การพัฒนาการสื่อสารที่มีความน่าเชื่อถือบนพื้นที่ภัยพิบัติ

นายธนภัทร เรืองสาตรา

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2558

Development of Trusted Communication for Disaster Recovery

Mr. Tanapat Ruengsatra

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Engineering Program in Computer Engineering
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2015

หัวข้อวิทยานิพนธ์	การพัฒนาการสื่อสารที่มีความน่าเชื่อถือบนพื้นที่ภัยพิบัติ
โดย	นายธนภัทร เรืองสาตรา
สาขาวิชา	วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร.กุลธิดา โรจน์วิบูลย์ชัย
อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม	ผู้ช่วยศาสตราจารย์ ดร.เกริก ภิรมย์โสภา

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะวิศวกรรมศาสตร์

(ศาสตราจารย์ ดร.บัณฑิต เอื้ออาภรณ์)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.ณัฐวุฒิ หนูไพโรจน์)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

(รองศาสตราจารย์ ดร.กุลธิดา โรจน์วิบูลย์ชัย)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

(ผู้ช่วยศาสตราจารย์ ดร.เกริก ภิรมย์โสภา)

.....กรรมการภายนอกมหาวิทยาลัย

(รองศาสตราจารย์ ดร.อนันต์ ผลเพิ่ม)

ธนภัทร เรืองสาตรา : การพัฒนาการสื่อสารที่มีความน่าเชื่อถือบนพื้นที่ภัยพิบัติ (Development of Trusted Communication for Disaster Recovery) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: รศ. ดร.กุลธิดา โรจน์วิบูลย์ชัย, อ.ที่ปรึกษาวิทยานิพนธ์ร่วม: ผศ. ดร. เกริก ภิรมย์โสภา, หน้า.

งานวิจัยนี้ได้เสนอการสื่อสารที่มีความน่าเชื่อถือบนพื้นที่ภัยพิบัติเมื่อเกิดภัยพิบัติขึ้น โครงสร้างพื้นฐาน จะถูกทำลายลงทำให้ผู้คนไม่สามารถสื่อสารกันในบริเวณพื้นที่ภัยพิบัติได้ ด้วยระบบการสื่อสารที่มีความน่าเชื่อถือนี้จะทำให้ ผู้คนในพื้นที่ภัยพิบัติสามารถสื่อสารกันได้อย่างทั่วถึง อีกทั้งผู้ประสบภัยยังได้รับข้อมูลที่มีความน่าเชื่อถือเพื่อเป็นประโยชน์ในสถานการณ์ภัยพิบัติ อีกทั้งผู้ประสบภัยยังสามารถแลกเปลี่ยนข้อมูลกับผู้ช่วยเหลือทำให้ผู้ประสบภัยสามารถได้รับความช่วยเหลือได้ทันท่วงที

ในการสร้างการสื่อสารบนพื้นที่ภัยพิบัตินั้น เครือข่ายแอดฮอกเป็นเครือข่ายที่เหมาะสมที่จะนำมาใช้แทนที่การสื่อสารในพื้นที่ภัยพิบัติได้เพราะเป็นเครือข่ายการสื่อสารที่ทำการติดตั้งง่ายและสามารถสื่อสารได้โดยไม่ต้องพึ่งพิงเครือข่ายอื่น เครือข่ายแอดฮอกนั้นสามารถติดตั้งบนพื้นที่ภัยพิบัติได้สองรูปแบบคือ เครือข่ายแอดฮอกแบบ peer-to-peer และการสร้างโครงสร้างพื้นฐานด้วยเครือข่ายแอดฮอกอย่างไรก็ตามการติดตั้งเครือข่ายแอดฮอกทั้งสองวิธีดังกล่าวยังไม่สามารถให้ความยืดหยุ่นในการสื่อสารและความเสถียรในการส่งสัญญาณพร้อมกันได้

งานวิจัยนี้จึงได้พัฒนาโครงสร้างการสื่อสารที่รวมกันระหว่างเครือข่ายแอดฮอกแบบ peer-to-peer และเครือข่ายแอดฮอกแบบโครงสร้างพื้นฐานทำให้ได้รับการสื่อสารที่มีความเสถียรและมีความยืดหยุ่นในการสื่อสาร นอกจากนั้นงานวิจัยนี้ยังได้พัฒนาระบบสื่อสารให้มีความน่าเชื่อถือ โดยพัฒนาวิธีการในการยืนยันตัวตนระหว่างการส่งข้อมูลอย่างมีประสิทธิภาพ ทำให้ผู้ใช้ระบบสื่อสารนั้นจะได้รับข้อมูลที่มีความน่าเชื่อถือโดยที่ไม่ส่งผลกระทบต่อความสามารถในการส่งข้อมูลของระบบสื่อสาร

จากผลการทดลองยังแสดงให้เห็นระบบการสื่อสารสามารถทำการส่งข้อมูลจากผู้ประสบภัยถึงผู้ช่วยเหลือด้วยความสามารถในการส่งข้อมูลมากกว่า 98% และส่งข้อมูลไปยังศูนย์กู้ภัยด้วยความสามารถในการส่งข้อมูลมากว่า 75% นอกจากนั้นผลการแสดงการวิเคราะห์ความปลอดภัยยังแสดงให้เห็นว่าระบบสื่อสารที่ได้พัฒนาขึ้นมานั้นสามารถป้องกันการโจมตีได้ 8 รูปแบบ [20]

ภาควิชา	วิศวกรรมคอมพิวเตอร์	ลายมือชื่อนิสิต .....
สาขาวิชา	วิศวกรรมคอมพิวเตอร์	ลายมือชื่อ อ.ที่ปรึกษาหลัก .....
ปีการศึกษา	2558	ลายมือชื่อ อ.ที่ปรึกษาร่วม .....

5770188921 : MAJOR COMPUTER ENGINEERING
KEYWORDS: AUTHENTICATION / MANET / DISASTER RECOVERY / HYBRID COMMUNICATION APPROACH / MULTI-DESTINATION / TRUSTWORTHY / PUBLIC KEY

TANAPAT RUENGSATRA: Development of Trusted Communication for Disaster Recovery. ADVISOR: ASSOC. PROF. KULTIDA ROJVIBOONCHAI, Ph.D., CO-ADVISOR: ASST. PROF. KRERK PIROMSOPA, Ph.D., pp.

We propose trusted communication system for disaster recovery situation. In disaster situation, infrastructures are always destroyed. It results in lacking of communication system in disaster area so victims cannot communicate to rescuers to request for help. Our system allows people in disaster area to communicate to each other properly. Therefore, rescuers are able to provide help to victims in time.

To create communication system in disaster area, mobile ad-hoc network (MANET) is considered to replace the ordinary communication system because it can be deployed in the area easliy and also does not depend on other networks. There are two approaches to deploy MANET: peer-to-peer approach and infrastructure approach. However, both approaches have limitation in flexibility and stability.

We developed a communication system which combines both approaches together. Our system can overcome the limitation of existing approaches by providing flexibility and stability together. Moreover, we also improve security to our communication system by developing authentication approach and embedded to the system. Our authentication approach allows the system to have trustworthyness without compromising the networks.

The results show that the system can have capability to transmit data from victims to rescuers with more than 98% of packet delivery ratio and also have capability to transmit data to base station with 75% of packet delivery ratio. Moreover, we also show the security analysis of the system. The analysis shows our approach can protect 8 types of attacks [20]

Department:	Computer Engineering	Student's Signature .....
Field of Study:	Computer Engineering	Advisor's Signature .....
Academic Year:	2015	Co-Advisor's Signature .....

กิตติกรรมประกาศ

ข้าพเจ้าขอขอบพระคุณอาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก รศ. ดร.กุลธิดา โรจน์วิบูลย์ชัย และ อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม ผศ. ดร.เกริก ภิรมย์โสภา ที่ให้ความช่วยเหลือ ความรู้ ข้อคิด และคำแนะนำที่เป็นประโยชน์ต่อการจัดทำวิทยานิพนธ์นี้ให้สำเร็จลุล่วงไปด้วยดี ขอขอบคุณ ผศ. ดร.ณัฐวุฒิ หนูไพโรจน์ และ รศ. ดร.อนันต์ ผลเพิ่ม ที่ให้คำแนะนำ และแนวคิดที่เป็นประโยชน์ต่อการทำวิทยานิพนธ์นี้

ขอขอบคุณเพื่อนนิสิต หลักสูตร วิศวกรรมศาสตร์มหาบัณฑิต ที่ช่วยให้คำแนะนำในการพัฒนาโปรแกรม นอกจากนี้ข้าพเจ้าขอขอบคุณพี่ๆ สมาชิกห้องปฏิบัติInformation System and Engineering Lab (ISEL) ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ที่ให้คำแนะนำ และความช่วยเหลือจนกระทั่งวิทยานิพนธ์นี้สำเร็จ

ขอขอบพระคุณครอบครัวของข้าพเจ้า ที่เข้าใจ มอบกำลังใจและให้ความสนับสนุนแก่ข้าพเจ้าเสมอมา ท้ายที่สุดนี้ ขอขอบพระคุณภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ที่ให้ทุนการศึกษาอัจฉริยะคืนรัง รวมถึงบัณฑิตวิทยาลัย จุฬาลงกรณ์ มหาวิทยาลัย ที่ให้ทุนสนับสนุนการนำเสนอผลงานวิจัยในต่างประเทศแก่ข้าพเจ้า

สารบัญ

หน้า

หน้า

หน้า

สารบัญรูปภาพ

สารบัญตาราง

บทที่ 1 บทนำ

ปัญหาและความสาคัญของปัญหา

การเกิดภัยพิบัติมีแนวโน้มที่จะเพิ่มขึ้นทุกปี ภัยพิบัติได้สร้างความเสียหายแก่บ้านเรือนและผู้ประสบภัยเป็นจำนวนมาก อีกทั้งยังส่งผลกระทบต่อพื้นที่ใกล้เคียงเป็นบริเวณกว้าง การกู้คืนการสื่อสารบนพื้นที่ภัยพิบัติจึงเป็นสิ่งจำเป็นสำหรับพื้นที่ที่ได้รับภัยพิบัติและพื้นที่รอบข้างที่ได้รับผลกระทบ การสื่อสารได้เข้ามามีบทบาทสำคัญในการกู้คืนภัยพิบัติเพราะการสื่อสารทำให้ผู้ประสบภัยสามารถร้องขอความช่วยเหลือจากทีมกู้ภัยได้อย่างทันท่วงที มีงานวิจัยหลายงานที่สร้างขึ้นมาเพื่อกู้คืนการสื่อสารบนพื้นที่ภัยพิบัติ โดยการกู้คืนการสื่อสารบนพื้นที่ภัยพิบัตินี้สามารถแยกออกเป็น 2 ประเภทได้ดังนี้

งานวิจัยประเภทแรกสร้างการสื่อสารบนพื้นที่ภัยพิบัติโดยใช้เครือข่าย Peer-to-peer ในการติดต่อสื่อสาร งานวิจัยประเภทนี้ใช้อุปกรณ์สื่อสารของผู้ประสบภัย และผู้ช่วยเหลือเป็นสื่อในการสื่อสาร เครือข่ายการสื่อสารจะถูกสร้างขึ้นมาโดยอาศัยเครือข่ายฮอทสปอท หรือ เครือข่ายแอดฮอก การสื่อสารในรูปแบบ Peer-to-peer นั้นมีข้อดีตรงที่ผู้ประสบภัยสามารถสื่อสารเพื่อขอความช่วยเหลือได้อย่างง่ายดายผ่านอุปกรณ์สื่อสารของตนเอง อย่างไรก็ตามปัญหาที่สำคัญของการสื่อสารแบบ Peer-to-peer คือปัญหาด้านความน่าเชื่อถือของข้อมูล เมื่อผู้ประสบภัยได้รับข้อความผู้ประสบภัยไม่อาจทราบได้อย่างแน่ชัดว่าข้อมูลนี้มาจากผู้ช่วยเหลือจริงและเป็นข้อมูลที่ถูกต้อง ผู้ไม่ประสงค์ดีอาจทำการปลอมแปลงข้อมูลเมื่อผลประโยชน์บางอย่างได้อีกทั้งข้อมูลที่ผู้ประสบภัยได้รับนั้นอาจจะเป็นข้อความที่มีความน่าเชื่อถือและความถูกต้องต่ำก่อให้เกิดความจลาลขึ้นในสถานการภัยพิบัติ นอกจากนี้การสื่อสารประเภทนี้จะมีการสูญเสียของข้อมูลสูงเนื่องจากเส้นทางส่งข้อมูลไปยังปลายทางนั้นขึ้นกับอุปกรณ์สื่อสารของเพื่อนบ้านซึ่งเคลื่อนที่ตลอดเวลา ทำให้การสื่อสารไม่คงที่ อีกทั้งอุปกรณ์สื่อสารบางกลุ่มจะไม่สามารถใช้งานการสื่อสารแบบแอดฮอกได้ ทำให้รูปแบบการสื่อสารแบบนี้จึงยังไม่เหมาะสม

งานวิจัยประเภทที่สองสร้างการสื่อสารบนพื้นที่ภัยพิบัติโดยอาศัยเครือข่ายโครงสร้างพื้นฐานที่มีอยู่หรือนำมาติดตั้งเองบนพื้นที่ภัยพิบัติ งานวิจัยส่วนมากจะเน้นไปที่การติดตั้งโครงสร้างพื้นฐานใหม่บนพื้นที่ภัยพิบัติโดยโครงสร้างพื้นฐานที่นำมาติดตั้งนั้นอาจจะอยู่ในรูปแบบของบอลลูนแอดฮอก หรือ จะเป็นเราท์เตอร์ไร้สายก็ได้ การสื่อสารประเภทนี้สามารถให้ความเสถียรของการเชื่อมต่อได้สูงกว่าเมื่อเทียบกับการสื่อสารโดยใช้เครือข่าย Peer-to-peer แม้ว่าการสื่อสารประเภทนี้จะสามารถใช้งานได้กับอุปกรณ์สื่อสารที่หาซื้อได้ในปัจจุบัน แต่ข้อจำกัดของการสื่อสารประเภทนี้คือไม่อาจสามารถครอบคลุมพื้นที่ภัยพิบัติได้ทั้งบริเวณ การที่จะติดตั้งโครงสร้างพื้นฐานให้ทั่วทั้งบริเวณพื้นที่ภัยพิบัตินั้น

เป็นไปได้ยากมากทำให้ขาดความยืดหยุ่นในการสื่อสาร เช่นในบริเวณที่มีสิ่งกีดกันสัญญาณเป็นต้น อีกทั้งการสื่อสารรูปแบบนี้ยังต้องอาศัยเวลาในการติดตั้งโครงสร้างพื้นฐาน ทำให้มีความล่าช้า ไม่สามารถใช้งานได้ทันที

สถานการณ์ภัยพิบัติเราสามารถแบ่งพื้นที่ประสบภัยออกได้เป็นสองบริเวณดังนี้ บริเวณแรกเป็นพื้นที่ที่หน่วยกู้ภัยสามารถติดตั้งเครือข่ายโครงสร้างพื้นฐานได้ ผู้ประสบภัยบริเวณนี้สามารถใช้อุปกรณ์สื่อสารติดต่อกับเครือข่ายโครงสร้างพื้นฐานได้โดยตรงเพื่อขอความช่วยเหลือข้อความจะถูกผ่านโครงสร้างพื้นฐานไปยังศูนย์กู้ภัยหรือเจ้าหน้าที่โดยตรง จากนั้นศูนย์กู้ภัยจะส่งผู้ช่วยเหลือไปยังบริเวณที่ข้อความถูกส่งมา บริเวณที่สองคือบริเวณที่หน่วยกู้ภัยไม่สามารถติดตั้งโครงสร้างพื้นฐานได้ บริเวณนี้ผู้ประสบภัยจะสามารถติดต่อกับหน่วยกู้ภัยได้โดยใช้การสื่อสารแบบ Peer-to-peer แต่การสื่อสารแบบ Peer-to-peer นั้นสามารถให้ทุกคนสื่อสารถึงกันได้โดยตรง ผู้ประสบภัยสามารถสื่อสารกับผู้คนในบริเวณที่มีอุปกรณ์สื่อสารได้ ดังนั้นจึงอาจจะทำให้เกิดปัญหาในด้านความน่าเชื่อถือของข้อมูลตามมา แน่นอนว่าสถานการณ์ภัยพิบัติเป็นสถานการณ์ที่มีช่องโหว่มากมาย ผู้ไม่ประสงค์ดีสามารถหาผลประโยชน์จากสถานการณ์นี้ได้อย่างง่ายดาย ผู้ประสบภัยอาจจะได้รับข้อความเท็จจากผู้ไม่ประสงค์ดีเพื่อกระทำการบางอย่างที่ทำให้ก่อเกิดความเสียหายแก่ชีวิตและทรัพย์สินก็เป็นได้ ยิ่งไปกว่านั้นแม้ว่าการสื่อสารแบบ Peer-to-peer จะสามารถใช้งานได้บนบริเวณนี้ แต่จะมีผู้ประสบภัยบางกลุ่มที่อุปกรณ์สื่อสารไม่สามารถใช้งานเครือข่ายแอดฮอกได้ ทำให้ผู้ประสบภัยกลุ่มนั้นขาดการเชื่อมต่อจากผู้ช่วยเหลือ

ในปัจจุบันเทคโนโลยีประเภทคอมพิวเตอร์ขนาดจิ๋วเช่น Raspberry PI [1] ได้ถูกพัฒนาขึ้นมา ซึ่งนอกจากจะมีขนาดเล็กแล้วยังสามารถประมวลผลซับซ้อนได้ เราจึงมีแนวคิดที่จะนำคอมพิวเตอร์ขนาดจิ๋วมาใช้ในการสร้างรูปแบบการสื่อสารแบบใหม่ที่สามารถให้การเชื่อมต่อการสื่อได้อย่างครอบคลุมบนพื้นที่ภัยพิบัติ ในงานวิจัยนี้เราจึงเสนอรูปแบบการสื่อสารที่มีความน่าเชื่อถือบนพื้นที่ภัยพิบัติ โดยรูปแบบการสื่อสารที่เสนอนี้จะเป็นการนำข้อดีของการสื่อสารแบบโครงสร้างพื้นฐานและ Peer-to-peer รวมกันเพื่อสร้างการสื่อสารแบบใหม่ อีกทั้งเรายังได้มีการนำเทคโนโลยีคอมพิวเตอร์จิ๋วมาประยุกต์เพิ่มเติมเพื่อให้ได้การสื่อสารที่ครอบคลุมผู้ประสบภัยทุกกลุ่มบนพื้นที่ภัยพิบัติอีกด้วย ในงานวิจัยนี้จะถูกแบ่งออกเป็นสองส่วนดังนี้ ส่วนแรกจะเป็นการพัฒนารูปแบบการสื่อสารอย่างมีประสิทธิภาพและครอบคลุมพื้นที่ภัยพิบัติ และส่วนที่สองจะเป็นการพัฒนาวิธีการสื่อสารบนเครือข่าย Peer-to-peer ที่มีความน่าเชื่อถือในการสื่อสาร เนื่องจากว่าเครือข่ายแบบโครงสร้างพื้นฐานนั้นผู้ประสบภัยสามารถติดต่อกับเจ้าหน้าที่ได้โดยตรง ทำให้ง่ายต่อการควบคุมความน่าเชื่อถือของข้อมูล แต่สำหรับเครือข่าย Peer-to-peer นั้นผู้ประสบภัยสามารถติดต่อกับผู้คนบริเวณรอบๆได้ และอีกทั้งอุปกรณ์สื่อสารมีทรัพยากรจำกัด จึงทำให้ไม่สามารถใช้การยืนยันตัวตนในแบบที่ได้มีการนำเสนอในปัจจุบันได้

วัตถุประสงค์ของการทำวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษา และออกแบบรูปแบบการสื่อสารที่มีความน่าเชื่อถือบนพื้นที่ภัยพิบัติ เพื่อให้ได้การสื่อสารที่มีความน่าเชื่อถือ และสามารถใช้งานได้ในทุกบริเวณพื้นที่ประสบภัย อีกทั้งรองรับกับอุปกรณ์การสื่อสารที่มีจำหน่ายทั่วไป

ขอบเขตการทำวิจัย

1. พัฒนารูปแบบการสื่อสารบนพื้นที่ภัยพิบัติ
2. พัฒนาการยืนยันตัวตนบนพื้นที่ภัยพิบัติที่ใช้การสื่อสารโดยเครือข่าย Peer-to-peer
3. พัฒนาและทดลองบนโปรแกรมจำลองเครือข่าย NS 3.15 [2]

วิธีปฏิบัติงานโดยย่อ

1. ศึกษารูปแบบของแอพพลิเคชั่น ในเครือข่ายไร้สายแบบแอดฮอกบนพื้นที่ภัยพิบัติจากงานวิจัยที่ผ่านมา
2. ศึกษาวิธีการยืนยันตัวตนจากงานวิจัยที่ผ่านมา
3. ออกแบบวิธีการยืนยันตัวตนที่สอดคล้องกับความต้องการระบบ
4. ออกแบบวิธีการสร้างเครือข่ายโครงสร้างพื้นฐานบนพื้นที่ภัยพิบัติ
5. ทดสอบ และเก็บผลข้อมูล
6. วิเคราะห์ผลการทดลอง
7. ปรับปรุง แก้ไข เพื่อให้ระบบสื่อสารทำงานได้อย่างมีประสิทธิภาพมากที่สุด
8. สรุปผล และเรียบเรียงวิทยานิพนธ์

แผนการปฏิบัติงาน

ความก้าวหน้า	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.
ศึกษางานวิจัย										
ออกแบบการสื่อสาร										
ทำการพัฒนาการสื่อสาร										
ทดสอบผล										
วิเคราะห์ผลทดลอง										
ตรวจสอบงานวิจัย										
เตรียมการตีพิมพ์										

ประโยชน์ที่คาดว่าจะได้รับ

1. เพิ่มทางเลือกในการสื่อสาร ภายใต้สถานการณ์ภัยพิบัติที่ส่งผลให้มีพื้นที่บ้างส่วนถูกตัดขาดการสื่อสาร อันเนื่องมาจากปัจจัยพื้นฐานถูกทำลาย
2. ทำให้การสื่อสารภายหลังถูกตัดขาดสามารถกู้คืนได้อย่างรวดเร็ว
3. วิธีที่นำเสนอ สามารถนำไปประยุกต์ใช้การสื่อสารบนพื้นที่ภัยพิบัติได้
4. สามารถนำงานวิจัยไปพัฒนาการต่อยอดได้

ผลงานตีพิมพ์

งานวิจัยนี้ได้มีการแบ่งออกเป็น 2 ส่วนในการตีพิมพ์บทความทางวิชาการ ในส่วนแรกนั้นจะเป็นเนื้อหาในส่วนของการพัฒนาวิธีการสื่อสารที่มีความน่าเชื่อถือบนเครือข่าย Peer-to-peer ใช้งานในพื้นที่ภัยพิบัติ โดยมีหัวเรื่องคือ “ETC: Effective Trustworthy Communication with Two mode authentication for Disaster Recovery” จัดทำโดย “Tanapat Ruengsatra, Kulit Na Nakorn, Kultida Rojviboonchai, Krerk Piromsopa” ถูกนำเสนอในงานประชุมวิชาการ “10th International Conference on Information Assurance and Security: IAS 2014” ที่จัดขึ้นในวันที่ 27-29 พฤศจิกายน 2557 ณ เมืองโอกินาวา ประเทศญี่ปุ่น

ส่วนที่สองเป็นเนื้อหาของการสร้างระบบสื่อสารบนพื้นที่ภัยพิบัติโดยมีหัวเรื่องคือ “A Hybrid Communication Approach for Disaster Recovery” จัดทำโดย “Tanapat Ruengsatra, Kulit Na Nakorn, Krerk Piromsopa, Kultida Rojviboonchai” ถูกนำเสนอในงานประชุมวิชาการ “16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing: SNPD 2015” ที่จัดขึ้นในวันที่ 1-3 มิถุนายน 2558 ณ เมืองทากามัสซึ ประเทศญี่ปุ่น

บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 เครือข่ายแอดฮอก (Ad hoc network)

เครือข่ายแอดฮอก[3] นั้นเป็นเครือข่าย Peer-to-peer สามารถใช้งานได้ผ่านอุปกรณ์สื่อสารที่พกพาได้ การใช้งานของเครือข่ายแอดฮอกนี้สามารถใช้งานได้โดยไม่ต้องพึ่งพิงกับโครงสร้างพื้นฐานที่ใช้ในการสื่อสาร ทำให้การสื่อสารนั้นสามารถใช้งานได้แม้ในสถานที่ที่ไม่มีการติดตั้งโครงสร้างพื้นฐานมาก่อน ในงานวิจัยนี้ได้นำเครือข่ายแอดฮอกมาใช้งานในการสื่อสารบนพื้นที่ภัยพิบัติ เนื่องจากว่าเครือข่ายแอดฮอกสามารถทำให้ผู้ประสบภัยเข้าถึงการสื่อสารได้โดยที่ไม่ต้องอาศัยโครงสร้างพื้นฐานซึ่งอาจจะถูกทำลายลงบนพื้นที่ภัยพิบัติ เครือข่ายแอดฮอกนั้นจะมีคุณสมบัติดังต่อไปนี้

<u>ลักษณะของเครือข่ายแอดฮอก</u>

1) ไม่ต้องอาศัยโครงสร้างพื้นฐานในการติดต่อสื่อสาร

   เครือข่ายแอดฮอกนั้นไม่จำเป็นต้องใช้โครงสร้างพื้นฐานในการสื่อกลางในการส่งข้อมูล อุปกรณ์ที่สื่อสารด้วยเครือข่ายแอดฮอกนั้นสามารถส่งข้อมูลหากันแบบ Peer-to-peer ได้เลย ซึ่งแตกต่างจากการสื่อสารบางประเภทเช่นการใช้งานอินเตอร์เน็ตซึ่งต้องผ่านเสาสัญญาณในการส่งข้อมูล ดังนั้นการสื่อสารโดยใช้เครือข่ายแอดฮอกจึงมีข้อได้เปรียบในด้านของความสะดวกในการสื่อสาร เนื่องจากไม่จำเป็นต้องติดตั้งโครงสร้างพื้นฐานเพิ่มเติมในบริเวณที่จะใช้งาน

2) มีลักษณะการสื่อสารแบบ Peer-to-peer

   เครือข่ายแอดฮอกนั้นจะมีการสื่อสารกันแบบ Peer-to-peer ไม่จำเป็นต้องใช้ศูนย์กลางในการส่งข้อมูล การใช้งานเครือข่ายแอดฮอกนั้นเริ่มต้นจากการที่มีอุปกรณ์ที่ปล่อยสัญญาณแอดฮอกออกมาโดยสัญญาณจะถูกแยกตามค่า SSID ถ้าอุปกรณ์ใดปล่อยค่าสัญญาณ SSID เดียวกัน และมีการตั้งค่า IP Address ให้อยู่ในเครือข่ายเดียวกันจะสามารถสื่อสารกันได้โดยตรง นอกจากนั้นเราสามารถจัดการการสื่อสารแบบแอดฮฮกให้สามารถสื่อสารทางไกลผ่านอุปกรณ์ตัวอื่นได้ด้วย โดยข้อมูลจะถูกส่งจากต้นทางไปยังปลายทางที่อยู่ห่างไกลได้

3) มีการเชื่อมต่อและขาดการเชื่อมต่อเป็นประจำ

เนื่องจากการสื่อสารโดยใช้แอดฮอกนั้นเป็นการสื่อสารที่สามารถใช้ได้กับอุปกรณ์เคลื่อนที่เพราะว่าเป็นการสื่อสารที่สามารถสื่อสารได้โดยไม่ต้องอาศัยโครงสร้างพื้นฐาน ดังนั้นอุปกรณ์สื่อสารจึงมักจะมีการเคลื่อนที่ไปมาเสมอ เมื่ออุปกรณ์สื่อสารเคลื่อนที่เข้ามาในระยะสื่อสาร การสื่อสารโดยเครือข่ายแอดฮอกจะเชื่อมต่อโดยอัตโนมิติ ในทางกลับกัน เมื่ออุปกรณ์เหล่านั้นเคลื่อนที่ไกลออกไปจากบริเวณเครือข่ายแอดฮอก อุปกรณ์สื่อสารจะไม่สามารถเชื่อมต่อกับเครือข่ายแอดฮอกเดิมได้ แต่อาจจะมีกาเปลี่ยนไปเชื่อมต่อกับเครือข่ายอีกที่หนึ่งก็เป็นได้ ดังนั้นการออกแบบรูปแบบการสื่อสารของแอดฮอกจึงจำเป็นต้องตระหนักถึงปัจจัยนี้เพื่อการออกแบบการสื่อสารได้อย่างมีประสิทธิภาพ

4) สื่อสารกันได้เมื่ออยู่ซับเน็ตเดียวกันเท่านั้น

การสื่อสารโดยแอดฮอกนั้นเปรียบเทียบได้กับการสื่อสารผ่านวงแลน (LAN) ภายในเครือข่ายส่วนตัว ถึงแม้ว่าอุปกรณ์ที่ใช้การสื่อสารแบบแอดฮอกนั้นสามารถเป็นทั้งผู้รับและผู้ส่ง แต่ก็ไม่สามารถส่งข้อความข้ามซับเน็ตได้ ดังนั้นถ้าต้องการใช้แอดฮอกสื่อสารกันจำเป็นต้องตั้งค่า IP Address ให้เครื่องของเราอยู่ในซับเน็ตเดียวกับเครื่องที่ต้องการจะสื่อสารด้วย

<u>ประเภทการส่งข้อมูล</u>

การสื่อสารบนเครือข่ายแอดฮอกนั้นเป็นการสื่อสารที่ไม่มีโครงสร้างพื้นฐานทำให้สามารถรองรับการสื่อสารได้อย่างหลากหลาย เนื่องจากเครือข่ายแอดฮอกนั้นสามารถติดตั้งและใช้งานได้ทันที ทำให้หลายองค์กรได้นำเอาเครือข่ายนี้ไปใช้งานและพัฒนาวิธีการสื่อสารขึ้น ซึ่งมีหลายงานวิจัยที่ได้ทำการออกแบบรูปแบบการสื่อสารบนเครือข่ายแอดฮอกขึ้นมา เมื่อนำมาจัดประเภทตามลักษณะการส่งข้อมูลนั้นสามารถแบ่งได้ 3 ประเภทดังนี้

1) การส่งข้อมูลแบบ Unicast

เป็นการสื่อสารที่มีการส่งข้อมูลไปยังผู้รับแค่คนเดียว ซึ่งผู้รับข้อมูลนั้นอาจจะอยู่ติดกันกับผู้ส่ง หรือจะอยู่ไกลจากผู้ส่งข้อความก็ได้ ถ้าผู้รับอยู่ติดกับกับผู้ส่งข้อความ ข้อความจะถูกส่งให้ผู้รับโดยตรง แต่ถ้าผู้รับอยู่ไกลจากผู้ส่ง การส่งข้อความจำเป็นจะต้องส่งผ่านเพื่อนบ้าน หรืออุปกรณ์สื่อสารบริเวณรอบๆ โดยทำการส่งต่อกันเป็นทอดๆเพื่อให้ถึงผู้รับ ซึ่งประสิทธิภาพในการส่งข้อความไปยังผู้รับนั้นขึ้นอยู่กับโปรโตคอลในการส่งข้อความ

2) การส่งข้อมูลแบบ Broadcast

เป็นการส่งข้อมูลไปยังผู้รับหลายคน หรืออุปกรณ์สื่อสารหลายเครื่องพร้อมๆกันโดยผู้รับนั้นจะเป็นอุปกรณ์สื่อสารบริเวณรอบๆ การส่งข้อความแบบนี้จะทำให้ข้อความนั้นถูกแพร่กระจายได้อย่างรวดเร็วบนเครือข่ายการสื่อสาร แต่อย่างไรก็ตามการส่งข้อความแบบ Broadcast นั้นมีโอกาสทำให้เกิดการขัดข้องบนเครือข่ายได้สูงเพราะถ้าเป็นเครือข่ายที่มีผู้ใช้อยู่ในระบบมาก จะทำให้เกิดการแลกเปลี่ยนข้อมูลมหาศาลส่งผลให้ระบบไม่สามารถทำงานได้อย่างปกติ เพื่อที่จะส่งข้อมูลแบบ Broadcast ได้อย่างมีประสิทธิภาพ จะต้องมีการคิดวิธีการส่งข้อความที่สามารถลดการแลกเปลี่ยนข้อมูลลงและยังคงส่งข้อความถึงผู้รับได้อย่างครบถ้วน

3) การส่งข้อมูลแบบ Multicast

เป็นการส่งข้อมูลไปยังผู้รับหลายคนเช่นกัน แต่สามารถกำหนดกลุ่มของผู้รับข้อความได้ ในการส่งข้อความแบบ Multicast นั้นจะเป็นจะต้องสร้างกลุ่มการสื่อสารขึ้นมาก่อน จากนั้นถ้าอุปกรณ์สื่อสารเครื่องไหนมีความประสงค์ที่จะรับข้อมูลจะทำการส่งข้อความร้องขอร่วมกลุ่มสื่อสาร เมื่อได้รับเข้าร่วมกลุ่มแล้ว อุปกรณ์ทุกเครื่องในกลุ่มนั้นสามารถแลกเปลี่ยนข้อความกันได้ผ่านการสื่อสารแบบ Multicast

<u>ระยะการส่งข้อมูลตามมาตรฐาน IEEE 802.11b</u>

นอกจากประเภทของการส่งข้อมูลแล้วสิ่งที่ต้องคำนึงเพิ่มเติมในการสื่อสารบนเครือข่ายแอดฮอกนั่นคือระยะการส่งข้อมูล อุปกรณ์สื่อสารในปัจจุบันมีความสามารถในการรองรับระยะการส่งข้อมูลได้หลายหลาย แต่สำหรับงานวิจัยนี้ได้นำเอาอุปกรณ์ Smart phone เข้ามาใช้งานในการสื่อสารด้วยเครือข่ายแอดฮอกซึ่งระยะการสื่อสารโดย IEEE 802.11 b ได้แสดงดังรายละเอียดด้านล่าง

ภายนอกอาคาร

- ความเร็วในการส่ง 11 Mbps ระยะทาง 160 เมตร
- ความเร็วในการส่ง 5.5 Mbps ระยะทาง 270 เมตร
- ความเร็วในการส่ง 2 Mbps ระยะทาง 400 เมตร
- ความเร็วในการส่ง 1 Mbps ระยะทาง 550 เมตร

ภายในอาคาร

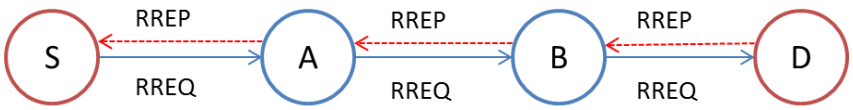
- ความเร็วในการส่ง 11 Mbps ระยะทาง 25 เมตร
- ความเร็วในการส่ง 5.5 Mbps ระยะทาง 35 เมตร
- ความเร็วในการส่ง 2 Mbps ระยะทาง 40 เมตร
- ความเร็วในการส่ง 1 Mbps ระยะทาง 50 เมตร

<u>รูปแบบโปรโตคอลที่ใช้ในการส่งข้อมูล</u>

การสื่อสารโดยใช้เครือข่ายแอดฮอกนั้นได้ถูกพัฒนาขึ้นในหลายหน่วยงานเพื่อตอบสนองการสื่อสารหลายรูปแบบ เนื่องจากการสื่อสารโดยใช้เครือข่ายแอดฮอกนั้นเป็นการสื่อสารแบบ Peer-to-peer นั่นคือไม่มีการใช้โครงสร้างพื้นฐานในการสื่อสาร การส่งข้อความในเครือข่ายแอดฮอกนั้นสามารถสื่อสารในระยะทางไกลออกไปหลาย Hop ได้จะต้องทำการส่งข้อมูลผ่านอุปกรณ์สื่อสารตัวอื่นต่อไปเป็นทอดๆจากผู้ส่งถึงผู้รับ ซึ่งการใช้งานเครือข่ายแอดฮอกนี้มีความต้องการการใช้งานที่หลากหลาย บางหน่วยงานที่ใช้งานอาจจะต้องการความรวดเร็วในการส่งข้อมูล แต่บางหน่วยงานอาจจะต้องการความครบถ้วนของข้อมูลเป็นต้น

ด้วยความต้องการในการใช้งานที่แตกต่างกันออกไปนี้ทำให้เกิดงานวิจัยรูปแบบโปรโตคอลในการสื่อสารออกมาที่หลากหลายโดยโปรโตคอลที่ใช้ในการสื่อสารบนเครือข่ายแอดฮอกนั้นจะเป็นตัวกำหนดลักษณะในการสื่อสารว่าผู้ส่งข้อความจะต้องส่งข้อความอย่างไร และอุปกรณ์สื่อสารระหว่างทางจะต้องทำงานอย่างไรที่จะทำให้การส่งข้อมูลไปถึงปลายทางได้สำเร็จ ซึ่งการทำงานหลักๆของโปรโตคอลในการสื่อสารคือการเก็บข้อมูลเส้นทางที่ใช้ในการสื่อสาร อุปกรณ์สื่อสารแต่ละตัวจะทำการบันทึกเส้นทางในการสื่อสารว่าจะต้องทำการส่งข้อมูลไปทางไหนเพื่อที่จะให้ถึงปลายทาง แต่ก่อนที่จะทำการบันทึกข้อมูลเส้นทางการสื่อสารได้นั้นโปรโตคอลจะต้องค้นหาเส้นทางการสื่อสารก่อน ซึ่งสามารถจำแนกโปรโตคอลตามประเภทของการค้นหาเส้นทางสื่อสารได้ 3 ประเภทดังนี้

1) โปรโตคอลค้นหาเส้นทางสื่อสารแบบ Reactive protocol

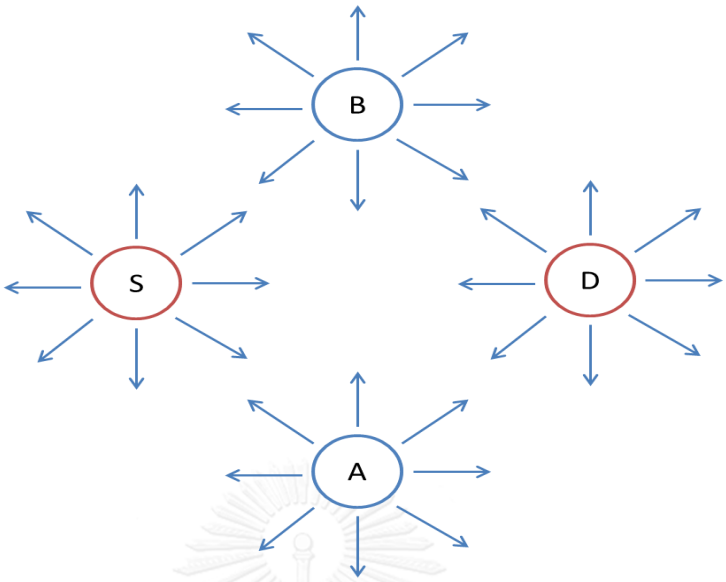


รูปที่ 1 การค้นหาเส้นทางแบบ Reactive protocol

โปรโตคอลแบบ Reactive protocol เป็นโปรโตคอลที่มีการค้นหาเส้นทางสื่อสารเมื่อต้องการจะส่งข้อมูล นั่นคือถ้าไม่มีการส่งข้อมูลเกิดขึ้น Reactive protocol จะไม่ทำการค้นหาเส้นทางการสื่อสาร แต่ถ้ามีข้อมูลที่ต้องการจะส่งนั้น อุปกรณ์ที่ต้องการจะส่งข้อความนั้นจะทำการค้นหาเส้นทางตามรูปที่ 2 โดยการส่ง Control packet ออกไปถามเส้นทางจากอุปกรณ์สื่อสารบริเวณรอบๆ หลังจากนั้นอุปกรณ์สื่อสารบริเวณรอบๆจะทำการตอบเส้นทางกลับมาถ้าอุปกรณ์นั้นรู้เส้นทาง แต่ถ้าอุปกรณ์ที่ถูกถามเส้นทางนั้นไม่ทราบเส้นทางการสื่อสาร อุปกรณ์สื่อสารตัวนั้นจะทำการส่งถามข้อมูลเส้นทางการสื่อสารออกไปอีก ดังนั้นการถามเส้นทางจึงถูกขยายออกเป็นวงกว้างจากผู้ส่งถึงผู้รับนั่นเอง ดังนั้นเมื่อ Control packet ที่ใช้ในการถามเส้นทางได้ถูกส่งถึงปลายทางนั้น อุปกรณ์ปลายทางจะรับรู้ได้ว่าจะมีข้อความที่ต้องการจะส่งให้ตนเอง ดังนั้นอุปกรณ์สื่อสารที่เป็นผู้รับข้อความปลายทางจะทำการตอบเส้นทางส่งกลับไปยังผู้ร้องขอเส้นทางนั่นเอง เมื่อทราบเส้นทางแล้วอุปกรณ์สื่อสารต้นทางก็จะสามารถส่งข้อความไปยังปลายทางได้

การค้นหาเส้นทางแบบ Reactive นี้มีข้อดีคือโปรโตคอลจะไม่จำเป็นต้องส่ง Control packet มากมายที่อาจส่งผลทำให้รบกวนระบบการสื่อสารได้ อีกทั้งด้วยกลไกของ Reactive protocol ที่มีการส่ง Packet ร้องขอเส้นทางเมื่อมีความจำเป็นเท่านั้น ทำให้อุปกรณ์สื่อสารประหยัดพลังงานที่ใช้ในการส่งลงอีกด้วย แต่ข้อเสียของ Reactive protocol คือการส่งข้อความจะเป็นไปได้ด้วยความล่าช้า เนื่องจากว่าจะต้องทำการถามเส้นทางการสื่อสารก่อน ตัวอย่าง Reactive protocol ที่ใช้ในปัจจุบันคือ Ad-hoc On Demand Distance Vector Routing Protocol (AODV) [4] เป็น Reactive protocol ที่เป็นมาตรฐาน RFC และใช้กันอยู่ในปัจจุบัน

2) โปรโตคอลค้นหาเส้นทางแบบ Proactive protocol

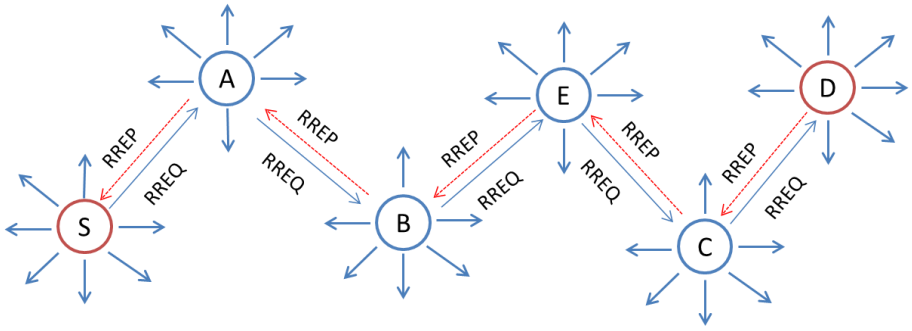


รูปที่ 2 การค้นหาเส้นทางแบบ Proactive protocol

โปรโตคอลค้นหาเส้นทางแบบ Proactive protocol นั้นจะเป็นโปรโตคอลที่จะทำการค้นหาเส้นทางที่ใช้ในการสื่อสารก่อนที่จะมีข้อมูลที่ต้องการจะส่ง โปรโตคอลแบบ Proactive นี้จะทำการส่ง Control packet เพื่อใช้ในการสอบถามเส้นทางออกเป็นระยะๆ ดังนั้น Proactive protocol จะมีเส้นทางในการส่งข้อความบันทึกอยู่ในตารางตลอดเวลา สำหรับกลไกในการหาเส้นทางนั้นแตกต่างกันไปในแต่ละโปรโตคอล แต่กลไกหลักๆคืออุปกรณ์สื่อสารจะส่ง Control packet กระจายออกไปทั้งระบบการสื่อสารเพื่อบอกข้อมูลที่ตนเองมีอยู่เช่น IP address ของตนเองและเพื่อนบ้านรอบๆ จากนั้นเมื่ออุปกรณ์สื่อสารเครื่องอื่นได้รับก็จะบันทึกข้อมูลนี้ลงในตารางเพื่อทำการจดจำเส้นทางเป็นต้น

ข้อดีของการใช้ Proactive protocol คือ เมื่อมีข้อความที่ต้องการจะส่งนั้นสามารถทำการส่งได้ทันทีโดยไม่ต้องทำการค้นหาเส้นทางอีกรอบ เพราะเส้นทางในการสื่อสารนั้นได้ถูกบันทึกไว้ในตารางก่อนที่จะมีข้อความที่ต้องส่งแล้ว แต่ข้อเสียของการใช้ Proactive protocol คือปัญหาทางด้านความคับคั่งของเครือข่ายการสื่อสาร เนื่องจากว่า Proactive protocol จำเป็นจะต้องส่ง Control packet ตลอดเวลาเพื่อทำการหาเส้นทาง ซึ่งตัว Control packet ที่ทำการส่งออกมาจากอุปกรณ์สื่อสารในทุกเครื่องนั้นทำให้เกิดความคับคั่งของการส่งข้อความขึ้นทำให้ข้อความที่ส่งอาจจะสูญหายได้

3) โปรโตคอลค้นหาเส้นทางแบบ Hybrid protocol



รูปที่ 3 การค้นหาเส้นทางแบบ Reactive protocol

โปรโตคอลในการค้นหาเส้นทางแบบ Hybrid protocol นั้นได้ทำการรวมข้อดีของการหาเส้นทางแบบ Proactive protocol และ Reactive protocol เข้าด้วยกันโดยการทำงานของการค้นหาเส้นทางแบบ Hybrid protocol จะมีการทำงานผสมสมกันระหว่างโปรโตคอลทั้งสองแบบนั่นเอง Hybrid protocol นั้นจะมีการส่ง Control packet เพื่อสอบถามเส้นทางออกมาเป็นระยะๆเหมือนกับ Proactive Protocol แต่ว่า Control packet ที่ทำการส่งออกมาเป็นระยะของ Hybrid protocol นั้นจะไม่ถูกส่งออกไปทั้งระบบการสื่อสาร Control packet จะถูกส่งออกไปแค่ในระยะจำกัดระยะหนึ่งเพื่อทำการลดปริมาณข้อมูลในระบบสื่อสารนั่นเอง ดังนั้น Hybrid protocol จะมีข้อมูลของเส้นทางการสื่อสารแค่ในช่วงระยะทางจำกัดระยะหนึ่ง

เมื่อมีข้อความที่ต้องการจะส่ง Hybrid protocol จะทำการตรวจสอบตารางเส้นทางการสื่อสารของตนเองว่ามีข้อมูลเส้นทางที่จะส่งไปยังปลายทางหรือไม่ ถ้ามีเส้นทาง Hybrid protocol จะทำการส่งข้อความในทันทีตามเส้นทางในตารางเส้นทางการสื่อสาร แต่ถ้าไม่มีเส้นทางการสื่อสาร Hybrid Protocol จะทำการค้นหาเส้นทางแบบเดียวกับ Reactive protocol นั่นคือจะมีการส่ง Control packet เพิ่มเติมออกไปยังพื้นที่ที่ไกลขึ้นเพื่อสอบถามเส้นทางจากปลายทางนั่นเอง เมื่อได้รับการตอบรับเส้นทางจากปลายทางแล้ว Hybrid protocol ก็จะทำการส่งข้อความออกไปยังปลายทาง

โปรโตคอลที่ใช้การค้นหาเส้นทางแบบ Hybrid นั้นได้รวมคุณสมบัติของการค้นหาเส้นทางแบบ Reactive และ Proactive เข้าด้วยกัน ข้อดีของการใช้การค้นหาเส้นทางแบบ Hybrid นั้นคือการที่อุปกรณ์สื่อสารสามารถส่งข้อความยังพื้นที่ใกล้เคียงได้รวดเร็วเนื่องจากไม่ต้องทำการค้นหาเส้นทางก่อนการส่ง อีกทั้งการส่งข้อความยังมีประสิทธิภาพมากกว่าการส่ง

ข้อความด้วยโปรโตคอลแบบ Proactive เนื่องจากโปรโตคอลการค้นหาเส้นทางแบบ Hybrid นั้นมีการส่ง Control packet น้อยกว่าทำให้มีความคับคั่งในระบบสื่อสารน้อยกว่านั่นเอง แต่อย่างไรก็ตามถ้าการส่งข้อความส่วนใหญ่เป็นการส่งข้อความไปยังพื้นที่ห่างไกลนั้น โปรโตคอลการค้นหาเส้นทางแบบ Hybrid นั้นจะต้องทำการค้นหาเส้นทางเหมือนโปรโตคอลที่ใช้การค้นหาเส้นทางแบบ Reactive ซึ่งจะทำให้เพิ่มการส่ง Control packet ขึ้นในระบบซึ่งทำให้เกิดความคับคั่งเพิ่มขึ้นในระบบสื่อสาร และยังทำให้การส่งข้อความมีความล่าช้าเนื่องจากว่าการส่งข้อความจำเป็นต้องค้นหาเส้นทางจากอุปกรณ์สื่อสารเครื่องอื่นๆอีกด้วย

2.1.2 Beaconing in Mobile Ad-hoc Network

Beacon คือการส่งสัญญาณซึ่งการส่งสัญญาณจะเป็นการส่งข้อความขนาดเล็กเพื่อใช้เพื่อการควบคุมเครือข่าย ในเครือข่ายแอดฮอกนั้นมีส่วนมากมีการสื่อสารโดยใช้ UDP ซึ่งไม่มีการทำ Three way handshake ทำให้การเชื่อมต่อไม่คงที่ การส่งสัญญาณจึงเป็นวิธีที่ใช้ในการควบคุมเพื่อให้สามารถส่งข้อมูลได้อย่างมีประสิทธิภาพ การส่งสัญญาณอาจจะใช้สำหรับการบอกสถานะของอุปกรณ์ว่าพร้อมใช้งานหรือไม่ หรือมีการทำงานแบบไหนเป็นต้น ซึ่งทั้งนี้แล้วขึ้นกับโพรโตคอลที่เกี่ยวข้องนั่นเอง ลักษณะของการส่งสัญญาณนั้นอาจจะเป็นแบบต่อเนื่องเป็นช่วงเวลาเช่น ส่งทุกวินาทีเป็นต้น การส่งสัญญาณควบคุมนั้นทำให้เราสามารถทราบได้ว่าตอนนี้เครือข่ายมีสภาพเป็นอย่างไรจะต้องทำการส่งข้อมูลอย่างไรเพื่อให้มีประสิทธิภาพ ณ เวลานั้นๆ ถึงแม้สัญญาณที่ส่งจะเป็นข้อความขนาดเล็กแต่แน่นอนว่าเมื่อมีการส่งข้อมูลเพิ่มขึ้นในเครือข่าย ก็จะเกิดการใช้ทรัพยากรของเครือข่ายมากขึ้น เช่น ความกว้างของเครือข่ายที่ใช้ในการส่งข้อความก็จะต้องถูกแบ่งให้กับการส่งสัญญาณ เป็นต้น ดังนั้นเมื่อจะต้องทำการส่งสัญญาณจึงจะต้องพิจารณาดังนี้

1) ขนาดของข้อมูลที่ใช้ส่งจะต้องไม่ใหญ่จนเกินไปเนื่องจากบนเครือข่ายแอดฮอกนั้นมีการสื่อสารแบบทางเดียว เมื่อมีการส่งสัญญาณอยู่นั้น ปลายทางจะไม่สามรถส่งข้อมูลมายังอุปกรณ์ที่ส่งสัญญาณได้ การที่ขนาดข้อมูลในสัญญาณที่ส่งนั้นมีขนาดใหญ่ทำให้ช่วงเวลาการส่งนาน อุปกรณ์ที่ทำการส่งสัญญาณก็จะไม่สามารถรับรู้ข้อมูลที่ผู้อื่นส่งมาได้นั่นเอง
2) ความถี่ในการส่งสัญญาณจะต้องมีความพอดี ไม่มากหรือน้อยจนเกินไป ถ้าความถี่ในการส่งสัญญาณมีน้อยนั้นจะทำให้ข้อมูลที่ได้รับจากเพื่อนบ้านเป็นข้อมูลที่ล่าช้า ไม่สามารถนำไปใช้งานได้ แต่ถ้าความถี่ในการส่งสัญญาณมากจะทำให้เครือข่ายมีความขัดสน ผู้ใช้จะส่งข้อความอื่นได้อย่างไม่สะดวก
3) การส่งต่อสัญญาณโดยส่วนมากสัญญาณจะมีการส่งให้แค่เพื่อนบ้านได้รับรู้แต่สำหรับบางโพรโตคอลนั้นสัญญาณที่ส่งแต่ละครั้งจะถูกส่งต่อไปยังเพื่อนบ้านที่อยู่ห่างไกลเกิน 1 ฮอพด้วย ดังนั้นจะต้องพิจารณาว่าโหนดไหนที่จะเป็นผู้ทำการส่งสัญญาณต่อ ถ้ามีผู้ส่งสัญญาณมากจะทำให้เกิดความขัดสนในเครือข่ายแต่ถ้ามีผู้ส่งสัญญาณน้อยเกินไปจะทำให้ไม่สามารถกระจายข้อความได้ครบจะมีบางโหนดที่ไม่ได้รับข้อมูลที่มีการเปลี่ยนแปลง

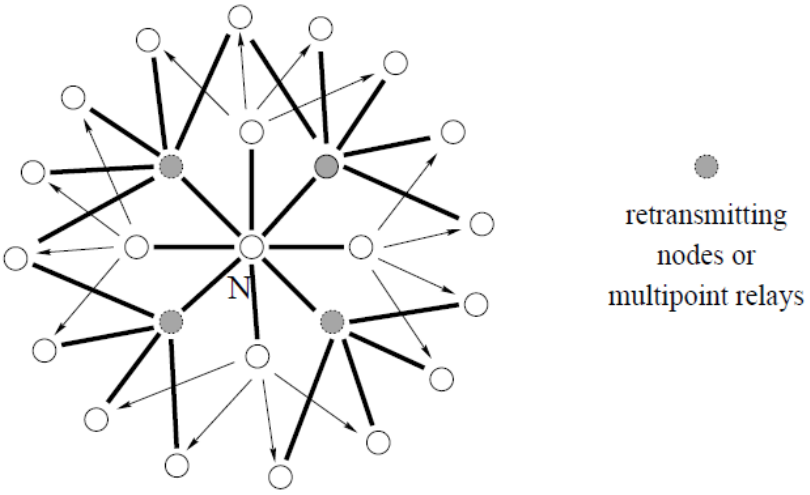
2.1.3 The Optimized State Routing Protocol (OLSR)

OLSR Protocol [5] เป็น Unicast Proactive Routing Protocol ในการส่งข้อความระหว่างอุปกรณ์สื่อสารโดยโปรโตคอลนี้จะทำการส่งข้อความแบบ Unicast โดยจะเลือกเส้นทางสั้นที่สุดจากผู้ส่งไปยังผู้รับในการส่งข้อความ ในการหาเส้นทางสั้นที่สุดระหว่างผู้ส่งและผู้รับนั้นจำเป็นต้องใช้กลไกในการช่วยนั้นคือ Control Message สำหรับโปรโตคอล OLSR นั้นมี Control Message ที่สำคัญอยู่ด้วยกันอยู่ 2 ประเภทด้วยกันคือ

1) Hello Message

เป็นข้อความที่ส่งระหว่างอุปกรณ์สื่อสารเพื่อทำการตรวจสอบสถานะของโหนดเพื่อนบ้าน ข้อมูลภายใน Hello Message นั้นจะบอกสถานะต่างๆของผู้ส่ง รวมทั้งรายการเพื่อนบ้านที่ผู้ส่งมีอยู่ทั้งหมดด้วย

2) Topology Control Message (Tc)



รูปที่ 4 Multipoint Relay nodes

เป็นข้อความที่ส่งเพื่อให้โหนดทุกโหนดในระบบรู้ข้อมูลโครงสร้างของระบบเพื่อใช้ในการเลือกเส้นทาง Tc Message นี้จะถูกส่งแบบแพร่กระจายไปยังโหนดทั้งระบบเพื่อให้โหนดทั้งระบบรับรู้ข้อมูลที่ถูกต้องในแบบเดียวกัน แต่เนื่องจากในการส่ง Tc Message เป็นการส่งข้อความแบบแพร่กระจาย โดย Tc Message นั้นมีการแพร่กระจายไปทั่วระบบสื่อสารตามรูปแบบของ Proactive protocol ทำให้มีโอกาสที่จะสร้างความคับคั่งขึ้นมาหรือรบกวนการส่งข้อมูลได้ โปรโตคอล OLSR จึงได้ทำการลดการส่ง Tc Message โดยให้ผู้ส่งเป็นตัวเลือกโหนดที่จะส่งโหนดถัดไป ในการเลือกโหนดที่จะส่ง Tc Message ไปยังเพื่อนบ้านใน Hop ถัดไปนั้นโหนดผู้ส่งจะเลือกกลุ่มของโหนดที่เล็กที่สุดที่สามารถครอบคลุมกลุ่มของโหนดใน

Hop ถัดไปได้ทั้งหมดในการส่งโดยกลุ่มนี้จะถูกเรียกว่า Multiple Relay Node (MPR) ซึ่งแสดงดังรูปที่ 4 ดังนั้นการส่งแบบแพร่กระจายจึงมีประสิทธิภาพสูงขึ้นและลดการรบกวนระบบได้มากขึ้น

นอกจากนี้โปรโตคอล OLSR ยังมี Control Message อื่นๆอีกเช่น MID Message และ HNA Message ซึ่ง Control Message ที่ไม่ได้เกี่ยวข้องกับงานวิจัยนี้ เนื่องจากงานวิจัยนี้ได้นำเอาโปรโตคอลมาพัฒนาบน Raspberry PI ซึ่งมีการส่งข้อความถึงกันแบบ Peer-to-peer ซึ่งมี Interface เดียว ดังนั้น MID และ HNA จึงไม่ได้ถูกใช้งานในงานวิจัยนี้

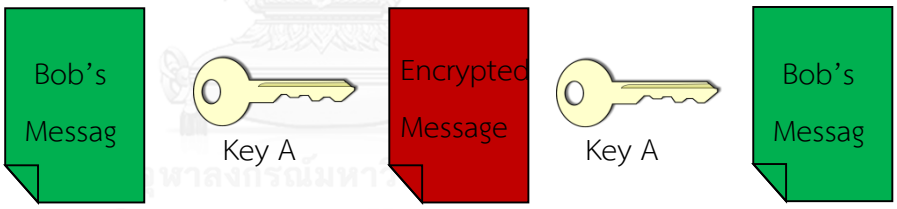
การใช้ Control Message ที่ได้กล่าวมาข้างต้นนี้ทำให้โปรโตคอล OLSR สามารถมีตารางค้นหาเส้นทางที่ใช้ในการส่งข้อความไปยังปลายทาง ดังนั้นเมื่อมีข้อความที่ต้องการจะส่งนั้นผู้ส่งจะทำการคำนวณหาเส้นทางในการส่งโดยวิธีการคำนวณหาเส้นทางในการส่งนั้นจะใช้การหาเส้นทางสั้นที่สุดในการส่งข้อความ การหาเส้นทางสั้นที่สุดนั้นโปรโตคอล OLSR ใช้วิธี Dijkstra’s algorithm ในการคำนวณเส้นทางสั้นที่สุด เมื่อได้เส้นทางแล้ว ผู้ส่งก็จะทำการส่งข้อความออกไปยังเส้นทางที่คำนวณได้

2.1.4 การเข้ารหัสข้อความ (Encryption)

ในการส่งข้อความระหว่างผู้รับและผู้ส่งนั้นผู้ที่ทำการส่งข้อความไม่สามารถส่งข้อความโดยตรงถึงผู้รับได้ จำเป็นต้องส่งผ่านตัวกลางเพื่อที่จะนำข้อความไปส่งให้ถึงผู้รับ ซึ่งบางข้อความเป็นข้อความที่ไม่ต้องการให้ตัวกลางสามารถเปิดอ่านหรือเข้าถึงข้อมูลได้ดังนั้นจึงได้มีการนำแนวคิดของการเข้ารหัสข้อความ [6] มาใช้ประโยชน์ในการส่งข้อความในปัจจุบัน ในการเข้ารหัสข้อความนั้นสามารถแบ่งได้สองประเภทคือการเข้ารหัสแบบ Symmetric key และการเข้ารหัสแบบ Asymmetric key หรือ Public Key

Symmetric key

การเข้ารหัสแบบ Symmetric key นั้นเป็นการเข้ารหัสข้อความโดยใช้กุญแจเข้ารหัสเพียงตัวเดียวโดยที่ผู้รับและผู้ส่งเท่านั้นที่จะรู้รหัสนั้น ตัวอย่างเช่น Bob ต้องการส่งข้อความให้ Alice ซึ่งเป็นผู้รับปลายทางนั้น Bob ก็จะทำการเข้ารหัสข้อความด้วย Key A ซึ่งเมื่อเข้ารหัสแล้วข้อความที่ถูกเข้ารหัสจะไม่สามารถถูกอ่านได้จากภายนอกถ้าไม่ได้ทำการถอดรหัสข้อความก่อน จากนั้นเมื่อข้อความได้ถูกส่งไปถึง Alice แล้ว Alice จะทำการถอดรหัสข้อความโดยใช้รหัสเดียวกันกับที่ Bob ได้ทำการเข้ารหัสมาAlice จึงสามารถอ่านข้อความได้



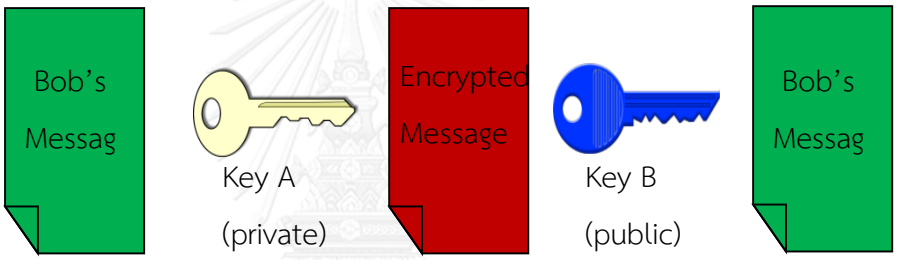
รูปที่ 5 การเข้ารหัสแบบ Symmetric key

รูปที่ 5 แสดงการเข้ารหัสแบบ Symmetric key ซึ่งการเข้ารหัสข้อความแบบ Symmetric key นั้นสามารถถูกถอดรหัสจากภายนอกได้ด้วยวิธีการ Brute Force ซึ่งประสิทธิภาพของคอมพิวเตอร์ในปัจจุบันมีความสามารถในการถอดรหัสที่ไม่ซับซ้อนได้ในเวลาอันสั้น ดังนั้นจึงมีหลากหลายวิธีการในการเข้ารหัสแบบ Symmetric key อย่างเช่นวิธีการ AES, DES, Blowfish เป็นต้น วิธีการเหล่านี้ทำให้การเข้ารหัสแบบ Symmetric key มีความซับซ้อนมากขึ้นทำให้ความสามารถของคอมพิวเตอร์ในปัจจุบันไม่สามารถถอดรหัสแบบ Brute Force ได้ในระยะเวลาอันสั้น จะต้องทำการใช้เวลาที่ค่อนข้างจะยาวนานในการถอดรหัส ดังนั้นการเข้ารหัสแบบ Symmetric key จึงสามารถรับประกันความปลอดภัยได้ในระดับที่สามารถยอมรับได้อย่างสากล เนื่องจากงานวิจัยนี้ใช้ประโยชน์จาก Asymmetric key เป็นหลักโดยมีการใช้ Symmetric key เป็นส่วนประกอบในการสร้างงานวิจัยนี้ขึ้นมา ดังนั้นจึงขอไม่กล่าวรายละเอียดของ Symmetric key ในเชิงลึก

ในการเข้ารหัสโดยใช้ Symmetric key นั้นจะมีปัญหาด้านการกระจายข้อมูล สมมติว่า Bob ต้องการจะส่งข้อความชุดเดียวกันไปให้เพื่อนในกลุ่ม 100 คน Bob จำเป็นจะต้องแจ้งให้เพื่อนทั้ง 100 คนทราบว่ารหัสคืออะไรเพื่อที่เพื่อนจะได้สามารถถอดรหัสข้อความของ Bob ออกมาได้ ซึ่งการที่มีคนจำนวนมากทราบรหัสของข้อความนี้ก็มีโอกาสสูงที่รหัสของข้อความจะไม่เป็นความลับอีกต่อไป ทำให้การส่งข้อความนั้นสามารถถูกแก้ไขได้ระหว่างทาง หรือสามารถถูกเปิดอ่านได้ระหว่างทางมากขึ้น ดังนั้นวิธีการแบบ Symmetric key จึงไม่เหมาะกับงานที่ต้องการความสามารถในการกระจายข้อมูล

Asymmetric key

การเข้ารหัสแบบ Public Key นั้นรู้จักในอีกชื่อหนึ่งคือ Asymmetric key ซึ่งเป็นวิธีการสำหรับเข้ารหัสข้อความประเภทหนึ่งซึ่งเป็นการเข้ารหัสและการถอดรหัสนั้นจะใช้กุญแจที่ต่างกันเพื่อที่จะแก้ปัญหาเรื่องการแจกจ่ายรหัสนั่นเอง



รูปที่ 6 การเข้ารหัสแบบ Asymmetric key

แนวคิด Asymmetric key จะเป็นกุญแจที่มาพร้อมกันเป็นคู่เรียกว่า Public key และ Private key ผู้ใช้สามารถเข้ารหัสข้อความด้วย Private key และทำการถอดรหัสด้วย Public key หรือจะเข้ารหัสด้วย Public key และทำการถอดรหัสด้วย Private key ก็ได้โดยกุญแจที่เป็นคู่กันเท่านั้นที่สามารถถอดรหัสซึ่งกันและกันได้ซึ่งแสดงดังรูปที่ 6 ข้อได้เปรียบของ Asymmetric key คือมีความสะดวกในการกระจายรหัสไปยังผู้รับหลายๆคน เมื่อเทียบกับ Symmetric key ที่ใช้เพียงแค่ Secret key เพียงอย่างเดียว ในตัวอย่างนี้เมื่อ Bob ต้องการส่งข้อความให้ Alice ที่เป็นผู้รับปลายทาง Bob จะทำการเข้ารหัสข้อความด้วย Key A ซึ่งจะเรียกอีกชื่อหนึ่งว่า Private key ของ Bob โดย Private key นี้จะมีแค่ Bob เท่านั้นที่รู้ จะไม่มีใครอื่นรู้รหัสตัวนี้อีก จากนั้น Bob จะทำการแจ้ง Key B ซึ่งเรียกอีกชื่อหนึ่งหว่า Public key ของ Bob ให้กับ Alice ทราบ เมื่อ Alice ที่อยู่ปลายทางได้ทำการรับข้อความแล้ว Alice จะทำการถอดรหัสข้อความโดยใช้ Public key ที่ Bob ได้แจ้งมาให้ทราบในการถอด จากนั้น Alice ก็จะสามารถอ่านข้อความที่ Bob ส่งมาให้ได้นั่นเอง ด้วยกลไกนี้ทำให้ Bob สามารถแจก Public key ของตนเองออกไปได้มากมายโดยไม่จำเป็นต้องกังวลว่า

จะมีใครที่ทราบรหัส เพราะถ้าทำการเข้ารหัสด้วย Public key นั้นคนที่มี Private key นั่นคือ Bob คนเดียวที่จะสามารถถอดรหัสข้อความได้

RSA algorithm

แนวคิดของ Public key นั้นได้ถูกพัฒนาขึ้นมาโดยนักวิจัยสามคนคือ Ron Rivest, Adi Shamir, และ Leonard Adleman โดยชื่อ RSA นั้นได้ถูกตั้งขึ้นจากนามสกุลของนักวิจัยสามท่านนี้ เพื่อเป็นการให้เกียรติในฐานะที่เป็นผู้คิดค้นวิธีการขึ้นมา RSA algorithm [7] ถูกคิดค้นขึ้นตั้งแต่ปี ค.ศ. 1977 แต่ได้ถูกนำมาใช้จริงตอนปี ค.ศ. 1997

RSA algorithm นั้นได้ใช้ทฤษฎีทางคณิตศาสตร์เข้ามาช่วยแก้ปัญหาโดยใช้ทฤษฎีจำนวนในการเข้ารหัสและถอดรหัสข้อความ โดยฟังก์ชั่นในการเข้ารหัสข้อความนั้นจะถูกสร้างขึ้นในรูปแบบของฟังก์ชั่นทางเดียว (One-way function) เพื่อจะเป็นการป้องกันไม่ให้รหัสถูกถอดได้โดยง่าย ซึ่งความสามารถของฟังก์ชั่นทางเดียวนั้นคือการที่จะคำนวณหาผลลัพท์ของฟังก์ชั่นนั้นจะต้องสามารถทำการคำนวณได้อย่างง่ายและใช้เวลารวดเร็วในการคำนวณ แต่ในทางกลับกัน ถ้าหากรู้ผลลัพท์ของฟังก์ชั่นแล้วจะไม่สามารถคำนวณหาตัวตั้งต้นได้ หรือถ้าคำนวณได้จะต้องใช้เวลาที่ยาวนานในการคำนวณ RSA algorithm ได้นำเอาคุณสมบัติของฟังก์ชั่นทางเดียวมาใช้งานทำให้เกิดกระบวนการเข้ารหัสที่มีความปลอดภัย โดยตัวRSA algorithm นั้นจะมีองค์ประกอบด้วยกัน 2 ส่วนคือ Public key และ Private key โดยที่ Public key นั้นสามารถแจกจ่ายให้กับทุกคนได้ และส่วน Private key นั้นเจ้าของรหัสจะเป็นคนเดียวที่ทราบโดยวิธีการคำนวนจะเป็นดังนี้

1) เลือกจำนวนเฉพาะ p และ q ที่แตกต่างกันขึ้นมา 2 จำนวน โดยการเลือกจำนวนเฉพาะ 2 จำนวนนี้ควรจะเลือกจากการสุ่มขึ้นมาและควรจะมีความยาว bit length เท่าๆกัน
2) คำนวณหาค่า n โดย n = p x q โดยที่ n นั้นจะถูกใช้เป็น modulus ในการเข้ารหัสของทั้ง Public key และ Private key ดังนั้นค่าความยาวของค่า n นั้นจะเป็นความยาวของรหัสนั่นเอง
3) คำนวณหาค่า Euler's totient function

$$\varphi(n) = \varphi(pq)$$
$$\varphi(n) = \varphi(p)\varphi(q)$$
$$\varphi(n) = (p-1)(q-1)$$

ค่าของ Euler's totient function จะถูกเรียกอีกชื่อหนึ่งคือ Euler's phi function โดยที่ฟังก์ชั่น $\varphi(n)$ จะทำการนับจำนวนเต็มบวกตั้งแต่ 1 ถึง n โดยที่จำนวนเต็มบวกนั้นจะต้อง

เป็นจำนวนเฉพาะสัมพัทธ์กับ n ในกรณีนี้ p และ q ทั้งคู่เป็นจำนวนเฉพาะ ดังนั้นค่าของ $\varphi(p)$ จึงมีค่าเป็น p-1 นั่นเอง

4) เลือกค่า e โดยที่ 1 < e < $\varphi(n)$ และค่า ห.ร.ม. ของ $\varphi(n)$ และ e มีค่าเท่ากับ 1 ค่า e นั้นจะถูกเรียกว่าเป็น public key ซึ่งในการเลือกค่า e นั้นไม่ควรเลือกค่า e ให้มีขนาดเล็กจนเกินไปเพราะจะทำให้การเข้ารหัสนั้นไม่ปลอดภัยและสามารถถูกถอดรหัสโดยวิธีการ Brute force จากภายนอกได้โดยง่าย

5) คำนวณค่า d ดังนี้

$$
\begin{aligned}
m^{\varphi(n)} &\equiv 1\ mod(n)\ ; \gcd(m,n) = 1 \\
m^{\mathrm{k}\times\varphi(n)} &\equiv 1^{k} \equiv 1\ mod(n) \\
m^{\mathrm{k}\times\varphi(n)+1} &\equiv m\ mod(n) \\
\text{กำหนดให้ } e \times d &= \mathrm{k} \times \varphi(n) + 1 \\
m^{e\times d} &\equiv m\ mod(n) \\
\text{ดังนั้น } d &= \frac{\mathrm{k} \times \varphi(n) + 1}{e}
\end{aligned}
$$

จากสมการจะได้ค่า d ออกมาซึ่งค่า d นี้คือค่า private key นั้นเอง โดยที่ค่า d นั้นจะถูกนำไปใช้ในการเข้ารหัสและเจ้าของรหัสเท่านั้นที่จะเป็นคนเดียวที่รู้ค่านี้

6) การเข้ารหัสโดย public key จะสามารถทำได้ดังสมการนี้

$$c \equiv m^{e} mod(n)$$

โดยที่ m คือข้อความที่ต้องการจะส่ง c คือข้อความที่ทำการเข้ารหัสเรียบร้อยแล้ว n และ e คือ public key

7) การถอดรหัสโดยวิธีการของ public key สามารถทำได้ดังนี้

$$m \equiv c^{d} mod(n)$$

โดยที่ m คือข้อความที่เป็นค่าเดียวกันกับข้อความต้นฉบับนั่นเอง

ตัวอย่างแสดงการเข้ารหัสโดยใช้ RSA algorithm

กระบวนการข้างต้นนี้เป็นกระบวนการที่ค่อนข้างจะซับซ้อนซึ่งสามารถจะแสดงตัวอย่างให้ดูได้ดังต่อไปนี้ สมมติว่า Bob ต้องการจะส่งข้อความหา Alice โดยที่ Bob มีข้อความที่เป็นตัวหนังสืออยู่ซึ่งสามารถแปลงข้อความตัวหนังสือเป็นตัวเลขได้หลายวิธี ในที่นี้อาจจะใช้การแปลงโดย Padding schemes ข้อความที่เป็นตัวหนังสือก็สามารถมาอยู่ในรูปแบบตัวเลขได้ ข้อดีของการแปลงข้อความโดยใช้ Padding schemes นั้นคือการแปลงข้อความให้อยู่ในรูปแบบที่มั่นใจได้ว่าตัวอักษรในข้อความ

จะไม่มีค่าอยู่ในช่วงของรูปแบบข้อความที่ไม่ปลอดภัย หลังจากที่ได้ทำการแปลงข้อความเป็นตัวเลขโดยใช้วิธีการ Padding schemes แล้วก็จะเริ่มทำการส่งข้อความซึ่งกระบวนการส่งข้อความจะเป็นดังนี้

1)

รูปที่ 7ตัวอย่างการใช้งาน RSA algorithm 1

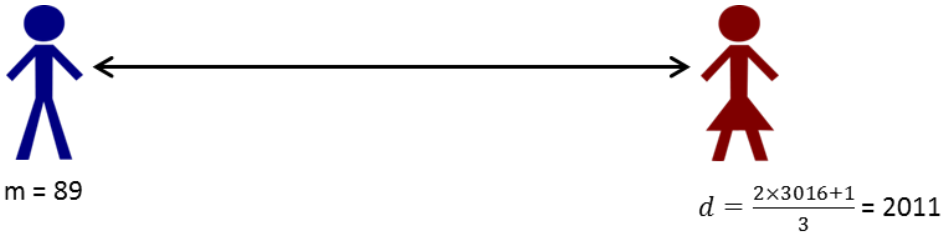
ขั้นแรกสมมติว่า Bob มีข้อความที่จะส่งคือเลข 89 ก่อนที่ Bob จะส่งข้อความนั้น Alice ก็ได้ทำการเลือกจำนวนเฉพาะขึ้นมา 2 จำนวนคือ 53 และ 59 จากนั้น Alice ก็ได้ทำการคำนวณค่า n ออกมาซึ่งมีค่าเท่ากับ 3127

2)

รูปที่ 8 ตัวอย่างการใช้งาน RSA algorithm 2

ขั้นต่อมา Alice ก็ได้ทำการคำนวณหาค่า Euler's phi function ของ 3127 ได้ค่าออกมาคือ 3016 จากนั้น Alice จึงทำการเลือกค่า e ให้มีค่าเท่ากับ 3

3)



รูปที่ 9 ตัวอย่างการใช้งาน RSA algorithm 3

Alice ได้ทำการคำนวณหาค่า d จากสมการข้างต้นโดยเลือกค่า k ให้เป็น 2 ดังนั้นค่า d ที่ Alice ได้ออกมาคือ 2011

4)

รูปที่ 10 ตัวอย่างการใช้งาน RSA algorithm 4

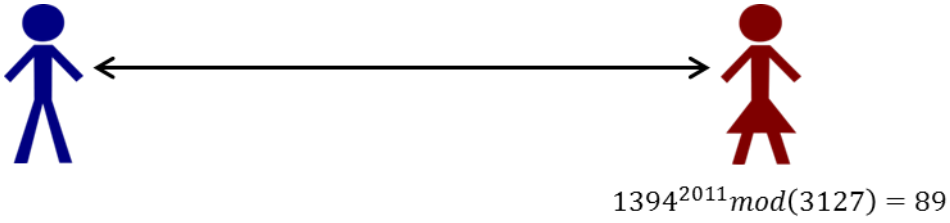
หลังจากที่ทำการคำนวณค่า d เสร็จแล้วนั้น Alice ก็ได้ทำการส่งค่า n และ e ไปให้ Bob โดยที่ค่า n และ e นั้นเป็นค่า public key ของ Alice นั่นเองจึงสามารถส่งไปให้สาธารณะรับรู้ได้

5)

รูปที่ 11 ตัวอย่างการใช้งาน RSA algorithm 5

เมื่อ Bob ได้รับ public key ของ Alice แล้ว Bob ก็ได้ทำการเข้ารหัสข้อความตามสมการข้างต้นทำให้ได้ค่า c ซึ่งเปรียบเป็นค่าของข้อความที่ได้ถูกทำการเข้ารหัสแล้ว จากนั้นก็ทำการส่งค่า c กลับไปให้ Alice

6)



รูปที่ 12 ตัวอย่างการใช้งาน RSA algorithm 6

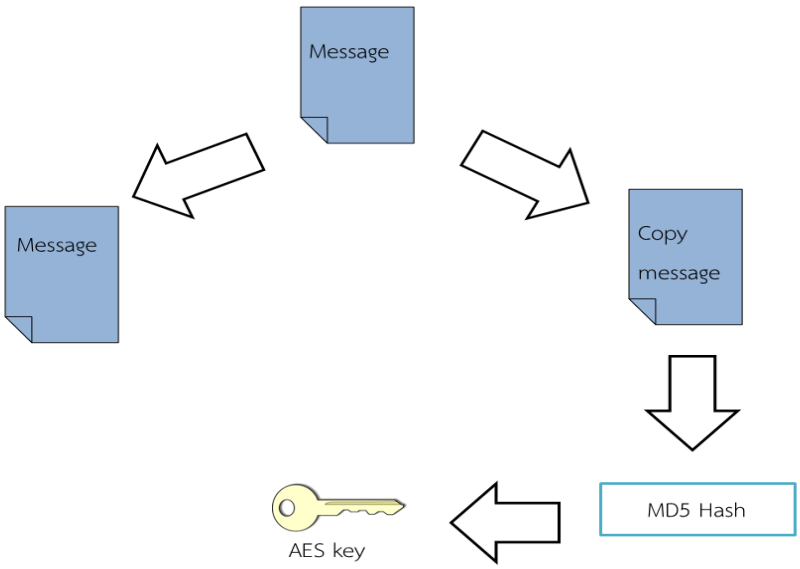
ในขั้นสุดท้ายหลังจากที่ Alice ได้รับข้อความที่ถูกเข้ารหัสมานั้น Alice ก็ใช้ private key ในการถอดรหัสและได้ค่าออกมาซึ่งเป็นค่าเดียวกับข้อความที่ Bob ต้องการจะส่งข้างต้น

จากข้างต้นจะเห็นว่าปลายทางจะทำการถอดรหัสได้นั้นจำเป็นจะต้องรู้ค่า d ซึ่งในการคำนวณหาค่า d นั้นสามารถคำนวณได้เพียงแค่รู้ค่า n แต่ว่าการคำนวณนั้นมีกระบวนการซับซ้อน เนื่องจากผู้ที่ต้องการจะแกะรหัสนั้นจำเป็นจะต้องคำนวณหาผลตัวประกอบของ n (prime factorization) เพื่อทำการคำนวณค่า Euler's phi function ในการคำนวณหาค่าตัวประกอบของ n นั้นถ้า n มีค่าที่ใหญ่เพียงพอการคำนวณหาค่า n จะต้องใช้เวลาเป็นปีเพื่อที่จะได้ค่าออกมา

จะเห็นได้ว่าการเข้ารหัสแบบ Asymmetric key นั้นมีข้อดีมากมายทั้งในด้านของความปลอดภัยและการแจกจ่ายรหัสไปให้กับผู้รับปลายทาง แต่อย่างไรก็ตามการเข้ารหัสแบบ Asymmetric key นั้นก็ยังคงมีข้อเสียอยู่ จากที่ตัวอย่างแสดงให้เห็นข้างต้นนั้นจะเห็นว่าข้อความที่ถูกทำการเข้ารหัสนั้นไม่สามารถเป็นข้อความที่มีความยาวมากๆได้ ในอีกความหมายหนึ่งคือการเข้ารหัสแบบ Asymmetric key ด้วยวิธีของ RSA นั้นสามารถเข้ารหัสข้อความได้แค่ 245 bytes ถ้าข้อความยาวกว่านี้จะไม่สามารถทำการเข้ารหัสได้ ดังนั้นการนำ RSA algorithm มาประยุกต์ใช้นั้นจึงต้องหาวิธีการที่เข้ามาช่วยในการเข้ารหัสเมื่อต้องการจะเข้ารหัสข้อความที่มีความยาวเกิน 245 bytes ซึ่งวิธีที่ใช้กันอย่างแพร่หลายนั่นคือการนำ Symmetric key มาช่วยในการเข้ารหัส

การเข้ารหัสแบบผสม

จากที่ได้กล่าวมาข้อเสียของ Asymmetric key นั้นคือไม่สามารถเข้ารหัสข้อความที่ยาวเกินกว่า 256 bytes ได้ ถ้าจะเข้ารหัสข้อความที่ยาวโดยใช้เพียง Asymmetric key เพียงอย่างเดียวนั้นจำเป็นจะต้องใช้ Asymmetric key หลายชุดซึ่งจะทำให้ขนาดข้อความเพิ่มขึ้นมากทำให้การส่งข้อความไม่มีประสิทธิภาพ ดังนั้นวิธีการใช้ Asymmetric key นั้นจำเป็นจะต้องใช้คู่กับ Symmetric key เพื่อที่จะเข้ารหัสข้อความชุดดังนั้นขั้นตอนการใช้งานในการเข้ารหัสแบบ Public key จะเป็นดังนี้



รูปที่ 13 การเข้ารหัสด้วย Asymmetric key 1

1) ในขั้นแรกจะมีการคัดลอกข้อคามที่ต้องการจะทำการเข้ารหัส
2) นำข้อความที่คัดลอกมาทำการเข้า hash function
3) นำค่า hash function ที่ได้มาสร้าง secret key ของการเข้ารหัสแบบ Symmetric key ในที่นี้จะใช้เป็นการเข้ารหัสแบบ AES ซึ่ง 3 ขั้นตอนที่ผ่านมาได้แสดงดังรูปที่ 13
4) นำข้อความที่ต้องการจะเข้ารหัสมาเข้ารหัสด้วยวิธี Symmetric key ผลที่ได้ออกมาคือข้อความที่ถูกเข้ารหัสโดยวิธีแบบ Symmetric key
5) นำ Secret key ของการเข้ารหัสแบบ Symmetric key มาทำการเข้ารหัสด้วย Asymmetric key
6) จากนั้นทำการนำ Encrypted key ที่ได้จากขั้นที่ผ่านมารวมกับ Encrypted message ส่งไปหาปลายทางพร้อมกับ public key
7) เมื่อปลายทางได้รับข้อความมานั้นปลายทางจะทำการถอดรหัสโดยใช้ public key ที่ได้รับมาทำการถอดรหัสเพื่อที่จะได้ Symmetric key
8) ปลายทางจะนำ Symmetric key ที่ได้จากการถอดรหัสนั้นมาทำการถอดรหัสข้อความอีกรอบหนึ่งซึ่งก็จะทำให้ปลายทางสามารถเข้าถึงข้อความต้นฉบับได้

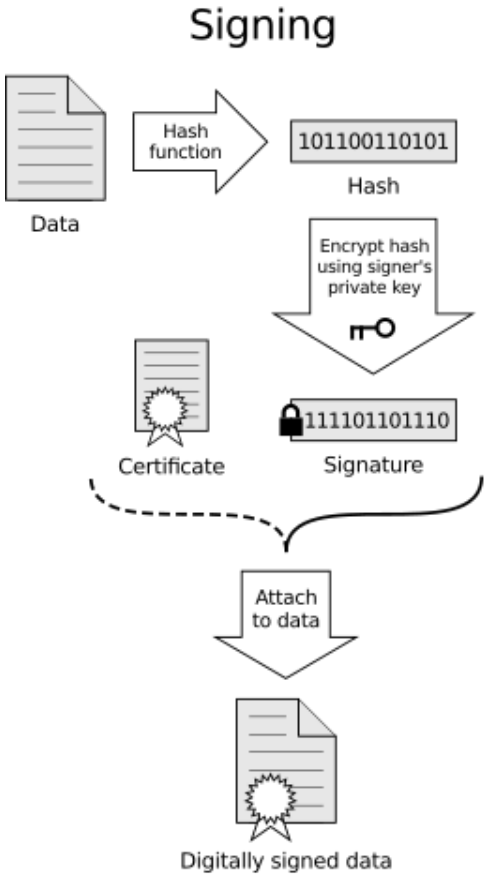
การนำการเข้ารหัสแบบ Asymmetric key มาประยุกต์ใช้

จากที่ได้กล่าวมาข้างต้นนั้นการเข้ารหัสแบบ Asymmetric key สามารถทำให้ผู้ใช้ส่งข้อความได้อย่างปลอดภัยและอีกทั้งยังให้ความสะดวกสบายในการแจกจ่ายรหัสไปยังที่สาธารณะได้ นอกจากการใช้งานเพื่อเข้ารหัสปกปิดข้อความแล้วนั้น การเข้ารหัสแบบ Asymmetric key ยังสามารถเอาไปใช้ในการยืนยันตัวตนได้อีกด้วย โดยหลักการคือ private key นั้นจะมีเพียงเจ้าของรหัสเพียงคนเดียวที่รู้ และ public key นั้นทุกคนจะสามารถรู้ได้ ถ้าได้รับข้อความที่ถูกเข้ารหัสด้วย private key มาข้อความหนึ่งโดยที่ผู้รับสามารถทำการถอดรหัสได้ด้วย public key ที่ผู้รับข้อความทราบอยู่แล้วว่าใครเป็นเจ้าของ public key ผู้รับปลายทางก็จะสามารถแน่ใจว่าข้อความนี้มาจากเจ้าของข้อความจริง

Digital Signature เป็นวิธีการที่ใช้สำหรับการยืนยันตัวตนในโลกของคอมพิวเตอร์นั่นเองโดย Digital Signature นั้นเปรียบเหมือนลายเซนของผู้ที่ต้องการจะยืนยันตัวตนที่ใช้ในการลงนามเอกสารเพื่อยืนยันการกระทำหรือยืนยันความเป็นเจ้าของหรือยืนยันความถูกต้องของเอกสาร Digital Signature นั้นได้ถูกนำมาใช้แทนลายเซนในหลายประเทศอย่างเช่นในสหรัฐอเมริกา ประชาชนสามารถใช้ Digital Signature ในการเซนเอกสารเพื่อทำการยืนยันตัวตนได้

แนวคิดของ Digital Signature คือการนำกระบวนการของ Asymmetric key มาใช้ในการยืนยันตัวตนโดยอาศัยความสามารถของ Asymmetric key ที่ประกอบด้วย public key ที่เชื่อมกับ private key ผู้ที่ต้องการจะทำการยืนยันตัวตนนั้นจะเซนเอกสารโดยใช้ private key และทำการแจก public key ให้กับผู้รับเอกสาร เมื่อผู้รับเอกสารได้รับเอกสารแล้วจะทำการตรวจสอบลายเซนด้วย public key ของผู้ส่ง การตรวจสอบเอกสารด้วยวิธีการ Digital Signature นั่นนอกจากจะตรวจสอบได้ว่าเป็นเอกสารที่ส่งมาจากผู้จริงแล้ว ยังสามารถตรวจสอบได้ด้วยว่าเอกสารไม่ได้มีการถูกเปลี่ยนแปลงระหว่างการส่ง โดยกระบวนการทำ Digital Signature จะเป็นดังนี้

การเซนเอกสาร

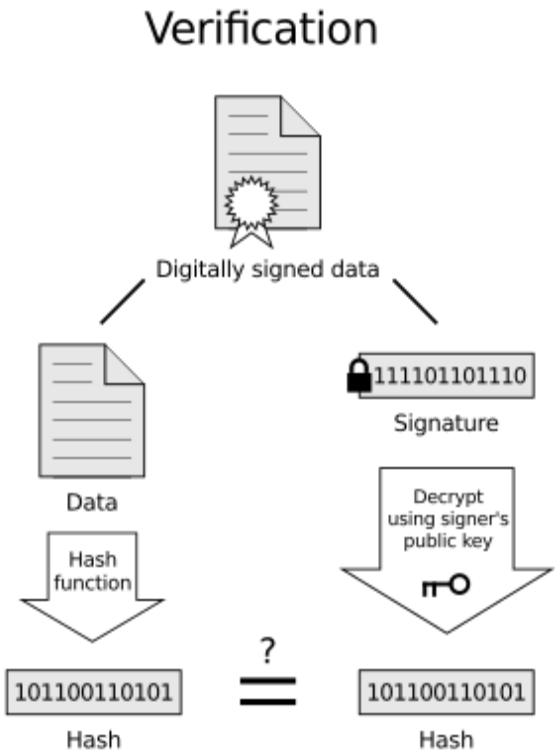


รูปที่ 14 การลงนามด้วย Digital Signature

การเซนเอกสารนั้นเป็นกระบวนการแรกในการสร้าง Digital Signature ขึ้นมา ซึ่งการทำ Digital Signature นั้นจะมีความคล้ายกับการเซนเอกสารแต่จะมีความแตกต่างกันเล็กน้อย การเซนเอกสารบนโลกแห่งความจริงนั้นผู้ที่ต้องการจะยืนยันตัวตนจะใช้ลายเซนเดิมในการเซนเอกสารทุกเอกสารไม่ว่าเอกสารจะเป็นเอกสารอะไรหรือจะเปลี่ยนไปอย่างไร ในอีกความหมายหนึ่งคือลายเซนของผู้ที่ต้องการจะลงนามนั้นไม่จำเป็นจะต้องผูกติดกับเอกสารนั่นเอง แต่สำหรับโลกของคอมพิวเตอร์นั้นการเซนเอกสารจะต้องมีกระบวนการเพื่อทำการยืนยันความถูกต้องของเอกสารต้นฉบับด้วย เพราะโลกของคอมพิวเตอร์นั้นทุกอย่างสามารถถูกแก้ไขจากภายนอกได้โดยง่าย ดังนั้นลายเซน Digital จะต้องทำการผูกกับเอกสารที่ต้องการจะลงนามในทุกฉบับเพื่อป้องกันการถูกเปลี่ยนแปลงของเอกสาร วิธีการในการสร้าง Digital Signature และนำมาใช้ในการลงนามในเอกสารนั้นนั้นมีกระบวนการดังรูปที่ 14 ดังนี้

1) ขั้นแรกจะเป็นการนำเอกสารที่ต้องการจะทำการลงนามมาทำการเข้า Hashing function
2) จากนั้นจะนำค่า Hash ที่ได้จากขั้นตอนแรกมาทำการเข้ารหัสด้วย Private key ของผู้ที่ต้องการจะลงนาม ซึ่งผลที่ได้ออกมาจะถูกเรียกว่า Signature
3) ขั้นสุดท้ายคือการนำ Signature ที่ได้ผูกติดเข้ากับข้อมูลต้นฉบับจะถือว่าการเซนเอกสารเป็นการเสร็จสิ้น

<u>การยืนยันลายเซน</u>



รูปที่ 15 การตรวจสอบการลงนามด้วย Digital Signature

การยืนยันลายเซนเป็นขั้นตอนที่ใช้สำหรับตรวจสอบความถูกต้องของลายเซนและเอกสาร ถ้านำไปเทียบกับโลกแห่งความจริงแล้วก็เปรียบได้กับกระบวนการตรวจสอบลายเซนของผู้ลงนามในเอกสาร การตรวจสอบลายเซนบนโลกแห่งความจริงนั้นผู้ตรวจสอบจะทำการตรวจสอบลายเซนว่าเหมือนลายเซนของต้นฉบับหรือไม่ดังการตรวจสอบลายเซนของธนาคาร ผู้ตรวจสอบจะทำการตรวจสอบโดยการนำลายเซนที่เซนบนเอกสารไปเทียบกับลายเซนต้นฉบับบนสมุดบัญชี ซึ่งแตกต่างจากการตรวจสอบลายเซนของการทำ Digital Signature ที่ใช้แนวคิดของ Public key ในการตรวจสอบความถูกต้องของ Digital Signature ที่แนบมากับเอกสาร นอกจากตรวจสอบความถูกต้อง

ของลายเซนแล้วกระบวนการตรวจสอบ Digital Signature นั้นยังมีกระบวนการในการตรวจสอบความถูกต้องของเอกสารอีกด้วยเพื่อป้องกันการปลอมแปลงเอกสารอีกด้วย กระบวนการตรวจสอบลายเซน Digital Signature มีขั้นตอนดังรูปที่ 15 ดังนี้

1) นำเอกสารที่ได้มาแยกเอกสารและ Digital Signature ออกจากกัน
2) นำเอกสารไปเข้า Hash function เช่นเดียวกันกับ Hash function ในขั้นตอนการทำ Signature
3) นำ Digital Signature ที่แนบมากับเอกสารถอดรหัสด้วย public key ของผู้ลงนามจะได้ค่า Hash function ของเอกสารต้นฉบับ
4) นำค่า Hash function ที่ได้มาเทียบกัน ถ้าค่า Hash function ที่ออกมาทั้งสองค่ามีค่าถูกต้องตรงกันจะถือว่าการตรวจสอบเอกสารนั้นผ่าน แต่ถ้าค่าที่ได้จาก Hash function ทั้งสองค่ามีค่าไม่ตรงกันจะถือว่าการตรวจสอบนั้นไม่ผ่าน

การทำ Digital Signature นั้นเป็นการนำเอาทฤษฎีทางด้าน Asymmetric key encryption มาประยุกต์ใช้งานทำให้ผู้ใช้สามารถทำการยืนยันตัวตนและความถูกต้องของเอกสารได้ ทุกวันนี้โลกได้มีการพัฒนาไปอย่างก้าวไกล การทำธุรกรรมหลายอย่างได้ถูกนำมาใช้งานบนโลกออนไลน์เพิ่มขึ้นอย่างมาก การใช้งาน Digital Signature นั้นก็เป็นส่วนหนึ่งที่ทำให้โลกได้มีการพัฒนาด้านการทำธุรกรรมบนโลกออนไลน์ เพราะ Digital Signature ทำให้การทำธุรกรรมบนโลกออนไลน์นั้นมีความง่ายขึ้นและอีกทั้งยังเพิ่มความน่าเชื่อถือขึ้นด้วย ทำให้ผู้ใช้งานสามารถมั่นใจได้ว่าการทำธุรกรรมที่ได้ทำลงไปนั้นมีความถูกต้องและน่าเชื่อถือ

Certificate Authentication

การทำ Digital Signature ดังที่ได้กล่าวมานั้นสามารถให้ความน่าเชื่อถือในด้านการทำธุรกรรมต่างๆบนโลกออนไลน์ อีกทั้งยังเพิ่มความน่าเชื่อถือในด้านความถูกต้องของเอกสารด้วย แต่อย่างไรก็ตาม Digital Signature นั้นผู้รับเอกสารปลายทางจำเป็นจะต้องทราบว่า public key ของผู้ส่งนั้นมีหน้าตาเป็นอย่างไร สำหรับบุคคลที่ไม่เคยรู้จักมาก่อนหรือไม่เคยติดต่อด้วยกันมาก่อนนั้น ผู้รับเอกสารปลายทางจะไม่สามารถทราบได้เลยว่าหน้าตาของ public key ของผู้ส่งนั้นเป็นอย่างไร ก่อให้เกิดการปลอมแปลง public key ได้อย่างง่ายดาย ดังนั้นการที่เราจะมั่นใจได้ว่าใครเป็นเจ้าของ public key นั้นสามารถกระทำได้โดยการใช้วิธีการของ Certificate Authentication ซึ่งวิธีการนี้เปรียบเหมือนกับเอกสารใบหนึ่งที่แจ้งให้กับผู้คนที่เราจะส่งเอกสารทราบว่า public key หน้าตาเช่นนี้เป็นของเราจริงๆ โดยใบ Certificate นี้จะประกอบด้วย public key ของเรา และ สิ่งที่เราไว้ใช้ในการยืนยันตัวตนของเราอย่างเช่น ชื่อจริง-นามสกุล หรือ เลขประจำตัวประชาชน เป็นต้น โดยกระบวนการของ Certificate Authentication นั้นมีขั้นตอนดังนี้

<u>การออก Certificate</u>

ก่อนที่ผู้ใช้จะสามารถใช้งาน public key ได้ในที่สาธารณะ ผู้ใช้จำเป็นจะต้องได้รับ Certificate เพื่อยืนยันก่อนว่า public key ที่ส่งให้กับผู้อื่นนั้นเป็นของเราจริงๆ ความน่าเชื่อถือของวิธีนี้จรึงขึ้นกับความน่าเชื่อถือของ Certificate ที่ผู้ส่งเอกสารได้แนบมากับเอกสาร ดังนั้นเพื่อให้ Certificate มีความน่าเชื่อถือนั้น Certificate จำเป็นจะต้องถูกออกโดยหน่วยงานที่หน้าเชื่อถือของสังคมกลุ่มนั้นๆ ซึ่งการออก Certificate นั้นก็ใช้แนวคิดของ Asymmetric key ในการยืนยัน Certificate เช่นกันโดยจะมีกระบวนการดังนี้

1) ผู้ที่ต้องการจะได้รับ Certificate จะต้องไปติดต่อกับหน่วยงานที่ทำหน้าที่ออก Certificate ให้โดยแจ้งสิ่งที่ใช้แสดงตัวตน อาจจะเป็นรหัสประชาชน หรือว่าชื่อ-นามสกุล พร้อมกับ public key
2) หน่วยงานที่ทำการออก Certificate จะรวม public key เข้ากับ ID ที่ใช้ในการยืนยันตัวตน จะเรียกว่า Unsigned Certificate
3) จากนั้นจะนำเอา Unsigned Certificate มาเข้ารหัสด้วย private key ของหน่วยงานนั้นทำให้ได้ Signed Certificate ออกมา

ผู้ใช้งานสามารถนำ Signed Certificate นี้ไปใช้ในการยืนยันความถูกต้องของ public key ที่ใช้งานในการทำธุรกรรม หรือในการส่งเอกสารต่างๆได้ ซึ่งความน่าเชื่อถือของ Certificate จะขึ้นอยู่กับความน่าเชื่อถือของหน่วยงานที่ออก Certificate ให้นั่นเอง

การตรวจสอบ Certificate

การตรวจสอบ Certificate นั้นจะสามารถให้ข้อมูลกับผู้ที่ทำการตรวจสอบได้ว่า public key ชุดที่ได้รับมาเป็นของผู้ที่ส่งให้จริง โดยวิธีการตรวจสอบนั้นสามารถตรวจสอบได้ดังนี้

1) ผู้ที่ต้องการจะตรวจสอบ Certificate นั้นจะต้องทราบ public key ของหน่วยงานที่ทำการออก Certificate ให้ โดยหน่วยงานนี้อาจจะแจ้ง public key บนที่สาธารณะ หรืออาจจะแจ้งเป็นการส่วนตัวต่อหน่วยงานที่ต้องการจะตรวจสอบก็ได้
2) ผู้ที่ต้องการจะตรวจสอบนำ public key ของหน่วยงานที่ทำการออก Certificate ให้มาทำการถอดรหัสของ Certificate ที่ได้รับมา ถ้าการถอดรหัสนั้นสำเร็จจะได้ว่า Certificate นั้นมีความถูกต้อง แต่ถ้าการถอดรหัสนั้นไม่สำเร็จจะถือว่า Certificate นั้นไม่ถูกต้อง
3) เมื่อถอดรหัส Certificate มาแล้วจะได้ public key ของผู้ที่ทำการส่งเอกสารมาให้เรา จากนั้นก็นำ public key ที่ได้มาทำการถอดรหัสเอกสารที่ได้รับมาเพื่อทำการตรวจสอบ Digital Signature ที่ได้แนบมากับเอกสารนั่นเอง

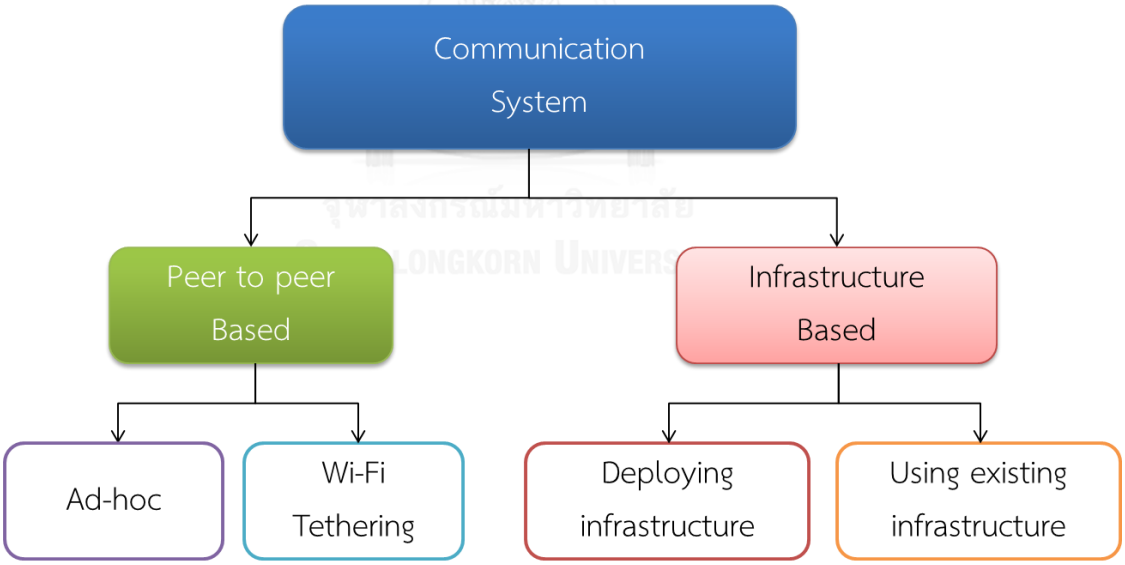
จะเห็นได้ว่าการใช้งานของ Digital Signature นั้นมาควบคู่กับการใช้งาน Certificate Authentication เพื่อเพิ่มความน่าเชื่อถือของการยืนยันตัวตน ในงานวิจัยนี้ได้นำเอาส่วนของ Digital Signature และ Certificate Authentication มาใช้งานในส่วนของการสร้างวิธีการสื่อสารที่มีความน่าเชื่อถือซึ่งจะกล่าวในบทถัดไป

2.2 งานวิจัยที่เกี่ยวข้อง

เนื่องจากวิทยานิพนธ์ฉบับนี้ได้มีการรวมงานวิจัยทางสองศาสตร์เข้าด้วยกัน คือศาสตร์ด้านการยืนยันตัวตน และ ศาสตร์ด้านโครงสร้างระบบสื่อสาร เพื่อสร้างการสื่อสารที่มีความน่าเชื่อถือบนพื้นที่ภัยพิบัติ ดังนั้นงานวิจัยที่เกี่ยวข้องจึงจะแยกเป็นสองส่วนดังต่อไปนี้

2.2.1 งานวิจัยที่เกี่ยวข้องกับโครงสร้างการสื่อสารบนพื้นที่ภัยพิบัติ

เมื่อเกิดเหตุภัยพิบัติขึ้น ระบบสื่อสารต่างๆบนพื้นที่ภัยพิบัติมักจะได้รับความเสียหายทำให้ไม่สามารถใช้งานระบบสื่อสารได้ ซึ่งการสื่อสารนั้นเป็นสิ่งสำคัญและจำเป็นบนพื้นที่ภัยพิบัติ ดังนั้นจึงมีหลายงานวิจัยที่จะพยายามกู้คืนระบบสื่อสารบนพื้นที่ภัยพิบัติขึ้นมาใหม่ ซึ่งการสร้างการสื่อสารบนพื้นที่ภัยพิบัตินั้นสามารถทำได้หลายวิธีขึ้นกับสมมติฐานของงานวิจัย เช่นบางงานวิจัยอาจจะมุ่งเน้นการสร้างระบบสื่อสารขึ้นมาใหม่บนพื้นที่ภัยพิบัติ บางงานวิจัยอาจจะสร้างระบบขึ้นมาเพื่อซ่อมแซมระบบสื่อสารบนพื้นที่ภัยพิบัติที่มีอยู่เดิม เป็นต้น การสร้างระบบสื่อสารขึ้นมานั้นมีปัจจัยหลายปัจจัยที่ต้องวิเคราะห์เช่น ความสามารถในการส่งข้อมูล, ความรวดเร็วในการติดตั้งระบบสื่อสาร หรืองบประมาณที่ใช้ในการติดตั้งระบบสื่อสาร เป็นต้น เราสามารถแบ่งงานวิจัยในการสร้างระบบสื่อสารบนพื้นที่ภัยพิบัติได้ออกเป็นสองกลุ่มใหญ่ๆ ดังนี้



รูปที่ 16 ประเภทของงานวิจัยด้านการสื่อสารบนพื้นที่ภัยพิบัติ

การสร้างระบบสื่อสารโดยใช้เครือข่าย Peer-to-peer

ระบบสื่อสารแบบ Peer-to-peer นั้นเป็นระบบที่มีความยืดหยุ่นสูง สามารถให้การสื่อสารได้โดยไม่ต้องติดตั้งโครงสร้างพื้นฐาน ทำให้มีความรวดเร็วในการเริ่มต้นใช้งานระบบสื่อสาร อีกทั้งระบบสื่อสารแบบ Peer-to-peer นั้นยังสามารถเข้าถึงพื้นที่ภัยพิบัติได้ทุกบริเวณ แต่อย่างไรก็ตาม

ระบบสื่อสารแบบ Peer-to-peer นั้นไม่สามารถให้การสื่อสารที่มีความเสถียรได้ การใช้งานการสื่อสารจึงมีความไม่ต่อเนื่องนั่นเอง การสร้างระบบสื่อสารแบบ Peer-to-peer นั้นสามารถแบ่งออกได้ 2 วิธีดังนี้

1) การสร้างระบบสื่อสารด้วยเครือข่ายแอดฮอก

เครือข่ายแอดฮอกนั้นเป็นเครือข่ายที่สามารถให้การสื่อสารแบบ Peer-to-peer ที่มีประสิทธิภาพ การใช้งานเครือข่ายแอดฮอกนี้สามารถใช้งานได้ในอุปกรณ์สื่อสารประเภท Smart phone หรือจะเป็น Laptop ก็ได้ การสื่อสารโดยใช้เครือข่ายแอดฮอกนั้นยังสามารถสื่อสารโดยใช้เทคโนโลยี IEEE 802.11 a/b/g/p ซึ่งความแรงของสัญญาณก็เปลี่ยนกันไปตามเทคโนโลยีที่นำมาใช้งาน เครือข่ายแอดฮอกจึงเป็นเครือข่ายที่มีความน่าสนใจและได้ถูกนำมาใช้ในการสร้างระบบสื่อสารบนพื้นที่ภัยพิบัติ

ตัวอย่างงานวิจัย Disaster Recovery System with a Hybrid Network [8] งานวิจัยนี้เป็นงานวิจัยที่จะทำมาต่อยอดเพื่อสร้างการยืนยันตัวตน งานวิจัยชิ้นนี้ได้ทำการสร้างระบบการสื่อสารแบบ Peer-to-peer บนพื้นที่ภัยพิบัติโดยใช้เครือข่ายแอดฮอกในการสื่อสาร การสื่อสารนั้นจะเป็นการสื่อสารผ่านโพรโตคอล DECA-SABI ซึ่งมีการส่งข้อความแบบกระจาย (Broadcast) ข้อความจะถูกส่งกระจายจากผู้ส่งไปทั้งระบบ ด้วยการสื่อสารวิธีนี้ทำให้ผู้ประสบภัยสามารถส่งข้อความขอความช่วยเหลือจากผู้คนบริเวณรอบข้างได้อย่างรวดเร็ว การส่งข้อความแบบกระจายนั้นอาจทำให้เครือข่ายเกิดความขัดสนได้ แต่โพรโตคอล DECA-SABI นี้ได้มีการแก้ปัญหาความขัดสนของเครือข่ายโดยการเลือกผู้ส่งต่อข้อความคือผู้ที่มีเพื่อนบ้านมากที่สุดนั่นเอง ด้วยวิธีนี้ข้อความจะถูกส่งไปยังประชากรในเครือข่ายอย่างรวดเร็ว

2) การสร้างระบบสื่อสารโดยใช้ Wi-Fi Tethering

เครือข่ายแอดฮอกนั้นยังมีข้อจำกัดในการใช้งานในการสร้างระบบสื่อสารเนื่องจากว่าอุปกรณ์สื่อสารประเภท Smart phone ในปัจจุบันนี้มีเพียงไม่กี่รุ่นที่รองรับการสื่อสารโดยใช้เครือข่ายแอดฮอก ดังนั้นการใช้งานเครือข่ายแอดฮอกจึงไม่สามารถใช้งานได้ครอบคลุมพื้นที่ภัยพิบัติ ด้วยเหตุนี้จึงได้มีการนำแนวคิดของ Wi-Fi Tethering มาประยุกต์ใช้เพื่อสร้างการสื่อสารแบบ Peer-to-peer บนพื้นที่ภัยพิบัติ

งานวิจัยที่นำ Wi-Fi Tethering มาใช้ในการสร้างระบบสื่อสารบนพื้นที่ภัยพิบัติคือ E-DARWIN: Energy Aware Disaster Recovery Network using Wi-Fi Tethering [9] งานวิจัยนี้จึงนำเอา Wi-Fi Tethering ในการสร้างเครือข่ายการสื่อสาร โดยอุปกรณ์สื่อสารนั้นจะทำการสลับหน้าที่ในการรับส่งข้อมูลระหว่างผู้รับข้อมูล และผู้ส่งข้อมูลเนื่องจากการทำงานของ Wi-Fi Tethering นั้นการรับและการส่งข้อมูลไม่สามารถทำได้พร้อมกันจึงจำเป็นต้องอาศัยโพรโตคอลในการทำงาน ใน

การอุปกรณ์สื่อสารของผู้ประสบภัยนั้นจะต้องเปิดการใช้งาน Wi-Fi Tethering mode จากนั้นโพรโตคอลจะทำการสลับหน้าที่ในการรับส่งข้อมูล

การสร้างระบบสื่อสารโดยการใช้งานโครงสร้างพื้นฐาน

จากที่ได้กล่าวมานั้นเครือข่าย Peer-to-peer นั้นยังมีข้อจำกัดในการสื่อสารเนื่องจากว่าการสื่อสารจะมีความไม่ต่อเนื่องเพราะการสื่อสารบนเครือข่าย Peer-to-peer นั้นจะทำการส่งข้อความผ่านอุปกรณ์สื่อสารที่มีการเคลื่อนที่อยู่ตลอดเวลา เมื่ออุปกรณ์สื่อสารเคลื่อนที่ห่างจากบริเวณของสัญญาณในการสื่อสาร ก็จะทำให้การสื่อสารนั้นถูกตัดขาดลง และเมื่ออุปกรณ์สื่อสารเคลื่อนที่กลับเข้ามาในช่วงของสัญญาณที่ใช้ในการสื่อสาร ผู้ใช้จะสามารถส่งข้อความได้ตามปกติ ด้วยความไม่ต่อเนื่องนี้ทำให้เครือข่าย Peer-to-peer มีข้อจำกัดในการสื่อสาร การสื่อสารโดยการใช้งานโครงสร้างพื้นฐานจึงได้ถูกนำมาพิจารณาใช้งานสำหรับระบบสื่อสารบนพื้นที่ภัยพิบัติ การใช้งานโครงสร้างพื้นฐานสามารถแบ่งได้ 2 วิธีดังนี้

1) การติดตั้งโครงสร้างพื้นฐานใหม่บนพื้นที่ภัยพิบัติ

การติดตั้งระบบสื่อสารแบบใช้โครงสร้างพื้นฐานบนพื้นที่ภัยพิบัตินั้นสามารถให้การสื่อสารที่มีความต่อเนื่อง เนื่องจากผู้ใช้ส่งข้อความผ่านโครงสร้างพื้นฐานที่ได้ทำการติดตั้งบนพื้นที่ภัยพิบัติซึ่งโครงสร้างพื้นฐานที่ได้ติดตั้งนั้นได้ถูกจัดวางห่างกันภายในระยะของสัญญาณและไม่ได้ถูกทำให้เคลื่อนที่ให้ห่างออกจากระยะสัญญาณ ทำให้ได้การสื่อสารที่มีประสิทธิภาพมากกว่าเมื่อเทียบกับการสื่อสารแบบ Peer-to-peer แต่อย่างไรก็ตามการสื่อสารโดยการติดตั้งโครงสร้างพื้นฐานนั้นจะไม่สามารถครอบคลุมพื้นที่ภัยพิบัติได้ทุกบริเวณ เพราะจะมีบางบริเวณที่ไม่สามารถติดตั้งโครงสร้างพื้นฐานทำให้ผู้ประสบภัยในบริเวณดังกล่าวไม่สามารถเข้าถึงการสื่อสารได้ อีกทั้งการติดตั้งโครงสร้างพื้นฐานนั้นยังต้องใช้งบประมาณในการติดตั้งสูงกว่าการสร้างระบบสื่อสารแบบ Peer-to-peer อีกด้วย

งานวิจัย A Disaster Information System by Ballooned Wireless Adhoc Network [10] ของ Shibata และทีมวิจัย ได้เสนอการวางโครงสร้างพื้นฐานโดยใช้บอลลูนแอดฮอกในการสื่อสาร การใช้เสาสัญญาณปกตินั้นอาจจะมีปัญหาในด้านของพื้นที่ที่ไม่อำนวยต่อการติดตั้ง ทำให้ไม่สามารถติดตั้งเสาสัญญาณได้ทุกบริเวณ เพื่อให้สามารถสื่อสารได้ครอบคลุมบริเวณพื้นที่ภัยพิบัติ งานวิจัยนี้เลือกการสร้างเครือข่ายโครงสร้างพื้นฐานผ่านบอลลูน โดยการนำเสาสัญญาณติดที่บอลลูนและปล่อยให้ลอยขึ้นฟ้าโดยมีเชือกยึดหลักไว้เพื่อป้องกันบอลลูนลอยเปลี่ยนที่ ผู้ประสบภัยสามารถสื่อสารผ่านบอลลูนได้โดยบอลลูนจะส่งข้อความหากันโดยใช้เครือข่ายแอดฮอก ในงานวิจัยนี้ผู้ประสบภัยจะสื่อสารกันด้วย Voice Over IP ผ่านโครงสร้างพื้นฐานที่ติดบนบอลลูน

การสื่อสารโดยเครือข่ายโครงสร้างพื้นฐานธรรมดาสามารถให้การสื่อสารได้แค่บนพื้นที่ภัยพิบัติ เพื่อที่จะสื่อสารได้ไกลออกไปมากยิ่งขึ้น Weiquan Lu และ ทีมวิจัยได้เสนอ Communications Support for Disaster Recovery Operation using Hybrid MANET [11] ซึ่งเป็นการทำเครือข่ายโครงสร้างพื้นฐานบนพื้นที่ภัยพิบัติโดยอาศัยการทำงานร่วมกันของหลายอุปกรณ์ ตั้งแต่เสาสัญญาณ อุปกรณ์สื่อสาร และดาวเทียม งานวิจัยนี้ได้ทำการติดอุปกรณ์รับสัญญาณดาวเทียมเข้ากับคอมพิวเตอร์ การทำงานนั้นจะคล้ายกับการทำงานปกติของเครือข่ายโครงสร้างแบบพื้นฐาน นั่นคือข้อความจะถูกส่งผ่านจากอุปกรณ์สื่อสารมายังเสาสัญญาณ และศูนย์กู้ภัยตามลำดับ จากนั้นศูนย์กู้ภัยจะส่งข้อความไปยังเครือข่ายดาวเทียมเพื่อทำการติดต่อกับพื้นที่ภายนอกเขตภัยพิบัติ

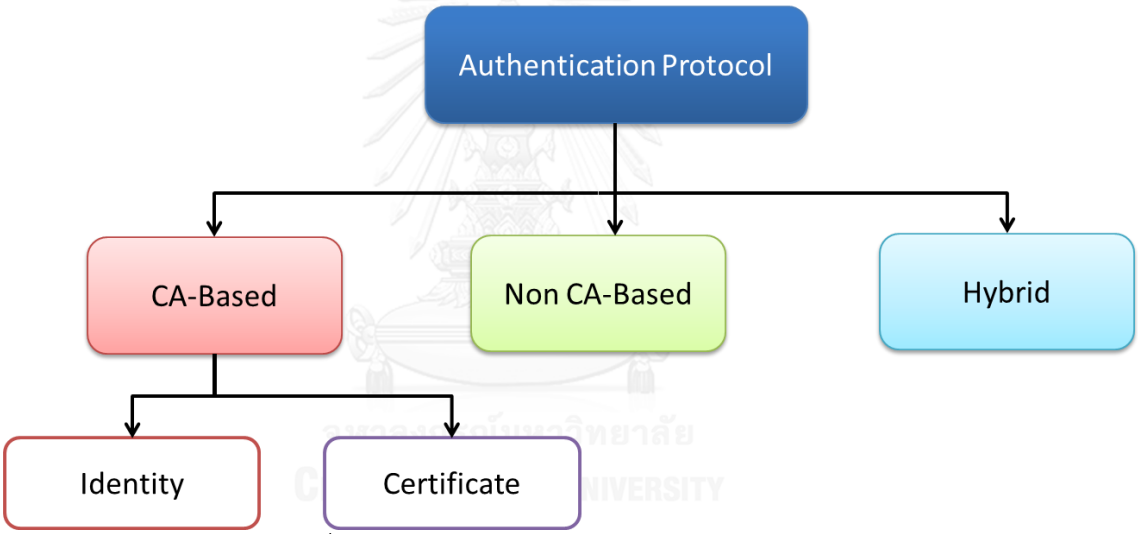
2) การใช้งานโครงสร้างพื้นฐานเดิมบนพื้นที่ภัยพิบัติ

การติดตั้งโครงสร้างพื้นฐานใหม่บนพื้นที่ภัยพิบัตินั้นทำให้ต้องสูญเสียงบประมาณจำนวนมากในการติดตั้งโครงสร้างพื้นฐาน บนสมมติฐานว่าโครงสร้างพื้นฐานบนพื้นที่ภัยพิบัติบางส่วนนั้นสามารถใช้การได้อยู่ ดังนั้นจึงสามารถใช้งานโครงสร้างพื้นฐานของเดิมบนพื้นที่ภัยพิบัติเพื่อกู้คืนระบบสื่อสารได้โดยไม่จำเป็นต้องติดตั้งโครงสร้างพื้นฐานใหม่

จากแนวคิดว่าพื้นที่ภัยพิบัตินั้นไม่ได้ถูกทำลายทั้งหมดโครงสร้างพื้นฐานบางส่วนนั้นยังสามารถใช้การได้บนพื้นที่ภัยพิบัติ Wei Lui และทีมวิจัย ได้เสนอ On Efficient Traffic Distribution for Disaster Area Communication Using Wireless Mesh Networks [12] ซึ่งเป็นงานวิจัยที่มุ่งเน้นไปที่การใช้งานโครงสร้างพื้นฐานบนพื้นที่ภัยพิบัติอย่างมีประสิทธิภาพ บนสมมติฐานที่ว่าบนพื้นที่ภัยพิบัตินั้นมีโครงสร้างพื้นฐานจำพวกเสาสัญญาณวางอยู่โดยรอบและเพียงพอสำหรับผู้ประสบภัยที่จะใช้งานเพื่อการสื่อสาร แต่โครงสร้างพื้นฐานเหล่านั้นไม่สามารถนำมาใช้งานกับการสื่อสารบนพื้นที่ภัยพิบัติได้ทันทีเนื่องจากว่าโครงสร้างพื้นฐานที่มีอยู่เดิมบนพื้นที่ภัยพิบัตินั้นไม่ได้มีการทำงานที่รองรับกับการส่งข้อมูลในสถานการณ์ภัยพิบัติ งานวิจัยนี้จึงได้พยายามทำการติดตั้งโปรแกรมเข้าไปที่โครงสร้างพื้นฐานที่มีอยู่เพื่อให้การจัดการส่งข้อมูลได้อย่างมีประสิทธิภาพ ทำให้โครงสร้างพื้นฐานที่มีอยู่เดิมสามารถทำงานรองรับสถานการณ์ภัยพิบัติได้

2.2.2 งานวิจัยที่เกี่ยวข้องกับการสร้างการยืนยันตัวตน

การยืนยันตัวตนนั้นเป็นวิธีการที่จะเพิ่มความน่าเชื่อถือให้กับข้อมูลที่ส่งจากผู้ส่งถึงผู้รับ การยืนยันตัวตนนั้นจะใช้หลักการของ Digital Signature หรือการใช้ Certificate Authentication แต่ในการยืนยันตัวตนในบางสถานการณ์นั้นมีข้อจำกัดบางอย่างเช่น ผู้ที่ต้องการจะยืนยันตัวตนไม่สามารถติดต่อกับหน่วยงานที่มีความน่าเชื่อถือได้ ทำให้ไม่สามารถได้รับ Certificate ที่จะนำมาใช้ในการยืนยันตัวตนได้ เป็นต้น อีกทั้งในการยืนยันตัวตนนั้นยังมีปัจจัยหลายประเด็นที่ต้องคำนึงถึงเช่น ประเด็นเรื่องการจัดการกับ Certificate ที่มอบให้กับผู้ใช้ว่า Certificate จะมีอายุอยู่นานเท่าไหร่ และจะทำการส่งไปให้ผู้ใช้อย่างไร เป็นต้น ดังนั้นจึงเกิดแนวคิดของการสร้างวิธีการยืนยันตัวตนขึ้นมาหลากหลายวิธีที่เหมาะสมกับสถานการณ์หนึ่งๆ เราสามารถแบ่งกลุ่มวิธีการยืนยันตัวตนออกเป็น 3 กลุ่มตามประเภทของผู้ที่มอบ Certificate ให้เราได้ดังนี้



รูปที่ 17 ประเภทของงานวิจัยด้านการยืนยันตัวตน

การยืนยันตัวตนโดยผ่านเจ้าหน้าที่

การยืนยันตัวตนประเภทนี้ผู้ที่ต้องการจะยืนยันตัวตนจะทำการยืนยันตัวตนได้ต้องสามารถติดต่อกับเจ้าหน้าที่ได้ โดยเจ้าหน้าที่จะเป็นผู้ที่ทำการตรวจสอบหลักฐานประจำตัวพร้อมกับ Public key ที่เราใช้นั่นเอง ซึ่งการยืนยันตัวตนโดยผ่านเจ้าหน้าสามารถแบ่งออกได้ 2 ประเภทดังนี้

1) การยืนยันตัวตนโดยใช้ ID ในการตรวจสอบหลักฐาน

การยืนยันตัวตนประเภทนี้ผู้รับข้อความปลายทางสามารถทราบ Public key ของผู้ส่งได้เพียงแค่รู้ ID ของผู้ส่ง โดยผู้รับข้อความปลายทางนั้นจะส่งข้อความร้องขอ Public key ของผู้ส่ง

จากเจ้าหน้าที่โดยใช้ ID ของผู้ส่งข้อความเป็นตัวค้นหา จากนั้นเจ้าหน้าที่จะส่ง Public key กลับมายังผู้ร้องขอนั่นเอง สำหรับขั้นตอนในการยืนยันตัวตนนั้นผู้ที่จะทำการยืนยันตัวตนจะส่ง ID พร้อมหลักฐานอื่นๆ ซึ่งใช้เป็นหลักฐานประจำตัวที่ใช้ในการยืนยันตัวตนให้กับเจ้าหน้าที่ตรวจสอบ ซึ่ง ID นี้อาจจะเป็นรหัสประชาชน หรือเป็นชื่อจริง-นามสกุล ก็ได้ จากนั้นเจ้าหน้าที่จะทำการตรวจสอบหลักฐานที่ส่งมา ถ้าหลักฐานที่ส่งมาสอดคล้องและมีความถูกต้องกับผู้ที่จะยืนยันตัวตน เจ้าหน้าที่จะบันทึก Public key และ ID ลงในฐานข้อมูลที่ใช้ในการให้บริการกับผู้ร้อง งานวิจัยนี้ถูกเสนอโดย Shamir และทีมวิจัยในชื่องาน Identity-Based Cryptography (IBC) [13]

แต่อย่างไรก็ตามด้วยกระบวนการของ IBC นั้น เจ้าหน้าที่จะรู้ Private key ของผู้ใช้ทุกคนซึ่งทำให้เจ้าหน้าที่สามารถปลอมแปลงเป็นบุคคลใดก็ได้ Al-Riyami and Paterson ได้เสนอ Certificateless Public Key Cryptography [14] ซึ่งเป็นวิธีการจัดการปัญหาบุคคลที่สามโดยการเพิ่ม Asymmetric key สำหรับผู้ใช้อีกชุด ผู้ใช้ทุกคนจะมี Asymmetric key ประจำตัวสองชุดด้วยกัน โดยชุดแรกจะได้จากเจ้าหน้าที่ อีกชุดเป็นรหัสที่สร้างเอง เมื่อจะทำการยืนยันตัวตนจะเข้ารหัสข้อความด้วยรหัสสองชุดพร้อมกัน โดยแนบ Public key ของรหัสชุดที่สร้างเองไปกับข้อความ ผู้รับข้อความปลายทางจะยืนยันตัวตนของผู้ใช้ตนทางผ่านกลไกเดียวกับวิธี IBC แต่วิธีนี้ทำให้เจ้าหน้าที่ไม่สามารถปลอมแปลงเป็นบุคคลต้นทางได้เนื่องจากเจ้าหน้าที่ไม่สามารถรู้รหัสชุดที่สองของผู้ใช้นั่นเอง

งานวิจัย Certificateless Public Key Cryptography ยังมีความไม่สมบูรณ์อยู่ เนื่องจากว่าผู้ที่ต้องการจะโจมตีระบบนั้นสามารถโจมตีผ่านวิธีการ Denial of Decryption ได้ ซึ่งวิธีนี้จะป้องกันผู้ใช้ในการถอดรหัสข้อความ ถึงแม้ว่าจะไม่สามารถปลอมแปลงเอกสารได้ แต่ผู้รับข้อความก็ไม่สามารถอ่านข้อความได้เช่นกัน ดังนั้น Liu และ Au ได้เสนอ Self-Generated-Certificate Public Key Encryption (SGC-PKE) [15] ซึ่งมีการเพิ่มกลไกในการป้องกันการโจมตีแบบ Denial of Decryption นั่นเอง

2) การยืนยันตัวตนโดยใช้ Certificate ในการตรวจสอบหลักฐาน

การใช้ Certificate ในการยืนยันตัวตนนั้นสามารถใช้วิธีมาตรฐานในการยืนยันตัวตนนั่นคือ Certificate Authentication ซึ่งวิธีนี้สามารถส่งคำร้องขอ Certificate ไปยังเจ้าหน้าที่พร้อมกับแนบหลักฐานที่จำเป็นในการยืนยันตัวตนและ Public key ที่ต้องการจะใช้ จากนั้นเจ้าหน้าที่จะทำการออก Certificate ให้กับผู้ใช้ ผู้ใช้สามารถนำ Certificate นี้ไปใช้ในการยืนยันตัวตนได้

การยืนยันตัวตนโดยผ่านเจ้าหน้าที่นั้นสามารถให้การยืนยันตัวตนที่มีความน่าเชื่อถือสูง บนสมมติฐานว่าเจ้าหน้าที่จะมีความน่าเชื่อถือ แต่ว่าการยืนยันตัวตนประเภทนี้จำเป็นจะต้องได้รับการติดต่อกับเจ้าหน้าที่ก่อนนั่นเองซึ่งทำให้มีข้อจำกัดในบางสถานการณ์

การยืนยันตัวตนโดยไม่อาศัยเจ้าหน้าที่

ในบางสถานการณ์ผู้ที่ต้องการจะยืนยันตัวตนนั้นไม่สามารถติดต่อกับเจ้าหน้าที่ได้ ทำให้ไม่สามารถใช้การยืนยันตัวตนโดยผ่านเจ้าหน้าที่ได้ ดังนั้นจึงมีแนวคิดของการเชื่อใจขึ้นมา แต่กระบวนการเชื่อใจนั้นเมื่อแปลงเป็นกระบวนการทางการยืนยันตัวตนนั้นจะเป็นการลงนามที่ Unsigned Certificate ของผู้ขอความเชื่อใจ ด้วยวิธีการนี้ผู้ใช้สามารถขอความเชื่อใจจากผู้คนในบริเวณรอบๆได้

Capkun และทีมวิจัยได้เสนอ Self-organized public-key management for mobile ad-hoc network (SOPKM) [16] ซึ่งเป็นวิธีการยืนยันตัวตนโดยไม่อาศัยเจ้าหน้าที่ในการยืนยันตัวตนโดยวิธีการเชื่อใจ ผู้ใช้จะทำการเชื่อใจกันเองผ่านการลงนามบน Unsigned Certificate ของผู้ที่ต้องการจะยืนยันตัวตน โดยผู้ที่จะยืนยันตัวตนนั้นจะต้องส่ง Certificate ของตนเองไปให้เพื่อนบ้านทำการยืนยัน ถ้าเพื่อนบ้านเชื่อใจผู้ที่ส่ง Certificate มาเพื่อนบ้านจะลงนามบน Unsigned Certificate ให้ จากนั้นผู้ที่จะทำการยืนยันตัวตนก็จะประกาศ Certificate ของตนเองออกไปเพื่อแจ้งรายชื่อของบุคคลที่เชื่อใจ เมื่อผู้ใช้อื่นได้รับข้อความประกาศ Certificate มาจากหลายๆที่นั้น จะสามารถสร้างกราฟความน่าเชื่อใจของ Certificate ที่ได้รับมา โดยจุดยอดแทน Public key ของผู้ใช้และ เส้นแทน Certificate มาทำการประมวลผลความน่าเชื่อถือ ผู้ใช้แต่ละคนจะมีการแลกเปลี่ยนข้อมูลความน่าเชื่อใจระหว่างเพื่อนบ้านเป็นระยะเพื่อตรวจสอบความถูกต้องและเพิ่มประสิทธิภาพการยืนยันตัวตน บุคคลที่น่าเชื่อถือจะเป็นบุคคลที่มี Path จากโหนดของผู้นั้นถึงโหนดตนเอง

Dahshan and Irvine ได้เสนอ On Demand Self-Organized Public Key Management for MANET (ODSOPKM) [17] โดยงานวิจัยนี้ได้ใช้โปรโตคอล AODV ในการสื่อสาร งานวิจัยนี้ได้มีการใช้กระบวนการการขอเส้นทาง (RREQ) และการตอบกลับเส้นทาง (RREP) ของโปรโตคอล AODV มาช่วยในการยืนยันตัวตน โดยการขอเส้นทางและการตอบกลับเส้นทางนั้นจะส่งข้อความผ่านอุปกรณ์สื่อสารที่มีความน่าเชื่อถือเท่านั้น เมื่อส่งข้อความไปยังอุปกรณ์สื่อสารที่น่าเชื่อถือแล้ว โปรโตคอลจะทำการแนบ Certificate ของตนเองผ่านกระบวนการร้องขอเส้นทาง โดย Certificate จะถูกแนบมาใน Packet ที่ใช้ในการสื่อสารทุกครั้งที่มีการส่งผ่านโหนดที่มีความน่าเชื่อถือ ผู้รับข้อความนั้นจึงทราบได้ว่าข้อความนี้ได้ส่งผ่านอุปกรณ์สื่อสารของใครมาบ้างโดยสามารถตรวจสอบจาก Certificate ที่แนบมานั่นเอง

การยืนยันตัวตนแบบไม่อาศัยเจ้าหน้าที่นั้นเป็นการยืนยันตัวตันที่มีความยืดหยุ่นสูง สามารถยืนยันตัวตนได้ผ่านการเชื่อใจ แต่ในทางกลับกันการยืนยันตัวตนประเภทนี้มีความน่าเชื่อถือน้อยกว่าการยืนยันตัวตนผ่านเจ้าหน้าที่ เพราะเราไม่สามารถรู้ประวัติอย่างละเอียดของผู้ที่เชื่อในบุคคลหนึ่งๆ ได้ทั้งหมด

การยืนยันตัวตนแบบผสม

การยืนยันตัวตนผ่านเจ้าหน้าที่นั้นจะมีข้อจำกัดในด้านการติดต่อกับเจ้าหน้าที่ ในทางกลับกันการยืนยันตัวตนแบบไม่ผ่านเจ้าหน้าที่นั้นก็จะมีข้อจำกัดในด้านความน่าเชื่อถือ ดังนั้นจึงมีงานวิจัยที่นำหลักการของงานวิจัยทั้งสองแบบข้างตนมารวมกันเป็นการยืนยันตัวตนแบบผสม การยืนยันตัวตนแบบผสมนี้จะรวมข้อดีของการยืนยันตัวตนแบบอาศัยเจ้าหน้าที่และการยืนยันตัวตนแบบไม่อาศัยเจ้าหน้าที่เข้าด้วยกัน

S. Choochotkaew ได้เสนองานวิจัยชื่อ Development of a trustworthy authentication system in mobile ad-hoc networks for disaster area [18] ซึ่งเป็นงานวิจัยที่เสนอการยืนยันตัวตนบนพื้นที่ภัยพิบัติโดยการนำการยืนยันตัวตนแบบอาศัยเจ้าหน้าที่และไม่อาศัยเจ้าหน้าที่มารวมกัน งานวิจัยนี้ได้นำข้อดีของงานวิจัยการยืนยันตัวตนผ่านเจ้าหน้าที่ SGC-PKE รวมเข้าด้วยกันกับงานวิจัยที่ใช้การยืนยันตัวตนโดยไม่ผ่านเจ้าหน้าที่ SOPKM ดังนั้นผู้ใช้งานจะสามารถได้รับการยืนยันตัวตนเหมาะสมกับสภาพแวดล้อมของตัวเองขณะนั้น ถ้าผู้ใช้สามารถติดต่อกับเจ้าหน้าที่ได้ ผู้ที่ต้องการจะยืนยันตัวตนนั้นจะทำการยืนยันตัวตนผ่านเจ้าหน้าที่โดยใช้วิธีของ SGC-PKE แต่ถ้าผู้ที่ต้องการจะยืนยันตัวตนไม่สามารถติดต่อกับเจ้าหน้าที่ได้ก็จะใช้การยืนยันตัวตนผ่านกลไกของ SOPKM ดังนั้นอุปกรณ์สื่อสารของผู้ใช้ก็จะมีกลไกการแลกเปลี่ยน Certificate graph อยู่เป็นระยะๆ อย่างไรก็ตามงานวิจัยนี้ยังไม่สามารถนำไปใช้ได้จริงบนพื้นที่ภัยพิบัติเนื่องจากกระบวนการยืนยันตัวตนแบบไม่ใช้เจ้าหน้าที่นั้นยังมีการแลกเปลี่ยนข้อมูลมากทำให้เกิดความคับคั่งในระบบ ดังนั้นไม่สามารถนำไปใช้งานบนพื้นที่ภัยพิบัติที่ต้องใช้ทรัพยากรอย่างจำกัดได้

การยืนยันตัวตนแบบผสมนั้นสามารถรวมข้อดีของวิธีการยืนยันตัวตนแบบอาศัยเจ้าหน้าที่และไม่อาศัยเจ้าหน้าที่เข้าด้วยกันซึ่งวิธีการแบบผสมนี้เหมาะกับการยืนยันตัวตนบนพื้นที่ภัยพิบัติซึ่งมีผู้คน 2 กลุ่ม กลุ่มแรกคือกลุ่มที่สามารถติดต่อสื่อสารกับเจ้าหน้าที่กู้ภัยได้ ดังนั้นกลุ่มนี้สามารถทำการยืนยันตัวตนผ่านเจ้าหน้าที่ได้ กับผู้ใช้อีกกลุ่มคือกลุ่มที่ไม่สามารถติดต่อกับเจ้าหน้าที่ได้ กลุ่มนี้ก็จะยังสามารถมีการสื่อสารที่มีความน่าเชื่อถือเพียงพอโดยใช้วิธีการยืนยันตัวตนแบบไม่ผ่านเจ้าหน้าที่ได้

บทที่ 3 การออกแบบและพัฒนา

ระบบสื่อสารเป็นสิ่งที่สำคัญในยามภัยพิบัติเพราะว่าระบบสื่อสารนั้นสามารถให้ผู้ประสบภัยได้รับความช่วยเหลือได้อย่างทันท่วงที นอกจากให้ความช่วยเหลือกับผู้ประสบภัยแล้วนั้นการสื่อสารยังเป็นสิ่งที่ช่วยคลายความกังวลของผู้คนในพื้นที่ภัยพิบัติได้อีกด้วย เนื่องจากผู้คนสามารถติดต่อสื่อสารกับคนรอบข้างหรือคนใกล้ตัวได้ทำให้ลดความกังวลและลดความตึงเครียดของสถานการณ์ลง แต่อย่างไรก็ตามเมื่อเกิดภัยพิบัติขึ้นไม่ว่าจะเป็นน้ำท่วม, พายุโซนร้อน หรือแผ่นดินไหว ภัยพิบัติเหล่านี้จะเข้าทำลายบ้านเรือนและโครงสร้างพื้นฐานเป็นส่วนมาก ผลที่ตามมาคือระบบสื่อสารที่ต้องอาศัยโครงสร้างพื้นฐานในการส่งข้อความนั้นได้ถูกทำลายลง ทำให้ผู้คนในบริเวณพื้นที่ภัยพิบัตินั้นไม่สามารถสื่อสารได้ในสถานการณ์หลังภัยพิบัติ

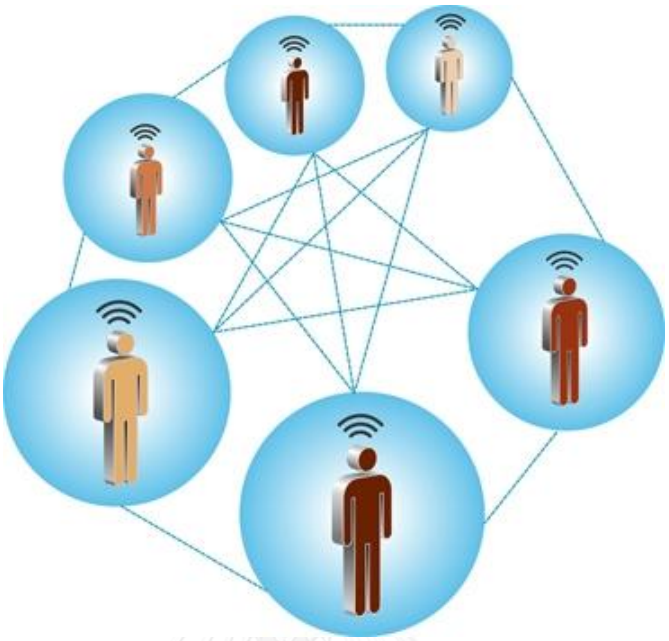
เมื่อระบบสื่อสารถูกทำลายลงนั้นทำให้เจ้าหน้าที่ที่เข้ามาทำการช่วยเหลือไม่สามารถติดต่อสื่อสารกับผู้คนในพื้นที่ได้อย่างสะดวก การช่วยเหลือจึงเป็นไปได้ยากขึ้น อีกทั้งความวิตกกังวลของผู้ประสบภัยยังจะเพิ่มความตึงเครียดให้กับสถานการณ์อีกด้วย ระบบสื่อสารจะสามารถทำหน้าที่สำคัญในพื้นที่ภัยพิบัติ นั่นคือระบบสื่อสารนั้นจะช่วยเชื่อมต่อผู้คนเข้าด้วยกันทำให้ผู้ช่วยเหลือสามารถเข้าช่วยเหลือผู้ประสบภัยได้ และอีกทั้งสามารถแจ้งรายละเอียดของสถานการณ์ต่างๆผ่านระบบสื่อสารไปยังผู้ประสบภัยได้อีกด้วย

แต่เนื่องจากระบบสื่อสารถูกทำลายลงทำให้จำเป็นจะต้องหาระบบสื่อสารใหม่เข้ามาใช้งานแทนระบบเดิม งานวิจัยนี้จึงได้ออกแบบระบบสื่อสารโดยใช้เครือข่ายแอดฮอกมาใช้สร้างระบบสื่อสารทดแทนหลังจากเกิดภัยพิบัติ ระบบสื่อสารที่สร้างขึ้นมาทดแทนนี้จะต้องสามารถติดตั้งใช้งานได้บนพื้นที่ภัยพิบัติได้อย่างรวดเร็วเพื่อที่จะได้ให้ความสะดวกกับผู้คนบนพื้นที่ประสบภัยได้ อีกทั้งถ้าระบบสื่อสารสามารถติดตั้งได้อย่างรวดเร็วนั้นยังสามารถเพิ่มอัตราการรอดชีวิตของผู้คนบนพื้นที่ประสบภัยได้อีกด้วย

นอกจากการระบบสื่อสารที่สามารถให้การเชื่อมต่อและการส่งข้อความที่มีประสิทธิภาพแล้วนั้น ความน่าเชื่อถือของการส่งข้อความก็เป็นอีกปัจจัยหนึ่งในการสื่อสาร เมื่อเกิดเหตุภัยพิบัติขึ้นแน่นอนว่าผู้คนที่ประสบภัยพิบัติต่างเดือดร้อน และผู้ประสบภัยบางคนตกอยู่ในสถานการณ์ที่ยากลำบาก ด้วยสถานการณ์เช่นนี้อาจจะทำให้ผู้คนเกิดความไม่ประสงค์ดีต่อผู้อื่นขึ้นมาเนื่องจากความต้องการในการอยู่รอดของมนุษย์ ผู้ไม่ประสงค์ดีอาจจะต้องการทรัพย์สินหรือสิ่งของจากผู้คนรอบๆเพื่อใช้ในการอยู่รอดเป็นต้น และด้วยสถานการณ์ภัยพิบัตินั้นก่อให้เกิดช่องโหว่ที่ยินยอมให้ผู้ไม่ประสงค์ดีก่อเหตุได้อย่างง่ายดาย ดังนั้นระบบสื่อสารจึงต้องมีความปลอดภัยเพียงพอที่ไม่ลดประสิทธิภาพในการสื่อสารบนพื้นที่ภัยพิบัติ

ในงานวิจัยนี้ได้เสนอระบบสื่อสารที่มีความน่าเชื่อถือขึ้นมาโดยระบบสื่อสารนี้จะเป็นการรวมข้อดีของการสื่อสาร 2 รูปแบบเข้าด้วยกัน นั่นคือการสื่อสารโดยเครือข่ายแอดฮอกแบบ Peer-to-peer และการสื่อสารโดยใช้เครือข่ายแอดฮอกแบบติดตั้งโครงสร้างพื้นฐานเพื่อใช้ในการสื่อสารบนพื้นที่ภัยพิบัติ

3.1 การออกแบบและพัฒนาระบบสื่อสารบนเครือข่ายแอดฮอกแบบ Peer-to-peer



รูปที่ 18 ระบบสื่อสารแบบ Peer-to-peer

ระบบสื่อสารบนเครือข่ายแบบ Peer-to-peer นั้นเป็นระบบสื่อสารที่ผู้ใช้สามารถสื่อสารได้โดยไม่ต้องผ่านโครงสร้างพื้นฐาน ระบบสื่อสารนี้เกิดขึ้นจากระบบเครือข่ายของอุปกรณ์สื่อสาร โดยผู้ใช้สามารถส่งข้อความโดยใช้อุปกรณ์สื่อสารตนเองผ่านไปยังอุปกรณ์สื่อสารผู้อื่นปลายทางได้โดยตรง ถ้าอุปกรณ์สื่อสารของผู้ที่ต้องการจะส่งข้อความให้นั้นต้องการจะส่งให้อุปกรณ์ปลายทางที่อยู่ไกลออกไปมากกว่า 1 Hop การส่งข้อความนั้นจะเป็นการส่งข้อความผ่านอุปกรณ์สื่อสารบริเวณรอบๆไปเรื่อยๆจนกระทั่งถึงปลายทางนั่นเอง

เครือข่ายการสื่อสารนี้จึงสามารถเกิดขึ้นได้โดยไม่ต้องมีอุปกรณ์ช่วยเหลือแต่อย่างใดดังนั้น การนำระบบการสื่อสารแบบ Peer-to-peer มาติดตั้งบนพื้นที่ภัยพิบัตินั้นจึงสามารถติดตั้งได้อย่างรวดเร็ว ผู้ใช้จะมีการส่งข้อความผ่านไปยังผู้ใช้อื่นได้อย่างอิสระทำให้เกิดความสะดวกในการสื่อสารอีกด้วย แต่อย่างไรก็ตามการสื่อสารโดยใช้เครือข่าย Peer-to-peer นั้นมีความไม่ปลอดภัยสูง ในการส่งข้อความผ่านอุปกรณ์สื่อสารผู้อื่นนั้น ผู้ไม่ประสงค์ดีอาจจะทำการดัดแปลงข้อความได้ทำให้ต้องสร้างวิธีการสื่อสารที่มีความปลอดภัยและมีความรวดเร็วในการส่งข้อความระหว่างผู้ใช้

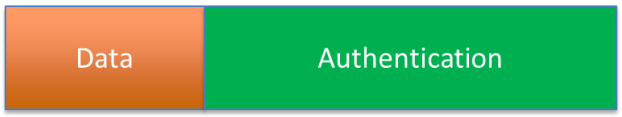
3.1.1 การออกแบบ Protocol ที่ใช้ในการสื่อสารบนเครือข่าย Peer-to-peer

จากที่ได้กล่าวมาข้างต้นว่าการสื่อสารในพื้นที่ภัยพิบัตินั้นจำเป็นต้องมีความรวดเร็วในการส่งข้อความเพื่อแจ้งข่าวสารให้กับผู้คนบริเวณรอบๆ และยังต้องมีความปลอดภัยเพียงพอที่จะทำให้ผู้ใช้งานมีความมั่นใจในการใช้งานได้ แต่อย่างไรก็ตามการเพิ่มความปลอดภัยเข้าไปในระบบสื่อสารนั้นจะต้องแลกกับประสิทธิภาพการทำงานของโปรโตคอล ดังนั้นจึงจะต้องหาวิธีการรวมกันระหว่างประสิทธิภาพการสื่อสารและความปลอดภัยที่ได้รับอย่างเหมาะสมเพื่อที่จะสร้างโปรโตคอลการสื่อสารที่มีประสิทธิภาพและมีความน่าเชื่อถือในการสื่อสารได้บนพื้นที่ภัยพิบัติ

ในการที่จะเพิ่มความปลอดภัยให้กับการสื่อสารนั้นสามารถทำได้ด้วยวิธีการยืนยันตัวตนโดยการยืนยันตัวตนนั้นจะทำให้ผู้ที่สื่อสารด้วยมั่นใจว่าข้อความนี้เป็นข้อความที่ส่งมาจากผู้ใช้คนใด และมีความน่าเชื่อถือมากน้อยแค่เพียงใด ในขั้นตอนการยืนยันตัวตนนั้นยังมีกลไกที่ช่วยป้องกันการแก้ไขหรือเปลี่ยนแปลงข้อความอีกด้วย ดังนั้นกลไกนี้จึงช่วยเพิ่มความปลอดภัยและความน่าเชื่อถือให้การโปรโตคอลที่ใช้ในการสื่อสารนั่นเอง งานวิจัยนี้ได้ทำการพัฒนากลไกการยืนยันตัวตนเข้ากับโปรโตคอลที่ใช้ในการสื่อสาร ซึ่งกลไกในการยืนยันตัวตนนั้นสามารถทำงานร่วมกับกลไกการส่งข้อความ ทำให้มีการส่งข้อความได้อย่างปลอดภัยและมีประสิทธิภาพ

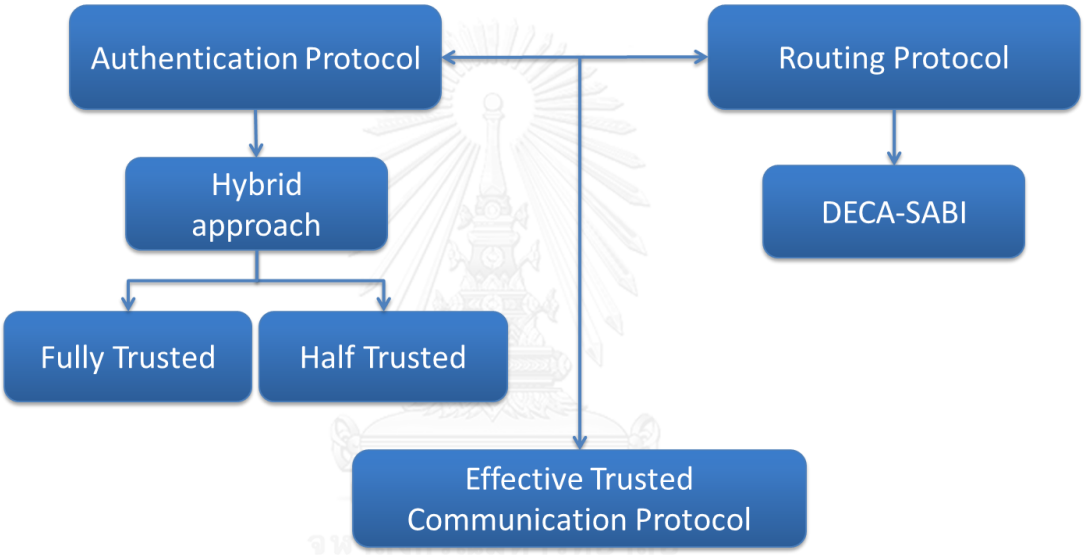
การยืนยันตัวตนผ่านอุปกรณ์สื่อสารที่ใช้งานบนพื้นที่ภัยพิบัตินั้นต้องคำนึงถึงการเชื่อมต่อเครือข่าย และทรัพยากรพลังงานของอุปกรณ์สื่อสารที่มีอยู่อย่างจำกัด เมื่อคำนึงถึงความสามารถในการเชื่อมต่อเครือข่ายของผู้คนบนพิบัตินั้น ผู้ใช้งานจะถูกแบ่งออกเป็นสองกลุ่มดังนี้ กลุ่มแรกจะเป็นกลุ่มที่เคยได้พบกับเจ้าหน้าที่หรือสามารถติดต่อกับเจ้าหน้าที่ได้มาก่อน กลุ่มนี้จะสามารถใช้การยืนยันตัวตนโดยผ่านเจ้าหน้าที่ได้ซึ่งเป็นการยืนยันตัวตนที่มีความน่าเชื่อถือสูง กลุ่มที่สองคือกลุ่มคนที่ไม่สามารถติดต่อกับเจ้าหน้าที่ได้มาก่อน กลุ่มนี้จึงไม่สามารถทำการยืนยันตัวตนโดยผ่านเจ้าหน้าที่ได้จำเป็นจะต้องใช้การยืนยันตัวตนผ่านการเชื่อใจ ดังนั้นการออกแบบการยืนยันตัวตนบนพื้นที่ภัยพิบัตินั้นจำเป็นจะต้องทำให้ครอบคลุมกับบุคคลทั้งสองกลุ่มนี้ ในงานวิจยนี้จึงเลือกวิธีการยืนยันตัวตนแบบผสมเพื่อใช้ในการยืนยันตัวตนบนพื้นที่ภัยพิบัติ

อีกหนึ่งปัจจัยที่ต้องคำนึงถึงในการพัฒนาการยืนยันตัวตนบนพื้นที่ภัยพิบัติคือเรื่องพลังงานของอุปกรณ์สื่อสารที่มีอยู่อย่างจำกัด มีหลายงานวิจัยที่สร้างการยืนยันตัวตนขึ้นมาแต่ไม่ได้คำนึงในด้านพลังงาน การยืนยันตัวตนหลายวิธีนั้นจึงมีขั้นตอนการประมวลผลที่ซับซ้อนอีกทั้งต้องมีการแลกเปลี่ยนข้อมูลกับอุปกรณ์สื่อสารเพื่อนบ้านอีกมากมายซึ่งเป็นการใช้พลังงานอย่างสิ้นเปลือง อีกทั้งยังเพิ่มความคับคั่งให้กับระบบสื่อสารทำให้ไม่สามารถมาประยุกต์ใช้บนพื้นที่ภัยพิบัติได้ โดยเฉพาะการสร้างการยืนยันตัวตนแบบไม่อาศัยเจ้าหน้าที่นั้น ข้อมูลในการยืนยันตัวตนของบุคคลจะมีปริมาณมากกว่าการยืนยันตัวตนแบบอาศัยเจ้าหน้าที่เพราะต้องมีการแลกเปลี่ยนข้อมูลความเชื่อใจทำให้ไม่สามารถนำวิธีจากงานวิจัยต่างๆมาปรับใช้งานบนพื้นที่ภัยพิบัติได้



รูปที่ 19 รูปแบบข้อความที่ใช้ในการสื่อสาร

เมื่อผู้ใช้ได้รับข้อมูลมานั้นผู้ใช้ต้องการจะทราบความน่าเชื่อถือของข้อมูลโดยนำความน่าเชื่อถือของบุคคลกระจายข้อมูลมาประกอบการตัดสินใจ ดังนั้นจึงเกิดสมมติฐานขึ้นว่าว่าการยืนยันตัวตนจำเป็นต่อเมื่อมีการส่งข้อมูล สำหรับผู้ใช้ที่ไม่ได้ทำการส่งข้อความนั้นก็จะไม่มีความจำเป็นที่จะต้องใช้งานกลไกการยืนยันตัวตน ดังนั้นจึงมีแนวคิดที่จะนำข้อมูลการยืนยันตัวตนแนบผ่านข้อความที่ใช้ส่งสื่อสารกัน (แสดงดังรูปที่ 19) เพื่อใช้เป็นตัววัดบอกระดับความน่าเชื่อถือของข้อความ



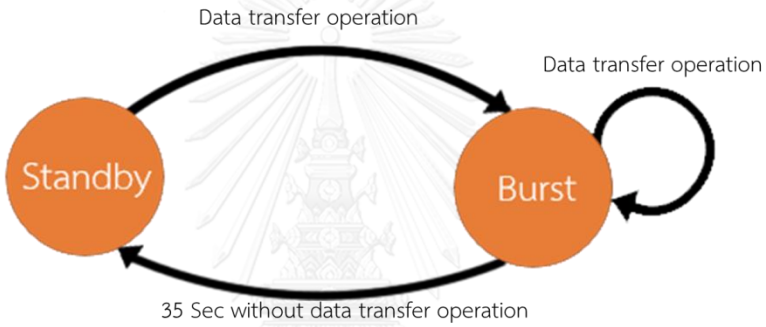
รูปที่ 20 โครงสร้างโปรโตคอล

จากแนวคิดของการนำการยืนยันตัวตนแนบกับข้อความที่ใช้ในการสื่อสารกันนั้นทำให้ความสามารถในการยืนยันตัวตนขึ้นกับความสามารถในการส่งข้อความของโปรโตคอล ดังนั้นเกิดแนวคิดของการสร้างโปรโตคอลที่สามารถส่งข้อความที่มีความน่าเชื่อถืออย่างมีประสิทธิภาพ (Effective Trustworthy Communication Protocol) ขึ้น(โครงสร้างโปรโตคอลนั้นได้แสดงดังรูปที่ 20) โดยโปรโตคอลนี้จะเป็นโปรโตคอลที่เกิดจากการรวมกันของโปรโตคอลที่ใช้สำหรับหาเส้นทางส่งข้อมูล และโปรโตคอลที่ใช้ในการยืนยันตัวตนนั่นเองโดยโปรโตคอลที่ใช้ในการส่งข้อความเราได้เลือกใช้โปรโตคอล DECA-SABI ซึ่งเป็นโปรโตคอลสื่อสารแบบแพร่กระจายที่ได้ถูกนำมาใช้งานบนการสื่อสารแบบ Peer-to-peer บนพื้นที่ภัยพิบัติ และเนื่องจากการยืนยันตัวตนที่ได้นำเสนอนั้นสร้างขึ้นมาเพื่อรองรับผู้ใช้ที่สามารถติดต่อกับเจ้าหน้าที่ได้ และผู้ใช้ที่ไม่สามารถติดต่อกับเจ้าหน้าที่ได้ ซึ่งเป็นการยืนยันตัวตนแบบผสมโดยมีการทำงานแบ่งออกเป็นสองโหมดซึ่งจะกล่าวในหัวข้อต่อๆไป

3.1.2 การเลือกใช้ Routing Protocol

สำหรับ Routing Protocol ที่ได้นำมาใช้งานนั้น ในงานวิจัยนี้เลือก Density-Aware Broadcasting with State Adaptive Beacon Interval Protocol (DECA-SABI) [8] ซึ่งเป็นโปรโตคอลที่ถูกใช้งานบนพื้นที่ภัยพิบัติที่ได้กล่าวถึงในบทที่ 2 ซึ่งโปรโตคอลนี้เป็นโปรโตคอลที่มีการสื่อสารโดยการส่งข้อความแบบแพร่กระจายซึ่งได้ถูกนำมาใช้งานบนการสื่อสารแบบ Peer-to-peer บนพื้นที่ภัยพิบัติ แต่โปรโตคอลนี้ไม่มีความสามารถให้การสื่อสารที่มีความปลอดภัยได้ ดังนั้นโปรโตคอลที่ได้ทำการพัฒนาขึ้นนั้นจำเป็นจะต้องพัฒนาโปรโตคอลนี้ในขั้นต่อไป ในส่วนนี้จะกล่าวถึงรายละเอียดและกลไกการทำงานของโปรโตคอล DECA-SABI โดยสังเขป ซึ่งโปรโตคอล DECA-SABI นั้นมีกลไกที่เกี่ยวข้องดังนี้

Beaconing Mechanism

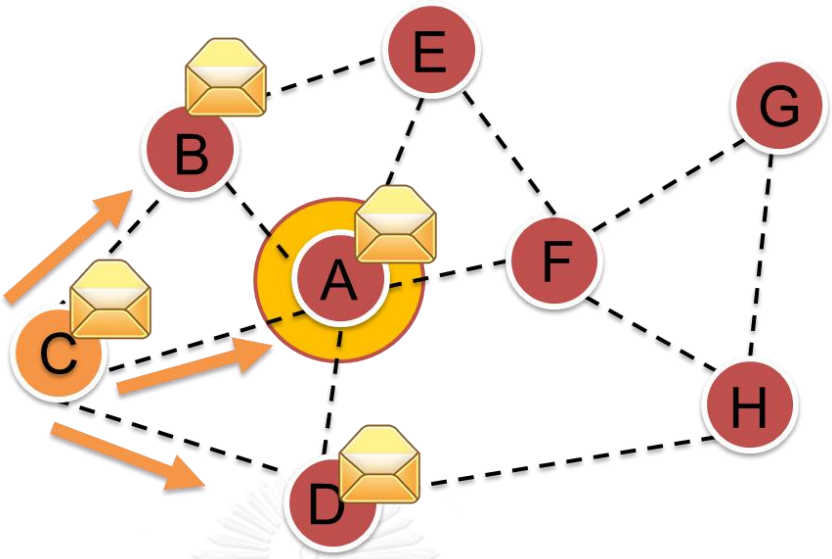


รูปที่ 21 กลไกในการส่ง Beacon

กลไกนี้เป็นกลไกในการส่งสัญญาณเพื่อแลกเปลี่ยนข้อมูลกับอุปกรณ์สื่อสารเพื่อนบ้านบริเวณรอบๆ โดยข้อมูลใน Beacon packet นั้นจะมีรายการของหมายเลข IP ของอุปกรณ์สื่อสารเพื่อนบ้านทั้งหมดอยู่ โดยรายการหมายเลข IP เพื่อนบ้านนั้นจะถูกนำมาคำนวณเพื่อนำข้อมูลเหล่านั้นมาประมวลผลเพื่อใช้ในการส่งข้อความนั่นเอง

การส่ง Beacon packet นั้นจะมีลักษณะในการส่งแบบแพร่กระจายไปรอบๆเป็นระยะโดยมีเพื่อนบ้านแค่ 1 Hop เท่านั้นที่จะรับรู้ ในการส่งสัญญาณ Beacon นั้นโปรโตคอลนี้จะไม่ทำการส่งสัญญาณด้วยความถี่เดิมตลอดเวลาเพื่อที่จะได้ประหยัดพลังงาน ถ้าไม่มีการส่งข้อความเกิดขึ้นนั้นการส่งสัญญาณ Beacon จะถูกส่งด้วยความถี่ 1 ครั้งต่อ 100 วินาที แต่เมื่อมีความต้องการที่จะส่งข้อมูลนั้น โปรโตคอลนี้จะเปลี่ยนสถานะของการส่งสัญญาณ Beacon เป็น 1 ครั้งต่อ 4-15 วินาที นอกจากนี้สัญญาณ Beacon นั้นยังมีรายการของหมายเลขข้อความที่ได้ทำการส่งบรรจุอยู่ ทำให้โปรโตคอลนี้สามารถกู้คืนข้อความที่ขาดหายหรือยังไม่ได้รับได้นั่นเอง

Forwarding Mechanism



รูปที่ 22 กลไกในการส่งข้อความ

เนื่องจากโปรโตคอลนี้เป็นโปรโตคอลการสื่อสารแบบแพร่กระจาย กลไกนี้เป็นกลไกที่ช่วยลดจำนวนครั้งในการกระจายข้อมูล ในการส่งข้อมูลแบบแพร่กระจายนั้นจะทำให้อุปกรณ์สื่อสารโดยรอบรับรู้ข้อมูลพร้อมๆกันซึ่งมีกลไกในการส่งข้อความดังนี้

ในการส่งข้อความแต่ละครั้งนั้นผู้ส่งจะส่งข้อความแบบแพร่กระจายไปยังอุปกรณ์สื่อสารโดยรอบ พร้อมทั้งระบบผู้ที่จะทำการแพร่กระจายต่อด้วย โดยอุปกรณ์สื่อสารที่มีจำนวนเพื่อนบ้านมากที่สุดจะเป็นผู้ทำการแพร่กระจายต่อ แต่ถ้าหากการแพร่กระจายนั้นไม่ได้มีการระบุผู้ที่จะทำการแพร่กระจายต่อ หรือผู้ที่ทำการแพร่กระจายต่อไม่สามารถแพร่กระจายข้อความได้ อุปกรณ์สื่อสารเครื่องอื่นจะทำการนับเวลาถอยหลังอย่างสุ่ม เมื่อการนับเวลาสิ้นสุดลงที่กำหนดอุปกรณ์สื่อสารตัวนั้นจะทำหน้าที่เป็นผู้แพร่กระจายข้อความต่อเอง

3.1.3 *การสร้าง* Authentication Protocol

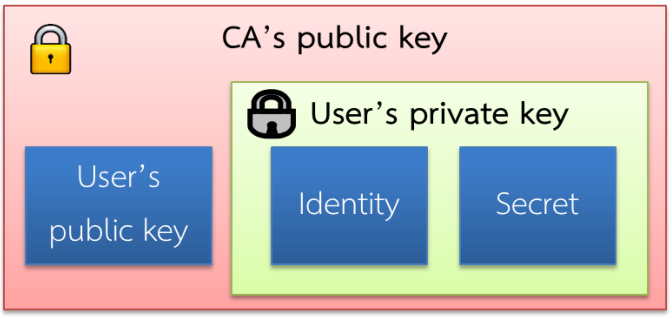
จากที่ได้กล่าวไว้นั้นโปรโตคอลที่ใช้ในการสื่อสารที่ได้ออกแบบมานั้นจะเป็นโปรโตคอลที่ใช้ร่วมกับโปรโตคอลในการยืนยันแบบผสมซึ่งเป็นการยืนยันตัวตนที่ได้นำข้อดีของการยืนยันตัวตนแบบอาศัยเจ้าหน้าที่และการยืนยันตัวตนแบบไม่อาศัยเจ้าหน้าที่ทำให้สามารถรองรับการใช้งานจากผู้ใช้งานได้ครอบคลุมทั้งกลุ่มที่สามารถติดต่อกับเจ้าหน้าที่ได้และกลุ่มที่ไม่สามารถติดต่อกับเจ้าหน้าที่ได้ โดยการทำงานของการยืนยันตัวตนนั้นจะแบ่งออกเป็น 2 โหมดดังนี้

1) การยืนยันตัวตนแบบ Fully Trusted Mode

การยืนยันตัวตนในโหมดนี้เป็นการยืนยันตัวตนโดยผ่านเจ้าหน้าที่ ทำให้ผู้ใช้งานสามารถได้รับความน่าเชื่อถือในระดับที่สูงสุด แต่เนื่องจากเป็นการยืนยันตัวตนผ่านเจ้าหน้าที่ ดังนั้นผู้ที่จะใช้งานการยืนยันตัวตนในโหมดนี้ได้จำเป็นจะต้องได้รับการติดต่อกับเจ้าหน้าที่ก่อน อาจจะเป็นการติดต่อโดยกายภาพ นั่นคือการพบเจอกัน หรือจะเป็นการติดต่อผ่านเครือข่าย นั่นคือการส่งข้อความหากันก็ได้ เมื่อผู้คนในบริเวณภัยพิบัติสามารถติดต่อกับเจ้าหน้าที่ได้แล้วนั้น จะสามารถใช้การยืนยันตัวตนแบบ Fully Trusted Mode ได้ซึ่งเป็นการยืนยันตัวตนโดยใช้ Certificate ในการยืนยันตัวตน การยืนยันตัวตนด้วย Certificate นั้นทำให้ผู้ใช้มีความสะดวกในการใช้งานบนพื้นที่ภัยพิบัติมากกว่าแบบการใช้ Identity ในการยืนยันตัวตน เนื่องจาก Certificate นั้นเมื่อส่งให้ผู้รับปลายทางแล้ว ผู้รับข้อความสามารถนำ Certificate ไปใช้ในการตรวจสอบความน่าเชื่อถือ พร้อมกับถอดรหัสข้อความได้เลยโดยไม่ต้องร้องขอ Public key จากทางเจ้าหน้าที่อีกโดยการทำงานของ Fully Trusted Mode มีดังนี้

การร้องขอ Signed Certificate

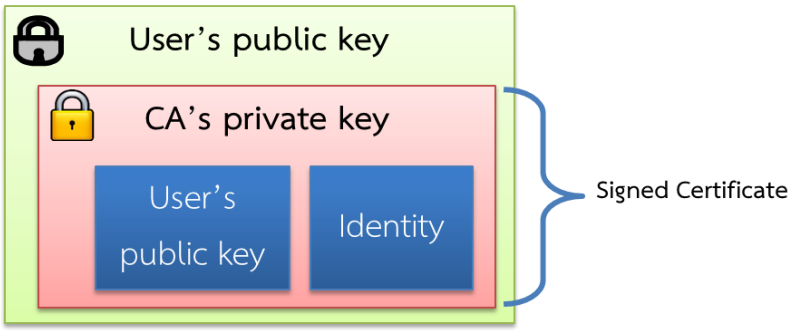
ก่อนที่ผู้ใช้จะสามารถยืนยันตัวตนในแบบ Fully Trusted Mode ได้ ผู้ใช้จำเป็นจะต้องได้รับ Signed Certificate จากเจ้าหน้าที่ก่อนถึงจะสามารถใช้งานได้ โดยขั้นตอนการที่จะได้รับ Signed Certificate จากเจ้าหน้าที่นั้นจะต้องขึ้นกับสมมติฐาน 2 ข้อดังนี้ ข้อแรกคือผู้ใช้จำเป็นจะต้องมีหลักฐานประจำตัวและรหัสลับประจำตัวที่มีความสอดคล้องกันเช่น อีเมลของผู้ใช้ และ พาสเวิด เป็นต้น ข้อสองคือ ผู้ใช้จะต้องทราบรหัส Public key ของเจ้าหน้าที่หรือหน่วยงานที่จะทำการออก Signed Certificate ให้ โดยรหัสนั้นอาจจะถูกบันทึกไว้ตั้งแต่ขั้นตอนการติดตั้งแอปพลิเคชั่นเพื่อใช้งานเลยก็ได้ ก่อนที่จะส่งข้อความร้องขอ Signed Certificate นั้นผู้ใช้จำเป็นจะต้องสร้างคู่รหัสของตนขึ้นมาซึ่งประกอบด้วย Public key และ Private key เพื่อที่จะใช้ในการยืนยันตัวตน



รูปที่ 23 รูปแบบ Request Signed Certificate packet

ในขั้นตอนการร้องขอนั้นผู้ใช้จะทำการสร้าง Request Certificate packet ขึ้นมา ซึ่งประกอบด้วย หลักฐานที่ใช้ยืนยันตัวตนพร้อมพาสเวิด โดยที่หลักฐานที่ใช้ในการยืนยันตัวตนพร้อมพาสเวิดของผู้ใช้นั้นจะถูกเข้ารหัสไว้ด้วย Private key ของผู้ใช้ ซึ่งจะถูกเรียกว่าข้อมูลส่วนตัวของผู้ใช้ จากนั้นจะนำข้อมูลส่วนตัวของผู้ใช้นั้นรวมเข้ากับ Public key ของผู้ใช้และทำการเข้ารหัสข้อความทั้งหมดด้วยรหัส Public key ของเจ้าหน้าที่ ดังนั้นข้อความที่ได้สร้างขึ้นนี้จะมีเพียงเจ้าหน้าที่ที่ทำการออก Certificate ให้เท่านั้นที่จะสามารถเปิดอ่านได้ คนกลางที่เป็นคนส่งต่อข้อมูลจะไม่สามารถเปิดอ่านเนื้อหาข้างในได้ ข้อความ Request Certificate packet นี้จะถูกส่งแบบกระจายผ่านกลไกการส่งของ Protocol DECA-SABI โดยโปรโตคอลจะทำการส่งผ่านเพื่อนบ้านต่อไปเรื่อยๆจนกระทั่งถึงเจ้าหน้าที่

เมื่อเจ้าหน้าที่ได้รับข้อความ Request Certificate packet มานั้นเจ้าหน้าที่จะทำการเปิดอ่านข้อความโดยก่อนการเปิดอ่านนั้นเจ้าหน้าที่จะต้องถอดรหัสข้อความด้วย Private key ของเจ้าหน้าที่ก่อน เจ้าหน้าที่จะสามารถอ่าน Public key ของผู้ใช้ได้ จากนั้นเจ้าหน้าที่จะนำ Public key นี้ไปทำการถอดรหัสข้อความต่อ ทำให้เจ้าหน้าที่สามารถเปิดอ่านข้อความข้างในได้ ซึ่งจะทำให้เจ้าหน้าที่ทราบข้อมูลลับของผู้ใช้ การนำ Public key ของผู้ใช้มาถอดรหัสข้อความนั้นนอกจากจะทำให้เจ้าหน้าที่อ่านข้อมูลส่วนตัวของผู้ใช้ได้ เจ้าหน้าที่ยังสามารถยืนยันได้ว่าผู้ใช้ที่ส่งข้อความมานั้นไม่ได้ทำการปลอมแปลง Public key ของผู้อื่นมา เพราะการถอดรหัสด้วย Public key สำเร็จ หมายความว่าผู้ใช้ที่ได้ทำการส่งข้อความ Request Certificate packet มานั้นจำเป็นจะต้องมี Private key ที่สามารถเข้าคู่กับ Public key ที่แนบมาได้นั่นเอง

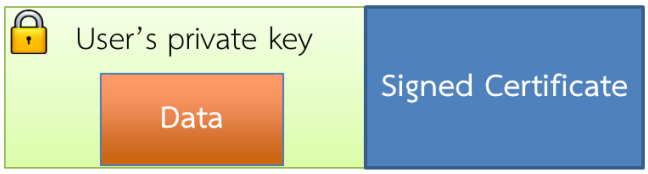


รูปที่ 24 Packet ตอบรับการร้องขอ Certificate จากเจ้าหน้าที่

หลังจากที่เจ้าหน้าที่ได้ทำการอ่านข้อมูลส่วนตัวของผู้ใช้แล้ว เจ้าหน้าที่จะนำของมูลส่วนตัวของผู้ใช้ไปตรวจสอบว่าหลักฐานนั้นมีความน่าเชื่อถือเพียงใด และพาสเวิดที่ผู้ใช้แนบมานั้นมีความถูกต้องและเข้าคู่กับหลักฐานหรือไม่อาจจะเป็นการตรวจสอบความถูกต้องของอีเมลและพาสเวิดว่าสามารถใช้งานได้หรือไม่ เป็นต้น ถ้าหลักฐานและพาสเวิดมีความถูกต้องเจ้าหน้าที่จะทำการออก Signed Certificate ให้โดย Signed Certificate จะประกอบด้วย Public key ของผู้ใช้และหลักฐานประจำตัวผู้ใช้ (อาจจะเป็นอีเมล, เลขประชาชน หรือชื่อจริงพร้อมกับนามสกุลจริงของผู้ใช้ก็ได้) นำมาเข้ารหัสด้วย Private key ของเจ้าหน้าที่ จากนั้นเจ้าหน้าที่จะส่ง Signed Certificate กลับไปให้ผู้ใช้โดยการนำ Signed Certificate เข้ารหัสซ้ำอีกรอบด้วย Public key ของผู้ใช้ที่ทำการร้องขอ Signed Certificate และจากนั้นเจ้าหน้าที่จะส่งข้อความนี้ผ่านไปยังอุปกรณ์สื่อสารเพื่อนบ้านเพื่อให้ทำการส่งต่อไปจนถึงตัวผู้ใช้ที่ได้ทำการร้องขอมานั่นเอง

เมื่อผู้ใช้ได้รับข้อความตอบรับคำร้องขอ Signed Certificate ที่ได้ส่งมาจากเจ้าหน้าที่เรียบร้อยแล้วนั้น ผู้ใช้จะสามารถเปิดอ่าน Signed Certificate ได้โดยการใช้ Private key ของตนเองถอดรหัสข้อความออกมาก็จะได้รับ Signed Certificate ซึ่งสามารถนำไปใช้งานในการยืนยันตัวตนแบบ Fully Trusted Mode ได้ทันที โดยข้อความตอบกลับคำร้องขอนี้จะมีเพียงผู้ใช้ที่ร้องขอมาเท่านั้นที่จะเป็นผู้เปิดอ่านได้เพราะข้อความได้ถูกเข้ารหัสไว้ด้วย Public key ของผู้ใช้ที่ทำการร้องขอ ทำให้คนกลางที่เป็นผู้ส่งต่อข้อมูลไม่สามารถเปิดอ่านข้อความได้

การยืนยันตัวตนแบบ Fully Trusted Mode



รูปที่ 25 การยืนยันตัวตนแบบ Fully Trusted Mode

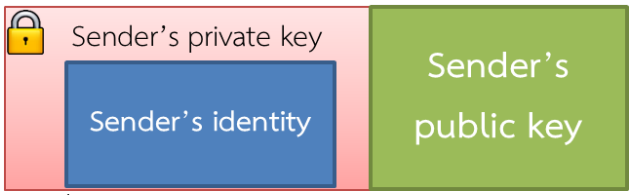
การยืนยันตัวตนแบบ Fully Trusted Mode นั้นสามารถทำได้โดยการนำ Signed Certificate ที่ได้รับมานั้นแนบไปกับ Packet ที่ต้องการจะส่งดังรูปที่ 25 จากนั้นนำข้อความที่ต้องการจะส่งเข้ารหัสด้วย Private key ของผู้ส่งก่อนจะทำการส่งข้อความไปยังเพื่อนบ้าน เมื่อส่งข้อความแล้วนั้นผู้รับข้อความสามารถตรวจสอบความถูกต้องของ Certificate โดยนำเอารหัส Public key ของเจ้าหน้าที่ทำการถอดรหัส Signed Certificate ถ้าสามารถถอดรหัสได้สำเร็จหมายความว่า Signed Certificate นั้นได้รับการยืนยันอย่างถูกต้อง พร้อมทั้งผู้รับข้อความจะสามารถทราบถึง Public key ที่ใช้ในการถอดรหัสเพื่ออ่านข้อความอีกด้วย

2) การยืนยันตัวตนแบบ Half Trusted Mode

การยืนยันตัวตนในโหมดนี้จะเป็นการยืนยันตัวตนโดยไม่ผ่านเจ้าหน้าที่ โหมดนี้มีขึ้นเพื่อรองรับสำหรับบุคคลที่ไม่สามารถติดต่อกับเจ้าหน้าที่ได้ การยืนยันตัวตนในโหมดนี้เป็นการยืนยันตัวตนผ่านการเชื่อใจจากบุคคลที่ได้พบเจอกัน ดังนั้นความน่าเชื่อถือจึงมีไม่เท่ากับการยืนยันตัวตนแบบ Fully Trusted Mode อย่างไรก็ตามการยืนยันตัวตนในโหมดนี้ไม่จำเป็นต้องทำการยืนยันตัวตนผ่านเจ้าหน้าที่ดังนั้นจึงมีความยืดหยุ่นสูง ผู้ใช้ที่ไม่ได้ติดต่อกับเจ้าหน้าที่ก็สามารถยืนยันตัวตนได้ด้วยโหมดนี้นั่นเอง

หลักการของการยืนยันตัวตนในโหมดนี้จะใช้หลักของความเชื่อใจ นั่นคือถ้าผู้ใช้คนไหนได้รับความเชื่อใจมาก ผู้ใช้คนนั้นจะมีความน่าเชื่อถือมากไปด้วย โดยผู้ใช้สามารถประกาศค่าความน่าเชื่อถือของตนเองผ่านทางข้อความที่ใช้ส่งเพื่อสื่อสารกัน และผู้ใช้แต่ละคนจะบันทึกความน่าเชื่อถือของเพื่อนบ้านไว้ด้วยเช่นกันเพื่อนำมาคำนวณระดับความน่าเชื่อถือของข้อมูลที่ได้รับ โดยหลักการการยืนยันตัวตนแบบ Half Trusted Mode มีกระบวนการดังนี้

การสร้าง Certificate เพื่อใช้ในการยืนยันตัวตน

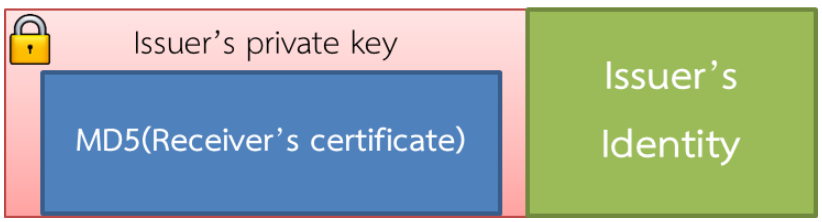


รูปที่ 26 การสร้าง Certificate ของ Half Trusted Mode

ในการยืนยันตัวตนในแบบ Half Trusted Mode นั้นผู้ใช้ยังคงต้องอาศัย Certificate ในการบ่งบอกตัวตน แต่ Certificate ที่ใช้นั้นจะเป็น Unsigned Certificate นั่นคือเป็น Certificate ที่ไม่ได้รับการยืนยันจากเจ้าหน้าที่นั่นเอง แต่ Certificate ที่สร้างขึ้นมานี้จะต้องผูกเข้ากับหลักฐานประจำตัวผู้ใช้เพื่อใช้ยืนยันความถูกต้องของข้อความ ในการผูก Certificate เข้ากับหลักฐานประจำตัวของผู้ส่งข้อความนั้นสามารถทำได้โดยการนำหลักฐานประจำตัวผู้ส่งมาทำการเข้ารหัสด้วย Private key ของผู้ส่ง เมื่อทำการเข้ารหัสเสร็จแล้วจะนำข้อมูลที่ได้มารวมกับ Public key ผู้ส่งดังรูปที่ 26 การสร้าง Certificate จะถือเป็นการเสร็จสิ้นโดย Certificate ที่ได้จะเรียกว่าเป็น Unsigned Certificate ซึ่งเป็น Certificate ที่ได้ไม่รับกับยืนยันจากเจ้าหน้าที่นั่นเอง

การเพิ่มระดับความน่าเชื่อถือ

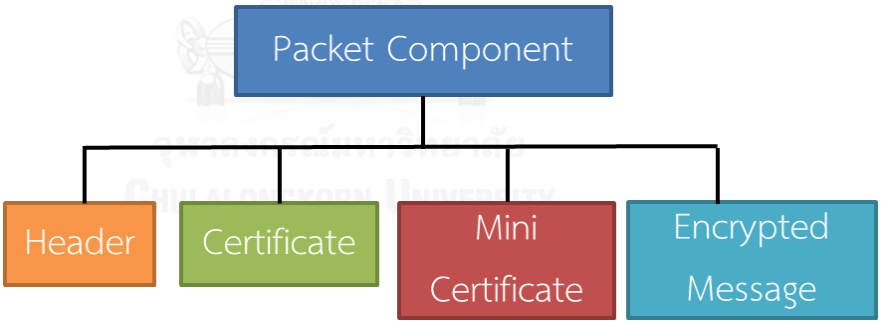
Certificate นั้นเป็นเพียงแค่เครื่องมีที่บ่งบอกความเป็นเจ้าของของข้อความที่ต้องการจะส่ง แต่ไม่ได้บอกความน่าเชื่อถือของข้อความนั้นแต่อย่างใด ดังนั้นจำเป็นจะต้องมีขั้นตอนการเพิ่มความน่าเชื่อถือให้กับข้อความนั้นๆด้วยกระบวนการเพิ่มความน่าเชื่อถือ แต่อย่างไรก็ตามด้วยวิธีการยืนยันตัวตนที่สร้างขึ้นเป็นการยืนยันตัวตนโดยแนบข้อมูลการยืนยันตัวตนผ่านข้อความที่ใช้สื่อสารกัน ดังนั้นจะต้องคำนึงถึงพื้นที่ของ Packet ที่ใช้ในการส่ง เนื่องจาก Packet ที่สื่อสารกันนั้นมีพื้นที่จำกัด งานวิจัยนี้จึงออกแบบ Mini-certificate ขึ้นเพื่อช่วยในการยืนยันตัวตน



รูปที่ 27 โครงสร้าง Mini-certificate

Mini-certificate จะสามารถเพิ่มความน่าเชื่อถือให้กับข้อความได้โดยผู้ที่ต้องการจะยืนยันตัวตนนั้นจะต้องขอ Mini-certificate จากเพื่อนบ้าน เมื่อได้รับ Mini-certificate มาแล้วจะสามารถใช้ในการเพิ่มความน่าเชื่อถือให้กับข้อความที่ส่งได้นั่นเอง โดย Mini-certificate คือการนำ Certificate ของต้องการจะยืนยันตัวตนให้มาเข้า MD5 Hashing ซึ่งจะถูกเรียกว่า User's fingerprint และมาเข้ารหัสอีกทีด้วย Private key ของผู้ที่จะทำการออก Mini-certificate ให้ จากนั้นนำไปรวมกับหลักฐานที่ใช้แสดงตัวของผู้ออก Certificate ให้ ดังรูปที่ 27

การจะได้มาซึ่ง Mini-certificate นั้น ผู้ที่ต้องการจะยืนยันตัวตนจะต้องทำการพบทางกายภาพกับผู้ที่ต้องการจะออก Mini-certificate ให้ นั่นคืออาจจะเป็นการพบเห็นหน้ากันคุยกันต่อหน้า เป็นต้น ซึ่งวิธีนี้จะทำให้การเชื่อใจมีประสิทธิภาพมากยิ่งขึ้น จากนั้นผู้ที่ต้องการจะยืนยันตัวตนจะต้องทำการส่ง Fingerprint ของตนเองไปให้กับผู้ที่จะออก Mini-certificate.ให้ จากนั้นถ้าผู้ที่ทำการออก Certificate ให้นั้นเชื่อใจผู้ใช้คนนั้น ก็จะทำการส่ง Mini-certificate กลับมาให้ยังผู้ใช้ เมื่อผู้ใช้ได้รับ Mini-certificate แล้วนั้นก็จะสามารถนำไปใช้แนบเข้ากับข้อความเพื่อทำการยืนยันตัวตน



รูปที่ 28 องค์ประกอบ Packet

ในการที่จะสร้างข้อความเพื่อส่งไปยังปลายทางนั้น ผู้ส่งจะต้องทำการแนบ Mini-certificate ไปกับข้อความทุกครั้งเพื่อให้ข้อความมีความน่าเชื่อถือ โดย Mini-certificate เปรียบเหมือนบัตรที่ผู้อื่นมอบให้เพื่อแสดงความไว้วางใจ ดังนั้นจึงสามารถแนบ Mini-certificate ไปยังข้อความได้มากกว่า 1 Mini-certificate ต่อ 1 ข้อความ แต่อย่างไรก็ตามจะต้องคำนึงถึงขนาด Packet ที่มีพื้นที่จำกัด ดังนั้นจึงต้องพิจารณาโครงสร้าง Packet

การส่งข้อความ 1 ครั้งนั้นสามารถส่งได้มากสุดด้วย Packet ขนาด 1500 Bytes ซึ่งต้องรายละเอียดตามโครงสร้าง Packet ที่ได้แสดงดังรูปที่ 28 สำหรับโปรโตคอลที่นำมาใช้งานนั้นมีขนาด Header ประมาณ 40 Bytes ขนาดของ Unsigned Certificate นั้นจะขึ้นกับขนาดของหลักฐานประจำตัวผู้ส่งที่ถูกเข้ารหัสด้วย Private key ซึ่งมีขนาด 128 Bytes และขนาดของ Public key ที่ได้แนบไปกับ Certificate ซึ่งมีขนาด 128 Bytes ดังนั้นขนาดของ Unsigned Certificate จึงมีขนาด 256 Bytes บนสมมติฐานว่าผู้ใช้นั้นจะไม่ส่งข้อความเกินกว่า 200 ตัวอักษร และเพื่อความน่าเชื่อถือในการส่งข้อความนั้น ข้อความที่ส่งจะเป็นข้อความที่ถูกเข้ารหัสด้วย Private key ของผู้ส่งทำให้ข้อความนั้นไม่สามารถถูกแก้ไขและส่งต่อจากคนกลางได้ จะสามารถถูกเปิดอ่านได้เพียงอย่างเดียว ดังนั้นขนาดของข้อความจะมีขนาดเพิ่มขึ้น 128 Bytes ซึ่งเป็นขนาดของ Symmetric key ที่ถูกเข้ารหัสด้วย Private key ของผู้ใช้ ดังนั้นนั้นขนาดของข้อความจึงมีขนาดเป็น 328 Bytes และ Mini-certificate จะมีขนาดขึ้นกับขนาดของ User’s fingerprint ที่ถูกเข้ารหัสด้วย Private key ซึ่งมีขนาด 128 Bytesและขนาดของหลักฐานประจำตัวซึ่งในกรณีนี้ใช้เป็นอีเมลซึ่งมีขนาดโดยเฉลี่ยประมาณ 25 Bytes ดังนั้นขนาดของ Mini-certificate จะมีค่าประมาณ 153 Bytes เราสามารถคำนวณหาพื้นที่สำหรับ Mini-certificate ได้ตามสมการดังนี้

$$N = \left\lfloor \frac{MTU - (Head + Msg + Cert)}{MinCertSize} \right\rfloor$$

เมื่อ N แสดงจำนวนของ Mini-certificate ที่สามารถถูกบรรจุลงไปใน Packet ได้, MTU คือขนาดมากที่สุดของ Packet ซึ่งมีค่า 1500 Bytes, Head คือขนาดของ Header ของโปรโตคอลที่ใช้ในการส่งข้อความ Msg คือขนาดของข้อความที่ถูกเข้ารหัส Cert คือขนาดของ Certificate ของผู้ใช้ MinCertSize คือขนาดของ Mini-certificate เมื่อคำนวณแล้วจะพบว่าด้วยโปรโตคอลนี้จะสามารถบรรจุ Mini-certificate ได้ถึง 6 ฉบับต่อหนึ่งข้อความ

การยืนยันตัวตนในแบบ Half Trusted Mode

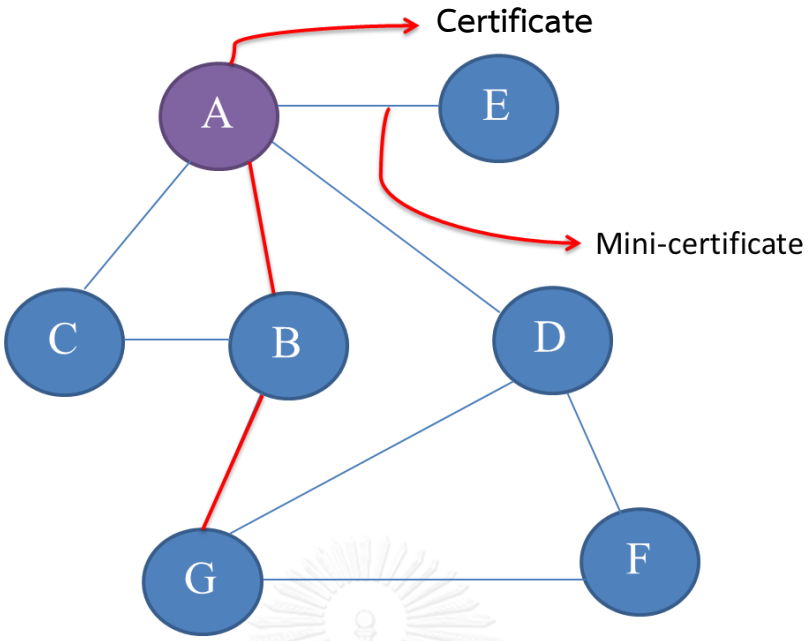
ในการยืนยันตัวตนนั้นผู้ใช้จะแนบ Unsigned Certificate และ Mini-certificate ไปพร้อมกับข้อความที่ทำการส่ง โดย Unsigned Certificate นั้นจะเป็นสิ่งที่ช่วยยืนยันตัวตนของผู้ส่งข้อความ ว่าเป็นคนที่มีอยู่จริง ไม่ใช่ โปรแกรมที่ส่งข้อความหลอกลวงอย่างอัตโนมัติ

และ Mini-certificate นั้นทำหน้าที่เพื่อเพิ่มความน่าเชื่อถือให้กับผู้ส่งข้อความนั่นเอง เมื่อปลายทางได้รับPacket ที่ได้ส่งมาจากต้นทางแล้ว ปลายทางจะเก็บข้อมูล Unsigned Certificate และ Mini-certificate ไปยังตารางเก็บข้อมูลความน่าเชื่อถือเพื่อคำนวณวัดระดับความน่าเชื่อถือของแต่ละบุคคล โดยตารางเก็บข้อมูลความน่าเชื่อถือแสดงดังรูปที่ 29

source	identity	certificate	mini-certificate	trust level
10.0.0.1	john@mail.com	john's cert	-	1
10.0.0.2	tom@mail.com	tom's cert	A, B, C	2
10.0.0.3	jame@mail.com	jame's cert	C, D, E, F	2

รูปที่ 29 ตารางความน่าเชื่อถือ

ความน่าเชื่อถือจะถูกแบ่งออกเป็น 3 ระดับดังนี้ ระดับแรกสำหรับผู้ที่มี Certificate ที่ถูกต้องแนบมากับข้อมูล นั่นคือสามารถนำ Public key ที่ได้รับมาใน Certificate ถอดรหัสข้อความได้อย่างถูกต้อง ความน่าเชื่อถือระดับนี้ถือว่าเป็นความน่าเชื่อถือระดับที่ต่ำที่สุด เนื่องจากเราจะทราบแค่ว่าผู้ส่งมีหลักฐานประจำตัวเป็นอย่างไร ซึ่งอาจจะเกิดจากการปลอมแปลงหลักฐานประจำตัวขึ้นก็เป็นได้ แต่บุคคลที่มีหลักฐานประจำตัวประกอบกับการส่งข้อมูลก็ยังมีความน่าเชื่อถือกว่าบุคคลที่ไม่มีหลักฐานประจำตัวบ่งบอกในการส่งข้อความ ความน่าเชื่อถือระดับที่สองคือผู้ใช้ที่มี Mini-certificate แนบมากับข้อความ ซึ่ง Mini-certificate นั้นจะเป็นสิ่งที่เพิ่มความน่าเชื่อถือให้กับบุคคล ดังนั้นเมื่อผู้ส่งมี Mini-certificate แนบมาด้วยนั่นหมายความน่าผู้ส่งนั้นเคยมีคนที่เชื่อถือผู้ส่งมาแล้ว ความน่าเชื่อถือของผู้ส่งจึงมีมากขึ้น แต่อย่างไรก็ตามเราผู้รับไม่มีทางทราบได้ว่าใครเป็นผู้ที่เชื่อใจผู้ส่งจนกว่าเราจะได้รับ Certificate ของบุคคลที่เชื่อใจผู้ส่งข้อความ การที่จะได้รับความน่าเชื่อถือในระดับที่ 2 ได้นั้นจึงจะต้องประกอบด้วยข้อมูล 2 สิ่งนั่นคือ Mini-certificate ที่แนบมากับข้อความ และ Certificate ของผู้ที่ออก Mini-certificate ให้นั่นเอง ด้วย Certificate ของผู้ที่ออก Mini-certificate ให้นั้นจะทำให้เราทราบได้ว่า Mini-certificate นั้นถูกต้องหรือไม่

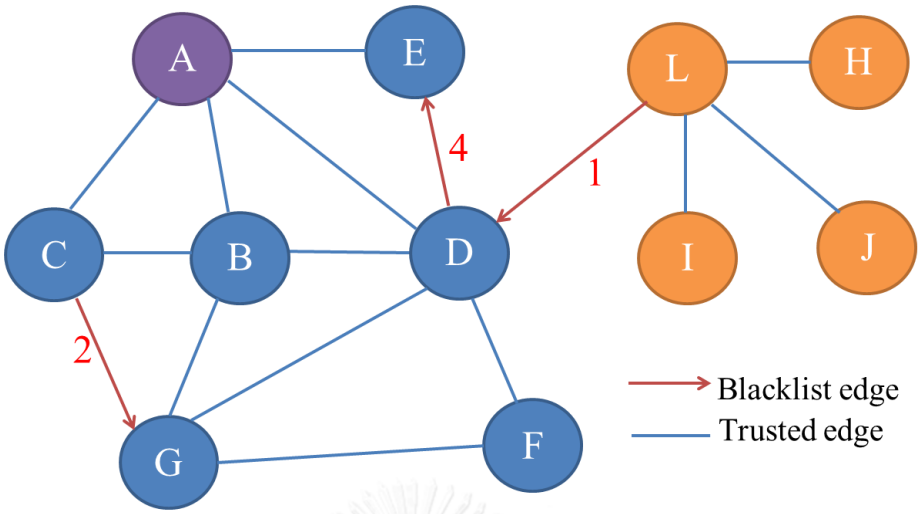


รูปที่ 30 กราฟการยืนยันตัวตน

ในการที่เราจะเชื่อถือข้อความที่ได้รับมากขึ้นนั้น ระบบจะสร้างกราฟความน่าเชื่อถือขึ้นมา โดยการคำนวณความน่าเชื่อถือจากกราฟความน่าเชื่อถือนั้นจะใช้หลักการของการถ่ายถอดความน่าเชื่อถือ นั่นคือถ้าเราเชื่อใจผู้ใช้คนใด และถ้าผู้ใช้คนนั้นเชื่อใจผู้อื่นต่อเท่ากับว่าเราจะเชื่อใจบุคคลนั้นได้ด้วย กราฟความน่าเชื่อถือได้แสดงดังรูปที่ 30 โดยจุดยอดบนกราฟแสดงถึง Certificate ของผู้ใช้และเพื่อนบ้าน เส้นบนกราฟ (Trusted edge) แสดง Mini-certificate ของผู้ใช้ การที่จะมีเส้นบนกราฟ (A, B) ก็ต่อเมื่อ A เชื่อใจ B หรือ B เชื่อใจ A จากคุณสมบัติของการถ่ายถอดความน่าเชื่อถือนั้นจะได้ว่าบุคคลผู้ที่มีความน่าเชื่อถือคือผู้ที่มีเส้นทางมาถึงโหนดตนเอง โดยจากรูปนั้นเป็นกราฟความน่าเชื่อถือของโหนด A ซึ่งเป็นโหนดของเจ้าของกราฟ โหนด G มีเส้นทางมายังโหนด A จึงได้ว่า โหนด G นั้นเป็นผู้ที่มีความน่าเชื่อถือสำหรับ A

การลดระดับความน่าเชื่อถือของผู้ที่ไม่น่าเชื่อถือ (Blacklisting Function)

เพื่อป้องกันการสร้างหลักฐานปลอม ระบบการสื่อสารนี้ยังยินยอมให้ผู้ใช้ช่วยกันตรวจสอบความน่าเชื่อถือของผู้ใช้อื่นได้อีกด้วย ผู้ใช้สามารถทำการลดความน่าเชื่อถือของผู้อื่นด้วยการทำ Blacklisting เมื่อผู้ใช้ได้รับข้อความที่ไม่น่าเชื่อถือ ผู้ใช้สามารถส่งต่อข้อความนั้นในรูปแบบของ Blacklist message ประกอบด้วย ข้อความที่ไม่น่าเชื่อถือ Certificate ของผู้ใช้ และ Certificate ของผู้ที่ไม่น่าเชื่อถือ เมื่อปลายทางได้รับ Blacklist message แล้ว ผู้ที่ได้รับจะทำการสร้างเส้น Blacklist edge ขึ้นบนกราฟแสดงดังรูปที่ 31



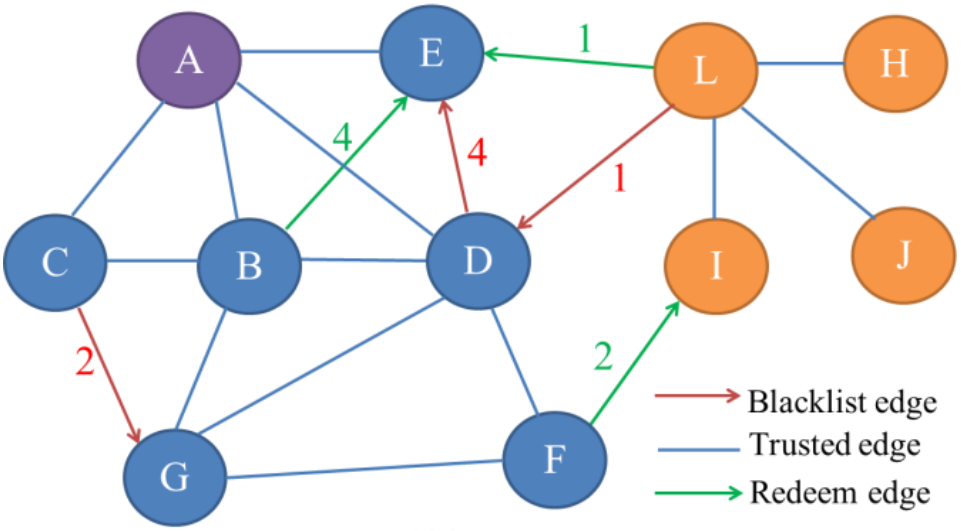
รูปที่ 31 การสร้าง Blacklist edge บนกราฟความน่าเชื่อถือ

บนสมมติฐานว่าความน่าเชื่อถือของข้อมูลแปรผันตามความน่าเชื่อถือของผู้ส่งข้อมูล ดังนั้น Blacklist edge จะมีน้ำหนักแสดงความน่าเชื่อถือด้วยโดยน้ำหนักของ Blacklist edge จะมีค่าเท่ากับน้ำหนักความน่าเชื่อถือของโหนดนั้น โหนดที่ขาดความน่าเชื่อถือคือโหนดที่มีผลรวมของน้ำหนักความน่าเชื่อถือน้อยกว่าผลรวมของน้ำหนัก Blacklist edge

จากรูปโหนด D มีน้ำหนักความน่าเชื่อถือ 4 ดังนั้นเมื่อ D ทำการ Blacklist E น้ำหนักของเส้น Blacklist จึงมีค่าเท่ากับ 4 ด้วย สำหรับโหนด L ซึ่งไม่ได้รับความเชื่อถือผ่าน Trusted edge ทำให้มีน้ำหนักของ Blacklist edge แค่ 1 สำหรับโหนด E ที่มีผลรวมของน้ำหนักของเส้นความน่าเชื่อถือน้อยกว่าผมรวมของน้ำหนัก Blacklist edge จะเป็นโหนดที่ไม่น่าเชื่อถือ ในทางกลับกันโหนด G ซึ่งเป็นโหนดที่มีผลรวมของน้ำหนักความน่าเชื่อถือมากกว่าผลรวมของน้ำหนัก Blacklist edge จะเป็นโหนดที่มีความน่าเชื่อถืออยู่

การกู้คืนระดับความน่าเชื่อถือของตนเอง (Redeeming Function)

ผู้ที่ไม่มีความน่าเชื่อถือสามารถได้รับความน่าเชื่อถืออีกครั้งโดย Redeeming เมื่อผู้ใช้ให้ข้อมูลที่มีประโยชน์ต่อเพื่อนบ้าน เพื่อนบ้านสามารถเลื่อนระดับความน่าเชื่อถือให้กับบุคคลนั้นโดยการส่งต่อข้อความแบบ Redeem message ซึ่งประกอบด้วยข้อความที่น่าเชื่อถือ Certificate ของผู้ส่งข้อความ และ Certificate ของผู้ส่งต่อ เมื่อปลายทางได้รับ Redeem message จะบันทึกข้อมูลไปยังกราฟความน่าเชื่อถือของตนเองในรูปแบบของ Redeem edge ดังที่แสดงในรูปที่ 32



รูปที่ 32 กราฟความน่าเชื่อถือแบบสมบูรณ์

บนสมมติฐานเดิมที่ได้กล่าวไว้ว่าความน่าเชื่อถือของข้อความแปรผันตรงกับความน่าเชื่อถือของผู้ส่ง ดังนั้น Redeem edge จึงมีน้ำหนักของความน่าเชื่อถือด้วย ซึ่งน้ำหนักของเส้น Redeem edge ขึ้นกับน้ำหนักความน่าเชื่อถือของโหนดผู้ส่ง โหนดที่มีความน่าเชื่อถือคือโหนดที่มีผลรวมกับเส้นความน่าเชื่อถือรวมกับผลรวมของน้ำหนัก Redeem edge มากกว่าผลรวมของ Blacklist edge

จากรูปกราฟความน่าเชื่อถือในรูปที่ 32 โหนด E จะได้รับความน่าเชื่อถืออีกครั้งเมื่อโหนด B ทำการกู้คืนความน่าเชื่อถือให้กับโหนด E สำหรับโหนด L ซึ่งไม่ได้รับความน่าเชื่อถือผ่านเส้นทางบนกราฟจะมีน้ำหนักของ Redeem edge เพียงแค่ 1 สำหรับโหนด I ซึ่งได้รับการ Redeeming จากโหนด F ทำให้โหนด I เป็นโหนดที่มีความน่าเชื่อถือระดับ 3 และผลพลอยได้คือทำให้โหนดที่ I เชื่อถือได้รับความน่าเชื่อถือในระดับ 3 ทั้งหมด แต่ทั้งนี้โหนด L ได้รับความน่าเชื่อถือระดับ 3 แต่ไม่ได้รับความน่าเชื่อถือผ่าน Trusted edge ทำให้โหนด L ยังมีน้ำหนักของ Blacklist edge และ Redeem edge เพียงแค่ 1 เท่านั้น

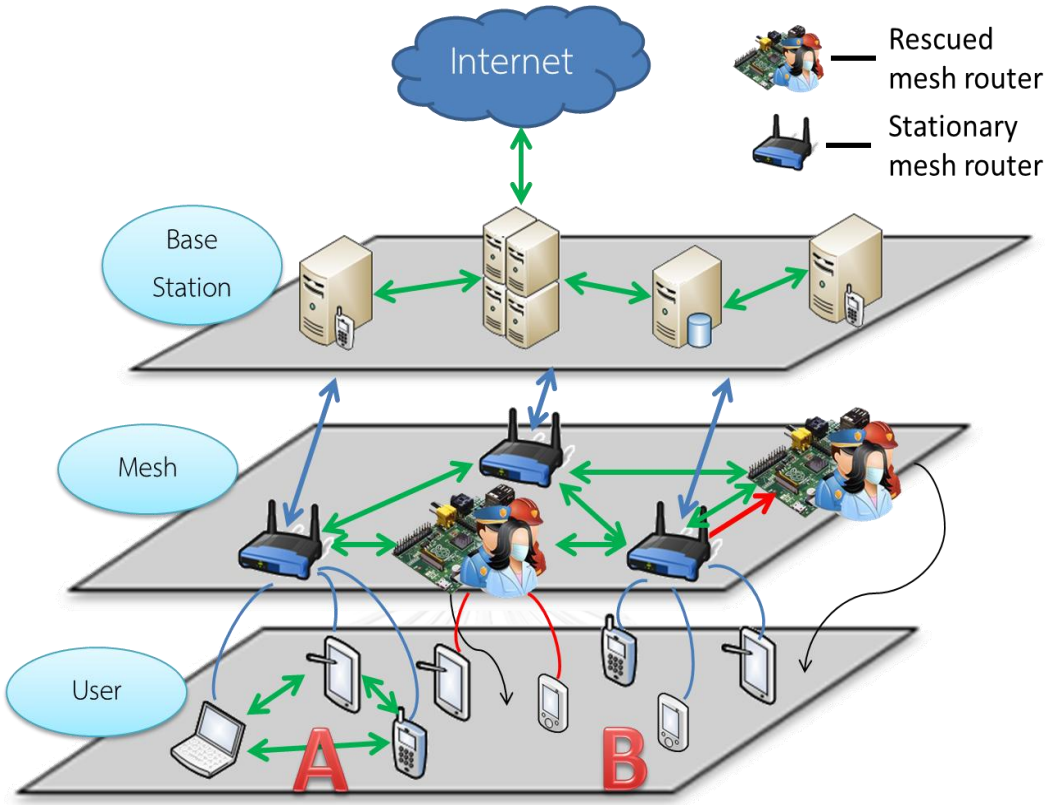
3.2 การออกแบบเครือข่ายโครงสร้างพื้นฐานแบบผสมสำหรับการสื่อสารบนพื้นที่ภัยพิบัติ

จากระบบที่ได้ทำการออกแบบมาในหัวข้อ 3.1 นั้นเป็นระบบที่รองรับการสื่อสารแบบ Peer-to-peer โดยอาศัยเครือข่ายแอดฮอกบนพื้นที่ภัยพิบัติซึ่งเมื่อนำมาพิจารณาดูแล้วพบว่าระบบสื่อสารได้ที่สร้างขึ้นมานั้นเป็นเพียงแค่ส่วนประกอบเดียวบนเครือข่ายการสื่อสาร เนื่องจากว่าอุปกรณ์สื่อสารประเภท Smart phone ในปัจจุบันนี้มีเพียงไม่กี่รุ่นที่ยังรองรับการสื่อสารบนเครือข่ายแอดฮอก ทำให้ระบบสื่อสารตามหัวข้อ 3.1 นั้นเป็นเพียงแค่ส่วนประกอบที่จะเติมเต็มระบบสื่อสารเท่านั้น ดังนั้นทำให้งานวิจัยนี้จึงจะต้องออกแบบระบบการสื่อสารเพิ่มเติมเพื่อให้รองรับอุปกรณ์สื่อสารที่หลากหลายได้อย่างเหมาะสม

ในการบนพื้นที่ภัยพิบัตินั้นจำเป็นต้องรองรับได้กับอุปกรณ์สื่อสารที่สามารถหาซื้อได้ทั่วไป เราได้แบ่งอุปกรณ์สื่อสารของผู้ประสบภัยออกเป็นสองกลุ่มดังนี้ กลุ่มแรกเป็นกลุ่มที่สามารถใช้งานเครือข่ายแอดฮอกได้ กลุ่มนี้สามารถใช้งานการสื่อสารแบบ Peer-to-peer โดยอาศัยเครือข่ายแอดฮอกเพื่อสื่อสารกับผู้ช่วยเหลือในพื้นที่ภัยพิบัติได้โดยใช้ระบบสื่อสารที่ได้กล่าวไว้ในหัวข้อ 3.1 ซึ่งทำให้ผู้ใช้กลุ่มนี้สามารถสื่อสารกันได้อย่างรวดเร็วและมีความน่าเชื่อถือ กลุ่มที่สองไม่สามารถใช้งานการสื่อสารแบบ Peer-to-peer โดยอาศัยเครือข่ายแอดฮอกได้ ดังนั้นการที่จะทำให้อุปกรณ์สื่อสารของผู้ใช้กลุ่มนี้สามารถติดต่อกับเจ้าหน้าที่เพื่อขอความช่วยเหลือ หรือแจ้งเหตุต่างๆได้ ทำให้จำเป็นต้องใช้โครงสร้างพื้นฐานเพื่อช่วยในการสื่อสาร

แต่อย่างไรก็ตามระบบสื่อสารที่เกิดจากการใช้งานผ่านโครงสร้างพื้นฐานโดยปกติ นั้นไม่สามารถให้การสื่อสารที่เหมาะสมบนพื้นที่ภัยพิบัติได้ เนื่องจากว่าโครงสร้างพื้นฐานโดยปกตินั้นไม่สามารถเคลื่อนที่ได้ ทำให้ผู้ใช้จำเป็นจะต้องเคลื่อนที่เข้าหาบริเวณที่มีการติดตั้งโครงสร้างพื้นฐานจึงจะสามารถทำการสื่อสารได้ ระบบการใช้งานการสื่อสารแบบติดตั้งโครงสร้างพื้นฐานนั้นจึงมีความยืดหยุ่นต่ำ ในบางสถานการณ์ผู้ใช้งานหรือผู้ประสบภัยนั้นไม่สามารถเคลื่อนย้ายตัวเองเข้ามายังบริเวณที่มีการติดตั้งโครงสร้างพื้นฐานได้ ทำให้ผู้ใช้ไม่มีความสะดวกและไม่สามารถใช้งานการสื่อสารได้ ด้วยเหตุนี้งานวิจัยนี้จึงต้องออกแบบระบบสื่อสารที่มีความเหมาะสมในการใช้งานบนพื้นที่ภัยพิบัติให้กับผู้ใช้

3.2.1 โครงสร้างระบบ



รูปที่ 33 โครงสร้างระบบสื่อสาร

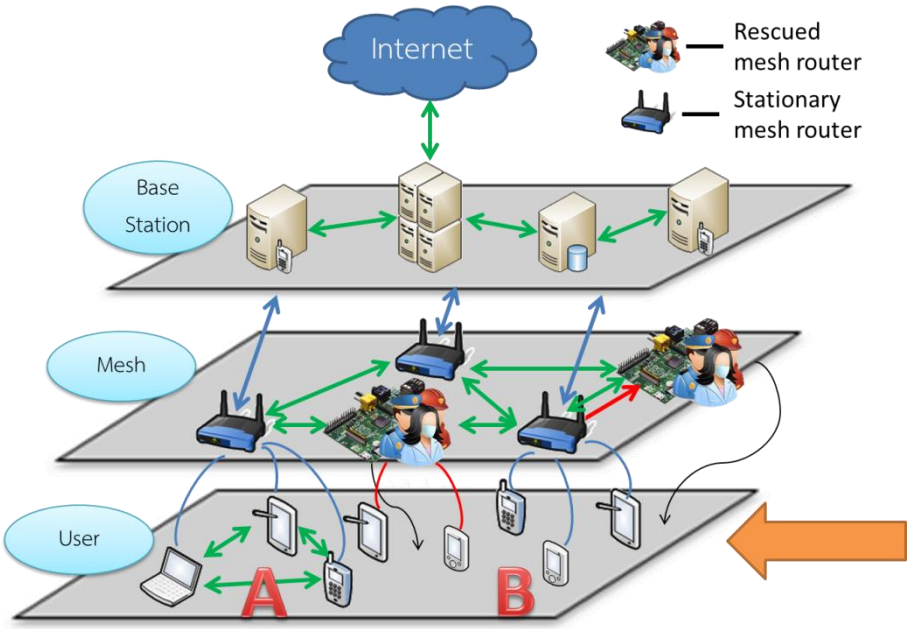
เนื่องจากโครงสร้างพื้นฐานโดยปกติไม่สามารถให้การเชื่อมต่อที่มีความยืดหยุ่นได้ ทำให้มีผู้ใช้งานบางกลุ่มไม่สามารถได้รับการเชื่อมต่อการสื่อสารได้อย่างทั่วถึง เราได้นำเอาเทคโนโลยีประเภท Smart board หรือ คอมพิวเตอร์ขนาดเล็กมาทำการพัฒนาเป็นส่วนหนึ่งของโครงสร้างพื้นฐานเพื่อเพิ่มความยืดหยุ่นให้กับระบบสื่อสาร ทำให้ผู้ใช้งานสามารถเข้าถึงระบบสื่อสารได้มากขึ้น ดังนั้นระบบสื่อสารที่ออกแบบมาจึงเป็นระบบที่นำลักษณะของระบบสื่อสารแบบระบบสื่อสารแบบการใช้โครงสร้างพื้นฐาน มารวมเข้ากับระบบที่มีการสื่อสารแบบ Peer-to-peer ทำให้การสื่อสารนั้นได้รับข้อดีของระบบสื่อสารทั้งสองแบบ นั่นคือระบบสื่อสารนั้นจะมีคุณลักษณะที่มีความยืดหยุ่นในการสื่อสารแบบระบบสื่อสาร Peer-to-peer อีกทั้งระบบสื่อสารนี้ยังสามารถให้การสื่อสารที่เสถียร ดังเช่นคุณลักษณะของระบบสื่อสารแบบติดตั้งโครงสร้างพื้นฐานอีกด้วย ผู้ใช้งานจึงสามารถได้รับการสื่อสารที่มีความยืดหยุ่น และมีความเสถียรในการสื่อสาร

ระบบสื่อสารนี้ออกแบบมาถูกออกแบบมาทำให้ผู้ใช้งานอุปกรณ์สื่อสารสามารถติดต่อสื่อสารกับเจ้าหน้าที่กู้ภัยบนพื้นที่ภัยพิบัติได้ ผู้ใช้สามารถสื่อสารส่งข้อความไปยังศูนย์กู้ภัยที่อยู่ไกลออกไปผ่านทางโครงสร้างพื้นฐานทำให้ข้อความสามารถส่งผ่านไปยังเจ้าหน้าที่ได้ จากนั้นเจ้าหน้าที่ที่ศูนย์กู้ภัยจะทำการส่งเจ้าหน้าที่เข้าไปปฏิบัติงานบนตำแหน่งที่ได้รับข้อความมานั่นเอง การที่ออกแบบ

ระบบสื่อสารให้ผู้ใช้สามารถสื่อสารกับเจ้าหน้าที่ได้เท่านั้นทำให้ไม่มีปัญหาด้านความน่าเชื่อถือของระบบสื่อสาร เพื่อความน่าเชื่อถือในการสื่อสาร ระบบสื่อสารนี้ไม่อนุญาตให้ผู้ใช้งานส่งข้อความถึงกันผ่านโครงสร้างพื้นฐาน (ผู้ใช้งานจะส่งข้อความถึงกันผ่านระบบสื่อสารแบบ Peer-to-peer ที่ได้กล่าวไว้ดังหัวข้อ 3.1 เท่านั้น) ดังนั้นผู้ใช้จึงไม่สามารถสื่อสารกับเพื่อนบ้านบริเวณรอบๆได้ ทำให้การใช้งานการสื่อสารผ่านโครงสร้างพื้นฐานนั้นจะเป็นช่องทางการสื่อสารระหว่างผู้ใช้งานกับเจ้าหน้าที่โดยตรง บนสมมติฐานว่าเจ้าหน้าที่ที่ให้การช่วยเหลือนั้นมีความน่าเชื่อถือทำให้ผู้ใช้งานการสื่อสารผ่านโครงสร้างพื้นฐานนั้นไม่จำเป็นจะต้องคำนึงถึงระดับความน่าเชื่อถือของข้อความ เนื่องจากว่าผู้ใช้งานจะมั่นใจได้ว่าข้อความที่ได้รับมานั้นเป็นข้อความจากเจ้าหน้าที่โดยตรง ไม่ได้ผ่านคนกลางที่รับข้อมูลก่อนหน้าดังเช่นการสื่อสารแบบ Peer-to-peer ระบบสื่อสารนี้จึงเป็นระบบสื่อสารที่สามารถให้ความยืดหยุ่นกับผู้ใช้งานบนพื้นที่ภัยพิบัติและให้การสื่อสารที่มีประสิทธิภาพมีความเสถียรในการสื่อสาร อีกทั้งยังสามารถให้ความน่าเชื่อถือการสื่อสารอีกด้วย

ระบบสื่อสารที่ได้กล่าวมานั้นมีการออกแบบเป็นระบบสื่อสาร 3 ชั้นลักษณะดังรูปที่ 33 ซึ่งประกอบด้วยชั้นล่างสุด คือชั้นของผู้ใช้งาน ชั้นกลางคือชั้นของโครงสร้างพื้นฐานที่เป็นตัวกลางในการส่งข้อมูลจากชั้นผู้ใช้งานไปยังเจ้าหน้าที่ และสุดท้ายจะเป็นชั้นของสถานีรับข้อมูล หรือศูนย์กู้ภัยนั่นเอง โดยชั้นนี้จะทำการรับข้อมูลจากชั้นผู้ใช้มาทำการประมวลผล และอาจจะส่งต่อไปยังเครือข่าย Internet โดยรายละเอียดการทำงานของแต่ละชั้นจะกล่าวในหัวข้อต่อไป

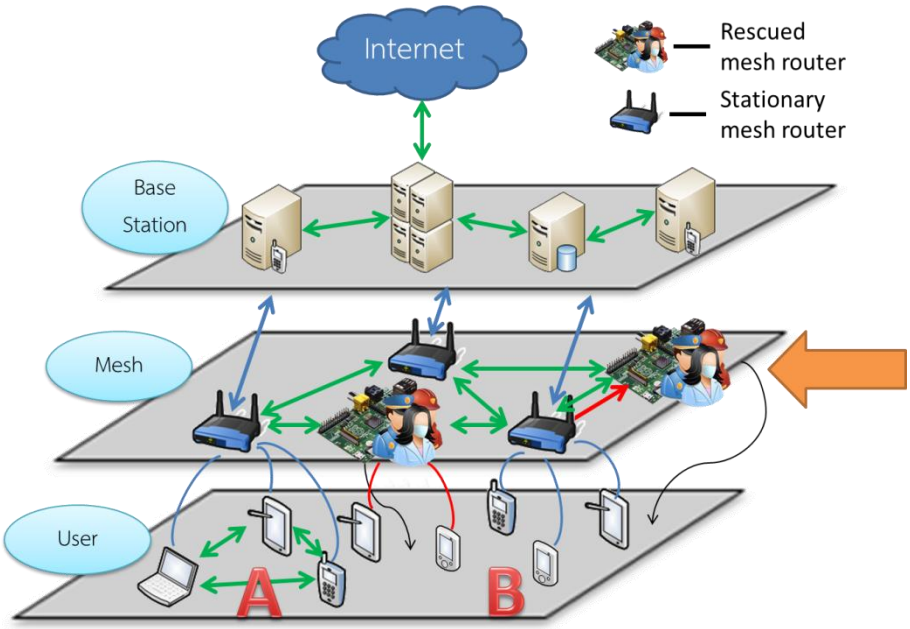
ระดับชั้นผู้ใช้งาน (User Layer)



รูปที่ 34 โครงสร้างระดับชั้นผู้ใช้งาน

ผู้ใช้งานในกรณีนี้จะหมายถึงผู้ใช้งานอุปกรณ์สื่อสามารถเชื่อมต่อเข้ากับ Access point ได้ซึ่งมีอยู่หลายประเภทด้วยกันอาจจะเป็นอุปกรณ์สื่อสารขนาดเล็กอย่างเช่น Smart phone ที่ใช้กันอยู่ในปัจจุบัน อุปกรณ์สื่อสารขนาดกลางอย่างเช่น Tablet ก็สามารถเชื่อมต่อการสื่อสารเข้ากับ Access point ได้เช่นกัน หรืออาจจะเป็นอุปกรณ์สื่อสารขนาดใหญ่ที่พกพาได้อย่างเช่น Laptop เป็นต้น อุปกรณ์เหล่านี้นั้นล้วนแล้วสามารถพกพาได้และนำไปเชื่อมต่อการสื่อสารเข้ากับเครือข่ายบนพื้นที่ภัยพิบัติได้ทั้งสิ้น เมื่อเชื่อมต่อเข้ากับเครือข่ายแล้ว ผู้ใช้สามารถสื่อสารผ่านไปยังเจ้าหน้าที่โดยการเปิดใช้งานแอพพลิเคชั่นที่มีการติดตั้งไว้ที่เครื่องก่อนหน้าที่จะเกิดเหตุภัยพิบัติได้ จากรูปที่ 34 นั้นผู้ใช้งานจะถูกแบ่งออกเป็น 2 กลุ่มด้วยกัน กลุ่มแรกจะเป็นกลุ่มที่สามารถเชื่อมต่อเครือข่ายการสื่อสารแบบ Peer-to-peer ผ่านทางเครือข่ายแอดฮอกได้ ผู้ใช้ในกลุ่มนี้นั้นสามารถใช้ระบบสื่อสารได้สองทางด้วยกัน ทางแรกนั้นผู้ใช้สามารถเชื่อมต่อเข้ากับเครือข่าย Peer-to-peer เพื่อสื่อสารผ่านไปยังเจ้าหน้าที่ หรือผู้ใช้ในบริเวณโดยผ่านโปรโตคอลที่ได้กล่าวไว้ดังหัวข้อ 3.1 และการสื่อสารอีกหนทางคือผู้ใช้ในกลุ่มแรกนี้สามารถทำการเชื่อมต่ออุปกรณ์สื่อสารของตนเองเข้ากับเครือข่ายโครงสร้างพื้นฐานที่ได้ทำการติดตั้งบนพื้นที่ภัยพิบัติอีกด้วย ผู้ใช้กลุ่มที่สองคือผู้ใช้ที่มีอุปกรณ์สื่อสารที่ได้ไม่ได้รองรับการสื่อสารแบบ Peer-to-peer ผ่านเครือข่ายแอดฮอก ดังนั้นผู้ใช้ในกลุ่มนี้จะสามารถเชื่อมต่อการสื่อสารผ่านระบบเครือข่ายโครงสร้างพื้นฐานที่ได้ทำการติดตั้งบนพื้นที่ภัยพิบัติเท่านั้น

ระดับชั้นตัวกลางส่งข้อมูล (Mesh Layer)



รูปที่ 35โครงสร้างระดับชั้นตัวกลางส่งข้อมูล

โครงสร้างในชั้นนี้ประกอบด้วยหน่วยตัวกลางโครงสร้างพื้นฐานพวกเราท์เตอร์ที่ใช้ทำหน้าที่ในการส่งต่อข้อมูลจากชั้นผู้ใช้ไปยังเจ้าหน้าที่ โครงสร้างชั้นนี้เป็นโครงสร้างชั้นที่สำคัญที่สุดในการสร้างระบบสื่อสารแบบผสมระหว่างการสื่อสารแบบ Peer-to-peer และการสื่อสารแบบใช้โครงสร้างพื้นฐานโดยทั่วไป การเลือกใช้เราท์เตอร์ในโครงสร้างชั้นนี้นั้นจะเป็นเราท์เตอร์ที่ได้มีการปรับปรุงให้สามารถใช้งานเข้ากับสถานการณ์ภัยพิบัติได้ และอีกทั้งเราเตอร์ที่ใช้งานจะไม่มีการต่อเข้ากับแหล่งพลังงานบนพื้นที่ประสบภัย แต่จะใช้พลังงานจากแหล่งพลังงานภายนอกแทน ดังนั้นเราท์เตอร์จึงสามารถทำงานบนพื้นที่ภัยพิบัติได้โดยไม่ต้องพึ่งพิงทรัพยากรพลังงานบนพื้นที่ภัยพิบัติ

เราท์เตอร์จะถูกติดตั้งโดยเจ้าหน้าที่ที่เข้ามาช่วยเหลือบนพื้นที่ประสบภัยพิบัตินั่นเอง เราท์เตอร์ที่ทำงานบนชั้นตัวกลางโครงสร้างพื้นฐานประกอบด้วยเราท์เตอร์สองประเภทด้วยกันซึ่งประกอบด้วย Stationary mesh router ซึ่งทำหน้าที่เป็นตัวกลางในการส่งข้อมูลระหว่างผู้ช่วยเหลือและผู้ประสบภัยตามปกติ และ Rescued mesh router ที่เป็นเราท์เตอร์พิเศษติดไว้กับผู้ช่วยเหลือทำให้สามารถเคลื่อนที่ไปพร้อมกับผู้ช่วยเหลือขณะปฏิบัติงานได้ ซึ่งมีรายละเอียดของเราท์เตอร์ทั้งสองประเภทดังนี้

Stationary mesh router

เราท์เตอร์ประเภทนี้จะเป็นเราท์เตอร์ที่ทำหน้าที่เป็นโครงสร้างพื้นฐานที่ถูกติดตั้งอยู่กับที่ ไม่สามารถเคลื่อนย้ายขณะปฏิบัติงานได้ มีหน้าที่ในการให้การเชื่อมต่อการสื่อสารกับ

ผู้ใช้งานการสื่อสารบนพื้นที่ภัยพิบัติ เมื่อผู้ใช้งานเชื่อมต่อการสื่อสารเข้ากับเครือข่ายการสื่อสารของเราท์เตอร์ประเภทนี้แล้ว ผู้ใช้งานสามารถส่งข้อมูลไปยังเจ้าหน้าที่โดยผ่านเราท์เตอร์ได้ โดยเราท์เตอร์จะทำการส่งต่อข้อมูลไปยังชั้นสถานที่รับข้อมูลและส่งต่อไปยัง Rescued mesh router อีกด้วย บนสมมติฐานว่าผู้ช่วยเหลือที่อยู่ใกล้นั้นจะสามารถให้ความช่วยเหลือได้รวดเร็วมากกว่าผู้ช่วยเหลือที่อยู่ห่างไกล ดังนั้น Stationary mesh router นั้นจะส่งต่อข้อมูลไปยัง Rescued mesh router ที่ใกล้ที่สุดโดยกลไกในการส่งต่อข้อมูลนั้นจะกล่าวในหัวข้อต่อไป

Stationary mesh router นั้นจะประกอบด้วย Interface หลัก 2 Interfaces โดยที่ Interface แรกจะเป็น Interface ที่ทำหน้าที่ในการปล่อยสัญญาณ Access point เพื่อสร้างเครือข่ายการสื่อสารบนพื้นที่ภัยพิบัติ และ Interface ที่สองจะเป็น Interface ที่ใช้ในการเชื่อมต่อกันระหว่างเราท์เตอร์ หลังจากที่เจ้าหน้าที่ทำการติดตั้ง Stationary mesh router แล้วนั้น เราท์เตอร์จะทำการสร้างเครือข่ายแอดฮอกขึ้นมาเพื่อเชื่อมต่อกันระหว่างเราท์เตอร์ โดยเครือข่ายแอดฮอกนั้นจะเป็นเครือข่ายที่แตกต่างกับเครือข่ายแอดฮอกที่ใช้สื่อสาร Peer-to-peer บนอุปกรณ์สื่อสารของผู้ใช้ เครือข่ายที่ใช้จะเป็นเครือข่ายแอดฮอกของเราท์เตอร์ด้วยกันเองและมีการตั้งค่าพาสเวิดของเครือข่ายโดยใช้รหัส WPA/WPA2 ไว้เพื่อป้องกันผู้ไม่ประสงค์ดีนำอุปกรณ์สื่อสารเข้ามาสร้างความรบกวนให้กับระบบสื่อสาร

Rescued mesh router

เราท์เตอร์ประเภทนี้เป็นเราท์เตอร์ที่สามารถเคลื่อนที่ได้ขณะทำงาน โดยเป็นเราท์เตอร์ที่นำเทคโนโลยีของ Smart board มาทำการพัฒนา ทำให้มีขนาดเล็กและยังสามารถทำงานเพื่อเชื่อมต่อการสื่อสารได้อย่างมีประสิทธิภาพเท่ากับ Stationary mesh router โดย Rescued mesh router นั้นจะถูกนำไปติดที่ตัวผู้ช่วยเหลือทำให้สามารถเคลื่อนที่ไปพร้อมกับผู้ช่วยเหลือได้ ดังนั้นRescued mesh router นั้นจะมีบทบาทในการเชื่อมต่อการสื่อสารในสถานที่ที่ไม่ได้มีการติดตั้ง Stationary mesh router ไว้ โดยผู้ช่วยเหลือสามารถเดินทางเข้าไปยังบริเวณดังกล่าวและสามารถให้การสื่อสารกับผู้คนบริเวณนั้น หรือจะนำ Rescued mesh router เข้าไปเชื่อมต่อเพื่อซ่อมแซมเครือข่ายการสื่อสารในบริเวณที่เครือข่ายเกิดความเสียหายชั่วขณะก็ได้

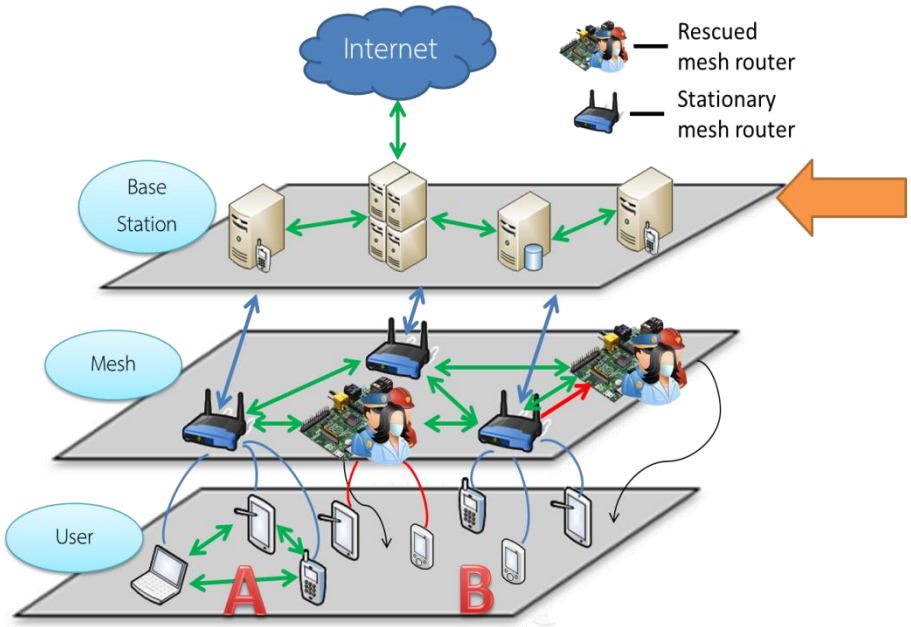
เนื่องจาก Rescued mesh router นั้นเป็นอุปกรณ์เชื่อมต่อเครือข่ายที่ติดไว้ที่ตัวผู้ช่วยเหลือดังนั้น Rescued mesh router จึงสามารถบ่งบอกตำแหน่งของผู้ช่วยเหลือได้

นั่นเอง เพื่อที่จะทำให้ Stationary mesh router ส่งข้อความหาผู้ช่วยเหลือที่อยู่ในบริเวณใกล้ที่สุดนั้น เราท์เตอร์ประเภทนี้จึงทำหน้าที่ในการแจ้งเตือนตำแหน่งของตนเองผ่านไปยังเราท์เตอร์ตัวอื่นๆ(ซึ่งกลไกในการแจ้งเตือนตำแหน่งจะกล่าวยังหัวข้อถัดไป) เมื่อ Rescued mesh router ทำการแจ้งเตือนตำแหน่งแล้วเราท์เตอร์ตัวอื่นๆจะบันทึกข้อมูลตำแหน่งของ Rescued mesh router ไว้ที่ตนเองจากนั้นเมื่อได้รับข้อความจากผู้ใช้งานเครือข่ายนั้นก็จะส่งต่อข้อความไปยังผู้ช่วยเหลือที่ใกล้ที่สุดโดยอาศัยข้อมูลที่รับมาจากการแจ้งเตือนของ Rescued mesh router นั่นเอง

ผู้ช่วยเหลือที่มี Rescued mesh router ติดอยู่นั้นจะสามารถใช้งานการสื่อสารได้ผ่านอุปกรณ์สื่อสารประเภท Smart device เช่นกัน นั่นคือผู้ช่วยเหลือจะนำอุปกรณ์สื่อสารเชื่อมต่อสัญญาณเข้ากับ Access point ที่ได้ถูกสร้างจาก Rescued mesh router เมื่อ Rescued mesh router ได้รับข้อความที่ส่งต่อมาจากผู้ประสบภัยนั้น Rescued mesh router จะทำการส่งต่อข้อความไปยังโครงสร้างพื้นฐานชั้นสถานีรับข้อมูลและอีกทั้งจะส่งข้อความต่อให้กับอุปกรณ์สื่อสารของผู้ช่วยเหลือที่เชื่อมต่อเข้ากับ Rescued mesh router ตัวนั้นด้วย

Rescued mesh router ยังสามารถกระจาย Access point เพื่อเชื่อมต่อการสื่อสารเหมือน Stationary mesh router ปกติดังนั้นจึงทำให้ผู้ประสบภัยสามารถเชื่อมต่อ Access point ของ Rescued mesh router ได้และสามารถสื่อสารกับผู้ประสบภัยได้โดยตรงเปรียบเสมือนการใช้งานการสื่อสารแบบ Peer-to-peer นั่นเอง ดังนั้นRescued mesh router จึงเป็นอุปกรณ์ที่ช่วยเพิ่มความยืดหยุ่นให้กับระบบสื่อสารในโครงสร้างการสื่อสารชั้นนี้ ทำระบบสื่อสารมีความแตกต่างไปจากระบบสื่อสารแบบการติดตั้งโครงสร้างพื้นฐานโดยทั่วไปนั่นเอง

ระดับชั้นสถานีรับข้อมูล (Base station Layer)



รูปที่ 36 โครงสร้างระดับชั้นสถานีรับข้อมูล

โครงสร้างชั้นนี้จะประกอบด้วยเครือคอมพิวเตอร์มากมายที่นำมาติดตั้งเพื่อเก็บข้อมูลมาประมวลผล โดยโครงสร้างชั้นนี้เป็นโครงสร้างที่เปรียบดังเป็นสมองของเครือข่ายการสื่อสาร ผู้ช่วยเหลือจะนำข้อมูลที่ได้จากการประมวลผลหรือการวิเคราะห์ต่างๆจากโครงสร้างชั้นนี้ไปใช้ประโยชน์ในการสื่อสาร โดยสถานีรับข้อมูลนั้นสามารถแบ่งออกได้เป็น 2 ประเภทดังนี้

สถานีรับข้อมูลหลัก (Main base station)

สถานีรับข้อมูลหลักนี้จะทำหน้าที่เป็นเหมือนส่วนกลางในการจัดการข้อมูลบนพื้นที่ภัยพิบัติ โดยข้อมูลจะถูกส่งจากผู้ใช้ผ่านเครือข่ายโครงสร้างพื้นฐานมายังสถานีหลัก นอกจากนี้สถานีรับข้อมูลหลักยังทำหน้าที่ให้ความช่วยเหลือกับหน่วยกู้ภัยในการส่งอุปกรณ์ช่วยเหลือเข้าไปในพื้นที่ประสบภัย ที่ตั้งของสถานีรับข้อมูลหลักนี้อาจจะติดตั้งบนพื้นที่ประสบภัยหรือจะติดตั้งที่พื้นที่ที่ไกลออกไปก็ได้

สถานีรับข้อมูลชั่วคราว (Temporary base station)

สถานีรับข้อมูลหลักนั้นบางครั้งอาจจะไม่สามารถให้ความช่วยเหลือกับผู้ประสบภัยได้ทันท่วงทีเนื่องจากตำแหน่งที่ตั้งอาจจะอยู่ไกลออกไปจากพื้นที่ประสบภัย ดังนั้นจึงจะต้องมีสถานีรับข้อมูลชั่วคราวที่ตั้งอยู่ภายในบริเวณเกิดสถานการภัยพิบัติช่วยในการส่งอุปกรณ์ต่างๆไปยังที่สถานที่ที่ต้องการความช่วยเหลือ ในการที่จะติดตั้งสถานีรับข้อมูลชั่วคราวนั้น

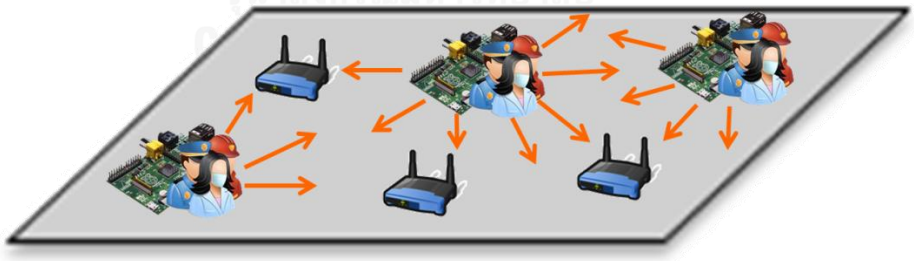
เจ้าหน้าที่ยังสามารถนำ Rescued mesh router ที่มีกลไกในการรับข้อมูลจากเราท์เตอร์ตัวอื่นๆอยู่แล้วมาสร้างเป็นสถานีรับข้อมูลได้ โดยสถานีรับข้อมูลชั่วคราวนั้นสามารถติดตั้งได้หลายสถานีพร้อมๆกันบนพื้นที่ภัยพิบัติ

3.2.2 กลไกในการเลือกเส้นทางการส่งข้อมูล

เนื่องจากระบบสื่อสารที่ออกแบบมานั้นสามารถอนุญาติให้ผู้ประสบภัยที่เชื่อมต่อกับระบบสื่อสารสามารถส่งข้อความไปยังเจ้าหน้าที่ได้โดยตรง นั่นคือการส่งข้อความไปยัง Rescued mesh router นั่นเองดังนั้นจึงต้องมีกลไกที่ใช้ในการส่งข้อมูลจาก Stationary mesh router ที่ผู้ใช้เชื่อมต่ออยู่ไปยัง Rescued mesh router โดยสมมติฐานว่าผู้ช่วยเหลือที่อยู่ใกล้นั้นจะสามารถให้ความสะดวกในการช่วยเหลือได้ดีกว่าผู้ช่วยเหลือที่อยู่ไกล กลไกนี้จึงเลือกที่จะส่งข้อมูลไปยัง Rescued mesh router ที่ใกล้ที่สุด ระบบเราจึงสามารถให้ความสะดวกกับผู้ประสบภัยในการส่งข้อมูลไปยังปลายทาง ผู้ประสบภัยนั้นไม่จำเป็นจะต้องรู้เส้นทางหรือรู้หมายเลข IP address ของเจ้าหน้าที่ข้อความก็สามารถถูกส่งไปยังเจ้าหน้าที่ได้

ในการที่จะทำให้เราท์เตอร์มีความสามารถในการส่งต่อข้อมูลไปยังผู้ช่วยเหลือได้นั้นเราได้ทำการติดตั้ง Middleware ลงบนที่เราท์เตอร์ โดย Middleware จะทำงานร่วมกับโปรโตคอลที่ใช้ในการสื่อสารเพื่อส่งข้อความไปยังผู้ช่วยเหลือ โดยโปรโตคอลในการสื่อสารที่เลือกใช้นั้นระบบเราได้เลือกใช้ Optimized Linked State Routing protocol (OLSR protocol) ในการส่งข้อความ โดย Middleware นั้นจะดึงข้อมูลของ OLSR protocol มาช่วยในกลไกการเลือกเส้นทางอีกด้วย โดยกลไกในการเลือกเส้นทางนั้นสามารถแบ่งออกได้เป็น 2 กลไกดังนี้

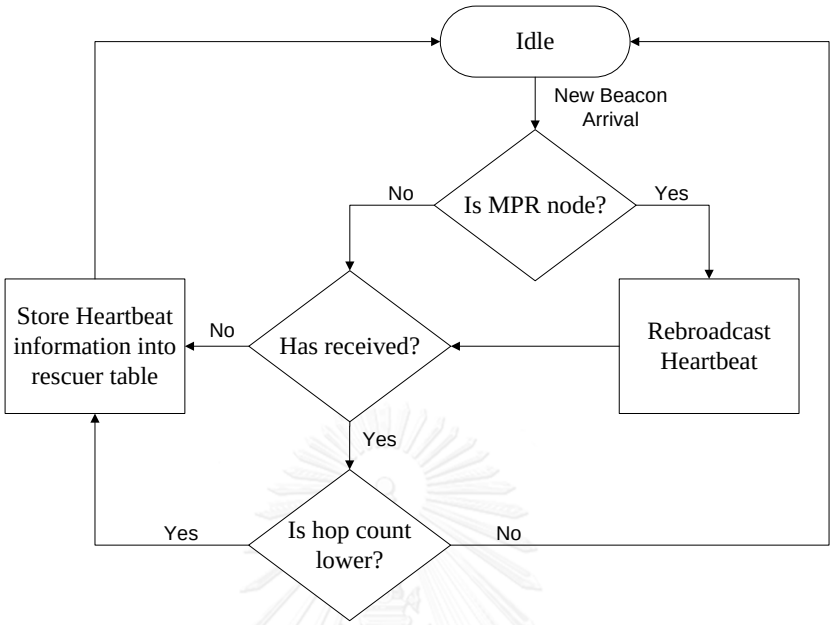
กลไกการส่งสัญญาณ (Heartbeat mechanism)



รูปที่ 37 กลไกการส่งสัญญาณ

กลไกนี้เป็นกลไกที่ทำให้ Stationary mesh router สามารถรู้ตำแหน่งของ Rescued mesh router ได้โดย Rescued mesh router จะทำการส่งสัญญาณ Heartbeat ออกมาเป็นระยะเพื่อประกาศตัวตนบนเครือข่าย จากนั้นข้อความที่ใช้ประกาศตัวตนจะถูกส่งกระจายออกไปทั่วเครือข่ายการสื่อสาร ทำให้ Stationary mesh router ในบริเวณสามารถทราบตำแหน่งของ Rescued mesh router และสามารถส่งข้อความไปยัง Rescued mesh router ที่ใกล้เคียงได้ การ

ส่งสัญญาณนั้นจะถูกส่งโดย Rescued mesh router เท่านั้นสำหรับ Stationary mesh router นั้นไม่มีความจำเป็นจะต้องส่งสัญญาณเพื่อประกาศตัวตน การส่งสัญญาณนั้นได้แสดงดังรูปที่ 37



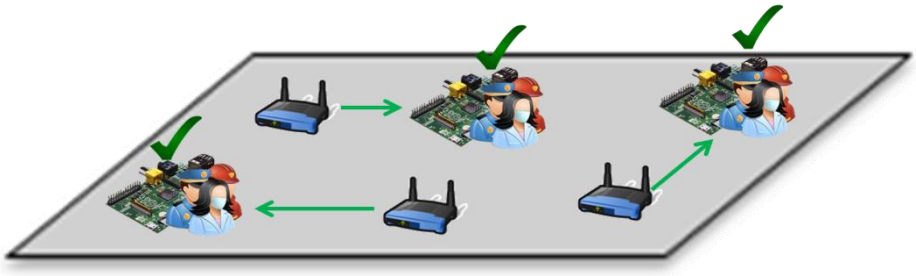
รูปที่ 38 วิธีการส่งต่อสัญญาณ

สัญญาณนั้นจะถูกส่งออกมาโดย Rescued mesh router เพื่อใช้ในการประกาศตัวตนซึ่งข้อมูลภายในสัญญาณจะประกอบด้วย หมายเลข IP ของผู้ส่ง, ตัวนับ Hop, และเวลาในขณะที่ส่งสัญญาณ(Timestamp) กลไกนี้จะใช้ตัวนับ Hop ในการระบุถึงระยะทาง โดยตัวนับ Hop จะเพิ่มขึ้นทุกครั้งเมื่อมีการส่งต่อสัญญาณ รูปที่ 38 แสดงวิธีการในการส่งต่อสัญญาณ เมื่อสัญญาณถูกส่งออกมาโดย Rescued mesh router แล้วนั้นเราท์เตอร์ตัวอื่น (ทั้ง Stationary mesh router และ Rescued mesh router) จะทำการส่งต่อสัญญาณถ้าเราท์เตอร์ตัวนั้นเป็น MPR node ของผู้ส่งสัญญาณ โดยข้อมูล MPR นั้นจะถูกดึงมาจาก OLSR protocol เพื่อใช้ช่วยในการลดจำนวนครั้งในการส่งต่อสัญญาณ การส่งต่อสัญญาณที่ MPR node จะเกิดขึ้นต่อเมื่อสัญญาณนั้นเป็นสัญญาณใหม่ที่ยังไม่เคยรับมาก่อนโดยสัญญาณใหม่สามารถระบุได้จากเวลาที่ใช้ในการส่งนั่นเอง และก่อนทำการส่งต่อสัญญาณนั้นจะทำการเพิ่มตัวนับ Hop ขึ้นไป 1 เพื่อเป็นการแจ้งระยะห่างให้กับเราท์เตอร์ตัวถัดไป

เนื่องจากสัญญาณนั้นจะสามารถส่งออกไปได้หลายทางทำให้ผู้รับสัญญาณนั้นมีโอกาสได้รับสัญญาณจากหลายทางเช่นกัน จึงจำเป็นต้องมีกลไกในการตรวจสอบว่าสัญญาณที่ได้รับมาจากทางไหนนั้นควรจะบันทึกเอาไว้ เมื่อผู้ที่ได้รับสัญญาณ ไม่ว่าจะเป็น MPR node หรือไม่ก็ตามได้รับสัญญาณมาแล้ว จะทำการตรวจสอบหมายเลข IP address และTimestamp ของสัญญาณว่าเคย

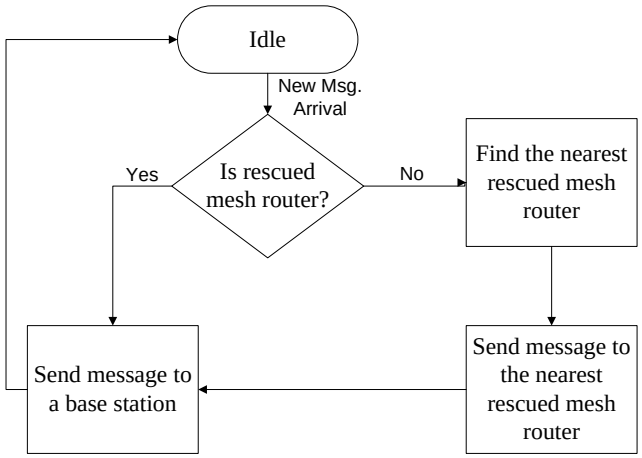
ได้รับสัญญาณจาก IP address หมายเลขนี้ที่ Timestamp ที่ระบุไว้หรือไม่ ถ้าไม่เคยได้รับมาก่อนจะทำการบันทึกข้อมูลทันที แต่ถ้าหากเคยได้รับมาแล้วจะเปรียบเทียบระยะทาง สัญญาณที่อาจถูกส่งมาจากหลายทางนั้นระยะทางสามารถเปลี่ยนแปลงได้หลากหลายขึ้นกับเส้นทางที่ส่งมาของสัญญาณ ดังนั้นข้อมูลจะถูกบันทึกเมื่อระยะทางของสัญญาณนั้นน้อยกว่าระยะทางที่เคยถูกบันทึกไว้

กลไกในการส่งต่อข้อมูล (Forward mechanism)



รูปที่ 39 กลไกการส่งต่อข้อมูล

กลไกนี้เป็นกลไกที่ทำให้ Stationary mesh router นั้นสามารถส่งข้อมูลไปยัง Rescued mesh router ได้ (แสดงดังรูปที่ 39) เมื่อ Rescued mesh router นั้นประกาศตัวตนผ่านกลไกการส่งสัญญาณแล้วจะทำให้ Stationary mesh router นั้นสามารถรู้ถึงตำแหน่งของ Rescued mesh router ได้ เมื่อผู้ประสบภัยที่ได้ทำการเชื่อมต่อเข้ากับเครือข่ายผ่าน Stationary mesh router และส่งข้อความออกมา Stationary mesh router ตัวนั้นจะทำการส่งต่อข้อความไปให้ Rescued mesh router ตัวที่ใกล้ที่สุดนั่นเอง



รูปที่ 40 วิธีการส่งต่อข้อความ

การส่งต่อข้อความนั้นได้แสดงดังรูปที่ 40 เมื่อได้รับข้อความมาใหม่นั้นถ้าสำหรับ Stationary mesh router จะทำการค้นหา Rescued mesh router ที่ใกล้ที่สุดจากข้อมูลสัญญาณที่ได้ทำการบันทึกไว้ จากนั้นจะทำการส่งต่อข้อความไปยัง Rescued mesh router ตัวนั้น อีกทั้ง Stationary mesh router จะทำการสำเนาข้อความอีก 1 ฉบับ เพื่อส่งต่อข้อความให้กับสถานีรับข้อมูล แต่สำหรับ Rescued mesh router นั้นจะทำการส่งข้อความต่อไปยังสถานีรับข้อมูลและอุปกรณ์สื่อสารของเจ้าหน้าที่ที่เชื่อมต่ออยู่เท่านั้น จะไม่ส่งต่อให้ Rescued mesh router ตัวอื่น

การเพิ่มประสิทธิภาพของกลไกส่งสัญญาณ (Heartbeat optimization)

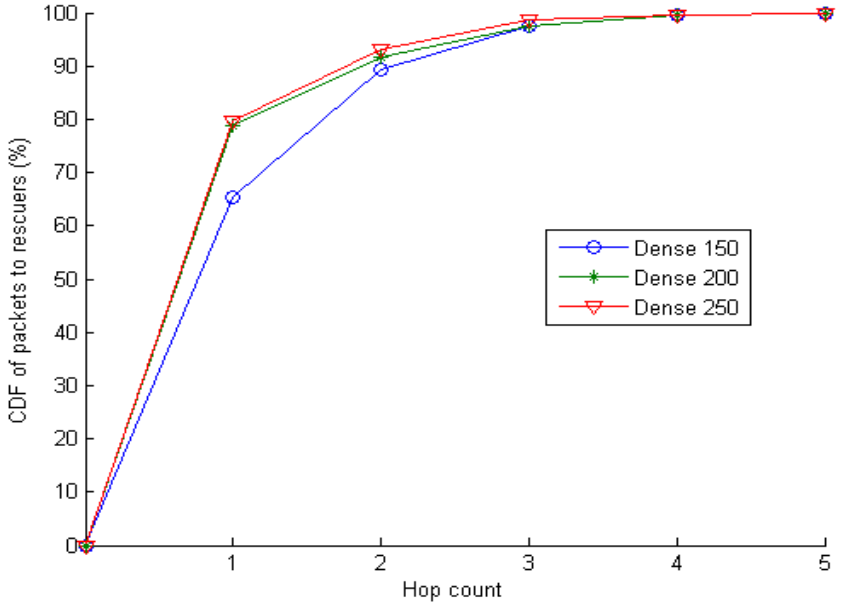
จากที่ได้กล่าวไว้นั้นกลไกในการส่งสัญญาณใช้สำหรับ Rescued mesh router ในการประกาศตำแหน่งและหมายเลข IP address ให้กับ Stationary mesh router เพื่อที่จะให้ Stationary mesh router สามารถส่งข้อความไปยัง Rescued mesh router ที่ใกล้ที่สุด โดยสัญญาณที่ส่งจาก Rescued mesh router นั้นถ้าทำการส่งได้น้อยครั้งเท่าไหร่จะยิ่งดีเท่านั้น เนื่องจากจะสามารถลดความคับคั่งของระบบการสื่อสารลงได้ดังนั้นสัญญาณที่ส่งจาก Rescued mesh router จึงไม่จำเป็นจะต้องถูกแพร่กระจายไปทั่วทั้งเครือข่ายการสื่อสาร เพียงแค่กระจายให้ครอบคลุมกับบริเวณ Stationary mesh router ที่จะส่งข้อความให้ก็เพียงพอต่อการส่งสัญญาณไปยัง Stationary mesh router

ความหนาแน่นของ Stationary mesh router (โหนด/ตร.ก.ม.)	150/200/250
พื้นที่ทดสอบ (ตร.ก.ม.)	1/1.5/2
ระยะในการส่ง (ม.)	100
จำนวนโหนดที่ส่งข้อความ (โหนด)	5
ระยะเวลาที่ทำการทดสอบ (วินาที)	100
ระยะเวลาในการส่งสัญญาณ (วินาที/ครั้ง)	5

ตารางที่ 1ตารางแสดงการตั้งค่าเพื่อการเพิ่มประสิทธิภาพในกลไกส่งสัญญาณ

งานวิจัยนี้จึงได้ทำการทดสอบเพิ่มเติมว่าควรจะส่งสัญญาณ Heartbeat อย่างไรให้มีประสิทธิภาพโดยทำการทดสอบโดยใช้โปรแกรมจำลองเครือข่าย Network Simulation (NS-3.15) [2] และมีการตั้งค่า โดยการทดลองมีการเปลี่ยนขนาดพื้นที่ทดสอบไปตามตารางที่ 1 และแต่ละพื้นที่ทดสอบนั้นก็ได้เปลี่ยนแปลงค่าความหนาแน่นของ Stationary mesh router ไปตามค่าที่กล่าวไว้ในตารางที่ 1 เช่นกัน สำหรับตัวแปรคาบเวลาที่ใช้ในการส่งสัญญาณต่อครั้งนั้นได้ตั้งไว้ค่า 5วินาทีต่อครั้ง เนื่องจากว่าได้มีการทำการทดสอบก่อนแล้วว่าคาบเวลาในการส่งสัญญาณที่เหมาะสมที่สุดนั้นคือ 5 วินาทีต่อครั้ง ดังนั้นในการทดสอบเพื่อเพิ่มประสิทธิภาพกลไกในการส่งสัญญาณ Heartbeatนั้นจึงตั้งค่าตัวแปรนี้ไว้ที่ 5 วินาทีต่อครั้งนั่นเอง และตัวแปรอื่นที่ใช้ในการทดสอบนั้นได้แสดงดังตารางที่ 1

ในการทดสอบนั้นจะทำการสุ่มโหนดที่ใช้ส่งข้อความมา 5 โหนดเพื่อทำการส่งข้อความข้อความจะถูกส่งไปยังผู้ช่วยเหลือที่ใกล้ที่สุดและทำการวัดผล การทดสอบใน 1 เงื่อนไขนั้นจะทำการทดสอบทั้งหมด 10 ครั้งโดยแต่ละครั้งที่ทำการทดสอบนั้นจะทำการสุ่มโหนดที่ใช้ส่งข้อความใหม่ จากนั้นนำผลลัพท์ที่ได้มาหาค่าเฉลี่ยและทำการวิเคราะห์ผล



รูปที่ 41 ผลทดสอบการเพิ่มประสิทธิภาพกลไกการส่งสัญญาณ

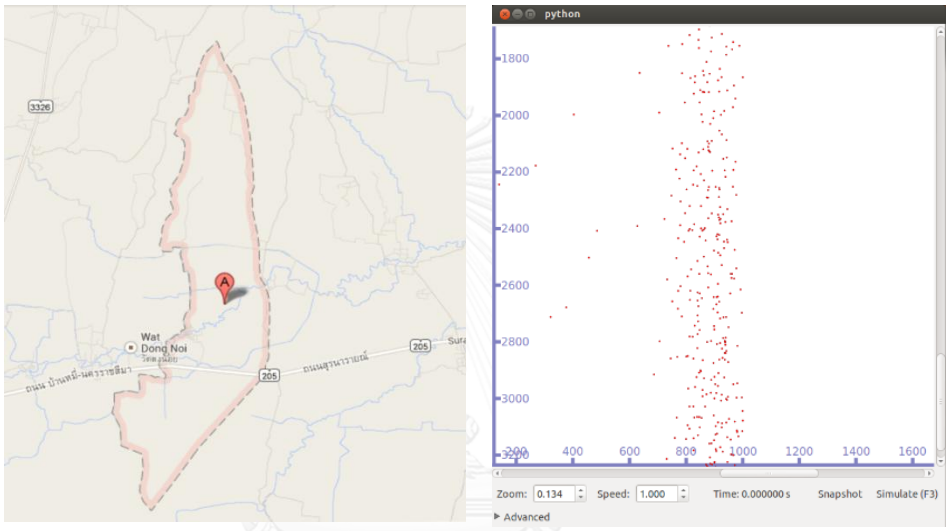
ผลทดสอบการเพิ่มประสิทธิภาพของกลไกส่งสัญญาณนั้นได้แสดงดังรูปที่ 41 จากผลทดสอบนั้นได้มีการนำผลมาพล็อตลงในกราฟโดยมีแกน x คือแกนของระยะทางซึ่งวัดในหน่วยของ Hop จากผู้ส่งข้อความ และแกน y ซึ่งเป็นเปอร์เซนของข้อความที่ได้รับที่ผู้ช่วยเหลือ จากกราฟนั้นยังได้แสดงข้อมูลที่แยกกันของแต่ละความหนาแน่นที่ใช้ในการทดสอบอีกด้วย

จากผลทดสอบพบว่าข้อความในทุกความหนาแน่นที่ใช้ทดสอบนั้นได้มีการส่งไปยังผู้ช่วยเหลือที่อยู่ไกลออกไปไม่เกิน 5 Hop นั่นคือเมื่อ Stationary mesh router ได้รับข้อความมาแล้วนั้นจะส่งต่อข้อความโดยใช้ Forward mechanism ออกไปให้ผู้ช่วยเหลือที่อยู่ไกลออกไปไม่เกิน 5 Hop นั่นเอง ดังนั้นจึงไม่มีความจำเป็นจะต้องส่งต่อสัญญาณ Heartbeat ของ Rescued mesh router ออกไปเกิน 5 Hop จากผลทดสอบนี้จึงทำให้ได้การตั้งค่าของ Time to live (TTL) ของสัญญาณของกลไกการส่งสัญญาณเป็น 5 ดังนั้นสัญญาณ Heartbeat จาก Rescued mesh router จึงถูกส่งออกไปแค่ในบริเวณ 5 Hop โดยรอบ

บทที่ 4 การทดสอบประสิทธิภาพ

เนื่องจากระบบสื่อสารบนพื้นที่ภัยพิบัติที่ได้ออกแบบมานั้นได้มีการออกแบบระบบออกเป็น 2 ส่วนนั่นคือ ส่วนแรกเป็นส่วนของการสื่อสารแบบ Peer-to-peer บนเครือข่ายแอดฮอก และอีกส่วนคือการสื่อสารผ่านโครงสร้างพื้นฐานแบบผสมบนพื้นที่ภัยพิบัติ ดังนั้นในการทดสอบประสิทธิภาพของระบบสื่อสารบนเครือข่ายภัยพิบัตินี้ได้มีการทดสอบแยกออกเป็นสองส่วนตามที่ได้ออกแบบไว้

4.1 การทดสอบประสิทธิภาพของการสื่อสารแบบ Peer-to-peer บนพื้นที่ภัยพิบัติ



รูปที่ 42 แผนที่ทำการทดสอบ

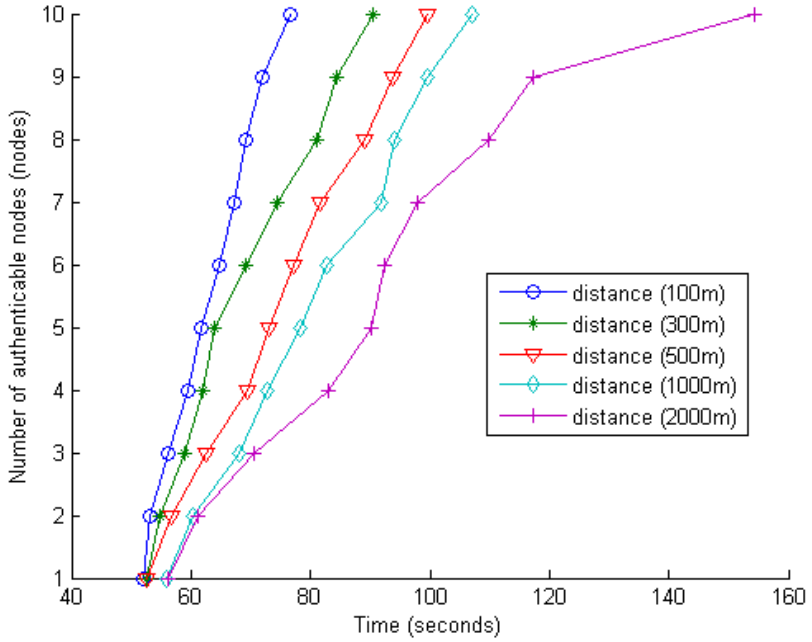
ในการสอบประสิทธิภาพของระบบการสื่อสารแบบ Peer-to-peer บนพื้นที่ภัยพิบัตินั้น ได้ใช้การทดสอบด้วยการจำลองโดยโปรแกรม Network Simulator (NS-3.15) [2] และ Bonn Motion [19] ในการกำหนดการเคลื่อนที่ของโหนดในการทดสอบ ซึ่งได้มีการตั้งค่าระบบให้ทำการจำลองมาจากสถานการณ์จริงในประเทศไทยนั่นคือตำบลดงพลับ อำเภอบ้านหมี่ จังหวัดลพบุรี สถานที่แห่งนี้ได้เกิดภัยพิบัติน้ำท่วมขึ้นทำให้ถูกตัดขาดจากโลกภายนอกไม่สามารถสื่อสารกับนอกเมืองได้ โดยตำบลดงพลับมีพื้นที่ประมาณ 1000 x 7000 ตารางเมตร จึงได้เลือกสถานที่นี้เป็นสถานที่ในการจำลองขึ้น นอกจากนั้นในการจำลองได้มีการตั้งจุดรวมประชากร(Attraction point) ของตำบลอยู่ที่บริเวณที่มีสถานที่สำคัญของตำบลที่มีทั้งสถานีอนามัยโรงเรียน และสถานที่สำคัญอีกด้วย โดยความหนาแน่นของประชากรจะมีมากที่บริเวณพื้นที่สำคัญและเบาบางลงบนพื้นที่ใกล้เคียงโดยแผนที่ทำการทดสอบได้แสดงดังรูปที่ 42

เวลาในการทดสอบ(วินาที)	400
ความหนาแน่นของประชากร(โหนด/ตร.ก.ม.)	150
เวลาที่เริ่มในการส่งข้อความ (วินาที)	50-60
ระยะการส่งสัญญาณ (ม.)	50
จำนวนโหนดที่ใช้ในการส่งข้อความ(โหนด)	10

ตารางที่ 2 ตารางแสดงการตั้งค่าทดสอบประสิทธิภาพการสื่อสารแบบ Peer-to-peer บนพื้นที่ภัยพิบัติ

การตั้งค่าการทดสอบนั้นได้แสดงยังตารางที่ 2 โดยในการทดสอบใช้ความหนาแน่นของประชากรอยู่ที่ 150 คนต่อตารางกิโลเมตรเนื่องจากเป็นความหนาแน่นของประชากรเฉลี่ยที่บริเวณนั้น เมื่อเริ่มทดสอบระบบได้ปล่อยให้โหนดในระบบทำการเดินอย่างสุ่ม(Random way point) ไปยังพื้นที่ต่างๆซักระยะหนึ่งก่อนทำการส่งข้อความ โหนดจะเริ่มส่งข้อความโดยการสุ่มเวลาในช่วงวินาทีที่ 50 – 60 ของการทดสอบ สำหรับการตั้งค่าอื่นๆนั้นได้แสดงยังดารางที่ 2

ผลทดสอบความสามารถในการยืนยันตัวตนในแบบ Fully Trusted Mode

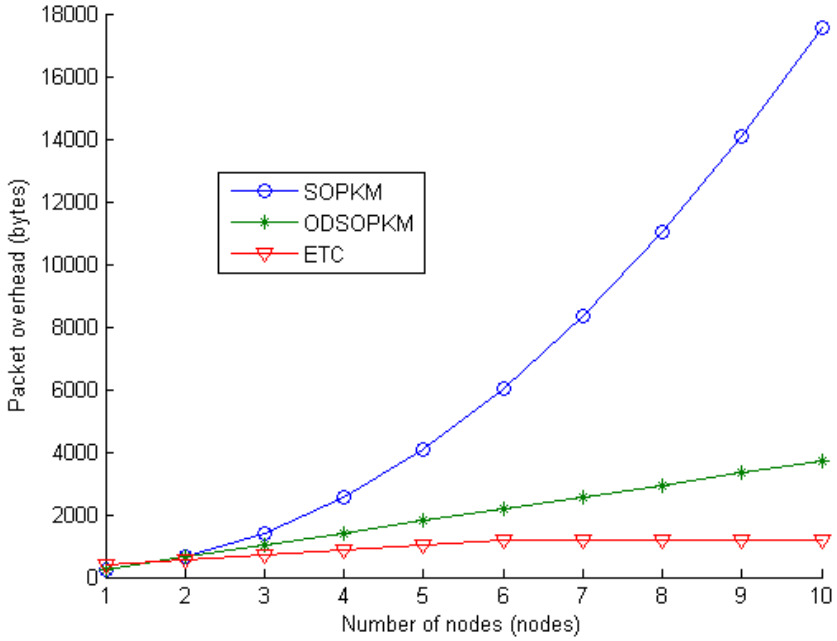


รูปที่ 43 ความสามารถในการยืนยันตัวตนของ Fully Trusted Mode

รูปที่ 43 แสดงผลการทดสอบความสามารถในการยืนยันตัวตนในแบบ Fully Trusted Mode โดยการทดสอบยืนยันตัวตนนั้นทำได้โดยการจำลองส่งข้อความโดยเลือกโหนดที่ทำการส่งข้อความมาทั้งหมด 10 โหนด จากนั้นก็เริ่มส่งข้อความไปยังโหนดที่ได้ตั้งไว้ให้เป็นสถานีรับข้อมูล เปรียบเสมือนการส่งขอ Certificate เมื่อสถานีรับข้อมูลได้รับข้อความจากโหนดแล้วจะทำการส่งข้อความกลับ เปรียบเสมือนการตอบกลับการขอ Certificate ถ้าการส่งสำเร็จลุล่วงนั้นจะถือว่าการ

ยืนยันตัวตนสำเร็จด้วย ในการทดสอบนั้นได้มีการแบ่งพื้นที่ทดสอบออกเป็น 5 ประเภทตามระยะห่างจากสถานีรับข้อมูล ในแต่ละพื้นที่ทดสอบนั้นได้ทำการทดสอบซ้ำพื้นที่ละ 10 ครั้ง โดยแต่ละครั้งจะทำการเลือกโหนดที่ใช้ในการส่งข้อมูลให้มีความแตกต่างกัน เมื่อทดสอบเสร็จสิ้นจะนำผลที่ได้มาหาค่าเฉลี่ยในแต่ละพื้นที่และทำการวิเคราะห์ผลทดสอบ จากผลทดลองสรุปได้ว่าด้วยประสิทธิภาพของโปรโตคอลที่ได้ทำการออกแบบมานั้นทำให้ผู้ใช้งานการสื่อสารแบบ Peer-to-peer บนพื้นที่ภัยพิบัตินั้นสามารถยืนยันตัวตนได้อย่างรวดเร็ว แม้ว่าจะอยู่ไกลจากสถานีรับข้อมูล การยืนยันตัวตนก็สำเร็จภายในเวลา 3 นาที

ผลการทดสอบ Overhead ของ Packet ในการยืนยันตัวตนแบบ Half Trusted Mode



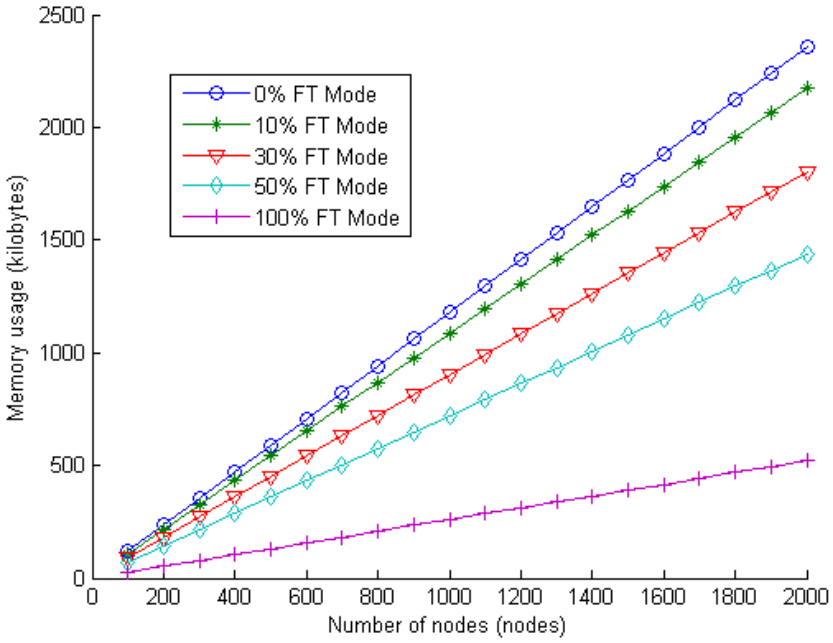
รูปที่ 44 ผลการทดสอบ Overhead ของ Packet ในการยืนยันตัวตนแบบ Half Trusted Mode

รูปที่ 44 ได้แสดงผลการวัด Overhead ของ Packet ที่ใช้ในการส่งข้อความโดยการทดสอบนี้ได้นำโปรโตคอลที่ได้ออกแบบไปเปรียบเทียบกับโปรโตคอลที่ใช้ในการยืนยันตัวตนแบบไม่อาศัยเจ้าหน้าที่ 2 โปรโตคอล นั่นคือ SOPKM และ ODSOPKM ในการทดสอบนั้นได้ทำการวัดขนาดของ Packet ที่ใช้เพื่อยืนยันตัวตนและนำผลที่ได้มาแสดงในกราฟ

จากผลทดสอบจะเห็นว่าสำหรับโปรโตคอล SOPKM นั้นจะมีการเพิ่มขนาดของ Packet เป็นแบบสมการกำลังสอง และสำหรับ ODSOPKM นั้นจะมีการเพิ่มขนาดของ Packet เป็นแบบสมการเส้นตรงเมื่อมีการส่งข้อความผ่านอุปกรณ์สื่อสารมากขึ้น แต่สำหรับโปรโตคอลที่ได้ออกแบบนั้น (ETC) ขนาดของ Packet จะโตแบบสมการเส้นตรงจนกระทั่งถึง 5-6 โหนดแรกจากนั้นขนาดของ Packet

จะไม่โตอีกเนื่องจากระบบได้ทำการกำหนดไว้แล้วว่า Packet จะต้องมีขนาดไม่เกิน 1500 Bytes นั่นเอง

ผลทดสอบการใช้หน่วยความจำของโปรโตคอล

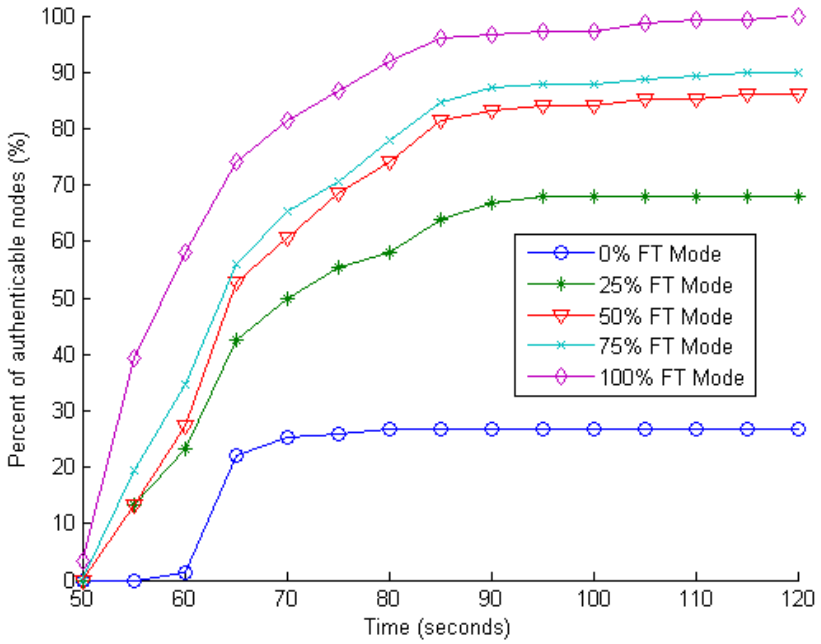


รูปที่ 45 ผลทดสอบการใช้หน่วยความจำของโปรโตคอล

เนื่องจากโปรโตคอลที่ได้ออกแบบนั้นจำเป็นจะต้องบันทึกข้อมูลของการยืนยันตัวตนไว้ในอุปกรณ์จึงได้มีการทดสอบการใช้งานหน่วยความจำเพื่อตรวจสอบขนาดของหน่วยความจำที่จะต้องใช้ในการใช้งานโปรโตคอล รูปที่ 45 แสดงผลทดสอบการใช้หน่วยความจำ ในการจำลองสถานการณ์นั้นได้มีการจำลองออกเป็น 5 สถานการณ์แยกประเภทตามความหนาแน่นของโหนดที่มีการยืนยันตัวตนแบบ Fully Trusted Mode ในระบบ เมื่อมีโหนดที่ได้รับการยืนยันตัวตนแบบ Fully Trusted Mode ในระบบมากทำให้ไม่ต้องใช้หน่วยความจำในการเก็บข้อมูลการยืนยันตัวตนมากเช่นกัน เนื่องจากว่าโหนดที่ได้ทำการยืนยันตัวตนแบบ Fully Trusted Mode แล้วจะถือว่าเป็นโหนดที่มีความน่าเชื่อถือ ทำให้ไม่จำเป็นต้องบันทึกค่าความเชื่อใจอีก

ผลทดสอบแสดงให้เห็นว่าหน่วยความจำที่ถูกใช้งานนั้นมีขนาดโตขึ้นแบบสมการเส้นตรงและมีการแปรผกผันกับความหนาแน่นของโหนดแบบ Fully Trusted Mode ในระบบ เมื่อมีโหนดที่มีการยืนยันตัวตนแบบ Fully Trusted Mode ในระบบมากการใช้หน่วยความจำจะน้อยลง

ผลการทดสอบเปอร์เซนของโหนดที่ได้รับการยืนยันตัวตน



รูปที่ 46 ผลการทดสอบเปอร์เซนของโหนดที่ได้รับการยืนยันตัวตน

ในการทดสอบนี้เป็นการทดสอบความสามารถของโปรโตคอลในการยืนยันตัวตนของข้อความที่ได้รับ เนื่องจากข้อความที่ได้รับมานั้นถ้าเป็นข้อความของผู้ใช้ที่มีการยืนยันตัวตนแบบ Half Trusted Mode นั้นจะไม่สามารถใช้ในการยืนยันตัวตนได้ทันที เพราะว่าการที่จะยืนยัน Mini-certificate ได้จำเป็นจะต้องได้รับ Certificate ของผู้ที่ออกให้เสียก่อน ซึ่งการที่จะได้รับ Certificate ของใครนั้นจำเป็นจะต้องได้รับข้อความจากบุคคลนั้น ดังนั้นความสามารถในการยืนยันตัวตนของโปรโตคอลจึงขึ้นกับความสามารถในการส่งข้อมูลของโปรโตคอลด้วย การทดสอบนี้จะแสดงให้เห็นถึงความสามารถในการยืนยันบุคคลเมื่อได้รับข้อความ

ในการทดสอบครั้งนี้ได้ทำการเลือกโหนดที่ใช้ส่งข้อมูลทั้งหมด 150 โหนดจากบริเวณต่างๆ โดยมีผู้รับแค่โหนดเดียว และมีการตั้งค่าก่อนเริ่มทดลองคือ อุปกรณ์สื่อสารนั้นจะได้รับ Mini-certificate ของเพื่อนบ้าน 2-6 Mini-certificate เก็บไว้ในอุปกรณ์อยู่แล้ว เมื่อทำการส่งข้อความจึงสามารถทำการยืนยันตัวตนได้ทันที การทดลองนี้ได้มีการเปลี่ยนค่าความหนาแน่นของโหนดที่มีการยืนยันตัวตนแบบ Fully Trusted Mode ตามกราฟในรูป 48 ที่แสดง โดยโหนดที่มีการยืนยันตัวตนแบบ Fully Trusted Mode นั้น เมื่อมีการส่งข้อความจะสามารถถูกยืนยันตัวตนได้ทันที เพราะไม่ต้องอาศัย Mini-certificate

ผลทดสอบในรูปที่ 46 แสดงให้เห็นว่าเมื่อมีจำนวนโหนดที่มีการยืนยันตัวตนแบบ Fully Trusted Mode มากจะทำให้มีโอกาสการยืนยันตัวตนสำเร็จมากขึ้นไปด้วย

4.2 การทดสอบประสิทธิภาพของระบบสื่อสารโดยใช้โครงสร้างพื้นฐานแบบผสม

ในการทดสอบประสิทธิภาพของระบบสื่อสารโดยใช้โครงสร้างพื้นฐานแบบผสมนั้นได้มีการทดสอบประสิทธิภาพโดยการใช้โปรแกรม Network Simulator (NS-3.15) เช่นเดียวกัน โดยการทดสอบนั้นได้ทำการสร้างสถานการณ์ทำการทดสอบ จากโครงสร้างของระบบนั้นชั้นการทำการที่มีการส่งข้อมูลหลักคือชั้นของตัวกลางส่งข้อมูล ดังนั้นโหนดในระบบทดสอบนั้นจะแทนด้วยเราท์เตอร์ซึ่งเป็นองค์ประกอบในชั้นนี้ และมีการติดตั้งสถานีรับข้อมูลไว้ในแผนที่เพื่อทำการรับข้อมูลจากเราท์เตอร์ด้วย

ก่อนการทดสอบนั้น ได้ทำการติดตั้ง Stationary mesh router ลงบนพื้นที่อย่างสุ่ม โดย Stationary mesh router จะเป็นตัวกลางในการส่งข้อมูลไปยังผู้ช่วยเหลือและสถานีรับข้อมูล สำหรับ Rescued mesh router นั้นเป็นสิ่งที่แสดงถึงผู้ช่วยเหลือในพื้นที่ประสบภัย ซึ่งสามารถเคลื่อนที่ได้ ดังนั้นจึงได้ทำการวาง Rescued mesh router แบบสุ่มลงบนพื้นที่ จากนั้นปล่อยให้ Rescued mesh router ทำการเคลื่อนที่ โดยการเคลื่อนที่ของ Rescued mesh router นั้นจะมีการเคลื่อนที่สลับกับหยุด เคลื่อนที่เข้าไปช่วยเหลือ และหยุดเพื่อทำการช่วยเหลือนั่นเอง โดยการหยุดนั้นจะหยุด 4 - 7 วินาทีอย่างสุ่ม

ระยะเวลาทดสอบ (วินาที)	100
ความหนาแน่นของ Stationary mesh router (โหนด/ตร.ก.ม.)	200
ขนาดของพื้นที่ทดสอบ (ตร.ก.ม.)	1
เวลาที่เริ่มส่งข้อความ (วินาที)	50-60
ระยะการส่งสัญญาณ (ม.)	100
จำนวนโหนดที่ทำการส่งข้อความ(โหนด)	5
คาบเวลาของการส่งสัญญาณ Heartbeat (วินาที)	3/5/7

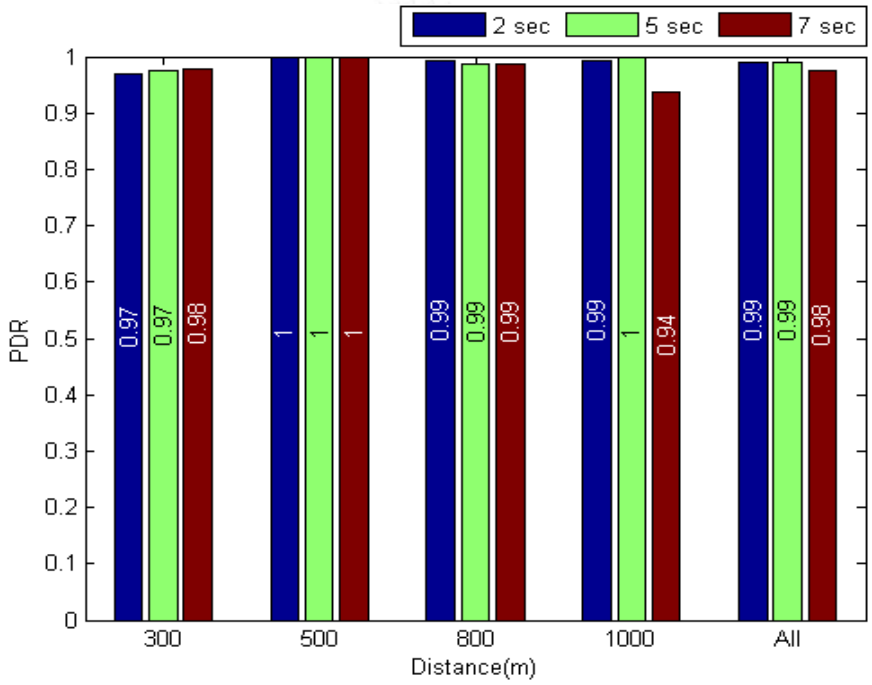
ตารางที่ 3 ตารางการตั้งค่าผลทดสอบระบบการสื่อสารโดยใช้โครงสร้างพื้นฐานแบบผสม

ตารางที่ 3 นั้นแสดงการตั้งค่าของการทดสอบโดยมีการทดสอบ 100 วินาทีและมีความหนาแน่นของ Stationary mesh router อยู่ที่ 200 โหนดต่อตารางกิโลเมตรและความหนาแน่นของ Rescued mesh router นั้นจะมีค่าเป็น 20% ของความหนาแน่น Stationary mesh router ในระหว่างการทดสอบได้มีการปล่อยให้ Rescued mesh router ได้มีการเคลื่อนที่ระยะหนึ่งก่อนทำการส่งข้อมูล การส่งข้อมูลนั้นใช้เป็นการส่งข้อมูลแบบ Constant bit rate (CBR) เนื่องจากแอพพลิเคชั่นที่ทำการส่งข้อมูลนั้นเป็นการส่งข้อความสั้นๆไม่เกิน 1 Packet ต่อการส่งข้อความ 1 ครั้ง ซึ่งขนาดของข้อความสั้นนั้นไม่มีความแตกต่างกันอย่างมีนัยสำคัญ ดังนั้นในการทดสอบนี้จึงจะวัด

ความสามารถในการส่งข้อมูลโดยใช้การส่งข้อมูลแบบ CBR เพื่อความสะดวกในการทำการทดลองผล โดยโหนดที่ทำการส่งข้อความจะส่งข้อความออกมา 5 ครั้ง ติดต่อกัน

ในกระบวนการทดสอบนั้นยังได้มีการเปลี่ยนค่าคาบเวลาในการส่งสัญญาณ Heartbeat โดยมีการเปลี่ยนค่าคาบการส่งสัญญาณที่ 3 วินาที, 5 วินาที, และ 7 วินาทีตามลำดับ โดยกลไกในการส่งสัญญาณ Heartbeat ที่ใช้ทดสอบนั้นเป็นกลไกในการส่งสัญญาณ Heartbeat ก่อนที่จะได้รับการพัฒนาให้ดีขึ้น ซึ่งเป็นกลไกที่มีการส่งสัญญาณไปทั่วเครือข่ายเพื่อประกาศตำแหน่งของ Rescued mesh router เนื่องจากผลที่ได้มานั้นจะนำไปใช้ในการเลือกค่าคาบเวลาของกลไกการส่งสัญญาณเพื่อใช้ในการปรับปรุงกลไกนั่นเอง

ผลทดสอบความสามารถในการส่งข้อมูลถึงผู้ช่วยเหลือ

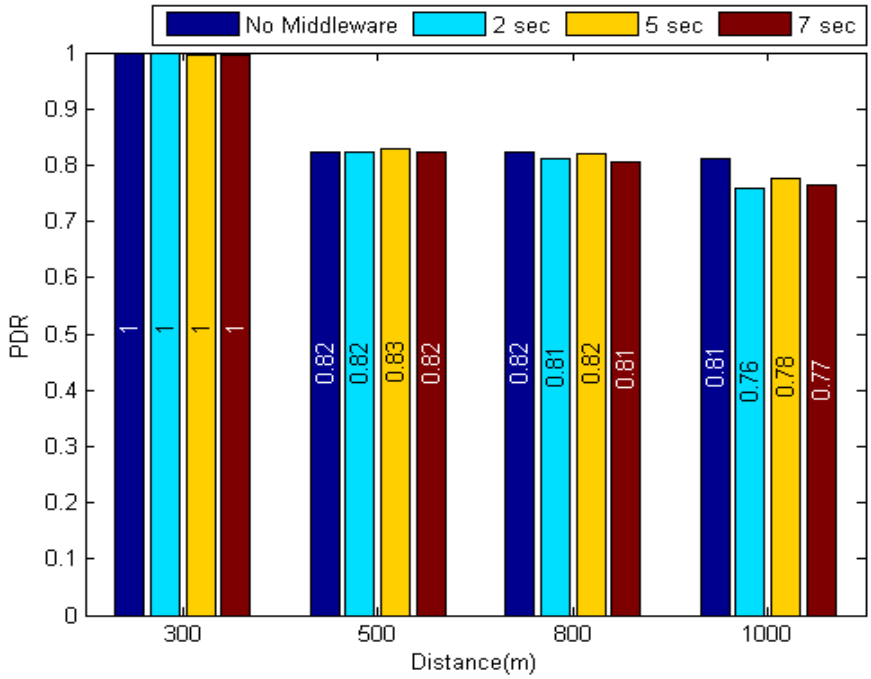


รูปที่ 47 ผลทดสอบความสามารถในการส่งข้อมูลถึงผู้ช่วยเหลือ

รูปที่ 47 นั้นได้แสดงความสามารถในการส่งข้อความไปยังผู้ช่วยเหลือของระบบสื่อสาร โดยผลทดสอบนั้นได้ทำการเปรียบเทียบผลที่ระยะทางต่างๆวัดจากสถานีส่งข้อมูล และสำหรับทุกระยะทางนั้นมีค่าเปลี่ยนแปลงค่าคาบการส่งสัญญาณ Heartbeat ด้วย โดยการตั้งค่าทดสอบหนึ่งครั้งจะทำการทดสอบซ้ำ 10 ครั้งและนำมาหาค่าเฉลี่ยของแต่ละกรณีทดสอบ โดยแต่ละกรณีทดสอบจะทำการเลือกโหนดที่ทำการส่งข้อมูลที่แตกต่างกัน โดยผลทดสอบนี้ได้ทำการวัดเปอร์เซนของข้อความที่ Stationary mesh ส่งไปยัง Rescued mesh router และทำการส่งได้อย่างสำเร็จ โดยข้อความที่ส่งไม่สำเร็จเกิดมาจากการสูญหายของข้อความหรือการที่ระยะส่งข้อความนั้นห่างเกินกว่าระยะที่ได้ทำการตั้งค่าไว้

จากผลทดสอบแสดงให้เห็นว่าข้อความเกือบจะทั้งหมดได้มีการส่งจาก Stationary mesh router ไปยังผู้ช่วยเหลือได้อย่างสำเร็จ มีเพียงข้อความแค่ 2-3% เท่านั้นที่ไม่สามารถส่งได้อย่างสำเร็จโดยการส่งไม่สำเร็จส่วนมากนั้นเกิดมาจากระยะห่างในการส่งเกินกว่า 100 เมตร

ผลการทดสอบความสามารถในการส่งข้อมูลไปยังสถานีรับข้อมูล



รูปที่ 48 ผลการทดสอบความสามารถในการส่งข้อมูลไปยังสถานีรับข้อมูล

รูปที่ 48 แสดงความสามารถในการส่งข้อมูล ซึ่งสามารถวัดได้โดยการส่งข้อความจากโหนดไปยังสถานีรับข้อมูลที่ได้มีการตั้งไว้บนพื้นที่ทดสอบ การทดสอบนี้ทำการเปรียบเทียบความสามารถในการส่งข้อมูลไปยังระยะต่างๆโดยมีการเปลี่ยนแปลงค่าระยะที่ 300 เมตร, 500 เมตร, 800 เมตร, และ 1000 เมตร โดยแต่ละระยะก็ได้ทำการทดสอบเปลี่ยนค่าคาบเวลาในการส่งสัญญาณ ในการทดสอบแต่ละครั้งก็ได้ทำการทดสอบซ้ำ 10 ครั้งเช่นเดียวกันในทุกระยะทางและทุกค่าคาบเวลาในการส่งสัญญาณ การทดสอบนี้ได้ทำการเปรียบเทียบกับระบบเดิมที่ไม่ได้มีการติดตั้ง Middleware ไว้โดยระบบที่ไม่ได้มีการติดตั้ง Middleware นั้นจะใช้โปรโตคอล OLSR ในการส่งข้อความอย่างเดียว ดังนั้นจะทำให้ไม่มีสัญญาณ Heartbeat เข้ามารบกวนระบบเพิ่มเติม

จากผลทดสอบจะเห็นได้ว่าที่ระยะห่าง 300 เมตรจากสถานีรับข้อมูลนั้นการส่งข้อความจะสามารถส่งได้สำเร็จ 100% ในทุกค่าคาบสัญญาณ รวมถึงระบบดั้งเดิมด้วย แต่เมื่อระยะห่างเพิ่มเป็น 500 เมตรเป็นต้นไป ความสามารถในการส่งข้อความนั้นจะลดลงเหลือ 80% โดยที่เมื่อเทียบกับระบบเดิมแล้ว ระบบที่ได้มีการติดตั้ง Middleware เพิ่มขึ้นมานั้นมีความสามารถในการส่งข้อความไปยังสถานีรับข้อมูลใกล้เคียงกับระบบเดิมอย่างมาก ไม่มีความแตกต่างอย่างมีนัยสำคัญ สาเหตุที่ความสามารถในการส่งข้อมูลลดลงนั้นเนื่องมาจาก โปรโตคอล OLSR นั้นเป็นโปโตคอลที่ไม่มีกลไกในการส่งข้อความซ้ำเมื่อข้อความเกิดการสูญหาย เมื่อระยะทางเพิ่มขึ้น โอกาสที่ข้อความสูญหายจึงเพิ่ม

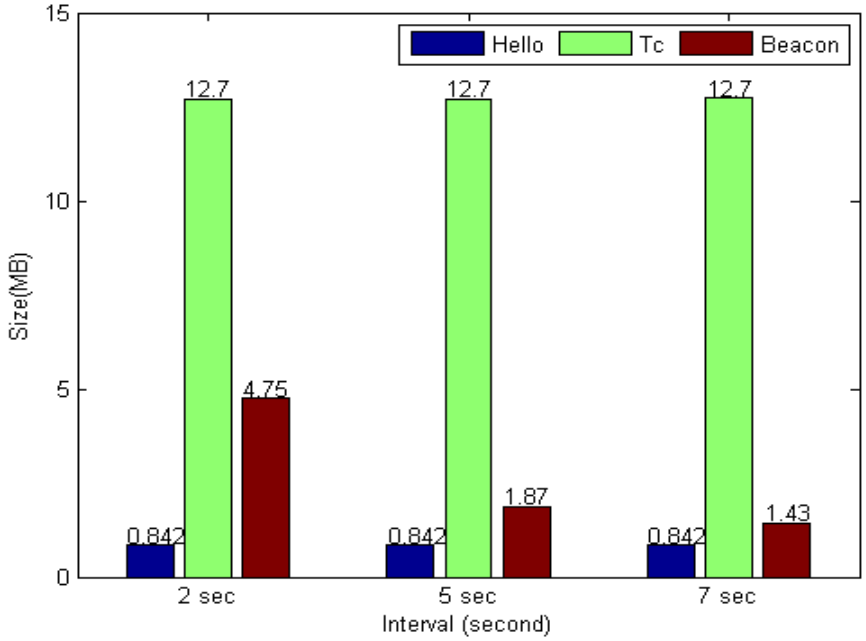
มากขึ้นด้วยโดยการสูญหายของข้อความส่วนมากจากการส่งข้อความในระยะทางมากเกินกว่าระยะสัญญาณ โดย 95% ของข้อความที่ไม่สามารถส่งได้เกิดจากการส่งข้อความมากกว่าระยะสัญญาณ

นอกจากนี้การเคลื่อนที่ของผู้ช่วยเหลือยังส่งผลต่อการส่งข้อความไปยัง Base station อีกด้วย ในการทดสอบนั้นได้ทำการตั้งค่าให้ผู้ช่วยเหลือมีการเคลื่อนที่และหยุดสลับกันโดยการเคลื่อนที่ของผู้ช่วยเหลือนั้นอาจส่งผลให้เกิดการส่งข้อความเกินระยะสัญญาณทำให้ข้อความไม่สามารถส่งได้เกิดการสูญหายของข้อความ โดยปัจจัยที่ส่งผลในการเคลื่อนที่คือ ความเร็วในการเคลื่อนที่ และระยะเวลาในการเคลื่อนที่และหยุดนิ่ง

ความเร็วในการเคลื่อนที่นั้นจะส่งผลต่อการสูญหายของข้อความเมื่อระยะห่างระหว่างโหนดที่เคลื่อนที่กับโหนดที่จะทำการแลกเปลี่ยนข้อมูลนั้นมีค่าใกล้เคียงกับระยะสัญญาณสูงสุด เนื่องจากว่าการค้นหาเส้นทางก่อนการส่งข้อความของโปรโตคอล OLSR นั้นจะสามารถเลือกเส้นทางที่สามารถส่งข้อความจากต้นทางไปปลายทางได้ก่อนการส่ง นั่นหมายความว่าเส้นทางนี่โปรโตคอล OLSR เลือกนั้นจะถูกทำการตรวจสอบเรียบร้อยแล้วว่าจะสามารถส่งข้อความได้ ดังนั้นการเคลื่อนที่จะส่งผลต่อช่วงเวลาสั้นๆก่อนส่งข้อความ ถ้าโหนดเคลื่อนที่เร็วมากก็จะสามารถทำให้ระยะห่างระหว่างโหนดมากกว่าระยะสัญญาณได้ หรือถ้าโหนดเคลื่อนที่ช้า แต่ว่าระยะห่างระหว่างโหนดก่อนส่งข้อความนั้นมีค่าใกล้เคียงกับระยะสัญญาณสูงสุดก็จะทำให้มีโอกาสที่โหนดจะมีระยะห่างมากกว่าระยะสัญญาณได้ส่งผลให้ข้อความที่ส่งนั้นสูญหาย

ระยะเวลาในการหยุดนิ่งก็มีผลต่อการส่งข้อความโดยที่ระยะเวลาหยุดนิ่งนั้นมีความเกี่ยวข้องกับอัตราการส่ง Tc Message ของโปรโตคอล OLSR ในขณะหยุดนิ่งโหนดจะทำการส่ง Tc Message เพื่อทำการเปลี่ยนแปลงตารางค้นหาเส้นทาง หลังจากที่โหนดมีการส่ง Tc Message แล้วนั้นถ้าโหนดมีการเคลื่อนที่ออกจากบริเวณเดิมจะทำให้ตารางค้นหาเส้นทางไม่ถูกต้องกับความเป็นจริงจะส่งผลให้การส่งข้อความล้มเหลวได้ แต่อย่างไรก็ตาม Tc Message จะถูกส่งออกมาเรื่อยๆทุกๆ 5 วินาทีทำให้ตารางค้นหาเส้นทางสามารถทำการเปลี่ยนแปลงได้ตลอดเวลา แต่ถ้าหากโหนดมีการเคลื่อนที่หลังจากส่ง Tc Message และมีการส่งข้อความภายใน 5 วินาทีก่อน Tc Message อีกข้อความจะถูกส่งออกมาจะทำให้มีโอกาสการส่งข้อความล้มเหลวได้เนื่องจาก Topology นั้นจะไม่ตรงกับตารางค้นหาเส้นทางนั่นเอง ถ้าหากโหนดหยุดนิ่งนานๆโหนด ที่เคลื่อนที่ก็จะทำหน้าที่เหมือนเสาสัญญาณหยุดนิ่งซึ่งจะทำให้การส่งสัญญาณมีความเสถียรมากขึ้น

ผลการทดสอบขนาด Overhead ของจำนวน Packet ของระบบ

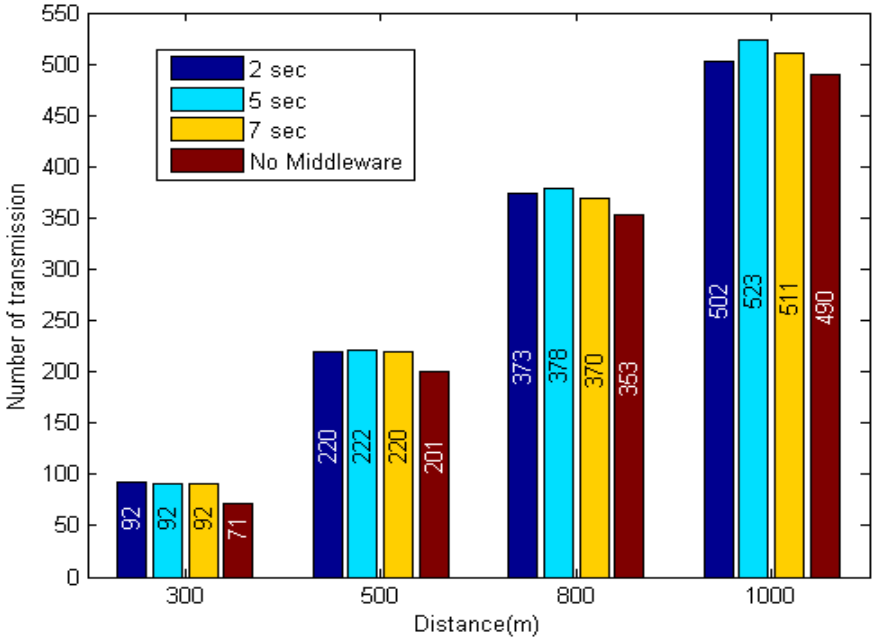


รูปที่ 49 ผลการทดสอบขนาดของ Overhead ของจำนวน Packet ของระบบ

การวัดขนาดของ Overhead ของจำนวน Packet ที่เพิ่มขึ้นมาในระบบนั้นสามารถวัดได้จาก Packet อื่นๆนอกจากข้อความที่ใช้ในการส่งจะถือว่าเป็น Overhead ของระบบทั้งหมด เนื่องจากโปรโตคอลที่ใช้นั้นเป็นโปรโตคอล OLSR ดังนั้น Overhead ของระบบนั้นจะมีเพียงแค่ Hello message, Topology control message, และ สัญญาณ Heartbeat ของ Middleware นั่นเอง ในการทดสอบนั้นได้ทำการเปรียบเทียบ Overhead ของ Middleware กับ Overhead ของ OLSR โดยมีการเปลี่ยนแปลงค่าคาบในการส่งสัญญาณของ Middleware ซึ่งผลทดสอบเป็นดังรูปที่ 49

ผลทดสอบแสดงให้เห็นว่า ขนาดของ Heartbeat message นั้นมีค่ามากกว่า Hello message แต่ว่าน้อยกว่าขนาดของ Tc message โดยขนาดของ Heartbeat message นั้นเทียบเป็น 35% ที่ค่าคาบเวลา 2 วินาที 13.8% ที่ค่าคาบเวลา 5 วินาที และ เป็น 10.8% ที่ค่าคาบเวลา 7 วินาที

ผลการทดสอบ Overhead ของจำนวนครั้งในการส่งข้อความ

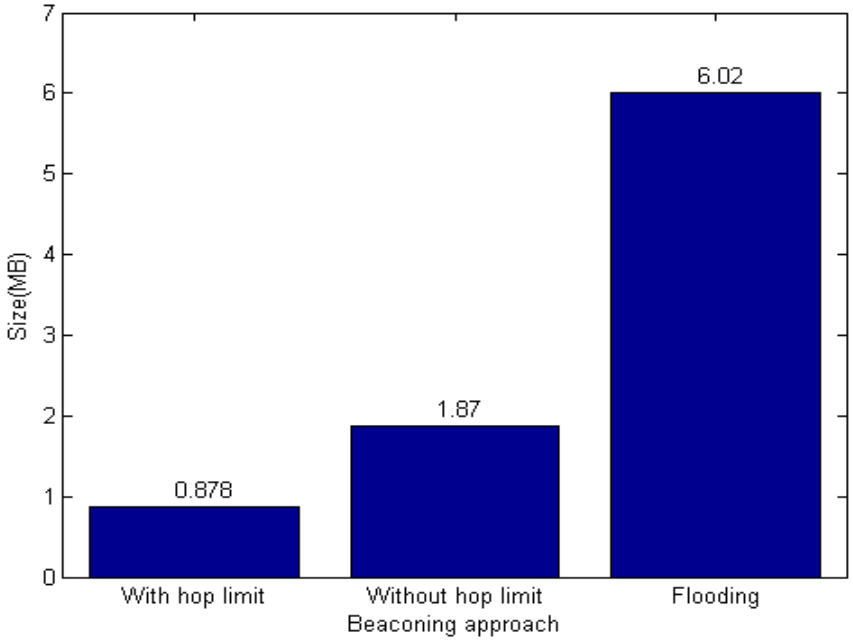


รูปที่ 50 ผลการทดสอบ Overhead ของจำนวนครั้งในการส่งข้อความ

Overhead ของจำนวนครั้งในการส่งข้อความนั้นหมายถึงการส่งต่อข้อความที่เป็นการส่งแล้วไม่ถึงผู้รับปลายทาง ซึ่งเมื่อมีการเพิ่ม Middleware เข้ามาในระบบนั้น กลไกการส่งสัญญาณ Heartbeat อาจจะมีผลในการเพิ่ม Overhead ของการส่งข้อความก็เป็นได้ การทดสอบนี้จึงได้ทำการวัดผลออกมาโดยทำการส่งข้อความจากโหนดในระบบไปยังสถานีรับข้อมูล และได้ทำการแบ่งประเภทของโหนดออกเป็น 4 ประเภทตามระยะห่างจากสถานีรับข้อมูล นอกจากนั้นยังได้ทำการเปลี่ยนค่าคาบเวลาในการส่งสัญญาณของกลไกการส่งสัญญาณด้วย ผลทดสอบนั้นได้นำมาเปรียบเทียบกันเองระหว่างค่าคาบเวลาต่างๆและยังเปรียบเทียบกับระบบเดิมที่ไม่มีการติดตั้ง Middleware ด้วย

ผลทดสอบในรูปที่ 50 นั้นแสดงให้เห็นว่าจำนวนครั้งในการส่งข้อความนั้นมีการเพิ่มขึ้นเรื่อยๆ ตามระยะห่างที่เพิ่มขึ้นจากสถานีรับข้อมูล เมื่อนำผลทดสอบมาเปรียบเทียบกันระหว่างระบบที่มีการติดตั้ง Middleware และระบบที่ไม่มีการติดตั้ง Middleware นั้นจะได้ว่า จำนวนครั้งการส่งข้อความของระบบที่ไม่มีการติดตั้ง Middleware นั้นมีค่าน้อยกว่า แต่อย่างไรก็ตามความแตกต่างของจำนวนครั้งในการส่งข้อความนั้นไม่ได้มีความแตกต่างกันอย่างมีนัยสำคัญ

ผลการทดสอบ Overhead ของกลไกในการส่งสัญญาณ



รูปที่ 51 ผลการทดสอบ Overhead ของกลไกในการส่งสัญญาณ

จากผลการทดสอบ 4 ผลการทดสอบข้างต้นนั้นจะเห็นได้ว่าเมื่อใช้คาบเวลาในการส่งสัญญาณอยู่ที่ 5 วินาทีนั้นจะทำให้การส่งข้อความนั้นมีประสิทธิภาพดีกว่าการใช้ค่าคาบเวลาอื่น อีกทั้ง Overhead ของการส่งสัญญาณนั้นเมื่อเปรียบเทียบกันกับค่าการส่งสัญญาณที่ 7 วินาทีนั้นค่า Overhead นั้นเพิ่มขึ้นมาไม่มาก แต่ว่าให้ประสิทธิภาพในการส่งข้อความมากกว่า ดังนั้นค่าคาบเวลาที่ 5 วินาทีจึงเป็นค่าที่เหมาะสมมาใช้ในการตั้งค่าในการทดสอบเพื่อทำการพัฒนากลไกในการส่งสัญญาณ

การพัฒนากลไกในการส่งสัญญาณนั้นได้ทำกระบวนการที่กล่าวไว้ในหัวข้อ 3.2.2 ซึ่งในผลทดสอบนี้จะแสดงให้เห็นถึง Overhead ของสัญญาณที่ลดลงจากระบบที่ไม่ได้มีการปรับปรุงกลไกในการส่งสัญญาณ โดยการทดสอบนี้จะทำการเปรียบเทียบกันระหว่างระบบที่ได้มีการพัฒนาการการจำกัดระยะทาง, ระบบที่ไม่ได้มีการจำกัดระยะทางในการส่ง, และระบบที่ใช้การแพร่กระจายแบบ Flooding ในการส่งสัญญาณ

การทดสอบนั้นจะเป็นกาวัดขนาดรวมของ Heartbeat packet ที่ระบบได้สร้างขึ้นมาโดยผลทดสอบนั้นได้แสดงดังรูปที่ 51 จากผลทดสอบจะเห็นว่าขนาดของ Heartbeat packet รวมของระบบที่ได้มีการปรับปรุงแล้วนั้นมีค่าลดลงอย่างมีนัยสำคัญ (ลดลงมากกว่า 50%) และเมื่อเทียบกับ Flooding แล้วนั้นจะมีค่าลดลงมากกว่า 85% เลยทีเดียว

ผลการทดสอบความทนทานของระบบ

Active node	Base Station PDR	Rescuer PDR	Total PDR
150	77%	99%	88%
200	73%	99%	86%
250	67%	99%	83%
300	67%	99%	83%

ตารางที่ 4 ผลทดสอบความทนทานของระบบ

ในการทดลอบนี้เป็นการทดสอบความทนทานของระบบเพื่อทดสอบหาประสิทธิภาพเมื่อระบบมีสภาพความหนาแน่นของเครือข่ายมากๆและมีข้อมูลในระบบมากๆ โดยจะทำการเพิ่มโหนดเข้าไปในระบบถึง 600 โหนดโดยประกอบด้วย Rescued mesh router 100 โหนด และ Stationary mesh router 500 โหนด ส่วนการตั้งค่าอื่นๆนั้นเหมือนกับการตั้งค่าของการทดสอบที่ได้กล่าวมาข้างต้น ในการทดสอบนี้มีการเพิ่มจำนวนโหนดที่ทำการส่งข้อมูลจาก 200 โหนด ถึง 300 โหนด โดยแต่ละโหนดที่มีการส่งข้อมูลจะทำการส่งข้อมูล 5 ครั้ง

จากผลทดลองแสดงให้เห็นว่าประสิทธิภาพการส่งข้อความไปถึงผู้ช่วยเหลือนั้นมีค่าประมาณ 99% ซึ่งใกล้เคียงกับระบบเมื่อมีจำนวนโหนดน้อยและมีการส่งข้อมูลน้อยเนื่องจากเป็นการส่งข้อความระยะใกล้จึงไม่ได้รับผลกระทบจากความหนาแน่นของโหนดในระบบและความหนานแน่นข้อมูลในระบบที่เพิ่มขึ้นมา แต่อย่างไรก็ตามประสิทธิภาพการส่งข้อความไปถึง Base station ลดลงเนื่องจากจำนวนโหนดที่เพิ่มขึ้น และความคับคั่งในระบบมากขึ้นทำให้เกิดการชนกันข้อการส่งข้อความ โดยผลทดสอบแสดงให้เห็นว่าเมื่อมีโหนดที่ทำการส่งข้อมูลเพิ่มขึ้นประสิทธิภาพในการส่งข้อความไปยัง Base station จะลดลงโดยเมื่อเพิ่มโหนดที่ส่งข้อความเป็น 200 โหนดจะมีประสิทธิภาพอยู่ที่ 73% และเมื่อเพิ่มจำนวนโหนดที่ส่งข้อความเป็น 250 โหนด และ 300 โหนดจะมีประสิทธิภาพในการส่งข้อความถึง Base station อยู่ที่ 67% ในความเป็นจริงแล้วเราสามารถตั้งค่า Channel ให้มีการส่งข้อมูลแบบ Multiple channel เพื่อลดการชนกันของข้อความได้ซึ่งอยู่นอกเหนือขอบเขตงานวิจัยนี้

วิเคราะห์การกระจายตัวแบบไร้รูปแบบของเสาสัญญาณในระบบ

การกระจายตัวของเสาสัญญาณในระบบที่ได้ทดลองนั้นเสาสัญญาณและผู้ช่วยเหลือได้มีการกระจายตัวทั่วทั้งพื้นที่การสื่อสารซึ่งผลทดลองได้ถูกแสดงข้างต้น แต่อย่างไรก็ตามบนพื้นที่ภัยพิบัตินั้นการกระจายตัวของเสาสัญญาณอาจจะไม่ได้เป็นการกระจายตัวแบบทั่วถึงทุกพื้นที่แบบที่ได้ทำการทดสอบ ในสถานการณ์ภัยพิบัติจริงการกระจายตัวของเสาสัญญาณอาจมีความเป็นกลุ่มเป็นก้อนในบางพื้นที่ และบางพื้นที่อาจไม่มีเสาสัญญาณติดตั้งอยู่ก็เป็นได้ซึ่งถ้าเสาสัญญาณมีการกระจายตัวเช่นนี้ผลทดลองที่กล่าวมาอาจจะมีการเปลี่ยนแปลงดังนี้

1) ความสามารถในการส่งข้อความไปถึงผู้ช่วยเหลือ

การส่งข้อมูลไปหาผู้ช่วยเหลือนั้นถ้าผู้ช่วยเหลือและเสาสัญญาณมีการกระจายตัวแบบเป็นกลุ่มก้อนนั้นการส่งสัญญาณไปยังผู้ช่วยเหลืออาจไม่มีการเปลี่ยนแปลงมาก เนื่องจากว่าบริเวณกลุ่มก้อนของเสาสัญญาณนั้นก็จะมีผู้ช่วยเหลือกระจายตัวอยู่เช่นกัน ดังนั้นความสามารถในการส่งข้อมูลไปยังผู้ช่วยเหลือจะมีค่าใกล้เคียงกับผลทดสอบ

2) ความสามารถในการส่งข้อความไปยัง Base station

เนื่องจากการกระจายตัวที่ไม่สม่ำเสมอของเสาสัญญาณนั้นทำให้มีผลต่อความสามารถในการส่งข้อความไปยัง Base station อย่างมีนัยสำคัญ การกระจายตัวที่ไม่สม่ำเสมอนั้นทำให้เสาสัญญาณแต่ละกลุ่มอยู่ห่างกันเกินระยะของสัญญาณซึ่งส่งผลให้ไม่สามารถส่งข้อความข้ามกลุ่มได้ ดังนั้นผู้ประสบภัยจึงอาจไม่สามารถส่งข้อความไปยัง Base station โดยตรงได้ ในการที่จะส่งข้อความไปยัง Base station จำเป็นจะต้องให้ผู้ช่วยเหลือทำหน้าที่ในการช่วยแลกเปลี่ยนข้อมูลระหว่างกลุ่มของเสาสัญญาณ โดยผู้ช่วยเหลือจะเก็บข้อความที่ได้รับจากผู้ประสบภัยไว้ เมื่อผู้ช่วยเหลือเดินทางเข้าไปยังบริเวณ Base station ผู้ช่วยเหลือก็จะทำหน้าที่ส่งต่อข้อความของผู้ประสบภัยไปยัง Base station

ในสถานการณ์ภัยพิบัติผู้ช่วยเหลืออาจจะทำการเดินทางไปเป็นกลุ่มซึ่งก่อให้เกิดการกระจายตัวของเสาสัญญาณในรูปแบบที่เป็นกลุ่มเป็นก้อนได้เนื่องจากเสาสัญญาณที่ใช้ในการสื่อสารของผู้ช่วยเหลือแต่ละคน แต่ในความเป็นจริงแล้วผู้ช่วยเหลือในกลุ่มไม่จำเป็นต้องใช้งานเสาสัญญาณทุกคน ถ้าหากต้องการสื่อสารในระยะการสื่อสารบริเวณใกล้เคียง จากความสามารถของระบบทดสอบระยะส่งสัญญาณสูงสุดของเสาสัญญาณอยู่ที่ 100 เมตร ดังนั้นถ้าผู้ช่วยเหลือไม่ได้เคลื่อนที่ห่างจากกลุ่มเกิน 100 เมตรก็ไม่มีความจำเป็นจะต้องเปิดการใช้งานเสาสัญญาณเนื่องจากจะทำให้มีความคับคั่งของระบบเพิ่มมากขึ้น

4.3 การวิเคราะห์ความปลอดภัยของระบบ

ระบบสื่อสารที่ได้ออกแบบมานั้นเป็นระบบสื่อสารที่มีความน่าเชื่อถือ ทำให้ผู้ใช้สามารถใช้งานระบบสื่อสารได้อย่างปลอดภัย ในหัวข้อนี้จะกล่าวถึงการวิเคราะห์ความปลอดภัยของระบบสื่อสารโดยการวิเคราะห์การโจมตีต่างๆที่สามารถเกิดขึ้นได้ในระบบ การโจมตีระบบสื่อสารนั้นสามารถเกิดขึ้นได้หลายรูปแบบ [20] แต่ละรูปแบบจะมีลักษณะที่แตกต่างกันออกไปดังนี้

1) การโจมตีการหาเส้นทางของระบบสื่อสาร (Routing path attacks)

การโจมตีการหาเส้นทางนั้นคือผู้โจมตีจะทำการเปลี่ยนเส้นทางการส่งข้อความ ทำให้ปลายทางไม่สามารถรับข้อความได้ซึ่งระบบสื่อสารในแบบ Peer-to-peer นั้นได้มีการใช้โปรโตคอลสื่อสารแบบแพร่กระจาย ทำให้การโจมตีประเภทนี้ไม่มีผล เนื่องจากว่าโปรโตคอลไม่จำเป็นจะต้องหาเส้นทางในการส่งข้อความ สำหรับระบบสื่อสารประเภทโครงสร้างพื้นฐานแบบผสมนั้น สำหรับระดับชั้นที่มีการส่งต่อข้อความคือชั้นของตัวกลางส่งข้อมูลซึ่งอุปกรณ์เราท์เตอร์ในชั้นนี้เชื่อมต่อเครือข่ายแอดฮอกกัน และได้มีการเข้ารหัสเครือข่ายไว้ด้วย WPA/WPA2 ซึ่งถ้าตั้งรหัสไว้เกิน 8 ตัวอักษรที่มีการผสมระหว่างตัวอักษรพิมพ์เล็กและพิมพ์ใหญ่อีกทั้งอักขระพิเศษนั้นการถอดรหัสจะเป็นไปได้ยากมาก ดังนั้นผู้โจมตีจึงไม่สามารถเข้าร่วมเครือข่ายชั้นนี้ได้ การโจมตีการค้นหาเส้นทางจึงไม่มีผลต่อระบบ

2) Sybil attacks [21]

การโจมตีประเภทนี้ผู้โจมตีจะครอบครอง Certificate หลายฉบับและนำ Certificate แต่ละฉบับไปใช้เพื่อหลอกลวงผู้ใช้อื่น ในระบบสื่อสารแบบ Peer-to-peer นั้นการยืนยันตัวตนแบบ Fully Trusted Mode จะไม่สามารถออก Certificate ให้กับผู้ใช้หนึ่งคนเกินหนึ่งฉบับได้ เพราะเป็นการออก Certificate โดยเจ้าหน้าที่ ซึ่งมีการตรวจสอบข้อมูลอย่างละเอียดก่อนแล้ว สำหรับการยืนยันตัวตนแบบ Half Trusted Mode นั้น ผู้โจมตีสามารถสร้าง Certificate ปลอมเพื่อใช้หลอกคนอื่นได้ แต่อย่างไรก็ตามผู้ใช้สามารถใช้กลไกการลดระดับความน่าเชื่อถือของผู้ไม่ประสงค์ดีได้ ทำให้ผู้ไม่ประสงค์ดีนั้นไม่สามารถได้รับความน่าเชื่อถือ สำหรับการสื่อสารแบบใช้โครงสร้างพื้นฐานแบบผสมนั้น Sybil attacks ไม่สามารถโจมตีระบบได้เนื่องจากว่าระบบนี้เป็นระบบที่ให้ผู้ใช้ส่งข้อความคุยกับเจ้าหน้าที่ได้โดยตรงโดยไม่จำเป็นต้องอาศัย Certificate ดังนั้นการโจมตีนี้จึงไม่เกี่ยวข้องกับระบบ

3) การโจมตีให้ปฏิเสธการถอดรหัสข้อความ (Denial of Decryption)

การโจมตีประเภทนี้ ผู้โจมตีจะทำการกีดกันปลายทางไม่ให้ปลายทางสามารถถอดรหัสข้อความได้โดยการเปลี่ยนแปลงข้อมูลของ Public key ที่ได้ส่งไปหาผู้รับปลายทาง สำหรับการ

สื่อสารแบบ Peer-to-peer บนเครือข่ายภัยพิบัตินั้นโปรโตคอลที่ออกแบบมาได้มีการแนบ Certificate ไปกับข้อความทุกฉบับที่ได้ทำการส่ง การที่จะโจมตีแบบระบบด้วยวิธีนี้นั้นจะต้องทำการเปลี่ยนแปลงข้อความทุกฉบับที่ส่งถึงผู้รับปลายทางถึงจะสามารถกีดกันการถอดรหัสได้ แต่อย่างไรก็ตามด้วยโปรโตคอลที่ออกแบบนั้นเป็นโปรโตคอลที่มีการส่งข้อความซ้ำ ทำให้ผู้รับปลายทางยังสามารถรับข้อความที่ถูกต้องจากเพื่อนบ้านได้ สำหรับการสื่อสารด้วยระบบโครงสร้างพื้นฐานแบบผสมนั้นไม่มีการเข้ารหัสข้อความ เนื่องจากข้อความส่งโดยตรงระหว่างผู้ประสบภัยกับเจ้าหน้าที่ ทำให้การโจมตีนี้ไม่มีผล

4) การลอกเลียน Certificate (Copy of Certificate)

ผู้โจมตีจะทำการลอกเลียน Certificate ของผู้ใช้งานและปลอมแปลงเป็นผู้ใช้งานคนดังกล่าว ซึ่งในระบบสื่อสารแบบ Peer-to-peer ที่ได้ออกแบบมานั้นได้มีการป้องกันการคัดลอก Certificate ไว้โดยอาศัยกลไกการเข้ารหัสด้วย Asymmetric key ผู้โจมตีไม่สามารถทราบ Private key ของผู้ใช้ได้ ทำให้การลอกเลียน Certificate นั้นไม่สมบูรณ์ไม่สามารถปลอมแปลงเป็นผู้ใช้งานคนอื่นได้นั่นเอง สำหรับการสื่อสารโดยใช้โครงสร้างพื้นฐานแบบผสมนั้นไม่ได้มีการใช้ Certificate ในการสื่อสา ดังนั้นการโจมตีนี้จึงไม่มีผล

5) การดัดแปลงข้อมูล (Modification of Data)

ในระหว่างการส่งข้อมูลจากผู้ส่งถึงผู้รับนั้น ข้อมูลอาจจะถูกเปลี่ยนแปลงได้ระหว่างทางโดยผู้ไม่ประสงค์ดี สำหรับการสื่อสารบนเครือข่าย Peer-to-peer บนพื้นที่ภัยพิบัตินั้นได้มีการส่งข้อความผ่านผู้ใช้ที่เป็นตัวกลาง แต่ว่าข้อความได้มีการเข้ารหัสด้วย Private key ไว้ ทำให้ผู้ใช้สามารถเปิดอ่านได้อย่างเดียว ไม่สามารถทำการแก้ไขข้อมูลได้ ดังนั้นการโจมตีนี้จึงไม่มีผลต่อระบบสื่อสารแบบ Peer-to-peer สำหรับการสื่อสารโดยใช้โครงสร้างพื้นฐานแบบผสมนั้นข้อความจะถูกส่งจากระดับชั้นผู้ใช้งานไปยังระดับชั้นตัวกลางส่งข้อมูล ซึ่งไม่มีการส่งผ่านตัวกลางที่เป็นผู้ใช้ การจะแก้ไขข้อมูลได้นั้นผู้โจมตีจำเป็นจะต้องเชื่อมต่อเข้ากับเครือข่ายของระดับชั้นส่งข้อมูลให้ได้เสียก่อน ซึ่งได้มีการเข้ารหัสของเครือข่ายไว้ด้วย WPA/WPA2 ดังที่ได้กล่าวไว้ ดังนั้นการโจมตีนี้จึงไม่สามารถทำได้บนเครือข่ายโครงสร้างพื้นฐานแบบผสม

6) การลดความน่าเชื่อถือของผู้ใช้ที่น่าเชื่อถือ (Blackmailing)

การโจมตีนี้จะเกี่ยวข้องกับระบบสื่อสารแบบ Peer-to-peer บนพื้นที่ภัยพิบัติเท่านั้น โดยผู้ไม่ประสงค์ดีอาจจะใช้กลไกในการลดระดับความน่าเชื่อถือในการลดระดับความน่าเชื่อถือของผู้อื่นได้

แต่อย่างไรก็ตามจากกลไกลดระดับความน่าเชื่อถือนั้น หากผู้ใช้กลไกนี้ไม่ได้เป็นผู้ที่ถูกเชื่อถือ นำหนักของเส้น Blacklist นั้นจะมีค่าแค่ 1 และสำหรับผู้ใช้ที่มีความน่าเชื่อถือนั้นจะมีผู้คนที่เชื่อถือมากอยู่แล้ว ผู้ใช้คนนั้นจะมีทั้งเส้นความน่าเชื่อถือ และเส้น Redeem ทำให้ระดับความน่าเชื่อถือมีมากกว่าเส้นลดระดับความน่าเชื่อถือ

7) การให้คำแนะนำที่ผิด (False Recommendation)

การโจมตีนี้เป็นการโจมตีที่มีแนวทางกลับกันกับการโจมตีแบบ Blackmailing โดยผู้ที่ไม่น่าเชื่อถือนั้นอาจสามารถถูกเพิ่มระดับความน่าเชื่อถือได้อีกครั้งโดยผู้ไม่ประสงค์ดี การทำงานของผู้ใช้ที่ไม่ประสงค์ดีนั้นอาจจะมีการทำงานเป็นกลุ่ม ทำให้สามารถเพิ่มระดับความน่าเชื่อถือของแต่ละคนได้อีกรอบ แต่อย่างไรก็ตาม จากกลไกการเพิ่มระดับความน่าเชื่อถือนั้น ถ้าผู้ที่ทำการเพิ่มระดับไม่ได้รับความน่าเชื่อถือ น้ำหนักของการเพิ่มระดับความน่าเชื่อถือก็จะมีค่าแค่ 1 ทำให้ต้องใช้กลุ่มคนจำนวนมากในการเพิ่มระดับความน่าเชื่อถือของผู้ที่ไม่น่าเชื่อถือ ซึ่งจะมีเส้น Blacklist มากเป็นทุนเดิมอยู่แล้วนั่นเอง ดังนั้นการทำ False Recommendation นั้นจึงเกิดขึ้นได้ยากในสังคมที่มีผู้คนไม่ประสงค์ดีน้อยกว่าผู้คนที่มีความน่าเชื่อถือ แต่ถ้าหากสังคมกลุ่มนั้นมีแต่คนที่ไม่มีความน่าเชื่อถือนั้น การโจมตีนี้จะสามารถเกิดขึ้นได้ง่ายและรวดเร็วมาก

8) การโยนข้อความทิ้ง (Dropping attacks)

การโจมตีประเภทนี้ เมื่อผู้ไม่ประสงค์ดีได้รับข้อความแล้วจะทำการโยนข้อความทิ้งและไม่ทำการส่งต่อ ทำให้ปลายทางไม่ได้รับข้อมูล ซึ่งการโจมตีประเภทนี้รวมไปถึง Blackhole attacks ซึ่งผู้ไม่ประสงค์ดีจะทำการโยนทิ้งทุกข้อความ Greyhole attacks ซึ่งผู้ไม่ประสงค์ดีจะทำการโยนทิ้งบางข้อความ สำหรับระบบสื่อสารแบบ Peer-to-peer บนเครือข่ายภัยพิบัตินั้นโปรโตคอลที่ออกแบบมาเป็นโปโตคอลที่มีกลการส่งซ้ำ ดังนั้นเมื่อข้อความถูกโยนทิ้งนั้นจึงไม่มีผล เพราะผู้รับยังสามารถรับข้อความที่ถูกต้องจากเพื่อนบ้านคนอื่นได้ สำหรับเครือข่ายโครงสร้างพื้นฐานแบบผสมนั้น ผู้ใช้ไม่ได้เป็นตัวกลางในการส่งข้อมูลทำให้การโยนข้อความทิ้งนั้นไม่มีผลต่อการส่งข้อความ แต่ว่าการที่ผู้ไม่ประสงค์ดีจะโจมตีระบบด้วยวิธีนี้ได้นั้นจำเป็นจะต้องเชื่อมต่อเข้ากับเครือข่ายตัวกลางในการส่งข้อมูลซึ่งมีการเข้ารหัสไว้ ผู้ไม่ประสงค์ดีจึงไม่สามารถเชื่อมต่อเครือข่ายได้ถ้าหากไม่ทราบรหัส การเจาะรหัสนั้นก็เป็นเรื่องที่ค่อนข้างจะยากถ้ามีการตั้งรหัสที่ดีเพียงพอ

9) การโจมตีรบกวนระบบ (Deny of Services)

การโจมตีประเภทนี้ ผู้โจมตีจะส่งข้อความออกมาเป็นจำนวนมากทำให้ระบบเกิดความคับคั่งและผู้ใช้ไม่สามารถส่งข้อความไปยังผู้ช่วยเหลือได้ สำหรับระบบสื่อสารแบบ Peer-to-peer บน

เครือข่ายภัยพิบัตินั้น โปรโตคอลที่ได้ออกแบบมาเป็นโปรโตคอลสื่อสารแบบแพร่กระจายทำให้การโจมตีประเภทนี้นั้นสามารถเกิดขึ้นได้ง่ายมาก โดยผู้ไม่ประสงค์ดีจะทำการส่งข้อความออกมา จากนั้นข้อความจะถูกแพร่กระจายออกไปเรื่อยๆทั่วทั้งเครือข่าย ทำให้ระบบเกิดความคับคั่งขึ้นมามากนั่นเอง ระบบสื่อสารแบบ Peer-to-peer บนพื้นที่ภัยพิบัตินั้นจึงไม่สามารถป้องกันการโจมตีประเภทนี้ได้ แต่อย่างไรก็ตามด้วยโปรโตคอลสื่อสารบนระบบสื่อสารแบบ Peer-to-peer มีกลไกในการส่งข้อความซ้ำ ดังนั้นจะช่วยลดการสูญหายของข้อความได้ สำหรับระบบสื่อสารโดยใช้โครงสร้างพื้นฐานแบบผสมบนพื้นที่ภัยพิบัตินั้น ผู้ใช้สามารถส่งข้อความออกมาอย่างต่อเนื่อง และข้อความจะถูกส่งไปยังผู้ช่วยเหลือที่ใกล้ที่สุด และส่งไปยังสถานีรับข้อมูล แต่อย่างไรก็ตามโปรโตคอลที่ใช้สื่อสารของระบบเป็นโปรโตคอล OLSR ซึ่งมีลักษณะการส่งแบบ Unicast ทำให้สามารถป้องกันการโจมตีประเภทนี้ได้ระดับหนึ่ง อีกทั้งต่อให้ผู้โจมตีนั้นส่งข้อความออกมามากเพียงพอทำให้ระบบคับคั่งมากจนกระทั่งผู้ใช้งานไม่สามารถส่งข้อความไปยังสถานีรับข้อมูลได้ ผู้ประสบภัยคนอื่นยังสามารถติดต่อกับเจ้าหน้าที่ที่อยู่ในบริเวณได้ด้วยกลไกการส่งข้อความของ Stationary mesh router นั่นเอง ดังนั้นการโจมตีประเภทนี้จึงเกิดขึ้นได้ยากบนระบบสื่อสารโดยใช้เครือข่ายโครงสร้างพื้นฐานแบบผสมถ้าผู้ใช้ใช้โจมตีจาก User layer

อย่างไรก็ตามถ้าหากผู้ที่จะทำการโจมตีระบบนั้นได้ทำการรบกวนสัญญาณบนชั้น Mesh layer จะส่งผลให้ Router บนชั้น Mesh layer บริเวณที่ถูกรบกวนสัญญาณไม่สามารถส่งข้อมูลได้หรือส่งข้อมูลได้ไม่ไกล ดังนั้นผู้ประสบภัยอาจไม่สามารถส่งข้อความไปยัง Base station ได้ แต่อย่างไรก็ตาม Stationary mesh router บริเวณที่ถูกรบกวนสัญญาณก็อาจจะสามารถส่งข้อความจากผู้ประสบภัยไปยัง Rescued mesh router ได้ดังผู้ประสบภัยยังมีโอกาสที่ได้รับความช่วยเหลือจากผู้ช่วยเหลือโดยขึ้นกับระดับการรบกวนสัญญาณ

10) Behavioral attacks

การโจมตีประเภทนี้ผู้ที่ทำการโจมตีจะตีบทเล่นสองหน้า ทำดีสลับกับทำไม่ดี ถ้าในการส่งข้อความนั่นก็จะหมายถึงเป็นการส่งข้อความที่น่าเชื่อถือสลับกับข้อความที่ไม่น่าเชื่อถือนั่นเอง ทำให้ผู้รับข้อความนั้นคาดเดายากว่าข้อความที่ได้รับนั้นมีความถูกต้องมากน้อยแค่ไหน การโจมตีนี้รวมไปถึง On-off attacks และ Conflicting behavior attacks สำหรับระบบสื่อสารแบบ Peer-to-peer นั้นด้วยกลไกของ Blacklisting และ Redeeming นั้นสามารถป้องกันการโจมตีนี้ได้แค่ระดับหนึ่งขึ้นกับวิจารณญาณของผู้รับข้อความว่าจะเชื่อถือข้อความมากน้อยเพียงใด แต่สำหรับระบบการสื่อสารโดยใช้โครงสร้างพื้นฐานแบบผสมนั้น การส่งข้อความจะถูกส่งไปยังเจ้าหน้าที่โดยตรง ดังนั้นผู้ที่จะถูกหลอกก็จะเป็นเจ้าหน้าที่นั่นเอง และถ้าเจ้าหน้าที่ที่ช่วยเหลือถูกหลอกทำให้โดนทำร้ายและแย่งชิง Rescued mesh router นั้นจะทำให้ผู้โจมตีสามารถรบกวนระบบได้ทั้งหมดด้วย Rescued

mesh router ที่ได้มา ดังนั้นระบบสื่อสารที่ออกแบบจึงสามารถป้องกันการโจมตีประเภทนี้ ได้แค่ระดับหนึ่งเท่านั้น

11) Social engineering

อย่างไรระดับความปลอดภัยของระบบจะลดลงถ้าหากมีผู้ไม่ประสงค์ดีสามารถแฝงตัวเข้ามาเป็นสมาชิกในทีมผู้ช่วยเหลือและได้รับรหัสจากทีมผู้ช่วยเหลือในการติดตั้งเสาสัญญาณ โดยผู้ไม่ประสงค์ดีนั้นสามารถนำเสาสัญญาณเทียมที่มีการเข้ารหัสเครือข่ายไว้มาติดตั้งเช่นเดียวกับเสาสัญญาณอื่น การโจมตีประเภทต่างๆจะสามารถเกิดขึ้นได้ไม่ว่าจะเป็น Routing path attacks, Dropping attacks หรือ Modification of data เสาสัญญาณของผู้ไม่ประสงค์ดีที่ทำการมาติดตั้งนี้อาจจะก่อให้เกิดการเปลี่ยนแปลงของรูปแบบการเชื่อมต่อได้ (Topology) โดยถ้าบริเวณที่มีการเปลี่ยนแปลงรูปแบบการเชื่อมต่อนั้นมีลักษณะเป็น Dense Networks นั่นคือมีจำนวนโหนดของเสาสัญญาณที่ถูกต้อง ณ บริเวณดังกล่าวมากการเปลี่ยนแปลงรูปแบบการสื่อสารอาจไม่ส่งผลกระทบมาก เนื่องจากข้อมูลที่ส่งจากผู้ประสบภัยนั้นสามารถใช้เส้นทางอื่นในการส่งข้อมูลทำให้ไม่กระทบต่อการส่งข้อมูล แต่ถ้าหากข้อมูลนั้นได้มีการส่งผ่านเสาสัญญาณของผู้ไม่ประสงค์ดี ข้อมูลอาจกมีการสูญหายหรือถูกดัดแปลงได้ สำหรับกรณีที่รูปแบบการเชื่อมต่อเป็น Sparse Networks เมื่อมีเสาสัญญาณจากผู้ไม่ประสงค์ดีที่แฝงตัวนำมาติดตั้งนั้นจะส่งผลกระทบต่อเครือข่ายการสื่อสารเป็นอย่างมากเพราะว่าการส่งสัญญาณในบริเวณ Sparse Network ซึ่งเป็นบริเวณที่มีเสาสัญญาณที่ทำงานถูกต้องอยู่ไม่หนาแน่น เมื่อมีการเปลี่ยนแปลง Topology โหนดที่ทำการส่งข้อความจึงมีทางเลือกไม่มากทำให้บางโหนดจำเป็นจะต้องส่งสัญญาณผ่านเสาสัญญาณของผู้ไม่ประสงค์ดีซึ่งก่อให้เกิดการสูญหายของข้อความหรือการเปลี่ยนแปลงของข้อความได้

รูปแบบการโจมตี	ระบบสื่อสารโดยใช้เครือข่าย Peer-to-peer	ระบบสื่อสารโดยใช้โครงสร้างพื้นฐานแบบผสม
Routing path attacks	✓	✓
Sybil attacks	✓	✓
Denial of Decryption	✓	✓
Copy of Certificate	✓	✓
Modification of Data	✓	✓
Blackmailing	✓	✓
False Recommendation	✓	✓
Dropping attacks	✓	✓
Deny of Services	!	!
Behavioral attacks	!	!
Social Engineering	!	!

ตารางที่ 5 ตารางสรุปความสามารถในการป้องกันการโจมตีของระบบสื่อสาร

ตารางที่ 5 นั้นได้สรุปความสามารถในการป้องกันการโจมตีของระบบสื่อสารที่ได้ทำการออกแบบไว้นั้นโดยเครื่องหมายถูกต้องนั้นจะหมายความว่าระบบสามารถป้องกันการโจมตีประเภทนั้นได้ แต่ถ้าเป็นเครื่องหมายอัศเจรีย์นั้นนั้นจะหมายความว่า ความสามารถในการป้องกันนั้นขึ้นกับสถานการณ์ว่าการโจมตีนั้นมีความรุนแรงมากน้อยเพียงใด ถ้าเป็นการโจมตีที่มีความรุนแรงมากอาจจะป้องกันไม่ได้ แต่ถ้าเป็นการโจมตีที่มีระดับความรุนแรงตั้งแต่เริ่มต้นถึงปานกลางนั้นระบบสามารถป้องกันได้

4.4 การวิเคราะห์คุณสมบัติของระบบการสื่อสาร

ในหัวข้อนี้จะกล่าวเกี่ยวกับคุณสมบัติของระบบสื่อสารแบบผสมเมื่อเทียบกับระบบสื่อสารที่มีอยู่ในปัจจุบัน โดยระบบสื่อสารที่มีอยู่ในปัจจุบันนี้เราจะแบ่งเป็น 2 ประเภทนั่นคือ ระบบสื่อสารแบบโครงสร้างพื้นฐานและระบบสื่อสารแบบ Peer-to-peer โดยคุณสมบัติของระบบนั้นได้มีการเปรียบเทียบดังนี้

Property	Infrastructure	Peer to peer	Hybrid
Stability	✓	✗	✓
Flexibility	✗	✓	✓
Compatibility	✓	✗	✓
Self-configure	✓	✓	✓
Self-healing	✗	✓	✓
Fast deployment	✗	✓	✓

ตารางที่ 6 ตารางเปรียบเทียบคุณสมบัติระบบสื่อสาร

ตารางที่ 6 แสดงการเปรียบเทียบคุณสมบัติต่างๆของระบบสื่อสาร โดยการเปรียบเทียบนั้นได้เลือกคุณสมบัติที่จำเป็นต่อระบบสื่อสารมาเปรียบเทียบ ระบบสื่อสารที่ดีนั้นจะต้องมีความเสถียรในการสื่อสาร นั่นคือสัญญาณในการสื่อสารนั้นต้องไม่ขาดหาย ผู้ใช้จะต้องสามารถส่งข้อความได้ต่อเนื่อง สำหรับระบบสื่อสารแบบใช้งานโครงสร้างพื้นฐานนั้นสามารถมีการสื่อสารที่มีความเสถียรได้เนื่องจากเสาสัญญาณนั้นไม่มีการเคลื่อนที่ ทำให้การส่งข้อความนั้นสามารถส่งได้ในระยะสัญญาณตลอดเวลาสัญญาณจึงไม่ขาดหาย แต่สำหรับระบบการสื่อสารแบบ Peer-to-peer นั้น การสื่อสารจะเป็นการสื่อสารผ่านอุปกรณ์สื่อสารผู้อื่นซึ่งสามารถเคลื่อนที่ได้ตลอดเวลา ทำให้การส่งข้อความบางครั้งนั้นไม่ได้อยู่ในระยะสัญญาณทำให้เกิดการสูญหายของข้อความได้ สำหรับระบบสื่อสารแบบผสมนั้น

โครงสร้างหลักของระบบสื่อสารนั้นประยุกต์มาจากระบบสื่อสารแบบเครือข่ายโครงสร้างพื้นฐานทำให้มีความเสถียรในการส่งข้อความในการสื่อสาร

ความยืดหยุ่นในการสื่อสารนั้นเป็นอีกหนึ่งคุณสมบัติที่มีความสำคัญในการสื่อสารในสถานการณ์ภัยพิบัติ ความยืดหยุ่นในการสื่อสารคือผู้ใช้งานสามารถใช้งานการสื่อสารได้หลากหลายบริเวณ ไม่จำเป็นจะต้องสื่อสารเฉพาะที่โล่งแจ้งเท่านั้น ซึ่งระบบสื่อสารแบบเครือข่ายโครงสร้างพื้นฐานนั้นไม่อาจจะตอบสนองผู้ใช้ในคุณสมบัตินี้ได้ เนื่องจากเสาสัญญาณนั้นจำเป็นจะต้องตั้งในที่โล่ง เมื่อเกิดเหตุภัยพิบัติขึ้นในบางบริเวณอาจจะไม่สามารถติดตั้งเสาสัญญาณได้ ทำให้บริเวณนั้นไม่สามารถเข้าถึงการสื่อสารได้ สำหรับระบบสื่อสารแบบ Peer-to-peer นั้นการสื่อสารไม่จำเป็นต้องขึ้นกับเสาสัญญาณ ผู้ใช้สามารถส่งสัญญาณผ่านอุปกรณ์สื่อสารผู้ใช้อื่นไปยังปลายทางได้ทำให้ผู้ใช้สามารถสื่อสารทุกบริเวณที่มีคนอยู่ ระบบสื่อสารแบบ Peer-to-peer จึงมีความยืดหยุ่นกว่าระบบสื่อสารแบบเครือข่ายโครงสร้างพื้นฐาน อย่างไรก็ตามระบบสื่อสารแบบผสมนั้นได้มีการนำ Rescued mesh router ที่สามารถเคลื่อนที่ได้เข้ามาใช้งานในระบบ ทำให้ระบบสื่อสารนั้นมีความยืดหยุ่นในการสื่อสารเพิ่มขึ้น เจ้าหน้าที่สามารถเคลื่อนที่ไปยังบริเวณต่างเพื่อให้การเชื่อมต่อการสื่อสารกับผู้ใช้ได้ อีกทั้งอุปกรณ์สื่อสารที่สามารถใช้งานเครือข่ายแอดฮอกได้นั้นก็สามารถเชื่อมต่อการสื่อสารผ่านเครือข่ายแอดฮอกได้เช่นกัน ทำให้ระบบนั้นได้รับความยืดหยุ่นในการสื่อสารที่สูงมาก เพราะเป็นการนำความสามารถของระบบสื่อสารทั้งสองชนิดมารวมกัน

เนื่องจากอุปกรณ์สื่อสารของผู้ใช้นั้นมีหลากหลายทำให้ต้องคำนึงถึงความเข้ากันได้ของอุปกรณ์สื่อสารกับระบบสื่อสาร ระบบสื่อสารแบบเครือข่ายโครงสร้างพื้นฐานนั้นสามารถให้การเชื่อมต่อการสื่อสารโดยผ่านการเชื่อมต่อแบบไวไฟ (WIFI) ซึ่งเป็นการเชื่อมต่อการสื่อสารที่เป็นมาตรฐานบนอุปกรณ์สื่อสารประเภท Smart device ในทุกรุ่น สำหรับระบบสื่อสารแบบ Peer-to-peer นั้นการเชื่อมต่อการสื่อสารนั้นจะทำได้โดยผ่านเครือข่ายแอดฮอก ซึ่งอุปกรณ์สื่อสารบางรุ่นนั้นไม่สามารถรองรับการเชื่อมต่อเครือข่ายแอดฮอกได้ แต่ระบบสื่อสารแบบ Peer-to-peer นั้นสามารถจำลองการเชื่อมต่อขึ้นมาโดยใช้สัญญาณบลูทูทหรือ WIFI Direct ก็ได้ แต่จะเป็นแค่การสื่อสาร Peer-to-peer แบบเสมือน ไม่มีคุณสมบัติเทียบเท่าเครือข่าย Peer-to-peer จริงๆ ดังนั้นการใช้งานเครือข่าย Peer-to-peer จึงมีปัญหาในด้านความเข้ากันได้กับอุปกรณ์สื่อสารนั่นเอง สำหรับระบบสื่อสารแบบผสมนั้นสามารถให้การเชื่อมต่อการสื่อสารกับอุปกรณ์สื่อสารผ่านการเชื่อมต่อแบบ WIFI ได้ และสำหรับอุปกรณ์สื่อสารที่รองรับการเชื่อมต่อแบบแอดฮอกนั้นก็สามารถใช้งานการสื่อสารแบบแอดฮอกได้ด้วยเช่นกัน ทำให้ระบบสื่อสารแบบผสมนั้นรองรับอุปกรณ์สื่อสารได้อย่างหลากหลาย

ในการวางระบบสื่อสารนั้น ผู้ติดตั้งระบบสื่อสารจะต้องตั้งค่าให้ระบบเพื่อให้สามารถใช้งานได้ และในระหว่างใช้งานนั้นระบบควรจะสามารถทำการเปลี่ยนแปลงการตั้งค่าของระบบเองเพื่อให้สอดคล้องกับสถานการณ์เช่นกัน ซึ่งตัวแปรต่างๆที่ใช้ในการตั้งค่าระบบนั้นขึ้นกับโปรโตคอลที่ใช้ใน

การสื่อสารซึ่งระบบสื่อสารที่ใช้งานอยู่นั้นจะมีโปรโตคอลที่ใช้ในการควบคุมระบบเพื่อเปลี่ยนค่าต่างๆ ให้สอดคล้องกับสถานกาณ์ ดังนั้นระบบทั้งสามแบบที่ได้นำมาเปรียบเทียบกันนั้นจึงสามารถทำการเปลี่ยนแปลงการตั้งค่าได้เองโดยขึ้นกับลักษณะของโปรโตคอลที่ได้นำมาติดตั้งนั่นเอง

ในระหว่างการสื่อสารนั้นระบบสื่อสารอาจจะเกิดความล้มเหลวในบางจุดได้ เช่นเกิดการชำรุดของเสาสัญญาณ ทำให้เกิดการขาดตอนของเส้นทางในการส่งข้อมูลเกิดขึ้น ด้วยเหตุการณ์เหล่านี้ระบบสื่อสารแบบ Peer-to-peer นั้นจะสามารถซ่อมแซ่มตัวเองได้ โดยเมื่อมีจุดที่อุปกรณ์สื่อสารของผู้ใช้บางคนไม่สามรถส่งข้อความต่อได้ ผู้ใช้คนอื่นสามารถเข้ามาแทนที่ในจุดนั้นได้อย่างง่ายดาย และไม่ต้องทำการตั้งค่าระบบใหม่ โดยโปรโตคอลจะเป็นตัวจัดการในการตั้งค่าระบบและหาเส้นทางในการส่งข้อมูลให้กับผู้ที่จะทำการส่งข้อความ แต่สำหรับระบบสื่อสารแบบใช้งานโครงสร้างพื้นฐานนั้น เมื่อมีเสาสัญญาณชำรุดเกิดขึ้น จำเป็นจะต้องหาเสาใหม่มาแทน ซึ่งตัวระบบเองไม่สามารถทำการซ่อมแซมตัวเองได้ อย่างไรก็ตามระบบสื่อสารแบบผสมนั้นสามารถนำข้อดีของระบบ Peer-to-peer เข้ามาปรับใช้งาน ซึ่ง Rescued mesh router นั้นจะสามารถเข้ามาซ่อมแซมเชื่อมต่อการสื่อสารในส่วนที่มีความชำรุดได้ ทำให้ระบบสื่อสารแบบผสมนั้นมีความสามารถในการซ่อมแซมตัวเองเมื่อระบบเกิดความผิดปกติขึ้นได้

ความซับซ้อนในการติดตั้งระบบนั้นก็เป็นอีกหนึ่งปัจจัยที่ควรคำนึง เนื่องจากเมื่อเกิดเหตุภัยพิบัติขึ้น ระบบสื่อสารควรจะสามารถทำให้ใช้งานได้เร็วที่สุด เพื่อที่จะได้ดำเนินการช่วยเหลือได้อย่างมีประสิทธิภาพ สำหรับระบบสื่อสารแบบใช้งานโครงสร้างพื้นฐานนั้น ผู้ช่วยเหลือจำเป็นจะต้องวางเสาสัญญาณให้เสร็จเรียบร้อยก่อนที่จะใช้งานระบบสื่อสาร ดังนั้นการใช้งานระบบสื่อสารแบบใช้งานโครงสร้างพื้นฐานนั้นจึงมีความซับซ้อนในการติดตั้งอย่างมาก เมื่อเทียบกับระบบสื่อสารแบบ Peer-to-peer นั้นเป็นระบบที่สามารถใช้งานได้ทันทีโดยไม่ต้องติดตั้งโครงสร้างพื้นฐาน ผู้ใช้เพียงแค่เปิดใช้งานอุปกรณ์สื่อสารก็สามารถติดต่อกับผู้ช่วยเหลือได้ทันที ดังนั้นความซับซ้อนในการติดตั้งระบบสื่อสารแบบ Peer-to-peer จึงมีความซับซ้อนน้อย สำหรับระบบสื่อสารแบบผสมนั้น ผู้ช่วยเหลือจะต้องทำการติดตั้งเสาสัญญาณบนพื้นที่ประสบภัย แต่อย่างไรก็ตามเนื่องจากระบบสื่อสารแบบผสมนั้นได้นำคุณสมบัติของระบบสื่อสารแบบ Peer-to-peer เข้ามารวมด้วยทำให้ระบบสื่อสารนั้นสามารถใช้งานได้โดยไม่จำเป็นจะต้องติดตั้งโครงสร้างพื้นฐานจนสมบูรณ์ ดังนั้นระบบสื่อสารแบบผสมนั้นจึงมีความสะดวกในการติดตั้งระบบบนพื้นที่ภัยพิบัติเช่นเดียวกับระบบสื่อสารแบบ Peer-to-peer

บทที่ 5 สรุปผลการวิจัย

งานวิจัยนี้ได้มีการเสนอโครงสร้างการสื่อสารสำหรับสถานการณ์ภัยพิบัติเนื่องจากพื้นที่ประสบภัยพิบัตินั้นมักจะมีการสูญเสียโครงสร้างพื้นฐานไปทำให้ผู้คนที่อยู่ในบริเวณไม่สามารถสื่อสารได้ โดยโครงสร้างการสื่อสารที่ได้นำเสนอในงานวิจัยนี้นั้นสามารถแบ่งออกเป็นสามส่วนคือส่วนสถานีรับข้อมูลจะทำหน้าที่ในการรับข้อมูลจากผู้ประสบภัยมาประมวลผลอีกทั้งยังทำหน้าที่ติดตามสถานการณ์และส่งผู้ช่วยเหลือเข้าไปช่วยในพื้นที่ประสบภัยพิบัติอีกด้วย ส่วนที่สองจะเป็นส่วนตัวกลางรับข้อมูล ส่วนนี้เป็นส่วนที่มีบทบาทในการส่งข้อมูลจากผู้ใช้มายังผู้ช่วยเหลือเนื่องจากผู้ใช้นั้นจะส่งข้อมูลผ่านผู้ช่วยเหลือโดยการส่งผ่านอุปกรณ์ในชั้นตัวกลางรับข้อมูล โดยในส่วนของตัวกลางรับข้อมูลนั้นจะถูกแบ่งออกเป็นสองส่วนหลักๆนั่นคือส่วนที่เป็นเสาสัญญาณอยู่นิ่ง (Stationary mesh router) และเสาสัญญาณเคลื่อนที่ (Resuced mesh router) ด้วยคุณสมบัติของโครงสร้างการสื่อสารที่มีการใช้เสาสัญญาณทั้งสองประเภทนั้นทำให้ผู้ใช้ได้รับการเชื่อมต่อการสื่อสารได้ทุกบริเวณอีกทั้งยังได้รับการสื่อสารที่มีประสิทธิภาพอีกด้วย ในส่วนที่สามจะเป็นระดับชั้นผู้ใช้งานซึ่งประกอบด้วยอุปกรณ์สื่อสารของผู้ประสบภัยและผู้ช่วยเหลือ เนื่องจากอุปกรณ์การสื่อสารของผู้คนในบริเวณพื้นที่ภัยพิบัตินั้นมีความหลากหลายดังนั้น ทำให้การสื่อสารในระดับชั้นนี้นั้นจะถูกแบ่งออกเป็นสองส่วนคือส่วนที่สามารถติดต่อสื่อสารกันแบบ Peer-to-peer ได้และส่วนที่ไม่สามารถติดต่อสื่อสารกันแบบ Peer-to-peer ได้ ผู้ใช้ทั้งสองกลุ่มสามารถสื่อสารกับเจ้าหน้าที่ผ่านเสาสัญญาณ และข้อความจะถูกส่งต่อไปยังเจ้าหน้าที่ แต่สำหรับผู้ใช้ที่สามารถสื่อสารแบบ Peer-to-peer ได้นั่นจะมีความสามารถมากขึ้น

ในส่วนของอุปกรณ์สื่อสารของผู้ใช้งานระบบสื่อสารในบริเวณที่ติดต่อสื่อสารแบบ Peer-to-peer ได้นั้นผู้คนในพื้นที่ประสบภัยจะสามารถสื่อสารไปยังผู้ช่วยเหลือโดยตรงผ่านโปรโตคอลสื่อสารบนเครือข่ายแอดฮอกได้ โดยโปรโตคอลสื่อสารบนเครือข่ายแอดฮอกนั้นมีการออกแบบมาให้สามารถสื่อสารได้อย่างปลอดภัย ผู้ที่ได้รับข้อความนั้นจะสามารถรับรู้ถึงระดับความน่าเชื่อถือของข้อความได้ทำให้ผู้ประสบภัยสามารถรับรู้สถานการณ์ที่ถูกต้องและใช้ข้อมูลที่ได้รับมาประกอบการตัดสินใจในสภาวะวิกฤติได้อย่างเหมาะสม โดยโปรโตคอลที่ออกแบบมานั้นสามารถให้ผู้ใช้งานยืนยันตัวตนได้สองรูปแบบนั่นคือยืนยันตัวตนผ่านเจ้าหน้าที่ และยืนยันตัวตนโดยใช้ความเชื่อใจจากผู้ใช้ด้วยกันเอง การยืนยันตัวตนผ่านเจ้าหน้าที่นั้นเป็นการยืนยันตัวตนแบบใช้ Certificate based นั่นคือเจ้าหน้าที่จะทำการส่งมอบ Certificate ให้กับผู้ใช้ผ่านทางโปรโตคอล จากนั้นผู้ใช้สามารถนำ Certificate ที่ได้ไปใช้ในการยืนยันตัวตนเมื่อต้องการจะส่งข้อมูล สำหรับผู้ใช้ที่ไม่สามารถติดต่อเจ้าหน้าที่ได้ก็จะสามารถยืนยันตัวตนได้ผ่านการเชื่อในของผู้ใช้ด้วยกัน ด้วยกลไกของ Half-Trusted Mode ทำให้ผู้ใช้สามารถ

ลงนามให้กับ Certificate ของผู้ใช้อื่นได้ ผู้ใช้สามารถวัดความน่าเชื่อถือผ่านกราฟยืนยันตัวตน โดยโหนดที่มีความน่าเชื่อถือคือโหนดที่มีเส้นทางไปยังโหนดผู้ใช้ นอกจากนั้นระบบการยืนยันตัวตนที่ได้ออกแบบมายังมีการทำระบบลงความเห็นสำหรับผู้ใช้ที่ให้ข้อมูลไม่ถูกต้อง โดยระบบลงความเห็นนั้นประกอบด้วยกัน 2 แบบคือ Blacklisting กับ Redeeming เมื่อผู้ใช้คนใดปล่อยข้อความที่ไม่น่าเชื่อถือออกมานั้น ผู้ใช้อื่นสามารถโหวดโดยใช้กลไกของ Blacklisting เพื่อลดความน่าเชื่อถือของผู้ใช้ดังกล่าวลง แต่เมื่อไรก็ตามที่ผู้ใช้ปล่อยข้อความที่มีความน่าเชื่อถือและเป็นประโยชน์ต่อผู้ใช้อื่น ผู้ใช้อื่นสามารถโหวดให้ผ่านกลไก Redeeming จะทำให้ผู้ใช้รายนั้นมีความน่าเชื่อถือมากขึ้น กลไก Redeeming ยังเป็นกลไกช่วยให้ผู้ใช้ที่ถูกลดความน่าเชื่อถือสามารถกลับมามีความน่าเชื่อถืออีกครั้งได้อีกด้วย

ในส่วนผลการทดลองนั้นได้มีการแบ่งการทดลองออกเป็นสองส่วนหลักนั่นคือผลทดลองฝั่งระบบโครงการสร้างสื่อสารและผลทดลองของโปรโตคอลสื่อสารบนเครือข่ายแอดฮอก ในส่วนโปรโตคอลที่ใช้สื่อสารบนเครือข่ายแอดฮอกนั้นเราได้แสดงให้เห็นว่าโปรโตคอลสามารถให้การสื่อสารที่มีความน่าเชื่อถือโดยที่มี package overhead ต่ำกว่าโปรโตคอลในการยืนยันตัวตนตัวอื่นที่ได้ถูกนำเสนอมา อีกทั้งยังวิเคราะห์ให้เห็นถึงการป้องกันจากการโจมตีแบบต่างๆที่จะเกิดขึ้นได้กับระบบ ในส่วนของโครงสร้างการสื่อสารนั้นได้มีการพัฒนาโครงสร้างการสื่อสารโดยใช้โปรโตคอล OLSR เป็นโปรโตคอลหลักในการส่งข้อมูล จากผลทดลองแสดงให้เห็นว่าผู้ใช้สามารถส่งข้อความไปยังเจ้าหน้าที่ได้ด้วยความสามารถในการส่งไม่ต่ำกว่า 97% อีกทั้งสามารถส่งข้อความไปยังสถานีรับข้อมูลด้วยความสามารถในการส่งไม่ต่ำกว่า 76% และยังแสดงให้เห็นว่าด้วยกลไกที่เพิ่มขึ้นมานั้นทำให้ Transmission overhead เพิ่มขึ้นอย่างไม่มีนัยสำคัญ

ในส่วนสุดท้ายเรายังแสดงการวิเคราะห์ระบบเปรียบเทียบกับโครงสร้างสื่อสารแบบใช้ Peer-to-peer และโครงสร้างสื่อสารที่ใช้เสาสัญญาณอย่างเดียว จากการวิเคราะห์เราได้แสดงให้เห็นว่าระบบเรานั้นสอดคล้องคุณสมบัติของระบบสื่อสารที่ดีนั่นคือสามารถให้การสื่อสารที่เสถียรและมีความยืดหยุ่นในการใช้งานนั่นคือ สามารถทำให้การสื่อสารเข้าถึงได้ในทุกบริเวณ นอกจากนั้นระบบที่ได้ออกแบบมานั้นยังสามารถติดตั้งระบบแบบ Incremental model ทำให้ระบบการสื่อสารที่ได้นำเสนอนั้นสามารถติดตั้งได้อย่างรวดเร็วสามารถนำไปใช้งานในพื้นที่ภัยพิบัติได้

รายการอ้างอิง

[1] Raspberry PI. [online]. (2015). Available from: http://www.raspberrypi.org/.[2015, January 21]

[2] The network simulator NS-3. [online]. (2015). Available from: http:/www.nsnam.org/. [2015, January 21]

[3] Jim Kurose, Keith Ross, *Computer Networking A Top Down Apporach*, 4th ed. 2007.

[4] C.E. Perkins and E.M. Royer, "Ad hoc on demand Distance Vector routing", mobile computing systems and applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, 1999, p90 -p100.

[5] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," RFC 3626, Oct. 2003.

[6] M. Bishop, *Introduction to Computer Security*, 1st ed. Addison Wesley Professional, 2004.

[7] ZIMMERMAN, P.: A proposed standard format for RSA cryptosystems',IEEE Computer. Magazine, 1986, pp. 21-34

[8]T. Ruengsatra, S. Phadungsilp, and K. Rojviboonchai, "Disaster Recovery System With a Hybrid Network," *The 2014 IEEE Student Conf. on Senior Capstone Project*, 2014.

[9] M. Raj, K. Kant, and S. K. Das, "E-DARWIN: Energy Aware Disaster Recovery Network using WiFi Tethering," in *Computer Communication and Networks (ICCCN), 2014 23rd International Conference on*, 2014, pp. 1–8.

[10] Y. Shibata, Y. Sato, N. Ogasawara, and G. Chiba, "A Disaster Information System by Ballooned Wireless Adhoc Network," 2009, pp. 299–304.

[11] W. Lu, W. K. G. Seah, E. W. C. Peh, and Y. Ge, "Communications Support for Disaster Recovery Operations using Hybrid Mobile Ad-Hoc Networks," 2007, pp. 763–770.

[12] M. M. Fouda, H. Nishiyama, R. Miura, and N. Kato, “On Efficient Traffic Distribution for Disaster Area Communication Using Wireless Mesh Networks,” *Wireless Personal Communications*, vol. 74, no. 4, pp. 1311–1327, Feb. 2014.

[13] A. Shamir. Identity-based cryptosystems and signature schemes. In CRYPTO 84, pages 47–53. Springer-Verlag, 1984. LNCS No. 196.

[14] S. S. Al-Riyami and K. Paterson. Certificateless public key cryptography. In ASIACRYPT 2003, pages 452–473. Springer-Verlag, 2003. LNCS No. 2894.

[15] J. K. Liu, M. H. Au, and W. Susilo, “Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model,” in *Proceedings of the 2nd ACM symposium on Information, computer and communications security*, 2007, pp. 273–283.

[16] S. Capkun, L. Buttyán, and J.-P. Hubaux, “Self-organized public-key management for mobile ad hoc networks,” *Mobile Computing, IEEE Transactions on*, vol. 2, no. 1, pp. 52–64, 2003.

[17] H. Dahshan and J. Irvine, “On demand self-organized public key management for mobile ad hoc networks,” in Vehicular Technology Conference, 2009. VTC Spring 2009. IEEE 69th, 2009, pp. 1–5.

[18] S. Choochotkaew and K. Piromsopa, “Development of a trustworthy authentication system in mobile ad-hoc networks for disaster area,” in *Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2014 11th International Conference on*, 2014, pp. 1–6.

[19] The bonnMonntion. [online]. (2015). Available from: http://sys.cs.uos.de/bonnmotion/. [2015, January 21]

[20] J.-H. Cho, A. Swami, and I.-R. Chen, “A Survey on Trust Management for Mobile Ad Hoc Networks,” IEEE Comm. Surveys & Tutorials, vol. 13, no. 4, pp. 562–583, 2011.

[21] S. Hashmi and J. Brooke, “Authentication Mechanisms for Mobile Ad-Hoc Networks and Resistance to Sybil Attack,” 2008, pp. 120–126.

ประวัติผู้เขียนวิทยานิพนธ์

นายธนภัทร เรืองสาตรา เกิดเมื่อวันที่ 8 กุมภาพันธ์ พ.ศ. 2535 สำเร็จการศึกษาระดับมัธยมที่โรงเรียนราชวินิตบางแก้วในพระบรมราชูปถัมภ์ จากนั้นได้เข้าศึกษาระดับปริญญาบัณฑิตที่ภาควิชาคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย และสำเร็จการศึกษาในปี พ.ศ. 2557