โพรโทคอลการชำระเงินผ่านเครือข่ายไร้สายด้วยข้อความสั้นสำหรับธุรกรรมชนิดชำระก่อนและชำระทีหลังที่มีคุณสมบัติการพิสูจน์ตัวจริง

An SMS-based Mobile Payment Protocol for Prepaid and Postpaid Transactions with Authentication

เมมินทร์ วรศาสตร์ [1] ธันยพร วิทยาบัณฑิต [2] ชาลี ธรรมรัตน์ [3] และ ศุภกร กังพิศดาร [4]
คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร
140 ถนนเชื่อมสัมพันธ์ เขตหนองจอก กรุงเทพฯ 10530 โทรศัพท์ 02-988-3655 ต่อ 4111
Emails: [1]maykin@miss.in.th, [2]thunyaporn.wit@gmail.com, [3]chalee@miss.in.th, [4]supakorn@mut.ac.th

บทคัดย่อ

การทำธุรกรรมด้วยบริการข้อความสั้น (Short Message Service หรือ SMS) เป็นช่องทางในการชำระเงินที่ได้รับความนิยมสูงขึ้นในปัจจุบัน ระบบชำระเงินสำหรับการทำธุรกรรมชนิดนี้เป็นสิ่งที่จำเป็นที่ผ่านมามีการเสนอโพรโทคอลสำหรับการชำระเงินผ่าน SMS จำนวนมาก แต่อย่างไรก็ตามโพรโทคอลดังกล่าวยังขาดคุณสมบัติทางด้านความมั่นคงปลอดภัยที่จำเป็น งานวิจัยฉบับนี้เสนอโพรโทคอลสำหรับการชำระค่าสินค้าและบริการผ่าน SMS ที่เปิดโอกาสให้ผู้ใช้งานสามารถชำระเงินโดยตรงกับผู้ให้บริการ หรือสามารถชำระเงินให้พ่อค้าผ่านผู้ให้บริการ นอกจากธุรกรรมที่เกิดขึ้นจะมีคุณสมบัติด้านความมั่นคงปลอดภัย เช่น การพิสูจน์ตัวจริงการส่ง SMS การเรียกเก็บค่าบริการตามจริง และนั้นยังคงมีความง่ายและเข้ากันได้กับโครงสร้างพื้นฐานของระบบ SMS อีกด้วย

คำสำคัญ : ข้อความสั้น, การพิสูจน์ตัวจริง, โพรโทคอลการเข้ารหัสลับ, การชำระเงินผ่านเครือข่ายไร้สาย, การชำระเงินผ่าน SMS, โพรโทคอลการชำระเงิน

Abstract

Conducting electronic transactions over Short Message Service (or SMS for short) has become more popular. A secure payment system for SMS transactions is required. A number of payment protocols for SMS transactions have been proposed, but they still lack necessary security properties. This paper introduces an SMS-based mobile payment protocol that allows a client to perform payment transactions directly to a merchant, or to perform transactions to a merchant via a mobile operator. The proposed protocol not only satisfies necessary security properties including authentication, but it is also simple and compatible with existing SMS infrastructure.

Keywords: Short Message Service, authentication, cryptographic protocols, mobile payment, SMS payment, payment protocols

1. บทนำ

ในปัจจุบันมีการใช้ SMS สำหรับการทำธุรกรรมการชำระเงินกันอย่างแพร่หลาย เช่น การชำระเงินสำหรับเสียงรอสาย (Ringtones) เพลง หรือรูปภาพจากผู้ให้บริการมือถือ โดยเรียกธุรกรรมในลักษณะนี้ว่า Mobile Payment ซึ่งหมายถึง การทำธุรกรรมการชำระเงินผ่านเครือข่ายไร้สายในขณะที่กำลังเคลื่อนที่อยู่ โดยผู้ชำระเงินโอนเงินให้ผู้รับเงิน แล้วรับสินค้าหรือบริการจากผู้รับเงิน ด้วยพื้นฐานของการสื่อสารไร้สายจึงนำมาซึ่งปัญหาที่เกิดขึ้นเกี่ยวกับธุรกรรม ความมั่นคงปลอดภัยของการชำระเงินบนมือถือ ข้อมูลที่ส่งผ่านเครือข่ายไร้สายถูกดักจับได้ง่าย แม้ว่าเครือข่าย GSM มีการเข้ารหัสลับของข้อมูลที่ส่งระหว่างอุปกรณ์เคลื่อนที่และสถานีฐาน ที่อาศัยเทคนิคการเข้ารหัสลับ A5/1 และ A5/2 ซึ่งมีรายงานถึงความอ่อนแอและช่องโหว่ตาม [1] ดังนั้นการรักษาความมั่นคงปลอดภัยของเครือข่าย GSM ที่ชั้นดาต้าลิงก์ (Data-link layer) จึงไม่เพียงพอ จำเป็นต้องมีช่องทางสำหรับการสื่อสารที่มั่นคงปลอดภัยบนเครือข่ายไร้สายที่ชั้นแอพลิเคชัน (Application layer) ซึ่งสามารถทำได้โดยใช้การเข้ารหัสลับนั่นเอง

เพื่อสร้างความมั่นคงปลอดภัยให้กับการชำระเงินผ่านมือถือโดยใช้ SMS นั้น มีโพรโทคอลสำหรับการชำระเงินมือถือจำนวนมากถูกนำเสนอ [1, 2, 3] โดย Toorani *et al.* [1] เสนอระบบ SSMS ซึ่งใช้วิทยาการเข้ารหัสลับแบบ Elliptic-curve (Elliptic-curve Cryptography) ที่มีคุณสมบัติด้านความมั่นคงปลอดภัยมากมาย เช่น การรักษาความลับของข้อมูล (Data Confidentiality) ความคงสภาพของข้อมูล (Data Integrity) การพิสูจน์ตัวจริง (Authentication) และการไม่สามารถปฏิเสธความรับผิดชอบได้ (Non-repudiation) นอกจากนี้ยังมีความสามารถในการตรวจสอบพับบลิคคีย์ (Public key) ของแต่ละฝ่าย และส่งต่อความลับ (Forward Secrecy) เนื่องจากเป็นระบบที่ใช้การเข้ารหัสลับแบบพับบลิคคีย์จึงจำเป็นต้องใช้บุคคลที่สามที่เชื่อถือได้ ทำหน้าที่เป็นผู้รับรอง

งานวิจัยที่น่าสนใจอีกงานได้แก่งานวิจัยของ Harb *et al.* [2] ซึ่งเสนอ SecureSMSPay ที่เป็นระบบการชำระเงินระหว่างผู้ชำระเงินและผู้รับเงิน โดยการโอนเงินทำจากธนาคารของผู้ชำระเงิน ผ่านทาง Payment Gateway แต่ระบบนี้จำเป็นต้องรู้หมายเลขโทรศัพท์มือถือของผู้ชำระเงินและผู้รับเงิน นอกจากนี้การรักษาความมั่นคงปลอดภัยของระบบจะขึ้นอยู่กับการเข้ารหัสลับแบบสมมาตรที่ต้องใช้คีย์ร่วมกัน การเปลี่ยนเซสชันคีย์นั้นระบบใช้ค่าแฮช (Hash Value) ของการหมุนเวียนของเซสชันคีย์ ซึ่งเสี่ยงต่อการถูกโจมตี

นอกจากนี้ Hashemi *et al.* [3] เสนอกรอบการทำงาน สำหรับการชำระเงินผ่านมือถือที่มีความมั่นคงปลอดภัยโดยใช้ SMS ที่อธิบายความสัมพันธ์ระหว่าง SMS gateway และ SMSC (Short Message Service Center) และภาพรวมของการชำระเงินที่เหมาะสมสำหรับ SMS โดยใช้การเข้ารหัสลับแบบ AES (Advanced Encryption Standard) เพื่อสร้างความมั่นคงปลอดภัยของธุรกรรมที่เกิดขึ้น ซึ่งเป็นวิธีการเข้ารหัสลับแบบสมมาตร (Symmetric Cryptography) โดยที่คีย์ (Key) ที่ใช้ร่วมกันระหว่างลูกค้าและธนาคารมีการกระจายเฉพาะตอนที่ลูกค้าลงทะเบียนใช้บริการเป็นครั้งแรกเท่านั้น แต่ไม่มีการแลกเปลี่ยนเซสชันคีย์ (Session key) ระหว่างกัน

ต่อมา Li-Chang *et al.* [5] ได้เสนอโพรโทคอลที่อยู่ในระดับชั้นแอพลิเคชันเพื่อสร้างความปลอดภัยแบบ End-to-end Security ด้วยเช่นกัน แต่โพรโทคอลนี้ให้คุณสมบัติในการรักษาความมั่นคงปลอดภัยเพียงบางส่วน ซึ่งยังไม่ครอบคลุมคุณสมบัติที่จำเป็นอีกหลายประการ

บทความวิจัยฉบับนี้เสนอโมเดลสำหรับการชำระค่าสินค้าและบริการผ่านข้อความสั้นที่มีคุณสมบัติทางด้านความมั่นคงปลอดภัยที่จำเป็น นอกจากนี้โพรโทคอลนี้ยังมีน้ำหนักเบาโดยใช้การเข้ารหัสลับแบบสมมาตรและฟังก์ชันแฮช ด้วยโพรโทคอลที่นำเสนอนี้ลูกค้าสามารถชำระเงินให้สินค้าบริการให้แก่ผู้ให้บริการ หรือชำระเงินให้กับร้านค้าผ่านผู้ให้บริการ ซึ่งทำให้สามารถนำไปใช้ในธุรกิจได้จริง รวมถึงยังมีคุณสมบัติในการรักษาความมั่นคงปลอดภัยของการทำธุรกรรมที่จำเป็น คือ การรักษาความลับข้อมูล ความคงสภาพของข้อมูล การพิสูจน์ตัวจริงของผู้ใช้ และการป้องกันการเรียกเก็บค่าบริการเกินจริง รวมถึงมีการใช้เทคนิคการกระจายคีย์ตาม [8] ซึ่งโพรโทคอลที่เสนอสามารถเข้ากันได้กับโครงสร้างพื้นฐานของ SMS ที่มีอยู่

โครงสร้างของงานวิจัยฉบับนี้ ประกอบด้วย 5 ส่วน โดยส่วนที่ 2 กล่าวถึงงานวิจัยที่เกี่ยวข้อง ส่วนที่ 3 งานวิจัยที่นำเสนอ ส่วนที่ 4 เสนอการวิเคราะห์ด้านความมั่นคงปลอดภัยของโพรโทคอลที่นำเสนอ และส่วนที่ 5 สรุปผลการวิจัย

2. งานวิจัยที่เกี่ยวข้อง

2.1. การชำระเงินผ่านเครือข่ายไร้สาย

จาก [9] ระบบการชำระเงินทั่วไปประกอบด้วย 5 ฝ่าย คือ Client (ลูกค้า) Merchant (พ่อค้า) Payment Gateway (หรือ PG) Issuer (สถาบันการเงินของลูกค้า) และ Acquirer (สถาบันการเงินของร้านค้า) การดำเนินการของ issuer และ acquirer กระทำผ่านอินเทอร์เน็ต ขณะที่การตัดเงินจากการชำระเงินกระทำภายในเครือข่ายระหว่างธนาคาร โดยที่การทำธุรกรรรม นั้น มี 3 รายการหลัก คือ การชำระเงิน การหักเงิน และการเพิ่มเงิน

การชำระเงิน (Payment) เป็นปฏิสัมพันธ์ที่เกิดขึ้นเมื่อลูกค้าต้องการซื้อสินค้าหรือบริการกับพ่อค้า รวมถึงพ่อค้าส่งใบเสร็จรับเงินการชำระเงินให้ลูกค้า การตัดเงินเกิดขึ้นที่ฝั่งลูกค้า โดยส่งคำขอไปยัง PG (ในนามของ Issuer) เพื่อหักเงินตามจำนวนที่ต้องการชำระจากบัญชีของลูกค้า และแจ้งลูกค้าว่าจำนวนเงินที่ต้องการถูกหักจากบัญชีของลูกค้าแล้ว การเพิ่มเงินทำโดยพ่อค้า โดยการร้องขอ PG (ในนามของ Acquirer) เพื่อขอโอนเงินไปยังบัญชีของพ่อค้า แล้วแจ้งพ่อค้าว่ามีการโอนเข้าบัญชีพ่อค้าแล้ว มีธุรกรรมในหลายโพรโทคอลสำหรับการชำระเงิน [2, 3, 17] เป็นไปตามขั้นตอนต่อไปนี้

C → M: *Payment (Request), Debit (Request)*

M → PG: *Debit (Request), Credit (Request)*

PG → M: *Credit (Response), Debit (Response)*

M → C: *Payment (Response), Debit (Response)*

โดย C, M, PG หมายถึง ลูกค้า พ่อค้า และ Payment Gateway ตามลำดับ อย่างไรก็ตามบางโพรโทคอลสำหรับการชำระเงินที่ทำงานแตกต่างออกไป ในบางระบบการชำระเงินมี PG เป็นศูนย์กลางที่ต้องทำธุรกรรมผ่านระหว่างลูกค้า ตัวอย่างที่เห็นได้ชัดเจนของระบบการชำระเงิน คือ ระบบธนาคารอินเทอร์เน็ต (Internet Banking) ซึ่งการทำธุรกรรมกระทำผ่านคนกลาง คือ PG โดยกระบวนการนี้น่าจะเหมาะสมกับระบบการชำระเงินโดยใช้ SMS ในปัจจุบันที่ผู้ให้บริการมือถือ ทำหน้าที่เป็น PG อยู่แล้วกล่าวคือลูกค้าสามารถสมัครรับบริการกับผู้ให้บริการมือถือ เช่น การชำระเงินค่าสินค้าหรือบริการรวมถึง โปรแกรม เสียงรอสาย เพลง คลิปวิดีโอ ฯลฯ ซึ่งลูกค้าจะได้รับสิทธิ์ในการสั่งซื้อสินค้าหรือบริการภายในวงเงินที่มี จากนั้นผู้ให้บริการมือถือจะทำการโอนเงินดังกล่าวให้พ่อค้า

2.2 SMSSec

Li-Chang *et al.* [4] ที่ได้นำเสนอ SMSSec ซึ่งเป็นโพรโทคอลที่ใช้ในการเพิ่มความมั่นคงปลอดภัยให้แก่การส่ง SMS ที่ผู้แต่งอ้างว่าสามารถให้ความมั่นคงปลอดภัยแบบ End-to-end Security นั้น ขั้นตอนการทำงานของ SMSSec มีดังต่อไปนี้

2.2.1 First Handshake

ครั้งแรก MS (Mobile Station) จะส่งข้อความที่ถูกเข้ารหัสลับด้วยพับบลิคคีย์ (Public key) ของ AS โดยที่มีการส่งพารามิเตอร์ที่ใช้ใน

การสร้างเซสชันคีย์ (Session key) สำหรับการเข้ารหัสลับครั้งต่อไป และส่ง *HMAC(U, PIN, Q)* เพื่อพิสูจน์ตัวจริงของ *MS* โดยที่ *U* คือ เบอร์โทรศัพท์ PIN คือ คีย์ที่มีเพียง *MS* และ *AS* เท่านั้นที่รู้ และ *Q* คือ หมายเลขลำดับของเซสชันจากนั้นเมื่อ *AS* ได้รับข้อความแล้วจะถอดรหัสลับด้วยไพรเวทคีย์ (Private key) ของตนเอง และจะนำข้อมูลที่ได้มาใช้สร้างเซสชันคีย์สำหรับเข้ารหัสลับและส่งข้อความกลับไปเพื่อส่ง Private Port Number ให้ *MS* ทราบว่าใช้พอร์ตดังกล่าวในการติดต่อ *AS* ครั้งต่อไป โดยที่ข้อความนี้จะถูกเข้ารหัสลับด้วยเซสชันคีย์ที่สร้างจากพารามิเตอร์ที่ *MS* ส่งมาให้ หลังจาก *MS* ได้รับข้อความ จะทำการตรวจสอบว่าเป็น *AS* ตัวจริงที่ติดต่อกลับมาหรือไม่ และส่งข้อมูลส่วนที่เป็นข้อความที่เข้ารหัสลับด้วยเซสชันคีย์ตัวเดิมให้ *AS* ผ่านพอร์ตที่ *AS* ระบุมาให้ และหาก *AS* ต้องการส่งข้อความให้ *MS* จะใช้เซสชันคีย์ตัวนี้ในการเข้ารหัสลับเช่นกัน

2.2.2 Next Handshake

หลังจาก First Handshake ถ้า *MS* จะส่งข้อความเพื่อระบุตัวตนของ MS เพื่อให้ *AS* รู้ว่าจะนำเซสชันคีย์ที่ใช้กับ *MS* ในการถอดรหัสลับ พร้อมกับส่งพารามิเตอร์ที่ใช้ในการสร้างเซสชันคีย์ตัวใหม่ ซึ่งข้อความจะถูกเข้ารหัสลับด้วยเซสชันคีย์ที่ใช้ในการส่งข้อความครั้งก่อน หลังจากนั้น *MS* และ *AS* จะใช้วิธีการคล้ายกับ First Handshake แต่จะแตกต่างกันตรงคีย์ที่ใช้ในการเข้ารหัสลับเป็นเซสชันคีย์ซึ่งสร้างจากพารามิเตอร์ใหม่ที่ *MS* ส่งไปให้ *AS* พร้อมกับข้อความแรก

2.2.3 ปัญหาและข้อจำกัดของ SMSSec

ปัญหาและข้อจำกัดของ SMSSec สามารถสรุปได้ดังต่อไปนี้

- การทำ First Handshake ใช้การเข้ารหัสลับด้วยพับบลิคคีย์ของ AS เป็นการพิสูจน์ตัวจริงเพียงฝั่งเดียวและ PIN ที่ใช้เป็นคีย์ที่ใช้เข้ารหัสลับ สามารถถูกวิเคราะห์หาค่าได้ และค่าของ U ก็เป็นค่าคงที่
- การทำ Next Handshake ทุกครั้งจะใช้ *U* ซึ่งเป็นค่าคงที่เพื่อระบุตัวตนของ *MS* ทำให้ผู้โจมตีสามารถปลอมแปลงข้อความขึ้นมาเพื่อหลอกให้ *AS* ส่งข้อมูลที่สำคัญไปยังผู้โจมตี
- โพรโทคอลนี้ไม่มีคุณสมบัติความคงสภาพของข้อมูล (Data Integrity) และการไม่สามารถปฏิเสธความรับผิดชอบ (Non-repudiation)
- เทคนิคในการสร้างเซสชันคีย์ที่ผู้แต่งนำเสนอนั้น ค่าคีย์เริ่มต้นคือ 0 ทำให้ผู้โจมตีสามารถคาดเดาและวิเคราะห์หาเซสชันคีย์ตัวถัดไปได้โดยใช้ค่าเริ่มต้นชุดเดียวกันนี้

2.3 SecureSMSPay

Harb *et al.* [2] ได้เสนอ SecureSMSPay ซึ่งเป็นระบบการชำระเงินโดยมีการเข้ารหัสลับแบบสมมาตร ระบบนี้ประกอบด้วย 5 ฝ่าย คือ ผู้รับ (Payee) ผู้ชำระเงิน (Payer) ธนาคารผู้รับเงิน (Payee's Bank) ธนาคารของผู้ชำระเงิน (Payer's Bank) และ PG ผู้รับเงินเปิดบัญชีกับธนาคารของตน ส่วนผู้ชำระเงินก็เปิดกับธนาคารของตน มี PG ทำหน้าที่เป็นคนกลางระหว่างธนาคาร การโอนเงินทำจากธนาคารของผู้ชำระเงินที่ธนาคารผู้รับเงินของการชำระเงินผ่านทาง PG

อย่างไรก็ตาม ระบบดังกล่าวมีข้อบกพร่อง คือบางข้อความจะถูกส่งโดยที่ไม่มีมีการเข้ารหัสลับ เช่น หมายเลขโทรศัพท์มือถือ และสถานะก็สามารถแก้ไขได้โดยผู้โจมตี นอกจากนี้การรักษาความปลอดภัยของระบบจะขึ้นอยู่กับการเข้ารหัสลับแบบสมมาตรที่ใช้คีย์ร่วมกัน การเปลี่ยนคีย์ของระบบ ได้มาจากค่าแฮชจากการเลื่อนบิตของเซสชันคีย์ปัจจุบัน จะสังเกตได้ว่าคีย์ที่สร้างจากฟังก์ชันแฮชมีความยาวคงที่ ไม่ได้เพิ่มความมั่นคงปลอดภัยจากการโจมตีแบบ Brute-force แต่อย่างใด

2.4 SSMS

นอกจากนี้ Toorani *et al.* [1] เสนอ SSMS โดยใช้การเข้ารหัสลับแบบ Elliptic-curve ซึ่งให้คุณสมบัติ ความลับของข้อมูล ความคงสภาพของข้อมูล การพิสูจน์ตัวจริง รวมถึงการไม่สามารถปฏิเสธความรับผิดชอบได้ นอกจากนั้นโพรโทคอลนี้ยังมีความสามารถในการตรวจสอบคีย์สาธารณะของแต่ละฝ่าย และมีคุณสมบัติการส่งต่อความลับได้ ซึ่งเป็นระบบที่ใช้การเข้ารหัสแบบคีย์สาธารณะ จึงจำเป็นต้องมีบุคคลที่สามที่เชื่อถือได้ทำหน้าที่เป็นผู้รับรอง

2.5 วิธีการของ Hashemi *et al.*

Hashemi *et al.* [3] เสนอกรอบการชำระเงินมือถือโดยใช้ SMS ที่อธิบายความสัมพันธ์ระหว่าง SMS gateway และ Short Message Service Center (หรือ SMSC) และภาพรวมของการชำระเงินด้วย SMS แบบต่างๆ โดยใช้ Advanced Encryption Standard (หรือ AES) เพื่อเพิ่มความมั่นคงปลอดภัยให้กับธุรกรรม ซึ่งเป็นวิธีการเข้ารหัสลับแบบสมมาตร ซึ่งคีย์ที่ใช้ร่วมกันระหว่างลูกค้าและธนาคารมีการกระจายเฉพาะในกรณีที่ ลูกค้าลงทะเบียนใช้บริการครั้งแรก แต่อย่างไรก็ตาม ไม่มีการกล่าวถึงการปรับเปลี่ยนคีย์ในบทความนี้

2.6 การสร้างและกระจายเซสชันคีย์แบบออฟไลน์

Kungpisdan *et al.* ได้นำเสนอวิธีการสร้างและกระจายคีย์แบบออฟไลน์ ซึ่งมีการสร้างและกระจายเซสชันคีย์โดยที่ไม่ต้องมีการส่งคีย์ดังกล่าวผ่านเครือข่าย [9] ซึ่งมีจุดเด่นเหนือเทคนิคการกระจายคีย์แบบออนไลน์ โดยเทคนิคการสร้างและกระจายคีย์แบบต่างๆ ถูกเสนอเสนอ [5, 6, 7, 8, 9, 10] โดยที่ Kungpisdan *et al.* ได้แนะนำเทคนิคการสร้างคีย์ที่ไม่เพียงแต่มีความปลอดภัยจากการโจมตีเท่านั้น แต่ยังสามารถทำงานได้แบบออฟไลน์

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

หลังจากมีแลกเปลี่ยนค่า $\{K_{AB}, DK, m\}$ ผู้ที่สื่อสารกันทำการสร้างเซ็ตของ *Preference keys* K_i, $i = 1,2,\ldots, m$ ดังสมการ

$$K_i = h(K_{i-1}, DK) \quad (2.1)$$

จากนั้น ทั้งคู่สร้างเซ็ตของ *Intermediate Keys (IK)* ซึ่งเป็นการเพิ่มความยากในการวิเคราะห์การถอดรหัสลับ เพิ่มความยากในการสืบค้นของ *Preference key* โดยมีรูปแบบดังนี้

$$IK^x_j = h(conc(IK^{x-1}_{mid}), IK^x_{j-1}) \quad (2.2)$$

โดย x เป็นจำนวนรอบของ j เป็นจำนวนของ 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 ที่ยังเหลืออยู่ในชุดข้อมูลของ 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* ในทุกๆรอบ จะทำการลบค่าออกจากระบบ ส่วนที่เหลือของ *Intermediate Keys* ในรอบอื่นๆ สามารถเขียนได้ดังนี้

$$\{K_1, K_2, ..., K_{rm}\},\{K^1_1, K^1_2, ..., K^1_{rm}\}, \{K^2_1, K^2_2, ..., K^2_{rm}\},...$$
$$\{K^n_1, K^n_2, ..., K^n_{rm}\}$$

ผลที่ได้ในรอบสุดท้ายของ *Intermediate Keys* ที่ได้จะถูกใช้เป็นเซสชันคีย์ (Session key) (SK_j) โดยที่ $j = 1,... ,m$ คือ

$$IK^n_1 = SK_1, IK^n_2 = SK_2, ..., IK^n_m = SK_m \quad (2.3)$$

จากเทคนิคนี้จะเห็นว่าจะมีการส่งเพียงค่าตัวแปร ที่เป็นค่าเริ่มต้นเพื่อนำไปใช้ในการสร้างคีย์ และคีย์ที่ถูกสร้างขึ้น ถูกนำมาใช้เพียงครั้งเดียวไม่มีการนำมาใช้ซ้ำและสามารถสร้างคีย์โดยโอกาสเกิดค่าคีย์ที่ซ้ำเป็นไปได้ยาก

3. งานวิจัยที่นำเสนอ

เพื่อเป็นการแก้ไขปัญหาและข้อจำกัดของงานวิจัยที่มีอยู่ งานวิจัยฉบับนี้นำเสนอโพรโทคอลใหม่สำหรับการพิสูจน์ตัวจริงและการเรียกเก็บค่า บริการตามจริงที่มีความมั่นคงปลอดภัยโดยนำเอาเทคนิคการสร้างและการกระจายเซสชันคีย์แบบออฟไลน์มาใช้งาน

3.1 นิยามและสมมติฐาน

ลูกค้า (Client หรือ *C*) คือ ผู้ที่สั่งซื้อสินค้าหรือบริการ, พ่อค้า (Merchant หรือ *M*) คือ ผู้ที่ขายสินค้าหรือบริการ, ผู้ให้บริการโทรศัพท์เคลื่อนที่ (Mobile Operator หรือ *O*) คือ ผู้ให้บริการโทรศัพท์มือถือ, Authentication Source (AS) คือ เซิร์ฟเวอร์ที่ใช้พิสูจน์ตัวจริงของการส่ง SMS โดยที่ *C* ใช้มือถือที่ติดตั้งซอฟต์แวร์ที่นำเสนอ และ *M* จดทะเบียนเป็นผู้ค้ากับ *O* ซึ่ง *O* ตั้งตัวเองเป็นเซิร์ฟเวอร์ เรียกว่า SMS Payment Server (SPS) เพื่อให้บริการการชำระเงินกับ *C* และ *M*

- S_{KABj} โดยที่ j = 1 ถึง *m* คือ เซสชันคีย์ใช้ร่วมกันระหว่าง *A* กับ *B*
- ID_A คือสิ่งที่ระบุว่าเป็น *A*
- $\{m\}_K$ เป็นข้อความที่เข้ารหัสสมมาตรของข้อความ *m* ด้วยคีย์ *K*
- *h(m)* คือค่าแฮชของข้อความ *m*
- *h(m, K)* เป็นรหัสพิสูจน์ตัวจริงข้อความ (MAC) ของข้อความ *m* ที่ใช้คีย์ *K*
- *PN* คือ หมายเลขโทรศัพท์ของ *C*
- *PIN* คือ คีย์ที่รู้ระหว่าง *C* และ *AS*
- *C* เปิดบัญชีกับ *O* สำหรับใช้บริการโทรศัพท์และใช้ข้อมูล
- *C* ลงทะเบียนกับ *AS* หลังจากลงทะเบียนเสร็จแล้ว *C* ก็จะส่ง PIN ของโทรศัพท์มือถือไปยัง *AS* ซึ่งจะดำเนินการผ่านช่องทางที่มั่นคงปลอดภัยเช่น WTLS (Wireless Transport Layer Security)

3.2 การลงทะเบียนของลูกค้า

ในการลงทะเบียนของลูกค้านั้น ลูกค้าทำการติดตั้งซอฟต์แวร์การชำระเงินด้วย SMS ตามโพรโทคอลที่นำเสนอ เมื่อซอฟต์แวร์ถูกดาวน์โหลดไปยังเครื่องของลูกค้า ลูกค้าต้องเข้าสู่ระบบการลงทะเบียนซึ่งการลงทะเบียนดำเนินการผ่านช่องทางที่มั่นคงปลอดภัย วัตถุประสงค์ของการลงทะเบียน คือ การแลกเปลี่ยน $\{K_{CO}, DK_{CO}, m_{CO}\}$ ระหว่างลูกค้าและผู้ให้บริการ ซึ่งโทรศัพท์มือถือของลูกค้าแต่ละรายอาจติดตั้ง SIM Application Toolkit (หรือ SAT) ซึ่งมีคีย์ที่ใช้ร่วมกับผู้ให้บริการโทรศัพท์มือถืออยู่แล้วก็ได้ ซึ่งหลังจากการแลกเปลี่ยน $\{K_{CO}, DK_{CO}, m_{CO}\}$ กัน ทั้งลูกค้าและผู้ให้บริการ สามารถสร้างเซสชันคีย์ SK_{COj} เมื่อ $j = 1$ ถึง *m* โดยใช้เทคนิคการสร้างคีย์ที่แสดงในหัวข้อที่ 2.6

3.3 การพิสูจน์ตัวจริง

ก่อนที่ *C* จะชำระค่าสินค้าหรือบริการ *C* แลกเปลี่ยน $\{K_{CAS}, DK_{CAS}, m_{CAS}\}$ แล้วทั้ง *AS* และ *C* สร้างเซสชันคีย์ SK_{CASj} เมื่อ j = 1 ถึง *m* โดยใช้เทคนิคการสร้างคีย์ที่แสดงในส่วน 2.6 โดย *C* ส่งข้อความดังนี้

C → AS: $PN, Authen, h(PIN, Authen, SK_{CASj+1}), h(PIN, SK_{COj+1})$

เมื่อ *AS* ได้รับการร้องขอการพิสูจน์ตัวจริงจาก *C* และหลังจากพิสูจน์ตัวจริงสำเร็จ *AS* จะส่งข้อความดังต่อไปนี้ไปยัง *C*

AS → C: $Yes/No, h(Yes/No, SK_{CSAj+1}), h(PIN, SK_{ASOj+1})$

การส่ง SMS ครั้งต่อไปจะนำข้อความ $h(PIN, SK_{CASj+1})$ ทุกครั้งเพื่อพิสูจน์ตัวจริงกับ *AS*

3.4 การชำระเงินโดยตรงกับผู้ให้บริการ

โดยสมมติฐานว่าผู้ให้บริการโทรศัพท์เคลื่อนที่มีสินค้าหรือบริการ เช่น เสียงเรียกเข้า เพลง และดาวน์โหลดซอฟต์แวร์ ซึ่งลูกค้าจะถูกเรียกเก็บเงินตามสิ่งที่ซื้อจากบัญชีของตน

3.4.1 การร้องขอวงเงิน (Purchase Credit Request)

การเติมเงินเพื่อใช้สำหรับการชำระเงินมี 2 แบบคือ แบบลงทะเบียน (Postpaid) และแบบจ่ายเงินล่วงหน้า (Prepaid)

3.4.2 การเติมเงินแบบลงทะเบียน (Postpaid)

ถ้า C ทำธุรกรรมที่มีราคามากกว่าจำนวนเงินที่มีอยู่ในบัญชี C จะต้องทำการร้องขอวงเงินจากผู้ให้บริการโทรศัพท์เคลื่อนที่ และการขอวงเงินจะไม่เกินวงเงินของการให้แต่ละเดือน ดังนี้

C → O: $PN, T_1, \{CL_1, h(CL_1, T_1, SK_{COj+1})\}_{SKCOj+1}, h(PIN, SK_{CASj+1})$

O → C: $T_1, T_2, h(CL_R, T_1, T_2, SK_{Coj+1}), \{h(PIN, {}_{SKCASj+1})\}_{SKCOj+1}$

โดยที่ CL_T คือจำนวนเงินที่ร้องขอ CL_R คือจำนวนเงินคงเหลือในบัญชี T_1 คือเวลาที่ร้องขอวงเงิน และ T_2 คือเวลาที่ออกวงเงินให้ลูกค้า โดยที่ C จะถูกเรียกเก็บเงินจาก O ทันที ที่การทำธุรกรรมสมบูรณ์

3.4.3 แบบจ่ายเงินล่วงหน้า (Prepaid)

หลังจากซื้อบัตรและเติมเงินเรียบร้อยแล้ว C เปิดโปรแกรมในมือถือของตนเองและกรอกข้อมูลที่จำเป็น แล้วส่งไปให้ผู้บริการ O

C → O: $PN, T_1, SN, h(CL_1, SN, SK_{Coj+1}), h(PIN, SK_{CASj+1})$

O → C: $T_1, T_2, h(T_1, T_2, SK_{Coj+1}), \{h(PIN, {}_{SKCASj+1})\}_{SKCOj+1}$

โดยที่ SN คือ หมายเลขบัตรเติมเงินใช้อ้างอิงวงเงิน (CL_1) ที่ C ใช้อ้างอิงการซื้อขายสิ้นค้าหรือบริการ และ C จะถูกเรียกเก็บเงินจาก O ทุกสิ้นเดือนเมื่อการทำธุรกรรมสมบูรณ์

3.4.4 การชำระเงิน (Making Payment)

หลังจาก C เลือกสินค้าและบริการเรียบร้อยแล้ว C สามารถชำระเงินโดยส่งข้อความต่อไปนี้ให้ O

C → O: $ID_C, \{T_P, OI\}_{SKcoj+1}, h(ID_C, T_P, OI, SK_{COj+1}), h(PIN, SK_{CASj+1})$

โดยที่ TP คือ เวลาขณะร้องขอเพื่อชำระเงิน OI คือ $\{TID, Price, OD\}$ TID คือหมายเลขของการทำรายการ Price คือ ราคาของสินค้าหรือบริการ และ OD คือรายละเอียดของสินค้าหรือบริการ

เมื่อ O ได้รับคำร้องขอ O จะตรวจสอบจำนวนเงินของในบัญชีของ C กับราคาของสินค้าหรือบริการ ถ้าจำนวนเงินของในบัญชีของ C ก็จะตอบ Yes กลับไป แต่ถ้าไม่พอก็จะตอบ No กลับไป ถ้า C ต้องการทำรายการต่อ C ก็ต้องกลับไปร้องขอวงเงินตามหัวข้อ แบบลงทะเบียน หรือแบบจ่ายเงินล่วงหน้าต่อไป

O → C: $Yes/No, h(Yes/No, CL_{RM}, h(T_P, OI, SK_{Coj+1}), SK_{COj+1}), h(PIN, SK_{CASj+1})$

โดยที่ CL_{RM} คือ จำนวนเงินคงเหลือหลังจากทำธุรกรรมสมบูรณ์

3.5 การชำระเงินให้พ่อค้าโดยผ่านผู้ให้บริการ

ในส่วนนี้ ผู้วิจัยเสนอโพรโทคอลสำหรับให้ผู้บริการเป็นผู้ที่จะช่วยให้ลูกค้าดำเนินธุรกรรมการชำระเงินกับพ่อค้าได้ ซึ่งมีสมมติฐานดังต่อไปนี้ C และ M เปิดบัญชีกับ O แล้ว C ได้รับอนุมัติวงเงินจากผู้ให้บริการ โดยผู้ให้บริการสำหรับสินค้าหรือบริการที่ซื้อไป โปรแกรมในฝั่งลูกค้าทำหน้าที่ 2 ส่วน คือ การค้นหาสินค้าและการชำระเงิน โดยที่พ่อค้า หมายถึงผู้ที่ขายสินค้าหรือบริการบนมือถือ ซึ่งดำเนินการโดยผู้ให้บริการมือถือ รายละเอียดมีดังนี้

1) หลังจากตัดสินใจเลือกใช้บริการการชำระเงินแล้ว C สร้างเซสชันโดยใช้ WTLS และแลกเปลี่ยน $\{K_{CO}, DK_{CO}, m_{CO}\}$ กับ O จากนั้น C และ O จะสร้างเซสชันคีย์ K_{COj} โดยที่ $j = 1$ ถึง m โดยใช้เทคนิคการสร้างคีย์ในส่วนที่ 2.6

2) M แลกเปลี่ยน $\{K_{MO}, DK_{MO}, m_{MO}\}$ กับ O ทั้ง 2 ฝ่ายสร้างเซสชันคีย์ K_{MOj} โดยที่ $j = 1$ ถึง m โดยใช้เทคนิคการสร้างคีย์ในส่วนที่ 2.6

3) C เปิดโปรแกรมในมือถือของตน เพื่อเรียกดูสินค้าหรือบริการ เมื่อเลือกสินค้าหรือบริการแล้ว C ดำเนินการขอสั่งซื้อสินค้าหรือบริการ ดังต่อไปนี้

C → O: $PN, T, \{ID_M, OI, T, h(OI, K_{CMj+1})\}_{KCOj+1}, h(PIN, SK_{CASj+1})$

O → M: $\{OI, h(OI, K_{CMj+1}), h(OI, K_{COj+1}), T\}_{KMOj}$

M → O: $\{Yes/No, h(Yes/No, OI, K_{CMj+1})\}_{KMOj+1}$

O → C: $\{Yes/No, CL_{RM}, h(Yes/No, OI, K_{CMj+1}), h(OI, K_{MOj+1})\}_{KCOj+1}, \{h(PIN, {}_{SKCASj+1})\}_{SKCOj+1}$

เมื่อ T คือ Timestamp ซึ่งหลังจาก C คลิกปุ่มทำการชำระเงินจะมีเซสชันใหม่เกิดขึ้นระหว่าง C และ M ชุดของคีย์ $\{K_{CM}, DK_{CM}, m_{CM}\}$ จะถูกใช้งานร่วมกัน ทั้งสองฝ่ายสามารถสร้างเซสชันคีย์ SK_{CMj} ได้โดยใช้เทคนิคของการสร้างและการจายคีย์แบบออฟไลน์ จากข้อความข้างต้นซึ่งจะพบว่า O ไม่สามารถสร้างข้อความแรกได้ เพราะมี $h(OI, K_{CMj})$ รวมอยู่ ซึ่ง K_{CMj} ถูกใช้ร่วมกันระหว่าง C และ M เท่านั้น

4. การวิเคราะห์คุณสมบัติด้านความมั่นคงปลอดภัย

การรักษาความลับของข้อมูล เนื่องจากการเข้ารหัสลับด้วยเซสชันคีย์แต่ละครั้งผู้ที่มีเซสชันคีย์ที่ตรงกันเท่านั้นที่จะสามารถถอดรหัสลับข้อมูลได้ และการสร้างเซสชันคีย์มีลักษณะเป็นแบบออฟไลน์ โดยไม่มีการส่งเซสชันคีย์ผ่านเครือข่าย จะทำให้การดักจับคีย์ไปทำการวิเคราะห์เป็นไปได้ยาก

การทนทานการโจมตีแบบ Brute Force Attack เพื่อค้นหาคีย์ที่ถูกต้องนั้นในโพรโทคอลที่นำเสนอนี้ทำได้ยากเนื่องจากมีการเปลี่ยนแปลงค่าของเซสชันคีย์ในทุกๆ ครั้งที่มีการทำธุรกรรม นอกจากนี้การนำเอาเทคการสร้างและการกระจายเซสชันคีย์แบบออฟไลน์ ทำให้การค้นหาคีย์ตั้งต้นในการสร้างชุดของเซสชันคีย์ทั้งหมดทำได้ยากยิ่งขึ้น จึงทำให้การโจมตีแบบ Brute Force Attack ประสบความสำเร็จน้อยลง

ความต้านทานต่อการโจมตีแบบ Replay Attack โดยการปลอมตัวเป็น C แล้วส่งข้อมูลที่ดักจับได้อีกครั้ง จะประสบความสำเร็จได้น้อย เนื่องจากการเปลี่ยนเซสชันคีย์ทุกครั้งที่มีการติดต่อสื่อสาร

ความคงสภาพของข้อมูล การใช้ฟังก์ชันแฮช ทำให้สามารถตรวจสอบได้ว่าข้อมูลที่ส่งมานั้นไม่ถูกแก้ไขระหว่างทางหรือถูกเปลี่ยนแปลงข้อมูลจากบุคคลอื่น

การพิสูจน์ตัวจริงของผู้ส่งข้อความ (Party Authentication) คุณสมบัตินี้เป็นการพิสูจน์ตัวจริงของผู้ส่งข้อความ โพรโทคอลที่นำเสนอมีคุณสมบัตินี้ในทุกๆ ข้อความ จากโพรโทคอลที่นำเสนอพบว่า

แต่ละข้อความมีการนำเอา Message Authentication Code มาประยุกต์ใช้ทำให้ผู้รับมั่นใจได้ผู้ส่งเป็นผู้ส่งข้อความมา

5. สรุปผลการวิจัย

ในบทความนี้ ผู้วิจัยพบว่า SMS เป็นช่องทางสื่อสารระหว่างผู้ใช้กับผู้ใช้และระหว่างผู้ใช้กับผู้ให้บริการมือถือ มากที่สุด แต่วิธีที่ใช้รักษาความปลอดภัยในการทำธุรกรรมการชำระเงินผ่าน SMS และซื้อสินค้าหรือบริการจากผู้ให้บริการมือถือ และร้านค้า ยังขาดคุณสมบัติที่จำเป็นต้องมีอยู่มาก ผู้วิจัยจึงนำเสนอโพรโทคอลการชำระค่าสินค้าและบริการซึ่งมีคุณสมบัติที่ครบถ้วนในการเพิ่มความมั่นคงปลอดภัยเช่น คุณสมบัติการพิสูจน์ตัวจริงการส่ง SMS และนอกจากนี้ยังมีคุณสมบัติการป้องกันการเรียกเก็บค่าบริการเกินจริง (Correct Billing) ซึ่งโพรโทคอลนี้ยังสามารถใช้งานร่วมกันระบบ SMS ที่มีการใช้งานอยู่ในปัจจุบันได้

เอกสารอ้างอิง

[1] 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.

[2] H. Harb, H. Farahat, and M. Ezz, SecureSMSPay: Secure SMS Mobile Payment Model, Proceedings of the 2nd International Conference on Anti-counterfeiting, Security and Identification 2008, Guiyang, Aug 20-23, 2008, pp. 11-17.

[3] M. R. Hashemi and E. Soroush, A Secure m-Payment Protocol for Mobile Devices, Proceedings of the Canadian Conference on Electrical and Computer Engineering 2006 (CCECE'06), May 2006, Ottawa, Ont., pp. 294-297.

[4] J. Li-Chang Lo, J. Bishop, and J.H.P. Eloff, SMSSec: An end-to-end protocol for secure SMS, COMPUTER & SECURITY, Vol. 27, 2008, pp. 154-167.

[5] S. Kungpisdan and S. Metheekul, A Secure Offline Key Generation With Protection Against Key Compromise, Proceedings of the 13th World Multi-conference on Systemics, Cybernetics, and Informatics 2009, Orlando, USA.

[6] O. Dandash et al., Fraudulent Internet Banking Payments Prevention using Dynamic Key, Journal of Networks, Vol.3(1), Academy Publisher, pp. 25-34, 2008.

[7] S. Kungpisdan, P.D. Le, and B. Srinivasan, A Limited-Used Key Generation Scheme for Internet Transactions, LNCS, Vol. 3325, 2005.

[8] Li, Y. and Zhang, X., 2004. 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 E-Commerce and E-Government Applications,

[9] S. Kungpisdan, B. Srinivasan, and P.D. Le, Lightweight Mobile Credit-card Payment Protocol, LNCS, Vol. 2904, 2003, pp. 295-308.

[10] A. D. Rubin and R.N. Wright, Off-line Generation of Limited-Use Credit Card Numbers, LNCS, Vol. 2339, 2002, pp. 196

[11] M. Bellare, J. A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, E. V. Herreweghen, and M. Waidner, Design, "Implementation, and Deployment of the iKP Secure Electronic Payment System", IEEE Journal of Selected Areas in Communications, 2000.

[12] Mastercard and Visa, "SET Protocol Specifications", 1997. http://www.setco.org/set_specifications.htm

[13] Announcing the Advanced Encryption Standard (AES), FIPS 197 November 26, 2001. Available: http://csrc.nist.gov /publications/ fips/fips197/fips-197.pdf

[14] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," RFC 2104, February 1997.

[15] RSA Laboratories, "PKCS #1 v2.1: RSA Cryptography Standard," June 14, 2002.

[16] D. Eastlake, P. Jones, " US Secure Hash Algorithm 1 (SHA1)," RFC 3174, September 2001.

[17] P. Soni, M-Payment Between Banks Using SMS, Proceedings of the IEEE, Vol. 98(6), June 2010, ISSN: 0018-9219, pp. 903-905.