ความรู้เบื้องต้นเครือข่ายไร้สาย WiFi

1. บทนำ

เทคโนโลยีการสื่อสารด้วยเครือข่ายไร้สาย (Wireless Local Area Network : Wireless LAN : WLAN) ได้เข้ามามีบทบาทสำคัญในปัจจุบันอย่างมาก เนื่องจากมีความคล่องตัวในการใช้งาน มีอิสระในการใช้งานสามารถเคลื่อนย้ายได้สะดวกไม่ยึดติดกับที่ อุปกรณ์สื่อสารไม่ว่าจะเป็นแบบพกพาหรือตั้งโต๊ะสามารถที่จะเชื่อมต่อถึงกันหรือเชื่อมต่อเข้ากับเครือข่ายจากตำแหน่งต่างๆ ที่อยู่ในรัศมีของสัญญาณได้โดยปราศจากความต้องการใช้สายนำสัญญาณในการเชื่อมต่อซึ่งเหตุนี้ทำให้การติดตั้งง่ายและประหยัดค่าใช้จ่ายในการเดินสายนำสัญญาณ โดยการติดต่อสื่อสารนั้นจะใช้การส่งคลื่นแม่เหล็กไฟฟ้าซึ่งอาจจะเป็นคลื่นย่านความถี่วิทยุ (Radio frequency: RF) หรือคลื่นอินฟาเรด ในการรับส่งข้อมูลระหว่างอุปกรณ์สื่อสารด้วยกันในแต่ละเครื่องผ่านสื่อกลางนำสัญญาณอากาศ ที่มีความสามารถทะลุทะลวงผ่านกำแพง ผนัง เพดาน และสิ่งก่อสร้างต่างๆ ได้

WiFi (Wireless Fidelity) เป็นชื่อขององค์กรหนึ่งที่ใช้เรียกและทำหน้าที่ทดสอบ รับรองอุปกรณ์หรือผลิตภัณฑ์ของเครือข่ายไร้สาย ให้สามารถติดต่อสื่อสารกันได้ ตามมาตรฐานการทำงานของระบบเครือข่ายไร้สาย IEEE802.11 ซึ่งกำหนดขึ้นโดย สถาบันวิชาชีพวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ (Institute of Electrical and Electronics Engineers: IEEE) หรือไอทริปเปิ้ลอี ซึ่งเป็นมาตรฐานกลางที่นำมาใช้เพื่อเป็นรูปแบบที่จะทำการเชื่อมโยงอุปกรณ์เครือข่ายไร้สายเข้าด้วยกันบนระบบเครือข่ายได้ โดยมีสมาคมการค้า Wi-Fi Alliance ที่ถูกจัดตั้งขึ้นนั้นเป็นเจ้าของเครื่องหมายการค้า Wi-Fi ในส่วนอุปกรณ์ที่ผ่านตามมาตราฐานจะได้รับตรา Wi-Fi certified และอุปกรณ์นั้นจะสามารถติดต่อสื่อสารกับอุปกรณ์ตัวอื่นที่มีตราได้ด้วยเช่นกัน ดังนั้น Wi-Fi (อ่านว่า ไวไฟ) จึงนิยมเรียกชื่อเป็นตัวแทนเทคโนโลยีเครือข่ายไร้สาย (Wireless LAN)

โดยในที่นี้จะกล่าวถึงความรู้เบื้องต้นเกี่ยวกับเครือข่ายไร้สาย ซึ่งประกอบด้วยหัวข้อดังต่อไปนี้

1. บทนำ
2. วิวัฒนาการของมาตรฐานเครือข่ายไร้สาย IEEE 802.11
3. ลักษณะการเชื่อมต่อของอุปกรณ์เครือข่ายไร้สาย WiFi
4. กลไกรักษาความปลอดภัย

2. วิวัฒนาการของมาตรฐานเครือข่ายไร้สาย IEEE 802.11

IEEE 802.11 เป็นมาตรฐานเครือข่ายไร้สายที่มีวิวัฒนาการเรื่อยมาหลายรูปแบบ โดยได้มีการกำหนดมาตรฐานต่างๆ เป็นอักษรย่อในที่จะกล่าวถึงเฉพาะมาตรฐานที่นิยมใช้งานกันอยู่ในปัจจุบัน ได้แก่ IEEE802.11, IEEE802.11a, IEEE802.11b, IEEE802.11g, IEEE802.11n, และ IEEE802.11ac โดยแต่ละมาตรฐานใช้คลื่นความถี่และมีความเร็วในการรับส่งข้อมูลที่แตกต่างกันมีรายละเอียดดังต่อไปนี้

- IEEE 802.11-1997 มาตรฐานแรกสุด ในปี ค.ศ. 1997 ใช้คลื่นความถี่ 2.4 Ghz มีความเร็วที่ 2 Mbps โดยได้ระยะครอบคลุมอยู่ที่ 66 ฟุตสำหรับในอาคาร และ 330 ฟุตสำหรับภายนอกอาคาร ซึ่งเหมาะกับการใช้งานในห้องใดห้องหนึ่งเท่านั้น

- IEEE 802.11a – ตีพิมพ์มาตรฐานหรือใช้งานในปี ค.ศ. 1999 ใช้คลื่นความถี่ 5 GHz มีความเร็วได้สูงสุดถึง 54 Mbps ซึ่งเกิดจากการใช้เทคโนโลยีที่เรียกว่า OFDM (Orthogonal Frequency Division Multiplexing) เพื่อปรับปรุงความเร็วในการส่งข้อมูลบนความถี่ 5Ghz ซึ่งความถี่นี้จะมีคลื่นรบกวนน้อยกว่าความถี่ 2.4 Ghz ที่มาตรฐานอื่นใช้กัน และที่ความเร็วนี้ยังสามารถทำการแพร่ภาพและข่าวสารที่ต้องการความละเอียดสูงได้ อย่างไรก็ตามมาตรฐาน IEEE 802.11a ก็มีข้อเสียในการใช้งาน คือ คลื่นความถี่ 5 GHz ในบางประเทศย่านความถี่นี้ไม่สามารถนำมาใช้งานได้อย่างสาธารณะ ในส่วนของรัศมีของการแพร่กระจายสัญญาณก็มีระยะทางค่อนข้างสั้นกว่าอุปกรณ์ที่ใช้คลื่นความถี่ 2.4 GHz คือ ประมาณ 35 เมตร ในโครงสร้างปิด 120 เมตรในที่โล่งแจ้ง และราคาอุปกรณ์ IEEE 802.11a ก็ยังมีราคาสูงกว่าเมื่อเทียบกับอุปกรณ์ในมาตรฐาน IEEE 802.11b ซึ่งจะกล่าวในหัวข้อต่อไป

- IEEE 802.11b - ตีพิมพ์มาตรฐานหรือใช้งานเมื่อปี ค.ศ. 1999 ใช้คลื่นความถี่ 2.4 GHz มีความเร็วสูงสุดที่ 11 Mbps โดยปรับปรุงความสามารถของอุปกรณ์ให้รับส่งข้อมูลที่สูงขึ้นด้วยการใช้เทคโนโลยีที่เรียกว่า CCK (Complimentary Code Keying) กับ DSSS (Direct Sequence Spread Spectrum) บนคลื่นความถี่ 2.4 GHz ซึ่งเป็นย่านความถี่ที่เรียกว่า ISM (Industrial Scientific and Medical) โดยทางสากลได้ถูกจัดสรรไว้สำหรับการใช้งานสาธารณะโดยเฉพาะด้านวิทยาศาสตร์ อุตสาหกรรม และการแพทย์ ข้อดีของการใช้อุปกรณ์ในมาตรฐาน IEEE 802.11b นี้คือ มีความสามารถในการส่งรัศมีคลื่นสัญญาณไปได้ไกลประมาณ 38 เมตรในโครงสร้างปิดและ 140 เมตรในที่โล่งแจ้ง รวมถึงสัญญาณสามารถทะลุทะลวงโครงสร้างตึกกำแพงได้ดีกว่าอุปกรณ์ที่รองรับในมาตรฐาน IEEE 802.11a เนื่องจากมีการใช้คลื่นความถี่ที่ต่ำกว่า ผลิตภัณฑ์อุปกรณ์เครือข่ายไร้สายภายใต้มาตรฐาน IEEE 802.11b นี้ได้รับการผลิตออกมาเป็นจำนวนมาก ตัวอย่างอุปกรณ์ที่ใช้ความถี่ย่านนี้ คือ IEEE 802.11, Bluetooth, โทรศัพท์ไร้สาย, และเตาไมโครเวฟ และที่สำคัญแต่ละผลิตภัณฑ์

ของแต่ละผู้ผลิตทุกยี่ห้อต้องผ่านการตรวจสอบจากสถาบัน Wi-Fi Alliance เพื่อตรวจสอบมาตรฐานของอุปกรณ์และความเข้ากันได้ของแต่ละผู้ผลิตให้สามารถทำงานร่วมกันได้

- IEEE 802.11g - ตีพิมพ์มาตรฐานหรือใช้งานเมื่อปี ค.ศ. 2003 ใช้คลื่นความถี่ 2.4 Ghz มีความความเร็วประมาณ 54 Mbs ซึ่งเกิดจากการที่ได้นำเอาเทคโนโลยี OFDM ที่ใช้อยู่บนคลื่นความถี่ 5 Ghz ของ 802.11a แล้วมาพัฒนาต่อยอดบนความถี่ 2.4 Ghz มาตรฐานนี้เป็นที่ยอมรับจากผู้ใช้เป็นจำนวนมาก และมีความเร็วที่สูงกว่ามาตรฐาน 802.11b

- IEEE 802.11n - ตีพิมพ์มาตรฐานหรือใช้งานเมื่อปี ค.ศ. 2009 ใช้ทั้งคลื่นความถี่ 2.4 และ 5 GHz ซึ่งเป็นที่มาของคำว่า Dual-Band โดยมีความเร็วในการรับส่งข้อมูลสูงสุดถึง 54-600 Mbps เป็นมาตรฐานแรกที่ใช้กับเสาอากาศแบบ MIMO (Multi-Input Multi-Output) มีความสามารถในการส่งคลื่นสัญญาณ ได้ระยะประมาณ 70 เมตรในโครงสร้างปิด และ 250 เมตรในที่โล่งแจ้ง มีความสามารถในการป้องกันสัญญาณกวนจากอุปกรณ์อื่นๆ ที่ใช้ความถี่ 2.4GHz เหมือนกัน และสามารถรองรับอุปกรณ์มาตรฐาน IEEE 802.11b และ IEEE 802.11g ได้

- IEEE 802.11ac - ตีพิมพ์มาตรฐานหรือใช้งานเมื่อปี ค.ศ. 2013 ใช้คลื่นความถี่ที่ 5 GHz มีอัตราความเร็วในการรับส่งข้อมูลระดับ Gbps โดยสามารถแบ่งเป็น 2 ประเภท คือ 802.11ac Wave 1 มีความเร็วรับส่งข้อมูลสูงสุดถึงประมาณ 1.3 Gbps มีแบนด์วิธที่กว้างสูงสุด 80 Mhz โดยทำงานแบบเทคโนโลยี SU-MIMO (Single User - MIMO) โดย access point จะมีความสามารถส่งข้อมูลให้ผู้ใช้งานได้ทีละ 1 เครื่องเท่านั้น ซึ่งเมื่อมีผู้ใช้งานพร้อมกันมากขึ้นอัตราการรับส่งข้อมูล (Throughput) โดยรวมของเครือข่ายจะลดลงอย่างมาก และประเภท 802.11ac Wave 2 จะมีความเร็วรับส่งข้อมูลสูงสุดถึงประมาณ 3.4 Gbps มีแบนด์วิธที่กว้างสูงสุดถึง 160 Mhz ใช้เทคโนโลยี MU-MIMO (Multi User - MIMO) ที่จะช่วยให้ access point สามารถส่งข้อมูลไปให้ผู้ใช้ได้หลายๆเครื่องพร้อมกัน

ตารางมารตฐาน IEEE 802.11						
802.11 Protocol	Release date	Frequency (GHz)	Bandwidth (MHz)	Stream Data Rate (Mbit/s)	Allowable MIMO streams	Modulation Antenna Tech.
802.11	Jun 1977	2.4	22	1-2	1	DSSS, FHSS
802.11a	Sep 1999	5	20	6-54	1	OFDM (SISO)
		3.7				
802.11b	Sep 1999	2.4	22	1-11	1	DSSS (SISO)
802.11g	Jun 2003	20	6-54	6-54	1	OFDM, DSSS (SISO)
802.11n	Oct 2009	2.4/5	20	Up to 288.8	4	OFDM (MIMO)
			40	Up to 600		
802.11ac	Dec 2013	5	20	Up to 346.8	8	OFDM (MIMO)
			40	Up to 800		
			80	Up to 1733.2		
			160	Up to 3466.8		

DSSS: Direct-sequence spread spectrum

FHSS: Frequency-hopping spread spectrum

SISO: Single input single output

MIMO: Multi-Input Multi-Output

3. ลักษณะการเชื่อมต่อของอุปกรณ์เครือข่ายไร้สาย WiFi

การเชื่อมต่อเครือข่ายไร้สาย Wi-Fi ได้มีการกำหนดลักษณะการเชื่อมต่อของอุปกรณ์ภายในเครือข่ายไว้ 2 ลักษณะคือโหมด Infrastructure และโหมด Ad-Hoc หรือ Peer-to-Peer

- **โหมด Infrastructure**

การเชื่อมต่อกันอุปกรณ์เครือข่าย WiFi ในลักษณะของโหมด Infrastructure นั้นคือ โหมดที่อุปกรณ์ภายในเครือข่ายไร้สายระบบหนึ่งสามารถที่จะเชื่อมต่อกับเครือข่ายอื่นได้ ซึ่งอุปกรณ์ในโหมดนี้จะประกอบไปด้วย 2 ประเภทด้วยกัน คือ ประเภทแรกสถานีผู้ใช้งาน (Client Station) กล่าวอีกนัยหนึ่งก็คืออุปกรณ์ปลายทาง (End User) เช่น คอมพิวเตอร์ (Desktop, Laptop), โทรศัพท์มือถือ เป็นต้น ซึ่งอุปกรณ์นั้นจะมี Client Adapter หรือ Wireless Lan Card เพื่อใช้รับส่งข้อมูลผ่านสัญญาณ Wi-Fi และประเภทที่สองสถานีแม่ข่าย (Access Point) ซึ่งทำหน้าที่ต่อเชื่อมสถานีผู้ใช้งานเข้ากับเครือข่ายอื่นโดยทั่วไปแล้วจะเป็นเครือข่าย

IEEE 802.3 Ethernet LAN หรือเชื่อมด้วยสายนำสัญญาณเข้ากับระบบ ลักษณะการทำงานในโหมด Infrastructure นี้ คือสถานีผู้ใช้จะสามารถรับส่งข้อมูลกับสถานีแม่ข่ายที่ให้บริการแก่สถานีผู้ใช้งานอยู่ในเครือข่ายเดียวเท่านั้น ส่วนสถานีแม่ข่ายจะทำหน้าที่ส่งต่อ (Forward) ข้อมูลที่ได้รับจากสถานีผู้ใช้ไปยังจุดหมายปลายทางที่อยู่เครือข่ายอื่น

Basic Service Set (BSS) หมายถึง บริเวณของเครือข่าย IEEE 802.11 WLAN ที่มีสถานีแม่ข่าย 1 สถานี ทุกสถานีผู้ใช้งานทุกสถานีใน BSS จะต้องสื่อสารข้อมูลผ่านสถานีแม่ข่ายภายในของตนเองเท่านั้น

Extended Service Set (ESS) หมายถึง บริเวณของเครือข่าย IEEE 802.11 WLAN ที่ประกอบด้วย BSS มากกว่า 1 BSS ซึ่งสามารถเชื่อมต่อถึงกันได้ สถานีผู้ใช้สามารถเคลื่อนย้ายจาก BSS หนึ่งไปยังอีก BSS หนึ่งได้ โดย BSS จะติดต่อสื่อสารกันเพื่อทำการโอนย้ายการให้บริการสำหรับสถานีผู้ใช้ ซึ่งการทำงานในลักษณนี้จะเรียกว่า Roaming

- **โหมด Ad-Hoc หรือ Peer-to-Peer**

การเชื่อมต่อกันอุปกรณ์เครือข่าย WiFi ในลักษณะของโหมด Ad-Hoc หรือ Peer-to-Peer นั้นคือโหมดที่อุปกรณ์ภายในเครือข่ายไร้สายไม่สามารถที่จะเชื่อมต่อกับเครือข่ายอื่นได้และเป็นเครือข่ายระบบปิดที่ไม่มีสถานีแม่ข่าย ลักษณะการทำงานในโหมด Ad-Hoc นี้ คือสถานีผู้ใช้หนึ่งจะสามารถรับส่งข้อมูลกับสถานีผู้ใช้หนึ่งที่อยู่ภายในเครือข่ายเดียวกันได้โดยตรงเท่านั้นไม่ผ่านสถานีแม่ข่าย ซึ่งบริเวณของเครือข่าย Wi-Fi ในโหมด Ad-Hoc ดังกล่าวนี้จะเรียกว่า Independent Basic Service Set (IBSS)

4. กลไกรักษาความปลอดภัย

กลไกรักษาความปลอดภัยสำหรับสร้างความปลอดภัยให้กับเครือข่ายไร้สาย Wi-Fi โดยมีชื่อเรียกได้แก่ WEP (Wired Equivalent Privacy) และ WPA (Wi-Fi Protected Access) มีรายละเอียดดังนี้

WEP (Wired Equivalent Privacy) คือรูปแบบการเข้าหรัส และถอดรหัสใช้เป็นอันเดียวกัน ใช้กุญแจ (key) ในการเข้ารหัสชุดเดียวกันไม่มีการเปลี่ยนแปลงตลอดการใช้งาน นอกจากนี้รหัสที่ใช้สามารถถูกถอดรหัสได้จากผู้ใช้งานโดยตรง ดังนั้นกลไกการเข้ารหัสแบบ WEP นี้ถือว่าไม่มีความปลอดภัยเท่าที่ควรเพราะมีช่องโหว่ให้สำหรับโจมตีอยู่มาก

WPA (Wi-Fi Protected Access) คือ รูปแบบการเข้ารหัสและถอดรหัสที่มีกุญแจ (Key) เปลี่ยนแปลงตลอดการใช้งาน กลไลนี้เรียกว่า TKIP (Temporal Key Integrity) ซึ่งเป็นกุญแจแบบชั่วคราวโดยจะกำหนดให้ใช้เฉพาะส่วนเป็นราย ๆ ไป ทำให้ยากแก่การคาดเดา กลไกนี้ยังทำงานร่วมกับระบบ MIC (Message

Integrity Code) ที่ช่วยตรวจสอบการปลอมแปลงของข้อมูลระหว่างการสื่อสารจากผู้บุกรุก นอกจากนี้ WPA ยังมีระบบพิสูจน์ตรวจสอบสิทธิ์ โดยการใช้มาตรฐานของ Extension Authentication Protocol (EAP) และเทคโนโลยีที่เรียกว่า Pre-shared Key (PSK) จะเห็นได้ว่ากลไลการเข้ารหัสแบบ WPA เป็นระบบที่มีมาตรฐานรักษาความปลอดภัยที่สูงกว่าแบบ WEP

WPA2 (Wi-Fi Protected Access2) คือ รูปแบบกลไกการรักษาความปลอดภัยที่เหมือนกับ WPA แต่จะพัฒนากลไกการเข้ารหัสและถอดรหัสเสริมความปลอดภัยมากขึ้น คือใช้โปรโตคตอล เรียกว่า Counter-Mode/CBC-MAC Protocol (CCMP) เป็นโปรโตคอลที่ใช้เพื่อการเข้ารหัสข้อมูล AES (Advanced Encryption Standard) ซึ่งเป็นการเข้ารหัสที่ซับซ้อนปลอดภัยกว่า TKIP

การทำงานของมาตรฐาน WPA ประกอบด้วย 2 โหมด คือ โหมด Enterprise และโหมด Personal ทั้งสองโหมดนี้ต่างก็ให้บริการเข้ารหัสและการพิสูจน์ตัวตนเช่นเดียวกัน โดยทั่วไปอุปกรณ์เครือข่ายไร้สายจะเป็นโหมด Personal และในส่วนของโหมด Enterprise จะเป็นการให้บริการรักษาความปลอดภัยในระดับองค์กรขนาดใหญ่ โดยจะนำโปรโตคอลยืนยันตัวตน (Extension Authentication Protocol:EAP) มาใช้ร่วมกับเครื่องคอมพิวเตอร์แม่ข่ายยืนยันตัวตน (Authentication Server) ที่ให้บริการพิสูจน์ตัวตน เช่น RADIUS, LDAP เป็นต้น เพื่อความเพิ่มความรัดกุมปลอดภัยอีกขั้นในการพิสูจน์ตรวจสอบสิทธิ์ระหว่างผู้ใช้งาน (Client) กับอุปกรณ์กระจายสัญญาณ (Access Point) และระหว่างอุปกรณ์กระจายสัญญาณ (Access Point) กับเครื่องคอมพิวเตอร์แม่ข่าย (Server)

เอกสารอ้างอิง

[1] เครือข่ายไร้สายไวไฟ https://th.wikipedia.org/wiki/ไวไฟ

[2] มาตรฐาน IEEE802.11, https://th.wikipedia.org/wiki/IEEE_802.11

[3] IEEE802.11 Standard, https://en.wikipedia.org/wiki/IEEE_802.11

[4] มาตรฐาน IEEE 802.11 WLAN: ความรู้เบื้องต้น ช่องโหว่ และการรักษาความปลอดภัย (ตอนที่ 1) ศิวรักษ์ ศิวโมกษธรรม, 29 พฤษภาคม 2546,

[5] ระบบรักษาความปลอดภัยเครือข่ายไร้สาย (3), วิรินทร์ เมฆประดิษฐสิน, 23 กุมภาพันธ์ 2558