โพรโตคอลน้ำหนักเบาสำหรับการติดต่อสื่อสารไร้สายระยะสั้นที่มีสมบัติการพิสูจน์ทราบตัวจริงแบบสองทางที่มีพื้นฐานจากเซสชันคีย์ที่มีการใช้งานอย่างจำกัด

Lightweight Protocol for NFC Communications with Mutual Authentication Based on Limited-Used Session Keys

ชาลี ธรรมรัตน์[1] และ ศุภกร กังพิศดาร[2]

คณะวิทยาการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยเทคโนโลยีมหานคร

51 หมู่1 ถนนเชื่อมสัมพันธ์แขวงกระทุ่มรายเขตหนองจอกกรุงเทพ 10530

Emails: [1]chalee23@gmail.com, [2]supakorn@mut.ac.th

ABSTRACT – Nowadays, mobile phones are equipped with enhanced short-range communication functionality called Near Field Communication (or NFC for short). NFC requires no pairing between devices but suitable for small amount of data in very limited area. A number of researchers proposed authentication techniques for NFC communications but they still lack of necessary authentication, especially mutual authentication and security properties. This paper introduces a new authentication protocols for NFC communication that provides mutual authentication between devices. Mutual authentication is a property of security that prevents replay and man-in-the-middle attack. The proposed protocols deploy a limited-use offline session key generation and use of distribution technique to enhance security and make our protocol lightweight.

KEY WORDS -- Cryptographic protocols; NFC; Near Field Communications; Security Protocols; Mutual Authentication Protocol; Network Security

บทคัดย่อ -- ปัจจุบันโทรศัพท์มือถือถูกพัฒนาให้มีความสามารถเพิ่มขึ้นและหนึ่งในความสามารถคือ NFC (Near field communication) ซึ่งเป็นการติดต่อสื่อสารไร้สายระยะสั้น ไม่มีขั้นตอนในการจับคู่อุปกรณ์ (Pairing) สามารถรับส่งข้อมูลในปริมาณไม่มากและระยะทางในการรับส่งมีระยะทางจำกัด เพื่อเน้นความรวดเร็วในการติดต่อสื่อสารเป็นหลักจึงทำให้ไม่มีการพิสูจน์ทราบตัวจริง มีงานวิจัยจำนวนมากได้นำเสนอการพิสูจน์ทราบตัวจริงของ NFC แต่อย่างไรก็ตามงานวิจัยที่ได้นำเสนอยังขาดความมั่นคงปลอดภัยในการพิสูจน์ทราบตัวจริง งานวิจัยฉบับนี้ได้นำเสนอการพิสูจน์ทราบตัวจริงที่มีความมั่นคงปลอดภัยและได้นำการสร้างเซสชันคีย์แบบออฟไลน์มาใช้งานซึ่งไม่มีการส่งเซสชันคีย์ผ่านเครือข่าย ทำให้มีความมั่นคงปลอดภัยที่เพิ่มขึ้นและโพรโทคอลที่นำเสนอยังส่งข้อความที่มีจำนวนข้อความน้อยทำให้มีประสิทธิภาพและใช้เวลาน้อย

คำ สำ คัญ --โพรโทคอลการเข้ารหัสลับ; NFC; Near field communication; โพรโทคอลความมั่นคงปลอดภัย; โพรโทคอลการพิสูจน์ทราบตัวจริงแบบสองทาง; ความมั่นคงปลอดภัยของเครือข่าย

1. บทนำ

อุปกรณ์สื่อสารไร้สายปัจจุบันได้นำ NFC มาเป็นอุปกรณ์เสริมทำให้มีความสะดวก NFC สามารถรับส่งข้อมูลในปริมาณไม่มากและระยะทางในการรับส่งข้อมูลมีระยะทางจำกัด เพื่อเน้นความรวดเร็วในการติดต่อสื่อสารเป็นหลักจึงทำให้ไม่มีการพิสูจน์ทราบตัวจริง นอกจากนี้ NFC ยังไม่มีการเข้ารหัสลับข้อมูลที่รับส่งในการทำงานระดับฮาร์ดแวร์ซึ่งทำให้ไม่มีความมั่นคงปลอดภัยเช่น การปลอมตัวทำธุรกรรมหรือการขโมยข้อมูล มีงานวิจัยจำนวนมากได้นำเสนอการพิสูจน์ทราบตัวจริงของ NFC โดย Lee *et al.* [7] ได้นำเสนอการพิสูจน์ทราบตัวจริงโดยใช้ NFC ในการติดต่อสื่อสารประกอบด้วย 3 ฝ่ายคือ *U1* (Mobile *U1*) คือ อุปกรณ์ที่ใช้พิสูจน์ทราบตัวจริง *U2* (Mobile *U2*) คืออุปกรณ์ที่เป็นตัวกลางในการพิสูจน์ทราบตัวจริงกับ *AuC* (Authentication Center) คือ ศูนย์กลางการพิสูจน์ทราบตัวจริง ซึ่งงานวิจัยดังกล่าวได้นำการเข้ารหัสลับแบบอสมมาตรและฟังก์ชันแฮช ซึ่งแบ่งได้ 2 โพรโทคอล คือ โพรโทคอลการพิสูจน์ทราบตัวจริง (Authentication Protocol) และโพรโทคอลการลงทะเบียน (Registration Protocol) งานวิจัยที่น่าสนใจอีกงานได้แก่งานวิจัยของ Ceipidor *et al.* [11] นำเสนอการพิสูจน์ทราบตัวจริงระหว่าง NFC กับจุดขายสินค้าซึ่งประกอบด้วย 3 ฝ่ายได้แก่ *POS* (Point of Sale) คือจุดขาย *N* (NFC Phone) คืออุปกรณ์สื่อสารไร้สายที่มี NFC และ *AS* (Authentication Server) คือผู้ให้บริการที่ใช้ในการพิสูจน์ทราบตัวจริงของ *N* ผ่าน *POS* โดยใช้การเข้ารหัสลับแบบสมมาตรและแฮชฟังก์ชัน โพรโทคอลนี้มีคุณสมบัติความมั่งคงปลอดภัยเช่น การพิสูจน์ทราบตัวจริงและการรักษาความรับของข้อมูล

อย่างไรก็ตามงานวิจัยจำนวนมากที่ได้นำเสนอก็ยังไม่มีความมั่นคงปลอดภัยในการพิสูจน์ทราบตัวจริงและคุณสมบัติความมั่งคงปลอดภัยเพียงพอ งานวิจัยฉบับนี้ได้นำเสนอโพรโทคอลสำหรับการพิสูจน์ทราบตัวจริงและได้นำการสร้างเซสชันคีย์แบบออฟไลน์มาใช้งานทำให้มีความมั่นคงปลอดภัยที่เพิ่มขึ้น

โครงสร้างของงานวิจัยฉบับนี้มีดังต่อไปนี้ หัวข้อที่ 2 กล่าวถึงทฤษฎีและหลักการที่เกี่ยวข้องกับงานวิจัย หัวข้อที่ 3 กล่าวถึงโพรโทคอลที่นาเสนอ หัวข้อที่ 4 การวิเคราะห์ความมั่นคงปลอดภัย หัวข้อที่ 5 การวิเคราะห์ประสิทธิภาพของโพรโทคอลและการอภิปราย และหัวข้อที่ 6 สรุปการวิจัย

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้องกับงานวิจัย

2.1 Near field communication

NFC (Near Field Communication) [8-10, 16, 18, 19] เป็นเทคโนโลยีการสื่อสารไร้สายผ่านคลื่นวิทยุ ที่ความถี่ 13.56 MHz ใช้ส่งข้อมูลได้ในระยะไม่เกิน 10 ซ.ม. มีความเร็วในการรับส่งข้อมูลได้สูงสุด 424 kbit/s สามารถจับคู่อุปกรณ์ได้อย่างรวดเร็วและใช้พลังงานต่ำ จากข้อดีดังกล่าว NFC จึงถูกนำมาใช้ในการรับส่งข้อมูลปริมาณเล็กน้อยภายในระยะเวลาสั้นๆ ดังนั้นอุปกรณ์ที่สามารถใช้งาน NFC ได้สะดวก จะเป็นอุปกรณ์พกพา เช่น โทรศัพท์มือถือหรือแท็บเล็ต ลักษณะการทำงานของ NFC จึงใกล้เคียงกับ RFID ความแตกต่างหลักๆ ของ NFC กับ RFID คือ NFC สามารถแลกเปลี่ยนข้อมูลระหว่าง NFC ด้วยกันได้ ซึ่งใน RFID นั้นสามารถอ่านข้อมูลได้อย่างเดียว แต่ระยะการทำงานของ NFC นั้นสั้นกว่า RFID มาก การทำงานของ NFC มีด้วยกัน 3 โหมดได้แก่ [16, 18]

1. Reader/Writer mode ในโหมดนี้ NFC ทำงานเป็น RFID การ์ด (RFID Tag) ในอุปกรณ์มือถือ ในโหมดนี้จะทำงานเสมือนเป็นบัตร Contactless ตามมาตรฐาน ISO 14443 และ FeliCa เช่น Contactless Smart Card ใช้ในการทำธุรกรรม โทรศัพท์มือถือที่มีเครื่องอ่าน NFC สามารถทำงานเป็น RFID Tag ได้ เช่นการจ่ายเงินชำระค่าผ่านทาง การจ่ายเงินตาม POS ต่าง ๆ แทนการชำระเงินด้วยบัตร RFID หรือเงินสด

2. Card emulation mode ในโหมดนี้ NFC ทำงานเป็นเครื่องอ่าน RFID อุปกรณ์มือถือ เช่นโทรศัพท์มือถือที่มีเครื่องอ่าน NFC ฝังอยู่ สามารถทำงานเป็นเครื่องอ่าน RFID เมื่อต้องการอ่านข้อมูลจาก RFID การ์ด (RFID Tag) ใน โหมดนี้อุปกรณ์ NFC สามารถทำตัวเสมือนเป็นเครื่องอ่านเขียน Contactless Smart Card (หรือบางครั้งเรียกว่า Tag) โดยจะสามารถอ่านข้อมูลจาก Tag ที่ติดอยู่ใน Smart Poster หรือจุดให้บริการข้อมูล

3. Peer to Peer (P2P) เป็นโหมดที่อุปกรณ์ NFC สองเครื่องสามารถที่จะติดต่อ สื่อสารกันโดยตรงได้ โหมดนี้จะทำการแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์ NFC ด้วยกัน เช่น นามบัตร รูปถ่าย แฟ้มข้อมูล การแลกเปลี่ยนข้อมูลกระทำผ่านโปรโตคอล TCP/IP หรือ OBEX นอกจากแลกเปลี่ยนข้อมูลแล้วยังสามารถใช้ทาการ Synchronize ข้อมูลกับอุปกรณ์อื่นๆ ได้

2.2 NFC based Authentication method for defense of the Man in the Middle Attack

Lee *et al.* [7] ได้นำเสนอการพิสูจน์ทราบตัวจริงโดยใช้ NFC ในการติดต่อสื่อสารประกอบด้วย 3 ฝ่ายคือ *U1* (Mobile *U1*) คือ อุปกรณ์ที่ใช้พิสูจน์ทราบตัวจริง *U2* (Mobile *U2*) คือ อุปกรณ์ที่เป็นตัวกลางในการพิสูจน์ทราบตัวจริงกับ *AuC* (Authentication Center) คือ ศูนย์กลางการพิสูจน์ทราบตัวจริง ซึ่งงานวิจัยดังกล่าวได้นำการเข้ารหัสลับแบบอสมาตรและฟังก์ชันแฮชมาใช้งาน ซึ่งแบ่งได้ 2 โพรโทคอล คือ โพรโทคอลการลงทะเบียน (Registration Protocol) และ โพรโทคอลการพิสูจน์ตัวจริง (Authentication Protocol) อธิบายรายละเอียดได้ดังข้างล่าง

2.2.1 โพรโทคอลการลงทะเบียน (Registration Protocol)

M1:Ux→AuC: *UIDx, Password, User Information*
M2:AuC→Ux: *h(UID, h(URx))*

M1: ก่อนที *U1* พิสูจน์ทราบตัวจริงกับ *AuC U1* จะต้องทำการลงทะเบียนกับ *AuC* ก่อน โดย *U1* จะส่ง *UIDx, Password* และ User Information ไปยัง *AuC* โดยที่ *UIDx* คือหมายเลขระบุตัวตนของอุปกรณ์มือถือ

M2: หลังจากนั้นเมื่อ *AuC* ได้รับขอความจาก *Ux Auc* จะนำ *UID* และ ค่าแฮชของ *x* ส่งกลับไปยัง *Ux* โดยที่ *URx* คือหมายเลขรหัสลับการพิสูจน์ทราบตัวจริง

2.2.2 โพรโทคอลการพิสูจน์ตัวจริง (Authentication Protocol)

M1:U1→U2: *Q1*
M2:U2→AuC: *UID2, Q2*
M3:AuC→U2: *R1, R2, R3*
M4:U2→U1: *h(UID1, n2) xor n2, n1 xor n2*
M5:U1→U2: *h(n1, n2, UID1)*

M1: เมื่อ *U1* ต้องการพิสูจน์ทราบตัวจริงกับ *AuC U1* นำ *UID1* และเข้ารหัสลับ *UID1, URx1* และ *n1* ด้วยกุญแจสาธารณะของ *AuC* แล้วส่งให้ *U2* โดยที่ *n* คือ ค่านอนซ์ (Nonce) สำหรับการป้องกันการโจมตีแบบรีเพลย์ (Replay Attack) $Q1 = UID1, \{UID1, URx1, n1\}_{EpukAuC}$

M2: *U2* ได้รับข้อความจาก *U1* *U2* นำ *UID2* ข้อความที่เข้ารหัสลับจาก *U1* และเข้ารหัสลับ *UID1, n2, UID2, URx2* ด้วยกุญแจสาธารณะของ *AuC* หลังจากนั้นส่งไปให้ *AuC* โดยที่ $Q2 = \{Q1, UID1, n2, UID2, URx2\}_{EpukAuC}$

M3: เมื่อ *AuC* ได้รับข้อความจาก *U2* *AuC* นำกุญแจส่วนตัวของตัวเองมาถอดรหัสลับข้อความ แล้วทำการตรวจสอบแล้วสร้างค่า *R1, R2* และ *R3* ส่งกลับไปยัง *U2* โดยที่ *R1 = h(UID1, n2) xor n2, R2 = h(UID2, n2, n2) xor n1, R3 = n1 xor n2*

M4: *U2* นำข้อความที่ได้จาก *AuC* นำ *R2* โดยใช้ *UID2* มาจรวจสอบถ้าถูกต้องก็จะทำการส่ง *R1* และ *R3* ไปยัง *U1*

M5: *U1* นำ *R1* โดยใช้ *UID1* ตรวจสอบถ้าถูกต้องก็จะทำการส่งค่าแฮชของ *n1, n2* และ *UID1* ไปให้กับ *U2*

งานวิจัยดังกล่าวได้อ้างว่าโพรโทคอลที่ได้นำเสนอสามารถต้านทานโจมตีแบบรีเพลย์ (Replay Attack) การโจมตีชนิดคนกลาง (Man in the middle attack) และการพิสูจน์ทราบตัวจริง(Authentication) แต่อย่างไรก็ตามงานวิจัยดังกล่าวยังขาดคุณสมบัติความมั่นคงปลอดภัยเช่น การพิสูจน์ทราบตัวจริงของผู้รับข้อความ การตรวจสอบความถูกต้องของข้อความและการพิสูจน์ทราบตัวจริงของข้อความ

2.3 A protocol for mutual authentication between NFC phones and POS terminals for secure payment transactions

Ceipidor *et al.* [11] นำเสนอการพิสูจน์ทราบตัวจริงระหว่าง NFC กับจุดขายซึ่งประกอบด้วย 3 ฝ่ายได้แก่ *POS* (Point of Sale) คือจุดขาย *N* (NFC Phone) คืออุปกรณ์สื่อสารไร้สายที่มี NFC และ *AS* (Authentication Server) คือผู้ให้บริการที่ใช้ในการพิสูจน์ทราบตัวจริงของ *N* และ *POS* ซึ่งประกอบด้วย 7 ขั้นตอน อธิบายรายละเอียดของแต้ละขั้นตอนได้ดังนี้

M1:POS→N: $\{R1, TS\}_{KP}$
M2:N→POS: $IDN, \{R2, \{R1, TS\}KP\}_{KN}$
M3:POS→AS: $IDP, IDN, \{R2, \{R1, TS\}_{KP}\}_{KN}$
M4:AS→POS: $\{K, IDN, TS\}_{KP}, \{K, IDP, R2\}_{KN}$
M5:POS→N: $\{K, IDP, R2\}_{KN}, \{R3\}_{K}$
M6:N→POS: $\{R3\text{-}1, R4\}_{K}$

M7:POS→N: $\{R4\text{-}1\}_K$

M1: Authentication request *POS* นำค่าสุ่ม *R1* และ *TS* มาเข้ารหัสลับด้วยเซสชันคีย์ *KP* ที่ใช้งานร่วมกันระหว่าง *POS* และ AS หลังจากนั้นส่งให้ *N* โดยที่ *TS* คือเวลาที่ร้องขอพิสูจน์ทราบตัวจริง

M2: Request confirmation เมื่อ *N* ได้รับข้อความจาก *POS N* ทำการนำ *IDN* ค่าสุ่ม *R2* และข้อความที่ได้จาก *POS* มาเข้ารหัสลับด้วยเซสชันคีย์ *KN* ที่ใช้งานร่วมกันระหว่าง *POS* และ *AS* แล้วส่งให้กับ *AS*

M3: Session request หลังจากที่ *POS* ได้รับข้อความจาก *N POS* นำ *IDP* และข้อความที่ได้รับจาก *N* แล้วส่งให้ *AS*

M4: Session confirmation เมื่อ *AS* ได้รับข้อความจาก *POS AS* ก็จะทำการสร้างเซสชันคีย์ *K* แล้วนำ *K, IDN* และ *TS* เข้ารหัสลับด้วยเซสชันคีย์ *KP* และนำ *K, IDP* และ *R2* มาเข้ารหัสลับด้วยเซสชันคีย์ *KN* แล้วส่งกลับไปยัง *POS*

M5: Verify request *POS* นำข้อความที่ได้รับจาก *AS* มาถอดรหัสลับด้วยเซสชันคีย์ *KP* แล้วนำ *TS* มาเปรียบเทียบถ้าตรงกัน *POS* ก็ทำการสร้างค่าสุ่ม *R3* มาเข้ารหัสลับด้วยเซสชันคีย์ *K* และนำ $\{K, IDP, R2\}_{KN}$ ส่งไปยัง *N*

M6: Verify confirmation from NFC phone เมื่อ *N* ได้รับข้อความจาก *POS* N นำข้อความ $\{K, IDP, R2\}_{KN}$ มาถอดรหัสลับด้วยเซสชันคีย์ *KN* แล้วนำเซสชันคีย์ *K* มาถอดรหัสลับ $\{R3\}_K$ ถ้าการถอดรหัสลับสมบูรณ์ *N* ก็จะนำ *R3-1* และค่าสุ่ม R4 มาเข้ารหัสลับด้วยเซสชันคีย์ *K* แล้วส่งให้ *POS*

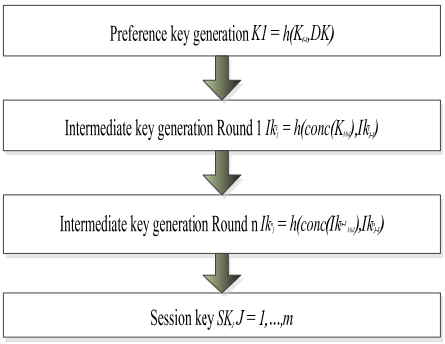
M7: Verify confirmation from POS POS นำข้อความที่ได้รับจาก *N* มาถอดรหัสลับด้วยเซสชันคีย์ *K* แล้วนำ *R4* มาตรวจสอบ ถ้าตรงกันก็จะการสิ้นสุดการพิสูจน์ทราบตัวจริง

จากรายละเอียดของโพรโทคอลการพิสูจน์ทราบตัวจริงที่ผู้วิจัยได้นำเสนอมีคุณสมบัติความมั่งคงปลอดภัยเช่น การพิสูจน์ทราบตัวจริงและการรักษาความลับของข้อความ แต่อย่างไรก็ตามเมื่อพิจารณารายละเอียดของโพโทคอลของงานวิจัยดังกล่าวพบว่ายังขาดคุณสมบัติด้านความมั่งคงปลอดภัยเช่น การตรวจสอบความถูกต้องของข้อความและการพิสูจน์ทราบตัวจริงของข้อความ นอกจากนี้เซสชันคีย์ *KN* และเซสชันคีย์ *KP* เป็นเซสชันคีย์ตัวเดิมตลอดไม่เปลี่ยนแปลงอาจถูกโจมตีแบบ Brute Force Attack เพื่อค้นหาคีย์ที่ถูกต้องได้ และงานวิจัยดังกล่าวยังมีการส่งคีย์ผ่านเครือข่ายทำให้ไม่มีความมั่นคงปลอดภัย

2.4 A Secure Offline key Generation with Protection Against key Compromise

Kungpisdan *et al.* ได้นำเสนอวิธีการสร้างและกระจายเซสชันคีย์แบบออฟไลน์ ซึ่งมีการสร้างและกระจายเซสชันคีย์โดยที่ไม่ต้องมีการส่งเซสชันคีย์ดังกล่าวผ่านเครือข่าย [1] ซึ่งมีจุดเด่นเหนือเทคนิคการกระจายเซสชันคีย์แบบออนไลน์ โดยเทคนิคการสร้างและกระจายเซสชันคีย์แบบต่างๆ ถูกเสนอเสนอ [2, 3, 4, 5, 6] โดยที่ Kungpisdan *et al.* ได้แนะนำเทคนิคการสร้างเซสชันคีย์ที่ไม่เพียงแต่มีความปลอดภัยจากการโจมตีเท่านั้น แต่ยังสามารถทำงานได้แบบออฟไลน์ รายละเอียดของวิธีการดังกล่าวมีดังนี้

ก่อนการสร้างเซสชันคีย์จะต้องดำเนินการแลกเปลี่ยนค่า $\{K_{AB}, D_K, m\}$ สมมติว่าเป็นการแลกเปลี่ยนโดยอลิสและบ๊อบ ซึ่งกำหนดให้ K_{AB} เรียกว่า Long-term key, D_K เรียกว่า Distribution key และ *m* คือค่าสุ่มที่ระบุจำนวนของเซสชันคีย์ที่ต้องการสร้างขึ้น โดยขั้นตอนการสร้างเซสชันคีย์ สามารถอธิบายได้ดังรูปที่ 1 ดังนี้



รูปที่ 1. ขั้นตอนการสร้างเซสชันคีย์

หลังจากมีแลกเปลี่ยนค่า $\{K_{AB}, D_K, m\}$ อลิสและบ๊อบ จะสร้างเซ็ตของ Preference keys K_i, i = 1,2,…, m ดังสมการ

$$K_i = h(K_{i-1}, D_K) \qquad (2.1)$$

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 $IK^{x}_{mid1} = mid(IK^{x}_{1}, IK^{x}_{rm})$ โดยที่ rm คือจำนวนของ Intermediate key ที่ยังเหลืออยู่ในชุดข้อมูลของ IK^{x}_{j} , $IK^{x}_{mid2} = mid(IK^{x}_{mid1}, IK^{x}_{rm})$, $IK^{x}_{mid3} = mid(IK^{x}_{1}, IK^{x}_{mid2})$, $IK^{1}_{mid1} = K^{mid}_{1}$, $IK^{1}_{mid2} = K^{mid}_{2}$, $IK^{1}_{mid3} = K^{mid}_{3}$ และ $IK_{xj-1} = \Phi$ การใช้ Intermediate Keys ในทุกๆรอบ จะทำการลบค่าออกจากระบบ ส่วนที่เหลือของ Intermediate Keys ในรอบอื่นๆ สามารถเขียนได้ดังนี้

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

ผลที่ได้ในรอบสุดท้ายของ Intermediate Keys ที่ได้จะถูกใช้เป็นเซสชันคีย์ (Session key) (*SKj*) โดยที่ j = 1,… ,m คือ

$$IK^{n}_{1} = SK_1, IK^{n}_{2} = SK_2, \ldots, IK^{n}_{m} = SK_m \quad (2.3)$$

จากเทคนิคนี้จะเห็นว่าจะมีการส่งเพียงค่าตัวแปร ที่เป็นค่าเริ่มต้นเพื่อนำไปใช้ในการสร้างเซสชันคีย์และเซสชันคีย์ที่ถูกสร้างขึ้น ถูกนำมาใช้เพียงครั้งเดียวไม่มีการนำมาใช้ซ้ำและการสร้างเซสชันคีย์โอกาสเกิดค่าเซสชันคีย์ที่ซ้ำเป็นไปได้ยาก

2.5 การเปรียบเทียบ NFC กับเทคโนโลยีที่มีอยู่

Timalsina *et al.* [12] ได้นำเสนอการเปรียบเทียบ NFC กับเทคโนโลยี Bluetooth V2.1 และ IrDA จากตารางที่ 1 NFC มีความถี่น้อยกว่า Bluetooth V2.1 และ IrDA ระยะการส่งข้อมูลของ NFC มีระยะน้อยกว่า V2.1 และ IrDA ข้อมูลที่ NFC ส่งส่งได้น้อยกว่า V2.1 และ IrDA เวลาในการ Setup Time ใช้เวลาน้อยกว่า V2.1 และ IrDA อย่างไรก็ตามเนื่องจาก NFC นั้นเน้นความรวดเร็วในการติดต่อสื่อสารเป็นหลัก ดังนั้นการรับส่งได้นั้นจะทำได้ในปริมาณไม่มากและระยะทางในการทำงานนั้นมีจำกัด

ตารางที่ 1. การเปรียบเทียบ NFC กับ Bluetooth V2.1 และ IrDA

	NFC	Bluetooth V2.1	IrDA
Information transmission	Coupling of magnetic field	Electromagnetic radiation	Infrared light
Operating frequency	13.56 MHz	2.4 GHz	~ 2MHz?
Modes	Active-active, active-passive	Active-active	Active-active
Transmission range	0.04 – 0.1 m	10 – 100 m	0 – 2 m
Network type	P2P	WPAN	P2P
Maximum data rate	424 kbps	2.1 Mbps	16 Mbps
Setup time	< 0.1s	~6s	~0.5s
Maximum current consumption	< 15mA	< 30mA	< 5mA
Line of sight	Yes	No	Yes
Authentication and encryption	Yes	Yes	No
Cost of device	Low	Moderate	Low

2.6 ช่องโหว่ของ NFC

งานวิจัยจำนวนมาก [12-15, 17, 18, 20-22] ได้นำเสนอช่องโหว่ของ NFC เนื่องจาก NFC เน้นความรวดเร็วในการติดต่อสื่อสารเป็นหลักจึงทำให้ไม่มีการยืนยันตัวตนที่ดีพอ นอกจากนี้ NFC ยังไม่มีการเข้ารหัสลับข้อมูลที่รับส่งในการทำงานระดับฮาร์ดแวร์ จึงทำให้เกิดปัญหาภัยคุกคาม เช่น

1. การดักรับข้อมูล (Eavesdropping)

ผู้ไม่หวังดีใช้เสาอากาศที่เหมาะสมเพื่อดักรับข้อมูลที่รับส่งให้ไกลขึ้นระหว่าง NFC เพราะ NFC ไม่มีกลไกในการป้องกันดักรับข้อมูล [17, 18, 20-22]

2. การแก้ไขข้อมูล (Data Manipulation)

ผู้ไม่หวังดีดักรับข้อมูลแล้วแก้ไขข้อมูลระหว่างทางให้มีความผิดพลาด การโจมตีนี้สามารถแบ่งออกเป็น 3 ประเภทดังนี้ [17, 18, 20-22]

- Data Alteration: ผู้โจมตีจะส่งข้อมูลที่ถูกต้อง แต่มีการปรับเปลี่ยนไปยังผู้รับ
- Data Insertion: ผู้โจมตีแทรกข้อมูลภายในช่วงเวลาสั้น ๆ ก่อนที่จะตอบรับไปส่ง
- Data Destruction: ผู้โจมตีขัดจังหวะหรือบล็อกข้อมูลที่ส่งทำให้ผู้รับ ทำให้ไม่สามารถอ่านข้อมูลได้หรือเรียกว่า DoS attack

3. การส่งข้อมูลซ้ำ (Relay Attack)

ผู้โจมตีรับสัญญาณจากผู้ส่งและแก้ไขหรือเปลี่ยนแปลงข้อมูลแล้วส่งไปยังผู้รับ ซึ่งเป็นการโจมตีในลักษณะคล้ายกับการโจมตีแบบคนกลาง (man in the middle attack) [20, 21]

3. โพรโทคอลที่นาเสนอ

เพื่อเป็นการแก้ไขปัญหาและข้อจำกัดของงานวิจัยที่มีอยู่ งานวิจัยฉบับนี้นำเสนอโพรโทคอลใหม่สำหรับการพิสูจน์ตัวจริงสองทางที่มีความมั่นคงปลอดภัยโดยนำเอาเทคนิคการสร้างและการกระจายเซสชันคีย์แบบออฟไลน์มาใช้งานทำให้โพรโทคอลมีความมั่นคงปลอดภัยเพิ่มขึ้น

3.1 นิยามและสมมติฐาน

ผู้ใช้งานโทรศัพท์มือถือ (NFC Phone หรือ *N*) คือ ผู้ใช้งานโทรศัพท์มือถือที่พิสูจน์ตัวทราบจริงกับเซิร์ฟเวอร์พิสูจน์ตัวทราบจริง Authentication Server (*AS*) คือ เซิร์ฟเวอร์ที่ใช้พิสูจน์ตัวทราบจริง โดยที่ผู้ใช้งานโทรศัพท์มือถือต้องติดตั้งซอฟต์แวร์ที่นำเสนอ

- $SK_{A\text{-}Bj}$ โดยที่ j = 1 ถึง *m* คือ เซสชันคีย์ใช้ร่วมกันระหว่าง *A* กับ *B*
- ID_A คือสิ่งที่ระบุว่าเป็น *A*
- $\{m\}_{SK}$ เป็นการเข้ารหัสสมมาตรของข้อความ *m* ด้วยเซสชันคีย์ *SK*
- *h(m)* คือค่าแฮชของข้อความ *m*
- *h(m, K)* เป็นรหัสพิสูจน์ตัวจริงข้อความ (MAC หรือ Message Authentication Code) ของข้อความ *m* ด้วยค่าเซสชันคีย์ *K*
- *n* คือ ค่านอนซ์ (Nonce) สำหรับการป้องกันการโจมตีแบบรีเพลย์ (Replay Attack)

3.2 การลงทะเบียน

อุปกรณ์มือถือต้องติดตั้งซอฟต์แวร์ตามโพรโทคอลที่นำเสนอ ผู้ใช้งานโทรศัพท์มือถือต้องเข้าสู่ระบบการลงทะเบียน ซึ่งการลงทะเบียนดำเนินการผ่านช่องทางที่มั่นคงปลอดภัย เช่น TLS (Transaction Layer Security) วัตถุประสงค์ของการลงทะเบียน คือ การแลกเปลี่ยน $\{K_{AB}, DK_{AB}, m_{AB}\}$ ระหว่างโทรศัพท์มือถือกับเซิร์ฟเวอร์ที่ใช้พิสูจน์ตัวทราบจริง ซึ่งหลังจากการแลกเปลี่ยน $\{K_{N\text{-}AS}, DK_{N\text{-}AS}, m_{N\text{-}AS}\}$ กัน ทั้งโทรศัพท์มือถือกับเซิร์ฟเวอร์พิสูจน์ตัวทราบจริง สามารถสร้างเซสชันคีย์ $SK_{N\text{-}ASj}$ เมื่อ j = 1 ถึง m โดยใช้เทคนิคการสร้างเซสชันคีย์ที่แสดงในส่วน 2.4 และแลกเปลี่ยน $\{K_{N\text{-}POS}, DK_{N\text{-}POS}, m_{N\text{-}POS}\}$ กัน ทั้งโทรศัพท์มือถือ *POS* สามารถสร้างเซสชันคีย์ $SK_{N\text{-}POSj}$ เมื่อ j = 1 ถึง m โดยใช้เทคนิคการสร้างเซสชันคีย์ที่แสดงในส่วน 2.4 ส่วนการแลกเปลี่ยนเซสชันคีย์ระหว่าง *POS* และ *AS* กระทำในขั้นตอนการสร้างระบบผ่านช่องทางที่มั่นคงปลอดภัย ได้เซสชันคีย์ $SK_{POS\text{-}ASj}$ เมื่อ j = 1 ถึง m

3.3 การพิสูจน์ทราบตัวจริงระหว่าง NFC Phone กับ NFC Reader (NFCAuthV1)

เป็นการพิสูจน์ตัวจริงระหว่าง NFC Phone กับ NFC Reader ก่อนที่ *N* จะใช้งานระบบ *N* จำเป็นต้องทำการพิสูจน์ทราบตัวจริงกับ *AS* ก่อนโดย *N* ส่งข้อความดังนี้

M1:N→AS: ID_N, *Authen*, n_1

M2:AS→N: n_2, $h(ID_N, n_1, n_2, SK_{N\text{-}ASj})$

M3:N→AS: n_3, $h(ID_N, n_1, n_2, n_3, SK_{N\text{-}ASj+1})$

M4:AS→N: *Accept/Reject*, n_4, $h(Accept, ID_N, n_1, n_2, n_3, SK_{N\text{-}ASj+1})$ *หรือ*

M4:AS→N : *Reject*

M1: *N* ส่ง ID_N พร้อมทั้งข้อความ *Authen* เป็นข้อความร้องขอการพิสูจน์ทราบตัวจริงของ *N* ซึ่ง *N* เป็นคนสร้างและค่านอนซ์ n_1 ซึ่งได้จากค่าสุ่มตัวอักษรแล้วส่งไปยัง *AS*

M2: เมื่อ *AS* ได้รับข้อความจาก *N* *AS* ก็จะทำการตรวจสอบ ID_N ว่าได้รับอนุญาตหรือไม่ ถ้าไม่ได้รับอนุญาตการติดต่อสื่อสารจะสิ้นสุดทันที แต่ถ้าได้รับอนุญาต *AS* ทำการสร้างค่านอนซ์ n_2 นำค่านอนซ์ n_1 และ n_2 พร้อมด้วย $SK_{N\text{-}ASj}$ ซึ่งเป็นเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *AS* และ *N* มาเข้าฟังก์ชันแฮชแล้วนำข้อความย่อยและค่านอนซ์ n_2 ส่งไปยัง *N*

M3: หลังจาก *N* ได้รับข้อความจาก *AS N* นำค่านอนซ์ n_1 และ n_2 พร้อมด้วยเซสชันคีย์ $SK_{N\text{-}ASj}$ มาเข้าฟังก์ชันแฮชแล้วนำมาเปรียบเทียบกับค่าแฮชที่ *AS* ส่งมาถ้าไม่ตรงกันการติดต่อสื่อสารจะสิ้นสุดทันที แต่ถ้าตรงกัน *N* ทำการสร้างค่านอนซ์ n_3 และนำ ID_N ค่านอนซ์ n_1, n_2 และ n_3 พร้อมด้วยเซสชันคีย์ $SK_{N\text{-}ASj+1}$ ตัวถัดไปมาเข้าฟังก์ชันแฮชแล้วนำข้อความย่อยและ n_3 ส่งไปยัง *AS*

M4: เมื่อ *AS* ได้รับข้อความจาก *N* *AS* ก็จะนำ ID_N ค่านอนซ์ n_1, n_2 และ n_3 พร้อมด้วยเซสชันคีย์ $SK_{N\text{-}ASj+1}$ ตัวถัดไปมาเข้าฟังก์ชันแฮชและนำมาเปรียบเทียบกับค่าแฮชของ *N* ที่ส่งมาถ้าไม่ตรงกัน *AS* ก็จะส่งข้อความ *Reject* กลับไปยัง *N* แต่ถ้าตรงกัน *AS* ทำการสร้างค่านอนซ์ n_4 และนำข้อความ *Accept*, ID_N ค่านอนซ์ n_1, n_2, n_3 และ n_4 ตัวถัดไปมาเข้าฟังก์ชันแฮชแล้วนำข้อความย่อยข้อความ *Accept* และค่านอนซ์ n_4 ส่งไปยัง *N* เป็นการสิ้นสุดการพิสูจน์ทราบตัวจริงระหว่าง *N* กับ *AS*

3.4 การพิสูจน์ทราบตัวจริงระหว่าง NFC Phone กับ Authentication Server ผ่าน POS (NFCAuthV2)

ในส่วนนี้เป็นการการพิสูจน์ทราบตัวจริงระหว่าง NFC Phone กับ Authentication Server ผ่าน *POS*

M1:N→POS: ID_N, n_1, $\{\{Authen, T_1\}_{SKN\text{-}ASj}, n_1\}_{SKN\text{-}POSj}$, $h(Authen, n_1, SK_{N\text{-}POSj})$, $h(Authen, T_1, ID_N, SK_{N\text{-}ASj})$

M2:POS→AS: ID_N, ID_{POS}, $\{\{Authen, T_1\}_{SKN\text{-}ASj}\}_{SKPOS\text{-}ASj}$, $h(Authen, T_1, ID_N, SK_{N\text{-}ASj})$

M3:AS→POS: *Accept/Reject*, $\{\{Accept/Reject, T_1, T_2\}_{SKN\text{-}ASj+1}\}_{SKPOS\text{-}ASj+1}$, $h(Accept/Reject, SK_{POS\text{-}ASj+1})$, $h(Accep/Reject, T_1, T_2, SK_{N\text{-}ASj+1})$

M4:POS→N: *Accept/Reject*, n_2, $\{Accept/Reject, T_1, T_2\}_{SKN\text{-}ASj+1}$, $h(n_1, n_2, SK_{N\text{-}POSj+1})$, $h(Accept/Reject, T_1, T_2, SKN\text{-}ASj+1)$

M1: เมื่อ *N* ต้องการพิสูจน์ตัวจริงกับ *AS* *N* นำข้อความ Authen และ T_1 มาเข้ารหัสลับด้วยเซสชันคีย์ $SK_{N\text{-}ASj}$ ซึ่งเป็นเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *N* และ *AS* หลังจากนั้นนำมาเข้ารหัสลับด้วยเซสชันคีย์ $SK_{N\text{-}POSj}$ ซึ่งเป็นเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *N* และ *POS* แล้วนำค่าแฮชของข้อความ *Authen* ค่านอนซ์ n_1 และเซสชันคีย์ $SK_{N\text{-}POSj}$ และค่าแฮชของข้อความ *Authen*, T_1, ID_N และเซสชันคีย์ $SK_{N\text{-}ASj}$ แล้วนำ ID_N, n_1 ส่งไปยัง *POS* โดยที่ T_1 คือเวลาขณะร้องขอการพิสูจน์ทราบตัวจริง

M2: *POS* ได้รับข้อความจาก *N POS* นำข้อความ *Authen* และ T_1 ที่เข้ารหัสลับด้วยเซสชันคีย์ $SK_{N\text{-}ASj}$ มาเข้ารหัสลับด้วยเซสชันคีย์ $SK_{POS\text{-}ASj}$ ซึ่งเป็นเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *POS* และ *AS* และนำค่าแฮชของข้อความ *Authen*, T_1, ID_N และเซสชันคีย์ $SK_{N\text{-}ASj}$ พร้อมทั้ง ID_N และ ID_{POS} ส่งไปยัง *AS*

M3: หลังจาก *AS* ได้รับข้อความจาก *POS AS* ก็จะทำการตรวจสอบว่า *N* ได้รับอนุญาตเหรอไม่ ถ้าไม่ได้รับอนุญาตก็จะส่งข้อความ *Reject* แต่ถ้าไม่ได้รับอนุญาตก็จะส่งข้อความ *Accept* โดยนำข้อความ *Accept/Reject* และนำข้อความ *Accept/Reject*, T_1 และ T_2 มาเข้ารหัสลับด้วยเซสชันคีย์ $SK_{N\text{-}ASj+1}$ ตัวถัดไปแล้วนำมาเข้ารหัสลับอีกครั้งด้วยเซสชันคีย์ $SK_{POS\text{-}ASj+1}$ ตัวถัดไปและนำค่าแฮชข้อความ *Accept/Reject* และเซสชันคีย์ $SK_{POS\text{-}ASj+1}$ ตัวถัดไป แฮชข้อความ *Accept/Reject*, T_1, T_2 และเซสชันคีย์ $SK_{N\text{-}ASj+1}$ ตัวถัดไปส่งไปให้ *POS* โดยที่ T_2 คือเวลายืนยันการพิสูจน์ทราบตัวจริง

M4: เมื่อ *POS* ได้รับข้อความจาก *AS POS* นำข้อความ *Accept/Reject* และนำข้อความ *Accept/Reject*, T_1 และ T_2 มา

เข้ารหัสลับด้วยเซสชันคีย์ $SK_{N\text{-}ASj+1}$ ที่ AS ส่งมา นำค่าแฮชของนอนซ์ n_1, n_2 และเซสชันคีย์ $SK_{POS\text{-}ASj+1}$ ตัวถัดไป ค่าแฮชของของข้อความ *Accept/Reject*, T_1, T_2 และเซสชันคีย์ $SK_{N\text{-}ASj+1}$ ตัวถัดไปแล้วส่งให้ N เพื่อยืนยันการพิสูจน์ทราบตัวจริงของ N และเป็นการสิ้นสุดการพิสูจน์ทราบตัวจริงระหว่าง N และ AS

4. การวิเคราะห์ความมั่นคงปลอดภัยและอภิปราย

4.1 การวิเคราะห์ความมั่นคงปลอดภัย

4.1.1 การต้านทานการโจมตีแบบ Brute Force Attack

การโจมตีชนิด Brute Force Attack เพื่อค้นหาเซสชันคีย์ที่ถูกต้องนั้นในโพรโทคอลที่นำเสนอนั้นทำได้ยากเนื่องจากมีการเปลี่ยนแปลงค่าของเซสชันคีย์ในทุกๆ ครั้งที่มีการติดต่อสมบูรณ์ นอกจากนี้การนำเอาเทคนิคการสร้างและการกระจายเซสชันคีย์แบบออฟไลน์ ทำให้การค้นหาคีย์ตั้งต้นในการสร้างชุดของเซสชันคีย์ทั้งหมดทำได้ยาก จึงทำให้การโจมตีแบบ Brute Force Attack ประสบความสำเร็จน้อยลง

4.1.2 การต้านทานการโจมตีแบบ Replay Attack

การโจมตีแบบ Replay Attack โดยการปลอมตัวเป็นไคลเอนท์ แล้วส่งข้อมูลที่ดักจับได้อีกครั้งจะประสบความสำเร็จได้น้อยเนื่องจากการเปลี่ยนเซสชันคีย์ทุกครั้งที่มีการติดต่อสื่อสารอย่างสมบูรณ์ จากโพรโทคอลส่วนที่ 3.3 ของข้อความ M2 และ M3

4.1.3 ความคงสภาพของข้อมูล

การใช้ฟังก์ชันแฮชทำให้สามารถตรวจสอบได้ว่าข้อมูลที่ส่งมานั้นระหว่างทางถูกเปลี่ยนแปลงข้อมูลจากบุคคลอื่นมาก่อนหรือไม่ ซึ่งแสดงในส่วนที่ 3.3 และ 3.4 ของทุกข้อความ

4.1.4 การพิสูจน์ทราบตัวจริงของผู้ส่งข้อความ (Party Authentication)

คุณสมบัตินี้เป็นการพิสูจน์ตัวจริงของผู้ส่งข้อความ โดยนำเอา Message Authentication Code มาประยุกต์ใช้ ทำให้ผู้รับมั่นใจได้ว่าผู้ส่งเป็นผู้ส่งข้อความมาจริงและผู้รับเป็นผู้รับข้อความจริง ซึ่งแสดงในส่วนที่ 3.3 และ 3.4 ของทุกข้อความ

4.1.5 การโจมตีชนิด Man in the middle attack

ผู้โจมตีไม่สามารถปลอมตัวเป็นผู้ที่มีความเกี่ยวข้องหรือดักฟังข้อความของได้เนื่องจากมีการใช้กลุ่มของเซสชันคีย์ในซึ่งมีการเปลี่ยนเซสชันคีย์ทุกครั้งในการสื่อสารและใช้การเข้ารหัสลับที่เหมาะสม

4.2 การวิเคราะห์การนำไปใช้งานจริง

งานวิจัยที่นำเสนอใช้ฟังก์ชันแฮช SHA1 (Secure Hash Algorithm) การเข้ารหัสลับแบบสมมาตรใช้ AES (Advanced Encryption Standard) 128 bit ค่านอนซ์มีขนาด 40 byte เซสชันคีย์ขนาด 40 byte และ การระบุตัวตนของ *N, POS* และ *AS* ขนาด 8 byte

ตารางที่ 2. ขนาดข้อความของ NFCAuthV1 และ NFCAuthV2

Message	**NFCAuthV1 (byte)**	**NFCAuthV2 (byte)**
M1	55	210
M2	80	140
M3	80	86
M4	86	144
Total (byte)	301	580

ตารางที่ 2 แสดงขนาดความยาวข้อความจากโพรโทคอลที่นำเสนอ ผู้วิจัยได้ฟังก์ชันแฮชและการเข้ารหัสแบบสมมาตรมาใช้งาน ทำให้โพรโทคอลมีน้ำหนักเบา ซึ่งสามารถนำมาใช้กับอุปกรณ์สื่อสารไร้สายในปัจจุบันได้เป็นอย่างดี และขนาดความยาวของข้อความที่ติดต่อสื่อสารที่ใช้รับส่งข้อความยังมีความยาวน้อยกว่าข้อความสูงสุดที่ NFC สามารถส่งได้ในแต่ละครั้ง

4.3 การวิเคราะห์การพิสูจน์ทราบตัวจริงแบบสองทาง

การนำการสร้างและกระจายเซสชันคีย์แบบออฟไลน์มาใช้งานทำให้สามารถยืนยันได้ว่าผู้ที่มีเซสชันคีย์ที่ตรงกันเท่านั้นที่สามารถเข้ารหัสลับและถอดรหัสลับได้ หรือสามารถตรวจสอบข้อความที่รับมาได้ และโพรโทคอลที่นำเสนอได้นำเอา Message Authentication Code มาประยุกต์ใช้ ทำให้สามารถยืนยันตัวผู้ส่งและตัวผู้รับได้

5. การวิเคราะห์ประสิทธิภาพของโพรโทคอล

งานวิจัยจำนวนมากได้นำเสนอโพรโทคอลการพิสูจน์ทราบตัวจริงผ่าน NFC แต่โพรโทคอลที่นำเสนอมีการส่งข้อความเป็นจำนวนมากทำให้ประสิทธิภาพของโพรโทคอลลดลง โดยที่ [7] มีการส่งข้อความจำนวน 5 ข้อความและ [11] มีการส่งข้อความจำนวน 7 ข้อความ ในขณะที่โพรโทคอล NFCAuthv1 และ โพรโทคอล NFCAuthv2 มีการส่งข้อความเพียง 4 ข้อความ จึงทำให้ NFCAuthv1 และ โพรโทคอล NFCAuthv2 มีประสิทธิภาพและใช้เวลาน้อยกว่า [7, 11] แสดงตามตารางที่ 3

ตารางที่ 3. เปรียบเทียบโพรโทคอลการพิสูจน์ทราบตัวจริงผ่าน NFC

	[7] Ceipidor et al.	[11] Leon-Coca et al.	NFCAuthv1	NFCAuthv2
Symmetric Encryption	-	7	-	3
Symmetric Decryption	-	7	-	3
Asymmetric Encryption	2	-	-	-
Asymmetric Decryption	2	-	-	-
Hash Function	3	-	3	6
Number of Message	5	7	4	4

6. สรุปการวิจัย

งานวิจัยนี้ได้นำเสนอโพรโทคอลสำหรับพิสูจน์ทราบตัวจริงทั้งสองทางโดยใช้ NFC ซึ่งได้นำการกระจายเซสชันคีย์แบบออฟไลย์ซึ่งจะมีการเปลี่ยนเซสชันคีย์ที่มีการติดต่อสื่ออย่างสมบูรณ์และการใช้ฟังก์ชันแฮชมาใช้งานทำให้โพรโทคอลมีนำหนักเบาเหมาะกับอุปกรณ์สื่อสารไร้สายในปัจจุบันเพราะมีการคำนวนน้อย นอกจากนี้ยังมีคุณสมบัติความมันคงปลอดภัยเช่น การพิสูจน์ทราบตัวจริง การรักษาความลับของข้อมูลและการคงสภาพของข้อมูล นอกจากนี้โพรโทคอลยังมีประสิทธิภาพและใช้เวลาน้อย

เอกสารอ้างอิง

[1] 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, Orlando, USA, 2009.

[2] O. Dandash et al., “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 Science, 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 E-Commerce 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] L. Yun-Seok, K. Eun and J. Min-Soo, "A NFC based Authentication method for defense of the Man in the Middle Attack", 3rd International Conference on Computer Science and Information Technology (ICCSIT'2013) January 4-5, Bali (Indonesia), 2013.

[8] ECMA, “Near Field Communication Whitepaper”, ECMA International, 2004.

[9] Near Field Communication. (2012) [Online]. Available:http://en.wikipedia.org/wiki/Near_field_communication.

[10] Security Risks of Near Field Communication, "http://www.nearfieldcommunication.org/NFC-security-risks.html".

[11] U.B. Ceipidor, C.M. Medaglia, S. Sposato and A. Moroni,"A protocol for mutual authentication between NFC phones and POS terminals for secure payment transactions",

Information Security and Cryptology (ISCISC), 2012 9th International ISC Conference on Digital Object Identifier: 10.1109/ISCISC.2012.6408203 Publication , page 115 – 120, 2012.

[12] T. Sunil K., B. Rabin, and M. Sangman,"NFC and Its Application to Mobile Payment: Overview and Comparison", pp. 203-206, 26-28 June 2012.

[13] E. Haselsteiner and K. Breitfu, "Security in near field communication (NFC)," Proc. of Workshop on RFID security, 2006.

[14] C. Mulliner, "Vulnerability analysis and attacks on NFC-enabled mobile phones," Proc. of International Conference on vailability, Reliability and Security (ARES '09), pp. 695-700, Mar. 2009.

[15] K. Martin, "Near Field Communication A survey of safety and security measures", July 17, 2011.

[16] M. Gerald, C. Kantner, and T. Grechenig, " Near Field Communication (Chapter 15)," Secure Smart Embedded Devices, Platforms and Applications. Springer New York, pp. 351-367, 2014.

[17] V.di Credico, S. Orcioni, and M. Conti, "Near Field Communication Technology for AAL," Ambient Assisted Living: Italian Forum 2013. Springer International Publishing, pp. 33-42, 2014.

[18] C.N. Ashraf, "NFC-Vulnerabilities and defense," Information Assurance and Cyber Security (CIACS), 2014 Conference on. IEEE, pp. 35-38, 2014.

[19] H. Mohamad, F. Peyrard, and E. Conchon, "An improvement of NFC-SEC with signed exchanges for an e-prescription-based application," Mobile Computing, Applications, and Services. Springer International Publishing, pp. 166-183, 2014.

[20] D. Prabakaran, M. I. Kumar, "Near Field Communication Based Security Through Condition Privacy Sequence Methodology," International Journal of Computer Network and Security (IJCNS), Vol 6. No.1, pp. 22-28, Jan-March 2014.

[21] S. Park and I. Lee, "Efficient mCoupon Authentication Scheme for Smart Poster Environments based on Low-cost NFC," International Journal of Security and Its Applications Vol.7, No.5, pp.131-138, 2013.

[22] N. Dakota, M. Qiao, and A. Carpenter, "Security of the near field communication protocol: an overview," Journal of Computing Sciences in Colleges 29.2 (2013), pp. 94-104, 2013.20. N. Dakota, M. Qiao, and A. Carpenter, "Security of the near field communication protocol: an overview," Journal of Computing Sciences in Colleges 29.2 (2013), pp. 94-104, 2013.