โปรโตคอลสำหรับระบบเก็บเงินค่าผ่านทางด่วนอัตโนมัติในเครือข่ายสื่อสารยานยนต์เฉพาะกิจ

A Protocol for Automatic Electronic Toll Collection System Based On VANET

โสภณ พัฒนะวิริยะศิริกุล[1] , สุรการ ดวงผาสุข[2] และ ศุภกร กังพิศดาร[3]

คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร

140 หมู่ 1 ถนนเชื่อมสัมพันธ์ เขตหนองจอก กรุงเทพ 10530

sophon.p@gmail.com[1], surakarn@mut.ac.th[2], supakorn@mut.ac.th[3]

บทคัดย่อ – เครือข่ายสื่อสารยานยนต์เฉพาะกิจ (Vehicular Ad-hoc Network หรือ VANET) คือ รูปแบบหนึ่งของเทคโนโลยีการสื่อสารไร้สายเฉพาะกิจเพื่อประยุกต์ให้เกิดการสื่อสารระหว่างรถยนต์และระหว่างรถยนต์กับสถานีฐานข้างทาง หนึ่งในแอพพลิเคชัน (Application) สำหรับเครือข่ายชนิดนี้คือ ระบบการเก็บค่าผ่านทางด่วนอัตโนมัติ (Automatic Electronic Toll Collection หรือ AETC) โดยมีปัจจัยที่สำคัญในด้านความมั่นคงปลอดภัยในการทำธุรกรรม งานวิจัยฉบับนี้นำเสนอการออกแบบระบบชำระเงินสำหรับ AETC การออกแบบมีพื้นฐานมากจากการชำระเงินแบบ Micropayment ซึ่งเหมาะสมกับการชำระสินค้ามูลค่าน้อยๆ และมีการนำเอาวิทยาการเข้ารหัสลับแบบสมมาตร (Symmetric Cryptography) มาใช้เพื่อรักษาความมั่นคงปลอดภัย รวมทั้งลดปริมาณการคำนวณ และลดขนาดของข้อมูลที่ต้องส่งผ่านเครือข่าย ได้อีกด้วย งานวิจัยฉบับนี้ยังได้แสดงให้เห็นว่าระบบที่นำเสนอมีความมั่นคงปลอดภัยรวมทั้งประสิทธิภาพที่สูงกว่าระบบการชำระเงินบนเครือข่าย VANET ที่ถูกนำเสนอมาก่อนหน้านี้

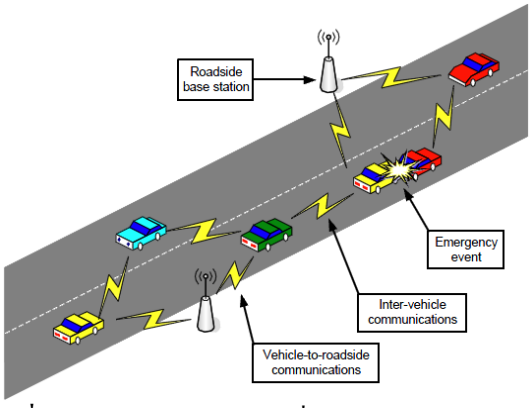
ABSTRACT – An automated electronic toll collection (AETC) system allows commuters to pay for a toll wirelessly while they are on the move. The type wireless network that facilitates the transactions between engaging parties in the AETC system is vehicular ad-hoc network (or VANET for short). It is clear that the transaction between a vehicle and the AETC must be performed in a secure and accountable manner. A number of payment protocols were developed to secure the AETC system. However, they still lack of necessary security and transaction performance. In this paper, we introduce a micropayment protocol for the AETC system that satisfies necessary transaction security properties. Moreover, our analysis shows that the proposed protocol has lower computation compared to the existing protocols. With the proposed protocol, engaging parties can complete each transaction faster than the existing approaches. This leads to better transaction performance.

KEY WORDS – Automated Electronic Toll Collection, micropayment, Vehicular Ad hoc Network, VANET, V2R

1. บทนำ

ในปัจจุบันได้มีการพัฒนาเครือข่ายไร้สายเพื่อประยุกต์ใช้งานบนรถยนต์ซึ่งติดต่อสื่อสารด้วยเทคโนโลยี IEEE 802.11 [1] กับ Wi-Fi hotspot รถยนต์จะมีการสื่อสารกันเรียกว่า Vehicle-to-Vehicle Communications (V2V) หรือ Inter-vehicle Communications รวมทั้งยังมีการ

ติดต่อสื่อสารระหว่าง รถยนต์กับสถานีฐาน (Road-side Unit) เรียกว่า Vehicle-to-Roadside Communications (V2R) โดยสถานีฐานจะติดตั้งอยู่ริมถนนในจุดต่าง ๆ ของถนน เครือข่ายที่มีการติดต่อระหว่างรถยนต์และสถานีฐานเรียกว่า Vehicular Ad-hoc Network (VANET) [2] ดังรูปที่ 1



รูปที่ 1 โครงสร้างของเครือข่ายสื่อสารยนต์ยานเฉพาะกิจ [3]

เป้าหมายหลักของเครือข่าย VANET จะให้ความปลอดภัยและความสะดวกสบายสำหรับผู้โดยสารโดยการใส่อุปกรณ์ที่ติดตั้งในรถเพื่อการติดต่อสื่อสารที่รู้จักกันในชื่อ Onboard Units (OBUs) และมีส่วนที่ติดต่อกับผู้ใช้เรียกว่า Application Units (AU) และจะใช้เครือข่ายในการสื่อสารแบบ Ad-hoc เราสามารถใช้เครือข่าย VANET ในการพัฒนาระบบเก็บเงินค่าผ่านทางอัตโนมัติโดยที่ผู้ขับขี่ไม่ต้องหยุดรอชำระเงินที่สถานีเก็บค่าผ่านทาง โดยสามารถเดินทางต่อได้เลย ระบบ Automated Electronic Toll Collection (AETC) ใช้ประโยชน์จากคุณสมบัติของเทคโนโลยีการสื่อสารแบบไร้สาย เพื่อช่วยในการโอนเงินแบบอิเล็กทรอนิกส์ระหว่างรถยนต์ (ลูกค้า) ที่วิ่งผ่านสถานีเก็บค่าผ่านทาง (พ่อค้า) และหน่วยงานจัดเก็บค่าผ่านทาง (Toll Agency ทำหน้าที่เหมือนธนาคาร) ซึ่ง AETC จะทำการตรวจสอบรถยนต์ที่วิ่งผ่านเข้ามาในระบบผ่าน สถานีเก็บค่าผ่านทาง (Road Side Unit หรือ RSU) บริเวณทางเข้า-ออกเลนถนนและทำการสื่อสารกับรถยนต์คันนั้นผ่าน OBUและป้ายทะเบียนรถยนต์อิเล็กทรอนิกส์ (Electronics License Plate) เมื่อรถยนต์ที่ได้ลงทะเบียนไว้วิ่งผ่าน ระบบจะทำการตรวจสอบและหักเงินค่าผ่านทางจากบัญชีผู้ขับขี่อัตโนมัติ ปัญหาในการนำระบบ AETC มาใช้ได้แก่ความถูกต้องในการรับส่งข้อมูลระหว่างรถยนต์ที่วิ่งผ่านสถานีเก็บค่าผ่านทางและหน่วยงานจัดเก็บค่าผ่านทาง รวมไปถึงประสิทธิภาพในการทำงานของระบบ ดังนั้นจึงได้มีการกำหนดความต้องการของคุณสมบัติในการรักษาความปลอดภัยของการติดต่อสื่อสารโดยจะต้องมีการทำงานของระบบที่รวดเร็วแต่ยังรักษาความปลอดภัยไว้ได้จึงได้มีการนำเสนอระบบความปลอดภัยในการชำระเงินค่าผ่านทางด่วนบนเครือข่ายสื่อสารยานยนต์เฉพาะกิจโดยใช้วิทยาการรหัสลับแบบสมมาตร ซึ่งทำให้ใช้เวลาน้อยในการประมวลผล แต่ยังคงรักษาความลับในการให้บริการการชำระเงินค่าผ่านทางด่วน

ระบบชำระเงินที่ถูกออกแบบมาสำหรับเครือข่าย VANET มีหลายระบบ J.T. Isaac *et al.* [4] ได้นำเสนอโปรโตคอลสำหรับชำระเงินบนเครือข่าย VANET ชนิด Vehical-to-roadside Communications โดยเรียกว่า KCM-VAN (Kiosk Centric Model Payment Protocol for VANETs) โดยนำวิธีการวิทยาการรหัสลับแบบอสมมาตร (Asymmetric key Cryptography) มาใช้ในธุรกรรม โปรโตคอลนี้ถูกออกแบบมาสำหรับการชำระเงินทั้งแบบเครดิต (Credit-based Payment) และแบบเดบิต (Debit-based Payment) และมีโครงสร้างการทำงานคล้ายกับระบบ Secure Electronic Transaction (SET) ซึ่งเป็นโปรโตคอลที่มีความมั่นคงปลอดภัยในระดับที่สูง

อย่างไรก็ตาม KCM-VAN นั้นไม่เหมาะกับการนำไปใช้งานจริงเนื่องจากการเข้ารหัสข้อความนั้นทำในลักษณะแบบ Sign-then-encrypt ที่ถือว่ามีการคำนวณที่หนัก นอกจากนี้ลักษณะการเข้ารหัสลับแบบซ้อนๆ กันเป็นชั้นๆ ถือว่าไม่เหมาะสมในการออกแบบเนื่องจากการเข้ารหัสซ้อนกันหลายชั้นอาจไม่ได้ช่วยเพิ่มความมั่นคงปลอดภัยให้แก่ระบบมากขึ้นเมื่อเทียบกับการเข้ารหัสลับแบบชั้น

เดียว ในขณะเดียวกัน โปรโตคอล KCM-VAN ก็ยังไม่เหมาะสมกับการนำมาประยุกต์ใช้กับการชำระค่าผ่านทางด่วนเนื่องจากโปรโตคอลนั้นมีค่าใช้จ่ายในการดำเนินการ (Operation Cost) มากจากการเลือกใช้การเข้ารหัสลับแบบสมมาตร ดังนั้นเทคนิคการชำระเงินแบบ Micropayment ที่เหมาะสมกับการชำระเงินปริมาณน้อยๆ จึงน่าจะเหมาะสมกว่าในการนำมาใช้ชำระค่าผ่านทางด่วนผ่านทางเครือข่าย VANET

บทความฉบับนี้นำเสนอการออกแบบระบบชำระเงินค่าผ่านทางโดยที่มีพื้นฐานมาจากระบบชำระเงินแบบ Micropayment ระบบที่นำเสนอนั้นยังถูกออกแบบให้มีคุณสมบัติทางด้านความปลอดภัยที่จำเป็นในการทำธุรกรรมอิเล็กทรอนิกส์ (Electronic Transactions) อย่างครบถ้วน เช่น Data Confidentiality, Party Authentication, Data Integrity, และ Non-repudiation of Transactions นอกจากนี้ผู้วิจัยยังได้ทำการเปรียบเทียบประสิทธิภาพของระบบที่นำเสนอโดยเทียบกับระบบที่มีอยู่แล้ว และพบว่าระบบที่นำเสนอมีปริมาณการคำนวณต่อการทำธุรกรรม 1 ครั้งน้อยกว่าระบบที่มีอยู่ จึงสรุปได้ว่าระบบที่นำเสนอมีประสิทธิภาพดีกว่าระบบที่มีอยู่

โครงสร้างในบทความฉบับนี้มีดังนี้ บทที่ 2 กล่าวถึงพื้นฐานที่จำเป็น บทที่ 3 นำเสนอโปรโตคอลสำหรับการชำระค่าผ่านทางบนเครือข่าย VANET ในบทที่ 4 เสนอการวิเคราะห์คุณสมบัติทางด้านความมั่นคงปลอดภัยในการทำธุรกรรมอิเล็กทรอนิกส์ด้วยระบบที่นำเสนอ และวิเคราะประสิทธิภาพ บทที่ 5 เป็นการสรุปผลและเสนอแนะแนวทางในการพัฒนางานวิจัยในอนาคต

2. พื้นฐานที่เกี่ยวข้อง

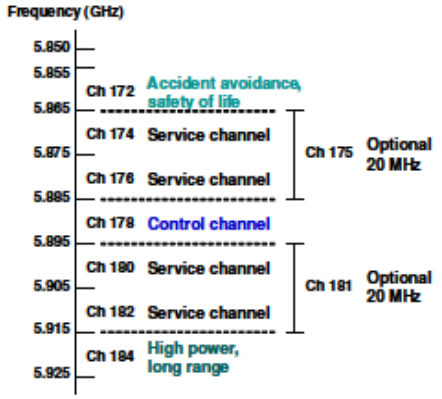
2.1 มาตรฐาน IEEE802.11p และ IEEE1609

ในปี 1999 องค์กร FCC (Federal Communication Commission) ได้กำหนดย่านการสื่อสารระยะใกล้ DSRC (Dedicated Shat Range Communications) ที่ความถี่ย่าน 5.9 GHz โดยจัดสรรช่วงความถี่ 75 MHz สำหรับการใช้งานด้าน Intelligent Transportation System ในอเมริกาเหนือ โดยย่านดังกล่าวถูกแบ่งเป็น 7 ช่องสัญญาณดังแสดงในรูปที่ 2 มาตรฐานชั้นกายภาพนั้นถูกพัฒนาขึ้นโดย ASTM (American Society for Testing and Material) ที่รู้จักกันในชื่อมาตรฐาน ASTM E2213 [8] โดยใช้เทคนิค OFDM (Orthogonal Frequency Division Multiplexing) สำหรับการมอดูเลชั่น (Modulation) และพัฒนาระดับชั้นการเชื่อมต่อ (Link layer) โดยมีพื้นฐานมาจากมาตรฐาน IEEE 802.11a แต่มีการปรับลดข้อมูลในส่วนของ Overhead ให้ลดน้อยลงและปรับรูปแบบข้อมูลใน MAC (Media Access Control) แล้วเรียกมาตรฐานที่พัฒนาขึ้นใหม่ว่า IEEE 802.11p เนื่องจากโหนด (Node) เคลื่อนที่ตลอดเวลา จึงใช้เทคนิคของ Diversity เพื่อลดปัญหาของ ICI (Inter Carrier Interference) และผลกระทบของ Doppler effect [8]

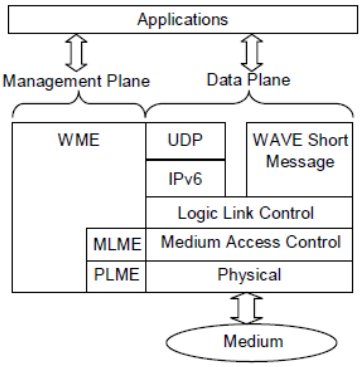
ในขณะที่มาตรฐาน ASTM E2213 กำลังพัฒนาก็มีกลุ่มผู้วิจัย IEEE 1609 working group [8] ออกมาตรฐาน IEEE P1609.1, P1609.2, P1609.3 และ P1609.4 สำหรับการใช้งานใน VANET โดย P1609.3 อยู่ในช่วงกำลังพัฒนา ส่วนที่เหลือได้มีการทดลองใช้งานอยู่ มาตรฐาน 1609 นั้นเป็นมาตรฐานที่มีพื้นฐานมาจาก IEEE 802.11p (ที่เป็นการปรับปรุงมาจาก IEEE 802.11a เพื่อใช้งานกับ DSRC) โดยเป็นการกำหนดชั้นการทำงานระดับสูง (Higher layer) และใช้งาน IEEE 802.11p เป็นชั้นการทำงานระดับล่าง (Based layer) โดยมาตรฐานทั้ง 4 นั้น แบ่งออกเป็น

- IEEE P1609.1 เป็นมาตรฐานสำหรับ Wireless Access For Vehicular Environment (WAVE) Resource Manager ซึ่งเป็นการกำหนดการประยุกต์ใช้งานพื้นฐาน (Basic application platform) ตลอดจนโปรโตคอลสื่อสารที่ใช้รับส่งข้อมูลระหว่าง RSU และ OBU

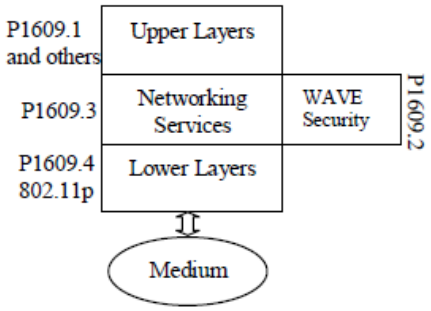
- IEEE P1609.2 เป็นมาตรฐานด้านความปลอดภัยสำหรับ WAVE 5.9 GHz. DSRC ในด้าน ความไม่มีลักษณะเฉพาะ (Anonymity) การระบุตัวตน (Authenticity) และการรักษาความลับ (Confidentiality)
- IEEE P1609.3 เป็นมาตรฐานด้านการจัดการเครือข่าย (Networking) สำหรับ WAVE 5.9 GHz DSRC
- IEEE P1609.4 เป็นมาตรฐานในการกำหนดการทำงานของเวฟหลายช่องสัญญาณ (WAVE Multichannel operation) ในการใช้งานและจัดการ DSRC ร่วมกัน เป็นการจัดการ DSRC ทั้ง 7 ช่องสัญญาณ การจัดการเลเยอร์ชั้นล่างๆ รวมถึงการประสานเข้ากับมาตรฐาน IEEE 802.11p



รูปที่ 2 ย่านความถี่ 5.9 GHz DSRC ในอเมริกาเหนือ [9]



รูปที่ 3 โครงสร้างมาตรฐาน IEEE 802.11p [8]



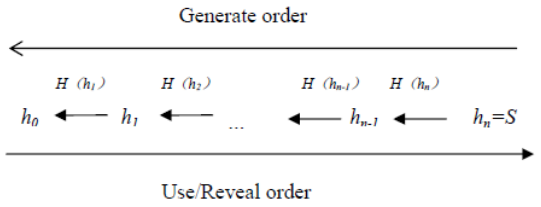
รูปที่ 4 โครงสร้างมาตรฐาน WAVE [8]

ในขณะที่มาตรฐาน IEEE 802.11p ยังคงอยู่ในขั้นการพัฒนา สำหรับฉบับร่าง (Draft version) ก็คือ WAVE นั่นเอง โดยทำงานที่อัตรารับส่งข้อมูล 3 ถึง 27 Mbps สำหรับช่องสัญญาณ 10 MHz และอัตรารับส่งข้อมูลจะเพิ่มขึ้นเป็น 6 ถึง 54 Mbps สำหรับช่องสัญญาณ 20 MHz มีการทำงานในแบบ Ad hoc mode โดย RSU จะกำหนด WBSS (WAVE Basic Service Set) ให้กับ OBU เพื่อการติดต่อสื่อสาร โดย RSU จะส่ง WBSS announcement frames และ OBU สามารถเลือกได้ที่จะทำการเชื่อมต่อ WBSS โดยที่ไม่มีการทำยืนยันตัวตน (Authentication) และ Association routines ใน WBSS และจะไม่ใช้ PCF (Point Coordination Function) ในมาตรฐานนี้ แต่จะใช้ EDCA (Enhanced Distributed channel Access) เหมือนกับที่ใช้ใน IEEE 802.11e [8] การใช้แพ็คเกท RTS/CTS (Request To Send/ Clear To Send) packets และวินโดว์ (Windows) ใน IEEE 802.11p ไม่ได้ช่วยแก้ปัญหา Hidden terminal และ Exposed terminals ใน V2V เนื่องจากการเคลื่อนที่ของโหนดที่เร็ว (High mobility nodes) การส่งแพ็คเกท DCF (Distributed Coordination Function) อาจเสียหายหรือชนกับแพ็คเกทอื่นจากการเคลื่อนที่ของโหนดที่ไม่ทราบถึง RTS/CTS hands shake (หรือจากโหนดที่อยู่ในถนนฝั่งตรงข้าม) ซึ่งส่งผลกระทบต่อความเร็วอัตราการรับส่งข้อมูลในV2Vได้ [1-12]

2.2 ฟังก์ชันแฮชทางเดียว (One-way Hash Chain Function)

ฟังก์ชันแฮชนั้นได้ถูกนำมาประยุกต์ใช้งานอย่างกว้างขวางในวิทยาการรหัสลับ (Cryptography) เพื่อกำเนิดกุญแจที่ใช้ครั้งเดียว (One-time key) จากการมีชุดกุญแจหรือรหัสลับ (Password) เพียงชุดเดียวซึ่งบางครั้งจะถูกเรียกว่า seed ฟังก์ชันแฮชนั้นมีการประยุกต์ใช้งานได้หลากหลาย โดยเฉพาะถูกนำไปใช้กับข้อมูลที่อยู่ในสิ่งแวดล้อมที่ไม่ปลอดภัย เช่น อินเทอร์เนท ระบบไร้สายต่างๆ สาเหตุที่มันเป็นที่นิยมมากเนื่องจากเป็นอัลกอริทึมที่รวดเร็วมาก (Very fast algorithm) มีขนาดOverheadต่ำและมีความทนทานต่อการถูกโจรกรรมสูง ด้วยคุณสมบัติดังกล่าว ทำให้นิยมนำฟังก์ชันแฮชมาประยุกต์ใช้งานกับระบบเครือข่ายไร้สายและระบบชำระเงินย่อย

เราสามารถอธิบายการกำเนิดชุดรหัสแฮชทางเดียวได้ดังรูปที่ 5 โดยมีขั้นตอนการทำงานดังต่อไปนี้ คือ ขั้นแรก เราทำการสุ่มตัวเลขมาหนึ่งค่าซึ่งจะถูกเรียกว่า seed S และทำให้มันเป็นอีลีเมนท์สุดท้าย (Last elements) ของขบวนแฮช (Hash chains) หลังจากนั้นทำการกำเนิดขบวนตัวเลขที่จะใช้กับฟังก์ชันแฮชทางเดียว H(.) โดยเรามีข้อกำหนดว่าการจะได้ขบวนตัวเลขแฮช $h_0 = H(h_1), h_{i-1} = h_n = S$ โดยค่าขององค์ประกอบแรก h_0 จะถูกเรียกว่า “Commitment” ต่อขบวนผ่าน h_0 โดยการตรวจสอบว่า $H^i(h_i) = h_0$ นอกจากนั้น ถ้าเราทราบค่า h_i ว่าอยู่ลำดับที่ i^{th} ขบวนการตัวเลขจะทำให้เราตรวจสอบค่า hj ว่าเป็นองค์ประกอบของขบวนตัวเลขโดยเราจะทำการตรวจว่าค่า $H^{(j-i)}(h_j) = h_i$ เมื่อกำหนดให้ $i < j$ ค่าฟังก์ชันแฮช H(.) จะถูกอธิบายว่าเป็นทางเดียว (One-way) เพราะว่ามันเป็นคุณสมบัติสำคัญของค่าตัวเลข x ที่กำหนดขึ้น มันจึงเป็นการง่ายในการกำหนดค่าแฮช H(x) แต่ว่าค่าแฮชที่ได้นี้จะเป็นการยากในการหาค่า x ดังนั้น เมื่อกำหนดค่าของ hj จึงเป็นการง่ายในการคำนวณหา $H^{(i-i)}(h_j)$ ในการตรวจสอบค่าของ h_j ว่าเป็นส่วนหนึ่งของขบวนตัวเลขหรือเปล่าแต่ว่ามันจะเป็น การยากมากในการหาค่า h_j เมื่อกำหนดค่า h_j ไว้ให้ (เราสมมติว่า $H^{(j-i)}(h_j) = h_i$) ดังนั้นเราจึงเชื่อว่าผู้ส่งข้อมูลจะเปิดเผยข้อมูลส่วนตัวและองค์ประกอบในลักษณะตรงข้ามกับกำลังของการกำเนิดคำนั้นขึ้นมา นั่นคือ เริ่มต้นด้วยค่า h_{01} ตามด้วย $h_1,\ldots,$ จนถึง h_n เมื่อกำหนดให้ใช้เป็นขบวนการแฮช ค่าตัวเลขอันดับแรก h_0 นั้นโดยทั่วไปจะถูกเซ็นต์ด้วยการใช้มาตรฐานการลงลายมือชื่อต่างๆ เช่น กุญแจส่วนตัว (private key) ผู้รับจะทำการตรวจสอบคำขององค์ประกอบแรก h_0 โดยการใช้กุญแจสาธารณะจากผู้ส่ง อย่างไรก็ตามการเปิดเผยองค์ประกอบ h_i สามารถตรวจสอบได้โดยง่ายจากการเปิดเผยองค์ประกอบก่อนหน้านั้น จึงเป็นเหตุผลว่าการตรวจสอบทำได้รวดเร็วโดยทำการตรวจสอบโดยใช้กุญแจส่วนบุคคล ณ องค์ประกอบ h_i ถูกตรวจสอบว่าเป็นส่วนหนึ่งของขบวนตัวเลขหรือเปล่า นั่นหมายถึงว่า ค่า h_i มาจากผู้ส่งคนเดียวกันจากค่าองค์ประกอบแรก h_0 เพราะว่าไม่มีใครจะสามารถกำเนิดค่า h_i ถึงแม้ว่าจะรู้ค่าของ h_0 ก็ตาม เนื่องจากคุณสมบัติเป็นทางเดียวเท่านั้น (one-way property) [10-13]



รูปที่ 5 One-way Hash chain function [10]

2.3 Micropayment

Micropayment เป็นระบบชำระเงินแบบอิเล็กทรอนิกส์ที่มีประสิทธิภาพ โดยถูกออกแบบให้เหมาะสมสำหรับการชำระเงินจำนวนไม่มากนัก แต่มีการชำระอยู่บ่อยๆเพื่อที่สามารถจัดเก็บรายการต่างๆด้วยต้นทุนที่ต่ำมากๆ ซึ่งระบบชำระเงินย่อยนี้จะช่วยลดขั้นตอนของการสื่อสารและการประมวลผลที่ต่ำลง เมื่อเปรียบเทียบกับระบบการจ่ายเงินแบบใหญ่ (Macro-payment) เช่น ระบบธนาคาร ระบบจ่ายเงินแบบย่อยจะช่วยให้การตรวจสอบการชำระเงินแบบออฟไลน์ (Offline payment verification) โดยใช้ Lightweight cryptosystems ซึ่งเหมาะสำหรับระบบที่ไม่ต้องการความปลอดภัยของรายการที่สูงมากนัก เพื่อเป็นการเพิ่มประสิทธิภาพ โดยพิจารณาว่าความพยายามที่จะ

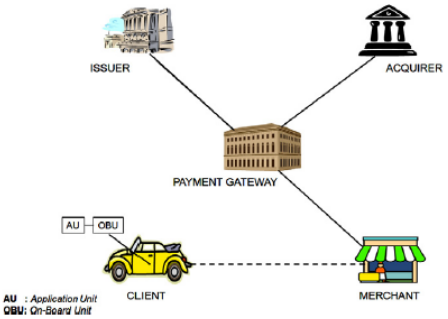
ทุจริตมีมูลค่าน้อยกว่าการโกงเงินค่าผ่านทางระบบชำระเงินย่อย โดยทั่วไปประกอบไปด้วย 3 องค์ประกอบ (Entities) เช่น ลูกค้า (Customer) ผู้ขาย (Vender) และคนกลาง (Broker) ลูกค้าจะเปิดบัญชีกับคนกลาง คนกลางจะเป็นคนออก (Issue) การรับรองลายเซ็นต์ดิจิตอล (Digitally Signed Certificates) เพื่อที่อนุญาตให้ลูกค้าทำรายการชำระเงิน (Payment chains) และมั่นใจได้ว่าผู้ขายสามารถรับเงินได้ ระบบชำระเงินจะประยุกต์คุณสมบัติการเข้ารหัสของลายเซ็นต์ดิจิตอลและฟังก์ชั่นแฮช (Hash chain function) ลูกค้าจะสร้างรายการชำระเงิน P_1, P_2,…,P_n ในลักษณะรายการย้อนกลับโดยเลือกรายการสุดท้าย Pn โดยการสุ่ม หลังจากนั้นคำนวณหา $P_i - 1 = h(P_i)$ โดยที่ h เป็น Collision-resistant hash function และ i = 1, …, n เมื่อ P_0 เป็นค่ารากของรายการชำระเงิน (Root of payment chain) และไม่สามารถทำรายการเพื่อจ่ายเงินให้กับตัวเองได้ สัญญาของระบบการจ่ายเงินจะประกอบด้วย ค่าราก P_0 แต่ไม่ใช่ทุกค่าของ P_i เมื่อ i มากกว่าหรือเท่ากับ 1 รายการชำระเงินที่ i (สำหรับ i = 1, 2,…) จากลูกค้าไปยังผู้ขายประกอบด้วยคู่ (P_i, i) ซึ่งผู้ขายสามารถตรวจสอบโดยการตรวจสอบกับสัญญาและค่า $P_0 = h^i(P_i)$ [10-13]

2.4 ระบบระบบชำระเงินบนเครือข่าย VANET โดยใช้วิทยาการรหัสลับแบบอสมมาตร KCM-VAN

J.T. Isaac *et al.* [4] ได้นำเสนอโปรโตคอล KCM-VAN (Kiosk Centric Model Payment Protocol for VANETs) ดังรูปที่ 6โดยนำวิธีการวิทยาการรหัสลับแบบอสมมาตร (Asymmetric key cryptography) มาใช้ในธุรกรรมชำระเงินบนเครือข่าย VANET โดยมีการใช้กุญแจในการเข้ารหัส 2 ชุดคือกุญแจสาธารณะ (Public key) และ กุญแจส่วนตัว (Private key) โดยมีกระบวนการในการทำงานดังต่อนี้

2.4.1 นิยามและสมมติฐาน

- **C, M, PG, I, A**: Client, Merchant, Payment Gateway, Issuer และ Acquirer
- **ID_P**: The identity of party *P* that contains the contact information of *P*
- **NID_C**: Client's nickname, temporary identity
- **K_P**: Party's *K* public key
- **K_S**:Party's *K* private key
- **TID:** Identity of transaction that includes time and date of the transaction
- **E_{Pi-Pj}(M)**: Message *M* signed and encrypted by the user ID_{Pi} to a specified & receiver ID_{Pj}
- **TST_P**: Timestamp generated by P
- **Stt:** The status of transaction (Stt = {Accepted, Rejected})
- **OI:** Order information (OI = {TID, OD, *h*(OD,Price)}) where OD and Price are order descriptions and its amount
- **TC:** The type of card used in the purchase process (TC = {Credit, Debit})
- **TIDReq:** The request for TID
- **MIDReq:** The request for ID_M
- **MPReq:** The request for M_P
- *h*(*M*): The one-way hash function of the message *M*
- **A ⟶ B**: A sending message x to B



รูปที่ 6 KCM-VAN Protocols [4]

2.4.2 กระบวนการทำงานของ KCM-VAN

ขั้นตอนที่ 1 : Client (C) ทำการติดต่อไปยัง Merchant (M) ทำการแลกเปลี่ยนข้อมูลที่จะใช้ในการเริ่มกระบวนการ

1) **C ⟶ M:** NID_C,*TIDReq*,*MIDReq*,*MPReq*

M ⟶ C: $E_{M-C}(TID,ID_M,M_P)$

ขั้นตอนที่ 2 : Client (C) จะทำการสร้างคำร้องขอในการทำธุรกรรม (Payment Request: (VSRequest)) [14][15] ไปยัง Merchant (M)

2) **C ⟶ M:** $E_{C-M}(OI,Price,$ $TST_C,NID_C,ID_P,VSRequest)$

$VSRequest = E_{C-I}(Price,TST_C,h(OI),TC,ID_M)$

ขั้นตอนที่ 3 : Merchant (M) จะทำการสร้างค่าของการร้องขอในการทำธุรกรรม (Value-Claim Request: (VCRequest)) ไปยัง Payment Gateway (PG)

3) **M ⟶ PG:** $VCRequest,ID_M$

$VCRequest = E_{M-PG}(VSRequest,TST_M,h(OI),TID,$ $Price,NID_C,ID_I)$

ขั้นตอนที่ 4 : Payment Gateway จะติดต่อไปยังธนาคาร (bank) เพื่อทำการตรวจสอบการร้องขอในการธุรกรรม

4.1) **PG ⟶ I:** $VSRequest,h(OI),TID,Price,NID_C,ID_M$

4.2) **PG ⟶ A:** $Price,ID_M$

4.3) **I,A ⟶ PG:** $VSResponse,Stt,h(Stt,h(OI))$

$VSResponse = E_{I-C}(Stt,h(OI))$

ขั้นตอนที่ 5 : Payment Gateway (PG) จะทำการสร้างค่าของการตอบกลับในการทำธุรกรรมที่ร้องขอ(Value-Claim Response: (VCResponse)) ไปยัง Merchant (M)

5) **PG ⟶ M:** *VCResponse*

$VCResponse = E_{PG-M}(Stt,VSResponse,h(Stt,h(OI$ $)))$

ขั้นตอนที่ 6 : Merchant (M) ทำการตอบกลับการร้องขอในการทำธุรกรรมไปยัง Client (C)

6) **M ⟶ C:** *PResponse*

$PResponse = E_{M-C}(VSResponse)$

อย่างไรก็ตาม KCM-VAN นั้นไม่เหมาะกับการนำไปใช้งานจริงเนื่องจากการเข้ารหัสข้อความนั้นทำในลักษณะแบบ Sign-then-encrypt ที่ถือว่ามีการคำนวณที่หนักนอกจากนี้ลักษณะการเข้ารหัสลับแบบซ้อนๆ กันเป็นชั้นๆ ถือว่าไม่เหมาะสมในการออกแบบเนื่องจากการเข้ารหัสซ้อนกันหลายชั้นอาจไม่ได้ช่วยเพิ่มความมั่นคงปลอดภัยให้แก่ระบบมากขึ้นเมื่อเทียบกับการเข้ารหัสลับแบบชั้นเดียว ในขณะเดียวกัน โปรโตคอล KCM-VAN ก็ยังไม่เหมาะสมกับการนำมาประยุกต์ใช้กับการชำระค่าผ่านทางด่วนเนื่องจากโปรโตคอลนั้นมีค่าใช้จ่ายในการดำเนินการ (Operation Cost) มากจากการเลือกใช้การเข้ารหัสลับแบบสมมาตร ดังนั้นเทคนิคการชำระเงินแบบ Micropayment ที่เหมาะสมกับการชำระเงินปริมาณน้อยๆ จึงน่าจะเหมาะสมกว่าในการนำมาใช้ชำระค่าผ่านทางด่วนผ่านทางเครือข่าย VANET นอกจากนี้การเลือกใช้วิทยาการเข้ารหัสลับแบบสมมาตรจะทำให้การคำนวณลดน้อยลงและส่งผลให้เกิดการทำงานที่เร็วขึ้น แต่ยังมีคุณสมบัติทางด้านการรักษาความปลอดภัยที่สมบูรณ์ได้ในระดับหนึ่ง ดังนั้นงานวิจัยฉบับนี้จึงมุ่งเน้นที่จะนำเสนอและพัฒนาระบบชำระค่าผ่านทางโดยใช้แนวคิดของการชำระเงินแบบ Micropayment และวิทยาการเข้ารหัสลับแบบสมมาตรมาใช้งาน ดังรายละเอียดในบทถัดไป

3. ระบบที่นำเสนอ

3.1 นิยามและสมมติฐาน

- C คือ ลูกค้า (หรือผู้ใช้บริการ), B คือ ธนาคาร, และ M คือ ผู้ให้บริการ
- ID_x คือ หมายเลขเฉพาะ (Identity) ของบุคคลชื่อ x
- LP_c คือ หมายเลขทะเบียนรถของลูกค้า (Client's license plate)
- DL_{ID} คือ หมายเลขใบขับขี่ของลูกค้า
- K_{CB} คือ รหัสกุญแจลับแบบใช้งานระยะยาวที่ใช้ร่วมกันระหว่างลูกค้าและธนาคาร
- X_{CM} คือ กุญแจรหัสลับที่ใช้ร่วมกันระหว่างลูกค้าและผู้ให้บริการ
- Y_{CB} คือ กุญแจรหัสลับที่ใช้ร่วมกันระหว่างลูกค้าและธนาคาร

- Z_{MB} คือ กุญแจรหัสลับที่ใช้ร่วมกันระหว่างผู้ให้บริการและธนาคาร
- X_i คือ ชุดกุญแจลับของ X
- Y_i คือ ชุดกุญแจลับของ Y
- Z_j คือ ชุดกุญแจลับของ Z
- $h\ (X,K)$ คือ ค่าของกุญแจแฮชของข้อความ X ด้วยค่าของกุญแจ K
- C_{max} คือ วงเงินสูงสุดของลูกค้า C ที่ร้องขอคูปองธนาคาร
- C_{mer} คือ วงเงินที่ลูกค้า C ที่ร้องขอคูปองบริการเพื่อจ่ายให้กับผู้ให้บริการ M
- C_{min} คือ วงเงินที่เหลืออยู่ในคูปองของลูกค้า
- c คือ ค่าตัวเลขสุ่มจากธนาคารเพื่อกำเนิดเหรียญอิเล็กทรอนิกส์ (Electronic coins)
- c_j คือ ชุดของเหรียญที่กำเนิดโดยลูกค้าสำหรับผู้ให้บริการ
- c_0 คือ ชุดของเหรียญที่กำเนิดโดยลูกค้าสำหรับแนบในคูปองบริการส่งให้ผู้ให้บริการ
- C_m คือ จำนวนเงินจากลูกค้าที่จ่ายให้กับผู้ให้บริการ
- TS_C คือ วันเวลาขณะเกิดรายการที่ร้องขอรายการธุรกรรม C_{max}
- TS_B คือ วันเวลาช่วงที่เกิดรายการธุรกรรม C_{max}
- TS_{co} คือ วันเวลาที่ใช้ในการกำหนดชุดของเหรียญ
- TS_{CR} คือ วันเวลาในขณะที่ร้องขอการยกเลิกรายการธุรกรรมการเงิน
- $Cancel_{ACK}$ คือ ยืนยันการยกเลิกรายการธุรกรรมการเงิน

ข้อสมมติฐานเบื้องต้น (Initial Assumptions) ของโปรโตคอลที่นำเสนอ มีดังต่อไปนี้

- ลูกค้า C จะใช้งาน K_{CB} ร่วมกันกับธนาคาร B ซึ่ง K_{CB} จะมีข้อมูลบัญชีธนาคารของ C ที่จะรู้กันเฉพาะ C และ B
- ลูกค้า C, ธนาคาร B และผู้ให้บริการ M จะทำการแลกเปลี่ยนกุญแจรหัสลับระหว่างกัน 3 ชุด คือ X_{cm}, Y_{CB}, Z_{mB}
- เมื่อกุญแจลับ X_{cm}, Y_{CB} และ Z_{mB} ถูกกระจายให้กับ C, M และ B แล้ว C, M, B ก็จะต้องมีการอัพเดท (update) ตามระยะเวลาที่แต่ละคู่การเชื่อมต่อร้องขอ หลังจากที่ได้กุญแจเหล่านี้มาแล้ว ก็จะทำการกำเนิดชุดรหัสลับ X_i, Y_i และ Z_j โดยที่ $i, j = 1, \ldots, n$ แล้วเก็บชุดกุญแจนี้ไว้ที่อุปกรณ์ในแต่ละคู่การเชื่อมต่อ ชุดกุญแจเหล่านี้ถูกใช้เพื่อเป็นกุญแจเข้ารหัสในโปรโตคอลเพื่อที่จะลดความถี่ของการอัพเดทชุดรหัสกุญแจและช่วยเพิ่มประสิทธิภาพในการรักษาความลับอีกชั้นหนึ่ง
- ลูกค้า C จะเชื่อถือธนาคาร B ว่าจะไม่เปิดเผยข้อมูลใน K_{CB} ให้กับผู้อื่น
- ค่าของ $h\ (X, K)$ หมายถึง ค่า Message Authentication Code ของข้อความ X ด้วยกุญแจ K

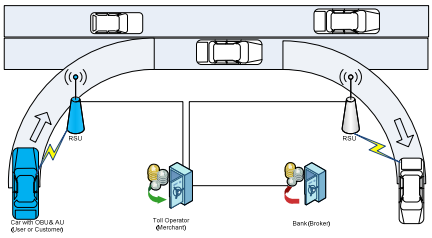
ระบบ AETC จะมีสถาปัตยกรรมของระบบที่มีองค์ประกอบดังต่อไปนี้

- *รถยนต์* ที่ติดตั้ง OBU และ AU ที่รองรับการทำงานของ VANET และเชื่อมต่อกับป้ายทะเบียนรถยนต์อิเล็กทรอนิกส์ (ELP)
- *สถานีรับส่งสัญญาณข้างทาง (RSU)* ทำหน้าที่เป็นสถานีฐาน (Base Station) หรือจุดเชื่อมต่อ (Access Point) นั่นเอง โดย RSU จะทำการรับส่งสัญญาณกับรถยนต์แบบไร้สายตามมาตรฐาน IEEE 802.11p 5.9 GHz. DSRC และ IEEE 1609 WAVE หลังจาก RSU รับส่งสัญญาณจากรถยนต์แล้วก็จะเชื่อมต่อรับส่งสัญญาณกับผู้ให้บริการค่าผ่านทางด่วนในแบบมีสายหรือไร้สายก็ได้ขึ้นอยู่กับการประยุกต์ใช้งานของผู้ให้บริการค่าผ่านทางด่วน
- *ผู้ให้บริการค่าผ่านทางด่วน (Toll Operation หรือ TO)* ทำหน้าที่เป็นผู้ให้บริการเก็บเงินค่าผ่านทางด่วนหรืออาจกล่าวได้ว่าเป็นพ่อค้า (Merchant) นั่นเอง

ตลอดจนเก็บข้อมูลที่จำเป็น เช่น วันที่, เวลา, ชื่อด่านเก็บเงินและข้อมูลรถ เป็นต้น เพื่อให้สามารถตรวจสอบข้อมูลย้อนหลังได้

- *ธนาคาร (Bank)* ทำหน้าที่เป็นผู้ให้บริการการเงินแก่ลูกค้าและ TO โดยลูกค้าและ TO จะมีบัญชีฝากไว้กับธนาคารและ TO สามารถหักเงินค่าทางด่วนจากบัญชีของลูกค้าที่ฝากไว้กับธนาคารได้

จากองค์ประกอบต่างๆสามารถแสดงเป็นโครงสร้างดังรูปที่ 7



รูปที่ 7 สถาปัตยกรรมของระบบAETC

3.2 รายละเอียดของระบบที่นำเสนอ

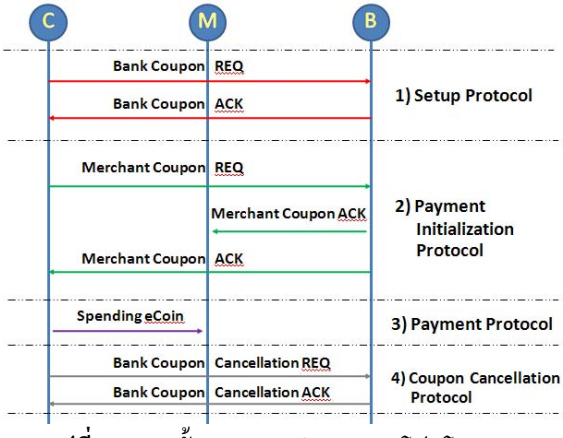
ขั้นตอนการทำงานของโปรโตคอลสามารถแสดงดังรูปที่ 8 ซึ่งประกอบด้วย 4 โปรโตคอลย่อย คือ

1) โปรโตคอลสำหรับการเริ่มต้น (Start protocol)
2) โปรโตคอลในการเริ่มธุรกรรมการเงิน (Payment Initialization Protocol)
3) โปรโตคอลธุรกรรมการเงิน (Payment Protocol) และ
4) โปรโตคอลในการยกเลิกการใช้งานคูปอง (Coupon Cancellation Protocol)

3.2.1 โปรโตคอลสำหรับการเริ่มต้น (Start protocol)

ลูกค้า C จะร้องขอไปยังธนาคาร B เพื่อร้องขอสิทธิ์ในการทำธุรกรรมการเงินย่อย (Micropayment transaction authorization) ด้วยจำนวนค่าเงิน C_{max} ดังสมการที่ 7)

7) **C → B:** $ID_C, DL_{ID}, C_{max}, TS_c, h(DL_{ID}, C_{max}, TS_c, Y_i)$



รูปที่ 8 แสดงขั้นตอนการทำงานของโปรโตคอล

หมายเหตุ ค่า $h(DL_{ID}, C_{max}, TS_c, Y_i)$ ใช้ในการปกป้องความมั่นคง (Data integrity) ของข้อความ DL_{ID}, C_{max}, TS_c, Y_i หลังจากธนาคาร B ได้รับการร้องขอแล้วก็จะทำการตรวจสอบบัญชีเงินฝากของลูกค้า C แล้วทำการหักบัญชีเงินฝากนั้นด้วยค่าของ C_{max} (เสมือนการถอนเงินจากบัญชีนั่นเอง) หลังจากนั้นก็จะทำการส่งคูปองธนาคารกลับไปยังลูกค้า C

8) **B → C:** $\{C_{max}, TS_B, TS_C, c\}_{Yi}$

คูปองธนาคารจะประกอบไปด้วย การอนุมัติ C_{max}, ค่าเวลา TS_B ในขณะที่เกิดรายการ C_{max} และค่า c คือ ค่าตัวเลขสุ่มที่ออกโดยธนาคารเพื่อใช้ในการกำเนิดเหรียญอิเล็กทรอนิกส์

ในขณะนี้ลูกค้าก็จะมีคูปองธนาคารที่สามารถเอาไปใช้ในการจ่ายค่าผ่านทางด่วนได้แล้วจนกว่ามูลค่า C_{max} ในคูปองธนาคารจะหมด หลังจากเงิน C_{max} ในคูปองธนาคารหมดแล้วลูกค้าต้องทำการร้องขอต่อธนาคารด้วยโปรโตคอลนี้เพื่อให้ได้ค่า C_{max} ใหม่มา

3.2.2 โปรโตคอลในการเริ่มธุรกรรมการเงิน (Payment Initialization Protocol)

เพื่อที่จะเริ่มทำธุรกรรมการเงินกับผู้ให้บริการ M, ลูกค้า C จะกำเนิดชุดของเหรียญ c_j โดยที่ $j = 0,..., m$ และ $m = C_{mer}$ ดังความสัมพันธ์ $c_m = \{c, TS_{co}\}$

9) $c_j = h(c_j + 1)$ โดย $j = 0,..., m - 1$

ลูกค้าจะกำหนดจำนวนเงิน C_{mer} ที่จะจ่ายให้กับผู้ให้บริการ M โดยลูกค้าจะทำการแนบเหรียญและ C_{mer} ไปกับคูปองบริการและส่งคูปองบริการกลับไปยังธนาคาร

10) **C → B:** $h(ID_m, LP_c, c_0, TS_{co}, C_{mer}, C_{max}, TS_B, Y_i)$, $h(c_0, TS_{co}, C_{mer}, X_i)$, TS_{co}, C_{mer}

หมายเหตุ เราจะเห็นว่า $h(c_0, TS_{co}, C_{mer}, Xi)$ มีข้อมูลส่วนหนึ่งของการร้องขอธุรกรรมการเงินจากลูกค้าไปหาผู้ให้บริการ M แต่ว่าจะไม่สามารถอ่านได้โดยธนาคาร

ธนาคารจะเอาค่า C_{max} และ C_{mer} จาก $h(ID_m, LP_c, c_0, TS_{co}, C_{mer}, C_{max}, TS_B, Y_i)$ ซึ่งอาจพิจารณาว่าเป็นการร้องขอการหักบัญชี (Debit request) และตรวจสอบว่าค่าของ $C_{max} < C_{mer}$ หรือไม่ ถ้าน้อยกว่าก็จะปฏิเสธการร้องขอนั้น (หมายความว่าเงินที่ร้องขอหักบัญชีจากคูปองบริการนั้นมีมูลค่ามากกว่ามูลค่าสูงสุดของคูปองธนาคารที่ร้องขอกับธนาคาร) ถ้า $C_{max} > C_{mer}$ ธนาคารจะคำนวนวงเงินที่เหลืออยู่ของ C_{min} โดยที่ $C_{min} = C_{max} - C_{mer}$ แล้วยังคงค่านี้ของ C_{min} นี้เพื่อป้องกันปัญหาจ่ายเงินซ้ำซ้อน (Over-spending problem) ณ จุดนี้ธนาคารจะโอนเครดิตเงิน C_{mer} ไปยังบัญชีของผู้ให้บริการ M หลังจากนั้นธนาคารทำการส่งข้อความไปยังผู้ให้บริการ M และลูกค้าดังต่อไปนี้

11) **B→ M:** $\{c_0, C_{mer}, h(ID_m, LP_c, C_{min}, Y_i)\}_{Zj}$, $h(c_0, C_{mer}, X_i)$

12) **B→ C:** $h(ID_m, C_{min}, Y_i)$

หมายเหตุ ค่าของ C_{min} ข้อความจากสมการ 11) ถูกพิจารณาได้ว่าเป็นเครดิตยอดเงินที่โอนจากธนาคารไปยังผู้ให้บริการ M ผู้ให้บริการจะหาค่า c_0 และ C_{mer} จากข้อความที่ถูกใส่รหัสไว้โดยจะทราบว่าลูกค้าประสงค์ที่จ่ายเงินให้กับผู้ให้บริการ M จาก $h(c_0, C_{mer}, X_i)$ และลูกค้าจะรู้ว่ารายการที่ร้องขอไปนั้นได้ผ่านการตรวจสอบสิทธิ์จากธนาคารจากข้อความที่ถูกเข้ารหัสด้วย Z_j ที่ใช้งานร่วมกันระหว่างธนาคารและตัวเอง

หลังจากได้รับข้อความในสมการ 12) แล้ว ในภายหลังลูกค้าสามารถใช้ C_{min} เพื่อทำธุรกรรมกับผู้ให้บริการรายอื่นๆ ได้

หมายเหตุ ข้อความจากสมการ 12) นั้น พิจารณาว่าเป็นการตอบกลับการหักเงินในบัญชีจากธนาคารไปยังลูกค้า ในโปรโตคอลนี้ผู้ให้บริการ M จะไม่สามารถทำตนเป็นลูกค้าได้เนื่องจากระหว่างการติดต่อสื่อสารระหว่างกันจะกระทำด้วยชุดกุญแจลับที่ต่างกันและกุญแจดังกล่าวไม่ได้ถูกแสดงในขณะทำธุรกรรมต่อกัน

3.2.3 โปรโตคอลจ่ายเงิน (Payment Protocol)

หลังจากจบกระบวนการที่กล่าวมาข้างต้นเสร็จแล้ว ลูกค้าจะสามารถทำการชำระเงินไปยังผู้ให้บริการโดยการส่งเหรียญ c_j ดังนี้

13) **C → M:** c_j, ID_c เมื่อ $j = 1,..., m$

หมายเหตุ ผลรวมของค่า c_j และ $h(ID_m, C_{min}, Y_i)$ จากข้อความในสมการ 11) และ 12) จะแสดงถึงใบสั่งซื้อ (Payment Ordering request) จากลูกค้า แล้วผู้ให้บริการจะตรวจสอบจำนวนที่ร้องขอโดยการเปรียบเทียบค่า c_j กับ c_0 หลังจากจบกระบวนการนี้แล้ว มูลค่าของเงินในคูปอง C_{mer} จะถูกหักออก ลูกค้าจะสามารถใช้เงินที่เหลือนี้ได้จนกว่าจะ

ถึงค่าของ C_{mer} โดยไม่ต้องมีการตรวจสอบสิทธิ์จากธนาคาร

3.2.4 โปรโตคอลในการยกเลิกคูปอง (Coupon Cancellation Protocol)

ในกรณีที่ลูกค้าต้องการแลกเงินคืนจากคูปองธนาคาร ที่ไม่ได้ถูกนำไปใช้ สามารถส่งข้อความต่อไปนี้ไปยังธนาคาร

14) **C→ B:** TS_{CR}, $h(C_{max}, TS_B, TS_{CR}, Y_i)$

ธนาคารจะทำการลบค่า C_{max} ในคูปองนี้ออกจากฐานข้อมูล หลังจากนั้นจะโอนเงินจำนวน C_{max} กลับคืนไปยังยัญชีของลูกค้าแล้วทำการส่งข้อความยืนยัน ดังต่อไปนี้

15) **C → B**: $Cancel_{ACK}$, $h(Cancel_{ACK}, TS_{CR}, Y_i)$

หลังจากรับข้อความ 14) แล้ว ลูกค้าจะทราบว่าคูปองนั้นไม่สามารถใช้ได้ต่อไปในระบบ ดังนั้น หากลูกค้าต้องการทำธุรกรรมการเงินกับผู้ให้บริการอีก ลูกค้าจะต้องทำขั้นตอนแรกในการซื้อคูปองธนาคารกับธนาคารแล้วเริ่มกระบวนการข้างต้นใหม่อีกครั้งหนึ่ง

4. การวิเคราะห์ความปลอดภัย

4.1 คุณสมบัติทางด้านความปลอดภัยของธุรกรรมการเงิน (Transaction Security Properties)

เพื่อให้ง่ายต่อการอธิบายจึงขอยกตัวอย่างสมการ 11) เพื่ออธิบายการวิเคราะห์ความปลอดภัยดังนี้

11) **B → M:** $\{c_0, C_{mer}, h(ID_m, LP_c, C_{min}, Y_i)\}_{Zj}$, $h(c_0, C_{mer}, X_i)$

- **สิทธิ์ในการเชื่อมต่อแต่ละฝ่าย (Party Authentication)** เป็นการรับรองว่าการเข้ารหัสแบบสมมาตรด้วย ค่า Z_j และ Y_i ที่ใช้ร่วมกันระหว่างลูกค้าและธนาคารนั้น ใครกันเป็นคนส่งข้อความ
- **ความเป็นส่วนตัวของธุรกรรมการเงิน (Transaction Privacy)** จะถูกรับรองโดยการเข้ารหัสแบบสมมาตรด้วยค่า Z_j
- **การไม่สามารถปฏิเสธว่าใครเป็นคนทำธุรกรรมการเงินได้ (Non-repudiation of Transactions)** จากการรับรองโดยค่า $h(ID_m, LP_c, C_{min}, Y_i)$ ที่ธนาคารไม่สามารถปฏิเสธได้ว่าไม่ได้เป็นคนออกข้อความ $\{c_0, C_{mer}, h(ID_m, LP_c, C_{min}, Y_i)\}_{Zj}$ เพราะมีเพียงธนาคารเท่านั้นที่รู้ทั้ง Z_j และ Y_i
- **สิทธิในธุรกรรมการเงิน (Transaction Authorization)** สามารถรับรองโดยค่าของ X_i และ Z_j ที่แสดงว่าลูกค้าและธนาคารมีสิทธิ์ในการทำธุรกรรมการเงินกับผู้ให้บริการ

4.2 การแก้ปัญหาข้อถกเถียงระหว่างกัน (Dispute Resolution)

โปรโตคอลที่นำเสนอนั้นสามารถแก้ปัญหาข้อถกเถียงระหว่างคู่สนทนาทั้งทางตรงและทางอ้อมพิจารณาสมการ 12) เราสามารถพิสูทธิ์ได้ว่าธนาคารเป็นคนออกข้อความเพราะว่า $h(ID_m, C_{min}, Y_i)$ สามารถถอดโดยลูกค้าและธนาคารแต่ว่าลูกค้าไม่มี Z_j จึงเชื่อได้ว่าลูกค้าไม่ใช่คนออกข้อความ

12) **B → C:** $h(ID_m, C_{min}, Y_i)$

4.3 ความลับของข้อมูล (Private Information)

ในโปรโตคอลที่นำเสนอนั้นค่าของ c_0 และ c_j จะถูกส่งออกไปโดยการเข้ารหัสทำให้รักษาความลับข้อมูลได้ และค่า c_j เท่านั้นที่จะถูกส่งจากลูกค้าไปยังธนาคารโดยการเชื่อมต่อไร้สาย เพราะว่าธนาคารสามารถหาค่า c_0 จาก $c_o = h^n(c, TS_{CO})$ เมื่อ n เป็นค่า C_{min} ในปัจจุบัน แล้วภายหลังส่ง

c_0 ไปยังผู้ให้บริการ ดังสมการ 12) ดังนั้นความลับของจำนวนที่ร้องขอก็จะถูกปกปิด

4.4 กุญแจลับ (Secret Key)

โปรโตคอลที่นำเสนอนั้นมีรูปแบบการใช้กุญแจลับถึง 3 ชุดด้วยยกัน กล่าวคือ ค่าของ $\{X_{cm}, Y_{CM}, Z_{mB}\}$ จะถูกใช้ร่วมกันระหว่างการเชื่อมต่อในแต่ละสายโดยกุญแจลับเหล่านี้จะถูกใช้งานเป็นกุญแจเข้ารหัส (Encrypting Key) และเป็นกุญแจสำหรับฟังก์ชันคีย์แฮช (Keyed Hash Function) ซึ่งต้องมีการอัพเดท (Update) เป็นช่วงๆ หรือขึ้นอยู่กับการร้องขอของผู้ที่เกี่ยวข้อง เพื่อเป็นการลดจำนวนครั้งของกระบวนการในการกระจายกุญแจให้น้อยลงและเพิ่มระดับความปลอดภัย เมื่อเราได้ X_{cm}, Y_{CB}, และ Z_{MB} แล้ว และทำการกระจายกุญแจลับแล้วแต่ละฝ่ายสามารถใช้เทคนิคการกำเนิดกุญแจ (Key generation technique) เพื่อกำเนิดชุดกุญแจ X_i, Y_i และ Z_j เมื่อ $i, j = 1,..., n$ และใช้กุญแจชุดนี้ในธุรกรรมอิเล็กทรอนิกส์แทน

4.5 ความสัมพันธ์ที่น่าเชื่อถือระหว่างผู้เกี่ยวข้องต่างๆ (Trust Relationships among Engaging Parties)

ความน่าเชื่อถือของผู้เกี่ยวข้องต่างๆ จะถูกกำหนดให้เหมาะกับพฤติกรรม เช่น ลูกค้าจะเชื่อถือธนาคารในการปกปิดความลับของข้อมูลส่วนตัวของลูกค้า แต่ขณะเดียวกันธนาคารไม่สามารถโกหกหรือส่งข้อมูล การร้องขอที่ปลอมได้เพราะข้อมูลกำเนิดมาจากลูกค้าซึ่งไม่สามารถสร้างขึ้นโดยธนาคาร

4.6 ความถูกต้อง (Correctness)

ระบบจะทำการอนุญาตเฉพาะผู้ขับขี่และรถถูกต้องตามกฎหมายเท่านั้น ในการใช้งานเครือข่ายเพราะผู้ให้บริการสามารถตรวจสอบป้ายทะเบียนและใบอนุญาตขับขี่รถยนต์ที่ส่งจากรถยนต์มายัง RSU หากพบการทุจริต เช่น กำลังถูกอายัติโดยเจ้าพนักงานตำรวจ อาจส่งข้อมูลเหล่านี้ไปให้ตำรวจ

4.7 ความไม่สามารถปลอมแปลงได้ (Unforgeability)

ระบบการชำระเงินที่นำเสนอนั้นไม่สามารถปลอมแปลงได้มีเพียงธนาคารเท่านั้นที่เป็นคนออกรายการและทำการชำระเงิน แต่ว่าธนาคารก็ไม่สามารถปลอมตัวเป็นลูกค้าได้

4.8 ความสามารถในการแบ่งแยกได้ (Separate Ability)

เนื่องจากระบบชำระเงินที่นำเสนอนั้นเป็นแบบระบบชำระเงินย่อยที่สามารถแบ่งจ่ายเป็นเหรียญจากมูลค่าคูปองตราใดก็ตามที่มูลค่าของเหรียญที่ถูกใช้ไปไม่เกินมูลค่าของคูปอง

4.9 การป้องกันการชำระซ้ำ (Double-spending proof)

ธนาคารสามารถตรวจสอบว่ามีการชำระเงินซ้ำหรือเปล่าจากค่า *TS* ที่บันทึกวันเวลาที่เกิดรายการธุรกรรมการเงิน

4.10 การป้องกันการจ่ายเงินเกิน (Over-Spending proof)

พิจารณาสมการ 13) เมื่อ $C_{min} = C_{max} - C_{mer}$ และจะคงค่าของ C_{min} นี้ไว้เพื่อป้องกันปัญหาจากการจ่ายเงินเกิน

4.11 เงื่อนไขการปกปิดความลับ (Conditional Anonymity)

พิจารณาโครงสร้างระบบที่นำเสนอซึ่งมีการติดต่อสื่อสารแบบ V2R เท่านั้น (ไม่มีโครงสร้างแบบ V2V) ทำให้มีเพียงลูกค้า ธนาคารและผู้ให้บริการเท่านั้นที่ติดต่อกัน ส่วนลูกค้าไม่สามารถติดต่อกับลูกค้าได้ตลอดจนการใช้กุญแจรหัสลับในการเข้ารหัสข้อมูลทั้งหมดจึงเป็นการรับรองการปกปิดความลับให้ลูกค้า

5. สรุปผลงานวิจัย

เครือข่าย VANET เป็นเครือข่ายไร้สายรูปแบบหนึ่งของเครือข่ายไร้สายเฉพาะกิจมีจุดประสงค์หลักเพื่อประยุกต์ใช้งานกับรถยนต์เพื่อความปลอดภัยบนท้องถนนและระบบขนส่งอัจฉริยะตลอดจนการนำไปประยุกต์ใช้งานเพื่อความบันเทิงต่างๆ การทำงานของระบบมีทั้งลักษณะ V2R และ V2V มาตรฐานที่นิยมใช้งานกันในปัจจุบัน คือ IEEE 802.11p 5.9 GHz DSRC และ IEEE 1609 WAVE การนำ VANET มาประยุกต์ใช้งานด้าน AETC จัดเป็นระบบหนึ่งของระบบ ITS ที่มีการทำงานในรูปแบบ V2R เท่านั้น ระบบ AETC ที่ออกแบบนั้นได้ทำการนำเสนอตั้งแต่ชั้นกายภาพ ชั้นการเชื่อมต่อ ชั้นการประยุกต์ใช้งาน

งานวิจัยฉบับนี้ได้นำเสนอระบบชำระเงินค่าผ่านทางด่วนที่เหมาะสมกับโครงสร้างของ VANET ในขณะที่ยังคงไว้ซึ่งความปลอดภัยของข้อมูลและในท้ายที่สุดได้นำเสนอการวิเคราะห์ความปลอดภัยของข้อมูลในรูปแบบต่างๆ

การประยุกต์ใช้ระบบ AETC ในอนาคตจะต้องมีการพิจารณาถึงพารามิเตอร์ต่างๆ เพื่อการใช้งานจริง เช่น การจัดสรรความถี่ในแต่ละประเทศ การลดผลกระทบของชั้นกายภาพให้น้อยที่สุด การปรับปรุงชั้น MAC การปรับปรุงระบบค้นหาเส้นทาง การพิจารณาวิศวกรรมจราจร (Traffic Engineering) และการปรับปรุงทางด้านความปลอดภัยของข้อมูล ตลอดจนการปรับปรุงรถยนต์เพื่อให้ทำงานกับ VANET ได้เหมาะสมมีประสิทธิภาพมากที่สุด จากเหตุผลดังที่ได้กล่าวมานี้ทำให้การวิจัยเครือข่าย VANET นั้นท้าทายความสามารถของผู้วิจัยจากทั่วโลก

เอกสารอ้างอิง

[1] IEEE Computer Society LAN MAN Standards Committee, *Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*, IEEE Std 802.11-1999. The Institute of Electrical and Electronics Engineers, 1999.

[2] D. Cottingham, I. Wassell, R. Harle, Performance of IEEE 802.11a in vehicular contexts, *Proceedings of Vehicular Technology Conference*, 2007, pp. 854–858.

[3] Maxim Raya *et al.*, "*Security Aspects of Inter-Vehicle Communication*", IC-LCA, EPFL Switzerland, 2005.

[4] J.T. Isaac *et al.*, "*A Secure Vehicle-To-Roadside Communication Payment Protocol In Vehicular Ad Hoc Networks*" Computer Communications Vol 31(10), June. 2008, pp. 2478-2484.

[5] K. Shin *et al.*, "A Practical Security Framework for a VANET-based Entertainment Service," *Proceedings of ACM PM2HW2N 09*, Oct. 2009, pp. 175-182.

[6] P. Papadimitratos *et al.*, "*Secure Vehicular Communication Systems: Design and Architecture*," IEEE Communications Magazine, vol. 46 (11), 2008, pp. 100-109.

[7] F. Kargl *et al.*, "*Secure Vehicular Communications Systems: Implementation, Performance, and Research Challenges*," IEEE Communications Magazine, vol. 46(11), 2008, pp. 110-118.

[8] E. Schoch *et al.*, "*Communication Patterns in VANETs,*" IEEE Communications Magazine, vol. 46(11), 2008, pp. 119-125.

[9] G. Kounga *et al.*, "Generating CAauthenticated public keys in ad hoc networks," *Proceedings of ACM Mobicom 08*, May 2008.

[10] X. Lin *et al.*, "*TSVC: Efficient and Secure Vehicular Communications with Privacy Preserving*," IEEE Trans. Wireless Communications, vol. 7(12), 2008, pp. 4987- 4998.

[11] U. Lee *et al.*, "*Dissemination and Harvesting of Urban Data Using Vehicular Sensing Platforms*," IEEE Trans. Vehicular Technology, vol.58(2), 2009, pp. 882-901.

[12] U. Lee *et al.*, "FleaNet: A Virtual Market Place on Vehicular Networks," *Proceedings of IEEE V2VCOM*, Jul. 2006, pp. 1-8.

[13] K. Plößl and H. Federrath, "*A Privacy Aware And Efficient Security Infrastructure For Vehicular Ad Hoc Networks,*" Computer Standards & Interfaces Vol 30(6), Aug. 2008, pp. 390-397.

[14] J. Abad-Peiro *et al.*, *Designing A Generic Payment Service*, IBM Systems Journal 37(1), 1998, pp. 72–88.

[15] S. Kungpisdan, A Secure Account-Based Mobile Payment System Protocol, *Proceedings of International Conference on Information Technology: Coding and Computing (ITCC)*, 2004, pp. 35–39.