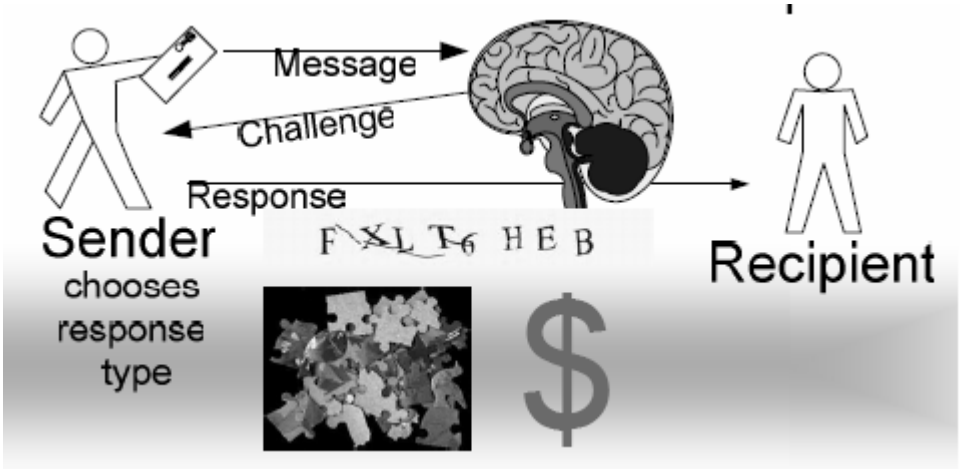
บทที่ 2
งานวิจัยที่เกี่ยวข้อง

ในบทนี้จะกล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้องกับการกรองอีเมล์ขยะ ซึ่งจะเริ่มด้วยเทคนิคต่างๆที่ใช้ในการกรองอีเมล์ขยะ และในส่วนของวิธีการในการกรองอีเมล์ขยะซึ่งเป็นที่นิยมใช้กันอย่างแพร่หลายซึ่งได้แก่การกรองอีเมล์ขยะโดยใช้เครื่องมือเรียนรู้และวิธีการทางสถิติ เช่นตัวกรองเบย์เซียนและตัวกรองที่ใช้การแบ่งแยกมาร์คอฟเวียน

2.1 เทคนิคต่างๆในการกรองอีเมล์ขยะ(Spam Filtering Techniques)

2.1.1 เทคนิคการกรองอีเมล์ขยะโดยใช้การกระตุ้นและตอบสนอง (Challenge and Respond)

การกระตุ้น (Challenge) คือการถามคำถามซึ่งผู้ส่งอีเมล์ต้องตอบอย่างถูกต้องก่อนที่อีเมล์จะถูกส่งไป โดยกรณีทั่วๆไปคือผู้ส่งจะต้องตอบคำถามหรือมีการตอบสนอง (Respond) ที่ถูกต้อง ระบบจึงจะทำการบันทึกผู้ใช้งานนี้ลงในไวท์ลิสต์ (White List) ถ้าตอบสนองไม่ถูกต้องก็จะทำการเก็บผู้ใช้งานนี้ไว้ในแบล็กลิสต์ (Black List) โดยที่การกระตุ้นจะต้องง่ายสำหรับคน แต่ยากสำหรับเครื่องจักรในการตอบสนองดังแสดงในรูปที่ 2.1 [1], [2]



รูปที่ 2.1 แสดงลำดับขั้นในกระบวนการกระตุ้น-ตอบสนองและชนิดของการตอบสนองที่ต้องการ

2.1.2 เทคนิคการกรองอีเมล์ขยะโดยใช้การวิเคราะห์ส่วนหัวของอีเมล์ (Header Analysis)

ส่วนหัวเรื่องของอีเมล์มักประกอบไปด้วย ชื่อเรื่อง วันที่ เวลา ที่อยู่อีเมล์(E-mail Address) ของทั้งผู้ส่งและผู้รับโดยในส่วนของหัวเรื่องนี้สิ่งเดียวที่ไม่สามารถปลอมแปลงได้คือส่วนที่บอกว่าผู้รับได้รับอีเมล์นี้มาจากใคร จากการวิเคราะห์หัวเรื่องพบว่ามีข้อสังเกตหลายอย่างที่ใช้บ่งชี้ได้เป็นอย่าง

ดีว่าอีเมล์เป็นอีเมล์ขยะหรือไม่ ยกตัวอย่างเช่น ไอพีซึ่งไม่ตรงกับโดเมน (Domain Name) เป็นตัวบ่งชี้ว่าอีเมล์เกิดจากการปลอมแปลง ดังนั้นส่วนหัวเรื่องของอีเมล์มักถูกนำมาใช้ในการสร้างกฎสำหรับการเรียนรู้ข่าวขยะของตัวกรอง [1], [2]

2.1.3 เทคนิคการกรองอีเมล์ขยะโดยใช้ลายเซ็นดิจิตอล (Digital Signature)

ลายเซ็นดิจิตอลในอีเมล์นั้นเปรียบเสมือนกับลายพิมพ์นิ้วมือของมนุษย์ ดังนั้นอีเมล์แต่ละฉบับจะมีลายเซ็นดิจิตอลที่แตกต่างกัน ดังนั้นถ้าต้องการทราบว่าอีเมล์ใดเป็นอีเมล์ขยะ เราสามารถนำลายเซ็นดิจิตอลของอีเมล์นั้นมาเปรียบเทียบกับฐานข้อมูลลายเซ็นดิจิตอลที่ได้ถูกรวบรวมไว้ ถ้าพบว่าลายเซ็นดิจิตอลนั้นตรงกันก็สรุปได้ว่าอีเมล์นั้นๆ เป็นอีเมล์ขยะ แต่วิธีการนี้มีข้อเสียคือเมื่อเปลี่ยนแปลงอีเมล์เพียงเล็กน้อยลายเซ็นดิจิตอลของอีเมล์ก็จะเปลี่ยนไป ดังนั้น สแปมเมอร์ (Spammer) มักจะเพิ่มสุ่มข้อความสุ่มลงไปในอีเมล์เพียงเล็กน้อยเพื่อให้ลายเซ็นดิจิตอลของอีเมล์เปลี่ยนไป [1]

2.1.4 เทคนิคการกรองอีเมล์ขยะโดยใช้บัญชีที่อยู่ (Address Lists)

บัญชีที่อยู่มี 2 ประเภทด้วยกันคือ บัญชีขาว (White List) ซึ่งคือบัญชีที่อยู่อีเมล์ของผู้ใช้ที่ต้องการติดต่อด้วย และบัญชีดำ (Black List) คือบัญชีที่อยู่อีเมล์ของสแปมเมอร์หรือบุคคลที่ไม่ต้องการติดต่อด้วย บัญชีที่อยู่ไม่ใช่เพียงแต่ประกอบไปด้วยที่อยู่อีเมล์เท่านั้นแต่ยังสามารถรวมชื่อเมนและส่วนขยายของชื่อโดเมนเช่น ".org" หรือ "edu" ได้ ถ้าหากพิจารณาทางฝั่งแม่ข่าย บัญชีดำประกอบไปด้วยที่อยู่อีเมล์ของสแปมเมอร์ที่รู้จักกันดี บัญชีเหล่านั้นจะถูกเรียกว่าบัญชีหลุมดำเรียลไทม์ (Real-Time Blackhole List) ส่วนระบบเครือข่ายซึ่งอนุญาตให้สแปมเมอร์ใช้ระบบในการส่งอีเมล์ขยะหรือไม่มีการป้องกันสแปมเมอร์ที่เข้ามาใช้ระบบในทางที่ผิดก็จะถูกจัดไว้ในกลุ่มบัญชีหลุมดำเรียลไทม์ด้วยเช่นกัน เมื่อมีการใช้บัญชีที่อยู่ จะต้องแน่ใจว่าไม่ไม่มีการเพิ่มที่อยู่ที่ไม่แน่ใจว่าถูกต้องลงไป เพราะสแปมเมอร์มักปลอมแปลงหัวเรื่องเพื่อให้ดูคล้ายกับอีเมล์ที่ส่งมาจากที่อื่นๆ การใช้ที่อยู่ไอพีจึงปลอดภัยกว่าเนื่องจากยากต่อการปลอมแปลง[1]

2.1.5 เทคนิคการกรองอีเมล์ขยะโดยใช้รายการคำสำคัญ (Keyword Lists)

บัญชีคีย์เวิร์ดมี 2 ประเภทด้วยกันคือ บัญชีคีย์เวิร์ดขาว (Keyword Whitelists) ซึ่งคือบัญชีของคีย์เวิร์ดที่บ่งชี้ว่าไม่น่าจะเป็นอีเมล์ขยะ และบัญชีคีย์เวิร์ดดำ (Keyword Blacklists) ซึ่งคือบัญชีของคีย์เวิร์ดที่บ่งชี้ว่าน่าจะเป็นอีเมล์ขยะ คีย์เวิร์ดนั้นพบได้จากชื่อเรื่อง หัวเรื่อง หรือเนื้อความของอีเมล์ โดยคีย์เวิร์ดอาจประกอบไปด้วย รูปแบบที่เกิดจากการผสมของคำที่หลากหลายหรือรหัสต่างๆ บัญชีคีย์เวิร์ดนั้นต้องการการสร้างอย่างถูกต้องและทันต่อข่าวสารเสมอ ซึ่งเป็นเรื่องที่ต้องใช้เวลาและความพยายามเป็นอย่างสูง [1]

2.1.6 เทคนิคการกรองอีเมล์ขยะโดยการพิจารณาโอเพนรีเลย์ (Open Relays)

โอเพนรีเลย์คือ โอเพนรีเลย์เซิร์ฟเวอร์ หรืออีเมล์เซิร์ฟเวอร์ที่อนุญาตให้กลุ่มที่สาม (Third Party) ส่งผ่านข้อความ เช่น การรับหรือการส่งอีเมล์ซึ่งไม่ใช่ส่งถึงหรือมาจากผู้ใช้งานภายใน โอเพนรีเลย์สร้างขึ้นเพื่อให้มีความสามารถในการใช้งานกับผู้ใช้เคลื่อนที่ (Mobile Users) เพื่อติดต่อกับเครือข่ายโดยต้องผ่านผู้ให้บริการอินเตอร์เนตก่อน (Internet Service Provider) ซึ่งจะส่งต่อข้อความไปยังที่อยู่ของผู้ให้บริการอินเตอร์เนต จากนั้นจึงส่งต่อข้อความไปยังจุดหมายปลายทาง เทคโนโลยีนี้ไม่ดีนักเนื่องจากสแปมเมอร์ผู้ใช้ช่องทางนี้ในการส่งอีเมล์ได้เพิ่มจำนวนขึ้นอย่างรวดเร็ว[8] การบล็อกโดยวิธีโอเพนรีเลย์นั้นมีทั้งข้อดีและข้อเสีย ข้อดีคือลดจำนวนของอีเมล์ขยะลงได้มาก ส่วนข้อเสียคืออีเมล์ดีที่ส่งมาจากผู้ให้บริการอินเตอร์เนตก็อาจถูกบล็อกไปด้วยหรือเมล์เซิร์ฟเวอร์ที่ใช้ร่วมกันก็อาจไม่มีความปลอดภัยไปด้วย แต่ในปัจจุบันระบบความรับผิดชอบของผู้ดูแลระบบนั้นรวดเร็วมากต่อการแก้ไขการปรับแต่งที่ผิดพลาด(Misconfiguration) ซึ่งอาจจะทิ้งเซิร์ฟเวอร์ที่ถูกเปิดเผยออกมาเป็นโอเพนรีเลย์ดังนั้นปริมาณของอีเมล์ดีที่ถูกบล็อกควรจะลดน้อยลงด้วย[9]

2.1.7 เทคนิคการกรองอีเมล์ขยะโดยการพิจารณาโอเพนพร็อกซี่ (Open Proxy)

โอเพนพร็อกซี่คือพร็อกซี่เซิร์ฟเวอร์ซึ่งสามารถเข้าถึงได้โดยผู้ใช้งานอินเตอร์เนตโดยทั่วไป แล้วพร็อกซี่เซิร์ฟเวอร์จะอนุญาตให้ผู้ใช้รับและส่งเว็บเซอร์วิส (Web Service) เช่น DNS อีเมล์ เว็บเพจ ภายในกลุ่มเครือข่ายเท่านั้น แต่สำหรับโอเพนพร็อกซี่ ผู้ใช้ภายนอกได้รับมอบอำนาจให้เข้ามาในระบบเพื่อวัตถุประสงค์ที่จะทำกิจกรรมใดก็ตามที่ส่งผลเสียแก่ระบบได้ [10] ซึ่งการบล็อกโดยวิธีโอเพนพร็อกซี่นั้นมีข้อดีและข้อเสียคล้ายคลึงกับการกรองโดยใช้วิธีโอเพนรีเลย์ [9]

2.2 การกรองอีเมล์ขยะโดยใช้เครื่องมือเรียนรู้และวิธีการทางสถิติ (Machine Learning and Statistical Method)

2.2.1 การกรองอีเมล์ขยะโดยใช้ตัวกรองเบย์เซียน (Bayesian Filter)

เป็นวิธีการทางสถิติที่นักวิจัยใช้กันมากในการสร้างตัวกรองอีเมล์ขยะ ในปี 1998 Sahami และคณะ [11] ได้เขียนบทความซึ่งเป็นบทความแรกที่ใช้เครื่องมือเรียนรู้ในการต่อสู้กับอีเมล์ขยะโดยใช้เบย์อย่างง่าย (Naïve Bayes) โดยพิจารณา คำ วลี และโดเมนเป็นหลักโดยผลที่ได้นั้น ถ้าไม่มีการพิจารณาโดเมนจะต่ำกว่าพิจารณาโดเมนร่วมด้วย ต่อมาในปี 2002 Paul Graham [12] ซึ่งได้รับการกล่าวถึงอย่างมากในชุมชนโอเพนซอร์ส ได้ทำการปรับเปลี่ยนเวอร์ชันของเบย์อย่างง่ายให้แกร่งขึ้นโดยให้โทเคนในเมล์ดีได้รับคะแนนเพิ่มขึ้นเป็นสองเท่า ในเวลาทดสอบจะใช้โทเคน 15 โทเคนที่มีค่าความน่าจะเป็นสูงที่สุด มีการออกแบบและปรับหลายๆ อย่างเพื่อหลีกเลี่ยงการทายอีเมล์ดีให้เป็นอีเมล์ขยะ(False Positive)

ส่วนที่นำมาพิจารณาได้แก่ คำในส่วนของหัวเรื่องและเนื้อเรื่อง ซึ่งจากการทดลองนี้พบว่าได้ผลที่ดีกว่า[11] เล็กน้อย

2.2.2 การกรองอีเมล์ขยะโดยใช้การแบ่งแยกมาร์คอฟเวียน (Markovian Discrimination)

เนื่องจากปัญหาหลักของการกรองโดยใช้เบย์อย่างง่าย (Naïve Bays) จะสนใจนัยสำคัญของคำแต่ละคำ โดยมองว่าแต่ละคำนั้นเป็นอิสระจากกันโดยไม่พิจารณาคำอื่นๆรอบๆตัวมันเลย ดังนั้นมันอาจนำมาซึ่งการถูกโจมตีได้โดยง่าย เพียงแค่การพยายามสุ่มเพิ่มคำดีๆ (Good Word) เข้าไปเพื่อลดคะแนนในส่วนของคำที่น่าจะเป็นขยะ (Spam Word) การแบ่งแยกของมาร์คอฟเวียนจะพิจารณากลุ่มของคำที่พบในอีเมล์ขยะ ซึ่งระดับความรุนแรงของคำที่น่าจะเป็นขยะขึ้นอยู่กับระยะทางของคำในกลุ่มนั้นเทียบกับคำที่พบว่าเป็นขยะจริงๆ W. S. Yerazuris [13] ได้ทดลองโดยเปรียบเทียบวิธีการกรองโดยใช้เบย์อย่างง่ายและกรองโดยใช้การแบ่งแยกของมาร์คอฟเวียน พบว่าผลที่ดีขึ้นโดยมีความผิดพลาดน้อยกว่าการกรองโดยใช้เบย์อย่างง่าย แต่ในแง่ของนัยสำคัญแล้ว วิธีเบย์อย่างง่ายมีนัยสำคัญน้อยมาก