ระบบควบคุมอุปกรณ์ไฟฟ้าผ่านเครือข่าย

ELECTRICAL APPLIANCE CONTROL VIA NETWORK

ชาญณรงค์ เนียมถนอม
Channarong Neamtanom
ตรีณัฐ ยูซูฟี
Treenut Yusufee
พันธ์ศักดิ์ วุฒินันทพงศ์
Phansak Wuttinanthapong

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
ภาควิชาวิศวกรรมอิเล็กทรอนิกส์
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2558

ระบบควบคุมอุปกรณ์ไฟฟ้าผ่านเครือข่าย

ELECTRICAL APPLIANCE CONTROL VIA NETWORK

โดย

ชาญณรงค์ เนียมถนอม 55010277

ตรีณัฐ ยูซูฟี 55010432

พันธ์ศักดิ์ วุฒินันทพงศ์ 55010846

อาจารย์ที่ปรึกษา

อ. ชินภัทร นันทจิวากรชัย

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
ภาควิชาวิศวกรรมอิเล็กทรอนิกส์
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ .ศ . 2558

ปริญญานิพนธ์ปีการศึกษา 2558

ภาควิชา	วิศวกรรมอิเล็กทรอนิกส์	
คณะ	วิศวกรรมศาสตร์	
	สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง	
เรื่อง	ระบบควบคุมอุปกรณ์ไฟฟ้าผ่านเครือข่าย	
	ELECTRICAL APPLIANCE CONTROL VIA NETWORK	
ผู้จัดทำ	นายชาญณรงค์ เนียมถนอม	55010277
	นายตรีณัฐ ยูซูฟี	55010432
	นายพันธ์ศักดิ์ วุฒินันทพงศ์	55010846

ปริญญานิพนธ์นี้ผ่านการตรวจสอบโดยอาจารย์ที่ปรึกษาแล้ว

(อ. ชินภัทร นันทจิวากรชัย)
อาจารย์ที่ปรึกษา

หัวข้อปริญญานิพนธ์	ระบบควบคุมอุปกรณ์ไฟฟ้าผ่านเครือข่าย
นักศึกษา	ชาญณรงค์ เนียมถนอม รหัส 55010277
	ตรีณัฐ ยูซูฟี รหัส 55010432
	พันธ์ศักดิ์ วุฒินันทพงศ์ รหัส 55010846
ปริญญา	วิศวกรรมศาสตรบัณฑิต
ภาควิชา	วิศวกรรมอิเล็กทรอนิกส์
ปีการศึกษา	2558
อาจารย์ที่ปรึกษาปริญญานิพนธ์	อ.ชินภัทร นันทจิวากรชัย

บทคัดย่อ

โครงงานนี้เป็นส่วนหนึ่งของปริญญานิพนธ์ระดับปริญญาตรี โครงงานชิ้นนี้มีชื่อว่าระบบควบคุมอุปกรณ์ไฟฟ้าแบบไร้สาย สามารถเปิด-ปิดอุปกรณ์ไฟฟ้าผ่านระบบเครือข่ายไร้สาย ควบคุมโดยไมโครคอนโทรลเลอร์ที่ได้โปรแกรมไว้ ซึ่งจะอำนวยความสะดวกแก่ผู้ใช้งาน โดยที่ไม่ต้องเอื้อมมือไปถอดปลั๊กไฟออก สามารถเชื่อมต่อผ่านระบบเครือข่ายเพื่อสั่งเปิด-ปิดอุปกรณ์ไฟฟ้าที่เราต้องการได้ทันที

Thesis Title	Electrical Appliance Control via Network
Student	Chanarong Neamtanom
	Treenut Yusufee
	Phansak Wutthinanthaphong
Degree	Bachelor of Engineering
Department	Electronic Engineering
Year	2015
Thesis Advisor	**Mr.** Chinnapat Nanthajiwakornchai

Abstract

This project is a part of bachelor's degree thesis. The thesis called Electrical Appliance control via network. That can switch on/off an Electricity with network system. Controlled by Microcontroller with program data in to it for more comfortable result even must not remove Plug. It can connect to the Socket Plug to turn on or turn off the electricity as soon as we need.

กิตติกรรมประกาศ

คณะผู้วิจัยขอขอบพระคุณ อาจารย์ชินภัทร นันทจิวากรชัย ซึ่งเป็นอาจารย์ที่ปรึกษาโครงงาน ท่านได้ให้ความ อนุเคราะห์ทางด้านทุนทรัพย์และคำแนะนำให้คำปรึกษาในสิ่งที่เป็นประโยชน์เกี่ยวกับโครงงาน อีกทั้ง ตลอดจนให้ยืมอุปกรณ์เพื่อใช้ในการทดสอบโครงงานเพื่อให้โครงงาน สำเร็จลุล่วงไปได้ด้วยดี

ขอขอบพระคุณ อาจารย์แผนกอิเล็กทรอนิกส์ทุกท่านที่ได้ให้ความกรุณาให้คำแนะนำความรู้ต่างๆ อีกทั้งเพื่อนๆ ที่ให้ความสะดวกในการจัดทำโครงงานให้ได้สำเร็จลุล่วงตามวัตถุประสงค์

สุดท้ายนี้ ขอขอบพระคุณ บิดา มารดา ครอบครัว ซึ่งได้ให้คำแนะนำและสนับสนุนใน ด้านการเงินแก่ผู้จัดทำเสมอจนสำเร็จการศึกษาจนถึงปัจจุบัน อีกทั้งคณาจารย์ภาควิชาวิศวกรรมไฟฟ้า คุณประโยชน์อันใดที่เกิดจากงานวิจัยนี้ ย่อมเป็นผลมาจากความกรุณาของท่านดังกล่าวข้างต้นผู้จัดทำจึงใคร่ขอขอบพระคุณมา ณ โอกาสนี้

ชาญณรงค์ เนียมถนอม

ตรีณัฐ ยูซูฟี

พันธ์ศักดิ์ วุฒินันทพงศ์

สารบัญ

หน้า

บทคัดย่อภาษาไทย I
บทคัดย่อภาษาอังกฤษ II
กิตติกรรมประกาศ III
สารบัญ IV
สารบัญรูป VII
สารบัญตาราง VIII
บทที่ 1 บทนำ
1.1 ที่มาและความสำคัญ 1
1.2 วัตถุประสงค์ของการศึกษา 1
1.3 ขอบเขตของโครงงาน 1
1.4 ขั้นตอนการดำเนินงาน 1
บทที่ 2 หลักการและทฤษฎี
2.1 บอร์ดอาดูโน่ 2
2.1.1 ข้อมูลทางเทคนิค 3
2.2 Internet of Thing 4
2.2.1 เกริ่นนำถึง Internet of Thing 4
2.2.2 ประวัติของ Internet of Thing 4
2.2.3 การประยุกต์ใช้งาน 5
2.3 Wi-Fi 6
2.3.1 เกริ่นนำถึง Wi-Fi 6
2.3.2 ประวัติของ Wi-Fi 6
2.3.3 ลักษณะการเชื่อมต่อของอุปกรณ์ 7
2.3.4 กลไกรักษาความปลอดภัย 8
2.3.5 การเข้าและถอดรหัสข้อมูล 8
2.3.6 การตรวจสอบผู้ใช้ 9
2.3.7 ข้อดี 11
2.3.8 พิสัย 11
2.3.9 ข้อจำกัด 11
2.3.10 ความเสี่ยงด้านความปลอดภัยของข้อมูล 12
2.3.11 การรบกวน 13
2.3 IP Address 13
2.5 SPI 14

สารบัญ(ต่อ)

หน้า

2.5.1 เกริ่นนำถึง SPI 14
2.5.2 อินเตอร์เฟส 15
2.5.3 การทำงาน 15
2.5.4 ขั้วของสัญญาณนาฬิกา และ มุมเฟส 16
2.5.5 เลขโหมด 16
2.5.6 Valid communications 17
2.5.7 อินเตอร์รัพ 17
2.5.8 ข้อได้เปรียบ 18
2.5.9 ข้อเสีย 19
2.6 WEP 20
2.7 WPA 20
2.8 โปรโตคอล 21
2.8.1 เกริ่นนำถึงโปรโตคอล 21
2.8.2 ความสำคัญของโปรโตคอล 22
2.8.3 การทำงานของโปรโตคอล 22
2.9 Client/Server 23
2.10 หลักการทำงาน 23
2.10.1 หลักการทำงานของภาคควบคุม 24
2.10.2 หลักการทำงานของคำสั่ง Code 25

บทที่ 3 วิธีการการทดลอง
3.1 วิธีที่ใช้ศึกษาค้นคว้าและการวิจัยทดลอง 28
3.2 ลักษณะข้อมูล การเลือกข้อมูล และการทดลอง 28
3.3 เครื่องมือและวิธีการวิจัยทดลอง 29
3.4 ขั้นตอนออกแบบและสร้างเครื่องมือ 29

บทที่ 4 ผลการทดลอง
4.1 หน้าจอแสดงข้อความต้อนรับ 31
4.2 การเชื่อมต่อบอร์ดอาดูโน่ด้วยสาย Lan 31
4.3 หน้าจอแสดงข้อความเมื่อยังไม่มีการเชื่อมต่อ 32
4.4 หน้าจอแสดงข้อความเมื่อเชื่อมต่อแล้ว 32
4.5 หน้าจอแสดงข้อความขณะกำลังเปิดเครื่องใช้ไฟฟ้า 33
4.6 หน้าจอแสดงข้อความขณะกำลังเปิดเครื่องใช้ไฟฟ้า 33
4.7 ชุดอุปกรณ์ที่ใช้ในการทดลอง 34
4.8 ชุดทดลองขณะกำลัง ON 34

สารบัญ(ต่อ)

หน้า

บทที่ 5 สรุปผลการทดลองและข้อเสนอแนะ
5.1 สรุปผลการทดลอง 35
5.2 ประโยชน์ที่ได้รับ 35
5.3 ข้อเสนอแนะ 36
5.4 ปัญหาที่พบ 37

เอกสารอ้างอิง 39

สารบัญรูป

รูปที่ หน้า

2.1 บอร์ดอาดูโนที่ใช้ในการทดลอง 3
2.2 สัญลักษณ์ของ Wi-Fi 6
2.3 ช่องความถี่ของ Wi-Fi ในแถบความถี่ 2.4 GHz 12
2.4 เครือข่ายการเชื่อมต่อของเครื่องคอมพิวเตอร์ 21
2.5 การเชื่อมต่ออินเตอร์เนตระหว่างเครื่องคอมพิวเตอร์ทั่วโลก 22
2.6 วงจรภาคควบคุม 24
2.7 Block Diagram แสดงการทำงานของ Web Server 26
3.1 Block Diagram ของทั้งระบบ 30
4.1 หน้าจอแสดงข้อความต้อนรับ 31
4.2 การเชื่อมต่อบอร์ดอาดูโน่ด้วยสาย LAN 31
4.3 หน้าจอแสดงข้อความเมื่อยังไม่มีการเชื่อมต่อ 32
4.4 หน้าจอแสดงข้อความเมื่อเชื่อมต่อแล้ว 32
4.5 หน้าจอแสดงข้อความขณะกำลังเปิดเครื่องใช้ไฟฟ้า 33
4.6 หน้าจอแสดงข้อความขณะกำลังปิดเครื่องใช้ไฟฟ้า 33
4.7 ชุดอุปกรณ์ที่ใช้ในการทดลอง 34
4.8 ชุดทดลองขณะกำลัง ON 34
5.1 การนำเทคโนโลยีของอินเตอร์เน็ตมาอำนวยความสะดวกภายในบ้าน 37

สารบัญตาราง

ตารางที่ หน้า

1 คุณสมบัติเบื้องต้นของบอร์ดอาดูโน่ 2
2 โหมดการทำงาน SPI สำหรับไมโครคอนโทรลเลอร์ "Microchip PIC" / "ARM-based" 17
3 โหมดการทำงาน SPI สำหรับไมโครคอนโทรลเลอร์อื่นๆ 17

บทที่ 1

บทนำ

1.1 ที่มาและความสำคัญ

สำหรับโครงงานระบบควบคุมเครื่องใช้ไฟฟ้าผ่านเครือข่ายไร้สายนั้น ได้แนวคิดจากการใช้สวิตช์ เปิด-ปิด ธรรมดา จะพบว่าสวิตช์เปิด-ปิด มีราคาถูก แต่ต้องใช้ระบบ Manual ในการควบคุม จากการประชุมกลุ่มเห็นว่าจะต้องสร้างระบบควบคุมไฟฟ้าแสงสว่างผ่านเครือข่ายไร้สาย ในการควบคุมการทำงานของวงจรควบคุมการเปิด-ปิดเครื่องใช้ไฟฟ้า คาดว่าจะอำนวยความสะดวก และเปิด-ปิด ได้ตามต้องการ

1.2 วัตถุประสงค์ของการศึกษา

โครงงานนี้มุ่งหมายให้เกิดความเข้าใจในระบบการสั่งงานผ่านระบบเครือข่ายเพื่อให้เกิดความสะดวกในการเปิด – ปิด เครื่องใช้ไฟฟ้า ความรู้ที่ได้จากการทำโครงงานนี้สามารถนำไปต่อยอดในการพัฒนาการสั่งการด้วยระยะที่ไกลขึ้น และ เพื่อการนำไปพัฒนาต่อยอดได้ง่าย และ หลากหลายมากขึ้น ซึ่งกระทำได้โดยผ่านทาง Web Server

1.3 ขอบเขตของโครงงาน

คาดว่าสามารถสั่งการ เปิด – ปิด เครื่องใช้ไฟฟ้าผ่านระบบ web server ได้ในระยะที่ไกล และ สะดวกรวดเร็ว อีกทั้งการตอบสนองต้องรวดเร็วด้วย

1.4 ขั้นตอนการดำเนินงาน

1) สามารถควบคุมการเปิดปิดระบบไฟฟ้า โดยใช้บอร์ด Arduino UNO เป็นตัวประมวลผล

2) สามารถแสดงสถานะการเปิด – ปิด ได้

3) การใช้งานจะเป็นแบบ wireless เท่านั้น

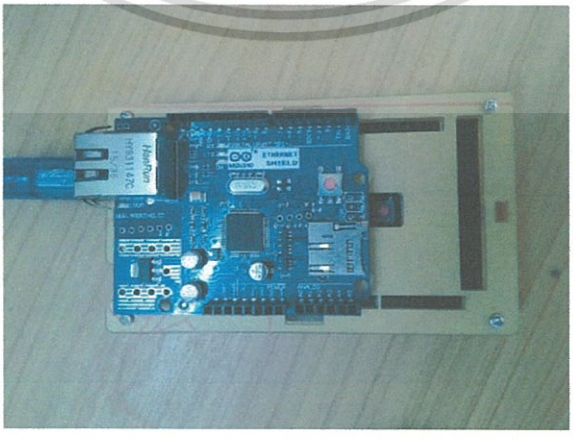
บทที่ 2

หลักการและทฤษฎี

ในปัจจุบัน สิ่งอำนวยความสะดวกในชีวิตประจำวันของผู้คนในสมัยใหม่ มีการนำวงจรอิเล็กทรอนิกส์ หลากหลายชนิดมาประยุกต์ และ ประดิษฐ์ เป็นอุปกรณ์ต่างๆ หนึ่งในนั้นที่เราให้ความสนใจ คือ เทคโนโลยี Smart Home ซึ่งกำลังเริ่มที่จะได้รับความนิยม มันคือเทคโนโลยีการสั่งการเครื่องใช้ไฟฟ้าภายในบ้าน ผ่านโทรศัพท์มือถือ เพื่อควบคุมเครื่องใช้ไฟฟ้าภายในบ้านให้เปิด หรือ ปิด ในตามต้องการ และ สามารถสั่งการได้ในระยะที่ไกล เทคโนโลยี Smart home ได้จัดว่าเป็นส่วนหนึ่งของ Internet of Thing คือ การประยุกต์ใช้ internet มาอำนวยความสะดวกให้กับมนุษย์ ซึ่งเมื่อมีการใช้ internet เกิดขึ้น ก็จะเกิดการติดต่อกันระหว่าง Client กับ Server (Client คือ อุปกรณ์ที่มาติดต่อขอรับบริการ ส่วน Server คือ อุปกรณ์ที่คอยให้บริการกับ client) การติดต่อจะเกิดความเข้าใจที่ตรงกันได้นั้น จำเป็นที่จะต้องมีมาตรฐานมารองรับ (Protocol) เพื่อการติดต่อสื่อสารระหว่างอุปกรณ์อื่นๆ และ บอร์ดอาดูโน่ (Server) สั่งการได้อย่างราบลื่น โดยส่วนมากการใช้งานในเรื่องของ Internet of Thing จะเป็นการใช้งานผ่านทางสัญญาณ Wi-Fi ซึ่งเป็นการติดต่อแบบไร้สาย แต่ในบางกรณีที่ต้องการนำ บอร์ดอาดูโน่ มาใช้งานแบบไม่ไร้สาย ซึ่งส่วนใหญ่จะมีวัตถุประสงค์เพื่อ ลงชุดคำสั่ง (Code) ลงไปในบอร์ดอาดูโน่ (การ Burn) ผู้ใช้งานจำเป็นที่จะต้องนำบอร์ดอาดูโน่ มาเชื่อมต่อกับคอมพิวเตอร์ เพื่อถ่ายโอนชุดคำสั่งที่เราต้องการลงไป จะจัดว่าเป็นการเชื่อมต่อแบบไม่ไร้สาย ระบบที่ใช้ในการเชื่อมต่อในลักษณะดังกล่าว เรียกว่า SPI (ในโครงงานนี้ใช้บอร์ดอาดูโน่เป็นทำการประมวลผล)

2.1 บอร์ดอาดูโน่

บอร์ดอาดูโน่ คือ ไมโครคอนโทรลเลอร์ที่ใช้ชิป ATmega2560 ดังรูปที่ 2.1



รูปที่ 2.1 บอร์ดอาดูโน่ที่ใช้ในการทดลอง

2.1.1 ข้อมูลทางเทคนิค

บอร์ดอาดูโน่เป็นบอร์ดที่ใช้งานได้หลากหลาย มีราคาไม่แพงมาก แต่มีประสิทธิภาพการทำงานที่สูง และมีอัตราการใช้กำลังไฟฟ้าที่ไม่มาก ข้อมูลเบื้องต้นของบอร์ดอาดูโน่ ได้แสดงไว้ในตารางที่ 1.1

ตารางที่ 1 คุณสมบัติเบื้องต้นของบอร์ดอาดูโน่

ไมโครคอนโทรลเลอร์	ATmega2560
แรงดันที่ใช้ในการทำงาน	5 โวลต์
แรงดันอินพุต (แนะนำ)	7-12 โวลต์
แรงดันอินพุต (ขีดจำกัด)	6-20 โวลต์
Digital I/O Pins	54 (4 ขาเป็นแบบ PWM output)
ขาอินพุตแบบอนาล้อก	16 ขา
กระแสขา I/O	40 มิลลิแอมแปร์
กระแสขาแรงดัน 3.3 โวลต์	50 มิลลิแอมแปร์
ขนาดหน่วยความจำ	256 กิโลไบต์
SRAM	8 กิโลไบต์
EEPROM	4 กิโลไบต์
ความเร็ว Clock	16 เมกะเฮิรตซ์

2.2. Internet of Thing

2.2.1. เกริ่นนำถึง Internet of Thing

ระบบเครือข่ายของวัตถุเชิงกายภาพ ซึ่งฝังตัวอยู่ในอุปกรณ์ที่เราจะใช้งาน เช่น ชิพสมองกลอัจฉริยะ ถูกนำมาประยุกต์ใช้ในทาง อิเล็กทรอนิกส์ ซอฟต์แวร์ เซนเซอร์ และ การเชื่อมต่อเน็ตเวิร์ค Iot ทำให้ ออปเจ็คต์ ใช้ในการตรวจจับ และ ควบคุมได้ในระยะไกล ผ่านโครงสร้างพื้นฐานของเน็ตเวิร์ค เพิ่มโอกาสให้เราสามารถทำอะไรได้หลากหลายมากยิ่งขึ้น ระหว่าง โลกของทางกายภาพ และ ระบบฐานข้อมูลของคอมพิวเตอร์ เป็นผลให้ มีการทำงานมีประสิทธิภาพและความแม่นยำ และ เกิดผลประโยชน์ทางด้านเศรษฐกิจด้วย ในแต่ละออปเจ็คต์ ได้รับการยอมรับว่ามีความเป็นอันหนึ่งอันเดียวกันในแง่ที่มันสามารถฝังตัวในระบบคอมพิวเตอร์ได้ แต่มันก็ยังสามารถ ทำงานระหว่างโครงสร้างพื้นฐานของคอมพิวเตอร์ที่มีอยู่ได้ จากการประมาณพบว่า Iot ประกอบด้วย 5 หมื่นล้าน ออปเจ็คต์ในปี 2020.

2.2.2. ประวัติของ Internet of Thing

Iot ได้ถูกคิดค้นโดย ผู้ประกอบการชาวอังกฤษ เคลวิน แอสทรอน ในปี 1999 ซึ่ง Iot ได้รับการคาดหวังในยุคนั้นว่าจะทำให้การเชื่อมต่อกับ อุปกรณ์ ระบบ และ บริการ แบบขั้นสูงได้ ซึ่งเราเรียกว่า machine-to-machine communications (M2M) ซึ่งครอบคลุมถึง ความหลากหลายของ โปรโตคอล , โดเมน และ แอพลลิเคชั่น การเชื่อมต่อระหว่างอุปกรณ์ที่ได้รับการฝังตัวเหล่านี้ (รวมถึง smart object ด้วย) ได้ถูกคาดหวังว่า มันจะเป็นการนำเครื่องจักรมาใช้แทนคนในการทำงาน นอกจากนี้ระบบฝังกลอัจฉริยะแบบขั้นสูง ในถูกนำมาประยุกต์ใช้งานจริงด้วย เช่น Smart Grid , Smart Cities

ในปี 2014 วิสัยทัศน์ของ Iot ได้รับการพัฒนา อันเนื่องมาจากการบรรจบกันของหลากหลาสายเทคโนโลยี , ขอบเขตจากการเชื่อต่อแบบไร้สายกับอินเตอร์เน็ต ระบบฝังตัว to MEMS (micro-electromechanical systems) ในแง่เชิงพาณิชย์ของระบบฝังตัว เช่น ระบบไร้สายของเซ็นเซอร์ , ระบบควบคุม, automaton (รวมไปถึงระบบอัตโนมัติในบ้านและสิ่งปลูกสร้างด้วย) , และสิ่งอื่นๆ ที่สนับสนุน Iot

คอมพิวเตอร์ในศตวรรษที่ 21 สถานที่มีการพบปะเชิงวิชาการ เช่น UbiComp และ PerCom ได้ผลิตรุ่นชั่วคราวของ Iot ในปี 1994 Reza Raji ได้อธิบายแนวคิดที่ IEEE Spectrum as (การเคลื่อนที่) ของ แพ็คเกจขนาดเล็กของข้อมูล to a large set of nodes, เป็นการรวม และ การทำให้อุปกรณ์ทำงานได้ด้วยตัวมันเอง (automation) จาก เครื่องใช้ภายในบ้าน ระหว่างปี 1993 และ 1996 หลายบริษัทได้เสนอ solutions เหมือน Microsoft's at Work or Novell's NEST. อย่างไรก็ตาม ปี 1999 ฟิลด์ของระบบ Iot ได้แพร่ขยายเป็นที่รู้จักและใช้งานมากขึ้น Bill Joy คิดค้นการติดต่อแบบอุปกรณ์ถึงอุปกรณ์ (Device to Device (D2D) communication) ซึ่งเป็นส่วนหนึ่งของ "Six Webs" framework ซึ่งได้ผ่านการนำเสนอที่เมืองดาวอส ปี 1999

แนวคิดของ the Internet of Things เพิ่งได้รับความนิยมในปี 1999 , ผ่าน Auto-ID Center ที่ MIT และ สัมพันธ์กับ สิทธิบัตรการวิเคราะห์ทางตลาด การระบุความถี่วิทยุ [Radio-frequency identification (RFID)] ได้ถูกค้นพบโดย Kevin Ashton (หนึ่งในผู้คิดค้น Auto-ID Center) ซึ่งมีมาก่อน Internet of Things ณ เวลานั้น

ถ้าออปเจ็คต์และผู้คนมาอยู่รวมกันในชีวิตประจำวัน พร้อมกับตัวบ่งชี้ , คอมพิวเตอร์ สามารถบริหารจัดการและคิดค้นได้ นอกจากนี้ ยังรวมไปถึงสิ่งที่อยู่ในขอบข่ายของ Iot เช่น barcodes, QR codes และ digital watermarking.

2.2.3. การประยุกต์ใช้งาน

การวิจัย ABI ได้ประมาณการณ์ว่า อุปกรณ์มากกว่า 30,000 ล้านตัว จะเชื่อมต่อกันแบบไร้สายแบบ IOT ได้ในปี 2020. จากการสำรวจและศึกษา ประสบผลสำเร็จ โดย Pew Research Internet Project ส่วนใหญ่ของผู้ที่เชี่ยวชาญทางด้านเทคโนโลยีผู้ใช้อินเตอร์เน็ตมี 83% --เห็นด้วยกับความคิดที่เกี่ยวกับ Internet/Cloud of Things จะเกิดผลกระทบอย่างกว้างขวางและมีประโยชน์ ในปี 2025. Iot จะประกอบไปด้วยอุปกรณ์จำนวนมากที่เชื่อมต่ออินเตอร์เน็ต

ด้วยความช่วยเหลือเพื่อที่จะคิดค้นนวัตกรรมใหม่ๆออกมา (emerging) ในปีงบประมาณ 2015 รัฐบาลอังกฤษ ได้อนุมัติเงินจำนวน £40,000,000 มาใช้ในการวิจัย Internet of Things Chancellor of the Exchequer George Osborne, จัดตั้ง Internet of Thing ให้เป็นอีกขั้นนหนึ่งของ ความก้าวหน้าด้านข้อมูลข่าวสาร และอ้างถึง การเชื่อมต่อระหว่างกันของทุกสิ่งทุกอย่าง จาก การขนส่งภายในตัวเมือง และ เครื่องมือทางการแพทย์ และ เครื่องใช้ภายในบ้าน

การรวมกับอินเตอร์เน็ต ส่อความว่า อุปกรณ์จะใช้ IP Address ในการระบุตัวตนของอุปกรณ์ อย่างไรก็ตาม เนื่องจาก ข้อจำกัดของพื้นที่สำหรับ แอดเดรส IPv4 (which allows for 4.3 billion unique addresses) , ออปเจ็คใน Iot จึงจำเป็นต้องใช้ IPv6 ในการติดต่อกัน ซึ่งต้องใช้ พื้นที่ในการจัดเก็บ แอดเดรสขนาดใหญ่มาก ซึ่ง ออปเจ็คใน Iot จะไม่ได้มีแค่ความสามารถในการตรวจจับได้อย่างเดียว แต่ยังให้ ความสามารถในการกระตุ้นได้ด้วย (ยกตัวอย่ง เช่น ควบคุมการล็อกของกุญแจ และหลอดไฟ ผ่านทางอินเตอร์เน็ต)

ในอนาคตข้างหน้าของ Iot เป็นไปไม่ได้เลย หากปราศจาก การสนับสนุนของ IPv6 ดังนั้น การนำ ipv6 มาใช้อย่างเป็นทางการทั่วโลกในปีอันใกล้นี้ เป็นการตอกย้ำถึงความสำเร็จในการพัฒนา Iot ในอนาคต

2.3. Wi-Fi

2.3.1. เกริ่นนำถึง Wi-Fi

Wi-Fi คือ เทคโนโลยีที่ได้รับความนิยมที่ช่วยให้อุปกรณ์อิเล็กทรอนิกส์ในการแลกเปลี่ยนข้อมูลหรือการเชื่อมต่ออินเทอร์เน็ตแบบไร้สายโดยใช้คลื่นวิทยุ คำๆนี้เป็นเครื่องหมายการค้าของ Wi-Fi Alliance ที่ได้ให้คำนิยามของวายฟายว่าหมายถึง "ชุดผลิตภัณฑ์ใดๆ ที่สามารถทำงานได้ตามมาตรฐานเครือข่ายคอมพิวเตอร์แบบไร้สาย (แลนไร้สาย) ซึ่งอยู่บนมาตรฐาน IEEE 802.11" อย่างไรก็ตามเนื่องจากแลนไร้สายที่ทันสมัยส่วนใหญ่จะขึ้นอยู่กับมาตรฐานเหล่านี้ คำว่า "วายฟาย" จึงถูกนำมาใช้ในภาษาอังกฤษทั่วไปโดยเป็นคำพ้องสำหรับ "แลนไร้สาย" เดิมทีวายฟายออกแบบมาใช้สำหรับอุปกรณ์พกพาต่างๆ และใช้เครือข่าย LAN เท่านั้น แต่ปัจจุบันนิยมใช้วายฟายเพื่อต่อกับอินเทอร์เน็ต โดยอุปกรณ์พกพาต่างๆ เช่นคอมพิวเตอร์ส่วนบุคคล เครื่องเล่นเกมส์ โทรศัพท์สมาร์ทโฟน แท็บเล็ต กล้องดิจิทัลและเครื่องเสียงดิจิทัล สามารถเชื่อมต่อกับอินเทอร์เน็ตได้ผ่านอุปกรณ์ที่เรียกว่าแอคเซสพอยต์ หรือฮอตสปอต และบริเวณที่ระยะทำการของแอคเซสพอยต์ครอบคลุมอยู่ที่ประมาณ 20 ม.ในอาคาร แต่ระยะนี้จะไกลกว่าถ้าเป็นที่โล่งแจ้ง

Wi-Fi มีความปลอดภัยน้อยกว่าการเชื่อมต่อแบบมีสาย (เช่น Ethernet) เพราะผู้บุกรุกไม่จำเป็นต้องเชื่อมต่อทางกายภาพ หน้าเว็บที่ใช้ SSL มีความปลอดภัย แต่การใช้อินเทอร์เน็ตที่ไม่ได้เข้ารหัสสามารถจะตรวจพบโดยผู้บุกรุก ด้วยเหตุนี้ Wi-Fi ได้พัฒนาเทคโนโลยีการเข้ารหัสต่างๆมากมาย WEP เป็นการเข้ารหัสรุ่นแรกๆ ถูกพิสูจน์แล้วว่าง่ายต่อการบุกรุก โพรโทคอลที่มีคุณภาพสูงกว่าได้แก่ WPA, WPA2 มีเพิ่มขึ้นมาในภายหลัง คุณลักษณะตัวเลือกที่เพิ่มเข้ามาในปี 2007 ที่เรียกว่า Wi-Fi Protected Setup (WPS) มีข้อบกพร่องร้ายแรงที่ยอมให้ผู้โจมตีสามารถกู้คืนรหัสผ่านของเราเตอร์ได้ Wi-Fi Alliance ได้ทำการปรับปรุงแผนการทดสอบและโปรแกรมการรับรองตั้งแต่นั้นเป็นต้นมาเพื่อให้แน่ใจว่าอุปกรณ์ที่ได้รับการรับรองใหม่ทั้งหมดสามารถต่อต้านการโจมตีได้

รูปที่ 2.2 สัญลักษณ์ของ Wi-Fi

2.3.2. ประวัติของ Wi-Fi

วายฟาย หรือ เทคโนโลยีเครือข่ายแบบไร้สาย มาตรฐาน IEEE 802.11 ถือกำเนิดขึ้นในปี ค.ศ. 1997 จัดตั้งโดยองค์การไอทริปเปิ้ลอี (สถาบันวิศวกรรมทางด้านไฟฟ้าและอิเล็กโทรนิคส์) มีความเร็ว 1 Mbps ในยุคเริ่มแรกนั้นให้ประสิทธิภาพการทำงานที่ค่อนข้างต่ำ ทั้งไม่มีการรับรองคุณภาพของการ

ให้บริการที่เรียกว่า QoS (Quality of Service) และมาตรฐานความปลอดภัยต่ำ จากนั้นทาง IEEE จึงจัดตั้งคณะทำงานขึ้นมาปรับปรุงหลายกลุ่มด้วยกัน โดยที่กลุ่มที่มีผลงานเป็นที่น่าพอใจและได้รับการยอมรับอย่างเป็นทางการว่า ได้มาตรฐานได้แก่กลุ่ม 802.11a, 802.11b และ 802.11g

เทคโนโลยี 802.11 มีต้นกำเนิดในปี ค.ศ. 1985 กำหนดขึ้นโดยคณะกรรมการการสื่อสารแห่งชาติสหรัฐอเมริกา(อังกฤษ: U.S. Federal Communications Commission) หรือ FCC ที่ประกาศช่วงความถี่สำหรับกิจการด้านอุตสาหกรรม วิทยาศาสตร์และการแพทย์ (ISM) สำหรับการใช้งานที่ไม่ต้องมีใบอนุญาต

ในปี ค.ศ. 1991 บริษัท เอ็นซีอาร์/เอทีแอนด์ที (ตอนนี้เป็น Alcatel-Lucent และ LSI คอร์ปอเรชั่น) ได้สร้างชุดตั้งต้นของ 802.11 ในเมือง Nieuwegein, เนเธอร์แลนด์ ตอนแรกนักประดิษฐ์ตั้งใจจะใช้เทคโนโลยีนี้สำหรับระบบเก็บเงิน ผลิตภัณฑ์ไร้สายตัวแรกที่ถูกนำออกสู่ตลาดอยู่ภายใต้ชื่อ WaveLAN ที่มีอัตราข้อมูลดิบของ 1 Mbit/s และ 2 Mbit/s

วิก เฮย์สผู้เป็นประธานของ IEEE 802.11 เป็นเวลา 10 ปีและถูกเรียกว่า "บิดาแห่ง Wi-Fi" ได้มีส่วนร่วมในการออกแบบ 802.11b และ 802.11a มาตรฐานเริ่มต้นภายใน IEEE.

นักวิทยุ-ดาราศาสตร์ชาวออสเตรเลียชื่อ จอห์น โอ ซัลลิแวนได้พัฒนาสิทธิบัตรที่สำคัญที่ใช้ใน Wi-Fi ที่เป็นผลพลอยได้ในโครงการวิจัย CSIRO "การทดลองที่ล้มเหลวในการตรวจสอบหาการระเบิดหลุมดำขนาดเล็กที่มีขนาดเท่าหนึ่งอนุภาคอะตอม" ในปี ค.ศ. 1992 และ ปี ค.ศ. 1996 องค์กรของออสเตรเลียชื่อ CSIRO (the Australian Commonwealth Scientific and Industrial Research Organization) ได้รับสิทธิบัตรสำหรับวิธีการที่ในภายหลังถูกใช้ใน Wi-Fi ในการ "กำจัดรอยเปื้อน"ของสัญญาณ.

ในปี ค.ศ. 1999, Wi-Fi Alliance ถูกจัดตั้งขึ้นเป็นสมาคมการค้าเจ้าของเครื่องหมายการค้า Wi-Fi ซึ่งผลิตภัณฑ์ส่วนใหญ่ที่ใช้ Wi-Fi จะมีเครื่องหมายนี้

ในเดือนเมษายน ค.ศ. 2009, 14 บริษัทเทคโนโลยีตกลงที่จะจ่าย 250 ล้าน$ ให้กับ CSIRO สำหรับการละเมิดสิทธิบัตรของ CSIRO สิ่งนี้ทำให้ Wi-Fi กลายเป็นสิ่งประดิษฐ์ ของออสเตรเลีย แม้ว่าจะเป็นเรื่องของการโต้เถียงกันอยู่ ในปี ค.ศ. 2012 CSIRO ยังชนะคดีและจะได้รับเงินชดเชยเพิ่มเติม 220 ล้าน$ สำหรับการละเมิดสิทธิบัตร Wi-Fi กับบริษัทระดับโลกในประเทศสหรัฐอเมริกา ซึ่งจะต้องจ่ายค่าลิขสิทธิ์แก่ CSIRO ที่คาดว่าจะมีมูลค่าเพิ่มอีก $ 1 พันล้านดอลลาร์

2.3.3. ลักษณะการเชื่อมต่อของอุปกรณ์

วายฟาย ได้กำหนดลักษณะการเชื่อมต่อของอุปกรณ์ภายในเครือข่ายแลน ไว้ 2 ลักษณะคือโหมด Infrastructure และโหมด Ad-Hoc หรือ Peer-to-Peer

2.2.3.1. โหมด Infrastructure

โดยทั่วไปแล้วอุปกรณ์ในเครือข่ายวายฟาย จะเชื่อมต่อกันในลักษณะของโหมด Infrastructure ซึ่งเป็นโหมดที่อนุญาตให้อุปกรณ์ภายใน LAN สามารถเชื่อมต่อกับเครือข่ายอื่นได้ ในโหมด Infrastructure นี้จะประกอบไปด้วยอุปกรณ์ 2 ประเภทได้แก่ สถานีผู้ใช้ (Client Station) ซึ่งก็คือ อุปกรณ์คอมพิวเตอร์ (Desktop, แล็ปท็อป, หรือ PDA ต่างๆ) ที่มีอุปกรณ์ Client Adapter เพื่อใช้รับส่งข้อมูลผ่านวายฟาย และสถานีแม่ข่าย (Access Point) ซึ่งทำหน้าที่ต่อเชื่อมสถานีผู้ใช้เข้ากับเครือข่ายอื่น (ซึ่งโดยปกติจะเป็นเครือข่าย IEEE 802.3 Ethernet LAN) การทำงานในโหมด Infrastructure มีพื้นฐานมาจากระบบเครือข่ายโทรศัพท์มือถือ กล่าวคือสถานีผู้ใช้จะสามารถรับส่งข้อมูลโดยตรงกับสถานีแม่ข่ายที่ให้บริการ แก่สถานีผู้ใช้นั้นอยู่เท่านั้น ส่วนสถานีแม่ข่ายจะทำหน้าที่ส่งต่อ (forward) ข้อมูลที่ได้รับจากสถานีผู้ใช้ไปยังจุดหมายปลายทางหรือส่งต่อข้อมูลที่ได้ รับจากเครือข่ายอื่นมายังสถานีผู้ใช้

2.2.3.2. โหมด Ad-Hoc หรือ Peer-to-Peer

เครือข่ายวายฟาย.ในโหมด Ad-Hoc หรือ Peer-to-Peer เป็นเครือข่ายที่ปิดคือไม่มีสถานีแม่ข่าย และไม่มีการเชื่อมต่อกับเครือข่ายอื่น บริเวณของเครือข่ายวายฟายในโหมด Ad-Hoc จะเรียกว่า Independent Basic Service Set (IBSS) ซึ่งสถานีผู้ใช้หนึ่งสามารถติดต่อสื่อสารข้อมูลกับสถานีผู้ใช้อื่นๆ ในเขต IBSS เดียวกันได้โดยตรงโดยไม่ต้องผ่านสถานีแม่ข่าย แต่สถานีผู้ใช้จะไม่สามารถรับส่งข้อมูลกับเครือข่ายอื่นๆได้

2.3.4. กลไกรักษาความปลอดภัย

วายฟายได้กำหนดให้มีทางเลือกสำหรับสร้างความปลอดภัยให้กับเครือข่ายแลนแบบไร้สาย ด้วยกลไกซึ่งมีชื่อเรียกว่า WEP (Wired Equivalent Privacy) ซึ่งออกแบบมาเพื่อเพิ่มความปลอดภัยกับเครือข่าย LAN แบบไร้สายให้ใกล้เคียงกับความปลอดภัยของเครือข่ายแบบที่ใช้สายนำสัญญาณ (IEEE 802.3 Ethernet) บทบาทของ WEP แบ่งเป็น 2 ส่วนหลักๆ คือ การเข้ารหัสข้อมูล (Encryption) และการตรวจสอบผู้ใช้ (Authentication)

2.3.5. การเข้าและถอดรหัสข้อมูล

การเข้าและถอดรหัสข้อมูล (WEP Encryption/Decryption) ใช้หลักการในการเข้าและถอดรหัสข้อมูลที่เป็นแบบ symmetrical (นั่นคือรหัสที่ใช้ในการเข้ารหัสข้อมูลจะเป็นตัวเดียวกันกับรหัสที่ใช้ สำหรับการถอดรหัสข้อมูล)

2.3.5.1. การทำงานของการเข้ารหัสข้อมูลในกลไก WEP Encryption

1. Key ขนาด 64 หรือ 128 บิต สร้างขึ้นโดยการนำเอารหัสลับซึ่งมีความยาว 40 หรือ 104 บิต มาต่อรวมกับข้อความเริ่มต้น IV (Initialization Vector) ขนาด 24 บิตที่กำหนดแบบสุ่มขึ้นมา

2. Integrity Check Value (ICV) ขนาด 32 บิต สร้างขึ้นโดยการคำนวณค่า CRC-32 (32-bit Cyclic Redundant Check) จากข้อมูลดิบที่จะส่งออกไป (ICV) ซึ่งจะนำไปต่อรวมกับข้อมูลดิบ มีไว้สำหรับตรวจสอบความถูกต้องของข้อมูลหลังจากการถอดรหัสแล้ว)

3. ข้อความที่มีความสุ่ม (Key Stream) ขนาดเท่ากับความยาวของข้อมูลดิบที่จะส่งกับอีก 32 บิต (ซึ่งเป็นความยาวของ ICV) สร้างขึ้นโดยหน่วยสร้างข้อความที่มีความสุ่มหรือ PRNG (Pseudo-Random Number Generator) ที่มีชื่อเรียกว่า RC4 ซึ่งจะใช้ Key ที่กล่าวมาข้างต้นเป็น Input (หรือ Seed) ซึ่ง PRNG จะสร้างข้อความสุ่มที่แตกต่างกันสำหรับ Seed แต่ละค่าที่ใช้

4. ข้อความที่ได้รับการเข้ารหัส (Ciphertext) สร้างขึ้นโดยการนำเอา ICV ต่อกับข้อมูลดิบแล้วทำการ XOR แบบบิตต่อบิตกับข้อความสุ่ม (Key Stream) ซึ่ง PRNG ได้สร้างขึ้น

5. สัญญาณที่จะส่งออกไปคือ ICV และข้อความที่ได้รับการเข้ารหัส (Ciphertext)

2.3.5.2. การทำงานของการเข้ารหัสข้อมูลในกลไก WEP Decryption

1. Key ขนาด 64 หรือ 128 บิต สร้างขึ้นโดยการนำเอารหัสลับซึ่งมีความยาว 40 หรือ 104 บิต (ซึ่งเป็นรหัสลับเดียวกับที่ใช้ในการเข้ารหัสข้อมูล) มาต่อรวมกับ IV ที่ส่งมากับสัญญาณที่ได้รับ

2. PRNG สร้างข้อความสุ่ม (Key Stream) ที่มีขนาดเท่ากับความยาวของข้อความที่ได้รับการเข้ารหัสและถูกส่งมา โดยใช้ Key ที่กล่าวมาข้างต้นเป็น Input

3. ข้อมูลดิบและ ICV ได้รับการถอดรหัสโดยการนำเอาข้อความที่ได้รับมา XOR แบบบิตต่อบิตกับข้อความสุ่ม (Key Stream) ซึ่ง PRNG ได้สร้างขึ้น

4. สร้าง ICV' โดยการคำนวณค่า CRC-32 จากข้อมูลดิบที่ถอดรหัสแล้วเพื่อนำมาเปรียบเทียบกับค่า ICV ที่ส่งมา หากค่าทั้งสองตรงกัน (ICV' = ICV) แสดงว่าการถอดรหัสถูกต้องและผู้ที่ส่งมาได้รับอนุญาต (มีรหัสลับของเครือข่าย) แต่หากค่าทั้งสองไม่ตรงกันแสดงว่าการถอดรหัสไม่ถูกต้องหรือผู้ที่ส่งมาไม่ได้รับอนุญาต

2.3.6. การตรวจสอบผู้ใช้

สำหรับเครือข่ายวายฟาย ผู้ใช้ (เครื่องลูกข่าย) จะมีสิทธิในการรับส่งสัญญาณข้อมูลในเครือข่ายได้ก็ต่อเมื่อได้รับการตรวจสอบ แล้วได้รับอนุญาต ซึ่งมาตรฐานวายฟายได้กำหนดให้มีกลไกสำหรับการตรวจสอบผู้ใช้ (Authentication) ใน 2 ลักษณะคือ Open System Authentication และ Shared Key Authentication ซึ่งเป็นดังต่อไปนี้

2.3.6.1. Open System Authentication

การตรวจสอบผู้ใช้ในลักษณะ นี้เป็นทางเลือกแบบ default ที่กำหนดไว้ในมาตรฐาน IEEE 802.11 ในการตรวจสอบแบบนี้จะไม่ตรวจสอบรหัสลับจากผู้ใช้ ซึ่งอาจกล่าวได้ว่าเป็นการอนุญาตให้ผู้ใช้

ใดๆ ก็ได้สามารถเข้ามารับส่งสัญญาณในเครือข่ายนั่นเอง แต่อย่างไรก็ตามในการตรวจสอบแบบนี้อุปกรณ์ที่ทำหน้าที่เป็นสถานีแม่ข่ายไม่จำเป็นต้องอนุญาตให้สถานีผู้ใช้เข้ามาใช้เครือข่ายได้เสมอไป ในกรณีนี้บทบาทของ WEP จึงเหลือแต่เพียงการเข้ารหัสข้อมูลเท่านั้น กลไกการตรวจสอบแบบ open system authentication มีขั้นตอนการทำงานดังต่อไปนี้

1. สถานีที่ต้องการจะเข้ามาร่วมใช้เครือข่ายจะส่งข้อความซึ่งไม่เข้ารหัสเพื่อขอรับการตรวจสอบ (Authentication Request Frame) ไปยังอุปกรณ์ที่ทำหน้าที่เป็นสถานีแม่ข่าย โดยในข้อความดังกล่าวจะมีการแสดงความจำนงเพื่อรับการตรวจสอบแบบ open system

2. อุปกรณ์ที่ทำหน้าที่เป็นสถานีแม่ข่ายโต้ตอบด้วยข้อความที่แสดงถึงการตอบรับหรือปฏิเสธ Request ดังกล่าว

2.3.6.2. Shared Key Authentication

การตรวจสอบผู้ใช้แบบ shared key authentication จะอนุญาตให้สถานีผู้ใช้ซึ่งมีรหัสลับของเครือข่ายนี้เท่านั้นที่สามารถเข้า มารับส่งสัญญาณกับอุปกรณ์ที่ทำหน้าที่เป็นสถานีแม่ข่ายได้ โดยมีการใช้เทคนิคการถามตอบที่ใช้กันทั่วไปผนวกกับการเข้ารหัสด้วย WEP เป็นกลไกสำหรับการตรวจสอบ (ดังนั้นการตรวจสอบแบบนี้จะทำได้ก็ต่อเมื่อมีการ Enable การเข้ารหัสด้วย WEP) กลไกการตรวจสอบดังกล่าวมีขั้นตอนการทำงานดังต่อไปนี้

1. สถานีผู้ใช้ที่ต้องการจะเข้ามาร่วมใช้เครือข่ายจะส่งข้อความซึ่งไม่เข้ารหัสเพื่อขอรับการตรวจสอบ (Authentication Request Frame) ไปยังอุปกรณ์ที่ทำหน้าที่เป็นสถานีแม่ข่าย โดยในข้อความดังกล่าวจะมีการแสดงความจำนงเพื่อรับการตรวจสอบแบบ shared key

2. หากสถานีแม่ข่ายต้องการตอบรับ Request ดังกล่าว จะมีการส่งข้อความที่แสดงถึงการตอบรับและคำถาม (challenge text) มายังเครื่องลูกข่าย ซึ่ง challenge text ดังกล่าวมีขนาด 128 ไบต์และสุ่มขึ้นมา (โดยอาศัย PRNG) หากอุปกรณ์แม่ข่ายไม่ต้องการตอบรับ Request ดังกล่าว จะมีการส่งข้อความที่แสดงถึงการไม่ตอบรับ ซึ่งเป็นการสิ้นสุดของการตรวจสอบครั้งนี้

3. หากมีการตอบรับจากสถานีแม่ข่าย สถานีผู้ใช้ที่ขอรับการตรวจสอบจะทำการเข้ารหัสข้อความคำถามที่ส่งมาโดยใช้รหัสลับของเครือข่ายแล้วส่งกลับไปยังสถานีแม่ข่าย

4. สถานีแม่ข่ายทำการถอดรหัสข้อความที่ตอบกลับมาโดยใช้รหัสลับของเครือข่าย หลังจากถอดรหัสแล้วหากข้อความที่ตอบกลับมาตรงกับข้อความคำถาม (challenge text) ที่ส่งไป สถานีแม่ข่ายจะส่งข้อความที่แสดงถึงการอนุญาตให้สถานีผู้ใช้นี้เข้าใช้เครือข่ายได้ แต่หากข้อความที่ตอบกลับมาไม่ตรงกับข้อความคำถาม สถานีแม่ข่ายจะโต้ตอบด้วยข้อความที่แสดงถึงการไม่อนุญาต

2.3.7. ข้อดี

Wi-Fi ช่วยให้การใช้งานของเครือข่ายท้องถิ่น (LANs) มีราคาถูกลง นอกจากนี้ยังมีบริเวณที่ไม่สามารถวางสายเคเบิลได้ เช่น พื้นที่กลางแจ้งและอาคารประวัติศาสตร์ เราจะสามารถให้บริการ LAN แบบไร้สายได้ ผู้ผลิตสามารถสร้างอแดปเตอร์เครือข่ายไร้สายในแลปท็อปได้ ส่วนใหญ่ราคาของชิปเซ็ตสำหรับ Wi-Fi ยังคงลดลงเรื่อยๆ ทำให้มีตัวเลือกที่เป็นเครือข่ายประหยัดรวมอยู่ในอุปกรณ์ ต่างๆได้มากขึ้น หลายๆแบรนด์ในการแข่งขันที่แตกต่างกันของ AP กับตัวเชื่อมต่อเครื่องลูกข่ายสามารถประสานทำงานกันได้ดีในระดับพื้นฐานของการให้บริการ ผลิตภัณฑ์ทั้งหลายที่ "รองรับ Wi-Fi" ที่ออกโดย Wi-Fi Alliance สามารถเข้ากันได้แบบย้อนหลัง ซึ่งแตกต่างจากโทรศัพท์มือถือ ที่อุปกรณ์ที่มีมาตรฐาน Wi-Fi ใดๆ สามารถที่จะทำงานร่วมกันได้ที่ใดๆก็ได้ในโลกนี้

2.3.8. พิสัย

เครือข่าย Wi-Fi มีพิสัยจำกัด AP ไร้สายโดยทั่วไปที่ใช้ 802.11b หรือ 802.11g กับเสาอากาศอาจมีพิสัยทำการที่ 35 เมตร (120 ฟุต) ในบ้านและ 100 เมตร (300 ฟุต)กลางแจ้ง แต่ IEEE 802.11n สามารถทำงานในพิสัยที่มากกว่าสองเท่า พิสัยนี้ยังขึ้นอยู่กับช่วงความถี่ Wi-Fi ในบล็อกความถี่ 2.4 GHz มีพิสัยทำการที่ดีกว่า Wi-Fi ในบล็อกความถี่ 5 GHz ซึ่งถูกใช้โดย 802.11a และ 802.11n ในเราเตอร์ไร้สายที่มีเสาอากาศถอดออกได้ มันเป็นไปได้ที่จะเพิ่มพิสัยโดยการติดตั้งเสาอากาศที่มีการเพิ่มเกนสูงขึ้นในทิศทางที่เฉพาะเจาะจง พิสัยกลางแจ้งสามารถเพิ่มไปได้หลายกิโลเมตรโดยการใช้เสาอากาศแบบทิศทางเกนสูงที่ เราเตอร์และอุปกรณ์ระยะไกล

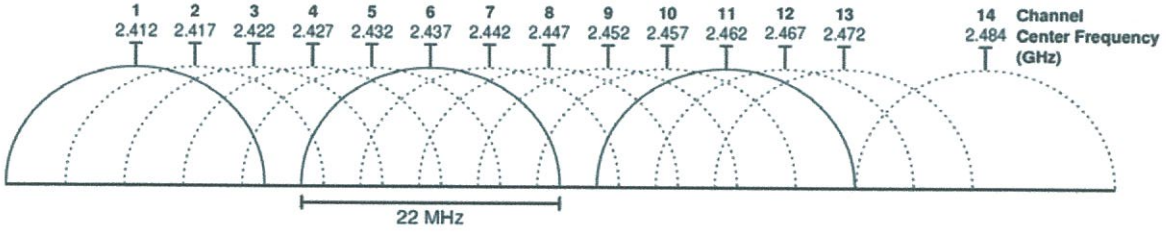
เพื่อเข้าถึงความต้องการสำหรับการใช้งานเครือข่ายไร้สาย Wi-Fi จึงมีการใช้พลังงานค่อนข้างสูงเมื่อเทียบกับมาตรฐานอื่นๆ เช่น บลูทูธ (ออกแบบมาเพื่อรองรับการใช้งาน PAN แบบไร้สาย) ให้พิสัยการกระจายคลื่นที่สั้นมาก ระหว่าง 1 ถึง 100 เมตร และโดยทั่วไปก็มีการใช้พลังงานที่ต่ำกว่า เทคโนโลยีพลังงานต่ำอื่นๆ เช่น ZigBee มีพิสัยค่อนข้างไกล แต่อัตรารับส่งข้อมูลต่ำกว่ามาก การใช้พลังงานที่สูงของ Wi-Fi ทำให้แบตเตอรี่ในโทรศัพท์มือถือหมดเร็ว

พิสัยของ Wi-Fi ในทางปฏิบัติขึ้นอยู่กับขอบเขตการใช้อุปกรณ์เคลื่อนที่เพื่อการใช้งาน เช่นเครื่องตรวจสอบสินค้าคงคลังในคลังสินค้า หรือในพื้นที่ค้าปลีก อุปกรณ์อ่านบาร์โค้ดที่เคาน์เตอร์เช็คเอาท์ หรือสถานีรับ/ส่งสินค้า การใช้ Wi-Fi พิสัยกว้างกับอุปกรณ์เคลื่อนที่เร็ว จะทำได้จำกัด เช่น การใช้งานในขณะที่รถยนต์เคลื่อนย้ายจากฮอทสปอตหนึ่งไปยังอีกฮอทสปอตหนึ่ง เทคโนโลยีไร้สายอื่นๆน่าจะมีความเหมาะสมมากกว่าสำหรับการสื่อสารกับยานพาหนะเคลื่อนที่เร็ว

2.3.9. ข้อจำกัด

การกำหนดคลื่นความถี่และข้อจำกัดในการดำเนินงานไม่สม่ำเสมอทั่วโลก เช่นที่ออสเตรเลียและยุโรป ได้อนุญาตให้มีอีกสองแชนแนลเพิ่มเติมนอกเหนือจากที่ได้รับอนุญาตในสหรัฐอเมริกาสำหรับแถบ

ความถี่ 2.4 GHz (แชนแนล 1 ถึง 13 เทียบกับ 1 ถึง 11) ในขณะที่ประเทศญี่ปุ่นมีมากขึ้นอีกหนึ่ง (1 ถึง 14)



รูปที่ 2.3 ภาพแสดงช่องความถี่ของ Wi-Fi ในแถบความถี่ 2.4 GHz

สัญญาณ Wi-Fi กินพื้นที่ห้าแชนแนลในแถบความถี่ 2.4 GHz ตามภาพประกอบ ตัวเลขของแชนแนลใดๆสองแชแนลที่แตกต่างกันมากกว่าหรือเท่ากับ 5 แชแนล เช่นแชนแนล 2 และ 7 จะใช้คลื่นความถี่ที่ไม่ทับซ้อนกัน เพราะฉะนั้น ความเชื่อเดิมๆที่ว่า แชนแนลที่ 1, 6 , และ 11 เท่านั้นที่เป็นแชนแนลที่ไม่ทับซ้อนกันจึงไม่ถูกต้อง แชนแนลที่ 1 , 6, และ 11 เป็นกลุ่มของสามแชนแนลที่ไม่ทับซ้อนกันในทวีปอเมริกาเหนือและสหราชอาณาจักร ในยุโรปและญี่ปุ่นจะแนะนำให้ใช้ ช่อง 1, 5 , 9, และ 13 สำหรับ 802.11g และ 802.11n

ค่าการส่งพลังงานที่เรียกว่า Equivalent isotropically radiated power (EIRP) ในสหภาพยุโรปจะถูกจำกัดที่ 20 dBm (100 mW)

ปัจจุบัน 802.11n ปกติที่ 'เร็วที่สุด' จะใช้สเปกตรัมวิทยุ/แบนด์วิดธ์เป็นสองเท่า (40 MHz) เมื่อเทียบกับ 802.11a หรือ 802.11g (20 MHz) ซึ่งหมายความว่า จะมี เพียงหนึ่งเครือข่าย 802.11n เท่านั้นในแถบความถี่ 2.4 GHz ณ สถานที่ที่กำหนด โดยไม่มีการรบกวนไปยัง/จากการจราจร WLAN อื่น ๆ นอกจากนี้ 802.11n ยังสามารถตั้งค่าการใช้แบนด์วิดธ์ที่ 20 MHz เพียงเพื่อที่จะป้องกันการรบกวนในชุมชนหนาแน่น

2.3.10. ความเสี่ยงด้านความปลอดภัยของข้อมูล

มาตรฐานการเข้ารหัสแบบไร้สายที่พบมากที่สุดคือ Wired Equivalent Privacy (WEP) พบว่าเปราะบางง่ายแม้ว่าจะคอนฟิคอย่างถูกต้องก็ตาม การเข้ารหัส Wi-Fi Protected Access (WPA และ WPA2) ซึ่งมีอยู่ในอุปกรณ์ในปี 2003 มีวัตถุประสงค์เพื่อแก้ปัญหานี้ Wi-Fi AP โดยปกติจะเริ่มต้นเป็นโหมดไม่เข้ารหัส (เปิด) มือใหม่จะได้ประโยชน์จากอุปกรณ์ที่กำหนดค่าเป็นศูนย์ที่ทำงานตอนแกะกล่อง แต่การเริ่มต้นนี้ไม่ได้ช่วยการรักษาความปลอดภัยไร้สายใดๆ แต่เปิดให้เชื่อมต่อไร้สายเข้ากับ LAN ในการเปิดการรักษาความปลอดภัย ผู้ใช้ต้องคอนฟิคอุปกรณ์ที่มักจะผ่านทางส่วนติดต่อผู้ใช้แบบกราฟิกซอฟต์แวร์ (GUI) บนเครือข่าย Wi-Fi ที่ไม่ได้เข้ารหัส อุปกรณ์ที่กำลังเชื่อมต่อ สามารถตรวจสอบและ

บันทึกข้อมูล (รวมถึงข้อมูลส่วนบุคคล)ได้ เครือข่ายดังกล่าวสามารถจะได้รับการป้องกันความปลอดภัย โดยการใช้วิธีการอื่น เช่น VPN หรือ Hypertext Transfer Protocol (HTTPS) over Transport Layer Security ที่ปลอดภัยเท่านั้น

2.3.11. การรบกวน

การเชื่อมต่อ Wi-Fi สามารถจะหยุดชะงักหรืออินเทอร์เน็ตมีความเร็วลดลงอันเนื่องมาจากอุปกรณ์อื่นๆในพื้นที่เดียวกัน หลายๆ AP ที่ใช้มาตรฐาน 802.11b และ 802.11g ที่ 2.4 GHz มีค่า default ในการเริ่มต้นที่เป็นแชนแนลเดียวกัน นำไปสู่ความแออัดในบางแชนแนล Wi-Fi ขยะหรือจำนวน AP ที่มากเกินไปในพื้นที่ โดยเฉพาะอย่างยิ่งในแชนแนลข้างเคียง สามารถกีดขวางการเข้าถึงและแทรกแซงการใช้ AP ของอุปกรณ์อื่น ๆ สาเหตุจากการซ้อนทับกันของแชนแนล ในแถบความถี่ของ 802.11g/b รวมทั้งมีการลดลงของอัตราส่วนสัญญาณต่อคลื่นรบกวน (Signal to Noise Ratio) หรือ SNR ระหว่าง AP ด้วยกัน สิ่งนี้จะกลายเป็นปัญหาในพื้นที่ที่มีความหนาแน่นสูง เช่น อพาร์ตเมนต์ หรืออาคารสำนักงานขนาดใหญ่ที่มีหลาย Wi-Fi AP

นอกจากนี้ อุปกรณ์อื่นๆที่ใช้แถบความถี่ 2.4 GHz เช่นเตาอบไมโครเวฟ อุปกรณ์ ISM กล้องรักษาความปลอดภัย อุปกรณ์ ZigBee อุปกรณ์ บลูทูธ , ผู้ส่ง วิดีโอ โทรศัพท์ไร้สาย เครื่องมอนิเตอร์ทารกและ (ในบางประเทศ) วิทยุสมัครเล่น ทั้งหมดที่สามารถก่อให้เกิดการรบกวนได้เช่นกัน

2.4 IP Address

IP Address คือ เลขรหัสประจำคอมพิวเตอร์ที่ต่ออยู่บนเครือข่าย ซึ่งประกอบด้วยตัวเลข 4 ชุด และมีเครื่องหมายจุดขั้นระหว่างชุด ยกตัวอย่างเช่น 192.168.1.1 เป็นต้นหรือนิยมเรียกสั้นๆว่า IP ซึ่งตัวเลข IP แต่ละเครื่องจะไม่ซ้ำกัน ดังนั้น จึงได้มีการก่อตั้งองค์กรเพื่อ แจกจ่าย IP Address โดยเฉพาะชื่อองค์กรว่า InterNIC (International Network Information Center) อยู่ที่ประเทศสหรัฐอเมริกา การแจกจ่ายนั้นทาง InterNIC จะแจกจ่ายเฉพาะ Network Address ให้แต่ละเครือข่าย ส่วนลูกข่ายของเครือง ทางเครือข่ายนั้นก็จะเป็น ผู้แจกจ่ายอีกทอดหนึ่ง ดังนั้นพอสรุปได้ว่า IP Address จะประกอบด้วยตัวเลข 2 ส่วน คือ

1. Network Address

2. Computer Address

การแบ่งขนาดของ Network Address แบ่งได้ หลายขนาด Class A หมายเลข IP Address จะอยู่ในช่วง 0.0.0.0 ถึง 127.255.255.255 มีไว้สำหรับจัดสรรให้กับองค์กรขนาดใหญ่ที่มีคอมพิวเตอร์เชื่อมต่อภายในเครือ ข่ายจำนวนมากๆ Class B หมายเลข IP Address จะอยู่ในช่วง 128.0.0.0 ถึง 191.255.255.255 มีไว้สำหรับจัดสรรให้กับองค์กรขนาดกลาง ซึ่งสามารถเชื่อมต่อคอมพิวเตอร์ใน

เครือข่ายได้มากถึง 65,534 เครื่อง Class C หมายเลข IP Address จะอยู่ในช่วง 192.0.0.0 ถึง 223.255.255.255 มีไว้สำหรับจัดสรรให้กับองค์กรขนาดเล็กและใช้กับคอมพิวเตอร์ส่วนใหญ่ในเครือ ข่ายอินเตอร์เน็ตสามารถต่อเชื่อมกับคอมพิวเตอร์ในเครือข่ายได้ 254 เครื่อง Class D หมายเลข IP Address จะอยู่ในช่วง 224.0.0.0 ถึง 239.255.255.255 สำหรับหมายเลข IP Address ของ Class นี้มีไว้เพื่อใช้ในเครือข่ายแบบ Multicast เท่านั้น Class E หมายเลข IP Address จะอยู่ในช่วง 240.0.0.0 ถึง 254.255.255.255 สำหรับหมายเลข IP Address ของ Class นี้จะเก็บสำรองไว้ใช้ในอนาคต ปัจจุบันจึงยังไม่ได้มีการนำมาใช้งาน

2.5 SPI

2.5.1. เกริ่นนำถึง SPI

SPI ย่อมาจากคำว่า Serial Peripheral Interface (SPI) คือ การติดต่อสื่อสารที่เกิดขึ้นในเวลาที่พร้อมกัน ซึ่งเหมาะแก่การใช้เฉพาะการติดต่อสื่อสารในระยะสั้นๆ ในระยะแรกได้ถูกนำมาใช้ในระบบฝังตัว (Embedded System) ซึ่งอินเตอร์เฟสของการสื่อสารได้ถูกพัฒนาโดย บริษัท โมโตโลร่า และได้กลายมาเป็นมาตรฐาน de facto ส่วนการนำมาประยุกต์ใช้งาน ได้แก่ เซ็นเซอร์ , Secure Digital cards , ระบบการแสดงผลแบบคริสตัลเหลว (liquid crystal displays)

อุปกรณ์สำหรับการติดต่อแบบ SPI ในโหมดการทำงานแบบ full duplex (การสื่อสารระหว่างสองจุด โดยที่ข้อมูลเดินทางไปมาได้ทั้งสองทิศทางพร้อมๆกันได้) ใช้สถาปัตยกรรมแบบ master-slave พร้อมกับ single master ซึ่ง master device เริ่มต้นขึ้นจาก เฟรม(หน่วยของการส่งถ่ายข้อมูลแบบดิจิตอล) สำหรับอ่านและเขียน อุปกรณ์ที่เป็น slave ได้รับการซัพพอร์ตผ่านทางการเลือกรายตัวอุปกรณ์ (slave select)

ในบางครั้ง SPI ถูกเรียกว่า four-wire serial bus SPI อาจสามารถอธิบายได้อย่างถูกต้องโดย synchronous serial interface แต่ความหมายที่ได้จะแตกต่างจากโปรโตคอล SSI (Synchronous Serial Interface) ซึ่งมันจะให้สัญญาณที่แตกต่างกัน และให้ช่องทางแบบ single simplex communication เท่านั้น

2.5.2. อินเตอร์เฟส

บัสของ SPI รับสัญญาณโลจิกได้ 4 ประเภทด้วยกัน ได้แก่

- SCLK : Serial Clock (เอาท์พุตจาก master).
- MOSI : Master Output, Slave Input (เอาท์พุตจาก master).
- MISO : Master Input, Slave Output (เอาท์พุตจาก slave).

- SS : Slave Select (active low, เอาท์พุตจาก master).

Serial Clock:

- SCLK : SCK, CLK.

Master Output --> Slave Input:

- MOSI : SIMO, SDI(for slave devices), DI, DIN, SI, MTST.

Master Input <-- Slave Output:

- MISO : SOMI, SDO (for slave devices), DO, DOUT, SO, MRSR.

Slave Select:

- SS : nCS, CS, CSB, CSN, EN, nSS, STE, SYNC.

ข้อตกลง (restriction) สำหรับสัญลักษณ์ MOSI/MISO บนตัวอุปกรณ์ ต้องใช้ชื่อที่แตกต่างกัน SDI บน master จะเชื่อมต่อกับ SDO บน slave และในทางกลับกัน การเลือกขั้วของชิพ นานๆครั้งที่จะเลือกแบบ active high แม้ว่าบางสัญลักษณ์ตัวย่อ (เช่น SS or CS แทนที่จะเป็น nSS or nCS)

2.5.3. การทำงาน (Operation)

SPI bus สามารถทำงานบน master เพียงตัวเดียว กับ slave หลายๆตัวได้ ถ้า slave ตัวใดตัวหนึ่งถูกใช้งาน , SS pin อาจจะถูกเซ็ตเอาท์พุตออกมาเป็น logic low ก็ต่อเมื่อ slave ยอมรับ logic แล้ว Slave บางตัว ต้องการ falling edge (ขอบขาลงของสัญญาณ) จากการเลือกสัญญาณของชิพ เพื่อที่จะทำงานได้

ยกตัวอย่าง เช่น ชิพ MAX1242 (ชิพที่แปลงสัญญาณจากอนาล็อกมาเป็นสัญญาณดิจิตอล) เริ่มจากการเปลี่ยนสถานะลอจิกจาก high มาเป็น low กับ อุปกรณ์ slave หลายๆตัว จากนั้น สัญญาณ SS ซึ่งเป็นอิสระต่อกัน จะถูกอุปกรณ์ master เรียกใช้มาสำหรับแต่ละ อุปกรณ์ slave ในแต่ล่ะตัว

อุปกรณ์ slave โดยส่วนมากจะมี 3 เอาต์พุต อุปกรณ์เหล่านั้นมีพฤติกรรม high impedance ต่อ สัญญาณแบบ MISO (logically disconnected) เมื่อ อุปกรณ์ไม่ได้ถูกเลือก ส่วนอุปกรณ์ที่ไม่มี 3 เอาต์พุต จะ ไม่สามารถใช้ตำแหน่ง SPI bus ร่วมกับอุปกรณ์อื่นได้ จะมีแค่ slave ที่สามารถติดต่อกับ master ได้

2.5.4. ขั้วของสัญญาณนาฬิกา และ มุมเฟส

ในการที่จะตั้งค่าของสัญญาณนาฬิกา master จะต้องปรับขั้วของสัญญาณนาฬิกา และ เฟส โดยคำนึงถึงข้อมูล Freescale's SPI Block Guide ได้ตั้งชื่อของทั้ง 2 ออพชั่น นี้ว่า CPOL และ CPHA และผู้ขายก็นำชื่อนี้ไปเป็นข้อตกลงในการซื้อขายด้วย

แผนภูมิทางเวลา (Timing Diagram) ได้ถูกใช้ในการบรรยายพฤติกรรมทางโลจิกของตัว master และ slave

ที่ CPOL=0 ค่าของ CLK จะเป็น 0

- ถ้า CPHA=0, ข้อมูลจะถูกเก็บเมื่อสัญญาณนาฬิกาเป็นขอบขาขึ้น (การเปลี่ยนสถานะจากโลว์เป็นไฮ) และเอาท์พุตจะออกมาเป็น ขอบขาลง (การเปลี่ยนสถานะจากไฮเป็นโลว์)
- ถ้า CPHA=1, ข้อมูลจะถูกเก็บเมื่อสัญญาณนาฬิกาเป็นขอบขาลง และเอาท์พุตจะออกมาเป็นขอบขาขึ้น

ที่ CPOL=1 ค่าของ CLK จะเป็น 1

- ถ้า CPHA=0, ข้อมูลจะถูกเก็บเมื่อสัญญาณนาฬิกาเป็นขอบขาลง และเอาท์พุตจะออกมาเป็นขอบขาขึ้น
- ถ้า CPHA=1, ข้อมูลจะถูกเก็บเมื่อสัญญาณนาฬิกาเป็นขอบขาขึ้น และเอาท์พุตจะออกมาเป็นขอบขาลง

นั้นหมายความว่า CPHA=0 มีการสุ่มสัญญาณ (sampling) บนสัญญาณนาฬิกาแบบนำ (leading (first) clock edge) ในขณะที่ CPHA=1 มีการสุ่มสัญญาณ (sampling) บนสัญญาณนาฬิกาแบบตาม (trailing (second) clock edge)

สัญญาณนาฬิกากาจะเป็นขอบขาขึ้น หรือ ขอบขาลง เมื่อ CPHA=0 ไม่ว่าจะอะไรก็ตาม ข้อมูลจะเสถียรในช่วงเวลา Half-Cycle ก่อน cycle แรก (the first clock cycle)

สัญญาณ MOSI และ MISO มีความเสถียร (ณ จุดที่มันรับ) สำหรับ ครึ่งไซเคิล จนกระทั่งสัญญาณนาฬิกามีการเปลี่ยนแปลงอีกครั้ง อุปกรณ์ SPI master และ slave อาจจะทำการสุ่มสัญญาณ ณ จุดที่แตกต่างกัน ในช่วงเวลาครึ่งไซเคิล เป็นการเพิ่มความยืดหยุ่นในการติดต่อสื่อสาร ระหว่าง master กับ slave

2.5.5. เลขโหมด

Mode คือ ตัวเลขที่ประกอบไปด้วย ขั้ว และ เฟส โดยข้อกำหนดของตัวแปร เป็นดังต่อไปนี้ คือ CPOL คือ บิตที่มีออเดอร์สูง ส่วน CPHA คือ บิตที่มีออเดอร์สูง คือ บิตมีออเดอร์ต่ำ

ตารางที่ 2 โหมดการทำงานของ SPI สำหรับ ไมโครคอนโทรลเลอร์ "Microchip PIC" / "ARM-based"

SPI Mode	Clock Polarity (CPOL/CKP)	Clock Edge (CKE/NCPHA)
0	0	1
1	0	0
2	1	1
3	1	0

ตารางที่ 3 โหมดการทำงาน SPI สำหรับไมโครคอนโทรลเลอร์อื่นๆ

Mode	CPOL	CPHA
0	0	0
1	0	1
2	1	0
3	1	1

2.5.6. Valid communications

Slave บางตัวได้ถูกออกแบบมาให้ ปฏิเสธการเชื่อมต่อแบบ SPI เนื่องจากจำนวนของพัลส์สัญญาณนาฬิกามากกว่าที่ระบุไว้

การปฏิเสธอินพุตแบบพิเศษ และ ความต่อเนื่องของ การเลื่อนของบิตเอาท์พุตที่เหมือนกัน มันเป็นเรื่องที่ปกติสำหรับอุปกรณ์ที่แตกต่างกัน ใช้การติดต่อสื่อสารแบบ SPI ที่ความยาวแตกต่างกัน และตัวอย่าง คือ , เมื่อ SPI ได้ถูกใช้ในการเข้าถึง scan chain ของ ดิจิตอล ไอซี โดยส่งคำสั่ง ขนาด 1 หน่วย (บางที 32 บิต) และหลังจากนั้น มันจะตอบสนองด้วย ขนาดของอาบัติที่แตกต่างกัน (บางที 153 บิต สำหรับแต่ละ pin)

2.5.7. อินเตอร์รัพ (Interrupt)

อุปกรณ์ SPI ในบางเวลาที่ใช้ signal line อันอื่น เพื่อส่งสัญญาณอินเตอร์รัพ ไปหา Host CPU ยกตัวอย่าง เช่น include pen-down interrupts จากทัชสกรีนเซนเซอร์ การแจ้งเตือนเมื่ออุณหภูมิเกินขีดจำกัด ข้อมูลจะถูกส่งไปที่ชิพทันที SDIO , headset jack insertions จาก sound codec ในโทรศัพท์มือถือ อินเตอร์รัพไม่ได้คลอบคลุมถึง มาตรฐานของ SPI อุปกรณ์เหล่านั้น หากไม่ได้ใช้ มาตรฐานที่ไม่ได้รับอนุญาต ก็ มาตรฐานที่จำเพาะเจาะจง

ตัวอย่างของ bit-banging the master protocol

โปรโตคอลของ SPI เช่น SPI master กับ เงื่อนไขของสัญญาณนาฬิกาที่ CPOL=0, CPHA=0 และ การโอนถ่ายข้อมูลขนาด 8 บิต / ครั้ง ตัวอย่างจะถูกเขียนขึ้นใน โปรแกรมภาษาซี เพราะ CPOL=0 สัญญาณนาฬิกาจะถูก pull low ก่อนการเลือกสัญญาณของชิพจะเกิดขึ้น Select line ของชิพจะทำงานโดยปกติจะตีความหมายว่า toggle low

สำหรับอุปกรณ์ต่อพ่วงกับคอมพิวเตอร์ ก่อนที่เริ่มการส่งถ่ายข้อมูล และหลังจากนั้นไม่นานก็หยุดทำงาน อุปกรณ์ต่อพ่วงกับคอมพิวเตอร์โดยส่วนมาก รับหรือต้องการการสางถ่ายข้อมูลที่หลากหลาย ในขณะที่ select line มีสถานะเป็น low งาน (routine) จะถูกเรียกหลายครั้ง ก่อนที่ ชิพจะหยุดเลือก (Deselecting)

2.5.8. ข้อได้เปรียบ

- การติดต่อสื่อสารแบบ Full Duplex จะอยู่ในเวอร์ชั่นเริ่มต้นของโปรโตคอลนี้
- ไดร์ฟเวอร์ พุช-พูล ให้ความเป็นหนึ่งอันเดียวของสัญญาณดี และ มีความเร็วสูง
- มีการส่งผ่านดีกว่า I²C or SMBus
- โปรโตคอลมีความยืดหยุ่น กับการส่งถ่ายข้อมูล (บิต)
- ไม่ได้จำกัดเพียงแค่ 8 บิต
- ใช้งานได้ที่ ขนาดของ ข้อความที่หลากหลาย
- ความเรียบง่ายของอินเตอร์เฟสของฮาร์ดแวร์
- ใช้พลังงานต่ำกว่า I²C หรือ SMBus เนื่องจากวงจรมีความซับซ้อนน้อยกว่า (รวมไปถึงตัวต้านทาน pull-up ด้วย)
- ไม่มีโหมดที่มีอำนาจก้าวก่ายกัน หรือ เกี่ยวข้องกับโหมดที่ล้มเหลว
- Slave ใช้สัญญาณนาฬิกาจาก master โดยไม่ต้องการ oscillators
- Slave ไม่ต้องการ unique address ซึ่งต่างจาก I²C
- ไม่ต้องการตัวรับ-ส่ง
- ใช้งานเพียงแค่ 4 ขาบนตัวไอซี และ การต่อสายบนเลย์เอาต์ หรือ การเชื่อมต่อต่างๆ จะน้อยกว่าอินเตอร์เฟสแบบขนาน
- ส่วนมากสัญญาณ Bus ไม่ซ้ำกันในแต่ละอุปกรณ์ ขณะที่ตัวอื่นจะใช้ร่วมกัน

- สัญญาณไปในทิศทางเดียว (Galvanic isolation)
- ไม่มีขีดจำกัดสำหรับความเร็ว clock สูงสุด สามารถใช้งานกับความเร็วสูงๆได้

2.5.9. ข้อเสีย

- จำนวนที่ต้องการเมื่อนำมาประกอบในรูปของไอซี มีจำนวนน้อยกว่าแบบ I^2C
- ไม่มีการควบคุมฮาร์ดแวร์ โดย slave (แต่ master สามารถหน่วงสัญญาณนาฬิกาได้ ในการเปลี่ยนสถานะครั้งต่อไป เพื่อลดอัตราการส่งถ่ายข้อมูลได้)
- อุปกรณ์ฮาร์ดแวร์ที่เป็น slave จะไม่รู่จักกัน (the master could be transmitting to nowhere and not know it)
- สนับสนุนกับ master เพียงแค่ตัวเดียว
- ไม่มีการตรวจสอบความผิดพลาดของโปรโตคอล
- ไม่มีมาตรฐานที่เป็นทางการ, ความสมบูรณ์ของความสอดคล้องเป็นไปไม่ได้เลย
- สามารถทำงาน (Handle) ได้แค่ในระยะสั้นๆ เมื่อเทียบกับ RS-232, RS-485, หรือ CAN-bus
- ตัวอุปกรณ์ที่มีอยู่มีหลากหลาย ทำให้ยากต่อการหาเครื่องมือมาพัฒนา เหมือนกับ ตัวปรับต่อ (Adapter) ของ Host ต้องสนับสนุนกับอุปกรณ์ที่มีอยู่อย่างหลากหลายได้
- SPI ไม่สามารถทำงานในแบบ Hot Swapping (การเพิ่มโหนดแบบพลวัต)ได้
- อินเตอร์ต้องถูกนำมาใช้ร่วมกับ สัญญาณ out-of-band หรือ ถูกจำลองขึ้นในทำนองเดียวกันโดยใช้ periodic polling กับ USB และ and 2.0

การประหยัดเนื้อที่บนบอร์ด เมื่อเทียบกับ I/O bus แบบขนาน เป็นสิ่งที่มีนัยสำคัญ และ have earned SPI a solid role in embedded systems. นั้นจริงสำหรับกระบวนการ system-on-a-chip ทั้งกับ การประมวลผลที่สูงกว่า 32 บิต (โดยใช้ ARM, MIPS, or PowerPC) และ กับไมโครคอนโทรลเลอร์ชนิดอื่นๆ เช่น AVR, PIC, และ MSP430. ซึ่งชิพไมโครคอนโทรเลอร์เหล่านี้ สามารถทำงาน โหมดของ master หรือ slave ก็ได้

เมื่อพิจารณาในระบบของคอนโทรลเลอร์แบบ programmable AVR (including blank ones) สามารถโปรแกรมโดยใช้ SPI ได้

2.6. WEP

WEP คือ อัลกอริทึ่มของมาตรฐานความปลอดภัย IEEE 802.11 ซึ่งเป็นการเชื่อมต่อไร้สาย WEP เป็นส่วนหนึ่งของมาตรฐาน 802.11 ซึ่งได้รับการอนุมัติในปี 1997 มันทำให้ความปลอดภัยไว้กับข้อมูล ซึ่งประกอบไปด้วยเลขฐาน 16 ตั้งแต่ 10-26 หลัก ในสมัยก่อนได้ถูกนำมาใช้กันอย่างกว้างขวาง เป็นตัวเลือกอันดับแรกของผู้ใช้งาน โดยเครื่องมือสำหรับจัดระบบของ router (Router Configuration Tool)

WEP ใช้ Stream Ciphor RC4 ในการเก้บข้อมูลให้เป็นความลับ และใช้ CRC-32 Checksum เพื่อให้เป็นอันเดียวกัน

WEP พื้นฐานขนาด 64 บิต (WEP-40) ซึ่ง 40 บิตได้ถูกใช้เป็น concatenate ส่วนอีก 24 บิต เป็น IV (Initialization Vector) มารวมกันสร้างเป็นรูปแบบของ RC4 Key WEP ได้ถูกสร้างโดยรัฐบาลสหรัฐอเมริกา (Export Restriction on Cryptographic Technology) ต่อมาภายหลังได้มีการพัฒนามาเป็น WEP-104 (ขนาดของ Key เป็น 104)

ตัวเลขฐาน 16 ประกอบด้วยอักขระ 0-9 และ A-F แต่ละอักขระจะมีขนาด 4 บิต เช่น สมมติว่าเลขฐาน 16 จำนวน 10 หลัก ก็จะมีขนาดเท่ากับ 40 บิต โย WEP ใช้อักขระเลขฐาน 16 ทั้งหมด 10 หลัก และ IV อีก 24 บิต รวมเป็น 64 บิต (Key ใน WEP)

แต่อุปกรณ์โดยส่วนมากรับส่งค่าเป็น รหัสแอสกี (ASCII Character) จำนวน 5 หลัก ในแต่ละหลัก มีขนาด 8 บิต รวมเป็น 40 บิตเช่นเดียวกับเลขฐาน 16 และ IV อีก 24 บิต เช่นกัน

อย่างไรก็ตาม เงื่อนไขและข้อกำหนดต่างๆ ของการใช้รหัส ASCII ช่วยลดพื้นที่ได้มากขึ้น ทำให้ประหยัดเนื้อที่ในการจัดเก็บข้อมูลมากขึ้น

2.7. WPA

WPA (Wi-Fi Protected Access) คือ โปรโตคอลความปลอดภัย และ โปรแกรมการยืนยันความปลอดภัย ได้รับการพัฒนาโดย Wi-Fi Alliance ซึ่งเป็นองค์กรที่ไม่แสวงหาผลกำไร (มีจุดประสงค์ในการประชาสัมพันธ์เทคโนโลยีของไฟไฟ) ซึ่งมันถูกพัฒนาขึ้นมาเพื่อรักษาความปลอดภัยกับการเชื่อมต่อแบบไร้สาย ซึ่งนักวิจัยได้พบจุดบกพร่องของระบบก่อนหน้านี้ คือ WEP

WPA มีคุณสมบัติถูกต้องตามมาตรฐาน IEEE 802.11 ซึ่ง WPA ถูกนำมาใช้งานผ่านทางการอัพเดต firmware บน wireless network interface card ซึ่งได้ออกแบบมาสำหรับ WEP

อย่างไรก็ตาม มีความต้องการการเปลี่ยนแปลง ใน wireless Access Point (APs) อย่างมาก ทำให้ Aps ที่สร้างก่อนปี 2003 ไม่สามารถสนับสนุนหรืออัพเดตกับ WPA ได้

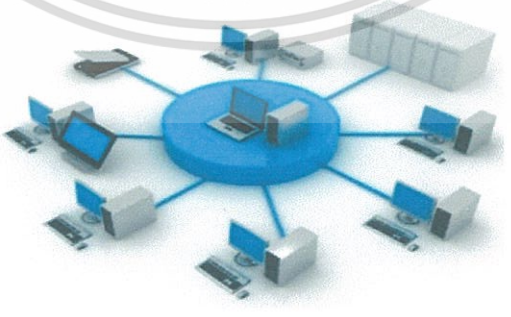
2.8. โปรโตคอล

2.8.1. เกริ่นนำถึงโปรโตคอล

โปรโตคอล (Protocol) หมายถึง ข้อกำหนดหรือข้อตกลงในการสื่อสารระหว่างคอมพิวเตอร์ซึ่งมีอยู่ด้วยกันมากมายหลายชนิด แต่ละชนิดก็มีข้อดี ข้อเสีย และใช้ในโอกาสหรือสถานการณ์แตกต่างกันไป คล้ายๆ กับภาษามนุษย์ที่มีทั้งภาษาไทย จีน ฝรั่ง หรือภาษาใบ้ ภาษามือ หรือจะใช้วิธียักคิ้วหลิ่วตาเพื่อส่งสัญญาณก็จัดเป็นภาษาได้เหมือนกัน ซึ่งจะสื่อสารกันรู้เรื่องได้จะต้องใช้ภาษาเดียวกัน ในบางกรณีถ้าคอมพิวเตอร์ 2 เครื่องสื่อสารกันคนละภาษากันและต้องการนำมาเชื่อมต่อกัน จะต้องมีตัวกลางในการแปลงโปรโตคอลกลับไปกลับมาซึ่งนิยมเรียกว่า Gateway ถ้าเทียบกับภาษามนุษย์ก็คือ ล่าม ซึ่งมีอยู่ทั้งที่เป็นเครื่องเซิร์ฟเวอร์แยกต่างหากสำหรับทำหน้าที่นี้โดยเฉพาะ หรืออาจจะเป็นโปรแกรมหรือไดร์ฟเวอร์ที่สามารถติดตั้งในเครื่องคอมพิวเตอร์นั้น ๆ ได้เลย

การที่คอมพิวเตอร์เครื่องหนึ่งจะส่งข้อมูลไปยังคอมพิวเตอร์อีกเครื่องหนึ่งได้นั้น จะต้องอาศัยกลไกหลายๆ อย่างร่วมกันทำงานต่างหน้าที่กัน และเชื่อมต่อเป็นเครือข่ายเข้าด้วยกัน ปัญหาที่เกิดขึ้นคือการเชื่อมต่อมีความแตกต่างระหว่างระบบและอุปกรณ์หรือเป็นผู้ผลิตคนละรายกัน ซึ่งเป็นสิ่งที่ทำให้การสร้างเครือข่ายเป็นเรื่องยากมาก เนื่องจากขาดมาตรฐานกลางที่จำเป็นในการเชื่อมต่อ

จึงได้เกิดหน่วยงานกำหนดมาตรฐานสากลขึ้นคือ International Standards Organization และทำการกำหนดโครงสร้างทั้งหมดที่จำเป็นต้องใช้ในการสื่อสารข้อมูลและเป็นระบบเปิด เพื่อให้ผู้ผลิตต่างๆ สามารถแยกผลิตในส่วนที่ตัวเองถนัด แต่สามารถนำไปใช้ร่วมกันได้ ระบบเครือข่ายคอมพิวเตอร์สมัยใหม่จะถูกออกแบบให้มีโครงสร้างที่แน่นอน และเพื่อเป็นการลดความซับซ้อน ระบบเครือข่ายส่วนมากจึงแยกการทำงานออกเป็นชั้นๆ (layer) โดยกำหนดหน้าที่ในแต่ละชั้นไว้อย่างชัดเจน แบบจำลองสำหรับอ้างอิงแบบ OSI (Open System Interconnection Reference Model) หรือที่นิยมเรียกกันทั่วไปว่า OSI Reference Model ของ ISO เป็นแบบจำลองที่ถูกเสนอและพัฒนาโดยองค์กร International Standard Organization (ISO) โดยจะบรรยายถึงโครงสร้างของสถาปัตยกรรมเครือข่ายในอุดมคติ ซึ่งระบบเครือข่ายที่เป็นไปตามสถาปัตยกรรมนี้จะเป็นระบบเครือข่ายแบบเปิด และอุปกรณ์ทางเครือข่ายจะสามารถติดต่อกันได้โดยไม่ขึ้นกับว่าเป็นอุปกรณ์ของผู้ขายรายใด



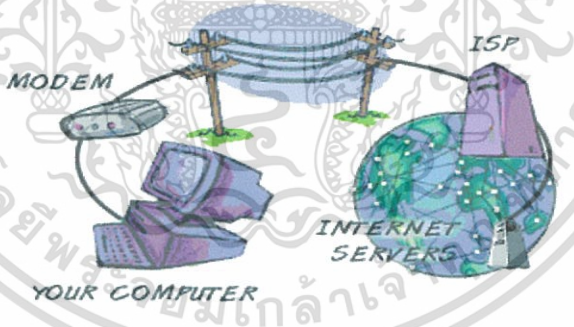
รูปที่ 2.4 เครือข่ายการเชื่อมต่อของเครื่องคอมพิวเตอร์

2.8.2. ความสำคัญของโปรโตคอล

ในการติดต่อสื่อสารข้อมูลผ่านทางเครือข่ายนั้น จำเป็นต้องมีโปรโตคอลที่เป็นข้อกำหนดตกลงในการสื่อสารขึ้น เพื่อช่วยให้ระบบสองระบบที่แตกต่างกันสามารถสื่อสารกันอย่างเข้าใจได้โปรโตคอลเป็นข้อที่กำหนดเกี่ยวกับการสื่อสารระหว่างเครื่องคอมพิวเตอร์ต่างๆ ทั้งวิธีการส่งและรับข้อมูล วิธีการตรวจสอบข้อผิดพลาดของการส่งและรับข้อมูล การแสดงผลข้อมูลเมื่อส่งและรับกันระหว่างเครื่องสองเครื่องดังนั้นจะเห็นได้ว่าโปรโตคอลมีความสำคัญมากในการสื่อสารบนเครือข่ายหากไม่มีโปรโตคอลแล้ว การสื่อสารบนเครือข่ายจะไม่สามารถเกิดขึ้นได้ในปัจจุบันการทำงานของเครือข่ายใช้มาตรฐานโปรโตคอลต่างๆ ร่วมกันทำงานมากมายนอกจากโปรโตคอลระดับประยุกต์แล้ว การดำเนินการภายในเครือข่ายยังมีโปรโตคอลย่อยที่ช่วยทำให้การทำงานของเครือข่ายมีประสิทธิภาพขึ้น โดยที่ผู้ใช้ไม่สามารถสังเกตเห็นได้โดยตรงอีกมาก

2.8.3. การทำงานของโปรโตคอล

เครือข่ายคอมพิวเตอร์ประกอบด้วยอุปกรณ์ที่ทำงานร่วมกันเป็นจำนวนมาก ผลิตภัณฑ์เหล่านั้นมีหลายมาตรฐานหลายยี่ห้อแต่ก็สามารถทำงานร่วมกันได้อย่างดีการที่เครือข่ายคอมพิวเตอร์ทำงานร่วมกันอย่างเป็นระบบ เพราะมีการใช้โปรโตคอลมาตรฐานที่มีข้อกำหนดให้ทำงานร่วมกันได้ผู้ใช้อินเตอร์เน็ตที่ทำหน้าที่เป็นผู้ใช้บริการหรือเป็นไคลแอนต์ (Client) สามารถเชื่อมต่อเครื่องคอมพิวเตอร์ของท่านไปยังเครื่องให้บริการหรือเซิร์ฟเวอร์ (Server) บนเครือข่าย การทำงานของพีซีที่เชื่อมต่อร่วมกับเซิร์ฟเวอร์ก็จำเป็นต้องใช้โปรโตคอลเพื่อประยุกต์ใช้งานรับส่งข้อมูล ซึ่งโปรโตคอลที่ใช้ในการสื่อสารนี้ก็มีมากมายหลายประเภทด้วยกัน



รูปที่ 2.5 การเชื่อมต่ออินเตอร์เนตระหว่างเครื่องคอมพิวเตอร์ทั่วโลก

2.9. Client/Server

Client คือ เครื่องคอมพิวเตอร์ที่ไปร้องขอบริการและรับบริการอย่างใดอย่างหนึ่งจาก Server

Server คือ เครื่องคอมพิวเตอร์หรือระบบปฏิบัติการหรือโปรแกรมคอมพิวเตอร์ ที่ทำหน้าที่ให้บริการอย่างใดอย่างหนึ่งหรือหลายอย่าง โดยอาศัยโปรแกรม Web server แก่เครื่องคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่เป็นลูกข่าย ในระบบเครือข่าย

Server แบ่งเป็น 3 ประเภทได้แก่

1. เครื่องคอมพิวเตอร์ที่ทำหน้าที่ให้บริการอะไรบางอย่างแก่คอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์อื่น

2. ระบบปฏิบัติการคอมพิวเตอร์ที่ทำหน้าที่ให้บริการอะไรบางอย่างแก่คอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์อื่น

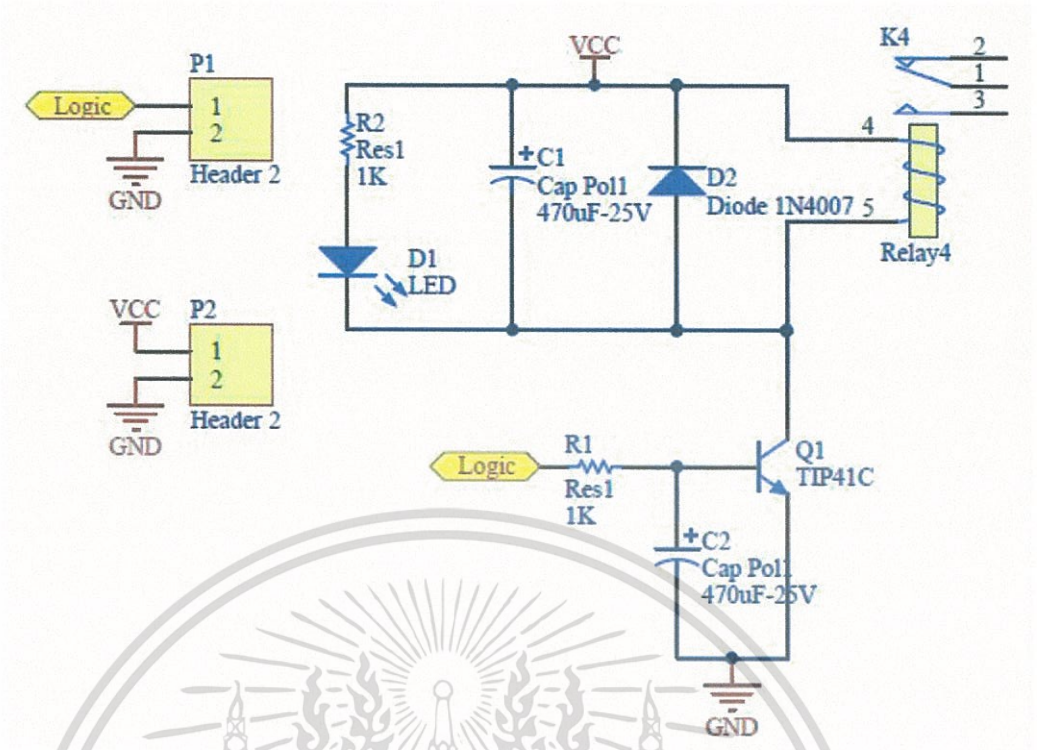
3. โปรแกรมคอมพิวเตอร์ที่ทำหน้าที่ให้บริการอะไรบางอย่างแก่คอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์อื่น

Client/Server คือ การที่มีเครื่องผู้ให้บริการ (server) และ เครื่องผู้ใช้บริการ (client) เชื่อมต่อกันอยู่ และเครื่องผู้ใช้บริการได้มีการติดต่อร้องขอบริการจากเครื่องผู้ให้บริการ เครื่องผู้ให้บริการก็จะจัดการตามที่เครื่องผู้ขอใช้บริการร้องขอ แล้วส่งข้อมูลกลับไปให้

เครือข่ายแบบ Client / server เหมาะกับระบบเครือข่ายที่ต้องการเชื่อมต่อกับเครื่องลูกข่ายจำนวนมาก โดยการรองรับจำนวนเครื่องลูกข่าย (Client) อาจเป็นหลักสิบ หลักร้อย หรือหลักพัน เพราะฉะนั้นเครื่องที่จะนำมาทำหน้าที่ให้บริการจะต้องเป็นเครื่องที่มี ประสิทธิภาพสูง เนื่องจากถูกต้องออกแบบมาเพื่อทนทานต่อความผิดพลาด (Fault Tolerance) และต้องคอยให้บริการทรัพยากรให้กับเครื่องลูกข่ายตลอดเวลา โดยเครื่องที่จะนำมาทำเป็นเซิร์ฟเวอร์อาจเป็นคอมพิวเตอร์แบบเมนเฟรม มินิคอมพิวเตอร์ หรือไมโครคอมพิวเตอร์ก็ได้

2.10. หลักการทำงาน

การสั่งการผ่าน web server จากผู้ใช้งาน จะไปสั่งการให้บอร์ดอาดูโน่ทำงาน ซึ่งบอร์ดอาดูโน่รับค่าอินพุตมาจาก web server เมื่อสั่งการบอร์ดอาดูโน่ มันจะส่งลอจิก 0 หรือ 1 เข้ามาที่บอร์ดควบคุม เพื่อควบคุมการทำงาน เปิด และ ปิด ดังรูปที่ 8 บอร์ดควบคุม ซึ่ง logic คือ เปิด และ logic 0 คือ ปิด



รูปที่ 2.6 วงจรภาคควบคุม

วงจรภาคควบคุม คือ วงจรที่ใช้ในการรับสัญญาณลอจิก จากบอร์ดอาดูโน่ (แรงดันต่ำ) มาใช้สั่งการเปิด ปิด ของ ไฟฟ้าบ้าน โดยทำงานผ่านรีเลย์ (relay)

2.10.1 หลักการทำงานของภาคควบคุม

เมื่อผู้ใช้งาน สั่งงานด้วยคำสั่งเปิด บอร์ด อาดูโน่จะ ส่ง Logic 1 ออกมา ป้อนเข้าที่เบสของทรานซิสเตอร์ เกิดแรงดันตกคร่อมขา เบส-อิมิตเตอร์ ทำการให้มีกระแสให้ผ่านระหว่างขาคอลเลกเตอร์ และ ขา อิมิตเตอร์ แต่ขดลวดของรีเลย์ ต่ออนุกรมขาของทรานซิสเตอร์ ขดลวดมีกระแสไหล หน้าสัมผัสในโลหะของรีเลย์ จะเกิดการเปลี่ยนขั้ว และ มีกระแสไหลผ่าน เครื่องใช้ไฟฟ้า ไดโอด D_2 ป้องกันการกลับขั้วของขดลวดในรีเลย์ ตัวเก็บประจุ C_1 ป้องกันการ Spark ของแรงดัน (รักษาระดับแรงดัน) เมื่อทรานซิสเตอร์อยู่ในโหมด ไม่ทำงาน แล้ว ตัวเก็บประจุ จะค่อยๆคายประจุ มีกระแสไหลผ่าน ตัวต้านทาน และ หลอด LED โดยที่หลอด LED ไว้สำหรับแสดงผลการทำงาน ถ้าหลอด LED ติด คือ เครื่องใช้ไฟฟ้าทำงาน (เปิด) และ หลอด LED ดับ คือ เครื่องใช้ไฟฟ้าไม่ทำงาน ตัวต้านทาน 1 K ป้องกันไม่ให้มีกระแสไหลผ่าน หลอด LED มากจนเกินไป

อินพุต : ไฟเลี้ยง (V_{CC}) และ ลอจิกจากบอร์ดอาดูโน่

เอาท์พุต : ไฟฟ้าบ้าน 220 v

2.10.2 หลักการทำงานของคำสั่ง Code

การทำงานของบอร์ดอาดูโน่ เมื่อทำการเขียน Source Code แล้ว แต่ต้องทำงานเบิร์น code นั้นลงไปยังบอร์ดก่อน ซึ่งเนื้อหาของชุดคำสั่งจะยาวหรือสั้นก็ได้ แต่ถ้ามีความยาวมาก ต้องขึ้นอยู่กับรุ่นของบอร์ดอาดูโน่ด้วย เนื่องจากขนาดของหน่วยความจำบอร์ดในแต่ละรุ่นมีขนาดไม่เท่ากัน

Code :

ไลบารี่

include "SPI.h	ไลบารี่เปิดการใช้งานเชื่อมต่อระหว่างบอร์ดอาดูโน่ กับ โมดูล ESP82226 เพื่อให้สามารถใช้งานไวไฟได้ โดยเสมือนว่าเป็นตัวเชื่อมการทำงานระหว่างอินเตอร์เฟส โมดูล กับ บอร์ดอาดูโน่
include "Ethernet.h	ไลบารี่เริ่มการทำงานของ Ethernet และ ตั้งค่าเน็ตเวิร์ค ซึ่ง Ethernet shield จะได้รับ IP Address โดยอัตโนมัติ
#include <Wire.h>	ไลบารี่ประกาศตัวแปรเพื่อเริ่มการเชื่อมต่อกับ I^2C

การประกาศไลบารี่ จะต้องทำการประกาศตัวแปรก่อนที่จะใช้งานฟังก์ชั่น ไลบารี่เปรียบเสมือนแหล่งรวมคำสั่งฟังก์ชั่นต่างๆ ซึ่งบอร์ดอาดูโน่ที่ยังไม่มีไลบารี่ จะต้องทำการติดตั้ง (Install) ไลบารี่ก่อนใช้งานทุกครั้ง

ฟังก์ชั่น

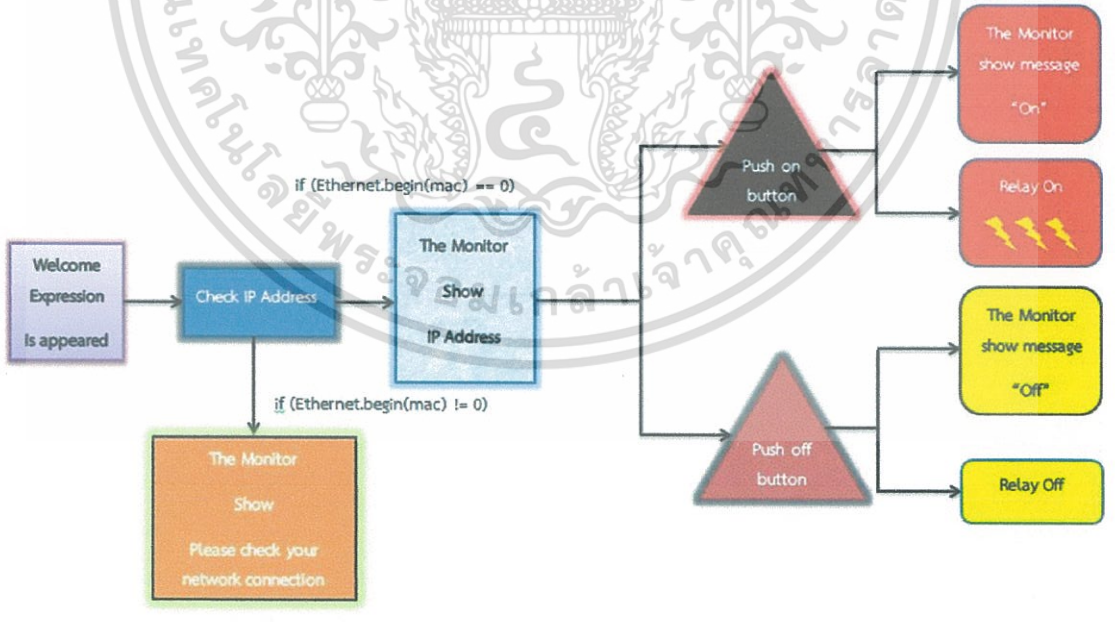
display.clearDisplay();	ฟังก์ชั่นนี้จะทำการล้างข้อความเก่าๆที่ยังตกค้างอยู่ที่หน้าจอ ให้หายไป ก่อนที่จะแสดงผลในส่วนของ Web Browser ซึ่งมีข้อความเหลือค้าง
display.setCursor(0,0)	ฟังก์ชั่นนี้จะทำการจะตั้งจุดเริ่มต้นของ cursor (เมาส์) มาที่พิกัด 0,0 (มุมบนทางซ้าย)
display.setTextSize(2)	ฟังก์ชั่นนี้จะตั้งค่าขนาดของตัวอักษรมาไว้ที่ 20 pixel
display.setTextColor(WHITE)	ฟังก์ชั่นนี้จะตั้งค่าสีของตัวอักษร ให้เป็นสีขาว
display.println("XXXX")	ฟังก์ชั่นนี้ใช้ในการแสดงผลข้อความ

Ethernet.begin(mac) ฟังก์ชั่นนี้แสดงสถานการณ์ทำงาน ของ Ethernet จะมีค่า 0 กับ 1 ถ้ามีค่า เท่ากับ 0 คือ ไม่มีการเชื่อมต่อกับ Ethernet แต่ถ้ามีค่าเท่ากับ 1 หมายถึง มีการเชื่อมต่อกับ Ethernet แล้ว

ในส่วนของการเชื่อมต่อ ถ้าค่าของฟังก์ชั่น Ethernet.begin(mac) มีค่าเท่ากับ 0 หน้าจอจะแสดงผลเป็นภาษาอังกฤษ ไปให้ User interface ว่าไม่มีมีการเชื่อมต่อ จะปรากฏข้อความดังต่อไปนี้ //Please check your network connection // และข้อความ Disconnected แต่ถ้าค่าของฟังก์ชั่น Ethernet.begin(mac) ไม่ได้มีค่าเท่ากับ 0 Web Browser จะแสดงผลออกมาเป็นข้อความว่า CONNECTED (มีการเชื่อมต่อ)

การเชื่อมต่อจะเชื่อมต่อ ต้องมีความพร้อมของทั้งสอง การติดต่อ เราจะแบ่งออกเป็น 1. ผู้ติดต่อขอบริการ (Client) และ 2. ผู้ให้บริการ (Server) ซึ่งในที่นี้ Client คือ Web Browser จากโทรศัพท์มือถือ หรือ Notebook ที่ทำต้องการที่จะเข้าถึงการเชื่อมต่อกับ Server และ Server คือ ชุดอุปกรณ์ Module ESP8226 และ board Arduino จึงใช้ฟังก์ชั่น EthernetClient client = server.available() เพื่อกำหนดการติดต่อ เมื่อทางฝั่งของ Client พร้อมที่จะทำการเชื่อมต่อแล้ว ดังนั้นการใช้ฟังก์ชั่นนี้ ถ้าฝั่งของผู้ให้บริการ จะต้องพร้อมที่ให้บริการก่อน (อยู่ในสถานะ ON) และการเชื่อมต่อจะเสร็จสมบูรณ์ (ฟังก์ชั่น EthernetClient client = server.available() เป็นจริง) เมื่อผู้ใช้งานทำการเชื่อมต่อ Wi-Fi ก่อน

เมื่อสรุปการทำงานตามลำดับขั้นออกมาเป็น Block Diagram แล้วจะได้ดังรูปที่ 2.7



รูปที่ 2.7 Block Diagram แสดงการทำงานของ Web Server

สำหรับในส่วนของการทำงานบนบอร์ดอาดูโน่ (Server) ในขั้นแรก จะแสดงข้อความ Welcome ออกมาทางหน้าจอก่อน จากนั้นจะ Check IP Address ของ Server ซึ่งก็คือตัวโมดูล Ethernet Shield ว่ามีการเชื่อมต่อหรือไม่ ถ้าหากยังไม่มีการเชื่อมต่อ หน้าจอจะแสดงผลว่า Please check your network connection แต่เมื่อมีการเชื่อมต่อระหว่าง Ethernet Shield กับบอร์ดอาดูโน่ แล้ว หน้าจอจะแสดงผลเป็นรหัส IP Address ของ Ethernet Shield เช่น 192.168.1.100:80 จากจุดนี้ ระบบพร้อมที่จะรองรับการสั่งการจาก Web Server แล้ว เมื่อผู้ใช้ทำการกดสั่งการเปิด บอร์ดอาดูโน่จะส่ง Logic ออกมามีค่าเท่ากับ 1 และบอร์ดควบคุมก็จะทำงาน รีเลย์จะยอมให้กระแสไหลผ่าน เครื่องใช้ไฟฟ้าทำงาน และเมื่อกดปิด บอร์ดอาดูโน่จะส่ง Logic 0 ออกไปทำให้บอร์ดควบคุมหยุดการทำงาน ไม่มีกระแสไหลผ่านเครื่องใช้ไฟฟ้า

บทที่ 3
วิธีการทดลอง

3.1. วิธีที่ใช้ศึกษาค้นคว้าและการวิจัยทดลอง

ศึกษาวงจรการทำงานของตัวอุปกรณ์รีเลย์เพื่อมาประกอบกันเป็นวงจร ใช้สำหรับควบคุมเครื่อใช้ไฟฟ้า รีเลย์จะถูกควบคุมการปิด – เปิดโดยบอร์ดอาดูโน่ การค้นคว้าในโครงงานี้ โดยส่วนใหญ่จะหาข้อมูลมาจากทางอินเตอร์เน็ต ส่วนการทดลองนั้น จะพิจารณาที่การเขียนอัลกิริทึ่มเป็นส่วนใหญ่ เนื่องจากส่วนประกอบของโครงงานนี้โดยส่วนมากจะเป็น Software ดังรูปที่ 2.7 แสดงลำดับขั้นของการทำงานของระบบ เมื่อได้ขั้นตอนแล้ว จึงนำมาออกแบบ Code สำหรับบอร์ดอาดูโน่ จากนั้นทดลอง code ลงบนบอร์ดอาดูโน่ เพื่อตรวจสอบการทำงานของบอร์ดอาดูโน่ว่า มีการทำงานตรงตาม Algorithm ที่วางไว้หรือไม่ ซึ่งพบว่ามีการทำงานที่ตรงกับ Algorithm ที่กำหนดเอาไว้ทุกประการ แต่ในส่วนของบอร์ดรีเลย์ได้ทำการทดลองต่ออนุกรมกับเครื่องใช้ไฟฟ้า และทำการป้อน Logic เข้าไปในวงจร พบว่า รีเลย์มีการปิด-เปิด เครื่องใช้ไฟฟ้าได้ตามปกติ โดยมีขีดจำกัดการดึงกระแสของเครื่องใช้ไฟฟ้าที่ไม่เกิน 10 แอมแปร์ (ตาม Specification ของรีเลย์)

3.2. ลักษณะข้อมูล การเลือกข้อมูล และการทดลอง

ข้อมูลที่ได้จะอยู่ในรูปของสัญญาณคลื่น sinusoid ขนาด 50 Hz ขนาด 220 โวลต์ ซึ่งจ่ายให้กับเครื่องใช้ไฟฟ้าให้ทำงาน และขนาด 5 โวลต์ เป็นแรงดันกระแสตรงที่บอร์ดอาดูโน่ป้อนให้กับ บอร์ดควบคุม การเลือกข้อมูลในเรื่องของแรงดันทางไฟฟ้านั้นจะพิจาณาจาก ข้อมูลของบอร์ดอาดูโนในแต่ล่ะรุ่น แต่ทุกรุ่นยังมีลักษณะ (Characteristic) ที่เหมือนกันบางประการ เช่น แรงดันไฟเลี้ยงบอร์ดอาดูโน่ จะอยู่ระหว่าง 7-20 โวลต์ ส่วนแรงดันทั้งขาออก มีค่า 5 โวลต์ และแรงดันขาเข้าที่ควรป้อนก็เช่นกัน ควรจะมีค่าประมาณ 5 โวลต์ ซึ่งข้อมูลเหล่านี้จำเป็นสำหรับการทำบอร์ดรีเลย์ เพื่อที่จะได้กำหนดขนาดของอุปกรณ์ต่างๆให้เหมาะสมกับเอาท์พุตของบอร์ดอาดูโน่ ซึ่งจะไปป้อนเป็นอินพุตให้กับบอร์ดควบคุมต่อไป (บอร์เอาดูโน่ทำการสั่งการบอร์ดควบคุม) และข้อมูลในการเลือกขนาดของรีเลย์ จะตรวจสอบจากเครื่องใช้ไฟฟ้าทั่วไป ซึ่งโดยส่วนใหญ่ มีกำลังไม่เกิน 1000 วัตต์ จากสูตรที่ใช้ในการคำนวณ P=IV จะพบว่า เครื่องใช้ไฟฟ้าส่วนใหญ่มีการกินกระแสไม่เกิน 4.55 แอมแปร์ รีเลย์เลยมีส่วนเผื่อ ซึ่งรีเลย์ที่ใช้ใน

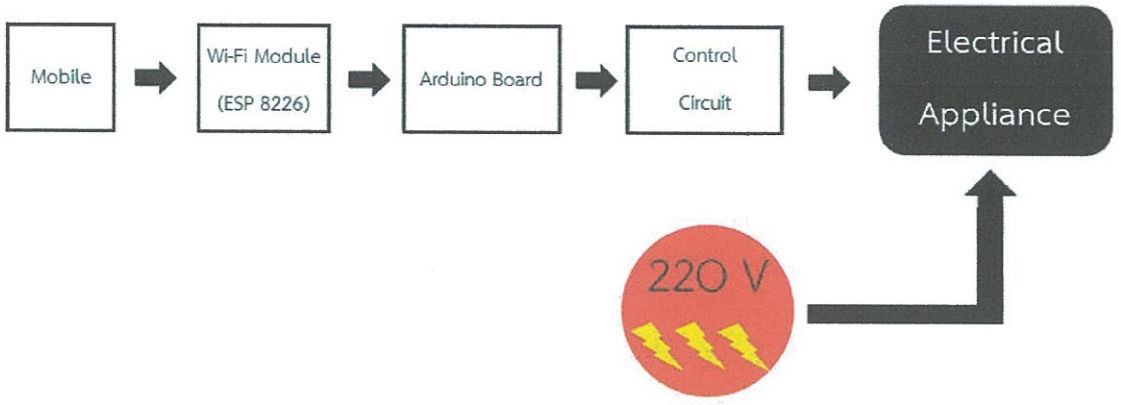
โครงงานนี้สามารถจ่ายกระแสได้มากถึง 10 แอมแปร์ เพื่อให้สามารถทำการเปิดปิดเครื่องใช้ไฟฟ้ามากกว่า 1 ตัวได้ ในเวลาเดียวกัน (เปิดปิดพร้อมกันได้) โดยสำรวจได้จากปลั๊กพ่วงตามท้องตลาดที่มักนิยมใช้ฟิวส์ขนาด 10 แอมแปร์

3.3. เครื่องมือและวิธีการวิจัยทดลอง

เครื่องมือที่ใช้ในการทดลอง ได้แก่ 1. บอร์ดอาดูโน่ รุ่น Mega 2560 , 2. หน้าจอ LCD , 3. สาย LAN , 4. เราท์เตอร์ , 5. ปลั๊กไฟ , 6. หลอดไฟ , 7. สายจัมพ์ วิธีวิจัยการทดลอง คือ ผู้ทดลองจะลำดับขั้นการทำงานของระบบ และ เขียน Code ออกมา หลังจากนั้นใช้คอมพิวเตอร์ เชื่อมต่อกับบอร์ดอาดูโน่ เพื่อทำการเบิร์น code ที่เขียนไว้ลงไป และทดลองสั่งการผ่าน Web Server เพื่อดูการทำงานตามการสั่งการ กดปิด และ กดเปิด

3.4. ขั้นตอนออกแบบและสร้างเครื่องมือ

เครื่องมือหลักที่ใช้ในการทำงานของระบบ คือ บอร์ดอาดูโน่ เป็นบอร์ดแบบสำเร็จรูปอยู่แล้ว การออกแบบโดยส่วนใหญ่ จึงเป็นการออกแบบ Algorithm มากกว่าที่จะเป็นการออกแบบที่ตัวฮาร์ดแวร์ แต่ส่วนประกอบหลักนั้น ยังมี Ethernet Shield Module ด้วย ต้องตรวจดูว่าระหว่างบอร์ดอาดูโน่ กับโมดูล Ethernet Shield มีความเข้ากันได้หรือไม่ โดยหาข้อมูลจากอินเตอร์เน็ต พบว่า Ethernet Shield ในโครงงานนี้ และ บอร์ดอาดูโน่ มีความเข้ากันได้ ทำงานร่วมกันได้เป็นอย่างดี ส่วนเราท์เตอร์ เป็น router ที่มีน้ำหนักเบา และใช้งานได้หลากหลาย กล่าวคือ router ในโครงงานนี้ สามารถนำมาใช้กระจายสัญญาณ Wi-Fi ได้ และ สามารถเอามาเชื่อมต่อ Network ระหว่างเครื่องคอมพิวเตอร์ ได้มากสูงสุดถึง 4 ช่องทางด้วย การต่อยอดในส่วนนี้ ทำให้การสั่งการปิดเปิดเครื่องใช้ไฟฟ้าสามารถสั่งผ่านแบบไร้สาย และแบบมีสายได้ด้วย แต่จะต้องทำการ Configuration ก่อน จะเห็นได้ว่าเป็นประโยชน์ที่สามารถต่อยอดได้อีก



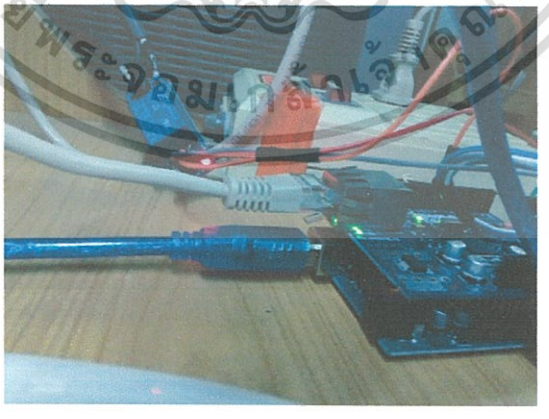
รูปที่ 3.1 Block Diagram ของทั้งระบบ

บทที่ 4
ผลการทดลอง

หน้าจอเมื่อเริ่มทำงานแสดงข้อความ “ยินดีต้อนรับ” เป็นการแสดงผลเมื่อเปิดเครื่อง จากนั้นทำการเสียบสาย Lan เข้ากับ Router ที่บ้าน เครื่องก็จะทำการตรวจสอบหมายเลข IP Address ที่จ่ายมาจาก Router ว่ามีการจ่ายมาหรือไม่

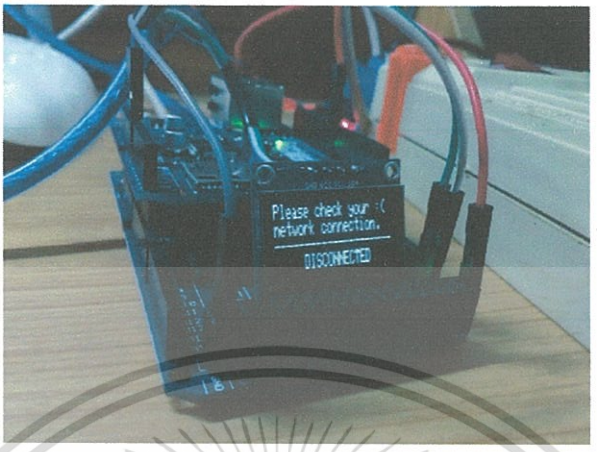
รูปที่ 4.1 หน้าจอแสดงข้อความต้อนรับ

เชื่อมต่อบอร์ดกับกับ Router ที่บ้าน โดยผ่านสาย LAN (ต้องใช้กับวง LAN เดียวกัน) ซึ่งส่งผ่านข้อมูลผ่านสายแบบ SPI



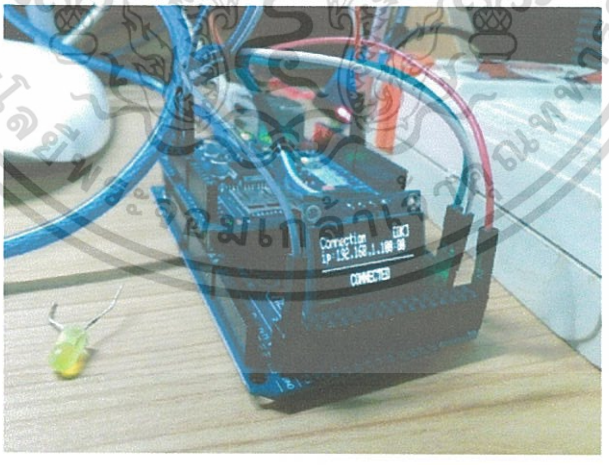
รูปที่ 4.2 การเชื่อมต่อบอร์ดอาดูโน่ด้วยสาย Lan

หาก Router ไม่มีการจ่ายหมายเลข IP Address มา หน้าจอก็จะขึ้นข้อความให้ตรวจสอบการเชื่อมต่อเครือข่ายอีกครั้ง จากนั้นให้กดปุ่ม Reset



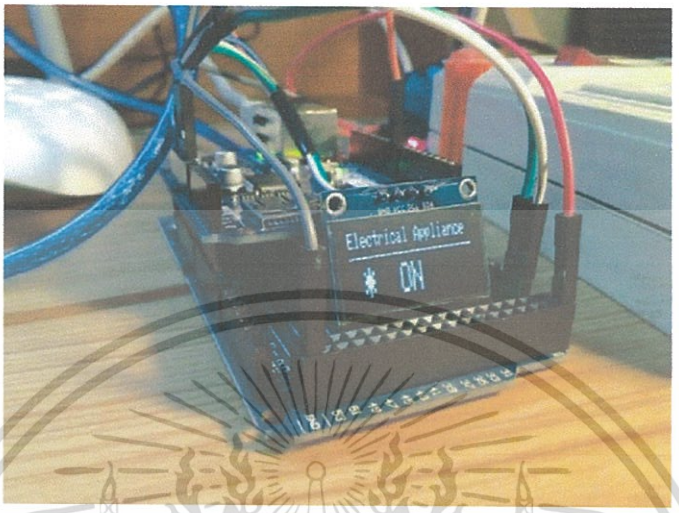
รูปที่ 4.3 หน้าจอแสดงข้อความเมื่อยังไม่มีการเชื่อมต่อ

หาก Router มีการจ่ายหมายเลข IP Address มาอย่างถูกต้อง หน้าจอก็จะแสดงหมายเลข IP Address ที่จ่ายมา ซึ่ง Router แต่ละรุ่นก็จะสุ่มจ่ายเลขไอพีมาให้ไม่เหมือนกัน จึงมีระบบแสดงหมายเลข IP Address ที่หน้าจอ เพื่อให้สะดวกต่อการใช้งาน และเป็น URL ที่จะใช้เข้า Web Server



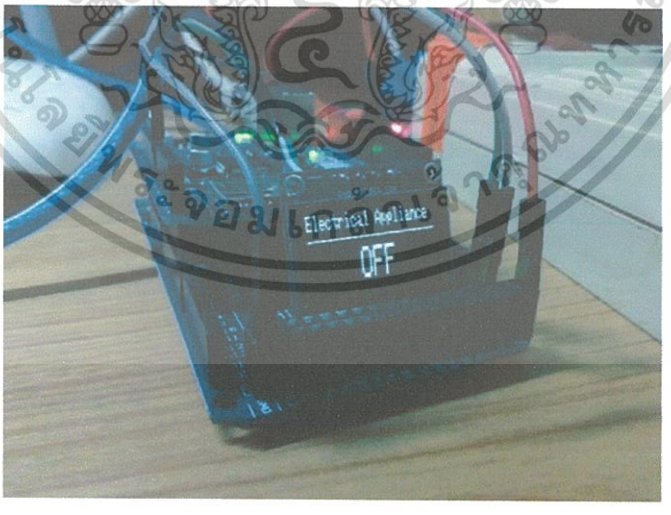
รูปที่ 4.4 หน้าจอแสดงข้อความเมื่อเชื่อมต่อแล้ว

เมื่อเข้าไปที่ Web Server ตาม URL ที่แสดงบนหน้าจอ เราก็สามารถควบคุมการเปิด-ปิดเครื่องใช้ไฟฟ้าได้ หากเรากดปุ่ม TURN ON เพื่อเปิดเครื่องใช้ไฟฟ้า หน้าจอก็จะแสดงสถานะว่าเครื่องใช้ไฟฟ้ามีการ ON อยู่



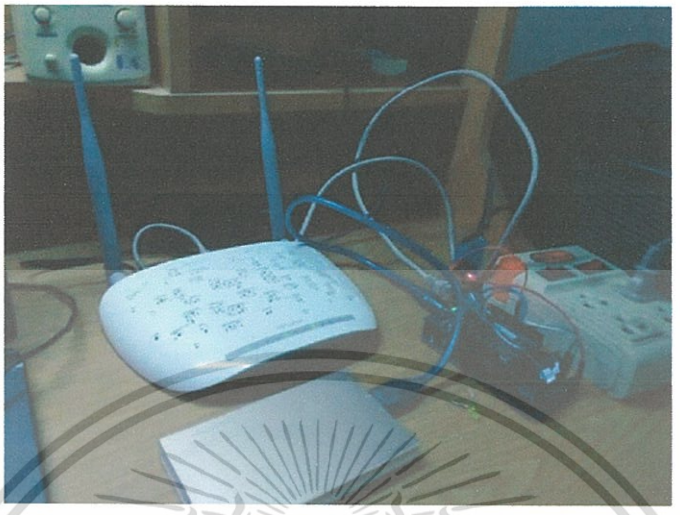
รูปที่ 4.5 หน้าจอแสดงข้อความขณะกำลังเปิดเครื่องใช้ไฟฟ้า

หากเรากดปุ่ม TURN OFF เพื่อเปิดเครื่องใช้ไฟฟ้า หน้าจอก็จะแสดงสถานะว่าเครื่องใช้ไฟฟ้ามีการ OFF อยู่



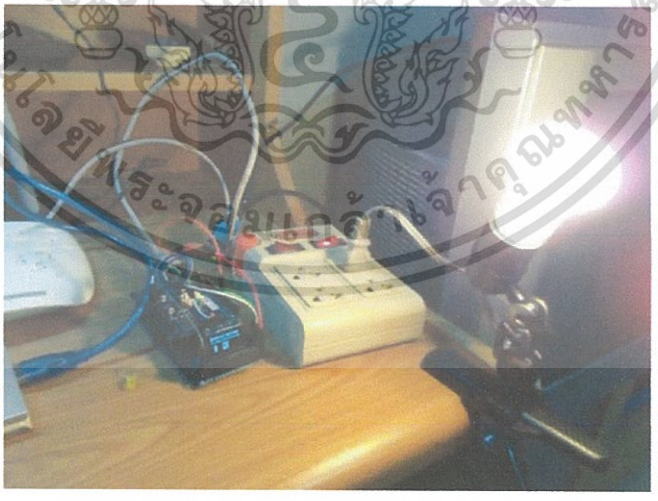
รูปที่ 4.6 หน้าจอแสดงข้อความขณะกำลังเปิดเครื่องใช้ไฟฟ้า

ในการจ่ายไฟเลี้ยงให้กับเครื่องนั้น เราสามารถใช้ Power Bank จ่ายให้ได้ เพราะมีใช้แรงดัน 5V กินกระแส 1 A ซึ่งก็จะช่วยอำนวยความสะดวกในการพกพาขึ้น



รูปที่ 4.7 ชุดอุปกรณ์ที่ใช้ในการทดลอง

ทดลองปิดเปิดเครื่องใช้ไฟฟ้า โดยทดลองปิด-เปิดผ่านระยะไกลออกไปเรื่อยๆ พบว่าระบบมีการตอบสนองได้ดี สามารถควบคุมผ่านระยะไกลได้ถึง 80 เมตร ทั้งนี้ขึ้นอยู่กับความสามารถของ Router ที่ใช้ด้วย



รูปที่ 4.8 ชุดทดลองขณะกำลัง ON

บทที่ 5
สรุปผลการทดลอง

5.1 สรุปผลการทดลอง

จากการทดลองโครงงาน ระบบควบคุมอุปกรณ์ไฟฟ้าผ่านเครือข่ายนั้น ในส่วนของชิ้นงานจะใช้พัดลมขนาดเล็กกับหลอดไฟในการทดลอง โดยเริ่มการทำงานจากการกดที่ปุ่ม Reset บอร์ดอาร์ดูโน่พบว่าที่หน้าจอแสดงผลขึ้นภาพว่า WELCOME จากนั้น ตัวบอร์ดจะเริ่มค้นหาเครือข่ายบริเวณนั้น จึงเมื่อพบเครือข่ายแล้วระบบทำการเชื่อมต่อเครือข่ายเรียบร้อยส่งผลให้หน้าจอแสดงผลขึ้นภาพว่า CONNECTED แต่เมื่อทดลองขณะที่ปิดเครือข่ายจะส่งผลให้หน้าจอแสดงผลขึ้นภาพว่า DISCONNECTED แล้วจะแสดงหมายเลข IP Address ขึ้นมา จากนั้นจึงนำหมายเลข IP Address นั้นมาป้อนเข้าที่เบราว์เซอร์ ซึ่งเบราว์เซอร์ที่ใช้ จะสามารถใช้ได้กับ UC Browser, Internet Explorer, Apple Safari เท่านั้น

เมื่อป้อนหมายเลข IP Address เรียบร้อยแล้วจะขึ้นภาพปุ่ม 2 ปุ่ม คือ SWITCH ON และ SWITCH OFF จากการทดลองพบว่าเมื่อกดที่ปุ่ม SWITCH ON ทำให้หน้าจอแสดงผลขึ้นภาพว่า ON ส่งผลให้เครื่องใช้ไฟฟ้าทำงาน ในที่นี้คือพัดลมเริ่มหมุน และ โคมไฟส่องสว่าง จากนั้นทำการกดที่ปุ่ม SWITCH OFF ทำให้หน้าจอแสดงผลขึ้นภาพว่า OFF ส่งผลให้พัดลมเริ่มหยุดหมุน และ โคมไฟดับลง ทั้งนี้ได้ทำการทดลอง ในระยะต่างๆพบว่าระบบสามารถสั่งการได้ ในระยะที่เครือข่ายครอบคลุม

5.2 ประโยชน์ที่ได้รับ

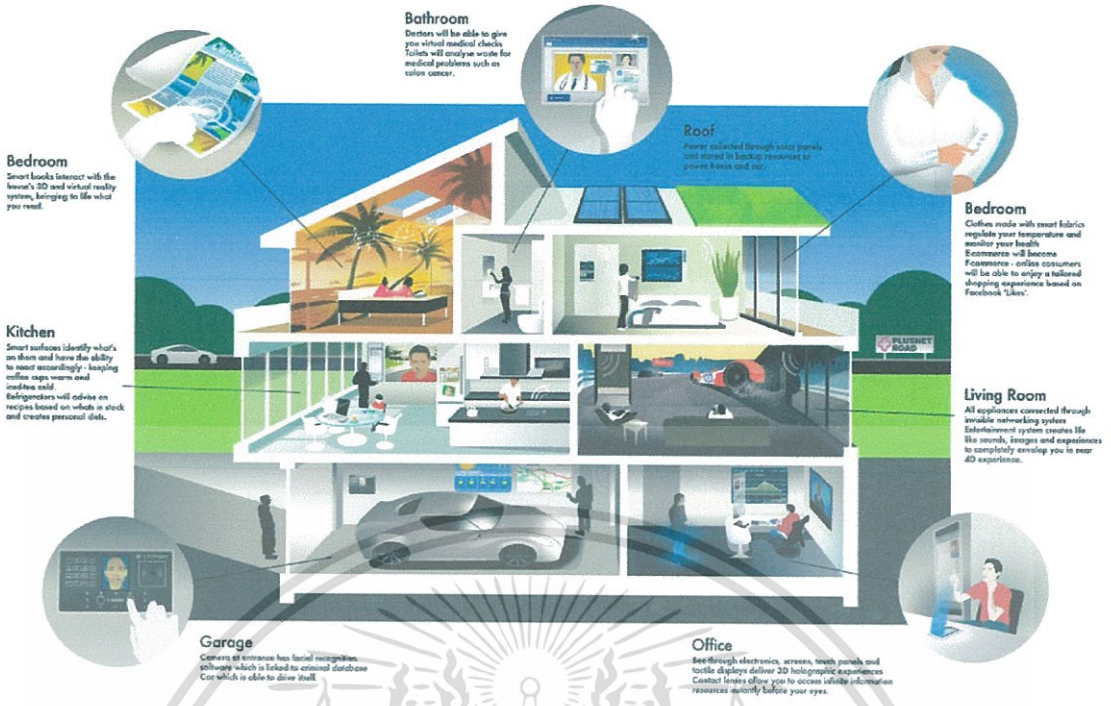
1. ได้ทราบถึงโครงสร้างและหลักการทำงานของ IoT (Internet of Things)
2. สามารถควบคุม การเปิด-ปิดเครื่องใช้ไฟฟ้า ด้วย IoT (Internet of Things)
3. ได้ทราบถึงแนวทางในการนำ IoT ไปประยุกต์ใช้ให้เกิดประโยชน์ในด้านต่างๆ
4. ได้ทราบถึงแนวทางในการพัฒนาหรือต่อยอดโครงงานนี้ต่อไป ให้มีความทันสมัย
5. สามารถทำเป็นธุรกิจได้และยังเป็นสิ่งที่เข้ามาในชีวิตประจำวันของเรามากขึ้น เพื่อช่วยอำนวยความสะดวกให้แก่ผู้ใช้งาน

5.3 ข้อเสนอแนะ

การทดลองครั้งนี้สามารถต่อยอดพัฒนาเทคโนโลยี Smart Home ได้ในอนาคต ทำให้สามารถควบคุมอุปกรณ์ไฟฟ้าได้จากระยะไกล เมื่อไม่มีผู้คนเข้าถึงอุปกรณ์ไฟฟ้าได้ในเวลานั้น ซึ่งในที่อยู่อาศัยที่มีระบบไฟฟ้าขนาดเล็ก เช่น บ้านเรือน ห้องเช่า อาจจะไม่ได้ใช้ประโยชน์จากระบบนี้มากนัก แต่ในห้างสรรพสินค้า บริษัทขนาดใหญ่ ที่มีพื้นที่มากนั้นการที่ควบคุมอุปกรณ์ไฟฟ้าทุกชนิดด้วยเครือข่าย ไม่ว่าจะควบคุมด้วยโทรศัพท์มือถือ หรือคอมพิวเตอร์นั้น ทำให้สะดวกกว่า และใช้เวลาน้อยกว่ามาก

ปัญหาที่เกิดขึ้นในการทดลองครั้งนี้ เกิดปัญหาในเรื่องของ การซื้อของในระยะเวลากระชั้นชิด ทำให้มีผู้คนมาซื้ออุปกรณ์เป็นจำนวนมาก ส่งผลให้การทำงานล่าช้า จึงควรต้องวางแผนและแบ่งเวลาซื้ออุปกรณ์ในการทำโครงงานให้เหมาะสม

การทดลองครั้งนี้ ทำให้ทราบว่าควรให้ความใส่ใจในเรื่องความสามารถในการควบคุมอุปกรณ์ไฟฟ้า ว่าระบบควบคุมอุปกรณ์ไฟฟ้าผ่านเครือข่ายนั้น สามารถควบคุมอุปกรณ์ไฟฟ้าได้ไกลที่สุดเป็นระยะเท่าไร และมีสิ่งกีดขวางระหว่างอุปกรณ์ไฟฟ้าจะส่งผลให้ควบคุมได้อยู่หรือไม่ แต่อย่างไรก็ตาม ระบบควบคุมการปิดเปิดเครื่องใช้ไฟฟ้า เป็นระบบแบบทางเดียว (One way system) การต่อยอด คือ การทำระบบตรวจสอบย้อนหลัง (Feedback) เพื่อตรวจสอบว่าเครื่องใช้ไฟฟ้าเปิดจริงหรือไม่ ในกรณีที่ไม่ได้ต่อเครื่องใช้ไฟฟ้าเข้ากับปลั๊กไฟ ควรจะให้มีการ Feedback ของสัญญาณไปยัง Router เพื่อแสดงให้กับผู้ใช้งานผ่าน Web Browser ว่าเครื่องใช้ไฟฟ้าไม่ได้ต่อเข้ากับแหล่งจ่ายไฟ ระบบการแจ้งเตือนนี้ คาดว่าน่าจะต่อยอดโครงงานนี้ต่อไปได้อีก และการต่อยอดในอีกเรื่องหนึ่ง คือ การเพิ่มช่องทางการควบคุมการปิดเปิดเครื่องใช้ไฟฟ้าให้มากกว่า 1 ช่องทาง โดยทำเพิ่มต่อจากต้นแบบเดิม คาดว่าน่าจะสามารถทำได้เช่นกัน ทั้งหมดนี้เป็นการต่อยอดในเรื่อง Smart Home คือ การประยุกต์ใช้ Internet ให้มีประโยชน์ต่อชีวิตประจำวันของมนุษย์ให้มากขึ้น คาดว่าระบบนี้น่าจะมีการใช้งานอย่างแพร่หลายในอนาคต ดังรูปที่ 5.1



รูปที่ 5.1 การนำเทคโนโลยีของอินเตอร์เน็ตมาอำนวยความสะดวกภายในบ้าน

5.4 ปัญหาที่พบ

การใช้งานระบบอุปกรณ์เปิดปิดเครื่องใช้ไฟฟ้า จำเป็นที่จะต้องทราบ IP Address ก่อนถึงจะติดต่อกันได้ เนื่องจากว่าการติดต่อสื่อสารระหว่างเครื่อง server (ผู้ให้บริการ) กับ เครื่อง Client (ผู้ติดต่อขอบริการ) IP Address เปรียบเสมือนที่อยู่ที่จะทำการติดต่อไป โดย Device อุปกรณ์ต่างๆ เราจะถือว่าเป็น Client ที่จะมาติดต่อขอบริการการเปิดปิดเครื่องใช้ไฟฟ้า ดังนั้น Client จำเป็นที่จะต้องทราบ IP Address ของเครื่อง Server ก่อนที่จะติดต่อ เมื่อทราบแล้ว ถึงจะติดต่อไปได้ การใช้งานก็จำเป็นที่จะต้องกรอก IP Address ลงไปใน Web Server ด้วย แต่เครื่อง Server เป็นผู้ที่ให้บริการไม่จำเป็นที่จะต้องทราบ IP Address ของเครื่อง Client ก็ได้ และ เมื่อทำการเชื่อมต่อเรียบร้อยแล้ว สั่งให้รีเลย์เปิดปิดเครื่องใช้ไฟฟ้า เราไม่สามารถทราบได้เลยว่า เครื่องใช้ไฟฟ้านั้นได้รับกระแสหรือไม่ กล่าวถึงในกรณีที่ Load (เครื่องใช้ไฟฟ้า) อยู่ในสภาวะ Open circuit (เช่น โคมไฟที่ไม่มีหลอดไฟ) เป็นปัญหาที่จะต้องได้รับการพัฒนาต่อยอดไปอีก เพื่อให้ระบบเปิดปิดเครื่องใช้ไฟฟ้ามีความสมบูรณ์มากยิ่งขึ้น และไม่เป็นอันตราย ในขณะที่อยู่ในสภาวะ Open circuit ฉะนั้นการต่อยอดที่สำคัญจะทำในส่วนของ Feedback System เพื่อตรวจสอบย้อนหลังว่ามีการจ่ายกระแสไฟฟ้าให้กับเครื่องใช้ไฟฟ้าจริงหรือไม่ และปัญหาในหัวข้อต่อไป

คือ ระยะเวลาที่เปิดเครื่องใช้ไฟฟ้า ซึ่งผู้ใช้งานจะไม่ทราบเลยว่าเครื่องใช้ไฟฟ้าเปิดมาเป็นเวลานานแค่ไหนแล้ว ระบบที่สามารถเพิ่มไปได้ คือระบบ BCD Counter ไว้ใช้สำหรับแสดงผลระยะเวลาที่วงจรทำงาน โดยตัวเลขที่แสดงออกมา จะเป็นในลักษณะของ 7 Segment ซึ่งระบบนี้จะต้องใช้ความรู้เรื่องวงจรดิจิตอล อาทิเช่น JK Flip Flop และ Gate ต่างๆ และปัญหาข้อสุดท้าย คือ เรื่องของสิ่งกีดขวาง ที่จะส่งผลต่อพิสัยความแรงของสัญญาณจากเราท์เตอร์ เมื่อเครื่อง client พ้นจากพิสัยการส่งสัญญาณ การเชื่อมต่อจะถูกตัดขาดได้

สรุปปัญหาที่พบ

1. ระบบไม่สามารถตรวจสอบได้ว่าเครื่องใช้ไฟฟ้าอยู่ในสภาวะ Open Circuit หรือไม่ ซึ่งอาจจะก่อให้เกิดอันตรายได้ เมื่อมีคนที่ไม่ทราบมาสัมผัสกับขั้วโลหะที่มีแรงดันตกคร่อม แต่ไม่มีโหลด (เครื่องใช้ไฟฟ้า) ได้

2. ระบบไม่สามารถระบุเวลาที่เปิดเครื่องใช้ไฟฟ้าได้ ว่าเปิดมาเป็นเวลานานแค่ไหนแล้ว

3. ระยะการสั่งการเปิดปิด ยังขึ้นอยู่กับความแรงของสัญญาณจากเราท์เตอร์ ถ้าหากพ้นจากพิสัยของการส่งสัญญาณจากเราท์เตอร์แล้ว จะไม่มีการตอบสนองอีก แม้จะกดปุ่มเปิดปิดผ่าน Web Server แล้วก็ตาม

เอกสารอ้างอิง

[1] Internet of Things ค้นเมื่อ 2 กุมภาพันธ์ 2559,จาก https://en.wikipedia.org/wiki/Internet_of_Things

[2] โปรโตคอล ค้นเมื่อ 24 กุมภาพันธ์ 2559, จาก https://sites.google.com/site/40224prim/protocol

[3] Transistor Relay Driver Circuit ค้นเมื่อ 5 มีนาคม 2559, จาก http://www.electroschematics.com/6283/relay-driver/