การประชุมวิชาการระดับชาติ “มหาวิทยาลัยบูรพา ๒๕๕๔” ๖ – ๗ กรกฎาคม ๒๕๕๔ ณ มหาวิทยาลัยบูรพา

รูปแบบการติดตั้งตัวกรองข้อความสแปม เพื่อลดปริมาณการส่งข้อมูลในเครือข่าย

Spam Filtering installation Location to Reduce the Network Traffic

สิทธิพร พุ่มพวง[1] เนื่องวงศ์ ทวยเจริญ[2]

[1,2] บัณฑิตศึกษาสาขาวิชาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม คณะวิศวกรรมศาสตร์

มหาวิทยาลัยธุรกิจบัณฑิตย์ กรุงเทพฯ

E-mail: [1]smallnoi@hotmail.com, [2]nuengwong.tun@dpu.ac.th

บทคัดย่อ

งานวิจัยนี้ได้พัฒนาระบบจดหมายอิเล็กทรอนิกส์ขึ้น ภายในกองยุทธการและการข่าว กรมพลาธิการทหารบก เพื่อเป็นการปฏิบัติตามมติคณะรัฐมนตรี เมื่อวันที่ 18 ธันวาคม พ.ศ.2550 ที่ให้ข้าราชการและพนักงานของรัฐยุติการใช้งานอีเมลฟรีของเอกชน ทั้งนี้ เพื่อแก้ปัญหาการรั่วไหลข้อมูลลับของทางราชการ

อย่างไรก็ตาม ในปัจจุบัน ผู้ให้บริการอีเมลต้องเสียพื้นที่และค่าใช้จ่ายไปกับสแปมเมลถึง 97% ดังนั้น การใช้ตัวกรองข้อความสแปมที่มีประสิทธิภาพจะสามารถลดค่าใช้จ่ายได้อย่างมหาศาล

ดังนั้น งานวิจัยนี้จึงศึกษาผลความแตกต่างของตำแหน่งการติดตั้งตัวกรองข้อความสแปมระหว่างตำแหน่งของแม่ข่ายและตำแหน่งของลูกข่าย โดยมีวัตถุประสงค์เพื่อออกแบบการติดตั้งตัวกรองข้อความสแปม เพื่อลดปริมาณการส่งข้อมูลในเครือข่าย

จากการวัดประสิทธิภาพของตัวกรองข้อความสแปมด้วยปริมาณการจราจรบนเครือข่าย พบว่า เมื่อติดตั้งตัวกรองข้อความสแปมที่เครื่องลูกข่าย สามารถลดปริมาณการจราจรลงได้ถึง 72.38% และเมื่อติดตั้งตัวกรองยังเครื่องแม่ข่าย ตัวกรองข้อความสแปมสามารถลดปริมาณการจราจรลงได้ถึง 81.55%

ดังนั้น ตัวกรองข้อความสแปมในฝั่งลูกข่ายสามารถลดปริมาณการส่งข้อมูลในเครือข่ายได้ใกล้เคียงกับตัวกรองที่ฝั่งแม่ข่าย พร้อมทั้งลดภาระการทำงานที่เครื่องแม่ข่าย ด้วยเหตุนี้ การติดตั้งตัวกรองข้อความสแปมในฝั่งลูกข่ายจึงเป็นอีกทางเลือกหนึ่งในการกรองข้อความสแปมที่น่าสนใจในอนาคต

คำสำคัญ-- Spam Mail; ระบบกรอง Spam Mail;

Abstract

Due to Thailand Cabinet Resolution on December 18th, 2007, the government agencies have to discontinue using free private email services, which lead to the disclosure of the government classified information. This research has developed an electronic mail system for the Battle and News Division, the Department of the Army Quartermaster.

However, a recent research indicates that most e-mail service providers need to waste 97% of space and money with spam mails. Therefore, an effective spam filter can reduce costs dramatically.

Therefore, this research is to study the impact of installing the spam-mail filters, i.e. server-side installation versus client-side installation. The objective is to explore various installation locations in the mail system architecture for the purpose of reducing the network traffic.

The experimental results show that installing the spam filter at the client can reduce the traffic up to 72.38%, while installing the filter at the server can reduce traffic up to 81.55%.

In conclusion, the client-side spam filter can reduce the network traffic as effective as the server-side filters. Also, it reduces the workload on the server as well. Additionally, the effectiveness of the client-side filtering can be improved if the filter is included in the default feature of a web browser, which will process all web mail forms. Therefore, client-side spam filtering is a promising alternative in spam filter.

Keywords: Spam Mail; Spam Mail Filter;

บทนำ

งานวิจัยนี้ได้พัฒนาระบบจดหมายอิเล็กทรอนิกส์ขึ้นภายในกองยุทธการและการข่าว กรมพลาธิการทหารบก เพื่อเป็นการปฏิบัติตามมติคณะรัฐมนตรี เมื่อวันที่ 18 ธันวาคม พ.ศ.2550 (รัฐบาลไทย , 2550) ที่ให้ข้าราชการและพนักงานรัฐยุติการใช้งานอีเมลฟรีของเอกชน ทั้งนี้ เพื่อแก้ปัญหาการรั่วไหลข้อมูลลับของทางราชการ อย่างไรก็ตาม ระหว่างที่หน่วยงานของรัฐได้ดำเนินการตามมตินี้อย่างค่อยเป็นค่อยไป การปฏิบัติตามมตินี้จำเป็นต้องพิจารณาถึงปัญหาด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างยิ่ง เนื่องจากปัจจุบันอีเมลได้กลายเป็นช่องทางการสื่อสารที่สำคัญที่กลุ่มอาชญากรไซเบอร์ใช้ในการสร้างความเสียหาย โดยเฉพาะอย่างยิ่งในรูปแบบของสแปมเมล (Spam Mail)

สแปมเมล หมายถึง จดหมายอิเล็กทรอนิกส์ที่ผู้ส่ง (ซึ่งมักจะไม่ปรากฏชื่อและที่อยู่ของผู้ส่ง) ได้ส่งไปยังผู้รับอย่างต่อเนื่อง โดยส่งจำนวนครั้งละมาก ๆ และมิได้รับความยินยอมจากผู้รับ โดยการส่งสแปมเมลนั้นอาจมีวัตถุประสงค์ในเชิงพาณิชย์หรือไม่ก็ได้ ซึ่งในปัจจุบันการส่งสแปมเมลนั้นสามารถส่งผ่านได้โดยทางอีเมล หรือทางโทรศัพท์มือถือเป็นข้อความสั้น (SMS) อย่างไรก็ตาม งานวิจัยนี้จะกล่าวถึงแต่การส่งสแปมเมล ทางไปรษณีย์อิเล็กทรอนิกส์เท่านั้น

องค์กรธุรกิจที่จดทะเบียน Domain จะมีที่อยู่ไอพี (IP Address) เป็นหลักแหล่ง ทำให้สแปมเมลสามารถส่งมาถึงได้โดยไม่มีสิทธิหลีกเลี่ยง นั่นหมายถึงค่าใช้จ่ายในการใช้งานอีเมลที่เพิ่มขึ้น พร้อม ๆ กับการสูญเสียทรัพยากรไปกับกองขยะ โดยเฉพาะ Mailbox จะต้องเสียค่าใช้จ่ายตามจำนวนข้อความที่ได้รับ เสียทั้งเวลา ทรัพยากร และเงินทุนของบริษัทในการดาวน์โหลดอีเมลขยะ นอกจากนี้ในปัจจุบันการเข้าถึงอีเมลสามารถเข้าถึงได้ด้วยช่องทางพิเศษ เช่น การเปิด

อีเมลผ่านระบบโทรศัพท์มือถือ ที่คิดค่าใช้จ่ายตามจำนวน Bandwidth ที่ใช้งาน เพราะฉะนั้นผู้ใช้ต้องเสียค่าใช้จ่ายให้อีเมลขยะ (Spam Mail) เป็นจำนวนมาก โดยไม่จำเป็น

ในปัจจุบันการใช้งานอีเมลส่วนใหญ่ผู้ให้บริการต้องเสียพื้นที่และค่าใช้จ่ายไปกับสแปมเมลถึง 97% (Microsoft,2554) ดังนั้นการใช้ตัวกรองสแปมที่มีประสิทธิภาพจะสามารถลดค่าใช้จ่ายได้อย่างมหาศาล

อย่างไรก็ตาม การติดตั้งโปรแกรมตรวจสอบและบล็อกข้อความสแปมสามารถทำได้หลายตำแหน่ง เช่น ที่เครื่องแม่ข่าย ที่เครื่องลูกข่าย หรือติดตั้งในอุปกรณ์เครือข่ายเช่น เราต์เตอร์ ซึ่งแต่ละตำแหน่งอาจให้ผลการกรองต่างกัน งานวิจัยนี้จึงต้องการศึกษาผลความแตกต่างของตำแหน่งการติดตั้งตัวกรองข้อความสแปม เพื่อลดปริมาณการส่งข้อมูลในเครือข่าย

วัตถุประสงค์

เพื่อออกแบบการติดตั้งตัวกรองข้อความสแปมที่สามารถลดปริมาณการส่งข้อมูลในเครือข่ายได้อย่างมีประสิทธิภาพ

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

จากอดีตทีผ่านมา มีการพัฒนาตัวกรองสแปมเมลอย่างแพร่หลาย ทั้งการพัฒนาด้านอัลกอริทึมในการวิเคราะห์ข้อความสแปม ได้แก่ (นนท์ ,2552) และ (Fidelis,2006) (Gordon,2007) (S. Dixit ,2005) และงานวิจัยด้านแนวคิดการกรองสแปม ได้แก่

1) การกรองสแปมเมลด้วยระบบ Whitelist (เวิลด์ไซเบอร์เซอร์วิส ,2554) ทำการตรวจสอบอีเมลของผู้ส่งกับรายการในบัญชี Whitelist หากไม่ปรากฏเบอร์อีเมลผู้ส่งในรายการบัญชีก็แสดงว่าอีเมลนั้นเป็นสแปม ให้ทำการลบทิ้งหรือคัดแยกไปไว้ในตู้สแปม เป็นต้น ข้อเสียของระบบนี้คือ มีข้อผิดพลาดสูงเนื่องจากผู้ที่มาติดต่อธุรกิจรายใหม่ อาจจะไม่มีรายชื่ออยู่ในบัญชี Whitelist ทำให้องค์กรหรือหน่วยงานพลาดโอกาสทางธุรกิจ

2) ระบบจดหมายอิเล็กทรอนิกส์กลางภาครัฐ “เมล์โกไทย” (สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ , 2550) การทำงานระบบเมลของ สบทร. การติดตั้งตัวกรองสแปม(โปรแกรม Mail Cleaner) จะติดตั้งตัวกรองที่ Server ของผู้ให้บริการ โดยกรองจดหมายขยะของผู้ใช้ ด้วยวิธีการเพิ่มข้อความ "[SPAM?]" ลงบนหัวจดหมาย จากนั้นก็ใช้ความสามารถของโปรแกรมอ่านอีเมลในการแยกจดหมายขยะ ที่มีคำว่า "[SPAM?]" ออกจากเมล์ปกติ

3) การกรองสแปมเมลด้วยระบบ Blacklist (กอบเกียรติ ,2552) เป็นระบบพื้นฐานที่นิยมใช้ทั่วไป ทำโดยการเก็บไอพีของเครื่องเซิร์ฟเวอร์ที่ส่งสแปมไว้ในฐานข้อมูล เพื่อทำการสกัดกั้นเมล

ที่ส่งมาจากเครื่องดังกล่าว จากงานวิจัยการกรองสแปมจากบอทเน็ต พบว่าการวิเคราะห์เฮดเดอร์ของอีเมล ด้วยระบบ Blacklist สามารถลดปริมาณ สแปมได้ ร้อยละ 96.23

4) การกรองสแปมเมลด้วยระบบเก็บเป็นลายเซ็น Signature (nectec,2554) โดยนำข้อความอีเมลผ่านฟังก์ชั่น Hash แล้วเก็บไว้เป็นข้อมูลลายเซ็นอีเมล ซึ่งเรียกว่า Signature อีเมลที่เป็นสแปมจะถูกบันทึกลายเซ็นเก็บไว้ในฐานข้อมูล เพื่อทำการเปรียบเทียบกับอีเมลที่เข้ามาใหม่ต่อไป

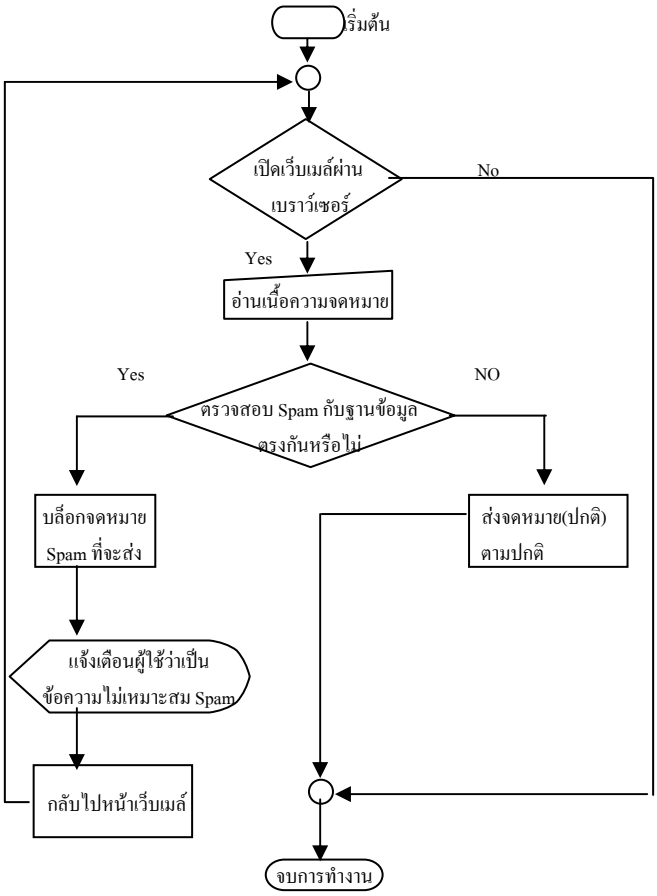
อย่างไรก็ตามงานวิจัยเหล่านี้เน้นการกรองสแปมเมลที่เครื่องแม่ข่ายเท่านั้น การติดตั้งตัวโปรแกรมตรวจสอบและบล็อกข้อความสแปมสามารถทำได้หลายตำแหน่งและให้ผลต่างกันได้ จึงเป็นที่มาของงานวิจัยชิ้นนี้

วิธีการวิจัย

งานวิจัยนี้ได้ทำการพัฒนาระบบเว็บเมลสำหรับที่กองยุทธการและการข่าว กรมพลาธิการทหารบก และติดตั้งตัวกรองข้อความสแปม โดยมีการดำเนินการดังนี้

*1. **การตรวจสอบข้อความไม่เหมาะสม***

ตัวกรองข้อความสแปมในงานวิจัยนี้ เป็นเพียงตัวอย่างการกรองข้อความสแปมอย่างง่ายที่ให้ความถูกต้องสูง และสามารถนำมาใช้งานทั่วไปได้ และเป็นตัวกรองที่กรองขณะส่งข้อความเพียงทางเดียว โดยใช้การเทียบคำในอีเมลที่ผู้ใช้ส่งกับคำในฐานข้อมูลข้อความไม่เหมาะสม ดังรูปที่ 1



รูปที่ 1 ผังงานโปรแกรมตรวจสอบข้อความไม่เหมาะสม (Spam)

รูปที่ 1 แสดงผังงานโปรแกรมตรวจสอบข้อความที่ไม่เหมาะสมสำหรับเครื่องคอมพิวเตอร์ลูกข่ายที่เรียกใช้งานระบบรับ – ส่งอีเมล ซึ่งส่วนนี้จะทำการตรวจสอบข้อความ (Text) ต่างๆ ที่ผู้ใช้เรียกใช้งานระบบรับ – ส่งอีเมลการทำงานในการตรวจสอบข้อความไม่เหมาะสม (Spam) ในฝั่ง client เป็นแบบอัตโนมัติ เมื่อผู้ใช้ทำการกรอกข้อความอีเมลผ่านโปรแกรมเบราว์เซอร์ และทำการคลิกปุ่ม Send เว็บเบราว์เซอร์จะนำข้อความดังกล่าวไปตรวจสอบด้วยการเปรียบเทียบกับรายชื่อของข้อความที่ไม่เหมาะสม โดยได้รับการสนับสนุนข้อมูลดังกล่าวจากบริษัท กสท. (นนท์ ,2552) ที่ได้เก็บไว้ในฐานข้อมูลของโปรแกรม หากพบว่าตรงกัน ระบบจะทำการป้องกันไม่ให้ส่งข้อความดังกล่าวไปยังเมล์เซิร์ฟเวอร์ เพื่อเป็นการลดปริมาณสแปมเมลที่จะเกิดขึ้นในระบบ

จากนั้นโปรแกรมจะทำการแจ้งเตือนผู้ใช้งานว่าจดหมายนี้มีเนื้อหาที่ไม่เหมาะสมเข้าข่ายการกระทำความผิดกฎหมาย มาตรา 11 (สำนักงานปลัดกระทรวง,2550) การส่งข้อความ Spam และระบบจะทำการบล็อกข้อความดังกล่าว พร้อมแจ้งเตือนผู้ใช้ในการกระทำความผิดนั้นทันที

2. การปรับปรุงฐานข้อมูลข้อความไม่เหมาะสม

เนื่องจากในงานวิจัยนี้เน้นการศึกษาที่ตำแหน่งการติดตั้งตัวกรองข้อความสแปม ซึ่งยังไม่ได้รวมถึงในส่วนของการปรับปรุงฐานข้อมูลแบบออนไลน์ ดังนั้น เราได้ใช้ฐานข้อมูลข้อความไม่เหมาะสมได้รับมาจากบริษัท กสท. (นนท์,2552) และผู้ดูแลระบบจะเป็นผู้ปรับปรุงแก้ไข ลบ เพิ่ม ฐานข้อมูลรายชื่อข้อความที่ไม่เหมาะสมด้วยตนเอง ซึ่งในงานวิจัยในอนาคต จะมีการเพิ่มเติมกลไกการปรับปรุงฐานข้อมูลข้อความไม่เหมาะสมแบบอัตโนมัติต่อไป

ผลการวิจัย

ในงานวิจัยนี้ได้มีการประเมินประสิทธิภาพของตัวกรองข้อความสแปมบนเว็บเมล์ที่พัฒนาขึ้นในมิติต่างๆ ดังต่อไปนี้

1) การประเมินประสิทธิภาพของผู้ให้บริการไปรษณีย์อิเล็กทรอนิกส์ต่างๆ ได้แก่ Hotmail Yahoo และ Gmail

2) การวัดความแม่นยำและถูกต้องของตัวกรองข้อความสแปมที่พัฒนาขึ้น

3) เปรียบเทียบผลการกรองจากการติดตั้งตัวกรองข้อความสแปมต่างสถานที่ และ

4) วิเคราะห์ผลการทดลอง

1. การประเมินประสิทธิภาพของผู้ให้บริการไปรษณีย์อิเล็กทรอนิกส์ต่าง ๆ

เราได้ทำการส่งข้อความจากข้อมูลทดสอบจำนวน 2,000 ข้อความ แบ่งเป็นข้อความปกติจำนวน 1,000 ข้อความ และข้อความสแปมจำนวน 1,000 ข้อความ โดยได้รับการสนับสนุนข้อความดังกล่าวจากบริษัท กสท. (นนท์,2552) และข้อความทั้งหมดถูกส่งโดยมนุษย์ทีละข้อความ ผลปรากฏว่า Microsoft Outlook 2003 , hotmail , gmail และ yahoo นั้นทำการส่งข้อความทั้ง 2,000 ข้อความ โดยไม่สามารถบล็อกข้อความที่เป็นสแปมได้ ดังแสดงในตารางที่ 1

ตารางที่ 1 ผลการประเมินประสิทธิภาพของผู้ให้บริการไปรษณีย์อิเล็กทรอนิกส์ต่างๆ

รายการประเมินประสิทธิภาพการทำงานของโปรแกรม	จำนวนชุดข้อมูล	ระดับประสิทธิภาพของโปรแกรม (จำนวนข้อความที่กรองได้)				
		เว็บเมล์	hotmail	gmail	yahoo	outlook
ข้อความปกติ	1000	1000	1000	1000	1000	1000
ข้อความ Spam	1000	956	0	0	0	0

สาเหตุที่เป็นเช่นนั้นเพราะผู้ให้บริการอีเมลเหล่านั้นเน้นการป้องกันสแปมอีเมลจาก Spam Bot เท่านั้น โดยไม่สามารถป้องกันการส่งสแปมจากมนุษย์ได้ ดังนั้นผู้ให้บริการอีเมลเหล่านี้จึงใช้ลักษณะการยืนยันตัวตน คือ CAPTCHA ซึ่งทำหน้าที่ตรวจสอบว่าคุณเป็นมนุษย์หรือไม่ ขณะที่กำลังโพสข้อความอยู่ เพื่อป้องกัน Spam Bot เท่านั้น

ดังนั้น งานวิจัยนี้จึงเสนอการกรอง Spam แบบอัตโนมัติที่สามารถป้องกันการส่งข้อความ Spam จากมนุษย์ได้ ซึ่งหากผู้ใช้ที่เป็นมนุษย์ทำการส่งข้อความที่เป็น Spam ระบบจะทำการบล็อกข้อความดังกล่าวทันที พร้อมแจ้งเตือนการกระทำความผิดให้ผู้ใช้รับทราบ

2. การวัดความถูกต้องแม่นยำของตัวกรองข้อความสแปมที่พัฒนาขึ้น

เราได้ทำการพัฒนาตัวกรองสแปมบนเว็บเมลอย่างง่าย โดยการเปรียบเทียบคำในฐานข้อมูลคำที่ไม่เหมาะสม ซึ่งได้รับการสนับสนุนจากบริษัท กสท. (นนท์,2552) ผลการทดสอบการทำงานของตัวกรองที่ได้พัฒนาขึ้น แสดงในตารางที่ 1 ในช่องเว็บเมล ซึ่งข้อมูลจากตารางที่ 1 แสดงให้เห็นว่าระบบตรวจสอบและบล็อกข้อความสแปมอย่างง่ายที่ใช้ในงานวิจัยนี้ มีความถูกต้องของการกรองข้อความ สแปมเฉลี่ยที่ 95.6% และความถูกต้องในการกรองข้อความปกติ 100%

3. เปรียบเทียบผลการกรองจากการติดตั้งตัวกรองข้อความสแปมต่างสถานที่

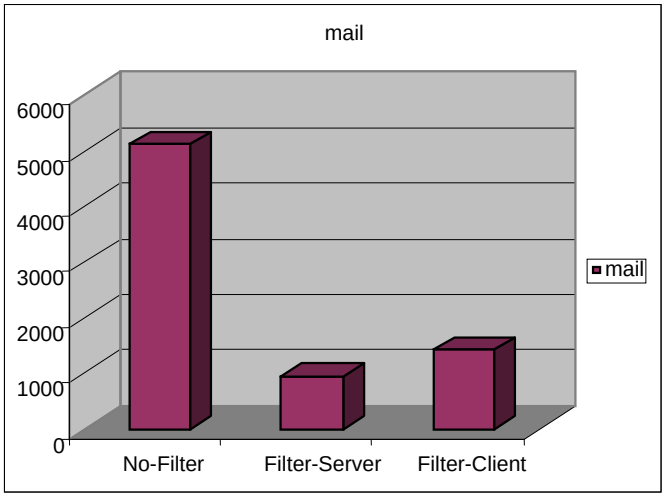
เราได้ทำการทดสอบระบบ ด้วยการติดตั้งตัวกรองข้อความสแปมต่างสถานที่ที่กรมพลาธิการทหารบก จำนวน 2 ตำแหน่งด้วยกัน โดยนำ ตัวกรองข้อความสแปมที่พัฒนาขึ้นไปทำการติดตั้งยัง

(1) เว็บเบราว์เซอร์ของเครื่องลูกข่าย (client) และ

(2) เครื่องแม่ข่ายผู้ให้บริการจดหมายอิเลกทรอนิกส์ (mail server)

เพื่อทำการเปรียบเทียบประสิทธิภาพของตัวกรองที่ติดตั้งต่างสถานที่ โดยพิจารณาประสิทธิภาพด้านการลดปริมาณการจราจรบนเครือข่ายเป็นหลัก ซึ่งโดยทั่วไป สามารถวัดได้จากปริมาณการจราจรที่เกิดขึ้นจริง ในหน่วยของ packet ซึ่งในการทดสอบระบบนี้ เราสนใจเฉพาะข้อมูลอีเมลบนเครือข่ายที่เกิดขึ้นจริง เราได้ทำการเก็บข้อมูลปริมาณการจราจรบนเครือข่ายที่มีการใช้งานจริงเป็นเวลา 4 สัปดาห์ ที่กองยุทธการและการข่าว กรมพลาธิการทหารบก โดยเครื่อง mail server เปิดให้บริการตามเวลาราชการ (0900–1200 น. และ 1300-1600น.) และปิดบริการนอกเวลาราชการ

รูปที่ 2 และตาราง 2 ถึง 4 แสดงผลการทดลองในรูปแบบปริมาณข้อมูลในช่วงเวลาที่ไม่มีการติดตั้งตัวกรองข้อความสแปม (No_Filter) ช่วงที่มีการติดตั้งตัวกรองข้อความสแปมยังตำแหน่งเครื่องแม่ข่าย (Server)และติดตั้งตัวกรองข้อความยังเครื่องลูกข่าย (Client) เพื่อศึกษาถึงผลความแตกต่างของตำแหน่งการติดตั้งตัวกรองข้อความสแปมในเครือข่ายต่อประสิทธิภาพของตัวกรองข้อความสแปม โดยเก็บปริมาณการจราจรเฉพาะข้อมูลอีเมลในแต่ละวิธีในรูปแบบ Packet ข้อมูล



รูปที่ 2 ปริมาณการจราจรข้อมูลบนเครือข่ายในภาพรวม

จากรูปที่ 2 พบว่าปริมาณข้อมูลเฉพาะอีเมลในช่วงเวลาที่ไม่ติดตั้งตัวกรองข้อความสแปมมีปริมาณข้อมูลรวม 5,117 packet เมื่อติดตั้งตัวกรองยังเครื่องแม่ข่าย (Server) มีปริมาณข้อมูลเฉพาะอีเมลรวม 944 packet (คิดเป็น 18.45%) และเมื่อติดตั้งตัวกรองข้อความสแปมยังเครื่องลูกข่าย (Client) มีปริมาณข้อมูลเฉพาะอีเมลรวม 1,413 packet (คิดเป็น 27.61%) ดังนั้นตัวกรองข้อความ

สแปมที่ฝั่ง Client มีประสิทธิภาพต่างจากตัวกรองข้อความสแปมที่ฝั่ง Server โดยเฉลี่ยเพียง 9.21% เท่านั้น ดังแสดงในตารางที่ 2

ตารางที่ 2 ข้อมูลการจราจรเฉพาะอีเมลบนเครือข่ายแยกตามสัปดาห์

ห้วงเก็บข้อมูล	No-Filter	Filter-Server		Filter-Client	
สัปดาห์ที่ 1	1208	248	20.53%	297	24.59%
สัปดาห์ที่ 2	864	163	18.87%	269	31.13%
สัปดาห์ที่ 3	1623	291	17.93%	465	28.65%
สัปดาห์ที่ 4	1422	242	17.02%	382	26.86%
รวม	5,117	944	18.45%	1,413	27.61%

ตารางที่ 3 แสดงข้อมูลการจราจรเฉพาะอีเมลบนเครือข่าย โดยแบ่งตามรายชั่วโมงที่เปิดให้บริการ เมื่อเปรียบเทียบปริมาณข้อมูลการจราจรบนเครือข่ายพบว่า ในช่วงเวลาที่มีปริมาณข้อมูลอีเมลจำนวนมาก (14.00 – 16.00 น.) ตัวกรองที่ Client ยิ่งเพิ่มความสามารถในการลดปริมาณข้อมูลที่เกิดจากสแปมลงได้ใกล้เคียงกับตัวกรองที่ติดตั้งที่ Server

ตารางที่ 3 ปริมาณข้อมูลอีเมลเฉลี่ยบนเครือข่าย รายชั่วโมง

Time	no_filter	server		client	
900	140	43	30.7%	80	57.14%
1000	701	125	17.83%	187	26.68%
1100	928	386	41.59%	592	63.79%
1300	611	156	25.53%	245	40.10%
1400	1169	197	16.85%	272	23.27%
1500	1231	37	3.01%	37	3.01%
1600	337	0		0	

จากตารางที่ 4 แสดงข้อมูลการจราจรเฉพาะอีเมลบนเครือข่าย โดยแบ่งตามวัน (จันทร์ – ศุกร์) เมื่อเปรียบเทียบปริมาณข้อมูลการจราจรบนเครือข่ายพบว่า การติดตั้งตัวกรองข้อความสแปมที่ Client สามารถลดปริมาณข้อมูลที่เกิดจากข้อความสแปมต่อวันลงได้ใกล้เคียงกับตัวกรองที่ Server (~10%)

ตารางที่ 4 ปริมาณข้อมูลอีเมลเฉลี่ยบนเครือข่ายแยกตามวัน

Day	จันทร์	อังคาร	พุธ	พฤหัส	ศุกร์
no_filter	1145	1397	522	1196	857
Server	203 (17.7%)	297 (21.3%)	38 (7.3%)	216 (18.1%)	190 (22.2%)
Client	327 (28.6%)	446 (31.9%)	75 (14.4%)	349 (29.2%)	216 (25.2%)

จากผลการเปรียบเทียบปริมาณข้อมูลข้างต้นแสดงให้เห็นว่า แม้ตัวกรองข้อความสแปมที่พัฒนาขึ้น จากการส่งตัวอย่างกลุ่มข้อมูลตามตารางที่ 1 จะให้ค่าความถูกต้องในการกรองเท่ากันที่ 95.6% แต่เมื่อเก็บข้อมูลการใช้งานจริง ด้วยปริมาณ Packet พบว่าการติดตั้งตัวกรองข้อความสแปมต่างสถานที่กลับให้ค่าการกรองที่แตกต่างกัน เมื่อติดตั้งตัวกรองข้อความสแปมยังเครื่องแม่ข่าย(Server) พบว่าสามารถลดปริมาณข้อมูลอีเมลลงได้เฉลี่ย 81.55 % และเมื่อติดตั้งตัวกรองข้อความสแปมยังเครื่องลูกข่าย (Client) พบว่าสามารถลดปริมาณข้อมูลอีเมลลงได้เฉลี่ย 72.38%

ดังนั้น ตัวกรองข้อความสแปมในฝั่ง Client สามารถลดปริมาณการส่งข้อมูลในเครือข่ายได้ใกล้เคียงกับฝั่ง Server โดยลดภาระการทำงานที่ Server อีกด้วย ถึงแม้ว่า ในงานวิจัยนี้จะใช้ตัวอย่างตัวกรอง เป็นตัวกรองข้อความสแปมอย่างง่ายก็ตาม ด้วยเหตุนี้ การติดตั้งตัวกรองข้อความสแปมในฝั่งลูกข่ายจึงเป็นอีกทางเลือกหนึ่งในการกรองข้อความสแปมที่น่าสนใจในอนาคต

สรุปผลการวิจัยและข้อเสนอแนะ

งานวิจัยนี้ได้ทำการพัฒนาระบบเว็บเมล์สำหรับที่กองยุทธการและการข่าว กรมพลาธิการทหารบก และติดตั้งตัวกรองข้อความสแปม จากการประเมินประสิทธิภาพของตัวอย่างตัวกรองสแปมอย่างง่าย พบว่า เมื่อทำการส่งข้อมูลทดสอบไปยังตัวกรองสแปมอย่างง่าย พบว่ามีความถูกต้องของการกรองข้อความสแปมเฉลี่ยที่ 95.6% และมีความถูกต้องในการกรองข้อความปกติ 100% และเมื่อเก็บข้อมูลการใช้งานจริงเป็นเวลา 4 สัปดาห์ด้วยปริมาณการจราจรข้อมูล Packet อีเมลพบว่า เมื่อติดตั้งตัวกรองข้อความ สแปมที่เครื่องลูกข่ายสามารถลดปริมาณการจราจรลงได้ถึง 72.38% ในขณะเดียวกัน เมื่อติดตั้งตัวกรองยังเครื่องแม่ข่าย ตัวกรองสแปมสามารถลดปริมาณการจราจรลงได้ถึง 81.55% ดังนั้น ตัวข้อความกรองสแปมในฝั่งลูกข่ายสามารถลดปริมาณการส่งข้อมูลในเครือข่ายได้ใกล้เคียงกับฝั่งแม่ข่ายและเป็นการลดการทำงานที่ ฝั่งแม่ข่ายอีกด้วย ซึ่งอาจทำการติดตั้งตัวกรองได้โดยการรวมตัวกรองสแปมในตัวติดตั้งเบราว์เซอร์โดยปริยาย เพื่อป้องกันผู้ใช้ถอดตัวกรองสแปมออกเอง และทำให้สามารถแจกจ่ายและติดตั้งโปรแกรมตัวกรองแก่เครื่อง

คอมพิวเตอร์จำนวนมากในหน่วยงานใหญ่ได้ง่าย ด้วยเหตุนี้ การติดตั้งตัวกรองข้อความสแปมในฝั่งลูกข่ายจึงเป็นอีกทางเลือกหนึ่งในการกรองข้อความสแปมที่น่าสนใจในอนาคต

เอกสารอ้างอิง

นนท์ บุญนิธิประเสริฐ และ ชัยพร เขมะภาตะพันธ์.(2552).**การกรองข้อความภาษาไทย และภาษาอังกฤษของบริการส่งข้อความสั้นบนเครือข่ายโทรศัพท์เคลื่อนที่.** กรุงเทพ : วิทยานิพนธ์วิศวกรรมศาสตร์มหาบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม คณะวิศวกรรมศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์

สำนักงานปลัดกระทรวง.(2550).พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550. สืบค้นเมื่อ 1 กันยายน 2553.จาก **http://www.mict.go.th/ewt_news.php?nid=345&filename=index**

รัฐบาลไทย.(2550).ผลการประชุมคณะรัฐมนตรีประจำวันที่ 18 ธันวาคม 2550 . สืบค้นเมื่อ 1 กันยายน 2553. จาก **www.thaigov.go.th**

ราชบัณฑิตยสถาน.ราชบัณฑิต ฯ ค้าน “ โปสกวน” เผยคำดิบหวั่นเป็นแฟชั่น. สืบค้นเมื่อ 17 กันยายน 2553 จาก **http://news.swu.ac.th/newsclips/doc/200811757.pdf**

สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ.(2550). โครงการระบบจดหมายอิเล็กทรอนิกส์กลางภาครัฐ. สืบค้นเมื่อ 8 ตุลาคม 2553 จาก **http://www.gits.net.th/index.asp**

กอบเกียรติ สระอุบล และ เบญจพร ลิ้มธรรมาภรณ์ (2552). **การกรองสแปมบอทเน็ต.** กรุงเทพ : วิทยานิพนธ์วิทยาศาสตร์มหาบัณฑิต สาขาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยพระจอมเกล้าพระนครเหนือ.

บริษัท Microsoft .Microsoft report . สืบค้นเมื่อ 18 มกราคม 2554 จาก **http://news.bbc.co.uk/2/hi/technology/7988579.stm#map** **http://www.microsoft.com/security/sir/**

บริษัท เวิลด์ ไซเบอร์ เซอร์วิส จำกัด. Anti Spam ระบบป้องกันอีเมล์ขยะ. สืบค้นเมื่อ 22 มกราคม 2554 จาก **http://www.wcs.co.th/antispam.php**

nectec. Digital Signature.สืบค้นเมื่อ 22 มกราคม 2554 จาก **wiki.nectec.or.th/ngiwiki/pub/Main/digital_signature.doc**

Fidelis Assis. (2006). OSBF-Lua, Text classification module for the Lua Programming Language and a production class anti-spam in Lua using the module. Retrieved April 14, 2007, from **http://osbf-lua.luaforge.net/**

Gordon V. Cormack, Jose Maria Gomez Hidalgo, Enrique Puertas Sanz. (2007). **Spam filtering for short messages.** P. 1-4.

S. Dixit, S. Gupta, and C.V. Ravishankar. (2005). **LOHIT: An Online Detection & Control System for Cellular SMS Spam**. P. 2-8.