การพิสูจน์ทราบตัวตนเพื่อความมั่นคงปลอดของการส่งข้อความสั้นด้วยเซสชันคีย์ที่จำกัด

A Secure SMS Authentication Based on Limited-Used Session Keys

สุรการ ดวงผาสุข และ ชาลี ธรรมรัตน์

คณะวิทยาการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยเทคโนโลยีมหานคร

51 หมู่1 ถนนเชื่อมสัมพันธ์แขวงกระทุ่มรายเขตหนองจอกกรุงเทพ 10530

Emails: surakarn@mut.ac.th และ chalee23@gmail.com

ABSTRACT – Currently, short message service (or SMS) is very popular like a payment transaction, payment products or services, vote or a comment to activities. A lot of researches have been presented SMS authentication. However, a number of researches were presented still lacking of security and authentication. This paper presents SMS authentication to increase security. Moreover, the proposed protocol deploys a limited-use offline session key generation and use of distribution technique to enhance security. The result of proposed protocol illustrated that it gained better performance and less time than existing papers and sending short text messages each time was less than the maximum.

KEY WORDS - Short Message Service, Security Protocol, Mutual Authentication Protocol, Network Security

บทคัดย่อ - ปัจจุบันการส่งข้อความสั้นได้รับความนิยมเช่น การทำธุรกรรมทางการเงิน การชำระเงินค่าสินค้าหรือบริการ การส่งข้อความสั้นเพื่อร่วมโหวต หรือการส่งข้อความแสดงความคิดเห็นเพื่อร่วมกิจกรรมต่างๆ ทั้งนี้มีงานวิจัยจำนวนมากได้นำเสนอการพิสูจน์ทราบตัวตนการส่งข้อความสั้น แต่อย่างไรก็ตามงานวิจัยจำนวนมากที่ได้นำเสนอเหล่านั้นยังขาดความมั่นคงปลอดภัยและการพิสูจน์ทราบตัวตนที่เพียงพอ ดังนั้นงานวิจัยฉบับนี้ได้นำเสนอการพิสูจน์ทราบตัวตน โดยได้นำการสร้างเซสชันคีย์แบบออฟไลน์มาใช้งาน ส่งผลทำให้มีความมั่นคงปลอดภัยที่เพิ่มขึ้น ผลลัพธ์ของโพรโทคอลที่นำเสนอมีประสิทธิภาพและใช้เวลาน้อยกว่างานวิจัยที่มีอยู่และการส่งข้อความสั้นแต่ละครั้งความยาวของข้อความที่ส่งน้อยกว่าข้อความสูงสุดที่ส่งได้

คำสำคัญ –ข้อความสั้น, โพรโทคอลความมั่นคงปลอดภัย, โพรโทคอลการพิสูจน์ทราบตัวตนสองทาง, ความมั่นคงปลอดภัยของเครือข่าย

1. บทนำ

ปัจจุบันโทรศัพท์มือถือสามารถส่งข้อความสั้นผ่านเครือข่าย เช่น GPRS (General Packet Radio Service), EDGE (Enhanced Data Rate for GSM Evolution) หรือ HSDPA (High-Speed Downlink Packet Access) โดยการเชื่อมต่ออินเทอร์เน็ตหรือการส่งข้อความสั้นนั้นมุ่งไปยังวัตถุประสงค์ต่าง ๆ เช่น การส่งข้อความสั้นหากัน การทำธุรกรรมทางการเงิน การสั่งซื้อสินค้า การส่งข้อความร่วมโหวตหรือการส่งข้อความแสดงความคิดเห็นเพื่อร่วมกิจกรรมต่าง ๆ ผ่านข้อความสั้นซึ่งยังได้รับความนิยมและต้องการความมั่นคงปลอดภัย เนื่องจากข้อความสั้นอาจถูกปลอมหรือแก้ไขข้อความได้ ดังนั้นข้อความที่ส่งจึงมีความสำคัญมากเพราะการส่งข้อความผ่านเครือข่ายไร้สายของ

GSM (Global System for Mobile Communications) นั้น เป็นการสื่อสารระดับชั้นกายภาพ (Physical) ยังขาดคุณสมบัติทางด้านความมั่นคงปลอดภัยเช่น การพิสูจน์ทราบตัวตนสองทางเพื่อป้องกันการปลอมเป็นผู้ส่งหรือผู้รับข้อความ (Mutual Authentication) การรักษาความลับข้อความ (Confidentiality) และการคงสภาพของข้อความ (Integrity) ด้วยเหตุนี้จึงมีงานวิจัยจำนวนมากที่มีการนำเสนอความมั่นคงปลอดภัยสำหรับการส่งข้อความสั้น [7] [8] [9] [10] แต่อย่างไรก็ตามงานวิจัยจำนวนมากที่ได้นำเสนอเหล่านั้นยังขาดความมั่นคงปลอดภัยและการพิสูจน์ทราบตัวตนที่เพียงพอ

บทความวิจัยฉบับนี้จึงได้นำเสนอความมั่นคงปลอดภัยและการพิสูจน์ทราบตัวตนข้อความสั้น นอกจากนี้โพรโทคอลที่นำเสนอยังมีการส่งข้อความที่สั้น เมื่อเปรียบเทียบกับโพรโทคอลอื่น ๆ เนื่องจากอาศัยการเข้ารหัสลับแบบสมมาตรและฟังก์ชันแฮช ขณะที่ยังคงมีคุณสมบัติความมั่งคงปลอดภัยที่จำเป็นเช่น การรักษาความลับข้อความ การคงสภาพและการพิสูจน์ทราบตัวตน ตลอดจนมีการสร้างเซสชันคีย์ที่มีการใช้งานจำกัดและเทคนิคการกระจายคีย์ [1] เพื่อป้องกันการใช้งานเซสชันคีย์ซ้ำและโพรโทคอลที่เสนอยังเข้ากันได้กับโครงสร้างพื้นฐานของการส่งข้อความสั้นที่มีอยู่

บทความวิจัยฉบับนี้มีโครงสร้างดังนี้ บทที่ 2 กล่าวถึงพื้นฐานที่เกี่ยวข้อง บทที่ 3 งานวิจัยที่นำเสนอ บทที่ 4 การวิเคราะห์และอภิปราย บทที่ 5 การวิเคราะห์ประสิทธิภาพของโพรโทคอลและบทที่ 6 สรุปผลการวิจัย

2. ทฤษฎีที่เกี่ยวข้อง

2.1 บริการส่งข้อความสั้น (Short Message Service หรือ SMS)

โทรศัพท์มือถือ [8] [9] [10] [12] [13] ในปัจจุบันสามารถใช้ในการส่งข้อความผ่านเครือข่ายการสื่อสาร เช่น GPRS EDGE หรือ HSPDA ซึ่งผู้ใช้งานสามารถเชื่อมต่ออินเทอร์เน็ต พร้อมทั้งใช้งานโปรแกรมประยุกต์บนอุปกรณ์มือถือ เพื่อส่งข้อความสั้น แม้ว่ารูปแบบของการส่งข้อความจะมีอยู่หลากหลายเนื่องจากความรวดเร็วของการส่งข้อความ แต่การส่งข้อความสั้นกลับได้รับความนิยม เพราะว่ามีต้นทุนต่ำและเป็นคุณสมบัติที่มีอยู่ในมือถือที่มีราคาต่ำ ในปัจจุบันมีการใช้การส่งข้อความสั้นเพื่อวัตถุประสงค์หลายอย่างได้แก่ การส่งข้อความสั้นหากัน การทำธุรกรรมทางการเงิน การสั่งซื้อสินค้าและการส่งข้อความร่วมโหวตหรือการส่งข้อความสั้นในการแสดงความคิดเห็นเพื่อร่วมกิจกรรมต่างๆ

การส่งข้อความสั้นเริ่มจาก MS (Mobile Station) ส่งข้อความสั้นผ่านอากาศ (OTA-Over the Air) ไปยัง BSS (Base Station System) ซึ่งทำหน้าที่เป็นทั้งตัวส่งและตัวรับสัญญาณผ่านทางอากาศซึ่งเชื่อมต่อกับระบบควบคุมสถานีฐาน จากนั้นจะส่งข้อความผ่านอินเตอร์เฟซไปยัง MSC (Mobile Switching Centre) ทำหน้าที่ควบคุมข้อความที่เข้าออกจากเครือข่ายโทรศัพท์อื่น และมีฟังก์ชันของการลงทะเบียน การพิสูจน์ทราบตัวตน การปรับตำแหน่งและการหาเส้นทางสำหรับส่งข้อความเพื่อหาเส้นทางในการส่งต่อไปยัง SMSC (Short Message Service Centre) ผ่านทางช่องทาง SS7 (Signaling System 7) ซึ่ง SMSC ส่งต่อไปยัง AS (Authentication Source) ที่ตนเองเชื่อมต่ออยู่ผ่านทางอินเทอร์เน็ต จากนั้น AS จะนำข้อความมาเพื่อพิสูจน์ทราบตัวตนของ MS และส่งข้อความตอบกลับไปยัง SMSC ต่อจากนั้นจะค้นหาตำแหน่งที่อยู่ของ MS ที่เก็บอยู่ใน MSC แล้วจึงส่งข้อความสั้นต่อไปยัง BSS ที่เชื่อมต่อกับ MS ปลายทางซึ่ง SMSC จะเก็บข้อความไว้จนกว่า MS ปลายทางพร้อมจะรับข้อความตอบกลับจาก BSS

2.2 ช่องโหว่ที่เกิดขึ้นใน SMS

การส่งข้อความสั้นนั้นมีช่องโหว่ที่ทำให้เกิดการโจมตีดังต่อไปนี้

1. SMS Disclosure: เทคนิคการเข้ารหัสลับข้อความด้วย A5/1 และ A5/2 ซึ่งมีบทความและงานวิจัยต่าง ๆ ระบุว่าเทคนิคการเข้ารหัสลับดังกล่าวนั้นสามารถถูกโจมตีได้ [15] การส่งข้อความบน SS7 ไม่มีการเข้ารหัสลับข้อความ นอกจากนี้ข้อความที่เก็บอยู่ใน SMSC ไม่มีการเข้ารหัสลับ ดังนั้นถ้าผู้ไม่หวังดีโจมตี SMSC สำเร็จ ส่งผลให้ผู้ไม่หวังดีเห็นข้อความและอ่านข้อความรู้เรื่อง สามารถนำไปใช้ประโยชน์ต่อไป [9] [11]
2. SMS Spoofing: ผู้ไม่หวังดีปลอมตัวเป็นโทรศัพท์มือถือหรือเซิร์ฟเวอร์พิสูจน์ทราบตัวตนเพื่อต้องการรู้ข้อความการพิสูจน์ทราบตัวตน [8] [9]
3. Replay Attack: ผู้ไม่หวังดีดักจับข้อความระหว่างที่รับส่งแล้วทำการส่งข้อความเดิมไปยังผู้รับ เพื่อให้ผู้รับส่งข้อความบางอย่างที่สามารถใช้ในการปลอมตัวหรือใช้ในการพิสูจน์ทราบตัวตน [8] [9] [11] [12] [13]

4. Man-in-the-middle Attack: ผู้ไม่หวังดีอยู่ระหว่างกลางสำหรับการรับส่งระหว่างผู้ส่งและผู้รับทำให้คนกลางนั้นสามารถที่จะเห็นข้อความที่มีการรับส่ง เนื่องจากเครือข่าย SS7 และ SMSC มีการรักษาความปลอดภัยที่ขึ้นอยู่กับระบบของผู้ให้บริการสัญญาณโทรศัพท์ทำให้ข้อความสั้นอาจถูกดักจับและแก้ไขข้อความได้ เพราะข้อความสั้นไม่มีการเข้ารหัสลับซึ่งทำให้ขาดคุณสมบัติความเป็นส่วนตัว (Privacy) ซึ่งหากผู้ไม่หวังดีใช้วิธีการโจมตีตามช่องโหว่ต่าง ๆ ที่กล่าวในข้างต้นแล้วก็สามารถทำการโจมตีแบบ Man-in-the-Middle ได้โดยสามารถทำตัวเป็นทางผ่านของข้อความที่ส่งไปมาระหว่าง MS และ AS พร้อมทั้งสามารถแก้ไขข้อความได้โดยที่ต่างฝ่ายไม่รู้เลยว่าข้อความนั้นถูกเปิดเผยหรือถูกแก้ไข [11] [12] [13]

5. Vulnerabilities of the BSS: ผู้ไม่หวังดีปลอมตัวเป็น BSS เพื่อดักจับข้อความจาก MS สามารถทำได้ง่าย เนื่องจาก BSS ไม่มีการพิสูจน์ทราบตัวตนกับ MS แต่ MS ที่ต้องทำการพิสูจน์ทราบตัวตนกับ BSS [8]

2.3 งานวิจัยที่มีอยู่

2.3.1 Security Mechanism for Secure SMS Communication

Ratshinanga *et al.* [7] ได้นำเสนอโพรโทคอลในระดับชั้นแอพพลิเคชัน (Application Layer) ที่มีความมั่นคงแบบ End-to-end Security ซึ่งมีคุณสมบัติความปลอดภัยเพียงบางส่วนและยังไม่ครอบคลุมคุณสมบัติทางด้านความปลอดภัยที่จำเป็นอีกหลายประการได้แก่ การพิสูจน์ทราบตัวตนและการรักษาความลับของข้อความ อย่างไรก็ตามเทคนิคนี้ยังมีข้อด้อยคือการที่นำเซสชันคีย์เดิมไปใช้ในการเข้ารหัสลับข้อความทุกครั้ง รวมถึงการใช้ค่า SQ ที่บวกค่า 1 ไปทุกครั้งที่มีการส่งข้อความส่งผลทำให้ผู้ไม่หวังดีสามารถที่จะคาดเดาค่า SQ ได้ง่ายและสามารถนำข้อความที่เข้ารหัสลับมาวิเคราะห์ เพื่อหาเซสชันคีย์ได้ ตลอดจนไม่มีคุณสมบัติการคงสภาพของข้อความ

2.3.2 SMSSec

Li-Chang *et al.* [8] ได้เสนอโพรโทคอล SMSSec ที่ทำงานในระดับชั้นแอพพลิเคชัน เพื่อสร้างความปลอดภัยแบบ End-to-end Security ด้วยเช่นกัน โพรโทคอลที่นำเสนอนี้ให้คุณสมบัติสำหรับการรักษาความมั่นคงปลอดภัยเพียงบางส่วนซึ่งยังไม่ครอบคลุมคุณสมบัติที่จำเป็นอีกหลายประการปัญหาและข้อจำกัดของ SMSSec คือการทำ First Handshake อาศัยการเข้ารหัสลับด้วยพับบลิคคีย์ (public key) ของ AS (Authentication Source) เป็นการพิสูจน์ทราบตัวตนเพียงฝั่งเดียวและ PIN การทำ Next Handshake ทุกครั้งจะใช้ค่า U (Cell Phone Number) ซึ่งเป็นค่าคงที่เพื่อระบุตัวตนของ C (Mobile Station) ทำให้ผู้โจมตีสามารถปลอมแปลงข้อความเพื่อหลอกให้ S ส่งข้อความที่สำคัญไปยังผู้โจมตี นอกจากนี้โพรโทคอลนี้ไม่มีคุณสมบัติความคงสภาพของข้อความ

2.3.3 PK-SIM

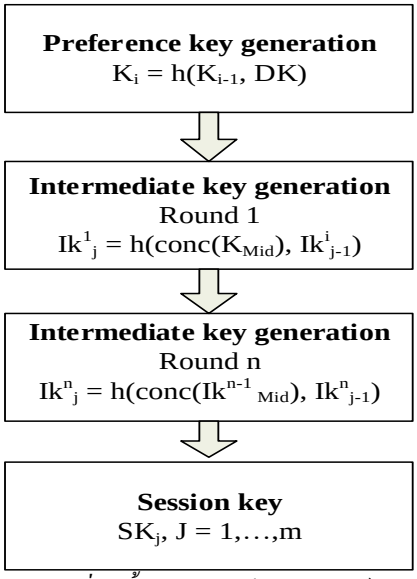
Rongyu *et al.* [9] ได้นำเสนอ PK-SIM เป็นโพรโทคอลที่มีความมั่งคงปลอดภัยแบบ End-to-end Security ได้มีการใช้เทคนิคการเข้ารหัสลับแบบอสมมาตรและสมมาตรที่อาศัยแฮชฟังก์ชันเพื่อคงสภาพของข้อความประกอบด้วย 2 โพรโทคอล คือ the authentication phase และ the session key establish and communication phase นอกจากนี้ยังมีความมั่นคงปลอดภัยเช่น การพิสูจน์ทราบตัวตนและการคงสภาพของข้อความและการรักษาความลับของข้อความ แต่อย่างไรก็ตามโพรโทคอลที่นำเสนอยังมีข้อด้อยอยู่ที่มีการพิสูจน์ทราบตัวตนเพียงฝั่งเดียว

2.3.4 SecureSMS

Saxena *et al.* [10] ได้นำเสนอความมั่นคงปลอดภัยการสื่อสารด้วย SMS เรียกว่า SecureSMS โดยใช้เทคนิคการเข้ารหัสลับแบบสมมาตรและแฮชฟังชันทำให้โพรโทคอลมีน้ำหนักเบา ประกอบด้วย 3 ฝ่ายได้แก่ MS (Mobile Station) คือโทรศัพท์มือถือ AS (Authentication Server) คือเซิร์ฟเวอร์พิสูจน์ตัวทราบตัวตนและ CA/RA (Certification /Registration Authority) คือเซิร์ฟเวอร์ที่เก็บรายละเอียดของโทรศัพท์มือถือ นอกจากนี้โพรโทคอลที่นำเสนอยังสามารถป้องกันการโจมตีเช่น reply attack, man-in-the-middle attack, SMS spoofing และ SMS disclosure อีกทั้งการเข้ารหัสลับเป็นแบบ End-to-end Security ส่งผลให้โพรโทคอลมีความมั่นคงปลอดภัย แต่อย่างไรก็ตามงานวิจัยของ Saxena *et al.* ยังมีข้อด้อยคือไม่มีการพูดถึงการเปลี่ยนเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง MS และ AS

2.4 การสร้างและกระจายเซสชันคีย์แบบออฟไลน์

Kungpisdan *et al.* ได้นำเสนอวิธีการสร้างและกระจายคีย์แบบออฟไลน์ ซึ่งมีการสร้างและกระจายเซสชันคีย์โดยที่ไม่ต้องมีการส่งคีย์ดังกล่าวผ่านเครือข่าย [1] ซึ่งมีจุดเด่นที่เหนือกว่าเทคนิคการกระจายคีย์แบบออนไลน์ โดยเทคนิคการสร้างและกระจายคีย์แบบออฟไลน์ถูกเสนอ [1] [2] [3] [4] [5] [6] โดยที่ Kungpisdan *et al.* ได้แนะนำเทคนิคการสร้างคีย์ที่ไม่เพียงแต่มีความปลอดภัยจากการโจมตีเท่านั้น แต่ยังสามารถทำงานได้แบบออฟไลน์ ทั้งนี้มีรายละเอียดของวิธีการดังกล่าวดังนี้



รูปที่ 1. ขั้นตอนการสร้างเซสชันคีย์

ก่อนการสร้างเซสชันคีย์จะต้องดำเนินการแลกเปลี่ยนค่าเริ่มต้น $\{K_{AB}, DK, m\}$ สมมติว่าเป็นการแลกเปลี่ยนโดยอลิสและบ๊อบ ซึ่งกำหนดให้ K_{AB} เรียกว่า Long-term key, DK เรียกว่า Distribution key และ m คือ ค่าสุ่มที่ระบุจำนวนของคีย์ที่ต้องการสร้างขึ้น โดยขั้นตอนการสร้างเซสชันคีย์สามารถอธิบายได้ดังนี้

หลังจากมีการแลกเปลี่ยนค่า $\{K_{AB}, DK, m\}$ อลิสและบ๊อบจะสร้างเซตของ Preference keys K_i, i = 1,2,…, m ดังสมการ 1

$$K_i = h(K_{i-1}, DK) \quad (1)$$

จากนั้นทั้งคู่สร้างเซ็ตของ Intermediate Keys (IK) ซึ่งเป็นการเพิ่มความยากในการวิเคราะห์การถอดรหัสลับ เพิ่มความยากในการสืบค้นของ Preference key ดังสมการ 2

$$IK^x_j = h(conc(IK^{x-1}{}_{mid}), IK^x_{j-1}) \quad (2)$$

โดย x คือจำนวนรอบของ j ซึ่ง j คือจำนวนของ Intermediate key ที่ถูกสร้างขึ้น $IK^{x-1}{}_{mid}$ เป็นค่าของ $\{IK^{x-1}{}_{mid1}, IK^{x-1}{}_{mid2}, IK^{x-1}{}_{mid3}\}$, $conc(IK^{x-1}{}_{mid})$ จะเป็นการเชื่อมต่อค่า $\{IK^{x-1}{}_{mid1}, IK^{x-1}{}_{mid2}, IK^{x-1}{}_{mid3}\}$ ตามลำดับ

การหาค่า $IKx\ mid1 = mid(IK^x{}_1, IK^x{}_{rm})$ โดยที่ rm คือจำนวนของ Intermediate key ที่ยังเหลืออยู่ในชุดข้อความของ $IK^x{}_j$, $IK^x{}_{mid2} = mid(IK^x{}_{mid1}, IK^x{}_{rm})$, $IK^x{}_{mid3} = mid(IK^x{}_1, IK^x{}_{mid2})$, $IK^1{}_{mid1} = K_{mid1}$, $IK^1{}_{mid2} = K_{mid2}$, $IK^1{}_{mid3} = K_{mid3}$ และ $IK^x{}_{j-1} = \Phi$ การใช้ Intermediate Keys ในทุก ๆ รอบจะทำการลบค่าออกจากระบบส่วนที่เหลือของ Intermediate Keys ในรอบอื่น ๆ สามารถเขียนได้ดังนี้

$$\{K_1, K_2, \ldots, K_{rm}\},\{K^1{}_1, K^1{}_2, \ldots, K^1{}_{rm}\}, \{K^2{}_1, K^2{}_2, \ldots, K^2{}_{rm}\},\ldots$$
$$\{K^n{}_1, K^n{}_2, \ldots, K^n{}_{rm}\}$$

ผลที่ได้รอบสุดท้ายของ Intermediate Keys ที่ได้จะถูกใช้เป็นเซสชันคีย์ (Session key) (SK_j) โดยที่ $j = 1,\ldots,m$ ดังสมการ 3

$$IK^n{}_1 = SK_1, IK^n{}_2 = SK_2, \ldots, IK^n{}_m = SK_m \quad (3)$$

จากเทคนิคนี้จะเห็นว่าจะมีการส่งเพียงค่าตัวแปรที่เป็นค่าเริ่มต้น เพื่อนำไปใช้ในการสร้างคีย์และคีย์ที่ถูกสร้างขึ้นถูกนำมาใช้เพียงครั้งเดียวไม่มีการนำมาใช้ซ้ำ สามารถสร้างคีย์โดยโอกาสเกิดค่าคีย์ที่ซ้ำเป็นไปได้ยาก

3. งานวิจัยที่นำเสนอ

ในส่วนนี้จะเป็นการนำเสนอโพรโทคอลการพิสูจน์ทราบตัวตนประกอบด้วย 2 โพรโทคอลคือ Authv1 เป็นการพิสูจน์ทราบตัวตนระหว่างโทรศัพท์มือถือกับเซิร์ฟเวอร์พิสูจน์ตัวตนทราบตน และ Authv2 เป็นการพิสูจน์ทราบตัวตนระหว่างโทรศัพท์มือถือกับเซิร์ฟเวอร์พิสูจน์ตัวทราบตัวตนโดยมีเซิร์ฟเวอร์เก็บรายละเอียดของโทรศัพท์มือถือช่วยในการระบุตัวตนของโทรศัพท์มือถือ

3.1 สมมติฐาน

โพรโทคอลที่นำเสนอประกอบด้วย 3 ฝ่ายได้แก่ MS (Mobile Station) คือโทรศัพท์มือถือ AS (Authentication Server) เซิร์ฟเวอร์พิสูจน์ทราบตัวตน นอกจากนี้ยังมี CA/RA (Certification/Registration Authority) ซึ่งจะทำหน้าที่เป็นเซิร์ฟเวอร์ที่เก็บรายละเอียดของโทรศัพท์มือถือ

- SK_{A-Bj} โดยที่ j = 1 ถึง n คือ เซสชันคีย์ใช้ร่วมกันระหว่าง A กับ B

- ID_A คือสิ่งที่ระบุว่าเป็น *A*
- *Msg* คือข้อความที่ต้องการติดต่อสื่อสารเช่น ข้อความสั้นหากัน การทำธุรกรรมทางการเงิน การสั่งซื้อสินค้าและการส่งข้อความร่วมโหวตหรือการส่งข้อความแสดงความคิดเห็นเพื่อร่วมกิจกรรมต่างๆ ผ่านโทรศัพท์มือถือ
- $\{Msg\}_{SK}$ เป็นการเข้ารหัสสมมาตรของข้อความ *Msg* ด้วยคีย์ *SK*
- *h(Msg)* คือค่าแฮชของข้อความ *Msg*
- *h(Msg, SK)* เป็นรหัสพิสูจน์ทราบตัวตนข้อความ (MAC หรือ Message Authentication Code) ของข้อความ *Msg* ด้วยค่าคีย์ *SK*

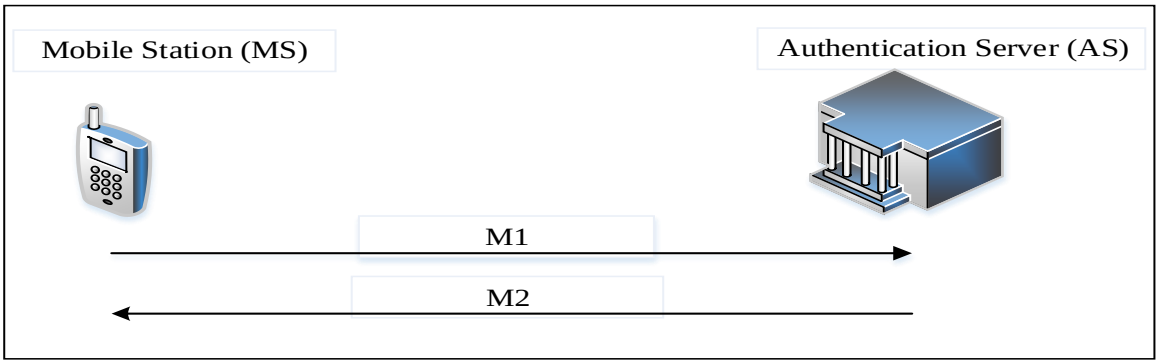
3.2 การลงทะเบียน

อุปกรณ์มือถือต้องติดตั้งซอฟต์แวร์การพิสูจน์ทราบตัวตนข้อความสั้นตามโพรโทคอลที่นำเสนอ เมื่อซอฟต์แวร์ถูกดาวน์โหลดไปยังเครื่องของผู้ใช้โทรศัพท์มือถือ จากนั้นผู้ใช้โทรศัพท์มือถือจำเป็นต้องลงทะเบียนซึ่งการลงทะเบียนดำเนินการผ่านช่องทางที่ปลอดภัย เช่น TLS (Transport Layer Security) โดยมีการนำ TLS เข้ามาใช้เพื่อความมั่นคงปลอดภัยในการสื่อสารไร้สายเรียกว่า WTLS (Wireless Transaction Layer Security) วัตถุประสงค์ของการลงทะเบียนคือ การแลกเปลี่ยนพารามิเตอร์ $\{DK, K, m\}$ โดยขั้นตอนการสร้างเซสชันคีย์แต่ละฝ่ายสามารถอธิบายได้ดังนี้

1. *MS* และ *AS* แลกเปลี่ยนพารามิเตอร์ $\{DK_{MS\text{-}AS}, K_{MS\text{-}AS}, m\}$ ซึ่งหลังจากการแลกเปลี่ยน $\{DK_{MS\text{-}AS}, K_{MS\text{-}AS}, m\}$ กัน *MS* และ *AS* สามารถสร้างเซสชันคีย์ $SK_{MS\text{-}ASj}$, เมื่อ j = 1 ถึง n โดยใช้เทคนิคการสร้างคีย์ที่แสดงในส่วน 2.4
2. *AS* และ *CA/RA* แลกเปลี่ยนพารามิเตอร์ $\{DK_{AS\text{-}CA/RA}, K_{AS\text{-}CA/RA}, m\}$ ซึ่งหลังจากการแลกเปลี่ยน $\{DK_{AS\text{-}CA/RA}, K_{AS\text{-}CA/RA}, m\}$ กันแล้ว ทั้ง AS และ CA/RA จะสามารถสร้างเซสชันคีย์ $SK_{AS\text{-}CA/RAj}$, เมื่อ j = 1 ถึง n โดยใช้เทคนิคการสร้างคีย์ที่แสดงในส่วน 2.4

3.3 Authv1

Authv1 เป็นการพิสูจน์ทราบตัวตนระหว่างโทรศัพท์มือถือกับเซิร์ฟเวอร์พิสูจน์ตัวทราบตัวตนตามแสดงในรูปที่ 2 แสดงการพิสูจน์ทราบตัวตนระหว่าง *MS* และ *AS* อธิบายได้ดังนี้



รูปที่ 2. การพิสูจน์ทราบตัวตนระหว่าง MS และ AS

M1: MS → AS: ID_{MS}, T_1, n_1, $\{Msg\}_{SKMS\text{-}ASj}$, $h(ID_{MS}, T_1, n_1, Msg, SK_{MS\text{-}ASj})$

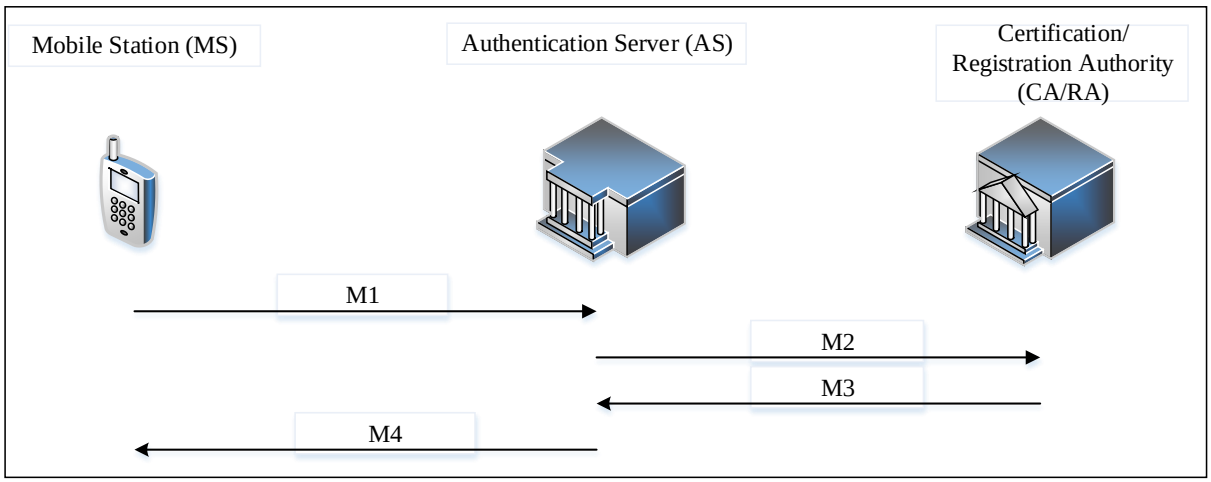
M2: AS → MS: T_2, n_2, *Accept/Reject*, $h(Accept/Reject, ID_{MS}, T_1, T_2, n_1, n_2, SK_{MS\text{-}ASj+1})$

M1: *MS* ส่งข้อความ ID_{MS}, T_1, n_1, $\{Msg\}_{SKMS\text{-}ASj}$, $h(ID_{MS}, T_1, n_1, Msg, SK_{MS\text{-}ASj})$ ข้อความร้องขอการพิสูจน์ทราบตัวตนกับ *AS* โดยที่ T_1 คือ เวลาที่ *MS* ร้องขอพิสูจน์พิสูจน์ทราบตัวตน n_1 คือค่าสุ่มตัวอักษรใช้เพื่อป้องกันการส่งข้อความซ้ำถูกสร้างโดย *MS* นอกจากนี้ค่าแฮชของ ID_{MS}, T_1, n_1, *Msg*, และ $SK_{MS\text{-}ASj}$ เป็นข้อความรหัสพิสูจน์ทราบตัวตนระหว่าง *MS* และ *AS* โดยที่ $SK_{MS\text{-}ASj}$ เป็นเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *MS* และ *AS*

M2: *AS* นำข้อความที่ได้รับจาก *MS* มาทำถอดรหัสลับข้อความ $\{Msg\}_{SKMS\text{-}ASj}$ ด้วยเซสชันคีย์ $SK_{MS\text{-}ASj}$ ซึ่งเป็นเซสชันคีย์ที่ใช้ร่วมกันระหว่าง *MS* และ *AS* แล้วนำข้อความ *Msg* และข้อความ ID_{MS}, T_1, n_1, $SK_{MS\text{-}ASj}$ มาเข้าฟังก์ชันแฮชตรวจสอบกับค่าแฮชของ $h(ID_{MS}, Msg, T_1, n_1, SK_{MS\text{-}ASj})$ ที่ *MS* ส่งมาถ้าตรงกัน *AS* ก็จะส่งข้อความ *Accept* แต่ถ้าไม่ตรงกันก็จะส่งข้อความ *Reject* กลับมาให้ *MS* โดยที่ *AS* ส่งข้อความ *Accept/Reject* และค่าแฮชของข้อความ $h(Accept/Reject, ID_{MS}, T_1, T_2, n_1, n_2, SK_{MS\text{-}ASj+1})$ กลับมาให้ *MS* เป็นการเสร็จสิ้นการพิสูจน์ทราบตัวตนระหว่าง *MS* และ *AS* ดยที่ $SK_{MS\text{-}ASj+1}$ เป็นเซสชันคีย์ตัวถัดไปที่ใช้งานร่วมกันระหว่าง *MS* และ *AS* โดยที่ T_2 คือ เวลาที่ *AS* ส่งคำร้องขอพิสูจน์พิสูจน์ทราบตัวตนกลับ n_2 คือค่าสุ่มตัวอักษรใช้เพื่อป้องกันการส่งข้อความซ้ำถูกสร้างโดย *AS* และข้อความ $h(Accept/Reject, ID_{MS}, T_1, T_2, n_1, n_2, SK_{MS\text{-}ASj+1})$ เป็นข้อความรหัสพิสูจน์ทราบตัวตนระหว่าง *MS* และ *AS*

3.4 Authv2

Authv2 เป็นการพิสูจน์ทราบตัวตนระหว่างโทรศัพท์มือถือกับเซิร์ฟเวอร์พิสูจน์ตัวทราบตัวตนโดยมีเซิร์ฟเวอร์เก็บรายละเอียดของโทรศัพท์มือถือ เพื่อช่วยในการระบุตัวตนของโทรศัพท์มือถือตามแสดงในรูปที่ 3 แสดงการพิสูจน์ทราบตัวตนระหว่าง *MS, AS* และ *CA/RA* อธิบายได้ดังนี้



รูปที่ 3. การพิสูจน์ทราบตัวตนระหว่าง MS, AS และ CA/RA

M1: MS → AS: ID_{MS}, T_1, n_1, $\{Msg, h(ID_{MS}, T_1, n_1, Msg, SK_{MS\text{-}ASj})\}_{SKMS\text{-}ASj+1}$

M2: AS → CA/RA: ID_{MS}, $h(ID_{MS}, SK_{AS\text{-}CA/RAj})$

M3: CA/RA → AS: $Yes/No, h(Yes/No, T_1, n_1, SK_{AS\text{-}CA/RAj+1})$

M4: AS → MS: $Accept/Reject, T_2, n_2, h(Accept/Reject, ID_{MS}, T_1, T_2, n_1, n_2, Msg, SK_{MS\text{-}ASj+1})$

M1: MS ส่งข้อความ ID_{MS}, T_1, n_1, $\{Msg, h(ID_{MS}, T_1, n_1, Msg, SK_{MS\text{-}ASj})\}_{SKMS\text{-}ASj+1}$ เพื่อร้องขอพิสูจน์ทราบตัวตนกับ *AS* ซึ่งข้อความ $\{Msg, h(ID_{MS}, T_1, n_1, Msg, SK_{MS\text{-}ASj})\}_{SKMS\text{-}ASj+1}$ ถูกเข้ารหัสลับด้วยเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *MS* และ *AS* ตัวแรก T_1 คือ เวลาที่ *MS* ร้องขอพิสูจน์พิสูจน์ทราบตัวตน n_1 คือค่าสุ่มตัวอักษรใช้เพื่อป้องกันการส่งข้อความซ้ำถูกสร้างโดย *MS* นอกจากนี้ข้อความ $h(ID_{MS}, T_1, n_1, Msg, SK_{MS\text{-}ASj})$ เป็นข้อความรหัสพิสูจน์ทราบตัวตนระหว่าง *MS* และ *AS*

M2: เมื่อ *AS* ได้รับข้อความจาก *MS* แล้ว *AS* ก็จะทำการตรวจสอบ ID_{MS} ว่าได้รับอนุญาตหรือไม่ ถ้าไม่ได้รับอนุญาตการติดต่อสื่อสารจะสิ้นสุดทันที แต่ถ้าได้รับอนุญาต *AS* นำข้อความ $\{Msg, h(ID_{MS}, T_1, n_1, Msg, SK_{MS\text{-}ASj})\}_{SKMS\text{-}ASj+1}$ ถอดรหัสลับด้วย $SK_{MS\text{-}ASj}$ ซึ่งเป็นเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *MS* และ *AS* ตัวแรก ต่อจากนั้นนำ *Msg* และ ID_{MS}, T_1, n_1, $SK_{MS\text{-}ASj}$ มาเข้าฟังก์ชันแฮช เปรียบเทียบกับค่าแฮช $h(ID_{MS}, T_1, n_1, Msg, SK_{MS\text{-}ASj})$ ที่ *MS* ส่งมาถ้าไม่ตรงกันการติดต่อสื่อสารจะสิ้นสุดทันที แต่ถ้าตรงกัน *AS* ก็จะส่งข้อความ ID_{MS}, $h(ID_{MS}, SK_{AS\text{-}CA/RAj})$ ให้กับ *CA/RA* โดยที่ $SK_{AS\text{-}CA/RAj}$ ซึ่ง

เป็นเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *AS* และ *CA/RA* ตัวแรก โดยที่ข้อความ $h(ID_{MS}, SK_{AS\text{-}CA/RAj})$ เป็นข้อความรหัสพิสูจน์ทราบตัวตนระหว่าง *AS* และ *CA/RA*

M3: หลังจาก *CA/RA* ได้รับข้อความ *CA/RA* ก็จะทำการตรวจสอบสองสิ่งคือตรวจสอบว่า ID_{MS} ว่าได้รับอนุญาตหรือไม่และ *CA/RA* เปรียบเทียบค่าแฮชของข้อความ $h(ID_{MS}, SK_{AS\text{-}CA/RAj})$ กับค่าแฮชของข้อความ $h(ID_{MS}, SK_{AS\text{-}CA/RAj})$ ที่ *AS* ส่งมาว่าตรงกันหรือไม่ ถ้าการเปรียบเทียบทั้งสองสิ่งไม่ตรงกัน *CA/RA* ส่งข้อความ *No* แต่ถ้าทั้งสองสิ่งตรงกันจะส่ง *Yes* กลับไปให้กับ *AS* โดยที่ *CA/RA* ส่งข้อความ *Yes/No*, $h(Yes/No, SK_{AS\text{-}CA/RAj+1})$ โดยที่ $SK_{AS\text{-}CA/RAj+1}$ เป็นเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *AS* และ *CA/RA* ตัวถัดไป โดยที่ข้อความ $h(Yes/No, SK_{AS\text{-}CA/RAj+1})$ เป็นข้อความรหัสพิสูจน์ทราบตัวตนระหว่าง *AS* และ *CA/RA*

M4: AS ได้รับข้อความจาก *CA/RA* แล้ว *AS* ตรวจสอบสองสิ่งคือ ตรวจสอบข้อความ *Yes/No* และค่าแฮชของข้อความ $h(Yes/No, SK_{AS\text{-}CA/RAj+1})$ ถ้าข้อความ *Yes* และค่าแฮชตรงกัน *AS* จะส่งข้อความ *Accept* แต่ถ้าข้อความ *No* หรือค่าแฮช $h(Yes/No, SK_{AS\text{-}CA/RAj+1})$ ไม่ตรง *AS* ส่งข้อความ *No* กลับให้ *MS* โดย *AS* ส่งข้อความ *Accept/Reject*, T_2, n_2, $h(Accept/Reject, ID_{MS}, T_1, T_2, n_1, n_2, Msg, SK_{MS\text{-}ASj+1})$ โดยที่ T_2 คือเวลาที่ *AS* ตอบกลับการร้องขอการพิสูจน์ทราบตัวตนและ $SK_{MS\text{-}AS+1}$ เป็นเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *MS* และ *AS* ตัวถัดไป n_2 คือค่าสุ่มตัวอักษรใช้เพื่อป้องกันการส่งข้อความซ้ำถูกสร้างโดย *AS* นอกจากนี้ข้อความ $h(Accept/Reject, ID_{MS}, T_1, T_2, n_1, n_2, Msg, SK_{MS\text{-}ASj+1})$ เป็นข้อความรหัสพิสูจน์ทราบตัวตนระหว่าง *MS* และ *AS*

4. การวิเคราะห์และอภิปราย

ในส่วนนี้เป็นการวิเคราะห์และอภิปรายโพรโทคอลที่ได้นำเสนอประกอบด้วย การวิเคราะห์ด้านความมั่นคงปลอดภัย การวิเคราะห์การนำไปใช้งานจริงและการวิเคราะห์การพิสูจน์ทราบตัวตนสองทางสามารถอธิบายได้ดังนี้

4.1 การวิเคราะห์ด้านความปลอดภัย

4.1.1 การรักษาความลับของข้อความ (Confidentiality)

เนื่องจากการเข้ารหัสลับด้วยเซสชันคีย์แต่ละครั้งผู้ที่มีเซสชันคีย์ที่ตรงกันเท่านั้นที่จะสามารถถอดรหัสลับข้อความได้และการสร้างเซสชันคีย์มีลักษณะเป็นแบบออฟไลน์ โดยไม่มีการส่งเซสชันคีย์ผ่านทางเครือข่ายทำให้การดักจับคีย์ไปทำการวิเคราะห์เป็นไปได้ยากทำให้ระบบมีความมั่นคงปลอดภัยเพิ่มยิ่งขึ้น

4.1.2 การพิสูจน์ทราบตัวตนของผู้ส่งข้อความ (Party Authentication)

โพโทคอลที่นำเสนอสามารถพิสูจน์ทราบตัวตนของผู้ส่งข้อความ โดยนำเอา Message Authentication Code (MAC) มาประยุกต์ใช้งานทำให้ผู้รับมั่นใจได้ว่าผู้ส่งเป็นผู้ส่งข้อความมาจริงและผู้รับเป็นผู้รับข้อความจริงและการใช้เซสชันคีย์ที่ใช้งานร่วมกันระหว่างผู้ส่งและผู้รับข้อความ

4.1.3 การต้านทานการโจมตีแบบ Replay Attack

การโจมตีแบบ Replay Attack โดยการปลอมตัวเป็นไคลเอนแล้วส่งข้อความที่ดักจับได้อีกครั้งจะประสบความสำเร็จได้น้อยเนื่องจากการเปลี่ยนเซสชันคีย์ทุกครั้งที่มีการติดต่อสื่อสารอย่างสมบูรณ์และการใช้ค่าสุ่มตัวอักษรที่ใช้แล้วจะไม่นำมาใช้ใหม่

4.1.4 การคงสภาพของข้อความ

โพโทคอลที่นำเสนอนำฟังก์ชันแฮชใช้งานทำให้สามารถตรวจสอบได้ว่าข้อความที่ส่งมานั้นระหว่างทางถูกเปลี่ยนแปลงข้อความจากบุคคลอื่นมาก่อนหรือไม่ นอกจากนี้ฟังก์แฮชยังเป็นการรักษาความลับของข้อความ

4.1.5 การต้านทานการโจมตีแบบ Brute Force Attack

การโจมตีชนิด Brute Force Attack เพื่อค้นหาคีย์ที่ถูกต้องนั้นโพรโทคอลที่นำเสนอนั้นทำได้ยาก เนื่องจากมีการเปลี่ยนแปลงค่าของเซสชันคีย์ในทุก ๆ ครั้งที่มีการติดต่อสมบูรณ์ นอกจากนี้การนำเอาเทคนิคการสร้างและการกระจายคีย์แบบออฟไลน์มาใช้งานทำให้การค้นหาคีย์ตั้งต้นในการสร้างชุดของเซสชันคีย์ทั้งหมดทำได้ยากจึงทำให้การโจมตีแบบ Brute Force Attack ประสบความสำเร็จน้อยลง

4.2 การวิเคราะห์การนำไปใช้งานจริง

จากโพรโทคอลที่นำเสนอผู้วิจัยได้ใช้ฟังก์ชันแฮชและการเข้ารหัสแบบสมมาตรมาใช้งานทำให้โพรโทคอลมีน้ำหนักเบา ซึ่งสามารถนำมาใช้กับอุปกรณ์สื่อสารไร้สายในปัจจุบันได้เป็นอย่างดีอีกทั้งขนาดความยาวของข้อความที่ติดต่อสื่อสารที่ใช้รับและส่งข้อความยังมีความยาวสั้นกว่าข้อความสูงสุดที่ข้อความสั้นสามารถส่งได้ในแต่ละครั้ง

4.3 การวิเคราะห์การพิสูจน์ทราบตัวตนสองทาง

การนำการสร้างและกระจายเซสชันคีย์แบบออฟไลน์มาใช้งานทำให้สามารถยืนยันได้ว่าผู้ที่มีคีย์ที่ตรงกันเท่านั้นที่สามารถเข้ารหัสลับและถอดรหัสลับได้หรือสามารถตรวจสอบข้อความที่รับมาได้และโพรโทคอลที่นำเสนอได้นำเอา Message Authentication Code (MAC) มาประยุกต์ใช้ ทำให้สามารถพิสูจน์ทราบตัวตนผู้ส่งและตัวตนผู้รับได้เช่น ข้อความที่ 1 ของ AuthV1

M1: MS → AS: ID_{MS}, T_1, n_1, {*Msg*, $h(ID_{MS}, T_1, n_1, Msg, SK_{MS\text{-}ASj})$}$_{SKMS\text{-}AS+1j}$

จากข้อความข้างบนการเข้ารหัสลับด้วยเซสชันคีย์ $SK_{MS\text{-}Asj+1}$ เป็นเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *MS* และ *AS* ตัวที่สองและค่าแฮชของ $h(ID_{MS}, T_1, n_1, Msg, SK_{MS\text{-}ASj})$ เซสชันคีย์ $SK_{MS\text{-}ASj}$ เป็นเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *MS* และ *AS* ตัวที่หนึ่ง ดังนั้นข้อความนี้ *MS* เท่านั้นที่สามารถสร้างข้อความและข้อความนี้ยังสามารถยืนยันผู้รับและส่งข้อความ

5. การวิเคราะห์ประสิทธิภาพของโพรโทคอล

ในส่วนนี้จะเป็นการวิเคราะห์ประสิทธิภาพของโพรโทคอลที่นำเสนอกับโพรโทคอลที่มีอยู่สามารถอธิบายได้ดังนี้

ตาราง 1. การเปรียบเทียบวิทยาการเข้ารหัสลับโพรโทคอลการพิสูจน์ทราบตัวตน

	[7]	[8]	[9]	[10]	Authv1	Authv2
Symmetric Encryption	4	3	1	3	1	1
Asymmetric Encryption	1	1	4	-	-	-
Hash Function	-	-	3	2	2	3
Number of Messages	5	4	5	5	2	4
Number of Parties	2	2	3	3	2	3

จากตารางที่ 1 โพรโทคอล Authv1 ใช้จำนวนการเข้ารหัสลับแบบสมมาตรและฟังก์ชันแฮชน้อยกว่า [7] [8] ขณะที่ Authv2 ใช้จำนวนการเข้ารหัสลับแบบสมมาตรและฟังก์ชันแฮชน้อยกว่า [9] [10] ดังนั้นโพรโทคอลที่นำเสนอจึงเหมาะสมสำหรับการสื่อสารผ่านข้อความสั้น

ตาราง 2. ขนาดความยาวและรูปแบบของข้อความ

Symbol	Size (Bits)	Example
T	160	01/01/2015 08:00:00
Yes/No	24	Yes/No
ID	80	0919596354
n	80	w@ht1&j4
Accept/Reject	48	Accept/Reject
Request	56	Request
Msg	736 (Max)	-

ตารางที่ 2 แสดงสัญลักษณ์ของข้อความ ขนาดความยาวและตัวอย่างของข้อความของโพรโทคอลที่นำเสนอโดยที่การเข้ารหัสลับใช้ AES (Advanced Encryption Standard) ความยาวคีย์ 128 bit แฮชฟังก์ชันใช้ SHA1 (Secure Hash Algorithm) 160 bit

ตารางที่ 3. ขนาดความยาวของโพรโทคอลที่นำเสนอ

Message	Authv1	Authv2
M1	37	142
M2	40	30
M3	112	23
M4	26	46
Total (Byte)	215	241

ตารางที่ 3 แสดงขนาดความยาวของข้อความแต่ละข้อความในการส่งแต่ละครั้งไม่เกินความยาวสูงสุดในการส่งข้อความ

สั้นคือ 160 byte (7-Bit ASCII) โดยที่ *Msg* มีความยาวสูงสุดค 736 bit ดังนั้นโพรโทคอลที่นำเสนอจึงเหมาะสำหรับข้อความสั้นขณะที่ยังคงมีความมั่นคงปลอดภัยที่เพียงพอ

ตารางที่ 4 การวิเคราะห์พื้นที่ที่สูญเสียให้แก่โพรโทคอล

Session		Protocol Overhead	%	7-Bit ASCII
Authv1	M1	37	23.12	123
	M2	40	25.00	120
	M3	112	70.00	48
	M4	26	16.25	134
Authv2	M1	142	88.75	18
	M2	130	81.25	30
	M3	23	14.37	137
	M4	46	28.75	144

จากตารางที่ 4 แสดงพื้นที่ที่สูญเสียให้แก่โพรโทคอลที่นำเสนอ โดยส่วนใหญ่พื้นที่ที่สูญเสียให้แก่โพรโทคอลน้อยเพราะการออกแบบโพรโทคอลจะเน้นการใช้ฟังก์ชันแฮชและการเข้ารหัสลับแบบสมมาตรเท่าที่จำเป็น แต่ยังคงมีความมั่นคงปลอดภัยที่เพียงพอ

ตารางที่ 5 พลังงานสูญเสียของวิทยาการการเข้ารหัสลับ

Algorithm	Key size bits	Output size bits	Energy (mJ/byte)
AES	128	-	1.21 (μJ/byte)
RSA	1,024	-	546.50 (μJ/byte)
SHA1	-	160	0.76 (μJ /byte)

ตารางที่ 5 พลังงานที่สูญเสียของวิทยาการการเข้ารหัสลับได้ถูกนำเสนอโดย [16] โดยทำการทดลองกับอุปกรณ์สื่อสารไร้สายแสดงรายละเดียดดังตารางที่ 5

ตารางที่ 6 การเปรียบเทียบพลังงานสูญเสียของวิทยาการการเข้ารหัสลับ

	[12]	[24]	[25]	[26]	Authv1	Authv2
AES	4.84	3.63	1.21	3.63	1.21	1.21
RSA	546.5	546.5	2186	0	0	0
SHA1	0	0	2.28	1.52	1.52	2.28
Total Energy (μJ/byte)	551.34	550.13	2,189.49	5.15	2.73	3.49

ตารางที่ 6 พลังงานสูญเสียของวิทยาการการเข้ารหัสลับเปรียบเทียบโพโทคอลที่มีอยู่กับโพรโทคอลที่นำเสนอโดยโพโทคอลที่นำเสนอพลังงานที่สูญเสียให้แก่โพรโทคอลน้อยกว่าโพโทคอลที่มีอยู่เพราะการออกแบบโพรโทคอลจะเน้นการใช้ฟังก์ชันแฮชและการเข้ารหัสลับแบบสมมาตรเท่าที่จำเป็น แต่ยังคงมีความมั่นคงปลอดภัยที่เพียงพอ

6. สรุปผลการวิจัย

จากข้อจำกัดของงานวิจัยที่มีอยู่เช่น การพิสูจน์ทราบตัวตนและความมั่นคงปลอดภัยการส่งข้อความสั้น งานวิจัยนี้ได้นำเสนอโพรโทคอลสำหรับพิสูจน์ทราบตัวตนโดยผ่านข้อความสั้น ซึ่งได้นำการกระจายเซสชันคีย์แบบออฟไลน์และการใช้แฮชฟังก์ชันมาใช้งานทำให้โพรโทคอลมีน้ำหนักเบาเหมาะกับอุปกรณ์สื่อสารไร้สายในปัจจุบัน เนื่องจากมีการคำนวณน้อย นอกจากนี้ยังมีคุณสมบัติความมั่นคงปลอดภัยเช่น การพิสูจน์ทราบตัวตน การรักษาความลับของข้อความและการคงสภาพของข้อความ รวมทั้งโพรโทคอลที่นำเสนอมีประสิทธิภาพและใช้เวลาน้อยดีกว่างานวิจัยที่มีอยู่และการส่งข้อความสั้นแต่ละครั้งน้อยกว่าข้อความสูงสุดอีกทั้งยังเข้ากันได้กับโครงสร้างการส่งข้อความสั้นในปัจจุบัน

งานวิจัยในอนาคตผู้วิจัยจะพัฒนาโปรแกรมต้นแบบจากโพรโทคอลที่นำเสนอ เพื่อให้สามารถใช้งานได้จริงและพัฒนาโพรโทคอลพิสูจน์ทราบตัวตนสองทางกับการชำระเงินผ่านข้อความสั้น

เอกสารอ้างอิง

[1] S. Kungpisdan and S. Metheekul, “A Secure Offline Key Generation With Protection Against Key Compromise,” Proceedings of the 1 3 th World Multi-conference on Systemics, Cybernetics, and Informatics, Orlando, USA, 2009.

[2] O. Dandash, Y. Wang, and P.D. Le, “Fraudulent Internet Banking Payments Prevention using Dynamic Key,”Journal of Networks,” Vol.3(1), Academy Publisher, pp. 25-34, 2008.

[3] S. Kungpisdan, P.D. Le, and B. Srinivasan, “A Limited-Used Key Generation Scheme for Internet Transactions,” Lecture Notes in Computer Scienc e, Vol. 3325, 2005.

[4] Li, Y. and Zhang, X, “A Security-enhanced One-time Payment Scheme for Credit Card,” Proc. of the Int’l Workshop on Research Issues on Data Engineering: Web Services for ECommerce and E-Government Applications, 2004.

[5] S. Kungpisdan, B. Srinivasan, and P.D. Le, “Lightweight Mobile Credit-card Payment Protocol,” Lecture Notes in Computer Science, Vol. 2904, pp. 295-308, 2003.

[6] A. D. Rubin and R.N. Wright, “Off-line Generation of Limited-Use Credit Card Numbers,” Lecture Notes in Computer Science, Vol. 2339, pp. 196, 2002.

[7] H. Ratshinanga, J. LO, and J. Bishop. "A Security Mechanism for Secure SMS Communication," Proceedings of SAICSIT, pp. 1-6, 2004.

[8] J. L. Lo, J. Bishop and J.H.P Eloff, "SMSSec: an end-to-end protocol for secure SMS," Computers & Security, vol. 27, no. 5-6, pp. 154-167, 2008.

[9] H. Rongyu, Z. Guolei, C. Chaowen, X. Hui, Q. Xi and Q. Zheng, "A PK-SIM card based end-to-end security framework for SMS", Computer Standards & Interfaces 31.4, pp. 629-641, 2009.

[10] N. Saxena and N.S. Chaudhari, "SecureSMS: A secure SMS protocol for VAS and other applications," Journal of Systems and Software 90 (2014): pp. 138-150, 2014.

[11] N. Saxena, N. S. Chaudhari and G. L. Prajapati, "An extended approach for SMS security using authentication functions", Industrial Electronics and Applications (ICIEA), 7th IEEE Conference on. IEEE, pp. 663-668, 2012.

[12] N. Saxena and A. Payal, "Enhancing Security System of Short Message Service for M-Commerce in GSM", International Journal of Computer Science & Engineering Technology (IJCSET), ISSN: 2229-3345 Vol. 2 No. 4, pp. 126-133, 2011.

[13] N. Saxena and N. S. Chaudhari, "A secure approach for SMS in GSM network", Proceedings of the CUBE International Information Technology Conference. ACM, pp. 59-64, 2012.

[14] M. Toorani and A. A. B. Shirazi, SSMS – A Secure SMS Messaging Protocol for the M-Payment Systems, Proceedings of the 13th IEEE Symposium on Computers and Communications (ISCC'08), Marrakech, July 6-9, 2008, pp. 700-705.

[15] A. Biryukov, A. Shamir and D. Wagner, Real Time Cryptanalysis of A5/1 on a PC, 2000 [Online]. Available: http://cryptome.org/a51-bsw.htm. Accessed on: 13 February 2007.

[16] N.R. Potlapally, S. Ravi, A. Raghunathan, and N.K. Jha, “A study of the energy consumption characteristics of cryptographic algorithms and security protocols,” IEEE Transactions on mobile computing, vol. 5, no. 2, pp. 128-143, 2006.