การจัดการอุปกรณ์ไฟฟ้าผ่านเครือข่ายอินเทอร์เน็ตด้วยโทรศัพท์เคลื่อนที่

อานนท์ ผ่องรัศมีเพ็ญ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)
คณะสถิติประยุกต์
สถาบันบัณฑิตพัฒนบริหารศาสตร์
2551

การจัดการอุปกรณ์ไฟฟ้าผ่านเครือข่ายอินเทอร์เน็ตด้วยโทรศัพท์เคลื่อนที่

อานนท์ ผ่องรัศมีเพ็ญ

คณะสถิติประยุกต์

คณะกรรมการสอบวิทยานิพนธ์ ได้พิจารณาแล้วเห็นสมควรอนุมัติให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)

ผู้ช่วยศาสตราจารย์ ..... ประธานกรรมการ
(ดร.โอม ศรนิล)

รองศาสตราจารย์ .....กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์
(ดร. พิพัฒน์ หิรัณย์วณิชชากร)

ผู้ช่วยศาสตราจารย์ ..... กรรมการ
(ดร.อภิรักษ์ จิรายุสกุล)

รองศาสตราจารย์ ..... คณบดี/ผู้อำนวยการ
(ดร.สุรพงค์ เอื้อวัฒนามงคล)
วันที่ ๒๕ เดือน ..... พ.ศ. 2552

บทคัดย่อ

ชื่อวิทยานิพนธ์	การจัดการอุปกรณ์ไฟฟ้าผ่านเครือข่ายอินเทอร์เน็ตด้วยโทรศัพท์เคลื่อนที่
ชื่อผู้เขียน	อานนท์ ผ่องรัศมีเพ็ญ
ชื่อปริญญา	วิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)
ปีการศึกษา	2551

งานวิจัยนี้มีจุดมุ่งหมายเพื่อนำเสนอวิธีการจัดการควบคุมอุปกรณ์ในบ้านหรือในสำนักงานผ่านระบบเครือข่ายอินเทอร์เน็ต (Internet) ด้วยโทรศัพท์เคลื่อนที่ โดยทำการติดต่อโดยตรงไปยังอุปกรณ์ที่ต้องการควบคุม ในเครือข่ายไร้สายความมั่นคงของข้อมูลเป็นปัญหาสำคัญ ในงานวิจัยนี้จึงได้เสนอโปรโตคอลที่มีการรักษาความมั่นคงของระบบที่มีการยืนยันบุคคล การตรวจสอบสิทธิ์ในการจัดการควบคุมอุปกรณ์ การป้องกันการปฏิเสธการส่งและรับข้อมูลด้วยการทำลายเซ็นอิเล็กทรอนิกและการดำรงไว้ซึ่งความมั่นคงของข้อมูลที่ใช้ในการติดต่อสื่อสารเช่น การส่งกุญแจต่าง ๆ จะใช้อัลกอริทึมการเข้ารหัสลับแบบกุญแจอสมมาตร ส่วนการส่งคำสั่งระหว่างอุปกรณ์กับโทรศัพท์เคลื่อนที่จะใช้อัลกอริทึมการเข้ารหัสลับแบบกุญแจสมมาตร และเพื่อให้การเข้ารหัสลับบนโทรศัพท์เคลื่อนที่ด้วยกุญแจอสมมาตรสามารถทำได้อย่างรวดเร็วงานวิจัยนี้จึงได้นำหลักการ Truncated Polynomials มาใช้ในการควบคุมจัดการอุปกรณ์ ในงานวิจัยนี้ได้ใช้โปรโตคอล Simple Network Management Protocol (SNMP) ที่มีการนำเทคโนโลยี Extensible Markup Language (XML) ซึ่งเป็นมาตรฐานในการส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ต มาประยุกต์ใช้ทั้งในส่วนข้อมูลสำหรับการจัดการ (Management Information Base; MIB) และในส่วนการส่งข้อมูลให้ทำได้สะดวกและมีประสิทธิภาพมากขึ้น จากการทดลองพบว่าความเร็วในการติดต่อระหว่างโทรศัพท์เคลื่อนที่กับอุปกรณ์ที่ต้องการควบคุมสามารถทำได้ด้วยความเร็วที่สามารถนำไปประยุกต์ใช้ได้จริง

ABSTRACT

Title of Thesis	The Management of Equipments Through Internet System by Mobile Phones
Author	Arnon Phongrusamepane
Degree	Master of Science (Computer Science)
Year	2008

The objective of this research is to present a method for managing equipments in homes or offices through internet systems by mobile phones. It is direct connection to the controlled instruments. To solve security problems in wireless network, in this research propose a protocol which handles authentication, non-repudiation, data integrity, secrecy of session keys by asymmetric-key algorithm. As command sending between managed equipments and mobile phone, symmetric-key algorithm is used. Moreover, truncated polynomials principle is introduced to entrance to encrypt quickly in mobile phone with asymmetric key. Internal communication system is simple network management protocol (SNMP), which extensible markup language (XML) technology, standard for data sending through internet network, are applied in management information base (MIB). In addition, data sending are more comfortable and effective. From the experiment, speed of connection between mobile phone and equipments is appropriate for real using.

กิตติกรรมประกาศ

วิทยานิพนธ์เรื่องการจัดการอุปกรณ์ไฟฟ้าผ่านเครือข่ายอินเทอร์เน็ตด้วยโทรศัพท์เคลื่อนที่สำเร็จได้ เนื่องจากบุคคลหลายท่านได้กรุณาช่วยเหลือให้ข้อมูล ข้อเสนอแนะ คำปรึกษา ความคิดเห็น กำลังใจ และร่วมแก้ปัญหาต่าง ๆ ระหว่างดำเนินการวิจัย

ผู้เขียนขอกราบขอบพระคุณ รองศาสตราจารย์ ดร.พิพัฒน์ หิรัณย์วณิชชากร ที่ได้ให้คำชี้แนะและตรวจสอบวิทยานิพนธ์ในทุกขั้นตอน และกราบขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร.โอม ศรนิล และ ผู้ช่วยศาสตราจารย์ ดร.อภิรักษ์ จิรายุสกุล ที่ได้แนะนำและตรวจสอบวิทยานิพนธ์นี้ให้สำเร็จตามวัตถุประสงค์

ขอขอบพระคุณคณาจารย์คณะสถิติประยุกต์ ที่ได้ถ่ายทอดและสร้างเสริมความรู้ให้แก่ผู้เขียน และขอขอบคุณเจ้าหน้าที่ของคณะสถิติประยุกต์ทุกท่าน ที่ได้ให้ความช่วยเหลือทั้งด้านเทคโนโลยีสนับสนุนต่าง ๆ และช่วยติดต่อประสานงานเป็นอย่างดีด้วยอัธยาศัยไมตรีที่อบอุ่นและเป็นกันเอง และ ขอขอบคุณเจ้าหน้าที่สำนักบรรณสารการพัฒนา ที่กรุณาช่วยตรวจสอบรูปเล่มวิทยานิพนธ์ให้ถูกต้องครบถ้วนตรงตามรูปแบบที่ทางสถาบันกำหนด

ท้ายที่สุด ขอกราบขอบพระคุณบิดา มารดา อันเป็นที่รักและเคารพอย่างสูง ที่ได้ช่วยส่งเสริมสนับสนุน และเป็นกำลังใจให้ผู้เขียนตลอดมา ขอขอบคุณเพื่อน พี่ น้อง ทุกท่าน และภรรยาของผู้เขียนที่ได้มีส่วนร่วมให้คำปรึกษาและกำลังใจตลอดระยะเวลาการทำวิทยานิพนธ์ฉบับนี้

อานนท์ ผ่องรัศมีเพ็ญ

พฤษภาคม 2552

สารบัญ

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญภาพ

ภาพที่ หน้า

สัญลักษณ์และคำย่อ

สัญลักษณ์	ความหมาย
K_s	แทนกุญแจที่ใช้ร่วมกันระหว่าง ผู้ใช้กับ AS
K_{sess}	แทนกุญแจที่ใช้ร่วมกันระหว่าง ผู้ใช้กับอุปกรณ์
K_P	แทนกุญแจสาธารณะของ AS
K_{PU}	แทนกุญแจสาธารณะของผู้ใช้
K_{PA}	แทนกุญแจสาธารณะของอุปกรณ์
K_{Pr}	แทนกุญแจส่วนตัวของ AS
K_{PrU}	แทนกุญแจส่วนตัวของผู้ใช้
K_{PrA}	แทนกุญแจส่วนตัวของอุปกรณ์
Uname	แทนชื่อของผู้ใช้ (Username)
Aname	แทนชื่อของอุปกรณ์
MIB_1	แทนรายชื่ออุปกรณ์ทั้งหมดที่มี
MIB_2	แทนรายละเอียดของแต่ละอุปกรณ์

คำย่อ	
AES	Advanced Encryption Standard
Bt Address	Bluetooth Address
DOM	Document Object Model
EDGE	Enhanced Data Rates for GSM Evolution
EPG	Electronic Program Guide
GB	Giga Bytes
GPRS	General Packet Radio Service
HTTP	Hypertext Transfer Protocol
IP Address	Internet Protocol Address
IrDA	Infrared Data Association
JVM	Java Virtual Machine
J2ME	Java 2 Platform, Micro Edition
J2EE	Java 2 Platform, Enterprise Edition

LAN	Local Area Network
MHP	Multimedia Home Platform
MIB	Management Information Base
NIST	National Institute of Standards and Technology
NTru , NTRU	N-th Degree Truncated Polynomials Ring
OS	Operating System
OID	Object Identifier
PC	Personal Computer
PDA	Personal Device Association
H/PCs	Handhel Personal Computers
SMI-MIB	Structure of Management Information – MIB
SNMP	Simple Network Management Protocol
STB	Set Top Box
WLAN	Wireless Local Area Network
XML	Extensible Markup Language
X-OR	Exclusive Or

บทที่ 1

บทนำ

1.1 ปัญหาและความเป็นมา

มนุษย์เรามีความต้องการความสะดวกสบายเพิ่มมากขึ้นเรื่อย ๆ อย่างไม่สิ้นสุด ทำให้ต้องมีการศึกษาค้นคว้าพัฒนาอุปกรณ์อำนวยความสะดวกต่าง ๆ อยู่เสมอ โดยอุปกรณ์ดังกล่าวจะมีความสลับซับซ้อนมากน้อยเพียงใดขึ้นกับเทคโนโลยีในขณะนั้น ๆ ในยุคแรก ๆ เริ่มจากการใช้เทคโนโลยีระดับต่ำหรือระดับเริ่มต้นที่ไม่สลับซับซ้อน แล้วค่อย ๆ พัฒนาขึ้นไปจนถึงการใช้เทคโนโลยีระดับสูงที่มีความสลับซับซ้อนมากขึ้น ตามพัฒนาการความรู้ด้านเทคโนโลยีของมนุษย์ที่นับวันยิ่งเพิ่มมากขึ้นเรื่อย ๆ อย่างไม่สิ้นสุดเช่นกัน อาจมีหลายสิ่งหลายอย่างที่เทคโนโลยีปัจจุบันยังไม่สามารถทำได้ แต่ในอนาคตอันใกล้นี้เมื่อมีการศึกษาพัฒนาเทคโนโลยีที่เหมาะสมเกิดขึ้น มนุษย์จะทำให้ สิ่งต่าง ๆ ที่ในอดีตเคยคิดกันว่าเป็นไปไม่ได้ มีความเป็นไปได้ขึ้นมา ซึ่งสิ่งเหล่านี้ได้เกิดขึ้นบ้างแล้วในปัจจุบัน เช่น มนุษย์สามารถพูดคุยโต้ตอบกันได้โดยไม่ต้องเห็นหน้ากันจากระยะทางที่ไกลกันมาก ๆ แม้กระทั่งอยู่คนละซีกโลกก็ตามซึ่งไม่เคยเกิดขึ้นในอดีต หรือแม้กระทั่งการพิมพ์ข้อความสนทนาโต้ตอบกันผ่านหน้าจอคอมพิวเตอร์จากทุกหนทุกแห่งในโลกที่มีการเชื่อมต่อกันผ่านเครือข่าย อินเทอร์เน็ต

อุปกรณ์เครื่องใช้ไฟฟ้าต่าง ๆ ภายในบ้านหรือในสำนักงานล้วนเป็นผลิตผลที่เกิดจากการใช้เทคโนโลยีเพื่อเพิ่มความสะดวกสบายให้แก่มนุษย์ทั้งสิ้น การควบคุมหรือสั่งงานอุปกรณ์เหล่านี้ในยุคเริ่มต้นที่เราคุ้นเคยคือหากเราต้องการใช้งานอุปกรณ์ชิ้นใดเราต้องเดินไปที่อุปกรณ์เหล่านั้นแล้วก็ กดปุ่ม หมุน เลื่อน หรือ กระทำการอย่างใดอย่างหนึ่งเพื่อให้อุปกรณ์เหล่านั้นเริ่มทำงานหรือหยุดการทำงาน ตามต้องการ เมื่อมนุษย์เริ่มเคยชินกับการควบคุมด้วยวิธีนี้แล้วก็เริ่มเกิดความรู้สึกว่าไม่สะดวกสบายอีกต่อไป จึงได้มีการคิดค้นและประดิษฐ์ อุปกรณ์ควบคุมที่สามารถควบคุมได้จากระยะไกล หรือที่เรียกว่า รีโมทคอนโทรล (Remote Controller) หรือที่เราเรียกกันสั้น ๆ อย่างคุ้นเคยว่า “รีโมท” ขึ้นมา ช่วยให้เราสามารถควบคุมอุปกรณ์ต่าง ๆ ได้โดยไม่ต้องลุกจากเก้าอี้ หรืออาจจะควบคุมได้จากบนเตียงนอนเลยก็สามารถทำได้ รีโมทคอนโทรล นี้ก็ยังมีข้อจำกัดในเรื่องระยะทางคือใช้ควบคุมอุปกรณ์ที่อยู่ในระยะที่ไม่ไกลจากอุปกรณ์ควบคุมมากนัก ผู้ควบคุม และ อุปกรณ์ที่ถูก

ควบคุมจะต้องอยู่ภายในพื้นที่หรือภายในห้องเดียวกันเท่านั้น จากข้อจำกัดนี้ทำให้มนุษย์เราต้องการที่จะหลุดพ้นจากมันโดยพยายามหาวิธีที่จะควบคุมอุปกรณ์เหล่านี้จากระยะที่ไกลมากขึ้นกว่าที่เป็นอยู่ถึงขนาดควบคุมจากที่ใดในโลกก็ได้ แนวความคิดนี้ไม่ใช่เรื่องเกินจริงอีกต่อไป เพราะทุกวันนี้เราสามารถติดต่อสื่อสารกันได้จากทั่วทุกมุมโลกอยู่แล้ว เทคโนโลยีอย่างหนึ่งที่กำลังได้รับความนิยมและได้รับความคุ้นเคยจากมนุษย์มากขึ้นในขณะนี้คือการเชื่อมต่อกันของเครื่องคอมพิวเตอร์จากสถานที่ต่าง ๆ ผ่านระบบเครือข่ายอินเทอร์เน็ต

ระบบเครือข่ายอินเทอร์เน็ตเป็นช่องทางการสื่อสารที่สามารถนำมาประยุกต์ใช้งานได้หลากหลายรูปแบบตามที่หลาย ๆ คนคุ้นเคยกันอยู่ ทุกวันนี้อาจกล่าวได้ว่าทุกบ้านล้วนแล้วแต่มีการใช้งาน ระบบเครือข่าย อินเทอร์เน็ต เพื่อวัตถุประสงค์อย่างใดอย่างหนึ่ง ซึ่งอาจเพื่อการศึกษา หรือเพื่อประโยชน์ทางธุรกิจ หรือเพื่อการแลกเปลี่ยนข้อมูลข่าวสารกันระหว่างเพื่อนหรือระหว่างคนในครอบครัว หรือใช้เป็นช่องทางสำหรับส่งผ่านคำสั่งจาก อุปกรณ์ควบคุม (Remote Controller) ไปทำการควบคุม อุปกรณ์ต่าง ๆ

โทรศัพท์เคลื่อนที่ (Mobile Phone or Cellular Phone) เป็นอีกหนึ่งอุปกรณ์อำนวยความสะดวกที่มีการพัฒนามาอย่างต่อเนื่อง จากเดิมที่สื่อสารกันแบบแอนาลอก (Analog) จนมาถึง การสื่อสารกันแบบ ดิจิตอล (Digital) เราเริ่มจากการใช้โทรศัพท์เคลื่อนที่เพื่อการสื่อสารกันด้วยเสียง หรือ ด้วยข้อความสั้น ๆ จนกระทั่งในปัจจุบันเราสามารถใช้โทรศัพท์เคลื่อนที่สำหรับการสื่อสารด้วยภาพนิ่ง หรือ ภาพเคลื่อนไหว หรือข้อความที่มีทั้งรูปภาพและเสียงที่เรียกว่า Multimedia Message นอกจากนี้เรายังสามารถใช้เครื่องโทรศัพท์เคลื่อนที่เพื่อเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต ได้อีกด้วย เรียกได้ว่าเครื่องโทรศัพท์เคลื่อนที่ยุคใหม่นี้มีความสามารถในการทำงานที่หลากหลายกว่าเดิม มีการนำเทคโนโลยีต่าง ๆ เข้ามารวมอยู่ในเครื่องโทรศัพท์เคลื่อนที่ เช่น กล้องถ่ายรูปดิจิตอล เครื่องเล่น Mp3 เครื่องรับวิทยุ FM นอกจากนี้ยังได้มีการพัฒนาระบบปฏิบัติการขึ้นมาให้ทำงานบนโทรศัพท์มือถือโดยเฉพาะเช่น Nokia OS Symbian OS หรือ Microsoft Smart Phone หรือ Linux OS และยังมีการพัฒนาโปรแกรมจัดการเอกสารที่ทำงานบนระบบปฏิบัติการดังกล่าว ถึงขนาดที่เราสามารถใช้เครื่องโทรศัพท์เคลื่อนที่ทำงานบางอย่างที่เราเคยทำบนเครื่องคอมพิวเตอร์ ส่วนบุคคล (Personal Computer : PC) เลยทีเดียว แม้จะยังทำงานได้ไม่ดีเท่ากับเครื่อง PC แต่การพัฒนาก็ยังมีต่อเนื่องไปเรื่อย ๆ จนในที่สุดเราจะสามารถใช้เครื่องโทรศัพท์เคลื่อนที่เพื่อทำงานแทนเครื่อง PC เลยก็เป็นได้

การควบคุมอุปกรณ์ผ่านระบบเครือข่ายอินเทอร์เน็ตกำลังได้รับความสนใจเป็นอย่างมาก มีผู้ทำการวิจัยที่เกี่ยวข้องอยู่หลายชิ้น เช่น ระบบ Home Automation (Koskela and Väänänen-Vainio-Mattila, 2004: 234-240) หรือ Home Monitor โดยมีการพัฒนาทั้งส่วนที่เป็นการควบคุมผ่านเครื่อง

PC ซึ่งมีข้อเสียคือ หากต้องการควบคุมอุปกรณ์เป้าหมายใด ๆ เราจะต้องใช้เครื่อง PC ที่มีโปรแกรมสำหรับควบคุมอุปกรณ์นั้นติดตั้งอยู่ กล่าวคือการควบคุมจะต้องทำในสถานที่เฉพาะที่มีเครื่อง PC ตั้งอยู่ เช่น ในสำนักงาน หรือ จากห้องนอน หรือห้องทำงาน คือเป็นการควบคุมอยู่กับที่ ไม่สามารถควบคุมในขณะที่เรากำลังเคลื่อนที่ได้ ซึ่งไม่สอดคล้องกับการดำเนินชีวิตที่เร่งรีบในปัจจุบันที่ต้องมีการเดินทางเสมอ ๆ จนอาจกล่าวได้ว่าผู้คนจะใช้ชีวิตส่วนใหญ่อยู่บนท้องถนนมากกว่าอยู่ที่บ้านหรือในสำนักงาน นอกจากนี้ยังมีงานวิจัยที่นำอุปกรณ์เคลื่อนที่ เช่น โทรศัพท์เคลื่อนที่ คอมพิวเตอร์แบบพกพา หรือ PDAs มาใช้เป็นอุปกรณ์ควบคุมซึ่งทำให้สามารถทำการควบคุมจากสถานที่ต่าง ๆ ได้มากขึ้นเช่น งานวิจัย (Itani and Ayman, 2003: 2015-2020; Sanguinetti, Haga, Funakoshi, Yoshida and Matsumoto, 2003: 163-168; Koskela and Väänänen-Vainio-Mattila, 2004: 234-240; Lin and Chen, 2005: 52-59) อย่างไรก็ดีงานวิจัยเหล่านี้ไม่สามารถสั่งงานอุปกรณ์เป้าหมายได้โดยตรงการควบคุมต้องผ่านแม่ข่ายให้บริการทำให้การโต้ตอบกันระหว่างอุปกรณ์ควบคุมและอุปกรณ์เป้าหมายต้องใช้เวลานาน และมีค่าใช้จ่ายเพิ่มขึ้นสำหรับอุปกรณ์เชื่อมต่อที่อยู่ตรงกลาง ถ้าเราสามารถส่งคำสั่งจากอุปกรณ์ควบคุมไปสู่อุปกรณ์เป้าหมายได้โดยตรงจะเป็นการประหยัดทั้งเวลาและ ค่าใช้จ่าย ซึ่งเป็นแนวคิดของงานวิจัยนี้ สำหรับอุปกรณ์เป้าหมายที่สนับสนุนแนวคิดนี้จะต้องมีความสามารถในการประมวลผลและปฏิบัติตามคำสั่งที่ได้รับจากอุปกรณ์ควบคุมได้อย่างถูกต้องและมีประสิทธิภาพกล่าวคือจะต้องมี หน่วยประมวลผล (Processor) อยู่ในตัว นอกจากนี้เพื่อให้สามารถควบคุมอุปกรณ์เครื่องใช้ไฟฟ้าเหล่านี้ผ่านระบบเครือข่าย อินเทอร์เน็ต ได้อุปกรณ์เหล่านี้จะต้องมีหมายเลขประจำตัวหรือ IP Address ที่ใช้สำหรับอ้างอิงในระบบเครือข่ายอินเทอร์เน็ต ด้วย ซึ่งด้วยความก้าวหน้าของเทคโนโลยีจะทำให้ในอนาคตอันใกล้นี้อุปกรณ์เครื่องใช้ของเราจะมีความสามารถดังกล่าวอย่างแน่นอน

โปรโตคอล SNMP (Simple Network Management Protocol) มีการใช้งานมาแล้วกว่า 20 ปี และยังเป็นที่นิยมอยู่จนกระทั่งทุกวันนี้หากแต่มีการปรับปรุงให้มีประสิทธิภาพมากขึ้นให้สอดคล้องกับเทคโนโลยีที่ทันสมัยขึ้นดังงานวิจัย (ประการ ผู้วิบูลย์สุข, 2546) ที่นำเทคโนโลยี XML มาปรับปรุงมาตรฐาน SNMP ให้มีประสิทธิภาพมากขึ้นโดยปรับปรุง MIB (Management Information Base) จาก SMI-MIB (Structure of Management Information – MIB) ซึ่งมีโครงสร้างข้อมูลรูปแบบของตัวอักษร (Text Based) เป็น XML-MIB แทนทำให้การเข้าถึงตัวแปรต่าง ๆ ทำได้รวดเร็วและมีประสิทธิภาพมากขึ้น และปรับปรุงในส่วนที่เกี่ยวกับข้อมูลที่ส่งระหว่างอุปกรณ์จัดการกับอุปกรณ์ที่ต้องการจัดการจากเดิมที่มีการเข้ารหัสด้วย Abstract Syntax Notation 1 มาเป็นการส่งข้อมูลในลักษณะที่เป็นเอกสาร XML เหตุผลสำคัญที่นำเทคโนโลยี XML มาใช้เนื่องจากการแลกเปลี่ยนข้อมูลในเครือข่ายอินเทอร์เน็ตโดยทั่วไปล้วนแล้วแต่ใช้ XML เป็นมาตรฐานประกอบ

กับมีเครื่องมือ (Tool) ต่าง ๆ ที่สนับสนุนการพัฒนาโปรแกรมด้วย XML ให้สามารถทำได้รวดเร็วและมีประสิทธิภาพมากขึ้นในงานวิจัยครั้งนี้จึงนำแนวคิดนี้มาประยุกต์ใช้เพื่อให้การจัดการควบคุมอุปกรณ์ทำได้รวดเร็วและมีประสิทธิภาพมากที่สุด

ความมั่นคงของระบบควบคุมเป็นอีกสิ่งหนึ่งที่มิอาจมองข้ามได้เพราะหากการจัดการอุปกรณ์ภายในบ้านหรือสำนักงานเกิดจากการกระทำของผู้ที่ไม่มีหน้าที่เกี่ยวข้องหรือผู้ที่ไม่หวังดีก็จะก่อให้เกิดอันตรายกับเจ้าของบ้านและอุปกรณ์ที่ถูกควบคุม จึงจำเป็นต้องมีการจำกัดการจัดการควบคุมให้สามารถทำได้เฉพาะผู้ที่มีหน้าที่เกี่ยวข้องหรือผู้ที่มีสิทธิ์ในการจัดการควบคุมเท่านั้น ดังนั้นก่อนที่ระบบจะยอมให้ใครจะสามารจัดการอุปกรณ์ได้จะต้องผ่านการพิสูจน์ตัวตนก่อน อีกทั้งความมั่นคงของข้อมูลที่ส่งก็เป็นสิ่งจำเป็นหากข้อมูลที่ส่งจากผู้ควบคุมถูกแก้ไขระหว่างทางโดยผู้ไม่หวังดีหรือด้วยข้อผิดพลาดใด ๆ ก็ตามหรือหากเกิดการรั่วไหลของข้อมูลระหว่างขั้นตอนการรับส่งย่อมก่อให้เกิดความเสียหายได้ไม่แพ้กัน จึงต้องมีการตรวจสอบความมั่นคงของข้อมูลด้วย มีงานวิจัย (Itani and Ayman, 2003: 2015-2020) เป็นการติดต่อระหว่าง J2ME Client กับ J2EE Server ที่มีการเข้ารหัสข้อมูลด้วย AES ซึ่งเป็นอัลกอริทึมแบบกุญแจสมมาตร เพื่อรักษาความลับของข้อมูลในงานด้านการธนาคาร นอกจากนี้ยังมีการยืนยันบุคคลด้วย Username และ Pin Code แต่ยังไม่มีการใช้ลายเซ็นอิเล็กทรอนิกเนื่องจากข้อจำกัดของโทรศัพท์เคลื่อนที่ทั้งหน่วยความจำที่มีอยู่จำกัดและความสามารถในการประมวลผลต่ำ เพื่อแก้ปัญหานี้จึงมีงานวิจัย (Prapoorna and Avadhani, 2007: 130-133) ที่นำเสนอเทคโนโลยี N-th Degree Truncated Polynomials Ring (NTru, NTRU) (NTRU Cryptosystem,1998) ซึ่งเป็นอัลกอริทึมแบบกุญแจอสมมาตรที่อาศัยหลักการของ Truncated Polynomials Ring มาใช้ในการเข้ารหัสลับข้อมูลและสร้างลายเซ็นอิเล็กทรอนิกเนื่องจากมีความรวดเร็วกว่า RSA มากแต่ประสิทธิภาพใกล้เคียงกัน

งานวิจัยนี้จึงได้นำเสนอวิธีการรักษาความปลอดภัยและความมั่นคงของระบบที่เข้มแข็งโดยใช้เทคโนโลยีการเข้ารหัสลับข้อมูลด้วยกุญแจอสมมาตรโดยพัฒนามาจากวิธีการ Truncated Polynomials ตามแนวทางงานวิจัยข้างต้น ร่วมกับหลักการกุญแจสมมาตรโดยเฉพาะอย่างยิ่งการนำมาใช้กับโทรศัพท์เคลื่อนที่ ซึ่งจากงานวิจัยที่ผ่านมายังไม่มีการนำหลักการกุญแจอสมมาตรมาใช้เนื่องจากเป็นหลักการที่ต้องใช้ทรัพยากรในการทำงานที่มีประสิทธิภาพสูง เพื่อทำการทดสอบหลักการดังกล่าวจึงได้ทำการวิจัยโดยสร้างต้นแบบระบบการจัดการอุปกรณ์ไฟฟ้าผ่านเครือข่ายอินเทอร์เน็ตด้วยโทรศัพท์เคลื่อนที่ขึ้น โดยพัฒนาระบบจากหลักการจัดการเครือข่ายด้วยโปรโตคอล Simple Network Management Protocol (SNMP) ที่มีการปรับปรุงโดยนำเทคโนโลยี XML มาใช้ตามแนวทางงานวิจัย (ประการ ผู้วิบูลย์สุข, 2546)

ภาพรวมของระบบทดสอบที่ใช้ในงานวิจัยจะแบ่งเป็นสองส่วน คือ ส่วนการรักษาความมั่นคง กับส่วนการจัดการอุปกรณ์ ในส่วนของการรักษาความมั่นคงนั้นจะใช้หลักการกุญแจอสมมาตรตามหลักการ Truncated Polynomials ร่วมกับ หลักการเคอร์เบอร์โรส สำหรับส่วนที่เกี่ยวกับการจัดการอุปกรณ์นั้นจะใช้หลักการกุญแจสมมาตรเนื่องจากใช้ทรัพยากรน้อยกว่า การสื่อสารทั้งสองส่วนจะใช้หลักการของโปรโตคอล SNMP ที่มีการนำเทคโนโลยี XML เข้ามาประยุกต์ใช้เพื่อให้การสื่อสารข้อมูลทำได้สะดวกรวดเร็วและมีประสิทธิภาพ และสอดคล้องกับเทคโนโลยีปัจจุบันที่ใช้ XML เป็นมาตรฐานในการส่งผ่านข้อมูล

1.2 วัตถุประสงค์การวิจัย

งานวิจัยนี้มีจุดมุ่งหมายเพื่อเสนอวิธีการจัดการควบคุมอุปกรณ์ ผ่านระบบเครือข่ายอินเทอร์เน็ต (Internet) ด้วยโทรศัพท์เคลื่อนที่โดยตรงไปยังอุปกรณ์ที่มีความสามารถในการประมวลผลที่เพียงพอ และเสนอวิธีการรักษาความมั่นคงของระบบโดยเพิ่มการยืนยันบุคคล การใช้ลายเซ็นอิเล็กทรอนิกและการตรวจสอบสิทธิ์ในการจัดการควบคุมอุปกรณ์รวมถึงการดำรงไว้ซึ่งความมั่นคงของข้อมูลที่ใช้ในการติดต่อสื่อสารเพื่อส่งคำสั่งสำหรับจัดการควบคุม

1.3 ขอบเขตการวิจัย

1.3.1 โทรศัพท์เคลื่อนที่ที่ใช้ทดลองในงานวิจัยนี้ คือ NOKIA 3110 ซึ่งรองรับโปรแกรมที่พัฒนาด้วยภาษาจาวาที่มีขนาดสูงสุด 1 GB และใช้ระบบปฏิบัติการของโนเกีย (NOKIA OS) สามารถเชื่อมต่อเข้าสู่อินเทอร์เน็ตด้วยเทคโนโลยี GPRS (Forum Nokia, 2007)

1.3.2 เครื่องแม่ข่ายในการยืนยันบุคคลใช้ ระบบปฏิบัติการ Windows XP Professional Version 2002 หน่วยประมวลผล Intel Pentium® M Processor 1.73 GHz หน่วยความจำภายใน 2 GB

1.3.3 เอเจนท์บนอุปกรณ์ไฟฟ้าจำลองด้วย ระบบปฏิบัติการ Windows XP Professional Version 2002 หน่วยประมวลผล Intel Pentium® M Processor 1.73 GHz หน่วยความจำภายใน 2 GB

1.3.4 ใช้โปรโตคอล SNMP ในการติดต่อระหว่างโทรศัพท์เคลื่อนที่ (Manager) กับอุปกรณ์ (Agent)

1.3.5 ใช้มาตรฐาน XML สำหรับข้อมูลการจัดการ (MIB) และสำหรับการสื่อสารข้อมูลด้วยโปรโตคอล SNMP

1.3.6 งานวิจัยนี้ตั้งอยู่บนสมมติฐานที่ว่าอุปกรณ์ที่ถูกจัดการนั้นเชื่อมต่อกับระบบเครือข่ายอินเทอร์เน็ต โดยมีสถานะเป็นโหนดหนึ่งมี IP Address ของตนเอง และมีหน่วยประมวลผลที่สามารถทำงานที่สนับสนุนโปรโตคอล SNMP และสนับสนุนหลักการเข้ารหัสข้อมูล (Encryption) และการถอดรหัสข้อมูล (Decryption) สำหรับการรักษาความมั่นคงของระบบได้

1.4 ทฤษฎีที่ใช้ในการวิจัย

ในการวิจัยนี้มีสาระและทฤษฎีที่ผู้วิจัยนำมาประยุกต์ใช้ดังต่อไปนี้

1.4.1 ทฤษฎีเกี่ยวกับโปรโตคอล SNMP

1.4.2 ทฤษฎีเกี่ยวกับ XML และ DOM

1.4.3 ทฤษฎีเกี่ยวกับ การรักษาความปลอดภัยบนระบบเครือข่าย อินเทอร์เน็ต ด้วยโปรโตคอล Kerberos

1.4.4 ทฤษฎีเกี่ยวกับ การเข้ารหัสลับ และ ถอดรหัสข้อมูลด้วยอัลกอริทึมกุญแจสมมาตร และ กุญแจแบบอสมมาตร

1.4.5 การพัฒนาโปรแกรมประยุกต์ด้วยภาษาจาวาในการติดต่อผ่านระบบเครือข่ายอินเทอร์เน็ต

1.4.6 การพัฒนาโปรแกรมประยุกต์บนโทรศัพท์เคลื่อนที่ด้วยเทคโนโลยี J2ME

1.4.7 การพัฒนาโปรแกรมประยุกต์ในการเข้ารหัส และ ถอดรหัสข้อมูลด้วย อัลกอริทึมกุญแจสมมาตร และ กุญแจอสมมาตร ด้วยภาษา จาวา

1.5 วิธีการดำเนินการวิจัย

1.5.1 ศึกษางานวิจัยที่เกี่ยวข้องเพื่อเปรียบเทียบข้อดี ข้อเสียและนำข้อดีของงานวิจัยเหล่านั้นมาประยุกต์ใช้ในงานวิจัย

1.5.2 รวบรวมคำสั่งที่ใช้ในการควบคุมอุปกรณ์เป้าหมายแต่ละชนิด และแบ่งประเภทตามลักษณะการดำเนินการกับตัวแปรต่าง ๆ

1.5.3 ศึกษาโปรโตคอล SNMP เพื่อนำมาประยุกต์สำหรับการจัดการอุปกรณ์ตามคำสั่งแต่ละประเภท

1.5.4 ศึกษาภาษา XML เพื่อนำมาใช้ในการกำหนดรูปแบบข้อความที่ใช้สื่อสารระหว่างผู้ใช้ กับ เอเจ้นท์

1.5.5 ศึกษาการใช้ DOM เพื่อตรวจสอบและวิเคราะห์เอกสาร XML

1.5.6 ศึกษาการเขียนโปรแกรมติดต่อระบบเครือข่าย อินเทอร์เน็ต ด้วยภาษาจาวา

1.5.7 ศึกษาการเขียนโปรแกรมเพื่อการเข้ารหัสและถอดรหัสข้อมูลด้วยภาษาจาวา

1.5.8 ศึกษาเกี่ยวกับการเขียนโปรแกรมประยุกต์บนโทรศัพท์เคลื่อนที่ด้วย J2ME

1.5.9 ศึกษาเทคโนโลยีต่าง ๆ ที่ใช้ในการสื่อสารข้อมูลผ่านโทรศัพท์เคลื่อนที่

1.5.10 ศึกษาเกี่ยวกับการรักษาความปลอดภัยบนระบบเครือข่ายอินเทอร์เน็ต

1.5.11 ออกแบบโปรแกรมประยุกต์ทั้งฝั่งอุปกรณ์จัดการ ฝั่งเอเจนท์ และโปรแกรมประยุกต์ที่เป็นแม่ข่ายเกี่ยวกับการรักษาความปลอดภัย

1.5.12 ทำการทดสอบการทำงานและปรับปรุงโปรแกรมทั้งระบบ

1.5.13 สรุปผลการวิจัย และ ข้อเสนอแนะ

1.6 ความสำคัญหรือประโยชน์ที่คาดว่าจะได้รับ

1.6.1 ทำให้มีความเข้าใจเกี่ยวกับโปรโตคอล SNMP ภาษา XML ภาษา จาวา และการจัดการด้านความปลอดภัยบนระบบเครือข่าย อินเทอร์เน็ต มากขึ้น

1.6.2 สามารถนำโปรโตคอล SNMP มาเป็นต้นแบบในการพัฒนาวิธีการควบคุมอุปกรณ์ไฟฟ้าผ่านระบบเครือข่ายอินเทอร์เน็ตที่ใช้ ภาษา XML เป็นมาตรฐานในการรับส่งข้อมูลได้

1.6.3 สามารถสร้างโปรแกรมประยุกต์สำหรับควบคุมอุปกรณ์ไฟฟ้าผ่านระบบเครือข่ายอินเทอร์เน็ต ผ่านโทรศัพท์เคลื่อนที่โดยใช้ไอพีแอ็ดเดรส (IP Address) ของอุปกรณ์ในการติดต่อส่งคำสั่งต่าง ๆ

1.6.4 ผลจากงานวิจัยนี้จะช่วยเพิ่มความสะดวกในการติดต่อสื่อสารเพื่อจัดการอุปกรณ์เป้าหมายให้สามารถทำได้จากที่ไหนเวลาใดก็ได้ตามความต้องการ โดยปราศจากข้อจำกัดด้านสถานที่และเวลา ไม่มีข้อยกเว้นแม้กระทั่งในขณะที่กำลังเดินทาง ก็สามารถทำได้เนื่องจากโดยปรกติคนส่วนใหญ่จะพกพาเครื่องโทรศัพท์เคลื่อนที่ติดตัวไปด้วยเสมอ นอกจากนี้ยังช่วยลดจำนวนอุปกรณ์สำหรับควบคุม (Controller) คือสามารถใช้ อุปกรณ์ควบคุมเพียงเครื่องเดียว สำหรับควบคุมอุปกรณ์เป้าหมายหลาย ๆ เครื่องแทนการใช้อุปกรณ์ควบคุม หนึ่งเครื่องสำหรับควบคุมอุปกรณ์เป้าหมายหนึ่งเครื่องเหมือนที่เป็นอยู่ในปัจจุบัน

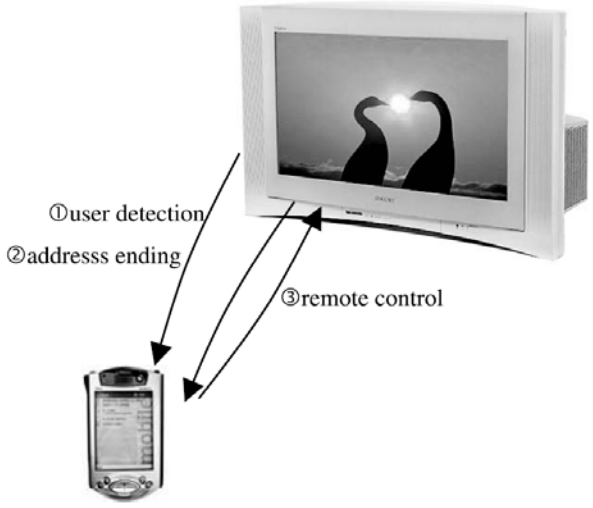
บทที่ 2

ทฤษฎีที่เกี่ยวข้อง และ การทบทวนวรรณกรรม

2.1 งานวิจัยที่เกี่ยวข้อง

2.1.1 FReCon: a Fluid Remote Controller for a Freely Connected World in a Ubiquitous Environment

งานวิจัยนี้ (Sanguinetti, Haga, Funakoshi, Yoshida and Matsumoto, 2003: 163-168) นำเสนอแนวคิดในการสร้างอุปกรณ์ควบคุมที่สามารถใช้ควบคุมอุปกรณ์ภายในบ้านหลาย ๆ เครื่อง ด้วยอุปกรณ์ควบคุมเพียงเครื่องเดียว โดยนำอุปกรณ์พกพา เช่น PDAs H/PCs หรือโทรศัพท์เคลื่อนที่มาประยุกต์ใช้เป็นอุปกรณ์ควบคุม โดยการส่งคำสั่งผ่านเครือข่ายไร้สายเฉพาะที่ที่มีขอบเขตการควบคุมอยู่ภายในบริเวณห้องเดียวกัน โดยแบ่งการทำงานของระบบเป็นสองส่วน คือ ส่วนของอุปกรณ์ที่ถูกควบคุม กับ ส่วนของอุปกรณ์ควบคุม ซึ่งเชื่อมต่อและส่งผ่านข้อมูลกันผ่านทาง Bluetooth ในงานวิจัยนี้นำเสนอระบบควบคุมโทรทัศน์ด้วยเครื่อง PDA เป็นต้นแบบดัง ภาพที่ 2.1



ภาพที่ 2.1 แสดงภาพรวมการทำงานของระบบ FReCon

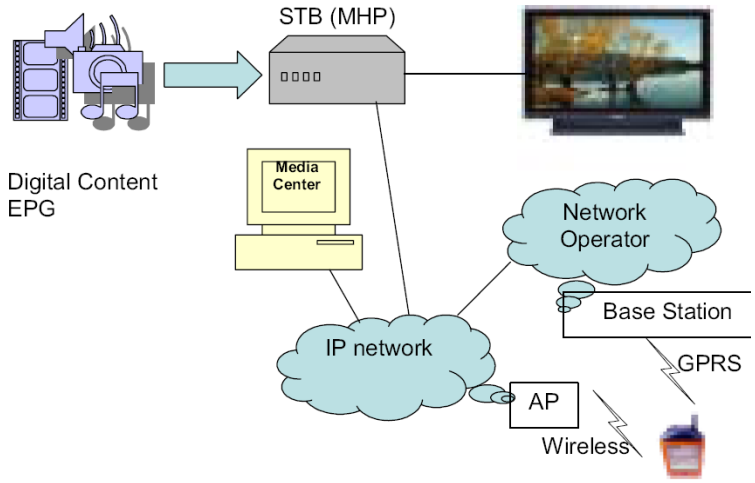
แหล่งที่มา: Sanguinetti, Haga, Funakoshi, Yoshida and Matsumoto, 2003: 164.

ระบบจะจำลองการทำงานของโทรทัศน์บนเครื่องคอมพิวเตอร์บุคคลซึ่งทำงานเป็นแม่ข่าย (Server) โดยเมื่อโทรทัศน์เริ่มทำงานจะส่ง Bluetooth Address ของตนออกมาทางพอร์ท IrDA (Infrared Data Association) ทุกๆ วินาที ในขณะที่เครื่องควบคุมที่ทำงานบนเครื่อง PDA ทำงานเป็นเครื่องผู้ใช้บริการกำลังรอรับข้อมูลอยู่ทางพอร์ท IrDA เมื่อได้รับ Bt Address ก็จะตรวจสอบว่าได้กำลังติดต่ออยู่กับ Address ดังกล่าวหรือไม่ ถ้าใช่ก็จะไม่สนใจและรอรับ Bt Address อื่นต่อไป แต่ถ้าไม่ใช่ ก็จะส่งคำขอสร้างการติดต่อผ่านพอร์ท Bluetooth กลับไปที่เซอร์ฟเวอร์ผ่านพอร์ท IrDA ซึ่งฝั่งโทรทัศน์เปิดรอรับข้อมูลอยู่ เมื่อได้รับการร้องขอดังกล่าวเข้ามาถือว่าโทรทัศน์ได้ตรวจเครื่องควบคุมแล้ว และเริ่มการติดต่อกับเครื่องควบคุมโดยใช้ โปรโตคอล Point to Point หากเครื่องรับโทรทัศน์นั้นไม่ได้ถูกควบคุมโดยเครื่องควบคุมอื่นอยู่ก็จะปรากฏหน้าเว็บสำหรับควบคุมอุปกรณ์บนเครื่องควบคุมหากไม่มีการควบคุมใด ๆเกิดขึ้นภายใน 30 วินาทีก็จะถูกตัดการเชื่อมต่อ แต่ถ้ามีการควบคุมโดยเครื่องควบคุมอื่นอยู่ก่อนแล้วหน้าเว็บ Busy ก็จะปรากฏขึ้นบนเครื่องควบคุมที่ติดต่อเข้ามาทีหลังแทน หากอยู่ในสถานะนี้โดยผู้ใช้ไม่ตัดการเชื่อมต่อเองภายใน 30 วินาทีก็จะถูกตัดการเชื่อมต่อ ระบบต้นแบบยินยอมการควบคุมโทรทัศน์แต่ละเครื่องเกิดจากเครื่องควบคุมเพียงเครื่องเดียวเท่านั้นในแต่ละขณะเวลา

ผู้ดูแลระบบสามารถกำหนดให้อุปกรณ์ที่ถูกควบคุมเครื่องเดียวสามารถมีผู้ควบคุมพร้อม ๆ กันมากกว่าหนึ่งรายได้ และ User สามารถเปลี่ยนอุปกรณ์เป้าหมายได้ตลอดเวลา

2.1.2 On Controlling Digital TV Set-Top-Box by Mobile Devices via IP Network

งานวิจัยนี้ (Lin and Chen, 2005: 52-59)ได้ออกแบบระบบที่ใช้ควบคุมเครื่องรับสัญญาณโทรทัศน์ ที่เรียกว่า Set-Top-Box โดยใช้ อุปกรณ์เคลื่อนที่ เช่น โทรศัพท์เคลื่อนที่ หรือ Laptops เป็นอุปกรณ์ควบคุม คณะผู้วิจัยได้พัฒนาการทำงานของระบบภายใต้เทคโนโลยี Multimedia Home Platform (MHP) ที่กำลังได้รับความนิยมในยุโรปในขณะนั้นซึ่งทำงานบน JVM และ สามารถทำงานสอดคล้องกับสถาปัตยกรรม Electronic Program Guide (EPG) ด้วยเทคโนโลยีทั้งสองนี้ทำให้สามารถควบคุมเครื่อง Set-Top-Box จากระยะไกลให้ทำการบันทึกรายการโทรทัศน์ระบบดิจิตอลได้ และสามารถรับชมรายการโทรทัศน์ระบบดิจิตอลแบบออนไลน์ได้ โดยหวังว่าหากในอนาคตทุกบ้านมี Personal Multimedia Server ติดตั้งอยู่ ซึ่ง Server เครื่องนี้สามารถทำงานได้หลากหลายไม่ว่าจะเป็นการแปลงฟอร์แมทของวิดีโอให้เหมาะกับอุปกรณ์แสดงภาพ และ การถ่ายทอดสัญญาณ ซึ่งมีส่วนช่วยให้สามารถนำรูปแบบงานวิจัยนี้ไปใช้ได้กับเทคโนโลยีโทรทัศน์ดิจิตอลในอนาคตได้



ภาพที่ 2.2 แสดงภาพรวมระบบควบคุมโทรทัศน์ดิจิตอลจากระยะไกล
แหล่งที่มา: Lin and Chen, 2005: 54.

การทำงานของระบบเป็นแบบ Client/Server รูปแบบของระบบเป็นดังภาพที่ 2.2 โดยในระบบจะมี STB (MHP) ที่ทำหน้าที่เป็น MHP Server รอรับการร้องขอจากผู้ใช้และประมวลผลตามการร้องขอนั้นและ Media Center หรือ PMS ซึ่งเป็นเครื่องคอมพิวเตอร์ส่วนบุคคล(Desktop PC) ทำหน้าที่เป็นตัวกลางประกอบด้วยสองส่วนได้แก่ Web Server คอยรับการร้องขอจากผู้ใช้ และ MHP Client ทำหน้าที่ส่งคำร้องขอไปที่ Server และรับการตอบกลับส่งให้ Web Server ประมวลผลส่งกลับยังผู้ใช้ในรูป Web Page โดยระบบจะให้บริการสองรูปแบบ คือ บริการให้รับชมคอนเท้นออนไลน์ และ บริการบันทึกรายการ ดังนั้นจึงแบ่งระบบการให้บริการออกเป็นสองระบบย่อย ได้แก่ ระบบย่อยสำหรับควบคุมการบันทึกรายการ และระบบย่อยสำหรับ การถ่ายทอดสัญญาณภาพดิจิตอล

ระบบย่อยระบบแรกเป็นระบบสำหรับการควบคุมการบันทึกรายการประกอบด้วย MHP Server ทำงานบน STB ทำหน้าที่ในการรอรับคำร้องขอจากผู้ใช้ ปรับช่องสำหรับรับชมรายการต่างๆ เล่นและบันทึกรายการ

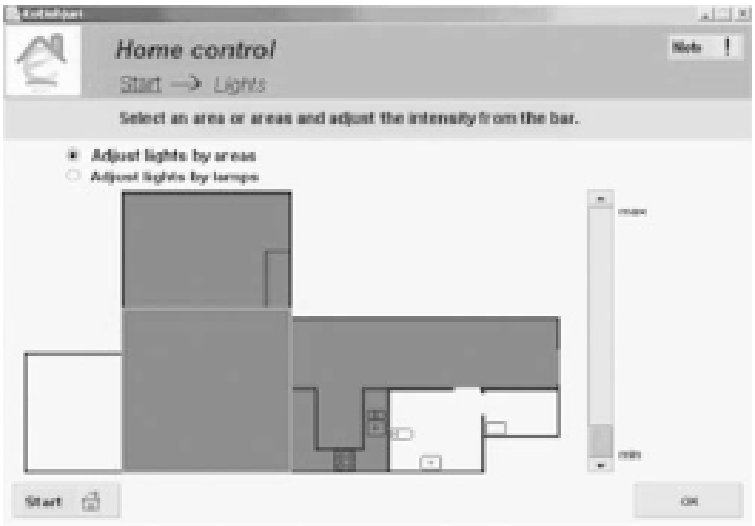
ด้าน Client แบ่งเป็น สองชนิด คือ ชนิดแรก เป็น Client สำหรับอุปกรณ์ที่มี Browser จะทำงานกับ Media Center เป็นตัวกลางรอรับคำสั่งจาก ผู้ใช้ผ่าน Web Server ที่อยู่บน Media Center เช่นกัน เพื่อส่งต่อไปยัง MHP Server และรับข้อมูลจาก MHP Server ส่งให้แก่ Web Server ประมวลผลและส่งกลับไปยังผู้ใช้ผ่าน Browser ส่วนชนิดที่สองเป็นแบบที่ไม่มี Browser เช่น

โทรศัพท์เคลื่อนที่ จะติดต่อส่งการร้องขอและรับการตอบกลับจาก MHP Server โดยตรงผ่านระบบ GPRS

ระบบย่อยระบบที่สองเป็นระบบถ่ายทอดรายการออนไลน์สำหรับอุปกรณ์เคลื่อนที่ที่ไม่มีข้อจำกัดในด้านความเร็วในการรับส่งข้อมูลและด้านการแสดงผลของจอภาพ และ มี Browser เช่น Laptop ผู้ใช้จะรับชมรายการที่ถ่ายทอดมาจาก MHP Server โดยติดต่อผ่าน Web Server ที่ทำงานบน Media Center ผ่าน Browser โดย Web Server จะทำหน้าที่ในการแปลงรูปแบบรายการโทรทัศน์ดิจิตอลที่ได้รับจาก MHP Server ให้อยู่ในรูป Video Streaming และถ่ายทอดสัญญาณนั้นต่อไปยังผู้ใช้

2.1.3 Evolution Towards Smart Home Environments: Empirical Evaluation of Three User Interfaces

งานวิจัยนี้ (Koskela and Väänänen-Vainio- Mattila, 2004: 234-240) นำเสนอการการควบคุมอุปกรณ์ภายในบ้านเช่น หลอดไฟ เครื่องปรับอากาศ ที่ต่อพ่วงกับอุปกรณ์ควบคุม Micro Controller ภายใต้ ระบบ Smart Home Environment ของ TAMPERE UNIVERSITY OF TECHNOLOGY (TUT) โดยควบคุมผ่านสามช่องทาง ได้แก่ ควบคุมผ่านเครื่อง PC (a Laptop) ด้วย GUI โดยผู้ใช้สามารถใช้เมาส์คลิกเลือก หรือใช้การสัมผัสหน้าจอดังภาพที่ 2.3 หรือควบคุมด้วยรีโมทคอนโทรลผ่านจอโทรทัศน์ (Media Terminal) โดยเลือกรายการอุปกรณ์จากการกดปุ่มลูกศรบนรีโมทคอนโทรล ดังภาพที่ 2.4 หรือควบคุมผ่านโทรศัพท์เคลื่อนที่โดยเลือกอุปกรณ์จากการกดปุ่มลูกศร ดังภาพที่ 2.5 อุปกรณ์ควบคุมทั้งสามทำหน้าที่เป็น User Interface โดยนำคำสั่งจากผู้ใช้ส่งไปยัง เครื่องคอมพิวเตอร์หลัก (Main PC) หรือ Controlling Server ที่ทำหน้าที่ส่งคำสั่งไปควบคุมอุปกรณ์ต่าง ๆ โดยการเชื่อมต่อไปยัง Main PC นั้น สำหรับโทรทัศน์จะเชื่อมต่อผ่านระบบ Ethernet LAN ส่วน PC จะเชื่อมต่อ ผ่าน WLAN หรือ Ethernet LAN ส่วนโทรศัพท์เคลื่อนที่จะเชื่อมต่อด้วยเทคโนโลยี GPRS จากเครื่องคอมพิวเตอร์หลักคำสั่งที่ได้รับก็จะถูกส่งต่อไปยังอุปกรณ์ได้ 2 ลักษณะ ได้แก่ แบบใช้สาย หรือใช้ เครือข่าย Radio Network โดยที่ตัวอุปกรณ์จะมีอุปกรณ์พิเศษสำหรับรับคำสั่งจาก Main PC แล้วทำการควบคุมอุปกรณ์อีกต่อหนึ่ง ซึ่งการส่งคำสั่งทั้งสองวิธีจะใช้ Protocol เดียวกัน โดยยึดตาม Radio Network เป็นหลัก คือ มีการใช้รูปแบบคำสั่งที่ ง่าย และ สั้น



ภาพที่ 2.3 แสดงตัวอย่างการควบคุมผ่าน PC

แหล่งที่มา: Koskela and Väänänen-Vainio- Mattila, 2004: 237.

ภาพที่ 2.4 แสดงตัวอย่างการควบคุมผ่านจอโทรทัศน์

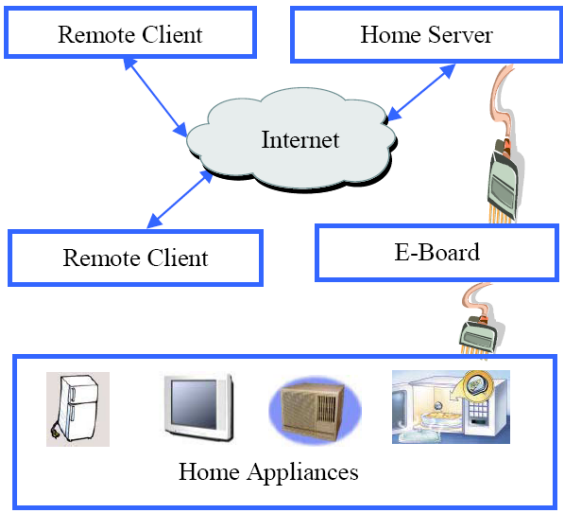
แหล่งที่มา: Koskela and Väänänen-Vainio- Mattila, 2004: 237.

ภาพที่ 2.5 แสดงตัวอย่างการควบคุมผ่านโทรศัพท์เคลื่อนที่

แหล่งที่มา: Koskela and Väänänen-Vainio- Mattila, 2004: 238.

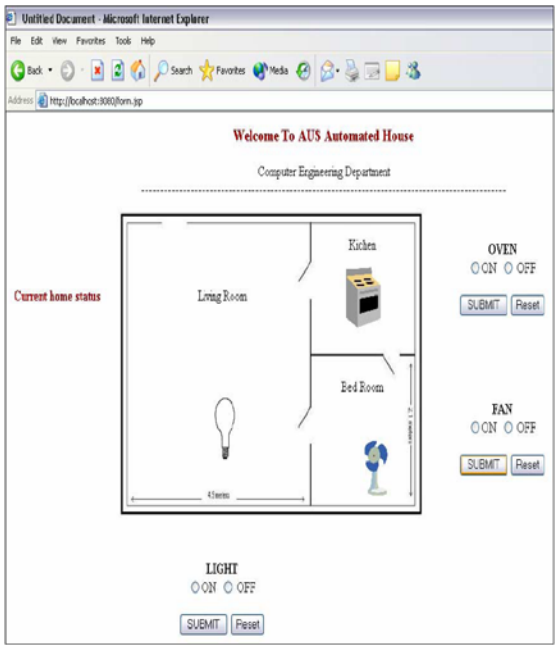
2.1.4 Java-Based Home Automation System

งานวิจัยนี้ (Al-Ali and Al-Rousan, 2004: 498-504) นำเสนอระบบ Home Automation ผ่านเครือข่าย Internet ที่มีต้นทุนต่ำบนพื้นฐานของเทคโนโลยี JAVA สำหรับใช้ในการควบคุมและตรวจสอบสถานะการทำงานของอุปกรณ์ไฟฟ้าภายในบ้าน ผ่าน Browser ไปยังเครื่อง Home Server ที่อยู่ภายในบ้าน เครื่อง Server จะทำหน้าที่ตรวจสอบสิทธิ์และส่งสถานะการทำงานของอุปกรณ์ หรือรับคำสั่งต่าง ๆ จาก User แล้วส่งต่อคำสั่งไปยังอุปกรณ์ควบคุม (E-Board) ซึ่งทำหน้าที่ในการควบคุมอุปกรณ์ไฟฟ้าในบ้านผ่าน Parallel Port ส่วนอุปกรณ์ไฟฟ้าภายในบ้านจะเชื่อมต่อกับ Input/Output Ports (Parallel Port) ของ E-Board ดังภาพที่ 2.6 การควบคุมและตรวจสอบสถานะการทำงานสามารถทำได้ทั้งจากเครือข่ายผ่าน Server และ จากภายในบ้านผ่าน E-Board โดยตรงขึ้นอยู่กับความต้องการของผู้ใช้ ข้อมูลที่ส่งระหว่าง Server กับ E-Board อยู่ในรูป Binary Code ขนาด 8 Bits



ภาพที่ 2.6 แสดงลักษณะการทำงานของระบบ

แหล่งที่มา: Al-Ali and Al-Rousan, 2004: 499.

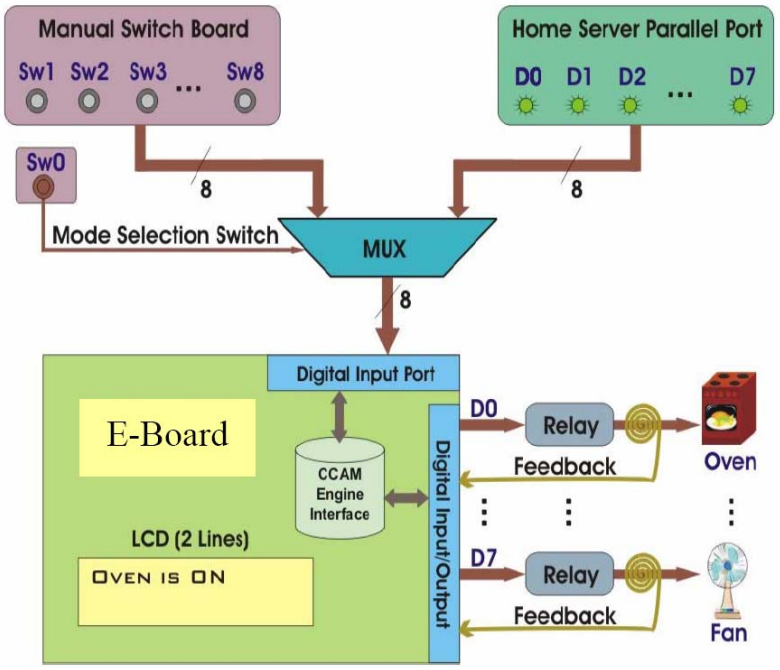


ภาพที่ 2.7 แสดงหน้าต่าง GUI สำหรับควบคุมอุปกรณ์ตัวอย่าง 3 ชนิด

แหล่งที่มา: Al-Ali and Al-Rousan, 2004: 503.

สำหรับการควบคุมผ่าน Internet โปรแกรมภาษา JAVA (Java-Based Control and Management: JCAM) จะเก็บและทำงานบนเครื่อง Home Server ซึ่งจะทำหน้าที่สื่อสารข้อมูลด้วยคำสั่งที่เขียนด้วยภาษา JAVA ระหว่าง User กับ E-Board โดยส่งคำสั่งไปยัง E-Board ในรูป Binary Code ที่อยู่ในช่วง 00000000 ถึง 11111111 ซึ่งสามารส่งคำสั่งที่ต่างกันได้ถึง 256 คำสั่ง แต่ละคำสั่งจะใช้ควบคุมฟังก์ชันของอุปกรณ์เป้าหมายเพียงเครื่องเดียวเท่านั้น ตัวอย่างคำสั่งแสดงดังภาพที่ 2.9 โปรแกรม ที่เขียนด้วยภาษา Interactive C ที่เก็บและทำงานบน E-Board จะทำหน้าที่ในการส่งคำสั่งควบคุมวงจรที่ต่อกับอุปกรณ์ไฟฟ้าโดยตรง

ส่วนการตรวจสอบ User จะนำ Username และ Password ที่ User ป้อนเข้ามาในหน้า Login แล้วนำมาเปรียบเทียบกับ ที่กำหนดไว้ใน LoginBean Code



ภาพที่ 2.8 แสดงการทำงานของระบบ Home Automation

แหล่งที่มา: Al-Ali and Al-Rousan, 2004: 500.

Command	Function	Location
1010 1001	Light bulb ON	Living room
1001 1100	Light bulb OFF	Living room
1001 1001	Microwave ON	Kitchen
1001 1111	Microwave OFF	Kitchen
1110 1110	Air conditioning ON	Living room
0110 0110	Air conditioning OFF	Living room
0110 1111	Air conditioning OFF	Bedroom

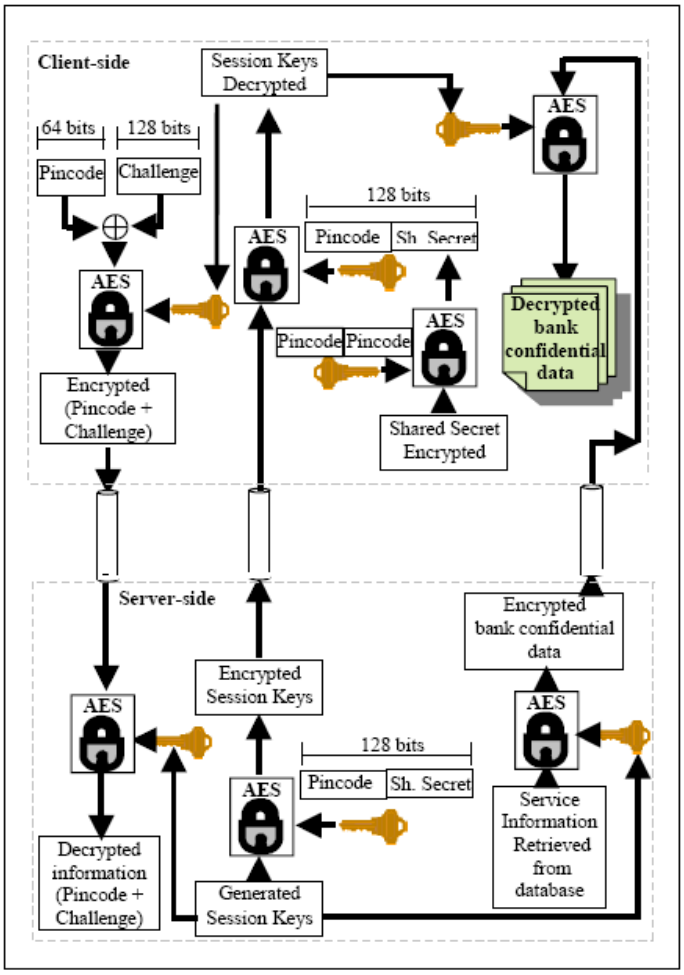
ภาพที่ 2.9 แสดงตัวอย่างคำสั่งในรูป Binary Code 8 บิต

แหล่งที่มา: Al-Ali and Al-Rousan, 2004: 500.

2.1.5 J2ME End-to-End Security for M-Commerce

งานวิจัยนี้ (Itani and Kayssi, 2003: 2015-2020) มุ่งหวังที่จะนำเสนอการใช้ Pure JAVA Component ในการสร้างการติดต่อ แบบ End-to-End ที่มีการ Authentication สำหรับ Client และการส่งข้อมูลที่เป็นความลับระหว่าง Wireless J2ME Based Client กับ J2EE Based Server โดยมีการนำเสนอการ Encryption ข้อมูลบน J2ME ในระดับ Application Layer โดยใช้ AES Rijndael Symmetric Block Cipher Algorithm เพื่อการยืนยันบุคคล (Authentication) และ รับประกันการส่งข้อมูลว่าเป็นความลับ ระหว่าง Mobile User กับ Banking Service แบบ End-to-End

วัตถุประสงค์หลักคือต้องการความปลอดภัยในระดับสูงที่ใช้งานได้ง่ายและสร้างขึ้นใช้งานได้ง่ายโดยไม่ต้องมีการปรับแต่งโปรโตคอลเดิมหรือ Infrastructure ใด ๆ ของ Wireless Network งานวิจัยนี้ได้เสนอแนวทางการรักษาความปลอดภัยโดยใช้ KSSL ซึ่งเป็น Lightweight SSL ซึ่งสนับสนุน RSA-RC4-128-MD5 และ RSA-RC4-40-MD5 Cipher Suit เนื่องจาก J2ME ไม่สนับสนุน Internet Protocol เช่น TCP/IP ดังนั้นจึงใช้ HTTP แทนซึ่งทำงานได้กับทั้ง Internet Protocol และ Non-internet Protocol โดยจะใช้ KSSL ที่ประยุกต์กับการใช้การเข้ารหัสแบบ AES ในการส่งกุญแจร่วมจากฝั่ง Server ไปยัง Client หลังจากนั้นจึงใช้กุญแจร่วมที่ได้รับในการสื่อสารข้อมูลถึงกัน



ภาพที่ 2.10 แสดงการทำงานของระบบ

แหล่งที่มา: Itani and Kayssi, 2003: 2019.

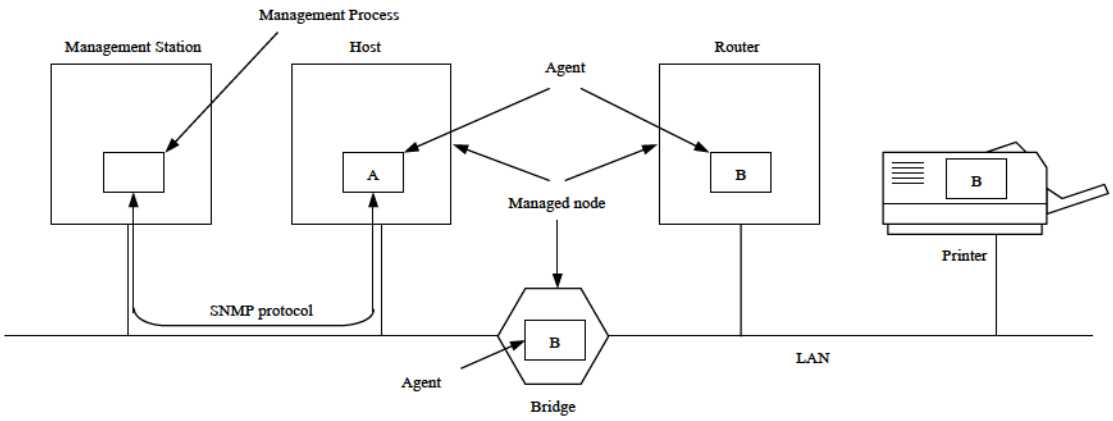
การทำงานของระบบใช้การเข้ารหัสแบบกุญแจสมมาตรโดย AES ในที่นี้ใช้กุญแจสองอัน คือ สำหรับตอนที่ Client ส่งข้อมูลไปยัง Server ใช้กุญแจอันหนึ่ง ส่วนตอนที่ Server ส่งข้อมูลไปยัง Client ใช้กุญแจอีกอันหนึ่ง ซึ่งได้รับจากฝั่ง Server ก่อนที่จะเริ่มการส่งข้อมูลถึงกัน ตามหลักการ KSSL จากภาพที่ 2.10 เริ่มจากฝั่ง Server ที่อยู่ด้านล่างของภาพ สร้างกุญแจลับ (Session Keys) ขึ้นมาคู่หนึ่ง แล้วนำมาเข้ารหัสด้วย AES ด้วยกุญแจลับที่สร้างจากการนำ Pin Code ของผู้ใช้และ Shared Secret ที่อ่านจากฐานข้อมูลมาต่อกัน ส่งไปให้ Client ดังส่วนตรงกลางของภาพ จากนั้น Client ถอดรหัสออกมาได้กุญแจลับสองอัน อันแรกใช้สำหรับการส่งข้อมูลของผู้ใช้ ดังส่วนด้านซ้ายของภาพ อันที่สองใช้สำหรับการรับข้อมูลของผู้ใช้ ดังส่วนด้านขวาของภาพ และภาพ

ด้านซ้ายแสดงการพิสูจน์ตัวตนของ Client โดยส่ง Pin Code และ Challenge ที่เข้ารหัสด้วยกุญแจลับที่ใช้สำหรับการส่ง Server ก็จะใช้กุญแจอันเดียวกันถอดรหัสข้อมูล และภาพด้านขวาเป็นการส่งข้อมูลที่เข้ารหัสลับด้วยกุญแจลับอีกอันหนึ่งกลับไป Client ก็จะใช้กุญแจลับอันเดียวกันนี้ถอดรหัสออกมา

2.2 ทฤษฎีที่เกี่ยวข้อง

2.2.1 Simple Network Management Protocol (SNMP)

SNMP (Tanenbaum, 1996: 630-643) เป็นโปรโตคอลที่ใช้ในการจัดการอุปกรณ์ภายในเครือข่ายที่ได้รับความนิยมอย่างแพร่หลายในปัจจุบัน มีองค์ประกอบ 4 ส่วน ดังภาพที่ 2.11 ได้แก่ 1) Managed Nodes 2) Management Stations 3) Management Information 4) A Management Protocol



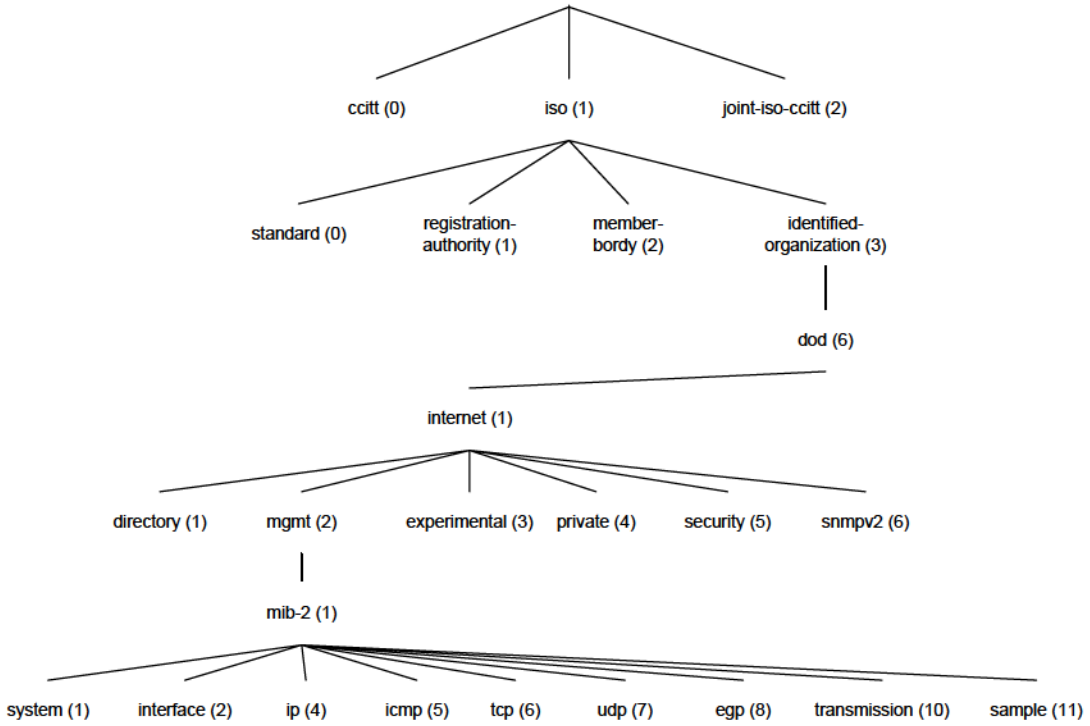
ภาพที่ 2.11 แสดงส่วนประกอบต่าง ๆ ใน SNMP Model
แหล่งที่มา: Tanenbaum, 1996: 631.

Managed Nodes คืออุปกรณ์ต่าง ๆ ที่อยู่ในระบบเครือข่าย ได้แก่ เราท์เตอร์ บริดจ์ เครื่องคอมพิวเตอร์ เครื่องพิมพ์ หรืออุปกรณ์อื่นที่สามารถสื่อสารข้อมูลกับอุปกรณ์อื่น ๆ ด้วยโปรโตคอล SNMP ได้ ภายในแต่ละ Managed Node จะมี Agent ซึ่งเป็น Process ที่ทำหน้าที่ในการรายงานสถานะการทำงานของอุปกรณ์ และข้อมูลเกี่ยวกับการทำงานของอุปกรณ์นั้นทั้งในอดีตและปัจจุบันจะเก็บไว้ที่ Agent

Management Stations โดยทั่วไปก็คือเครื่องคอมพิวเตอร์ที่มีโปรเซส อย่างน้อยหนึ่งตัวที่ทำหน้าที่ในการสื่อสารกับ Agent ที่อยู่บนเครือข่ายเพื่อจัดการกับ Agent เหล่านั้นและแสดงผลต่อผู้ดูแลระบบเป็นรูปภาพ

Management Information เป็นรูปแบบของข้อมูลที่แต่ละ Agent จะต้องเก็บและใช้ในการสื่อสารกันระหว่าง Management Stations และ Agent อุปกรณ์ทั่วไปใน SNMP จะต้องมีการเก็บค่าตัวแปรที่เรียกว่า Objects ที่บรรยายสถานะต่าง ๆ กลุ่มของ Objects เหล่านี้จะรวมกันเป็นกลุ่มข้อมูลที่เรียกว่า MIB (Management Information Base) การอ้างถึงตัวแปรต่าง ๆ ใน MIB จะใช้หมายเลขประจำตัว (Object Identifier; OID) โดยอาจใช้ชื่อที่ระบุถึงตัวแปรนั้นในรูปแบบของการท่องทรีร่วมกับหมายเลขหรืออาจใช้ ตัวเลขในวงเล็บเพียงอย่างเดียว ซึ่งตัวแปรแต่ละตัวจะมีหมายเลข OID ไม่ซ้ำกัน โครงสร้างของ MIB เป็นดังภาพที่ 2.12 ตัวอย่างการอ้างถึง ตัวแปรเช่น ip อ้างถึงโดยชื่อได้เป็น {iso (1).identified-organization (3).dod (6).internet (1).mgmt (2).mib-2 (1).ip (4)} หรืออ้างด้วยหมายเลขได้เป็น {1.3.6.1.2.1.4}

A Management Protocol เป็นข้อกำหนดที่ Management Station ใช้ในการเรียกดูข้อมูลเกี่ยวกับสถานะของ Object ของ Agent หรือแก้ไขข้อมูลได้ตามต้องการ นอกจากนี้ยังมีข้อกำหนดสำหรับ Agents เพื่อแจ้งเหตุการณ์หรือข้อผิดพลาดที่เกิดขึ้นภายในเครือข่ายให้ Management Station ทราบว่าเกิดเหตุการณ์ใดขึ้น รายงานดังกล่าวนี้เรียกว่า SNMP Trap ซึ่งเมื่อได้รับ Trap แล้ว Management Station จะเรียกดูรายละเอียดหรือไม่ก็ได้ แต่เนื่องจากการสื่อสารระหว่าง Managed Node กับ Management Stations เป็นแบบ Unreliable จึงอาจใช้รูปแบบของการเรียกดูข้อมูลเป็นระยะตามช่วงเวลาที่เรียกว่า Trap Directed Polling เพื่อตรวจสอบข้อผิดพลาดที่เกิดขึ้นในเครือข่ายที่อาจสูญหายระหว่างที่มีการส่ง Trap มาจาก Agent

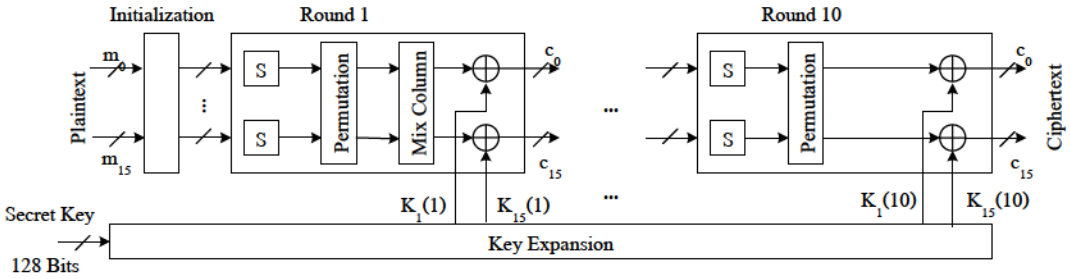


ภาพที่ 2.12 แสดงโครงสร้างของ MIB

แหล่งที่มา: Tanenbaum, 1996: 635.

2.2.2 Advanced Encryption Standard (AES)

AES (Mir, 2007: 259) เป็นอัลกอริทึมที่ใช้ในการเข้ารหัส (Encryption) และ ถอดรหัส (Decryption) แบบกุญแจสมมาตร (Symmetric Key Algorithm) แบบ Block Cipher ที่เผยแพร่ออกมาโดย National Institute of Standards and Technology (NIST) ในเดือนธันวาคม 2544 ซึ่งมีความปลอดภัยมากกว่า DES ในการเข้ารหัสข้อมูลจะมีการแบ่งข้อมูลออกเป็นบล็อคขนาด 128 Bits (16 Bytes) นำไปใช้ได้กับกุญแจขนาด ต่าง ๆ ได้แก่ 128 192 หรือ 256 Bits ซึ่งมีการทำงานหลาย ๆ รอบ ตั้งแต่ 10 ถึง 14 รอบ ขึ้นอยู่กับขนาดของกุญแจ และ ขนาดของบล็อกข้อมูล ภาพที่ 2.13 แสดงภาพรวมการทำงานของโปรโตคอล AES ที่ใช้กุญแจขนาด 128 Bits ซึ่งต้องทำการเข้ารหัส 10 รอบโดย 9 รอบแรกจะเหมือนกันยกเว้นรอบสุดท้ายจะไม่มีการมิกซ์คอลัมน์



ภาพที่ 2.13 แสดงภาพรวมของ AES

แหล่งที่มา: Mir, 2007: 259.

จากภาพที่ 2.13 แสดงข้อมูลหนึ่งบล็อคขนาด 128 บิตป้อนเข้าทางด้านซ้ายมือโดยข้อมูลจัดเป็น 16 Bytes ตั้งแต่ m_0 ถึง m_{15} เมื่อผ่านขั้นตอนเริ่มต้นแล้วก็จะผ่านเข้าสู่รอบที่ 1 เริ่มจากการแทนที่ตัวอักษรแบบไบท์ต่อไบท์ ใช้สัญลักษณ์ S แล้วส่งต่อข้อมูลที่อยู่ในลักษณะที่เป็นแถว และคอลัมน์ผ่านขั้นตอนการสับเปลี่ยน (Permutation Stage) เพื่อทำการเลื่อนแถว และผสมคอลัมน์ ขั้นตอนสุดท้ายของรอบแรกนี้ข้อมูลทั้ง 16 บล็อกจะถูกทำ X-OR กุญแจประจำรอบขนาด 16 ไบท์ จาก k_0 (1) ถึง k_{15} (1) กุญแจลับที่ใช้ในการเข้ารหัสขนาด 128 บิท จะถูกนำมาขยายเพื่อใช้งานทั้งสิ้น 10 รอบ สำหรับการถอดรหัสนั้นจะดำเนินการย้อนกลับกับการเข้ารหัสในแต่ละขั้นตอนของแต่ละรอบเป็นจำนวน 10 รอบเช่นกัน

2.2.3 Kerberos

Kerberos (Forouzan, 2007: 981-986) เป็นโปรโตคอลที่ใช้สำหรับการพิสูจน์ตัวตน และการแจกจ่ายกุญแจ (Key Distribution Center : KDC) ที่กำลังได้รับความนิยมและนำไปใช้ในระบบงานจริงหลายระบบ เช่น Windows 2000 คิดค้นขึ้นโดยมหาวิทยาลัย M.I.T. ช่วยให้เครื่องผู้ใช้สามารถติดต่อไปยังทรัพยากรต่าง ๆ ที่อยู่ในเครือข่ายได้อย่างปลอดภัย โดยตั้งอยู่บนสมมุติฐานว่านาฬิกาของเครื่องคอมพิวเตอร์ในระบบเครือข่ายนั้นตั้งไว้ตรงกัน

การทำงานภายใต้โปรโตคอล เคอร์เบอร์โรสนั้นต้องประกอบไปด้วยเครื่องแม่ข่าย (Server) จำนวนสามเครื่อง ได้แก่ 1) Authentication Server (SA) ทำหน้าที่ให้บริการตรวจสอบผู้ใช้ 2) Ticket-Granting Server (TGS) ทำหน้าที่ให้บริการออกตั๋วสำหรับใช้ติดต่อกับแม่ข่ายให้บริการ “Proof of Identity Tickets” 3) Server เป็นแม่ข่ายให้บริการตามความต้องการของผู้ใช้

2.2.4 N-th Degree Truncated Polynomials Ring (Ntru)

Ntru หรือ NTRU (NTRU Cryptosystems, 1998) เป็น Algorithm สำหรับการเข้ารหัสลับข้อมูลด้วยกุญแจแบบอสมมาตร (Asymmetric Key Encryption Algorithm) เพื่อรักษาความปลอดภัยในการส่งข้อมูลผ่านเครือข่าย คิดค้นขึ้นโดยนักคณิตศาสตร์ 4 ท่านแห่งมหาวิทยาลัยบราวน์ (Brown University) ได้แก่ Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman และ Daniel Lieman โดยนำหลักการของวงรอบพหุนาม (Polynomials Ring) ที่มีเลขชี้กำลังสูงสุดไม่เกินค่าคงที่ค่าหนึ่งที่กำหนดไว้มาดำเนินการทางคณิตศาสตร์ ร่วมกับหลักการมอดูโล (Modulo) ดังเช่นที่ใช้ในวิธีการ RSA

2.2.4.1 ความรู้ทางคณิตศาสตร์ที่เกี่ยวข้อง

NTRU อาศัยความรู้เกี่ยวกับพหุนามที่มีลักษณะพิเศษ คือ จะจำกัดค่าเลขชี้กำลังให้อยู่ในช่วง 0 ถึง N-1 โดย N คือจำนวนพจน์สูงสุดที่สามารถมีได้ของพหุนาม และเรียกพหุนามดังกล่าวว่า วงรอบพหุนาม (Truncated Polynomials Ring; R)

โดยการดำเนินการบนวงรอบพหุนามดังกล่าวนี้กระทำในสองลักษณะ ได้แก่ การบวก ซึ่งจะทำตามหลักการบวกพหุนามทั่วไป และ การคูณซึ่งจะคำนวณผลคูณตามหลักการคูณพหุนามทั่วไปก่อน จากนั้นก็จะต้องปรับค่าเลขชี้กำลังให้มีค่าไม่เกิน N-1 โดยจะแทนค่าพจน์ที่มีเลขชี้กำลังตั้งแต่ N ขึ้นไปโดยให้ $x^{N+k} = x^k$ ดังนี้ ให้ $x^N = 1$, $x^{N+1} = x$, $x^{N+2} = x^2$, $x^{N+3} = x^3$ ... ตัวอย่างเช่น ให้ $N = 3$, $a = 2 - x + 3x^2$, $b = 1 + 2x - x^2$ จะได้ว่า

$$a + b = (2 - x + 3x^2) + (1 + 2x - x^2) = 3 + x + 2x^2 \text{ และ}$$

$$a*b = (2 - x + 3x^2) * (1 + 2x - x^2) = 2 + 3x - x^2 + 7x^3 - 3x^4$$

จะเห็นว่า ค่า เลขชี้กำลังของ a*b นั้น เท่ากับ 4 ซึ่งมากกว่า N-1 คือ มากกว่า 3 – 1 = 2 จึงต้องจัดรูปของพหุนามใหม่ได้ดังนี้

$$a*b = 2 + 3x - x^2 + 7 - 3x = 9 - x^2$$

สำหรับการคูณกันของสองพหุนาม ใน R นั้นเขียนในรูปทั่วไปได้เป็น

$$a*b = c_0 + c_1x + c_2x^2 + \ldots + c_{N-2}x^{N-2} + c_{N-1}x^{N-1}$$

และค่าสัมประสิทธิ์ของแต่ละพจน์ (c_k) หาได้จาก

$$c_k = a_0b_k + a_1b_{k-1} + \ldots + a_kb_0 + a_{k+1}b_{N-1} + a_{k+2}b_{N-2} + \ldots + a_{N-1}b_{k+1}$$

อาจสรุปได้ว่า c_k หาได้จากผลรวมของผลคูณของสัมประสิทธิ์ของ a และ b ที่หมายเลขลำดับพจน์ของทั้งสองพหุนามรวมกันได้เท่ากับ k หรือเท่ากับ N+k

NTRU Encrypt PKCS จะใช้วงรอบของพหุนาม R ที่จำกัดค่าเลขชี้กำลังสูงสุดร่วมกับการลดค่าสัมประสิทธิ์ โดยการ Modulo ด้วยจำนวนเฉพาะ q ที่เป็นจำนวนเต็มนั่นคือ

$$a \bmod q$$

จะหมายถึงการลดค่าสัมประสิทธิ์ของพหุนาม a แต่ละพจน์โดยการหารด้วย q แล้วนำเศษที่เหลือมาเป็นสัมประสิทธิ์แทนในพจน์ดังกล่าว นอกจากนี้ยังมีความสัมพันธ์

$$a \equiv b \pmod q$$

หมายถึง ผลต่างระหว่างสัมประสิทธิ์ของ a และ b แต่ละพจน์ $(a_n - b_n)$ มีค่าเป็นจำนวนเท่าของ q

2.2.4.2 พารามิเตอร์ที่ใช้

องค์ประกอบพื้นฐานของ NTRU Public Key Cryptosystem (PKCS) คือการใช้วงรอบของพหุนาม (Polynomials Ring) R ที่จำกัดค่าเลขชี้กำลัง (Degree) อยู่ในช่วง 0 ถึง N-1 โดย N คือ จำนวนพจน์สูงสุดของพหุนามใน R และมีสัมประสิทธิ์เป็นจำนวนเต็ม เขียนได้ดังนี้

$$R = Z[x]/(x^N-1)$$

$$= (Z_0x^0 + Z_1x^1 + Z_2x^2 + \ldots) \bmod (x^N - 1)$$

$$= a = a_0x^0 + a_1x^1 + \ldots + a_{N-2}x^{N-2} + a_{N-1}x^{N-1}$$

พารามิเตอร์ที่ต้องกำหนดได้แก่ N ซึ่งเป็นจำนวนพจน์สูงสุดของพหุนาม

2.2.4.3 การจัดตั้งกุญแจ (Keys Generation)

ในการสร้างกุญแจส่วนตัวและกุญแจสาธารณะ ของ NTRU PKCS นั้นเริ่มจากการสุ่มเลือก พหุนามที่มีสัมประสิทธิ์ค่าน้อย ๆเมื่อเทียบกับ q ซึ่งอยู่ในวงรอบ R ขึ้นมาสองพหุนามให้ชื่อเป็น f และ g ตามลำดับและจะต้องเก็บไว้เป็นความลับ โดยมีรูปแบบดังนี้

$$f = f_0 + pf_1 \quad \text{และ} \quad g = g_0 + pg_1$$

โดย f_0 f_1 g_0 และ g_1 เป็นพหุนามที่มีสัมประสิทธิ์เป็น -1,0,1 เท่านั้น

q เป็นตัวเลขที่มีค่ามาก ๆ เมื่อเทียบกับ p เช่น 32, 128, 256

p เป็นจำนวนเฉพาะที่มีค่าน้อย ๆ เช่น 2 หรือ 3

จากนั้นต้องทำการคำนวณหาค่า Inverse ของ f Modulo q (f_q) และ Inverse ของ f Modulo p (f_p) โดย f_q และ f_p ต้องมีคุณสมบัติดังนี้

$$f * f_q = 1 \pmod q \text{ และ } f * f_p = 1 \pmod p$$

หากไม่สามารถหา f_q และ f_p ได้ก็ต้องกลับไปเลือก f ใหม่ จากนั้นก็คำนวณหากุญแจสาธารณะที่จะใช้ในการเข้ารหัสลับ (Encryption) ดังนี้

$$h = f_q * g \pmod q$$

สรุปได้ว่า กุญแจส่วนตัว คือ คู่ของ f กับ f_p และกุญแจสาธารณะคือ h

2.2.4.4 การเข้ารหัสลับ (Encryption)

ในการเข้ารหัสนั้น จะต้องสุ่มเลือก พหุนามขึ้นมาอีกหนึ่งพหุนาม เรียกว่า Blinding ให้ชื่อว่า r จากนั้นดำเนินการตามสมการต่อไปนี้

$$e = (pr*h+m)(\text{mod } q)$$

จะได้ข้อมูลที่มีการเข้ารหัสแล้ว (Cipher Text) สำหรับส่งให้ผู้รับ

2.2.4.5 การถอดรหัส (Decryption)

ในการถอดรหัสนั้นจะต้องใช้กุญแจส่วนตัว (Private Key) f และ f_p ถอดรหัสข้อความที่ได้รับตามสมการ

$$a = f*e(\text{mod } q)$$

$$= f*(r*h + m)(\text{mod } q) \quad \text{เนื่องจาก} \quad e =(r*h + m)(\text{mod } q)$$

$$= f*(r*pf_q*g + m)(\text{mod } q) \quad \text{เนื่องจาก} \quad h = pf_q*g(\text{mod } q)$$

$$= (pr*g + f*m)(\text{mod } q) \quad \text{เนื่องจาก} \quad f*f_q = 1(\text{mod } q)$$

จากนั้นนำผลลัพธ์ที่ได้ไปลดค่าสัมประสิทธิ์เทียบกับ p ตามสมการ

$$b = a(\text{mod } p)$$

จากนั้นนำพหุนามที่ได้ไปคำนวณเพื่อให้ได้ข้อความต้นฉบับตามสมการ

$$c = f_p*b(\text{mod } p)$$

$$c = f_p* b \ (\text{mod } p)$$

$$= f_p* f*m(\text{mod } p) = m \ (\text{mod } p) \quad \text{เนื่องจาก} \quad f*f_p = 1(\text{mod } p)$$

ผลลัพธ์ที่ได้คือ ข้อมูลดั้งเดิมก่อนการเข้ารหัส

2.2.4.6 ลายเซ็นอิเล็กทรอนิก (Digital Signature)

สำหรับลายเซ็นอิเล็คทรอนิกนั้นเป็นการนำ กุญแจส่วนตัว (Private Key) มาทำการเข้ารหัส (Encrypt) ข้อมูลที่ต้องการทำเป็นลายเซ็นซึ่งข้อมูลที่จะนำมาทำเป็นลายเซ็นนั้นส่วนใหญ่จะต้องทำการปรับลดขนาด (Message Digest) โดยการผ่านฟังก์ชัน Hash

การสร้างลายเซ็นเริ่มจากการนำข้อมูลที่ต้องการส่งมาสร้าง Message Digest (d) แล้วนำมาคำนวณหาพหุนามที่จะใช้เป็นข้อมูลจากสมการ

$$m = (d \text{ mod } p)$$

และเลือกพหุนาม w ที่อยู่ในรูป

$$w = m + w_1 + pw_2$$

โดย w_1 และ w_2 เป็นพหุนามที่มีสัมประสิทธิ์น้อย ๆ เมื่อเทียบกับ q จากนั้นสร้างลายเซ็น (s) ตามสมการ

$$s = f*w(\text{mod } q)$$

จากนั้นจัดรูปแบบข้อมูลที่จะส่งให้อยู่ในรูปข้อความพร้อมการเซ็นชื่อกำกับ คือคู่ของพหุนาม (m,s) นั่นเอง

2.2.4.7 การตรวจสอบลายเซ็นอิเล็กทรอนิก (Signature Verification)

ฝั่งผู้รับจะต้องตรวจสอบลายเซ็นก่อนว่ามีลายเซ็นหรือไม่ โดยตรวจสอบว่า $s \neq 0$ เมื่อถูกต้องแล้วจึงเริ่มตรวจสอบเงื่อนไขสองประการดังนี้

1) คำนวณจำนวนพจน์ที่สัมประสิทธิ์ต่างกันของพหุนาม s กับ f_0*m หลังจากนำไปลดค่าด้วย q และ p ตามลำดับ ว่าอยู่ในช่วงที่ยอมรับได้หรือไม่ดังนี้

$$D_{min} \leq Dev(s,f_0*m) \leq D_{max}$$

2) นำกุญแจสาธารณะของผู้ส่งมาคำนวณหาพหุนาม t ดังสมการ

$$t = h*s \text{ (mod } q)$$

แล้วคำนวณจำนวนพจน์ที่สัมประสิทธิ์ต่างกันของพหุนาม t กับ g_0*m หลังจากนำไปลดค่าด้วย q และ p ตามลำดับ ว่าอยู่ในช่วงที่ยอมรับได้หรือไม่ดังนี้

$$D_{min} \leq Dev(t,g_0*m) \leq D_{max}$$

D_{min} เป็นจำนวนพจน์ที่สัมประสิทธิ์ต่างกันน้อยที่สุดที่ยอมรับได้

D_{max} เป็นจำนวนพจน์ที่สัมประสิทธิ์ต่างกันมากที่สุดที่ยอมรับได้

ถ้าผ่านการตรวจสอบทั้งสองข้อดังกล่าวถือว่าเป็นลายเซ็นที่ถูกต้องดังนั้นก่อนที่จะส่งลายเซ็นผู้ส่งจะต้องตรวจสอบลายเซ็นให้ผ่านเงื่อนไขทั้งสองข้อก่อนเพื่อให้แน่ใจว่าจะผ่านการตรวจสอบที่ฝั่งรับได้แน่นอน

2.2.4.8 คุณสมบัติที่สำคัญของลายเซ็นอิเล็กทรอนิก

1) การพิสูจน์ตัวตนผู้ส่งข้อมูลสามารถยืนยันได้จากการตรวจสอบสองขั้นตอนดังนี้

(1) นำ Message Digest ไปผ่านการคำนวณค่า $f_0*m(\text{mod } q)(\text{mod } p)$ ซึ่งได้ผลลัพธ์เป็นพหุนาม แล้วนำไปเปรียบเทียบกับ ลายเซ็นที่ผ่านการคำนวณ e (mod q)(mod p) ว่ามีจำนวนพจน์ที่สัมประสิทธิ์ที่ไม่เท่ากันอยู่ในช่วงที่ยอมรับได้หรือไม่

(2) นำลายเซ็นไปผ่านการคำนวณ $t = h*s \text{ (mod } q)(\text{mod } p)$ แล้วนำไปเปรียบเทียบกับผลลัพธ์จากการคำนวณ $g_0*m(\text{mod } q)(\text{mod } p)$ ว่ามีจำนวนพจน์ที่สัมประสิทธิ์ต่างกันอยู่ในช่วงที่ยอมรับได้หรือไม่

หากผ่านเงื่อนไขทั้งสองข้อถือว่าการยืนยันสำเร็จ

2) การยืนยันว่าเป็นข้อความที่ผู้ส่งเป็นผู้สร้างขึ้นมาจริงทำได้โดยการนำข้อมูลที่ไม่ได้ถูกเข้ารหัส (Plain Text) มาทำ Message Digest แล้วนำไปเปรียบเทียบกับ Message Digest ที่ได้รับมาจากผู้ส่งหากตรงกันก็ยืนยันได้ว่าเป็นข้อมูลเดียวกัน

3) การยืนยันว่าผู้รับได้รับข้อมูลนั้นแล้วจริงโดยไม่ได้ทำการแก้ไข หากผ่านการตรวจสอบในข้อ 1) และข้อ 2) แล้วแสดงว่าเป็นข้อความเดียวกัน ซึ่งแสดงให้เห็นว่าผู้รับไม่ได้แก้ไขอย่างแน่นอนเพราะถ้ามีการแก้ไขจะทำให้ Message Digest ไม่ตรงกัน

2.2.5 การรักษาความปลอดภัยโดยใช้เทคนิค Truncated Polynomials

จากหลักการของ NTRU ที่กล่าวข้างต้นยังมีข้อบกพร่องอยู่บางประการคือการเข้ารหัส และการถอดรหัสข้อมูลไม่สามารถทำย้อนกลับกันได้ซึ่งแตกต่างกับหลักการ RSA ทำให้การสร้างลายเซ็นอิเล็กทรอนิกต้องใช้กระบวนการที่แตกต่างจากการเข้ารหัสธรรมดากล่าวคือมิใช่เพียงแค่สลับกุญแจเท่านั้น

จากปัญหาดังกล่าวจึงมีงานวิจัย (Prapoorna and Avadhani, 2007: 130-133) ได้เสนออัลกอริทึมที่ใช้หลักการ Truncated Polynomials เช่นเดียวกับใน NTRU แต่มีการพัฒนาให้มีข้อดีมากขึ้นโดยรวมข้อดีของ RSA กับ NTRU เข้าด้วยกัน ซึ่งมีข้อดีดังต่อไปนี้ 1) การเข้ารหัสและการทำลายเซ็นอิเล็กทรอนิกใช้อัลกอริทึมเดียวกัน เพียงแต่ต้องสลับหน้าที่กุญแจกัน เหมือน RSA แต่การทำงานเร็วกว่า 2) การถอดรหัสและการตรวจสอบลายเซ็นใช้อัลกอริทึมเดียวกันแต่ต้องสลับหน้าที่กุญแจเช่นกัน 3) การสร้างลายเซ็นอิเล็กทรอนิกด้วยกุญแจส่วนตัวของผู้ส่ง สามารถตรวจสอบได้ด้วยกุญแจสาธารณะของผู้ส่ง เช่นเดียวกับ RSA ซึ่ง NTRU ไม่สามารถทำได้

2.2.5.1 พารามิเตอร์ที่ใช้

องค์ประกอบพื้นฐานยังคงเหมือนกับ NTRU Public Key Cryptosystem (PKCS) คือการใช้วงรอบของพหุนาม (Polynomials Ring) R ที่จำกัดค่าเลขชี้กำลัง (Degree) อยู่ในช่วง 0 ถึง N-1 โดย N คือ จำนวนพจน์สูงสุดของพหุนามใน R และมีสัมประสิทธิ์เป็นจำนวนเต็ม เขียนได้ดังนี้

$$R = Z[x]/(x^N-1)$$

$$= (Z_0x^0 + Z_1x^1 + Z_2x^2 + \ldots) \bmod (x^N - 1)$$

$$= a = a_0x^0 + a_1x^1 + \ldots + a_{N-2}x^{N-2} + a_{N-1}x^{N-1}$$

พารามิเตอร์ที่ต้องกำหนดได้แก่

N เป็นจำนวนพจน์สูงสุดของพหุนามที่มีค่าเป็นพหุคูณของ p

q เป็นตัวเลขที่มีค่ามาก ๆ เมื่อเทียบกับ p และไม่มีตัวประกอบร่วมกับ p เช่น 32 , 128 , 256

p เป็นจำนวนเฉพาะที่มีค่าน้อย ๆ เช่น 2 หรือ 3

เช่น กำหนด N = 6, p = 3, q = 32

2.2.5.2 การจัดตั้งกุญแจ

เริ่มต้นผู้ส่งต้อง เลือกพหุนาม f ที่มีดีกรีน้อยกว่า N สำหรับใช้เป็นกุญแจส่วนตัว จากนั้นคำนวณหา ค่า Inverse ของ f Modulo q (f_q) การเลือกพหุนาม f นั้นต้องสามารถหา f_q ได้ เช่นเดียวกับใน NTRU จากนั้นเลือกพหุนาม g ที่มีดีกรีน้อย ๆ และเลือกพหุนาม r แบบสุ่ม โดยที่ค่าของ q และ p สามารถเผยแพร่สู่สาธารณะได้

เช่น กำหนด

$f = -1+x+x^4$ มีสัมประสิทธิ์เป็น (-1, 1, 0, 0, 1, 0)

$f_q = 27+23x+14x^2+28x^3+23x^4+14x^5$ มีสัมประสิทธิ์เป็น (27, 23, 14, 28, 23, 14)

$g = -1+x^2+x^3-x^5$ มีสัมประสิทธิ์เป็น (-1, 0, 1, 1, 0, -1)

$r = -1+x^2-x^3+x^5$ มีสัมประสิทธิ์เป็น (-1, 0, 1, -1, 0, 1)

กุญแจสาธารณะสามารถคำนวณได้จากสมการ

$$h = f_q+N*g$$
$$= 27+23x+14x^2+28x^3+23x^4+14x^5+6(-1+x^2+x^3-x^5)$$
$$= 27+23x+14x^2+28x^3+23x^4+14x^5 -6+6x^2+6x^3-6x^5$$
$$= 21+23x+20x^2+34x^3+23x^4+8x^5$$

โดยที่ N เป็นค่าพหุคูณของ p และจะต้องเก็บค่า f และ f_q ไว้เป็นความลับ

2.2.5.3 การเข้ารหัสข้อมูล (Encryption)

ทำได้โดยนำข้อมูลมาทำเป็นพหุนาม เช่น ข้อมูลเริ่มต้นเป็น “&” มีรหัสเป็น 100110 ทำเป็นพหุนามได้เป็น $1+x^3+x^4$

แล้วนำมาคำนวณตามสมการ

$$e = h*(m + r*q)$$
$$= (21+23x+20x^2+34x^3+23x^4+8x^5)\,(1+x^3+x^4 +32(-1+x^2-x^3+x^5))$$
$$= (-651+736x^6-1054x^6+20x^6+736x^6)$$
$$+(-713x+256x^7-713x^7+34x^7+640x^7)$$
$$+(-620x^2+672x^2-248x^8+23x^8+1088x^8)$$
$$+(-1054x^3+736x^3-651x^3+8x^9+736x^9)$$

$+(-713x^4+640x^4-713x^4+21x^4+256x^{10})$

$+(-248x^5+1088x^5-620x^5+23x^5+672x^5)$

$= -213-496x+915x^2-225x^3-509x^4+915x^5$

ซึ่งเป็นพหุนามของข้อมูลที่เข้ารหัสแล้ว (Cipher Text) สำหรับส่งไปยังผู้รับ

2.2.5.4 การถอดรหัสข้อมูล (Decryption)

เมื่อได้รับข้อมูลที่เข้ารหัสมาแล้วฝั่งรับจะทำการถอดรหัสข้อมูลด้วยกุญแจส่วนตัว โดยนำมาคำนวณตามสมการ (1) และ (2) ตามลำดับ

$a = f*e \pmod q$ (1)

$= f * \{ h (m+(r*q))\} \bmod q$

$= (f*h*m) \bmod q$

$= f*m* \{f_q+N*g\} \bmod q$

$= (m \bmod q) +(N*f*m*g) \bmod q$

$b = a \bmod p$ (2)

$b = m \bmod p$ เนื่องจาก $N = k*p$

จากนั้นนำพหุนาม b ไปแปลงเป็นข้อมูลก็จะได้ข้อมูลที่ถอดรหัสแล้ว (Plain Text)

เช่น $a = (-1+x+x^4)(-213-496x+915x^2-225x^3-509x^4+915x^5) \bmod 32$

$= \{(213+496x-915x^2+225x^3+509x^4-915x^5)$

$+(-213x-496x^2+915x^3-225x^4-509x^5+915x^6)$

$+(-213x^4-496x^5+915x^6-225x^7-509x^8+915x^9)\} \bmod 32$

$= \{(213+915x^6+915x^6)+(496x-213x-225x^7)+(-915x^2-496x^2-509x^8)$

$+(225x^3+915x^3+915x^9)+(509x^4-225x^4-213x^4)$

$+(-915x^5-509x^5-496x^5)\} \bmod 32$

$= (2043+58x-1920x^2+2055x^3+71x^4-1920x^5) \bmod 32$

$= 27+26x+7x^3+7x^4 = -5-6x+7x^3+7x^4$

$b = a \bmod p$

$= (-5-6x+7x^3+7x^4) \bmod 3$

$= 1+x^3+x^4$

นำ b มาทำเป็นข้อมูลจะได้ 100110 ซึ่งตรงกับ “&”

2.2.5.5 การทำลายเซ็นอิเล็กทรอนิก

ทำได้โดยสร้าง Message Digest (m) แล้วทำเป็นพหุนาม เช่น กำหนดข้อมูลที่ทำ Message Digest แล้วเป็น 101000 ดังนั้น

$m = 1+x^2$ และกำหนดให้

$f = -1+x+x^4$ มีสัมประสิทธิ์เป็น (-1, 1, 0, 0, 1, 0)

$f_q = 27+23x+14x^2+28x^3+23x^4+14x^5$ มีสัมประสิทธิ์เป็น (27, 23, 14, 28, 23, 14)

$g = -1+x^2+x^3-x^5$ มีสัมประสิทธิ์เป็น (-1, 0, 1, 1, 0, -1)

$r = -1+x^2-x^3+x^5$ มีสัมประสิทธิ์เป็น (-1, 0, 1, -1, 0, 1)

$h = 21+23x+20x^2+34x^3+23x^4+8x^5$ มีสัมประสิทธิ์เป็น (21, 23, 20, 34, 23, 8)

จากนั้นนำมาเข้ารหัสด้วยกุญแจส่วนตัวตามสมการ

$e = f*(m + r*q)$ โดยที่ r เป็นพหุนามที่เลือกอย่างสุ่ม

$= (27+23x+14x^2+28x^3+23x^4+14x^5)\{(1+x^2)+32(-1+x^2-x^3+x^5)\}$

$= 96-63x-33x^2+97x^3-63x^4-32x^5$

ซึ่งเป็นลายเซ็นที่จะส่งไปพร้อมกับข้อมูล จะเห็นว่าใช้อัลกอริทึมเดียวกับการเข้ารหัสเพียงแต่เปลี่ยนจากกุญแจสาธารณะมาใช้กุญแจส่วนตัวในการเข้ารหัสแทน

2.2.5.6 การตรวจสอบลายเซ็นด้วยกุญแจสาธารณะ

โดย นำ ลายเซ็นที่ได้รับมาคำนวณร่วมกับกุญแจสาธารณะตามสมการ

$a = h*e \pmod q$

$= \{(21+23x+20x^2+34x^3+23x^4+8x^5)$

$(96-63x-33x^2+97x^3-63x^4-32x^5)\} \bmod 32$

$= 7+6x+x^2-6x^3-6x^4$

จากนั้นคำนวณ

$b = a \bmod p$

$= (7+6x+x^2-6x^3-6x^4) \bmod 3$

$= 1+x^2$

นำ b มาทำเป็นข้อมูลจะได้ 101000 ซึ่งคือ Message Digest m ออกมา

ในทำนองเดียวกันจะเห็นว่าใช้อัลกอริทึมเดียวกับการถอดรหัสข้อมูลเพียงแต่เปลี่ยนจากกุญแจส่วนตัวมาใช้กุญแจสาธารณะในการถอดรหัสแทน

2.2.5.7 คุณสมบัติที่สำคัญของลายเซ็นอิเล็กทรอนิก

1) การพิสูจน์ตัวตนผู้ส่งข้อมูลสามารถยืนยันได้จากการใช้กุญแจสาธารณะของผู้ส่งถอดรหัสลายเซ็นที่ได้รับ หากสามารถทำได้ถือว่ายืนยันสำเร็จ

2) การยืนยันว่าเป็นข้อความที่ผู้ส่งเป็นผู้สร้างขึ้นมาจริงทำได้โดยการนำข้อมูลที่ไม่ได้ถูกเข้ารหัส (Plain Text) มาทำ Message Digest แล้วนำไปเปรียบเทียบกับ Message Digest ที่ได้จากการถอดรหัสด้วยกุญแจสาธารณะหากเหมือนกันก็ยืนยันได้ว่าเป็นข้อมูลเดียวกัน

3) การยืนยันว่าผู้รับได้รับข้อมูลนั้นแล้วจริงโดยไม่ได้ทำการแก้ไข หากผ่านการตรวจสอบในข้อ 2) แล้วแสดงว่าเป็นข้อความเดียวกัน ซึ่งแสดงให้เห็นว่าข้อความที่ใช้กุญแจสาธารณะของผู้ส่งถอดรหัสออกมาได้นั้นผู้รับไม่สามารถแก้ไขได้อย่างแน่นอนเพราะไม่ทราบกุญแจส่วนตัวของผู้ส่ง

จากการตรวจสอบอัลกอริทึมที่ใช้ในการเข้ารหัสและถอดรหัสพบว่า การเลือกพหุนาม f และ g นั้นจะต้องทำการทดสอบกับกุญแจคู่หนึ่งก่อนว่าเมื่อทำการเข้ารหัสด้วยกุญแจอันหนึ่งแล้วต้องสามารถถอดรหัสด้วยกุญแจอีกอันหนึ่งที่คู่กันได้ค่าที่ถูกต้อง

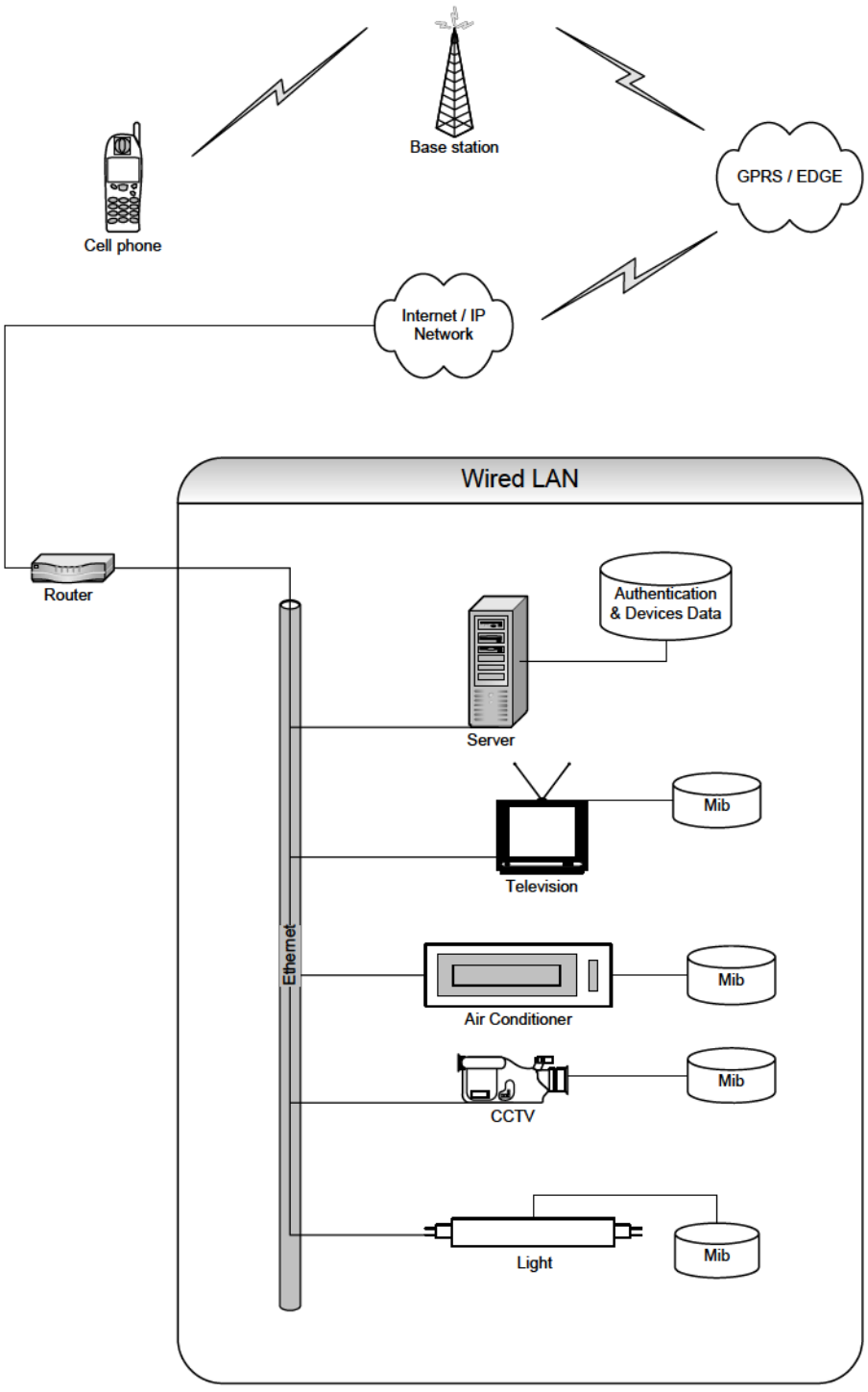
บทที่ 3

การจัดการอุปกรณ์ไฟฟ้าผ่านเครือข่ายอินเทอร์เน็ตด้วยโทรศัพท์เคลื่อนที่

3.1 แนวคิดในการวิจัย

จากภาพที่ 3.1 แสดงภาพรวมการทำงานของระบบซึ่งการควบคุมจะดำเนินการจากโทรศัพท์เคลื่อนที่ทำการเชื่อมต่อผ่านระบบ GPRS (General Packet Radio Service) ซึ่งมีอัตราการส่งข้อมูล 56 – 114 กิโลบิตต่อวินาที และอาจใช้เทคโนโลยี EDGE (Enhanced Data Rates for GSM Evolution) ช่วยเพิ่มอัตราการส่งข้อมูลได้สูงถึง 236.8 – 473.6 กิโลบิตต่อวินาที (General Packet Radio Service, 2007) ทำการเชื่อมต่อเข้าสู่เครือข่ายอินเทอร์เน็ต (IP Network) ด้วยไอพีแอดเดรสไปยังเอเจ้นท์ที่ทำงานบนอุปกรณ์โดยผ่านเร้าท์เตอร์เข้าสู่ระบบเครือข่ายเฉพาะที่ (Local Area Network; LAN) โดยมีข้อกำหนด (Protocol) ว่าก่อนที่จะติดต่อกับอุปกรณ์ได้จะต้องติดต่อไปที่แม่ข่ายให้บริการที่ทำหน้าที่ในการรักษาความปลอดภัยของระบบเพื่อทำการตรวจสอบยืนยันบุคคลและแลกเปลี่ยนข้อมูลสำคัญที่ต้องใช้ในการจัดการควบคุมอุปกรณ์ เช่น ตั๋วสำหรับใช้ติดต่อกับอุปกรณ์ กุญแจร่วม กุญแจสาธารณะของอุปกรณ์ หลังจากผ่านขั้นตอนดังกล่าวก็สามารถติดต่อไปยังอุปกรณ์เป้าหมายเพื่อจัดการควบคุมได้โดยตรงซึ่งมีการเข้ารหัสลับข้อมูลที่สื่อสารระหว่างโทรศัพท์เคลื่อนที่กับอุปกรณ์ที่ต้องการจัดการและมีการใช้ลายเซ็นดิจิตอลสำหรับคำสั่งเปลี่ยนค่าของตัวแปรบนอุปกรณ์เพื่อป้องกันการปฏิเสธความรับผิดชอบของผู้ใช้

ในการสื่อสารข้อมูลระหว่างผู้ใช้ (โทรศัพท์เคลื่อนที่) กับเอเจนท์นั้น หากสื่อสารกันด้วยรหัสคำสั่งจะทำให้ไม่สะดวกในการใช้งานกล่าวคือผู้ใช้จะต้องจำรหัสคำสั่งต่าง ๆ ได้ซึ่งเป็นการเพิ่มภาระแก่ผู้ใช้ นอกจากนี้ในส่วนของอุปกรณ์ก็จะต้องเก็บรหัสคำสั่งไว้เป็นจำนวนมากซึ่งเป็นการสิ้นเปลืองทรัพยากรเพื่อขจัดปัญหาดังกล่าวจึงนำโปรโตคอล SNMP ซึ่งมีการใช้งานด้านการจัดการเครือข่ายอยู่แล้วและมีข้อกำหนดสำหรับการสื่อสารข้อมูลคำสั่งที่เป็นมาตรฐานสามารถนำมาประยุกต์ใช้ในงานวิจัยได้เป็นอย่างดี แต่ก็ยังมีข้อที่ต้องปรับปรุงให้มีประสิทธิภาพมากขึ้นให้สอดคล้องกับเทคโนโลยีที่ทันสมัยขึ้นดังงานวิจัย (ประการ ผู้วิบูลย์สุข, 2546) ที่นำเทคโนโลยี XML มาปรับปรุงมาตรฐาน SNMP ให้มีประสิทธิภาพมากขึ้นโดยปรับปรุง MIB (Management Information Based) จาก SMI-MIB (Structure of Management Information – MIB) ซึ่งมีโครงสร้าง



ภาพที่ 3.1 แสดงสถาปัตยกรรมของระบบ

ข้อมูลรูปแบบของตัวอักษร (Text Based) เป็น XML-MIB แทนทำให้การเข้าถึงตัวแปรต่าง ๆ ทำได้รวดเร็วและมีประสิทธิภาพมากขึ้น และปรับปรุงในส่วนที่เกี่ยวกับข้อมูลที่ส่งระหว่างอุปกรณ์จัดการกับอุปกรณ์ที่ต้องการจัดการจากเดิมที่มีการเข้ารหัสด้วย Abstract Syntax Notation 1 มาเป็นการส่งข้อมูลในลักษณะที่เป็นเอกสาร XML เหตุผลสำคัญที่นำเทคโนโลยี XML มาใช้เนื่องจากการแลกเปลี่ยนข้อมูลในเครือข่ายอินเทอร์เน็ตโดยทั่วไปล้วนแล้วแต่ใช้ XML เป็นมาตรฐานประกอบกับมีเครื่องมือ (Tool) ต่าง ๆ ที่สนับสนุนการพัฒนาโปรแกรมด้วย XML ให้สามารถทำได้รวดเร็วและมีประสิทธิภาพมากขึ้นในงานวิจัยครั้งนี้จึงนำแนวคิดนี้มาประยุกต์ใช้เพื่อให้การจัดการควบคุมอุปกรณ์ทำได้รวดเร็วและมีประสิทธิภาพมากที่สุดและด้วยเทคโนโลยีปัจจุบันความสามารถในการรับส่งข้อมูลของโทรศัพท์เคลื่อนที่อยู่ในระดับ 80 – 100 kbps ถ้าใช้งานผ่านระบบ GPRS จึงสามารถสื่อสารด้วย XML ได้สะดวกและรวดเร็วและมีประสิทธิภาพ

ตามหลักการของ SNMP นั้นที่สถานีจัดการจะต้องเก็บข้อมูลสำหรับการจัดการ (MIB) ไว้ในฐานข้อมูลด้วยแต่เนื่องจากเครื่องโทรศัพท์มีหน่วยความจำที่จำกัดงานวิจัยนี้จึงออกแบบระบบไม่ให้มีการเก็บข้อมูลสำหรับการจัดการของอุปกรณ์ที่ต้องการจัดการไว้ที่เครื่องโทรศัพท์เคลื่อนที่ (Management Station) แต่จะใช้การร้องขอจาก อุปกรณ์ที่เราต้องการจัดการในขณะทำการจัดการแทน เพื่อประหยัดหน่วยความจำ และข้อมูลสำหรับการจัดการที่ได้ จะถูกนำมาแปลงเป็นข้อความสำหรับติดต่อกับผู้ใช้ (User Interface: UI) ที่สื่อความหมายให้ผู้ใช้เข้าใจง่ายก่อนนำขึ้นแสดงบนหน้าจอโทรศัพท์เคลื่อนที่ ทำให้การใช้งานทำได้ง่าย ผู้ใช้งานเพียงแค่เลือกคำสั่งบนหน้าจอโทรศัพท์เคลื่อนที่ให้ตรงกับที่ต้องการจัดการโดยการกดปุ่มแทนการป้อน Object ID จากนั้นโทรศัพท์เคลื่อนที่ก็จะนำ Object ID ไปจัดการตามโปรโตคอลของระบบต่อไปซึ่งถือว่าผู้ใช้ได้ทำงานกับอุปกรณ์นั้นแล้ว โดยผู้ใช้ไม่ต้องจดจำ Object ID ต่าง ๆ ของอุปกรณ์ที่ต้องการจัดการซึ่งเป็นเรื่องที่ยุ่งยาก และผู้ใช้งานไม่จำเป็นต้องมีความรู้เกี่ยวกับโปรโตคอลที่ใช้ด้วย นั่นคือบุคคลทั่วไปก็สามารถใช้งานได้

เนื่องจากการสื่อสารกันระหว่างผู้ใช้ กับ เอเจนท์ เป็นการสื่อสารผ่านเครือข่าย อินเทอร์เน็ต ซึ่งเป็นเครือข่ายสาธารณะอาจถูกจู่โจมจากผู้ไม่ประสงค์ดีได้ง่าย จึงจำเป็นต้องมีการรักษาความปลอดภัยอย่างเข้มงวด ในงานวิจัยนี้ได้นำเทคนิคและวิธีการในการรักษาความปลอดภัยต่าง ๆ มาใช้ได้แก่ การป้องกันการปฏิเสธการส่งและรับข้อมูลด้วยการใช้ลายเซ็นอิเล็กทรอนิค (Digital Signature) การใช้ตั๋ว (Ticket) ตามหลักการของเคอร์เบอร์โรส (Kerberos) ซึ่งออกโดย Authentication Server และการใช้รหัสผ่าน (Password or Pin Code) เพื่อป้องกันบุคคลภายนอกผู้ไม่มีสิทธิ์ในการจัดการอุปกรณ์ ไม่ให้เข้ามาจัดการกับอุปกรณ์เป้าหมายได้ กล่าวคือต้องมีการพิสูจน์ตัวตนของผู้ใช้ก่อน เอเจนท์ จึงจะยอมรับคำสั่งใด ๆ และดำเนินการตามคำสั่งที่ได้รับส่วนการรักษา

ความลับของข้อมูล (Confidential) ใช้เทคนิคการเข้ารหัสข้อมูล (Encryption) ด้วยอัลกอริทึม (Algorithm) ทั้ง 2 แบบโดย อัลกอริทึมแบบกุญแจสมมาตร (Symmetric Key) ใช้อัลกอริทึมแบบ AES และอัลกอริทึมแบบกุญแจอสมมาตร (Asymmetric Key) ใช้อัลกอริทึมแบบ Truncated Polynomials ที่มีความรวดเร็วมากกว่าและใช้ทรัพยากรในการเข้า / ถอดรหัสน้อยกว่า RSA นอกจากนี้ยังมีการใช้เทคนิคการลดขนาดข้อมูล (Message Digest) ในการตรวจสอบความถูกต้องของข้อมูล (Integrity Control)

3.2 คำสั่งที่ใช้ในการควบคุมอุปกรณ์และหลักการทำงาน

จากการพิจารณาคำสั่งที่ใช้ในการควบคุมอุปกรณ์ต่าง ๆ สามารถสรุปได้ว่า มีคำสั่งที่ต่างกัน 5 คำสั่ง แสดงรายละเอียดดังตารางที่ 3.1 ได้แก่

1. คำสั่งเปิดเครื่อง
2. คำสั่งปิดเครื่อง
3. คำสั่งตรวจสอบสถานะ
4. คำสั่งเปลี่ยนสถานะ
5. คำสั่งปรับค่าต่าง ๆ

คำสั่งทั้งหมดที่ใช้ควบคุมอุปกรณ์ต่าง ๆ ซึ่งการควบคุมจะเกิดจากฝั่ง Manager สามารถแบ่งเป็น 2 ประเภท ได้แก่ คำสั่งสำหรับเปลี่ยนหรือกำหนดค่า (Write/Set) ของตัวแปรที่เก็บใน MIB ของอุปกรณ์ต่าง ๆ และคำสั่งสำหรับตรวจสอบหรืออ่านค่า (Read/Get) ปัจจุบันของตัวแปร เมื่อเปรียบเทียบกับโปรโตคอล SNMP แล้วนำมาปรับปรุงเป็นโปรโตคอลเพื่อใช้สำหรับควบคุมอุปกรณ์ ซึ่งประกอบด้วยคำสั่งดังนี้

1. Get-request
2. Set-request
3. Get-response

ตารางที่ 3.1 แสดงตัวอย่างรายการอุปกรณ์และคำสั่งที่เกี่ยวข้อง

รายการอุปกรณ์	คำสั่งที่ใช้ควบคุม
หลอดไฟฟ้า	เปิด ปิด ตรวจสอบสถานะ
หม้อหุงข้าว	เปิด ปิด ตรวจสอบสถานะ เปลี่ยนสถานะ
กาต้มน้ำร้อน	เปิด ปิด ตรวจสอบสถานะ ปรับอุณหภูมิ
เตาอบไมโครเวฟ	เปิด ปิด ตรวจสอบสถานะ ปรับเลือกโหมด ปรับอุณหภูมิ
เตาไฟฟ้า	เปิด ปิด ตรวจสอบสถานะ ตรวจสอบอุณหภูมิ ปรับเปลี่ยนอุณหภุมิ
โทรทัศน์	เปิด ปิด เปลี่ยนช่อง ปรับระดับเสียง
เครื่องบันทึกรายการโทรทัศน์	เปิด ปิด เริ่มบันทึก หยุดบันทึก
เครื่องปรับอากาศ	เปิด ปิด ปรับอุณหภูมิ ปรับระดับพัดลม เลือกโหมด
พัดลม	เปิด ปิด ปรับส่ายหรือไม่ส่าย ปรับระดับแรงลม ปรับมุมก้มหรือเงย
กล้องวงจรปิด	เปิด ปิด หมุนซ้าย – ขวา ปรับมุมก้มหรือเงย

3.2.1 Get-request

ต่อไปนี้เป็นตัวอย่างข้อมูลที่ส่งจาก Manager ไปยัง เอเจนท์ ด้วยคำสั่ง Get-request

```
<SNMP>
<Header ver= ‘2.0’ comn= “public” cmd= “Get-request” reqId = ‘0’ />
<Data>
        <Object id= ‘{1 3 6 1 2 1 10 175 1 }’ />
        <Object id= ‘{1 3 6 1 2 1 10 175 2 }’ />
        <Object id= ‘{1 3 6 1 2 1 10 175 3 }’ />
</Data>
</SNMP>
```

การส่งคำสั่ง Get-request เริ่มต้นด้วย Manager จะส่งการร้องขอไปยัง เอเจนท์ โดยระบุ Version ของโปรโตคอล Community ที่ใช้ในการติดต่อ ชนิดของคำสั่ง Get-request หมายเลขการร้องขอ และระบุ ObjectID ของ Object ที่ต้องการข้อมูล

เมื่อ เอเจนท์ ได้รับการร้องขอจาก Manager ก็จะตรวจสอบข้อมูล และไปค้นหาข้อมูลจาก MIB ของอุปกรณ์ตาม ObjectID ที่ได้รับ แล้วตรวจสอบว่า Object ดังกล่าวสามารถเข้าถึงได้แบบใดตาม Max-Access ใน MIB ของอุปกรณ์หากเป็นชนิดที่ไม่สามารถอ่านได้ก็ตอบกลับเป็นข้อผิดพลาดแจ้งว่าเป็นข้อมูลที่ไม่อนุญาตให้อ่าน แต่ถ้าเป็นชนิดที่สามารอ่านได้ก็จะอ่านออกมาแล้วนำมาตอบกลับไปยัง Manager ด้วยคำสั่ง Get-response

3.2.2 Get-response

ต่อไปนี้เป็นตัวอย่างข้อมูลที่ส่งจาก เอเจนท์ ไปยัง Manager ด้วยคำสั่ง Get-response

```
<SNMP>
<Header ver= '2.0' comn= "public" cmd= "Get-response" reqId = '0' />
<Data>
  <Object id= '{1 3 6 1 2 1 10 175 1 }' code = ' 2 '>
    1297152600
  </Object >
  <Object id= '{1 3 6 1 2 1 10 175 2 }' code = '64' > 127.0.0.1 </Object >
  <Object id= '{1 3 6 1 2 1 10 175 3 }' code = '64' > 127.0.0.1 </Object >
</Data>
</SNMP>
```

คำสั่ง Get-response จะระบุ Version ของโปรโตคอล Community ที่ใช้ในการติดต่อชนิดของคำสั่ง Get-response หมายเลขการร้องขอที่ได้รับจาก Manager และระบุค่า ObjectID ชนิดของข้อมูลระบุด้วย code = ' ' สถานะความผิดพลาด ระบุด้วย err = '0' และ ค่าของ Object ที่ได้รับการร้องขอ หากไม่มีข้อผิดพลาดใด ๆ แต่ถ้าเกิดข้อผิดพลาดก็จะระบุ err = '1' และใส่รหัสของข้อผิดพลาดที่เกิดขึ้นแทนค่าของ Object

3.2.3 Set-request

ต่อไปนี้เป็นตัวอย่างข้อมูลที่ส่งจาก Manager ไปยัง เอเจนท์ ด้วยคำสั่ง Set-request

```
<SNMP>
<Header ver= '2.0' comn= "public" cmd= "Set-response" reqId = '1' />
<Data>
  <Object id= '{1 3 6 1 2 1 10 175 4 }' code = ' 2 '> 1 </Object >
  <Object id= '{1 3 6 1 2 1 10 175 5 }' code = ' 2 '> 1 </Object >
  <Object id= '{1 3 6 1 2 1 10 175 6 }' code = ' 64 '> 202.28.16.232 </Object >
</Data>
</SNMP>
```

หากต้องการแก้ไขค่าที่เอเจนท์ ฝั่ง Manager จะส่งคำสั่ง Set-request โดยจะส่งข้อมูลที่ระบุ Version ของโปรโตคอล Community ที่ใช้ในการติดต่อ ชนิดของคำสั่ง Set-request หมายเลขการร้องขอ และระบุค่า ObjectID และชนิดของข้อมูล ของ Object ที่ต้องการแก้ไขข้อมูลพร้อมระบุค่าใหม่ของ Object ที่ต้องการให้ เอเจนท์ นำไปใช้

เมื่อเอเจนท์ได้รับคำสั่ง Set-request จาก Manager ก็จะตรวจสอบข้อมูล และไปค้นหาข้อมูลจาก MIB ของอุปกรณ์ตาม ObjectId ที่ได้รับ และทำการตรวจสอบว่า Object ดังกล่าวสามารถเข้าถึงได้แบบใด ตาม Max-Access ใน MIB ของอุปกรณ์ หากเป็นชนิดที่แก้ไขได้ ก็จะทำการแก้ไขค่าตามที่ได้รับมาจาก Manager และส่งคำสั่งไปควบคุมให้อุปกรณ์ทำงานตามที่ได้รับคำสั่งมา เช่น หากได้รับคำสั่งให้หมุนขวา หลังจากแก้ไขค่าตัวแปรใน MIB แล้วก็จะสั่งงานให้ทำการหมุนขวาตามที่ได้รับการร้องขอมา จากนั้นก็จะตอบกลับไปยัง Manager ด้วยคำสั่ง Get-response เหมือนกับการตอบกลับ คำสั่ง Get-request ต่างกันตรงที่ค่าของ Object ที่ตอบกลับไปจะเป็นค่าหลังจากแก้ไขแล้ว หากเป็นชนิดที่ไม่สามารถแก้ไขได้ก็จะ ไม่ทำการแก้ไขและส่งคำสั่ง Get-request กลับไปและมีการระบุ err = '1' และใส่รหัสของข้อผิดพลาดที่เกิดขึ้นแทนค่าของ Object

3.3 การออกแบบการทำงานของระบบ

เนื่องจากการติดต่อกันระหว่าง Manager หรือผู้ใช้ (User) กับเอเจนท์หรืออุปกรณ์(Device) ในงานวิจัยนี้มุ่งเน้นไปที่การติดต่อกันแบบไร้สายผ่านเครือข่ายสาธารณะ (Wireless Network) ซึ่งมีความปลอดภัยต่ำและมีความเสี่ยงต่อการถูกโจมตีโดยผู้บุกรุกได้ง่ายจึงมีความจำเป็นอย่างยิ่งที่

จะต้องมีระบบการรักษาความปลอดภัย (Security) ที่เข้มแข็งเพียงพอ ในงานวิจัยนี้ได้นำเทคนิคและวิธีการในการรักษาความปลอดภัยต่าง ๆ มาใช้ ได้แก่ การตรวจสอบผู้ใช้หรือการยืนยันตัวบุคคล (Authentication) ด้วยวิธีการต่าง ๆ ได้แก่ การใช้ลายเซ็นอิเล็กทรอนิก (Digital Signature) การใช้ตั๋ว (Ticket) ตามหลักการของเคอร์เบอร์โรส (Kerberos) ซึ่งออกโดย Authentication Server และการใช้รหัสผ่าน (Password or Pin Code) ส่วนการรักษาความลับของข้อมูล (Confidential) ใช้เทคนิคการเข้ารหัสข้อมูล (Encryption) ด้วยอัลกอริทึม (Algorithm) ทั้ง 2 แบบโดย อัลกอริทึมแบบกุญแจสมมาตร (Symmetric Key) ใช้อัลกอริทึมแบบ AES และ อัลกอริทึมแบบกุญแจอสมมาตร (Asymmetric Key) ใช้อัลกอริทึมแบบ Truncated Polynomials ที่มีความรวดเร็วมากกว่าและใช้ทรัพยากรในการเข้า / ถอดรหัสน้อยกว่า RSA นอกจากนี้ยังมีการใช้เทคนิคการลดขนาดข้อมูล (Message Digest) ในการตรวจสอบความถูกต้องของข้อมูล (Integrity Control) เหตุที่ต้องใช้การเข้ารหัสทั้งสองแบบเนื่องจากข้อมูลที่ส่งมีทั้งกรณีที่ต้องการการระบุตัวตนของผู้เข้ารหัสและกรณีที่ต้องการเพียงรักษาความลับของข้อมูลที่ส่งเท่านั้น ในส่วนที่ต้องการการระบุตัวตนของผู้เข้ารหัส เช่นการยืนยันบุคคลและการส่งกุญแจที่จะใช้ในการสื่อสารกัน หรือกรณีลายเซ็นดิจิตอลก็จะใช้อัลกอริทึมแบบกุญแจอสมมาตร แต่ในส่วนที่ต้องการเพียงรักษาความลับของข้อมูลจะใช้อัลกอริทึมแบบกุญแจสมมาตรก็เพียงพอเนื่องจากจะใช้เวลาน้อยกว่า

โปรโตคอลที่ใช้ในงานวิจัยนี้แบ่งเป็น 3 ส่วนได้แก่ 1) โปรโตคอลสำหรับการส่งกุญแจสาธารณะให้แก่ Authentication Server และการยืนยันตัวบุคคลของ User กับ Authentication Server 2) โปรโตคอลสำหรับการร้องขอ Ticket และ กุญแจลับ (Session Key) จาก Authentication Server และการยืนยันตัวบุคคลของ User กับ เอเจนท์ 3)โปรโตคอลสำหรับการส่งและรับคำสั่งในการควบคุมอุปกรณ์ระหว่างผู้ใช้ กับ เอเจนท์

สัญลักษณ์ที่ใช้ในภาพแสดงโปรโตคอล มีรายละเอียดดังต่อไปนี้

อัลกอริทึมแบบกุญแจสมมาตร (Symmetric Keys Algorithm) ใช้ อัลกอริทึม AES

K_s หมายถึงกุญแจที่ใช้ร่วมกันระหว่าง ผู้ใช้กับ Authentication Server

K_{sess} หมายถึงกุญแจที่ใช้ร่วมกันระหว่าง ผู้ใช้กับอุปกรณ์

อัลกอริทึมแบบกุญแจอสมมาตร (Asymmetric Keys Algorithm) ใช้อัลกอริทึม Truncated Polynomials

K_P หมายถึงกุญแจสาธารณะของ Authentication Server

K_{PU} หมายถึงกุญแจสาธารณะของผู้ใช้

K_{PA} หมายถึงกุญแจสาธารณะของอุปกรณ์

K_{Pr} หมายถึงกุญแจส่วนตัวของ Authentication Server

K_{PrU} หมายถึงกุญแจส่วนตัวของผู้ใช้

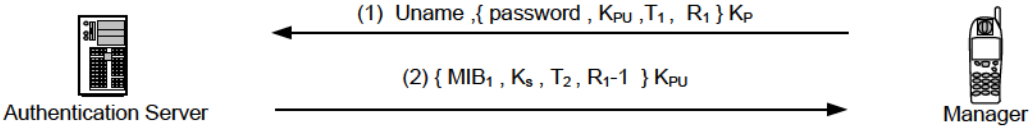
K_{PrA} หมายถึงกุญแจส่วนตัวของอุปกรณ์

Uname หมายถึงชื่อของผู้ใช้ (Username)

Aname หมายถึงชื่อของอุปกรณ์

MIB_1 หมายถึงรายชื่ออุปกรณ์ทั้งหมดที่มี

MIB_2 หมายถึงรายละเอียดของแต่ละอุปกรณ์



ภาพที่ 3.2 แสดงการส่งกุญแจสาธารณะและการยืนยันตัวบุคคลของ Manager กับ AS

3.3.1 การยืนยันบุคคลและส่งกุญแจสาธารณะ

โปรโตคอลที่ใช้สำหรับการส่งกุญแจสาธารณะให้แก่ Authentication Server และการยืนยันตัวบุคคลของ Manager หรือผู้ใช้ (User) กับ Authentication Server ใช้อัลกอริทึมแบบกุญแจอสมมาตร (Asymmetric Key Algorithm) ดังภาพที่ 3.2 มีรายละเอียดดังต่อไปนี้

3.3.1.1 User ทำการ Login ด้วย Username และ Password โปรแกรมฝั่ง Manager จะสร้างข้อมูลที่ประกอบด้วย Username Password กุญแจสาธารณะของผู้ใช้ (User's Public Key; K_{PU}) บันทึกเวลา (Time Stamp; T_1) และตัวเลขสุ่ม (Random Number; R_1) ซึ่งผ่านการเข้ารหัสด้วยกุญแจสาธารณะของ Authentication Server (K_P) ส่งไปให้แก่ Authentication Server โดยที่ใช้รหัสผ่านสำหรับการยืนยันบุคคลว่าเป็นเจ้าของพลับบลิกกุญแจแทนการใช้ใบรับรอง (Certificate)

3.3.1.2 Authentication Server ทำการถอดรหัส (Decryption) ข้อมูลที่ได้รับด้วยกุญแจส่วนตัว (Private Key; K_{Pr}) จากนั้นนำ Username ไปค้นหารหัสผ่าน (Password) ในฐานข้อมูล หากไม่พบก็จะแจ้งกลับไปว่าไม่พบ Username ดังกล่าว หากพบก็จะนำ Password ที่อ่านได้มาเปรียบเทียบกับที่ได้รับมา หากตรงกันแสดงว่าเป็นผู้ใช้ตัวจริงก็จะบันทึกกุญแจสาธารณะนั้นเข้ากับ Username ในฐานข้อมูลเพื่อใช้ในโอกาสต่อไป ขณะเดียวกันก็สร้างกุญแจลับที่ใช้ระหว่างผู้ใช้กับ AS เก็บลงฐานข้อมูลของผู้ใช้ และ สร้างข้อมูลขึ้นมาใหม่ประกอบด้วย MIB ซึ่งแสดงรายการอุปกรณ์ทั้งหมดที่สามารถควบคุมได้ กุญแจลับ บันทึกเวลา (T_2) และผลจากการแก้ไขตัวเลขสุ่ม (R_1-1) ซึ่ง

ข้อมูลเหล่านี้ต้องผ่านการเข้ารหัสด้วยกุญแจสาธารณะของผู้ใช้ (User's Public Key; K_{PU}) ก่อนส่งกลับไปยังฝั่ง Manager เพื่อแจ้งผลการตรวจสอบผู้ใช้

3.3.1.3 เมื่อฝั่ง Manager ได้รับข้อมูลที่ (2) ตามภาพที่ 3.2 จะทำการถอดรหัสด้วยกุญแจส่วนตัวของผู้ใช้ (User's Private Key; K_{PrU}) หากได้ข้อมูลที่สามารถอ่านได้และตรวจสอบ R_1-1 ว่าถูกต้องแล้วแสดงว่าการส่งกุญแจประสบความสำเร็จจากนั้นจะนำ MIB ที่ได้รับไปพิจารณาว่ามีรายการอุปกรณ์ใดบ้างอยู่ในระบบและแต่ละอุปกรณ์มีตัวแปรหมายเลขประจำตัว (OID) อะไรบ้างที่จะใช้สำหรับการติดต่อเพื่อจัดการกับอุปกรณ์แต่ละชิ้นต่อไป

จากการวิเคราะห์ด้านความปลอดภัยในขั้นตอนนี้พบว่าสามารถป้องกัน

1) การปลอมตัวเป็นผู้ใช้ด้วย Password ซึ่งต้องสอดคล้องกับ Username

2) การปลอมตัวเป็น AS ด้วยการใช้ R_1-1 ที่คำนวณจาก R_1 ที่เข้ารหัสลับด้วยกุญแจสาธารณะของ AS หากไม่สามารถถอดรหัสข้อความที่ (1) ได้ก็ไม่สามารถคำนวณ R_1-1 ได้

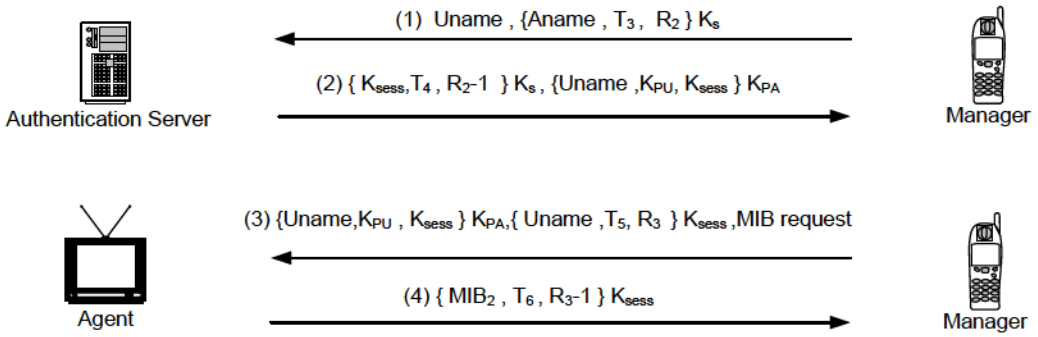
3) การโจมตีแบบคนกลาง (Man in the Middle Attack) ได้ เนื่องจากมีเพียงผู้ใช้และ AS เท่านั้นที่ทราบ Password และ Password นี้จะต้องสอดคล้องกับ Username และผู้ที่ถอดรหัสข้อความ (1) ได้คือ AS เท่านั้น ส่วนผู้ที่ถอดรหัสข้อความที่ (2) ได้คือ ผู้ใช้เท่านั้น

4) การโจมตีโดยส่งข้อความซ้ำ (Replay Attack) เนื่องจากมีการใช้การลงเวลากำกับร่วมกับ Nonce (R_x) ที่สามารถใช้ได้เฉพาะในช่วงเวลาที่ตกลงกัน เริ่มนับจากเวลาที่ส่งมากับข้อความ

3.3.2 การร้องขอตั๋วเพื่อติดต่อกับอุปกรณ์

โปรโตคอลที่ใช้ในการติดต่อระหว่าง Manager หรือผู้ใช้ (User) กับ Authentication Server (AS) เพื่อร้องขอตั๋วสำหรับติดต่อกับอุปกรณ์ (Ticket) และกุญแจที่ใช้ร่วมกับอุปกรณ์ (Session Key; K_{sess}) และการยืนยันตัวบุคคลต่อ เอเจนท์ และขอ MIB ใช้อัลกอริทึมแบบกุญแจสมมาตร ดังภาพที่ 3.3 มีรายละเอียดดังต่อไปนี้

3.3.2.1 เริ่มต้นด้วยผู้ใช้เลือกรายการอุปกรณ์ที่ต้องการจัดการทำให้ Program ฝั่ง Manager (Cell Phone) สร้างข้อมูลที่ประกอบด้วยรายชื่อของอุปกรณ์ หรือ เอเจนท์ (Aname) ที่ต้องการจัดการ ในรูปข้อความธรรมดา (Plain Text) ไปพร้อมกับข้อมูลที่ผ่านการเข้ารหัสด้วยกุญแจร่วมระหว่างผู้ใช้กับ AS (Session Key; K_s) ซึ่งข้อมูลดังกล่าวประกอบด้วย ชื่อของผู้ใช้ (Uname) บันทึกเวลา (Time Stamp; T_3) และตัวเลขสุ่ม (Random Number; R_2) ไปขอตั๋วและกุญแจที่จะใช้ร่วมกับ เอเจนท์ จาก AS



ภาพที่ 3.3 แสดงการขอตั๋วต่อ AS และการยืนยันบุคคลต่อเอเจนท์ของ Manager

3.3.2.2 Authentication Server (AS) นำรายชื่อของอุปกรณ์ไปตรวจสอบในฐานข้อมูลว่ามีอุปกรณ์ดังกล่าวหรือไม่หากไม่พบก็จะแจ้งกลับไปว่าไม่มีอุปกรณ์ที่ต้องการติดต่อ แต่หากพบอุปกรณ์ดังกล่าวก็จะถอดรหัสข้อความที่ได้รับมาจากฝั่งผู้ใช้ด้วยกุญแจลับ (K_S) แล้วฝั่ง AS ก็จะทำการสร้างกุญแจลับ ที่ใช้ร่วมกันระหว่าง ผู้ใช้กับอุปกรณ์ (Session key; K_{sess}) แล้วนำไปรวมกับ ตัวเลขสุ่มที่แก้ไขจากที่ได้รับมาจาก ผู้ใช้ (R_2-1) แล้วลงเวลา (T_4) โดยข้อมูลทั้งหมดนี้ผ่านการเข้ารหัสด้วยกุญแจลับ (K_S) ซึ่ง AS ค้นมาจากฐานข้อมูลของผู้ใช้ตามชื่อ Username จากนั้น AS ก็ทำการสร้างตั๋วสำหรับให้ผู้ใช้ติดต่อกับอุปกรณ์ (Ticket; {Uname, K_{PU} , K_{sess} }K_{PA}) ประกอบด้วย ชื่อของผู้ใช้ กุญแจสาธารณะของผู้ใช้ (K_{PU}) กุญแจลับ (K_{sess}) ตั๋วดังกล่าวนี้ผ่านการเข้ารหัสด้วยกุญแจสาธารณะของอุปกรณ์ (K_{PA}) แล้วนำข้อมูลทั้งหมดส่งไปให้ฝั่ง Manager

3.3.2.3 Manager เมื่อได้รับการตอบกลับจาก AS แล้วก็นำกุญแจลับ (K_S) มาถอดรหัสข้อมูลแล้วตรวจสอบว่าเป็นข้อมูลใหม่หรือไม่จากตัวเลขสุ่ม (R_2-1) และเวลาที่บันทึกไว้โดย AS (Time Stamp; T_5) หากไม่ใช่ข้อมูลใหม่ก็จะทิ้งไปและรอรับข้อมูลถัดไป แต่ถ้าเป็นข้อมูลใหม่ก็จะนำข้อมูลสำคัญที่ได้มาสร้างข้อมูลสำหรับติดต่อกับอุปกรณ์โดย นำชื่อของผู้ใช้ รวมกับตัวเลขสุ่ม (R_3) และบันทึกเวลา(T_5) มาเข้ารหัสด้วยกุญแจลับระหว่างผู้ใช้กับอุปกรณ์ (K_{SESS}) แล้วนำข้อมูลนี้ไปรวมกับตั๋วสำหรับติดต่อกับอุปกรณ์ และคำร้องขอ MIB แล้วส่งข้อมูลทั้งหมดนี้ไปยังอุปกรณ์

3.3.2.4 เมื่อได้รับข้อมูลจาก Manager แล้วเอเจนท์ฝั่งอุปกรณ์จะทำการถอดรหัสตั๋วเพื่อให้ได้กุญแจลับ (K_{SESS}) กุญแจสาธารณะของผู้ใช้ (K_{PU}) และชื่อผู้ใช้ (Uname) ออกมา จากนั้นก็นำกุญแจลับ (K_{SESS}) ไปถอดรหัสข้อความที่ได้รับจากผู้ใช้ แล้วตรวจสอบว่าชื่อของผู้ใช้ตรงกับในตั๋วหรือไม่ หากไม่ตรงกันก็จะปฏิเสธการร้องขอทันที หากตรงกันก็จะนำ MIB ของอุปกรณ์นั้น ๆ

ไปรวมกับตัวเลขสุ่มที่ทำการแก้ไขแล้ว (R_3-1) และบันทึกเวลา (T_6) แล้วเข้ารหัสด้วยกุญแจลับ (K_{SESS}) ก่อนที่จะส่งข้อมูลทั้งหมดไปให้ ผู้ใช้นำไปใช้งานต่อไป

จากการวิเคราะห์ด้านความปลอดภัยในขั้นตอนนี้พบว่าสามารถป้องกัน

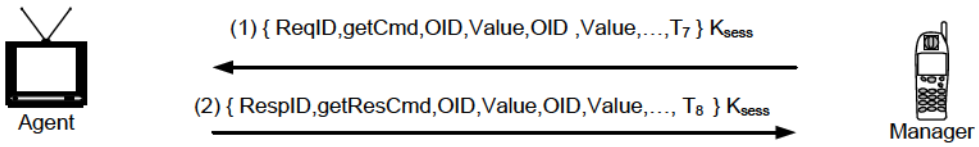
1) การปลอมตัวเป็นผู้ใช้ในขั้นตอนการร้องขอตั๋วด้วยกุญแจลับ K_s ซึ่งมีเพียงผู้ใช้และ AS เท่านั้นที่ทราบ ส่วนในขั้นตอนการร้องขอ MIB ป้องกันโดยการใช้ตั๋วที่ได้รับจาก AS

2) การปลอมตัวเป็น ASในขั้นตอนการส่งตั๋วให้ผู้ใช้ด้วยกุญแจลับ K_s ซึ่งมีเพียงผู้ใช้และ AS เท่านั้นที่ทราบ

3) การปลอมตัวเป็นอุปกรณ์โดยการเข้ารหัสตั๋วด้วยกุญแจสาธารณะของอุปกรณ์หากไม่สามารถถอดรหัสตั๋วได้ก็จะไม่สามารถสร้างข้อความที่ (4) ได้ เนื่องจากไม่ทราบ (K_{SESS}) ที่ใช้ร่วมกับผู้ใช้

4) การโจมตีแบบคนกลาง (Man in the Middle Attack) ได้ เนื่องจากมีเพียงผู้ใช้และ AS เท่านั้นที่ทราบ กุญแจลับ (K_S) และ มีเพียงผู้ใช้และอุปกรณ์เท่านั้นที่ทราบ K_{SESS} นอกจากนี้ในข้อความที่ (3) ยังมีการใช้ตั๋วในการยืนยันผู้ใช้อีกด้วย

5) การโจมตีโดยส่งข้อความซ้ำ (Replay Attack) เนื่องจากมีการใช้การลงเวลากำกับร่วมกับ Nonce ที่สามารถใช้ได้เฉพาะในช่วงเวลาที่ตกลงกันเริ่มนับจากเวลาที่ลงกำกับมากับข้อความที่ส่ง



ภาพที่ 3.4 แสดงการติดต่อส่งคำสั่งตรวจสอบสถานะระหว่าง Manager กับ เอเจนท์

3.3.3 การส่งคำสั่งตรวจสอบค่าตัวแปร

โปรโตคอลที่ใช้ในการติดต่อระหว่าง Manager หรือ ผู้ใช้ (User) กับ เอเจนท์ หรือ อุปกรณ์ เพื่อส่งคำสั่งในการตรวจสอบสถานะอุปกรณ์ (Get Request Command) ใช้อัลกอริทึมแบบกุญแจสมมาตาร ดังภาพที่ 3.4 มีรายละเอียดดังต่อไปนี้

3.3.3.1 Manager สร้างข้อมูลที่ประกอบด้วย หมายเลขการร้องขอ (Request Id; ReqID) ชนิดของคำสั่งในที่นี้คือ การร้องขอดูค่าข้อมูล (Get Request Command; GetCmd) รหัสประจำตัวของ Object (Object ID; OID) ตามด้วยค่าของ Object (Object Value) ซึ่งเป็นค่าว่าง และ

บันทึกเวลา (Time Stamp; T_7) แล้วเข้ารหัส (Encrypt) ข้อมูลทั้งหมดด้วยกุญแจลับ (Session Key; K_{SESS}) ก่อนที่จะส่งไปยังอุปกรณ์

3.3.3.2 เอเจนท์ จะทำการถอดรหัส (Decrypt) ข้อมูลที่ได้รับด้วยกุญแจลับ (K_{SESS}) แล้วตรวจสอบเวลาที่บันทึกไว้ ถ้าไม่เป็นปัจจุบันก็จะทิ้งข้อมูลนั้นไป หากเป็นเวลาปัจจุบันก็จะไปตรวจสอบ MIB ว่ามี Object ตามที่ได้รับการร้องขอมาหรือไม่หากมีก็อ่านค่าออกมาจนครบ แล้วนำไปรวมกับ หมายเลขการตอบสนอง (Response ID; RespID) ซึ่งต้องสอดคล้องกับ หมายเลขการร้องขอจาก Manager ตามด้วยชนิดของการตอบสนองในที่นี้คือ การตอบสนองต่อการร้องขออ่านค่า (Get Response Command; GetResCmd) บันทึกเวลา (Time Stamp; T_8) แล้วเข้ารหัสข้อมูลทั้งหมดด้วยกุญแจลับ (K_{SESS}) ก่อนที่จะส่งไปยัง Manager

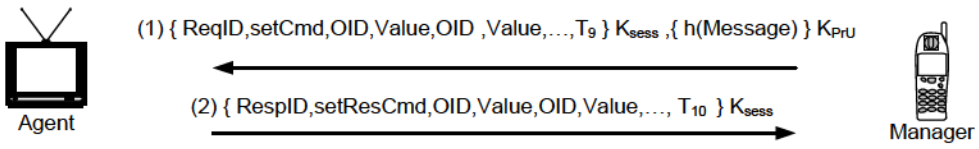
3.3.3.3 Manager จะทำการถอดรหัสข้อมูลด้วยกุญแจลับ (K_{SESS}) ตรวจสอบหมายเลขการตอบสนอง กับหมายเลขการร้องขอที่ส่งไปหากไม่ใช่การร้องขอที่เป็นปัจจุบันก็ทิ้งข้อความนั้นไป แต่หากเป็นการร้องขอที่เป็นปัจจุบันก็จะตรวจสอบเวลาที่บันทึกไว้ถ้าไม่ใช่เวลาปัจจุบันก็จะทิ้งข้อมูลนั้นไปและรอรับข้อมูลถัดไป แต่ถ้าเป็นเวลาปัจจุบันก็นำข้อมูลออกแสดงให้ผู้ใช้เห็นเพื่อดำเนินการต่อไป

จากการวิเคราะห์ด้านความปลอดภัยในขั้นตอนนี้พบว่าสามารถป้องกัน

1) การปลอมตัวเป็นผู้ใช้และอุปกรณ์ด้วยกุญแจลับ (K_{SESS}) ที่ทั้งสองฝั่งใช้ร่วมกัน

2) การโจมตีแบบคนกลาง (Man in the Middle Attack) ได้ เนื่องจากมีเพียงผู้ใช้และอุปกรณ์เท่านั้นที่ทราบ K_{SESS}

3) การโจมตีโดยส่งข้อความซ้ำ (Replay Attack) เนื่องจากมีการลงเวลากำกับหากข้อความที่ส่งมาเหมือนกันและลงเวลาซ้ำกันก็สามารถตรวจสอบได้ว่าเป็นข้อความเดียวกัน



ภาพที่ 3.5 แสดงการติดต่อส่งคำสั่งกำหนดค่าให้แก่ เอเจนท์ โดย Manager

3.3.4 การส่งคำสั่งกำหนดค่าตัวแปร

โปรโตคอลที่ใช้ในการติดต่อระหว่าง Manager หรือ ผู้ใช้ (User) กับ เอเจนท์ หรือ อุปกรณ์ เพื่อส่งคำสั่งในการกำหนดค่าให้แก่อุปกรณ์ (Set Request Command) ใช้อัลกอริทึมแบบกุญแจสมมาตรและใช้ลายเซ็นอิเล็กทรอนิคในการยืนยันตัวบุคคลและป้องกันการปฏิเสธความรับผิดชอบ ดังภาพที่ 3.5 มีรายละเอียดดังต่อไปนี้

3.3.4.1 Manager สร้างข้อมูลที่ประกอบด้วย หมายเลขการร้องขอ (Request Id; ReqID) ชนิดของคำสั่งในที่นี้คือ การร้องขอกำหนดค่าข้อมูล (Set Request Command; SetCmd) หมายเลขของ Object (Object ID; OID) ตามด้วยค่าของ Object (Value) ที่ต้องการกำหนดให้แก่ Object นั้น ๆ และบันทึกเวลา (Time Stamp; T_9) แล้วเข้ารหัส (Encrypt) ข้อมูลทั้งหมดด้วยกุญแจลับ (Session Key; K_{SESS}) ในขณะเดียวกันก็นำข้อมูลทั้งหมดไปทำการปรับลดขนาด (Message Digest; h (Message)) แล้วนำไปเข้ารหัสด้วยกุญแจส่วนตัวของผู้ใช้ (User's Private Key; K_{PrU}) เพื่อทำเป็นลายเซ็นอิเล็กทรอนิค แล้วส่งข้อมูลทั้งสองส่วนไปยังอุปกรณ์

3.3.4.2 เอเจนท์ จะทำการถอดรหัสข้อมูลด้วยกุญแจลับ (K_{SESS}) ตรวจสอบเวลาที่บันทึกไว้ถ้าไม่ใช่เวลาปัจจุบันก็จะไม่มีการตอบสนองใด ๆ แต่ถ้าเป็นเวลาปัจจุบันก็นำลายเซ็นของผู้ใช้ไปถอดรหัสด้วยกุญแจสาธารณะของผู้ใช้ซึ่งจะได้ ข้อมูลที่ถูกปรับลดขนาด (Message Digest) แล้วนำมาเปรียบเทียบกับ Message Digest ที่ได้จากการนำข้อมูลที่ได้รับไปทำ h (Message) หากไม่ตรงกันแสดงว่ามีการแก้ไขข้อมูลก็จะทิ้งข้อมูลนั้นไป หากตรงกันแสดงว่าไม่มีการแก้ไขข้อมูลก็เริ่มค้นหา Object จาก MIB และทำการแก้ไขค่าตามที่ได้รับการร้องขอมา แล้วบันทึกค่าใหม่ลงในMIB และนำค่าต่าง ๆ ที่แก้ไขแล้วไปรวมกับ หมายเลขการตอบสนอง (Response ID; RespID) ซึ่งต้องสอดคล้องกับ หมายเลขการร้องขอจาก Manager ตามด้วยชนิดของการตอบสนองในที่นี้คือ การตอบสนองต่อการร้องขอกำหนดค่า (Set Response Command; SetResCmd) บันทึกเวลา (Time Stamp; T_{10}) แล้วเข้ารหัสข้อมูลทั้งหมดด้วยกุญแจลับ (K_{SESS}) ก่อนส่งไปยัง Manager

3.3.4.3 Manager จะทำการถอดรหัสข้อมูลด้วยกุญแจลับ (K_{SESS}) ตรวจสอบหมายเลขการตอบสนอง กับหมายเลขการร้องขอที่ส่งไปหากไม่ใช่การร้องขอที่เป็นปัจจุบันก็ทิ้งข้อมูลนั้นไป แต่หากเป็นการร้องขอที่เป็นปัจจุบันก็จะตรวจสอบเวลาที่บันทึกไว้ถ้าไม่ใช่เวลาปัจจุบันก็ทิ้งข้อมูลนั้นและรอรับข้อมูลถัดไป แต่ถ้าเป็นเวลาปัจจุบัน ก็นำค่าของ แต่ละ Object แสดงออกให้ผู้ใช้ตรวจสอบว่าตรงตามที่กำหนดไปหรือไม่เพื่อดำเนินการต่อไป

จากการวิเคราะห์ด้านความปลอดภัยในขั้นตอนนี้พบว่าสามารถป้องกัน

1) การปลอมตัวเป็นผู้ใช้และอุปกรณ์ด้วยกุญแจลับ (K_{SESS}) ที่ทั้งสองฝั่งใช้ร่วมกัน

2) การโจมตีแบบคนกลาง (Man in the Middle Attack) ได้ เนื่องจากมีเพียงผู้ใช้และอุปกรณ์เท่านั้นที่ทราบ K_{SESS} นอกจากนี้ยังมีการใช้ลายเซ็นอิเล็กทรอนิกซึ่งผู้ใช้เพียงคนเดียวเท่านั้นที่สามารถเซ็นได้

3) การโจมตีโดยส่งข้อความซ้ำ (Replay Attack) เนื่องจากมีการลงเวลากำกับหากข้อความที่ส่งมาเหมือนกันและลงเวลาซ้ำกันก็สามารถตรวจสอบได้ว่าเป็นข้อความเดียวกัน

ตามหลักการ Kerberos ในการติดต่อกับแต่ละอุปกรณ์ Manager จะต้องใช้ Ticket และ Session Key ที่แตกต่างกัน แต่การติดต่อกับอุปกรณ์เดียวกันจะใช้ Ticket และ Session Key คู่เดิม นั่นคือ Manager จะทำการติดต่อกับ AS เพื่อขอ Ticket และ Session Key เพียงครั้งแรกที่ต้องการติดต่อไปยังอุปกรณ์เท่านั้นไม่ต้องขอ Ticket และ Session Key ทุกครั้งที่ต้องการส่งคำสั่งไปยังอุปกรณ์ ทำให้การติดต่อและจัดการกับอุปกรณ์ต่าง ๆ ทำได้สะดวกและรวดเร็วขึ้น หากต้องการจัดการอุปกรณ์อื่นก็จะต้องทำการร้องขอต่อ AS อีกครั้งซึ่งจะได้รับ Ticket และ Session Key คู่ใหม่สำหรับใช้ติดต่อกับอุปกรณ์ที่ต้องการจัดการ

บทที่ 4

การพัฒนาระบบควบคุมอุปกรณ์ไฟฟ้าผ่านเครือข่ายด้วยโทรศัพท์เคลื่อนที่

4.1 ข้อมูลเบื้องต้นเกี่ยวกับระบบที่ใช้ในการทดลอง

จากปัญหาความเป็นมาและแนวคิดในการวิจัยดังที่กล่าวแล้วจึงทำการทดลองพัฒนาระบบควบคุมอุปกรณ์ไฟฟ้าผ่านเครือข่ายด้วยโทรศัพท์เคลื่อนที่โดยแสดงตัวอย่างการควบคุม กล้องวงจรปิด (Camera) ซึ่งจำลองการทำงานบนเครื่องคอมพิวเตอร์ที่เชื่อมต่ออยู่ในเครือข่ายเฉพาะที่ (Local Area Network; LAN) ของผู้ใช้ด้วยโทรศัพท์เคลื่อนที่จากเครือข่ายภายนอกที่เชื่อมต่อผ่านเทคโนโลยี GPRS โดยข้อมูลสำหรับการจัดการ (MIB) ของกล้องวงจรปิดมีรายละเอียดดังนี้

```
<?xml version="1.0"?><!DOCTYPE MIB []>

<MIB VER="1" NAME="CAMERA" >
  <MODULE>CAMERA</MODULE>
  <LAST-UPDATED> 1242542759328 </LAST-UPDATED>
  <ORGANIZATION>FUJICON WORKING GROUP</ORGANIZATION>
  <OID>TRANSMISSION 155</OID>
  <OBJECT>
      <TYPE>NAME</TYPE>
      <SYNTAX>STRING</SYNTAX>
      <MAX-ACCESS>READ-ONLY</MAX-ACCESS>
      <STATUS>CURRENT</STATUS>
          <DESCRIPTION>THE VENDOR DESCRIPTION OF THE DEVICE
UNDER MANAGEMENT</DESCRIPTION>
      <OID>CAMERA 1</OID>
  </OBJECT>
```

<OBJECT>

<TYPE>RESOLUTION</TYPE>

<SYNTAX>STRING</SYNTAX>

<MAX-ACCESS>READ-ONLY</MAX-ACCESS>

<STATUS>CURRENT</STATUS>

<DESCRIPTION>THE NUMBER OF DISTINCT PIXELS IN EACH DIMENSION SUPPORTED BY THIS DEVICE</DESCRIPTION>

<OID>CAMERA 2</OID>

</OBJECT>

<OBJECT>

<TYPE>TYPE</TYPE>

<SYNTAX>STRING</SYNTAX>

<MAX-ACCESS>READ-ONLY</MAX-ACCESS>

<STATUS>CURRENT</STATUS>

<DESCRIPTION>THE TYPE OF THE CAMERA </DESCRIPTION>

<OID>CAMERA 3</OID>

</OBJECT>

<OBJECT>

<TYPE>LOCATION</TYPE>

<SYNTAX>STRING</SYNTAX>

<MAX-ACCESS>READ-WRITE</MAX-ACCESS>

<STATUS>CURRENT</STATUS>

<DESCRIPTION>THE PHYSICAL LOCATION OF THE CAMERA IN QUESTION</DESCRIPTION>

<OID>CAMERA 4</OID>

</OBJECT>

<GROUP>MONITOR<OID>CAMERA 5</OID>

<OBJECT>

<TYPE> STATUS</TYPE>

<SYNTAX>STRING</SYNTAX>

<MAX-ACCESS>READ-WRITE</MAX-ACCESS>

<STATUS>CURRENT</STATUS>

<DESCRIPTION>THE OPERATING STATUS OF THE CAMERA IN QUESTION</DESCRIPTION>

<OID>MONITOR 1</OID>

</OBJECT>

<OBJECT>

<TYPE>H-POSITION</TYPE>

<SYNTAX>STRING</SYNTAX>

<MAX-ACCESS>READ-WRITE</MAX-ACCESS>

<STATUS>CURRENT</STATUS>

<DESCRIPTION>THE HORIZENTAL POSITION OF CAMERA UNDER MANAGEMENT</DESCRIPTION>

<OID>MONITOR 2</OID>

</OBJECT>

<OBJECT>

<TYPE>V-POSITION</TYPE>

<SYNTAX>STRING</SYNTAX>

<MAX-ACCESS>READ-WRITE</MAX-ACCESS>

<STATUS>CURRENT</STATUS>

<DESCRIPTION> THE VERTICAL POSITION OF CAMERA UNDER MANAGEMENT </DESCRIPTION>

<OID>MONITOR 3</OID>

</OBJECT>

<OBJECT>

<TYPE>START-TIME</TYPE>

<SYNTAX> TimeTicks </SYNTAX>

<MAX-ACCESS>READ-WRITE</MAX-ACCESS>

<STATUS>CURRENT</STATUS>

<DESCRIPTION>THE TIME IN SECONDS SINCE JAN 1 1970 TO START THE CAMERA</DESCRIPTION>

<OID>MONITOR 4</OID>

</OBJECT>

<OBJECT>

<TYPE>LAST-START-TIME</TYPE>

<SYNTAX>TimeTicks</SYNTAX>

<MAX-ACCESS>READ-ONLY</MAX-ACCESS>

<STATUS>CURRENT</STATUS>

<DESCRIPTION>THE AMOUNT OF TIME IN TIMETICKS SINCE THE CAMERA MAKING PROCESS WAS INITIATTED</DESCRIPTION>

<OID>MONITOR 5</OID>

</OBJECT>

</GROUP>

</MIB>

MIB ข้างต้นสมมุติให้มี OID (Object Identifier) เป็น { 1 3 6 1 2 1 10 155 } หรือ Transmission 155 ชื่อ CAMERA ประกอบด้วยข้อมูลต่อไปนี้

NAME สำหรับแสดงชื่อบริษัทที่ผลิตอุปกรณ์ เป็นข้อมูลชนิด String ที่ไม่สามารถแก้ไขได้ มี OID เป็น {1 3 6 1 2 1 10 155 1} หรือ Camera 1

RESOLUTON สำหรับแสดงค่าความละเอียดในการบันทึกของอุปกรณ์เป็นข้อมูลชนิด String ที่ไม่สามารถแก้ไขค่าได้มี OID เป็น {1 3 6 1 2 1 10 155 2} หรือ Camera 2

TYPE สำหรับแสดงประเภทการใช้งานอุปกรณ์เป็นข้อมูลชนิด String ที่ไม่สามารถแก้ไขค่าได้มี OID เป็น {1 3 6 1 2 1 10 155 3} หรือ Camera 3

LOCATION สำหรับแสดงตำแหน่งที่ใช้งานอุปกรณ์ เช่น Front, Left-side, Right-side เป็นข้อมูลชนิด String ที่สามารถแก้ไขค่าได้มี OID เป็น {1 3 6 1 2 1 10 155 4} หรือ Camera 4

STATUS สำหรับแสดงสถานการณ์ทำงานปัจจุบันของอุปกรณ์ได้แก่ ON และ OFF เป็นข้อมูลชนิด String ที่สามารถแก้ไขค่าได้ อยู่ในกลุ่มย่อย ชื่อ MONITOR มี OID เป็น {1 3 6 1 2 1 10 155 5 1} หรือ Monitor 1

H-POSITION สำหรับแสดงตำแหน่งของกล้องในแนวนอนได้แก่ Left, Center และRight เป็นข้อมูลชนิด String ที่สามารถแก้ไขค่าได้ อยู่ในกลุ่มย่อย ชื่อ MONITOR มี OID เป็น {1 3 6 1 2 1 10 155 5 2} หรือ Monitor 2

V-POSITION สำหรับแสดงตำแหน่งของกล้องในแนวดิ่ง ได้แก่ Top, Center และ Bottom เป็นข้อมูลชนิด String ที่สามารถแก้ไขค่าได้ อยู่ในกลุ่มย่อย ชื่อ MONITOR มี OID เป็น {1 3 6 1 2 1 10 155 5 3} หรือ Monitor 3

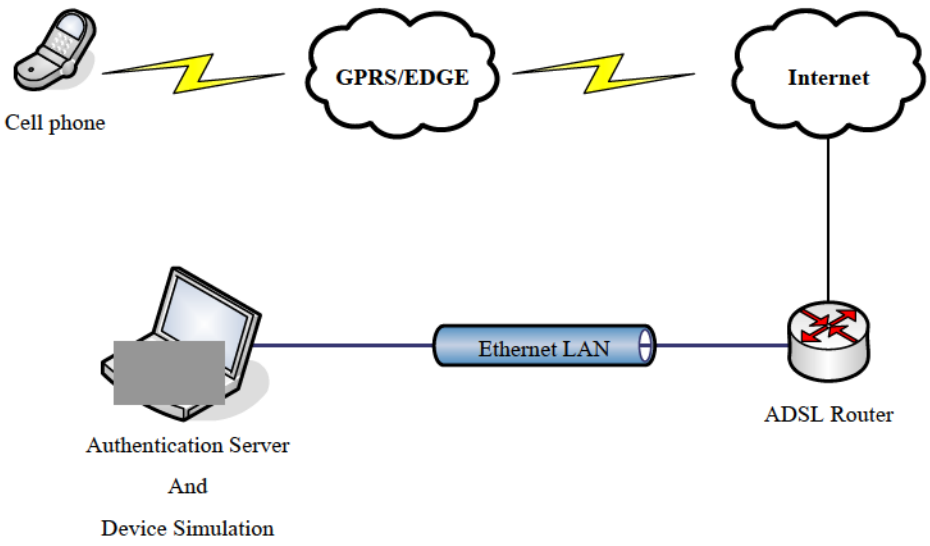
START-TIME สำหรับแสดงเวลาที่จะเริ่มใช้งานอุปกรณ์ ข้อมูลชนิด TimeTicks ที่สามารถแก้ไขค่าได้ อยู่ในกลุ่มย่อย ชื่อ MONITOR มี OID เป็น {1 3 6 1 2 1 10 155 5 4} หรือ Monitor 4

LAST-START-TIME สำหรับแสดงเวลาที่เริ่มใช้งานอุปกรณ์ครั้งล่าสุด ข้อมูลชนิด TimeTicks ที่ไม่สามารถแก้ไขค่าได้ อยู่ในกลุ่มย่อย ชื่อ MONITOR มี OID เป็น {1 3 6 1 2 1 10 155 5 5} หรือ Monitor 5

4.2 การพัฒนาโปรแกรมประยุกต์

4.2.1 โครงสร้างของระบบ

โครงสร้างของระบบแบ่งออกเป็นสามส่วนตามภาพที่ 4.1 ดังรายละเอียดต่อไปนี้



ภาพที่ 4.1 แสดงโครงสร้างของระบบ

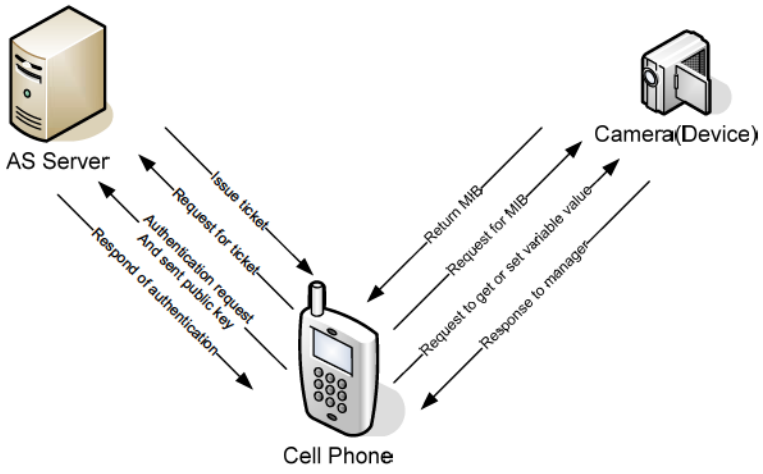
4.2.1.1 ส่วนแม่ข่ายสำหรับการตรวจสอบบุคคลและแจกตั๋วสำหรับใช้ติดต่อกับอุปกรณ์ ทำหน้าที่ในการตรวจสอบผู้ใช้จากชื่อและรหัสผ่านเมื่อผู้ใช้ล็อกอินเข้าสู่ระบบ และทำการแจกตั๋วเมื่อได้รับการร้องขอจากผู้ใช้ที่ผ่านการตรวจสอบบุคคลแล้ว

4.2.1.2 ส่วนโปรแกรมประยุกต์บนโทรศัพท์เคลื่อนที่ทำหน้าที่รับข้อมูลจากผู้ใช้นำมาประมวลผลและส่งต่อข้อมูลไปยังแม่ข่ายต่าง ๆ ภายในระบบและในทางกลับกันก็ทำหน้าที่ในการรับข้อมูลจากแม่ข่ายต่าง ๆ มาแสดงต่อผู้ใช้เพื่อนำเนินการอย่างใดอย่างหนึ่งต่อไป

4.2.1.3 ส่วนโปรแกรมประยุกต์แม่ข่ายบนอุปกรณ์ทำหน้าที่ในการตอบสนองต่อคำสั่งจากผู้ใช้ที่ส่งมาจากโทรศัพท์เคลื่อนที่หลังจากประมวลผลตามที่ได้รับการร้องขอมา

4.2.1.4 อุปกรณ์ควบคุมที่ใช้ในการทดลองคือ โทรศัพท์เคลื่อนที่ NOKIA 3110 C ระบบปฏิบัติการ NOKIA OS เชื่อมต่อเครือข่ายด้วย EDGE/GPRS ความเร็ว 236.8 Kbps ส่วน AS และอุปกรณ์ที่ต้องการควบคุม ใช้เครื่อง Notebook PC ASUS ระบบปฏิบัติการ Windows XP Professional Version 2002 หน่วยประมวลผล Intel Pentium ® M Processor 1.73 GHz

4.2.2 การทำงานของระบบ



ภาพที่ 4.2 แสดงภาพรวมการทำงานของระบบ

โปรแกรมประยุกต์ที่ใช้ในงานวิจัยนี้โดยรวมดังภาพที่ 4.2 มีรายละเอียดดังต่อไปนี้

เมื่อผู้ใช้ต้องการจัดการอุปกรณ์ก็จะเปิดโปรแกรมที่ติดตั้งบนโทรศัพท์เคลื่อนที่เพื่อล็อกอินเข้าสู่ระบบและเริ่มการติดต่อไปยัง แม่ข่ายให้บริการตรวจสอบยืนยันบุคคล (Authentication

Server; AS) โดยป้อน ชื่อ (Username) และ รหัสผ่าน (Password) ดังภาพที่ 4.3 และภาพที่ 4.4 แสดงตัวอย่างข้อความที่ฝั่ง AS ได้รับ

โปรแกรมบนโทรศัพท์จะสร้างการติดต่อและส่งข้อมูลในการตรวจสอบยืนยันบุคคลและกุญแจสาธารณะของผู้ใช้ให้แก่แม่ข่าย AS ซึ่งข้อมูลจะอยู่ในรูปแบบ XML ดังนี้

<Uname>Username</Uname>

<NTRU>-288x-576x864x-288x-576x864x</NTRU>

<NTRU>-132x-219x904x-288x-226x302x</NTRU>

…

…

…

<NTRU>-182x-467x959x-182x-455x972x</NTRU>

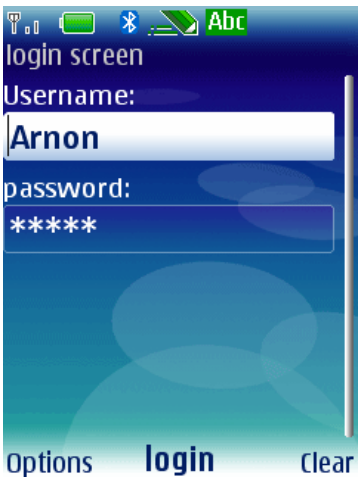
ซึ่งข้อมูลในแท็ก <NTRU> ถูกเข้ารหัสด้วยกุญแจสาธารณะของแม่ข่าย AS ประกอบด้วย

<Pass>99999</Pass>

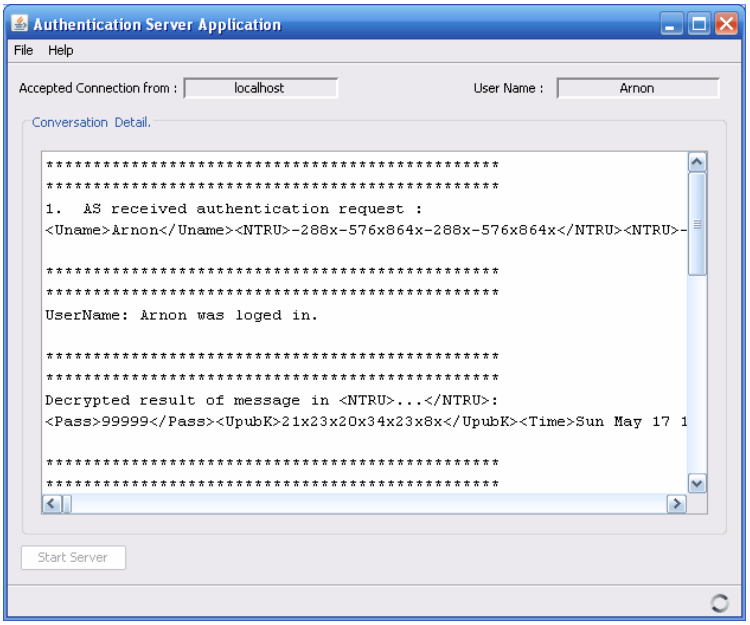
<UpubK>21x23x20x34x23x8x</UpubK>

<Time>Sat May 16 17:37:00 UTC 2009 </Time>

<Ran>88060510</Ran>



ภาพที่ 4.3 แสดงหน้าจอการ Login



ภาพที่ 4.4 แสดงข้อมูลที่ฝั่ง AS ได้รับ

ฝั่งแม่ข่ายAS จะตอบกลับด้วยข้อความที่เข้ารหัสด้วยกุญแจสาธารณะของผู้ใช้ ซึ่งข้อมูลจะอยู่ในรูปแบบ XML ดังนี้

<NTRU>-202x-501x936x-190x-476x949x</NTRU>

<NTRU>272x-235x566x-786x-977x128x</NTRU>

…

…

…

<NTRU>-223x-376x215x-567x-762x178x</NTRU>

ซึ่งข้อมูลในแท็ก <NTRU> ถูกเข้ารหัสด้วยกุญแจสาธารณะของผู้ใช้ประกอบด้วย

<MIB>Camera</MIB><Ks>11111…10110<Ks>

<Time>Sun May 17 00:37:02 ICT 2009</Time>

<Ran-1>88060510</Ran-1>

เมื่อได้รับการตอบกลับว่าผ่านการยืนยันบุคคลแล้วมาพร้อมกับรายชื่ออุปกรณ์ในระบบ โปรแกรมจะนำรายการอุปกรณ์แสดงออกหน้าจอเพื่อให้ผู้ใช้เลือกอุปกรณ์ที่ต้องการจัดการในที่นี้มีเพียงอุปกรณ์เดียวคือ กล้องวงจรปิด (Camera) ดังภาพที่ 4.5

ภาพที่ 4.5 แสดงรายการอุปกรณ์ที่มีอยู่ในระบบ

เมื่อผู้ใช้เลือกอุปกรณ์แล้วโปรแกรมจะส่งคำขอตั๋ว (Ticket) สำหรับติดต่อกับอุปกรณ์ไปยัง TGS ซึ่งข้อมูลจะอยู่ในรูปแบบ XML ดังนี้

<Uname>Arnon</Uname>

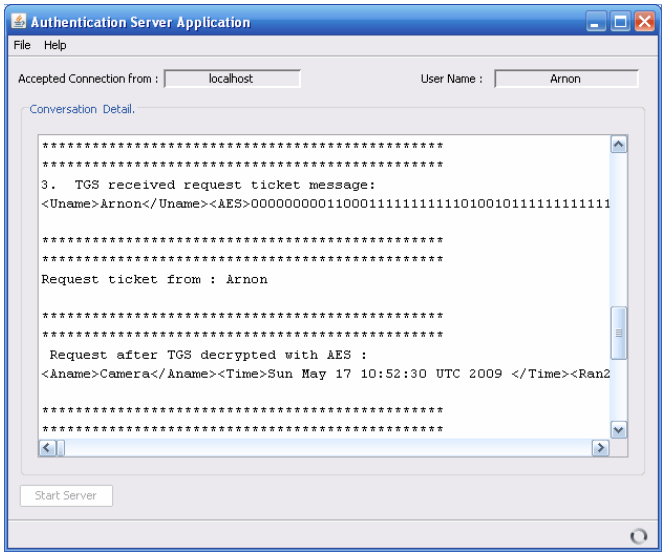
<AES>111111… 100110</AES>

ซึ่งข้อมูลในแท็ก <AES> ที่ TGS ได้รับดังภาพที่ 4.6 ถูกเข้ารหัสด้วยกุญแจร่วมที่ใช้กับแม่ข่าย AS ประกอบด้วย

<Aname>Camera</Aname>

<Time>Sat May 16 17:37:00 UTC 2009 </Time>

<Ran2>88060510</Ran2>



ภาพที่ 4.6 แสดงหน้าจอ TGS เมื่อได้รับการร้องขอตั๋ว

เมื่อTGS ได้รับการร้องขอตั๋วจะตอบกลับด้วยข้อความสองส่วนดังนี้

<AES>110100…001110</AES>

<Ticket>

<NTRU>-288x-576x864x-288x-576x864x</NTRU>

<NTRU>128x-436x445x-328x-366x256x</NTRU>

…

…

…

<NTRU>-182x-467x959x-182x-455x972x</NTRU>

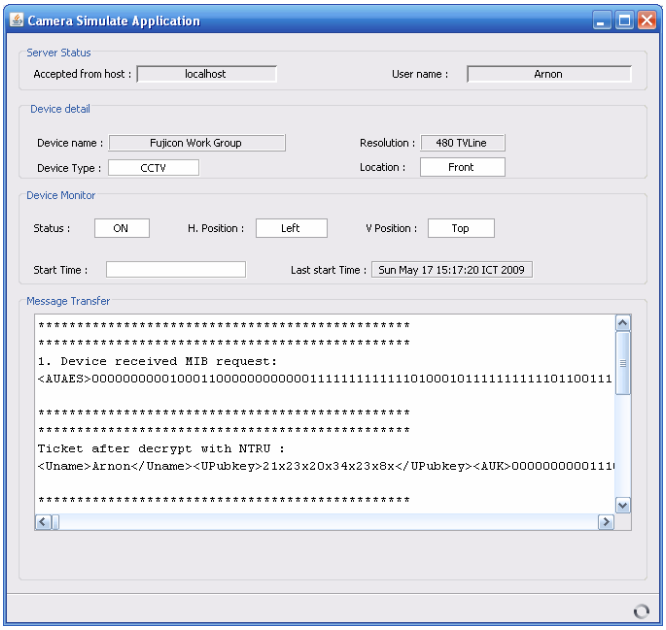
</Ticket>

ข้อมูลในแท็ก <AES> ถูกเข้ารหัสด้วยกุญแจร่วมระหว่าง TGS กับ ผู้ใช้อยู่ในรูป XML ดังนี้

<AUK>0000…11011</AUK>

<Time>Sun May 17 01:01:39 ICT 2009</Time>

<Ran2-1>88060510</Ran2-1>



ภาพที่ 4.7 แสดงตัวอย่างหน้าจออุปกรณ์เมื่อได้รับการร้องขอ MIB

เมื่อได้รับตั๋วและกุญแจร่วมที่ใช้ร่วมกับอุปกรณ์แล้ว โปรแกรมก็จะปิดการเชื่อมต่อกับ AS และสร้างการติดต่อไปยังอุปกรณ์โดยมีตั๋วส่งไปเพื่อยืนยันว่าเป็นตัวจริง ดังภาพที่ 4.7 ซึ่งข้อมูล จะอยู่ในรูปแบบ XML ดังนี้

<AUAES>00000…10011</AUAES>

<NTRU>-288x-576x864x-288x-576x864x</NTRU>

<NTRU>128x-436x445x-328x-366x256x</NTRU>

…

…

…

<NTRU>-182x-467x959x-182x-455x972x</NTRU>

ซึ่งข้อมูลในแท็ก <NTRU> ถูกเข้ารหัสด้วยกุญแจสาธารณะของอุปกรณ์ ประกอบด้วย

<Uname>Arnon</Uname>

<UPubkey>21x23x20x34x23x8x</UPubkey>

<AUK>000000…01110</AUK>

และข้อมูลในแท็ก <AUAES> ถูกเข้ารหัสด้วยกุญแจร่วมที่ใช้กับอุปกรณ์ ประกอบด้วย

<Uname>Arnon</Uname>

<Ran>827913287</Ran>

<Time>Sun May 17 08:18:43 UTC 2009</Time>

ซึ่งเมื่อผ่านขั้นตอนนี้อุปกรณ์จะส่ง MIB มาให้ ดังรายละเอียดต่อไปนี้

<AUAES>00000... 011101</AUAES>

รายละเอียดในแท็ก <AUAES> ที่ส่งกลับมายังผู้ใช้มีดังนี้

<Name>DEVICENAME</Name>

<OID>cam1</OID><ACC>Read only</ACC>

…

…

…

<Name>LAST-START-TIME</Name>

<OID>mon5</OID><ACC>Read only</ACC>

โปรแกรมจะนำรายการตัวแปรใน MIB แสดงออกหน้าจอให้ผู้ใช้เลือกจัดการดังภาพที่ 4.8

เมื่อผู้ใช้เลือกตัวแปรที่ต้องการจัดการแล้วหากเลือกคำสั่งขอดูค่าตัวแปรโปรแกรมบนโทรศัพท์จะส่งข้อมูลไปยังอุปกรณ์ดังนี้

<AES>000111…00011</AES>

ข้อมูลข้างต้นเข้ารหัสด้วยกุญแจร่วมที่ใช้กับอุปกรณ์ซึ่งมีรายละเอียดดังนี้

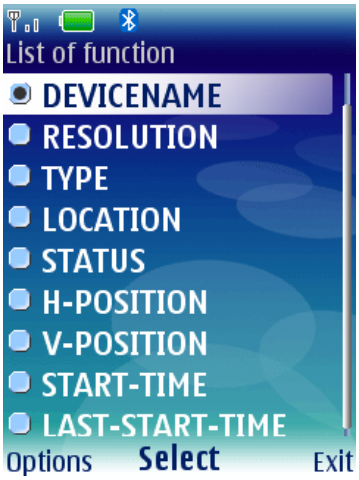
<OID>cam1</OID>

เมื่อข้อมูลส่งถึงอุปกรณ์ดังภาพที่ 4.9 โปรแกรมที่ทำงานบนอุปกรณ์จะทำการอ่านค่าตัวแปรดังกล่าวแล้วตอบกลับด้วยข้อมูล

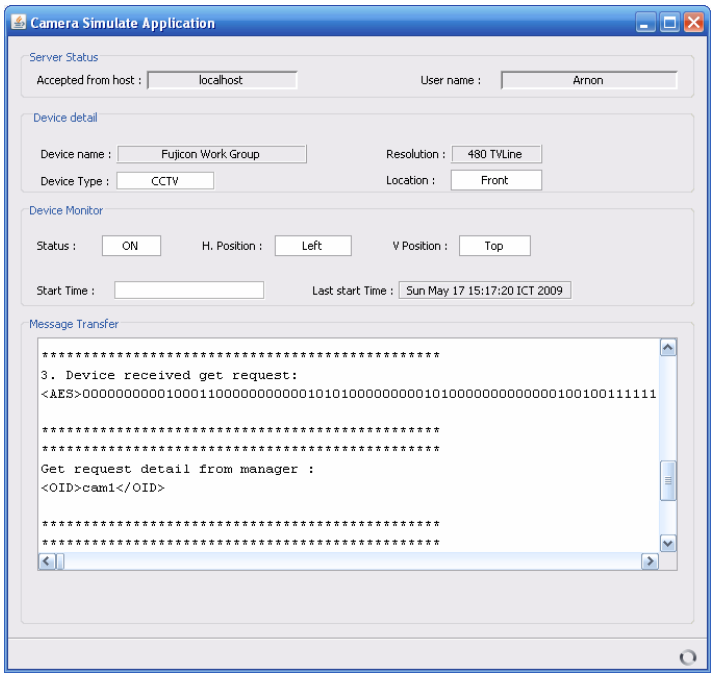
<OID>cam1</OID><VAL>Fujicon Work Group</VAL>

ข้อมูลข้างต้นเข้ารหัสด้วยกุญแจร่วมอันเดียวกันกับฝั่งผู้ใช้ดังนี้

<AES>0000000…00010</AES>



ภาพที่ 4.8 แสดงรายการตัวแปรของอุปกรณ์ที่เลือก



ภาพที่ 4.9 แสดงข้อความร้องขอดูค่าข้อมูลที่ได้รับจากผู้ใช้

ภาพที่ 4.10 แสดงสถานะอุปกรณ์ที่ได้รับหลังจากส่งคำสั่งขอดูค่าตัวแปร

ข้อมูลที่ได้รับจะถูกนำออกแสดงที่หน้าจอโทรศัพท์ดังภาพที่ 4.10 หากเป็นคำสั่งกำหนดค่าตัวแปรจะต้องมีการส่งลายเซ็นกำกับไปด้วยตามภาพที่ 4.11 ซึ่งมีรายละเอียดดังต่อไปนี้

<AES>00000000…111100</AES>

<NTRU>-288x-576x864x-288x-576x864x</NTRU>

<NTRU>184x-256x-204x-328x-421x112x</NTRU>

…

…

…

<NTRU>-182x-467x959x-182x-455x972x</NTRU>

รายละเอียด ใน <AES>ประกอบด้วย

<OID>cam4</OID><VAL>Back</VAL>

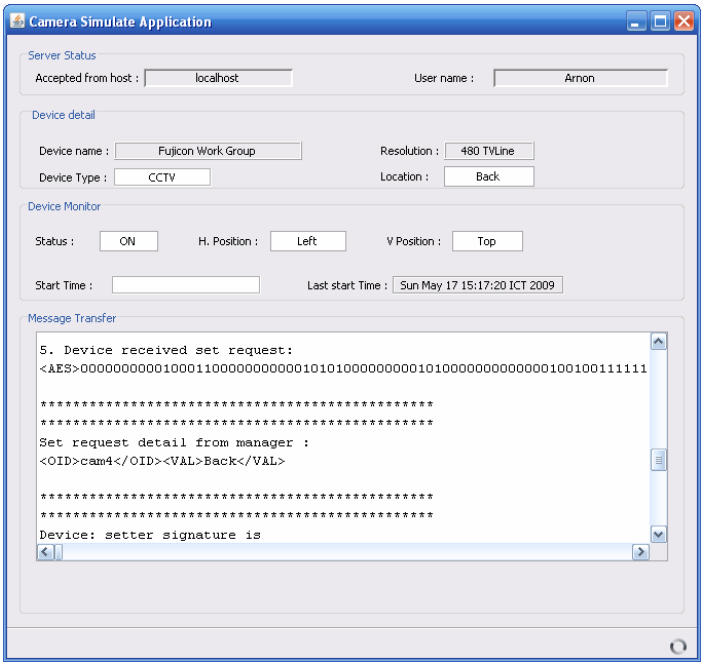
และในแท็ก<NTRU>เป็นลายเซ็นซึ่งสร้างจากการย่อยข่าวสาร(Message Digest) ซึ่งเมื่อถอดรหัสลับข้อมูลแล้วจะได้ข้อความดังเช่น x0vaNRwG3kzieg1K7Abrzd6p/FM=

หลังจากตรวจสอบลายเซ็นเป็นที่เรียบร้อยอุปกรณ์จะทำการเปลี่ยนค่าตัวแปรตามที่ได้รับการร้องขอและส่งผลจากการทำงานกลับไปแสดงที่หน้าจอโทรศัพท์ดังภาพที่ 4.12 ดังนี้

<OID>cam4</OID><VAL>Back</VAL>

ข้อมูลดังกล่าวถูกเข้ารหัสด้วยกุญแจร่วมได้ข้อความดังนี้

<AES>00001100…111100</AES>



ภาพที่ 4.11 แสดงข้อความร้องขอให้กำหนดค่าตัวแปร

ภาพที่ 4.12 แสดงหน้าจอการกำหนดค่าให้แก่ตัวแปรของอุปกรณ์

ข้อมูลที่สื่อสารระหว่างโทรศัพท์เคลื่อนที่กับ AS และอุปกรณ์จะอยู่ในรูป XML ดังตัวอย่างข้างต้นเพื่อสะดวกในการนำไปใช้ในการจัดการ

ข้อมูลในแท็ก <AES> <AUAES> และ <AUK> ถูกเข้ารหัสด้วยกุญแจร่วมที่ใช้กับอุปกรณ์

ข้อมูลในแท็ก <NTRU> เป็นข้อมูลที่ถูกเข้ารหัสด้วยกุญแจสาธารณะในกรณีส่งข้อความธรรมดาส่วนในกรณีลายเซ็นดิจิตอลจะเข้ารหัสด้วยกุญแจส่วนตัวของผู้ใช้และจะต้องทำการย่อยข่าวสารก่อน

ข้อมูลระหว่างโทรศัพท์เคลื่อนที่กับ AS มีการเข้ารหัสข้อมูล ด้วยหลักการ Truncated Polynomials และ AES

ข้อมูลระหว่างโทรศัพท์เคลื่อนที่กับอุปกรณ์มีการเข้ารหัสด้วยหลักการ AES และการเซ็นด้วยลายเซ็นดิจิตอลด้วยหลักการ Truncated Polynomials

ระบบที่ใช้ในการทดลองมีการเก็บกุญแจส่วนตัวไว้ในเครื่องโทรศัพท์เพื่อสะดวกในการทดลอง แต่สำหรับการประยุกต์ใช้งานจริงนั้นจะต้องทำการสร้างกุญแจส่วนตัวและกุญแจสาธารณะขึ้นเองก่อนเริ่มใช้งานระบบ และอาจให้ผู้ใช้ป้อนค่ากุญแจส่วนตัวเข้าสู่โปรแกรมประยุกต์เอง

บทที่ 5

สรุปผลการวิจัยและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

ในงานวิจัยนี้ได้เสนอแนวคิดในการจัดการควบคุมอุปกรณ์ ผ่านระบบเครือข่ายอินเทอร์เน็ต (Internet) ด้วยโทรศัพท์เคลื่อนที่โดยตรงไปยังอุปกรณ์ที่มีความสามารถในการประมวลผลที่เพียงพอโดยไม่ต้องผ่านแม่ข่ายให้บริการ (Server) เป็นการช่วยลดจำนวนโหนดในการติดต่อและมีการนำเทคโนโลยี XML ซึ่งช่วยให้การสื่อสารข้อมูลระหว่างผู้ใช้และอุปกรณ์ทำได้สะดวกและมีประสิทธิภาพ นอกจากนั้นยังมีการนำ SNMP ซึ่งเป็นโปรโตคอลที่ใช้ในการจัดการเครือข่ายอยู่แล้วมาใช้เป็นโปรโตคอลหลักในการสื่อสารระหว่างโทรศัพท์เคลื่อนที่กับแม่ข่ายต่าง ๆ ในงานวิจัยนี้ยังได้เสนอวิธีการรักษาความมั่นคงของระบบซึ่งนำหลักการของกุญแจอสมมาตรคือ Truncated Polynomials ที่มีประสิทธิภาพสูงและใช้ทรัพยากรไม่มาก สามารถใช้งานได้ดีในโทรศัพท์เคลื่อนที่มาประยุกต์ใช้ในการยืนยันบุคคล ลายเซ็นอิเล็กทรอนิกและตรวจสอบสิทธิ์ในการจัดการควบคุมอุปกรณ์รวมถึงการดำรงไว้ซึ่งความมั่นคงของข้อมูลที่ใช้ในการติดต่อสื่อสาร

จากการทดลองพบว่า ตามหลักการ Truncated Polynomials การเข้ารหัสลับใช้เวลาเฉลี่ย 1. 24 วินาที สำหรับข้อมูล 110 ไบท์ ส่วนการถอดรหัสลับใช้เวลาเฉลี่ย 19.36 วินาทีสำหรับข้อมูล 4223 ไบท์ ซึ่งอัตราการเข้ารหัสลับ และถอดรหัสลับดังกล่าวแสดงให้เห็นว่าสามารถนำหลักการ Truncated Polynomials มาประยุกต์ใช้ได้จริงบนโทรศัพท์เคลื่อนที่

การตอบสนองที่ได้รับหลังจากส่งข้อมูลต่าง ๆ ใช้เวลาประมาณ 18 – 28 วินาทีสำหรับข้อมูลที่เข้ารหัสแบบกุญแจอสมมาตรสำหรับข้อมูล 10280 - 12423 ไบท์ ส่วนในการเข้ารหัสลับข้อมูลที่ส่งระหว่างโทรศัพท์เคลื่อนที่กับอุปกรณ์ที่ต้องการควบคุมใช้การเข้ารหัสแบบ AES ซึ่งเป็นอัลกอริทึมแบบกุญแจสมมาตร ในการทดลองโดยใช้ AES ปรากฏว่าใช้เวลาประมาณ 2-4 วินาทีสำหรับข้อมูล 250 - 720 ไบท์ ซึ่งอัตราการตอบสนองในการเข้ารหัสลับข้อมูลดังกล่าวแสดงให้เห็นว่าสามารถใช้งานได้กับโทรศัพท์เคลื่อนที่ในปัจจุบัน ประกอบกับโทรศัพท์ที่ใช้ในการทดลองเป็นรุ่นที่ความสามารถปานกลางหากใช้รุ่นที่มีความสามารถสูงกว่านี้จะทำให้อัตราการตอบสนองเพิ่มขึ้น และเป็นที่แน่นอนว่าในอนาคตหากมีการนำหลักการตามงานวิจัยนี้ไปใช้ทดสอบกับ

โทรศัพท์เคลื่อนที่ที่มีการพัฒนาอย่างต่อเนื่องจนมีความสามารถสูงกว่านี้หลายเท่าก็จะทำให้อัตราการตอบสนองสูงกว่านี้หลายเท่าเช่นกัน

ในงานวิจัยนี้ยังได้นำเสนอโปรโตคอลที่ใช้ในการควบคุมการจัดการเครือข่ายที่มีความมั่นคงของระบบสูงอีกทั้งยังได้เสนอการใช้กุญแจอสมมาตรโดยไม่ต้องใช้ใบรับรอง (Certificate) จากหน่วยงานรับรองกุญแจ (Certificate Authority)

5.2 ข้อเสนอแนะ

5.2.1 หากใช้โทรศัพท์เคลื่อนที่ที่มีศักยภาพสูง ซึ่งในอนาคตจะมีราคาที่ถูกลง จะสามารถทำงานได้เร็วขึ้น

5.2.2 ในการเข้ารหัสลับของข้อมูลด้วยหลักการของพหุนาม (Truncated Polynomials) ในการทดลองนี้ใช้กุญแจที่มีจำนวนพจน์ของพหุนามเท่ากับ 6 พจน์ (N=6) หากต้องการความมั่นคงของระบบเพิ่มขึ้นควรใช้กุญแจที่ยาวขึ้น

5.2.3 การส่งข้อมูลที่มีการเข้ารหัสแบบกุญแจสมมาตรในการทดลองนี้มีการแปลงข้อมูลเป็นไบนารี่ก่อนส่งซึ่งทำให้ปริมาณข้อมูลเพิ่มจากข้อมูลจริงจึงควรพัฒนาวิธีการส่งข้อมูลโดยไม่ต้องแปลงข้อมูลก่อนเพื่อเป็นการลดปริมาณข้อมูลที่ส่งในเครือข่าย

5.2.4 เนื่องจากงานวิจัยนี้เป็นการเสนอแนวคิดในอนาคตว่าจะมีการผลิตอุปกรณ์ที่มีหน่วยประมวลผลติดมาด้วยแต่ในการทดลองได้จำลองการทำงานของอุปกรณ์ที่ต้องการควบคุมด้วยเครื่องคอมพิวเตอร์เครื่องหนึ่ง

5.2.5 การควบคุมอุปกรณ์ในงานวิจัยนี้ทำการศึกษาการส่งข้อมูลที่เป็นข้อความในเบื้องต้นหากต้องการให้ระบบมีความสามารถมากขึ้นควรมีการพัฒนาให้สามารถส่งข้อมูลชนิดอื่น ๆ เช่น ภาพนิ่ง เสียง หรือ ภาพเคลื่อนไหวได้ด้วย

บรรณานุกรม

ประการ ผู้วิบูลย์สุข. 2546. **การประยุกต์ใช้ XML บนโปรโตคอล SNMP**. วิทยานิพนธ์ปริญญามหาบัณฑิต สถาบันบัณฑิตพัฒนบริหารศาสตร์.

สัลยุทธ์ สว่างวรรณ. 2547. **เครือข่ายคอมพิวเตอร์.** กรุงเทพมหานคร: ซีเอ็ดยูเคชั่น.

Al-Ali, A. R. and Al-Rousan. M. 2004. Java-Based Home Automation System. **IEEE Transactions on Consumer Electronics.** 50(May): 498-504.

Cisco System. 1992-2009. **Simple Network Management Protocol (SNMP)**. Retrieved April 19, 2009 from http://www.cisco.com/en/US/docs/internetworking/technology/handbook/SNMP.html.

Forouzan, Behrouz A. 2007. **Data Communications and Networking**. New York: McGraw-Hill Higher Education.

Forum nokia. 2007. **Device Details – Nokia 3110 Classic**. Retrieved October 19, 2007 from http://www.forum.nokia.com/devices/3110_classic.

Hoffstien, Jeffrey; Pipher, Jill and Silverman, Joseph H. 1998. **NSS: The NTRU Signature Scheme.** Retrieved May 25, 2009 from http://www.ntru.com/cryptolab/pdf/nss.pdf.

Itala, Markus; Tieranta, Tomi and Vanhala, Jukka. 2003. **Context Aware User Interface System for Smart Home Control**. Retrieved May 25, 2009 from. http://www.crito.uci.edu/noah/hoit/hoit%20papers/context%20aware%20user%20interface.pdf.

Itani, Wassim and Ayman I. 2003. J2me End-to-End Security for M-Commerce. **Wireless Communications and Networking.** 28(May): 2015-2020.

Koskela, Tiiu and Väänänen-Vainio- Mattila, Kaisa. 2004. Evolution Towards Smart Home Environments: Empirical Evaluation of Three User Interfaces. **Personal and Ubiquitous Computing.** 8(June): 234-240.

Lin, Chi-Chia and Chen, Ming-Syan. 2005. On Controlling TV SET-Top-Box by Mobile Devices via IP Network. **Proceedings of the Seventh IEEE International Symposium on Multimedia**. 8(December): 52-59.

Mir, Nader F. 2007. **Computer and Communication Networks**. Upper Saddle River, NJ: Pearson Hall.

NTRU Cryptosystems. 1998. **Cryptolab Tutorials**. Retrieved January 18, 2008 from http://www.ntru.com/cryptolab/tutorials.htm.

Prapoorna, Roja P. and Avadhani, P. S. 2007. Digital Signature Development Using Truncated Polynomials. **International Journal of Computer Science and Network Security.** 7(July): 130 – 133.

Sanguinetti, Alexandre; Haga, Hirohide; Funakoshi, Aya; Yoshida, Atsushi and Matsumoto Chiho. 2003. FreCon: a Fluid Remote Controller for a Freely Connected World in a Ubiquitous Environment. **Personal and Ubiquitous Computing.** 7(July): 163-168.

Tanenbaum. 1996. **Computer Networks.** Upper Saddle River, NJ: Prentice-Hall.

Wikipedia. 2007. **General Packet Radio Service**. Retrieved May 25, 2009 from http://en.wikipedia.org.

ประวัติผู้เขียน

ชื่อ-นามสกุล	อานนท์ ผ่องรัศมีเพ็ญ
ประวัติการศึกษา	การศึกษาบัณฑิต (วิทยาศาสตร์-ฟิสิกส์) มหาวิทยาลัยศรีนครินทรวิโรฒ ประสานมิตร พ.ศ. 2539
ตำแหน่งและสถานที่ทำงานปัจจุบัน	อาจารย์พิเศษ แผนกคณิตศาสตร์-วิทยาศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก วิทยาเขตจักรพงษภูวนารถ