การพัฒนาการเข้ารหัสข้อมูลบนเครือข่ายที่ทนทานต่อความล่าช่า

Improve Identity Based Cryptography on Delay Tolerant Network

น.ส.วิจิตรา ขจร,น.ส.อาทิตยาพร โรจรัตน์,น.ส.เทวิกา จันทอง และนายเชิดพงศ์ ตาปราบ
ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น

***Abstract*— Delay Tolerant Network (DTN) เป็นเครื่อข่ายไร้สายแบบเคลื่อนที่ที่มีปัญหาในด้านการรับส่งข้อมูลมาก เนื่องจากโหนดอาจมีการเคลื่อนที่ออกจากระยะการติดต่อสื่อสาร การสื่อสารอาจมีความล่าช้าหรือล้มเหลวได้ง่าย จึงต้องมีการออกแบบโปรโตคอลต่างๆสำหรับการจัดการการรับส่งข้อมูลบนเครือข่าย DTN โดยเฉพาะ รวมทั้งการจัดการทางด้านความปลอดภัยด้วย**

หนึ่งในการรักษาความปลอดภัยบน DTN ที่ใช้งานได้คือระบบเข้ารหัสข้อมูลแบบ Identity Based Cryptography (IBC) แต่ทั้งนี้ระบบ IBC เดิมยังมีข้อจำกัดการใช้งานอยู่บางประการ ในการแก้ไขปัญหาดังกล่าวจึงต้องใช้วิธีการพัฒนาอัลกอรึทึมของ Public Key Generater จากที่มีเดิมให้สามาแก้ไขข้อจำกัดที่เกิดขึ้นได้ โดยผลที่ได้รับคืออัลกอรึทึม PKG ใหม่สามารถแก้ไขข้อจำกัดที่เกิดขึ้นได้แต่มีความซับซ้อนในการทำงานและการติดต่อสื่อสารมากขึ้น อัลกอรึทึม PKG แบบใหม่จึงเหมาะแก่ระบบเครือข่าย DTN ที่มีจำนวนผู้ใช้งานที่ไม่มากจนเกินไป

Keywords-component; Delay Tolerant Network (DTN),Network Security, Identity Based Cryptography

1. บทนำ

Delay Tolerant Network (DTN) เป็นเครือข่ายไร้สายแบบเคลื่อนที่ที่มีความล่าช้าในการติดต่อสื่อสารกันมาก และมีความล้มเหลวในการติดต่อสื่อสารกันได้สูง เนื่องจากการติดต่อสื่อสารกันระหว่างโหนดอาจมีการขาดหายเกิดขึ้นจากการเคลื่อนที่ออกนอกระยะที่สามารถติดต่อกัน โหนดต้นทางจึงต้องมีการพยายามส่งข้อมูลหลายๆครั้งเพื่อเพิ่มอัตราความสำเร็จในการส่งข้อมูล หรือต้องรอเวลาให้โหนดปลายทางเดินทางกลับมาในระยะที่ติดต่อสื่อสารกันได้เสียก่อน

ปัญหาต่างๆเหล่านี้ที่เกิดขึ้นใน DTN วิธีการติดต่อสื่อสารกันแบบต่างๆที่ใช้ในเครือข่ายแบบปกติไม่สามารถนำมาใช้ใน DTN ได้ จึงต้องมีการกำหนดโปรโตคอลต่างๆสำหรับ DTN ขึ้นมาใหม่ให้สามารถรองรับกับการส่งข้อมูลที่ไม่ต่อเนื่องได้ เช่น การกระจายข้อมูลไปโหนดอื่นๆเพื่อช่วยส่งต่อไปยังโหนดปลายทาง หรือการกำหนดเส้นทางจากการคาดเดารูปแบบการเดินทางของโหนด เป็นต้น นอกจากนั้นยังมีการกำหนดการจัดการเครือข่ายในด้านอื่นๆ รวมทั้งทางด้านความปลอดภัยที่ใช้ใน DTN ขึ้นมาใหม่ให้รองรับกับสภาพแวดล้อม โดยเน้นการลดการติดต่อสื่อสารที่ไม่จำเป็นออก เพื่อลดทรัพยากรที่มีอยู่จำกัดบน DTN ทั้งในด้านของแบนวิทธ์และแบตเตอร์รี่ที่มีอยู่จำกัด เป็นต้น

ใน DTN นั้นจำเป็นที่จะต้องมีการรักษาความปลอดภัยบนเครือข่าย เช่นเดียวกับระบบเครือข่ายแบบปกติทั่วไป ระบบหนึ่งที่นิยมนำมาใช้และแก้ปัญหาทางด้านความปลอดภัยบนได้ดีคือการเข้ารหัสข้อมูลแบบ Identity Based Cryptography (IBC) เนื่องจากสามารถเข้ารหัสข้อมูลที่ส่งออกไปทำให้ยากต่อการดักจับข้อมูล และแต่ละโหนดจะต้องมีการยืนยันตัวเองก่อนจึงจะสามารถติดต่อสื่อสารกันได้ ทำให้สามารถป้องกันการโจมตีแบบต่างๆจากบุคคลภายนอกได้

ระบบ IBC บน DTN พัฒนาขึ้นมาจากระบบ Public Key Infrastructure (PKI) ซึ่งเป็นการเข้ารหัสข้อมูลที่นิยมใช้กันบนเครือข่ายแบบปกติ โดยใน IBC จะอนุญาตให้แต่ละยูสเซอร์สามารถใช้ Private Key Generater (PKI) ในการสร้าง Private Key ของตนเอง และสร้าง Public Key ของยูสเซอร์อื่นๆได้จากการใช้พารามิเตอร์ที่ใช้ระบุตัวตนของยูสเซอร์ เช่น ชื่อเครื่อง หมายเลขไอพี หรือ Mac Address เป็นต้น แทนการกระจาย Public Key ให้กับยูสเซอร์อื่นๆในระบบ PKI ทำให้สามารถลดภาระในการติดส่อสื่อสารบนเครือข่ายลงได้ แต่ทั้งนี้การใช้งาน PKG เพื่อสร้างกุญแจในแต่ละยูสเซอร์นั้นเป็นการใช้งาน PKG ตัวเดียวกันทั้งเครือข่าย ซึ่งทำให้มีข้อจำกัดบางประการอยู่ ทำให้ความปลอดภัยเครือข่ายนั้นมีน้อยกว่าการใช้งานระบบ PKI แบบเดิมได้แก่

- ยูสเซอร์อาจมีการปลอมแปลง Private Key ของยูสเซอร์อื่นๆได้ เนื่องจาก PKG สามารถสร้างกุญแจต่างๆของ User อื่นๆได้ทั้งหมด
- ยูสเซอร์ไม่สามารถปกปิด Public Key ของตนเองกับบางยูสเซอร์ที่ไม่ต้องการ แต่ใช้บนเครือข่ายเดียวกันได้ เนื่องจากใน PKG จะส่งพารามิเตอร์สำหรับสร้าง Public Key นั้นเป็นข้อมูลทั่วไปที่ทุกเครื่องสามารถทราบได้ การติดต่อสื่อสารกันภายในเครือข่ายกลุ่มใหญ่กลุ่มเดียวไม่สามารถแบ่งเป็นกลุ่มย่อยๆที่ใช้กุญแจที่แตกต่างกันได้
- ไม่สามารถเปลี่ยนแปลงหรือเพิกถอนกุญแจที่มีอยู่เดิมได้ เนื่องจากพารามิเตอร์ที่ใช้ระบุตัวตันเพื่อสร้าง Public Key จาก PKG ตั้งค่าที่ผูกติดกับตัวเครื่องเพื่อให้ยูสเซอร์อื่นๆทราบได้โดยง่าย เช่น ชื่อเครื่อง

หมายเลขไอพี หรือ Mac Address เป็นต้น หากต้องการเปลี่ยน Public Key พารามเตอร์เหล่านี้

ในงานวิจัยชิ้นนี้จึงได้นำเสนอแนวทางการแก้ไขปัญหาการใช้ PKG ทั้งสองอย่าง โดยปัญหาการปลอมแปลง Private Key นั้นจะใช้อัลกอริทึมเพื่อตรวจสอบกระบวนการสร้าง Private Key โดยตรวจสอบว่า Private Key ที่สร้างขึ้นมานั้นเป็น Private Key ของตนเองหรือไม่ หากไม่ใช่จะลบทิ้งไป ส่วนปัญหาของการไม่สามารถปกปิด Public Key ได้ เพื่อแบ่งกลุ่มของยูสเซอร์ได้จะใช้การสร้างกุญแจย่อยขึ้นมาอีกหนึ่งชุดจาก PKG เดิม โดยใช้พารามิเตอร์เดิมที่ใช้ระบุตัวตนร่วมกับข้อมูลเวลาเพื่อสร้าง Public Key และ Private Key ชุดใหม่สำหรับการติดต่อสื่อสารกันในเฉพาะยูสเซอร์ที่ต้องการเท่านั้น รวมทั้งใช้ข้อมูลเวลาในส่วนในการกำหนดอายุของกุญแจที่สร้างขึ้นมาเพื่อแก้ไขปัญหาเดิมที่ไม่สามารถยกเลิกหรือเปลี่ยนแปลงกุญแจเดิมได้

2. งานวิจัยที่เกียวข้อง

ในส่วนนี้จะกล่าวถึงงานวิจัยทางด้านการรักษาความปลอดภัยบน DTN ทั้งในแบบที่อาศัยการเข้ารหัสข้อมูลที่มีพื้นฐานมาจาก IBC และ PKI และการป้องกันการโจมตีแบบต่างๆ รวมถึงการทำงานเบื้องต้นของ IBC และ PKI

2.1 การรักษาความปลอดภัยของ DTN

ในงานวิจัยทางด้านการรักษาความปลอดภัยบน DTN นั้น มีทั้งในรูปแบบของการกำหนดโปรโตคอลกำหนดเส้นทาง เช่น งานวิจัยของ Feng Cheng Lee [9] ใช้วิธีการเข้าติดตามคุณสมบัติของความน่าจะเป็น เรียกว่า Probabilistic Routing Protocol using History of Encounters and Transitivity (PRoPHET) จะใช้ประวัติการเคลื่อนที่ของโหนดเป็นตัวแปรในการตัดสินใจเพื่อกำหนดเส้นทาง นอกจากนั้นตัวแปรเหล่านี้ยังสามารถใช้ในการรักษาความปลอดภัยใน DTN ได้ด้วย โดยที่ PRoPHET สามารถทำงานได้โดยไม่จำเป็นที่จะต้องทราบข้อมูลโครงสร้างต่างๆภายในเครือข่ายทั้งหมด จึงมีความเหมาะสมกับการทำงานบน DTN ในงานวิจัยนี้มี attack คือ การโจมตีแบบฟลัด (flooding attack) และงานวิจัยของ Ahmad [1] ใช้ CSP ที่มีการคำนวณใหม่โดยใช้ Failure Divergence Model (FDR) สำหรับการเช็ค เป็นการรักษาความปลอดภัยในเครือข่ายที่ทนต่อความล่าช้าโดยไม่ได้อาศัยการเข้ารหัสข้อมูล แต่ใช้การคำนวณค่า Failure และมีการเปรียบเทียบกับ CSP ที่ยังไม่มีการคำนวณ เพื่อป้องกันการโจมตีแบบ Denial of Service (DOS)

นอกจากนั้นยังมีการรักษาความปลอดภัยแบบบน DTN ที่ใช้การเข้ารหัสข้อมูลแบบต่างๆ เช่น การเข้ารหัสแบบ BEK [1] หรือเรียกว่า bundle encrypting key ที่มีการทำงานคล้ายกับ PKI ซึ่งสามารถใช้งานได้ดีแต่ยังมีข้อบกพร่องทางด้านความล่าช้าเมื่อนำมาใช้งานใน DTN การรักษาความปลอดภัยแบบอื่นๆที่ IBC ที่พัฒนามาจาก PKI มาใช้งานเพื่อป้องกันการโจมตีในสภาวะแวดล้อมแบบต่างๆ และลดภาระการส่งข้อมูลจากการใช้ PKI เช่น งานวิจัยของ M.R. Fida [7], Farrell S. และ Cahill V [12], A. Seth และ S. Keshav [5], P.T. Edelman [4] เพื่อยืนยันตัวตนเข้ารหัสข้อมูลและป้องกันการโจมตีแบบ DOS ได้ และมีการใช้ในการป้องกันการโจมตีแบบ pollution attack [11] ได้อีกด้วย

การใช้งาน IBC ได้มีการพัฒนาในรูปแบบต่างๆเพื่อให้รองรับเครือข่ายที่มีขนาดใหญ่ขึ้นซึ่งเรียกว่า Hierarchical Identity Based Cryptography (HIBC) [8] และการเข้ารหัสแบบ SOK [10] ซึ่งทั้งสองมีการทำงานที่คล้ายกันคือใช้ PKG สองชุดต่อหนึ่งยูสเซอร์ ชุดแรกเรียกว่า Local PKG ใช้สำหรับติดต่อสื่อสารระหว่างยูสเซอร์ที่อยู่ภายในโดเมนหรือเราท์เตอร์เดียวกัน อีกชุดเรียกว่า Long Range PKG สำหรับสื่อสารนอกโดเมน โดยมีการเรียงลำดับชั้นของ PKG ในรูปแบบของผังต้นไม้เพื่อลดภาระการทำงานของ PKG เมื่อใช้งานในเครือข่ายที่มีขนาดใหญ่

ตารางที่ 1 เปรียบเทียบการรักษาความปลอดภัยบน DTN ในรูปแบบต่างๆ

Security of DTN	วิธีการ	ประเภทการถูกโจมตี	เปรียบเทียบ	โปรโตคอล	สภาพแวดล้อม
Hierarchical Identity Based Cryptography for End-to-End Security in DTNs	มีการเข้ารหัสข้อมูลแบบ IBC	No attack	มีการเปรียบเทียบกับการเข้ารหัสแบบ PKI	BAH, PSH	มีผล
Secure Network Coding in DTNs	ใช้ลายเซ็นเข้ารหัสเครือข่ายความปลอดภัย	pollution attack	มีการเปรียบเทียบกับการเข้ารหัสแบบ PKI	ไม่มี	ไม่มีผล
Security Considerations in Space and Delay Tolerant Networks	ใช้ข้อมูลการเข้ารหัสลับในการรักษาความปลอดภัย	DoS attack	มีการเปรียบเทียบระหว่างโปรโตคอล LTP และ Bundle Protocol	LTP, Bundle Protocol	มีผล
Pseudonymised communication in delay tolerant networks	ใช้ CSP ที่มีการคำนวณใหม่โดยใช้ Failure Divergence Model (FDR) สำหรับการเช็ค	DoS attacks, Traffic analysis attack	มีการเปรียบเทียบกับ CSP ที่ยังไม่มีการคำนวณ	TCP/IP protocol, Bundle Protocol	ไม่มี
Adaptive Service Provisioning for Emergency Communications with DTN	การเข้ารหัส BEK (ลายเซ็นดิจิตอล(	No attack	ไม่มี	Bundle Protocol	ไม่มี
SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks	SMART scheme, มีการเข้ารหัสข้อมูลแบบ IBC	No attack	มีการเปรียบเทียบกับการเข้ารหัสแบบ PKI	DTN routing protocol, SWB protocol	มีผล
Queuing Mechanism to Alleviate Flooding Attacks in Probabilistic Delay Tolerant Networks	วิธีการเข้าติดตามคุณสมบัติของความน่าจะเป็น	Flooding attack	มีการเปรียบเทียบกับการเข้ารหัสแบบ PKI	ProPHET	มีผล
Secure Group Communications for Delay-Tolerant Networks	มีการเข้ารหัสข้อมูลแบบ IBC	No attack	มีการเปรียบเทียบกับการเข้ารหัสแบบเดิม	Bundle Protocol, SGCP, SGA	มีผล

ตารางที่ 2 เปรียบเทียบการรักษาความปลอดภัยบน DTN ในรูปแบบต่างๆ(ต่อ)

Security of DTN	วิธีการ	ประเภทการถูกโจมตี	เปรียบเทียบ	โปรโตคอล	สภาพแวดล้อม
Anonymity and Security in Delay Tolerant Networks	มีการเข้ารหัสข้อมูลแบบ SOK	No attack	มีการเปรียบเทียบกับการเข้ารหัสแบบ PKI	ไม่มี	มีผล
Practical Security for Disconnected Nodes	มีการเข้ารหัสแบบ IBC	redirection attacks, DoS attack	มีการเปรียบเทียบกับการเข้ารหัสแบบ PKI	RTT Protocol	มีผล
Security Analysis of DTN Architecture and Bundle Protocol Specification for Space-Based Networks	ใช้ข้อมูลการเข้ารหัสลับในการรักษาความปลอดภัย	No attack	ไม่มี	Bundle Protocol	มีผล
Region-Based Security Architecture for DTN	มีการเข้ารหัสข้อมูลแบบ IBC	No attack	มีการเปรียบเทียบกับการเข้ารหัสแบบ PKI	ไม่มี	มีผล

จากตารางจะเห็นได้ว่าการรักษาความปลอดภัยมีทั้งแบบที่อาศัยการเข้ารหัสและใช้โปรโตคอลแบบอื่นๆ โดยที่การเข้ารหัสแบบ IBC นั้น สามารถป้องกันการโจมตีในแบบต่างๆได้มากที่สุด โดยการใช้งาน IBC นั้นมักจะใช้เปรียบเทียบกับการทำงานของ PKI ในเรื่องของการรับส่งข้อมูลที่น้อยกว่า แต่ทั้งนี้งานวิจัยต่างๆข้างต้นนั้นยังมีข้อจำกัดของการ PKG ใน IBC ตามที่ได้กล่าวไว้ในบทนำข้างต้น ทำให้ประสิทธิภาพทางด้านการรักษาความปลอดภัยยังมีจุดบกพร่องอยู่

2.2 การทำงานของ PKI และ IBC

การทำงานของระบบ Private Key Generater ที่ใช้ในระบบเครือข่ายทั่วไปนั้นมีการทำงานดังนี้

PKI จะใช้กุญแจในการเข้ารหัสและถอดรหัสข้อมูลประกอบด้วย กุญแจ Private Key และกุญแจ Public Key กุญแจทั้ง 2 นี้จะได้มาพร้อมกับใบรับรองที่ CA ออกให้ โดยการเข้ารหัสด้วยกุญแจหนึ่งจะต้องถอดรหัสด้วยอีกกุญแจหนึ่งเท่านั้น Private Key จะเก็บไว้ที่เจ้าของใบรับรองส่วน Public Key CA จะแจกจ่ายให้กับผู้อื่นเพื่อนำไปใช้ในการติดต่อกับเจ้าของใบรับรอง ทำให้มีความน่าเชื่อถือและความปลอดภัยมากขึ้นในการทำธุรกรรมอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต

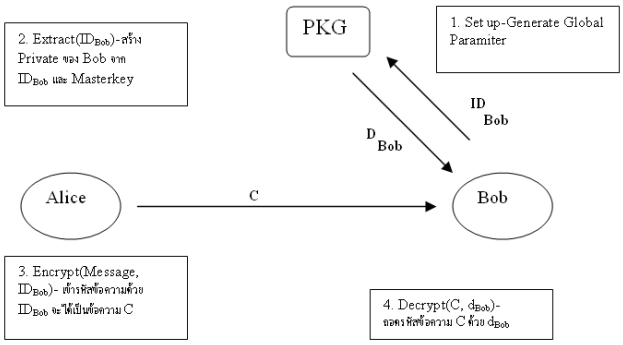
PKI Cryptography หรือ ระบบการเข้ารหัสลับ หมายถึงระบบที่ผู้ส่งข้อความเข้ารหัส (Encrypt) เปลี่ยนแปลงข้อมูลจากข้อความปกติ (Plain Text) ไปเป็นข้อความที่เข้ารหัส (Cipher text) หลังจากนั้นจึงส่งข้อความไปให้ผู้รับ ทางผู้รับจะถอดรหัสข้อมูล (Decrypt) เพื่อให้ได้ข้อความปกติเหมือนดังที่ส่งมา วัตถุประสงค์ของ Cryptography ก็เพื่อที่จะปกปิดข้อมูลให้เป็นความลับในระหว่างที่ส่งข้อมูล โดยแม้จะมีผู้แอบลักลอบดูข้อมูลก็ไม่สามารถอ่านข้อความนั้นๆได้ เนื่องจากจะได้เป็นข้อมูลที่อ่านไม่ออก เพราะไม่สามารถถอดรหัสให้อ่านออกได้

สรุปโดยปกติทั่วไปหน้าที่ของผู้ออกใบรับรองมีดังนี้

1. สร้างคู่กุญแจ (Key pairs) ตามคำขอของผู้ขอใช้บริการ
2. ออกใบรับรองฯ เพื่อยืนยันตัวบุคคลของผู้ขอใช้บริการ
3. จัดเก็บกุญแจสาธารณะ (Public Key) ในฐานข้อมูล
4. เปิดเผยกุญแจสาธารณะต่อสาธารณชนที่ติดต่อผ่านทางระบบเครือข่าย
5. ยืนยันตัวบุคคลที่เป็นเจ้าของกุญแจสาธารณะตามคำขอของบุคคลทั่วไป
6. เปิดเผยรายชื่อใบรับรองอิเล็กทรอนิกส์ที่ถูกยกเลิกแล้ว (Certificate Revocation List หรือ CRL) เพื่อเป็นการบอกแก่สาธารณชนว่าใบรับรองฯ นั้นไม่สามารถนำมาใช้ได้อีกต่อไป

การทำงานของ Identity Based Encryption ซึ่งเป็นระบบที่พัฒนามาจากระบบ PKI เพื่อใช้ใน DTN มีการทำงานที่เหมือนกัน แต่มีการปรับปรุงในด้านการแจกจ่ายกุญแจต่างๆให้แต่ละยูสเซอร์ สามารถสร้าง Public Key สำหรับติดต่อยูสเซอร์อื่นๆได้เอง โดยที่ยูสเซอร์ไม่ต้องส่งกระจาย Public Key ของตนไปให้ยูสเซอร์อื่นๆ ทำให้ลดภาระการทำงานของเครือข่ายเองได้ ซึ่งมีขั้นตอนต่างๆดังนี้

รูปที่ 1 การทำงานของ IBC

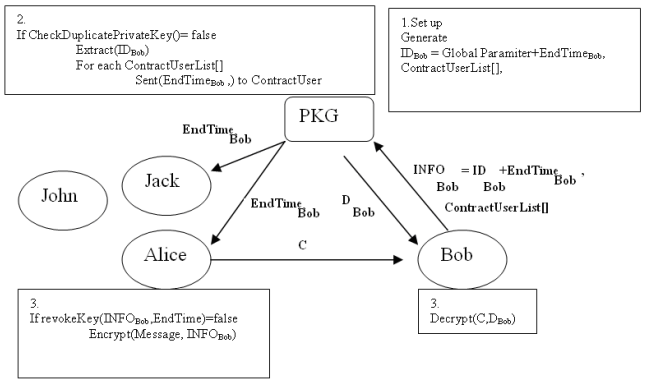


1. ขั้นตอนการติดตั้ง: เมื่อยูสเซอร์ได้ทำการเชื่อมต่อเข้ามาในระบบ Bob จะทำการส่ง Global System Parameters (จากรูปคือ ID_{Bob}) ซึ่งเป็นข้อมูลที่ใช้ระบุตัวตน (เช่น ชื่อยูสเซอร์,หมายเลข IP หรือ Mac address) ไปให้ PKG เพื่อสร้าง Private Key ของตน
2. ขั้นตอนกำหนด Key: ยูสเซอร์จะใช้ Master Key + Parameters สร้าง Private Key ของตนเองขึ้นมาโดยจะต้องเป็น Key ที่สามารถถอดรหัสข้อมูลที่เข้ารหัสโดย Public Key ของตนได้ จากนั้นจะสร้าง Public Key ของยูสเซอร์อื่นๆจาก Global System Parameters ที่มีอยู่
3. การเข้ารหัสข้อมูล: เมื่อ Alice ต้องการส่งข้อมูลไปหา Bob Alice จะใช้ Public Key ของ Bob ที่สร้างสร้างไว้แล้วเข้ารหัสข้อมูล แล้วจึงส่งไปหา Bob
4. การถอดรหัสข้อมูล: เมื่อ Bob ได้รับข้อมูลจาก Alice Bob จะใช้ Private Key ของตนถอดรหัสข้อมูลที่ได้รับมาจาก Alice

3. การปรับปรุงการทำงานของ IBC

สำหรับการแก้ไขปัญหาของ IBC นั้นจะใช้การปรับปรุงอัลกอริทึมของ PKG ในส่วนของการสร้างกุญแจทั้งสองแบบ เมื่อได้กุญแจมาแล้วในส่วนของการเข้ารหัสและถอดรหัสจะยังเหมือนกับ PKG เดิม โดยมีขั้นตอนการทำงานดังนี้

รูปที่ 2 การทำงานของ IBC ที่มีการปรับปรุง PKG แล้ว



1. ขั้นตอนการติดตั้ง: เมื่อยูสเซอร์ Bob เข้ามาในระบบจะทำการส่ง Global System Parameters(ID_{Bob}) เวลาสิ้นสุดการใช้งานของกุญแจ $EndTime_{Bob}$ และ ContractUserList ซึ่งเป็นรายชื่อยูสเซอร์ที่ต้องการติดต่อด้วย ไปให้ PKG โดยที่ $INFO_{Bob}$ นั้นจะได้จาก ID_{Bob} เดิม + $EndTime_{Bob}$

2. ขั้นตอนกำหนด Key: ก่อนที่จะสร้าง Private Key PKG จะทำการตรวจสอบก่อนว่า ยูสเซอร์นั้นมี Private Key เดิมหากมีจะไม่สามารถสร้างได้เพื่อป้องกันการปลอมแปลง Private Key ของยูสเซอร์อื่นๆ หากไม่มี Private Key เดิม PKG ก็จะทำการสร้าง Private Key จาก ID_{Bob} และ Master Key ขึ้นมา

หลังจากนั้น จะทำการกระจาย $EndTime_{Bob}$ ไปให้ยูสเซอร์ที่มีอยู่ใน ContractUserList เพื่อให้ยูสเซอร์ต่างๆนำ $EndTime_{Bob}$ ไปรวมกับ ID_{Bob} ให้เป็น $INFO_{Bob}$

จากนั้นยูสเซอร์ที่มี $INFO_{Bob}$ (จากภาพได้แก่ Aliceและ Jack) จะใช้ $INFO_{Bob}$ สร้าง Prublic Key ของ Bob ขึ้นมาไว้ใช้งาน

3. การเข้ารหัสข้อมูล: เมื่อ Alice (หรือ Jack) ต้องการส่งข้อมูลไปหา Bob Alice จะทำการตรวจสอบก่อน ว่าเวลาในปัจจุบันเกินเวลาที่ $EndTime_{Bob}$ แล้วหรือยัง หากเกินหมายถึง Public Key นั้นหมดอายุแล้วจะทำให้ Alice ไม่สามารถใช้ Public Key นั้นได้ หากยังไม่เกิน Alice จะใช้ Public Key ของ Bob ที่สร้างสร้างไว้แล้วเข้ารหัสข้อมูล แล้วจึงส่งไปหา Bob

4. การถอดรหัสข้อมูล: เมื่อ Bob ได้รับข้อมูลจาก Alice Bob จะใช้ Private Key ของตนถอดรหัสข้อมูลที่ได้รับมาจาก Alice

จากการทำงานข้างต้นจะเห็นได้ว่า IBC ที่ได้แก้ไขอัลกอริทึมของ PKG ใหม่จะมีความซับซ้อนและมีการรับส่งข้อมูลที่มากกว่าแบบเดิม แต่สามารถแก้ไขปัญหาต่างๆที่เกิดขึ้นในการใช้งาน PKG แบบเดิมได้

4. เปรียบเทียบการทำงานของระบบ IBC เดิม และ IBC แบบใหม่

ในหัวข้อนี้จะกล่าวถึงการเปรียบเทียบอัลกอริทึมของ PKG แบบเดิมและแบบที่ได้รับการแก้ไขแล้วว่ามีความซับซ้อนและมีการติดต่อสื่อสารที่เพิ่มขึ้นมาแตกต่างกันเท่าไหร่ และคุ้มค่าหรือไม่หากต้องมีการใช้ทรัพยากรเพิ่มขึ้นเพื่อแก้ไขปัญหาต่างๆที่มีอยู่บน PKG แบบเดิม

อัลกอริทึมของการทำงาน PKG แบบเดิมมีดังนี้

1. ขั้นตอน Set Up
   Setup{
   Get ID_{user}
   }
2. ขั้นตอนการสร้าง Private Key
   Private Key_{user} = Extract(ID_{user})
   sent($PrivateKey_{user}$) to User
   ขั้นตอนการสร้าง Public Key
   Public Key_{user} = ID_{user}
3. ขั้นตอนการ Encrypt ข้อมูล
   C = Encrypt(Message,ID_{user})
   sent(C)
4. ขั้นตอนการ DeCrypt ข้อมูล
   recive(C)
   Decrypt(C,$PrivateKey_{user}$)

จากอัลกอริทึมข้างต้นจะเห็นได้ว่าเวลาการทำงานเป็นค่าคงที่หากเขียนในรูปของ Big-O จะได้ว่า O(c) และมีจำนวนการติดต่อสื่อสารสามครั้ง คือครั้งแรกในขั้นตอนการ set up เพื่อส่งค่า ID_{user} ไปให้ PKG และครั้งที่สองคือ PKG ส่ง Private Key กลับมาให้ ส่วนครั้งสุดท้ายคือการส่งข้อความจากต้นทางไปยังปลายทาง

อัลกอริทึมของการทำงาน PKG แบบใหม่มีดังนี้

1. ขั้นตอน Set Up
   Setup{
   INFOuser=IDuser+EndTimeuser
   Get $INFO_{user}$,$EndTime_{user}$,ContractUserList[]
   }
2. ขั้นตอนการสร้าง Private Key
   if duplicateKey = false{
   Private Key_{user} = Extract($INFO_{user}$)
   sent($PrivateKey_{user}$) to User
   Foreach ContractUserList[]{
   sent($EndTime_{user}$)
   }
   }
   ขั้นตอนการสร้าง Public Key
   Public Key_{user} = $INFO_{user}$

3. ขั้นตอนการ Encrypt ข้อมูล

```
if currentTime < EndTimeUser{
        C = Encrypt(Message,ID_user)
        sent(C)
}else{
        Revoke(Public Key_user)
}
```

4. ขั้นตอนการ DeCrypt ข้อมูล

```
recive(C)
Decrypt(C,PrivateKey_user)
```

จะเห็นได้ว่าอัลกอริทึมใหม่จะมีการทำงานที่ซับซ้อนขึ้น โดยต้องมีการวนลูปเพื่อส่งข้อมูล $EndTime_{user}$ ไปให้ยูสเซอร์อื่นๆ ทำให้ค่า Big-O มีค่าเท่ากับ O(n) และการติดต่อสื่อสารมีจำนวน 3+n ครั้ง โดยสามครั้งแรกจะเป็นกระบวนการเดียวกับ PKG แบบเดิม n ครั้งคือ จำนวนที่ต้องส่งข้อมูล $EndTime_{user}$ ไปหายูสเซอร์ที่ต้องการ

ตารางที่ 3 เปรียบเทียบการทำงานของ PKG

PKG	Big-O	การติดต่อสื่อสาร	ปัญหาการปลอมแปลง **Private Key**	ปัญหาการแบ่งกลุ่มย่อย	ปัญหาการยกเลิก **Key**
แบบเดิม	**O(c)**	**3**	มี	มี	มี
แบบใหม่	**O(n)**	**3+n**	แก้ไขได้	แก้ไขได้	แก้ไขได้

จากตารางจะเห็นได้ว่า PKG แบบใหม่จะความเร็วในการทำงานน้อยกว่าแบบแรก แต่สามารถแก้ไขปัญหาต่างๆได้ หากจำนวนยูสซอร์ที่ต้องการติดต่อสื่อสารนั้นมีน้อย ความเร็วในการทำงาน PKG แบบใหม่ก็จะเพิ่มขึ้น ซึ่งหมายความว่า PKG แบบใหม่นั้นเหมาะสมกับการทำงานที่มียูสเซอร์ในระบบจำนวนไม่มากนั่นเอง

5. สรุปผลการวิจัย

จากผลการทำงาน ในการแก้ไขปัญหาของ IBC ได้แก่ การป้องกันการปลอมแปลง Private Key, การปกปิด Public Key เพื่อแบ่งกลุ่มของยูสเซอร์, และปัญหาที่ไม่สามารถเปลี่ยนแปลงหรือเพิกถอน Public Key ได้ ทั้งหมดสามารถแก้ไขได้จากการพัฒนาอัลกอริทึมของ PKG จากเดิม โดยที่ PKG ใหม่ จะมีความซับซ้อนและต้องการการติดต่อสื่อสารที่มากขึ้น โดยหากยูสเซอร์มีจำนวนน้อย อัลกอริทึมจะสามารถทำงานได้เร็ว หากยูสเซอร์มากขึ้นจะมีการทำงานที่ช้าลง จึงสามารถสรุปได้ว่าอัลกอริทึม PKG แบบใหม่ บนเครือข่าย DTN ที่มีจำนวนยูสเซอร์จำนวนไม่มาก

สำหรับแนวทางการพัฒนางานวิจัยต่อนั้น ได้แก่การนำอัลกอริทึม PKG ใหม่ไปใช้งานในระบบจริงเพื่อทดสอบประสิทธิภาพ และนำไปใช้ร่วมกับอัลกอริทึมแบบอื่นๆ เช่น HIBC เพื่อให้สามารถรองรับยูสเซอร์ที่มีจำนวนมากขึ้นได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

6. บรรณานุกรม

[1] N. Ahmad, H. Cruickshank, S. Zhili and M. Asif, "Pseudonymised communication in delay tolerant networks," in Proc.of 2011 Ninth Annual International Conference on Privacy, Security and Trust (PST), 2011, pp.1-6.

[2] J. Peng, J. Bigham, and E. Bodanese, “Adaptive Service Provisioning for Emergency Communications with DTN,” in Proc.of 2011 IEEE Wireless Communications and Networking Conference (WCNC), 2011, pp.2125-2130.

[3] Z. Haojin, L. Xiaodong, L. Rongxing , F. Yanfei Fan and S. Xuemin Shen, “SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks,” in Proc.of IEEE Transactions on Vehicular Technology, 2011, pp.4628-4639.

[4] P.T. Edelman, M.J. Doonahoo, D.B. Sturgill, "Secure group communications for Delay-Tolerant Networks", Proc. of International Conference for Internet Technology and Secured Transactions (ICITST),2010,pp.1-8.

[5] A. Seth, S. Keshav, "Practical security for disconnected nodes" in Proc. of 1st IEEE ICNP Workshop on Secure Network Protocols, 2005, pp.31-36.

[6] W.D. Ivancic, “Security analysis of DTN architecture and Bundle Protocol Specification for space-based networks,” in Proc.of 2010 IEEE Aerospace onference, 2010, pp. 1-12.

[7] M.R. Fida, M. Ali, A. Adnan, A.S. Arsalaan, “Region-Based Security Architecture for DTN,” in Proc.of 2011 Eighth International Conference on Information Technology: New Generations (ITNG), 2011, pp. 387-392.

[8] R.Patra,S.Surana and S.Nedevschi, "Hierarchical Identity Based Cryptography for End-to-End Security in DTNs",in Proc.of 4th International Conference on Intelligent Computer Communication and Processing,pp.223 - 230,2008

[9] Feng Cheng Lee, Weihan Goh and Chai Kiat Yeo, "A Queuing Mechanism to Alleviate Flooding Attacks in Probabilistic Delay Tolerant Networks ", Telecommunications (AICT), 2010 Sixth Advanced International Conference on, 2010, pp. 329 - 334.

[10] Kate, Aniket, Zaverucha Gregory M. and Hengartner Urs, "Anonymity and security in delay tolerant networks", Security and Privacy in Communications

Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on , 2007, pp.504 - 513.

[11] Czap L.,Vajda I., "Secure Network Coding in DTNs ", Communications Letters, IEEE, 2011, pp.28 - 30.

[12] Farrell S. Cahill V., “Security considerations in space and delay tolerant networks”, Space Mission Challenges for Information Technology, 2006. SMC-IT 2006. Second IEEE International Conference on, 2006, pp.8 – 38.