การปรับปรุงกลไกการต่อต้านวอยซ์สแปมโดยใช้การทดสอบทัวริงแบบย้อนกลับ

Improvement on the anti-VoIP spam mechanisms using Reverse Turing Test

ศิวะพร วิวัฒน์ภิญโญ และ วรพล ลีลาเกียรติสกุล

ภาควิชาเทคโนโลยีสารสนเทศ คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร

51 หมู่ 1 ถนนเชื่อมสัมพันธ์ แขวงกระทุ่มราย เขตหนองจอก กรุงเทพ 10530

Email : marklvswp@gmail.com , woraphon@mut.ac.th

บทคัดย่อ – วอยซ์สแปมนั้นเป็นภัยคุกคามที่สำคัญของบริการโทรศัพท์ผ่านอินเทอร์เน็ต ไม่เพียงแต่สร้างความรำคาญแก่ผู้ใช้ยังเป็นเครื่องมือในการก่ออาชญากรรมทางอีเล็กทรอนิคส์ด้วย เนื่องจากว่าวอยซ์สแปมเกิดการการสร้างเสียงแบบอัตโนมัติซึ่งสามารถโทรติดต่อไปยังผู้รับโดยไม่ต้องขออนุญาตจากผู้รับปลายทาง ดังนั้นเราจึงนำเสนอการปรับปรุงกลไกการต่อต้านวอยส์สแปมโดยใช้การทดสอบทัวริงแบบย้อนกลับเพื่อพิสูจน์ว่าการโทรนั้นมาจากมนุษย์หรือไม่ก่อนที่การโทร จะถึงผู้รับสายปลายทาง ถ้าการโทรมาจากมนุษย์ ระบบจะทำการส่งต่อการโทรไปยังผู้รับ และทำการบันทึกชื่อผู้ใช้ลงในไวท์ลิสท์ เพื่อที่ไม่ต้องมีการทดสอบทัวริง สำหรับการโทรครั้งต่อไป ในทางกลับกัน ถ้าการทดสอบแสดงว่าการโทรไม่ได้มาจากมนุษย์ ระบบจะทำการตัดสินว่าเป็น สแปมซึ่งจะไม่ทำการส่งต่อการโทรนี้ และชื่อของผู้ใช้จะถูกบันทึกไว้ในแบ็คลิสท์ ซึ่งการโทรในครั้งต่อไปจะถูกทิ้งไป

คำสำคัญ – โทรศัพท์ทางอินเทอร์เน็ต, วอยซ์โอเวอร์ไอพี, สปิท, วอยซ์สแปม, การทดสอบทัวริง, รายการต้องห้าม, รายการอนุญาต

ABSTRACT – Voice-Spams have been one of a major threat of Internet telephony services not only annoying users but being a tool for some electronic criminals also. Since, voice-spam is a suite of automated voice that will call for any purposes without permission of callees. We thus propose an improvement on the anti-VoIP spam mechanism using Reverse Turing Test to prove whether the call is from human or not before reaching the recipient. If it is a call from human, system will forward the call and the username belonging to the call will be recorded in white list, not be tested for next time calling. On the other hands, if the test indicates that calls is not from human, system will mark it as a spam then call is not forwarded and username will be recorded in black list, calls will be dropped for next time calling.

KEYWORDS – Internet Telephony, VoIP, SPIT, VoIP spam, Turing Test, Blacklist, Whitelist

1. บทนำ

วอยซ์สแปมหรือสปิทเป็นปัญหาของผู้ให้บริการโทรศัพท์ผ่านอินเทอร์เน็ต และเป็นปัญหาที่ก่อความรำคาญแก่ผู้ใช้บริการ โดยสปิทนั้นจะเป็นโปรแกรมที่ถูกเขียนขึ้นมาเพื่อจุดมุ่งหมายให้ทำการโทรศัพท์ไปหาเป้าหมายโดยอาศัยบริการโทรศัพท์ผ่านอินเทอร์เน็ตของผู้ให้บริการ โดยโปรแกรมดังกล่าวจะเป็นตัวจัดการเล่นเสียงซึ่งได้มีการบันทึกไว้ล่วงหน้าจากคนจริงๆ หรือเกิดจากการสังเคราะห์ด้วยโปรแกรมสังเคราะห์เสียงต่างๆ เพื่อให้ผู้รับสายได้รับฟัง ด้วยจุดประสงค์ต่างๆ เช่นการโฆษณา การชักชวนให้สนใจสมัครสมาชิก หรือสั่งซื้อของ หรือแม้กระทั้งทำให้ผู้รับสูญเสียค่าโทรศัพท์ไปโดยไม่รู้ตัว ซึ่งสปิทนี้สามารถที่จะทำการโทรไปยังปลายทางได้ครั้งละหลายๆ เบอร์พร้อมๆ กัน และสามารถทำงานได้ตลอด 24 ชั่วโมงโดยไม่ต้องหยุดพัก แนวทางที่จะป้องกันสปิทได้นั้นคือผู้ให้บริการต้องทำการพิสูจน์ให้ได้ว่า ผู้ที่กำลังจะโทรไปหาผู้ใช้บริการคนอื่นนั้นเป็นมนุษย์จริงๆ มิใช้คอมพิวเตอร์ที่ได้ติดตั้งโปรแกรมสปิทลงไป ในงานวิจัยนี้ได้ใช้วิธีการทดสอบทัวริงแบบย้อนกลับในการทดสอบความเป็นมนุษย์ของผู้ที่จะโทรไปหาผู้อื่น ซึ่งจะใช้คำถามจากเลขที่สุ่มขึ้นมาสองค่าถามไปยังผู้ที่โทรเข้ามา โดยคำตอบของคำถามจะเป็นผลรวมของเลขสองจำนวนนั้น ซึ่งการตอบคำถามนั้นผู้ที่โทรเข้ามาจำเป็นต้องกดแป้นของโทรศัพท์ หรือโปรแกรมที่ใช้โทรเข้ามาเป็นผลรวมของเลขสองจำนวนจากการฟังคำถาม ดังนั้นหากมิใช้มนุษย์ก็จะไม่สามารถฟังคำถามและตอบคำถามนั้นได้ ทั้งนี้ผู้ที่ผ่านหรือไม่ผ่านการทดสอบก็ตาม จะถูกเก็บข้อมูลไว้เพื่อนำมาตัดสินใจและระบุลงในรายการเพื่อจะได้ไม่ต้องทำการทดสอบทุกครั้งเมื่อทำการโทร แต่ชื่อผู้ใช้ทั้งที่ผ่านการทดสอบและไม่ผ่านการทดสอบจะถูกบันทึกในรายการนานที่สุดเพียง 30 วันเพื่อเปิดโอกาสให้ถูกทดสอบอีกครั้ง ทั้งนี้ผู้ที่จะถูกทดสอบนั้นไม่ใช้ทุกคนแต่ระบบจะทำการทดสอบเฉพาะผู้ที่มีพฤติกรรมน่าสงสัยว่าจะเป็นสปิทเท่านั้น โดยใช้การตรวจสอบอัตราความถี่ในการโทรต่อช่วงเวลาที่กำหนดไว้ หากเกินกว่าเกณฑ์ที่กำหนดไว้ก็จะถูกทดสอบโดยระบบต่อไป

2. แนวคิดและวิธีการที่นำเสนอ

การพิสูจน์ความเป็นมนุษย์ของผู้ที่โทรเข้ามานั้น ในงานวิจัยนี้ได้ใช้วิธีการถามคำถาม เพื่อให้ผู้โทรตอบคำถามซึ่งเป็นผลลัพท์ของผลรวมเลขสองจำนวนซึ่งเกิดจากการสุ่มขึ้นมา แล้วเก็บสถิติของการตอบคำถามถูกและผิดไว้เพื่อใช้กำหนดว่าผู้ใช้คนใดเป็นมนุษย์หรือไม่ใช้มนุษย์

2.1 SPam over Internet Telephony (SPIT) Prevention Framework [2]

แนะนำโดย Roman Schlegel และคณะ งานวิจัยนี้คือการออกแบบการป้องกันสปิทโดยมีสองขั้นตอน ซึ่งมีความสามารถในการปรับเปลี่ยนได้ โดยมีความเป็นไปได้ที่จะเพิ่มและลบโมดูลที่จะมีการทำงานในขณะนั้นโดยได้ออกแบบให้ระบบมีสองขั้นตอนในการตรวจสอบสปิทคือในขั้นตอนแรกจะมีโมดูลที่ทำหน้าที่วิเคราะห์การโทรเท่านั้นที่ทำงานโดยจะดูจากข้อมูลก่อนหน้านี้ที่ได้เก็บไว้โดยจะตรวจสอบจากค่าที่ได้จากโมดูล White List, Black List, ข้อมูลการโทรที่พร้อมกัน, อัตราค่าโทร, ความสัมพันธ์ของ IP และ Domain ซึ่งการทำงานร่วมกันที่เหมาะสมของทุกส่วนทำให้เกิดการทำงานที่สมบูรณ์และเพื่อให้ได้วิธีการในการป้องกันสปิทที่มีประสิทธิภาพ ส่วนต่อมาคือขั้นตอนที่สอง นั้นคือในทางกลับกันระบบจะประกอบด้วยโมดูลที่ดำเนินการกับผู้โทรเพื่อทำให้เกิดการปรับแต่งการตรวจจับที่มีประสิทธิภาพ ดังนั้นโมดูลเหล่านี้ในความเป็นจริงก่อให้เกิดความไม่สะดวกในการโทรหรือผู้โทร และพวกเค้ายังได้มีการใช้โมดูลการทดสอบทัวริงซึ่งได้รับการพัฒนาเป็นต้นแบบสำหรับขั้นตอนนี้ด้วย ข้อได้เปรียบของสถาปัตยกรรมนี้คือมันลดการปฏิสัมพันธ์กับผู้โทรเมื่อต้องพิจารณาว่าผู้โทรนั้นคือ สปิทแต่อย่างไรก็ตามในที่สุดแล้วโมดูลการป้องกันนี้ยังไม่สามารถใช้บังคับและป้องกันสปิทได้ถ้าหากจุดเริ่มต้นของสปิท มีการเปลี่ยนไปและทำให้มีผลกระทบในการยืนยันตัวของ SIP สำหรับการโทรที่ตามมาอีกด้วย วิธีการหนึ่งที่จะหลีกเลี่ยงปัญหานี้คือการใช้การตรวจสอบข้อมูลที่เข้มแข็งมากขึ้นกว่านี้ แต่ถึงอย่างไรงานวิจัยนี้มีข้อได้เปรียบคือลดการปฏิสัมพันธ์ระหว่างระบบกับผู้ใช้ในกระบวนการตรวจสอบสปิทนอกจากนี้การทำงานของระบบได้ออกแบบให้มีการทำงานแต่ละส่วนแบบโมดูลซึ่งสามารถเพิ่มลบการทำงานได้ตามความเหมาะสม และยังมีการใช้

ความสัมพันธ์ของ Domain และหมายเลข IP เข้ามาช่วย แต่ก็ยังมีขอเสียอยู่คือ ยังไม่สามารถที่ทำการตรวจสอบสปิท ที่มีการเปลี่ยนแหล่งกำเนิดได้และไม่มีการตรวจสอบซ้ำหากหมายเลข IP นั้นถูกพบใน Blacklist หรือ Whitelist อยู่แล้ว

2.2 Using E-Mail SPAM DNS Blacklists for Qualifying the SPAM-over-Internet-Telephony Probability of a SIP Call [3]

M. Hirschbichler และคณะได้นำเสนอวิธีในการตรวจสอบ SIP ด้วยวิธีที่รู้จักดีและใช้อย่างแพร่หลายนั้นคือการใช้เทคนิคบัญชีดำ (Blacklist) ที่ได้ถูกดำเนินการอย่างกว้างขวางในการป้องกันอีเมล์ขยะ(Email Spam) เทคนิคนี้จะใช้ DNS เพื่อทำการค้นหาว่าพบหมายเลข IP อยู่ในรายการบัญชีดำ(Blacklist)หรือไม่ ซึ่งพวกเขาเชื่อว่าการติดต่อโทรศัพท์ VoIP จากลูกค้าที่มีหมายเลข IP อยู่ในบัญชีดำสำหรับเมล์ขยะ(Email Spam)อยู่แล้ว นั้นมีความน่าจะเป็นอย่างสูงที่จะเป็น สปิทสำหรับการเริ่มต้นการโทรของ VoIP ที่มิได้มีหมายเลข IP อยู่ในบัญชีดำ(Blacklist)ด้วย สำหรับการแยกวิเคราะห์ข้อความ SIP นั้นชื่อโฮสต์และหมายเลข IP จะต้องถูกแยกจากข้อความ SIP โดยชื่อโฮสต์และหมายเลข IP เหล่านี้สามารถพบได้ใน ส่วนหัวที่ส่งผ่านมา, ส่วนหัวของการติดต่อ, SDP-messages, หมายเลข IP ต้นทาง, สำหรับการดำเนินงานของพวกเขานั้นพวกเขาได้พัฒนาโมดูลสำหรับ OpenSER (SIP proxy server) โดยทำการปรับเปลี่ยน Spam Assassin ซึ่งเป็นโปรแกรมที่ถูกใช้โดย Perl modular ของผู้ให้บริการเมลเซิร์ฟเวอร์เพื่อวิเคราะห์และทำเครื่องหมายอีเมลที่เข้ามานอกจากนี้พวกเขายังแสดงให้เห็นว่าการใช้ DNSBLs สำหรับการตรวจสอบที่อยู่ IP อย่างน้อยหนึ่ง IP หรือมากกว่านั้นต่อการโทรไม่ได้เพิ่มความล่าช้าของการตั้งค่าการเรียกร้องเพื่อเริ่มการโทร กับค่าที่ยอมรับไม่ได้ ตราบใดที่พลังอำนาจของ CPU เพียงพอ ข้อได้เปรียบของงานวิจัยนี้มีข้อได้เปรียบความเร็วในการตรวจสอบวิเคราะห์ว่า IP ดังกล่าวเป็น สปิท หรือไม่โดยใช้ Blacklist ของการตรวจสอบ Email Spam เข้ามาร่วมด้วยกับการใช้ DNSBLs แต่ก็มีข้อเสียคือมีการทำงานกับ Blacklist เท่านั้น นั้นคือกำหนดว่าจะป้องกันไม่ให้ผ่านไปเฉพาะหมายเลข IP ที่พบใน Blacklist และ DNSBLs ดังนั้นหากมี สปิทที่ใช้หมายเลข IP ใหม่ๆ ที่ยังไม่มีการตรวจสอบก็จะยังสามารถผ่านไปได้

2.3 A VoIP ANTI-SPAM system based on modular mechanism design [1]

Alexander J. Johansen และ คณะ นั้นได้สร้างโมดูลเพื่อใช้เป็นระบบในการต่อต้านและป้องกันการโทรที่เป็น สปิทโดยใช้วิธีการทดสอบแบบทัวริง เข้ามาช่วยโดยแบ่งเป็น 2 ขั้นตอน ในขั้นตอนแรกนั้นระบบจะเริ่มโดย การนำหมายเลข IP ที่โทรเข้ามาไปเปรียบเทียบกับข้อมูลรายการอนุญาต (White list) หากพบว่าหมายเลข IP ดังกล่าวอยู่ในรายการก็จะอนุญาตให้มีการโทรไปยังปลายทางได้ แต่ถ้าหากหมายเลข IP ดังกล่าวไม่พบในรายการอนุญาตก็จะส่งต่อหมายเลข IP ดังกล่าวเพื่อตรวจสอบเปรียบเทียบกับรายการต้องห้าม (Black List) และหากพบหมายเลข IP ดังกล่าวในส่วนนี้ก็จะทำการยุติการโทรนั้นทันที แต่ในกรณีที่ไม่พบหมายเลข IP ในรายการต้องห้าม(Blacklist)ก็จะเป็นหน้าที่ของ DNSBL Module ซึ่งในส่วนนี้จะนำ IP ดังกล่าวไปตรวจสอบกับฐานข้อมูลของ Spamhaus Block List[5] ซึ่งเป็นตัวอย่างของผู้ให้บริการ DNSBL เพื่อทำการตรวจสอบกับหมายเลข IP ที่ถูก Block ของผู้ให้บริการอื่นๆ หากพบว่าหมายเลข IP ดังกล่าวอยู่ใน Block List ของ DNSBL ก็จะทำการยุติการโทรทันที แต่ถ้าไม่พบก็จะทำการตรวจสอบต่อไปในส่วนต่อไป นั้นคือ Rate-Limit Module ซึ่งในส่วนนี้จะเป็นการตรวจสอบว่าหมายเลข IP ดังกล่าวพยายามโทรเข้ามาเกินกว่าเกณฑ์ที่กำหนดไว้หรือยังถ้าหากว่ายังไม่เกินกว่าเกณฑ์ที่กำหนดไว้ก็จะอนุญาตให้โทรไปยังปลายทางได้ แต่หากพบว่าเกินกว่าเกณฑ์ที่กำหนดไว้ ก็จะถูกส่งไปยังขั้นตอนที่สอง เพื่อทำการทดสอบด้วยวิธีการทดสอบทัวริงเพื่อคัดกรอง ให้การโทรที่มาจากมนุษย์เท่านั้นที่จะสามารถทำการติดต่อไปยังปลายทางได้ โดยพวกเค้าได้ใช้คุณสมบัติการทำงานแบบ CAPTCHA[4] ร่วมกับโมดูลของการทดสอบทัวริง เพื่อสร้างตัวเลขแบบสุ่ม 2 จำนวนขึ้นมาจากนั้นก็จะทำการเรียกเสียงจาก Asterisk Server ที่ได้บันทึกไว้ก่อนหน้านี้แล้วของจำนวนทั้ง 2 เพื่อเป็นคำถามสำหรับสายโทรเข้าดังกล่าว หากเป็นมนุษย์จะต้องสามารถฟังคำถามและตอบคำถามผลรวมของเลข 2 จำนวนผ่านแป้นพิมพ์ตัวเลขที่ระบบถามได้ นั้นคือมีการโต้ตอบกับระบบ ซึ่ง

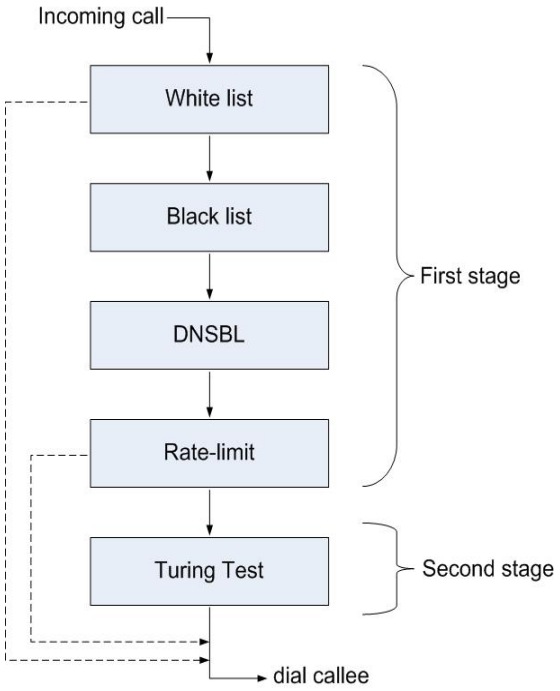
ระบบก็จะอนุญาตให้สายเข้านั้นสามารถติดต่อไปยังปลายทางที่ต้องการได้หากคำตอบที่ได้นั้นถูกต้อง แต่หากว่าเป็นคอมพิวเตอร์ก็จะไม่สามารถตอบคำถามนั้นได้ซึ่งกระบวนการทดสอบ ได้จำกัดการพยายามตอบคำถามไว้หากมีการตอบผิดจนครบตามค่าที่กำหนดไว้แล้วหรือไม่มีการโต้ตอบกับระบบเลย ระบบก็จะยุติการโทรนั้นทันทีเนื่องจากระบบสรุปว่า IP ดังกล่าวเป็นสปิท ข้อดีของงานวิจัยนี้คือมีการออกแบบการทำงานของระบบโดยแยกเป็นส่วนๆ ทำให้ง่ายต่อการจัดการเมื่อต้องการให้บางส่วนไม่ทำงาน ในการทดสอบความเป็นมนุษย์ได้ใช้หลักการของการถามคำถามและให้อีกฝ่ายตอบคำถามโดยการกดแป้นตัวเลข ซึ่งหากมิใช้มนุษย์ก็ไม่สามารถฟังคำถามได้และจะตอบคำถามไม่ได้ นอกจากนี้ยังใช้ Blacklist / Whitelist และ ยังมีการสอบถามไปยัง DNSBLs ด้วยแต่ก็ยังมีข้อเสียคือ ถึงแม้จะมีการใช้งานโมดูล Blacklist และ Whitelist แต่ถึงอย่างไรแม้จะมีขั้นตอนในการทดสอบเพื่อแยกระหว่างการโทรจากมนุษย์และการโทรที่ไม่ได้มาจากมนุษย์ แต่อย่างไรก็ตามหากมีการโทรที่ไม่ได้เกิดขึ้นโดยมนุษย์จากหมายเลข IP เดิมเข้ามาอีกระบบก็ยังต้องกระทำการทดสอบอีกครั้งถึงแม้ว่าเคยทดสอบไปแล้วและได้ผลลัพท์แล้วว่าการโทรจากหมายเลข IP ดังกล่าวเป็น สปิทก็ตาม จึงทำให้เสียเวลาในการทดสอบซ้ำซึ่งหากมีการโทรเข้ามาจากหมายเลข IP ดังกล่าวเป็นจำนวนมากก็จะทำให้ระบบทำงานหนักและเสียเวลาในการทดสอบซ้ำโดยเปล่าประโยชน์

2.4 วิธีการที่นำเสนอ

งานวิจัยนี้ได้เสนอแนวคิดที่ใช้ในการปรับปลุงกลไกการทำงานของ Anti-SPIT Framework[1] แต่ทั้งนี้ไม่ได้ปรับปรุงทุกโมดูลของ Anti-SPIT Framework[1] แต่จะทำการปรับปรุงเพียงรายการต้องห้าม(Black List), รายการอนุญาต(White List) และการทดสอบทัวริง เพื่อจุดมุ่งหมายที่จะลดเวลาในการทดสอบซ้ำซ้อนที่เกิดขึ้นจากงานที่ผ่านมาของ Alexander J. Johansen และคณะ[1] โดยยังคงโครงสร้างของ Anti-SPIT Framework เดิมไว้เพียงแค่ปรับปรุงการทำงานภายในโมดูลเท่านั้น ดังนั้นการปรับปรุงจึงแบ่งเป็น 3 ส่วนด้วยกันคือ

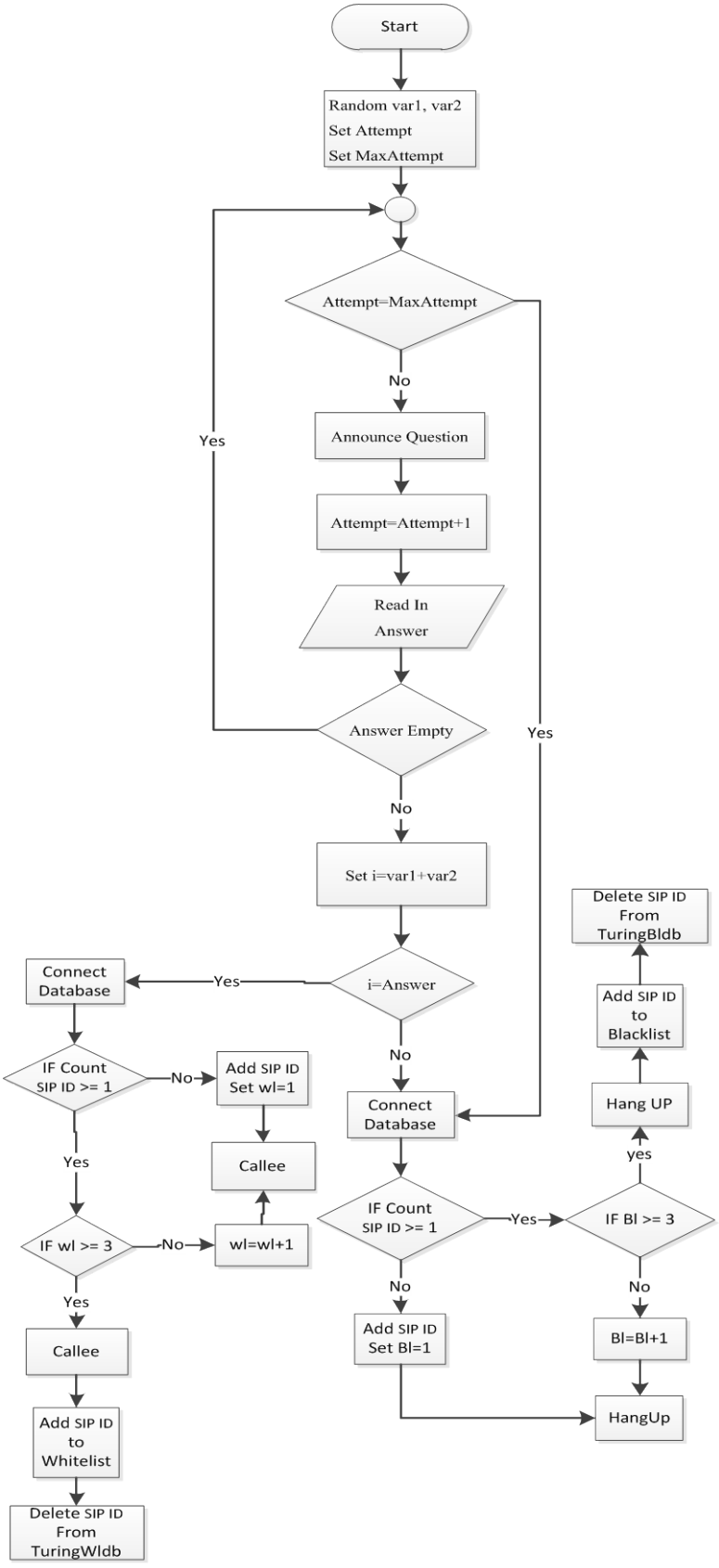
2.4.1 การปรับปรุงกลไกการทำงานของการทดสอบทัวริง

งานวิจัยนี้จึงมุ่งพัฒนาโมดูลการทดสอบทัวริงให้สามารถทำการเพิ่ม SIP ID แทนหมายเลข IP เข้าไปยังรายการต้องห้าม(Black List)ในกรณีที่ไม่ผ่านการทดสอบ และจะเพิ่ม SIP ID ไปยังรายการอนุญาต(White List)ในกรณีที่ผ่านการทดสอบโดยอัตโนมัติเพื่อเป็นการลดเวลาที่จะเสียไปของการทดสอบซ้ำซ้อน



รูปที่ 1. โครงสร้างของ Anti-SPIT Framework[1] ของAlexander J. Johansen และคณะ[1]ซึ่งไม่มีการเปลี่ยนแปลงโครงสร้างเพียงแต่จะทำการปรับปรุงการทำงานเท่านั้นในงานวิจัยนี้

แต่ถึงอย่างไรการที่จะเพิ่ม SIP ID ไปยังรายการทั้งสอง หากยึดจากผลเพียงครั้งเดียวก็อาจทำให้เกิดข้อผิดพลาดได้ดังนั้นในงานวิจัยนี้จึงกำหนดให้มีฐานข้อมูลที่จะทำหน้าที่เก็บค่าทางสถิติของการทดสอบไว้โดยกำหนดค่า Wl และ Bl เก็บจำนวนของการทดสอบผ่านและไม่ผ่านจากการทดสอบทัวริงโดยกำหนดค่าสูงสุดไว้ที่ 3 ครั้งดังนั้นหากการทดสอบพบว่า SIP ID ใดมีค่า Wl หรือ Bl เท่ากับ 3 ก็จะทำการย้าย SIP ID ดังกล่าวไปไว้ที่รายการอนุญาต(White List) หรือรายการต้องห้าม(Black List) ต่อไปซึ่งแสดงการทำงานดังรูปที่ 2



รูปที่ 2. แสดง Flow Chart การทำงานของ Turing Test Module ที่ได้ปรับปรุงแล้ว

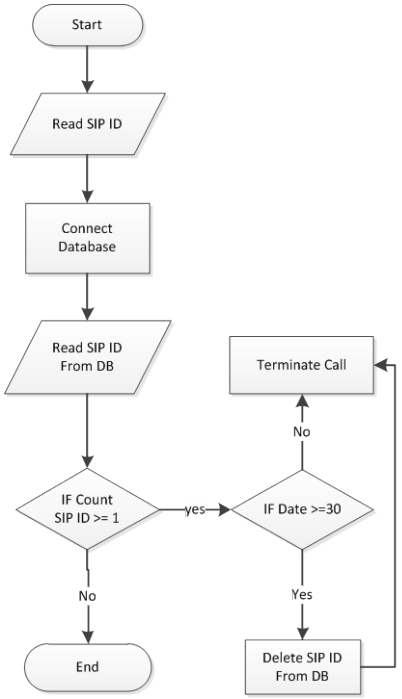
ซึ่งในส่วนนี้จะมีการปรับปรุงการทำงานเพิ่มเติมเข้ามาเพื่อให้สามารถเก็บ SIP ID ที่เคยผ่านการทดสอบแล้วและระบบตัดสินว่าเป็นสปิทหรือเป็นการโทรจากมนุษย์ไปแล้ว แต่การที่จะระบุเจาะจงว่าห้ามหรืออนุญาตการโทรจาก SIP ID ดังกล่าวตั้งแต่การตรวจสอบในครั้งแรกนั้นอาจจะทำให้เกิดข้อผิดพลาดจากการทดสอบได้เช่นในส่วนของรายการต้องห้ามอาจจะเป็นไปได้ว่ามนุษย์ตอบคำถามผิดถึง 3 ครั้งได้ ดังนั้นในงานวิจัยนี้จึงกำหนดให้เก็บ SIP ID ดังกล่าวไว้ในรายการ Turingbl และ Turingwl เพื่อสร้างค่า Bl(สำหรับ SIP ID ที่สงสัยว่าจะเป็นสปิท) และ Wl(สำหรับ SIP ID ที่คาดว่าจะเป็นการโทรจากมนุษย์) มาเป็นค่าสำหรับการระบุจำนวนครั้งในการทดสอบของแต่ละ SIP ID โดยผู้วิจัยได้กำหนดไว้ที่ 3 ครั้ง ดังนั้นหากค่า Bl มีค่าเท่ากับหรือมากกว่า 3 ก็ทำการบันทึก SIP ID นั้นในรายการต้องห้าม (Blacklist) และหากค่า Wl มีค่าเท่ากับหรือมากกว่า 3 ก็ทำการบันทึก SIP ID นั้นในรายการอนุญาต (Whitelist) การทำงานของการทดสอบทัวริง จะเริ่มจากการสุ่มค่ามาสองค่าและกำหนดค่าความพยายามสูงสุดตามที่กำหนดไว้จากนั้นจะทำการตรวจสอบค่าความพยายาม (Attempt) ว่ามีค่าเท่ากับค่าความพยายามสูงสุดที่กำหนดไว้หรือยัง (MaxAttempt) หากมีค่าเท่ากันก็จะยุติการโทรทันทีแต่หากว่ายังระบบจะเล่นเสียงของคำถามและเสียงตัวเลขตามค่าที่สุ่มขึ้นมาเพื่อให้ผู้โทรตอบคำถามนั้นหากไม่มีการตอบคำถามก็จะมีการทวนคำถามอีกครั้งด้วยคำถามเดิมแต่จะเพิ่มค่า Attempt+1 เข้าไป หากไม่มีการตอบคำถามจนค่า Attempt เท่ากับค่า MaxAttempt ระบบจะทำการตรวจสอบเช่นเดียวกับการตอบคำถามผิดซึ่งจะอธิบายในส่วนต่อไป แต่หากว่ามีการตอบคำถามเข้ามาระบบก็จะมีการตรวจสอบว่าคำตอบนั้นถูกต้องหรือไม่ หากคำตอบที่รับมาถูกต้องระบบก็จะติดต่อกับฐานข้อมูลและตรวจสอบว่าพบ SIP ID ที่ตรงกันหรือไม่ หากไม่พบให้บันทึก SIP ID พร้อมทั้งกำหนดค่า Wl=1 และส่งต่อการโทรไปยังผู้รับปลายทาง แต่หากว่าพบ SIP ID ที่ตรงกันก็จะตรวจสอบต่อไปว่า Wl มีค่าเท่ากับหรือมากกว่า 3 แล้วหรือยังหาก Wl มีค่ามากกว่าหรือเท่ากับ 3 แล้วระบบจะส่งต่อการโทรไปยังผู้รับปลายทางและนำค่า SIP ID ไปใส่ไว้ในรายการอนุญาตพร้อมลบข้อมูล SIP ID ออกจาก Turingwl แต่ถ้าค่า Wl น้อยกว่า 3 จะทำการเพิ่มค่า Wl=Wl+1 แต่หากว่าคำตอบนั้นผิดระบบก็จะติดต่อกับฐานข้อมูล Turingbl และตรวจสอบว่าพบ SIP ID ที่ตรงกันหรือไม่ หากไม่พบให้บันทึก SIP ID พร้อมทั้งกำหนดค่า Bl=1 และจบการโทร แต่หากว่าพบ SIP ID ที่ตรงกันก็จะตรวจสอบต่อไปว่า Bl มีค่าเท่ากับหรือมากกว่า 3 แล้วหรือยังหาก Bl มีค่ามากกว่าหรือเท่ากับ 3 แล้วระบบจะยุติการโทรนั้นแล้วนำค่า SIP ID ใส่ไว้ในรายการต้องห้ามพร้อมลบข้อมูล SIP ID ออกจาก Turingbl แต่ถ้าค่า Bl น้อยกว่า 3 จะทำการเพิ่มค่า Bl=Bl+1 การทำงานของการทดสอบทัวริงดังแสดงในรูปที่ 2 แสดง Flow Chart การทำงานของ Turing Test Module ที่ได้ปรับปรุงแล้ว

2.4.2 การปรับปรุงกลไกการทำงานของรายการต้องห้าม

รายการต้องห้าม(Black List)ในงานวิจัยที่ผ่านมา[1] ทำหน้าที่เก็บหมายเลข IP ที่ต้องการให้ยุติการโทรในทันทีที่ระบบตรวจพบ แต่การเพิ่มหมายเลข IP เข้าไปยังรายการต้องห้ามนั้นจะต้องดำเนินการโดยการกระทำของผู้ดูแลระบบ(admin)เท่านั้น ในงานวิจัยนี้มีการปรับปรุงกลไกในส่วนนี้ให้เพิ่ม SIP ID แทนหมายเลข IP เข้ามายังรายการต้องห้ามและมีกลไกการตรวจสอบอายุของ SIP ID ที่ถูกเก็บอยู่ในรายการต้องห้ามเพื่อให้มีโอกาสที่ SIP ID เหล่านี้สามารถกลายเป็น SIP ID ที่ไม่ใช้ สปิทได้ในอนาคตเนื่องจากเมื่อมีการปิดกัน SIP ID แล้วผู้โจมตีก็อาจเปลี่ยนไปใช้งาน SIP ID อื่นและ SIP ID ที่ถูกกีดกันก็สามารถย้ายเจ้าของเป็นผู้ใช้งานปกติรายอื่นๆ ได้ ดังนั้นผู้วิจัยถึงกำหนดอายุของการคงอยู่ของ SIP ID ในรายการต้องห้ามนี้ไว้ที่ 30 วัน ดังนั้นเมื่อ SIP ID ใดอยู่ในรายการต้องห้ามนานเท่ากับหรือมากกว่า 30 วันก็จะถูกลบออกจากรายการต้องห้ามเพื่อให้ SIP ID เหล่านี้ได้ถูกทดสอบใหม่ซึ่งหากทดสอบผ่าน SIP ID ดังกล่าวก็จะถูกบันทึกที่รายการอนุญาตและใช้งานได้ตามปกติ

ซึ่งในโมดูลนี้แสดงการทำงานตามรูปที่ 3 แสดง Flow Chart การปรับปรุงการทำงานของ Black List Module โดยการทำงานของ Black List Module นี้จะเริ่มตั้งแต่รับ SIP ID ของสายโทรมาเก็บไว้จากนั้นติดต่อกับฐานข้อมูลเพื่อเข้าถึงรายการต้องห้ามที่เก็บไว้จากนั้นนำ SIP ID มาเปรียบเทียบกับ SIP ID ที่เก็บไว้ซึ่งหากพบว่ามี SIP ID ที่ตรงกันระบบก็จะทำการตรวจสอบต่อไปว่า SIP ID ดังกล่าวมีอายุตั้งแต่วันที่ถูกบันทึกเข้ามา เท่ากับ 30 วันหรือยังหากว่ายังมีอายุไม่ถึง 30 วันก็จะทำการยุติการโทรทันทีแต่หากว่ามีอายุเท่ากับหรือมากกว่า 30 วันแล้วระบบ

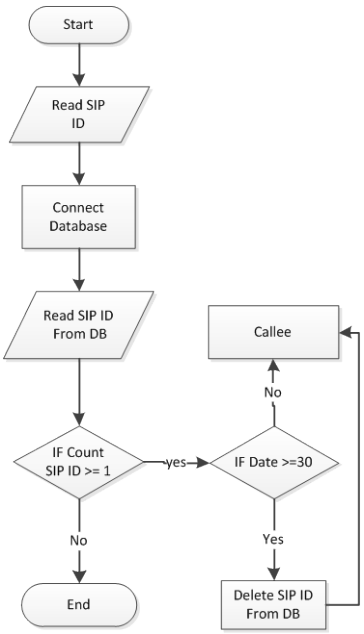
จะทำการลบ SIP ID ดังกล่าวออกจากฐานข้อมูลของรายการต้องห้ามและจบการทำงานของโมดูลและยุติการโทร



รูปที่ 3. แสดง Flow Chart การปรับปรุงการทำงานของ Black List Module

2.4.3 การปรับปรุงกลไกการทำงานของรายการอนุญาต

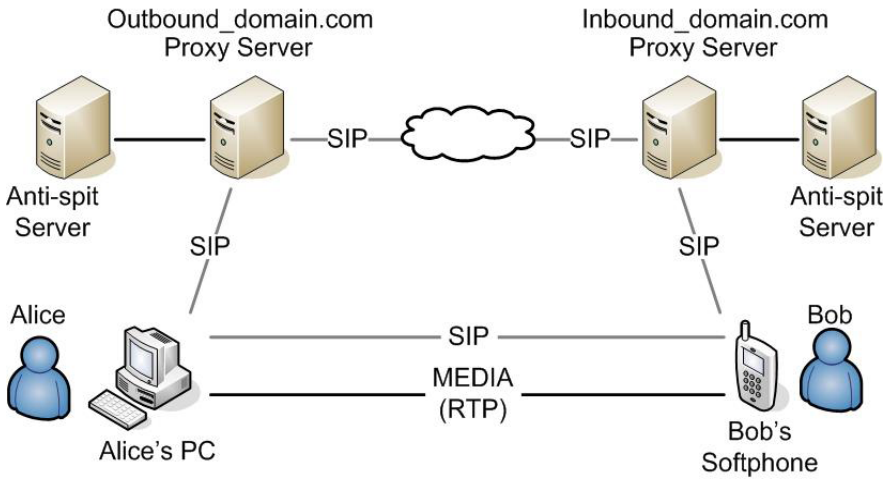
ในส่วนของรายการอนุญาต(White List) จะทำหน้าที่เก็บ SIP ID ที่ได้รับความไว้ใจว่าไม่ใช่สปิทนั้นคือหากตรวจสอบ SIP ID ที่โทรเข้ามาแล้วพบว่ามีบันทึกในรายการอนุญาตนี้ระบบก็จะส่งสายโทรนั้นไปยังผู้รับทันทีโดยไม่ผ่านการทดสอบทัวริง ซึ่งการที่เป็นเช่นนี้ก็อาจจะมีผู้ไม่หวังดีที่ได้ SIP ID ที่อยู่ในรายการอนุญาตนำไปใช้เพื่อสร้างสปิทได้ ในงานวิจัยนี้จึงกำหนดให้ SIP ID ในรายการอนุญาตนี้สามารถคงอยู่ได้โดยมีอายุ 30 วันเพื่อให้ SIP ID ที่อยู่ในรายการอนุญาตนี้ได้ถูกทดสอบเพื่อยืนยันว่ายังเป็นมนุษย์ที่ใช้งานมิใช่สปิท การทำงานของโมดูลรายการอนุญาตสามารถแสดงได้ดังรูปที่ 4 แสดง Flow Chart การปรับปรุงการทำงานของ White List Module ซึ่งโมดูลจะเริ่มทำงานโดยการอ่านค่า SIP ID จากสายโทรจากนั้นจะทำการติดต่อกับฐานข้อมูลเพื่อเข้าถึงรายการอนุญาต(White List) เพื่อนำ SIP ID ที่ได้มานั้นไปเปรียบเทียบกับข้อมูล SIP ID ที่เก็บไว้หากไม่พบ SIP ID ดังกล่าวในรายการอนุญาตก็จะจบการทำงานของโมดูลและส่งต่อการทำงานไปที่โมดูลอื่นต่อไป แต่หากพบ SIP ID ที่ตรงกันโมดูลนี้ก็จะทำการตรวจสอบต่อไปว่า SIP ID ดังกล่าวมีอายุครบ 30 หรือยังหากว่ายังมีอายุไม่ถึง 30 วันก็จะอนุญาตให้การโทรนั้นไปยังปลายทางได้ แต่หากว่ามีอายุครบ 30 วันแล้วระบบจะทำการลบ SIP ID ดังกล่าวออกจากรายการอนุญาตและต่อสายไปยังปลายทางต่อไป



รูปที่ 4. แสดง Flow Chart การปรับปรุงการทำงานของ *White List Module*

3. การทดลอง

ในการทดสอบเราใช้คอมพิวเตอร์ที่ใช้ซีพียู Core2Dual ความเร็ว 3.0Ghz, หน่วยความจำ 2 Gb, ฮาร์ดดิสก์ความจุ 250Gb โดยติดตั้งโปรแกรมแบบเปิดชื่อ Asterisk บนระบบปฏิบัติการ CentOS 5.4 และเขียนแผนการโทรให้มีการเรียกใช้ AGI Script ที่พัฒนาด้วยภาษา Perl เพื่อเรียกโมดูลต่างๆ มาทำงานตามขั้นตอนที่ระบุไว้ในรูปที่ 1 โดยทำการทดสอบตามโครงสร้างการทดสอบดังรูปที่ 5



รูปที่ 5. โครงสร้างของระบบที่ทำการทดสอบ

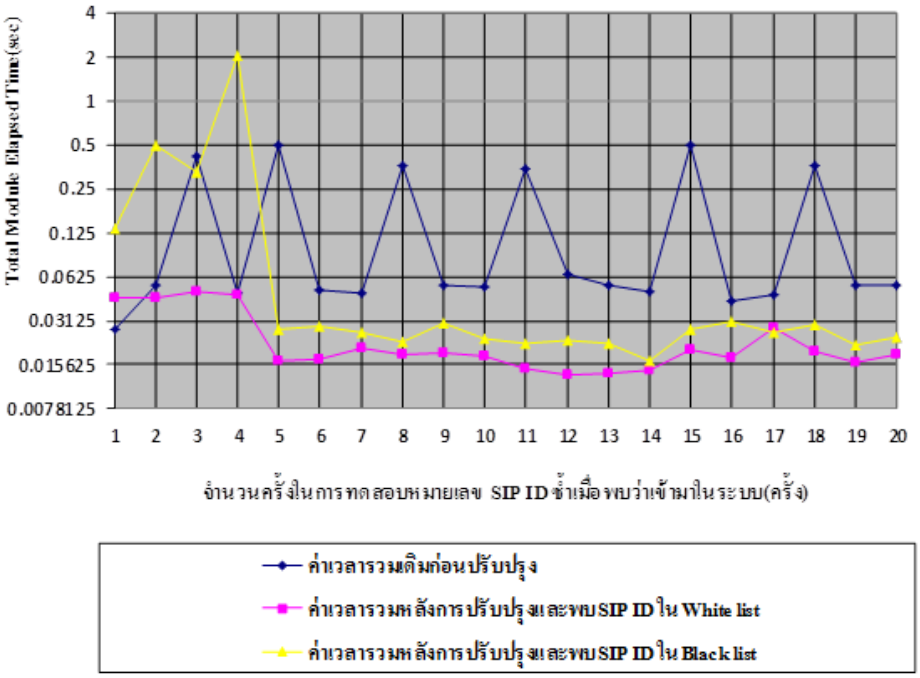
โดยจะเริ่มจากการทดสอบการทำงานของ Black List ในส่วนนี้จะทำการทดลองโดยสร้างสถานการณ์ให้เกิดการทดสอบทัวริงโดยบันทึกค่า SIP ID และ bl ใน Turingbl ดังรูปที่ 6 เมื่อตอบคำถามผิดหรือไม่ตอบคำถามและเมื่อไม่ผ่านการทดสอบจำนวน 3 ครั้ง นั้นคือค่า bl >=3 หมายเลข SIP ID ของการโทรก็จะถูกย้ายจาก Turingbl บันทึกลงใน Blacklist แทนดังรูปที่ 7 และเมื่อหมายเลข SIP ID ดังกล่าวมีอายุ 30 วันก็จะถูกลบออกจากฐานข้อมูลแต่หากหมายเลข SIP ID ดังกล่าวยังอยู่ใน Blacklist เมื่อมีสายมาจากหมายเลข SIP ID นั้นอีกครั้งระบบจะทำการวางสายทันที ถัดมาคือการทดลองการทำงานของ White Listโดยในส่วนนี้จะทำการตรวจสอบ SIP ID ที่เก็บไว้ใน Turingwlโดยกำหนดให้เมื่อการโทรที่ผ่านการทดสอบทัวริงครบ 3 ครั้งแล้วนั้น SIP ID ก็จะถูกย้ายจาก Turingwl ไปบันทึกลงในรายการ Whitelist แทนและเมื่อมีการโทรเข้ามาจากหมายเลข SIP ID เดิมอีก ระบบจะส่งไปยังผู้รับทันทีโดยไม่จำเป็นต้องทดสอบอีก แต่ทั้งนี้ SIP ID ก็จะถูกเก็บไว้ในฐานข้อมูลเป็นเวลา 30 วันเท่านั้น เมื่อครบกำหนดก็จะถูกลบออกจากฐานข้อมูล ในการทดสอบเราได้ทำการเปลี่ยนเวลาของเครื่องให้ต่างไปจากเวลาจริงมากกว่า 30 วันเพื่อทดสอบว่ามีการลบ SIP ID ดังกล่าวออกจากระบบจริงหรือไม่ ซึ่งจากการทดสอบหมายเลข SIP ID ที่มีอายุเกิน 30 วันจะถูกลบออกไปจากฐานข้อมูล สุดท้ายทำการทดลองการทำงานของการทดสอบทัวริง ในส่วนของการทดสอบทัวริงนี้จะมีการทำงาน โดยเมื่อไม่พบหมายเลข SIP ID ในฐานของมูล Blacklist และ Whitelist และผลจากการตรวจสอบด้วยโมดูล DNSBL ไม่พบว่าเป็น SPAM รวมถึงการโทรนั้นไม่เกินกว่าเกณฑ์ที่กำหนดไว้ในโมดูล Rate-limit จึงจะมีการทดสอบหมายเลข SIP ID นั้น หากผลการทดสอบที่ได้ไม่ผ่านการทดสอบก็จะนำหมายเลข SIP ID ดังกล่าวบันทึกใน Turingbl เพื่อเก็บค่าสถิติจนกว่าจะมีค่า Flag Bl=>3 จึงย้ายไปบันทึกในรายการ Blacklist ต่อไปแต่หากว่าหมายเลข SIP ID ดังกล่าวผ่านการทดสอบก็จะถูกบันทึกในฐานข้อมูล Turingwl ก่อนเพื่อเก็บค่าสถิติไว้จนกว่าจะมีค่า Flag Wl => 3 จึงย้ายไปบันทึกในรายการ Whitelist ต่อไป จากการทดสอบเมื่อหมายเลข SIP ID มาถึงส่วนการทดสอบทัวริงระบบจะทำการสุ่มตัวเลขขึ้นมาสองค่าเพื่อสร้างเป็นเสียงเพื่อส่งไปถามผู้ที่โทรเข้ามา หากไม่มีการตอบสนองใดๆ ระบบจะถามคำถามซ้ำเพื่อให้ตอบคำถามอีกจนกว่าจะครบ 3 ครั้งตามค่าสูงสุดที่กำหนดไว้ หากครบกำหนดแล้วไม่มีการตอบคำถามเลยหรือตอบผิดก็จะบันทึกหมายเลข SIP ID ใน Turingbl แต่หากตอบคำถามได้ถูกต้องระบบก็จะบันทึกหมายเลข SIP ID ใน Turingwl แทน

รูปที่ 6. แสดงข้อมูล SIP ID ที่บันทึกใน Turingbl

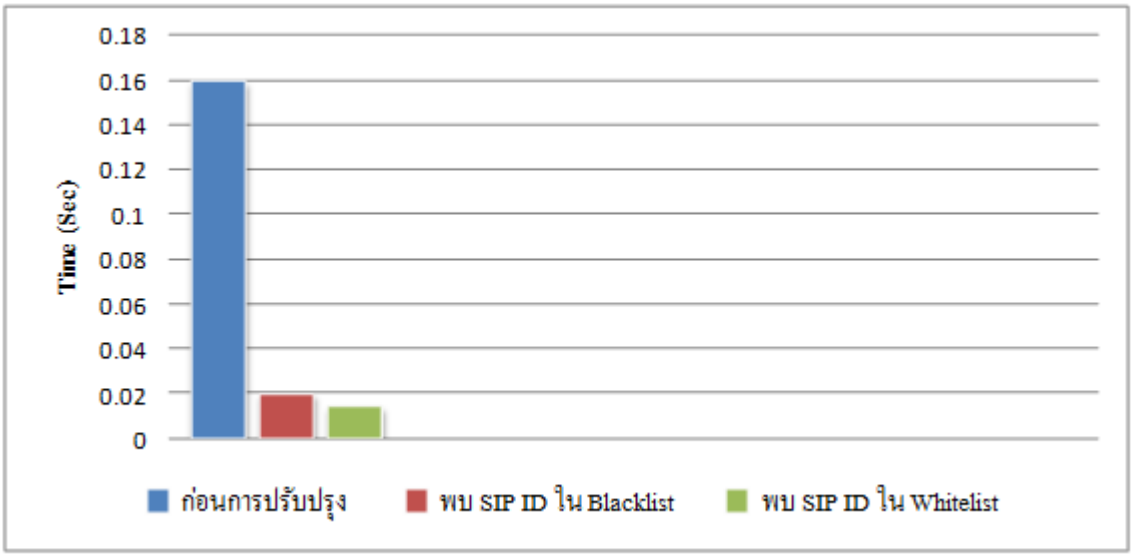
รูปที่ 7. แสดงข้อมูล SIP ID ที่ย้ายจาก Turingbl มาบันทึกใน blacklist แทน โดยจะมีการใส่ วันที่ที่ได้รับการบันทึกไว้ด้วยเพื่อใช้ในการตรวจสอบอายุต่อไป

3. สรุปผลการทดลอง

งานวิจัยนี้ได้เสนอแนวทางในการปรับปรุงการทำงานของโมดูล White List, Black List และ Turing Test เพื่อลดเวลาในการทดสอบที่ซ้ำซ้อน อันเกิดจากการตรวจสอบสายโทรว่ามาจากมนุษย์หรือไม่ โดยเพิ่มความสามารถในการนำ SIP ID ที่ได้พิสูจน์แล้วว่าเป็นการโทรจากมนุษย์เก็บไว้ใน White List หรือการโทรที่ไม่ใช่มนุษย์ ไปเก็บไว้ในรายการ Black List โดยได้กำหนดให้ SIP ID ที่เก็บไว้ในรายการทั้งสองจำเป็นต้องมีการทดสอบซ้ำโดยกำหนดค่าอายุไว้ที่ 30 วันนับจากวันที่ถูกนำมาเพิ่มไว้ในรายการทั้งสอง จากผลการทดลองในรูปที่ 8 กราฟเปรียบเทียบค่าเวลารวมในการทำงานของโมดูลทั้งหมดพบว่าเมื่อ SIP ID ถูกระบุในรายการ whitelist หรือ blacklist ทำให้ค่าเวลารวมการทำงานของทุกโมดูลลดลงดังแสดงให้เห็นในการทดลองครั้งที่ 5 ทั้งนี้เนื่องจากผู้วิจัยกำหนดว่าเมื่อค่า wl หรือ bl มีค่าเท่ากับ 3 จึงย้าย SIP ID มาที่รายการ whitelist หรือ blacklist จึงทำให้เงื่อนไขเป็นจริงในการทดสอบครั้งที่ 4 ค่าเวลารวมจึงลดลงในครั้งที่ 5 และพบว่าค่าเวลารวมเมื่อพบ SIP ID ในรายการ whitelist หรือ blacklist รายการใดรายการ หนึ่งทำให้เวลาเฉลี่ยรวมของเวลาที่เสียไปลดลงดังแสดงในรูปที่ 9 กราฟเปรียบเทียบค่าเวลาเฉลี่ยรวมของการทำงานก่อนการปรับปรุงกับหลังปรับปรุงและพบ SIP ID ใน Blacklist และ Whitelist จึงสรุปได้ว่าการปรับปรุงให้มีการเพิ่ม SIP ID ไปยังรายการ Whitelist และ Blacklist นั้นทำให้ค่าเวลาเฉลี่ยรวมของการทำงานของ Anti-SPIT Framework ลดลง



รูปที่ 8. แสดงกราฟเปรียบเทียบค่าเวลารวมในการทำงานของโมดูลทั้งหมด



รูปที่ 9. แสดงกราฟเปรียบเทียบค่าเวลาเฉลี่ยรวมของการทำงานก่อนการปรับปรุงกับ หลังปรับปรุง และพบ SIP ID ใน Blacklist และ Whitelist

4. เอกสารอ้างอิง

[1] Alexander J. Johansen, and Woraphon Lilakiatsakun., “A VoIP ANTI-SPAM system based on modular mechanism design.”, ICIIT 2010, V1-407

[2] Roman Schlegel et al. “SPam over Internet Telephony (SPIT) Prevention Framework”

[3] M. Hirschbichler, et al., "Using E-Mail SPAM DNS Blacklists for Qualifying the SPAM-over-Internet-Telephony Probability of a SIP Call," in Digital Society, 2009. ICDS '09. Third International Conference on, 2009, pp. 254-259.

[4] CAPTCHA. สามารถเข้าถึงข้อมูลได้จาก : http://en.wikipedia.org/wiki/CAPTCHA.

[5] “Spamhaus Block List.”, สามารถเข้าถึงข้อมูลได้จาก : http://www.spamhaus.org/whitepapers/dnsbl_function.html