โพรโตคอลน้ำหนักเบาสำหรับการสื่อสารด้วย RFID ที่มีคุณสมบัติการยืนยันตัวตนแบบสองทาง

สิรภูมิ เพ็ชรโต[1] และ ศุภกร กังพิศดาร[2]
คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร
Emails: [1]dimongimiss@gmail.com, [2]supakorn@mut.ac.th

บทคัดย่อ

เทคโนโลยีอาร์เอฟไอดี (RFID) ได้รับความนิยมเพิ่มขึ้นในปัจจุบันเนื่องจากความยืดหยุ่นในการใช้งานเมื่อเทียบกับบาร์โค้ด (Barcode) อย่างไรก็ตามยังมีปัญหาทางด้านความมั่นคงปลอดภัยในการสื่อสารระหว่างป้าย RFID และเครื่องอ่าน บทความวิจัยฉบับนี้นำเสนอการโพรโตคอลสำหรับการยืนยันตัวตนของป้าย RFID และเครื่องอ่าน ที่มีความมั่นคงปลอดภัยสูงกว่าระบบที่มีอยู่ รวมทั้งยังสามารถยืนยันตัวตนของทั้งสองฝ่ายได้ ซึ่งดีกว่าวิธีการที่มีอยู่ ที่สามารถยืนยันตัวตนของป้าย RFID ต่อเครื่องอ่านเท่านั้น นอกจากนี้ยังได้มีการประยุกต์เอาเทคนิคการกระจายเซสชั่นคีย์แบบออฟไลน์เพื่อเพิ่มความมั่นคงปลอดภัยให้แก่ระบบ

คำสำคัญ— อาร์เอฟไอดี(RFID); เครื่องอ่าน(RFID Reader); ป้าย RFID (RFID Tag); เซสชั่นคีย์ (Session Key); ค่านอนซ์ (Nonce)

1. บทนำ

ปัจจุบันเทคโนโลยี RFID (Radio Frequency Identification) มีประโยชน์และสร้างความสะดวกมากมาย จากคุณสมบัติที่ป้าย RFID (RFID Tag) สามารถเก็บข้อมูลได้ในปริมาณมาก และคุณสมบัติของการตรวจสอบความคงอยู่ของป้าย RFID ที่ง่ายกว่าบาร์โค้ด (Barcode) ทำให้อุตสาหกรรมหลายประเภทได้ประยุกต์ใช้ RFID ในหลายแอพพลิเคชั่น (Application) เช่น ระบบตรวจสอบยอดการส่งออกและรับเข้าสินค้าได้อย่างอัตโนมัติซึ่งทำให้ลด กระบวนการในการนับซ้ำ รวมไปถึงความสามารถที่จะคำนวณจำนวนสินค้าที่จะเก็บในแต่ละช่วงเวลาได้อย่างแม่นยำโดยการประมวลผลแบบเรียลไทม์จากยอดการสั่งซื้อ ซึ่งทำให้ไม่จำเป็นต้องสต๊อกสินค้าเกินจำนวน เพื่อที่จะแก้ปัญหาเวลามียอด การสั่งซื้อมากกว่าปกติ [1] หรือเพื่อใช้ระบุว่า เมื่อใดที่สินค้าถูกหยิบออกจากชั้นไป RFID จะมีการส่งสัญญาณเตือนไปยังพนักงานให้นำสินค้ามาเติมใหม่ ทำให้ไม่จำเป็นต้องเก็บสต๊อกสินค้า แต่สามารถสั่งให้ บริษัทคู่ค้า (Suppliers) มาส่งของได้ทันทีรวมทั้งช่วย ยืนยันได้ว่าสินค้ามีวางจำหน่ายตลอดเวลา เป็นต้น อย่างไรก็ตามคุณสมบัติของการเก็บข้อมูลในป้าย RFID อาจส่งผลเสียต่อผู้ใช้งานได้เช่นกัน เช่น ประวัติการซื้อสินค้า หรือข้อมูลประจำตัวของผู้ซื้ออาจถูกบันทึกไว้ในขณะที่ซื้อสินค้าภายในร้านหรือมีการใช้งาน RFID [2, 3, 4] เป็นต้น ข้อมูลเหล่านี้ บางส่วนเป็นข้อมูลส่วนตัวอาจถูกเจ้าของร้านหรือเจ้าของป้าย RFID นำไปใช้ในทางที่ไม่พึงประสงค์ได้ หรือในกรณีที่เรามีป้าย RFID อยู่กับตัว (ไม่ว่าจะติดอยู่กับเสื้อผ้า รองเท้า หรือสิ่งของต่างๆ) เมื่อเราอยู่ในระยะการอ่านของเครื่องอ่าน RFID ข้อมูลที่เกี่ยวกับตัวเรา และสินค้าก็จะถูกเปิดเผย ในปัจจุบันประเทศไทย ประชาชนยังให้ความสำคัญต่อข้อมูลส่วนบุคคลค่อนข้างน้อย

แม้ว่าเทคโนโลยี RFID นั้นได้รับความนิยมสูงขึ้น แต่ยังพบเรื่องปัญหาเรื่องการละเมิดความเป็นส่วนตัว ปัญหาหลักนั้นมาจากการขาดคุณสมบัติทางด้านความมั่นคงปลอดภัยที่จำเป็น เช่น การรักษาความลับของข้อมูล (Confidentiality) และการยืนยันตัวตนของข้อความที่ส่ง (Message Authentication) ทำให้ข้อมูลที่เป็นความลับถูกเปิดเผยและอาจไม่สามารถระบุตัวตนของผู้ที่เป็นผู้ส่งข้อมูลได้

งานวิจัยจำนวนมากได้ถูกเสนอขึ้นเพื่อเพิ่มความมั่นคงปลอดภัยให้แก่การสื่อสารผ่านเทคโนโลยี RFID [2, 5, 6] หนึ่งในงานวิจัยที่น่าสนใจได้แก่ งานของ Dimitriou [6] ซึ่งได้เสนอโพรโตคอลสำหรับการสื่อสารระหว่างเครื่องอ่าน (RFID Reader) และป้าย RFID โพรโตคอลนี้ใช้ฟังก์ชั่นแฮช (Hash function) เพื่อลดขนาดของข้อมูลที่ใช้ในการติดต่อสื่อสาร และได้เสนอแนวทางการป้องกันการโจมตีประเภทต่างๆ เช่น การติดตามข้อมูลภายในป้าย RFID และการโคลนนิ่ง (Cloning Attack) เป็นต้น อย่างไรก็ตามงานวิจัยดังกล่าวมีข้อบกพร่องและข้อจำกัดดังนี้ กล่าวคือ พบว่าพารามิเตอร์ที่ใช้เป็นคีย์สำหรับ Message Authentication หรือ MAC นั้นแม้ว่ามีการเปลี่ยนค่าในทุกๆ การเชื่อมต่อ แต่ค่าแต่ละค่าที่ใช้มีการเปลี่ยนแปลงจากค่าเดิมเพียงเล็กน้อยเท่านั้นก่อนที่จะถูกแฮช สิ่งนี้อาจทำให้เกิดปัญหาจากการถูกดักจับและวิเคราะห์ค่าคีย์สำหรับการสื่อสารในครั้งต่อไปได้ นอกจากนี้หากค่าคีย์ที่ใช้มีความยาวไม่มาก ทำให้มีโอกาสใช้คีย์ซ้ำได้ สิ่งนี้เป็นการสร้างโอกาสให้ผู้ไม่หวังดี (Attacker) สามารถสุ่มข้อมูลเพื่อหาค่าคีย์ที่มีการติดต่อสื่อสารกันได้

งานวิจัยฉบับนี้เสนอโพรโตคอลสำหรับการสื่อสารผ่าน RFID อย่างมั่นคงปลอดภัย สามารถแก้ไขปัญหาและข้อจำกัดของงานวิจัยที่มีอยู่ [6] จากการที่พบว่าโพรโตคอลที่ [6] นำเสนอมีปัญหาของการจัดการคีย์ ในงานวิจัยนี้ได้ประยุกต์เอาเทคนิคการสร้างและกระจายเซสชั่นคีย์ (Session key) แบบออฟไลน์ (Offline) ของ Kungpisdan *et al.* [7] เพื่อเพิ่มความมั่นคงปลอดภัย

โครงสร้างของงานวิจัยฉบับนี้มีดังต่อไปนี้ หัวข้อที่ 2 กล่าวถึงพื้นฐานที่เกี่ยวข้อง หัวข้อที่ 3 นำเสนอโพรโตคอลสำหรับการสื่อสารผ่าน

RFID ที่ปลอดภัย หัวข้อที่ 4 การวิเคราะห์คุณสมบัติความมั่นคงปลอดภัย หัวข้อที่ 5 สรุปผลการวิจัย

2. ทฤษฎีที่เกี่ยวข้อง

2.1 พื้นฐานของเทคโนโลยี RFID

เทคโนโลยี RFID (Radio Frequency Identification) เป็นระบบที่บ่งชี้ด้วยคลื่นความถี่วิทยุ มีหลักการทำงานคล้ายกับบัตรสมาร์ทการ์ด (Smart Card) หากแต่ป้าย RFID ไม่ต้องอาศัยการสัมผัสในการส่งพลังงานและข้อมูลระบบ RFID ประกอบด้วยองค์ประกอบหลัก 2 ส่วน คือ

1. เครื่องอ่าน (RFID Reader หรือ Interrogator) ทำหน้าที่ติดต่อสื่อสารกับป้าย RFID โดยใช้คลื่นความถี่วิทยุในการอ่านและเขียนข้อมูลลงในป้าย RFID [2, 3, 4, 8] โดยเครื่องจะส่งพลังงานไปยังป้าย RFID เพื่ออ่านข้อมูลจากป้าย RFID เมื่อทำหน้าที่เป็นเครื่องเขียนข้อมูล เครื่องอ่านจะส่งพลังงานไปยังป้าย RFID และเขียนข้อมูลลงป้าย RFID เครื่องอ่านประกอบด้วยภาครับและภาคส่งสัญญาณวิทยุ (Transceiver) ภาคสร้างสัญญาณพาหะ (Carrier) ขดลวดที่ทำหน้าที่เป็นสายอากาศ (Antenna) วงจรจูนสัญญาณ (Tuner) หน่วยประมวลผลข้อมูล และภาคติดต่อกับคอมพิวเตอร์ (Processing Unit)

2. ป้าย RFID (Tag หรือ Transponder) ถูกออกแบบให้มีรูปแบบและขนาดต่างๆ ตามความเหมาะสมของแต่ละแอพพลิเคชั่น เพื่อให้สามารถยึดติดกับวัตถุหรือสินค้าที่ต้องการระบุตัวตน หรือติดตามการตรวจนับด้วยเทคโนโลยี RFID [2, 9] โดยมีการแบ่งตามจำนวนบิตที่เก็บข้อมูลเป็น 2 ประเภท คือ

- เก็บข้อมูลที่การบ่งชี้เพียง 1 บิต (Bit) เพื่อระบุว่ามีหรือไม่มีบัตรนั้นในรัศมีการทำงานแต่ไม่สามารถชี้เฉพาะได้ นิยมใช้ในระบบป้องกันการขโมยสินค้าในร้านค้า
- เก็บข้อมูลที่บ่งชี้ที่มีมากกว่า 1 บิต เพื่อระบุว่ามีหรือไม่มีป้าย RFID นั้นในรัศมีการทำงาน และสามารถชี้เฉพาะได้ว่าชิ้นไหน ตัวอย่างเช่น ป้าย RFID บอกราคาสินค้า บัตรผ่านเข้า-ออกประตู บัตรโดยสารรถไฟฟ้าใต้ดิน หนังสือเดินทาง และบัตรเครดิต เป็นต้น

หากแบ่งประเภทของระบบ RFID ตามฟังก์ชั่นการประมวลผลข้อมูลและขนาดของหน่วยความจำภายในป้าย RFIDสามารถแบ่งได้ 3 กลุ่ม [2] ดังนี้

1. กลุ่มระดับล่าง: มีอยู่ในระบบ EAS (Electronic Article Surveillance) ซึ่งใช้ในการตรวจสอบตัวตนของป้าย RFID โดยป้าย RFID เหล่านี้จะบันทึกข้อมูลที่เป็นหมายเลขรหัส ID อย่างถาวร (ไม่สามารถแก้ไขได้) ตั้งแต่การผลิต
2. กลุ่มระดับกลาง: ป้าย RFID มีความสามารถในการเขียนซ้ำข้อมูลภายในป้าย RFID ได้โดยทั่วไปจะมีขนาดของหน่วยความจำตั้งแต่ไม่กี่ไบต์จนถึงมากกว่า 100 กิโลไบต์ (KB) มีทั้งหน่วยความจำแบบ EEPROM (ใช้กับป้าย RFID แบบพาสซีฟ (Passive)) และ SRAM (ใช้กับป้าย RFID แบบแอ็กทีฟ (Active)) สามารถประมวลผลคำสั่งที่ไม่ซับซ้อน ป้าย RFID ชนิดนี้ยังมีความสามารถในการป้องกันการชนกันของข้อมูล (Anti-Collision) รวมทั้งรองรับกลไกการตรวจสอบยืนยันการใช้งาน (Authentication) และการเข้ารหัสลับ (Encryption) ได้อีกด้วย
3. กลุ่มระดับบน: ป้าย RFID จะมีไมโครโปรเซสเซอร์ (Microprocessor) และระบบปฏิบัติการอยู่ภายใน เพื่อทำหน้าที่ประมวลผลและทำงานที่มีความซับซ้อนสูง เช่น การยืนยันการใช้งานและการเข้ารหัสลับข้อมูลที่ใช้ขั้นตอนวิธี (Algorithm) ที่มีความซับซ้อนสูงกว่าป้าย RFID ในกลุ่มระดับกลาง ในปัจจุบันระบบ RFID ในกลุ่มระดับบนทำงานที่ย่านความถี่ 13.56 MHz

2.2 ปัญหาทางด้านความมั่นคงปลอดภัยของ RFID

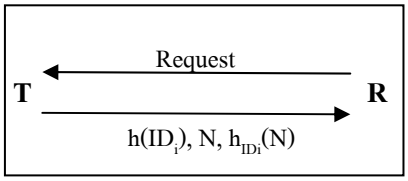
ปัจจุบันเทคโนโลยี RFID ได้ถูกนำมาใช้มากขึ้นทั้งในส่วนงานที่ต้องการความมั่นคงปลอดภัยสูง เช่น การควบคุมการเข้าถึง (Access Control) ระบบการชำระเงิน (Payment System) ระบบการตรวจสอบย้อนกลับของผลิตภัณฑ์ (Traceability System) เทคโนโลยีการใช้ระบบปิดตู้สินค้าแบบอิเล็กทรอนิกส์เพื่อช่วยในการขนส่งสินค้าอย่างปลอดภัย (E-Seal) [9] หรือการพิสูจน์ตัวตน เช่น พาสปอร์ต (Passport) ในบางประเทศ เป็นต้น ซึ่งในงานเหล่านี้ต้องมีการใช้มาตรการรักษาความมั่นคงปลอดภัยเพื่อป้องกันการโจมตีโดยผู้ไม่ประสงค์ดี [2, 5, 6, 7] ซึ่งเทคโนโลยี RFID สามารถถูกโจมตีด้วยวิธีการต่างๆ เช่น

- การดักฟังการติดต่อสื่อสารแล้วนำข้อมูลเดิมกลับมาใช้ เพื่อให้สามารถเข้าถึงข้อมูลที่ต้องการได้ (Replay Attack)
- การติดต่อสื่อสารระหว่างป้าย RFID และเครื่องอ่านต้องเป็นความลับ (Confidentiality) เพื่อป้องกันคนอื่นที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลต่างๆ ของป้าย RFID ได้
- ข้อมูลที่ใช้ในการติดต่อสื่อสารต้องไม่เปลี่ยนแปลงในระหว่างการส่งและรับข้อมูล (Message Integrity) เป็นต้น

2.3 งานวิจัยที่เกี่ยวข้อง

2.3.1 โพรโตคอลของ Dimitriou

Dimitriou [6] ได้เสนอโพรโตคอลเพื่อใช้การสื่อสารข้อมูลระหว่าง Tag และ Reader ที่มีขนาดเล็กและเป็นข้อมูลแฝง มีคุณสมบัติทางด้านความมั่นคงปลอดภัยและรับรองความถูกต้องของป้าย RFID และเครื่องอ่าน โดยใช้ฟังก์ชั่นแฮชเพื่อลดขนาดของข้อมูลที่ใช้ในการติดต่อสื่อสาร โดยค่า ID เป็นค่าเกิดจากการสุ่มข้อมูลถูกจัดเก็บทั้งในฐานข้อมูลและป้าย RFID (ทั้งคู่มีค่าข้อมูลเหมือนกัน) ซึ่งมีหลักการดังรูปที่ 1 ด้านล่างนี้



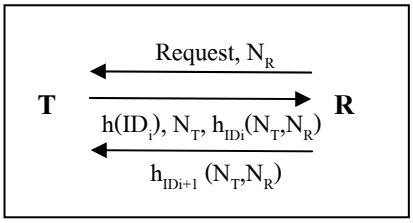
รูปที่ 1 A simple protocol ensuring user privacy

1. เครื่องอ่าน (R) ทำการส่งสัญญาณร้องขอ (Request) เพื่อต้องการติดต่อกับป้าย RFID (T)

2. เมื่อป้าย RFID ได้รับ Request จะทำการสร้างค่านอนซ์ (N) และจากนั้นจึงส่งค่า $\{h(ID_i), N, h_{IDi}(N)\}$ กลับยังเครื่องอ่าน และถูกส่งต่อเพื่อตรวจสอบกับฐานข้อมูลผู้ใช้งาน

ค่า $h(ID_i)$ จะถูกสร้างและเชื่อมโยงกับค่าข้อมูลหลัก (Identity) ของป้าย RFID ซึ่งถูกเก็บไว้ในฐานข้อมูล เมื่อฐานข้อมูลได้รับค่า $h(ID_i)$ จากนั้นจะนำค่านี้ไปทำการค้นหาเพื่อนำค่า Identity ของป้าย RFID กลับมาใช้ เมื่อฐานข้อมูล มีค่า ID_i แล้วจะนำค่าแฮชของ $h(ID_i)$ มาทำการแฮชค่า N อีกครั้ง $h_{IDi}(N)$ แล้วนำค่าดังกล่าวเปรียบเทียบกับค่าที่ได้จากป้าย RFID ว่าตรงกันหรือไม่

จากนั้น Dimitriou ได้เสนอการปรับปรุงเทคนิคของโพรโตคอลเพื่อใช้ในการตรวจสอบตัวตนของเครื่องอ่าน โดยมีหลักการดังนี้



รูปที่ 2 A Challenge response protocol for tag-reader authentication

1. เครื่องอ่าน (R) ทำการส่งสัญญาณร้องขอ (Request) และค่านอนซ์ (Nonce) ของเครื่องอ่าน N_R เพื่อต้องการติดต่อกับป้าย RFID

2. เมื่อป้าย RFID ได้รับ Request และ N_R จะทำการสร้างค่านอนซ์ของป้าย RFID N_T และส่ง $\{h(ID_i), N_T, h_{IDi}(N_T,N_R)\}$ กลับไปยังเครื่องอ่านและจะถูกส่งต่อเพื่อตรวจสอบกับฐานข้อมูล

3. เมื่อตรวจสอบถูกต้อง ฐานข้อมูลจะใช้ค่าคีย์ใหม่โดยให้ ID_{i+1} แล้วนำค่าแฮชของ $h(ID_{i+1})$ มาทำการแฮชค่า N_T,N_R อีกครั้ง $\{h_{IDi+1}(N_T,N_R)\}$ แล้วส่งค่าดังกล่าวไปยังป้าย RFID หากค่าที่ได้รับตรงกับค่าที่ส่งมาแล้ว ป้าย RFID ทำการลบข้อมูล ID_i, N_T และ N_R ออกจากหน่วยความจำของป้าย

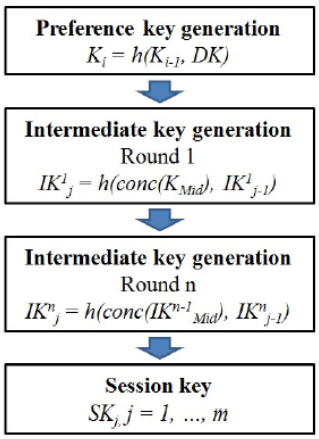
อย่างไรก็ตาม พบว่าความมั่นคงปลอดภัยของเทคนิคดังกล่าวขึ้นอยู่กับการเลือกใช้ค่า ID_i เป็นค่าของ ID ของป้าย RFID ลำดับที่ i เมื่อทำการดักฟังค่า ID_{i+1} นั้นจะสามารถวิเคราะห์ค่า ID ค่าถัดไปได้ และเนื่องจากการที่ค่า ID เป็นค่าคงที่ไม่มีการเปลี่ยนแปลง โอกาสที่ ID_{i+1} จะชนกับค่า ID อื่นๆ ก็จะสามารถเกิดขึ้นได้ และขนาดของป้าย RFID ต้องสามารถรองรับปริมาณของข้อมูลที่เก็บเหมือนกับฐานข้อมูล

2.3.2 เทคนิคการสร้างและกระจายเซสชั่นคีย์แบบออฟไลน์ของ Kungpisdan et al.

Kungpisdan *et al.* [7] ได้นำเสนอวิธีการสร้างและกระจายคีย์แบบออฟไลน์ ซึ่งมีการสร้างและกระจายเซสชั่นคีย์ (Session Key) โดยที่ไม่ต้องส่งคีย์ดังกล่าวผ่านเครือข่าย [10] รายละเอียดของวิธีการดังกล่าวมีดังนี้

<u>การสร้างเซสชั่นคีย์ (Session Key Generation)</u>

ก่อนการสร้างเซสชั่นคีย์ จะต้องดำเนินการแลกเปลี่ยนค่า $\{K_{AB}, DK, m\}$ สมมติว่าเป็นการแลกเปลี่ยนโดยอลิสและบ๊อบ ซึ่งกำหนดให้ K_{AB} เรียกว่า Long-term key, DK เรียกว่า Distribution key และ m คือค่าสุ่มที่ระบุจำนวนของคีย์ที่ต้องการสร้างขึ้น โดยขั้นตอนการสร้างเซสชั่นคีย์ สามารถอธิบายได้ดังรูปที่ 3 ดังนี้



รูปที่ 3 Session Key Generation

หลังจากทำการแลกเปลี่ยนค่า $\{K_{AB}, DK, m\}$ อลิสและบ๊อบ จะสร้างเซตของ Preference keys K_i, i = 1,2,…, m ดังสมการ

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

จากนั้น ทั้งคู่สร้างเซตของ Intermediate Keys (IK) ซึ่งเป็นการเพิ่มความยากในการวิเคราะห์การถอดรหัสลับ เพิ่มความยากในการสืบค้นของ Preference key โดยมีรูปแบบดังนี้

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

โดย x เป็นจำนวนรอบ, 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}) , $IK^{1}_{mid1} = K_{mid1}$, $IK^{1}_{mid2} = K_{mid2}$, $IK^{1}_{mid3} = K_{mid3}$ และ $IK^{x}_{j-1} = \emptyset$ การใช้ Intermediate Keys ในทุกๆรอบ จะทำการลบค่าออกจากระบบ ส่วนที่เหลือของ Intermediate Keys ในรอบอื่นๆ สามารถเขียนได้ดังนี้

$\{K_1, K_2, \ldots, K_{rm}\}$,

$\{K^1_1, K^1_2, \ldots, K^1_{rm}\}$,

$\{K^2_1, K^2_2, \ldots, K^2_{rm}\}$,

…

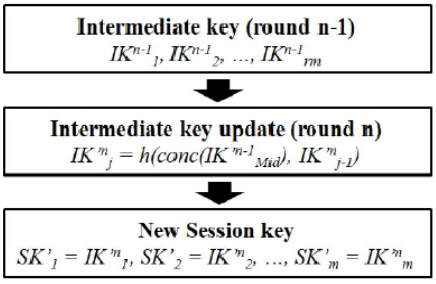
$\{K^n_1, K^n_2, \ldots, K^n_{rm}\}$

ผลที่ได้ในรอบสุดท้ายของ Intermediate Keys ที่ได้พิจารณาจากเซสชั่นคีย์ (Session key) (SK_j) โดยที่ j = 1,… ,m คือ

$$IK^n_1 = SK_1, IK^n_2 = SK_2, \ldots, IK^n_m = SK_j \quad (3)$$

จากรูปแบบข้างต้น อลิสและบ๊อบสามารถใช้ค่า SK_j ในการเพิ่มความปลอดภัยในการสื่อสารได้

<u>การปรับปรุงเซสชั่นคีย์และ Intermediate Key</u>



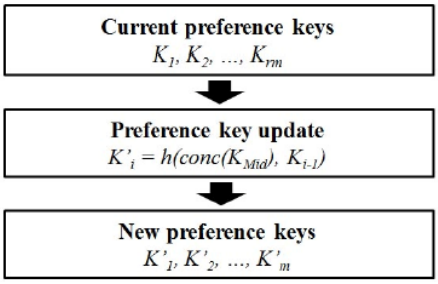
รูปที่ 4 Session Key Update

ภายหลังจากที่อลิสและบ๊อบได้ใช้เซสชั่นคีย์ (หรือ Intermediate key) ไประยะหนึ่ง ควรที่จะสร้างชุดของเซสชั่นคีย์ชุดใหม่ เพื่อความปลอดภัย โดยสมมติว่ามีการใช้เซสชั่นคีย์ถึงค่า SK_j และต้องการเปลี่ยนเซสชั่นคีย์ชุดใหม่ อลิสและบ๊อบจะต้องทำการสร้างเซสชั่นคีย์ชุดใหม่ดังสมการที่ (4)

$$IK'^n_j = h(conc(IK'^{n-1}_{mid}), IK'^n_{j-1}) \quad (4)$$

จากรูปที่ 4 แสดงให้เห็นถึงขั้นตอนการปรับปรุงเซสชั่นคีย์หรือ Intermediate key โดยที่ $IK'^n_0 = \emptyset$ หลังจากทำการสร้างเซสชั่นคีย์หรือ Intermediate key ใหม่แล้ว ค่าเดิมที่มีการใช้งานจะถูกลบออกจากระบบ เพื่อหลีกเลี่ยงการใช้งานค่าข้อมูลเดิมและสร้างความมั่นคงปลอดภัยให้กับระบบเพิ่มมากขึ้น

<u>การปรับปรุง Preference Key</u>



รูปที่ 5 Preference Key Update

หากชุดข้อมูลของ Preference key ต้องการปรับปรุง โดยสมมติว่าอลิสและบ๊อบ มีการใช้งาน Preference key ถึงค่า K_i สามารถดำเนินการดังสมการที่ (5)

$$K'_i = h(conc(K_{mid}), IK'_{i-1}) \quad (5)$$

จากรูปที่ 5 แสดงให้เห็นถึงขั้นตอนการปรับปรุง Preference key และหลังจากได้ชุดของ Preference key ใหม่แล้วจะดำเนินการลบข้อมูลชุดเดิมออกจากระบบ อลิสและบ๊อบสามารถใช้ค่า K'_i โดย i = 1, …, m ในการสร้าง Intermediate key และเซสชั่นคีย์ต่อไป

จากเทคนิคนี้จะเห็นว่าจะมีการส่งเพียงค่าตัวแปล ที่เป็นค่าเริ่มต้นเพื่อนำไปใช้ในการสร้างคีย์ และคีย์ที่ถูกสร้างขึ้น ถูกนำมาใช้เพียงครั้งเดียวไม่มีการนำมาใช้ซ้ำและสามารถสร้างคีย์โดยโอกาสเกิดค่าคีย์ที่ซ้ำเป็นไปได้ยาก

ในบทความวิจัยนี้จะมีการนำเอาเทคนิคการกระจายคีย์ดังกล่าวมาใช้ เพื่อเพิ่มความมั่นคงปลอดภัยให้กับ โพรโตคอล RFID ซึ่งรายละเอียดของเทคนิคที่นำเสนอนั้นจะกล่าวในบทถัดไป

3. งานวิจัยที่นำเสนอ

เพื่อเป็นการแก้ไขปัญหาและข้อจำกัดงานงานวิจัยที่มีอยู่ [6] งานวิจัยฉบับนี้นำเสนอโพรโตคอลสำหรับการสื่อสารผ่านเทคโนโลยี RFID อย่างมั่นคงปลอดภัย โดยมีการประยุกต์นำเอาเทคนิคการสร้างและกระจายเซสชั่นคีย์แบบออฟไลน์ [7] ดังรายละเอียดด้านล่าง

3.1 นิยามศัพท์ที่เกี่ยวข้อง

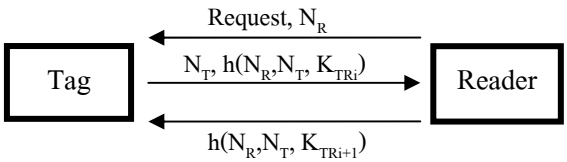
- K_{AB} = คีย์ (Key) ที่แลกเปลี่ยนกันระหว่างผู้ใช้ A และ B อนึ่ง A และ B อาจเป็นเครื่องอ่านและป้าย RFID ตามลำดับ
- N = ค่านอนซ์ (Nonce) สำหรับการป้องกันการโจมตีแบบรีเพลย์ (Replay Attack)
- h(M, K) = ค่า Message Authentication Code (MAC) ของข้อความ M ด้วยคีย์ K

3.2 รายละเอียดของโพรโตคอลที่นำเสนอ

ระบบนี้ประกอบด้วยผู้ที่เกี่ยวข้องจำนวน 2 ส่วน คือ ป้าย RFID (RFID Tag) และเครื่องอ่าน (RFID Reader) ก่อนการเชื่อมต่อระหว่างป้าย RFID และเครื่องอ่าน จะมีการส่งค่าข้อมูลชุดหนึ่ง $\{K_{AB}, DK, m\}$ เพื่อใช้เป็นค่าในการคำนวณเพื่อหาเซสชั่นคีย์ของทั้งป้าย RFID และเครื่องอ่านโดยใช้เทคนิคการสร้างและกระจายเซสชั่นคีย์แบบออฟไลน์ของ Kungpisdan *et al.* [7] ซึ่งมีความมั่นคงปลอดภัยในการดำเนินงานเป็นอย่างมาก เนื่องจากเซสชั่นคีย์ที่ถูกสร้างขึ้นจะถูกใช้เพียงครั้งเดียว ไม่มีการใช้ซ้ำ และไม่มีการส่งค่าคีย์ที่แท้จริงระหว่างการการติดต่อสื่อสาร

โดยเมื่อทำการส่งค่าคีย์ตั้งต้น $\{K_{AB}, DK, m\}$ ป้าย RFID และเครื่องอ่าน จะทำการคำนวณหาชุดข้อมูลของ Preference key (K_i) โดยที่ i = 1, …, m ดังสมการที่ (1) และรูปที่ 3 เมื่อทำการสร้างชุดข้อมูลของ K_i เรียบร้อยแล้วสามารถลบค่า K_{AB}, DK ออกจากระบบได้ หลังจากนั้น ป้าย RFID และเครื่องอ่านจะสร้างเซตของ Intermediate Keys (IK) ซึ่งเป็นการเพิ่มความยากในการวิเคราะห์การถอดรหัสลับ เพิ่มความยากในการสืบค้นของ Preference key โดยมีรูปแบบดังสมการที่ (2) โดย x เป็นจำนวนรอบ, 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} , $IK^{x}_{mid2} = mid(IK^{x}_{mid1}, IK^{x}_{rm})$, $IK^{x}_{mid3} = mid(IK^{x}_{1}, IK^{x}_{mid2})$, $IK^{1}_{mid1} = K_{mid1}$, $IK^{1}_{mid2} = K_{mid2}$, $IK^{1}_{mid3} = K_{mid3}$ และ $IK^{x}_{j-1} = \emptyset$

การใช้ Intermediate Keys ในทุกๆรอบ จะทำการ ลบค่าออกจากระบบ ส่วนที่เหลือของ Intermediate Keys ในรอบอื่นๆ ผลที่ได้ในรอบสุดท้ายของ Intermediate Keys ที่ได้พิจารณาจาก เซสชั่นคีย์ (Session key) (SK_j) ดังสมการที่ (3) ป้าย RFID และเครื่องอ่านทำการสร้างชุดเซสชั่นคีย์ SK_j โดยจะใช้ค่าดังกล่าวเป็นค่าที่ติดต่อสื่อสารระหว่างกัน เพื่อให้สะดวกในการจดจำ $SK_1 = K_{TR1}$, $SK_2 = K_{TR2}$, …, $SK_j = K_{TRi}$ โดยที่ i = 1, …, m ป้าย RFID จะถูกติดเข้ากับสินค้าและถูกจัดการโดยบริษัทเจ้าของสินค้า การเขียนและอ่านข้อมูลผ่านป้าย RFID สามารถทำได้โดยผ่านทางเครื่องอ่าน ซึ่งรายละเอียดของโพรโตคอลที่นำเสนอมีดังนี้



รูปที่ 6 ขั้นตอนการสื่อสารระหว่างป้าย RFID และเครื่องอ่านโดยใช้เซสชั่นคีย์

1. จากรูปที่ 6 เครื่องอ่านส่งสัญญาณ Request และค่านอนซ์ (Nonce) ของเครื่องอ่าน NR เพื่อต้องการติดต่อกับป้าย RFID
2. เมื่อป้าย RFID ได้รับ {Request, NR} แล้วทำการสร้างค่านอนซ์ของป้าย RFID NT แล้วสร้างค่า h(NR, NT, KTRi) จากนั้นจึงส่งค่า { NT, h(NR,NT, KTRi)} กลับไปยังเครื่องอ่าน ข้อมูลดังกล่าว และจะถูกส่งไปตรวจสอบความถูกต้องกับฐานข้อมูล (ฐานข้อมูลนั้นเป็นส่วนสำคัญในการจัดเก็บข้อมูลเพื่อใช้ในการเปรียบเทียบและประมวลผลข้อมูลต่างๆ ระหว่างป้าย RFID และเครื่องอ่าน โดยการเชื่อมต่อระหว่างเครื่องอ่านและฐานข้อมูลนั้นได้มีการตั้งสมมติฐานว่าเป็นการเชื่อมต่อที่มีความมั่นคงปลอดภัยแล้ว) ฐานข้อมูลทำการตรวจสอบความถูกต้องของข้อมูล โดยการนำค่า KTRi และ NR ที่ตนเองมีอยู่ พร้อมค่า NT สร้างค่าแฮช แล้วเปรียบเทียบกับค่าที่ได้รับจากป้าย RFID หากค่าที่ได้ตรงกันจะเป็นการยืนยันตัวตนของป้าย RFID
3. เมื่อตรวจสอบถูกต้องแล้ว ฐานข้อมูลเปลี่ยนค่าของเซสชั่นคีย์ใหม่เพื่อความมั่นคงปลอดภัย โดยที่จะไม่มีการใช้คีย์ซ้ำ โดยใช้ค่า KTRi+1 จากนั้นจึงสร้างข้อความ $h(N_R,N_T, K_{TRi+1})$ และส่งค่าดังกล่าวกลับไปยังป้าย RFID
4. เมื่อป้าย RFID ได้รับค่า $h(N_R,N_T, K_{TRi+1})$ แล้วจึงทำการเปรียบเทียบกับค่าแฮชที่สร้างขึ้นใหม่เพื่อเปรียบเทียบค่าเซสชั่นคีย์ที่ต้องใช้ในการสื่อสารครั้งต่อไป ซึ่งป้าย RFID จะใช้ค่า K_{TRi+1} ที่เป็นค่าเดียวกันกับค่าที่มีในฐานข้อมูล และนำค่าเซสชั่นคีย์ที่มีอยู่มาตรวจสอบ เมื่อมีการพิสูจน์เรียบร้อยแล้ว ป้าย RFID และเครื่องอ่านทำการลบข้อมูลเซสชั่นคีย์เดิมและค่านอนซ์ต่างๆ ออกจากระบบ เพื่อป้องกันการใช้ข้อมูลซ้ำ

หากต้องการทำการปรับปรุงเซสชั่นคีย์, Intermediate Key หรือ Preference Key สามารถทำตามเทคนิคการปรับปรุงเซสชั่นคีย์, Intermediate Key หรือ Preference Key ของ Kungpisdan et al. [7]

4. การวิเคราะห์คุณสมบัติความมั่นคงปลอดภัย

4.1 การรักษาความลับ (Confidentiality)

จากการที่มีการสื่อสารกันด้วยเซสชั่นคีย์ K_{TRi} นั้น ผู้ที่มีเซสชั่นคีย์ที่ตรงกันเท่านั้น จึงจะสามารถเข้าถึงหรือติดต่อสื่อสารกันระหว่างป้าย RFID และเครื่องอ่านได้ ซึ่งการสร้างเซสชั่นคีย์นั้นมีลักษณะเป็นแบบออฟไลน์ (Offline) โดยจะไม่มีการส่งคีย์ดังกล่าวข้ามเครือข่าย จึงทำให้โอกาสในการถูกดักจับ (Sniff) แล้วได้ค่าคีย์ที่ถูกต้องไปนั้นทำได้ยากมาก จึงทำให้ระบบมีความมั่นคงปลอดภัยมากยิ่งขึ้น

4.2 การยืนยันตัวผู้ส่งข้อความ (Message Authentication)

เป็นการใช้สำหรับการยืนยันความถูกต้องของข้อมูลระหว่างการสื่อสารและยังเป็นการป้องกันการปลอมแปลงข้อมูล หากพิจารณาจากโพรโตคอลข้างต้น $\{N_T, h(N_R,N_T, K_{TRi})\}$และ $\{h(N_R,N_T, K_{TRi+1})\}$ จะพบว่า ข้อความที่มีการส่งผ่านระหว่างกันนั้น จะใช้เซสชั่นคีย์และนอนซ์เป็นหลักเพื่อพิสูจน์ว่าข้อมูลที่ใช้ในการสื่อสารมาจากป้าย RFID และเครื่องอ่านที่สามารถเชื่อถือได้

4.3 การทนทานต่อการถูกโจมตีด้วย Replay Attack

แม้จะถูกโจมตีด้วย Replay Attack ด้วยวิธีการต่างๆ เช่น การปลอมตัวเป็นป้าย RFID หรือเครื่องอ่าน การโจมตีดังกล่าวจะไม่สามารถประสบความสำเร็จได้ เนื่องจากเซสชั่นคีย์ที่ใช้เปลี่ยนแปลงตลอดเวลา เมื่อมีการติดต่อกันอย่างสมบูรณ์ระหว่างป้าย RFID และเครื่องอ่าน และการใช้นอนซ์ $\{N_R,N_T\}$ ก็เป็นส่วนสำคัญในการป้องกัน เนื่องจากเป็นการแสดงค่าเพื่อบ่งบอกว่าค่าดังกล่าวถูกสร้างจากป้าย RFIDหรือเครื่องอ่านที่แท้จริง

4.4 การทนทานต่อการถูกโจมตีแบบ Brute Force Attack

ด้วยเทคนิคการสร้างและกระจายเซสชั่นคีย์แบบออฟไลน์ [7] ทำให้การสืบค้นเพื่อหา Preference key ทำได้ยากขึ้น เนื่องจากกระบวนการดังกล่าวเป็นการเข้ารหัสลับที่มีความซับซ้อน และค่าของ Intermediate key (IK^x_j) มีการเปลี่ยนไปเรื่อยๆ จึงทำให้โอกาสที่การโจมตีแบบ Brute Force ไม่ประสบผลสำเร็จ

5. สรุปผลการวิจัย

งานวิจัยฉบับนี้ได้นำเสนอรูปแบบการติดต่อสื่อสารระหว่างป้าย RFID และเครื่องอ่าน เพื่อเกิดความความมั่นคงปลอดภัยในด้านต่างๆ โดยใช้หลักการรหัสลับแบบสมมาตร (Symmetric Encryption) นอกจากนี้ยังได้เพิ่มความมั่นคงปลอดภัยให้กับวิธีการที่นำเสนอโดยวิธีการสร้างและกระจายคีย์แบบออฟไลน์ งานวิจัยที่นำเสนอสามารถใช้งานได้ดีกับป้าย RFID ที่สามารถประมวลผลด้วยตนเองได้ เช่น การสร้างค่านอนซ์และเซสชั่นคีย์ เป็นต้น เพื่อให้เกิดประสิทธิภาพสูงสุด

สำหรับแนวทางการพัฒนางานวิจัยต่อไปนั้น จะมุ่งเน้นการพัฒนาต้นแบบของระบบการสื่อสารผ่านเทคโนโลยี RFID โดยที่มีพื้นฐานมาจากงานวิจัยที่นำเสนอ โดยจำเป็นต้องเริ่มต้นศึกษาป้าย RFID ที่สามารถทำการประมวลผลต่างๆ ด้วยตนเอง ซึ่งอาจจะอยู่ในกลุ่มของการประมวลผลข้อมูลของป้าย RFID (RFID Tag) ระดับกลางและระดับบน [2] เพื่อให้การสื่อสารกันระหว่างป้าย RFID และเครื่องอ่าน เกิดประสิทธิภาพสูงสุด

เอกสารอ้างอิง

[1] ศูนย์ข้อมูลธุรกิจและข้อมูลการตลาด. “RFID เทคโนโลยีคลื่นวิทยุสุดฮิต”.http://www.businessthailand.org/technology-ebusiness/ebusiness/1094-rfid--

[2] ปิยะ โควินท์ทวีวัฒน์ และคณะ. “ระบบบ่งชี้ด้วยคลื่นความถี่วิทยุ : Radio Frequency Identification (RFID) System” พิมพ์ครั้งที่ 1. ปทุมธานี : ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (สวทช.), 2552.

[3] วีระศักดิ์ ชื่นตา. “การออกแบบและพัฒนาระบบควบคุมการผ่านเข้าออกด้วยเทคโนโลยีอาร์เอฟไอดี”, ECTI-CARD. 2009 : 415-420.

[4] สิทธิชัย เพชรพะยอง และคณะ. “เทคโนโลยีอาร์เอฟไอดีเพื่อการบริหารจัดการรถทัวร์โดยสาร”, ECTI-CARD. 2009 : 283-288.

[5] Hoda Daou et al. “RFID Security Protocol”, Innovations in Information Technology, 2008. IIT 2008, 16-18 Dec. 2008. 593 – 597.

[6] Tassos Dimitriou. “A Lightweight RFID Protocol to protect against Traceability and Cloning attacks”, Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005, 05-09 Sept. 2005. 59 – 66.

[7] Kungpisadan *et al.* “A Secure Offline Key Generation With Protection Against Key Compromise”, Proceedings of the 13th World Multi-conference on Systemics, Cybernetics, and Informatics 2009, Orlando, Florida, July, 2009, pp. 63-67.

[8] สุธรรม จินดาอุดม และคณะ. “ระบบควบคุมประตูด้วย RFID ที่เชื่อมต่อผ่านแลนไร้สาย” , ECTI-CARD. 2009 : 397-402.

[9] สถาบันส่งเสริมความเป็นเลิศทางเทคโนโลยีอาร์เอฟไอดีแห่งประเทศไทย. http://www.rfid.or.th

[10] วิชชุณา วามนตรี และ ศุภกร กังพิศดาร, เทคนิคการกระจายคีย์แบบควอนตัม, 7th International Joint Conference on Computer Science and Software Engineering. 2010.178-183.