โพรโทคอลชำระค่าบริการแบบเคลื่อนที่ผ่านตัวแทนที่มีความมั่นคงปลอดภัย

An Agent-based Secure Mobile Bill Payment Protocol

เปมิกา ลิ้มพิทยา[1] เมฆินทร์ วรศาสตร์[2] และ ศุภกร กังพิศดาร[3]
คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร
140 ถนนเชื่อมสัมพันธ์ เขตหนองจอก กรุงเทพฯ 10530 โทรศัพท์ 02-988-3655 ต่อ 4111
[1]pemika_L@hotmail.co.th, [2]maykin@webmaster.in.th, [3]supakorn@mut.ac.th

Abstract

Nowadays, an agent-based mobile payment has become more popular. However, existing payment systems still lack of necessary mobile payment properties. Especially, they should be shorter and lightweight for making payment on the move. This paper introduces a new secure lightweight agent-based mobile payment protocol. This protocol not only satisfies necessary transaction security properties, but it is also simple and compatible to existing mobile payment infrastructure

Keywords: Mobile Payment, Agent-based Payment, Wireless Security, Cryptographic Protocols, Network Security

บทคัดย่อ

การชำระค่าสินค้าและบริการแบบเคลื่อนที่ผ่านตัวแทน (Agent-assisted Mobile Payment) ได้รับความนิยมสูงขึ้นในปัจจุบัน ระบบดังกล่าวควรมีขนาดข้อความที่สั้นและมีน้ำหนักเบา เพื่อให้ผู้ใช้สามารถทำธุรกรรมทางการเงินในขณะที่กำลังเคลื่อนที่อยู่ได้ บทความวิจัยฉบับนี้นำเสนอโพรโทคอลชำระค่าบริการแบบเคลื่อนที่ผ่านตัวแทนที่มีความมั่นคงปลอดภัย โดยออกแบบให้มีขนาดของข้อความสั้นลงและมีน้ำหนักเบา นอกจากธุรกรรมที่ทำจะมีคุณสมบัติด้านความมั่นคงปลอดภัยแล้ว ยังได้อำนวยความสะดวกสบายให้กับผู้บริโภคและเจ้าของสินค้า ในการทำธุรกรรมทางการเงินในปัจจุบันอีกด้วย

คำสำคัญ การชำระเงินผ่านเครือข่ายไร้สาย, ระบบตัวแทน, เครือข่ายไร้สาย, วิทยาการเข้าหัสลับ, ความมั่นคงของระบบเครือข่าย

1. บทนำ

การทำธุรกรรมทางการเงินในชีวิตประจำวันมีแนวโน้มเจริญเติบโตเพิ่มมากขึ้น รวมถึงการชำระค่าสินค้าหรือบริการผ่านธนาคาร โดยมีช่องทางเลือกและรูปแบบในการชำระค่าสินค้าและบริการให้แก่ผู้บริโภคและเจ้าของสินค้าหลากหลายรูปแบบ โดยทางเลือกหนึ่งที่ได้รับความนิยมอยู่ในขณะนี้ คือ การชำระค่าสินค้าและบริการที่เรียกกันว่า Bill Payment ในปัจจุบัน มีการชำระค่าสินค้าและบริการผ่านทางเคาน์เตอร์ธนาคาร หรือช่องทางอิเล็กทรอนิกส์ต่างๆ ของธนาคาร และรวมไปถึงการทำธุรกรรมการชำระเงินผ่านเครือข่ายไร้สายในขณะที่กำลังเคลื่อนที่ หรือที่เรียกกันว่า Mobile Payment

ที่ผ่านมามีการนำเสนอโพรโทคอลสำหรับการชำระเงินอิเล็กทรอนิกส์แบบผ่านระบบตัวแทน โดยระบบจะทำหน้าที่รวมรวบใบแจ้งการชำระเงินและทำการชำระเงินให้กับแต่ละบริษัทแทนลูกค้าในคราวเดียว ซึ่งโพรโทคอลที่ถูกออกแบบมานั้นยังมีข้อเสียในเรื่องขนาดของข้อความในการรับส่งข้อมูล เนื่องจากการใช้วิทยาการเข้ารหัสลับแบบอสมมาตร ดังนั้นจึงแก้ปัญหาโดยการนำวิทยาการเข้ารหัสลับแบบสมมาตรเข้ามาช่วย และใช้เทคนิคการกระจายเซสชันคีย์แบบจำกัดการใช้งานเพื่อเพิ่มความมั่นคงปลอดภัยให้กับระบบ

บทความวิจัยฉบับนี้เสนอโพรโทคอลชำระค่าบริการแบบเคลื่อนที่ผ่านตัวแทนที่มีความมั่นคงปลอดภัย ซึ่งออกแบบให้มีขนาดของข้อความสั้นลงและมีน้ำหนักเบา เพื่อเพิ่มประสิทธิสำหรับการประมวลผลและการเข้ารหัสลับได้อย่างรวดเร็ว โดยโพรโทคอลที่นำเสนอมีคุณสมบัติด้านความมั่นคง

ปลอดภัยที่จำเป็นดังนี้ การรักษาความลับ ความคงสภาพของข้อมูล การพิสูจน์ตัวจริงข้อความ และการส่งต่อความลับ

2. ทฤษฎีที่เกี่ยวข้อง

2.1 หลักการทำงานพื้นฐานระบบชำระเงิน

ระบบชำระเงิน คือ การจ่ายเงินค่าสินค้าหรือค่าบริการให้แก่เจ้าของสินค้าหรือบริการ เมื่อผู้ซื้อทำการสั่งซื้อสินค้าหรือบริการจากพ่อค้าเขาจะทำการแลกเปลี่ยนเงินกับสินค้าหรือบริการกับพ่อค้า ปัจจุบันวิธีการชำระเงินค่าสินค้าและบริการนั้น กระทำผ่านระบบอินเทอร์เน็ต โดยเป็นการทำธุรกรรมที่เกี่ยวข้องกับการเงิน เช่น การชำระค่าบริการโทรศัพท์ หรือค่าสาธารณูปโภค

โดยทั่วไปประกอบด้วยผู้เกี่ยวข้อง 5 ฝ่าย คือ

- ลูกค้า (Client) คือ ผู้สั่งซื้อสินค้าจากพ่อค้า
- พ่อค้า (Merchant) คือ เจ้าของสินค้า
- Payment Gateway มีหน้าที่จัดการธุรกรรมระหว่างสถาบันทางการเงินของลูกค้าและพ่อค้าผ่านเครือข่ายของธนาคาร และลูกค้ากับพ่อค้าจะทำธุรกรรมผ่านอินเทอร์เน็ต
- สถาบันการเงินของลูกค้า (Issuer) คือ สถาบันทางการเงินหรือธนาคารที่ลูกค้าเปิดใช้บริการทางการเงินหรือได้ทำการบัญชีเงินฝากกับสถาบันทางการเงินนั้น เช่น ธนาคาร หรือบริษัทให้บริการสินเชื่อต่างๆ ซึ่งสถาบันเหล่านี้จะเป็นผู้ทำหน้าที่จัดการเกี่ยวกับเงินในบัญชีของลูกค้า
- สถาบันการเงินของพ่อค้า (Acquirer) คือ สถาบันทางการเงินที่พ่อค้าเปิดใช้บริการทางการเงินหรือได้ทำการบัญชีเงินฝากเอาไว้กับสถาบันทางการเงินนั้น เช่น ธนาคาร หรือบริษัทให้บริการสินเชื่อต่างๆ ซึ่งสถาบันเหล่านี้จะเป็นผู้ทำหน้าที่จัดการเกี่ยวกับเงินในบัญชีของพ่อค้า

การดำเนินการของ Issuer และ Acquirer จะกระทำบนอินเทอร์เน็ต ในขณะที่การตัดเงินจากการชำระค่าสินค้าหรือค่าบริการจะกระทำโดยตรงภายในเครือข่ายของธนาคารด้วยกันเอง โดยการทำธุรกรรมการชำระเงินประกอบด้วย 3 กระบวนการ ได้แก่

- คำสั่งชำระเงิน
- การหักเงินจากบัญชี และ
- การเพิ่มเงินเข้าบัญชี

2.2 งานวิจัยที่เกี่ยวข้อง

2.2.1 งานวิจัยของ Kungpisdan *et al.*

Kungpisdan *et al.* [1] ได้เสนอระบบชำระเงินแบบรวมศูนย์ซึ่งเป็นระบบชำระเงินขึ้นอยู่กับบุคคลคนเดียวในการส่งข้อความที่เกี่ยวข้องกับการทำธุรกรรมการชำระเงินจากฝ่ายหนึ่งไปยังอีกฝ่ายหนึ่ง เช่น การให้บริการแบบอินเทอร์เน็ตแบ็งค์กิ้ง โดยธนาคารเป็นที่ให้บริการการชำระเงินกับลูกค้า โดยธนาคารทำหน้าที่เป็นศูนย์กลางที่ส่งคำขอการชำระเงินและการตอบสนองให้กับกลุ่มลูกค้า (ลูกค้าหรือร้านค้า) ที่มีบัญชีของธนาคาร ซึ่งลูกค้าทำการชำระเงินค่าบริการผ่านธนาคารและพ่อค้าส่งใบเสร็จรับเงินให้ลูกค้าผ่านธนาคาร

ในงานวิจัยนี้เสนอ BPAC ซึ่งเป็นโพรโทคอลการชำระเงินแบบความรับผิดชอบ โดยเป็นการสร้างความมั่นใจในการชำระเงินให้กับลูกค้าและพ่อค้า โดย BPAC จะเป็นเซิร์ฟเวอร์ที่อยู่ตรงกลาง เพื่อให้บริการชำระเงินสำหรับลูกค้าและพ่อค้าโดยมีความรับผิดชอบเป็นเป้าหมายหลัก ระบบนี้มีขั้นตอนการทำงาน 3 ขั้นตอน ได้แก่ การลงทะเบียน การวางใบแจ้งหนี้ให้กับลูกค้า และการขอชำระค่าสินค้าหรือบริการของลูกค้า (Bill Payment) โดย BPAC จะมีคีย์สาธารณะของลูกค้าและพ่อค้าซึ่งทุกคนที่เกี่ยวข้องในระบบจะใช้คีย์ ที่ทำการแลกเปลี่ยนกันสำหรับเข้ารหัสลับ เพื่อติดต่อสื่อสารในระบบการชำระเงินค่าสินค้า

2.2.2 งานวิจัยของพรชัย ทุราศและคณะ

พรชัย ทุราศ *et al.* [2] เสนอรูปแบบการชำระเงินผ่านระบบตัวแทน โดยระบบจะทำหน้าที่รวมรวบใบแจ้งหนี้และทำการชำระเงินให้กับแต่ละบริษัทในคราวเดียว เมื่อลูกค้าต้องการชำระเงินจะส่งคำร้องขอชำระเงินให้กับตัวแทนเพื่อรวบรวมข้อมูลการชำระเงินของสมาชิกที่ลงทะเบียนเอาไว้แล้ว เช่นเดียวกันเมื่อพ่อค้าต้องการแจ้งให้ ลูกค้าทราบจำนวนเงินรายการสินค้า ระยะเวลาที่ต้องทำการชำระเงิน จะต้องส่งใบแจ้งหนี้ให้กับตัวแทน ถ้ารับข้อมูลได้อย่างถูกต้องก็จะทำการรวบรวมใบแจ้งหนี้ดังกล่าวไว้ แล้วส่งต่อให้กับ BPAC เพื่อทำการตัดเงินกับธนาคารของลูกค้าให้กับพ่อค้าต่อไป งานวิจัยนี้ใช้เทคนิคการเข้ารหัสลับแบบคีย์คู่ ซึ่งจะกำหนดให้ทุกคนในระบบจะต้องมี คีย์ส่วนตัว ซึ่งเก็บเป็นความลับ และ คีย์สาธารณะซึ่งเปิดเผยให้กับสาธารณะทราบ ผู้ที่เกี่ยวข้องทุกคน

จะต้องแลกเปลี่ยนคีย์สาธารณะซึ่งกันและกันสำหรับการเข้ารหัสลับข้อความ เพื่อติดต่อสื่อสารกันในระบบการชำระเงินค่าสินค้าผ่านระบบตัวแทน

2.3 การสร้างและการกระจายเซสชันคีย์แบบจำกัดการใช้งาน

การสร้างและกระจายคีย์ แบ่งได้เป็น 2 ประเภท คือ เทคนิคแบบออนไลน์และแบบออฟไลน์ สำหรับการกระจายคีย์แบบออนไลน์จำเป็นต้องมีการส่งคีย์ผ่านทางเครือข่าย ถึงแม้ว่าจะมีการเข้ารหัสลับเอาไว้ แต่ก็ยังสามารถถูกดักจับได้ สำหรับการกระจายคีย์แบบออฟไลน์นั้น คีย์ที่สร้างขึ้นใหม่ไม่จำเป็นต้องส่งผ่านไปในเครือข่าย ผู้โจมตีจึงไม่สามารถดักจับได้ [4, 5, 6] โดยวิธีของ Kungpisdan *et al.* [3] จะกำหนดให้อลิซ และบ๊อบใช้ $\{K_{AB}, DK, m\}$ ร่วมกัน เมื่อ K_{AB} เป็นคีย์ระยะยาว (Long-term key) DK เป็นคีย์กระจาย (Distributed key) และ m เป็นเลขสุ่มที่ใช้ระบุจำนวนคีย์ที่จะสร้าง $conc(M_1, M_2, M_3)$ คือการต่อกันของข้อความ M_1, M_2 และ M_3 ตามลำดับ กระบวนการสร้างเซสชันคีย์เป็นดังนี้

$$K_i = h(K_{i-1}, DK)$$
$$IK^1_j = h(conc(K_{Mid}), IK^1_{j-1})$$
$$IK^n_j = h(conc(K_{Mid}), IK^n_{j-1})$$
$$SK_j, j = 1, \ldots, m$$

หลังจากมีการแลกเปลี่ยน $\{K_{AB}, DK, m\}$ กัน อลิซและบ๊อบจะสร้างคีย์ที่ใช้ในการตั้งค่า (preference key) K_i เมื่อ $i = 1,\ldots,m$ ดังนี้ $K_i = h(K_{i-1}, DK)$ เมื่อ $K_0 = K_{AB}$ ซึ่ง K_i จะถูกใช้เป็นข้อมูลสำหรับการสร้างเซสชันคีย์ต่อไป หลังจากสร้างเซ็ตของ K_i แล้ว สามารถลบ K_{AB} และ DK ออกจากระบบได้ ทั้งอลิซและบ๊อบสร้างคีย์กลาง (Intermediate key) เพื่อเพิ่มความยากสำหรับการทำ Cryptanalysis คือ การเพิ่มความยากในการย้อนกลับไปหาคีย์ที่ใช้ในการตั้งค่าหากเซสชันคีย์ถูกดักจับได้ โดยคีย์กลางจะถูกสร้างตามจำนวนรอบที่สูงสุด ซึ่งให้ความมั่นคงปลอดภัยที่สูงกว่าการสร้างคีย์กลางทำได้ดังนี้ $IK^x_j = h(conc(IK^{x-1}_{Mid}), IK^x_{j-1})$ เมื่อ x คือจำนวนรอบ j คือ จำนวนของคีย์กลางที่สร้าง โดยที่ $j = 1$ ถึง m IK^{x-1}_{Mid} คือเซ็ตของ $\{IK^{x-1}_{Mid1}, IK^{x-1}_{Mid2}, IK^{x-1}_{Mid3}\}$ โดย $IK^x_{Mid1} = mid(IK^x_1, IK^x_{rm})$ ซึ่ง rm คือ จำนวนคีย์กลางที่เหลือในเซ็ต IK^x_j

$$IK^x_{Mid2} = mid(IK^x_{Mid1}, IK^x_{rm})$$
$$IK^x_{Mid3} = mid(IK^x_1, IK^x_{Mid2})$$
$$IK^1_{Mid1} = K_{Mid1}, IK^1_{Mid2} = K_{Mid2}, \text{ และ } IK^1_{Mid3} = K_{Mid3}$$

ในการสร้าง K_{Mid1}, K_{Mid2} และ K_{Mid3} จะเหมือนกันกับการสร้าง IK^x_{Mid1}, IK^x_{Mid2} และ IK^x_{Mid3} ตามลำดับ

$IK^x_{j-1} = \phi$ คือผลลัพธ์สุดท้ายของการสร้างคีย์กลาง ซึ่งใช้เป็นเซสชันคีย์ SK_j โดยที่ $j = 1$ ถึง m ซึ่งแสดงได้ดังนี้

$IK^n_1 = SK_1$, $IK^n_2 = SK_2, \ldots, IK^n_m = SK_m$ ทั้งอลิซและบ๊อบสามารถใช้ SK_j เพื่อใช้เป็นคีย์ในการเข้ารหัสลับ หรือใช้สร้างรหัสพิสูจน์ตัวจริงข้อความ (หรือ MAC) ซึ่งเซสชันคีย์นี้ถูกสร้างขึ้นแบบออฟไลน์ และใช้คีย์เพื่อติดต่อสื่อสารระหว่างกัน โดยไม่ต้องมีการส่งคีย์ใดๆ ผ่านเครือข่าย เมื่อเซสชันคีย์ไม่ต้องมีการส่งผ่านเครือข่ายจะไม่มีโอกาสถูกดักจับได้

3. งานวิจัยที่นำเสนอ

โพรโทคอลชำระค่าบริการแบบเคลื่อนที่ผ่านตัวแทนที่มีความมั่นคงปลอดภัย ประกอบด้วย 3 กระบวนการด้วยกัน คือ การลงทะเบียน การวางใบแจ้งหนี้ให้กับลูกค้า และการขอชำระค่าสินค้าของลูกค้า

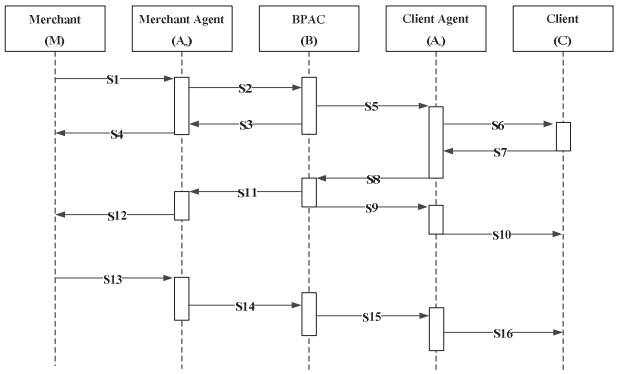
3.1 นิยามและสมมติฐาน

โพรโทคอลที่นำเสนอ มีสมมติฐานดังต่อไปนี้

- ในระบบประกอบด้วยผู้ที่เกี่ยวข้องกัน 5 ฝ่าย ได้แก่ ลูกค้า (Client หรือ C), พ่อค้า (Merchant หรือ M), ตัวแทนลูกค้า (Client Agent หรือ A_C), ตัวแทนพ่อค้า (Merchant Agent หรือ A_M) และ BPAC (BPAC Server หรือ B)
- ID_B, ID_M, ID_C, ID_{Ac}, ID_{Am} คือสิ่งที่ระบุตัวตนของผู้ใช้
- TID คือ Transaction ID หรือใบกำกับสินค้า (Invoice ID)
- OD คือ Order descriptions หรือใบสั่งซื้อสินค้า
- Date คือ วันที่และเวลาของการทำธุรกรรม
- Price คือ ราคาสินค้า
- SK_{XYj} โดย j=1 ถึง m คือ คีย์ที่ใช้ร่วมกันระหว่าง X กับ Y
- $h(m, K)$ เป็นรหัสพิสูจน์ตัวจริงข้อความของข้อความ m ที่ใช้คีย์ K

3.2 การลงทะเบียนและแลกเปลี่ยนเซสชันคีย์

C ทำการลงทะเบียนกับ A_C, M ทำการลงทะเบียนกับ A_M และ A_C กับ A_M ทำการลงทะเบียนกับ BPAC การลงทะเบียนทั้งหมดทำผ่านช่องทางที่มั่นคงปลอดภัย วัตถุประสงค์ของการลงทะเบียนเพื่อการแลกเปลี่ยนตัวแปรในการสร้างและกระจายเซสชันคีย์ $\{DK_{XY}, K_{XY}, m_{XY}\}$ ซึ่งกระทำผ่านช่องทางที่ปลอดภัย สร้างเซสชันคีย์ SK_{XYj} โดยที่ j = 1 ถึง m



รูปที่ 1 การส่งข้อมูลภายในระบบ

3.3 การวางใบแจ้งหนี้ให้กับลูกค้า (Bill Presentment)

S1: M → A_m : $\{ID_M, ID_C, TID, Price, Date, h(OD, Price, SK_{BMj})\}SK_{BMj}, \{ID_B, TID, Price, Date\}SK_{MAmj}$

ขั้นตอนที่ 1 เมื่อ M ต้องการส่งใบแจ้งหนี้ให้กับ C ซึ่งกระทำได้โดยทำผ่าน A_m เพื่อให้ A_m รวบรวมใบแจ้งหนี้ก่อนที่จะส่งให้กับ BPAC โดยข้อมูลภายในข้อความ ประกอบด้วย 2 ส่วน คือ ส่วนที่ 1 เป็นข้อมูลที่ต้องการส่งให้กับ BPAC โดยการสร้างค่า MAC ที่ใช้เซสชันคีย์ระหว่าง M และ BPAC (SK_{BMj}) เพื่อตรวจสอบว่าข้อความที่ส่งมานั้นมาจาก M จริง และนำ ID_M, ID_C, *TID, Price, Date* และค่า MAC มาเข้ารหัสลับด้วยเซสชันคีย์ระหว่าง M และ BPAC เพื่อทำให้ A_m ไม่สามารถอ่านข้อมูลได้ ส่วนที่ 2 เป็นข้อมูล ID_B, *TID, Price, Date* ที่ส่งให้กับ A_m โดยจะถูกเข้ารหัสลับด้วยเซสชันคีย์ที่สร้างขึ้นระหว่าง M และ A_m(SK_{MAmj}) เพื่อให้ A_m เท่านั้นที่สามารถถอดรหัสลับออกมาได้

S2: A_m → B : $\{ID_M, ID_C, TID, Price, Date, h(OD, Price, SK_{BMj})\}SK_{BMj}, \{h(\{ID_M, ID_C, TID, Price, Date, h(OD, Price, SK_{BMj},)\}SK_{BMj}, SK_{BAmj})\}SK_{BAmj}$

ขั้นตอนที่ 2 จากนั้น A_m ส่งต่อใบแจ้งหนี้ที่มีให้กับ BPAC โดยการสร้างค่า MAC ที่ใช้เซสชันคีย์ระหว่าง A_m และ BPAC (SK_{BAmj}) เพื่อใช้ตรวจสอบว่าข้อความที่ถูกส่งมานั้น มาจาก A_m จริง และเมื่อ BPAC ถอดรหัสลับ โดยใช้เซสชันคีย์ที่สร้างขึ้นระหว่าง M และ BPAC มาถอดจะทำให้ทราบถึงข้อมูลการร้องขอให้ลูกค้าทำการชำระเงินจาก ID_C เพื่อให้ BPAC ส่งใบแจ้งหนี้ให้กับลูกค้าต่อไปเมื่อถึงกำหนดการส่งใบแจ้งหนี้

S3: B → A_m : $\{\{Confirm_{bill}\}SK_{BMj+1}, ID_M\}SK_{BAmj+1}$

ขั้นตอนที่ 3 BPAC ต้องการส่งข้อความยืนยันการได้รับข้อความให้กับ M โดย BPAC กระทำผ่านตัวแทน A_m และ A_m ส่งต่อข้อความนี้ต่อไปยัง M อีกครั้ง

S4: A_m → M : $\{\{Confirm_{bill}\}SK_{BMj+1}, (\{Confirm_{bill}\}SK_{BMj+1}, SK_{MAmj+1})\}SK_{MAmj+1}$

ขั้นตอนที่ 4 A_m ต้องการส่งต่อข้อความยืนยันไปยัง M โดย A_m สร้างข้อความเพิ่มขึ้นอีก 1 ชุด ซึ่งข้อความที่สร้างใหม่นั้นเป็นค่า MAC เพื่อใช้ตรวจสอบว่าข้อความที่ถูกส่งมานั้นมาจาก M จริง ถ้าหากข้อความที่ได้รับถูกต้อง M ก็จะทราบได้ว่า BPAC เป็นผู้อนุมัติให้โอนเงินตามจำนวนที่ต้องการโอนเข้าบัญชีของพ่อค้า

S5: B → A_c : $\{ID_M, ID_C, TID, Price, Date, h(OD, Price, SK_{BCj})\}SK_{BCj}, \{h(\{ID_M, ID_C, TID, Price, Date, h(OD, Price, SK_{BCj})\}SK_{BCj}, SK_{BAcj}), TID, Date\}SK_{BAcj}$

ขั้นตอนที่ 5 เมื่อถึงกำหนดส่งใบแจ้งหนี้ BPAC จะนำ $\{ID_M, ID_C, TID, Price, Date, h(OD, Price, SK_{BMj})\}SK_{BMj}$ ที่ได้รับมาจาก M ซึ่งมีการใช้เซสชันคีย์ระหว่าง BPAC กับ M (SK_{BMj}) มาสร้างค่า MAC ใหม่ และเข้ารหัสลับด้วยเซสชันคีย์ระหว่าง BPAC กับ C (SK_{BCj}) เป็น $\{ID_M, ID_C, TID, Price, Date, h(OD, Price, SK_{BCj})\}SK_{BCj}$ เพื่อส่งให้ C ผ่านทาง A_c และข้อความอีกส่วนที่จะส่งให้กับ A_c นั้น BPAC จะสร้างค่า MAC ที่ใช้เซสชันคีย์ระหว่าง A_c กับ BPAC (SK_{BAcj}) และระบุ TID และ Date เข้าไปด้วย เมื่อ A_c ได้รับข้อความนี้จะสามารถอ่านข้อมูล ID_C,*TID, Date* ได้ซึ่งจะบอก A_c ให้ทราบว่าต้องส่งข้อมูลไปให้กับ C คนใด

S6: A_c → C : $\{ID_M, ID_C, TID, Price, Date, h(OD, Price, SK_{BCj})\}SK_{BCj}, \{h(\{ID_M, ID_C, TID, Price, Date, h(OD, Price, SK_{BCj})\}SK_{BCj}, SK_{CAcj})\}SK_{CAcj}$

ขั้นตอนที่ 6 A_c ส่งข้อความต่อไปยัง C โดยสร้างข้อความเพิ่มขึ้นอีก 1 ชุด ซึ่งข้อความที่สร้างใหม่นั้นจะเป็นค่า MAC เพื่อใช้ตรวจสอบว่าข้อความที่ถูกส่งมานั้น มาจาก A_c จริง และเมื่อ C ถอดรหัสลับด้วยเซสชันคีย์ที่สร้างขึ้นระหว่าง C และ

BPAC มาถอดข้อความ ถ้าหากสามารถถอดข้อความได้นั้นก็หมายความว่า C ได้รับใบแจ้งหนี้จาก M ที่แจ้งให้ไปชำระเงินค่าสินค้า ซึ่ง C จะทราบได้จาก ID_M

3.4 การขอชำระค่าสินค้าของลูกค้า (Bill Payment)

S7: C → A_c : $\{ID_B, ID_M, ID_C, TID, Price, Date, h(OD, Price, SK_{BCj})\}SK_{CAcj}$

ขั้นตอนที่ 7 เมื่อ C ต้องการชำระเงินให้กับ M โดยทำผ่าน A_c และ BPAC ซึ่งข้อความทั้งหมด $\{ID_B, ID_M, ID_C, TID, Price, Date, h(OD, Price, SK_{BCj})\}SK_{CAcj}$ จะถูกนำมาใช้พิจารณาในการหักเงินผ่านบัญชีของลูกค้าที่ร้องขอไปยัง BPAC หลังจาก A_c ได้รับข้อความความต้องการชำระเงินจาก C แล้วนั้น A_c จะต้องทำการตรวจสอบ Price และ Date เพื่อคำนวณจำนวนเงินที่ใช้สำหรับชำระเงินและระยะเวลาของการชำระเงิน ส่วน TID นั้น A_c จะเก็บเป็นรายการของการทำธุรกรรมการเงินที่ทำผ่านตัวแทน เพื่อเรียกเก็บค่าบริการกับลูกค้า

S8: A_c → B : $\{ID_B, ID_M, ID_C, TID, Price, Date, h(OD, Price, SK_{BCj}), h(ID_B, ID_M, ID_C, TID, Price, Date, h(OD, Price, SK_{BCj}), SK_{BAcj})\} SK_{BAcj}$

ขั้นตอนที่ 8 A_c ส่งความต้องการชำระเงินให้กับ BPAC โดย A_c สร้างค่า MAC ที่ใช้เซสชันคีย์ระหว่าง A_c และ BPAC (SK_{BAcj}) และเมื่อ BPAC ถอดรหัสลับ ก็จะพบข้อมูลที่ทำให้ BPAC ทราบความต้องการของลูกค้าจาก ID_M, ID_C, *TID, Price* โดยจะตรวจสอบจำนวนเงินในบัญชีของลูกค้าว่ามีเพียงพอที่จะชำระเงินหรือไม่ ถ้าเพียงพอ BPAC จะหักเงินจากบัญชีของลูกค้าตามจำนวนเงินที่ขอหักพร้อมกับโอนจำนวนเงินดังกล่าวให้กับพ่อค้าจากข้อมูล ID_M

S9: B → A_c : $\{\{Confirm_{payment}\}SK_{BC\,j+1}, ID_C\}SK_{BAcj+1}$

ขั้นตอนที่ 9 BPAC สร้างข้อความยืนยันการชำระเงินเพื่อจะส่งให้กับ C โดย BPAC จะแจ้งผ่าน A_c และ A_c ส่งต่อข้อความนี้ต่อไปยัง C อีกครั้ง

S10: A_c → C : $\{\{Confirm_{payment}\}SK_{BC\,j+1}, h(\{Confirm_{payment}\}SK_{BC\,j+1}, SK_{CAc\,j+1})\}SK_{CAc\,j+1}$

ขั้นตอนที่ 10 A_c ส่งข้อความยืนยันการชำระเงินให้กับ C โดย A_c สร้างข้อความเพิ่มขึ้นอีก 1 ชุด ซึ่งข้อความที่สร้างใหม่นั้นเป็นค่า MAC เพื่อใช้ตรวจสอบว่าข้อความที่ถูกส่งมานั้นมาจาก C จริง ถ้าหากข้อความที่ได้รับถูกต้อง C ก็จะทราบได้ว่า BPAC ได้อนุมัติการหักเงินจากบัญชีของลูกค้าตามที่ขอหัก

S11: B → A_m : $\{\{ID_C, h(ID_M, ID_C, TID, Price, Date, SK_{BMj+1})\}SK_{BM\,j+1}, ID_M\}SK_{BAm\,j+1}$

ขั้นตอนที่ 11 BPAC ส่งข้อความขอชำระเงินให้กับ A_m โดยที่ TID สามารถนำมาใช้ระบุรายการสินค้าหรือบริการของลูกค้าที่ชำระเงิน ซึ่งข้อความนี้ $h(ID_M, ID_C, TID, Price, Date, SK_{BMj+1})$ จะใช้ในการพิจารณาการตอบกลับของ BPAC เกี่ยวกับการอนุมัติการโอนเงินตามจำนวนที่ M ต้องการโอนเข้าบัญชี โดยที่ข้อความทั้งหมดจะถูกส่งผ่าน A_m และ A_m ส่งต่อข้อความนี้ต่อไปยัง M อีกครั้ง

S12: A_m → M : $\{\{ID_C, h(ID_M, ID_C, TID, Price, Date, SK_{BM\,j+1})\}SK_{BM\,j+1}\}SK_{MAm\,j+1}$

ขั้นตอนที่ 12 A_m ส่งข้อความอนุมัติการโอนเงินให้กับ M โดย A_m สร้างข้อความเพิ่มขึ้นอีก 1 ชุด ซึ่งข้อความที่สร้างใหม่นั้นเป็นค่า MAC เพื่อใช้ตรวจสอบว่าข้อความที่ถูกส่งมานั้นมาจาก M จริง ถ้าหากข้อความที่ได้รับถูกต้อง M ก็จะทราบได้ว่า BPAC ได้อนุมัติการโอนเงินเข้าสู่บัญชีของพ่อค้า

S13: M → A_m : $\{\{Confirm_{payment}, ID_C\}SK_{BM\,j+1}, h(\{Confirm_{payment}, ID_C\}SK_{BM\,j+1}, SK_{MAm\,j+1})\}SK_{MAm\,j+1}$

ขั้นตอนที่ 13 M ส่งใบเสร็จรับเงินให้กับ A_m โดย M สร้างใบเสร็จรับเงินการชำระเงินค่าสินค้าของ C โดยส่งผ่าน A_m, BPAC และ A_c ซึ่งทั้ง 3 จะส่งต่อข้อความไปจนถึง C

S14: A_m → B : $\{\{Confirm_{payment}, ID_C\}SK_{BM\,j+1}, h(\{Confirm_{payment}, ID_C\}SK_{BM\,j+1}, SK_{BAm\,j+1})\}SK_{BAm\,j+1}$

ขั้นตอนที่ 14 A_m ส่งใบเสร็จรับเงินให้กับ BPAC โดย A_m สร้างข้อความเพิ่มขึ้น 1 ชุด ซึ่งข้อความนั้นเป็นค่า MAC เพื่อใช้ตรวจสอบว่าข้อความที่ถูกส่งมานั้นมาจาก A_m จริง

S15: B → A_c : $\{\{Confirm_{payment}\}SK_{BC\,j+1}, ID_C, \{h(\{Confirm_{payment}\}SK_{BC\,j+1}, ID_C\}SK_{BAc\,j+1})\}SK_{BAc\,j+1}$

ขั้นตอนที่ 15 BPAC ส่งใบเสร็จรับเงินให้กับ A_c โดย BPAC จะสร้างข้อความเพิ่มขึ้นอีก 1 ชุด ซึ่งข้อความนั้นเป็นค่า MAC ที่ใช้เซสชันคีย์ระหว่าง A_c และ BPAC (SK_{BAcj+1})

S16: $A_c \rightarrow C$: $\{\{Confirm_{payment}\}SK_{BC\,j+1}, \{h(\{Confirm_{payment}\}SK_{BC\,j+1}\} SK_{CAc\,j+1})\}SK_{CAc\,j+1}$

ขั้นตอนที่ 16 A_c ส่งใบเสร็จรับเงินให้ C เมื่อ A_c ได้รับแล้วก็จะส่งต่อให้ C โดยสร้างข้อความเพิ่มขึ้นอีก 1 ชุด ซึ่งข้อความนั้นเป็นค่า MAC เพื่อใช้ตรวจสอบว่าข้อความที่ส่งมานั้นมาจาก A_c จริง หากถูกต้อง C ก็จะทราบจากข้อความว่า M ได้รับการชำระเงินจาก C เรียบร้อยแล้ว

4. การวิเคราะห์ทางด้านความมั่นคงปลอดภัย

4.1 ความมั่นคงปลอดภัยของระบบ

โพรโทคอลที่เสนอควรมีคุณสมบัติที่จำเป็น ดังนี้

- การรักษาความลับ (Confidentiality)

มีการเข้ารหัสลับแบบสมมาตรเพื่อรักษาความลับ ซึ่งใช้คีย์ที่ตกลงกันระหว่าง 2 ฝ่ายที่ตกลงทำการสื่อสารกันเท่านั้น

- ความคงสภาพของข้อมูล (Integrity)

การตรวจสอบความคงสภาพของข้อมูลนั้น กระทำโดยการใช้ค่า MAC ของข้อความ ซึ่งจะต้องมีคีย์ที่แชร์กันระหว่างผู้ส่งกับผู้รับเท่านั้น จึงจะสามารถสร้างค่า MAC ได้

- การพิสูจน์ตัวจริงข้อความ (Message Authentication)

ใช้การเข้ารหัสลับสมมาตรร่วมกับรหัสพิสูจน์ตัวจริงข้อความ ในแต่ละข้อความที่ทำการส่ง จึงมั่นใจได้ว่าข้อความถูกส่งมาจากบุคคลที่ใช้คีย์ร่วมกันเท่านั้น

- การส่งต่อความลับ (Forward Secrecy)

ระบบยังสามารถรักษาความมั่นคงปลอดภัยอยู่ได้ แม้ว่าเซสชันคีย์จะถูกดักจับ และสามารถถอดรหัสลับได้สำเร็จจนกระทั่งได้ SK_{CM1} ซึ่งใช้ร่วมกันระหว่างลูกค้ากับพ่อค้า ซึ่งผู้โจมตีจะไม่สามารถใช้ SK_{CM1} สำหรับการถอดรหัสลับข้อความใดๆ ได้ เพราะคีย์สามารถใช้ได้เพียงครั้งเดียวเท่านั้น โดยเป็นไปตามเทคนิคที่นำเสนอใน Kungpisdan *et al.* [3] คือ ผู้โจมตีไม่สามารถสร้าง SK_{CM2} จาก SK_{CM1} ได้

4.2 ความมั่นคงปลอดภัยของเซสชันคีย์

เพื่อความมั่นคงปลอดภัย ไม่ควรนำคีย์กลับมาใช้ใหม่ ตามโพรโทคอลที่นำเสนอ ได้มีการนำเอาเทคนิคการสร้างและกระจายคีย์แบบจำกัดมาใช้ เพื่อให้การรับส่งข้อความในแต่ละครั้งใช้เซสชันคีย์ใหม่โดยไม่มีการส่งเซสชันคีย์เดิม

5. สรุปผลการวิจัย

ผู้วิจัยพบว่าการชำระเงินผ่านตัวแทนบนเครือข่ายไร้สายนั้นเป็นช่องทางในการทำธุรกรรมทางการเงินที่อำนวยความสะดวกให้กับผู้ใช้มากขึ้น และยังมีคุณสมบัติด้านความมั่นคงปลอดภัยที่มีความจำเป็นต่างๆ เพื่อช่วยรักษาข้อมูลของผู้ใช้ให้อยู่ในสภาพมั่นคงปลอดภัยต่อการถูกโจมตีจากผู้ไม่หวังดี

โดยโพรโทคอลที่เสนอนี้ใช้หลักการเข้ารหัสลับแบบสมมาตร ซึ่งมีความรวดเร็วในการเข้ารหัสลับและถอดรหัสลับเมื่อเปรียบเทียบกับการเข้ารหัสลับอสมมาตร นอกจากนี้ยังได้เพิ่มความมั่นคงปลอดภัยให้กับวิธีการที่นำเสนอโดยวิธีการสร้างและกระจายคีย์แบบออฟไลน์อีกด้วย

เอกสารอ้างอิง

[1] S. Kungpisdan, Accountability in Centralized Payment Environments, Proceedings of the 9th International Symposium on Communications and Information Technology 2009, Sept 28-30, 2009, Incheon, pp. 1022-1027.

[2] S. Kungpisdan and T. Pornchai, A Bill Payment System Via An Intermediary Supporting Bulk Transactions, Proceedings of the 7th International Joint conference on Computer Science and Software Engineering (JCSSE2010), on May 12-14, 2010, Bangkok

[3] 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.

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

[5] S. Kungpisdan, P.D. Le, and B. Srinivasan, "A Limited-Used Key Generation Scheme for Internet Transactions", Lecture Notes in Computer Science, Vol. 3325, 2005.

[6] S. Kungpisdan, B. Srinivasan, and P.D. Le, Lightweight Mobile Credit-card Payment Protocol, Lecture Notes in Computer Science, Vol. 2904, 2003, pp. 295-30