่เกิดขึ้นคือถ้ามีการจัดแบ่งหมายเลขที่อยู่ไอพีที่มีอยู่ให้กับเครือข่ายในลักษณะนี้ จะทำให้เกิดปัญหาหมายเลขที่อยู่ไอพีมีจำนวนไม่เพียงพอ นอกจากนี้การตรวจสอบและการจัดสรรหมายเลขที่อยู่ไอพีจะทำได้ยาก รวมถึงการรักษาความปลอดภัยในเครือข่ายจะทำได้ยากขึ้นด้วย

จากปัญหาดังกล่าวมาองค์กรที่มีชื่อว่า ไอเอเน็นเอ (IANA: Internet Assigned Number Authority) ซึ่งเป็นผู้รับผิดชอบ ดูแลในการจัดสรรหมายเลขที่อยู่ไอพีให้กับผู้ใช้งานทั่วโลก ได้กำหนดช่วงของเลขที่อยู่ไอพีที่ทุกๆ คนสามารถนำไปใช้ได้โดยไม่จำเป็นต้องขึ้นทะเบียนก่อนเรียกว่า ช่วงส่วนบุคคล (Private IP) ซึ่งหมายเลขที่อยู่ไอพีในช่วงนี้จะไม่สามารถนำมาเชื่อมต่อกับเครือข่ายอื่นๆ ได้โดยตรง

ช่วงของหมายเลขที่อยู่ไอพีที่เป็นช่วงส่วนบุคคลนั้น จะแบ่งเป็น 3 กลุ่มด้วยกันคือ

(1) ช่วงหมายเลข 10.0.0.0 – 10.255.255.255 (10 / 8)

(2) ช่วงหมายเลข 172.16.0.0 – 172.32.255.255 (172.16 / 12)

(3) ช่วงหมายเลข 192.168.0.0 – 192.168. 255.255 (192.168 / 16)

ซึ่งจากที่มีหมายเลขที่อยู่ไอพีส่วนบุคคล เป็นสาเหตุที่ทำให้เกิดวิธีการแปลงที่อยู่เครือข่าย (NAT: Network Address Translation) [2] ซึ่งการแปลงที่อยู่เครือข่ายนั้นเกิดจากความคิดที่จะนำหมายเลขที่อยู่ไอพีส่วนบุคคล ซึ่งเป็นหมายเลขที่อยู่ไอพีที่ใช้สำหรับเครือข่ายเฉพาะ ซึ่งไม่สามารถใช้งานข้ามเครือข่ายได้ให้นำมาใช้งานข้ามเครือข่ายได้ ซึ่งจากการที่นำวิธีการแปลงที่อยู่

เครือข่ายมาใช้งาน ทำให้เกิดผลพลอยได้ ที่ทำให้ระบบเครือข่ายเฉพาะมีความปลอดภัยมากขึ้น อีกทั้งยังเป็นการแก้ปัญหาเรื่องหมายเลขที่อยู่ไอพีที่มีจำนวนจำกัดลงได้

และจากการศึกษาวิธีการแปลงที่อยู่เครือข่าย จะพบว่าเป็นการยากที่จะสามารถตรวจสอบและวิเคราะห์หาจำนวนเครื่องคอมพิวเตอร์ที่ใช้งานผ่านวิธีการแปลงที่อยู่เครือข่าย จากภายนอกเครือข่ายเฉพาะ ซึ่งการที่ทราบจำนวนเครื่องคอมพิวเตอร์ที่ใช้งานผ่านวิธีการแปลงที่อยู่เครือข่ายจากภายนอก จะทำให้ผู้ให้บริการการเชื่อมต่อระบบสามารถวิเคราะห์หาปัญหาเรื่องการเกิดคอขวดในระบบ หรืออาจจะนำไปใช้หาการบุกรุกเครือข่ายเฉพาะที่อาศัยวิธีการแปลงที่อยู่เครือข่ายจากหมายเลขที่อยู่ไอพีที่เชื่อถือได้ และอีกทั้งยังมีงานวิจัยที่เกี่ยวข้องกับการหาโครงสร้างของเครือข่าย[13], งานวิจัยที่เกี่ยวกับการหาแผนที่ของระบบอินเทอร์เน็ต[14] ที่สามารถนำงานวิจัยส่วนนี้ไปเพิ่มเติมให้มีความถูกต้องเพิ่มเติ่มขึ้นได้ จากเหตุผลดังกล่าว จึงมีงานวิจัยนี้ที่ผู้เขียนจะนำเสนอวิธีการที่จะตรวจสอบหาจำนวนคอมพิวเตอร์ที่ใช้งานการเชื่อมเครือข่ายโดยผ่านวิธีการแปลงที่อยู่เครือข่ายจากภายนอกเครือข่ายเฉพาะ

1.2 วัตถุประสงค์ของการวิจัย

เพื่อออกแบบกระบวนการที่ใช้การตรวจสอบ เครือข่ายส่วนบุคคลที่ทำการผ่านวิธีการแปลงที่อยู่เครือข่าย โดยจะทำการตรวจสอบเครือข่ายส่วนบุคคลขนาดกลาง จากภายนอกเครือข่ายส่วนบุคคลนั้น โดยจะมีการตรวจสอบในช่วงเวลาหนึ่งๆ หรือณ.เวลานั้น ว่ามีเครื่องที่ผ่านวิธีการแปลงที่อยู่เครือข่ายมาใช้บริการนอกเครือข่ายเป็นจำนวนเท่าไร ซึ่งสามารถทำการตรวจสอบโดยการใช้กระบวนการที่นำเสนอเพิ่มเติมเข้าไปใหม่ โดยการใช้ข้อมูลระดับชั้นการรับส่งข้อมูล (Transport Layer) มาใช้แก้ปัญหาเพิ่มเติมในส่วนที่ใช้ข้อมูลระดับเครือข่าย (Network Layer) เพียงอย่างเดียวทำไม่ได้

1.3 ขอบเขตของการวิจัย

1. การตรวจสอบเครื่องโดยใช้ข้อมูลระดับเครือข่าย จะทำการตรวจสอบเฉพาะในข้อมูลส่วนหัวของอินเทอร์เน็ตโพรโทคอลเท่านั้น
2. การตรวจสอบเครื่องโดยใช้ข้อมูลระดับชั้นการรับส่งในงานวิจัยนี้ จะทำการตรวจสอบเฉพาะโพรโทคอล ทีซีพีโพรโทคอล และยูดีพีโพรโทคอล
3. งานวิจัยนี้ใช้ข้อมูลที่ทำการบันทึกจากข้อมูลเครือข่ายจริงที่มีการเปรียบเทียบจากเครือข่ายส่วนบุคคล และเครือข่ายภายนอก โดยได้กำหนดขนาดของเครือข่ายที่ใช้ระดับกลาง โดยขนาดของเครื่องลูกข่ายในเครือข่ายมีจำนวนน้อยกว่า 40 เครื่อง

4. งานวิจัยมีระดับขั้นของการแปลงที่อยู่เครือข่ายในระดับชั้นเดียว ไม่ได้รองรับการแปลงที่อยู่เครือข่ายที่มีระดับชั้นซ้อนลงไป
5. งานวิจัยนี้มีการทดสอบกับระบบปฏิบัติการของโฮสต์ที่เป็น Windows XP, Linux (Kernel 2.6), Solaris , OSX และ Windows Mobile 2003
6. งานวิจัยนี้ใช้วิธีการแปลงที่อยู่เครือข่ายแบบเปลี่ยนแปลงเลขหมายพอร์ต
7. งานวิจัยนี้ได้มีการวัดผลของงานวิจัยเป็นเปอร์เซนต์ความถูกต้อง โดยได้มีการวัดผลบวกลวง และผลลบลวง เพื่อวัดความถูกต้องของงานวิจัย

1.4 ขั้นตอนและวิธีดำเนินการวิจัย

1. ศึกษาเทคนิคต่างๆ ที่เกี่ยวข้องกับการแปลงที่อยู่เครือข่าย
2. ศึกษางานวิจัยที่เกี่ยวข้อง แล้วทำตรวจสอบเพื่อหาความถูกต้องในการตรวจสอบหาจำนวนเครื่อง
3. ศึกษาหาแนวทาง ที่จะเพิ่มขีดความสามารถในการตรวจสอบหาจำนวนเครื่อง
4. ออกแบบขั้นตอนวิธี(Algorithm)ใหม่ที่ใช้ในการตรวจสอบหาจำนวนเครื่อง
5. ทำการสร้างเครื่องมือในการช่วยวิเคราะห์ขั้นตอนวิธีใหม่ เพื่อหาความถูกต้องในการหาจำนวนเครื่อง
6. ทำการเก็บข้อมูลในเครือข่ายจริง เพื่อนำมาใช้ตรวจสอบขั้นตอนวิธีใหม่ที่นำเสนอ
7. ทำการวิเคราะห์ผลเปรียบเทียบระหว่างขั้นตอนวิธีการเก่า และขั้นตอนวิธีการใหม่เพื่อหาค่าความถูกต้อง
8. สรุปผลการทำวิจัยและจัดทำวิทยานิพนธ์เป็นรูปเล่ม

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. ทำให้สามารถวิเคราะห์เครือข่ายส่วนบุคคลบนเครือข่ายขนาดกลาง โดยสามารถตรวจสอบจากภายนอกครือข่ายส่วนบุคคล
2. สามารถนำวิธีการนี้ไปใช้เป็นเครื่องมือช่วยในการตรวจสอบหาจำนวนเครื่องคอมพิวเตอร์ที่ผ่านการแปลงที่อยู่เครือข่าย เพื่อนำไปวิเคราะห์ผลหาโครงสร้างเครือข่ายของอินเทอร์เน็ตได้
3. สามารถนำวิธีการนี้ไปหาผู้ที่บุกรุกเครือข่าย โดยใช้วิธีการแปลงที่อยู่เครือข่ายได้

1.6 ลำดับการจัดเรียงเนื้อหาในวิทยานิพนธ์

วิทยานิพนธ์นี้แบ่งเนื้อหาออกเป็น 5 บทดังต่อไปนี้ บทที่ 1 เป็นบทนำซึ่งกล่าวถึง ความเป็นมาและความสำคัญของปัญหา รวมถึงวัตถุประสงค์ของการวิจัย บทที่ 2 กล่าวถึงทฤษฎีพื้นฐานและงานวิจัยที่เกี่ยวข้องในงานวิจัยนี้ บทที่ 3 กล่าวถึงการออกแบบขั้นตอนวิธี และขั้นตอนดำเนินงาน บทที่ 4 กล่าวถึงการผลการทดสอบ บทที่ 5 กล่าวถึงสรุปผลการวิจัยและข้อเสนอแนะ

1.7 ผลงานที่ตีพิมพ์จากวิทยานิพนธ์

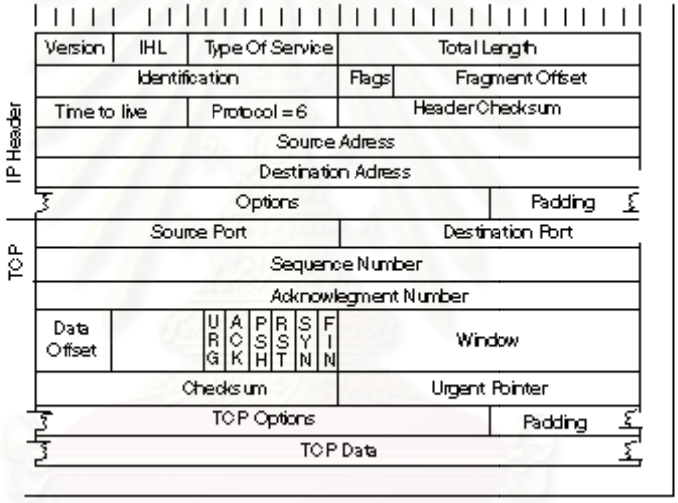
ส่วนหนึ่งของวิทยานิพนธ์นี้ได้รับการตีพิมพ์เป็นบทความทางวิชาการในหัวข้อเรื่อง “วิธีการที่ล่วงรู้ระดับชั้นขนส่งสำหรับนับจำนวนเครื่องที่ผ่านการแปลงที่อยู่เครือข่าย” โดยธนาภูมิ แดนมณี และเฉลิมเอก อินทนากรวิวัฒน์, ในงานประชุมวิชาการ “The 5rd International Joint Conference on Computer Science and Software Engineering (JCSSE 2008)” ณ ห้องประชุม โรงแรมเฟลิกซ์ ริเวอร์ แคว รีสอร์ท จังหวัดกาญจบุรี ระหว่างวันที่ 7-9 พฤษภาคม 2551

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 อินเทอร์เน็ตโพรโทคอล (IP: Internet Protocol)[1][12]

อินเทอร์เน็ตโพรโทคอล[1] เป็นการส่งข้อมูลผ่านเครือข่ายผ่านหมายเลขที่อยู่ไอพี โดยอินเทอร์เน็ตโพรโทคอลได้แบ่งข้อมูลในการส่งออกเป็นส่วนๆ โดยการแบ่งข้อมูลออกเป็นส่วนๆ ในการส่งแต่ละครั้งของการส่งข้อมูล มีส่วนที่สำคัญที่ใช้ในการเก็บข้อมูลรายละเอียดของ เครื่องคอมพิวเตอร์ที่ส่งข้อมูลออกไปในเครือข่าย โดยจัดเก็บในส่วนหัวของข้อมูล (IP Header) ที่ทำการส่งออกไป รายละเอียดชนิดข้อมูลที่ส่งออกไปผ่านเครือข่ายแสดงในรูปที่ 1



รูปที่ 1 แสดงรายละเอียดชนิดข้อมูลของการส่งในอินเทอร์เน็ตโพรโทคอล [5]

2.1.2 การแปลงที่อยู่เครือข่าย (NAT: Network Address Translation)[2][8][9]

การแปลงที่อยู่เครือข่าย[2][8][9] คือวิธีการทางเครือข่ายที่เปลี่ยนค่าหมายเลขที่อยู่ไอพีจากหมายเลขหนึ่งไปเป็นอีกหมายเลขหนึ่ง ซึ่งทำให้เกิดการเชื่อมต่อเครื่องปลายทางได้ โดยเครื่องต้นทางและเครื่องปลายทางไม่จำเป็นต้องเปลี่ยนแปลงการทำงาน หรือค่าต่างๆ ทางเครือข่าย การใช้วิธีการนี้ช่วยทำให้การใช้งานเครือข่ายทำได้อย่างมีประสิทธิภาพมากขึ้นกว่าที่เป็นอยู่ รวมทั้งมีส่วนในการรักษาความปลอดภัยในเครือข่ายได้ด้วย

2.1.2.1 คุณสมบัติของอุปกรณ์การแปลงที่อยู่เครือข่าย

อุปกรณ์เครือข่ายหรือโปรแกรมที่ใช้ในการแปลงที่อยู่เครือข่าย จะต้องมีคุณสมบัติหรือความสามารถในการทำงานต่างๆ ดังต่อไปนี้

(1) สามารถกำหนดหมายเลขที่อยู่ไอพีได้อย่างไร้ร่องรอย (Transparent address assignment) อุปกรณ์ที่จะทำการแปลงที่อยู่เครือข่าย นั้นจะต้องสามารถเปลี่ยนค่าหมายเลขที่อยู่ไอพีของข้อมูลในเครือข่าย ซึ่งเป็นหมายเลขที่อยู่ไอพีในกลุ่มของส่วนบุคคล ให้กลายเป็นหมายเลขที่อยู่ไอพีที่ใช้ในเครือข่ายอินเทอร์เน็ตหรือที่ใช้ในการเชื่อมต่อเครือข่าย และสามารถเปลี่ยนหมายเลขที่อยู่ไอพีที่ใช้ในเครือข่ายอินเทอร์เน็ตหรือที่ใช้ในการเชื่อมต่อเครือข่าย ให้กลายเป็นหมายเลขที่อยู่ไอพีในช่วงส่วนบุคคลได้อย่างถูกต้อง อีกทั้งในบางกรณีอาจจำเป็นที่ต้องมีการเปลี่ยนแปลงค่าข้อมูลในชั้นการควบคุมการรับส่ง (Transport Layer) บางส่วนด้วยเช่น หมายเลขพอร์ตของทีซีพีโพรโทคอล (TCP: Transmission Conttrol Protocol) และหมายเลขพอร์ตของยูดีพีโพรโทคอล (UDP: User Datagram Protocol) ในการเปลี่ยนค่าเลขที่อยู่ไอพีนั้นสามารถทำได้ 2 แบบคือแบบคงที่ และแบบเปลี่ยนแปลงได้

(1.1) การกำหนดค่าหมายเลขที่อยู่ไอพีแบบคงที่ (Static address assignment) เป็นการเปลี่ยนแปลงค่าหมายเลขที่อยู่ไอพี แบบมีการจับคู่ของหมายเลขที่อยู่ไอพีตลอดการทำงานของอุปกรณ์การแปลงที่อยู่เครือข่าย ซึ่งเป็นการทำงานโดยแปลงค่าหมายเลขที่อยู่ไอพีจากส่วนบุคคล เป็นหมายเลขที่อยู่ไอพีภายนอก แบบหนึ่งต่อหนึ่ง

(1.2) การกำหนดค่าเลขที่อยู่ไอพีแบบเปลี่ยนแปลงได้ (Dynamic address Assignment) เป็นการเปลี่ยนแปลงค่าหมายเลขที่อยู่ไอพี โดยมีการจับคู่ของหมายเลขที่อยู่ไอพีส่วนบุคคล กับหมายเลขที่อยู่ไอพีภายนอกเพียงชั่วคราว ซึ่งการใช้งานหมายเลขที่อยู่ไอพีนั้นจะจดจำค่าไว้ตลอดเวลาที่มีการเชื่อมต่อ ซึ่งเมื่อสิ้นสุดการเชื่อมต่อจะมีการเลือกหมายเลขที่อยู่ไอพีใหม่เมื่อการเชื่อมต่อในครั้งใหม่ ซึ่งค่าหมายเลขที่อยู่ไอพีที่ได้ใหม่ไม่จำเป็นที่ต้องเป็นค่าหมายเลขที่อยู่ไอพีเดิม

(2) สามารถส่งผ่านแพ็กเก็ตของข้อมูลที่มีการเปลี่ยนแปลงที่อยู่ได้ (Transparent address routing address transition) เนื่องจากอุปกรณ์การแปลงที่อยู่เครือข่ายนั้นจะทำงานอยู่หมายเลขที่อยู่ไอพี 2 ระบบ คือ หมายเลขที่อยู่ไอพีส่วนบุคคล และหมายเลขที่อยู่ไอพีภายนอก ดังนั้นอุปกรณ์ต้องสามารถทำการส่งผ่านแพ็กเก็ต ที่ไม่ขัดต่อการทำงานของระบบหมายเลขที่อยู่ทั้ง 2 ระบบ และต้องไม่เป็นปัญหาในการหาเส้นทาง และการรับส่งข้อมูลด้วย

(3) สามารถเปลี่ยนแปลงข้อมูลของไอซีเอ็มพีได้ (ICMP error message payload translation) การทำงานในเครือข่ายนั้น เมื่อมีการทำงานที่ผิดพลาดเกิดขึ้นในเครือข่าย จะมีการส่งรายละเอียดต่างๆ ไปกับแพ็กเก็ตไอซีเอ็มพี (ICMP: Internet Control Message Protocol) ซึ่งในกรณีของที่มีการใช้งานการแปลงที่อยู่เครือข่าย เมื่อมีการทำงานผิดพลาดหรือผิดปกติในเครือข่าย อุปกรณ์การแปลงที่อยู่เครือข่ายต้องสามารถทำการเปลี่ยนแปลงข้อมูลในแพ็กเก็ตไอซีเอ็มพีนั้นให้ถูกต้องได้ด้วย

2.1.2.2 **กระบวนการในการเปลี่ยนหมายเลขที่อยู่ไอพี**

กระบวนการในการเปลี่ยนหมายเลขที่อยู่ไอพีที่ใช้ในการแปลงที่อยู่เครือข่าย มีขั้นตอนในการทำงานทั้งหมดอยู่ 3 ขั้นตอนหลัก ดังต่อไปนี้

(1) การทำงานในการจับคู่หมายเลขที่อยู่ไอพี (Address binding) เป็นขั้นตอนที่จะเปลี่ยนหมายเลขที่อยู่ไอพีจาก หมายเลขที่อยู่ไอพีส่วนบุคคล ให้กลายไปเป็นหมายเลขที่อยู่ไอพีภายนอก ซึ่งสามารถทำได้ทั้งแบบ การกำหนดค่าหมายเลขที่อยู่ไอพีแบบคงที่ หรือ การกำหนดค่าหมายเลขที่อยู่ไอพีแบบเปลี่ยนแปลงได้ ซึ่งในการจับคู่นั้นจะไม่มีการเปลี่ยนหมายเลขที่อยู่ไอพีคู่นั้นจนกว่าจะมีการสิ้นสุดการเชื่อมต่อนั้น

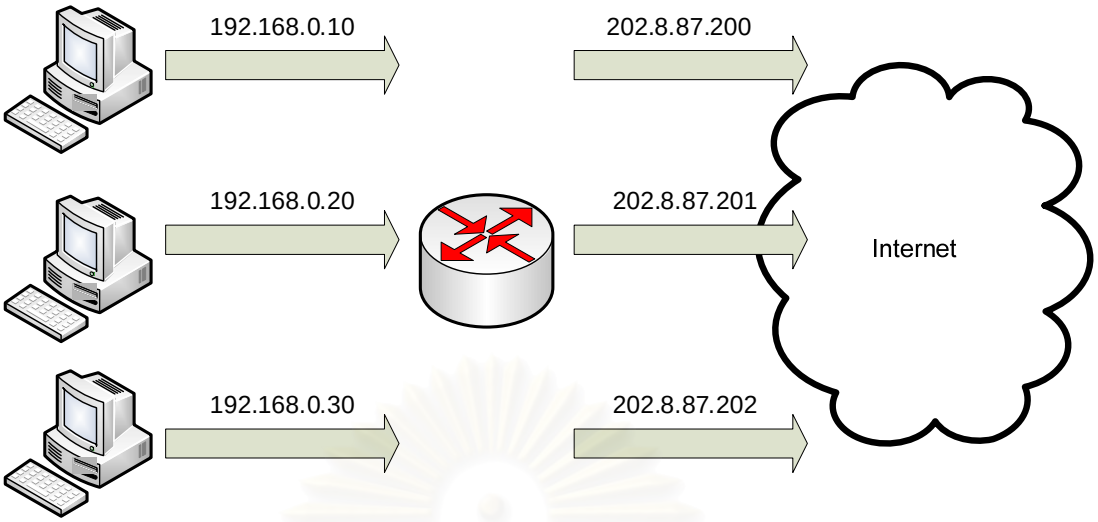
(2) การทำงานขณะมีการเชื่อมต่อแล้ว (Address lookup and translation) เป็นขั้นตอนหลังมีการเชื่อมต่อกันได้แล้ว เมื่อมีการส่งข้อมูลในลำดับถัดมา อุปกรณ์การแปลงที่อยู่เครือข่ายจะมีการเปลี่ยนแปลงหมายเลขที่อยู่ไอพีในข้อมูลนั้น โดยวิธีการค้นหาจากหน่วยความจำว่าเคยจับคู่กับหมายเลขที่อยู่ไอพีอะไร เพื่อส่งผ่านข้อมูลให้ได้ถูกต้อง

(3) การทำงานเมื่อสิ้นสุดการเชื่อมต่อ (Address unbinding) เป็นขั้นตอนเมื่อเกิดการสิ้นสุดการเชื่อมต่อ อุปกรณ์การแปลงที่อยู่เครือข่ายจะมีการตรวจจับการสิ้นสุดการเชื่อมต่อของหมายเลขที่อยู่ไอพีนั้น และลบข้อมูลการจับคู่ออกจากหน่วยความจำ

2.1.2.3 **ลักษณะการทำงานของการแปลงที่อยู่เครือข่าย**

สามารถสรุปลักษณะการทำงานของการแปลงที่อยู่เครือข่ายได้เป็น 4 รูปแบบการทำงานดังต่อไปนี้

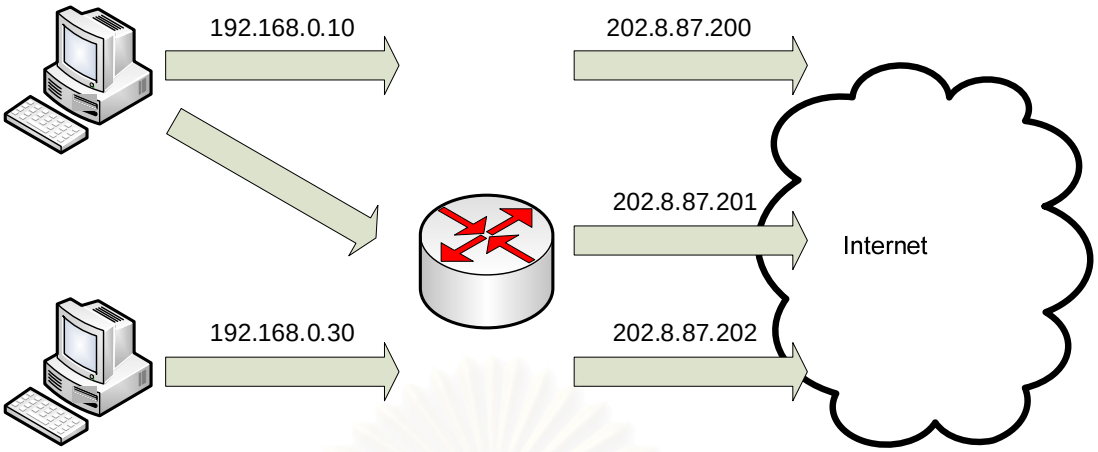
(1) การแปลงที่อยู่เครือข่ายแบบคงที่ (Static NAT) เป็นการทำการแปลงที่อยู่เครือข่ายโดยการทำงานนั้นจะเป็นการจับคู่ระหว่างหมายเลขที่อยู่ไอพีที่เป็น หมายเลขที่อยู่ไอพีส่วนบุคคล กับหมายเลขที่อยู่ไอพีภายนอกในลักษณะหนึ่งต่อหนึ่ง ดังตัวอย่างที่แสดงอยู่ในรูปที่ 2



รูปที่ 2 แสดงตัวอย่างการแปลงที่อยู่เครือข่ายแบบคงที่

(2) การแปลงที่อยู่เครือข่ายแบบเปลี่ยนแปลงได้ (Dynamic NAT)

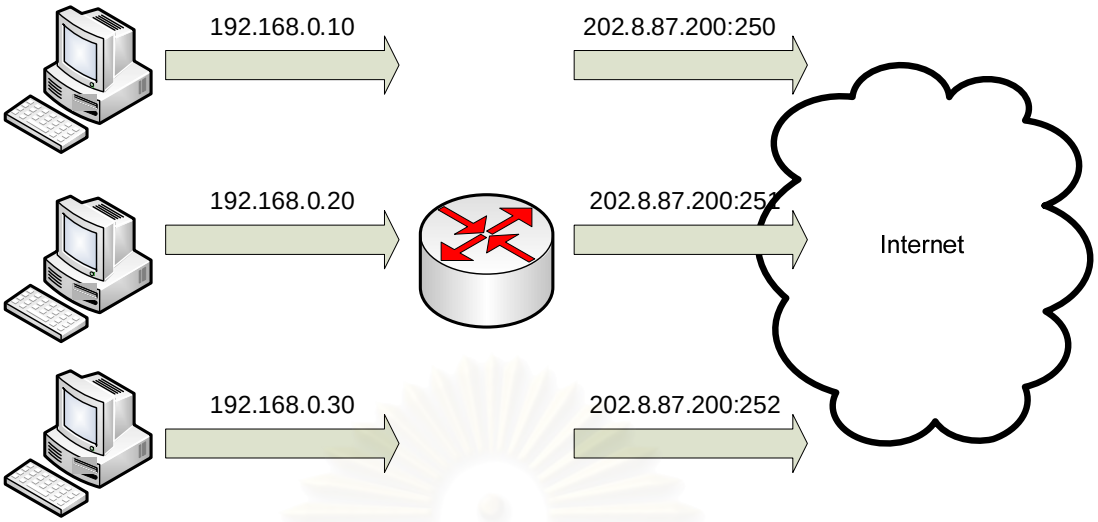
เป็นการทำงานการแปลงที่อยู่เครือข่าย โดยมีการจับคู่ระหว่างหมายเลขที่อยู่ไอพีที่เป็นหมายเลขที่อยู่ไอพีส่วนบุคคล กับหมายเลขที่อยู่ไอพีภายนอกโดยการสุ่มเลือกหมายเลขที่อยู่ไอพีภายนอก ซึ่งการทำงานลักษณะนี้จะช่วยให้เครือข่ายที่มีหมายเลขที่อยู่ไอพีในช่วงหมายเลขที่อยู่ไอพีส่วนบุคคล สามารถติดต่อไปยังเครือข่ายอื่นๆ ได้ แต่การทำการแปลงที่อยู่เครือข่ายแบบเปลี่ยนแปลงได้นี้ เครื่องคอมพิวเตอร์จากภายนอกเครือข่ายจะไม่สามารถติดต่อเข้ามายังเครื่องคอมพิวเตอร์ภายในเครือข่ายได้โดยตรง เนื่องจากเครื่องคอมพิวเตอร์ภายนอกจะไม่สามารถทราบได้เลยว่า หมายเลขที่อยู่ไอพีของเครื่องที่จะเชื่อมต่อด้วยนั้นคือหมายเลขอะไร ซึ่งการทำการแปลงที่อยู่เครือข่ายแบบเปลี่ยนแปลงได้นี้ จึงมีความสามารถที่นำมาใช้เพื่อรักษาความปลอดภัยในเครือข่ายได้ด้วย ซึ่งตัวอย่างการแปลงที่อยู่เครือข่ายแบบเปลี่ยนแปลงได้ ได้แสดงอยู่ในรูปที่ 2



รูปที่ 3 แสดงตัวอย่างการแปลงที่อยู่เครือข่ายแบบเปลี่ยนแปลงได้

(3) การแปลงที่อยู่เครือข่ายแบบเปลี่ยนเลขหมายพอร์ต (Address Port Transalation)

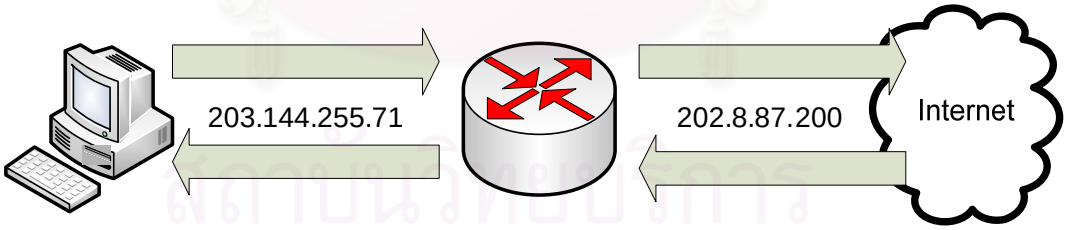
เป็นวิธีการหนึ่งที่ช่วยให้ประหยัดหมายเลขที่อยู่ไอพีคือการนำเอาวิธีการของการแปลงที่อยู่เครือข่ายแบบเปลี่ยนหมายเลขพอร์ตมาใช้ โดยเครื่องลูกข่ายทั้งหมดในเครือข่ายที่มีหมายเลขที่อยู่ไอพีส่วนบุคคลเมื่อมีการเชื่อมต่อไปยังเครือข่ายอื่นๆ จะถูกเปลี่ยนแปลงเป็นหมายเลขที่อยู่ไอพีหมายเลขเดียวกันทั้งหมด แต่มีการเปลี่ยนแปลงหมายเลขพอร์ตต้นทางในการเชื่อมต่อแทน เมื่อมีการตอบกลับจากเครื่องภายนอกเครือข่ายแล้ว อุปกรณ์การแปลงที่อยู่เครือข่าย จะตรวจสอบหมายเลขพอร์ตปลายทางในส่วนหัวของข้อมูลว่าเป็นหมายเลขอะไร แล้วจึงเปลี่ยนข้อมูลส่วนหัวให้ตรงกับเครื่องลูกข่ายที่ทำการร้องขออีกครั้ง ซึ่งตัวอย่างการแปลงที่อยู่เครือข่ายแบบเปลี่ยนเลขหมายพอร์ตที่กล่าวมานี้ได้แสดงอยู่ในรูปที่ 4



รูปที่ 4 แสดงตัวอย่างการแปลงที่อยู่เครือข่ายแบบเปลี่ยนหมายเลขพอร์ต

(4) การแปลงที่อยู่เครือข่ายแบบส่งผ่าน (Overlapping: Twice-NAT)

ในกรณีที่หมายเลขที่อยู่ไอพีในเครือข่าย เป็นหมายเลขที่อยู่ไอพีซึ่งใช้งานอยู่ในเครือข่ายอื่นๆ หรือเป็นหมายเลขที่อยู่ไอพีที่เรานำมาใช้งานกันเอง โดยไม่ได้จดทะเบียนขอใช้งาน เมื่อมีการเชื่อมต่อกับเครือข่ายอื่นๆ จะทำให้เกิดปัญหาขึ้นในระบบเครือข่าย เนื่องจากถ้ามีการรับส่งข้อมูลกันในเครือข่ายจะทำให้เกิดการมีเส้นทางเดินของข้อมูลที่ผิดผลาดเกิดขึ้น แต่การใช้งานในลักษณะนี้ก็ยังสามารถใช้งานได้ ซึ่งตัวอย่างการแปลงที่อยู่เครือข่ายแบบส่งผ่านที่กล่าวมานี้ได้แสดงอยู่ในรูปที่ 5

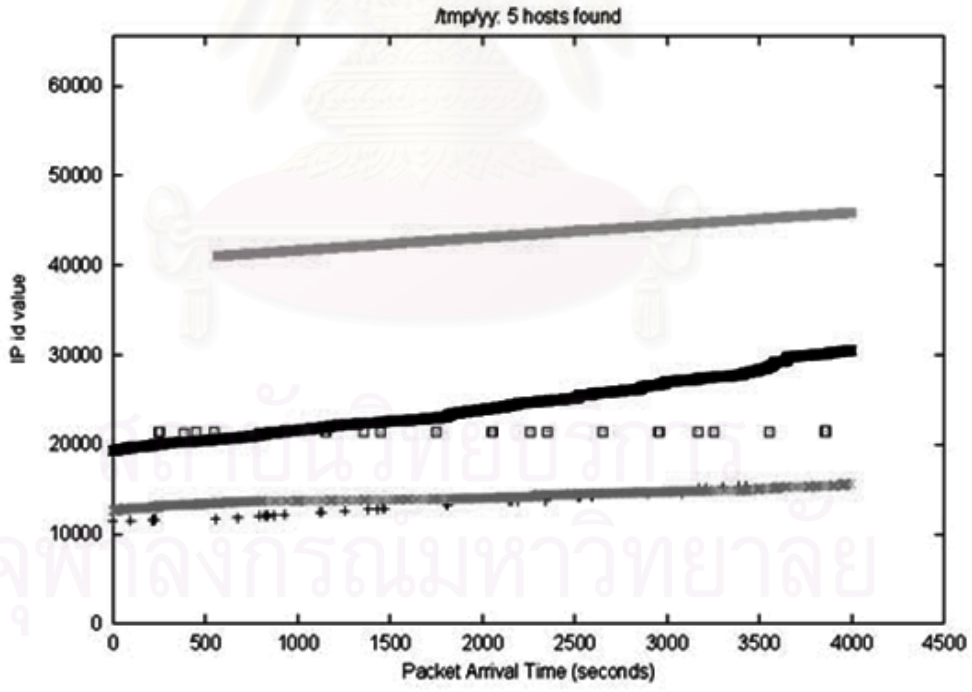


รูปที่ 5 แสดงตัวอย่างการแปลงที่อยู่เครือข่ายแบบส่งผ่าน

2.2 เอกสารและงานวิจัยที่เกี่ยวข้อง

2.2.1 A Technique for Counting NATted Hosts โดย Steven M. Bellovin [3]

งานวิจัยนี้เป็นการค้นหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายออกมา โดยการตรวจสอบข้อมูลของเครือข่าย ในระดับชั้นเครือข่าย (Network Layer) เพียงอย่างเดียว โดยจะนำค่าของ Identification หรือที่เรียกว่า IP id (ซึ่งต่อไปในงานวิจัยนี้จะเรียกค่านี้ว่าไอพีไอดี) ซึ่งเป็นข้อมูลที่บรรจุอยู่ในส่วนหัวของอินเทอร์เน็ตโพรโทคอล ซึ่งค่าดังกล่าวจะถูกนำตรวจสอบโดยการสร้างแผนภูมิเทียบกับเวลาที่รับค่าไอพีไอดีได้จากเครือข่าย ซึ่งค่าไอพีไอดีนั้นเป็นค่าที่ถูกบรรจุในส่วนหัวของอินเทอร์เน็ตโพรโทคอล โดยทั่วไปจะมีขนาด 16 บิต และจะมีการบันทึกเลขลงไปโดยที่เลขนั้นเป็นค่าที่ระบบปฏิบัติการของเครื่องลูกข่ายส่งออกมาโดยการสุ่มเลือกค่าเริ่มต้น แล้วทำการเพิ่มค่าของเลขนั้น จนกระทั้งค่าไอพีไอดีมีเลขขนาดถึง 16 บิต จึงทำการวนเลขกลับมาใช้ใหม่ จากการทดลองพบว่าค่าไอพีไอดีมีการเพิ่มขึ้นอย่างมีแบบแผน [10][12] ดังรูปที่ 6 โดยที่ในแต่ละระบบปฏิบัติการจะมีค่าการเพิ่มขึ้นที่แตกต่างกันด้วย



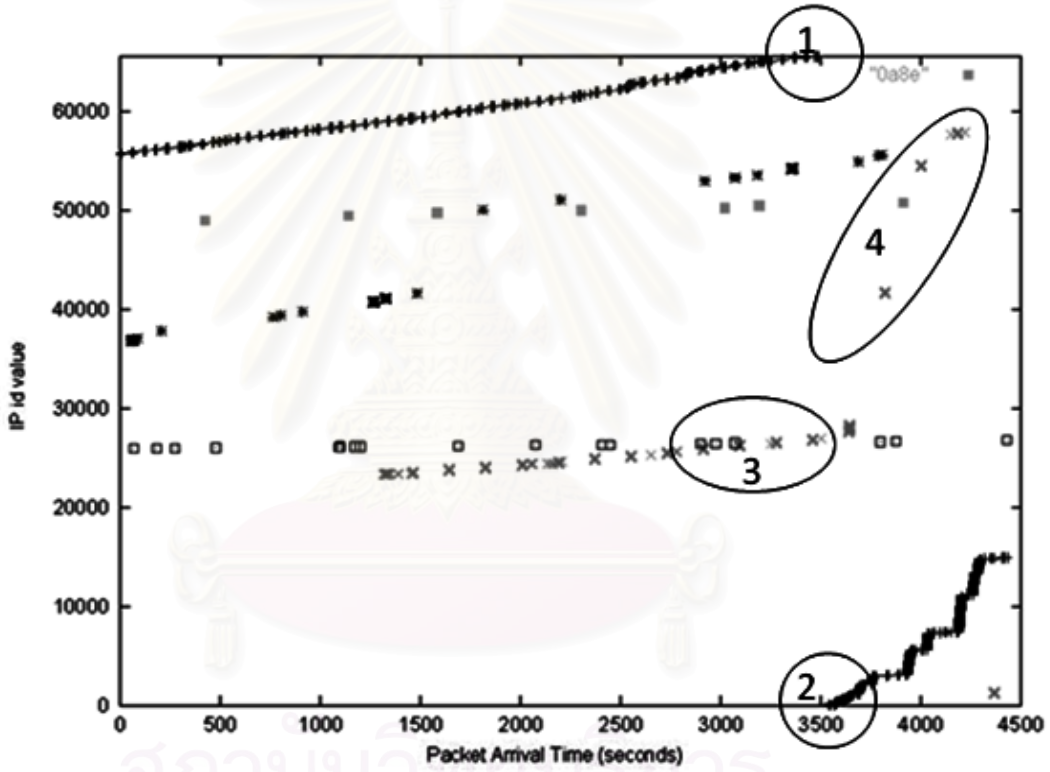
รูปที่ 6 ค่าไอพีไอดีเทียบกับเวลาเพื่อหาจำนวนเครื่อง [3]

จากการค้นพบครั้งนี้ ทำให้สามารถแยกจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายออกมาได้ โดยขั้นตอนวิธีการนี้สามารถทำได้เมื่อมีการรับข้อมูลของค่าไอพีไอดีเป็น

ระยะเวลาหนึ่ง จากรูปที่ 6 จะพบว่าสามารถนับจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายได้จำนวน 5 เครื่อง

ปัญหาที่พบในงานวิจัยนี้

เนื่องจากในข้อมูลค่าไอพีไอดีในส่วนหัวของอินเทอร์เน็ตโพรโทคอลมีความจุเพียง 16 บิต ซึ่งเมื่อระบบปฏิบัติการทำการเพิ่มค่าไปถึง 16 บิต หรือค่าที่ 65536 ทำเกิดการวนค่ามาใช้ใหม่ (Wrap Around) เพื่อนำค่าไอพีไอดีที่ถูกใช้ไปแล้วนำมาใช้ใหม่ ซึ่งในเหตุกรณ์ที่เกิดขึ้นนี้จะทำให้วิธีการนี้ ไม่สามารถหาจำนวนเครื่องที่ผ่านวิธีการแปลงที่อยู่เครือข่ายได้ถูกต้อง ตามรูปตัวอย่างที่ 7 ภายในวงกลมที่ 1 และ 2 แสดงให้เห็นถึงการเกิดการวนค่าไอพีไอดีมาใช้ใหม่



รูปที่ 7 แสดงปัญหาเมื่อระบบปฏิบัติการนำค่าไอพีไอดีมาวนใช้ใหม่ [3]

เนื่องจากวิธีการนี้ใช้ค่าไอพีไอดีในส่วนหัวของอินเทอร์เน็ตโพรโทคอลเพียงอย่างเดียวในระดับชั้นเครือข่ายเท่านั้น จากการตรวจสอบพบว่ามีปัญหาในขั้นตอนวิธีเพิ่มเติมดังต่อไปนี้

เมื่อระบบปฏิบัติการของเครื่องลูกข่ายภายในเครือข่ายส่วนบุคคล จะมีการสุ่มค่าไอพีไอดีที่ใกล้เคียงกันเกิดขึ้น หรือเมื่อเกิดการชนกันของค่าไอพีไอดี จะทำให้เกิดการกลืนกันของค่าไอพีไอดี ซึ่งทำให้ขั้นตอนวิธีการนี้ไม่มีประสิทธิภาพที่เพียงพอในการแยกจำนวนเครื่องลูกข่ายออกจากกัน ดังวงกลมที่ 3 ในรูปที่ 7 จะเห็นได้ว่าในช่วงเวลา 3000 ถึง 3500 วินาที ซึ่งถ้านำช่วงเวลานี้มา

ทดสอบตามวิธีการนี้จะตรวจสอบพบเครื่องลูกข่ายที่ผ่านวิธีการแปลงที่อยู่เครือข่ายจำนวน 1 เครื่อง ทั้งที่ในความเป็นจริงแล้ว มีเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายอยู่ 2 เครื่อง และในความเป็นจริงแล้วเครือข่ายส่วนบุคคลไม่ได้มีการใช้งานข้ามเครือข่ายเพียงอย่างเดียวทั้งยังมีการใช้ในเครือข่ายส่วนบุคคลนั้นด้วย ซึ่งในกรณีนี้จะทำให้ค่าไอพีไอดีที่ตรวจสอบเกิดการกระโดด ดังในวงกลมที่ 4 เป็นเหตุให้วิธีการนี้ไม่สามารถนำมาใช้ได้

2.2.2 Passive Fingerprinting โดย Honeynet Project [4]

งานวิจัยนี้เป็นการตรวจสอบค่าทีทีแอล (TTL: Time To Leave) และค่าทีโอเอส (TOS: Type Of Service) ในข้อมูลส่วนหัวของอินเทอร์เน็ตโพรโทคอลในระดับชั้นเครือข่าย และค่าขนาดของวินโดว์ (Window Size) ของทีซีพีโพรโทคอลในระดับชั้นการรับส่งข้อมูล ซึ่งในงานวิจัยชิ้นนี้จะพบว่าระบบปฏิบัติการในเครื่องลูกข่ายที่มีระบบปฏิบัติการที่แตกต่างกันจะมีค่ามาตรฐาน ทีทีแอล ทีโอเอส และขนาดวินโดว์ ที่ส่งออกมาในข้อมูลส่วนหัวของอินเทอร์เน็ตโพรโทคอลและทีซีพีโพรโทคอลที่แตกต่างกัน ซึ่งในขั้นตอนวิธีการนี้จะทำให้สามารถระบุระบบปฏิบัติการของเครื่องลูกข่ายที่ส่งข้อมูลออกมาได้ โดยอาศัยค่ามาตรฐาน ทีทีแอล ทีโอเอส และขนาดของวินโดว์ โดยค่ามาตรฐานของระบบปฏิบัติการต่างๆ ที่ตรวจสอบพบจากงานวิจัยนี้ได้แสดงอยู่ในตารางที่ 1

ตารางที่ 1 ค่ามาตรฐาน ทีทีแอล ทีโอเอส และขนาดวินโดว์ที่ระบบปฏิบัติการต่างๆ ใช้

OS	VERSION	PLATFORM	TTL	WINDOW	DF	TOS
DC-OSx	1.1-95	Pyramid/NILE	30	8192	N	0
Windows	9x/NT	Intel	32	5000-9000	Y	0
NetApp	OnTap	5.1.2-5.2.2	54	8760	Y	0
HPJetDirect	?	HP_Printer	59	2100-2150	N	0
AIX	4.3.x	IBM/RS6000	60	16000-16100	Y	0
AIX	4.2.x	IBM/RS6000	60	16000-16100	N	0
Cisco	11.2	7507	60	65535	Y	0
DigitalUnix	4	Alpha	60	33580	Y	16
IRIX	6.x	SGI	60	61320	Y	16
OS390	2.6	IBM/S390	60	32756	N	0
Reliant	5.43	Pyramid/RM1000	60	65534	N	0
FreeBSD	3.x	Intel	64	17520	Y	16
JetDirect	G.07.x	J3113A	64	5804-5840	N	0
Linux	2.2.x	Intel	64	32120	Y	0
OpenBSD	2.x	Intel	64	17520	N	16
OS/400	R4.4	AS/400	64	8192	Y	0
SCO	R5	Compaq	64	24820	N	0
Solaris	8	Intel/Sparc	64	24820	Y	0
FTX(UNIX)	3.3	STRATUS	64	32768	N	0
Unisys	X	Mainframe	64	32768	N	0
Netware	4.11	Intel	128	32000-32768	Y	0
Windows	9x/NT	Intel	128	5000-9000	Y	0
Windows	2000	Intel	128	17000-18000	Y	0
Cisco	12	2514	255	3800-5000	N	192
Solaris	2.x	Intel/Sparc	255	8760	Y	0

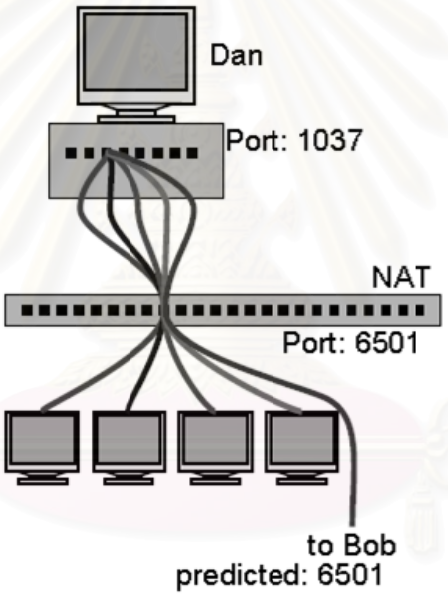
2.2.3 Characterization and Measurement of TCP Tracersal through NATs and Firewalls **โดย** Saikat Guha **และ** Paul Francis [16]

งานวิจัยนี้เป็นการศึกษาคุณสมบัติของอุปกรณ์การแปลงที่อยู่เครือข่ายโดยเป็นการทดสอบอุปกรณ์การแปลงที่อยู่เครือข่าย เพื่อดูคุณสมบัติของอุปกรณ์การแปลงที่อยู่เครือข่ายที่สามารถรองรับการใช้งาน สตันโพรโทคอล (Protocol STUNT) [15]

สตันโพรโทคอล เป็นโพรโทคอลที่ออกแบบให้สนับสนุนการเชื่อมต่อระหว่างเครื่องลูกข่ายที่อยู่หลังอุปกรณ์การแปลงที่อยู่เครือข่ายทั้งสองเครื่องลูกข่ายเชื่อมเข้าหากันได โดยใช้ทีซีพีโพรโทคอลเป็นโพรโทคอลระดับชั้นการรับส่งข้อมูล และจะต้องไม่มีการขัดขวางการเชื่อมต่อจากอุปกรณ์การแปลงที่อยู่เครือข่าย

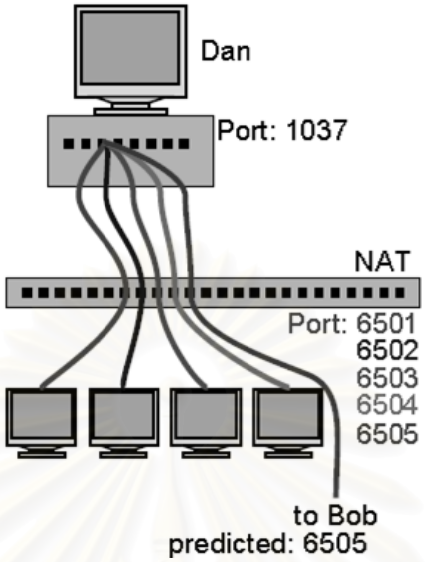
ซึ่งในงานวิจัยนี้สิ่งที่เกี่ยวข้องเป็นเรื่องการที่อุปกรณ์การแปลงที่อยู่เครื่องข่ายมีพฤติกรรมการเปิดพอร์ตที่ใช้งานในการเชื่อมต่อจากอุปกรณ์การแปลงที่อยู่เครือข่ายเข้ากับเครื่องลูกข่ายที่สามารถจำแนกวิธีการเปิดพอร์ตได้ โดยงานวิจัยนี้ได้จำแนกพฤติกรรมการเปิดพอร์ตเชื่อมต่อได้ดังต่อไปนี้

(1) กรณีที่ทุกการเชื่อมต่อจากทุกเครื่องลูกข่ายภายใต้อุปกรณ์การแปลงที่อยู่เครือข่ายเดียวกันจะทำการเชื่อมต่อโดยใช้หมายเลขพอร์ตเดิมทุกครั้ง เมื่อเชื่อมต่อข้อมูลไปยังจุดหมายปลายทางเดียวกัน และหมายเลขพอร์ตปลายทางเดียวกัน ดังตัวอย่างที่แสดงในรูปที่ 8 และจากงานวิจัยนี้จะพบว่าพฤติกรรมของอุปกรณ์การแปลงที่อยู่เครือข่ายที่มีลักษณะนี้ จะมีประมาณ 5% ของอุปกรณ์การแปลงที่อยู่เครือข่ายที่มีจำหน่ายทั่วไป



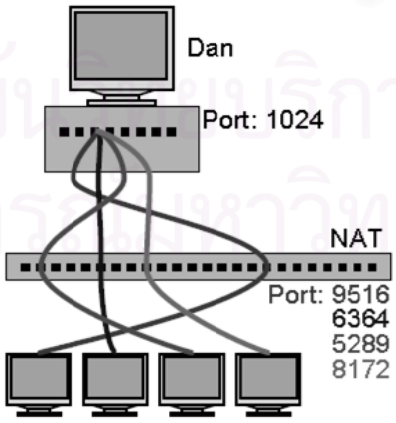
รูปที่ 8 การใช้หมายเลขพอร์ตของอุปกรณ์การแปลงเครือข่ายแบบซ้ำๆ

(2) กรณีที่ทุกการเชื่อมต่อจากทุกเครื่องลูกข่ายภายใต้อุปกรณ์การแปลงที่อยู่เครือข่ายเดียวกันจะทำเลือกหมายเลขพอร์ตที่ทำการเชื่อมต่อเรียงลำดับกันไป เมื่อเชื่อมต่อข้อมูลไปยังจุดหมายปลายทางเดียวกัน และหมายเลขพอร์ตปลายทางเดียวกัน ดังแสดงในรูปตัวอย่างที่ 9 และจากงานวิจัยนี้พบว่าพฤติกรรมของอุปกรณ์การแปลงที่อยู่เครือข่ายที่มีลักษณะนี้ มีประมาณ 95% ของอุปกรณ์การแปลงที่อยู่เครือข่ายที่มีจำหน่ายทั่วไป



รูปที่ 9 การใช้หมายเลขพอร์ตของอุปกรณ์การแปลงเครือข่ายแบบเรียงลำดับ

(3) กรณีที่ทุกการเชื่อมต่อจากทุกเครื่องลูกข่ายภายใต้อุปกรณ์การแปลงที่อยู่เครือข่ายเดียวกันจะทำเลือกหมายเลขพอร์ตที่ทำการเชื่อมต่อโดยการสุ่มค่าหมายเลขพอร์ต เมื่อเชื่อมต่อข้อมูลไปยังจุดหมายปลายทางเดียวกัน และหมายเลขพอร์ตปลายทางเดียวกัน ดังตัวอย่างที่แสดงในรูปที่10 และจากงานวิจัยชิ้นนี้พบว่าพฤติกรรมของอุปกรณ์การแปลงที่อยู่เครือข่ายที่มีลักษณะนี้ มีน้อยกว่าประมาณ 1% ของอุปกรณ์การแปลงที่อยู่เครือข่ายที่มีจำหน่ายโดยทั่วไป



รูปที่ 10 การใช้หมายเลขพอร์ตของอุปกรณ์การแปลงเครือข่ายแบบสุ่มค่า

บทที่ 3
ขั้นตอนการดำเนินงานวิจัย

จากงานวิจัยที่ผ่านมา พบว่ามีการใช้ของข้อมูลส่วนหัวของอินเทอร์เน็ตโพรโทคอลในระดับชั้นเครือข่ายเพียงอย่างเดียวในการตรวจสอบ ซึ่งพบว่าข้อมมูลที่นำมาใช้ยังไม่เพียงพอที่จะนำมาใช้ในการแยกเครื่องลูกข่ายที่ผ่านวิธีการแปลงที่อยู่เครือข่ายได้ถูกต้องเพียงพอ อีกทั้งยังไม่สามารถแยกเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่าย ณ เวลานั้นได้ในทันทีเพราะยังต้องอาศัยปริมาณข้อมูลที่มีจำนวนมากเพียงพอในการแยกเครื่องลูกข่าย ในงานวิจัยนี้จึงได้มีแนวคิดที่จะเสนอขั้นตอนวิธีการเพิ่มขีดความสามารถในการตรวจสอบหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายบนเครือข่ายขนาดกลางโดยใช้ข้อมูลสารสนเทศของชั้นการรับส่งข้อมูล

3.1 การเพิ่มขีดความสามารถในการตรวจสอบหาจำนวนเครื่องลูกข่ายที่ผ่านเครือข่าย

จากการที่งานวิจัยที่ผ่านมาใช้เพียงข้อมูลในระดับชั้นเครือข่ายเพียงอย่างเดียวนั้น ซึ่งทำให้การหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายมีข้อจัดกัดบ้างประการ ในงานวิจัยนี้จึงได้มีการนำข้อมูลสารสนเทศในส่วนระดับชั้นการรับส่งข้อมูลมาเพิ่มขีดความสามารถในการหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่าย

ซึ่งโพรโทคอลที่ใช้ในการรับส่งข้อมูลเครือข่ายที่นำมาใช้ในงานวิจัยนี้ได้แก่ ยูดีพีโพรโทคอล (UDP: User Datagram Protocol) และ ทีซีพีโพรโทคอล (TCP: Transmission Control Protocol) โดยโพรโทคอลทั้งสองที่กล่าวมาเป็นโพรโทคอลที่นิยมใช้ในการรับข้อมูลในเครือข่ายที่การใช้อินเทอร์เน็ตโพรโทคอลมากที่สุด โดยขั้นตอนวิธีการที่นำเสนอสามารถแยกตามโพรโทคอลที่ใช้ในระดับชั้นการรับส่งข้อมูลได้ดังต่อไปนี้

(1) กรณีศึกษาการใช้ข้อมูลยูดีพีโพรโทคอล ร่วมกับข้อมูลอินเทอร์เน็ตโพรโทคอล

จากการศึกษาข้อมูลสารสนเทศในเครือข่ายจริง โดยใช้ยูดีพีโพรโทคอลรับส่งข้อมูลจากเครือข่ายส่วนบุคคลออกไปยังเครือข่ายภายนอก โดยผ่านวิธีการแปลงที่อยู่เครือข่าย จะพบว่าขั้นตอนวิธีการแปลงที่อยู่เครือข่ายจะทำการเปลี่ยนแปลงข้อมูลในส่วนหัวของข้อมูล ซึ่งรูปแบบการเปลี่ยนข้อมูลแสดงให้เห็นได้จากรูปที่ 11

Type Of Service	0x0
Identification	9855
Time to live	128
PROTOCOL	UDP
Source Address	192.168.1.102
Destination Address	202.8.87.201
Source Port	1035
Destination Port	53

Type Of Service	0x0
Identification	**9855**
Time to live	127
PROTOCOL	UDP
Source Address	**192.168.0.1**
Destination Address	202.8.87.201
Source Port	**12548**
Destination Port	53

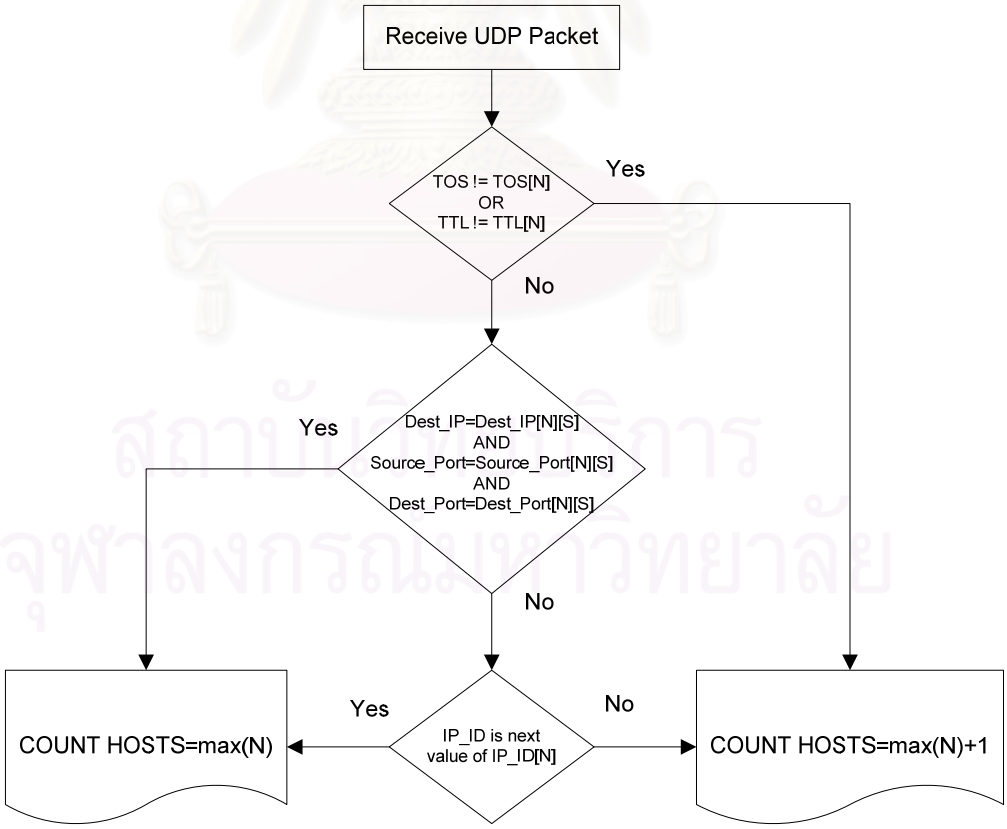
รูปที่ 11 ตัวอย่างข้อมูลสารสนเทศในส่วนหัวของยูดีพีแพ็คเก็ตในกรณีที่ใช้การแปลงที่อยู่เครือข่ายในการเชื่อมต่อจากภายในเครือข่ายส่วนบุคคลไปยังภายนอกเครือข่าย

ซึ่งจากการศึกษาข้อมูลเครือข่ายในกรณีที่มีการรับส่งข้อมูลด้วยยูดีพีโพรโทคอล จะพบว่าเมื่อเกิดการแปลงที่อยู่เครือข่าย จะมีข้อมูลในส่วนหัวของข้อมูลบางส่วนไม่ได้เกิดการเปลี่ยนไป ซึ่งจะพบข้อมูลดังต่อไปนี้ ทีโอเอส (TOS: Type of Service), ไอพีไอดี (IP id: Identification), โพรโทคอล, หมายเลขที่อยู่ไอพีปลายทาง (Destination Address) และหมายเลขพอร์ตปลายทาง (Destination Port) ซึ่งค่าข้อมูลเหล่านี้สามารถนำมาใช้เป็นการสร้างตัวคัดกรองสำหรับการเพิ่มขีดความสามารถของการหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายได้ ส่วนในของค่าทีทีแอล ซึ่งมีการเปลี่ยนแปลงค่าเมื่อเกิดการแปลงที่อยู่เครือข่ายนั้น ก็สามารถนำมาใช้ในการเพิ่มขีดความสามารถของการหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายได้เช่นกัน เนื่องจากค่าที่เปลี่ยนไปของทีทีแอล จะเกิดขึ้นเนื่องจากเมื่อข้อมูลได้มีการส่งผ่านอุปกรณ์ตัวกลางที่ส่งต่อข้อมูล (ในกรณีนี้คืออุปกรณ์การแปลงที่อยู่เครือข่าย) จะมีการลดค่าทีทีแอล 1 ค่าทุกครั้ง ซึ่งจากการงานวิจัยนี้จะพบว่าเครื่องลูกข่ายในเครือข่ายไม่ได้มีการเปลี่ยน

ตำแหน่งในช่วงเวลาสั้นๆ จึงสามารถสรุปได้ว่าค่าทีทีแอลของเครื่องลูกข่ายเดียวกัน เมื่อผ่านการแปลงที่อยู่เครือข่ายแล้ว จะมีค่าทีทีแอลหลังจากการแปลงที่อยู่เครือข่ายที่เท่ากันตลอด

และจากการศึกษาพบว่าเครื่องลูกข่ายที่ใช้ยูดีพีโพรโทคอลในการรับส่งข้อมูลเมื่อมีการแปลงที่อยู่เครือข่ายไปหาเครื่องที่ติดต่อได้แล้ว ตลอดการรับส่งข้อมูลในช่วงเวลาหนึ่ง ค่าหมายเลขพอร์ตต้นทางของอุปกรณ์การแปลงที่อยู่เครือข่าย (Source Port) ถูกใช้ค่าเดิมตลอดช่วงเวลานั้น สาเหตุที่พบการเกิดเหตุการณ์นี้ขึ้น เพราะการแปลงที่อยู่เครือข่ายเป็นการสร้างตารางเปรียบเทียบข้อมูลระหว่างข้อมูลก่อนการแปลงที่อยู่ และข้อมูลหลังการแปลงที่อยู่เครือข่าย ซึ่งตารางที่ใช้ในการจัดเก็บข้อมูลเปรียบเทียบนี้ จะถูกเก็บอยู่จนกว่าสิ้นสุดการเชื่อมต่อ แต่อุปกรณ์การแปลงที่อยู่เครือข่ายส่วนมากจะนิยมตั้งเวลาสิ้นสุด หลังจากไม่ได้รับข้อมูลจากเครื่องลูกข่าย หรือเมื่อค่าหมายเลขพอร์ตต้นทางของอุปกรณ์การแปลงที่อยู่เครือข่ายที่ใช้นี้ได้ถูกใช้โดยเครื่องลูกข่ายเครื่องอื่น

ซึ่งจากการศึกษาข้อมูลการแปลงที่อยู่เครือข่ายของยูดีพีโพรโทคอล สามารถนำมาวิเคราะห์หาขั้นตอนวิธีการเพิ่มขีดความสามารถของการแปลงที่อยู่เครือข่ายได้ ซึ่งแสดงอยู่ในรูปที่ 12 ดังต่อไปนี้



รูปที่ 12 ขั้นตอนวิธีการนับจำนวนเครื่องที่ผ่านการแปลงที่อยู่เครือข่าย โดยใช้ข้อมูลสารสนเทศอินเทอร์เน็ตโพรโทคอล และยูดีพีโพรโทคอล

จากรูปที่ 12 สามารถอธิบายได้ดังต่อไปนี้

(1.1) เมื่อรับข้อมูลของเครือข่ายเข้ามาในกรณีที่ข้อมูลเครือข่ายเป็นการใช้ ยูดีพีโพรโทคอลในการรับส่งข้อมูลเครือข่าย จะทำการตรวจสอบลำดับแรกตรงค่าทีโอเอสของข้อมูล โดยเทียบกับข้อมูลของเครื่องลูกข่ายที่จำแนกได้แล้วซึ่งจะเก็บค่าไว้ ถ้าค่าทีโอเอสไม่ตรงกับข้อมูลทั้งหมดที่มี ก็สามารถข้ามการคำนวณไปได้เลยเนื่องจากเป็นการยืนยันแล้วว่าข้อมูลสารสนเทศที่ได้รับเป็นเครื่องลูกข่ายใหม่ที่ยังไม่ได้จำแนก

(1.2) การตรวจสอบลำดับถัดมาจะเป็นการตรวจสอบด้วยข้อมูลค่าทีทีแอล โดยจะทำการตรวจสอบกับข้อมูลเครื่องลูกข่ายที่จำแนกไว้แล้ว ถ้าข้อมูลของค่าทีทีแอลที่ตรวจสอบไม่ตรงกับข้อมูลของเครื่องลูกข่ายที่จำแนกไว้ได้ก่อนแล้ว แสดงข้อมูลสารสนเทศของเครือข่ายที่ได้รับ เป็นข้อมูลของเครื่องลูกข่ายใหม่ที่ยังไม่ได้จำแนก เพราะจากค่าทีทีแอลจะเป็นการยืนยันว่าข้อมูลนั้นมาจากระบบปฏิบัติการที่แตกต่าง หรือมีโครงสร้างของเครือข่ายที่อยู่คนละระดับชั้นกับเครื่องลูกข่ายที่จำแนกไว้ก่อนหน้านี้

(1.3) ขั้นตอนในการตรวจสอบข้อมูลสารสนเทศของเครือข่ายที่ผ่านการแปลงที่อยู่เครือข่าย โดยใช้ค่าหมายเลขที่อยู่ไอพีปลายทาง, หมายเลขพอร์ตปลายทาง และหมายเลขพอร์ตต้นทางร่วมกัน โดยเทียบกับข้อมูลเครือข่ายของลูกข่ายที่จำแนกได้แล้ว (ในหนึ่งเครื่องลูกข่ายอาจจะประกอบไปด้วย การเชื่อมต่อเครือข่ายไปที่ตำแหน่งต่างๆพร้อมกัน เป็นสาเหตุที่ต้องแยกข้อมูลการเชื่อมเครือข่ายของเครื่องลูกข่ายเป็นหลายระดับตามจุดหมายปลายทาง) สาเหตุที่ต้องใช้ค่าทั้งสามพร้อมๆ กัน เนื่องจากถ้าเราใช้เพียงหมายเลขที่อยู่ไอพีปลายทาง และหมายเลขพอร์ตปลายทาง จะสามารถบอกได้เพียงว่ามีการส่งข้อมูลไปยังตำแหน่งปลายทางนั้น แต่ยังไม่สามารถแยกแยะออกได้ในกรณีที่มีเครื่องลูกข่ายมากว่าหนึ่งเครื่องส่งออกไปยังปลายทางตำแหน่งนั้น

(1.4) ขั้นตอนตรวจสอบในขั้นสุดท้าย เป็นการตรวจสอบโดยการหาค่าความต่อเนื่องของค่าไอพีไอดี ซึ่งจะใช้ในกรณีที่ทั้งสามกรณีที่กล่าวมาไม่สามารถแยกข้อมูลเครือข่ายได้ ซึ่งจะเกิดเมื่อมีเหตุกรณ์ดังต่อไปนี้ เป็นเครื่องลูกข่ายใหม่ที่ไม่สามารถแยกได้ใน 2 กรณีแรกที่กล่าวมา หรือเป็นเครื่องลูกข่ายที่ถูกจำแนกแล้วแต่มีการส่งข้อมูลไปยังตำแหน่งปลายทางที่ยังไม่เคยได้มีการส่งข้อมูลออกไป

(2) กรณีศึกษาการใช้ข้อมูลทีซีพีโพรโทคอล ร่วมกับข้อมูลอินเทอร์เน็ตโพรโทคอล

ซึ่งจากศึกษาโดยการใช้ข้อมูลสารสนเทศของเครือข่ายจริง โดยใช้ทีซีพีโพรโทคอล เป็นโพรโทคอลการรับส่ง จากการส่งข้อมูลจากเครื่องลูกข่ายภายในเครือข่ายส่วนบุคคล ออกไปยังเครื่องลูกข่ายข้างนอก โดยผ่านการแปลงที่อยู่เครือข่าย จะพบว่าข้อมูลเครือข่ายในส่วนหัวของทีซีพีโพรโทคอล และอินเทอร์เน็ตโพรโทคอลได้ถูกเปลี่ยนแปลงเป็นบ้างส่วน ซึ่งสามารถแสดงได้จากรูปที่ 13

Type Of Service	0x0
Identification	61713
Time to live	64
PROTOCOL	TCP
Source Address	192.168.1.8
Destination Address	202.90.4.62
Source Port	4925
Destination Port	80
Acknowlegment Number	904
Windows Size	65535

Type Of Service	0x0
Identification	61713
Time to live	**63**
PROTOCOL	TCP
Source Address	**192.168.0.1**
Destination Address	202.90.4.62
Source Port	**52025**
Destination Port	80
Acknowlegment Number	904
Windows Size	65535

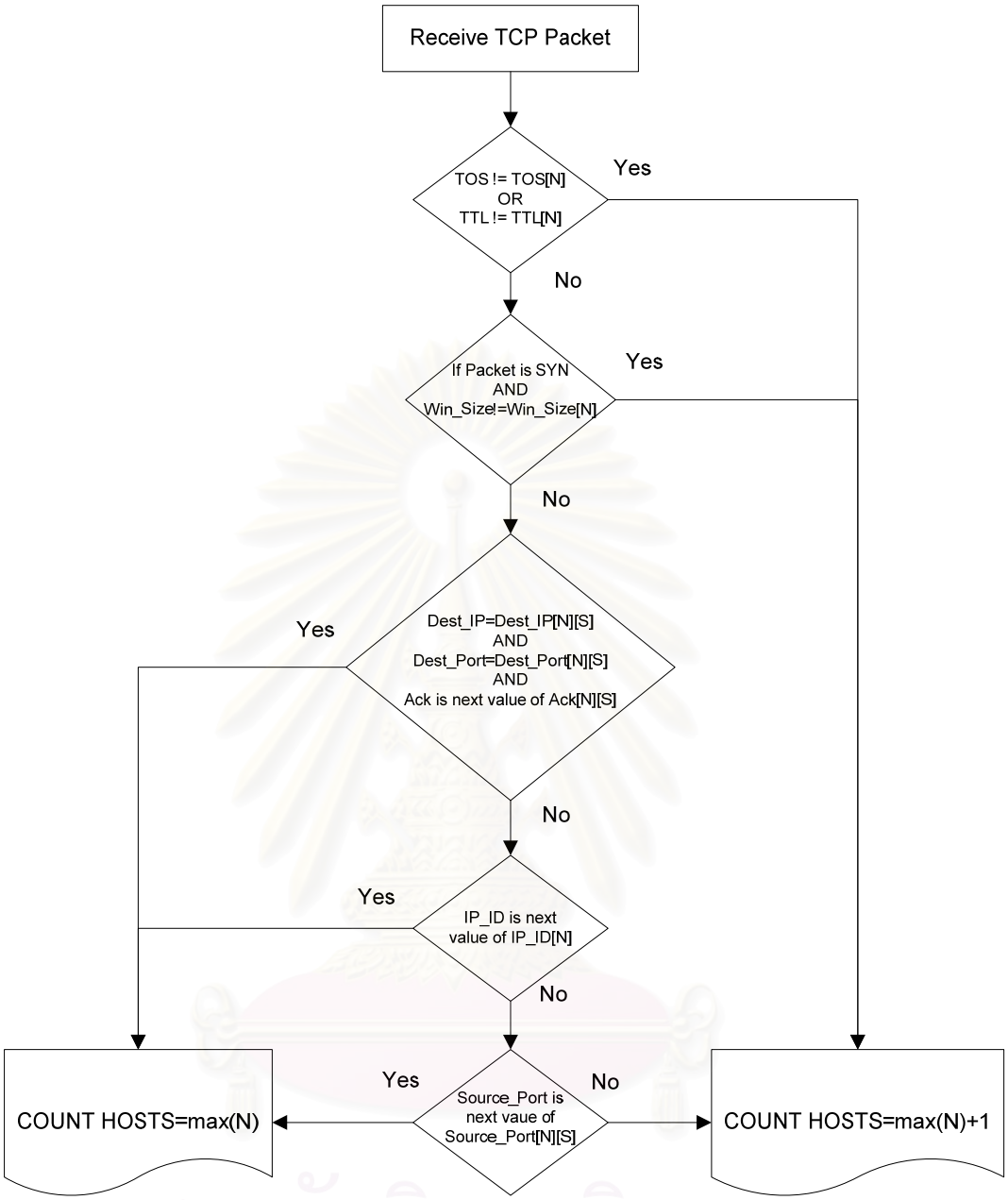
รูปที่ 13 ตัวอย่างข้อมูลสารสนเทศในส่วนหัวของอินเทอร์เน็ตโพรโทคอลและทีซีพีโพรโทคอลในกรณีที่ใช้การแปลงที่อยู่เครือข่ายในการเชื่อมต่อ

ซึ่งจากการศึกษาข้อมูลเครือข่ายของทีซีพีโพโทรคอล จะพบว่าข้อมูลเครือข่ายภายหลังจากการแปลงที่อยู่เครือข่ายจะมีข้อมูลบางส่วนที่ไม่ได้ถูกเปลี่ยนแปลงไป ซึ่งจะมีข้อมูลในส่วนต่อไปนี้ ทีโอเอส (Type Of Service) ไอพีไอดี (IP id:Identification) โพรโทคอล หมายเลขที่อยู่ไอพีปลายทาง (Destination Address) หมายเลขพอร์ปลายทาง (Destination Port) ค่าการ

รับรู้ชุดข้อมูล (Acknowlegment Number) และขนาดวินโดว์ (Windows Size) ซึ่งข้อมูลสารสนเทศที่กล่าวมาข้างต้นสามารถนำมาใช้เป็น ตัวคัดกรองเพื่อเพิ่มความสามารถในการหาจำนวนเครื่องที่ผ่านการแปลงที่อยู่เครือข่ายได้ โดยเฉพาะค่าการรับรู้ชุดข้อมูลในทีซีพีโพรโทคอล ซึ่งทีซีพีโพรโทคอลมีความสามารถในการรับส่งข้อมูลโดยไม่สูญหายระหว่างทางการรับส่ง ค่าการรับรู้ชุดข้อมูลจึงเป็นค่าที่แสดงถึงจำนวนข้อมูลที่ใช้ในการรับส่งแล้ว ซึ่งค่านี้มีลักษณะเพิ่มขึ้นตามลำดับชุดข้อมูลที่รับส่ง ซึ่งสามารถนำมาวิเคราะห์เพิ่มขีดความสามารถของการหาจำนวนเครื่องที่ผ่านการแปลงที่อยู่เครือข่ายได้

ส่วนค่าทีทีแอลที่เปลี่ยนแปลงภายหลังผ่านการแปลงที่อยู่เครือข่ายเกิดจากสาเหตุเดียวกับยูดีพีโพรโทคอลที่กล่าวไว้ก่อนหน้านี้ ซึ่งค่าทีทีแอลก็สามารถนำมาวิเคราะห์ได้เช่นเดียวกัน ในทีซีพีโพรโทคอลจะมีความแตกต่างบางประการกับยูดีพีโพรโทคอล ในเรื่องค่าหมายเลขพอร์ตต้นทางของอุปกรณ์การแปลงที่อยู่เครือข่าย (Source Port) ภายหลังผ่านการแปลงที่อยู่เครือข่ายที่ไม่ได้ใช้หมายเลขพอร์ตเดิมตลอดการเชื่อมต่อไปยังจุดหมายปลายทางเดียวกันและหมายเลขพอร์ตปลายทางเดียวกัน เนื่องจากทีซีพีโพรโทคอลมีความสามารถในการป้องกันข้อมูลสูญหาย จึงทำให้ทีซีพีโพรโทคอลทำงานได้ช้ากว่า ยูดีพีโพรโทคอล ดังนั้นในโพรโทคอลต่างๆที่นิยมใช้ในอินเทอร์เน็ตที่ใช้ทีซีพีโพรโทคอลเป็นโพรโทคอลการรับส่งจึงนิยมทำการรับส่งข้อมูลโดยการทำการรับส่งแบบขนาน ทำให้เมื่อมีการรับส่งข้อมูลไปยังเครื่องลูกข่ายข้างนอกเครือข่ายส่วนบุคคล โดยการผ่านวิธีการแปลงที่อยู่เครือข่ายจะมีการรับส่งข้อมูลออกไปพร้อมๆ กันหลายชุด ทำให้ค่าหมายเลขพอร์ตต้นทางที่ผ่านการแปลงที่อยู่เครือข่ายมีหลายค่า ทั้งที่ออกจากเครื่องลูกข่ายเดียวกันและไปที่ตำแหน่งปลายทางเดียวกัน ดังตัวอย่างเช่น การรับข้อมูลของเอชทีทีพีโพรโทคอล (Http: Hypertext Transfer Protocol) ซึ่งโพรโทคอลนี้เป็นโพรโทคอลที่ใช้ในการรับส่งข้อมูลเว็บไซต์ ซึ่งภายในเว็บไซต์อาจจะประกอบด้วยเนื้อหาหลายๆ ส่วนเช่น เนื้อหาและรูปภาพ เครื่องลูกข่ายอาจจะร้องขอข้อมูลของเนื้อหา และข้อมูลของรูปภาพไปได้พร้อมๆ กัน เป็นต้น แต่จากงานวิจัยของ Saikat Guha และ Paul Francis [16] ที่กล่าวมาก่อนหน้านี้ จะสามารถหาขั้นตอนวิธีการนับจำนวนเครื่องที่ผ่านการแปลงเครือข่าย ได้โดยเพิ่มการคาดเดาหมายเลขพอร์ตต้นทาง (PP: Port Prediction) ที่อุปกรณ์การแปลงที่อยู่เครือข่ายสามารถเลือกใช้เพื่อเชื่อมต่อเครือข่ายได้ แต่เนื่องจากขั้นตอนวิธีการนี้ไม่สามารถทำได้ทุกอุปกรณ์การแปลงที่อยู่เครือข่าย โดยเฉพาะอุปกรณ์การแปลงที่อยู่เครือข่ายที่มีพฤติกรรมแบบสุ่มค่าหมายเลขพอร์ตต้นทาง ดังนั้นผู้วิจัยจึงเสนอขั้นตอนวิธีการนี้เป็นเพียงตัวเลือกเพิ่มเติม

ซึ่งจากการศึกษาข้อมูลการแปลงที่อยู่เครือข่ายของทีซีพีโพรโทคอล สามารถนำมาวิเคราะห์หาวิธีการเพิ่มขีดความสามารถของการหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายได้ ซึ่งแสดงในรูปที่ 14



รูปที่ 14 ขั้นตอนวิธีการนับจำนวนเครื่องที่ผ่านการแปลงที่อยู่เครือข่าย โดยใช้ข้อมูลสารสนเทศอินเทอร์เน็ตโพรโทคอล และทีซีพีโพรโทคอล

จากรูปที่ 14 สามารถอธิบายได้ดังต่อไปนี้

(2.1) ขั้นตอนแรกและขั้นตอนที่สองคือการตรวจสอบค่าทีโอเอส และค่าทีทีแอล ซึ่งเหตุผลในการตรวจสอบเป็นเช่นเดียวกับการตรวจสอบกรณีการใช้ยูดีพีโพรโทคอลเป็นโพรโทคอลรับส่งข้อมูล

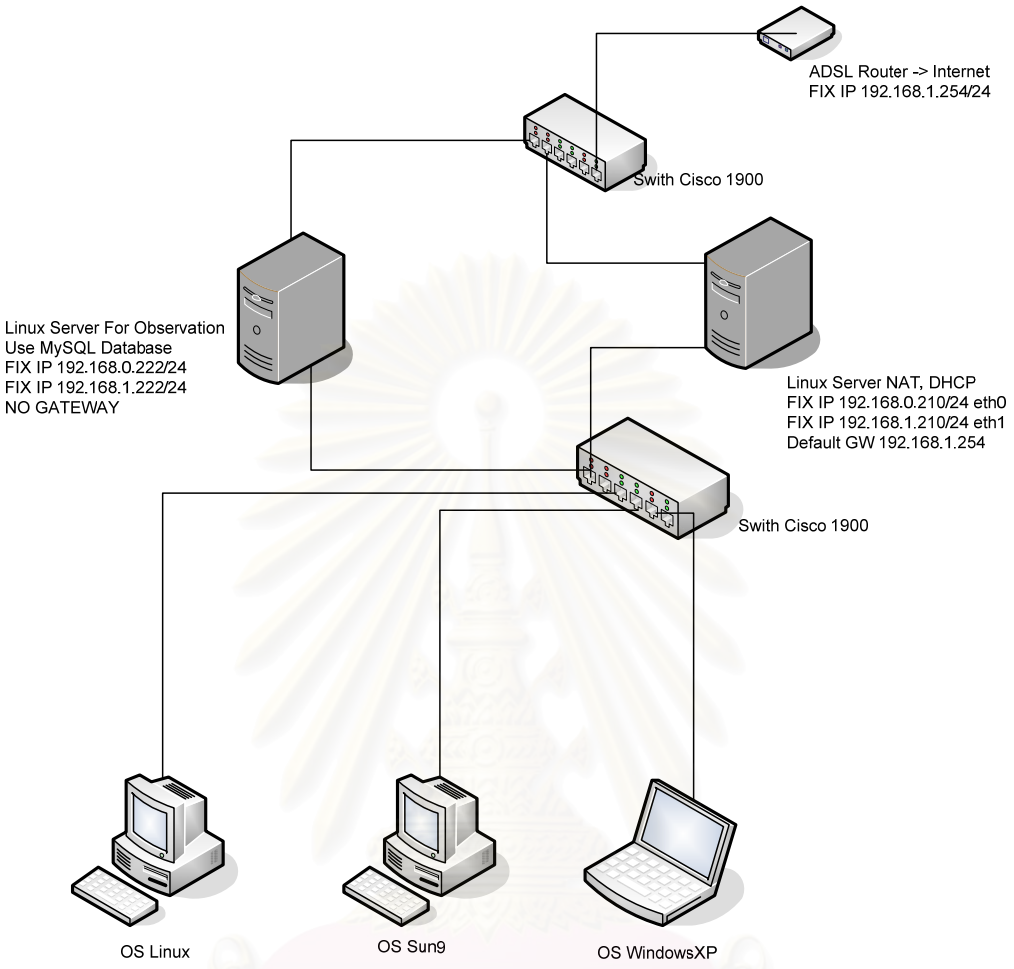
(2.2) ขั้นตอนที่สามเป็นการตรวจสอบค่าขนาดวินโดว์ โดยตรวจสอบกับข้อมูลของเครื่องลูกข่ายที่จำแนกได้แล้ว โดยแพ็คเก็ตของทีซีพีที่ตรวจสอบจะเป็น SYN แพ็คเก็ตเท่านั้น เนื่องจากการตรวจสอบทุกๆแพ็ตเก็ต ในบางครั้งโพรโทคอลทีซีพีจะลดขนาดวินโดว์ลงเนื่องจากป้องกันการเกิดความหนาแน่นในเครือข่าย กรณีที่ค่าที่ตรวจสอบไม่ตรงกับข้อมูลของเครื่องลูกข่ายที่จำแนกได้แล้ว จากงานวิจัยที่กล่าวมาแล้วจะแสดงให้เห็นว่า ข้อมูลเครือข่ายที่ได้รับมา มาจากเครื่องลูกข่ายที่มีระบบปฏิบัติการที่แตกต่างจากเครื่องลูกข่ายที่จำแนกได้ก่อนหน้านี้ จึงสามารถสรุปได้ว่าข้อมูลสารสนเทศที่ตรวจสอบมาจากเครื่องลูกข่ายใหม่ที่ยังไม่ได้จำแนก

(2.3) ขั้นตอนการตรวจสอบค่าหมายเลขที่อยู่ไอพีปลายทาง, หมายเลขพอร์ตปลายทาง และค่าการรับรู้ชุดข้อมูลพร้อมกัน โดยเป็นการตรวจสอบข้อมูลเทียบกับข้อมูลเครื่องลูกข่ายที่จำแนกได้แล้วก่อนหน้านี้ สาเหตุที่จำเป็นในการตรวจสอบค่าทั้งสามค่าพร้อมๆ กัน เนื่องจากเครื่องลูกข่ายจากหลายๆ เครื่องอาจจะมีการส่งข้อมูลเครือข่ายออกไปยังที่จุดหมายปลายทางเดียวโดยมีการใช้บริการที่เหมือนกันได้ ดังนั้นการใช้ค่าการรับรู้ชุดข้อมูลจะเป็นการสร้างความมั่นใจเพิ่มขึ้นว่าเครื่องที่ส่งออกไปยังจุดหมายนั้นเป็นเครื่องๆ เดียวกัน

(2.4) ขั้นตอนสุดท้ายเป็นการตรวจสอบด้วยค่าไอพีไอดี โดยเทียบกับข้อมูลเครื่องลูกข่ายที่จำแนกได้แล้วล่าสุด โดยดูค่าความต่อเนื่องที่เพิ่มขึ้น ของค่าไอพีไอดีซึ่งจะถูกนำมาใช้ในกรณีที่วิธีการในข้อ (2.1) ถึง (2.3) ไม่สามารถทำการจำแนกเครื่องลูกข่ายออกได้ และในกรณีของทีซีพีโพรโทคอลได้เพิ่มตัวเลือกพิเศษในกรณีที่ค่าไอพีไอดีไม่สามารถตรวจสอบได้ โดยขั้นตอนวิธีพิเศษนี้จะเป็นการคาดเดาหมายเลขพอร์ตต้นทางที่ได้รับจากเครือข่ายว่าจะมีความเป็นไปได้ว่าเครื่องลูกข่ายใดบ้างที่จะใช้หมายเลขพอร์ตต้นทางนี้บ้าง

3.2 วิธีการออกแบบขั้นตอนการจัดเก็บข้อมูลที่ใช้ในการทดลอง

งานวิจัยนี้ใช้ข้อมูลของระบบเครือข่ายจริง โดยเลือกข้อมูลเครือข่ายจากบริษัทเอกชนแห่งหนึ่งซึ่งมีขนาดเครือข่ายขนาดกลาง มีเครื่องลูกข่ายประมาณ 80 เครื่อง มีการใช้งานบริการต่างๆ ในเครือข่ายตามปกติ และมีการใช้งานวิธีการแปลงที่อยู่เครือข่ายเพื่อการเชื่อมต่อกับเครือข่ายภายนอก โดยมีขนาดแบนด์วิดท์ในการเชื่อมเครือข่ายขนาด 2 เมกะบิต มาทำการทดลอง โดยมีลักษณะโครงสร้างเครือข่ายที่ใช้ในการจัดเก็บข้อมูล ดังรูปตัวอย่างที่ 15



รูปที่ 15 โครงสร้างเครือข่ายที่ใช้ในการเก็บข้อมูลในงานการวิจัย

ซึ่งเครื่องลูกข่ายที่นำข้อมูลเครือข่ายมาทำการวิจัย เป็นเครื่องลูกข่ายที่มีการใช้งานโดยทั่วไปมีแอปพลิเคชั่นการใช้งานโดยไม่ได้มีการควบคุมการใช้งาน ซึ่งโพรโทคอลที่ใช้งานเครือข่ายนี้ประกอบด้วย ทีซีพีโพรโทคอล และยูดีพีโพรโทคอล โดยเครื่องลูกข่ายที่ใช้ในงานวิจัยประกอบด้วยระบบปฏิบัติการต่างๆดังต่อไปนี้

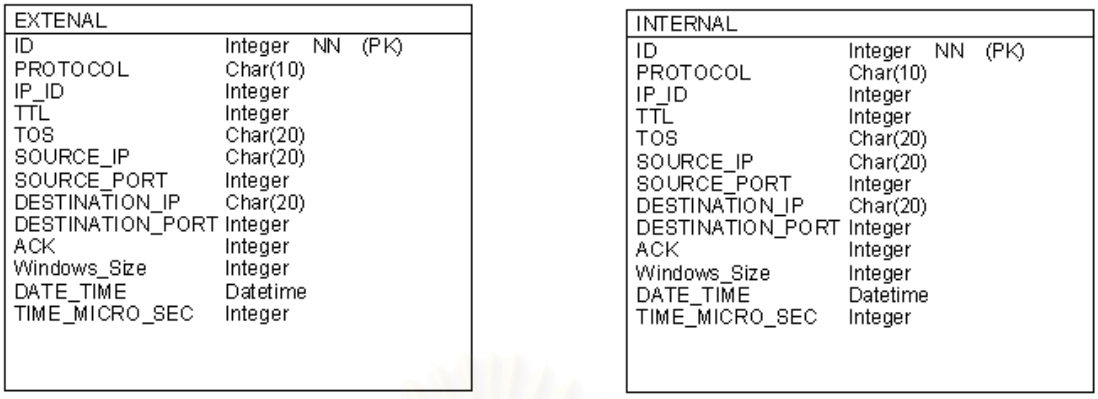
ตารางที่ 2 แสดงรายละเอียดระบบปฏิบัติการของเครื่องลูกข่ายที่ใช้ในงานวิจัย

ลำดับที่	ระบบปฏิบัติการ	จำนวนเครื่อง
1	Windows XP	38
2	Windows Vista	5
3	Windows Server 2008	2
4	Mac OSX	33
5	Linux (Kernel 2.6)	4
6	Solaris 9	1
7	Windows Mobile 2003	1
รวม		**84**

ซึ่งสาเหตุที่เลือกให้เครื่องลูกข่ายที่ทำการวิจัยมีระบบปฏิบัติการหลากหลายเนื่องจากข้อมูลสารสนเทศในเครือข่ายที่ส่งมาจากเครื่องลูกข่าย ในแต่ระบบปฏิบัติการมีค่ามาตรฐานที่ไม่เหมือนกันทุกระบบปฏิบัติการ

ข้อมูลเครือข่ายที่จัดเก็บในงานวิจัยนี้ ได้จัดเก็บเฉพาะในส่วนหัวของข้อมูลเครือข่ายเพียงอย่างเดียว โดยไม่ได้จัดเก็บเนื้อข้อมูลที่ส่งออกมาจากเครื่องลูกข่าย เพื่อประหยัดขนาดพื้นที่ในการจัดเก็บข้อมูลทำการวิจัย โดยข้อมูลสารสนเทศที่ทำการวิจัยทั้งหมดได้จัดเก็บอยู่ในฐานข้อมูลโดยได้เลือกใช้ MySQL เป็นฐานข้อมูลการจัดเก็บ

โดยการจัดเก็บข้อมูลสารสนเทศที่ทำการวิจัย จะจัดเก็บเป็นข้อมูลภายในเครือข่ายก่อนที่จะถูกทำการแปลงที่อยู่เครือข่าย และข้อมูลภายนอกหลังจากที่ข้อมูลสารสนเทศถูกแปลงที่อยู่เครือข่ายแล้ว โดยเก็บเฉพาะส่วนที่ส่งออกไปจากเครือข่ายส่วนบุคคล โดยรูปแบบข้อมูลที่ใช้จัดเก็บแสดงอยู่ในรูปที่ 16 ส่วนตัวอย่างข้อมูลสารสนเทศที่จัดเก็บได้แสดงอยู่ในภาคผนวกที่ 1



EXTENAL			
ID	Integer	NN	(PK)
PROTOCOL	Char(10)		
IP_ID	Integer		
TTL	Integer		
TOS	Char(20)		
SOURCE_IP	Char(20)		
SOURCE_PORT	Integer		
DESTINATION_IP	Char(20)		
DESTINATION_PORT	Integer		
ACK	Integer		
Windows_Size	Integer		
DATE_TIME	Datetime		
TIME_MICRO_SEC	Integer		

INTERNAL			
ID	Integer	NN	(PK)
PROTOCOL	Char(10)		
IP_ID	Integer		
TTL	Integer		
TOS	Char(20)		
SOURCE_IP	Char(20)		
SOURCE_PORT	Integer		
DESTINATION_IP	Char(20)		
DESTINATION_PORT	Integer		
ACK	Integer		
Windows_Size	Integer		
DATE_TIME	Datetime		
TIME_MICRO_SEC	Integer		

รูปที่ 16 แสดงโครงสร้างการจัดเก็บข้อมูลสารสนเทศของเครือข่ายที่ใช้ในการวิจัย

3.3 การออกแบบเครื่องมือช่วยในการวิเคราะห์ข้อมูลเพื่อหาความถูกต้องของขั้นตอนวิธี

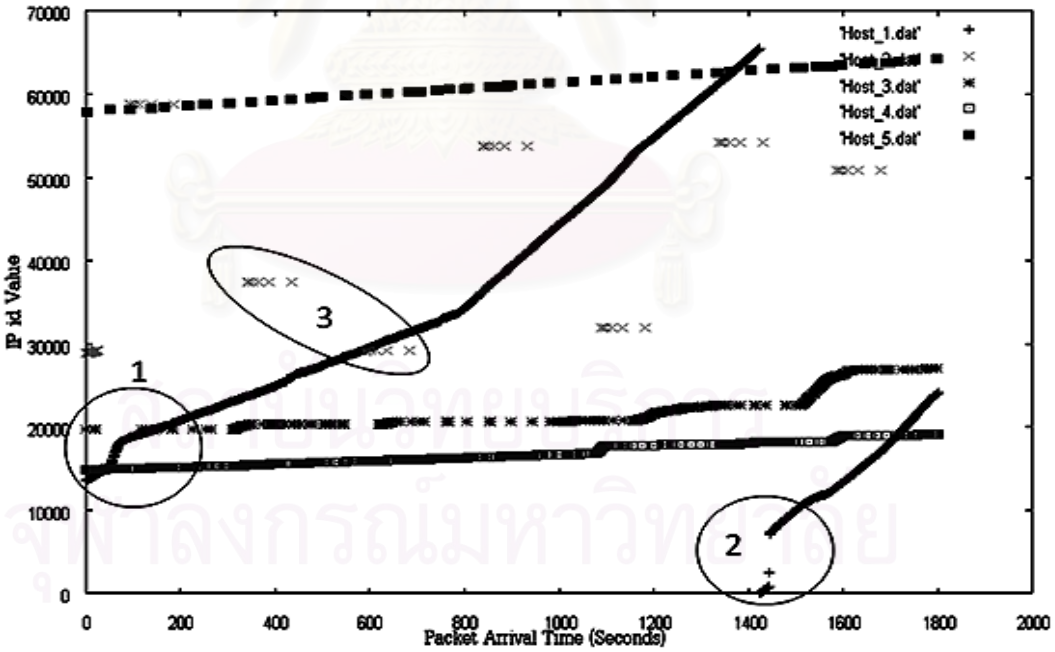
ในงานวิจัยนี้ได้มุ่งเน้นที่ศึกษาขั้นตอนวิธีการเพิ่มขีดความสามารถในการจำนวนเครื่องที่ผ่านการแปลงที่อยู่เครือข่าย ซึ่งจำเป็นต้องมีการเก็บข้อมูลเครือข่ายจริง ไม่ว่าจะเป็นภายในเครือข่ายส่วนบุคคล และจากเครือข่ายภายนอกที่ผ่านการแปลงที่อยู่เครือข่ายแล้ว จากข้อมูลสารสนเทศที่กล่าวมา ทำให้ข้อมูลสารสนเทศของเครือข่ายที่นำมาใช้ในงานวิจัยนี้ มีข้อมูลเป็นปริมาณมาก ซึ่งจัดเก็บลงในฐานข้อมูล จึงทำการออกแบบเครื่องมือที่ใช้ในการวิเคราะห์ ตามขั้นตอนวิธีการที่เสนอในหัวข้อที่ 3.1 โดยเลือกภาษาคอมพิวเตอร์พีเอชพี (PHP Hypertext Preprocessor) ในการออกแบบและสร้างเครื่องมือ เนื่องจากพีเอชพีเป็นภาษาที่มีความสามารถในการเชื่อมต่อฐานข้อมูล อีกทั้งยังสามารถทำงานได้บนระบบปฏิบัติการหลากหลาย

บทที่ 4
ผลการทดลอง

จากการศึกษาและการออกแบบขั้นตอนวิธีการเพิ่มความถูกต้องการนับจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่าย ในงานวิจัยนี้จึงแบ่งการทดลองออกเป็นสองส่วน โดยส่วนแรกเป็นการทดลองที่จะตรวจสอบหาความถูกต้องของขั้นตอนวิธีที่นำเสนอ โดยเป็นการแก้ไขปัญหาที่พบจากงานวิจัยของ M. Bellovin และส่วนที่สองเป็นการหาความถูกต้องของขั้นตอนวิธีที่นำเสนอโดยตรวจสอบกับข้อมูลสารสนเทศของเครือข่ายขนาดกลาง

4.1 ผลการทดลองในการตรวจสอบหาความถูกต้องของขั้นตอนวิธีที่เสนอ

ซึ่งในการทดลองนี้ ทางผู้วิจัยได้เลือก ข้อมูลสารสนเทศของเครือข่ายที่ผ่านการแปลงที่อยู่เครือข่ายบ้างส่วน มาผ่านขั้นตอนวิธีการที่นำเสนอ เพื่อตรวจสอบผลลัพทธ์ที่ได้จากขั้นตอนวิธีที่นำเสนอว่าสามารถแก้ไขปัญหาที่พบจากงานวิจัยก่อนหน้านี้ได้หรือไหม ซึ่งผลการทดลองที่ผ่านขั้นตอนวิธีที่นำเสนอ ได้นำค่าไอพีไอดีที่แยกได้จากการนับจำนวนเครื่อง มาสร้างแผนภูมิเทียบกับเวลาที่รับค่าไอพีไอดี ได้ดังรูปตัวอย่างที่ 17



รูปที่ 17 ค่าไอพีไอดีเทียบกับเวลาที่รับค่าได้

ซึ่งจากรูปที่ 17 จะพบว่าข้อมูลสารสนเทศของเครือข่ายภายในวงกลมที่ 1 ซึ่งเป็นการตัดกันของค่าไอพีไอดี ซึ่งกรณีการใช้ค่าไอพีไอดีอย่างเดียวในการนับจำนวนเครื่องลูกข่ายจะทำให้นับ

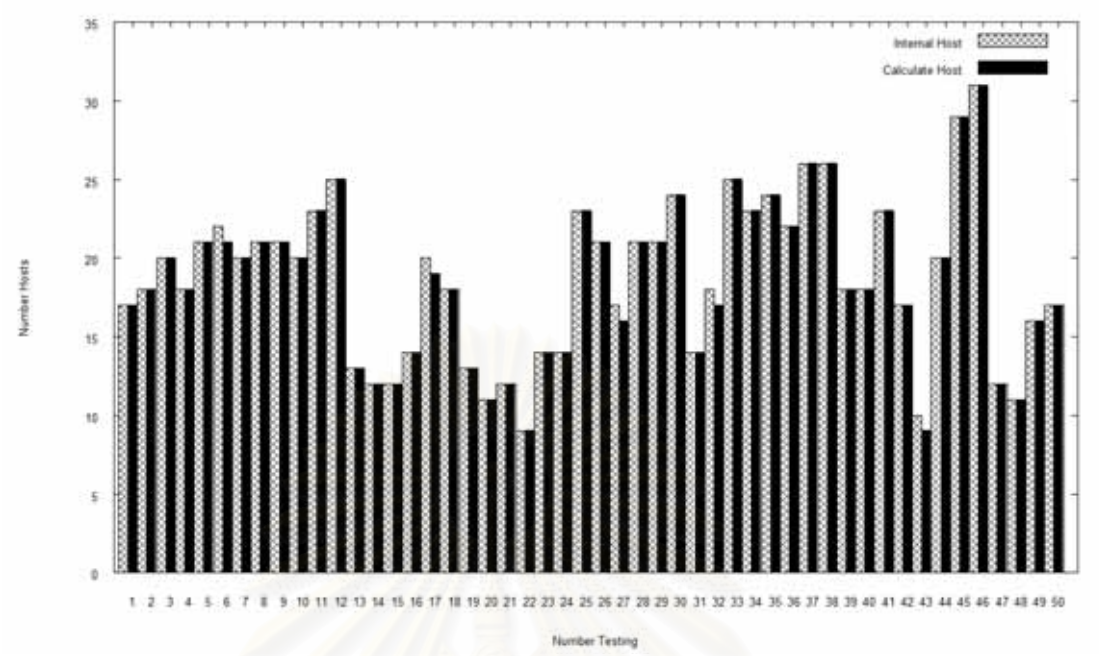
ผิดผลาดได้ที่ตำแหน่งนี้ แต่การใช้ขั้นตอนวิธีใหม่ที่เสนอสามารถแก้ปัญหาได้ ในวงกลมที่ 2 ในรูปที่ 17 แสดงถึงเมื่อค่าไอพีไอดีที่ระบบปฏิบัติการใช้เต็มค่า 16 บิต แล้วถูกวนค่ากลับมาใช้ใหม่ ก็สามารถแก้ไขได้จากขั้นตอนวิธีใหม่ที่เสนอ เพราะเป็นการเกิดในช่วงของการรับส่งของทีซีพีโพรโทคอล ซึ่งในขั้นตอนวิธีใหม่มีเงื่อนไขเพิ่มเติมในการตรวจสอบเพิ่มเติม ส่วนในวงกลมที่ 3 เป็นการส่งข้อมูลโดยใช้ยูดีพีโพรโทคอล และใช้บริการดีเอ็นเอส (DNS: Domain Name Service) จากภายนอกเครือข่ายส่วนบุคคล ของอุปกรณ์ในเครือข่ายบางชนิด โดยอุปกรณ์นั้นมีพฤติกรรมในการสุ่มค่าไอพีไอดีใหม่ทุกครั้งในการเริ่มต้นส่งข้อมูล ซึ่งถ้ามีการใช้ค่าไอพีไอดีเพียงอย่างเดียวในการนับจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายจะพบเครื่องลูกข่ายมากกว่าความเป็นจริง (ผลบวกลวง) แต่จากขั้นตอนวิธีใหม่ที่เสนอก็สามารถแก้ปัญหานี้ได้ สาเหตุเพราะขั้นตอนวิธีใหม่ที่เสนอจะดูเพียงหมายเลขพอร์ตต้นทาง หมายเลขที่อยู่ไอพีปลายทาง และหมายเลขพอร์ตปลายทาง ก่อนการตรวจสอบด้วยค่าไอพีไอดี ซึ่งจะทำปัญหานี้สามารถแก้ไขลงได้

4.2 ผลการทดลองการวัดผลความถูกต้องของขั้นตอนวิธีในช่วงเวลาทดสอบ

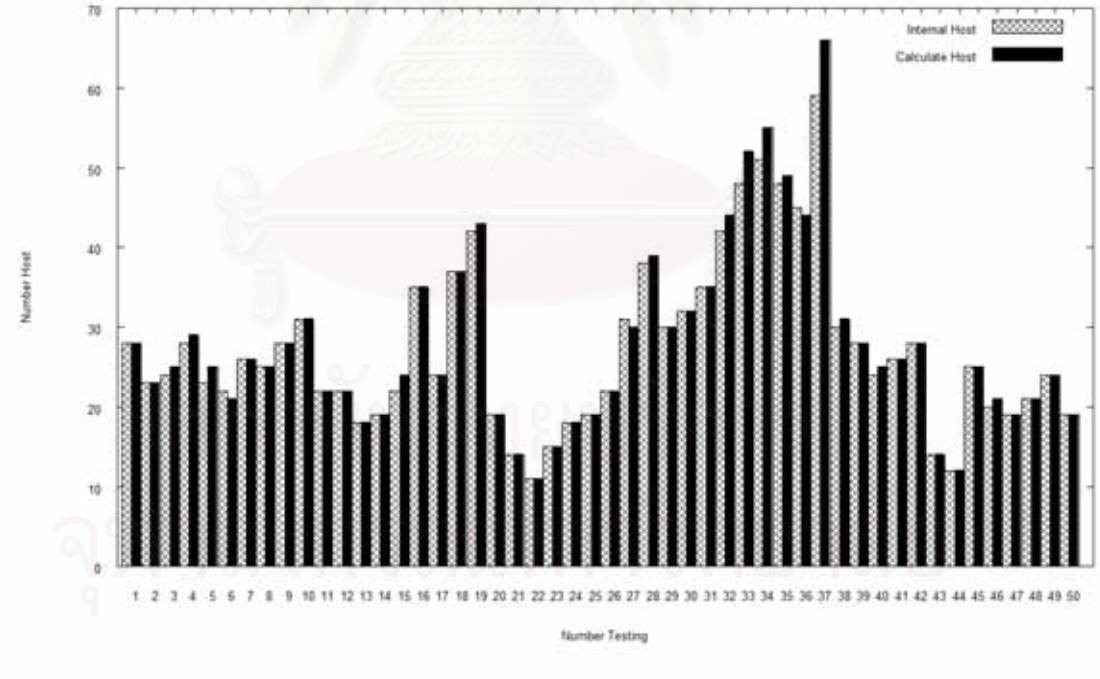
การทดลองนี้เป็นการวัดผลเพื่อหาความถูกต้องของขั้นตอนวิธีที่เสนอ โดยการทดลองจะนำข้อมูลสารสนเทศของเครือข่ายจริงที่มีขนาดกลาง โดยมีจำนวนเครื่องลูกข่าย 84 เครื่อง มาทำการทดลองโดยผลการทดลองได้แบ่งออกเป็น 2 ส่วน ประกอบด้วยการทดลองโดยเลือกช่วงเวลาทดสอบระยะต่ำกว่า 20 นาที มาทำการหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายเพื่อหาช่วงเวลาที่ดีสุดในการใช้งานขั้นตอนวิธีที่เสนอ และผลการทดลองพยายามหาเครื่องที่ผ่านการแปลงที่อยู่เครือข่ายทั้งหมดของเครือข่ายส่วนบุคคล

4.2.1 ผลการทดลองการเลือกช่วงเวลาทดสอบ

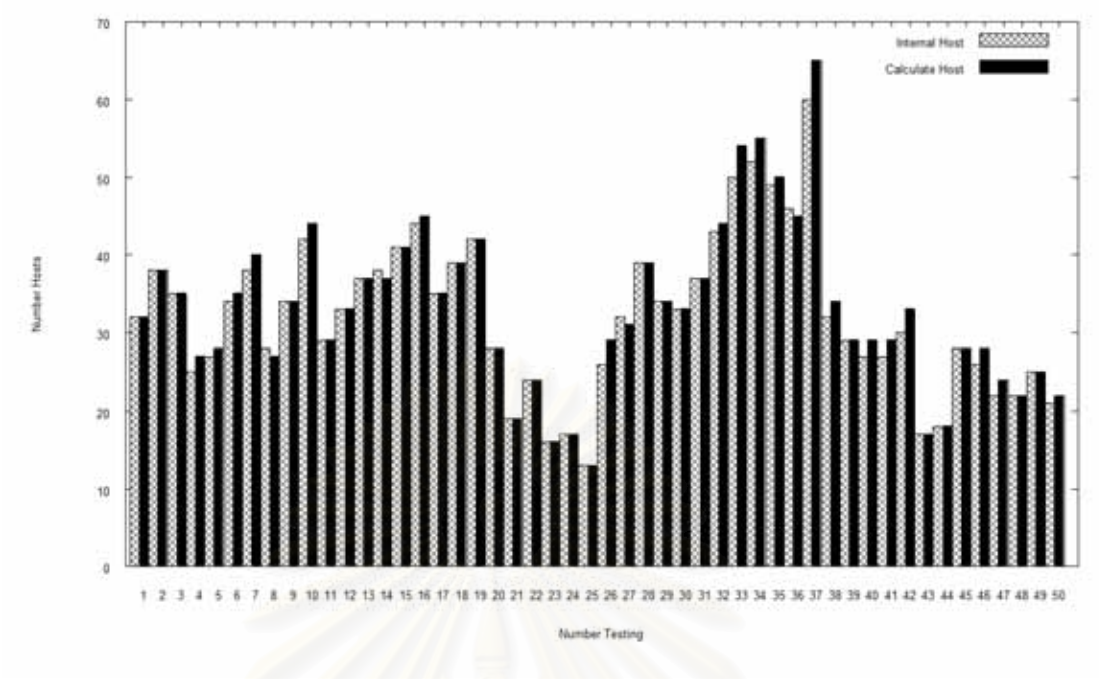
ในการทดลองนี้ได้เลือกช่วงเวลาที่ทดสอบ ใช้ในการหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่าย 7 ค่าดังนี้คือ 1 นาที 3 นาที 5 นาที 7 นาที 10 นาที 15 นาที และ 20 นาที โดยในการทดสอบแต่ละครั้งจะทำการสุ่มเลือกช่วงข้อมูลมาทำการทดสอบซึ่งใช้ 50 ตัวอย่างการสุ่มโดยมีการเปรียบเทียบเพื่อหาความถูกต้องของข้อมูล เทียบกับข้อมูลเครือข่ายภายในที่มีการส่งค่าผ่านการแปลงที่อยู่เครือข่าย ผลการทดลองที่ได้แสดงอยู่ในรูปต่อไปนี้ตามลำดับ



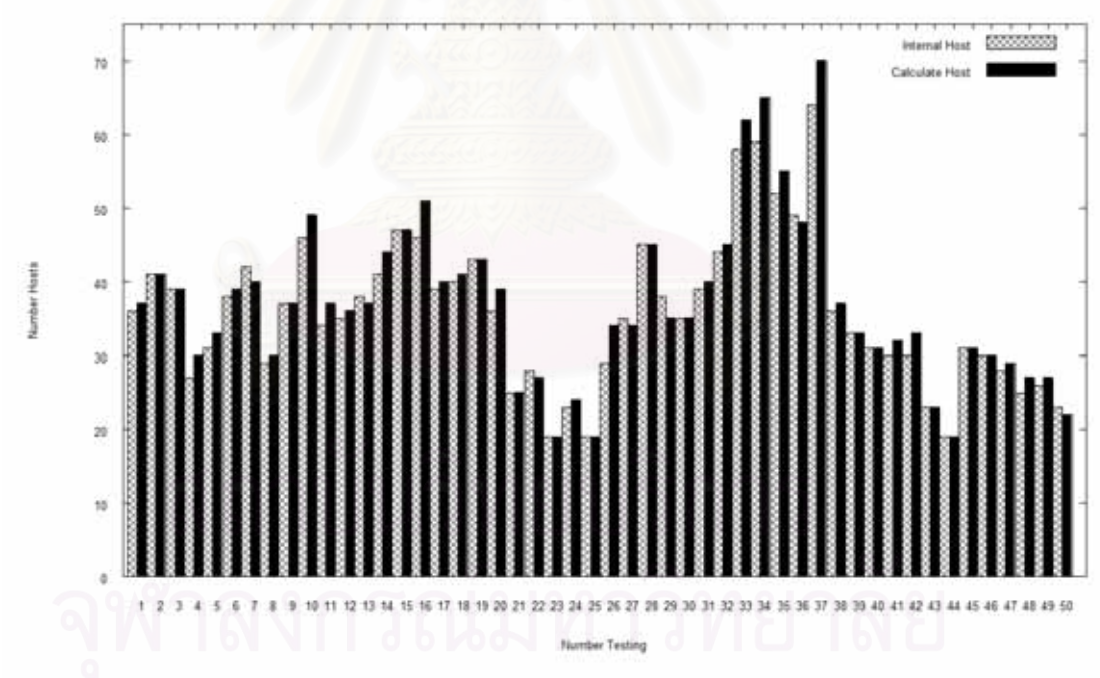
รูปที่ 18 การหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายโดยใช้ช่วงเวลาทดสอบ 1 นาที



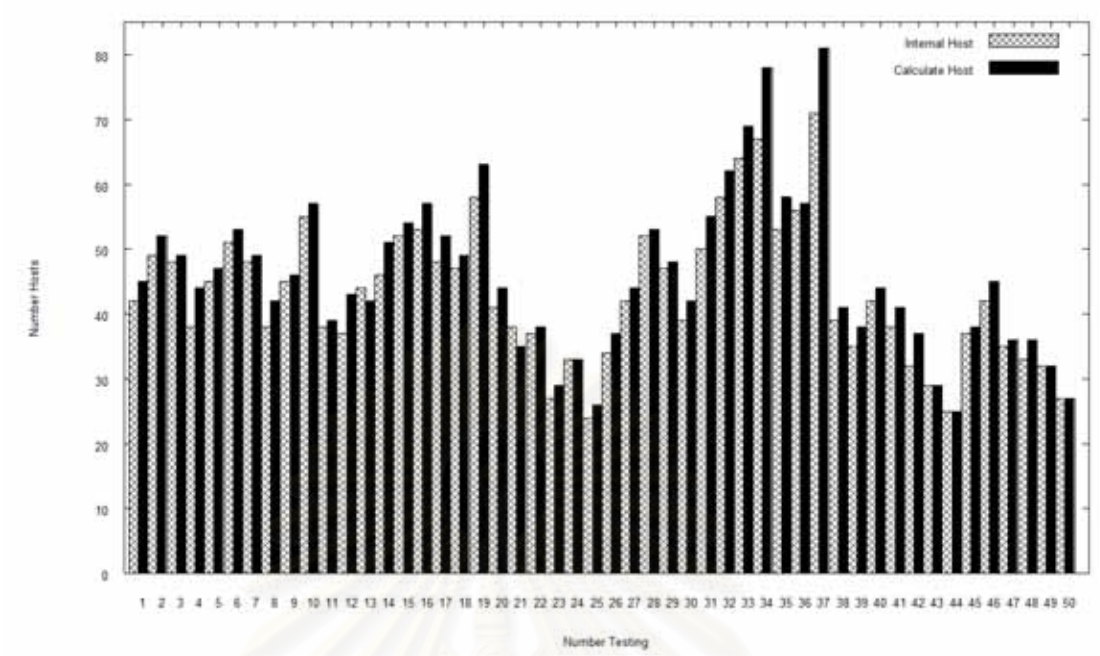
รูปที่ 19 การหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายโดยใช้ช่วงเวลาทดสอบ 3 นาที



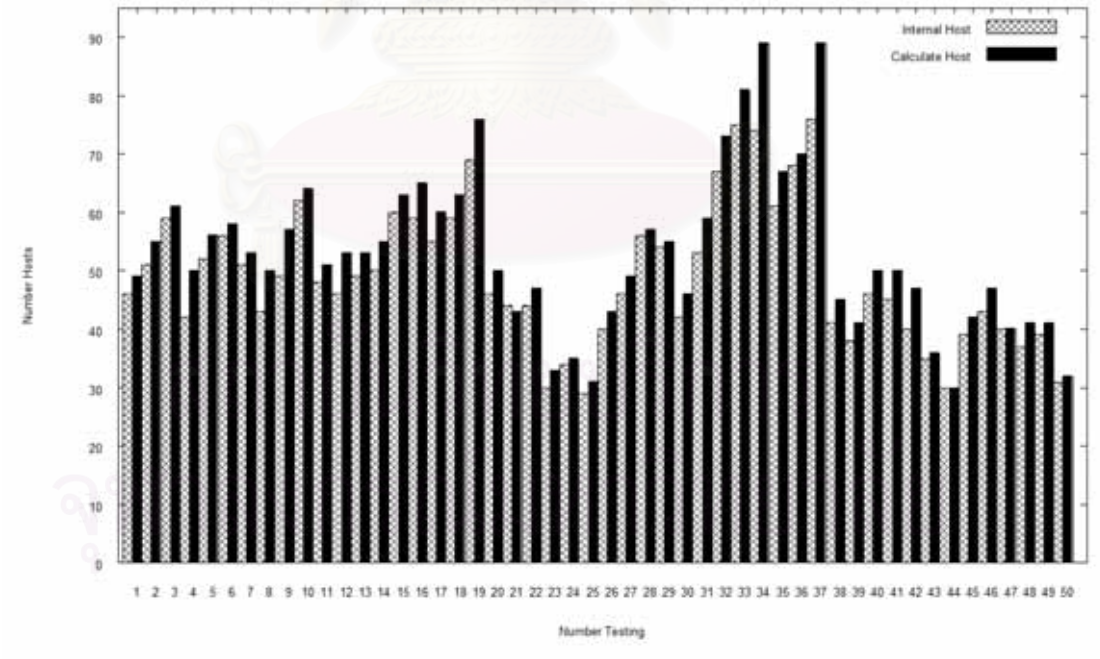
รูปที่ 20 การหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายโดยใช้ช่วงเวลาทดสอบ 5 นาที



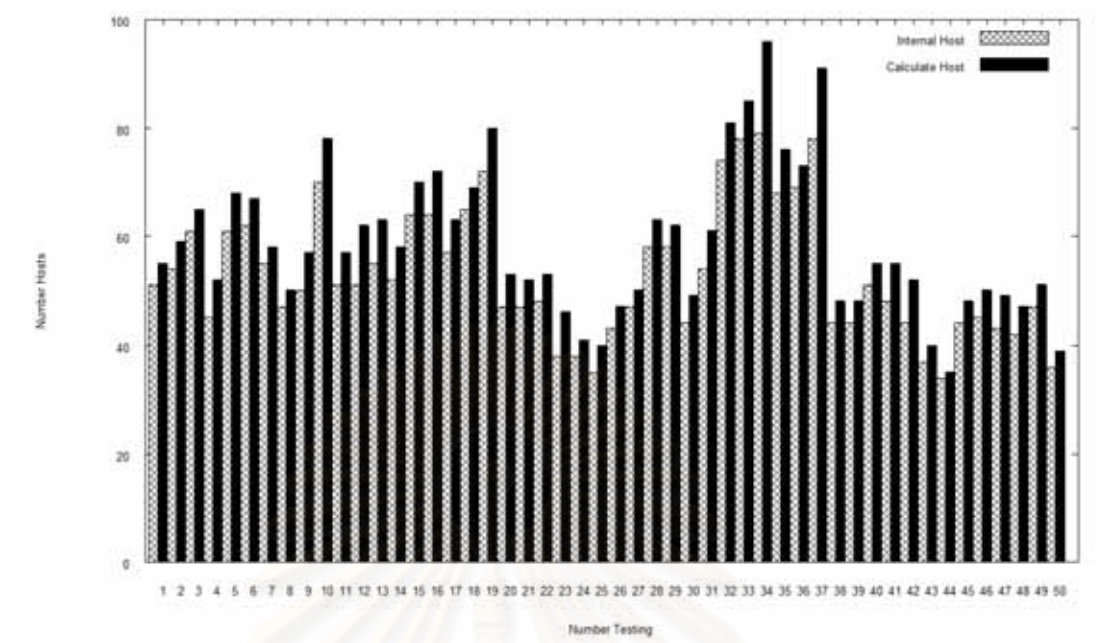
รูปที่ 21 การหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายโดยใช้ช่วงเวลาทดสอบ 7 นาที



รูปที่ 22 การหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายโดยใช้ช่วงเวลาทดสอบ 10 นาที



รูปที่ 23 การหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายโดยใช้ช่วงเวลาทดสอบ 15 นาที



รูปที่ 24 การหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายโดยใช้ช่วงเวลาทดสอบ 20 นาที

ซึ่งจากผลการทดลองจำนวน 50 ตัวอย่าง ที่ยังไม่ได้เปิดวิธีการคาดเดาหมายเลขพอร์ตต้นทางของอุปกรณ์การแปลงที่อยู่เครื่องข่าย จะพบว่าขั้นตอนวิธีที่เสนอสามารถในค่าประสิทธิภาพในการหาจำนวนเครื่องที่ผ่านการแปลงที่อยู่เครือข่ายได้สูง โดยสามารถทำงานได้สูงถึง 99.47% ในช่วงเวลาที่ทดสอบ 1 นาที ซึ่งมีผลบวกลวงเพียง 0.11% (ผลบวกลวงคือการนับจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายได้มากกว่าความเป็นจริง) และผลลบลวงเพียง 0.64% (ผลลบลวงคือการนับจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายได้น้อยกว่าความเป็นจริง) และเมื่อตรวจสอบผลการทดลองโดยนับผลเป็นจำนวนครั้งที่สามารถนับจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายถูกต้องจะพบว่าที่ช่วงเวลาที่ทดสอบ 1 นาที สามารถทำงานได้ถูกต้องมากที่สุดที่ 90% และที่ 88% ในกรณีที่ไม่มีผลบวกลวงและผลลบลวงแฝงในคำตอบ ซึ่งเหตุผลที่ช่วงเวลาทดสอบ 1 นาทีมีค่าความถูกต้องสูงเพราะว่าในช่วงเวลาที่ทดสอบจะมีเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายน้อยกว่าช่วงเวลาทดสอบอื่นๆ และที่ช่วงเวลาทดสอบอื่นที่สูงขึ้นมีค่าความถูกต้องลดลงเป็นลำดับเพราะจำนวนเครื่องที่ผ่านการแปลงที่อยู่เครือข่ายมีจำนวนมากขึ้นตามระยะเวลาทดสอบและพฤติกรรมการใช้งานเครือข่ายของผู้ใช้งาน สรุปการทดลองได้แสดงผลอยู่ในตารางที่ 3

ตารางที่ 3 ความถูกต้องของผลการทดลอง

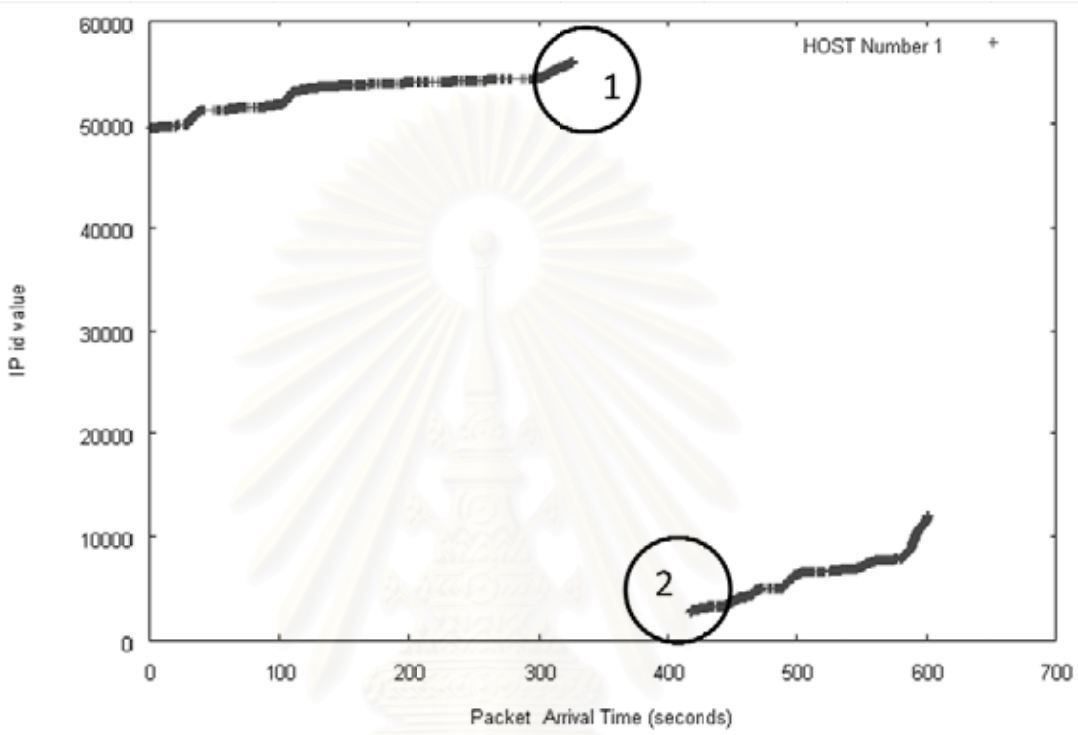
ช่วงเวลาทดสอบ	จำนวนเครื่องเฉลี่ย	ขั้นตอนวิธีปกติ						
		ค่าเฉลี่ยความถูกต้อง	ผลลบลวง	ผลบวกลวง	อัตราส่วนการทำนายได้ถูกต้อง 100%	อัตราส่วนการทำนายได้ถูกต้อง 100% โดยไม่เกิดผลลวง	ค่าทำนายสูงสุด	ความผิดพลาดสูงสุด
1 นาที	18.7	99.47%,±0.03	0.64%	0.11%	90%	88%	31	10.00%
3 นาที	27.3	98.10%,±0.04	0.51%	2.42%	66%	66%	59	11.86%
5 นาที	32.3	97.77%,±0.04	0.81%	3.04%	54%	46%	65	11.53%
7 นาที	35.8	96.93%,±0.04	0.89%	4.19%	32%	24%	70	17.24%
10 นาที	43.2	93.94%,±0.03	0.93%	6.85%	10%	8%	81	16.42%
15 นาที	48.9	91.75%,±0.04	0.86%	9.11%	4%	4%	89	20.27%
20 นาที	52.9	89.05%,±0.03	0.83%	11.78%	0%	0%	96	21.57%

สำหรับสาเหตุเกิดผลบวกลวง และผลลบลวงที่เกิดขึ้นในการทดลอง โดยการวิเคราะห์ผ่านขั้นตอนวิธีที่นำเสนอ แสดงอยู่ในรูปตัวอย่างที่ 25 และ 26 ตามลำดับ

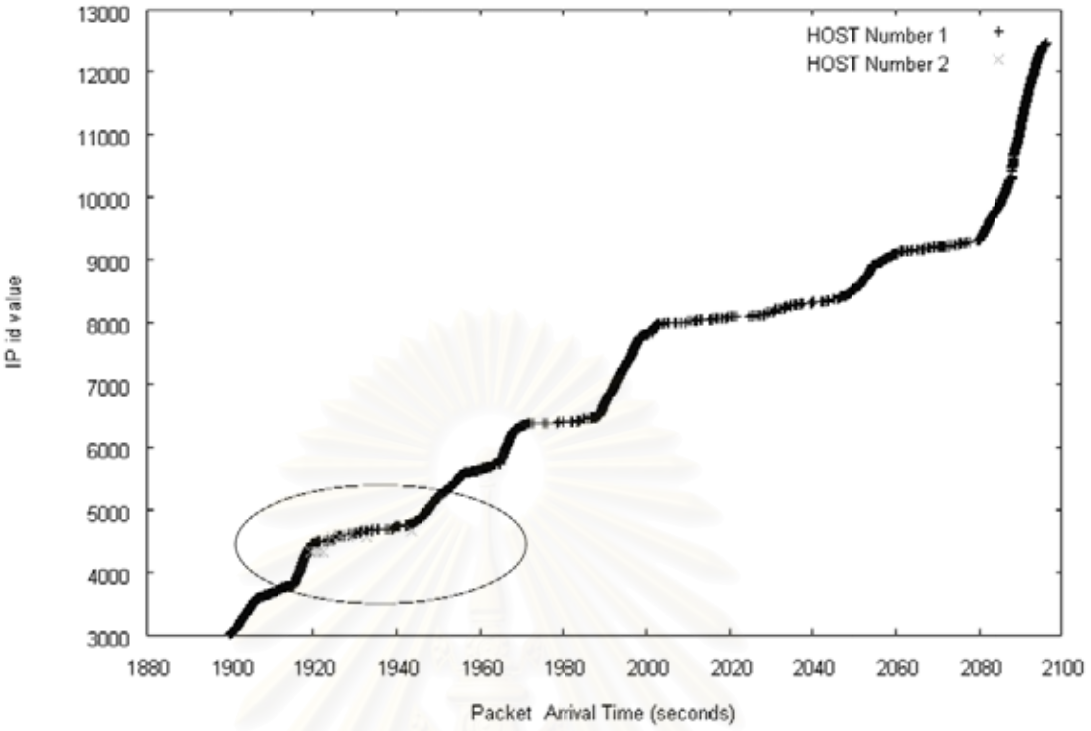
ซึ่งสาเหตุส่วนมากที่ทำให้เกิดผลบวกลวงมักจะเกิดขึ้นจากการที่เครื่องลูกข่ายมีการเชื่อมต่อเครือข่ายออกไปข้างนอกโดยวิธีการการแปลงที่อยู่เครือข่าย หลังจากที่มีการเชื่อมต่อเครือข่ายเสร็จเรียบร้อย แล้วเครื่องลูกข่ายมิได้มีการเชื่อมต่อเครือข่ายภายนอกโดยวิธีการการแปลงที่อยู่เครือข่าย แต่มีการใช้ภายในเครือข่ายส่วนบุคคล เช่นการโอนถ่ายแฟ้มข้อมูล จะทำให้ค่าไอพีดีที่รับได้ใหม่รับจากที่มีการเชื่อมต่อออกเครือข่ายภายนอก จะมีค่าที่เปลี่ยนแปลงโดยไม่สามารถที่จะคาดกรณ์ได้ ดังรูปที่ 25 ค่าไอพีไอดีเปลี่ยนจากวงกลมที่ 1 ไปยังวงกลมที่ 2 ซึ่งสาเหตุพฤติกรรมที่ทำให้เกิดผลบวกลวงนี้สามารถที่จะแก้ไขได้จากวิธีการคาดเดาหมายเลขพอร์ตต้นทางของอุปกรณ์การแปลงที่อยู่เครือข่าย (PP: Port Prediction) โดยจะมีการแสดงผลการทดลองโดยขั้นตอนวิธีที่มีการเพิ่มการคาดเดาหมายเลขพอร์ตต้นทางของอุปกรณ์แปลงที่อยู่เครือข่ายต่อไป

ส่วนสาเหตุส่วนมากที่ทำให้เกิดผลลบลวง มักจะเกิดจากครื่องลูกข่ายที่มีการเชื่อมต่อเครือข่ายภายนอกโดยวิธีการแปลงที่อยู่เครือข่าย เมื่อเริ่มมีการเชื่อมต่อเครือข่าย มีการสุ่มเลือกค่าไอพีดีจากระบบปฏิบัติการของเครื่องลูกข่ายที่ใกล้เคียงกันมากกับเครือลูกข่ายอื่นที่มีการเชื่อมต่อเครือข่ายอยู่ภายในขณะนั้น ซึ่งจะทำให้วิธีการที่เสนอเห็นเครื่องลูกข่ายที่ทำการเชื่อมต่อเครือข่าย

ทั้งสองเครื่องเป็นเครื่องเดียวกัน แต่เสมือนว่าเป็นการเชื่อมต่อไปยังจุดหมายปลายทางที่แตกต่างกัน ซึ่งในกรณีนี้การลดค่าผลลบลวงจะขึ้นอยู่กับปริมาณข้อมูลและคาบเวลาที่ทดสอบ ดังจุดที่วงกลมในรูปที่ 26

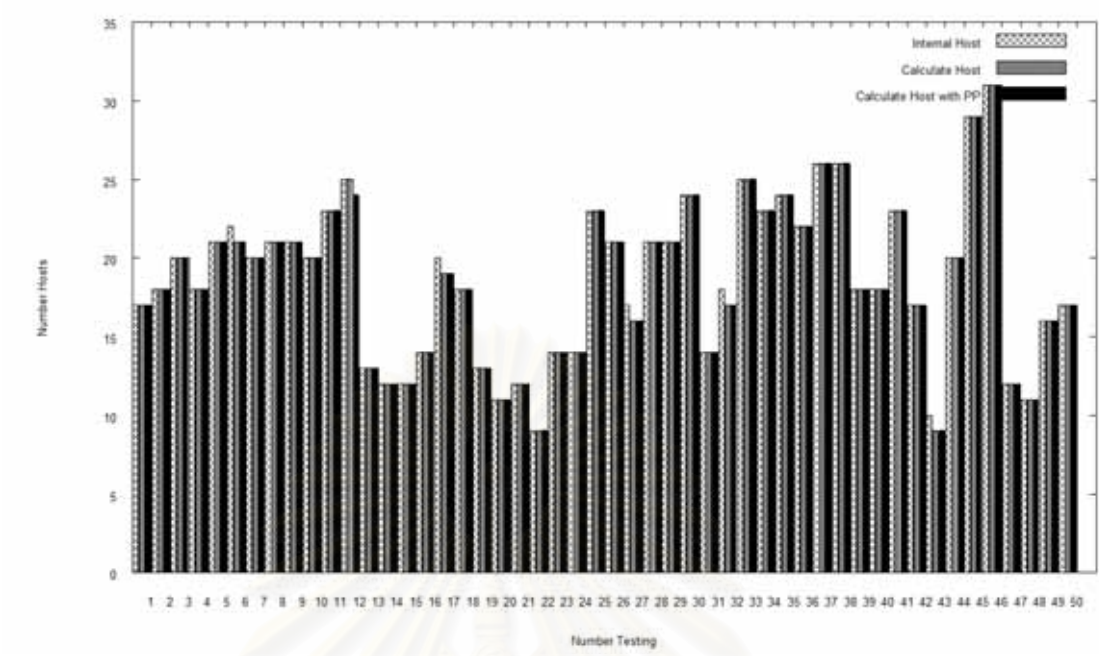


รูปที่ 25 ตัวอย่างสาเหตุการเกิดผลบวกลวงของขั้นตอนวิธีการที่เสนอใหม่

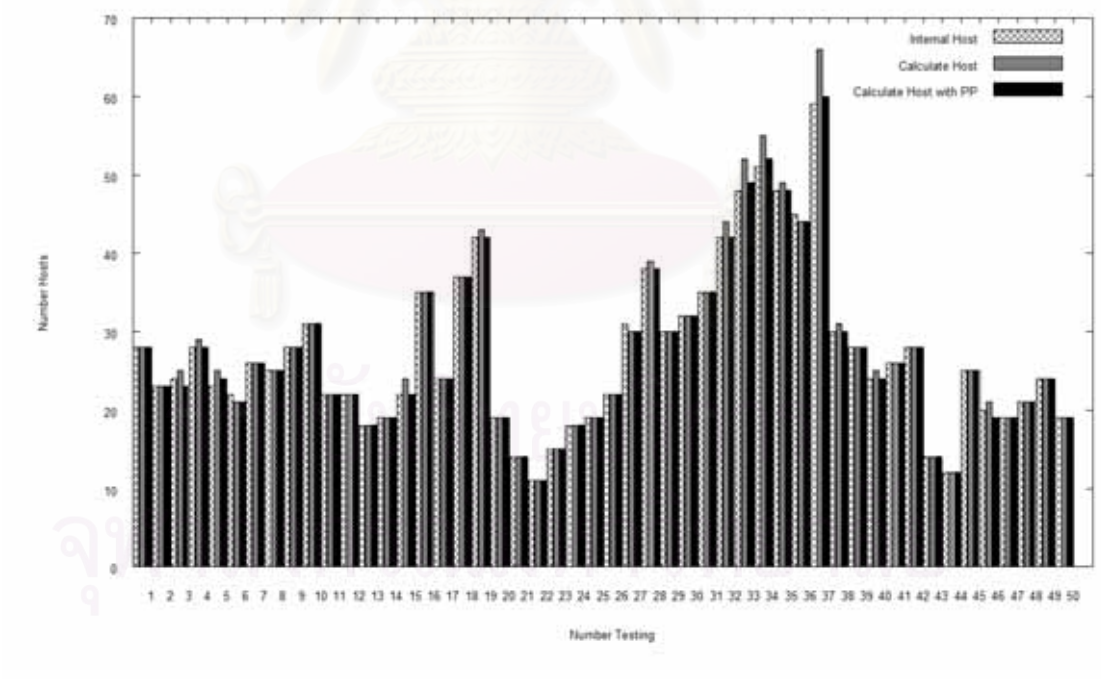


รูปที่ 26 ตัวอย่างสาเหตุการเกิดผลลบลวงของขั้นตอนวิธีการที่เสนอใหม่

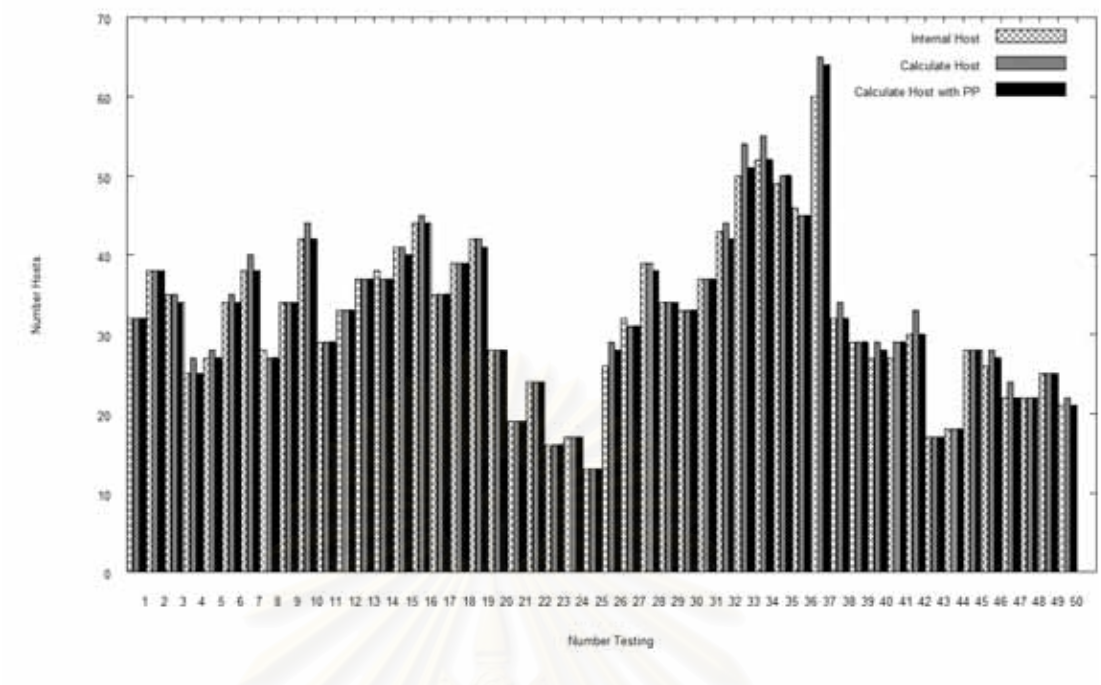
ซึ่งจากทดลองที่ผ่านมา จะเห็นได้ว่ายังมีแนวทางที่จะสามารถลดผลบวกลวงที่เกิดได้จากวิธีการเพิ่มการคาดเดาหมายเลขพอร์ตต้นทางของการใช้งานของทีซีพีโพรโทคอล ซึ่งในการทดลองถัดไปจึงเป็นการทดลองโดยเพิ่มวิธีการคาดเดาหมายเลขพอร์ตต้นทางของอุปกรณ์การแปลงที่อยู่เครือข่ายที่ใช้งาน ซึ่งโดยความเป็นจริงแล้ววิธีการคาดเดาหมายเลขพอร์ตต้นทาง จะขึ้นอยู่กับชนิดอุปกรณ์การแปลงที่อยู่เครือข่ายว่ามีการเลือกหมายเลขพอร์ตการเชื่อมต่อของอุปกรณ์เป็นรูปแบบใด ซึ่งถ้าอุปกรณ์การแปลงที่อยู่เครือข่ายมีการเลือกหมายเลขพอร์ตการเชื่อมต่อแบบสุ่มขั้นตอนวิธีการนี้จะใช้ไม่ได้เลย จึงมีแนวคิดให้ขั้นตอนวิธีการนี้เป็นเพียงตัวเลือกเพิ่มเติมในขั้นตอนวิธีการที่นำเสนอ โดยการทดลองนี้อุปกรณ์การแปลงที่อยู่เครือข่ายที่ใช้ในการทดลองเป็นแบบเรียงลำดับหมายเลขพอร์ตการใช้งานเวลาเชื่อมต่อ ซึ่งผลการทดลองที่ช่วงเวลาทดสอบต่างๆ ได้แสดงผลอยู่ในรูปต่อไปนี้



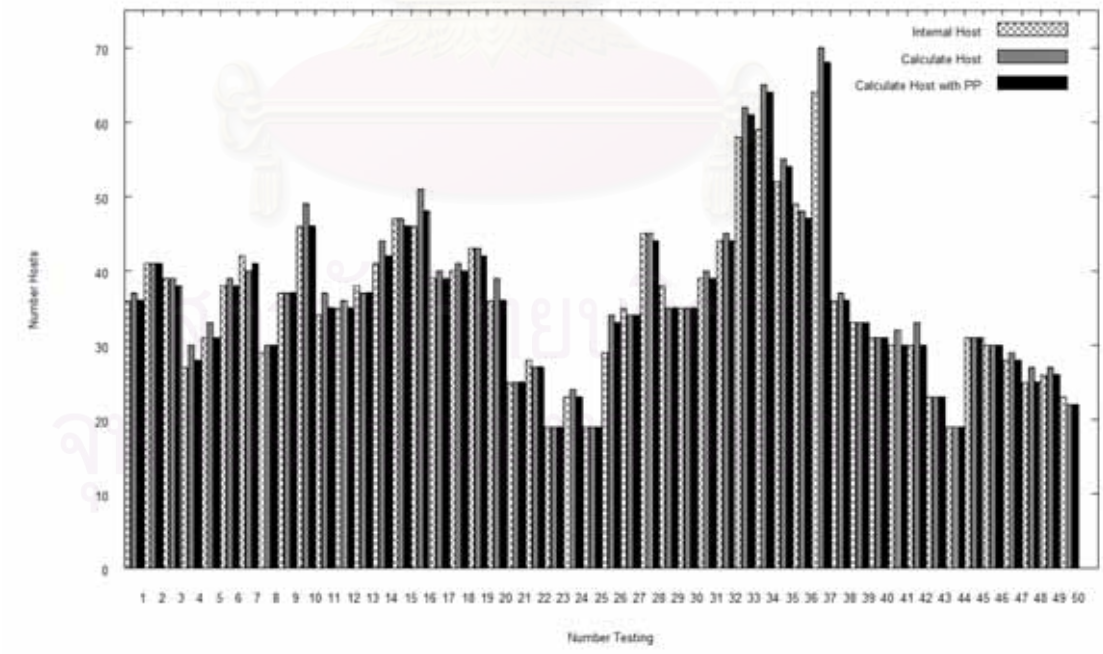
รูปที่ 27 การหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายโดยใช้ช่วงเวลาทดสอบ 1 นาที และมีการคาดเดาหมายเลขพอร์ตต้นทางในขั้นตอนวิธี



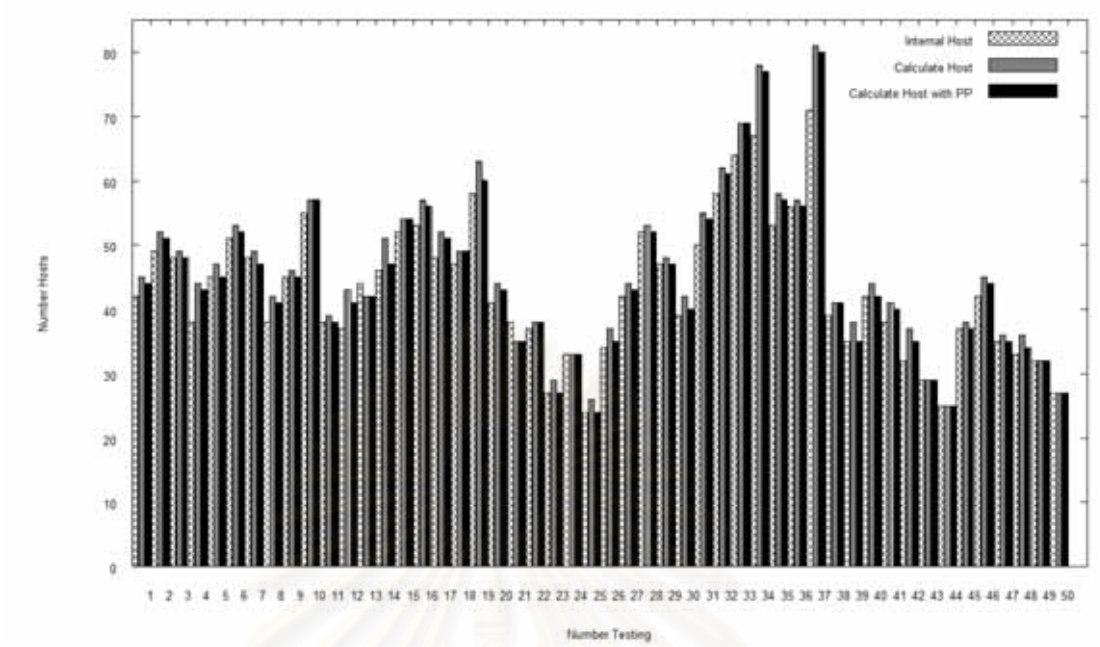
รูปที่ 28 การหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายโดยใช้ช่วงเวลาทดสอบ 3 นาที และมีการคาดเดาหมายเลขพอร์ตต้นทางในขั้นตอนวิธี



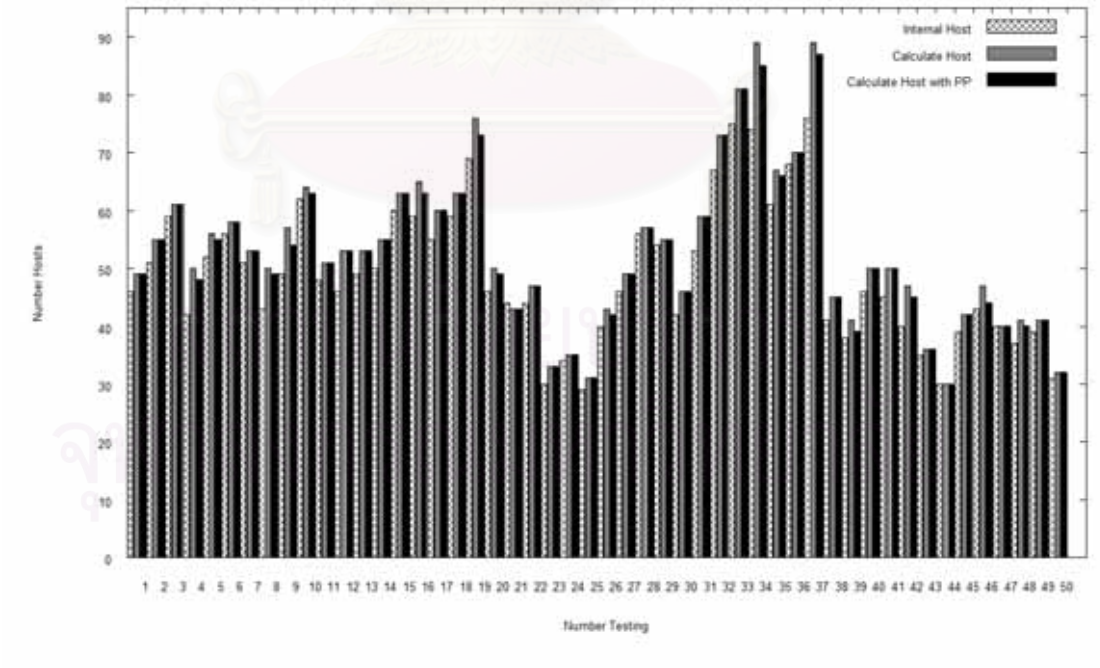
รูปที่ 29 การหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายโดยใช้ช่วงเวลาทดสอบ 5 นาที และมีการคาดเดาหมายเลขพอร์ตต้นทางในขั้นตอนวิธี



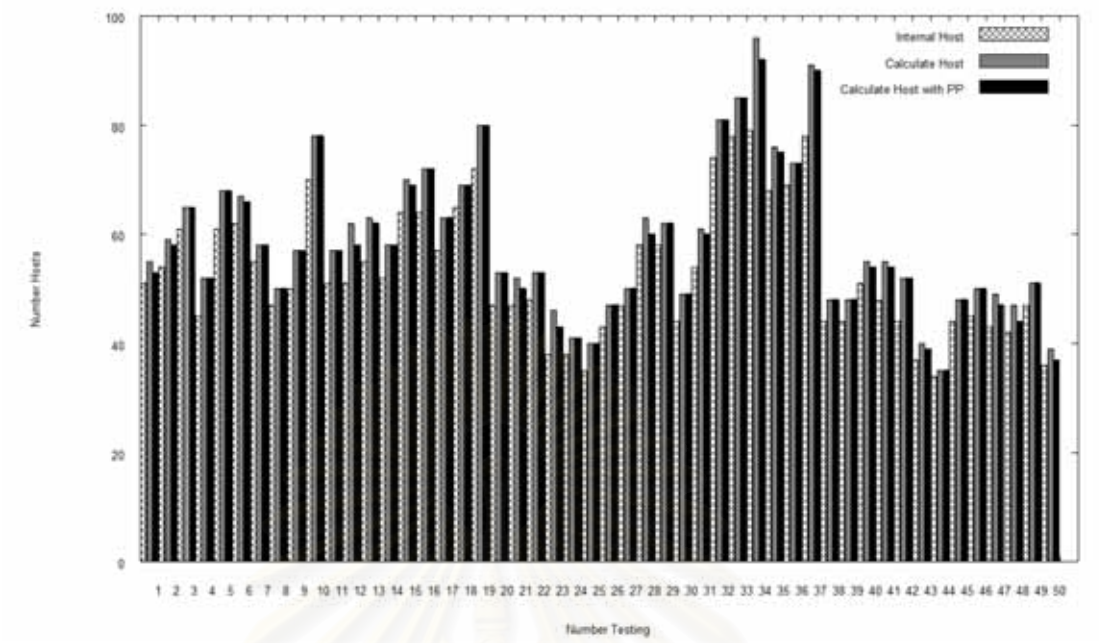
รูปที่ 30 การหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายโดยใช้ช่วงเวลาทดสอบ 7 นาที และมีการคาดเดาหมายเลขพอร์ตต้นทางในขั้นตอนวิธี



รูปที่ 31 การหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายโดยใช้ช่วงเวลาทดสอบ 10 นาที และมีการคาดเดาหมายเลขพอร์ตต้นทางในขั้นตอนวิธี



รูปที่ 32 การหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายโดยใช้ช่วงเวลาทดสอบ 15 นาที และมีการคาดเดาหมายเลขพอร์ตต้นทางในขั้นตอนวิธี



รูปที่ 33 การหาจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายโดยใช้ช่วงเวลาทดสอบ 20 นาที และมีการคาดเดาหมายเลขพอร์ตต้นทางในขั้นตอนวิธี

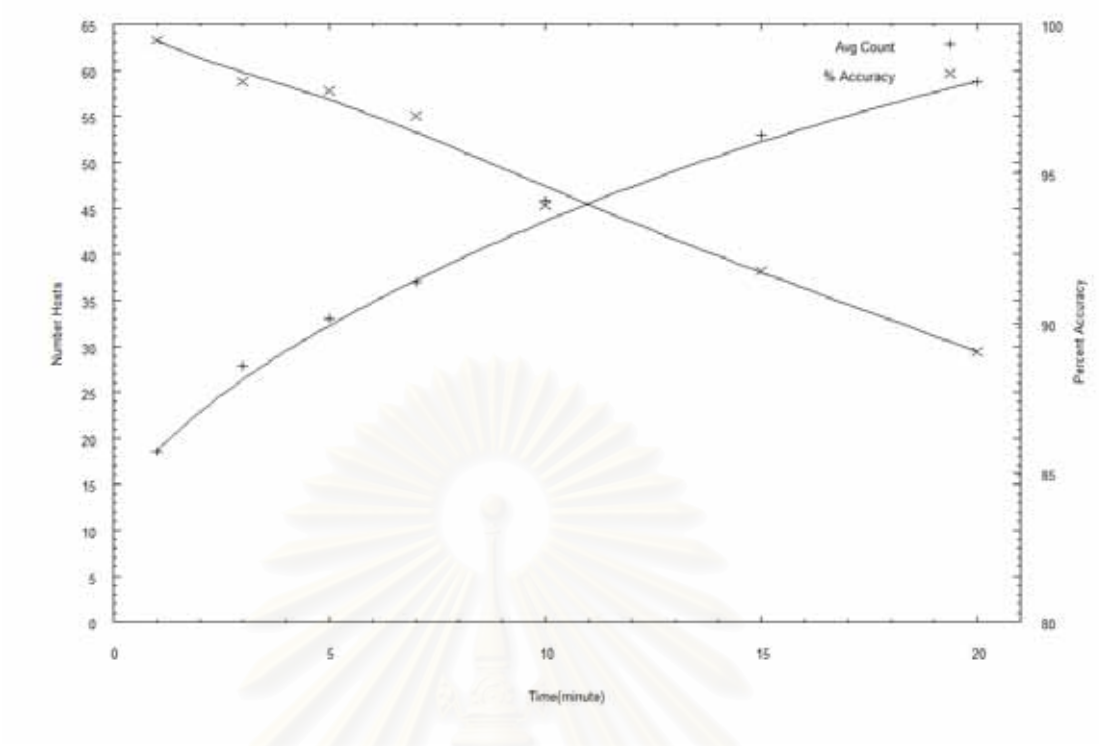
ซึ่งผลจากทดลองจำนวน 50 ตัวอย่าง โดยวิธีการเพิ่มการคาดเดาหมายเลขพพอร์ตต้นทางของอุปกรณ์การแปลงที่อยู่เครือข่ายในทีซีพีโพรโทคอลสามารถสรุปได้ดังนี้คือ จากการที่เพิ่มวิธีการดังกล่าวเข้าไปจะสามารถทำให้ลดผลบวกลวงของการทดลองได้ทุกช่วงเวลาทดสอบโดยจะเห็นได้ว่าที่ช่วงเวลาทดสอบ 1 นาทีผลบวกลวงแทบจะไม่มีการเกิดขึ้นเลย แต่กรณีดังกล่าวในบางครั้งทำให้เกิดผลลบลวงขึ้นมาแทน เพราะจากที่เป็นการคาดเดาหมายเลขพอร์ตต้นทางงานในบางครั้งเครื่องลูกข่ายที่เป็นสองเครื่องทำการเชื่อมต่อไปยังปลายทางเดียวกัน อาจจะมีการใช้งานที่หมายเลขพอร์ตต้นทางที่ต่อเนื่องกัน และมีค่าไอพีไอดีที่ใกล้เคียงกัน จึงทำให้วิธีการนี้ทำการนับจำนวนเครื่องที่ผ่านการแปลงที่อยู่เครือข่ายผิดพลาดโดยเสมือนมองว่าเครื่องลูกข่ายทั้งสองเครื่องนั้นเป็นเครื่องเดียวกัน แต่เหตุกรณ์ที่กล่าวมาเป็นเหตุกรณ์ที่เป็นไปได้น้อยมาก เนื่องจากการที่เชื่อมต่อไปยังปลายทางเดียวกันณ.เวลาที่ใกล้เคียงกันมาก มีการใช้งานหมายเลขพอร์ตต้นทางที่ต่อเนื่องกัน และมีค่าไอพีไอดีที่ใกล้เคียงกันซึ่งในการทดลองจำนวน 50 ตัวอย่างไม่ได้เกิดเหตุกรณ์นี้ขึ้นเลย จากผลการทดลองจะพบว่าค่าเฉลี่ยในการทดลองที่ทุกๆ คาบเวลาทดสอบ จะดีขึ้นเป็นจำนวนมาก โดยเฉพาะที่คาบเวลาทดสอบ 3 นาทีจะพบว่าค่าเฉลี่ยที่ได้จะดีกว่าคาบเวลา 1 นาที สาเหตุที่เป็นเช่นนั้นเนื่องจากค่าผลบวกลวงที่เกิดขึ้นนั้น มีค่าลดลงจากเดิมเป็นจำนวนมาก

เนื่องจากพฤติกรรมของผู้ใช้อินเตอร์โดยทั่วไปส่วนมาก จะมีลักษณะใช้ข้อมูลเครือข่ายจำนวนมากในช่วงต้น แล้วเว้นระยะเวลาช่วงหนึ่งแล้วจึงใช้งานเครือข่ายต่อ ซึ่งในเหตุกรณ์นี้การคาดเดาหมายเลขพอร์ตต้นทางของอุปกรณ์การแปลงที่อยู่เครือข่าย จะเป็นการช่วยได้อย่างมาก (ตัวอย่างเช่นการเปิดเว็บไซต์ในช่วงของการเปิดจะมีการรับส่งข้อมูลจำนวนหนึ่ง หลังจากที่ทำการรับส่งข้อมูลเสร็จแล้ว ผู้ใช้งานมักจะทำการอ่านเนื้อความในเนื้อหาก่อน ซึ่งจะทำให้ไม่มีการรับส่งข้อมูลในช่วงนั้น หลังจากนั้นจึงมีการทำรับส่งข้อมูลใหม่ ซึ่งในกรณีนี้จะทำให้การรับส่งข้อมูลเป็นลักษณะขาดช่วงเป็นระยะๆ โดยลักษณะนี้จะทำให้เกิดผลบวกลวงเกิดขึ้น) ซึ่งผลสรุปการทดลองได้แสดงอยู่ในตารางที่ 4

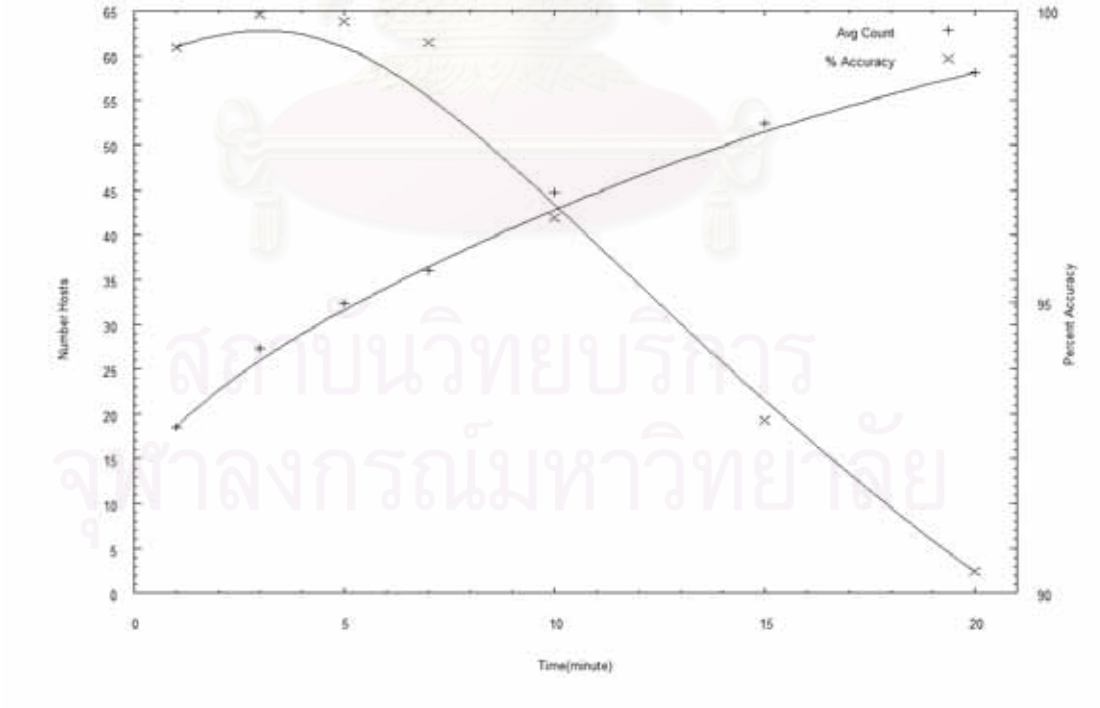
ตารางที่ 4 ความถูกต้องของผลการทดลองในกรณีทดลองที่เพิ่มเรื่องการคาดเดาหมายเลขพอร์ตต้นทางของอุปกรณ์การแปลงที่อยู่เครือข่าย

ช่วงเวลาทดสอบ	จำนวนเครื่องเฉลี่ย	ขั้นตอนวิธีที่มีการเพิ่มการคาดเดาพอร์ตต้นทาง						
		ค่าเฉลี่ยความถูกต้อง	ผลลบลวง	ผลบวกลวง	อัตราส่วนการทำนายได้ถูกต้อง 100%	อัตราส่วนการทำนายได้ถูกต้อง 100% โดยไม่เกิดผลลวง	ค่าทำนายสูงสุด	ความผิดพลาดสูงสุด
1 นาที	18.7	99.36%,±0.03	0.64%	0.00%	88%	88%	31	10%
3 นาที	27.3	99.93%,±0.03	0.51%	0.44%	82%	78%	60	6.67%
5 นาที	32.3	99.81%,±0.04	0.81%	0.99%	68%	60%	64	7.69%
7 นาที	35.8	99.44%,±0.04	0.89%	1.56%	58%	52%	68	8.47%
10 นาที	43.2	96.44%,±0.04	0.97%	4.40%	36%	24%	80	13.43%
15 นาที	48.9	92.98%,±0.04	0.86%	7.88%	4%	4%	87	19.57%
20 นาที	52.9	90.37%,±0.04	0.83%	10.46%	0%	0%	92	18.18%

จากผลการทดลองจะพบว่า ผลบวกลวงได้มีค่าลดลงในทุกช่วงเวลาทดสอบ ซึ่งส่งผลให้ความถูกต้องโดยไม่เกิดผลลวงหรือผลลบลวงในทุกช่วงเวลาทดสอบในการทดลองมีค่าเพิ่ม และจากตารางที่ 3 และ 4 สามารถนำมาสร้างแผนภูมิเพื่อตรวจสอบช่วงเวลาทดสอบที่เหมาะสมเพื่อนำเสนอในขั้นตอนวิธีที่นำเสนอ โดยเลือกจากค่าเฉลี่ยจะนำเครื่องที่ตรวจสอบผล และค่าเฉลี่ยความถูกต้อง ซึ่งแสดงในรูปที่ 34 และ 35 ตามลำดับ



รูปที่ 34 การเลือกช่วงเวลาทดสอบที่เหมาะสมในขั้นตอนวิธี



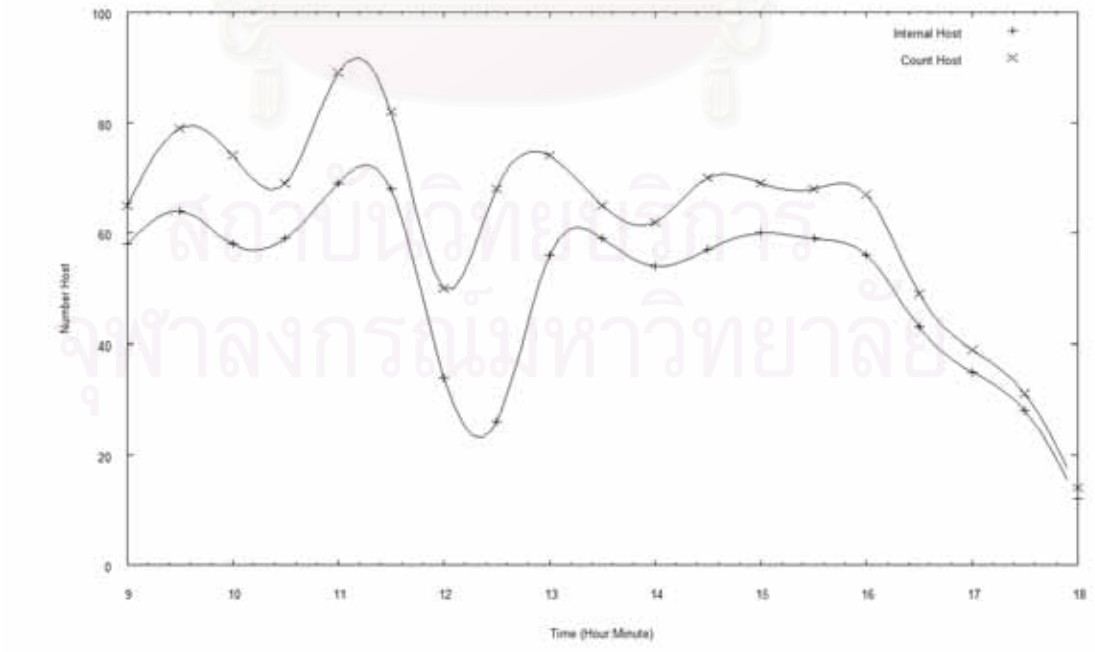
รูปที่ 35 การเลือกช่วงเวลาทดสอบที่เหมาะสมในขั้นตอนวิธีที่มีการเพิ่มการคาดเดาพอร์ตต้นทาง

สรุปผลการทดลองในการเลือกช่วงเวลาการทดสอบจะพบว่า การเลือกช่วงเวลาช่วงทดสอบ ถ้ามีเลือกช่วงเวลาทดสอบสั้นเท่าไรก็จะพบว่าค่าความถูกต้องจะยิ่งมีค่ามาก แต่จะส่งผลกับจำนวนเครื่องลูกข่ายที่นับได้มีจำนวนน้อย ซึ่งสาเหตุที่เป็นเช่นนี้ เนื่องจากพฤติกรรมการใช้งานการเชื่อมเครือข่ายโดยทั่วไปจะไม่ค่อยมีการรับส่งข้อมูลพร้อมกันในช่วงเวลาเดียวกัน ดังนั้นช่วงเวลาทดสอบที่ใช้จะส่งผลกระทบกับจำนวนเครื่องที่นับได้เป็นอย่างมาก ดังนั้นในขั้นตอนวิธีแนะนำให้เลือกค่าช่วงเวลาทดสอบที่ 10 ถึง 11 นาที สำหรับการทดสอบจำนวนหลายๆครั้งเพื่อหาค่าเฉลี่ย เพราะค่าเฉลี่ยนความถูกต้องจะอยู่ที่ 93% ถึง 96% ในกรณีมีการคาดเดาพอร์ตต้นทาง แต่สำหรับกรณีที่ต้องการทดสอบจำนวนครั้งน้อยๆ แนะนำให้ใช้ช่วงเวลาทดสอบที่ 1 ถึง 3 นาทีซึ่งจะมีอัตราส่วนการทำนายถูกต้อง 100% และมีค่าเฉลี่ยความถูกต้องที่สูงเช่นกัน

4.2.2 ผลการทดลองความพยายามหาเครื่องทั้งหมดในเครือข่าย

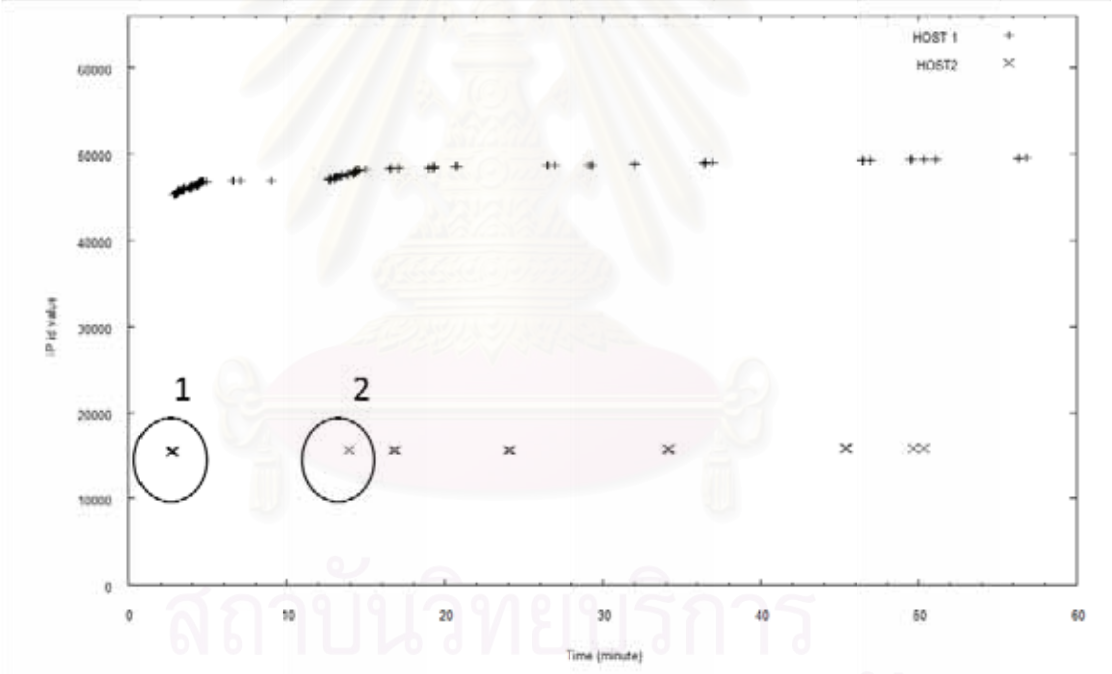
จุดประสงค์ของการทดลองนี้ จะตรวจสอบความเป็นไปได้ที่จะนำขั้นตอนวิธีการที่นำเสนอมานับจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่าย โดยต้องการหาว่าเครื่องลูกข่ายทั้งหมดมีจำนวนเท่าไรที่ผ่านการแปลงที่อยู่เครือข่าย

ซึ่งจากจุดประสงค์ของการทดลองนี้ ผู้วิจัยได้เลือกการตรวจสอบขั้นแรกสุด โดยการทดสอบข้อมูลเครือข่ายตลอดทั้งวันตั้งแต่เวลา 9.00น. ถึง 18.00น. ซึ่งเป็นช่วงเวลาทำงานปกติที่มีการใช้งานเครือข่าย โดยการเลือกคาบเวลาทดสอบทุก 30 นาที ซึ่งผลการทดลองที่ได้แสดงอยู่ในรูปตัวอย่างที่ 36



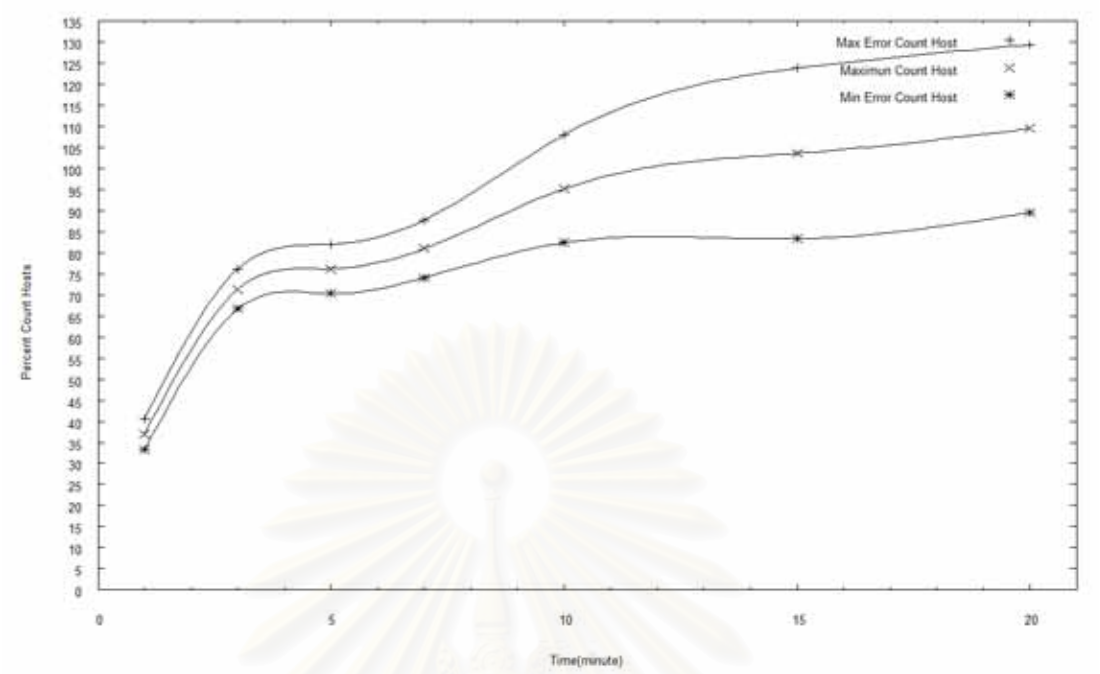
รูปที่ 36 การทดลองโดยเลือกช่วงเวลาทดสอบที่ 30 นาที ช่วงเวลาทดสอบตั้งแต่ 9.00น.-18.00น.

ซึ่งจากการทดลองจะพบว่ามีผลบวกลวงเป็นจำนวนมากในการเลือกช่วงเวลาทดสอบที่ 30 นาที ซึ่งเป็นไปตามการทดลองที่ผ่านซึ่งพบว่ายิ่งมีการเลือกคาบเวลาทดสอบที่มากขึ้น จะทำให้ผลบวกลวงมากขึ้น ซึ่งได้มีการตรวจสอบต่อไปเพื่อหาว่าผลบวกลวงที่เกิดขึ้นไปเป็นเป็นจำนวนมากเกิดจากสาเหตุใด ซึ่งจากข้อมูลเครือข่ายภายในที่แสดงในรูปที่ 37 จะพบว่าเครื่องลูกข่ายเป็นจำนวนมากได้มีการส่งข้อมูลออกมาเป็นจำนวนน้อยๆ ออกไปโดยมีการทิ้งช่วงเวลาในการส่งข้อมูล ดังจากวงกลมที่ 1 ไปยังวงกลมที่ 2 ในรูปที่ 37 ซึ่งสาเหตุที่เกิดขึ้นนี้เนื่องจากเครื่องลูกข่ายที่ทำการทดลองส่วนมากมีการตั้งเวลาในเครื่องแบบอัตโนมัติในการไปตรวจสอบอีเมล์ การกระทำแบบจะทำให้เกิดผลบวกลวงเป็นจำนวนมาก เพราะข้อมูลเครือข่ายที่ได้รับค่าไอพีไอดีที่ได้จะไม่ต่อเนื่อง อีกทั้งเมื่อเครื่องลูกข่ายทิ้งช่วงเวลาไปนานก่อนที่จะมีการแปลงเครือข่ายอีกครั้ง อุปกรณ์การแปลงที่อยู่เครือข่ายก็จะลบสถานะการใช้หมายเลขพอร์ตต้นทางการเชื่อมต่อของเครื่องลูกข่ายนั้นแล้ว ทำให้วิธีการคาดเดาหมายเลขพอร์ตต้นทางไม่สามารถทำได้เช่นกัน



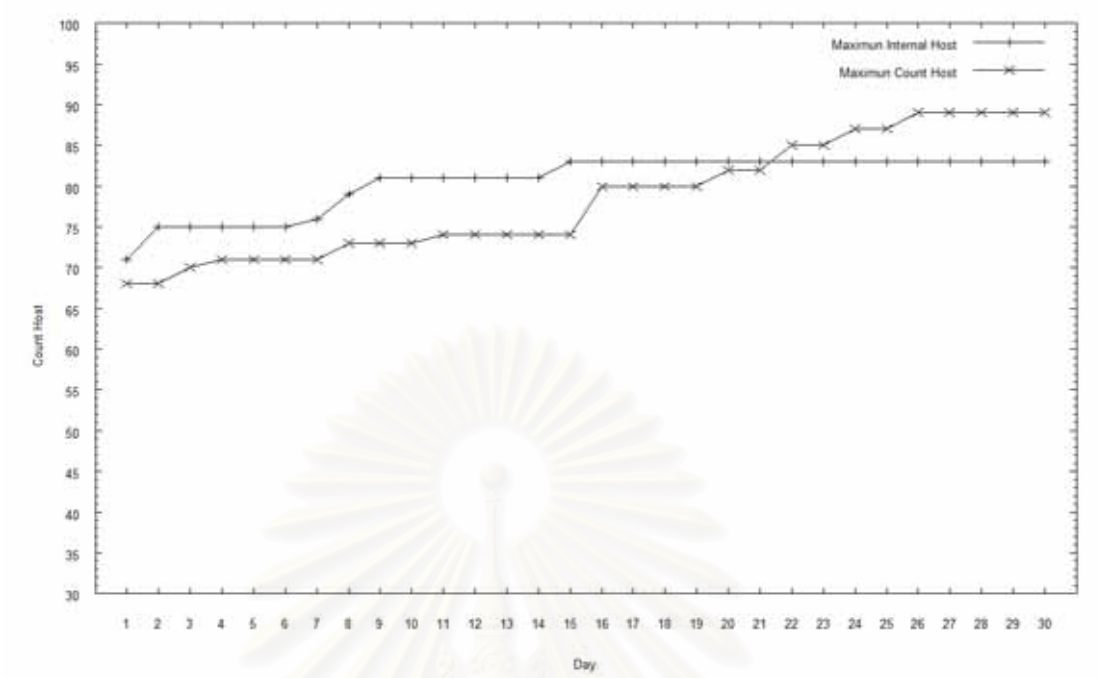
รูปที่ 37 ปัญหาการนับจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่าย
ที่เลือกเวลาทดสอบสูง

จากจุดประสงค์ของการทดลองนี้ ผู้วิจัยจึงได้ทดลองวิธีการนับจำนวนเครื่องที่ผ่านการแปลงที่อยู่เครือข่าย โดยได้ออกแบบการทดลองใหม่โดยใช้หลักสถิติ มีการเลือกช่วงเวลาทดสอบที่สั้นลง โดยได้สร้างแผนภูมิจากค่าสูงสุดในขั้นตอนวิธีที่นับได้ ±ค่าผิดพลาดสูงสุด โดยเทียบกับจำนวนเครื่องในเครือข่ายได้จากตารางที่ 4 เพื่อเลือกช่วงเวลาที่จะนำมาใช้ในการทดลอง แผนภูมิแสดงในรูปที่ 38



รูปที่ 38 การเลือกช่วงเวลาที่ใช้ในการทดลองการพยายามหาเครื่องทั้งหมด

จากรูปที่ 38 ได้เลือกช่วงเวลาทดสอบที่ 10 นาที ซึ่งเป็นช่วงเวลาทดสอบที่ทำให้สามารถนับจำนวนเครื่องลูกข่ายที่ได้ใกล้เคียงกับจำนวนเครื่องทั้งหมด โดยทำการทดลองโดยเลือกใช้ข้อมูลเป็นเวลา 30 วัน โดยในแต่ละวันการทดสอบจะเลือกช่วงเวลา 9.00น. ถึง 18.00น. โดยทดสอบทุกช่วงเวลา 10 นาที แล้วทำการบันทึกหาค่าสูงสุดในแต่ละวันการทดสอบ เพื่อหาค่าสูงสุดในระยะเวลา 30 วัน เพื่อดูค่าเปรียบเทียบที่ได้ ว่ามีค่าเข้าใกล้ความเป็นจริงของเครื่องลูกข่ายทั้งหมดที่ผ่านการแปลงที่อยู่เครือข่ายหรือไหม ซึ่งผลการทดลองแสดงอยู่ในรูปที่ 39



รูปที่ 39 การพยายามหาเครื่องทั้งหมดโดยการใช้ช่วงเวลา 10 นาที โดยใช้ค่าสูงสุดแบบสะสม

จากการผลการทดลองจะสามารถสรุปผลการทดลองได้ว่า จะพบว่าเครื่องลูกข่ายที่มีการแปลงที่อยู่เครือข่ายสูงที่สุดในรอบ 30 วันอยู่ที่ 83 เครื่อง แต่จากทดลองจะพบว่าจะสามารถนับจำนวนหาเครื่องลูกข่ายที่มีการใช้งานการแปลงที่อยู่เครือข่ายตลอด 30 วัน ทุกช่วงเวลาทดสอบ 10 นาทีได้ 89 เครื่องซึ่งสูงกว่าความเป็นจริงอยู่ 6 เครื่องหรือคิดเป็น 7.23% สาเหตุที่เป็นเช่นนี้เพราะในความเป็นจริงแล้วเครื่องลูกข่ายที่มีการแปลงที่อยู่เครือข่ายอาจจะมิได้มีการใช้งานพร้อมกันเป็นจำนวนทั้งหมดภายในเวลา 10 นาที แต่ที่ทำให้ในขั้นตอนวิธีนับนับได้สูงกว่าความเป็นจริงเกิดจากค่าความผิดพลาดของผลลวงบวกที่ได้แสดงอยู่ในรูปที่ 36 ซึ่งทำให้ขั้นตอนวิธีนี้ยังไม่สามารถหาเครื่องที่ผ่านการแปลงที่อยู่เครือข่ายทั้งหมดได้ถูกต้องทั้งหมด

บทที่ 5
สรุปผลการวิจัยและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

ผลลัพทธ์ที่ได้จากงานวิจัยนี้ ทำให้ได้ขั้นตอนวิธีที่ใช้ในการเพิ่มความถูกต้องวิธีการนับจำนวนเครื่องที่ผ่านการแปลงที่อยู่เครือข่ายบนเครือข่ายขนาดกลางโดยใช้ข้อมูลสารสนเทศของชั้นการรับส่งข้อมูล ซึ่งขั้นตอนวิธีดังกล่าวสามารถใช้งานได้ในเครือข่ายที่มีขนาดกลางลงมา โดยขั้นตอนวิธีดังกล่าวมีเงื่อนไขที่เป็นข้อเสนอแนะในการใช้งานดังต่อไปนี้

1. กรณีที่ใช้ในการตรวจสอบเครื่องที่ผ่านการแปลงที่อยู่เครือข่ายโดยต้องการใช้ข้อมูลปริมาณน้อย และจำนวนการทดสอบที่น้อย ขั้นตอนวิธีนี้สามารถใช้ได้มีประสิทธิภาพโดยมีช่วงเวลาทดสอบตั้งแต่ 3 นาทีลงมา โดยอัตราส่วนการทำนายได้ถูกต้อง 100% จะสูงกว่า 66% และมีประสิทธิภาพสูงมากขึ้นเมื่อลดเวลาช่วงทดสอบลงมา แต่จำนวนเครื่องที่ตรวจสอบพบจะเป็นไปตามการใช้งานของผู้ใช้ช่วงเวลาที่ทดสอบนั้น ซึ่งอาจจะไม่ได้มีการแปลงที่อยู่เครือข่ายพร้อมกันในเวลาสั้นๆ ที่เลือกมาทดสอบทำให้เครื่องที่ตรวจสอบพบมีจำนวนน้อย
2. กรณีที่ใช้ในการตรวจสอบเครื่องโดยทดสอบหลายครั้งเพื่อหาค่าเฉลี่ย ขั้นตอนวิธีนี้สามารถทำงานได้มีประสิทธิภาพสูงที่สุดที่ 10 นาทีเทียบกับจำนวนเครื่องที่ตรวจสอบพบ โดยช่วงเวลาทดสอบดังกล่าวมีค่าเฉลี่ยความถูกต้องที่ 93% ในขั้นตอนปกติ และที่ 96% ในขั้นตอนที่มีการคาดเดาพอร์ตต้นทาง
3. ขั้นตอนวิธีที่การคาดเดาพอร์ตต้นทางที่เสนอเป็นเพียงตัวเลือกเพิ่ม สำหรับกรณีที่ผู้นำขั้นตอนวิธีนี้ไปใช้งานสามารถทราบพฤติกรรมการใช้งานพอร์ตของอุปกรณ์การแปลงที่อยู่เครือข่ายที่ต้องการตรวจสอบหาจำนวนเครื่อง เพราะขั้นตอนวิธีนี้ไม่สามารถใช้งานกับอุปกรณ์การแปลงที่อยู่เครือข่ายที่ลักษณะแบบสุ่มพอร์ต
4. กรณีที่ต้องการนำขั้นตอนวิธีไปพยายามหาเครื่องที่ผ่านการแปลงที่อยู่เครือข่ายทั้งหมด ขั้นตอนนี้สามารถทำได้ใกล้เคียงกับความเป็นจริงต่อเมื่อพฤติกรรมของเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายใช้งานพร้อมกันทั้งหมดในช่วงเวลาทดสอบ แต่จากประสิทธิภาพของขั้นตอนวิธีนี้จะลดลงเมื่อเวลาทดสอบที่สูงขึ้น จึงมีความเป็นไปได้ยากที่จะนำขั้นตอนวิธีไปใช้ในการพยายามหาเครื่องที่ผ่านการแปลงที่อยู่เครื่องข่ายทั้งหมด ในกรณีที่เครื่องลูกข่ายไม่ได้มีการใช้งานพร้อมๆกันในช่วงเวลาสั้นๆ

และจากงานวิจัยนี้จะพบว่าขั้นตอนวิธีการนับจำนวนเครื่องที่ผ่านการแปลงที่อยู่เครือข่ายที่เสนอใหม่สามารถทำการทดสอบหาจำนวนเครื่องลูกข่ายได้ภายในช่วงเวลาทดสอบที่สั้น ซึ่งหมายถึงปริมาณข้อมูลสารสนเทศของเครือข่ายที่ต้องทำการจัดเก็บเพื่อนำมาใช้ทดสอบจะมีขนาดที่เล็กลง อีกทั้งยังเป็นการทำให้นำขั้นตอนวิธีการนี้ไปประยุกต์ใช้ในการออกแบบโปรแกรมแอพพลิเคชันที่ทำการนับจำนวนเครื่องลูกข่ายที่ผ่านการแปลงที่อยู่เครือข่ายแบบทันกาลได้ และจากค่าเฉลี่ยความถูกต้องของผลการทดลอง จะพบว่าขั้นตอนวิธีดังกล่าวมีประสิทธิภาพเพียงที่สามารถนำไปประยุกต์ใช้ในงานวิจัยอื่นๆ เช่นงานวิจัยการหาโครงสร้างเครือข่าย[13] งานวิจัยการหาแผนที่ของระบบอินเทอร์เน็ต[14] ซึ่งในงานวิจัยดังกล่าวยังมีข้อจำกัดในการหาปริมาณเครื่องลูกข่ายซึ่งอยู่ภายใต้อุปกรณ์การแปลงที่อยู่เครือข่าย

6.2 ข้อจำกัด

งานวิจัยนี้ในส่วนของขั้นตอนวิธีการที่นำเสนอใหม่ เมื่อได้ทำการทดลองเพื่อหาจำนวนเครื่องลูกข่ายโดยใช้ช่วงเวลาที่ทดสอบสูงขึ้น จะพบว่าค่าผลบวกลวงที่เกิดขึ้นจะสูงขึ้นมากตามไปกับช่วงเวลาที่ทดสอบ ซึ่งข้อจำกัดนี้จะขึ้นอยู่กับพฤติกรรมการใช้เครือข่ายของผู้ใช้ภายในเครือข่ายส่วนบุคคลเป็นหลัก ซึ่งในเครือข่ายส่วนบุคคลแต่ละแห่งอาจจะมีพฤติกรรมเหล่านี้แตกต่างกันไปตามผู้ใช้งาน อีกทั้งการใช้อุปกรณ์แปลงเครือข่ายในแต่ละแห่งอาจจะมีพฤติกรรมที่แตกต่างจะในการทดลอง ซึ่งทำให้เกิดเป็นข้อจำกัดขั้นตอนวิธีที่เสนอ

6.3 แนวทางการวิจัยต่อ

ขั้นตอนวิธีการที่เสนอ เป็นขั้นตอนที่ได้จากการใช้ข้อมูลสารสนเทศในการหาความสัมพันธ์ต่างๆ ของข้อมูลก่อนและหลังการแปลงที่อยู่เครือข่าย ซึ่งในกรณีนี้อาจจะสามารถหาความสัมพันธ์เพิ่มเติมได้ ซึ่งอาจทำได้หลายแนวทาง อาทิเช่น การใช้วิธีการทำเหมืองข้อมูลเพื่อวิเคราะห์ความสัมพันธ์ของข้อมูลสารสนเทศก่อนและหลังการแปลงที่อยู่เครือข่ายได้ อีกทั้งจากทดลองจะพบว่าข้อมูลสารสนเทศในเครือข่ายที่เกิดขึ้นยังมีความสัมพันธ์กับโปรแกรมแอพพลิเคชันที่เครื่องลูกข่ายใช้งานอยู่ขณะนั้น ซึ่งอาจจะใช้เป็นแนวทางศึกษาพฤติกรรมของโปรแกรมแอพพลิเคชันต่างๆ ในการสร้างความสัมพันธ์เพิ่มเติม หรือไม่ว่าจะเป็นการตรวจสอบระดับแอพพลิเคชันโพรโทคอลเพื่อหาพฤติกรรมเพื่อใช้ในการวิจัยการนับจำนวนเครื่องที่ผ่านการแปลงที่อยู่เครือข่ายได้ต่อไป

รายการอ้างอิง

[1] J. Postel, “Internet Protocol,” RFC 791, Internet Engineering Task Force, Sept. 1981.

[2] P. Srisuresh and K. Egevang, “Traditional IP network address translator (traditional NAT),” RFC 3022, Internet Engineering Task Force, Jan. 2001.

[3] M. Bellovin, “A Techique for Counting NATted Hosts,” Internet Measurement Conference (IMC), Nov. 2002.

[4] Honeynet Project, “Know your enemy: Passive fingerprinting,” March 2002, http://project.honeynet.org/papers/finger

[5] G. Huston, “TCP Performance,” Cisco Systems, Jan. 1998.

[6] Ratul Mahajan, Neil T. Spring, and David Wetherall, “Measuring ISP topologies with Rocketfuel,” in *Proceedings of SIGCOMM 2002*, 2002, to appear

[7] J. C. Mogul and S. E. Deering, “Path MTU discovery,” RFC1191, Internet Engineering Task Force, Nov. 1990.

[8] M. Holdrege and P. Srisuresh, “Protocol complications with theIP network address translator,” RFC 3027, Internet Engineering Task Force, Jan. 2001.

[9] D. Senie, “Network address translator (nat)-friendly application design guidelines,” RFC 3235, Internet Engineering Task Force,Jan. 2002.

[10] Jim Reeds, ““Cracking” a random number generator,” *Cryptologia*, vol. 1, no. 1, January 1977.

[11] Jacques Stern, “Secret linear congruential generators are not cryptographically secure,” in *Proceedings of the IEEE Symposium on Foundations of Computer Science*, 1987.

[12] S. Kent and R. Atkinson, “Security architecture for the internet protocol”, RFC 2401, Internet Engineering Task Force, Nov.1998.

[13] R. Govindan and H. Tangmunarunkit, “Heuristics for Internet Map Discovery.” In Proceedings of the 2000 IEEE INFOCOM Conference, Mar. 2000.

[14] H. Tangmunarunkit, R. Govindan, S. Jamin, S. Shenker and W. Willinger, “Network Topology Generators: Degree-Based vs. Structural” In Proceedings ACM SIGCOMM 2002.

[15] S. Guha, Y. Takeda and P. Francis, "NUTSS: A SIP based approach to UDP and TCP connectivity," in *Proceedings of SIGCOMM'04 Workshops*, Portland, OR, Aug 2004.

[16] S. Guha and P. Francis. "Characterization and Measurement of TCP Traversal through NATs and Firewalls," in *Proceedings of Interet Measurement Conference (IMC)*, Berkeley, CA, Oct 2005.

ภาคผนวก

ภาคผนวก ก.
ตัวอย่างข้อมูลสารสนเทศที่ใช้ในงานวิจัย

ตารางที่ 5 แสดงตัวอย่างข้อมูลสารสนเทศที่จัดเก็บภายในเครือข่ายส่วนบุคคล

ID	Protocol	IP_ID	TTL	TOS	SOURCE_IP	SOURCE PORT	DESTINATION IP	DEST PORT	ACK NUMBER	WINDOW SIZE	DATE TIME	TIME MICRO SEC
1100082	TCP	62644	64	0x0	192.168.1.90	51548	61.91.88.114	80	1821700	2896	30/5/2008 16:05:31	2857
1100083	TCP	62645	64	0x0	192.168.1.90	51548	61.91.88.114	80	1821700	39760	30/5/2008 16:05:31	3279
1100084	TCP	62646	64	0x0	192.168.1.90	51548	61.91.88.114	80	1821700	65535	30/5/2008 16:05:31	4149
1100085	TCP	62647	64	0x0	192.168.1.90	51548	61.91.88.114	80	1821700	65535	30/5/2008 16:05:31	33609
1100086	TCP	62648	64	0x0	192.168.1.90	51548	61.91.88.114	80	1824596	65535	30/5/2008 16:05:31	95860
1100087	TCP	62649	64	0x0	192.168.1.90	51548	61.91.88.114	80	1827492	65535	30/5/2008 16:05:31	186611
1100088	TCP	62650	64	0x0	192.168.1.90	51548	61.91.88.114	80	1830388	65535	30/5/2008 16:05:31	258040
1100089	TCP	62651	64	0x0	192.168.1.90	51548	61.91.88.114	80	1833284	65535	30/5/2008 16:05:31	309051
1100090	TCP	16493	128	0x0	192.168.1.74	1065	65.74.180.187	80	773094	64294	30/5/2008 16:05:31	317519
1100091	TCP	62652	64	0x0	192.168.1.90	51548	61.91.88.114	80	1836180	65535	30/5/2008 16:05:31	360095
1100092	TCP	62653	64	0x0	192.168.1.90	51548	61.91.88.114	80	1839076	65535	30/5/2008 16:05:31	412925
1100093	TCP	62654	64	0x0	192.168.1.90	51548	61.91.88.114	80	1841972	65535	30/5/2008 16:05:31	466170
1100094	TCP	62655	64	0x0	192.168.1.90	51548	61.91.88.114	80	1844868	65535	30/5/2008 16:05:31	513192
1100095	TCP	62656	64	0x0	192.168.1.90	51548	61.91.88.114	80	1847764	65535	30/5/2008 16:05:31	544814
1100096	TCP	62657	64	0x0	192.168.1.90	51548	61.91.88.114	80	1850660	65535	30/5/2008 16:05:31	584350
1100097	TCP	62658	64	0x0	192.168.1.90	51548	61.91.88.114	80	1853556	65535	30/5/2008 16:05:31	637353
1100098	TCP	62659	64	0x0	192.168.1.90	51548	61.91.88.114	80	1855004	65535	30/5/2008 16:05:31	679991
1100099	TCP	62660	64	0x0	192.168.1.90	51548	61.91.88.114	80	1857900	65535	30/5/2008 16:05:31	763195
1100100	TCP	62661	64	0x0	192.168.1.90	51548	61.91.88.114	80	1859348	65535	30/5/2008 16:05:31	820855
1100101	TCP	16494	128	0x0	192.168.1.74	1065	65.74.180.187	80	773921	63467	30/5/2008 16:05:31	838619
1100102	UDP	62662	64	0x0	192.168.1.90	51548	61.91.88.114	80	0	0	30/5/2008 16:05:31	847887
1100103	TCP	16496	128	0x0	192.168.1.74	1065	65.74.180.187	80	773921	63467	30/5/2008 16:05:32	29581
1100104	TCP	16497	128	0x0	192.168.1.74	1065	65.74.180.187	80	776841	64512	30/5/2008 16:05:32	436812
1100105	TCP	16498	128	0x0	192.168.1.74	1065	65.74.180.187	80	778301	64512	30/5/2008 16:05:32	512952
1100106	TCP	16499	128	0x0	192.168.1.74	4143	207.46.106.70	1863	90317	63890	30/5/2008 16:05:32	540736
1100107	TCP	16500	128	0x0	192.168.1.74	1065	65.74.180.187	80	781221	64512	30/5/2008 16:05:32	810757
1100108	TCP	16501	128	0x0	192.168.1.74	1065	65.74.180.187	80	782681	64512	30/5/2008 16:05:32	881600
1100109	TCP	16502	128	0x0	192.168.1.74	1065	65.74.180.187	80	785601	61592	30/5/2008 16:05:32	982389
1100110	TCP	16503	128	0x0	192.168.1.74	1065	65.74.180.187	80	788521	58672	30/5/2008 16:05:33	197468
1100111	TCP	16504	128	0x0	192.168.1.74	1065	65.74.180.187	80	789981	60972	30/5/2008 16:05:33	262235
1100112	TCP	16505	128	0x0	192.168.1.74	1065	65.74.180.187	80	792901	58052	30/5/2008 16:05:33	364308
1100113	TCP	62663	64	0x0	192.168.1.90	51549	66.249.89.127	80	214	65535	30/5/2008 16:05:33	375385
1100114	TCP	62664	64	0x0	192.168.1.90	51544	61.91.88.112	80	683	65535	30/5/2008 16:05:33	375516
1100115	TCP	62665	64	0x0	192.168.1.90	51544	61.91.88.112	80	684	65535	30/5/2008 16:05:33	461061

ตารางที่ 6 แสดงตัวอย่างข้อมูลสารสนเทศที่จัดเก็บภายหลังผ่านการแปลงที่อยู่เครือข่าย

ID	Protocol	IP_ID	TTL	TOS	SOURCE PORT	DESTINATION IP	DEST PORT	ACK NUMBER	WINDOW SIZE	DATE_TIME	TIME MICRO SECOND
10000000	UDP	15370	127	0x0	1035	202.8.87.201	53			26/5/2008 11:57:22	847655
10000001	TCP	16315	63	0x0	49773	203.149.1.133	80	34783	65535	26/5/2008 11:57:22	853377
10000002	TCP	16316	63	0x0	49782	203.149.1.136	80	59369	65535	26/5/2008 11:57:22	863854
10000003	TCP	16317	63	0x0	49783	203.149.1.136	80	17377	65535	26/5/2008 11:57:22	870083
10000004	TCP	16318	63	0x0	49779	84.53.136.34	80	17281	65535	26/5/2008 11:57:22	876710
10000005	UDP	56730	127	0x0	65535	80.59.109.174	28400			26/5/2008 11:57:22	878553
10000006	TCP	16319	63	0x0	49729	203.149.1.136	80	21528	65535	26/5/2008 11:57:22	882481
10000007	TCP	16320	63	0x0	49782	203.149.1.136	80	60817	65535	26/5/2008 11:57:22	882501
10000008	TCP	16321	63	0x0	49727	203.149.1.136	80	45494	65535	26/5/2008 11:57:22	882517
10000009	TCP	16322	63	0x0	49780	84.53.136.34	80	25382	65535	26/5/2008 11:57:22	882532
10000010	TCP	16323	63	0x0	49779	84.53.136.34	80	20161	65535	26/5/2008 11:57:22	890081
10000011	UDP	56731	127	0x0	65535	83.54.126.221	18166			26/5/2008 11:57:22	893842
10000012	TCP	16324	63	0x0	49783	203.149.1.136	80	20273	65535	26/5/2008 11:57:22	895504
10000013	TCP	16325	63	0x0	49761	203.149.1.136	80	2734	65535	26/5/2008 11:57:22	901828
10000014	TCP	16326	63	0x0	49782	203.149.1.136	80	63713	65535	26/5/2008 11:57:22	901936
10000015	TCP	16327	63	0x0	49779	84.53.136.34	80	23041	65535	26/5/2008 11:57:22	903823
10000016	TCP	16328	63	0x0	49786	66.198.156.139	80	98156	65535	26/5/2008 11:57:22	904562
10000017	TCP	16329	63	0x0	49787	66.198.156.139	80	98156	65535	26/5/2008 11:57:22	904599
10000018	TCP	16330	63	0x0	49783	203.149.1.136	80	23169	65535	26/5/2008 11:57:22	921948
10000019	TCP	16331	63	0x0	49783	203.149.1.136	80	26065	65535	26/5/2008 11:57:22	940706
10000020	TCP	16332	63	0x0	49783	203.149.1.136	80	28961	65535	26/5/2008 11:57:22	953322
10000021	TCP	16333	63	0x0	49779	84.53.136.34	80	25921	65535	26/5/2008 11:57:22	956894
10000022	TCP	16334	63	0x0	49783	203.149.1.136	80	31857	65535	26/5/2008 11:57:22	966057
10000023	TCP	16335	63	0x0	49729	203.149.1.136	80	21528	65535	26/5/2008 11:57:22	966567
10000024	TCP	16336	63	0x0	49727	203.149.1.136	80	45494	65535	26/5/2008 11:57:22	968873
10000025	TCP	16337	63	0x0	49783	203.149.1.136	80	34753	65535	26/5/2008 11:57:22	978762
10000026	TCP	16338	63	0x0	49757	203.149.1.136	80	31339	65535	26/5/2008 11:57:22	990160
10000027	UDP	15372	127	0x0	1035	202.8.87.201	53			26/5/2008 11:57:22	991567
10000028	TCP	16340	63	0x0	49783	203.149.1.136	80	37649	65535	26/5/2008 11:57:22	991733
10000029	TCP	16341	63	0x0	49783	203.149.1.136	80	40545	65535	26/5/2008 11:57:23	4237
10000030	TCP	16342	63	0x0	49729	203.149.1.136	80	23165	65535	26/5/2008 11:57:23	11180
10000031	TCP	16343	63	0x0	49788	203.149.1.133	80	1491	65535	26/5/2008 11:57:23	13500
10000032	TCP	16344	63	0x0	49789	203.149.1.133	80	1491	65535	26/5/2008 11:57:23	13540
10000033	TCP	56732	127	0x0	2727	61.229.234.132	15991	29234	65535	26/5/2008 11:57:23	18761
10000034	TCP	16345	63	0x0	49783	203.149.1.136	80	43441	65535	26/5/2008 11:57:23	18824
10000035	TCP	16346	63	0x0	49783	203.149.1.136	80	46337	65535	26/5/2008 11:57:23	31335
10000036	TCP	16347	63	0x0	49727	203.149.1.136	80	46486	65535	26/5/2008 11:57:23	36246
10000037	TCP	56733	127	0x0	2732	86.159.8.127	34568	1	65535	26/5/2008 11:57:23	41295
10000038	TCP	56734	127	0x0	2732	86.159.8.127	34568	1	65535	26/5/2008 11:57:23	41308
10000039	TCP	16348	63	0x0	49757	203.149.1.136	80	31340	65535	26/5/2008 11:57:23	42201
10000040	TCP	16349	63	0x0	49783	203.149.1.136	80	49233	65535	26/5/2008 11:57:23	48944
10000041	TCP	16350	63	0x0	49788	203.149.1.133	80	1	65535	26/5/2008 11:57:23	52133
10000042	TCP	16351	63	0x0	49788	203.149.1.133	80	1	65535	26/5/2008 11:57:23	53102

ประวัติผู้เขียนวิทยานิพนธ์

นายธนาภูมิ แดนมณี เกิดเมื่อวันที่ 2 ตุลาคม พ.ศ. 2516 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาหลักสูตรปริญญาวิศวกรรมศาสตร (วศ.บ.) สาขาวิศวกรรมโยธา คณะวิศวกรรมศาสตร์ มหาวิทยาสงขลานครินทร์ ในปีการศึกษา 2540 และเข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิทยาศาสตร์คอมพิวเตอร์ ที่ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2549