KKU Engineering Journal

http://www.en.kku.ac.th/enjournal/th/

การพัฒนาโปรแกรมผ่านโทรศัพท์เคลื่อนที่ในการรักษาความปลอดภัยรถยนต์

Mobile application for automobile security system

อิทธิพล สวยสม และ สุวรรณี อัศวกุลชัย*

Ittipon Suaysom and Suwannee Adsavakulchai*

สาขาวิชาวิศวกรรมคอมพิวเตอร์และมัลติมีเดีย คณะวิศวกรรมศาสตร์ มหาวิทยาลัยหอการค้าไทย จังหวัดกรุงเทพมหานคร 10400

Department of Computer Engineering and Multimedia, School of Engineering University of the Thai Chamber of Commerce,Bangkok, 10400

Received October 2012

Accepted April 2013

บทคัดย่อ

การพัฒนาโปรแกรมผ่านโทรศัพท์เคลื่อนที่ในการรักษาความปลอดภัยรถยนต์ผ่านบลูทูธ โดยเริ่มจากการออกแบบระบบฝังตัวโดยใช้ไมโครคอนโทรเลอร์ (ET-BASEPIC18F 8722 (ICD2)) ติดตั้งในรถยนต์ และพัฒนาโปรแกรม Python Paraniwin และ MPlab เชื่อมโยงทุกระบบ เมื่อต้องการปลดล็อคโดยใช้โทรศัพท์เคลื่อนที่ ระบบจะทำการเชื่อมต่อบลูทูธภายในระบบฝังตัว เพื่อเป็นการพิสูจน์ตัวตนเจ้าของรถยนต์ด้วยรหัสผ่าน ซึ่งเป็นระบบรักษาความปลอดภัย นอกจากนี้ระบบยังเพิ่มการแจ้งเตือนโดยการส่งข้อความเตือน SMS ไปยังโทรศัพท์เคลื่อนที่ เมื่อเซ็นเซอร์ที่ติดตั้งไว้ในรถยนต์ถูกรบกวน เพื่อให้เจ้าของรถยนต์สามารถโดยอัตโนมัติ จากผลการศึกษาการทำงานของระบบล็อคสามารถใช้งานทำงานได้ดีในพื้นที่โล่งระยะทาง 12 เมตร สำหรับระยะเวลาในการส่ง SMS ตั้งแต่เซ็นเซอร์ตรวจจับสิ่งผิดปกติได้จนกระทั่งได้รับข้อความใช้เวลาประมาณ 5 วินาที และเซ็นเซอร์ไม่ทำการตรวจจับการกระทำที่อยู่นอกห้องผู้โดยสาร สรุปผลการศึกษาแสดงให้เห็นว่าระบบรักษาความปลอดภัยรถยนต์ผ่านโทรศัพท์ เคลื่อนที่ทำงานได้อย่างมีประสิทธิภาพ ใช้งานง่าย และต้นทุนต่ำ

คำสำคัญ : ระบบรักษาความปลอดภัยรถยนต์ โทรศัพท์เคลื่อนที่ บลูทูธ ET-BASE PIC18F8722 (ICD2) Python Paraniwin และ MPlab

Abstract

This paper presents the application of the mobile phone as a remote control for motor vehicle to open-close the door. This security system uses a wireless network to receive the information and transmits it to the motor vehicle. A user uses a communication device, such as a Bluetooth (ESD200) in mobile phone, to send instructions to the wireless network. The research idea focuses on the users into authorized ones by

* Corresponding author.

Email address: ensak@hotmail.com

simulation. Firstly, to develop the embedded system into a security system is to identify the authorized drivers in response to the real time. A microcontroller (ET-BASE PIC18F8722 (ICD2)) is installed in the car for transmitter Bluetooth in mobile phone using Python, Paraniwin and MPlab program to interface that is complete and showing on the mobile phone screen that is available. Finally, the experimental results verify that the proposed method is valid and useful against the vehicle thefts problem with a success rate of 100% within surrounding distance12 meters within 5 seconds then the door opening intrusion message (SMS) alert via mobile phone. It can be concluded that the security system is efficient, easy to use and economical.

Keywords : Mobile phone application, Remote control system, Embedded system, SMS, Bluetooth

1. บทนำ

ปัจจุบันมีการพัฒนาระบบรักษาความปลอดภัยของรถยนต์ในหลากหลายรูปแบบ เช่น เครื่องกันขโมยควบคุมทางโทรศัพท์เคลื่อนที่ ซึ่งประกอบด้วยโทรศัพท์เคลื่อนที่ 2 ตัวคือ ภายในและภายนอกรถยนต์ หลักการควบคุมโดยการสั่งจากโทรศัพท์ เคลื่อนที่ภายนอกให้โทรศัพท์เคลื่อนที่ภายในดำเนินการต่างๆ เช่น โทรศัพท์เข้าไปที่วงจรควบคุมและไมโครคอนโทรลเลอร์ในชุดควบคุมจะทำการรับ ข้อมูล แล้วทำการสั่งงานออกมายังเอาต์พุตรีเลย์ว่าจะให้ไซเรนดัง หรือเปิดปิดประตูรถยนต์ เป็นต้น [1] การใช้ GPS ป้องกันรถหายด้วยสัญญาณ Microwave Sensor ระบบสั่งดับเครื่องยนต์หรือสั่งตัดการจ่ายน้ำมัน ทำให้รถยนต์ไม่สามารถเคลื่อนที่หรือ Start ได้และทราบตำแหน่งของรถได้ตลอดเวลา ผ่านโทรศัพท์ เคลื่อนที่หรือคอมพิวเตอร์ [2] และบริษัท BMW ได้พัฒนาแอพพลิเคชั่น My BMW Remote สำหรับรุ่นที่ผลิตตั้งแต่เดือนมีนาคมปี 2551 เป็นต้นไป สามารถใช้สมาร์ทโฟนเพื่อควบคุมฟังก์ชั่นเบื้องต้นในรถยนต์ เช่น ใช้แทนรีโมทเปิดปิดประตูรถ และเปิดปิดเสียงแตรและไฟหน้ารถ เป็นต้น [3]

งานวิจัยนี้นำเสนอวิธีการรักษาความปลอดภัยของรถยนต์ โดยการประยุกต์ใช้โทรศัพท์เคลื่อนที่แทนกุญแจรีโมท ใช้เปิด-ปิดรถยนต์ได้ทุกยี่ห้อ และช่วยในกรณีที่มีการโจรกรรมรถยนต์ ระบบจะแจ้งเตือนผ่าน SMS เข้าโทรศัพท์เคลื่อนที่ของเจ้าของรถยนต์อัตโนมัติ

2. วิธีการดำเนินงานและการออกแบบ

2.1 วัสดุอุปกรณ์ที่ใช้

2.1.1 ฮาร์ดแวร์

- เครื่องคอมพิวเตอร์ CPU E5200 2.5GHz, RAM 2 GB, Hard disk 250 GB

- อุปกรณ์ ZX-BT232 เป็นโมดูลที่ใช้ในการตั้งค่าต่างๆ รวมไปถึงจ่ายกระแสไฟฟ้าให้กับโมดูลบลูทูธ ESD200 ผ่านโปรแกรม Paraniwin และ Hyper terminal รวมถึงติดต่อกับไมโครคอนโทรลเลอร์

- อุปกรณ์ ET-ICDX v1.0 ทำหน้าที่ในการติดต่อระหว่างโปรแกรม และโมดูล ET-BASE PIC18F8722 (ICD2)

- อุปกรณ์ ZX-PIR เป็นโมดูลตรวจจับความเคลื่อนไหว โดยใช้หลักการตรวจจับรังสีอินฟราเรด

- อุปกรณ์ GR-64 GSM/GPRS เป็นโมดูล GSM/ GPRS ที่รองรับคลื่นวิทยุ 4 ความถี่ ได้แก่ GSM 850/ 950/1800/ 1900 MHz เพื่อส่ง SMS และการทำงานของ GPRS

- SIM Card ใช้ในการส่ง SMS เพื่อให้ GR-64 GSM/ GPRS Module เชื่อมต่อกับระบบเครือข่ายโทรศัพท์เคลื่อนที่

- โทรศัพท์เคลื่อนที่ ใช้เป็นรีโมทเสมือน

2.1.2 ซอฟต์แวร์

- ระบบปฏิบัติการ (OS) ได้แก่ Microsoft Windows XP Service Pack 3

- โปรแกรม MPlab ตัวแปลภาษา (Compiler)

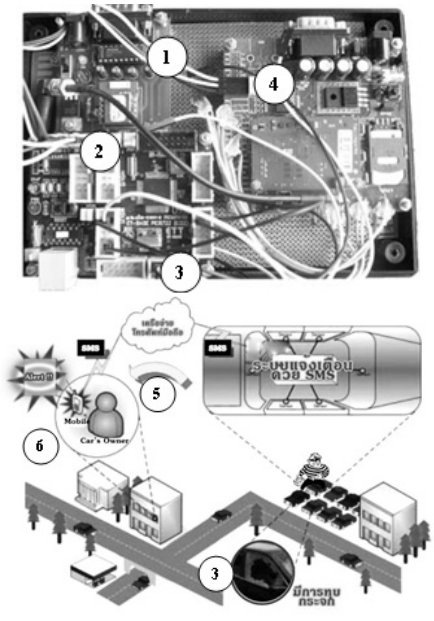
- โปรแกรม Paraniwin ตั้งค่าให้กับบลูทูธ ESD200

- โปรแกรม Nokia Pc Suite ใช้ในการติดต่อกับโทรศัพท์เคลื่อนที่ของโนเกีย

- Python ภาษาสคริปต์ในส่วนของการ Runtime และการ Execute

2.2 การออกแบบและวิธีการดำเนินงาน

2.2.1 การออกแบบระบบฝังตัวโดยใช้ไมโครคอนโทรลเลอร์ (ET-BASE PIC18F8722 (ICD2)) ติดตั้งในรถยนต์ ซึ่งสามารถแสดงภาพรวมการทำงานของระบบรักษาความปลอดภัย ดังรูปที่ 1

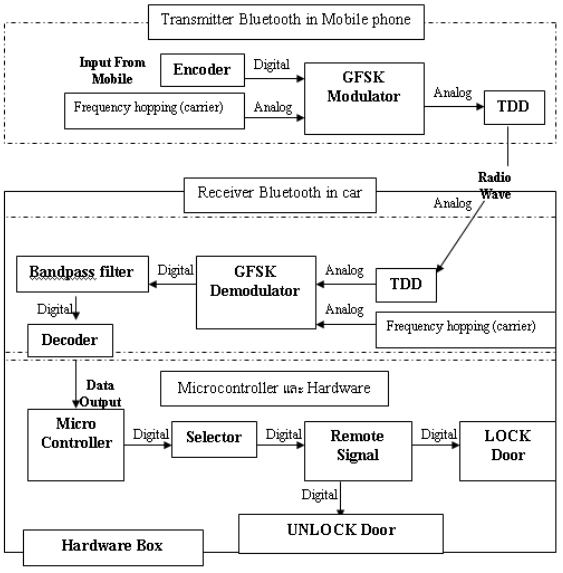


รูปที่ 1 ภาพรวมของระบบรักษาความปลอดภัยรถยนต์ผ่านระบบโทรศัพท์เคลื่อนที่

จากรูปที่ 1 ระบบรักษาความปลอดภัยรถยนต์เริ่มจาก(1) โปรแกรม Python ในโทรศัพท์เคลื่อนที่ติดต่อกับบลูทูธ ESD200 โดยส่งคำสั่งผ่านทางโมดูล ESD200 ไปยังโมดูล ET-BASEPIC18F8 722 (ICD2) (2) ประมวลผลคัดแยกคำสั่ง ถ้าต้องการเปิดปิดประตูคำสั่งจะส่งไปยังโมดูลรีโมท แต่ถ้าเกิดจากโจรกรรม จะรับคำสั่งจาก Sensor ZX-PIR (3) กรณีที่เกิดความผิดปกติกับรถยนต์ คำสั่งจะถูกประมวลผลและส่ง AT Command ไปยังโมดูล GR-64 GSM/GPRS Module (4) โมดูล GR-64 GSM/ GPRS Module ทำการส่ง SMS ผ่านเครือข่ายโทรศัพท์เคลื่อนที่ (5) ระบบแจ้งไปยังโทรศัพท์ของเจ้าของรถยนต์ (6) เจ้าของรถยนต์ได้รับข้อความแจ้งเตือนว่ารถยนต์อาจถูกโจรกรรม [4, 5, 6]

2.2.2 การออกแบบบล็อคไดอะแกรม การทำงานของระบบเปิด-ปิดประตูด้วยบลูทูธ

การออกแบบโมดูลบลูทูธ เป็นโมดูลที่ใช้ในพิสูจน์ตัวตน ป้องกันคลื่นรบกวนโดยการปรับค่าวิทยุ เพื่อทำการปลดล็อคได้ มีระยะการทำงานไม่เกิน 12 เมตร โดยโมดูลบลูทูธติดตั้งคู่กับไมโครคอนโทรลเลอร์ (PIC18F8722) ทำหน้าที่ประมวลผลหลัก และอยู่ในภายในรถยนต์ เพื่อให้ระบบเซ็นทรัลล็อคสมบรูณ์ โดยบล็อคไดอะแกรมของระบบการทำงานบลูทูธ ดังแสดงในรูปที่ 2 เริ่มจากเข้าเมนูเปิดโปรแกรม Python ทำการเชื่อมต่อโดยการค้นหาผ่านบลูทูธ โดย Frequency hopping (carrier) ทำหน้าที่ค้นหา และเชื่อมต่อ (Request-Reply) ทำให้ทราบว่ามีจำนวนอุปกรณ์ปลายทางที่สามารถเชื่อมต่อได้ จากนั้นแจ้งมายังผู้ใช้ที่หน้าจอโทรศัพท์เคลื่อนที่ [7, 8]

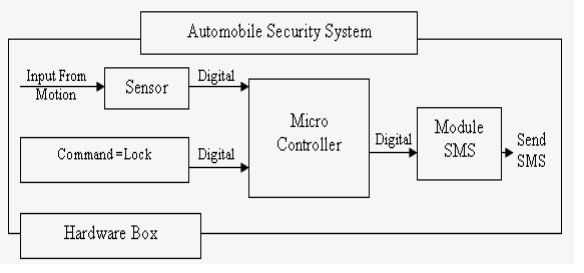


รูปที่ 2 บล็อกไดอะแกรมการทำงานของบลูทูธ

จากนั้นผู้ใช้เลือกปลายทางที่ค้นหามาได้เพื่อเชื่อมต่อ คือ โมดูลบลูทูธที่ติดตั้งไว้ภายในรถยนต์ (Receiver Bluetooth in car) หลังจากนั้นโมดูลบลูทูธที่อยู่ภายในโทรศัพท์เคลื่อนที่ หรือ Transmitter Bluetooth ทำการร้องขอเพื่อเชื่อมต่อ ดังนั้นเพื่อความปลอดภัย จึงมีการกำหนดให้มีการยืนยันตัวตนก่อนที่จะใช้โทรศัพท์เคลื่อนที่นั้นเป็นรีโมทเสมือนเพื่อเปิดปิดประตู โดยส่งคำร้องขอ ซึ่งก็คือค่าอินพุต (data) จากโทรศัพท์เคลื่อนที่นำเข้ารหัสด้วยขั้นตอน encoder เพื่อทำให้ได้ข้อมูลออกมาเป็นสัญญาณดิจิตอล ด้วยการทำ modulation แบบ GFSK ร่วมกับ Frequency hopping (carrier) ซึ่งเป็นการรวมคลื่นความถี่ของ data ที่มีความยาวคลื่นน้อยเข้ากับคลื่นความถี่พาหะ ที่มีความยาวคลื่นมาก เพื่อให้ในการรับ - ส่งข้อมูลได้ระยะทางไกลขึ้น และ GFSK Modem ทำหน้าที่เลือกช่องสัญญาณ จากนั้นจะได้สัญญาณออกมาเป็นแบบ Analog ที่ทำให้ส่งได้ไกลกว่า ส่วน TDD (time-division duplex) ทำหน้าที่ส่งและรับสัญญาณ ไปสู่อุปกรณ์หลายตัวพร้อมกันเสมือนสวิตช์ที่ปิด-เปิด ระหว่างการส่งสัญญาณที่มีความถี่เดียวกันโดยมีการแบ่งเวลาช่อง สัญญาณ เพื่อให้มีการรับและส่งข้อมูลได้ถูกต้อง ดังนั้นสัญญาณที่ได้ออกมาจึงอยู่ในรูปแบบ Radio Wave ตามรูปแบบของการ spread spectrum แบบ GFSK

2.2.3 บล็อคไดอะแกรม การทำงานของระบบการรักษาความปลอดภัยรถยนต์

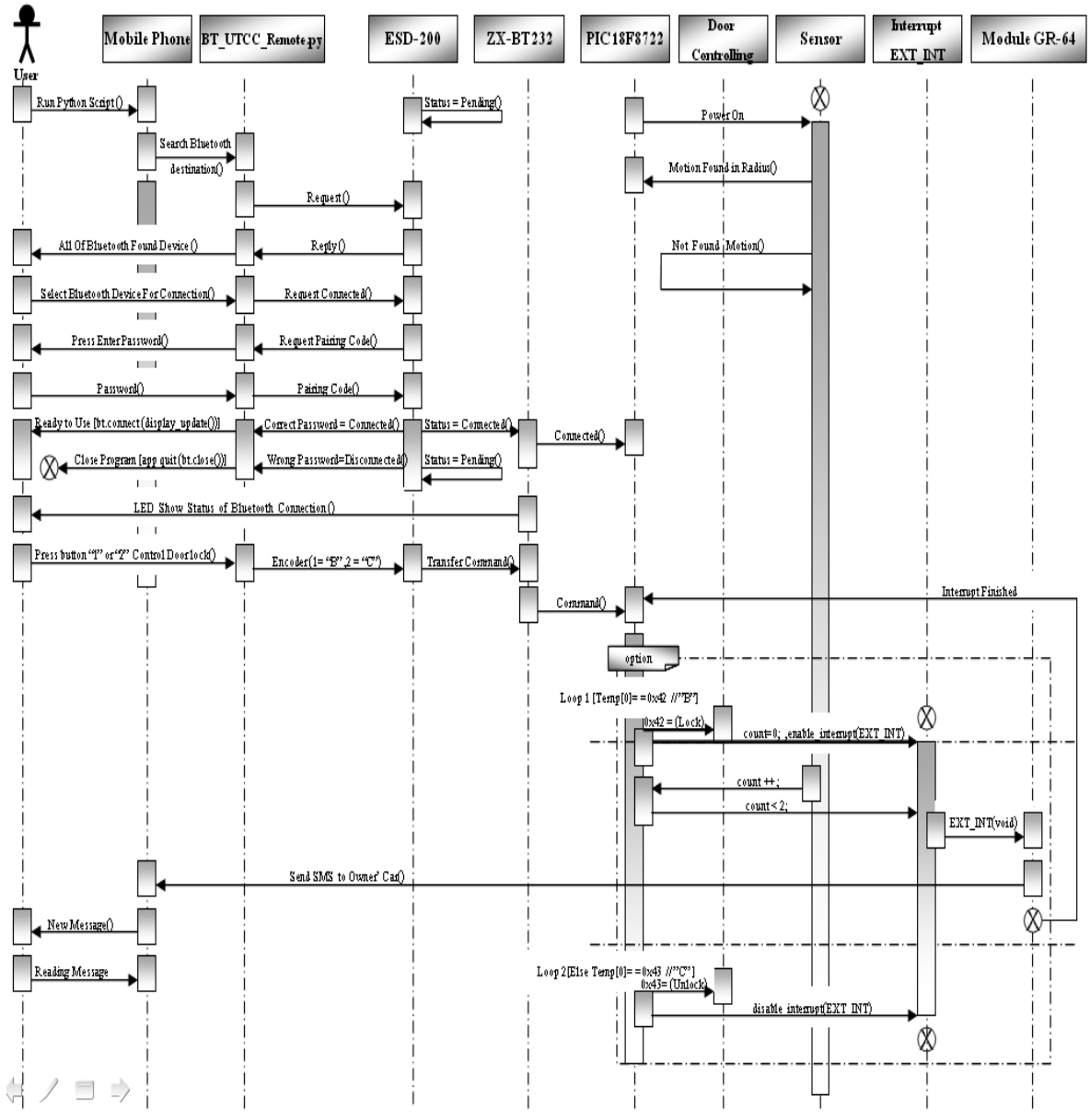
ระบบการรักษาความปลอดภัยรถยนต์ ในส่วนของภายในบริเวณห้องผู้โดยสาร อาศัยการทำงานของโมดูลเซ็นเซอร์ ที่ตรวจจับรังสีอินฟราเรด โมดูลเซ็นเซอร์จะส่งสัญญาณแบบดิจิตอลมาที่ไมโครคอนโทรลเลอร์ตลอดเวลาที่ตรวจจับได้ แต่ระบบยังไม่ทำการส่ง SMS จนกว่าจะมีคำสั่งล็อคด้วยโทรศัพท์เคลื่อนที่ เมื่อรับคำสั่งล็อคแล้วสัญญาณที่ส่งมาจากเซ็นเซอร์จึงมีผลต่อโปรแกรม และถูกนำไปประมวลที่ไมโครคอนโทรลเลอร์ (PIC18F8722) จากนั้นส่งคำสั่ง AT Command ให้โมดูล SMS เพื่อส่งข้อความแจ้งเตือนไปยังโทรศัพท์ของเจ้าของรถยนต์ ซึ่งสามารถแสดงบล็อคไดอะแกรม การทำงานของระบบการรักษาความปลอดภัย [9,10,11] ดังรูปที่ 3



รูปที่ 3 บล็อคไดอะแกรม การทำงานของโมดูล เซ็นเซอร์กรณีที่รถยนต์อาจถูกโจรกรรม

2.2.4 การออกแบบสารสนเทศ

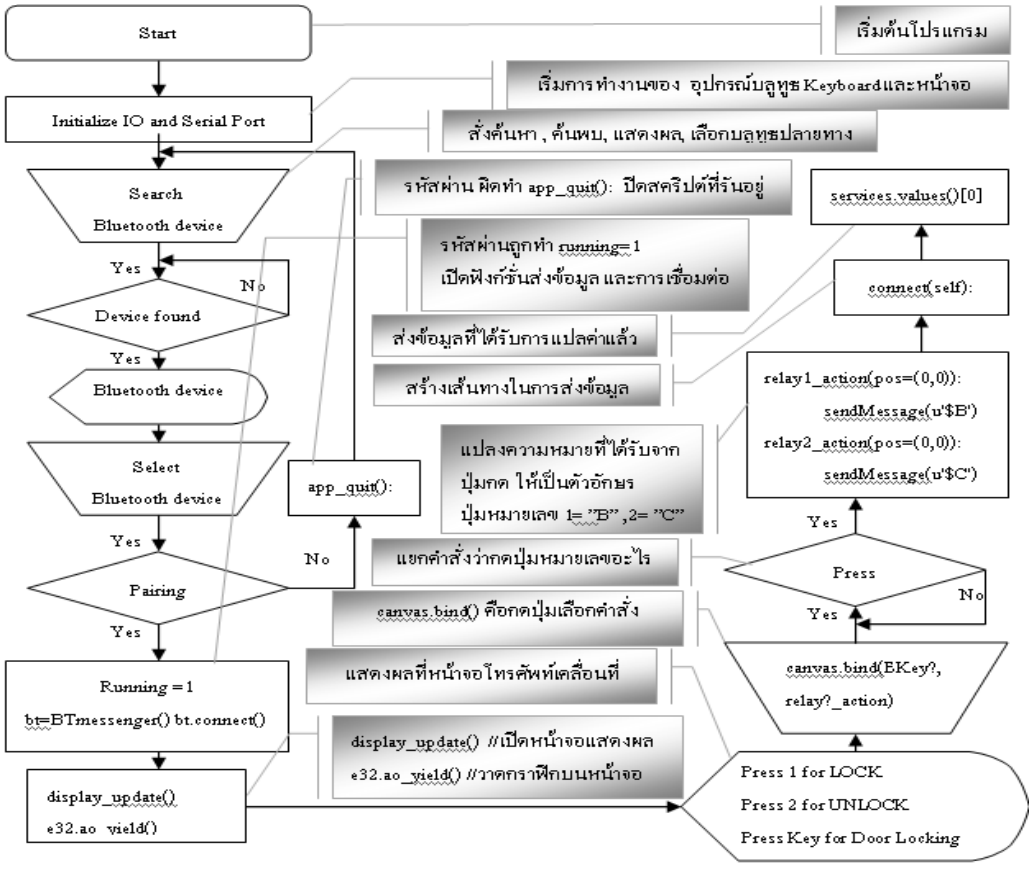
จากการวิเคราะห์และออกแบบระบบสารสนเทศโดยใช้วิธีการเชิงวัตถุด้วยมาตรฐานภาษา Unified Modeling Language (UML) อธิบายการทำงานของระบบทั้งหมด ซึ่งในการศึกษาครั้งนี้ใช้ Sequence Diagram เพื่ออธิบายฟังก์ชั่นในการทำงานของระบบโดยรวม ดังรูปที่ 4



รูปที่ 4 Sequence Diagram การทำงานของระบบ

2.2.5 การพัฒนาโปรแกรม

แบ่งออกเป็น 2 ส่วน ส่วนที่หนึ่งเป็นโปรแกรมการโอนถ่ายข้อมูลจากโมดูล ESD-200 และ ZX-BT232 มายังโมดูล ET-BASE PIC18F8722 (ICD2) เพื่อทำการคัดแยกและแปลงคำสั่ง เพื่อใช้ในการประมวลผลของโปรแกรมที่ได้ทำการตั้งค่าไว้ในโมดูล BT-BASEPIC18F8722 (ICD2) เพื่อสั่งรีโมทให้ทำการล็อคหรือปลดล็อคประตูรถยนต์ นอกจากนี้โมดูล ET-BASE PIC18F8722 (ICD2) ยังมีหน้าที่ในการรับค่าที่ได้การตรวจจับการรบกวนซึ่งมาจากเซ็นเซอร์ ZX-PIR เอามาประมวลผลเพื่อส่งคำสั่ง AT Command ไปยังโมดูล GR-64 GSM/ GPRS เพื่อให้ทำการส่ง SMS ไปยังโทรศัพท์เคลื่อนที่ เพื่อแจ้งเตือนเจ้าของรถยนต์ ส่วนที่สองทำหน้าที่เสมือนรีโมท ดังแสดงผังงาน (Flowchart) ในรูปที่ 5

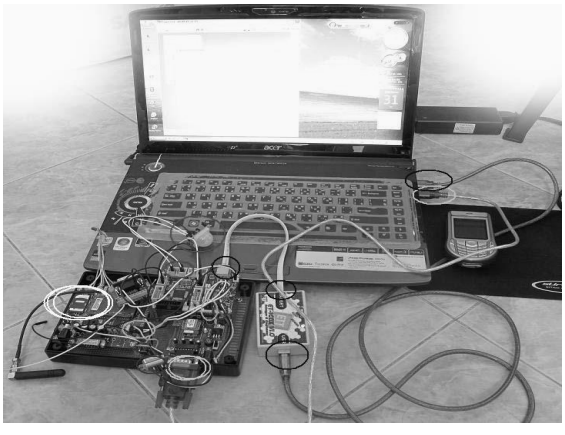


รูปที่ 5 ผังงานโปรแกรมบนโทรศัพท์เคลื่อนที่

3. ผลการศึกษา

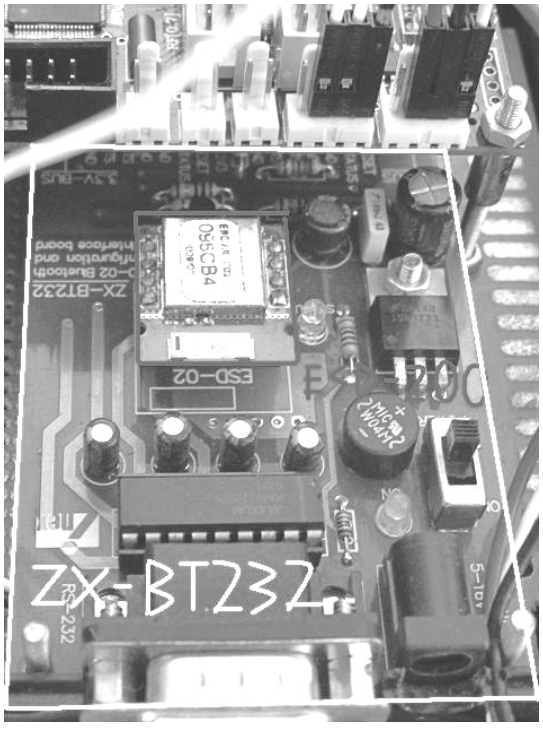
3.1 การเชื่อมต่ออุปกรณ์กับคอมพิวเตอร์

การต่อโมดูลต่างๆ เข้ากับคอมพิวเตอร์นั้นเพื่อทำการตั้งค่าและติดตั้งโปรแกรมดังรูปที่ 6



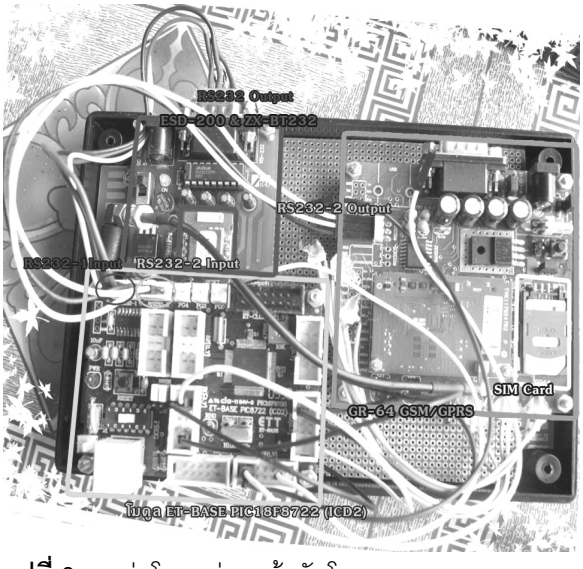
รูปที่ 6 การเชื่อมต่อโมดูลต่างๆ โดยรวม

จากรูปที่ 6 การเชื่อมต่ออุปกรณ์ต่างๆ เข้ากับแล้ว ทำการติดตั้งโปรแกรมควบคุมหลักลงโมดูล ET-BASEPIC1 8F8722 (ICD2) และทำการ Debug โปรแกรมโดยการเชื่อมต่อผ่านโมดูล ET-ICDX V1.0 ซึ่งหลังจากทำการติดตั้งโปรแกรม จากนั้นต่ออุปกรณ์ โมดูล ESD-200 เข้ากับโมดูล ZX-BT232 ดังรูปที่ 7



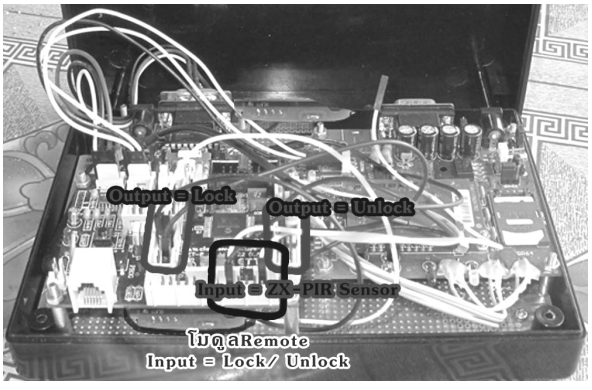
รูปที่ 7 การต่อโมดูล ESD-200 เข้ากับโมดูล ZX-BT232

การต่อโมดูลต่างๆ เข้ากับโมดูลควบ คุม หรือ โมดูล ET-BASE PIC18F8722 (ICD2) ดังรูปที่ 8



รูปที่ 8 การต่อโมดูลต่างๆเข้ากับโมดูลควบคุม

จากนั้นต่อโมดูลรีโมทเข้ากับโมดูลควบคุมเพื่อรับสัญญาณ Input จากโมดูล ET-BASE PIC18F8722 (ICD2) ดังรูปที่ 9



รูปที่ 9 การต่อโมดูลรีโมทเข้ากับโมดูลควบคุม

*3.2 ผลการทำงานของระบบเปิด-ปิดประตู*ด้วยโทรศัพท์เคลื่อนที่ผ่านบลูทูธ ภายหลังติดตั้งโปรแกรม Python ดังรูปที่ 10

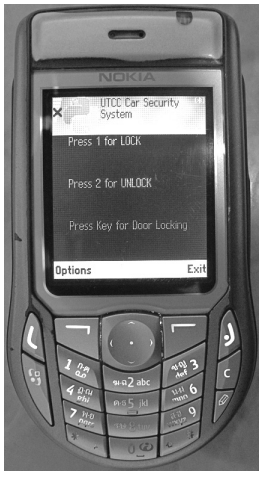
รูปที่ 10 การติดตั้งโปรแกรม Python

จากนั้นแสดงการควบคุมระบบล็อครถยนต์ผ่านโทรศัพท์เคลื่อนที่ ซึ่งระยะทำการในการออกคำสั่งควบคุมระบบล็อคในพื้นที่โล่ง 12 เมตร และแสดงในหน้าจอโทรศัพท์เคลื่อนที่มีการแสดงข้อความว่า “UTCC Car Security System” ดังรูปที่ 11

Press 1 for LOCK

Press 2 for UNLOCK

Press Key for Door Locking”

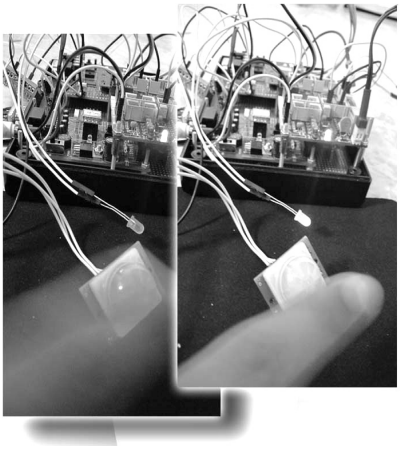


รูปที่ 11 การควบคุมระบบล็อครถยนต์ผ่านโทรศัพท์เคลื่อนที่

3.3 ผลการทำงานของระบบแจ้งเตือนหากถูกโจรกรรม

การนำเซ็นเซอร์ตรวจจับความเคลื่อนไหวไปติดตั้งภายในรถยนต์บริเวณใต้พวงมาลัยเหนือตำแหน่งเบรกและคันเร่ง จากการทดสอบโดยการทุบกระจก พบว่ามีการเปลี่ยนแปลงของรังสีอินฟราเรดจากภายนอกโมดูล แล้วนำค่าที่ได้รับมาผ่านวงจรขยายและวงจรเปรียบเทียบ ซึ่งอยู่ในโมดูล ZX-PIR นำค่าที่อ่านได้และแปลความหมายออกมาทางเอาท์พุตสัญญาณที่ได้มาต่อเข้ากับโมดูลควบคุมหลัก หรือ ET-BASE PIC18F8722 (ICD2) แล้วนำไปประมวลผลเป็นเอาท์พุตออกมาจากโมดูล ET-BASEPIC18F8 722 (ICD2) เพื่อแสดงผลการตรวจจับดังรูปที่ 12

ผลการทดสอบระบบสามารถตรวจจับความเคลื่อนไหวการโจรกรรมรถยนต์ได้อย่างมีประสิทธิภาพ ทั้งการขโมยรถยนต์ หรือทุบกระจกเพื่อมาหยิบของมีค่าในรถยนต์ โดยใช้เวลาตั้งแต่ตรวจจับความเคลื่อนไหวได้ จนสิ้นสุดขั้นตอนการส่ง SMS เป็นเวลา 3 วินาที ดังรูปที่ 13



รูปที่ 12 ทดสอบการตรวจจับและแสดงผลเซ็นเซอร์

รูปที่ 13 ข้อความ SMS แจ้งเตือนรถยนต์ของท่านกำลังจะถูกโจรกรรม

4. สรุปผลการศึกษา

ระบบรักษาความปลอดภัยรถยนต์ผ่านระบบโทรศัพท์เคลื่อนที่ สามารถออกคำสั่งเปิด-ปิดประตูด้วยโทรศัพท์เคลื่อนที่เป็นรีโมทเสมือน ช่วยในการแก้ปัญหาการลืมกุญแจรีโมทไว้ภายในรถยนต์ได้ส่วนหนึ่ง ซึ่งระยะทำการในการออกคำสั่งควบคุมระบบล็อคในพื้นที่โล่ง 12 เมตร แต่ยังไม่สามารถทำการล็อครถยนต์โดยอัตโนมัติได้อย่างเต็มรูปแบบ ซึ่งหมายถึงการล็อคอัตโนมัติได้ทันทีที่มี

การปิดประตูรถยนต์โดยไม่ต้องรอคำสั่งล็อคจากรีโมท สั่งการล็อคหรือไขกุญแจเพื่อล็อคประตู ยังไม่สามารถทำได้ เนื่องจากการมีข้อจำกัดทางด้านฮาร์ดแวร์บลูทูธ ซึ่งคำสั่ง AT Command เป็นความลับทางการค้า และโปรโตคอลที่ใช้ในการเชื่อมต่อมีขีดจำกัด แต่มีข้อดีที่ระบบรักษาความปลอดภัยมีความเข้มงวดขึ้นกว่าระบบเซ็นทรัลล็อคแบบเก่า และสามารถใช้งานได้จริง และใช้ได้ง่ายทั้งการติดตั้งและการใช้งาน

สำหรับระบบเตือนภัยการโจรกรรมนั้นในขณะที่รถยนต์ยังทำคำสั่งล็อคอยู่ ถ้ามีการเข้าไปรบกวนรถยนต์ในห้องผู้โดยสาร เช่นมีการทุบกระจก ระบบจะทำการแจ้งเตือนผ่านระบบเครือข่ายโทรศัพท์เคลื่อนที่ด้วยระบบการส่ง SMS ซึ่งผลการทดสอบการตรวจจับความเคลื่อนไหว สามารถตรวจจับได้ก็ต่อเมื่อเข้ามาในห้องผู้โดยสารเท่านั้น ซึ่งแสงภายนอก และการสั่นสะเทือน ไม่มีผลต่อโมดูลตรวจจับความเคลื่อนไหว ซึ่งทำให้สามารถตรวจจับความเคลื่อนไหวได้ทั้งกลางวัน และกลางคืน โดยการแจ้งเตือนทางการส่ง SMS นั้นใช้เวลาภายใน 5 วินาที ซึ่งนับตั้งแต่โมดูลตรวจจับความเคลื่อนไหวอ่านค่าได้นั้นจนถึงขั้นที่ส่งออกไปนั้นใช้เวลา 3 วินาที แต่มีการรีเลย์ในช่วงของการส่งจากเครือข่ายโทรศัพท์เคลื่อนที่ ซึ่งขึ้นอยู่กับผู้ใช้บริการขณะนั้นด้วย ดังนั้นข้อความถูกส่งถึงผู้ใช้โดยใช้เวลาประมาณ 5 วินาทีนับตั้งแต่โมดูลตรวจจับความเคลื่อนไหวอ่านค่าได้ แนวทางในพัฒนาต่อไป คือ ฮาร์ดแวร์บลูทูธ ESD-200 เนื่องจาก AT Command เป็นความลับทางการค้า และขีดจำกัดในเรื่องโปรโตคอล ซึ่งไม่สามารถทำงานตอบสนองระบบรักษาความปลอดภัยผ่านโทรศัพท์เคลื่อนที่ได้ทุกกรณี คือต้องมีโปรโตคอลอย่างน้อยหนึ่งตัวที่ทำหน้าที่คอยนำข้อมูลแสดงผลการ pairing จากโปรโตคอล HCI ซึ่งถ้าเทียบกับ OSI model จะอยู่ใน Transport layer จากนั้นแสดงผลใน Application layer แบบ Real time หรือแบบที่ต้องนำข้อมูลส่งมาทุกครั้งในทันทีที่มีการ Paring สำเร็จซึ่งการ Pair กันนั้นจะเกิดขึ้นในชั้นล่างสุดคือระดับชั้น Radio ซึ่งถ้าเทียบกับของ OSI model จะอยู่ใน Physical layers ซึ่งระบบล็อคประตูรถยนต์ที่ปลอดภัยดีที่สุด นั่นคือสามารถทำให้สร้างระบบล็อคแบบอัตโนมัติเมื่อปิดประตูทันทีหรือภายในกำหนดเวลาได้ โดยไม่ต้องรอคำสั่งจากกุญแจรีโมทหรือการล็อคด้วยกุญแจ ซึ่งป้องกันการลืมล็อคประตูรถยนต์อย่างดีที่สุด และไม่ต้องกังวลเรื่องการลืมกุญแจรีโมทไว้รถยนต์ เพราะสามารถใช้โทรศัพท์เคลื่อนที่ที่มีบลูทูธเครื่องใดก็ได้เพื่อใช้ในการปลดล็อค ดังนั้นการพัฒนาโปรแกรมในส่วนของโปรโตคอลนั้นเป็นทางเลือกที่ดี

5.เอกสารอ้างอิง

[1] Gibson JD (Ed), “The mobile communications handbook.” 2nd Ed, CRC Press Ltd., USA, 1999.

[2] Harte L, Levine R, Livingston G. GSM superphones. McGraw Hill, New York, pp.105-116, 1999.

[3] Steuernagel R A. The cellular connection, A guide to cellular telephones.”, John Wiley, New York, 2000.

[4] Lee C Y. Mobile cellular telecom- munications analog and digital systems. 2nd ed., McGraw Hill, Lisbon, 1995.

[5] Janes M. Microcontroller cookbook, Newnes, 1997.

[6] Spacor P. Microcontroller technology, Prentice Hall, USA, 1993.

[7] Ludwig R, Bretchko P. RF Circuit design-theory and applications. Prentice Hall, USA, 2000.

[8] Carr J J. RF Circuit design, 3rd McGraw Hill, Brisbane, 2001.

[9] Jugren R K. Automotive electronics handbook. 2nd ed., McGrawHill, New York, 1999