การเพิ่มขยายเครือข่าย UPnP และบริการกลุ่มสื่อสารปลอดภัย

Extensions to UPnP Networks and Secure Group Services

จักรพันธ์ สัวบุตร

Jakapan Surbot

วิทยานิพนธ์นี้สำหรับการศึกษาตามหลักสูตรปริญญา

วิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์

มหาวิทยาลัยสงขลานครินทร์

A Thesis Submitted in Fulfillment of the Requirements for the Degree of

Master of Engineering in Computer Engineering

Prince of Songkla University

2553

ชื่อวิทยานิพนธ์ การเพิ่มขยายเครือข่าย UPnP และบริการกลุ่มสื่อสารปลอดภัย
ผู้เขียน นายจักรพันธ์ สัวบุตร
สาขาวิชา วิศวกรรมคอมพิวเตอร์

อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	**คณะกรรมการสอบ**
…….....	……ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.สุนทร วิทูสุรพจน์)	(ดร.แสงสุรีย์ วสุพงศ์อัยยะ)
	……..…….กรรมการ
	(ผู้ช่วยศาสตราจารย์ ดร.สุนทร วิทูสุรพจน์)
	……..…….กรรมการ
	(ดร.สกุณา เจริญปัญญาศักดิ์)
	……..…….กรรมการ
	(ดร.วรวรรณ ดีอัซ การ์บาโย (มะเริงสิทธิ์))

บัณฑิตวิทยาลัย มหาวิทยาลัยสงขลานครินทร์ อนุมัติให้นับวิทยานิพนธ์ฉบับนี้สำหรับการศึกษา ตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์

……..……

(ศาสตราจารย์ ดร.อมรรัตน์ พงศ์ดารา)
คณบดีบัณฑิตวิทยาลัย

ชื่อวิทยานิพนธ์ การเพิ่มขยายเครือข่าย UPnP และบริการกลุ่มสื่อสารปลอดภัย

ผู้เขียน นายจักรพันธ์ สัวบุตร

สาขาวิชา วิศวกรรมคอมพิวเตอร์

ปีการศึกษา 2552

บทคัดย่อ

มาตรฐานยูพีแอนพี (UPnP ย่อมาจาก Universal Plug and Play) เป็นชุดโพรโทคอลการเชื่อมต่อเครือข่ายคอมพิวเตอร์ที่มีพื้นฐานสถาปัตยกรรมจากโพรโทคอลของเครือข่ายอินเทอร์เน็ตและเทคโนโลยีเว็บ เพื่อให้คอมพิวเตอร์หรืออุปกรณ์สื่อสารต่างๆ เชื่อมต่อเข้าด้วยกันได้อย่างอัตโนมัติ โดยไม่จำเป็นต้องกำหนดค่าไว้ล่วงหน้า อย่างไรก็ตาม เครือข่ายยูพีแอนพียังมีข้อด้อยสำคัญเชิงสถาปัตยกรรมซึ่งได้แก่ 1) การขาดกลไกสนับสนุนการสื่อสารแบบกลุ่มปลอดภัย และ 2) การไม่รองรับบริการจากอุปกรณ์สื่อสารที่อยู่ต่างประเภทเครือข่ายกันได้ ซึ่งวิทยานิพนธ์นี้ได้ศึกษาการแก้ไขปัญหาเหล่านี้ โดยนำกลไกทำงานของเทคนิคการยืนยันตัวตนแบบกลุ่มและกลไกชาญฉลาดของหน่วยทำงานเอเจนท์เข้ามาทำงานร่วมกัน การแก้ปัญหาเพื่อให้เครือข่ายยูพีแอนพีสนับสนุนการสื่อสารแบบกลุ่มปลอดภัยนั้น ได้นำเสนอการเพิ่มขยายโพรโทคอลที่เกี่ยวข้องกับกระบวนการค้นหาและเรียกใช้บริการ เพื่อสามารถให้บริการกลุ่มสื่อสารปลอดภัยในระดับชั้นบริการได้ โดยกลไกทำงานได้ใช้พื้นฐานการกระจายคีย์เพื่อการยืนยันตัวตนแบบคีย์พรีดิสทริบิวชัน (Key Pre-Distribution) ซึ่งประนีประนอมคุณลักษณะด้านการรักษาความปลอดภัยและความประหยัดทรัพยากรในการประมวลผล เพื่อให้ทำงานร่วมกับโพรโทคอลตามมาตรฐานเดิมได้ โดยได้นำเสนอกลไกประสานการทำงานร่วมกัน เพื่อการใช้บริการต่างๆ ของกลุ่มสื่อสารปลอดภัยได้แม้ว่าจะอยู่ต่างเครือข่ายกันก็ตาม นอกจากนั้น ยังได้ศึกษาการใช้ประโยชน์ของหน่วยทำงานแบบเอเจนท์ที่อยู่ในบริเวณเกตเวย์ของคู่เครือข่ายในการส่งต่อสถานะให้กับเครือข่ายต่างชนิดกันได้อีกด้วย โดยใช้กรณีศึกษาระหว่างเครือข่ายยูพีแอนพีและเครือข่ายโทรศัพท์พื้นฐาน ผ่านระบบสาธิตงานประยุกต์ทางการแพทย์เพื่อเฝ้าระวังเหตุการณ์ในเครือข่ายยูพีแอนพีจากระยะไกล เพื่อการแจ้งเตือนเป็นเสียงพูดในเครือข่ายโทรศัพท์ได้ แม้ว่าจะมีความแตกต่างกันในเชิงสถาปัตยกรรมก็ตาม

คำสำคัญ ยูพีแอนพี คีย์พรีดิสทริบิวชัน กลุ่มสื่อสารปลอดภัย

Thesis Title	Extensions to UPnP networks and Secure Group Services
Author	Mr. Jakapan Surbot
Major Program	Computer Engineering
Academic Year	2009

ABSTRACT

The Universal Plug and Play (UPnP) is a standard network architecture working on the basis of Internet protocols and Web technology for allowing computers or modern communication devices to be connected together without any configurations in priori. However, UPnP has two notable limitations. First, its infrastructure does not support any secured group communication. Second, it cannot provide any remote services for devices which located in different networks. The works in this thesis aim to tackle these limitations by means of secure group authentication techniques and smart mechanisms in agents. To enable secure group communication in the UPnP network, this work proposes to extend existing protocols related to service discovery and invocation processes. This is done with the Key Pre-Distribution technique, which has a good compromise between complexity and security. Therefore service level security can be provided even for using across networks. In addition, the collaboration of agents located at the UPnP and Telephony gateways is proposed for allowing UPnP event notification to be realized in a remote telephone network as a form of emergency call. As evidences, a demonstration of telemedical applications for remote monitoring has been developed so that the event notification from UPnP network can cause an alarm similar to an emergency phone call in the telephone network, where the architecture is not in common.

Keywords: UPnP, Key Pre-Distribution, Secure Group Communication

กิตติกรรมประกาศ

ขอแสดงคำขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร.สุนทร วิทูสุรพจน์ ประธานกรรมการที่ปรึกษางานวิจัย ที่ได้กรุณาอุทิศเวลาให้คำปรึกษา แนะนำความรู้ในด้านการทำวิจัย เอกสาร ข้อมูลต่างๆ เป็นอย่างดี รวมทั้งแนวความคิดและกำลังใจในการแก้ปัญหา ตลอดจนตรวจทานแก้ไขวิทยานิพนธ์ให้ดำเนินไปอย่างสมบูรณ์

ขอขอบพระคุณ ดร.แสงสุรีย์ วสุพงศ์อัยยะ ประธานกรรมการสอบวิทยานิพนธ์ ดร.สกุณา เจริญปัญญาศักดิ์ และ ดร.วรวรรณ ดีอัซ การ์บาโย (มะเริงสิทธิ์) กรรมการสอบวิทยานิพนธ์ ที่ได้กรุณาให้คำปรึกษา คำแนะนำ และตรวจทานวิทยานิพนธ์ให้ดำเนินไปอย่างสมบูรณ์

ขอขอบพระคุณ คณาจารย์และเจ้าหน้าที่ในภาควิชาวิศวกรรมคอมพิวเตอร์ทุก ๆ ท่านที่ให้ความช่วยเหลือในด้านต่างๆ มาโดยตลอด จนกระทั่งงานสำเร็จลุล่วง

ขอขอบพระคุณ บัณฑิตวิทยาลัย มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่ ที่ให้ความช่วยเหลือด้านการประสานงานต่าง ๆ

ขอขอบคุณ พี่ๆ เพื่อน ๆ และน้องๆ นักศึกษาปริญญาโท ภาควิชาวิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยสงขลานครินทร์ โดยเฉพาะกลุ่มงานวิจัยห้อง WIG ซึ่งมี นายกิติศักดิ์ วัฒนกุล นายกิตติ เชี่ยวชาญ นายพิทักษ์ เศวตสุนทร นายณัฐพล หนูฤทธิ นายฤทธิชัย จิตภักดีบดินทร์ และทุกท่านที่ได้ให้คำแนะนำ คำปรึกษา และเป็นกำลังใจที่ดีมาโดยตลอด

สุดท้ายนี้ ข้าพเจ้าขอน้อมรำลึกถึงพระคุณของบิดา มารดา และน้องสาวของข้าพเจ้า ที่ส่งเสริมสนับสนุน ให้คำแนะนำ ให้คำปรึกษา ให้กำลังใจ และทุนทรัพย์แก่ข้าพเจ้าตลอดมา จนกระทั่งทำให้ข้าพเจ้าประสบความสำเร็จ

จักรพันธ์ สัวบุตร

สารบัญ

หน้า

บทคัดย่อ.....(3)

ABSTRACT.....(4)

กิตติกรรมประกาศ.....(5)

สารบัญ.....(6)

สารบัญตาราง.....(9)

สารบัญภาพประกอบ.....(10)

บทที่ 1 บทนำ.....1

1.1 ความสำคัญ และที่มาของวิทยานิพนธ์.....1

1.2 วัตถุประสงค์.....3

1.3 ขอบเขตของการวิจัย.....3

1.4 ขั้นตอนการวิจัยและวิธีการวิจัย.....4

1.5 ประโยชน์ที่คาดว่าจะได้รับ.....4

1.6 โครงสร้างของวิทยานิพนธ์.....5

บทที่ 2 การตรวจเอกสาร.....6

2.1 เทคโนโลยีที่เกี่ยวข้อง.....6

2.1.1 สถาปัตยกรรมและโพรโทคอลสื่อสารของเครือข่ายยูพีแอนพี.....6

2.1.2 กระบวนการค้นหาบริการภายในเครือข่ายยูพีแอนพี.....7

2.1.3 กระบวนการแจ้งเตือนเหตุการณ์.....9

สารบัญ (ต่อ)

หน้า

2.1.4 กลไกการยืนยันตัวตนสำหรับกลุ่มสื่อสารปลอดภัย 11
2.1.5 การเปรียบเทียบคุณลักษณะระหว่างเทคนิควิธีพีเคไอกับเคพีดี 15
2.1.6 เกตเวย์โทรศัพท์ที่พัฒนาด้วยซอฟต์แวร์แอสเทอริสก์ 16
2.2 งานวิจัยที่เกี่ยวข้อง 17
2.2.1 การรองรับบริการแบบกลุ่มสื่อสารปลอดภัยบนระบบเครือข่ายยูพีแอนพี 17
2.2.2 การยืนยันตัวตนผ่านศูนย์กลางแบบพลวัตในกลุ่มสื่อสารปลอดภัย 19
2.2.3 การเพิ่มขยายเครือข่ายยูพีแอนพีด้วยหน่วยการทำงานเอเจนท์ 20
บทที่ 3 วิธีดำเนินการวิจัย 22
3.1 การออกแบบกลไกบริการสำหรับกลุ่มสื่อสารปลอดภัยในเครือข่ายยูพีแอนพี 22
3.1.1 แนวความคิดและสถาปัตยกรรมระบบ 22
3.1.2 การเพิ่มขยายโพรโทคอลที่เกี่ยวข้องเพื่อรองรับกลุ่มสื่อสารปลอดภัย 25
3.2 การออกแบบกลไกประสานการทำงานระหว่างเอเจนท์ของคู่เครือข่าย 29
3.2.1 แนวความคิดและสถาปัตยกรรมระบบ 29
3.2.2 กรณีศึกษา: การเตือนด้วยเสียงพูดไปยังเครื่องโทรศัพท์ที่ต้องการ 31
บทที่ 4 ผลการวิจัย 37
4.1 ผลการศึกษาเปรียบเทียบเทคนิควิธียืนยันตัวตนอุปกรณ์ 37
4.1.1 สภาพแวดล้อมการทดสอบและวัดผล 37
4.1.2 การวิเคราะห์ผล 39
4.2 ผลการทดสอบกลไกบริการกลุ่มสื่อสารปลอดภัยที่พัฒนาขึ้น 40

สารบัญ (ต่อ)

หน้า

4.2.1 การศึกษาด้านระยะการหน่วงเวลาของการเข้าร่วม/ออกกลุ่มสื่อสาร 40

4.2.2 การศึกษาด้านการสนับสนุนงานกลุ่มสื่อสารข้ามเครือข่าย 41

4.3 ผลการศึกษากลไกประสานงานระหว่างเครือข่ายโทรศัพท์และยูพีแอนพีที่พัฒนาขึ้น 43

4.3.1 สภาพแวดล้อมการทดสอบ 43

4.3.2 ผลการทดสอบ 44

4.4 กรณีศึกษา: การประยุกต์ทางการแพทย์เพื่อดูแลผู้สูงอายุระยะไกล 45

บทที่ 5 บทสรุปและข้อเสนอแนะ 47

5.1 สรุปผลการวิจัย 47

5.2 ข้อเสนอแนะ 48

เอกสารอ้างอิง 49

ภาคผนวก 52

ภาคผนวก ก. ผลงานตีพิมพ์เผยแพร่จากวิทยานิพนธ์ 53

ประวัติผู้เขียน 70

สารบัญตาราง

หน้า

ตารางที่ 2.1 เวลาที่ใช้ในการถอดรหัสของอัลกอริทึมที่ใช้คีย์แบบสมมาตร 16
ตารางที่ 2.2 สรุปการเปรียบเทียบงานวิจัยที่เกี่ยวข้องกับแนวทางวิจัย 18
ตารางที่ 3.1 ขั้นตอนการสื่อสารของกลุ่มสื่อสารปลอดภัยกับของเครือข่ายยูพีแอนพี 24
ตารางที่ 4.1 ผลทดสอบระยะเวลาประมวลผลที่ใช้ในกระบวนการยืนยันตัวตนอุปกรณ์ 39

สารบัญภาพประกอบ

หน้า

รูปที่ 2.1 ระดับชั้นโพรโทคอลของเครือข่ายยูพีแอนพี 6
รูปที่ 2.2 ลำดับของกระบวนการเพื่อเชื่อมต่อเข้าเป็นเครือข่ายยูพีแอนพี 7
รูปที่ 2.3 ตัวอย่างข้อความค้นหาบริการ กรณีหน่วยควบคุมเชื่อมต่อเข้าสู่เครือข่าย 8
รูปที่ 2.4 ตัวอย่างข้อความประกาศบริการ กรณีอุปกรณ์เชื่อมต่อเข้าสู่เครือข่าย 9
รูปที่ 2.5 ตัวอย่างข้อความสมัครเพื่อรับแจ้งเตือนเหตุการณ์ 10
รูปที่ 2.6 ตัวอย่างข้อความแจ้งเตือนเหตุการณ์ 10
รูปที่ 2.7 การยืนยันตัวตนด้วยเทคนิควิธีการเข้ารหัสแบบพีเคไอ 12
รูปที่ 2.8 การยืนยันตัวตนด้วยเทคนิควิธีเคพีดี 13
รูปที่ 2.9 อัลกอริทึมของบลอมในการคำนวณคีย์คู่ระหว่างอุปกรณ์ i และ j 14
รูปที่ 2.10 การควบคุมการทำงานผ่านไฟล์ของซอฟต์แวร์แอสเทอริสก์ 17
รูปที่ 2.11 การจำแนกเทคนิคการยืนยันตัวตนผ่านศูนย์กลาง 19
รูปที่ 2.12 การเพิ่มขยายเครือข่ายยูพีแอนพีด้วยหน่วยการทำงานเอเจนท์ 20
รูปที่ 3.1 ลำดับชั้นโพรโทคอลของเอสจี-ยูพีแอนพี บนมาตรฐานของเครือข่ายยูพีแอนพี 23
รูปที่ 3.2 ลำดับการเปลี่ยนสถานะของการทำงานในเครือข่ายเอสจี-ยูพีแอนพี 23
รูปที่ 3.3 ข้อความ NOTIFY ที่ถูกปรับแต่ง 25
รูปที่ 3.4 การเลือกหัวหน้ากลุ่มสื่อสารของเครือข่ายเอสจี-ยูพีแอนพี 26
รูปที่ 3.5 การค้นหาหัวหน้ากลุ่มสื่อสารของเครือข่ายเอสจี-ยูพีแอนพี 27
รูปที่ 3.6 ลำดับการสื่อสารเพื่อยืนยันตัวตนอุปกรณ์ 28
รูปที่ 3.7 สถาปัตยกรรมประสานงานของหน่วยการทำงานแบบเอเจนท์ 30
รูปที่ 3.8 แผนภาพที่ใช้แสดงคลาสของหน่วยควบคุม 31
รูปที่ 3.9 ตัวอย่างซอร์สโค้ดของฟังก์ชัน EventListener 32
รูปที่ 3.10 แผนภาพที่ใช้แสดงคลาสของสคริปต์เอจีไอ 32

สารบัญภาพประกอบ (ต่อ)

หน้า

รูปที่ 3.11 ตัวอย่างซอร์สโค้ดของคลาส HelloAgiScript 34
รูปที่ 3.12 ตัวอย่างข้อความในคอลไฟล์ 34
รูปที่ 3.13 ตัวอย่างการกำหนดค่าไดออลแพลน 35
รูปที่ 3.14 ลำดับการทำงานของกลไกแจ้งเตือนเหตุการณ์ 35
รูปที่ 4.1 ระบบทดสอบการยืนยันตัวตนอุปกรณ์ 38
รูปที่ 4.2 ผลการเปรียบเทียบระยะเวลาการเข้าร่วมกลุ่มสื่อสาร 41
รูปที่ 4.3 ผลการเปรียบเทียบระยะเวลาการออกจากกลุ่มสื่อสาร 41
รูปที่ 4.4 ระบบทดสอบกลไกทำงานกลุ่มสื่อสารปลอดภัยข้ามเครือข่าย 42
รูปที่ 4.5 ตัวอย่างกลุ่มสื่อสารแบบปลอดภัยของระบบทดสอบ 42
รูปที่ 4.6 หน้าต่างแสดงสถานะอุปกรณ์ต่างๆ ภายในกลุ่มสื่อสารปลอดภัยเดียวกัน 43
รูปที่ 4.7 สภาพแวดล้อมการทดสอบระบบแจ้งเตือนเหตุการณ์ผ่านเครือข่ายโทรศัพท์ 43
รูปที่ 4.8 แผนภาพแสดงกิจกรรมของการแจ้งเตือนเหตุการณ์ผ่านเครือข่ายโทรศัพท์ 44
รูปที่ 4.9 ลำดับการทดสอบระบบดูแลผู้สูงอายุระยะไกล 45

บทที่ 1
บทนำ

1.1 ความสำคัญ และที่มาของวิทยานิพนธ์

ปัจจุบันความแพร่หลายของเทคโนโลยีด้านการสื่อสารไร้สาย และอุปกรณ์คอมพิวเตอร์ชนิดพกพา ได้ส่งผลให้เกิดการขยายตัวของเครือข่ายโทรคมนาคมกันอย่างกว้างขวาง จนเอื้อให้สามารถนำคอมพิวเตอร์ไปใช้งานได้หลายสถานที่และเวลา ทั้งในสถานที่ทำงานหรือบ้านพักอาศัย โดยเฉพาะอย่างยิ่งในสภาพแวดล้อมของบ้านสมัยใหม่แบบอัจฉริยะหรือสมาร์ทโฮม (Smart Home) นั้น อุปกรณ์สื่อสารหรือเครื่องใช้ไฟฟ้าแบบใหม่ซึ่งได้รับการพัฒนาให้รองรับมาตรฐานยูพีแอนพี (UPnP ย่อมาจาก Universal Plug and Play) [1] เพื่อให้มีคุณลักษณะเด่นทางด้านการเชื่อมต่อเข้ากันเป็นเครือข่ายได้อย่างอัตโนมัติ โดยที่ไม่จำเป็นต้องมีการตั้งค่าล่วงหน้า (Zero Configuration) เช่น ค่าหมายเลขไอพี (IP Address) ของอุปกรณ์นั้นๆ หรือของอุปกรณ์เกตเวย์เครือข่าย เป็นต้น ดังนั้น เมื่อมีการประกาศแจ้งลักษณะบริการ หรือค้นหาบริการจากอุปกรณ์ต่างๆ ภายในเครือข่าย จึงกระทำได้โดยสะดวกมากขึ้น

อย่างไรก็ตาม เนื่องจากกลไกสนับสนุนเพื่อให้ทำงานเป็นเครือข่ายอัตโนมัติตามมาตรฐานยูพีแอนพี จะมีจุดมุ่งหมายในการสนับสนุนการใช้งานระหว่างอุปกรณ์ภายในเครือข่ายส่วนบุคคลขนาดเล็ก (Small Private Network) จึงให้ความสำคัญด้านการรักษาปลอดภัยเพียงเฉพาะแบบพื้นฐาน รวมถึงการเลือกใช้โพรโทคอลที่ทำงานอยู่บนพื้นฐานการกระจายสัญญาณแบบบรอดคาสก์ (Broadcast) เพื่อลดความซับซ้อนของโพรโทคอลที่พัฒนาขึ้นใหม่ในกระบวนการต่างๆ ภายในเครือข่ายยูพีแอนพีลง จึงส่งผลทำให้เกิดข้อด้อยเชิงสถาปัตยกรรมบางประการ ที่ไม่เอื้อต่อการสนับสนุนงานประยุกต์บางลักษณะ ดังนี้

1) ปัญหาด้านการไม่รองรับบริการแบบกลุ่มสื่อสารปลอดภัย

เนื่องจาก ข้อกำหนดด้านการให้บริการแบบสื่อสารปลอดภัยตามมาตรฐานเครือข่ายยูพีแอนพี [2] ได้กำหนดแนวทางไว้เฉพาะเพียงการให้บริการการรักษาความปลอดภัยแบบยูนิคาสก์ (Unicast) ระหว่างอุปกรณ์คู่สื่อสารหนึ่งๆ เท่านั้น จึงสร้างภาระงานที่ไม่จำเป็นในการสร้างช่อง

ทางการสื่อสารแบบปลอดภัย (Secure Channel) ระหว่างอุปกรณ์ทีละคู่ๆ จนครบตามจำนวนทั้งหมดที่มีอยู่ภายในระบบ เพื่อให้สามารถใช้บริการในลักษณะของกลุ่มสื่อสารได้ เป็นที่น่าสังเกตว่า ปัญหาดังกล่าวนี้ก็ยังคงมีอยู่ในปัจจุบัน แม้ว่าจะได้มีงานวิจัยที่พยายามแก้ไขปัญหานี้เช่นเดียวกัน ตัวอย่างเช่น Lee และคณะ [3] เสนอให้มีการนำเครื่องแม่ข่ายเข้ามาใช้งาน เพื่อทำหน้าที่เป็นศูนย์กลางในการกระจายคีย์ข้อมูล (Secret Key) ซึ่งใช้สำหรับถอดรหัสข้อมูลกับอุปกรณ์ทั้งหมดภายในกลุ่ม อย่างไรก็ตาม กลไกทำงานที่นำเสนอในงานวิจัยดังกล่าวยังมีข้อด้อยดังต่อไปนี้

- ปัญหาการล่มสลายของทั้งระบบจากความล้มเหลวของเครื่องแม่ข่ายเพียงที่เดียวเท่านั้น (Single Point of Failure) ซึ่งเป็นผลจากลักษณะการทำงานแบบมีศูนย์กลางของการสื่อสารทั้งระบบ นอกจากนั้น ในกรณีที่ระบบศูนย์กลางถูกเจาะ (Single Point of Attack) ก็อาจส่งผลต่อเสถียรภาพของระบบโดยรวมได้ง่าย
- ปัญหาการออกแบบโพรโทคอลพิเศษ (Proprietary Protocol) เพื่อสื่อสารระหว่างสมาชิกของกลุ่มโดยใช้ช่องทางสื่อสารพิเศษแบบปลอดภัย จึงสร้างปัญหาความเข้ากันไม่ได้ระหว่างโพรโทคอลที่นำเสนอขึ้นใหม่กับของมาตรฐานเดิม (Backward Compatability Problem) นอกจากนั้น ยังเกิดความสิ้นเปลืองในการนำระบบไปใช้งานอีกด้วย

งานวิจัยในวิทยานิพนธ์นี้จะได้พิจารณาแนวทางที่สามารถหลีกเลี่ยงปัญหาในงานวิจัยข้างต้น โดยศึกษาการนำเทคนิคการกระจายคีย์ข้อมูลเพื่อการยืนยันตัวตน และเทคนิคการเข้ารหัสแบบกลุ่มที่เหมาะสมเข้ามาประยุกต์ใช้งาน นอกจากนี้ ยังจะได้ศึกษากระบวนการค้นหาและประกาศแจ้งบริการเพื่อที่จะนำเทคนิคที่ศึกษาข้างต้นเข้ามาร่วมทำงาน เพื่อเป็นการเพิ่มขยายโพรโทคอลที่เกี่ยวข้องกับมาตรฐานเครือข่ายยูพีแอนพีแทนการพัฒนาขึ้นใหม่ดังเช่นที่พบในงานวิจัยอื่น

2) ปัญหาด้านการให้บริการกับอุปกรณ์ที่อยู่ต่างเครือข่ายกัน

เนื่องจาก ข้อจำกัดทางสถาปัตยกรรมของเครือข่ายที่ทราฟิกของการกระจายข้อมูลแบบมัลติคาสก์จะไม่สามารถถูกส่งกระจายข้ามออกไปยังเครือข่ายภายนอกได้นั้น ส่งผลทำให้ข้อมูลภายในกระบวนการต่างๆ เช่น การค้นหา และการประกาศแจ้งบริการของเครือข่ายยูพีแอนพีหนึ่งๆ ไม่สามารถใช้งานจากอุปกรณ์ที่อยู่ต่างเครือข่ายกันได้โดยตรง งานวิจัยเป็นจำนวนมากจึงได้พยายามเสนอกลไกทำงานเพื่อการเพิ่มขยายขอบเขตการให้บริการไปยังภายนอกของเครือข่ายได้ ซึ่งโดยพื้นฐานแล้วเป็นการนำหน่วยการทำงานแบบเอเจนท์ (Agent) เข้ามาใช้งาน เพื่อการรับเข้า

หรือส่งต่อข้อมูลระหว่างเครือข่ายยูพีแอนพีกับเครือข่ายภายนอก ตัวอย่างเช่น เพื่อการจับคู่บริการ (Mapping) ระหว่างโพรโทคอลค้นหาบริการ SSDP ในเครือข่ายยูพีแอนพีกับโพรโทคอลค้นหาบริการ SLP ของเครือข่ายอินเทอร์เน็ต [4] หรือ กับโพรโทคอลค้นหาบริการ Jini สำหรับงานประยุกต์ที่พัฒนาด้วยภาษาจาวา [5] เป็นต้น แต่เป็นที่น่าสังเกตว่างานวิจัยจำนวนมากเหล่านี้ให้ความสนใจในการเพิ่มขยายบริการให้กับอุปกรณ์ที่อยู่ต่างเครือข่ายยูพีแอนพีภายในเครือข่ายอินเทอร์เน็ตเป็นสำคัญงานวิจัยในวิทยานิพนธ์นี้ แม้ว่าจะศึกษาการเพิ่มขยายบริการต่างเครือข่ายยูพีแอนพี เช่นกัน แต่เน้นการทำงานร่วมกับเครือข่ายโทรศัพท์ ซึ่งเป็นเครือข่ายโทรคมนาคมที่มีค่าใช้จ่ายในการสื่อสารต่ำ และใช้งานกันแพร่หลายในพื้นที่ชนบทห่างไกล (Urban Area) ของประเทศไทย

1.2 วัตถุประสงค์

1) เพื่อเปรียบเทียบเทคนิควิธีการเข้ารหัสข้อมูลที่เหมาะสม สำหรับการประยุกต์ใช้ในการให้บริการแบบกลุ่มสื่อสารปลอดภัยภายในเครือข่ายยูพีแอนพี พร้อมเสนอแนวทางการเพิ่มขยายโพรโทคอลต่างๆ ที่เกี่ยวข้อง
2) เพื่อพัฒนากลไกทำงานในการเพิ่มขยายเครือข่ายยูพีแอนพีให้สามารถส่งผ่านการควบคุมในการแจ้งเตือนสถานการณ์ไปยังอุปกรณ์ของเครือข่ายโทรศัพท์พื้นฐานได้

1.3 ขอบเขตของการวิจัย

1) ศึกษาเปรียบเทียบประสิทธิภาพทางด้านความเร็วในการประมวลผลระหว่างกลไกยืนยันตัวตนอุปกรณ์ด้วยเทคนิคการเข้ารหัสข้อมูลแบบคีย์พรีดิสทริบิวชัน (Key Pre-Distribution) และพับลิคคีย์อินฟราสตรัคเจอร์ (Public Key Infrastructure) แบบมาตรฐาน พร้อมนำเสนอแนวทางการเพิ่มขยายโพรโทคอลของเครือข่ายยูพีแอนพีให้รองรับบริการกลุ่มสื่อสารปลอดภัยอย่างเหมาะสม โดยที่ยังสามารถทำงานร่วมกับโพรโทคอลตามมาตรฐานเดิมได้
2) ทดสอบประสิทธิภาพของกลไกที่นำเสนอในข้อที่ 1 ข้างต้น ทั้งในสภาพแวดล้อมของการใช้งานจากอุปกรณ์ที่อยู่ภายในเครือข่ายเดียวกันหรือต่างเครือข่ายกันได้
3) ศึกษาข้อจำกัดของกลไกการสื่อสารข้อมูลในเครือข่ายยูพีแอนพี พร้อมนำเสนอแนวทางการแก้ไขปัญหาเพื่อเพิ่มขยายขอบเขตการให้บริการทั้งจากเครือข่ายอินเทอร์เน็ต แบบ

เดียวกัน หรือเครือข่ายโทรศัพท์ที่ต่างเทคโนโลยีกันได้ โดยจะใช้ระบบเกตเวย์โทรศัพท์ที่พัฒนาขึ้นโดยใช้ซอฟต์แวร์แบบโอเพนซอร์สแอสเทอริสก์ (Asterisk) เป็นกรณีศึกษา

1.4 ขั้นตอนการวิจัยและวิธีการวิจัย

1) ศึกษาข้อจำกัดของกลไกการสื่อสารข้อมูลในเครือข่ายยูพีแอนพีทางด้านการให้บริการแบบกลุ่มสื่อสารปลอดภัย และการสื่อสารข้ามเครือข่าย
2) ศึกษาเปรียบเทียบการนำเทคนิควิธีการยืนยันตัวตนแบบต่างๆ ให้กับอุปกรณ์ภายในเครือข่ายยูพีแอนพี ในการสร้างกลุ่มสื่อสารปลอดภัย พร้อมนำเสนอการเพิ่มขยายอย่างเหมาะสมให้กับโพรโทคอลที่เกี่ยวข้องในกระบวนการต่างๆ ของเครือข่ายยูพีแอนพี พร้อมระบบทดสอบต้นแบบ เพื่อศึกษาประสิทธิภาพของกลไกกลุ่มสื่อสารปลอดภัยที่นำเสนอขึ้น ทั้งในสภาพแวดล้อมของเครือข่ายเดียวกันและต่างเครือข่าย
3) ศึกษากลไกการควบคุมเพื่อสั่งการระบบเกตเวย์โทรศัพท์ของซอฟต์แวร์แอสเทอริสก์ พร้อมนำเสนอกลไกการประสานงานระหว่างเอเจนท์ของเครือข่ายยูพีแอนพี และของเกตเวย์ของเครือข่ายโทรศัพท์ เพื่อการส่งผ่านสถานะการควบคุม
4) รวบรวมผลการทดสอบ สรุปผล จัดทำวิทยานิพนธ์ฉบับสมบูรณ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1) แนวทางการเพิ่มขยายโพรโทคอลของเครือข่ายยูพีแอนพีอย่างเหมาะสม เพื่อให้รองรับบริการแบบกลุ่มสื่อสารปลอดภัย ผ่านการประยุกต์ใช้กลไกการกระจายคีย์เพื่อการยืนยันตัวตนของกลุ่มอุปกรณ์
2) กลไกการประยุกต์ใช้หน่วยทำงานเอเจนท์ เพื่อสามารถให้บริการสื่อสารแบบกลุ่มปลอดภัยข้ามเครือข่ายกันได้
3) แนวทางการเพิ่มขยายขอบเขตการให้บริการของเครือข่ายยูพีแอนพีอย่างเหมาะสม เพื่อให้สามารถส่งผ่านสถานะการควบคุมกับอุปกรณ์ของเครือข่ายโทรศัพท์พื้นฐาน จากการใช้ประโยชน์ของหน่วยทำงานเอเจนท์ที่เกตเวย์ของเครือข่ายทั้งสองนั้น

1.6 โครงสร้างของวิทยานิพนธ์

วิทยานิพนธ์นี้ได้จัดวางโครงสร้างเป็นบทๆ รวมทั้งสิ้นเป็นจำนวน 5 บท ดังต่อไปนี้

- บทที่ 1 เป็นบทนำ เริ่มต้นกล่าวถึงความสำคัญ ที่มาของปัญหาวิจัยที่จะดำเนินการ รวมถึงวัตถุประสงค์ และขอบเขตของวิทยานิพนธ์
- บทที่ 2 เป็นการตรวจเอกสาร โดยเริ่มต้นจากการอธิบายเทคโนโลยีที่เกี่ยวข้อง เช่น มาตรฐานของเครือข่ายยูพีแอนพี เทคนิคการเข้ารหัสข้อมูล เป็นต้น จากนั้นจึงเป็นการทบทวนวรรณกรรมที่เกี่ยวข้องกับงานวิจัย
- บทที่ 3 เป็นการอธิบายวิธีดำเนินการวิจัย ซึ่งเกี่ยวข้องกับประเด็นหลัก 2 ประการ คือ 1) การศึกษา เพื่อออกแบบและพัฒนาการเพิ่มขยายโพรโทคอลภายในเครือข่ายยูพีแอนพีเพื่อให้บริการแบบกลุ่มสื่อสารปลอดภัยในระดับชั้นบริการที่พัฒนาขึ้นใหม่ข้างต้น และ 2) แนวทางการพัฒนากลไกประสานงานเพื่อให้เอเจนท์ของทั้งเครือข่ายยูพีแอนพี และเครือข่ายโทรศัพท์พื้นฐานสามารถทำงานร่วมกันเพื่อขยายขอบเขตการให้บริการจากเครือข่ายต่างประเภทกันได้
- บทที่ 4 เป็นการรายงานผลการศึกษาวิจัยจากขั้นตอนวิธีที่ได้อธิบายในบทที่ผ่านมา รวมถึงการวิเคราะห์ผล และรายละเอียดผลการทดสอบเบื้องต้นในห้องปฏิบัติการ โดยใช้กรณีศึกษาจากระบบประยุกต์ทางการแพทย์เพื่อดูแลผู้สูงอายุจากระยะไกล ซึ่งเป็นการรวมกลไกทำงานที่ได้ดำเนินการวิจัยข้างต้น
- บทที่ 5 เป็นบทสรุปการวิจัยเพื่อวิทยานิพนธ์

บทที่ 2

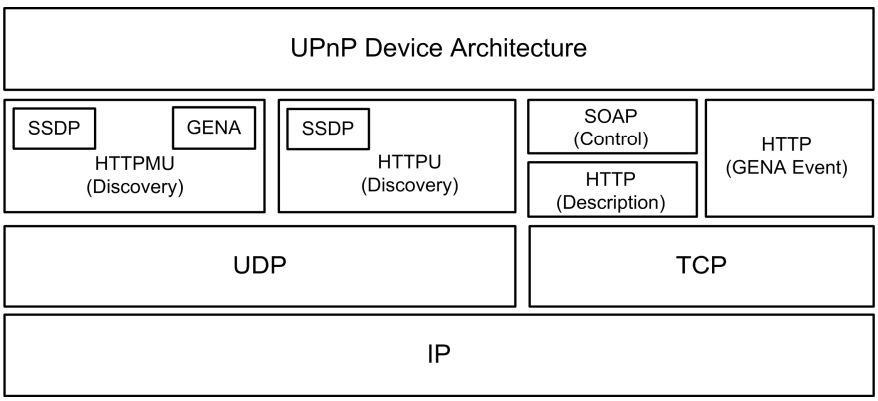
การตรวจเอกสาร

ในบทนี้จะเป็นการกล่าวนำถึงความรู้พื้นฐานของเทคโนโลยีที่เกี่ยวข้องกับประเด็นปัญหาของงานวิจัยในวิทยานิพนธ์นี้ โดยได้จัดแบ่งเนื้อหาออกเป็นส่วนๆ เริ่มจากการแนะนำสถาปัตยกรรมและโพรโทคอลสื่อสารที่เกี่ยวข้องกับเครือข่ายยูพีแอนพี ภายในกระบวนการทำงานต่างๆ จากนั้นจึงเป็นการแนะนำถึงกลไกการยืนยันตัวตนแบบกลุ่มสื่อสารปลอดภัยและเทคนิควิธีการเข้ารหัสแบบกลุ่มแบบต่างๆ สถาปัตยกรรมของระบบชุมสายโทรศัพท์ที่พัฒนาขึ้นด้วยซอฟต์แวร์แอสเทอริสก์ สุดท้ายจึงเป็นรายละเอียดของงานวิจัยที่มีความเกี่ยวข้องกัน

2.1 เทคโนโลยีที่เกี่ยวข้อง

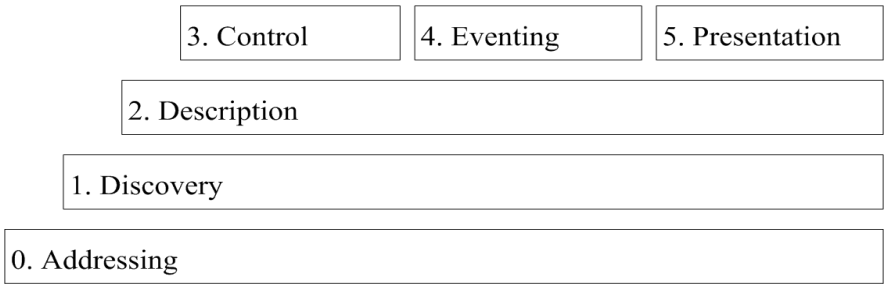
2.1.1 สถาปัตยกรรมและโพรโทคอลสื่อสารของเครือข่ายยูพีแอนพี

เครือข่ายยูพีแอนพี [1] สนับสนุนการเชื่อมต่อโดยอัตโนมัติให้กับอุปกรณ์ที่ทำหน้าที่เป็นหน่วยควบคุม (Control Point) และอุปกรณ์ที่ถูกควบคุม (Controlled Device) (ซึ่งต่อไปจะขอเรียกเพียงย่อว่า อุปกรณ์ (Device) เท่านั้น) โดยหากพิจารณาจากรูปที่ 2.1 จะพบว่าโพรโทคอลของเครือข่ายยูพีแอนพีล้วนมีพื้นฐานมาจากโพรโทคอลมาตรฐานที่ใช้งานกันอยู่แพร่หลายภายในเครือข่ายอินเทอร์เน็ตและเทคโนโลยีเว็บทั้งสิ้น



รูปที่ 2.1 ระดับชั้นโพรโทคอลของเครือข่ายยูพีแอนพี [1]

จากรูปที่ 2.2 แสดงลำดับของกระบวนการทำงานได้ 6 สถานะที่เกิดขึ้นภายในเครือข่ายยูพีแอนพี โดยเริ่มต้นจากกระบวนการที่ 0 เพื่อการร้องขอหมายเลขไอพี (Addressing) กระบวนการที่ 1 เพื่อการค้นหาบริการ (Discovery) กระบวนการที่ 2 เพื่อการประกาศแจ้งบริการของอุปกรณ์ต่างๆ ให้หน่วยควบคุมได้รับทราบ (Description) กระบวนการที่ 3 เพื่อการควบคุมหรือสั่งการอุปกรณ์ (Control) กระบวนการที่ 4 เพื่อการแจ้งเตือนสถานะ (Eventing) และกระบวนการที่ 5 เพื่อการแสดงผลสถานะของอุปกรณ์ผ่านทางเว็บเบราเซอร์ (Presentation)



รูปที่ 2.2 ลำดับของกระบวนการเพื่อเชื่อมต่อเข้าเป็นเครือข่ายยูพีแอนพี [1]

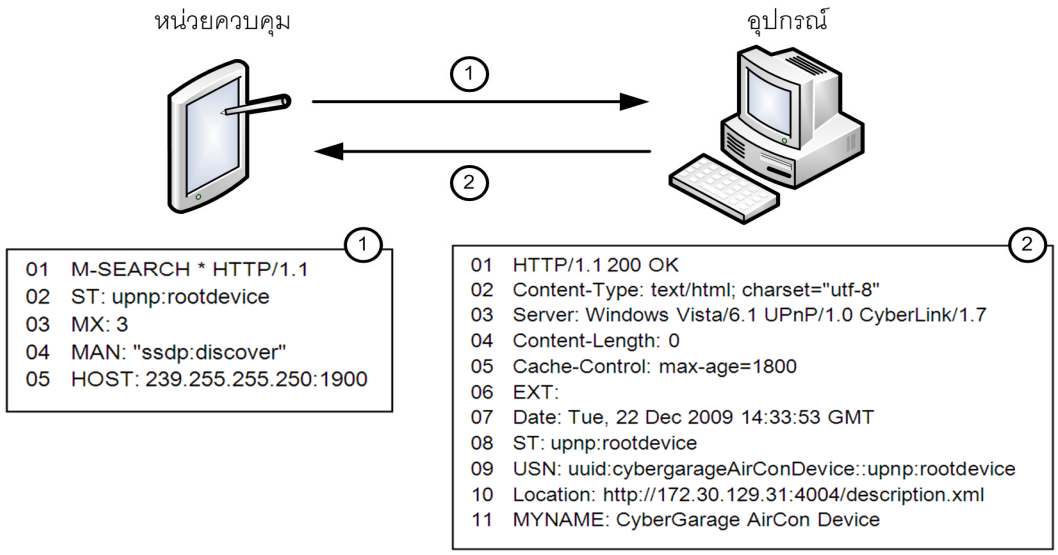
หากพิจารณาจากรูปแผนภาพลำดับการเกิดของกระบวนการข้างต้นทั้งหมดแล้ว จะเห็นได้ว่าตั้งแต่กระบวนการที่ 0 ถึง 2 จะเป็นพื้นฐานสำคัญให้กับกระบวนการอื่นๆ ทั้งสิ้น หรือกล่าวอีกนัยหนึ่งได้ว่า ในการควบคุมเพื่อสั่งการอุปกรณ์ หรือการแจ้ง/รายงานเหตุการณ์เมื่อเสร็จสิ้นบริการของอุปกรณ์หนึ่งๆ ก็จำเป็นที่อุปกรณ์นั้นจะต้องถูกค้นพบ หรือประกาศก่อนว่าสามารถให้บริการอะไรได้บ้าง อย่างไรก็ตาม การอธิบายในหัวข้อย่อยถัดไปจะเลือกเฉพาะกระบวนการที่จะเกี่ยวข้องกับงานวิจัยในวิทยานิพนธ์นี้เท่านั้น

2.1.2 กระบวนการค้นหาบริการภายในเครือข่ายยูพีแอนพี

การค้นหาบริการของอุปกรณ์ภายในระบบทั้งหมด ใช้การดำเนินการผ่านทางโพรโทคอล Simple Service Discovery Protocol (SSDP) ซึ่งจะเรียกใช้บริการผ่านโพรโทคอลยูพีแอนพีอีกต่อหนึ่ง ขึ้นกับว่าเป็นการกระจายข้อมูลแบบกลุ่มมัลติคาสก์ ก็จะใช้โพรโทคอล HTTPMU หรือแบบยูนิคาสก์ ก็จะใช้โพรโทคอล HTTPU โดยจำแนกตามกรณีของการสื่อสารแบ่งตามการเริ่มต้นเข้าสู่เครือข่ายของอุปกรณ์เป็น 2 กรณี ดังต่อไปนี้

1) <u>กรณีที่หน่วยควบคุมเชื่อมต่อเข้าสู่เครือข่าย</u>

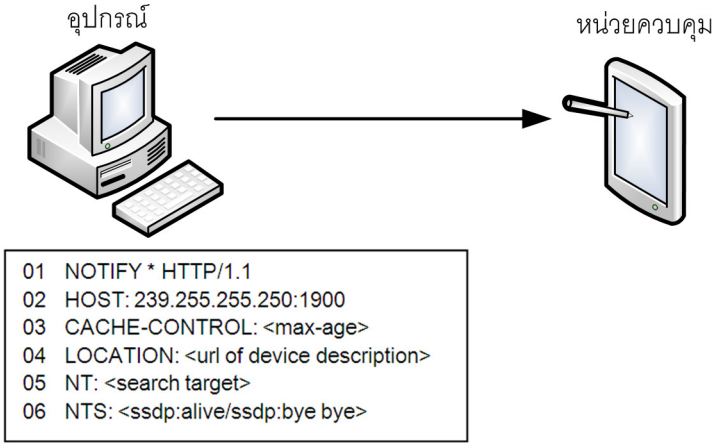
หน่วยควบคุมเริ่มต้นทำกระบวนการค้นหาบริการด้วยการประกาศข้อความ M-SEARCH (รูปที่ 2.3 วงกลมหมายเลข 1) ออกไปในเครือข่ายผ่านทางโพรโทคอล HTTPMU เมื่ออุปกรณ์ที่เชื่อมต่ออยู่กับเครือข่ายได้รับข้อความดังกล่าวจะตอบกลับเป็นข้อมูลเกี่ยวกับบริการของอุปกรณ์นั้น (วงกลมหมายเลข 2 บรรทัดที่ 10) ไปยังหน่วยควบคุมตามหมายเลขไอพีที่ร้องขอ ซึ่งปรากฏในข้อความ M-SEARCH สำหรับรายละเอียดข้อความสื่อสารเพิ่มเติมอื่นๆ ของกระบวนการค้นหาบริการนี้สามารถอ่านได้จาก [1]



รูปที่ 2.3 ตัวอย่างข้อความค้นหาบริการ กรณีหน่วยควบคุมเชื่อมต่อเข้าสู่เครือข่าย

2) <u>กรณีที่อุปกรณ์เชื่อมต่อเข้าสู่เครือข่าย</u>

อุปกรณ์จะเริ่มกระบวนการประกาศแจ้งข้อมูลเกี่ยวกับบริการ ด้วยการส่งข้อความ NOTIFY (รูปที่ 2.4) ให้กับสมาชิกอื่นๆ ภายในเครือข่ายยูพีแอนพี โดยผ่านโพรโทคอล HTTPMU ดังนั้น หากต้องการจะขยายกิจกรรมเพิ่มเติมสำหรับกลุ่มสื่อสารแบบปลอดภัย เช่น การค้นหาสมาชิก หรือค้นหาหมายเลขของกลุ่มสื่อสาร ก็สามารถทำได้โดยการเพิ่มเติมพารามิเตอร์ภายในข้อความประกาศบริการของโพรโทคอล SSDP ด้วย

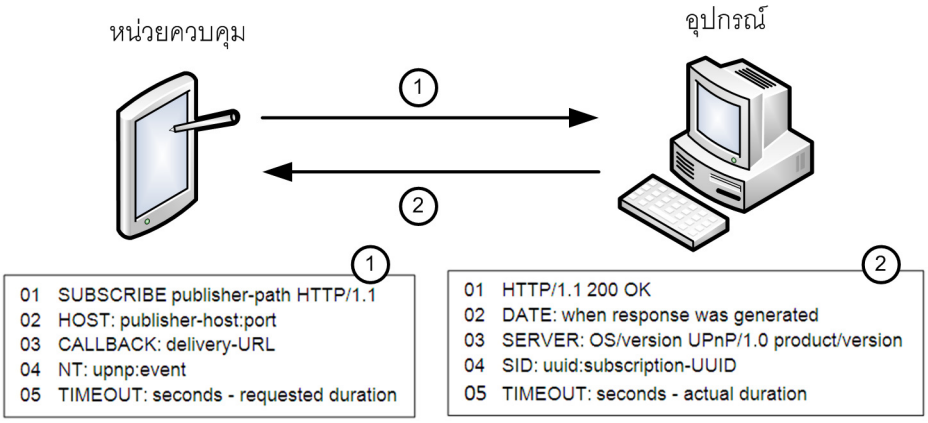


รูปที่ 2.4 ตัวอย่างข้อความประกาศบริการ กรณีอุปกรณ์เชื่อมต่อเข้าสู่เครือข่าย

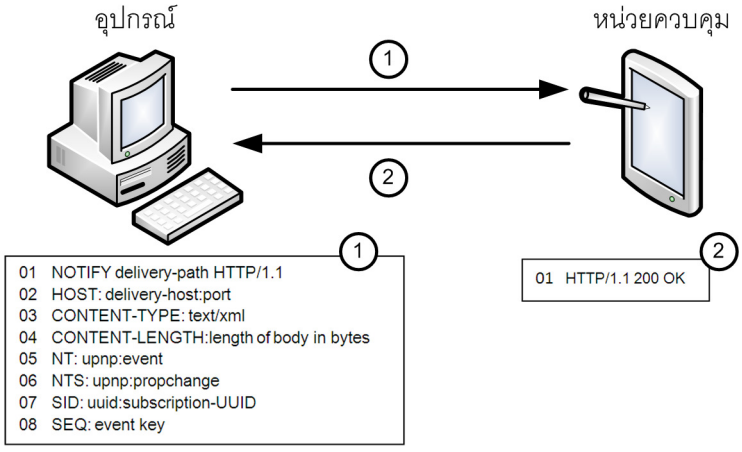
2.1.3 กระบวนการแจ้งเตือนเหตุการณ์

การแจ้งเตือนเหตุการณ์ของอุปกรณ์ให้กับหน่วยควบคุมที่สั่งการได้รับทราบ ณ ช่วงเวลาหลังจากที่อุปกรณ์นั้นๆ เสร็จสิ้นบริการแล้ว ประกอบด้วยกระบวนการย่อย 2 กระบวนการ ดังนี้

- กระบวนการสมัคร (Subscribe) เพื่อรับการแจ้งเตือนเหตุการณ์ กระบวนการนี้หน่วยควบคุมจะต้องส่งข้อความ SUBSCRIBE (รูปที่ 2.5 วงกลมหมายเลข 1) ไปยังอุปกรณ์ที่สนใจ ซึ่งอุปกรณ์นี้จะเก็บบันทึกข้อมูลต่างๆ ไว้ เช่น CALLBACK ในบรรทัดที่ 3 เป็นข้อมูล URL ของหน่วยควบคุมที่ต้องการแจ้งกลับ และหมายเลข SID (รูปที่ 2.5 วงกลมหมายเลข 2 บรรทัดที่ 4) ซึ่งเป็นหมายเลขประจำตัวในการสมัครครั้งนั้นๆ เพื่อจะนำไปใช้ในการระบุเพื่ออ้างอิงถึงหน่วยควบคุมได้ถูกต้องหากมีจำนวนมากหลายตัว
- กระบวนการแจ้งเตือนเหตุการณ์ (Notification) เพื่อแจ้งเตือนเหตุการณ์เมื่อมีการเปลี่ยนแปลงสถานะของอุปกรณ์เกิดขึ้น โดยอุปกรณ์จะส่งข้อความ NOTIFY (รูปที่ 2.6 วงกลมหมายเลข 1) ไปยังหน่วยควบคุมที่สมัครรับแจ้งเตือนเหตุการณ์เอาไว้ เช่น SEQ ในบรรทัดที่ 8 เป็นหมายเลขบอกลำดับของการแจ้งเตือน ที่จะเพิ่มขึ้นตามจำนวนครั้งของการแจ้งเตือนเหตุการณ์จากอุปกรณ์นั้น



รูปที่ 2.5 ตัวอย่างข้อความสมัครเพื่อรับแจ้งเตือนเหตุการณ์



รูปที่ 2.6 ตัวอย่างข้อความแจ้งเตือนเหตุการณ์

จากลักษณะแนวทางการทำงานข้างต้น กระบวนการแจ้งเตือนเหตุการณ์นี้จะถูกนำไปใช้ในหลายลักษณะตามประเด็นวิจัยในวิทยานิพนธ์ คือ

1) กรณีการเพิ่มขยายโพรโทคอลให้รองรับการสื่อสารแบบกลุ่มปลอดภัย โดยจะนำกระบวนการแจ้งเตือนเหตุการณ์ไปใช้เพื่อกระจายข้อมูลภายในกลุ่ม เช่น การกระจาย

ข้อมูลคีย์กลุ่มที่คำนวณขึ้นใหม่ เมื่อมีการเปลี่ยนแปลงจำนวนสมาชิกภายในกลุ่ม เป็นต้น

2) กรณีการเพิ่มขยายบริการข้ามเครือข่ายยูพีแอนพีกับเครือข่ายโทรศัพท์ โดยจะนำกระบวนการแจ้งเตือนเหตุการณ์นี้ไปใช้เพื่อการส่งต่อเหตุการณ์ที่แจ้งเตือนให้กับหน่วยทำงานเอเจนท์ที่ทำงานอยู่บริเวณเกตเวย์ของเครือข่าย

2.1.4 กลไกการยืนยันตัวตนสำหรับกลุ่มสื่อสารปลอดภัย

กลไกการยืนยันตัวตนของอุปกรณ์ในระบบกลุ่มสื่อสารปลอดภัย ได้มีการจำแนกไว้เป็นสามลักษณะ [6] ได้แก่ 1) แบบการใช้โพรโทคอลจัดการคีย์กลุ่มแบบรวมศูนย์ (Centralized group key management protocols) 2) แบบการใช้โพรโทคอลจัดการคีย์กลุ่มแบบกระจาย (Distributed key management protocols) และ 3) แบบการใช้สถาปัตยกรรมเพื่อกระจายการจัดการคีย์ไปยังกลุ่มย่อย (Decentralized architectures) อย่างไรก็ตาม ในวิทยานิพนธ์นี้เลือกพิจารณาศึกษาเฉพาะในแบบที่ 1 ซึ่งใช้ศูนย์กลางในการจัดการคีย์แบบกลุ่ม เนื่องจาก มีความซับซ้อนน้อย เหมาะสมกับการนำไปประยุกต์ใช้กับเครือข่ายยูพีแอนพี ซึ่งมักมีอุปกรณ์จำนวนไม่มากนัก และจัดการปัญหาการปรับค่าและการกระจายคีย์กลุ่มเพียงเฉพาะที่ศูนย์กลาง จึงมีความสะดวก แม้ว่าอัตราการเปลี่ยนแปลงจำนวนสมาชิกในกลุ่มจะสูงก็ตาม อย่างไรก็ตาม แม้ว่าจะใช้สถาปัตยกรรมของระบบกลุ่มสื่อสารปลอดภัยแบบรวมศูนย์แล้ว ก็ยังจำเป็นต้องอาศัยเทคนิควิธีการเข้ารหัสเพื่อช่วยในการยืนยันตัวตนของอุปกรณ์ ดังที่จะอธิบายต่อไป

2.1.4.1 เทคนิควิธีการเข้ารหัสแบบพับลิคคีย์อินฟราสตรัคเจอร์

พับลิคคีย์อินฟราสตรัคเจอร์ (Public Key Infrastructure) หรือเรียกโดยย่อว่าพีเคไอ (PKI) [7] เป็นระบบป้องกันข้อมูลการสื่อสารที่นิยมใช้งานทั่วไปบนระบบอินเทอร์เน็ต โดยเฉพาะกับธุรกรรมของการพาณิชย์อิเล็กทรอนิกส์ เนื่องจากมีความปลอดภัยสูง โดยมีองค์ประกอบพื้นฐานที่ใช้ในการรักษาความปลอดภัย ได้แก่ เทคนิควิธีการเข้ารหัส(Cryptography) ลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) และใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ซึ่งกำหนดขึ้นโดยส่วนกลางขององค์กรเรียกว่า Certification Authority (CA)

เทคนิควิธีพีเคไอจะใช้คีย์คู่ในการเข้ารหัสประกอบไปด้วย คีย์ส่วนตัว (Private Key) และคีย์สาธารณะ (Public Key) โดยคีย์ทั้งสองนี้จะได้มาพร้อมกับใบรับรองที่ CA ออกให้ การเข้ารหัส

จะใช้คีย์สาธารณะ ส่วนการถอดรหัสจะใช้คีย์ส่วนตัว ดังนั้น คีย์สาธารณะของอุปกรณ์ทุกตัวจะถูกแจกจ่ายออกไปภายในกลุ่มสื่อสาร

รูปที่ 2.7 การยืนยันตัวตนด้วยเทคนิควิธีการเข้ารหัสแบบพีเคไอ

การยืนยันตัวตนของพีเคไอสามารถทำได้โดยใช้ใบรับรองอิเล็กทรอนิกส์ และลายมือชื่ออิเล็กทรอนิกส์ ยกตัวอย่าง การยืนยันตัวตนระหว่างหน่วยควบคุมกับอุปกรณ์ ดังแสดงในรูปที่ 2.7 มีขั้นตอน ดังต่อไปนี้

1) หน่วยควบคุมและอุปกรณ์แลกเปลี่ยนใบรับรองอิเล็กทรอนิกส์ระหว่างกัน ซึ่งนำมาตรวจสอบด้วยใบรับรองอิเล็กทรอนิกส์ (Verification) ของ CA ทำให้สามารถทราบได้ว่าใบรับรองอิเล็กทรอนิกส์ของหน่วยควบคุมเป็นของจริง แต่ไม่สามารถยืนยันได้ว่าเป็นเจ้าของหรือไม่ จึงต้องทำการตรวจสอบจากลายมือชื่ออิเล็กทรอนิกส์อีกครั้ง
2) หน่วยควบคุมร้องขอตัวแปรสุ่มที่จะใช้ประกอบในการยืนยันตัวตน เพื่อพิสูจน์ความทันสมัย (Freshness) ของการสื่อสารและป้องกันผู้ที่ดักจับข้อมูลสื่อสารภายในเครือข่าย ไม่ให้สามารถยืนยันตัวตนด้วยการปลอมแปลงข้อมูลที่สื่อสารที่บันทึกเอาไว้(Replay Attack)
3) หน่วยควบคุมยืนยันตัวตนกับอุปกรณ์ ด้วยลายมือชื่ออิเล็กทรอนิกส์ ด้วยการเซ็น (Signing) รับรองข้อมูลสุ่ม ที่ได้มาในขั้นตอนก่อนหน้าด้วยคีย์ส่วนตัว ทำให้สามารถยืนยันได้ว่าเป็นเจ้าของใบรับรองอิเล็กทรอนิกส์จริง

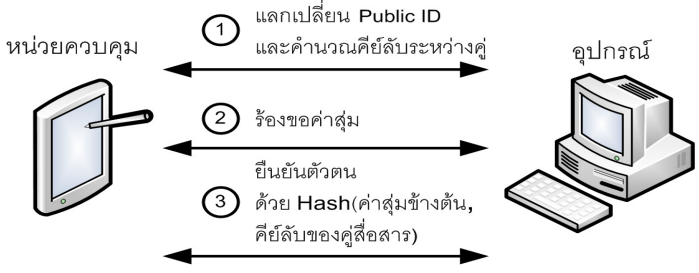
โดยสรุปกลไกการยืนยันตัวตนระหว่าง หน่วยควบคุมกับอุปกรณ์ สามารถทำได้โดยการพิสูจน์ว่าใบรับรองอิเล็กทรอนิกส์เป็นของจริงที่ออกจาก CA และหน่วยควบคุมเป็นเจ้าของใบรับรองอิเล็กทรอนิกส์จริง จากการพิสูจน์ข้างต้น

2.1.4.2 เทคนิควิธีการเข้ารหัสแบบคีย์พรีดิสทริบิวชัน

คีย์พรีดิสทริบิวชัน (Key Pre-Distribution) หรือเรียกโดยย่อว่าเคพีดี (KPD) [8] เป็นเทคนิควิธีการเข้ารหัสที่นิยมใช้งานกับสภาพแวดล้อมที่มีทรัพยากรจำกัด เช่น เครือข่ายเซ็นเซอร์ไร้สาย โดยที่สมาชิกทุกตัวภายในกลุ่มสื่อสารจะต้องมีการติดตั้งคีย์เอาไว้ล่วงหน้า ซึ่งประกอบด้วย 2 ส่วน คือ Public Identification หรือเรียกสั้นๆ ว่า Public ID และ Secret Information ซึ่งจะนำไปใช้คำนวณคีย์ลับของคู่สื่อสาร (Pair-wise Secret Key) กับสมาชิกภายในกลุ่มเดียวกัน โดยต่อไปจะได้กล่าวถึงขั้นตอนการยืนยันตนด้วยเทคนิควิธีเคพีดี จากนั้นจะกล่าวถึงรายละเอียดการทำงานของกลไก และแนวทางในการนำไปประยุกต์ใช้กับกลุ่มสื่อสารปลอดภัยดังนี้

ขั้นตอนการยืนยันตนด้วยเทคนิควิธีเคพีดี ระหว่างหน่วยควบคุมกับอุปกรณ์ ซึ่งแสดงในรูปที่ 2.8 ประกอบด้วย 3 ขั้นตอน ดังต่อไปนี้

1) หน่วยควบคุมและอุปกรณ์แลกเปลี่ยน Public ID กัน เพื่อนำไปใช้ในการคำนวณคีย์ลับของคู่สื่อสาร
2) หน่วยควบคุมร้องขอตัวแปรสุ่มที่จะใช้ในการยืนยันตัวตน เพื่อพิสูจน์ความทันสมัย แบบเดียวกันกับเทคนิควิธีของพีเคไอ
3) หน่วยควบคุมยืนยันตัวตนกับอุปกรณ์ โดยใช้ผลจากฟังก์ชัน Hash (One-way-function) โดยมีพารามิเตอร์เป็นค่าสุ่มที่ได้จากขั้นที่สองและคีย์ลับของคู่สื่อสาร



รูปที่ 2.8 การยืนยันตัวตนด้วยเทคนิควิธีเคพีดี

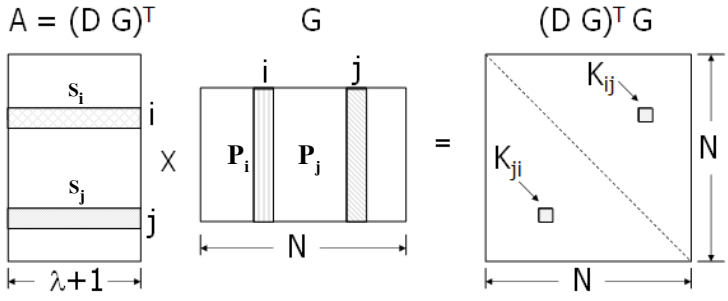
รายละเอียดการทำงานของกลไกเข้ารหัสเคพีดี มีพื้นฐานมาจากอัลกอริทึมของบลอม (Blom's algorithm) [9] มีชื่อเรียกว่า λ-secure ซึ่งเมื่อกำหนดค่า λ มากโอกาสในการเดาสุ่มค่าคีย์ของทั้งระบบก็จะทำได้ยากยิ่งขึ้นตามไปด้วย โดยกำหนดให้

- K_{ij} และ K_{ji} เป็นคีย์ลับของคู่สื่อสาร i และ j
- G เป็นเมตริกซ์ขนาด $(\lambda + 1) \times N$ มีสมาชิกภายในเป็นตัวเลขในฟิลด์จำกัด (Finite Field) โดนมี N เป็นจำนวนอุปกรณ์ภายในเครือข่าย และ λ ควรมีค่ามากกว่าขนาดจำนวนของอุปกรณ์ภายในเครือข่าย ข้อมูลภายในเมตริกซ์ G สามารถเปิดเผย
- D เป็นเมติกเมตริกซ์ขนาด $(\lambda + 1) \times (\lambda + 1)$ เป็นจำนวนจากฟิลด์จำกัด ข้อมูลภายในเมตริกซ์ D เป็นความลับ
- A เป็นเมติกเมตริกซ์ ที่คำนวณค่าจาก $A = (A \cdot G)^T$ โดยที่ $(A \cdot G)^T$ คือ ทรานซ์โพสของ $(A \cdot G)$

จากสมการที่ 2.1 สามารถแสดงคุณสมบัติของ $A \cdot G$ ซึ่งเป็นเมตริกซ์สมมาตร (Symmetric Matrix) ได้ดังนี้

$$A \cdot G = (D \cdot G)^T \cdot G = G^T \cdot D^T \cdot G = G^T \cdot D \cdot G = (A \cdot G)^T \quad (2.1)$$

ดังนั้น ด้วยหลักการคำนวณดังกล่าวข้างต้น จะสามารถนำไปประยุกต์ใช้งานกับการสร้างคีย์ลับของคู่สื่อสาร K_{ij} กับ K_{ji} สำหรับอุปกรณ์ i และ j ดังแสดงในรูปที่ 2.9



รูปที่ 2.9 อัลกอริทึมของบลอมในการคำนวณคีย์คู่ระหว่างอุปกรณ์ i และ j [9]

เทคนิควิธีเคพีดีอาศัยเครื่องแม่ข่ายส่วนกลาง ในการสร้างคีย์ของทั้งระบบเรียกว่า Trusted Authority (TA) โดยมีขั้นตอน ดังต่อไปนี้

1) TA สร้างข้อมูล $A \cdot G$ ตามสมการ 2.1 โดยกำหนดค่า N และ λ ให้เหมาะสมกับจำนวนอุปกรณ์ภายในเครือข่ายตามข้อกำหนด ดังอธิบายข้างต้น
2) TA ติดตั้งคีย์เอาไว้ล่วงหน้าให้อุปกรณ์แต่ละชิ้น ดังตัวอย่างจากรูปที่ 2.9 ซึ่งอุปกรณ์ลำดับที่ i จะได้รับการติดตั้ง Public ID (P_i) จากข้อในมูลคอลัมน์ที่ i ของเมตริกซ์ G และ Secret Information (S_i) จากข้อมูลในแถวที่ i ของเมตริกซ์ A

จากคุณสมบัติของกลไกการเข้ารหัสทั้งสองแบบที่ได้กล่าวไปข้างต้น พบว่าสามารถรองรับการนำไปใช้ในการยืนยันตัวตนแบบพลวัตได้ทั้งคู่ อย่างไรก็ตาม กลไกการเข้ารหัสทั้งสองมีคุณสมบัติการใช้ทรัพยากรในด้านการประมวลผลที่แตกต่างกัน ซึ่งจะได้ศึกษาเปรียบเทียบความเหมาะสมในการนำไปประยุกต์ใช้กับโพรโทคอลของเครือข่ายยูพีแอนพีต่อไป

2.1.5 การเปรียบเทียบคุณลักษณะระหว่างเทคนิควิธีพีเคไอกับเคพีดี

เทคนิควิธีพีเคไอนิยมใช้งานกันโดยแพร่หลาย เนื่องจากข้อดีในด้านความเข้มแข็งในการเข้ารหัสข้อมูลสูง และการรองรับการสื่อสารแบบกลุ่มปลอดภัยได้โดยตรง ผ่านทางกลไกยืนยันตัวตนจากใบรับรองอิเล็กทรอนิกส์ที่ออกโดย CA แต่มีข้อเสียในด้านความต้องการใช้ทรัพยากรในการประมวลผลมาก [7] ซึ่งเป็นผลจากการใช้อัลกอริทึมของการเข้ารหัสเป็นคีย์แบบอสมมาตร (Asymmetric) จึงไม่เหมาะสมกับเครือข่ายยูพีแอนพี ซึ่งมีทรัพยากรของหน่วยประมวลผลและทรัพยากรเครือข่ายที่จำกัด

สำหรับเทคนิควิธีเคพีดีใช้อัลกอริทึมการเข้ารหัสเป็นคีย์แบบสมมาตร (Symmetric) จึงใช้ทรัพยากรในการประมวลผลน้อยกว่าของอัลกอริทึมการเข้ารหัสที่ใช้คีย์แบบอสมมาตรมาก นอกจากนี้ยังสามารถนำไปใช้เพื่อรองรับการสื่อสารแบบกลุ่มปลอดภัยได้เช่นกัน โดยการกระจายคีย์ไว้ที่อุปกรณ์ภายในกลุ่มล่วงหน้า อย่างไรก็ตาม หากพิจารณาด้านความเข้มแข็งของการป้องกันการเจาะรหัสข้อมูลแล้ว แม้ว่าจะด้อยกว่าแบบที่ใช้ในเทคนิควิธีพีเคไอ แต่สามารถที่จะเพิ่มระดับความเข้มแข็งในการป้องกันการเจาะรหัสข้อมูลได้ หากใช้ความยาวรหัสคีย์มากกว่า 128 บิต [10] (ดูข้อมูลจากตารางที่ 2.1 ประกอบ) ทั้งนี้เทคนิควิธีเคพีดี อาจนำไปสู่ปัญหาการขโมยคีย์จากอุปกรณ์โดยตรง แต่อุปกรณ์ที่ใช้ในงานนี้ส่วนใหญ่เน้นอุปกรณ์พกพาซึ่งจะอยู่ติดตัวผู้ใช้ทำให้การขโมยอาจทำได้ยาก อีกทั้งการใช้งานในสภาพแวดล้อมของเครือข่ายภายในบ้านมีขอบเขตจำกัด ดังนั้นความเสี่ยงในการถูกเจาะระบบโดยการขโมยคีย์จากอุปกรณ์สื่อสารไร้สายจึงถูกจำกัดไปด้วยเช่นกัน

ตารางที่ 2.1 เวลาที่ใช้ในการถอดรหัสของอัลกอริทึมที่ใช้คีย์แบบสมมาตร [10]

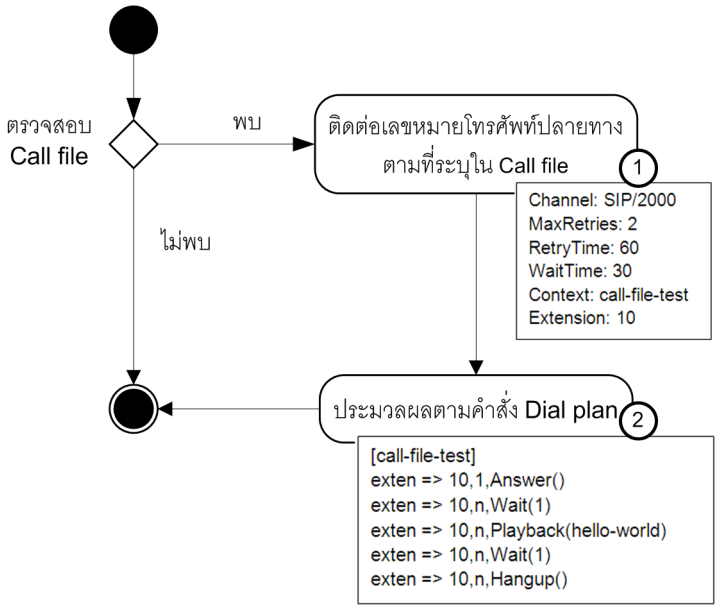
ขนาดของคีย์ (บิต)	จำนวนคีย์ที่เป็นไปได้ (ค่า)	เวลาที่ใช้ในการถอดรหัส ณ ความเร็ว 1 คีย์/μs	เวลาที่ใช้ในการถอดรหัส ณ ความเร็ว 1 ล้านคีย์/μs
32	$2^{32} = 4.3 \times 10^{9}$	2^{31} μs = 35.8 นาที	2.15 มิลลิวินาที
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 ปี	10.01 ชั่วโมง
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} ปี	5.4×10^{18} ปี
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} ปี	5.9×10^{30} ปี

2.1.6 เกตเวย์โทรศัพท์ที่พัฒนาด้วยซอฟต์แวร์แอสเทอริสก์

ซอฟต์แวร์โอเพนซอร์สแอสเทอริสก์ (Asterisk) [11] ช่วยให้สามารถพัฒนาจุดเชื่อมต่อ (หรือเกตเวย์) ระหว่างเครือข่ายคอมพิวเตอร์และเครือข่ายโทรศัพท์ได้โดยง่าย จึงสนใจนำมาประยุกต์ใช้เพื่อเพิ่มขยายการให้บริการของเครือข่ายยูพีแอนพีออกไปยังเครือข่ายโทรศัพท์ โดยซอฟต์แวร์นี้จะมีคำสั่งใช้งานเพื่อช่วยในการสร้างคุณลักษณะที่จำเป็นต่อการพัฒนางานให้เครื่องคอมพิวเตอร์ทั่วไปกลายเป็นระบบตอบรับโทรศัพท์อัตโนมัติ (Interactive Voice Response) ได้ ซึ่งในที่นี้ขออธิบายโดยสังเขปถึงวิธีการสั่งงานด้วยซอฟต์แวร์เพื่อให้เริ่มต้นการใช้โทรศัพท์ผ่านทางกลไกไดออลแพลน (Dial Plan) รวมถึงการระบุคำสั่งด้วยสคริปต์เอจีไอ (AGI ย่อมาจาก Asterisk Gateway Interface) ของซอฟต์แวร์แอสเทอริสก์ ซึ่งจะนำไปใช้ในการอธิบายการออกแบบในหัวข้อ **ผิดพลาด! ไม่พบแหล่งการอ้างอิง** ต่อไป

จากรูปที่ 2.10 แสดงให้เห็นวิธีการสั่งงานควบคุมให้ซอฟต์แวร์แอสเทอริสก์ เพื่อเรียกไปยังเลขหมายปลายทางแบบ SIP [12] เริ่มจากผู้ใช้กำหนดรายละเอียดของคำสั่งในการเรียกออกไปยังหมายเลขปลายทางลงในไฟล์แบบตัวอักษรที่ใช้ชื่อว่าคอลไฟล์ (Call File) ดังตัวอย่างในล้อมกรอบวงกลมหมายเลข 1 `Channel: SIP/2000` เป็นการระบุโทรศัพท์ติดต่อปลายทางเป็นโทรศัพท์แบบ SIP หมายเลขปลายทาง 2000 ตามด้วยพารามิเตอร์ที่จำเป็นอื่นๆ เช่น จำนวนครั้งของการเรียกซ้ำ (`MaxRetries`) ระยะเวลาในการรอสาย (`WaitTime`) และหมายเลขต้นทางที่จะเริ่มสนทนาด้วย (`Extension`) เป็นต้น เนื่องจากในตัวอย่างนี้มีค่าของหมายเลขที่จะสนทนากับโทรศัพท์แบบ SIP หมายเลข 200 ระบุเป็นค่า 10 ซึ่งหมายถึงโทรศัพท์หมายเลข 10 ดังนั้นเมื่อโทรศัพท์ SIP

ปลายทางมีการยกหูตอบรับ ซอฟต์แวร์แอสเทอริสก์ จึงดำเนินการตามคำสั่งสริปต์แบบเอจีไอ ที่กำหนดไว้ในไฟล์แบบตัวอักษรที่ใช้ชื่อว่า `Dial Plan` ดังตัวอย่างในล้อมกรอบวงกลมหมายเลข 2 เป็นชุดของสคริปต์ที่เริ่มด้วยการสั่งให้ตอบรับการเรียก (`Answer`) รอคอยนาน 1 วินาที (`Wait`) เล่นไฟล์เสียง (`Playback`) ที่บันทึกอยู่ในไฟล์ชื่อว่า `hello-world` รอคอยอีก 1 วินาที (`Wait`) และสิ้นสุดด้วยการวางหู (`Hangup`)



รูปที่ 2.10 การควบคุมการทำงานผ่านไฟล์ของซอฟต์แวร์แอสเทอริสก์

2.2 งานวิจัยที่เกี่ยวข้อง

2.2.1 การรองรับบริการแบบกลุ่มสื่อสารปลอดภัยบนระบบเครือข่ายยูพีแอนพี

วิทยานิพนธ์นี้ได้ศึกษางานวิจัยที่มีความเกี่ยวข้องกับการนำเสนอกลไกทำงานให้รองรับบริการแบบกลุ่มสื่อสารปลอดภัยในเครือข่ายยูพีแอนพี งานวิจัยของ Lee และคณะ [3] ได้แนะนำให้เห็นถึงข้อจำกัดด้านการรองรับบริการแบบกลุ่มสื่อสารปลอดภัยบนระบบเครือข่ายยูพีแอนพี พร้อมนำเสนอโพรโทคอลสำหรับการยืนยันตัวตนอุปกรณ์ขึ้นใหม่ ให้ชื่อว่า Secure UPnP (SUPnP) โดยระบุให้มีอุปกรณ์หลักตัวหนึ่งภายในระบบ รับทำหน้าที่เป็นศูนย์กลางในการยืนยันตัวตนอุปกรณ์ (ผ่านกลไกชื่อผู้ใช้และรหัสผ่าน) และประสานงาน เพื่อการส่งต่อข้อมูลกลุ่มแบบปลอดภัยทั้งหมด

ผ่านทางช่องสื่อสารพิเศษ (Secure Commmunication Channel) ที่แยกออกไปจากข้อมูลปกติ ดังนั้นจึงเกิดข้อด้อยทางสถาปัตยกรรมหลายประการ เช่น

- ปัญหาความล้มเหลวทั้งระบบจากความล้มเหลวที่ศูนย์กลางเพียงจุดเดียว
- ปัญหาความสิ้นเปลืองในการนำไปใช้งาน ที่เป็นผลสืบเนื่องจากการเข้ากันไม่ได้ (Incompatibility) ของโพรโทคอลที่นำเสนอขึ้นใหม่กับโพรโทคอลมาตรฐาน
- ปัญหาการไม่รองรับการให้บริการข้ามเครือข่ายยูพีแอนพี ทั้งนี้เนื่องจากไม่มีกลไกทำงานส่วนใดที่ช่วยจัดการข้อจำกัดทางสถาปัตยกรรมของเครือข่ายยูพีแอนพี

ดังนั้นแนวทางการวิจัยของวิทยานิพนธ์นี้ จึงศึกษาหาแนวทางการออกแบบและพัฒนาโพรโทคอลที่สามารถหลีกเลี่ยงปัญหาข้อด้อยในงานวิจัยของ Lee และคณะ (ดูตารางที่ 2.2 ประกอบ) ดังนี้

- ศึกษาการยืนยันตัวตนอุปกรณ์แบบพลวัต เพื่อที่สามารถจะกระจายศูนย์กลางของกลุ่มไปยังอุปกรณ์ใดๆ หากมีการล้มเหลวของอุปกรณ์ศูนย์กลางเดิมเกิดขึ้น
- ศึกษาการนำเทคนิคการกระจายคีย์ข้อมูลแบบกลุ่ม เพื่อทำงานร่วมในการเพิ่มขยายให้กับโพรโทคอลมาตรฐานของเครือข่ายยูพีแอนพี เพื่อความประหยัดในการนำไปใช้งาน

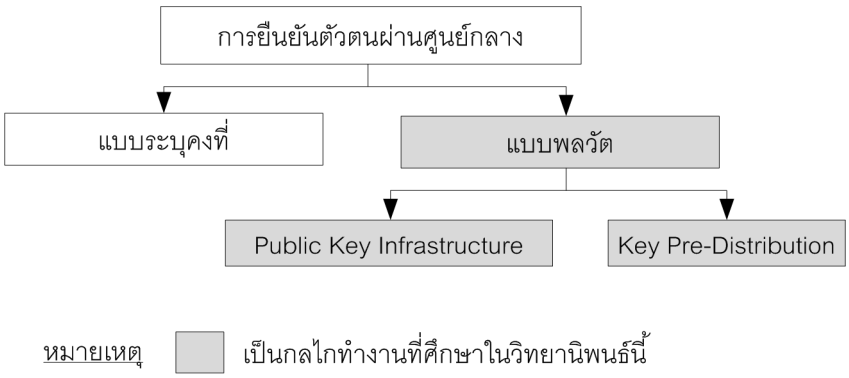
ตารางที่ 2.2 สรุปการเปรียบเทียบงานวิจัยที่เกี่ยวข้องกับแนวทางวิจัย

งานวิจัย	**สถาปัตยกรรม**	**การเพิ่มขยายโพรโทคอลยูพีแอนพี**	**กลไกการยืนยันตัวตนอุปกรณ์**
Lee และคณะ	มีศูนย์กลางการยืนยันตัวตนแบบระบุคงที่	ไม่ใช่	แบบพื้นฐาน (ชื่อผู้ใช้/รหัสผ่าน)
งานวิจัยในวิทยานิพนธ์นี้	มีศูนย์กลางการยืนยันตัวตนแบบพลวัต	ใช่	แบบกระจายคีย์ข้อมูลแบบกลุ่ม

2.2.2 การยืนยันตัวตนผ่านศูนย์กลางแบบพลวัตในกลุ่มสื่อสารปลอดภัย

เมื่อพิจารณาถึงแนวทางการแก้ปัญหาการล้มเหลวของระบบจากอุปกรณ์ศูนย์กลางเพียงจุดเดียวซึ่งได้กล่าวในหัวข้อที่ผ่านนั้น ปัญหาดังกล่าวสามารถลดลงได้จากการกำหนดให้มีศูนย์กลางในระบบได้หลายตัวแต่มีการเปลี่ยนกันทำหน้าที่แบบพลวัต โดยจะต้องอาศัยกลไกการยืนยันตัวตน

กันเอง เพื่อสร้างกลุ่มสื่อสารซึ่งอยู่บนพื้นฐานเทคนิควิธีการเข้ารหัสแบบพีเคไอ และเคพีดี (ดูรูปที่ 2.11 ประกอบ) เช่นที่พบในงานวิจัย ดังต่อไปนี้



รูปที่ 2.11 การจำแนกเทคนิคการยืนยันตัวตนผ่านศูนย์กลาง

งานวิจัยของ Byeong-Thaek และคณะ [13] นำเสนอให้เห็นถึงตัวอย่างในการนำใบรับรองอิเล็กทรอนิกส์ (Public Key Certificate) มาใช้ในการยืนยันตัวตนระหว่างกลุ่มอุปกรณ์ โดย Kerberos ทำหน้าที่เป็นตัวแจกใบรับรองอิเล็กทรอนิกส์และเทคนิควิธีพีเคไอ นำมาใช้เพื่อการเข้า/ถอดรหัสข้อมูลที่ระบุเฉพาะการสื่อสารภายในกลุ่มที่มีสิทธิเท่านั้น อย่างไรก็ตาม แม้ว่าเทคนิควิธีพีเคไอจะมีความเข้มแข็งในการป้องกันการเจาะรหัส แต่เนื่องจากพื้นฐานการทำงานของอัลกอริทึมในการเข้ารหัสแบบอสมมาตร (Asymmetric Cryptographic Algorithm) จึงมีความต้องการทรัพยากรในการประมวลผลสูง และอาจเป็นอุปสรรคต่อการนำไปใช้งานกับอุปกรณ์ที่มีทรัพยากรจำกัด ซึ่งงานวิจัยของ Ki-Woong และคณะ [14] ได้แสดงให้เห็นว่าหากมีการปรับปรุงเวลาที่ใช้ในกระบวนการยืนยันตัวตนอุปกรณ์แล้ว ก็สามารถที่จะนำเทคนิควิธีพีเคไอ ไปใช้ในสภาพแวดล้อมที่มีทรัพยากรจำกัดได้เช่นกัน

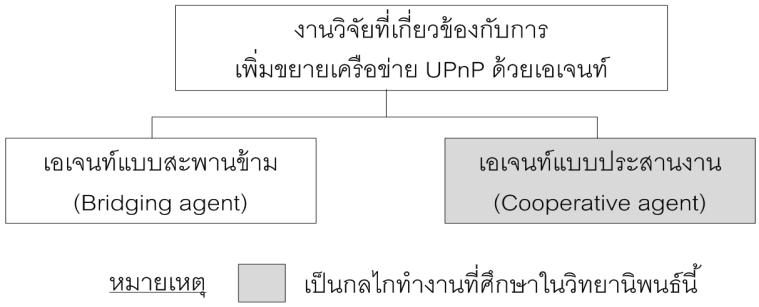
งานวิจัยของ Du และคณะ [9] แนะนำให้เห็นทางเลือกในการนำเทคนิควิธีเคพีดี เข้ามาใช้แทนที่เทคนิควิธีพีเคไอ เนื่องจากมีความเหมาะสมต่อการนำไปใช้ในการยืนยันตัวตนอุปกรณ์แบบพลวัตที่มีข้อจำกัดทางด้านทรัพยากรเช่นในเครือข่ายอุปกรณ์เซ็นเซอร์ไร้สาย แต่มีข้อด้อยด้านความเข้มแข็งในการป้องกันการเจาะรหัสข้อมูล สืบเนื่องจากพื้นฐานของอัลกอริทึมในการเข้ารหัสแบบ

สมมาตร (Symmetric Cryptographic Algorithm) ซึ่งงานวิจัยของ Ramkumar และ Memon [15] ได้นำเสนอแนวทางการปรับปรุงข้อด้อยของเทคนิควิธีเคพีดี นี้เช่นกัน

วิทยานิพนธ์นี้ได้สนใจการนำเทคนิควิธีทั้งแบบพีเคไอ และเคพีดี มาใช้กับการยืนยันตัวตนผ่านศูนย์กลางแบบพลวัตในกลุ่มสื่อสารปลอดภัย เพื่อศึกษาเปรียบเทียบด้านความรวดเร็วในการทำงาน เพื่อความเหมาะสมในการเพิ่มขยายโพรโทคอลต่างๆ ในสภาพแวดล้อมของเครือข่ายยูพีแอนพี

2.2.3 การเพิ่มขยายเครือข่ายยูพีแอนพีด้วยหน่วยการทำงานเอเจนท์

งานวิจัยส่วนมากที่เกี่ยวข้องกับการแก้ไขข้อจำกัดเชิงสถาปัตยกรรมของยูพีแอนพี ในการให้บริการข้ามเครือข่าย ใช้แนวทางการแก้ปัญหาผ่านกลไกทำงานเอเจนท์ซึ่งติดตั้งอยู่ที่บริเวณเกตเวย์ของเครือข่ายยูพีแอนพี อย่างไรก็ตาม หากจำแนกตามลักษณะงานที่ดำเนินการของเอเจนท์ [16] สามารถจะแบ่งออกได้เป็น 2 แนวทาง คือ แบบสะพานข้ามและแบบประสานงาน ดังแสดงในรูปที่ 2.12



รูปที่ 2.12 การเพิ่มขยายเครือข่ายยูพีแอนพีด้วยหน่วยการทำงานเอเจนท์

งานวิจัยที่นำแนวทางการทำงานของเอเจนท์แบบสะพานข้าม (Bridging Agent) มาใช้งานเพื่อการขยายขอบเขตการให้บริการของเครือข่ายยูพีแอนพีนั้น มักจะเป็นการทำงานในระดับการเชื่อมโยงข้อมูล (Link Level) ระหว่างเครือข่าย เพื่อแปลงข้อมูลสื่อสารจากโพรโทคอลในเครือข่ายยูพีแอนพี ให้เป็นโพรโทคอลในมาตรฐานอื่นที่สมนัยกัน จึงทำงานได้โดยใช้เอเจนท์เพียงตัวเดียวเท่านั้น ตัวอย่างเช่น การจับคู่ระหว่างโพรโทคอลค้นหาบริการ SSDP ในเครือข่ายยูพีแอนพีและโพรโทคอลค้นหาบริการ SLP ในงานวิจัยของ Chiewchan และ Witosurapot [4] หรือการจับคู่

ระหว่างโพรโทคอลค้นหาบริการ SSDP ในเครือข่ายยูพีแอนพีและโพรโทคอลค้นหาบริการ Jini จากโปรแกรมประยุกต์ทางด้านเครือข่ายที่พัฒนาขึ้นด้วยภาษาจาวา ในงานวิจัยของ Allard และคณะ [5] เป็นต้น

งานวิจัยที่นำแนวทางการทำงานของเอเจนท์แบบประสานงาน (Cooperative Agent) มักเป็นการทำงานในระดับบริการ (Service Level) เพื่อการส่งผ่านข้อมูลสื่อสารที่ต้องการ จึงต้องการเอเจนท์ในทั้งสองเครือข่าย เพื่อประสานงานร่วมกัน ตัวอย่างเช่นการประสานงานในระดับแอพพลิเคชันกับเครือข่ายยูพีแอนพีและงานประยุกต์ทางด้านเครือข่าย Jini ในงานวิจัยของ Lin และคณะ [16] หรือการประสานงานเพื่อจัดการทรัพยากรระหว่างหน่วยทำงานเอเจนท์หลายตัวในงานวิจัยของ Chira และ Dumitrescu [17] เป็นต้น ดังนั้น ในบริบทของการเพิ่มขยายบริการของเครือข่ายยูพีแอนพี ให้ทำงานร่วมได้กับเครือข่ายโทรศัพท์พื้นฐานซึ่งต่างเทคโนโลยีกัน ดังที่จะได้ศึกษาวิจัยในวิทยานิพนธ์นี้ จึงได้พิจารณาเลือกใช้แนวทางการทำงานของเอเจนท์แบบประสานงานเพื่อให้สามารถส่งผ่านสถานะการควบคุมระหว่างเครือข่ายทั้งสองนั้น

บทที่ 3

วิธีดำเนินการวิจัย

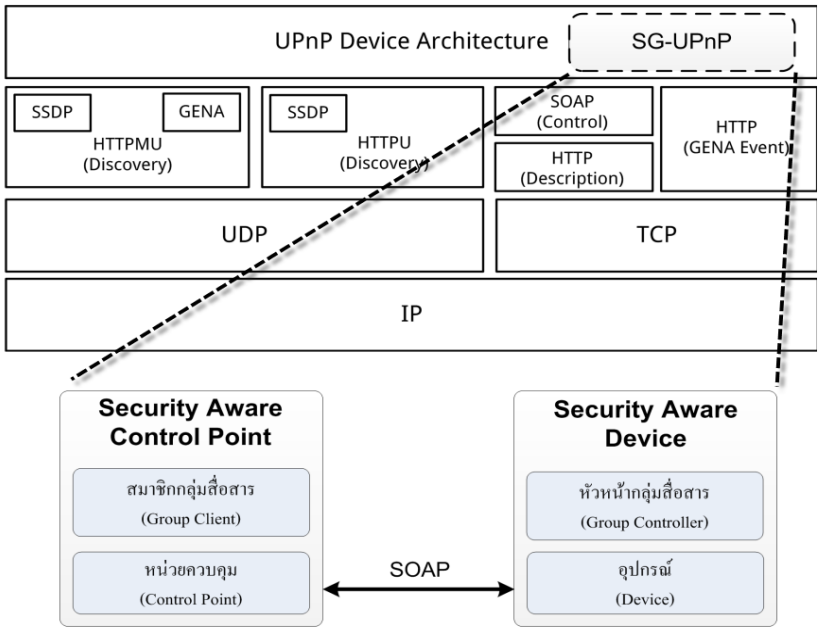
ในบทนี้เป็นการกล่าวถึงรายละเอียดกลไกทำงานเพื่อแก้ปัญหาต่างๆ ซึ่งได้อธิบายในบทที่ผ่านมา โดยจะเริ่มจากการอธิบายแนวทางการเพิ่มขยายโพรโทคอลสื่อสารปลอดภัยด้วยเทคนิคการยืนยันตัวด้วยเทคนิควิธีเคพีดี หลังจากนั้น จะเป็นการอธิบายถึงกลไกการทำงานเพื่อประสานงานผ่านเอเจนท์ระหว่างเครือข่ายยูพีแอนพีกับเครือข่ายโทรศัพท์ เพื่อแสดงให้เห็นว่ากลไกที่นำเสนอในงานวิจัยนี้สามารถทำงานกับเครือข่ายต่างประเภทได้เช่นกัน

1.1 การออกแบบกลไกบริการสำหรับกลุ่มสื่อสารปลอดภัยในเครือข่ายยูพีแอนพี

1.1.1 แนวความคิดและสถาปัตยกรรมระบบ

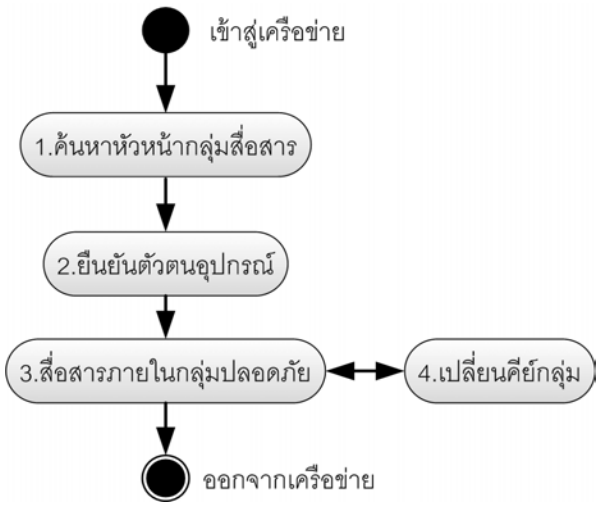
กลไกบริการกลุ่มสื่อสารปลอดภัยที่ออกแบบขึ้นเรียกว่าเอสจี-ยูพีแอนพี (SG-UPnP ย่อมาจาก Secure Group UPnP) ซึ่งต่อไปในวิทยานิพนธ์นี้จะเรียกว่าเอสจี-ยูพีแอนพี โดยมีแนวคิดการออกแบบด้วยการเพิ่มเติมบนลำดับชั้นโพรโทคอล UPnP Device Architecture ของมาตรฐานเครือข่ายยูพีแอนพีเดิม (ดูรูปที่ 1.1) ทำให้ได้หน่วยควบคุมและอุปกรณ์แบบใหม่ ซึ่งรองรับการสื่อสารแบบกลุ่มปลอดภัยในระดับบริการ (Service-level Security) ได้ ดังนี้

- *เอสเอดี (SAD ย่อมาจาก Security Aware Device)* ออกแบบขึ้นโดยการรวมหน่วยการทำงานอุปกรณ์เดิม กับหน่วยการทำงานหัวหน้ากลุ่มสื่อสาร (Group Controller) เพื่อทำงานเป็นหัวหน้ากลุ่มสื่อสาร ด้วยบริการกลุ่มสื่อสารปลอดภัยที่สื่อสารผ่านโพรโทคอล SOAP
- *เอสเอซี (SAC ย่อมาจาก Security Aware Control Point)* ออกแบบขึ้นโดยรวมหน่วยการทำงานที่เป็นหน่วยควบคุมเดิม กับหน่วยการทำงานสมาชิกกลุ่มสื่อสาร (Group Client) เพื่อให้สามารถสื่อสารผ่านบริการกลุ่มสื่อสารปลอดภัยได้



รูปที่ 1.1 ลำดับชั้นโพรโทคอลของเอสจี-ยูพีแอนพี บนมาตรฐานของเครือข่ายยูพีแอนพี

ดังนั้นการรักษาความปลอดภัยในระดับบริการของเครือข่ายเอสจี-ยูพีแอนพีที่นำเสนอนั้น จึงสามารถสื่อสารกับอุปกรณ์ของเครือข่ายยูพีแอนพีแบบธรรมดาได้ โดยจะรับทราบว่ามีบริการแบบกลุ่มปลอดภัย แต่ก็ไม่สามารถเรียกใช้งานได้ เนื่องจากผลการเข้ารหัสข้อมูลสื่อสาร



รูปที่ 1.2 ลำดับการเปลี่ยนสถานะของการทำงานในเครือข่ายเอสจี-ยูพีแอนพี

จากรูปที่ 1.2 แสดงการทำงานของสถานะการทำงานของอุปกรณ์เอสเอดี และเอสเอซี จำนวน 4 สถานะ ดังต่อไปนี้

1. *สถานะการค้นหาหัวหน้ากลุ่มสื่อสาร* เริ่มต้นเมื่อเอสเอซีเชื่อมต่อเข้าสู่เครือข่าย (Join) เพื่อค้นหาหัวหน้ากลุ่มสื่อสาร
2. *สถานะการยืนยันตัวตนอุปกรณ์* เกิดขึ้นเมื่อเอสเอซียืนยันตัวตนอุปกรณ์กับเอสเอดี เพื่อรับคีย์กลุ่มที่ใช้ในกลุ่มสื่อสารปลอดภัย
3. *สถานะการสื่อสารภายในกลุ่มปลอดภัย* เกิดขึ้นเมื่อมีการสื่อสารข้อมูลบริการแบบปลอดภัยระหว่างเอสเอซีกับเอสเอดี
4. *สถานะการเปลี่ยนคีย์กลุ่ม* เกิดขึ้นเมื่อมีการเปลี่ยนแปลงของสมาชิกภายในกลุ่ม ซึ่งจะส่งผลทำให้มีการคำนวณและกระจายคีย์กลุ่มใหม่ไปสู่สมาชิกโดยเอสเอดี

จากตารางที่ 1.1 แสดงให้เห็นถึงลำดับขั้นตอนของการสื่อสารกลุ่มปลอดภัย ซึ่งได้บูรณาการเข้ากับกระบวนการทำงานเดิมของเครือข่ายยูพีแอนพี เพื่อสร้างความกระชับของระบบงานโดยรวมและช่วยให้เกิดคุณลักษณะความเข้ากันได้ของการทำงานร่วมระหว่างอุปกรณ์ตามมาตรฐานเดิมกับที่เพิ่มขยายขึ้นใหม่อีกด้วย ตัวอย่างเช่น ในขั้นตอนของการค้นหาหัวหน้ากลุ่มสื่อสาร ก็จะดำเนินการให้เสร็จสิ้นภายในกระบวนการทำงานค้นหาบริการของเครือข่ายยูพีแอนพีไปพร้อมกัน เป็นต้น สำหรับการทำงานโดยละเอียดในขั้นตอนเหล่านี้จะได้อธิบายในหัวข้อถัดไป

ตารางที่ 1.1 ขั้นตอนการสื่อสารของกลุ่มสื่อสารปลอดภัยกับของเครือข่ายยูพีแอนพี

ลำดับ	**สถานะทำงานของกลุ่มสื่อสารปลอดภัย**	**กระบวนการภายในเครือข่ายยูพีแอนพี**
1	การค้นหาหัวหน้ากลุ่มสื่อสาร	กระบวนการค้นหาบริการ (Discovery)
2	การยืนยันตัวตนอุปกรณ์	กระบวนการควบคุม/สั่งการ (Control)
3	การเปลี่ยนคีย์กลุ่ม	กระบวนการแจ้งเตือนเหตุการณ์ (Eventing) และ กระบวนการควบคุม/สั่งการ (Control)
4	การสื่อสารภายในกลุ่มปลอดภัย	กระบวนการควบคุม/สั่งการ (Control)

1.1.2 การเพิ่มขยายโพรโทคอลที่เกี่ยวข้องเพื่อรองรับกลุ่มสื่อสารปลอดภัย

1.1.2.1 การติดตั้งข้อมูลเกี่ยวกับคีย์ล่วงหน้า

กลไกเข้ารหัสเคพีดี จะต้องมีการติดตั้งข้อมูลเกี่ยวกับคีย์บางส่วนเอาไว้ล่วงหน้า จากเครื่องแม่ข่าย TA ซึ่งผู้ดูแลระบบจะดำเนินการติดตั้งบนอุปกรณ์ในครั้งแรกก่อนนำไปใช้งาน ในขั้นตอนนี้เป็นการบันทึกลงที่ตัวอุปกรณ์โดยตรงในลักษณะไฟล์ที่บันทึกข้อมูลเกี่ยวกับคีย์ เนื่องจากดำเนินการเพียงครั้งเดียว ดังนั้นขั้นตอนดังกล่าวจึงไม่ขัดแย้งกับกระบวนการทำงานอัตโนมัติของเครือข่ายยูพีแอนพี นอกจากนี้การขโมยข้อมูลจากอุปกรณ์โดยตรงสามารถทำได้ยากเนื่องจากลักษณะของอุปกรณ์ที่ใช้งานอยู่ภายในบ้านพักอาศัย

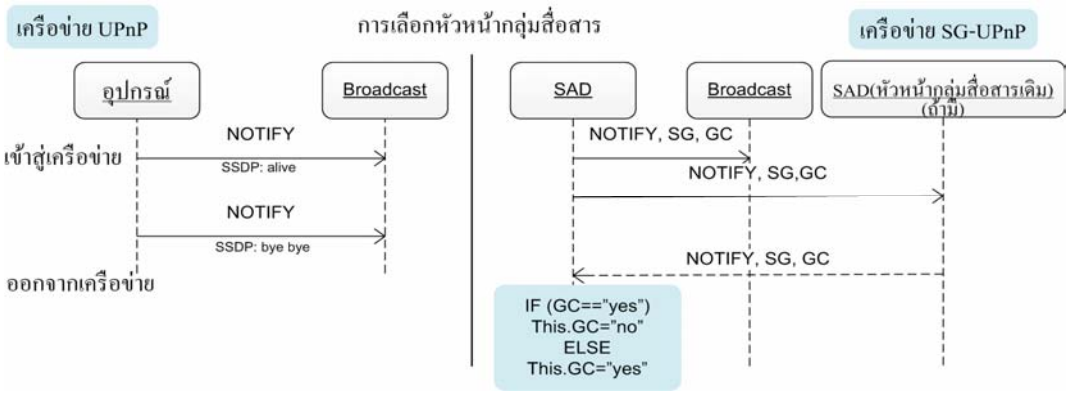
1.1.2.2 อัลกอริทึมการค้นหาเพื่อเลือกหัวหน้ากลุ่มสื่อสาร

ข้อความ NOTIFY และ M-SEARCH ของเครือข่ายเอสจี-ยูพีแอนพี จะถูกเพิ่มเติมเนื้อหาส่วนหัว ได้แก่ SG และ GC ดังแสดงในรูปที่ 1.3 (ตัวหนา) โดย <device secure group id> แสดงหมายเลขของกลุ่มสื่อสาร ซึ่งถูกกำหนดเอาไว้ล่วงหน้าในขั้นตอนการติดตั้งคีย์ครั้งแรก ส่วน <yes/no> ใช้บอกสถานะว่าเป็นหัวหน้ากลุ่มสื่อสารหรือไม่

```
NOTIFY * HTTP/1.1
HOST: 239.255.255.250:1900
CACHE-CONTROL: <max-age>
LOCATION: <url of device description>
NT: <search target>
NTS: <ssdp:alive/ssdp:bye bye>
SG: <device secure group id>
GC: <yes/no>
```

รูปที่ 1.3 ข้อความ NOTIFY ที่ถูกปรับแต่ง

เมื่ออุปกรณ์เชื่อมต่อเข้าสู่เครือข่ายเอสจี-ยูพีแอนพี จะมีการค้นหาหัวหน้ากลุ่มสื่อสารจากภายในเครือข่าย โดยอาศัยการเพิ่มเติมข้อความในกระบวนการค้นหาบริการของเครือข่ายยูพีแอนพีเดิม เพื่อให้สามารถเลือกทำหน้าที่เป็นหัวหน้ากลุ่มสื่อสารได้



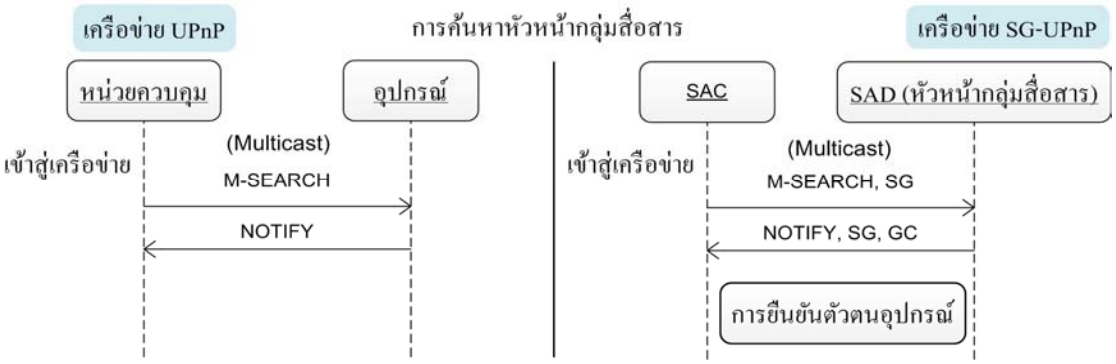
รูปที่ 1.4 การเลือกหัวหน้ากลุ่มสื่อสารของเครือข่ายเอสจี-ยูพีแอนพี

จากรูปที่ 1.4 ขั้นตอนการเลือกหัวหน้ากลุ่มสื่อสารมีดังนี้

1) เอสเอดีผู้ร้องขอส่งข้อความ NOTIFY ที่เพิ่มเติมเนื้อหาในส่วนหัว ได้แก่ GC (เครื่องหมายระบุความเป็นหัวหน้ากลุ่มสื่อสาร) และ SG (หมายเลขกลุ่ม) โดยเมื่อต้องการร้องขอออกไปในเครือข่ายเพื่อทำหน้าที่หัวหน้ากลุ่มสื่อสารจะส่งค่า GC:yes ออกไป
2) เอสเอดีผู้ร้องขอจะได้รับข้อความ NOTIFY ที่มี GC: yes และ SG ตรงกัน แต่ถ้ากลุ่มนั้นมีเอสเอดี ที่ทำหน้าที่เป็นหัวหน้ากลุ่มสื่อสารอยู่ก่อนแล้วเอสเอดี ผู้ร้องขอก็จะทำหน้าที่เป็นสมาชิกกลุ่มสื่อสารธรรมดาโดยค่า GC จะถูกปรับเป็น GC: no

การค้นหาหัวหน้ากลุ่มสื่อสารเกิดขึ้นเมื่อเอสเอซี เชื่อมต่อเข้าสู่เครือข่ายเอสจี-ยูพีแอนพี โดยมีขั้นตอนดังแสดงในรูปที่ 1.5 ดังต่อไปนี้

1) เอสเอซีส่งข้อความ M-SEARCH ที่เพิ่มเติมเนื้อหาส่วนหัว คือ SG ของอุปกรณ์ชิ้นนั้น ซึ่งส่วนเพิ่มเติมดังกล่าว จะไม่ถูกประมวลผลโดยอุปกรณ์ตามมาตรฐานเครือข่ายยูพีแอนพีเดิม จึงสามารถค้นหาอุปกรณ์ทั้ง 2 แบบไปได้พร้อมๆ กัน
2) เอสเอดีซึ่งทำหน้าที่หัวหน้ากลุ่มสื่อสารนั้น จะตอบกลับที่อยู่ของตัวเอง เพื่อให้เอสเอซีเข้ายืนยันตัวตนอุปกรณ์เข้าสู่กลุ่มสื่อสาร



รูปที่ 1.5 การค้นหาหัวหน้ากลุ่มสื่อสารของเครือข่ายเอสจี-ยูพีแอนพี

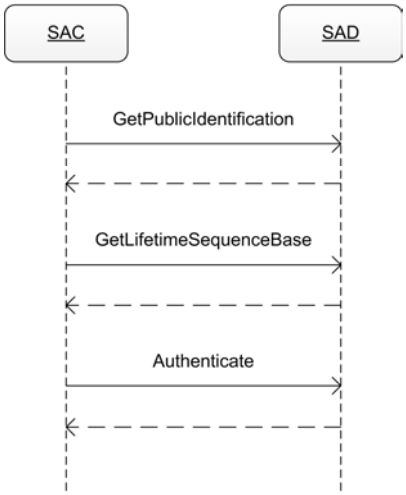
การเปลี่ยนหัวหน้ากลุ่มสื่อสารเกิดขึ้น 2 กรณี ได้แก่ กรณีหัวหน้ากลุ่มสื่อสารออกจากเครือข่ายโดยแจ้งให้สมาชิกทราบก่อนล่วงหน้า และกรณีหัวหน้ากลุ่มสื่อสารออกจากเครือข่ายโดยไม่แจ้งให้ทราบล่วงหน้า ในกรณีแรกจะมีขั้นตอนการเปลี่ยนหัวหน้ากลุ่มสื่อสาร ดังต่อไปนี้

1) เอสเอดีหัวหน้ากลุ่มสื่อสารส่งข้อความ `NOTIFY` ซึ่งมี `ssdp: bye bye` ให้กับสมาชิกภายในเครือข่าย
2) เอสเอดีอื่นในเครือข่าย เริ่มกระบวนการเลือกหัวหน้ากลุ่มสื่อสารใหม่อัตโนมัติ เมื่อได้รับข้อความแจ้งจากหัวหน้ากลุ่มสื่อสารเดิม

กรณีหัวหน้ากลุ่มสื่อสารออกจากเครือข่ายโดยไม่มีการแจ้งให้ทราบก่อนล่วงหน้า สมาชิกภายในเครือข่ายอาศัยการตรวจสอบเวลาอายุขัยของข้อความประกาศ (Lease Time) จากหัวหน้ากลุ่มสื่อสาร ถ้าหากไม่มีการประกาศซ้ำภายในเวลาที่กำหนด จะเริ่มกระบวนการเลือกหัวหน้ากลุ่มสื่อสารใหม่เองโดยอัตโนมัติ

1.1.2.3 กระบวนการยืนยันตัวตนของอุปกรณ์

หลังจากเอสเอซีค้นพบหัวหน้ากลุ่มสื่อสารแล้ว เป็นขั้นตอนการยืนยันตัวตนอุปกรณ์ เพื่อรับคีย์กลุ่มจากเอสเอดี กระบวนการนี้ใช้พื้นฐานจากเทคนิคการเข้ารหัสแบบเคพีดี และทำการสื่อสารด้วยโพรโทคอล SOAP ที่เป็นมาตรฐานเดิมของเครือข่ายยูพีแอนพี



รูปที่ 1.6 ลำดับการสื่อสารเพื่อยืนยันตัวตนอุปกรณ์

จากรูปที่ 1.6 การยืนยันตัวตนอุปกรณ์มีลำดับดังนี้

1) เอสเอซีและเอสเอดีใช้คำสั่ง `GetPublicIdentification()` เพื่อแลกเปลี่ยน `PID` โดยส่งค่า `PID` ประจำตัวอุปกรณ์ไปเป็นตัวแปรพารามิเตอร์ ซึ่งหากคู่อุปกรณ์เป็นสมาชิกกลุ่มเดียวกันจะสามารถใช้ `PID` ของอีกฝ่ายในการคำนวณคีย์คู่ร่วมกันได้
2) เอสเอซีใช้คำสั่ง `GetLifeTimeSequenceBase()` เพื่อร้องขอค่าของตัวแปร `SequenceBase` จากเอสเอดี ด้วยคำสั่ง เพื่อใช้ประกอบในการยืนยันตัวตน โดยค่าตัวแปรนี้ใช้ป้องกันการโจมตีระบบแบบเล่นซ้ำ (Replay attack) จากอุปกรณ์ที่ดักจับข้อความสื่อสารในเครือข่าย จึงเปลี่ยนไปทุกครั้งของการสื่อสาร
3) เอสเอซียืนยันตัวกับเอสเอดี ด้วยคำสั่ง `Authenticate()` โดยมีพารามิเตอร์ 3 ตัว ดังนี้ `ControlPointID SequenceBase` และ `AuthSecret` ซึ่งเป็นผลลัพท์จากฟังก์ชัน `Hash(SequenceBase, PairwiseSecretKey)` ที่เป็นลักษณะฟังก์ชันทางเดียว (One-way Function) เพื่อตรวจสอบค่า `PairwiseSecretKey` โดยไม่ต้องส่งค่าจริงออกไปในเครือข่าย ค่าดังกล่าวจะถูกนำไปเปรียบเทียบกับค่าที่คำนวณได้จากเอสเอดี

1.1.2.4 กระบวนการเข้าร่วมกลุ่มสื่อสาร

หลังจากการยืนยันตัวตนอุปกรณ์แล้ว คีย์กลุ่มเดิมจะต้องถูกเปลี่ยนใหม่ (Rekey) เพื่อรักษาความลับจากอุปกรณ์ที่เข้ามาใหม่ ซึ่งอาจสามารถถอดรหัสข้อความสื่อสารย้อนหลังได้ (Backward Secrecy) โดยการเปลี่ยนคีย์กลุ่ม ในที่นี้จะอาศัยพื้นฐานโพรโทคอลในเครือข่ายยูพีแอนพีเดิม โดยทำได้ 2 แนวทาง ได้แก่

- *การกระจายคีย์กลุ่มให้สมาชิกทั้งหมดในคราวเดียว* แนวทางนี้จะต้องปรับแต่งกลไกแจ้งเตือนเหตุการณ์ของเครือข่ายยูพีแอนพี ให้รองรับการแจ้งเตือนเหตุการณ์ผ่านโพรโทคอล GENA (แบบมัลติคาสก์) ซึ่งต้องดัดแปลงไลบรารีของเครือข่ายยูพีแอนพี
- *การกระจายคีย์กลุ่มให้สมาชิกทีละตัวตามลำดับ* แนวทางนี้สามารถใช้การแจ้งเตือนเหตุการณ์ของเครือข่ายยูพีแอนพีเดิมผ่านโพรโทคอล GENA (แบบยูนิคาสก์) ซึ่งรองรับโดยไลบรารีของเครือข่ายยูพีแอนพีเดิม

อย่างไรก็ตาม เนื่องจากลักษณะของการแจกคีย์กลุ่มให้สมาชิกทีละตัวๆ ตามลำดับ ทำให้เครือข่ายยูพีแอนพี ซึ่งมีจำนวนอุปกรณ์ไม่มากนักมีผลกระทบต่อกลุ่มสื่อสารโดยรวมน้อยกว่าเครือข่ายมีขนาดใหญ่แบบอื่นๆ ดังนั้น กลไกต้นแบบที่เสนอในวิทยานิพนธ์นี้ จึงพิจารณาใช้การแจ้งเตือนเหตุการณ์ตามมาตรฐานของเครือข่ายยูพีแอนพีเดิม

1.1.2.5 กระบวนการออกจากกลุ่มสื่อสาร

กระบวนการนี้ใช้หลักการเดียวกับกระบวนการเข้าร่วมกลุ่มสื่อสาร โดยการเปลี่ยนคีย์กลุ่มใหม่จะต้องดำเนินการทุกครั้งเมื่อมีสมาชิกออกจากกลุ่ม เพื่อรักษาความลับภายในกลุ่มจากสมาชิกที่ออกจากกลุ่มไปแล้ว ไม่ให้สามารถถอดรหัสการสื่อสารได้อีกต่อไป (Forward Secrecy) ดังนั้น ในกระบวนการนี้หัวหน้ากลุ่มสื่อสารจะต้องส่งคีย์กลุ่มให้กับสมาชิกภายในกลุ่มทีละตัวๆ ซึ่งต้องใช้การเข้ารหัสด้วยคีย์คู่ระหว่างหัวหน้ากลุ่มสื่อสารกับสมาชิกนั้นๆ

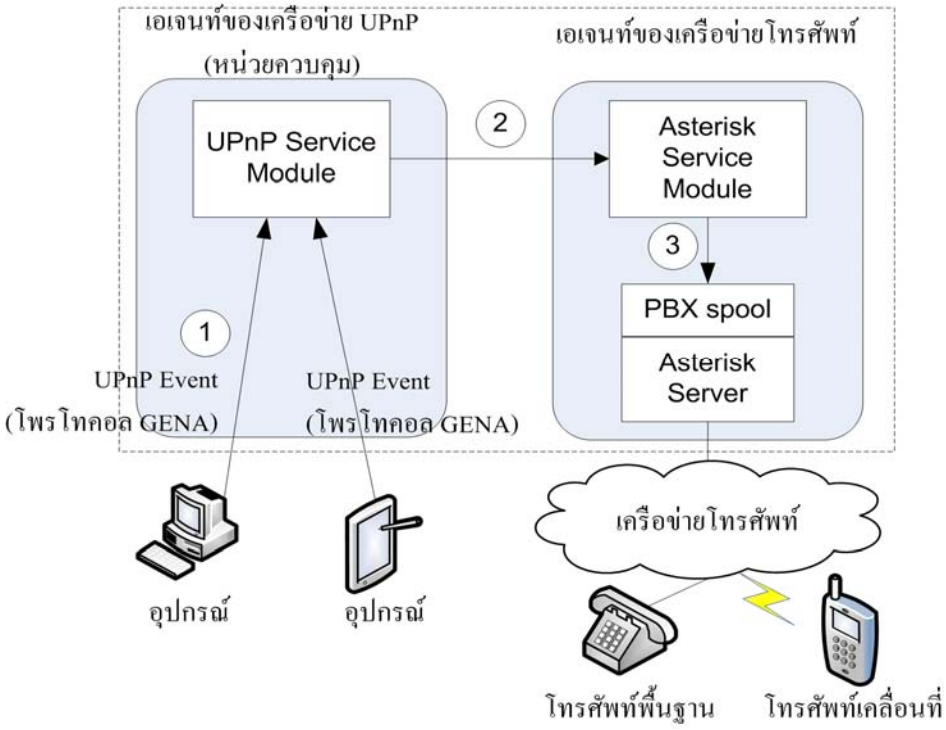
1.2 การออกแบบกลไกประสานการทำงานระหว่างเอเจนท์ของคู่เครือข่าย

1.2.1 แนวความคิดและสถาปัตยกรรมระบบ

กลไกทำงานเพื่อเพิ่มขยายบริการของเครือข่ายยูพีแอนพีให้ทำงานร่วมกับเครือข่ายโทรศัพท์พื้นฐาน อาศัยหน่วยทำงานเอเจนท์ซึ่งทำหน้าที่อ่านสถานะของบริการบนอุปกรณ์ภายใน

เครือข่ายยูพีแอนพี และทำงานประสานกับหน่วยทำงานเอเจนท์ที่เกตเวย์โทรศัพท์ เพื่อส่งต่อสถานะหรือรับคำสั่งควบคุมจากผู้ใช้ผ่านทางอุปกรณ์โทรศัพท์ ดังนั้น สถาปัตยกรรมของระบบดังกล่าวจึงมี 2 ส่วน ได้แก่ หน่วยทำงานเอเจนท์ของเครือข่ายยูพีแอนพีและของเครือข่ายโทรศัพท์ ดังแสดงในรูปที่ 1.7 ซึ่งจะถูกติดตั้งที่เครื่องเกตเวย์โทรศัพท์ โดยมีรายละเอียดดังนี้

- *เอเจนท์ของเครือข่ายยูพีแอนพี:* ทำงานโดยมีหน่วยควบคุม (UPnP Service Module) ทำหน้าที่รอรับการแจ้งเตือนเหตุการณ์จากอุปกรณ์ที่สนใจในเครือข่ายยูพีแอนพี โดยจะต้องมีการตั้งค่าเกี่ยวกับสถานะบริการที่สนใจไว้ล่วงหน้า (ดูรูปที่ 1.7 วงกลมหมายเลข 1 ประกอบ)
- *เอเจนท์ของเครือข่ายโทรศัพท์:* ทำงานโดยมีหน่วยบริการซอฟต์แวร์แอสเทอริสก์ (Asterisk Service Module) ทำหน้าที่รอรับการแจ้งเตือนเหตุการณ์ต่อจากหน่วยทำงานเอเจนท์ของเครือข่ายยูพีแอนพี (วงกลมหมายเลข 2) และเปลี่ยนเป็นสัญญาณเสียงพูดเพื่อแจ้งเตือนเหตุการณ์ไปยังอุปกรณ์ในเครือข่ายโทรศัพท์พื้นฐาน ด้วยการส่งคำสั่งควบคุมไปที่ `PBX Spool` ของเครื่องแม่ข่ายแอสเทอริสก์ (วงกลมหมายเลข 3)

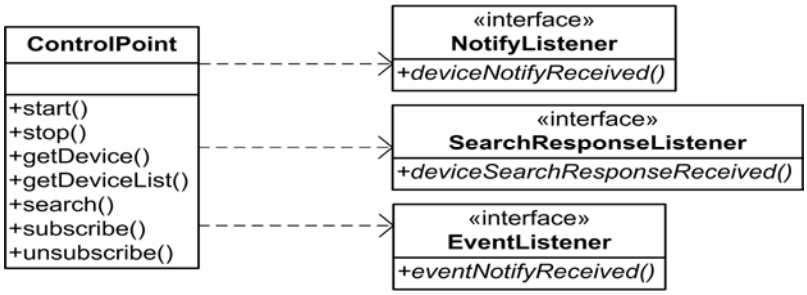


รูปที่ 1.7 สถาปัตยกรรมประสานงานของหน่วยการทำงานแบบเอเจนท์

1.2.2 กรณีศึกษา: การเตือนด้วยเสียงพูดไปยังเครื่องโทรศัพท์ที่ต้องการ

1.2.2.1 การออกแบบเอเจนท์ของเครือข่ายยูพีแอนพี

เอเจนท์ของเครือข่ายยูพีแอนพีออกแบบบนพื้นฐานไลบรารี CyberLink for Java [18] ซึ่งใช้สำหรับพัฒนาหน่วยควบคุมและอุปกรณ์ตามมาตรฐานของเครือข่ายยูพีแอนพี เนื่องจากง่ายต่อการใช้งานและมีการปรับปรุงพัฒนาให้ทันสมัยอยู่เสมอ ดังนั้น เอเจนท์ของเครือข่ายยูพีแอนพี จึงใช้งานหน่วยควบคุมซึ่งมีแผนภาพที่ใช้แสดงคลาสดังรูปที่ 1.8



รูปที่ 1.8 แผนภาพที่ใช้แสดงคลาสของหน่วยควบคุม [18]

การพัฒนาคลาส `ControlPoint` ต้องพัฒนาส่วนของโปรแกรมตามที่กำหนดเอาไว้ใน `Interfaces` ดังต่อไปนี้

- `NotifyListener` ทำหน้าที่รับการแจ้งเตือน เมื่ออุปกรณ์เข้า/ออกจากเครือข่าย
- `SearchResponseListener` ทำหน้าที่รับข้อความตอบกลับ จากการค้นหาอุปกรณ์
- `EventListener` ทำหน้าที่รับการแจ้งเตือนเหตุการณ์ เมื่อมีการเปลี่ยนแปลงสถานะของอุปกรณ์ที่สมัครรับการแจ้งเตือนเอาไว้

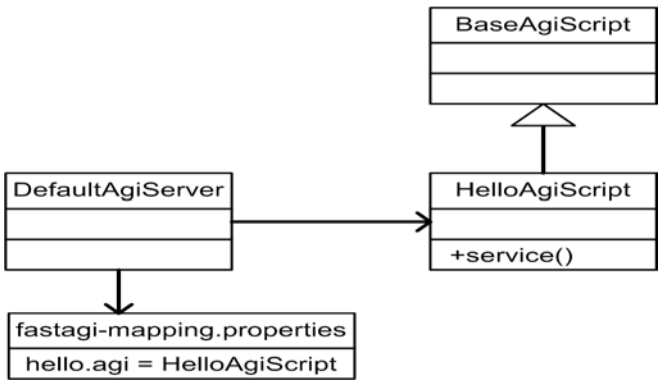
จากรูปที่ 1.9 การตรวจสอบสถานะที่อุปกรณ์แจ้งเตือน เพื่อประสานกับเอเจนท์ของเครือข่ายโทรศัพท์ต่อไป ได้ถูกกำหนดไว้ในฟังก์ชัน `eventNotifyRecieved()` โดยมีลำดับดังนี้

1) ตรวจสอบชื่ออุปกรณ์และสถานะของการแจ้งเตือนว่าตรงเงื่อนไขที่ต้องการหรือไม่
2) ประสานไปยังเอเจนท์ของเครือข่ายโทรศัพท์ หากมีเงื่อนไขตรงตามที่กำหนด โดยเรียกใช้ฟังก์ชัน `makeCallFile()` ซึ่งจะสร้างคอลไฟล์ตามที่ตั้งค่าเอาไว้ล่วงหน้า

และย้ายไปใน PBX spool (/var/spool/asterisk/outgoing/) เพื่อส่งคำสั่งให้เครื่องแม่ข่ายแอสเทอริสก์ ดำเนินการต่อ ในส่วนที่เป็นเอเจนท์ของเครือข่ายโทรศัพท์

```
01. public void eventNotifyReceived(String uuid, long seq,
02.                                 String varName, String value) {
03.     Device device;
04.     String friendlyName = "";
05.     Service service =  controlPoint.getSubscriberService(uuid);
06.
07.     if ((varName != null) && (value.length() < 0)){
08.           //Trace back to check what a device is
09.           device = service.getDevice();
10.           friendlyName = device.getFriendlyName();
11.      }
12.      if ((value.equals("Finish") && friendlyName.equals ("My Device")) {
13.           makeCallFile();
14.      }
15. }
16.
17. // Create a call file
18. // then move it to the PBX spooling directory
19. private void makeCallFile(){
20.      ...
21. }
```

รูปที่ 1.9 ตัวอย่างซอร์สโค้ดของฟังก์ชัน EventListener



รูปที่ 1.10 แผนภาพที่ใช้แสดงคลาสของสคริปต์เอจีไอ

1.2.2.2 สคริปต์เอจีไอและโปรแกรมประยุกต์จาวา

เอเจนท์ของเครือข่ายโทรศัพท์ทำงานโดยการสั่งควบคุมซอฟต์แวร์แอสเทอริสก์ เป็นหลักโดยสคริปต์เอจีไอ ที่กำหนดเอาไว้จะถูกเรียก เมื่อมีการแจ้งเตือนเหตุการณ์จากเอเจนท์ของเครือข่ายยูพีแอนพี ในที่นี้จะเลือกพัฒนาสคริปต์เอจีไอ ด้วยไลบรารี Asterisk-Java [19] โดยสคริปต์เอจีไอ มีแผนภาพคลาส ดังแสดงในรูปที่ 1.10

- `DefaultAgiServer` เป็นคลาสของโปรแกรมหลักที่จะรอรับการแจ้งเตือนเหตุการณ์จากเอเจนท์ของเครือข่ายยูพีแอนพี
- `fastagi-mapping.propoerties` เป็นไฟล์สำหรับกำหนดการจับคู่สคริปต์เอจีไอ กับคลาสที่ทำงาน เช่น `hello.agi = HelloAgiScript` หมายถึง ให้เรียกคลาส `HelloAgiScript` ขึ้นมาทำงาน เมื่อเรียกสคริปต์ชื่อ `hello.agi`
- `HelloAgiScript` เป็นคลาสที่สืบทอดมาจาก `BaseAgiScript` ของไลบรารี Asterisk-Java ซึ่งจะถูกเรียกใช้งานโดยคลาส `DefaultAgiServer` เพื่อเริ่มทำงานสคริปต์เอจีไอ ที่กำหนดไว้ในฟังก์ชัน `service()`

ตัวอย่างจากรูปที่ 1.11 ของคลาส `HelloAgiScript` เริ่มทำงานจะส่งคำสั่งเอจีไอ ไปยังซอฟต์แวร์แอสเทอริสก์ สั่งให้รับสาย เล่นไฟล์เสียงที่ชื่อ `welcome` และวางสาย โดยไฟล์เสียงดังกล่าวจะต้องถูกบันทึกเอาไว้ล่วงหน้าที่เครื่องแม่ข่ายแอสเทอริสก์ ดังนั้น ผู้พัฒนาระบบจะต้องกำหนดชื่อไฟล์เสียงที่ตรงกับข้อความแจ้งเตือนเอาไว้ก่อนล่วงหน้า

1.2.2.3 คำสั่งควบคุมในคอลไฟล์และไดออลแพลน

วิธีการเพื่อให้เลขหมายปลายทางได้เชื่อมต่อกับโปรแกรมต้นทางที่ทำงานด้วยสคริปต์เอจีไอ ให้ถูกต้องสามารถทำได้โดยการตั้งค่าลงในคอลไฟล์ และไดออลแพลน ซึ่งเอเจนท์ของเครือข่ายยูพีแอนพีจะสร้างคอลไฟล์ดังกล่าว และย้ายไปใน `PBX Spool` ต่อมาซอฟต์แวร์แอสเทอริสก์ จะทำตามคำสั่งควบคุมที่กำหนดทันที โดยชุดคำสั่งถูกแบ่งออกเป็น 2 กลุ่ม (แสดงในรูปที่ 1.12) ต่อไปนี้

คำสั่งควบคุมการโทรออก

- `Channel` กำหนดช่องทางการสื่อสารที่ใช้ในการเชื่อมต่อ เช่น `SIP` สำหรับเชื่อมต่อไปยังระบบโทรศัพท์ SIP และ `ZAP` สำหรับเชื่อมต่อไปยังระบบโทรศัพท์พื้นฐาน

- `WaitTime` กำหนดค่าเวลาสูงสุดในการรอระหว่างเรียกสาย
- `RetryTime` และ `Maxretries` กำหนดค่าเวลาที่รอเพื่อเรียกสายซ้ำ และจำนวนครั้งสูงสุดที่จะพยายามเรียกสายใหม่

คำสั่งควบคุมหลังจากมีผู้ใช้รับสาย

- `Context` กำหนดชื่อหมวดหมู่ในไดออลแพลน ซึ่งใช้จัดกลุ่มเลขหมายปลายทาง
- `Extension` กำหนดค่าเลขหมายปลายทางที่จะติดต่อ
- `Priority` กำหนดค่าระดับความสำคัญของคำสั่ง โดยจะใช้ในการตัดสินใจลำดับก่อนหลังในการทำงาน

```
01. import org.asteriskjava.fastagi.AgiChannel;
02. import org.asteriskjava.fastagi.AgiException;
03. import org.asteriskjava.fastagi.AgiRequest;
04. import org.asteriskjava.fastagi.BaseAgiScript;
05. public class HelloAgiScript extends BaseAgiScript {
06.     public void service(AgiRequest request, AgiChannel channel) throws AgiException {
07.         //Answer the call
08.         answer();
09.         //Play the audio file named welcome.gsm
10.         streamFile("welcome");
11.         //finish the call
12.         hangup();
13.     }
14. }
```

รูปที่ 1.11 ตัวอย่างซอร์สโค้ดของคลาส `HelloAgiScript`

```
# How to initial a call
Channel: SIP/jakky
WaitTime: 30
RetryTime: 60
MaxRetries: 1
# What to do when call answered
Context: outgoing
Extension: 1300
Priority: 1
```

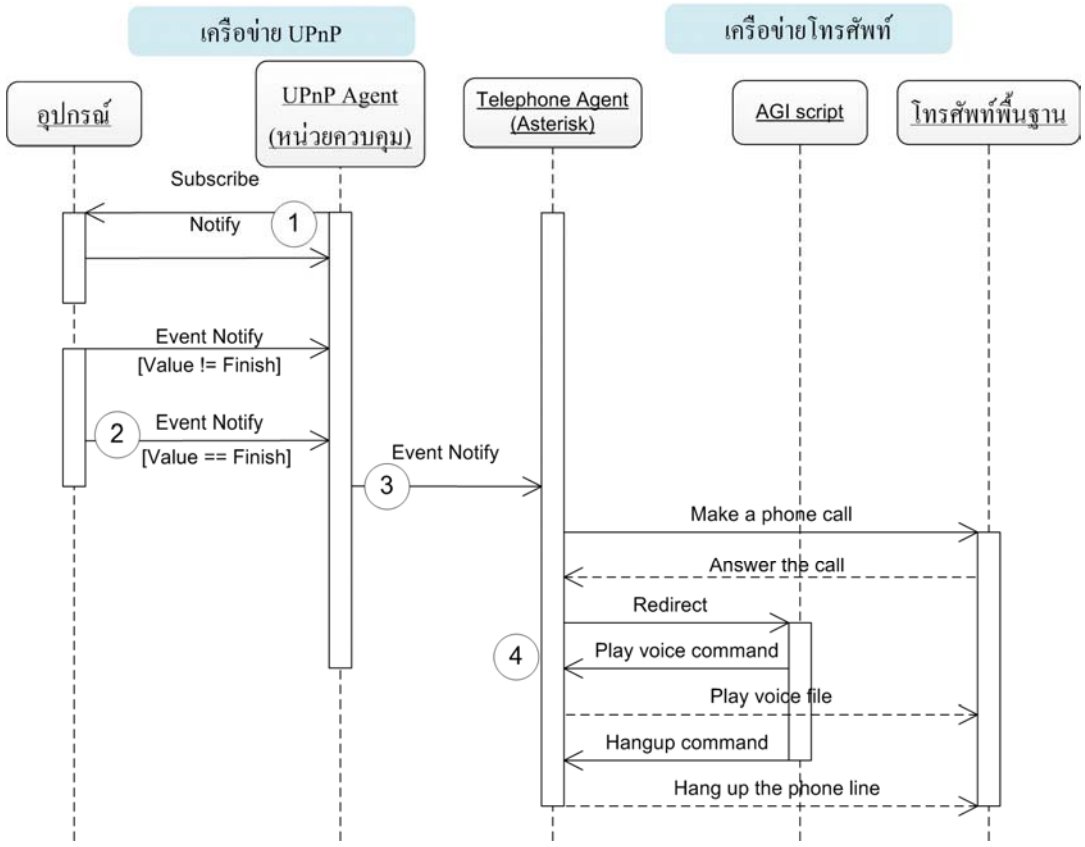
รูปที่ 1.12 ตัวอย่างข้อความในคอลไฟล์

```
[outgoing]
exten => 1300,1,Agi(agi://172.30.132.195/hello.agi)
```

รูปที่ 1.13 ตัวอย่างการกำหนดค่าไดออลแพลน

ตัวอย่างจากรูปที่ 1.13 เมื่อผู้ใช้รับสาย ซอฟต์แวร์แอสเทอริสก์ จะโอนสายไปยังหมายเลขสคริปต์เอจีไอ ที่กำหนดค่าเอาไว้ในไดออลแพลน ซึ่งมีรายละเอียดดังนี้

- `172.30.132.195` คือหมายเลขไอพี (IP Address) ของเครื่องแม่ข่ายที่ทำงานของสคริปต์เอจีไอ ในที่นี้เป็นเครื่องเดียวกับแม่ข่ายแอสเทอริสก์ได้
- `hello.agi` คือชื่อของสคริปต์เอจีไอที่อ้างถึง



รูปที่ 1.14 ลำดับการทำงานของกลไกแจ้งเตือนเหตุการณ์

1.2.2.4 ลำดับการทำงานของกลไกแจ้งเตือนเหตุการณ์

จากรูปที่ 1.14 ลำดับการทำงานโดยสรุปการประสานงานร่วมกันระหว่างเอเจนท์ของเครือข่ายยูพีแอนพีและเอเจนท์ของเครือข่ายโทรศัพท์มีดังนี้

1) เอเจนท์ของเครือข่ายยูพีแอนพี สมัครรับการแจ้งเตือนเหตุการณ์ (Subscribe) กับอุปกรณ์ที่ต้องการ ซึ่งกำหนดไว้ล่วงหน้าโดยผู้ใช้ ในครั้งแรกอุปกรณ์จะตอบข้อความ `Notify` ที่แจ้งสถานะของอุปกรณ์ก่อน
2) อุปกรณ์จะแจ้งเตือนไปยังเอเจนท์ของเครือข่ายยูพีแอนพี เมื่อมีการเปลี่ยนสถานะด้วยข้อความ `Event Notify`
3) เอเจนท์ของเครือข่ายยูพีแอนพี ตรวจสอบเงื่อนไขของสถานะที่ต้องแจ้งเตือนไปยังเครือข่ายโทรศัพท์ เช่น `Value` เท่ากับ `Finish` แล้วแจ้งเตือนไปยังเอเจนท์ของเครือข่ายโทรศัพท์
4) เอเจนท์ของเครือข่ายโทรศัพท์เรียกสคริปต์เอจีไอ ที่กำหนดให้แจ้งเตือนเหตุการณ์ด้วยเสียงพูดไปยังผู้ใช้ผ่านอุปกรณ์โทรศัพท์พื้นฐานและวางสาย จึงสามารถแจ้งเตือนเหตุการณ์ได้ตามต้องการ

บทที่ 4

ผลการวิจัย

ในบทนี้ จะเป็นการอธิบายผลการทดสอบแนวคิดซึ่งได้อธิบายในบทที่ผ่านมา โดยเริ่มจากผลการศึกษาเปรียบเทียบด้านระยะเวลาของเทคนิควิธีที่เหมาะสม ในการนำมาใช้เพื่อการยืนยันตัวตนอุปกรณ์ ผลการทดสอบประสิทธิภาพด้านเวลาของการเข้าร่วม/ออกจากกลุ่มสื่อสารที่อยู่ภายในเครือข่ายเดียวกัน ตามด้วยผลการทดสอบกลไกที่นำเสนอ เพื่อทดสอบการใช้งานบนเครือข่ายชนิดเดียวกัน (ระหว่างเครือข่ายยูพีแอนพี) และต่างชนิดกัน (เครือข่ายยูพีแอนพีกับเครือข่ายโทรศัพท์) สุดท้ายจะนำเสนอแนวทางการประยุกต์ใช้กลไกทำงานที่ได้ดำเนินการทั้งหมดบนระบบประยุกต์ทางการแพทย์ เพื่อดูแลผู้สูงอายุจากระยะไกล

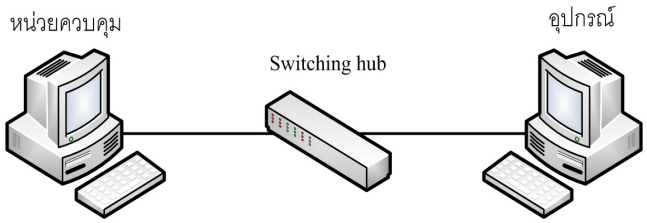
4.1 ผลการศึกษาเปรียบเทียบเทคนิควิธียืนยันตัวตนอุปกรณ์

การศึกษาในส่วนนี้นำเสนอผลการทดสอบเปรียบเทียบระยะเวลาในการประมวลผล (Execution Time) เพื่อการยืนยันตัวตนอุปกรณ์ด้วยเทคนิคการเข้ารหัสแบบพีเคไอและเคพีดี โดยมีรายละเอียดการทดสอบ ดังต่อไปนี้

4.1.1 สภาพแวดล้อมการทดสอบและวัดผล

จากรูปที่ 4.1 แสดงให้เห็นถึงระบบเครือข่ายแบบพื้นฐานที่นำมาใช้ในการทดสอบ โดยมีข้อกำหนดของคอมพิวเตอร์ที่นำมาใช้งานร่วมกัน ดังต่อไปนี้

- หน่วยควบคุมและอุปกรณ์ทำงานอยู่บนเครื่องที่มีหน่วยประมวลผลกลาง Intel Core i3 2.93 GHz หน่วยความจำ 2 GB และ ระบบปฏิบัติการ Windows 7
- อุปกรณ์เชื่อมต่อเครือข่ายท้องถิ่นแบบ Switching Hub 5 port 10/100 Mbps
- โปรแกรมทดสอบสำหรับส่วนหน่วยควบคุมและอุปกรณ์ พัฒนาขึ้นโดยใช้โปรแกรมไลบรารี CyberLink for Java เพื่อตรวจสอบระยะเวลาการทำงานของเทคนิควิธีต่างๆ



รูปที่ 4.1 ระบบทดสอบการยืนยันตัวตนอุปกรณ์

รายละเอียดของอัลกอริทึมการเข้ารหัสข้อมูล มีดังต่อไปนี้

- การเข้ารหัสของเทคนิควิธีเคพีดี ใช้อัลกอริทึมการเข้ารหัสแบบคีย์สมมาตรที่เลือกนำมาทดสอบคือ Advanced Encryption Standard (AES) เนื่องจากใช้ทรัพยากรน้อยแต่ยังคงมีความเข้มแข็งในการป้องกันการเจาะรหัสมากกว่าอัลกอริทึมแบบอื่น [20]
- การเข้ารหัสของเทคนิควิธีพีเคไอ ใช้อัลกอริทึมการเข้ารหัสแบบคีย์อสมมาตร Rivest, Shamir and Adleman (RSA) ซึ่งเป็นมาตรฐานของเทคนิควิธีพีเคไอ
- ความยาวของคีย์ที่ใช้ในการทดสอบเป็นค่าสูงสุด/ต่ำสุดของคีย์เข้ารหัสข้อมูล ที่ถูกจำกัดโดยค่าปริยายของไลบรารีที่ช่วยจัดการด้านการรักษาความปลอดภัยข้อมูลของภาษาจาวา (Java Cryptography Architecture: JCA) [21] โดยกำหนดค่าความยาวคีย์ของ AES สูงสุด 256 บิต และ RSA ต่ำสุด 1024 บิต เพื่อให้มีระดับความเข้มแข็งในการป้องกันการเจาะรหัสข้อมูลใกล้เคียงกันมากที่สุด

การวัดเวลาที่ใช้ในการประมวลผลวัดที่อุปกรณ์และหน่วยควบคุม ใช้วิธีบันทึกเวลา ณ จุดเริ่มต้น (t_{start}) และจุดสิ้นสุด (t_{finish}) ของกระบวนการเข้ารหัส จากนั้นเวลาที่ใช้ (t_{esp}) จะสามารถคำนวณได้จากสมการที่ (4.1)

$$t_{esp} = t_{finish} - t_{start} \tag{4.1}$$

ผลการทดสอบเพื่อวัดเวลาในกระบวนการย่อยของการยืนยันตัวตนอุปกรณ์ โดยอุปกรณ์และหน่วยควบคุม มีหน้าที่เป็นแม่ข่าย และลูกข่าย ในกระบวนการนี้ ซึ่งผลทดสอบได้สรุปไว้ในตารางที่ 4.1

ตารางที่ 4.1 ผลทดสอบระยะเวลาประมวลผลที่ใช้ในกระบวนการยืนยันตัวตนอุปกรณ์

กระบวนการ	อุปกรณ์ (แม่ข่าย) (ms)		หน่วยควบคุม (ลูกข่าย) (ms)	
	พีเคไอ	เคพีดี	พีเคไอ	เคพีดี
การตรวจสอบความเป็นสมาชิก	2.59	0.20	2.65	0.20
การกระจายคีย์กลุ่มให้สมาชิก	10.08	0.11	12.34	0.11
ระยะเวลารวม	12.67	0.31	14.99	0.31
ร้อยละส่วนต่างของระยะเวลารวม	97.55		97.93	

4.1.2 การวิเคราะห์ผล

ผลการทดสอบจากตารางที่ 4.1 พบว่าการใช้เทคนิคการเข้ารหัสแบบเคพีดี จะใช้ระยะเวลาในการประมวลผลน้อยกว่าเทคนิควิธีการเข้ารหัสแบบพีเคไอ ซึ่งระยะเวลารวมที่ลดลง คิดเป็นร้อยละ 97.55 และ 97.93 เมื่อทำการทดสอบที่เครื่องแม่ข่ายและเครื่องลูกข่ายตามลำดับ โดยผลการทดสอบในกระบวนการย่อยมีรายละเอียดดังนี้

- การตรวจสอบความเป็นสมาชิก ระยะเวลาประมวลที่เครื่องแม่ข่ายและลูกข่าย ของเทคนิควิธีเคพีดีเป็น 0.20 มิลลิวินาทีเท่ากัน แต่เทคนิควิธีพีเคไอเป็น 2.59 และ 2.65 มิลลิวินาที ซึ่งเป็นผลจากความแตกต่างระหว่างการคำนวณคีย์คู่ของเทคนิควิธีเคพีดี และการตรวจสอบใบรับรองอิเล็กทรอนิกส์ของเทคนิควิธีพีเคไอ
- การกระจายคีย์กลุ่มให้สมาชิก ระยะเวลาประมวลที่เครื่องแม่ข่ายและลูกข่าย ของเทคนิควิธีเคพีดี เป็น 0.11 มิลลิวินาทีเท่ากัน แต่เทคนิควิธีพีเคไอเป็น 10.08 และ 12.34 มิลลิวินาที ซึ่งเป็นผลมาจากอัลกอริทึมการเข้ารหัสเพื่อป้องกันข้อมูลคีย์กลุ่มที่จะรับ/

ส่งผ่านเครือข่าย โดยใช้อัลกอริทึม AES และ RSA ตามลำดับ ส่งผลให้เทคนิควิธีเคพีดีใช้ระยะเวลาประมวลผลเร็วกว่าเทคนิควิธีพีเคไอ ดังข้อมูลข้างต้น

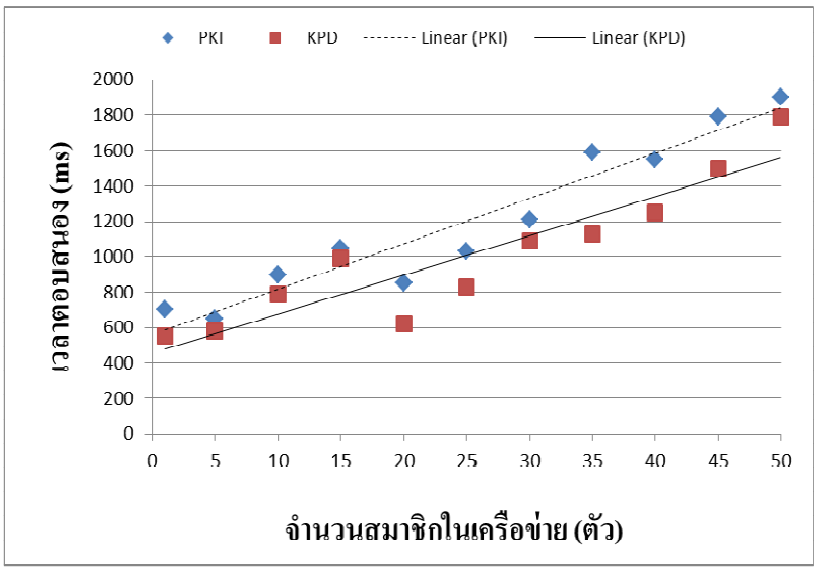
ดังนั้น การนำเทคนิควิธีเคพีดี เข้ามาใช้แทนเทคนิควิธีพีเคไอ จะช่วยลดการใช้ทรัพยากรด้านการประมวลผลในกระบวนการยืนยันตัวตนอุปกรณ์ลงได้มาก โดยที่แนวโน้มของเวลาที่ใช้ดังกล่าวจะมีความแตกต่างกันมากยิ่งขึ้นในสภาพแวดล้อมที่มีทรัพยากรจำกัด เช่น ระบบอุปกรณ์แบบฝังตัวในเครือข่ายยูพีแอนพี

4.2 ผลการทดสอบกลไกบริการกลุ่มสื่อสารปลอดภัยที่พัฒนาขึ้น

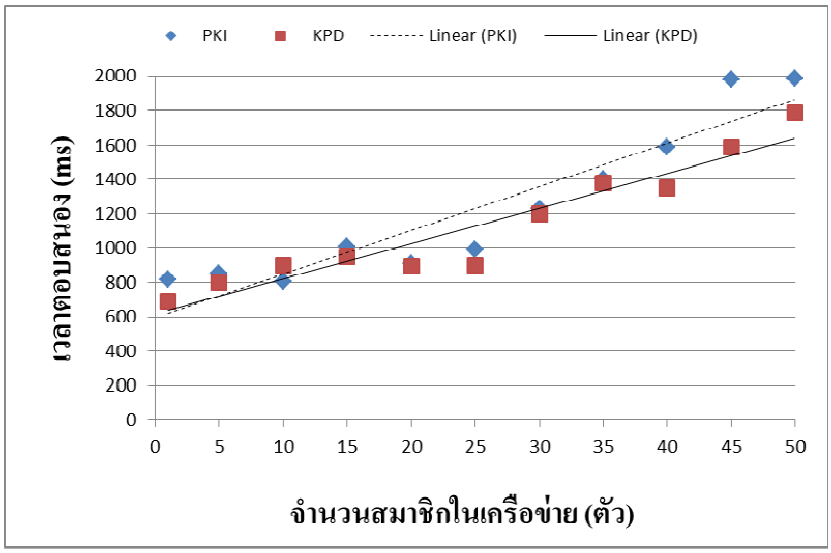
4.2.1 การศึกษาด้านระยะการหน่วงเวลาของการเข้าร่วม/ออกกลุ่มสื่อสาร

การศึกษาในส่วนนี้ใช้การจำลองหน่วยควบคุมด้วยงานย่อย (Thread) บนเครื่องคอมพิวเตอร์ของหน่วยควบคุมในระบบทดสอบดังรูปที่ 4.1 ที่ใช้ในการศึกษาหัวข้อที่ผ่านมา เพื่อศึกษาระยะเวลาของการหน่วงเวลา (Delay Time) ในกรณีที่มีการเปลี่ยนแปลงจำนวนสมาชิกเข้า/ออกจากกลุ่ม โดยการทดสอบใช้การเพิ่มของจำนวนสมาชิกได้กำหนดให้เพิ่มเป็นชุดๆ ละ 5 ตัว โดยกำหนดค่าสุ่มเวลาในช่วง 0 - 30 วินาที (ซึ่งค่าระยะเวลานี้เป็นค่าโดยปริยายของโพรโทคอล SSDP ที่ใช้ในการตอบกลับในกระบวนการค้นหาบริการ) การเพิ่มนี้จะทำไปเรื่อยๆ จนครบ 50 ตัว โดยการบันทึกเวลา จะใช้การบันทึก ที่หน่วยควบคุมตัวสุดท้าย (ของแต่ละชุด) ณ ขณะเวลาเมื่อเข้าร่วมหรือออกจากกลุ่มสื่อสาร

จากรูปที่ 4.2 และรูปที่ 4.3 เป็นผลที่ได้รับจากการทดสอบข้างต้น ในกรณีเมื่อสมาชิกเข้าร่วม และออกจากกลุ่มสื่อสาร ตามลำดับ ซึ่งหากพิจารณาทั้งสองกรณีแล้ว จะเห็นถึงแนวโน้มของระยะเวลาของการหน่วงเวลาหน่วงเพิ่มขึ้นตามจำนวนหน่วยควบคุมในลักษณะเชิงเส้น สอดคล้องกับกระบวนการกระจายคีย์กลุ่มให้กับสมาชิกภายในกลุ่มทีละตัวที่นำมาใช้ ไม่ว่าจะใช้เทคนิควิธีเคพีดี หรือพีเคไอ ก็ตามแต่เทคนิควิธีเคพีดี จะมีเวลาตอบสนองที่เร็วขึ้นเล็กน้อย



รูปที่ 4.2 ผลการเปรียบเทียบระยะเวลาการเข้าร่วมกลุ่มสื่อสาร

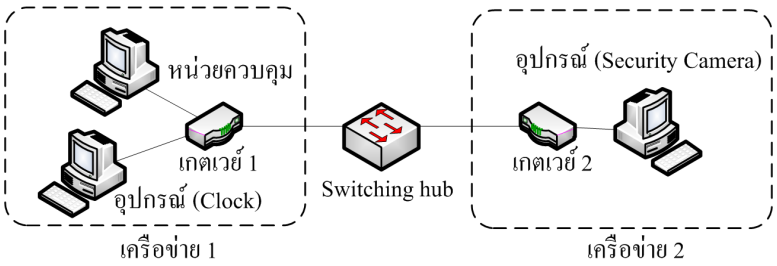


รูปที่ 4.3 ผลการเปรียบเทียบระยะเวลาการออกจากกลุ่มสื่อสาร

4.2.2 การศึกษาด้านการสนับสนุนงานกลุ่มสื่อสารข้ามเครือข่าย

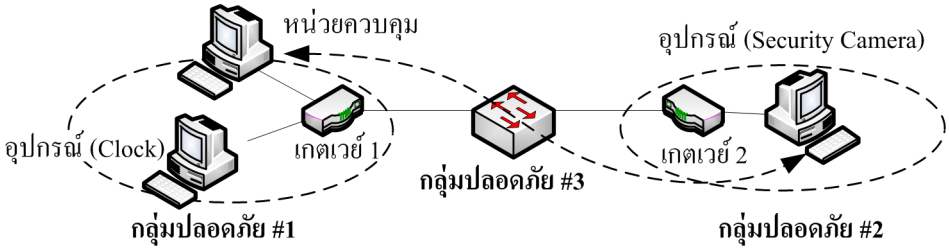
ระบบกลไกกลุ่มสื่อสารปลอดภัยที่นำเสนอในงานวิจัยนี้สามารถนำไปใช้งานระหว่างเครือข่ายที่อยู่ห่างไกลออกไปได้ (ตัวอย่างเครือข่ายจากรูปที่ 4.4) โดยเครือข่ายทั้งสองนั้นต้องสามารถเชื่อมต่อกันเป็นเครือข่ายได้ก่อนแล้ว (เช่น ผ่านกลไกทำงานในระดับการเชื่อมโยง Secure

Socket Layer (SSL) หรือในระดับเครือข่าย เช่น Vitual Private Network (VPN) เป็นต้น) และต้องกำหนดให้มีหัวหน้ากลุ่มสื่อสารปลอดภัยทำงานอยู่ที่อุปกรณ์เกตเวย์ของเครือข่ายด้วย



รูปที่ 4.4 ระบบทดสอบกลไกทำงานกลุ่มสื่อสารปลอดภัยข้ามเครือข่าย

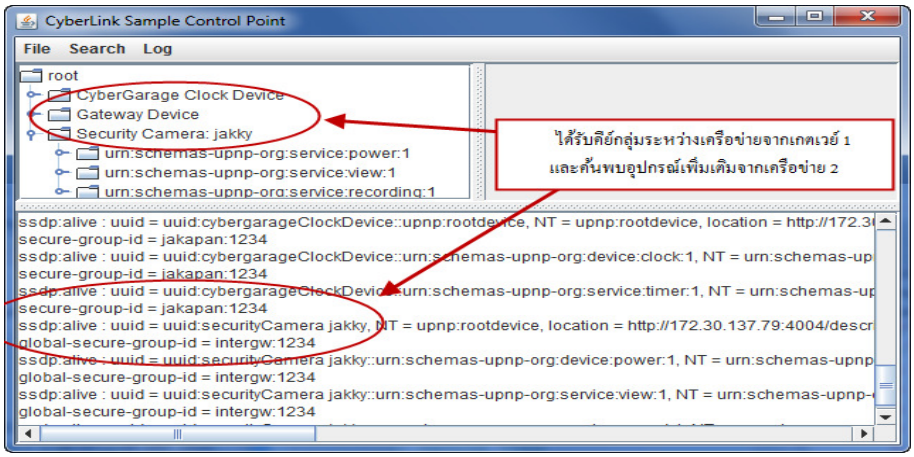
ในการทดสอบระบบต้นแบบ (หน่วยควบคุมและอุปกรณ์) ที่พัฒนาขึ้นด้วยภาษาจาวา และไลบรารี CyberLink for Java เพื่อให้ทำงานร่วมกับโพรโทคอลของเครือข่ายยูพีแอนพี ที่เสนอแนะการเพิ่มขยายให้รองรับกลุ่มสื่อสารปลอดภัย พบว่าหากได้มีการกำหนดกลุ่มสื่อสารที่ประกอบขึ้นด้วยสมาชิกที่อยู่ต่างเครือข่ายกันแล้ว (เช่น กลุ่มปลอดภัยหมายเลข 3 จากรูปที่ 4.5) การเข้าถึงบริการของอุปกรณ์จากข้ามเครือข่ายก็จะสามารถทำงานได้อย่างตามต้องการ



รูปที่ 4.5 ตัวอย่างกลุ่มสื่อสารแบบปลอดภัยของระบบทดสอบ

จากรูปที่ 4.6 แสดงให้เห็นตัวอย่างหน้าต่างแสดงสถานะระบบ เมื่อสังเกต ณ หน่วยควบคุมที่อยู่ภายในเครือข่าย 1 โดยจะสามารถค้นพบอุปกรณ์ Security Camera ของเครือข่าย 2 ได้

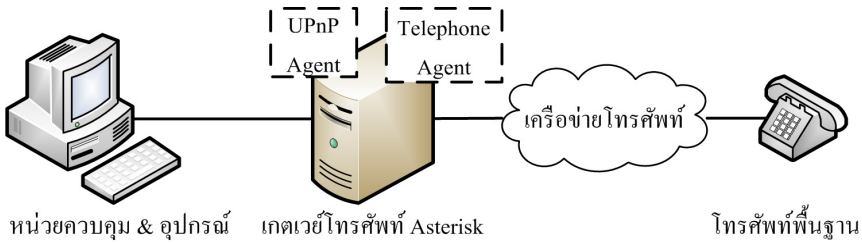
(นอกเหนือจากอุปกรณ์นาฬิกา (Clock) ที่อยู่ภายในเครือข่าย 1) ทั้งนี้เนื่องจากเป็นอุปกรณ์ที่อยู่ภายในกลุ่มสื่อสารแบบปลอดภัยเดียวกัน แม้ว่าจะอยู่ต่างเครือข่ายกันก็ตาม



รูปที่ 4.6 หน้าต่างแสดงสถานะอุปกรณ์ต่างๆ ภายในกลุ่มสื่อสารปลอดภัยเดียวกัน

4.3 ผลการศึกษากลไกประสานงานระหว่างเครือข่ายโทรศัพท์และยูพีแอนพีที่พัฒนาขึ้น

การศึกษาในส่วนนี้ เป็นการทดสอบกลไกการประสานงานระหว่างหน่วยทำงานเอเจนท์ของเครือข่ายยูพีแอนพีและเครือข่ายโทรศัพท์พื้นฐาน ที่ได้นำเสนอขึ้นใหม่ โดยใช้ระบบต้นแบบที่พัฒนาขึ้นด้วยซอฟต์แวร์แอสเทอริสก์ เพื่อทำหน้าที่เป็นอุปกรณ์เกตเวย์ไปยังเครือข่ายโทรศัพท์ โดยมีสภาพแวดล้อมของการทดสอบ ดังแสดงในรูปที่ 4.7



รูปที่ 4.7 สภาพแวดล้อมการทดสอบระบบแจ้งเตือนเหตุการณ์ผ่านเครือข่ายโทรศัพท์

4.3.1 สภาพแวดล้อมการทดสอบ

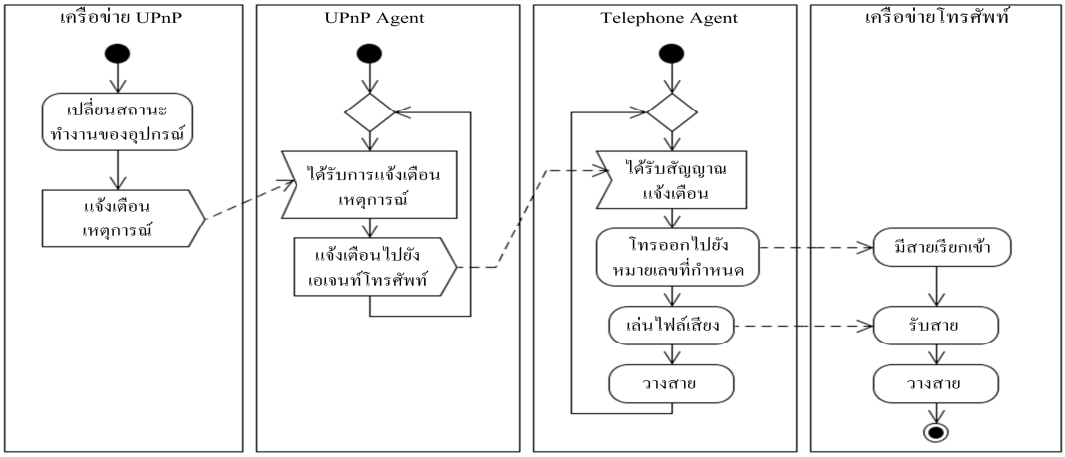
- เกตเวย์โทรศัพท์แอสเทอริสก์ เวอร์ชัน 1.4 เป็นคอมพิวเตอร์ระบบปฏิบัติการ Linux Ubuntu 8.04 ที่เชื่อมต่อได้ทั้งเครือข่ายอินเทอร์เน็ตและเครือข่ายโทรศัพท์ (ผ่านทาง

แผงวงจรโทรศัพท์ OpenVox A400P) และทำงานบน โดยมีการเชื่อมต่อกับทั้งเครือข่ายยูพีแอนพีและเครือข่ายโทรศัพท์

- โปรแกรมเอเจนท์ของเครือข่ายโทรศัพท์ พัฒนาบนไลบรารี Asterisk-Java และติดตั้งบนเกตเวย์โทรศัพท์แอสเทอริสก์ เช่นเดียวกันกับเอเจนท์ของเครือข่ายยูพีแอนพี (โดยได้อธิบายความละเอียดไว้แล้วในหัวข้อที่ **ผิดพลาด! ไม่พบแหล่งการอ้างอิง** ของบทที่ 3)
- หน่วยควบคุมและอุปกรณ์ทำงานอยู่บนคอมพิวเตอร์ระบบปฏิบัติการ Windows XP และเชื่อมต่อกับเกตเวย์โทรศัพท์แอสเทอริสก์
- เครื่องโทรศัพท์พื้นฐาน
- คู่สายโทรศัพท์ 2 เลขหมาย สำหรับเกตเวย์โทรศัพท์แอสเทอริสก์ และเครื่องโทรศัพท์พื้นฐาน เพื่อใช้ในการรับสายและโทรออกในการแจ้งเตือนเหตุการณ์

4.3.2 ผลการทดสอบ

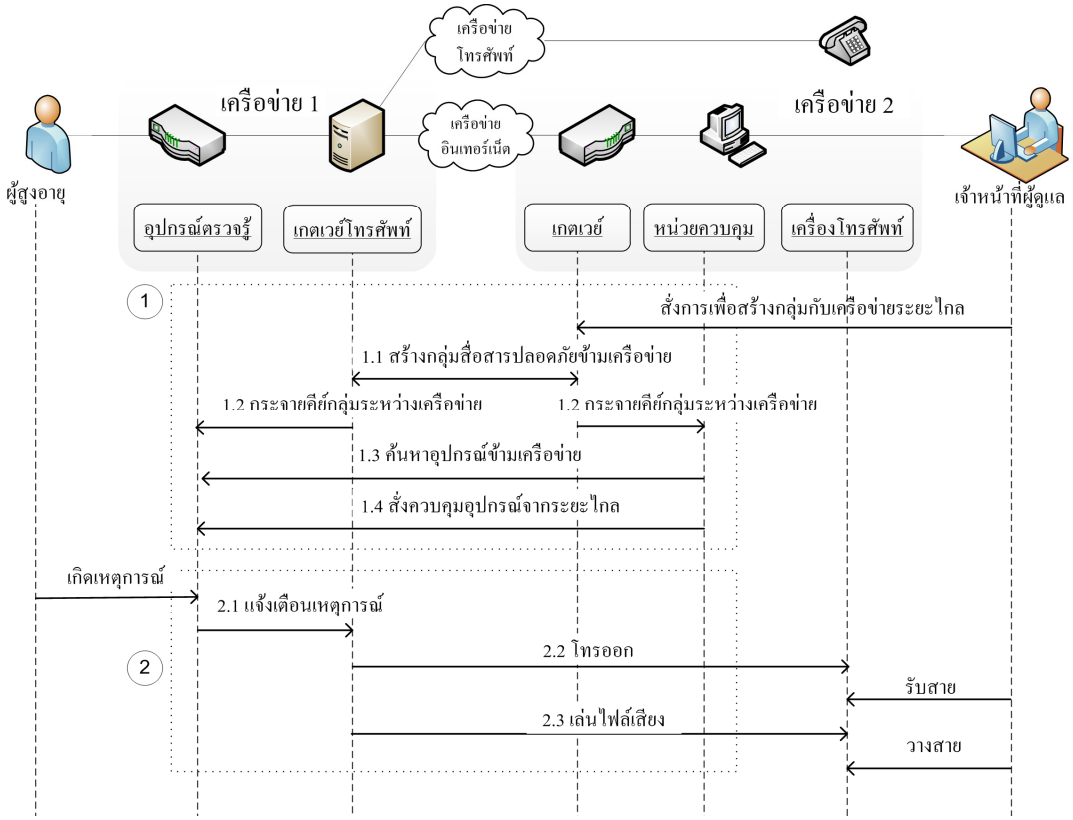
การทดสอบได้จำลองสถานการณ์เพื่อให้อุปกรณ์ในเครือข่ายยูพีแอนพี ส่งการแจ้งเตือนเหตุการณ์ผ่านทางหน่วยทำงานเอเจนท์ที่ประสานงานร่วมกันของทั้งสองเครือข่ายเป็นเสียงพูด (ซึ่งได้บันทึกเป็นไฟล์เสียงไว้ล่วงหน้าแล้ว) ไปยังหมายเลขเครื่องโทรศัพท์ที่ต้องการ โดยได้รับผลจากการทดสอบเป็นไปตามที่คาดหมายไว้ทุกประการ กล่าวคือหน่วยทำงานเอเจนท์สามารถรับรู้การแจ้งเตือนเหตุการณ์จากอุปกรณ์ในเครือข่ายยูพีแอนพี เมื่อสั่งควบคุมให้อุปกรณ์เปลี่ยนสถานะทำงาน จากนั้นมีสายเรียกเข้าที่เครื่องโทรศัพท์เลขหมายซึ่งตั้งค่าไว้ และเมื่อรับสายจะได้ยินเสียงพูดที่บันทึกไว้ถูกต้องทุกครั้ง (ดูรูปที่ 4.8 ประกอบ)



รูปที่ 4.8 แผนภาพแสดงกิจกรรมของการแจ้งเตือนเหตุการณ์ผ่านเครือข่ายโทรศัพท์

4.4 กรณีศึกษา: การประยุกต์ทางการแพทย์เพื่อดูแลผู้สูงอายุระยะไกล

การศึกษาในส่วนนี้เป็นการนำเสนอแนวทางการบูรณาการกลไกทำงานที่ได้ศึกษาและนำเสนอทั้งหมดในวิทยานิพนธ์นี้ เพื่อจุดประสงค์ในการประยุกต์ใช้งานในสิ่งแวดล้อมที่เป็นจริง



รูปที่ 4.9 ลำดับการทดสอบระบบดูแลผู้สูงอายุระยะไกล

กรณีศึกษาระบบดูแลผู้สูงอายุจากระยะไกล เป็นสถานการณ์ตัวอย่าง เพื่อสาธิตให้เห็นการนำกลไกที่นำเสนอในวิทยานิพนธ์นี้ไปประยุกต์ใช้งาน ซึ่งจะได้นำกลไกบริการกลุ่มสื่อสารปลอดภัย และกลไกเชื่อมต่อระหว่างเครือข่ายยูพีแอนพีกับเครือข่ายโทรศัพท์มาประยุกต์ใช้งานร่วมกัน โดยแผนภาพลำดับการทำงานโดยรวมแสดงไว้ในรูปที่ 4.9 ซึ่งสามารถแบ่งได้เป็น 2 ช่วง โดยขั้นตอนในช่วงเริ่มต้น (ล้อมกรอบวงกลมหมายเลข 1) เป็นการเตรียมระบบเพื่อสร้างกลุ่มสื่อสารปลอดภัยกับเครือข่ายระยะไกล เริ่มจากเจ้าหน้าที่ผู้ดูแลเป็นคนสั่งการ ส่งผลให้เกิดการสื่อสารระหว่างเกตเวย์ทั้งสองเครือข่าย โดยใช้กลไกของการสร้างกลุ่มสื่อสารปลอดภัยที่ได้นำเสนอในวิทยานิพนธ์นี้ เมื่อเสร็จสิ้นขั้นตอนนี้ เจ้าหน้าที่ก็สามารถพบเห็นอุปกรณ์ตรวจรู้ และเฝ้าตรวจสถานะต่อไปได้ ในส่วนของขั้นตอนในช่วงหลังจากนั้น (ล้อมกรอบวงกลมหมายเลข 2) เป็นการสมมติให้เกิดสถานการณ์ที่อุปกรณ์ตรวจรู้จะต้องส่งการแจ้งเตือนไปยังเกตเวย์โทรศัพท์ เช่น การหกล้มของผู้สูงอายุ เป็นต้น ซึ่งในการแจ้งเตือนเหตุการณ์กลไกประสานงานระหว่างเอเจนท์ทั้งสองเครือข่ายที่ได้นำเสนอในวิทยานิพนธ์นี้เช่นกัน ก็จะส่งผ่านการควบคุมเพื่อให้เกิดการโทรศัพท์ออกไปยังหมายเลขที่ต้องการ พร้อมกับเล่นไฟล์เสียงเมื่อมีการยกหูตอบรับจากเจ้าหน้าที่ผู้ดูแลระบบ

บทที่ 5

บทสรุปและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

วิทยานิพนธ์นี้ได้นำเสนอแนวทางการแก้ปัญหาข้อด้อยเชิงสถาปัตยกรรมของเครือข่ายยูพีแอนพี ซึ่งไม่รองรับการสื่อสารแบบกลุ่มปลอดภัย ของอุปกรณ์ภายในระบบ และไม่สามารถสื่อสารระหว่างอุปกรณ์ที่อยู่ต่างเครือข่ายกันได้ ส่งผลให้เกิดข้อจำกัดในงานประยุกต์ที่คำนึงถึงเรื่องความปลอดภัยเป็นสำคัญ เช่น ระบบให้ความช่วยเหลือทางการแพทย์จากระยะไกล ในที่นี้ได้เสนอแนวทางการแก้ปัญหาข้างต้น ดังต่อไปนี้

1) เสนอแนะให้มีการนำกลไกการเข้ารหัสแบบเคพีดี เข้ามาใช้ในการทำงานแบบกลุ่มสื่อสารปลอดภัย ซึ่งนิยมใช้ในอุปกรณ์ที่มีข้อจำกัดด้านทรัพยากร โดยผลจากการเปรียบเทียบประสิทธิภาพด้านการยืนยันตัวตนอุปกรณ์ดีกว่า การใช้กลไกการเข้ารหัสแบบพีเคไอ ที่ใช้ในมาตรฐานรักษาความปลอดภัยเดิม นอกจากนี้ ยังได้เสนอแนวทางการปรับเปลี่ยนโพรโทคอล เพื่อให้สนับสนุนกลไกทำงานข้างต้นดังนี้
   - เพิ่มเติมหมายเลขระบุตัวตนของกลุ่มสื่อสารปลอดภัย ที่โพรโทคอลค้นหาบริการ (SSDP) เพื่อสนับสนุนกระบวนการเลือกหัวหน้ากลุ่มสื่อสาร ให้สามารถทำได้พร้อมกันกับกระบวนการค้นหาบริการในช่วงเริ่มการทำงานของเครือข่ายยูพีแอนพี
   - เพิ่มกลไกการยืนยันตัวตนอุปกรณ์ และกลไกการแลกเปลี่ยนคีย์กลุ่ม โดยอาศัยโพรโทคอล SOAP ซึ่งเป็นมาตรฐานของเครือข่ายยูพีแอนพีเดิม โดยไม่ต้องเพิ่มเติมโพรโทคอลเฉพาะ ทำให้กลไกที่นำเสนอดังกล่าว ง่ายต่อการเรียนรู้และพัฒนา เพื่อสามารถใช้งานได้จริง
2) แสดงให้เห็นประสิทธิภาพของกลไกทำงาน เพื่อสนับสนุนบริการกลุ่มสื่อสารปลอดภัยข้างต้น ทั้งในสภาพแวดล้อมของเครือข่ายเดียวกัน หรือต่างเครือข่ายกันก็ตาม โดยในกรณีหลัง จะเกิดขึ้นได้ภายหลังจากที่ได้เชื่อมต่อเครือข่ายก่อนไว้ล่วงหน้าแล้ว

เช่น ด้วยกลไกทำงาน VPN หรือ SSL เป็นต้น

3) นำเสนอกลไกการประสานการทำงานร่วมกันระหว่างหน่วยทำงานเอเจนท์ ซึ่งติดตั้งอยู่ที่บริเวณอุปกรณ์เกตเวย์ของเครือข่ายยูพีแอนพีและเครือข่ายโทรศัพท์ เพื่อส่งต่อข้อมูลการแจ้งเตือนเหตุการณ์ข้ามเครือข่ายกันได้ โดยใช้กรณีศึกษาของการสั่งงานผ่านทางเกตเวย์โทรศัพท์ที่พัฒนาขึ้นด้วยซอฟต์แวร์โอเพนซอร์สแอสเทอริสก์ เพื่อให้สถานะจากอุปกรณ์ภายในเครือข่ายยูพีแอนพีที่เฝ้าระวัง สามารถส่งผ่านไปยังเครือข่ายโทรศัพท์ได้ โดยการแจ้งเตือนด้วยข้อความเสียงไปยังเครื่องโทรศัพท์หมายเลขที่ต้องการ

5.2 ข้อเสนอแนะ

1) ควรเพิ่มเติมกลไกการขับไล่สมาชิกออกจากกลุ่มสื่อสารปลอดภัย เพื่อป้องกันการเข้าถึงข้อมูลสื่อสารภายในกลุ่มจากอุปกรณ์ที่อาจถูกโจรกรรมไป เนื่องจากเทคนิควิธีเคพีดีจะเกี่ยวข้องกับกระบวนการยืนยันตัวอุปกรณ์ในการเข้าร่วมกลุ่มสื่อสารปลอดภัยเท่านั้น

2) ควรนำเทคนิคการกระจายคีย์กลุ่มแบบ Logical Key Hierarchy tree [22] เข้ามาใช้ร่วมด้วย เพื่อลดระยะเวลาในการกระจายคีย์ ในกรณีที่ต้องการเพิ่มการรองรับจำนวนสมาชิกที่เพิ่มมากขึ้นภายในกลุ่มสื่อสารปลอดภัย เช่น กรณีที่มีการเชื่อมต่อระหว่างเครือข่ายยูพีแอนพี

3) ควรเพิ่มเติมคำสั่งสคริปต์เอจีไอ ของซอฟต์แวร์แอสเทอริสก์ เพื่อเพิ่มคุณลักษณะในการโต้ตอบแบบสองทิศทางระหว่างผู้ใช้ของเครือข่ายโทรศัพท์ (ผ่านการกดคีย์ตัวเลขบนเครื่องโทรศัพท์) กับอุปกรณ์ภายในเครือข่ายยูพีแอนพี ให้รับการควบคุมจากระยะไกลได้

เอกสารอ้างอิง

[1] UPnP Contribute member, “UPnP Specifications,” *UPnP Forum*, Jun-2005. [Online]. Available: http://upnp.org/resources/upnpresources.zip. [Accessed: 09-Jul-2010].

[2] C. Ellison, “UPnP Security Ceremonies,” *Design Document for UPnP device architecture 1.0*, 03-Oct-2003. [Online]. Available: http://www.upnp.org/download/standardizeddcps/UPnPSecurityCeremonies_1_0secure.pdf. [Accessed: 15-Feb-2010].

[3] J. Lee, C. Huang, L. Lee, and C. Lei, “Design and Implementation of Secure Communication Channels over UPnP Networks,” presented at the Multimedia and Ubiquitous Engineering, 2007. MUE '07. International Conference on, pp. 307-312, 2007.

[4] K. Chiewchan and S. Witusurapot, “Applying OSGi-based Services for Cooperation between UPnP networks with SLP Protocol,” presented at the Proceeding of Science and Technology for Community Development 2010 (STCD 2010), Prathum Thani, Thailand, 2010.

[5] J. Allard, V. Chinta, S. Gundala, and G. Richard, “Jini meets UPnP: an architecture for Jini/UPnP interoperability,” in *Applications and the Internet, 2003. Proceedings. 2003 Symposium on*, pp. 268-275, 2003.

[6] S. Rafaeli and D. Hutchison, “A survey of key management for secure group communication,” *ACM Comput. Surv.*, vol. 35, no. 3, pp. 309-329, 2003.

[7] C. Barnes et al., “Understanding Public Key Infrastructures and Wireless Networking,” in *Hack Proofing Your Wireless Network*, Massachusetts, USA: Syngress, 2002, pp. 63-67.

[8] M. Ramkumar and N. Memon, “Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC,” presented at the Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC, pp. 153-160, 2004.

[9] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, “A pairwise key pre-distribution scheme for wireless sensor networks,” Washington D.C., USA, pp. 42-51, 2003.

[10] W. Stallings, *Cryptography and network security: principles and practice*, 4th ed. Prentice Hall, 2006.

[11] B. Jackson and C. C. III., *Asterisk hacking : toolkit and liveCD*. Burlington, MA: Syngress,

2007.

[12] S. Wintermeyer, “Call files,” *Practical Asterisk 1.4*, 01-Jan-2007. [Online]. Available: http://www.the-asterisk-book.com/unstable/call-file.html. [Accessed: 01-Jun-2008].

[13] B. Oh, S. Lee, and H. Park, “A Peer Mutual Authentication Method using PKI on Super Peer based Peer-to-Peer Systems,” in *Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on*, vol. 3, pp. 2221-2225, 2008.

[14] K. Park, H. Seok, and K. Park, “pKASSO: Towards Seamless Authentication Providing Non-Repudiation on Resource-Constrained Devices,” in *Advanced Information Networking and Applications Workshops, 2007, AINAW '07. 21st International Conference on*, vol. 2, pp. 105-112, 2007.

[15] M. Ramkumar and N. Memon, “On the security of random key pre-distribution schemes,” in *Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC*, pp. 153-160, 2004.

[16] C. Lin, C. Huang, Z. Wu, P. Wang, and T. Hou, “A Collaboration Proxy for Converging UPnP and Jini Devices Based on OSGi,” in *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE*, pp. 916-919, 2007.

[17] C. Chira and D. Dumitrescu, “Multi-Agent Cooperative Design Support in Distributed Environments,” in *Distributed Computing Systems Workshops, 2007. ICDCSW '07. 27th International Conference on*, p. 76, 2007.

[18] S. Konno, “CyberLink for Java,” *CyberLink for Java*, May-2005. [Online]. Available: http://sourceforge.net/projects/cgupnpjava/. [Accessed: 01-Jun-2008].

[19] S. Reuter, “Asterisk-Java,” *Asterisk-Java*, Jun-2007. [Online]. Available: http://asterisk-java.org/. [Accessed: 01-Jan-2008].

[20] S. Goldwasser and M. Bellare, “Advanced Encryption Standard (AES),” in *Lecture Notes on Cryptography*, 2008, p. 57.

[21] Oracle Corporation, “Java Cryptography Architecture,” 25-Jul-2004. [Online]. Available: http://download.oracle.com/javase/1.5.0/docs/guide/security/CryptoSpec.html. [Accessed: 01-Jan-2010].

[22] D. Kwak, S. J. Lee, J. W. Kim, and E. Jung, “An efficient LKH tree balancing algorithm for

group key management," *Communications Letters, IEEE*, vol. 10, no. 3, pp. 222-224, 2006.

ภาคผนวก

ภาคผนวก ก. ผลงานตีพิมพ์เผยแพร่จากวิทยานิพนธ์

- J. Surbot and S. Witosurapot, “A Collaboration Agent for Exploiting Legacy Phones in Assistive UPnP-based Home Environments,” in *Proceeding of The 7th International Joint Conference on Computer Science and Software Engineering (JCSSE 2010),* Bangkok, Thailand, May. 12-14, 2010, pp. 199-203.
- J. Surbot and S. Witosurapot, “Integrating Group Key Distribution for Securing UPnP Services,” in *Proceeding of The 2nd International Conference on Computer Engineering and Technology (ICCET 2010),* Chengdu, China, Apr. 16-18, 2010, pp. 181-185.
- J. Surbot and S. Witosurapot, “Discovering Secured Group Services among UPnP Networks,” in *Proceeding of The 6th National Conference on Computing and Information Technology (NCCIT’ 06), Bangkok, Thailand*, Jun. 3-5, 2010. pp. 329-334.

ประวัติผู้เขียน

ชื่อ สกุล นายจักรพันธ์ สัวบุตร

รหัสประจำตัวนักศึกษา 5010120005

วุฒิการศึกษา

วุฒิ	ชื่อสถาบัน	ปีที่สำเร็จการศึกษา
วิศวกรรมศาสตรบัณฑิต (วิศวกรรมคอมพิวเตอร์)	มหาวิทยาลัยสงขลานครินทร์	2550

ทุนการศึกษา (ที่ได้รับในระหว่างการศึกษา)

ทุนบัณฑิตศึกษาภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์มหาวิทยาลัยสงขลานครินทร์

การตีพิมพ์เผยแพร่ผลงาน

- J. Surbot and S. Witosurapot, "A Collaboration Agent for Exploiting Legacy Phones in Assistive UPnP-based Home Environments," in *Proceeding of The 7th International Joint Conference on Computer Science and Software Engineering (JCSSE 2010),* Bangkok, Thailand, May. 12-14, 2010, pp. 199-203.
- J. Surbot and S. Witosurapot, "Integrating Group Key Distribution for Securing UPnP Services," in *Proceeding of The 2nd International Conference on Computer Engineering and Technology (ICCET 2010),* Chengdu, China, Apr. 16-18, 2010, pp. 181-185.
- J. Surbot and S. Witosurapot, "Discovering Secured Group Services among UPnP Networks," in *Proceeding of The 6th National Conference on Computing and Information Technology (NCCIT' 06), Bangkok, Thailand*, Jun. 3-5, 2010. pp. 329-334.