AuthenticationWimax Security

กิตติมา สนิทชน, ณัฏฐ์อินทรโก, ภานุวัตรอุทัยบาล, มัณฑนศิลป์ ผาโคตร,
ยุพินพูนศรีวิวัฒน์, สรไกรจันทอง, สุวรรณีวานมุลตรี, อัตพลคุณเลิศ

บทคัดย่อ

เอกสารนี้จัดทำขึ้นเพื่อศึกษาวิธีการรักษาความปลอดภัยในด้าน Authentication ของเครือข่ายไร้สายไวแมกซ์ ซึ่งเป็นเทคโนโลยีบรอดแบนด์ไร้สายความเร็วสูงที่ถูกพัฒนาขึ้นมาบนมาตรฐาน IEEE 802.16 จากความต้องการใช้งานบอร์ดแบนด์ไร้สายในขณะเคลื่อนที่ จึงได้เกิดการพัฒนามาตรฐาน IEEE802.16 ให้รองรับการใช้งานแบบเคลื่อนที่โดยตั้งชื่อกลุ่มว่า IEEE 802.16e มาตรฐานใหม่นี้มีความสามารถในการส่งกระจายสัญญาณในลักษณะจากจุดเดียวไปยังหลายจุด (Point-to-multipoint) ได้พร้อมๆ กัน โดยมีความสามารถรองรับการทำงานในแบบ Non-Line-of-Sight สามารถทำงานได้แม้กระทั่งมีสิ่งกีดขวาง (ต้นไม้ อาคาร) อีกทั้งในเรื่องของความปลอดภัยยังได้รับอนุญาต (authentication) ก่อนที่จะเข้าออกเครือข่ายและข้อมูลต่างๆ ที่รับส่งก็จะได้รับการเข้ารหัส (encryption) อีกด้วย ทำให้การรับส่งข้อมูลบนมาตรฐานตัวนี้มีความปลอดภัยมากขึ้น ในเอกสารนี้ได้นำเสนอ สถาปัตยกรรมด้านความปลอดภัยของมาตรฐาน IEEE 802.16 รูปแบบความปลอดภัยบนเครือข่ายไวแมกซ์ ภัยคุกคามที่เกิดขึ้นได้เพื่อโจมตีเครือข่ายและการป้องกันเครือข่ายจากภัยคุกคามเหล่านั้น ซึ่งในเอกสารนี้จะกล่าวถึง กระบวนการทำ Authentication ของ 802.16e โดยจะมีการทำอยู่ 4 ชนิดคือ 1. Symmetric Key ที่นำมาใช้ใน Authentication ใน Wimax นั้นมี 3ชนิดคือ DES, 3DES และ AES 2. Asymmetric Key Encryptions ที่นำมาใช้ใน Authentication ใน Wimax นั้นมี 1 ชนิดคือ RSA โดยนำมาใช้งานร่วมกับ X.509 3. EAP based Extensible Authentication Protocol (EAP) วิธีการของ EAP คือ กระทำผ่านสิ่งที่โอเปอเรเตอร์ออกให้ ไม่ว่าจะเป็น SIM หรือ X.509 ซึ่งมีหลายแบบ เช่น EAP-MD5, EAP-PEAP, EAP-TLS, EAP-TTLS, EAP-LEAP,EAP-FAST และ EAP-SPEAK เป็นต้น โดยจะทำการตรวจสอบกับเครือข่ายเอง เช่น AAA Server 4. ฟังก์ชั่น Hash อัลกอลิทึ่ม Hash ที่นำมาใช้งานในการ Authentication ใน Wimax นั้นมี 2 ชนิดคือ SHA-1 และ HMAC โดยในแต่ละชนิดได้ศึกษาทั้งข้อดีข้อเสีย และเปรียบเทียบกัน ซึ่งแต่ละวิธีที่นำมาใช้ในการ Authentication ใน Wimax นั้น สามารถป้องกันภัยคุกคามได้ต่างกันชนิดกัน

คำสำคัญ

WiMAX, Wimax Security, Authentication, Authentication Protocol,

I. บทนำ

WiMAXคือ Metropolitan Broadband Wireless Access หรือ “เครือข่ายบริการ อินเตอร์เน็ตไร้สายความเร็วสูง ที่มีพื้นที่ครอบคลุมบริเวณกว้าง” ซึ่งบรอดแบนด์ไร้สายความเร็วสูงนี้ถูกพัฒนาขึ้นบนมาตรฐานการสื่อสาร IEEE 802.16 [1] ซึ่งต่อมาก็ได้พัฒนามาอยู่บนมาตรฐาน IEEE 802.16a โดยได้มีการอนุมัติออกมาเมื่อเดือนมกราคม 2004 โดยสถาบันวิศวกรรมไฟฟ้าและอิเล็กทรอนิกส์ หรือ IEEE (Institute of Electrical and Electronics Engineers) ซึ่งมีระยะรัศมีทำการที่ 31 ไมล์ หรือประมาณ 48 กิโลเมตร อีกทั้งยังมีอัตราความเร็วในการรับส่งข้อมูล ไม่ว่าจะเป็นมัลติมีเดียที่มีทั้งภาพและเสียงหรือจะเป็นข้อมูลล้วน ๆ ก็ตามได้สูงสุดถึง 75 เมกกะบิตต่อวินาที (Mbps) โดยมาตรฐาน IEEE 802.16a หรือ WiMAXมีความสามารถในการส่งกระจายสัญญาณในลักษณะจากจุดเดียวไปยังหลายจุด (Point-to-multipoint) ได้พร้อมๆ กัน และยังรองรับการทำงานในแบบ Non-Line-of-Sight ได้คือทำงานได้แม้กระทั่งมีสิ่งกีดขวาง เช่น ต้นไม้ หรือ อาคารได้เป็นอย่างดี ส่งผลให้ไวแมกซ์ช่วยให้ผู้ที่ใช้งานสามารถขยายเครือข่ายเชื่อมต่ออินเตอร์เน็ตได้กว้างขวางด้วยรัศมีทำการถึง 31 ไมล์ หรือประมาณ 48 กิโลเมตร และมีอัตราความเร็วในการรับส่งข้อมูลสูงสุดถึง 75 Mbps มาตรฐาน IEEE 802.16a นี้ใช้งานอยู่บนคลื่นไมโครเวฟที่มีความถี่ระหว่าง 2-11 กิกะเฮิรตซ์ (GHz) และยังสามารถใช้งานร่วมกับอุปกรณ์มาตรฐานชนิดอื่นๆ ที่ออกมาก่อนหน้านี้ได้เป็นอย่างดี [2]

ตาราง 1 เปรียบเทียบเทคโนโลยีเครือข่ายแบบไร้สาย

เทคโนโลยี	มาตรฐาน	เครือข่าย	อัตราความเร็ว	ระยะทาง	ย่านความถี่
Wi-Fi	IEEE 802.11a	WLAN	สูงสุด 54Mbps	100 เมตร	5GHz
Wi-Fi	IEEE 802.11b	WLAN	สูงสุด 11Mbps	100 เมตร	2.4GHz
Wi-Fi	IEEE 802.11g	WLAN	สูงสุด 54Mbps	100 เมตร	2.4GHz
WiMAX	IEEE 802.16d	WMAN	สูงสุด 75Mbps (20MHz BW)	ปกติ 6.4 - 10 กิโลเมตร	Sub 11GHz
WiMAX	IEEE 802.16e	Mobile WMAN	สูงสุด 30Mbps (10MHz BW)	ปกติ 1.6 – 5 กิโลเมตร	2 - 6 GHz
WCDMA/UMTS	3G	WWAN	สูงสุด 2Mbps/10Mbps (HSDPA)	ปกติ 1.6 – 8 กิโลเมตร	1800, 1900, 2100MHz
CDMA2000 1x EV-DO	3G	WWAN	สูงสุด 2.4Mbps	ปกติ 1.6 – 8 กิโลเมตร	400, 800, 900, 1700, 1800, 1900, 2100MHz
EDGE	2.5G	WWAN	สูงสุด 348Kbps	ปกติ 1.6 – 8 กิโลเมตร	1900MHz
UWB	IEEE 802.15.3a	WPAN	110 – 480Mbps	10 เมตร	7.5GHz

1. มาตรฐาน IEEE 802.16 สามารถแยกได้ดังนี้

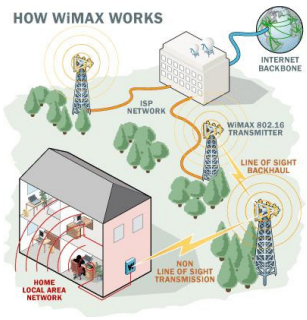
1) IEEE 802.16 เป็นมาตรฐานที่ให้ระยะทางการเชื่อมโยง1.6 – 4.8 กิโลเมตร เป็นมาตรฐานเดียวที่สนับสนุน LoS (Line of Sight) โดยมีการใช้งานในช่วงความถี่ที่สูงมากคือ 10-66GHz

2) IEEE 802.16a เป็นมาตรฐานที่แก้ไขปรับปรุงจาก IEEE 802.16 เดิม โดยใช้งานที่ความถี่ 2-11GHz ซึ่งคุณสมบัติเด่นที่ได้รับการแก้ไขจากมาตรฐาน 802.16 เดิม คือคุณสมบัติการรองรับการทำงานแบบที่ไม่อยู่ในระดับสายตา (NLoS-Non-Line-of-Sight) ทั้งยังมีคุณสมบัติการทำงานเมื่อมีสิ่งกีดขวาง อาทิเช่น ต้นไม้, อาคาร ฯลฯ นอกจากนี้ก็ยังช่วยให้สามารถขยายระบบเครือข่ายเชื่อมต่ออินเทอร์เน็ตไร้สายความเร็วสูงได้อย่างกว้างขวางด้วยรัศมีทำการที่ไกลถึง 31 ไมล์ หรือประมาณ 48 กิโลเมตรและมีอัตราความเร็วในการรับส่งข้อมูลสูงสุดถึง 75Mbps ทำให้สามารถรองรับการเชื่อมต่อการใช้งานระบบเครือข่ายของบริษัทที่ใช้สายประเภท ที1 (T1-type) กว่า 60 ราย และการเชื่อมต่อแบบ DSL ตามบ้านเรือนที่พักอาศัยอีกหลายร้อยครัวเรือนได้พร้อมกันโดยไม่เกิดปัญหาในการใช้งาน [1]

3) IEEE 802.16e เป็นมาตรฐานที่ออกแบบมาให้สนับสนุนการใช้งานร่วมกับอุปกรณ์พกพาประเภทต่างๆ เช่น อุปกรณ์พีดีเอ โน้ตบุ๊ก โทรศัพท์ไร้สาย เป็นต้น โดยให้รัศมีทำงานที่ 1.6 – 4.8 กิโลเมตร มีระบบที่ช่วยช่วยให้ผู้ใช้งานยังสามารถสื่อสารได้โดยให้คุณภาพในการสื่อสารที่ดีและมีเสถียรภาพขณะใช้งาน แม้ว่ามีการเคลื่อนที่อยู่ตลอดเวลาก็ตาม [3]

2. หลักการทำงานของไวแมกซ์

ไวแม็กซ์ (WiMAX) บนเทคโนโลยีแบบไร้สายมาตรฐานใหม่ IEEE 802.16 มีความสามารถในการใช้งานอย่างมีประสิทธิภาพสูง โดยใช้หลักการของเทคโนโลยี OFDM (Orthogonal Frequency Division Multiplexing) ซึ่งเป็นคลื่นความถี่ของวิทยุขนาดเล็กมาใช้ให้เกิดประโยชน์อย่างสูงสุด



รูปที่ 1 หลักการทำงานของ WiMAX

เทคโนโลยีไวแมกซ์จะจัดสรรคลื่นความถี่วิทยุในระดับ KHz ให้แก่ผู้ใช้ตามข้อกำหนดของคลื่นความถี่วิทยุ จนเกิดเป็นเครือข่ายแบบไร้สายที่มีขนาดใหญ่ และรองรับการรับส่งข้อมูลด้วยความเร็วสูง โดยใช้กลไกการเปลี่ยนคลื่นสัญญาณที่ให้ประสิทธิภาพสูง สามารถส่งสัญญาณออกไปได้ระยะไกล นอกจากนี้สถานีฐาน (Base Station) ยังสามารถพิจารณาความเหมาะสมในการรับส่งระหว่างความเร็วและระยะทางได้อีกด้วย

ในส่วนของพื้นที่บริการ ก็สามารถครอบคลุมพื้นที่ได้อย่างกว้างขวางโดยใช้เทคนิคของการแปลงสัญญาณที่มีความคล่องตัวสูงสำหรับการใช้งานบนมาตรฐาน IEEE 802.16a บนระบบเครือข่ายที่ใช้สถาปัตยกรรมแบบผสมผสาน (Mesh Topology) และเทคนิคการใช้งานกับเสาอากาศ แบบอัจฉริยะ (Smart Antenna) ที่ช่วยประหยัดต้นทุน และมีความน่าเชื่อถือสูง

3. ความปลอดภัยของเทคโนโลยี WiMAX

ระบบเครือข่ายไร้สาย เมื่อพูดถึงจุดที่น่าเป็นห่วงมากที่สุด นั่นก็คือ ด้านความปลอดภัย หลังจากที่ทุกระบบใช้เครือข่ายไร้สายและต้องทำทุกสิ่งทุกอย่างผ่านเครือข่าย สิ่งที่สำคัญที่ต้องนำมาพิจารณาเป็นอันดับแรกคือด้านความปลอดภัย นอกจากนี้เครือข่ายไร้สายที่เปิดให้ใช้อย่างอิสระ จะพบว่ามีความปลอดภัยต่ำเพราะฉะนั้นจึงมีการออกแบบระบบความปลอดภัยใหม่ ให้มีความแข็งแรงมากขึ้นในอดีต

เมื่อมองจาก end user ความปลอดภัยที่ต้องคำนึงถึงอันดับแรกคือ เรื่องของความเป็นส่วนตัวและความปลอดภัยของข้อมูล โดย user ต้องการการรับรองว่าจะไม่มีการดักฟังการกระทำของพวกเขาซึ่งทำได้โดยการ encryption ข้อมูล

หากมองจากผู้ให้บริการจะเห็นได้ว่าสิ่งที่สำคัญที่สุดด้านความปลอดภัยก็ คือ การป้องกันการเข้าถึงการบริการเครือข่ายอย่างไม่ถูกต้อง ซึ่งต้องมีการ authentication ที่ดี ซึ่งการauthentication

สามารถกระทำได้หลายระดับด้วยกันเช่นกระทำใน physical layer หรือ ใน transportL layer เป็นต้น โดยผู้ให้บริการต้องหาวิธีรองรับการเข้าใช้เครือข่ายอย่างไม่ถูกต้อง [2]

II. สถาปัตยกรรมด้านความปลอดภัยของมาตรฐานIEEE 802.16

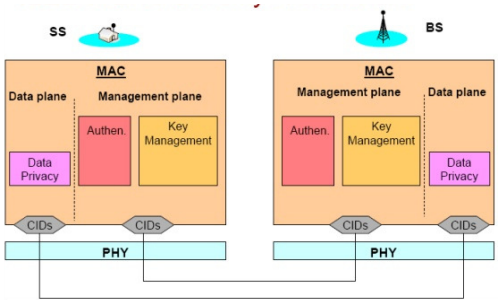
การรักษาความปลอดภัยในชั้น Security sub-layer ได้รับการนิยามใหม่ใน IEEE802.16e-2005 เนื่องจากความจริงที่ว่าการรักษาความปลอดภัยใน IEEE 802.16-2004 ยังมีภัยคุกคาม (เช่นไม่มีการรับรองความถูกต้องของสถานีฐาน) และต้องการความปลอดภัยสำหรับ mobile services ซึ่งจะไม่เหมือนกับการรักษาความปลอดภัยในบริการแบบคงที่ (fixed services) ใน IEEE802.16e-2005 มาตรฐานการรักษาความปลอดภัยชั้นย่อยของ WiMAXhas จึงถูกนิยามขึ้นมาใหม่

แผนการรักษาความปลอดภัยที่เกี่ยวข้องในงานสถาปัตยกรรม WiMAX network security (รวมถึงผู้ใช้ user authentication และอุปกรณ์device authentication), การเข้ารหัสข้อมูล (รวมถึงความสมบูรณ์และความลับของข้อมูล), การเข้าถึง (access control) และการจัดการกุญแจ (key management) การรักษาความปลอดภัยในชั้นย่อย (sub-layer) สามารถให้ความเป็นส่วนตัวในการตรวจสอบและรักษาความลับผ่านเครือข่ายไร้สายbroadband โดยใช้การแปลงการเข้ารหัสลับเพื่อให้ MAC protocol data units ดำเนินการในการเชื่อมต่อระหว่างสถานีสมาชิกและสถานีฐาน นอกจากนี้การรักษาความปลอดภัยเครือข่ายของสถานีฐานยังสามารถป้องกันการเข้าถึงอีกครั้งด้วยการ authorized access (ระบุตัวตน) นอกจากนี้กลไกการรักษาความปลอดภัยขั้นพื้นฐานยังเพิ่มความแข็งแกร่งด้วยใบรับรองดิจิตอล (digital-certificate-based) เพื่อตรวจสอบอุปกรณ์ในการเข้าถึงเครือข่าย โดยจะใช้ key management protocol ในการตรวจสอบ

การรักษาความปลอดภัยย่อยชั้น (Sub-layer) มีสองโปรโตคอลหลัก ดังต่อไปนี้

• data encapsulation protocol สำหรับการรักษาความปลอดภัยแพ็กเก็ตข้ามเครือข่ายถาวร BWA โปรโตคอลนี้กำหนดชุดที่สนับสนุนการเข้ารหัสลับ, ซึ่งก็คือการจับคู่เพื่อเข้ารหัสข้อมูลเพื่อตรวจสอบและกฎเพื่อประยุกต์ใช้อัลกอริทึม MAC PDU

• key management protocol (PKM)ให้กระจายการรักษาความปลอดภัยของ keying data จาก BS(สถานีฐาน) ไปยัง SS (สถานีบริการ) ผ่านโปรโตคอลการจัดการคีย์นี้ SS และ BS จะประสาน keying data นอกจากนี้ BS ยังใช้โปรโตคอลกำหนดเงื่อนไขเพื่อการเข้าถึงบริการเครือข่ายใน IEEE 802.16e-2005 มีการแก้ไขมาตรฐาน IEEE 802.16e-2005 ด้วยกำหนดคุณสมบัติ PKMv2เพิ่มขึ้น [2]

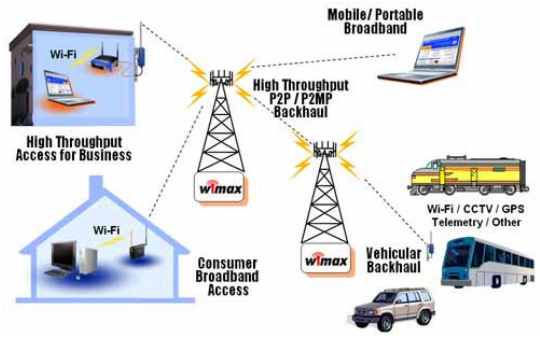


รูปที่ 2 สถาปัตยกรรมด้านความปลอดภัยของมาตรฐาน IEEE 802.16

ถึงแม้ว่า IEEE 80216e จะกำหนดไว้เพียงส่วนของแอร์อินเตอร์เฟซเท่านั้น แต่ส่วนนี้เป็นส่วนที่สำคัญมากและสร้างความแตกต่างให้กับการบริการการสื่อสารไร้สายได้เป็นอย่างมาก เนื่องจากทรัพยากรทางความถี่วิทยุมีอยู่จำกัด และอุปกรณ์ไร้สายก็จะมีพลังงานจากแบตเตอรี่ที่มีให้ใช้อยู่อย่างจำกัด

ดังนั้นภายใต้ข้อจำกัดเหล่านี้ การกำหนดมาตรฐานทางด้านความถี่วิทยุและการรับส่งผ่านคลื่นความถี่ให้มีประสิทธิภาพสูงสุดจึงเป็นสิ่งที่สร้างความแตกต่างเป็นอย่างมาก จึงทำให้เทคโนโลยีไวแมกซ์เป็นที่สนใจมากในปัจจุบันแต่กว่าที่มาตรฐาน IEEE 802.16e จะดูเพียบพร้อมสมบูรณ์เช่นนี้ มันได้มีการสั่งสมประสบการณ์และการแก้ไขมาตรฐานที่ผ่านมาอย่างยาวนานพอสมควร โดยไวแมกซ์นั้นเป็นมาตรฐานที่เกิดขึ้นครั้งแรกในปี ค.ศ. 2001 ดั้งเดิมนั้น IEEE ก็เพียงแต่ต้องการเทคโนโลยีไร้สายที่เข้ามาตอบสนองการสื่อสารข้อมูลระดับบรอดแบนด์ที่มีความเร็วสูงๆ ระยะทางไกลๆ หรือระดับ MAN (Metropolitan Area Network) ซึ่งทำให้มาตรฐาน 802.16 ตัวแรกๆ จะเป็นแบบแนวสายตา (LOS) ที่ช่วงความถี่ 10-66 GHz และใช้ความถี่แบบความถี่เดียว แต่อาศัยแบนด์กว้างในการสื่อสารข้อมูล หากแต่ก็ทำให้การให้บริการพื้นที่กว้างๆ ในความเป็นจริงมีปัญหา เช่น ในพื้นที่ส่วนใหญ่มักจะมีสิ่งกีดขวางอยู่เสมอ เช่น อาคารบ้านเรือน ต้นไม้ ภูเขา ฯลฯ ทำให้การรับส่งแบบ LOS ไม่มีประสิทธิภาพเพียงพอ อีกทั้งคลื่นความถี่สูงจะมีปัญหามากในการส่งระยะทางไกล ๆดังนั้นจึงทำให้มีการปรับปรุงมาตรฐานให้รับส่งแบบ NLOS และทำงานในช่วงความถี่ต่ำลงเป็น 2-11 GHz นั้นคือ 802.16 revision D ที่ออกมาเมื่อมี ค.ศ. 2004 และ revision E

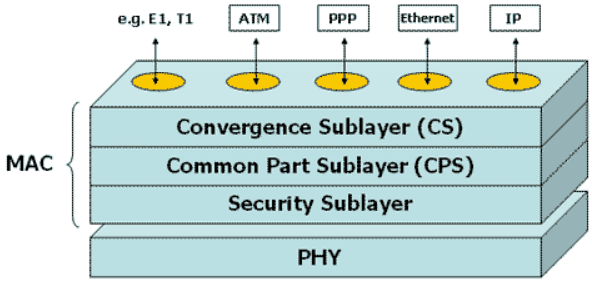
หรือ 802.16e ซึ่งเป็นเวอร์ชั่นที่ผู้ผลิตและผู้ให้บริการหลายๆ รายมุ่งที่จะให้บริการและอาจจะเข้ามาเปลี่ยนแปลงหน้าตาการสื่อสารของโลกได้ โดยมาตรฐาน 802.16 revision E ออกมาเมื่อปลายปี ค.ศ. 2005และผู้ผลิตได้เริ่มที่จะทยอยออกผลิตภัณฑ์ออกมาบ้างแล้ว และมีเครือข่ายที่เริ่มให้บริการไปไม่กี่ราย และการใช้งานก็ยังไม่มาก



รูปที่ 3 WiMAX Usage Scenarios

ในเวอร์ชั่น802.16d จะมีความสามารถในการให้บริการทั้งแบบ Fixed ซึ่งเป็นการให้บริการแบบอยู่กับที่ไม่มีการเคลื่อนที่ใดๆ และแบบ Nomadic ซึ่งเป็นการให้บริการแบบที่เคลื่อนย้ายตำแหน่งได้บ้าง แต่ไม่สามารถที่จะเคลื่อนที่ได้ในขณะที่กำลังใช้งานได้ ตัวอย่างเช่น เราสามารถที่จะย้ายที่นั่งภายในร้านขายกาแฟเพื่อหามุมสงบในการทำงานได้ แต่ไม่ใช่อยู่บนรถที่เคลื่อนที่ เป็นต้น ความสามารถในการให้บริการแบบเคลื่อนที่ได้นั้นจะมีใน revision E เท่านั้น ซึ่งผู้ใช้จะสามารถใช้งานได้ขณะเคลื่อนที่ เช่น บนรถประจำทางหรือรถไฟ เป็นต้น ซึ่งเป็นความแตกต่างหลักของทั้ง 2 เวอร์ชั่นนี้ และเป็นสาเหตุให้ผู้ผลิตจับตามอง revision E กันอย่างใกล้ชิด เพราะความสามารถที่โดดเด่นกว่านั่นเอง ดังนั้นในส่วนที่เหลือต่อจากนี้จะเน้น revision E เป็นหลัก เนื่องจากเป็นมาตรฐานที่สนใจกันมากกว่า

จากพัฒนาการของ IEEE 802.16 จนกระทั่งมาถึง 802.16e ดังที่ได้กล่าวถึงไปแล้วนั้น โปรโตคอล 802.16 ได้ถูกพัฒนาขึ้นมาด้วยตามลำดับ อย่างไรก็ตามโปรโตคอลหลักๆ ที่ได้กำหนดไว้ใน IEEE 802.16 ก็ยังคงมีอยู่เพียง 2 เลเยอร์ ก็คือ Physical Layer หรือที่นิยมเรียกกันสั้น ๆ ว่า PHY และ Media Access Control Layer หรือ MAC Layer เท่านั้น [3]



รูปที่ 4 โครงสร้างPHY Layer และMAC Layer ของ802.16e

ชั้น PHY จะเป็นชั้นที่ว่าด้วยรายละเอียดทางกายภาพลักษณะการรับส่งสัญญาณต่างๆ ไม่ว่าจะเป็นเรื่องการควบคุมกำลังการรับส่ง การมอดูเลชั่น การทำมัลติเพิลแอกเซสสำหรับหลายยูสเซอร์ การเข้ารหัสต่างๆ ลักษณะของเสาอากาศที่ใช้ เป็นต้นส่วนชั้น MAC จะว่าด้วยเรื่องการเข้าถึงระบบ การควบคุมรักษาและการตรวจสอบความปลอดภัยต่างๆ การเชื่อมโยงเข้ากับโปรโตคอลต่างๆ ที่สูงกว่า เป็นต้น

PHY Layer เป็นเลเยอร์ที่เทียบเท่ากับเลเยอร์Physical ของ OSI โดยในมาตรฐานของ 802.16 ทั้งหมดนี้จะมีการกำหนด PHY เลเยอร์ทั้งหมด 5 แบบด้วยกันดังต่อไปนี้

a. Wireless MAN SC จะเป็นลักษณะของ Single Carrier ซึ่งเป็น 802.16 ตัวแรกสุดที่ได้กำหนดขึ้น ความถี่ที่ใช้งานจะอยู่ในย่านที่สูงกว่า 11 GHz สามารถที่จะทำงานได้ทั้งแบบ FDD หรือ TDD และไม่มีการใช้งาน OFDM

b. Wireless MAN SCaได้ปรากฏอยู่ใน 802.16a เป็นการใช้งานแบบ Single Carrier เช่นกัน จึงไม่มีการใช้งาน OFDM โดยใช้งานกับความถี่ 2-11 GHz ที่ให้บริการแบบ point to Multipoint และมีทั้งแบบ FDD และ TDD นับเป็นจุดเริ่มต้นของการใช้ไวแมกซ์แบบ Last Mile เป็นครั้งแรกเพื่อรองรับผู้ใช้งานทั่วไป

c. Wireless MAN OFDM เป็นการเพิ่มความสามารถของ OFDM เข้าไปใน 802.16a และใช้เป็นรากฐานจนถึงปัจจุบันที่เป็น 802.16e โดยการใช้งาน FFT ขนาด 256 เพื่อรองรับการใช้งานแบบ NLOS และแบบ Point to Multipoint ที่ความถี่ 2-11 GHz มันสามารถที่จะใช้ได้ทั้ง FDD หรือ TDD และออกมาใช้งานกันใน 802.16d เป็นครั้งแรก จึงอาจจะเป็นที่รู้จักกันในชื่อ Fixed WiMAX เพราะว่า 802.16d ยังให้บริการแบบไม่เคลื่อนที่อยู่นั่นเอง แต่จริงๆ แล้วมันก็สามารถที่จะให้บริการแบบเคลื่อนที่ได้ ดังจะพบใน 802.16e และรองรับการเชื่อมต่อแบบแมส (Mesh) ได้อีกด้วย

d. Wireless MAN OFDMA เป็นผลของ 802.16a โดยจะมีขนาด FFT เท่ากับ 2048 ใช้งานความถี่ 2-11 GHz รองรับได้ทั้ง

FDD และ TDD และรองรับการใช้งานแบบเคลื่อนที่ได้ด้วย และในมาตรฐาน 802.16e ของปี ค.ศ. 2005 นั้นก็ได้มีการปรับเปลี่ยนรูปแบบจาก OFDMA ปกติเป็น SOFDMA นั่นคือสามารถปรับเปลี่ยนขนาด FFT ได้ตั้งแต่ 256, 512, 1024 ไปจนถึง 2048 โดยการกำหนดช่วงห่างระหว่าง subcarrier ไว้ให้คงที่นั่นเอง ซึ่งจะทำให้มีความยืดหยุ่นไปตามสภาพของแบนด์วิดธ์ที่มีให้ และสภาวะแวดล้อมต่างๆ ได้ดีขึ้น เหมาะสมกับการใช้งานแบบเคลื่อนที่ได้ และนั่นจึงทำให้ 802.16e ได้รับความสนใจเป็นอย่างสูงนั่นเอง

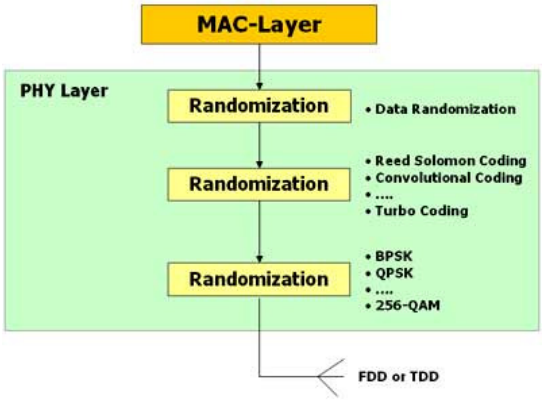
e. Wireless MAN Human เป็นผลงานของ 802.16b ซึ่งไม่ได้มีการใช้งานในปัจจุบัน มันทำงานได้ในแบบ TDD เท่านั้น และใช้งาน OFDM หรือ OFDMA ได้ด้วย

สำหรับไวแมกซ์802.16e นั้นจะใช้งาน Wireless MAN OFDM ในกรณีที่มีการใช้งานอยู่เพียงยูสเซอร์เดียว และใช้ Wireless MAN (S) OFDMA สำหรับในกรณีที่มีการใช้งานร่วมกันหลายๆ ยูสเซอร์ [2] ดังนั้นในครั้งนี้เราจะเน้นที่ทั้งสองนี้เป็นหลัก

III. โครงสร้างของไวแมกซ์

A. PHY Layer

โครงสร้างระดับPHY มีกระบวนการในการสร้างขึ้นเป็นลำดับ ซึ่งจะประกอบกันขึ้นเป็นเลเยอร์Physical ทั้งนี้ในโครงสร้างคร่าวๆ ของPHY Layer นั้นจะเริ่มจากการทำ Date Randomization จากนั้นก็ทำการเข้ารหัสFEC ต่างๆ [4] ก่อนที่จะส่งไปทำมอดูเลชั่นและเข้าสู่การทำMultiple Access ต่อไปโดยมีรายละเอียดของแต่ละขั้นตอนดังนี้



รูปที่ 5 โครงสร้างคร่าวๆ ของPHY Layer

1. Data Randomization ในส่วนนี้จะเปรียบเสมือนเป็นการเข้ารหัส encryption ในระดับเลเยอร์แรกของข้อมูลทั้งดาวน์ลิงก์ (จากสถานีฐานไปยังเครื่องลูกข่าย) และอัพลิงก์ (จากเครื่องลูกข่ายไปที่สถานีฐาน) เพื่อสร้างความปลอดภัยจากการดักฟังข้อมูลต่างๆ หลังจากได้ข้อมูลจากการ Randomization แล้วก็จะส่งต่อไปยังส่วนของ Channel Coding หรือ FEC ต่อไป

2. FEC (Forward Error Coding) เพื่อเป็นการเพิ่มความน่าเชื่อถือและประสิทธิภาพของการรับส่งข้อมูล จึงต้องมีการเพิ่มความสามารถที่จะตรวจจับปัญหาหรือแก้ไขความผิดพลาดในการรับส่งข้อมูล และใน 802.16e นั้นก็ได้ใช้การเข้ารหัสมาช่วยเหลือในส่วนนี้ ซึ่งในส่วนของ Channel Coding นั้นจะประกอบด้วยการเข้ารหัสหลายๆ แบบที่มีวัตถุประสงค์และการใช้งานแตกต่างกัน (ไวแมกซ์สามารถทำการ Adaptive Modulation เพื่อให้ได้ประสิทธิภาพสูงสุดในสภาพแวดล้อมการรับส่งความถี่ต่างๆ กันออกไป และนี่ก็คือสิ่งหนึ่งที่มีการปรับให้เข้ากับสภาพแวดล้อมนั้น) โดยการเข้ารหัส ที่มีความจำเป็น คือการเข้ารหัสแบบ Convolutional Coding แบบ Binary non-recursive ที่อัตรา Code Rate แตกต่างกันไปตามสภาพการรับส่งข้อมูลนั้นๆ ว่าดีเพียงใด ถ้ามีการรบกวนน้อยก็ทำการป้องกันน้อย หากมีการรบกวนมากจะเพิ่มการป้องกันมากขึ้น และมีออฟชั่นในการเข้ารหัสแบบ Convolutional Turbo Code, Block Turbo Code และ Low Density Parity Check (LDPC) แต่แนวโน้มที่เกิดขึ้นก็คือผู้ผลิตส่วนใหญ่เลือกที่จะใช้เพียง Convolutional Turbo Code คู่กับ Convolutional Coding ธรรมดาเท่านั้น เพราะข้อดีของ Convolutional Turbo Code ที่มีเหนือกว่าการเข้ารหัสแบบอื่นๆ มาก ไม่ว่าจะเป็นเรื่องของความยืดหยุ่นในการเข้ารหัส และประสิทธิภาพที่เหนือกว่าในการป้องกันความผิดพลาด เป็นต้นสำหรับการเข้ารหัสแบบ Convolutional Code นั้น ในด้านดาวน์ลิงก์หากไม่มีการทำ Subchannelเพื่อใช้งานร่วมกับยูสเซอร์อื่นแต่อย่างใดแล้ว (ซึ่งก็จะตรงกับกรณี Wireless MAN OFDM) จะมีการเข้ารหัสแบบ Reed-Solomon เพิ่มเติมเข้าไปด้วย ทั้งนี้เพื่อสร้างความน่าเชื่อถือในการรับส่งข้อมูลให้เพิ่มขึ้น จากนั้นจึงเข้ากระบวนการ Puncturing เพื่อลดความซ้ำซ้อนของบิตข้อมูลต่อไป

สิ่งที่น่าสนใจใน 802.16e อีกประการหนึ่ง ก็คือมีกระบวนการในการทำ Hybrid ARQ ทั้งสองแบบคือ type I หรือ Chase Combining และ type II หรือ Incremental Redundancy อยู่ด้วย ซึ่งในแบบแรกนั้นหากข้อมูลที่รับมานั้นผิดพลาด จะมีการเก็บข้อมูลเก่าที่ผิดพลาดเอาไว้ก่อน และหลังจากรับข้อมูลที่ส่งมาใหม่ก็จะ

นำมารวมกัน ก่อนที่จะทำการถอดรหัส FEC เพื่อแกะข้อมูลต่อไป ทำให้ข้อมูลที่ได้รับมีความถูกต้องมากขึ้น ส่วนในแบบที่ 2 ก็จะเปลี่ยนแปลงการเข้ารหัสในข้อมูลที่จะส่งซ้ำด้วย ทำให้มีความถูกต้องและประสิทธิภาพที่ดีกว่าแบบแรกนั่นเอง

3. Interleaving เป็นกระบวนการในการสลับย้ายตำแหน่งของส่วนต่างๆ ของข้อมูลเพื่อลดโอกาสที่จะเกิดความผิดพลาดในการรับส่งข้อมูลโดยไม่ต้องสูญเสียแบนด์วิดธ์หรือขีดความสามารถในการรับส่งข้อมูลแต่อย่างใด สำหรับไวแมกซ์หรือ 802.16e นั้นก็ได้ใช้วิธีนี้หลังการทำ Channel Coding ด้วยเพื่อประสิทธิภาพที่เพิ่มขึ้นดังกล่าว

วิธีการใน 802.16e จะมีด้วยกัน 2 ขั้นตอนดังต่อไปนี้

1) ทำการสลับหรือย้ายตำแหน่งบิตข้อมูลที่ติดกันไปไว้กับความถี่ subcarrier ที่ไม่ติดกันของ OFDMA ที่ใช้งานอยู่เพื่อให้โอกาสที่จะถูกรบกวนจากความถี่รบกวนลดลง เป็นการสร้าง Frequency Diversity ที่ดี เพิ่มประสิทธิภาพในการถอดรหัสให้มากขึ้น

2) จากนั้นทำการย้ายตำแหน่งบิตข้อมูลที่ติดกันให้ไปอยู่บนบิตที่ significant ต่างกันในการมอดูเลชั่นเพื่อให้กระจายความเสี่ยงที่จะเกิดจากการรบกวนสัญญาณที่ผ่านการมอดูเลต เพราะโอกาสที่จะเกิดความผิดพลาดในแต่ละบิตของ 16QAM และ 54QAM จะแตกต่างกันออกไป บิตที่เป็น Most significant จะมีโอกาสเกิดความผิดพลาดได้น้อยกว่าบิตที่เป็น Least significant นั่นเอง

4. Symbol Mapping กระบวนการนี้เป็นกระบวนที่เชื่อมโยงข้อมูลเข้ากับการมอดูเลชั่น โดยจะจับกลุ่มของไบนารีบิตของข้อมูลเพื่อแสดงเป็น symbol ที่เป็นตัวแทนการมอดูเลชั่นค่าใน QPSK, 16QAM และ 64QAMแม้ว่ามาตรฐาน 802.16e จะกำหนดให้มีเพียง QPSK และ 16QAM เป็นการมอดูเลชั่นภาคบังคับที่จะต้องมีก็ตาม แต่ผู้ผลิตส่วนใหญ่ก็ได้เลือกที่จะมี 64QAM รวมอยู่ด้วย เพื่อให้การรับส่งข้อมูลในสภาพแวดล้อมที่เหมาะสมเป็นไปอย่างรวดเร็วมากขึ้นในไวแมกซ์นั้นจะมีการทำ Adaptive Modulation ซึ่งจะทำการปรับมอดูเลชั่นและการเข้ารหัสให้เหมาะสมกับสัญญาณรบกวนที่เกิดขึ้น ทำให้ได้ความเร็วสูงสุดเท่าที่จะเป็นไปได้ในสภาพแวดล้อมนั้นโดยอัตโนมัติ ดังนั้นในระยะทางต่างๆ ซึ่งมีค่าสัญญาณต่อสัญญาณรบกวน (S/N ratio) แตกต่างกัน ก็จะทำให้มีการมอดูเลชั่นและการเข้ารหัสที่แตกต่างกันไปตามค่าสัญญาณต่อสัญญาณรบกวน และเป็นสาเหตุให้ความเร็วในการรับส่งข้อมูลลดลง สืบเนื่องมาจากการปรับใช้การมอดูเลชั่นต่างๆ เมื่อระยะทางระหว่างสถานีฐานกับเครื่องลูกข่ายมากขึ้นนั่นเอง [5]

B. MAC Layer

ในระดับ MAC Layer ของไวแมกซ์นั้นจะเป็นตัวเชื่อมต่อเลเยอร์PHY เข้ากับเลเยอร์ที่สูงกว่า ดังนั้นมันจึงมีหน้าที่ปรับรูปแบบข้อมูลจากเลเยอร์ที่สูงกว่าที่เรียกว่า MSDU (MAC Service Data Unit) [6] ที่อยู่ในรูปของโปรโตคอลในเลเยอร์ที่สูงกว่า เช่น IP, Ethernet และ ATM เป็นต้น ซึ่งแน่นอนว่ามันไม่จำเป็นต้องแปลงในรูปแบบหนึ่งต่อหนึ่งเสมอไป อาจจะหลายๆ MSDU รวมเข้าด้วยกัน ปรับเปลี่ยนเฮดเดอร์จนกลายเป็น MPDU เพียงยูนิตเดียวก็ได้ หรืออาจจะแบ่ง MSDU ก้อนโตๆ ให้เป็น MSDU หลาย ๆ ตัวก็ได้ แล้วแต่ความเหมาะสมกับงาน สภาพแวดล้อมทางแอร์อินเตอร์เฟซ เป็นต้น

ในทุกๆ เฟรมของ MAC Layer นั้นจะต้องมี Generic MAC Header (GMH) ที่มีทั้ง Connection Identifier (CID) ความยาวเฟรม บิตที่บอกถึง CRC ที่อยู่ในตอนท้ายเฟรม เฮดเดอร์ย่อย การระบุการทำ Encryption เป็นต้น จากนั้นก็จะเป็น Payload ชนิดต่างๆ เช่น MSDU Payload, Transport Payload, ARQ เป็นต้น

นอกจากหน้าที่ในการปรับเปลี่ยนโปรโตคอลระหว่างเลเยอร์แล้ว ฟีเจอร์ต่างๆ ที่สำคัญๆ ของไวแมกซ์เองก็มาอยู่ที่เลเยอร์นี้ด้วยเช่นกัน สิ่งต่างๆ เหล่านั้นได้แก่

1. Channel Access Mechanism

ในเลเยอร์นี้จะทำหน้าที่ในการกำหนดแบนด์วิดธ์ให้กับทุกยูสเซอร์ โดยอาจจะผ่านการควบคุม Scheduling ในสถานีฐาน โดยในดาวน์ลิงก์จะกำหนดจาก Traffic ที่เกิดขึ้น แต่สำหรับอัพลิงก์นั้นจะผ่านการกำหนดจากความต้องการของอุปกรณ์ไวแมกซ์ที่ยูสเซอร์ใช้และร้องขอเข้าระบบ

2. Quality of Service

ส่วนนี้เป็นหัวใจของเทคโนโลยีการสื่อสารสมัยใหม่เลยทีเดียวครับ เพราะจะทำให้มีหลายๆ บริการใช้เทคโนโลยีบรอดแบนด์เดียวกันนี้ได้อย่างคุ้มค่าและเกิดประสิทธิภาพสูงสุด ซึ่งสำหรับไวแมกซ์นั้นจะพัฒนา QoSจากระบบ DOCSIS ที่ใช้กับเคเบิลโมเด็มเป็นหลัก เพราะว่าไวแมกซ์เองก็เน้นที่การให้บริการบรอดแบนด์ได้ด้วยความเร็วสูงราวกับมีสายเคเบิลเชื่อมต่ออยู่นั่นเอง พารามิเตอร์ที่ไวแมกซ์ใช้ในการควบคุม QoSก็ได้แก่ Traffic priority, Maximum sustained traffic rate, Maximum burst rate, Minimum tolerable rate เป็นต้น

3. ฟีเจอร์ Power Saving

ใน 802.16e จะเป็น Mobile WiMAXที่เน้นการเคลื่อนที่ในขณะให้บริการอุปกรณ์ใช้งานที่เคลื่อนที่ได้นั้นก็ต้องมีขนาดเล็ก

ดังนั้นเรื่องการประหยัดพลังงานจึงเป็นประเด็นที่สำคัญ ด้วยเหตุนี้เองใน 802.16e จึงต้องกำหนดในเรื่องของวิธีการประหยัดพลังงานในรูปแบบต่างๆ ไม่ว่าจะด้วยการมีโหมดในการทำงานต่างๆ ที่ใช้พลังงานแตกต่างกัน เช่น Sleep mode, Idle mode และ Active mode และแน่นอนว่าแต่ละโหมดนั้นก็จะมีวิธีการที่จะช่วยในการประหยัดพลังงานที่แตกต่างกันไป

4. การทำ Mobility

อธิบายด้านบนแล้วว่า 802.16e เป็น Mobile WiMAXซึ่งเป็นพัฒนาการสำคัญแห่งไวแมกซ์ จึงจำเป็นที่จะต้องมีกลไกช่วยเหลือในการเคลื่อนที่ เพื่อให้มีการติดต่อสื่อสารระหว่างการเคลื่อนที่ได้อย่างสมบูรณ์ไม่สะดุดติดขัด และกลไกที่ว่านี้ก็อยู่ในส่วนของ MAC Layer ทำหน้าที่ควบคุมให้สามารถทำงานได้อย่างถูกต้องไม่ติดขัดนั่นเอง

5. การรักษาความปลอดภัย

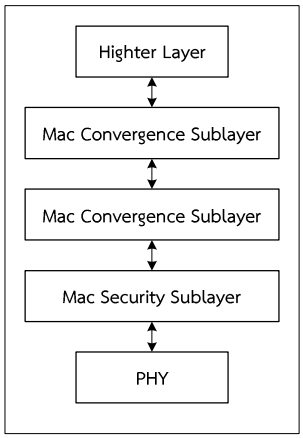
เนื่องจากในwifiนั้น การรักษาความปลอดภัยนับว่าเป็นจุดบกพร่องที่สำคัญในช่วงแรกๆ ดังนั้นIEEE จึงไม่ต้องการให้เกิดความผิดพลาดในเรื่องนี้ขึ้นอีก ด้วยเหตุนี้เองจึงได้มีการกำหนดกลไกการรักษาความลับความปลอดภัยของข้อมูลอย่างชัดเจน ถึงขนาดที่มีการกำหนด Security Sublayerไว้เฉพาะภายใน MAC Layer เพื่อดูแลในเรื่องนี้โดยเฉพาะ

จะเห็นได้ว่าฟังก์ชั่นหรือฟีเจอร์สำคัญๆ ของไวแมกซ์มาอยู่ที่ MAC Layer เป็นส่วนใหญ่ ดังนั้น MAC Layer จึงเป็นส่วนที่สำคัญมากในระบบไวแมกซ์ซึ่งในMAC Layer นั้นสามารถที่จะแบ่งออกเป็น 3 ส่วนหลัก ๆ ด้วยกัน แต่ละส่วนนั้นเราเรียกมันว่า Sublayerดังนั้น MAC Layer จึงสามารถที่จะแบ่งออกได้ดังนี้

1) Convergence Sublayerเป็นส่วนที่ช่วยในการปรับโปรโตคอลจากเลเยอร์บนและเลเยอร์ล่างเข้าหากัน

2) Common Part Sublayerเป็นส่วนหลักที่ทำหน้าที่ต่าง ๆ ของ MAC Layer รวมถึงฟีเจอร์ต่างๆ ของไวแมกซ์ด้วย

3) Security Sublayerเป็นส่วนที่เปรียบเสมือนเจ้าหน้าที่รักษาความปลอดภัยของไวแมกซ์ที่คอยตรวจตราดูความเรียบร้อยและรักษาความลับในการสื่อสารต่างๆ [7]



รูปที่ 6 ส่วนต่างๆ ของMAC Layer ในไวแมกซ์

1) Convergence Sublayer

ในส่วนนี้จะทำหน้าที่หลักในการปรับรูปแบบในการติดต่อระหว่างโปรโตคอลเลเยอร์บนกับเลเยอร์ล่าง โดยมันจะเป็นเสมือนหน้าด่านที่จะทำการคุยกับลูกค้า ซึ่งก็คือโปรโตคอลเลเยอร์สูงกว่าโดยจะรับข้อมูลหรือที่เราเรียกว่า MSDU เข้ามาแล้วปรับแปลงให้ติดต่อสื่อสารได้ ดังนั้นในเลเยอร์นี้จะขึ้นกับโปรโตคอลเลเยอร์บนที่ใช้งานนั้นว่าเป็นโปรโตคอลอะไร มีรูปแบบต่าง ๆ อย่างไร เพื่อที่จะทำการปรับเรื่องเฮดเดอร์ต่างๆการทำ Address Mapping (เช่น การจับคู่ IP Address เป็นค่าของ PHY Layer) เป็นต้น

มีชนิดของ Convergence Sublayerที่ถูกกำหนดขึ้นมาพอสมควรเพื่อให้รองรับกับโปรโตคอลระดับสูงต่างๆ ไม่ว่าจะเป็น ATM, WiMAX, Ethernet แต่อย่างไรก็ตามทาง WiMAX Forum ก็เลือกที่จะใช้แค่เพียง IP และ Ethernet ก่อนในระยะแรกนี้

เนื่องจาก MAC Layer ของไวแมกซ์นั้นเป็นแบบ Connection Oriented จึงต้องมีการเชื่อมต่อระหว่าง MS และ BS และมีการกำหนดเลขที่ของการเชื่อมต่อนั้นขึ้น เรียกว่า Connection Identifier (CID) โดยจะมีความแตกต่างกันทั้งทางด้านอัพลิงก์และดาวน์ลิงก์ เรียกว่าเป็น Unidirectional Connection ที่เชื่อมต่อระหว่าง MAC Layer Peer ของผู้ที่ทำการติดต่อซึ่งกันและกัน โดยจะทำการรับส่งทั้งข้อมูลจริงๆ และข้อมูลในการควบคุมต่างๆ

และ Convergence Sublayerจะต้องมีการเก็บข้อมูลว่า CID นั้นติดต่อกันระหว่างผู้ส่งคนใดและผู้รับคนใด และไม่ใช่ว่าสำหรับผู้ส่งผู้รับคู่หนึ่งนั้นจะมีเพียง CID เดียวที่เชื่อมต่ออยู่เท่านั้น มันอาจจะมีหลายๆ การเชื่อมต่อเกิดขึ้นก็ได้แตกต่างกันไปตามการบริการที่ใช้งาน และแน่นอนว่าจะต้องมี QoSที่แตกต่างกันด้วย ทำให้ต้องมีหลายๆ การเชื่อมต่อเกิดขึ้น และมี CID หลายๆ ตัวที่แตกต่างกันไปในระหว่างการสื่อสารคู่หนึ่ง

อีกสิ่งหนึ่งที่ Convergence Sublayerจะต้องทำก็คือการทำ Packet Header Suppression (PHS) ซึ่งทำหน้าที่ตัดส่วนที่ซ้ำซ้อนกันในแต่ละแพ็กเก็ตออกไป เช่น สำหรับการเชื่อมต่อหนึ่ง ๆ ของโปรโตคอลไอพีนั้น จะต้องมีการระบุ IP Address ทั้งทางด้าน Source และ Destination ในทุกๆ แพ็กเก็ต แต่สำหรับใน MAC Layer นั้นจะมีการกำหนด CID เพื่อการเชื่อมต่อระหว่าง Source และ Destination อยู่แล้ว และทุกๆ แพ็กเก็ตก็จะเดินทางไปบนเส้นทางเดียวกันอยู่แล้ว ไม่จำเป็นที่จะต้องวิเคราะห์แอดเดรสเพื่อกำหนดเส้นทางใหม่อีกครั้ง ดังนั้นการที่จะต้องส่งแอดเดรสในทุก ๆ แพ็กเก็ตจึงเป็นการสิ้นเปลือง และทำให้ประสิทธิภาพของระบบลดลง

ด้วยเหตุนี้เองการทำ PHS จึงช่วยเพิ่มประสิทธิภาพของเครือข่ายให้เพิ่มขึ้น โดยจะนำสิ่งที่ซ้ำซ้อนกันใน SDU Header ออกไปก่อนที่จะเข้าทำงานใน MAC Layer หรือเลเยอร์ที่ต่ำกว่า

เริ่มจากจะมีการกำหนด PHS Rule ซึ่งกำหนดมาจากโปรโตคอลเลเยอร์ที่สูงกว่า โดยแต่ละ Rule จะแตกต่างกันไปตามบริการที่ใช้งาน เช่น สำหรับ VoIP นั้น Source IP Address, Destination IP Address หรือ Length ของแพ็กเก็ตจะไม่แตกต่างกัน ดังนั้นจะเป็นสิ่งที่ซ้ำซ้อนกันและจำเป็นที่จะต้องจัดการกับมัน ในขณะที่ HTTP นั้น Length เป็นสิ่งที่ไม่เท่ากันในแต่ละแพ็กเก็ต และจำเป็นที่จะต้องเก็บมันไว้

เมื่อ SDU มาถึงก็จะจับคู่กับ PHS Rule ที่กำหนด และวิเคราะห์ในส่วนของเฮดเดอร์ของมัน โดยจะแยกเป็นส่วนที่ซ้ำซ้อนและส่วนที่จะเก็บไว้ ส่วนที่ซ้ำซ้อนนั้นเราจะเรียกว่า PHS Field (PHSF) ซึ่งหากมีการทำ Verify (PHSV) แล้ว CS จะทำหน้าที่ตรวจสอบหน่วยความจำ Cache ว่ามีเก็บเอาไว้หรือไม่ หากตรงกันก็จะทำการตัดส่วน PHSF ออกไป และแทนที่ด้วย PHS index (PHSI) ซึ่งจะมีความยาว 8 บิต และอ้างถึง PHSF ที่เก็บไว้ใน Cache นั้น แต่หากไม่มีใน Cache ก็จะไม่มีการ Suppression และใช้ค่า PHSI 0 แทน

ถ้าไม่มีการ Verify จะไม่มีการตรวจสอบและจะทำการ Suppression สำหรับทุก ๆ SDU นั่นเอง แน่นอนว่าเมื่อจะต้องติดต่อกับโปรโตคอลที่สูงกว่าก็จะทำในสิ่งที่ตรงกันข้าม และใส่ค่า PHSF ลงไปในทุกแพ็กเก็ตที่ทำการรับส่ง [8]

2) Common Part Sublayer

Common Part Sublayerเป็นส่วนงานต่างๆที่จะต้องทำหน้าที่ร่วมกันในการสร้างโปรโตคอลไวแมกซ์ในระดับ MAC Layer เพื่อให้ทำงานได้อย่างถูกต้องและมีประสิทธิภาพเช่นการร้องขอและกำหนดแบนด์วิดธ์ QoS,การให้บริการ Mobility และความสามารถในการประหยัดพลังงานของไวแมกซ์

การสร้างและประกอบ MPDU อินพุตของ MAC Layer จะเรียกว่า MSDU (MAC Service Data Unit) ซึ่งเมื่อเข้าสู่MAC Layer แล้วจะมีการใส่บริการและข้อมูลต่างๆ ของ MAC Layer ลงไป จากนั้นก็จะประกอบกันและสร้างเป็น MPDU (MAC Protocol Data Unit) ซึ่งใช้ส่งไปยังPHY Layer ต่อไปและด้วยขนาดของ Payload ที่มีการกำหนดไว้จึงอาจเป็นได้ทั้งที่ว่ามีหลายๆSDU มาประกอบกันเข้าเป็น1MPDU หรืออาจจะเป็นSDU เดียวแต่แบ่งออกเป็นหลายๆMPDU ก็ได้โดยในกรณีนี้จะมีการกำหนด Sequence Number เพื่อให้ใช้ประกอบกลับเข้ามาได้และในการส่งออกไปในburst เดียวกันนั้นก็จะมีหลายๆ MPDU ที่ส่งออกไปพร้อมกัน

การสร้างและประกอบ MPDU มีความสำคัญมาก ถ้าในส่วนนี้พลาดไปสิ่งต่างๆ ที่สร้างขึ้นมาทั้งหมดก่อนก็จะไม่สามารถใช้งานได้ เช่นเดียวกันก่อนที่จะส่งไปยัง PHY Layer นั้น MAC Layer จำเป็นที่จะต้องควบคุมประกอบส่วนต่างๆ เข้าด้วยกันอย่างถูกต้องและสมบูรณ์เพื่อให้ PHY Layer สามารถที่จะทำงานต่อไปได้อย่างมีประสิทธิภาพ

ในขั้นตอนนี้กรณีของการเชื่อมต่อแบบ Non-ARQ จะส่งข้อมูลของ SDU ไปตามลำดับ แต่ถ้าเป็นกรณีแบบ ARQ จะมีการแบ่ง SDU ออกเป็นบล็อกเท่าๆ กัน มีการกำหนดหมายเลขลำดับ BSN (Block Sequence Number) ในแต่ละบล็อก แล้วส่งไปจนกระทั่งปลายทางได้รับและทำการตอบรับทุกๆ บล็อก จึงจะประกอบทุกบล็อกเข้าด้วยกันอีกครั้ง การตอบรับของไวแมกซ์จะมีอยู่ด้วยกัน 2 ชนิดคือ Selective ACK และ Cumulative ACK

Selective ACK จะเป็นการตอบรับเฉพาะ ARQ Block หรือ BSN นั้นๆ ที่มาถึงได้อย่างสมบูรณ์ แต่หากเป็น Cumulative ACK จะเป็นการตอบรับโดยรวมตั้งแต่ ARQ บล็อกก่อนหน้านี้จนถึงตัวล่าสุดว่าส่งมาถึงอย่างปลอดภัยไร้ข้อผิดพลาด

แต่ละ MPDU จะมีทั้ง Header, payload และ Cyclic Redundancy Check (CRC) ตามมาตรฐาน IEEE 802.3 ที่จะทำการตรวจสอบทั้ง MPDU ไม่เฉพาะแค่ส่วนใดส่วนหนึ่ง

ในไวแมกซ์นั้นเราสามารถที่จะแบ่ง MPDU ออกได้เป็น 2 ชนิด นั่นคือ Generic PDU และ Bandwidth-Request PDU โดย Generic PDU จะทำหน้าที่นำพาทั้งข้อมูลและ Signaling ต่างๆ ไปยังปลายทาง โดยจะมีลักษณะของ Header จากนั้นก็จะตามด้วย Payload และ CRC ตามลำดับ

ส่วน Bandwidth-Request PDU จะใช้งานโดย MS เพื่อส่งไปยัง BS เพื่อร้องขอแบนด์วิดธ์ด้านอัปลิงก์ โดยในตัวของ Bandwidth-Request PDU นี้จะมีเพียง Bandwidth-Request Header เท่านั้น ไม่มีส่วนของ Payload และ CRC เนื่องจากไม่ต้องนำพาข้อมูลอะไรมากนัก

นอกจากนี้ไวแมกซ์ยังมี Subheaderอยู่อีก 5 ชนิดที่จะเพิ่มต่อจาก Header ปกติเมื่อมีความจำเป็น นั่นคือ

a. Meshsubheaderใช้กับกรณีที่มีการต่อแบบ Mesh โดยจะต่อท้ายกับ Generic Header

b. Fragmentationsubheaderใช้กับ Generic header เพื่อที่จะบอกว่ามี SDU นี้ที่ได้มีการ Fragment ไว้ในหลาย ๆ MPDU

c. Packingsubheaderอันนี้จะเป็นกรณีกลับกันกับกรณีที่แล้ว จะเป็นกรณีที่มี SDU หรือส่วนของ SDU (SDU fragment) หลายๆ ตัวประกอบกันใน MPDU นั้น[9]

d. Fast-Feedback allocation subheaderใช้ในการแจ้งข้อมูลจาก MS เกี่ยวกับสถานะต่าง ๆ ของช่องสัญญาณทางด้านดาวน์ลิงก์ ซึ่งจะใช้งานทั้งกรณีที่มีการใช้งาน MIMO หรือไม่ทั้งคู่

e. Grant-Management subheaderกรณีนี้จะใช้งานโดย MS เพื่อทำการสื่อสารเกี่ยวกับงานด้าน Bandwidth Management ต่างๆ เช่น การร้องขอ Polling หรือการร้องขอเพิ่มเติมแบนด์วิดธ์ เป็นต้น ซึ่งในกรณีหลังนี้จะแตกต่างกับกรณีที่ใช้ Bandwidth-Request PDU เพราะเราจะใช้ Grant-Management subheaderซึ่งต่อท้ายกับ Generic Header ในกรณีที่มีการเชื่อมต่อ Session อยู่แล้ว และต้องการการเปลี่ยนแปลงแบนด์วิดธ์เพิ่ม ซึ่งจะทำให้ดูกะทัดรัดกว่าไม่ต้องส่ง PDU เพิ่มเติม เพราะสอดแทรกไปกับ Generic PDU ธรรมดาได้เลย ส่วนกรณีของ Bandwidth-Request PDU จะใช้ในกรณีที่มีการขอแบนด์วิดธ์ใหม่เมื่อเริ่มแรก

จากนั้นเมื่อประกอบ MPDU เสร็จเรียบร้อยแล้ว จะมีการส่งไปที่ Scheduler เพื่อที่จะส่งไปยัง PHY Layer โดยเจ้า Scheduler จะอ่านข้อมูลต่าง ๆ ก่อนที่จะมีการรวบรวมความต้องการและจัด QoSเพื่อให้ใช้งานทรัพยากร PHY ได้อย่างเหมาะสมต่อไป

การร้องขอและการกำหนดแบนด์วิดธ์ด้านดาวน์ลิงก์แบนด์วิดธ์ที่กำหนดให้แก่ MS แต่ละตัวจะกำหนดขึ้นโดย BS ในแต่ละ CID โดยที่ตัว MS จะไม่ได้มีส่วนร่วมในการร้องขอหรือกำหนดแต่อย่างใด เพราะว่า BS จะรู้ปริมาณข้อมูลที่ต้องการส่งและตัวเครื่อง MS ปลายทางอยู่แล้ว จึงทำให้มีความรวดเร็วมากขึ้น โดย BS จะกำหนดทรัพยากร PHY ได้ตาม QoSและบอกแก่ MS ด้วย DL-MAP Message

ทางด้านอัปลิงก์MS จะต้องทำการร้องขอทรัพยากร โดยอาจจะใช้ Bandwidth-Request MPDU หรือการเพิ่มเติม Grant-Management subheaderใน Generic Header ก็ได้ ซึ่งการร้องขอจะร้องขอเป็น Bytes ที่ต้องการส่งมากกว่าการร้องขอในเชิงทรัพยากร PHY ที่ต้องการ (เช่น จำนวนช่องสัญญาณย่อยหรือจำนวน OFDM Symbols เป็นต้น เพราะตรงนี้จะเป็นสิ่งที่ทาง BS กำหนดมาให้)

ในการร้องขอทรัพยากรด้านอัปลิงก์ สามารถที่จะร้องขอได้ทั้งแบบที่เป็น Incremental และแบบ Aggregate ก็ได้ โดยหากเป็น Incremental นั้นจะเป็นการร้องขอแบบเพิ่มเติม ซึ่งทาง BS ก็จะกำหนดทรัพยากรเพิ่มเติมให้ตามความเหมาะสม แต่หากเป็นกรณี Aggregate ก็จะนำตัวเลขใหม่ของแบนด์วิดธ์มาใส่แทนตัวเก่า โดยที่ Type ในตัวของ Bandwidth-Request Header จะเป็นตัวบอกว่าใช้ชนิดไหน แต่สำหรับกรณี Grant-Management subheaderก็จะมีแค่กรณี Incremental เท่านั้น

ในกรณีที่มีหลายๆ CID ใน MS ทาง BS ก็จะมอบทรัพยากรให้ในลักษณะแบบ Aggregate แทนที่จะเป็นแบบมอบให้แต่ละ CID และหากว่ารวมแล้วยังน้อยกว่าที่ได้มีการร้องขอไว้ Uplink Scheduler ภายใน MS ก็จะทำการกำหนดแบนด์วิดธ์ให้ตามปริมาณ Traffic คงค้าง หรือตามที่ QoSกำหนดไว้ในแต่ละ CID

ในระบบไวแมกซ์นั้นกระบวนการในการกำหนดทรัพยากรทางด้านอัปลิงก์ให้แก่ MS จะเป็นลักษณะ Polling ในการร้องขอแบนด์วิดธ์ ซึ่งการกำหนดเช่นนี้อาจเป็นการกำหนดแบบรายบุคคลหรือเป็นกลุ่มก็ได้ หากมีการ Poll MS เพียงแค่ตัวเดียวจะเรียกว่า Unicast จากนั้นจะกำหนดทรัพยากรอัปลิงก์ให้แก่ MS ที่ร้องขอแบนด์วิดธ์โดยผ่าน UL-MAP Message ที่อยู่ใน Downlink subframeโดยใช้ CID ในการระบุ ในกรณีที่เป็น UGS Connection ก็จะไม่มีการ Poll เพราะการร้องขอแบนด์วิดธ์จะส่งผ่าน UGS Allocation อยู่แล้ว ซึ่งในกรณีนี้หากไม่มีการร้องขอก็จะมีการส่ง Dummy MPDU แทน เพราะเป็นการ Poll แบบ Unicast ที่ต้องมีการคุยกันตลอด

แต่ถ้าในกรณีแบนด์วิดธ์ไม่เพียงพอต่อการ Poll แต่ละคนก็จะใช้ Multicast หรือการ Broadcast ซึ่ง MS ของ Group ก็จะสามารถร้องขอแบนด์วิดธ์ในจังหวะที่ Multicast และ Broadcast กำหนดให้ และมีเพียง MS เท่านั้นที่ต้องการด้านแบนด์วิดธ์ที่จะทำการส่งออก ไม่มีตัวส่งอื่น (เพื่อไม่ให้มีการชนกันมากนัก) โดยเรื่องของ Contention Resolution ปกติจะมีทั้งการ Retry และการ Discard เช่นเดียวกัน [10]

QoS (Quality of Service)ในระบบไวแมกซ์นั้นจะมีเรื่องของQoSเป็นประเด็นสำคัญหรือจุดขายอีกประเด็นหนึ่งด้วย ซึ่งแนวคิดของ MAC Layer ในไวแมกซ์นั้นจะได้มาจากมาตรฐานของ DOCSIS ที่ใช้งานในตัวโมเด็ม และ QoSที่ดีก็จะได้จากการเชื่อมต่อระดับ MAC Layer แบบ Connection Oriented ที่มีการเชื่อมต่อทั้งดาวน์ลิงก์และอัปลิงก์ที่ควบคุมโดย BS

ปกติแล้วการเชื่อมต่อระหว่าง BS กับ MS นั้นจะมีการกำหนด Connection Identifier (CID) เอาไว้ หากแต่ในระบบไวแมกซ์นั้นจะมีการกำหนด SFID (Service Flow Identifier) ที่จะมีการกำหนดพารามิเตอร์ของ QoSต่าง ๆ [13] ไว้ด้วย เช่น Traffic priority, Max sustained rate, Max burst rate, Main tolerable rate, Scheduling type, ARQ type และอื่น ๆ เป็นต้น โดย BS จะเป็นผู้กำหนด SFID ให้และจับคู่เข้ากับ CID อาจจะมีการแม็ปเข้ากับ MPLS frame หรือ DiffServ code points ด้วย

ในระบบไวแมกซ์จะมีการแบ่งบริการออกเป็น 5 บริการที่มีการ Scheduling ที่แตกต่างกัน ดังนี้

a. UGS (Unsolicited Grant Services) บริการนี้จะรองรับการเชื่อมต่อที่มีแพ็กเก็ตขนาดคงที่เข้ามาอย่างสม่ำเสมอ มีบิตเรตคงที่ ซึ่งเหมาะสมกับการใช้งานที่ต้องการความสม่ำเสมอ เช่น งาน T1/E1, งาน VoIP ที่ไม่มีการทำ Silence Suppression และเพราะความสม่ำเสมอของมัน จึงไม่จำเป็นที่จะต้องทำการร้องขอแบนด์วิดธ์เพิ่มเติม จึงตัดการสูญเสียที่เกิดจาก Overhead หรือการสื่อสารเพื่อร้องขอแบนด์วิดธ์เพิ่มไปได้

ในกรณีนี้สิ่งที่จะต้องมีการควบคุมก็คือ Max Sustained Traffic Rate, Max Latency และ Tolerated Jitter เป็นต้น

b. rtPS (Real-time Polling Services) เหมาะสมกับงานที่จะมีการรับส่งแบบ Real-time เช่น การสื่อสารไฟล์ MPEG (Motion Picture Expert Group) เหมาะกับงานที่มีขนาดแพ็กเก็ตที่หลากหลาย แต่การรับส่งเป็นแบบ Periodic อย่างสม่ำเสมอ โดย BS จะทำหน้าที่ในการมอบโอกาส Polling แบบ Unicast ให้แก่ MS เพื่อใช้ในการร้องขอแบนด์วิดธ์ และจังหวะในการ Polling นั้นจะมีเพียงพอที่จะให้บริการแก่งาน Real-time ได้ ซึ่งแน่นอนว่าจะมีเรื่องของ Overhead ที่มากกว่า แต่ก็มีประสิทธิภาพมากกว่าในงานที่มีแพ็กเก็ตหลากหลายขนาด หรือมีการใช้งานไม่ถึง 100 เปอร์เซ็นต์ ในการรับส่งเช่นนี้มีสิ่งที่จะต้องมีการดูแลก็คือเรื่องของ Min Reserved Traffic Rate, Max Sustained Rate และ Max Latency

c. nrtPS (Non Real-time Polling Services) ให้บริการที่เหมาะสมสำหรับที่เป็นแบบ Stream ทนต่อการดีเลย์ได้ เช่น การทำ FTP ซึ่งจะเป็นงานที่มีขนาดแพ็กเก็ตไม่คงที่ มีการรับประกันอัตราการส่งไม่มาก โดย MS จะใช้การ Polling แบบ Contention-based ในด้านอัปลิงก์เพื่อร้องขอแบนด์วิดธ์ และถึงแม้ว่าจะมีการ Polling แบบ Unicast ด้วย แต่ว่าจังหวะการ Poll จะเป็นระดับวินาที ซึ่งนับว่ายาวนานพอสมควรค่าพารามิเตอร์สำหรับบริการเช่นนี้ได้แก่ Min Reserved Rate, Max Sustained Rate และ Max Latency

d. BE (Best-Effort services) บริการนี้เหมาะสมกับงานที่ไม่ต้องมีการควบคุมคุณภาพมากนัก เช่น การใช้งานเว็บ ไม่มีการรับประกันอัตราการส่ง โดยจะทำการตั้งค่า Max Sustained Rate และ Traffic Priority

e. ERT-VR (Extended Real-time Variable Rate) เป็นการเพิ่มเติมจากคุณภาพการบริการแบบ ERT-VR ที่มีเฉพาะใน IEEE 802.16e หรือ Mobile WiMAXเท่านั้น โดยจะเหมาะสมกับงานประเภท Real-time Application เช่น VoIP ที่มีการทำ Silence Suppression ซึ่ง UL Allocation ที่อยู่เป็นระยะ ๆ นั้นจะทำหน้าที่ทั้งการรับส่งข้อมูลและการกำหนดแบนด์วิดธ์ที่เพิ่มขึ้น ซึ่งจะเหมาะกับงานที่แบนด์วิดธ์เปลี่ยนแปลงไปตามเวลาค่าพารามิเตอร์ก็คือ Variable Data Rate, Guaranteed Data Rate และ Delay เป็นต้น

3) Security Sublayer

ความปลอดภัยนั้นเป็นเรื่องที่สำคัญมากในวงการสื่อสารในปัจจุบันยิ่งสำหรับการสื่อสารไร้สายอย่างไวแมกซ์ด้วยเพราะด้วยตัวเครือข่ายไร้สายนั้นจะใช้ความถี่เป็นสื่อในการสื่อสารข้อมูลซึ่งการดักจับความถี่เพื่อลักลอบฟังหรือทำให้การสื่อสารข้อมูลคลาดเคลื่อนสามารถที่จะทำได้ง่ายเมื่อเทียบกับระบบที่มีสายสื่อสัญญาณสิ่งที่จำเป็นต่อความปลอดภัยของเครือข่ายสื่อสารไร้สายมีอะไรกันบ้างละสำหรับเครือข่ายสื่อสารไร้สายนั้นจำเป็นที่จะต้องมีฟังก์ชั่นดังต่อไปนี้

รูปแบบความปลอดภัยเครือข่าย Wimax มีฟังก์ชั่นดังต่อไปนี้

a. Privacy สำหรับยูสเซอร์ทุกคนที่ใช้เครือข่ายสื่อสารข้อมูลนั้นย่อมต้องการความเป็นส่วนตัวในการรับส่งข้อมูล ไม่ต้องการให้ข้อมูลที่สื่อสารกันนั้นถูกเปิดเผยออกไปไม่ว่าจะกับใครทั้งนั้น ดังนั้นเครือข่ายสื่อสารที่ดีจะต้องปิดช่องทางในการดักฟังได้ โดยเฉพาะเครือข่ายไร้สายนั้นจะต้องมีการปิดช่องทางการดักสัญญาณความถี่ได้ เช่น การเข้ารหัสเพื่อให้การดักฟังข้อมูลไม่ประสบความสำเร็จเป็นต้น

b. Data Integrity เรื่องความถูกต้องไม่ขาดหายของข้อมูลถือเป็นเรื่องสำคัญและเรื่องหลักของการสื่อสารข้อมูล เพราะหาก

ข้อมูลที่สื่อสารขาดหายหรือผิดเพี้ยนก็อาจจะทำให้การสื่อสารข้อมูลนั้นประสบความล้มเหลวได้ นอกจากนี้ในด้านความปลอดภัยของข้อมูลนั้น สิ่งที่จะต้องทำการดูแลป้องกันก็คือการลักลอบดัดแปลงข้อมูลที่รับส่งกันเพื่อให้การสื่อสารข้อมูลประสบความสำเร็จ

c. Authenticationสำหรับการตรวจสอบผู้ใช้หรืออุปกรณ์ที่เข้ามาในระบบก็มีความสำคัญ เพราะการลักลอบใช้บริการเครือข่ายสื่อสารไร้สายนั้น นอกจากจะทำให้สิ้นเปลืองทรัพยากรเครือข่ายโดยไร้ประโยชน์ อาจจะทำให้ทรัพยากรเครือข่ายไม่เพียงพอ และยังอาจจะทำให้เกิดปัญหาอื่นขึ้นได้ เช่น การปล่อยไวรัสเข้าสู่ระบบเครือข่าย การโจมตีเครือข่ายด้วยวิธี DoSเป็นต้น ดังนั้นจึงจำเป็นอย่างยิ่งที่จะต้องมีการตรวจสอบหรือ Authentication ว่าผู้ใช้บริการหรืออุปกรณ์นั้นเป็นผู้ที่ใช้บริการได้จริงตามที่กล่าวอ้างหรือไม่ นอกจากนี้ผู้ใช้บริการหรืออุปกรณ์เองก็จะต้องตรวจสอบเครือข่ายด้วยว่าใช่เครือข่ายที่ต้องการจะทำการติดต่อจริงหรือไม่ ซึ่งการตรวจสอบทั้งสองฝ่ายนี้เรียกว่า Mutual Authentication นั่นเอง

d. Authorization อกจากการตรวจสอบว่าเป็นยูสเซอร์ของระบบจริงหรือไม่แล้ว ยังต้องมีการตรวจสอบว่ามีสิทธิในการใช้บริการอะไรบ้าง มากน้อยเพียงไร และเช่นเดียวกันยูสเซอร์แต่ละคนก็จะมีสิทธิในการใช้งานบริการบางอย่างไม่เท่ากัน ดังนั้นก็จะต้องมีการตรวจสอบว่าใช้บริการนั้นได้ไหม เรียกว่าการ Authorization

e. Access Control และเมื่อตรวจสอบว่าใช้งานอะไรได้หรือไม่ เป็นยูสเซอร์จริงหรือไม่ ก็จะต้องมีการควบคุมการเข้าถึงบริการต่าง ๆ จึงจะเป็นเครือข่ายที่ปลอดภัยในการให้บริการ ซึ่งส่วนนี้จะว่าไปก็เป็นเรื่องของ Policy ที่เรากำหนดไว้ [3]

ซึ่งในเอกสารนี้ จะกล่าวถึงเฉพาะ Authentication เท่านั้น

ตาราง 2 แสดงเลเยอร์ต่างๆ ของการสื่อสารจะมีกลไกการรักษาความปลอดภัยต่างกัน

Layer	Description	Security Mechanism
7	Application Layer	Digital Signature, Certificate, End-to-End Security
4	Transport Layer	Transport Layer Security(TLS)
3	Network Layer	IPsec, AAA Infrastructure, RADIUS
2	Data Link Layer	AES, PKI, X.509
1	Physical Layer	Wimax PHY

MAC Layer ซึ่งเป็นเลเยอร์หลักของ 802.16e จะมีการทำ Encryption แบบ AES ที่จะช่วยในเรื่อง Privacy มี PKI ในการควบคุมการแลกเปลี่ยน Public/Private Key และการตรวจสอบ Certificate ซึ่งจะใช้ X.509 เพื่อใช้ในการทำ Authentication และ Authorization ซึ่งนำไปสู่ Data Integrity และ Access Control ที่มีประสิทธิภาพ

ส่วนในระดับ Network Layer ซึ่งเป็นเลเยอร์ที่ทำงานในระบบไอพีก็จะมีทั้งไฟร์วอลล์, IPSec, AAA (RADIUS, Diameter) ซึ่งในส่วนนี้จะไม่ใช่ส่วนประกอบใน 802.16e เพราะเป็นส่วนที่จะอยู่ในเลเยอร์ที่สูงกว่า และจะอยู่ในเครือข่าย CSN ที่เป็นเครือข่ายแกนกลางของเครือข่ายไวแมกซ์ ซึ่งจะคล้ายคลึงกับเครือข่ายไอพีทั่วไป

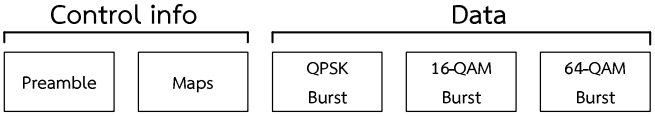
IVภัยคุกคามที่ส่งผลกระทบต่อไวแมกซ์

จากที่ได้กล่าวไปแล้วว่าไวแมกซ์นั้นเป็นเทคโนโลยีการสื่อสารที่มีความน่าสนใจ มีความเป็นไปได้ที่จะมีการนำมาใช้อย่างแพร่หลาย นอกจากนี้ไวแมกซ์ยังเป็นเทคโนโลยีที่มีความยืดหยุ่นในสภาพพื้นที่ที่มีความห่างไกลหรือทุรกันดาร โดยปัญหาที่เกิดขึ้นสำหรับไวแมกซ์นั้น มีมากมาย แต่เราจะรายงานเฉพาะปัญหาในเรื่องความปลอดภัย นั่นคือ ภัยคุกคามที่เกิดกับไวแมกซ์นั้นเอง

จากที่ทราบกันไปแล้ว ในสถาปัตยกรรมไวแมกซ์จะทำงานอยู่บนชั้น Physical Layer และ Mac Layerซึ่งจะอธิบายถึงภัยคุกคามดังนี้

A ภัยคุกคามในชั้นPHY layer

ที่ชั้นกายภาพการไหลของบิตมีโครงสร้างเป็นลำดับของเฟรมที่ยาวกว่ากัน ดูที่รูป 7 มี downlink ของเฟรมย่อยและ uplink ของเฟรมย่อย มีสองโหมดการดำเนินงาน คือ Frequency Division Duplex (FDD) และ Time Division Duplex (TDD)



รูปที่ 7 TDD downlink ของเฟรมย่อย [11]

รายละเอียดของ TDD downlink เฟรมย่อยแสดงให้เห็นถึงธรรมชาติการปล่อยออกมาของการส่ง; ดูรูปที่ 7, downlink ย่อย

ประกอบด้วยสองส่วนหลัก คือในส่วนแรกมีการควบคุมข้อมูลในขณะที่ส่วนที่สองมีข้อมูลของ Mobile Station (MS) ซึ่งสามารถที่จะปล่อยข้อมูลออกมาแต่ไม่สามารถที่จะdemodulateรักษาความปลอดภัยทั้งชั้นย่อยและชั้นที่อยู่เหนือไปได้ จึงกล่าวได้ว่าในชั้นกายภาพไม่มีหลักประกันเรื่องความปลอดภัยเลยดังภาพที่ 6 ดังนั้น WiMax/802.16 นั้นมีความเสี่ยงที่จะถูกโจมตีในชั้นกายภาพ จากการ jamming and scrambling.

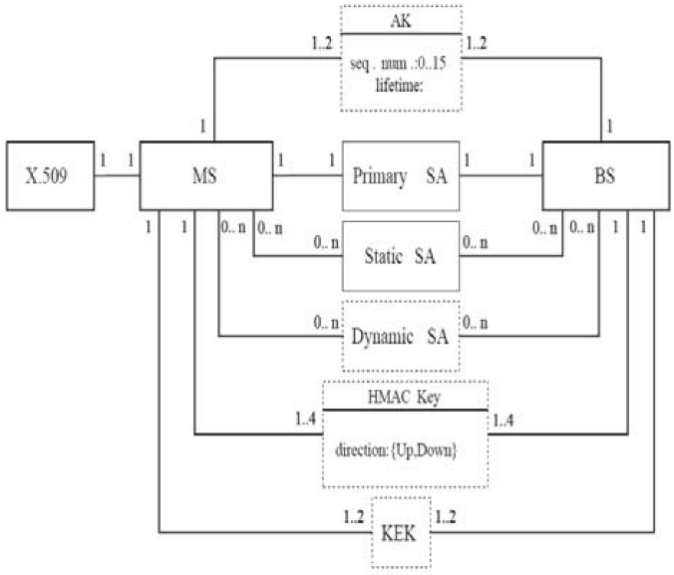
- Jamming (ตัวอย่างของโจมตีแบบขัดจังหวะ ซึ่งทำหน้าที่ปฏิเสธการให้บริการเพราะเครือข่ายเต็ม) คือ จะทำการส่งเสียงขอช่องสัญญาณ จนทำให้เต็มความจุช่องสัญญาณ ทำให้ช่องสัญญาณติดขัด สามารถหลีกเลี่ยงได้ด้วยการกระจายสเปรกตัม

- Scrambling เป็นการติดขัดประเภทหนึ่ง แต่สำหรับช่วงเวลาสั้นๆ โดยจะเจาะจงเป้าหมายไปเฉพาะเฟรม หรือบางส่วนของเฟรม Scrambling สามารถช่วงชิงการควบคุมหรือการจัดการระบบเครือข่ายโดยมีจุดมุ่งหมายเพื่อให้เครือข่ายทำงานผิดปกติ ปัญหานี้เป็นปัญหาที่กว้างมาก ทำให้เกิดการการล้าช้า สามารถตรวจหาได้จากการวัดขนาดของช่องสัญญาณหรือการตอบสนองของScrambling และ scramblersซึ่งการตรวจสอบนี้สามารถตรวจสอบได้ในเกณฑ์การปฏิบัติงาน [12]

B ภัยคุกคามในชั้นMAC Layer

ชั้น MAC Layer เป็นการเชื่อมต่อแบบ connection oriented ซึ่งมีการเชื่อมต่อสองชนิด คือ การจัดการการเชื่อมต่อและการเชื่อมต่อข้อมูลการขนส่ง การจัดการการเชื่อมต่อ มี 3 ชนิด คือ ขั้นพื้นฐาน, ขั้นปฐมภูมิและขั้นทุติยภูมิ โดยการเชื่อมต่อแบบพื้นฐานสร้างขึ้นมาเพื่อให้แต่ละ MS เมื่อเข้าร่วมเครือข่าย แต่มันจะใช้สำหรับระยะสั้น และ Massage เร่งด่วน การเชื่อต่อขั้นปฐมภูมิ ถูกสร้างขึ้นให้เวลาแต่ละ MS ในการเข้าสู่เครือข่าย แต่มันจะใช้สำหรับdelay tolerant management messages เท่านั้น ในการจัดการการเชื่อมต่อขั้นทุติยภูมิ ทำงานต่อจากขั้นปฐมภูมิ โดยจะใช้ IP encapsulated management messages (ตัวอย่างเช่น Dynamic Host Control Protocol DHCP, และ Simple Network Management Protocol SNMP) กลุ่มของการรักษาความปลอดภัย หรือ SA (i) มีแนวคิดที่จับพารามิเตอร์รักษาความปลอดภัยสำหรับการเชื่อมต่อโดยใช้กุญแจและรหัสลับ ดังแสดงในรูปที่ 8

กุญแจความปลอดภัยและความเชื่อมโยงที่สร้างขึ้นจาก MS และ BS (ii) ในระหว่างขั้นตอนการอนุมัติในการเข้าสู่เครือข่าย ซึ่งจะมีขั้นตอนของการแลกเปลี่ยน โดยมีเส้นอธิบายความสัมพันธ์กับจำนวนสมาชิกที่จุดสิ้นสุด องค์ประกอบที่มีอยู่ก่อนแล้วจะใช้เส้นทึบ การเชื่อมต่อแบบไดนามิกจะถูกแทนด้วยเส้นประ โดยมี Sas สามประเภท กล่าวคือ primary SA, static SA และ dynamic SA ซึ่งแต่ละ SA เป็นตัวระบุ (SAID) นอกจากนี้ยังมีการระบุชุดการเข้ารหัสลับ (อัลกอริทึมที่เลือก) Traffic Encryption Keys (TEKs) และ Initialization vectors เริ่มต้นจากSA ในแต่ละ MS จะมีแกนข้อมูลที่มีใบรับรองX.509 AK (Authorization Key), KEK (Key Encryption Key) และ HMAC Key (message authentication key) ทุก MS จะมีการตั้งรหัสกับใบรับรอง X.509โดย X.509 จะมีคีย์สาธารณะ (Public Key) ของ MS ซึ่ง MS จะใช้สำหรับการตรวจสอบสถานีฐาน (BS) ในทุกๆ คีย์ระหว่างการขออนุญาตเข้าสู่เครือข่าย [12]



รูปที่ 9 รูปแบบการรักษาความปลอดภัย [11]

การเชื่อมต่อการขนส่งแต่ละครั้ง (คำที่ใช้ หมายถึงการเชื่อต่อชั้น MAC layer เฉพาช่องทางของผู้ใช้) มี SA คนใดคนหนึ่ง (ทั้งการ uplink และ downlink) หรือสอง SA (คนหนึ่ง Uplink และอีกคน downlink)

i. SAหรือ Security Association เป็นกลุ่มข้อมูลด้านความปลอดภัยที่ใช้ร่วมกันระหว่าง BS กับ MS เพื่อให้ช่องสื่อสารระหว่างกันมีความปลอดภัย

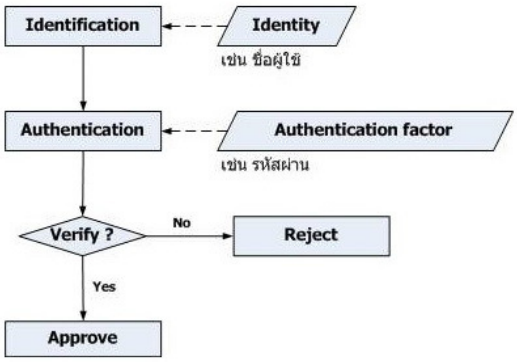
ii BSหรือ Base Station อุปกรณ์หรือสถานีที่เชื่อมต่อเข้ากับโครงข่ายหลัก (Core Network) ของผู้ให้บริการ และให้บริการการเชื่อมต่อเข้ากับโครงข่ายแก่ผู้ใช้งาน ลักษณะการทำงานของ BS จะเหมือนกับอุปกรณ์ Access Point ของระบบ WiFi

II. AuthenticationWimax Security

Authenticationคือ กระบวนการตรวจสอบตัวตน เพื่อเป็นการพิสูจน์ตัวตนในการเข้าใช้งานระบบ โดยวิธีการพิสูจน์ตัวตนนั้นมีหลายวิธีตามความเหมาะสม และความสะดวกในการใช้งาน [10]

กระบวนการ Authentication โดยทั่วไปจะมีอยู่ 2 ประเภท ก็คือ Unilateral Authentication ซึ่งในกรณีไวแมกซ์จะใช้รูปแบบนี้ จะเป็นการตรวจสอบทางเดียว โดยจะตรวจสอบ user เป็นหลัก และแบบ Mutual Authentication ที่จะมีทั้งการตรวจสอบ user และการตรวจสอบระบบว่าเป็นระบบของจริงหรือไม่ โดยตามมาตรฐานเครือข่ายไวแมกซ์จะเป็นการตรวจสอบแบบทางเดียว (Unilateral Authentication)และแบบสองทาง(Mutual Authentication)

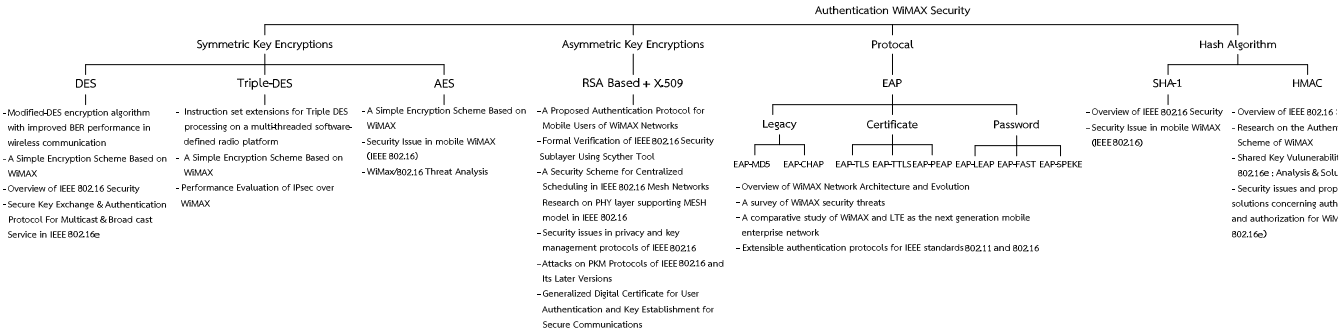
ใน WIMAX 802.16e จะใช้โปรโตคอล Privacy and Key Management Protocol เวอร์ชั่น2 (PKM v2) ในการควบคุมดูแลความปลอดภัยของ Key โดยหลักการก็คือจะสร้าง Secret Key ที่เรียกว่า Authorization Key (AK) ระหว่างยูสเซอร์กับ BS (สถานีฐานของไวแมกซ์) จากนั้นก็จะมีการสร้าง Key Encryption Key (KEK) เพื่อที่จะทำการ Encrypt กระบวนการที่จะทำการแลกเปลี่ยน Traffic Encryption Key ต่อไป [3]



รูปที่ 10 แผนผังแสดงกระบวนการการพิสูจน์ตัวตน

ในกระบวนการทำ Authentication ของ 802.16e จะมีการทำ Authentication ได้ 4 ชนิดคือ

1. Symmetric Key Encryptions
2. Asymmetric Key Encryptions
3. EAP based
4. ฟังก์ชั่น Hash



รูปที่ 9 รูปแบบของ Authentication Wimax Security

A. Symmetric Key Encryptions

โดยปกติแล้วการเข้ารหัส (Encryption) จะถูกนำมาใช้เพื่อทำให้เกิดความลับ (Confidentiality) อย่างไรก็ตามการเข้ารหัสถูกนำมาใช้อย่างกว้างขวางในปัจจุบันเพื่อประโยชน์ในการพิสูจน์ตัวตน (Authentication) โดยแต่ละฝ่ายจะต้องพิสูจน์ว่าตนเองทราบข้อมูลบางอย่างซึ่งผู้อื่นไม่มีทางทราบได้และข้อมูลอันเป็นความลับเฉพาะนี้ก็อาจจะหมายถึงกุญแจในการเข้ารหัส (Encryption Key) นั่นเอง

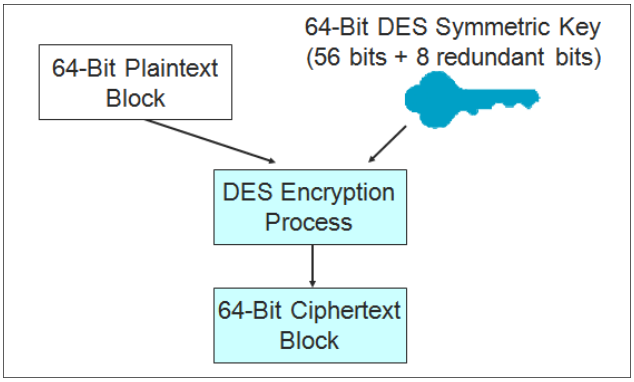
การเข้ารหัสกุญแจแบบสมมาตร เป็นการ Authentication ใน Wimaxวิธีการหนึ่งที่ใช้ โดยมีอยู่ 3 รูปแบบ คือ

1. Data Encryption Standard – DES

ในปีค.ศ.1977 สำนักงานมาตรฐานแห่งชาติของประเทศสหรัฐอเมริกา (The U.S. National Bureau of Standards) ซึ่งในเวลาต่อมาแปรสภาพเป็นสถาบันกำหนดมาตรฐานและเทคโนโลยี

แห่งชาติของประเทศสหรัฐอเมริกา (The National Institute of Standards and Technology – NIST) ได้กำหนดมาตรฐานกลางในการเข้ารหัสขึ้นมาเรียกว่ามาตรฐานในการเข้ารหัสหรือที่เรียกว่ามาตรฐานเดส (Data Encryption Standard – DES) ซึ่งในเวลาต่อมา DES ได้กลายมาเป็นกรรมวิธีในการเข้ารหัสที่ถูกนำมาใช้งานอย่างแพร่หลายมากที่สุดในขณะนั้นซึ่งแน่นอนว่าต่อมาในภายหลังถึงได้เริ่มมีกรรมวิธีใหม่ๆ ออกมาทดแทนแต่มาตรฐาน DES ถือเป็นจุดเริ่มต้นของมาตรฐานการเข้ารหัสแบบสมมาตร [14]

ในรูปที่ 10 แสดงให้เห็นว่า DES ใช้กรรมวิธีการเข้ารหัสแบบเป็นกลุ่ม (Block Encryption) ขนาด 64 บิตต่อการเข้ารหัส 1 ครั้ง โดยมีค่านำเข้า (Inputs) ขนาด 64 บิตจำนวน 2 ค่าได้แก่กุญแจรหัสขนาด 64 บิตและข้อความตั้งต้น (Plaintext) ขนาด 64 บิตโดยเมื่อผ่านกระบวนการเข้ารหัสแล้วจะได้ผลลัพธ์ (Output) เป็นข้อความที่ผ่านการเข้ารหัสแล้ว (หรือไซเฟอร์เท็กท์) ขนาด 64 บิตจำนวน 1 ค่าต่อการเข้ารหัส 1 ครั้ง



รูปที่ 11 มาตรฐานการเข้ารหัสข้อมูลแบบ Data Encryption Standard (DES)

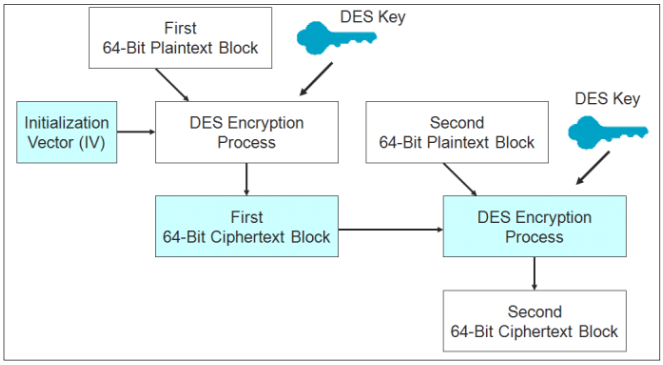
- มาตรฐาน DES (Attractions of DES)

ปัจจัยที่ทำให้มาตรฐานการเข้ารหัสแบบ DES ยังคงมีความโดดเด่นอยู่แม้กระทั่งในปัจจุบันก็เพราะมันเป็นมาตรฐานการเข้ารหัสที่ได้รับการออกแบบพัฒนามาเป็นอย่างดีซึ่งสามารถคงทนต่อภัยคุกคามทุกรูปแบบ [14] ยกเว้นปัญหาการถูกลักลอบถอดรหัสข้อความด้วยการโจมตีในลักษณะของการค้นหาลึกลงไปในรายละเอียด(Exhaustive Search Attack) เช่นกรรมวิธีแบบบรู๊ทฟอร์ส (Brute-Force เป็นต้นนอกจากนี้แล้วDES ยังได้ยังสามารถทำงานร่วมกันกับสิ่งอุปกรณ์ที่ใช้เร่งการทำงานของฮาร์ดแวร์(Hardware Accelerators) ได้เป็นอย่างดี

- การเข้ารหัสแบบ DES-CBC (DES – Cipher Block Chaining)

ปัญหาหนึ่งที่เกิดขึ้นกับมาตรฐานการเข้ารหัสแบบ DES ทั่วไปคือถ้าใช้ข้อมูลขาเข้า (Input Plaintext) เป็นข้อมูลเดียวกันจะได้ข้อมูลขาออกที่ผ่านการเข้ารหัสแล้ว (Output Cipher text) ที่เหมือนกันเสมอซึ่งลักษณะนี้อาจส่งผลให้นักถอดรหัสข้อมูล (Cryptanalysts) ที่มีทักษะสูงสามารถที่จะแกะกุญแจรหัส DES ที่ใช้เข้ารหัสนั้นได้ [15]

- กระบวนการห่วงโซ่ของกลุ่มข้อมูลไซเฟอร์เท็กท์(Cipher Block Chaining – CBC) อันเนื่องมาจากสาเหตุข้างต้นในการดำเนินการด้านการเข้ารหัสด้วยมาตรฐาน DES ส่วนใหญ่จะใช้กรรมวิธีที่เรียกว่า DES-CBC ซึ่งCBC หมายถึงกระบวนการห่วงโซ่ของกลุ่มข้อมูลไซเฟอร์เท็กท์ดังที่ได้แสดงไว้ในรูปที่11จะเห็นว่าในการเข้ารหัสจะมีข้อมูลขาเข้า (Inputs) จำนวน 3 ส่วนซึ่งนอกจากกุญแจรหัส (Key) และข้อมูลตั้งต้น (Plaintext) ที่ถูกนำมาใช้เป็นข้อมูลขาเข้า(Input) แล้วในกระบวนการแบบDES-CBC นี้ยังได้เพิ่มข้อความไซเฟอร์เท็กท์ที่เกิดจากกลุ่มข้อมูลก่อนหน้า (Previous block) เข้ามาเป็นข้อมูลขาเข้าอีกส่วนหนึ่งด้วยด้วยเหตุนี้เองทำให้กลุ่มข้อมูลตั้งต้นขนาด 64 บิต (64-Bit Plaintext) เมื่อผ่านการเข้ารหัสแบบนี้แล้วจะไม่ทำให้เกิดไซเฟอร์เท็คท์ขนาด 64 บิตที่เหมือนกันตลอดถือเป็นการพยายามในการป้องกันนักถอดรหัสอีกวิธีหนึ่ง อย่างน้อยที่สุดก็ทำให้นักถอดรหัสต้องใช้ความพยายามมากขึ้นในการที่จะถอดรหัสข้อมูลชุดนั้นหนทางในการดำเนินการตามกรรมวิธีเข้ารหัสแบบ DES-CBC นี้จำเป็นต้องสร้างเวกเตอร์เริ่มต้น (Initialization Vector – IV) ขนาด 64 บิตขึ้นมาก่อนสำหรับใช้เข้ารหัสร่วมกับกลุ่มข้อมูลขนาด 64 บิตกลุ่มแรก [16] ดังที่ได้แสดงไว้ในรูปที่ 12



รูปที่ 12 DES-CBC (DES-Cipher Block Chaining)

2. Triple Data Encryption Standard –3DES, TDES

การเข้ารหัสแบบ Triple DES (TDES) ในสถานการณ์ที่การเข้ารหัสแบบDES ไม่มีความปลอดภัยเพียงพอหลายองค์กรได้มีความพยายามในการที่จะปรับเปลี่ยนมาใช้การเข้ารหัสแบบTriple DES หรือที่เรียกกันย่อๆ ว่า3 DES แทนซึ่งเป็นวิธีการที่ขยายขอบเขตการใช้งานกุญแจรหัส DES ให้มีความซับซ้อนและปลอดภัยมากขึ้นแทนการใช้การเข้ารหัสมาตรฐาน DES แบบพื้นฐานทั่วไป [15] ดังแสดงไว้ในตารางที่ 3

ตาราง 3 การเข้ารหัสแบบ Triple DES (TDES) ด้วยกุญแจรหัสมาตรฐาน DES จำนวน 3 ชุด (คิดเป็น168 บิต)

Sender	Receiver
Encrypts plaintext with 1st key	Decrypts ciphertext with 3d key
Decrypts output of first step with the 2nd key	Encrypts output of the first step with the 2nd key
Encrypts output of second step with the 3d key; gives the ciphertext to be sent	Decrypts output of second step with the 1st key; gives the original plaintext

การเข้ารหัสแบบ TDES ด้วยกุญแจรหัส DES จำนวน 3 ชุด168-Bit TDES Operation [17]

วิธีการนี้โดยปกติแล้วผู้ส่งและผู้รับจะต้องใช้กุญแจรหัสตามมาตรฐาน TDES (ที่มีความยาวขนาด 56 บิต) จำนวน 3 ชุดเพื่อทำการเข้ารหัสจำนวน 3 ครั้ง (Triple Encryption) ทำให้พิจารณาได้ว่าเป็นการใช้กุญแจรหัสรวมแล้วขนาด 168 บิต (กุญแจรหัสแบบDES ขนาด 56บิตคูณ 3 เท่ากับ 168 บิต) ซึ่งถือว่ามีความแข็งแกร่งเพียงพอสำหรับการเข้ารหัสแบบสมมาตรในปัจจุบัน (อย่าลืมว่าการเข้ารหัสด้วยกุญแจรหัสแบบสมมาตรที่มีความยาวตั้งแต่ 100 บิตขึ้นไปถือว่าเป็นกุญแจรหัสที่มีความแข็งแกร่งเพียงพอ) แม้แต่ธนาคารขนาดใหญ่หลายแห่งก็ใช้กรรมวิธีนี้ในการดำเนินธุรกรรมทางการเงิน

ให้พิจารณาตารางที่ 3 ข้างต้นจะเห็นกระบวนการว่าผู้ส่ง (Sender) ทำการเข้ารหัส(Encrypts) ข้อมูลตั้งต้น (Plaintext) ด้วยกุญแจรหัสชุดแรกเมื่อได้ผลลัพธ์ออกมาก็นำมาถอดรหัส (Decrypts) ด้วยกุญแจชุดที่ 2 เมื่อได้ผลลัพธ์ครั้งที่ 2 ออกมาก็นำมาเข้ารหัสอีกครั้งด้วยกุญแจรหัสชุดที่ 3 ก็จะได้เป็นไซเฟอร์เท็กท์ที่จะส่งออกไปยังผู้รับ (Receiver) ในทางกลับกันทางฝั่งผู้รับก็จะทำกระบวนการย้อนกลับคือนำไซเฟอร์เท็กท์ที่ได้รับมานั้นมาดำเนินการถอดรหัส(Decrypts) ด้วยกุญแจรหัสชุดที่ 3 เมื่อได้ผลลัพธ์ออกมาก็นำไปเข้ารหัส(Encrypts) ด้วยกุญแจรหัสชุดที่ 2 และสุดท้ายก็นำผลลัพธ์จากขั้นตอนที่ 2 มาทำการถอดรหัสด้วยกุญแจชุดที่ 1 ซึ่งก็จะทำให้ได้กลับมาเป็นข้อความตั้งต้น (Plaintext) ตรงตามความต้องการของผู้ส่ง

ถึงแม้ว่าการเข้ารหัส (Decrypt) เพื่อให้เกิดความลับในขั้นตอนที่ 2 ของระบบการเข้ารหัสแบบ TDES นั้นดูคร่าวๆว่าเป็นหนทางที่ดีแต่อย่างไรก็ตามต้องตระหนักว่าเฉพาะระบบการรหัสแบบDES และในหลายๆระบบการรหัสนั้นการเข้ารหัส (Encryption) และการถอดรหัส (Decryption) ต้องสามารถทำงานร่วมกันได้ในแนวทางที่ว่าการถอดรหัสนั้น(Decryption) ต้องสามารถทำให้เกิดเป็นไซเฟอร์เท็กท์ได้และไซเฟอร์เท็กท์นั้นจะต้องสามารถถูกดำเนินการผ่านกระบวนการย้อนกลับให้เป็นข้อความตั้งต้น (Plaintext) ได้ด้วยการเข้ารหัส (Encryption) ข้อความข้างต้นถือว่าสำคัญที่อาจขัดกับความรู้สึกบ้างในแง่ที่ว่าโดยปกติแล้วข้อความตั้งตน (Plaintext) จะต้องถูกเข้ารหัส(Encrypt) ถึงจะกลายมาเป็นข้อความที่ถูกเข้ารหัสแล้ว(Ciphertext) ไม่ใช่ผ่านกระบวนการถอดรหัส (Decrypt) และในทางกลับกันไซเฟอร์เท็กท์ก็ควรจะผ่านกระบวนการถอดรหัส (Decrypt) ถึงจะกลับมาเป็นข้อความตั้งต้น (Plaintext) ได้ (ไม่ใช่ผ่านกระบวนการเข้ารหัสกลับมาเป็นเพลนเท็กซ์) ซึ่งนั่นก็หมายความว่าถ้าระบบการรหัสใดไม่รองรับกระบวนการย้อนกลับแบบนี้ก็ไม่สามารถนำกรรมวิธีในการเข้ารหัสแบบTDES มาประยุกต์ใช้ร่วมกันได้

แล้วถ้ามีพิจารณาต่อว่าถ้าอย่างนั้นกระบวนการรหัสแบบ 3 ขั้นตอนข้างต้นของ TDES ถือว่าเป็นกระบวนการที่ดีหรือมีประโยชน์หรือไม่คำตอบก็คือว่าเป็นกระบวนการที่ดีและมีประโยชน์เพราะเป็นกระบวนการที่สามารถนำมาใช้ร่วมกันกับการเข้ารหัสตามมาตรฐาน DES เดิมได้แม้ว่าจะใช้กุญแจรหัสเพียงชุดเดียวหรือสองชุดก็ยังสามารถทำงานร่วมกันกับ TDES ได้นั่นก็หมายความว่าซอฟต์แวร์ชุดเดียวกันนั้นสามารถนำมาประยุกต์ใช้กับการเข้ารหัสได้ทั้งแบบ TDES และแบบ DES ธรรมดาด้วยเช่นเดียวกัน [18] พิจารณาตารางที่ 4และตารางที่ 5

ตาราง 4 การเข้ารหัสแบบ Triple DES (TDES) ด้วยกุญแจรหัสมาตรฐานDES จำนวน 2 ชุด (คิดเป็น112 บิต)

Sender	Receiver
Encryptsplaintext with the 1st key	Decrypts ciphertext with the 1st key

Decrypts output with the 2nd key	Encrypts output with the 2nd key
Encrypts output with the 1st key	Decrypts output with the 1st key

ตาราง 5 การเข้ารหัสแบบ Triple DES (TDES) ด้วยกุญแจรหัสมาตรฐาน DES จำนวน 1 ชุด (56บิต)

Sender	Receiver
Encrypts plaintext with the key	Descryptsciphertext with the key
Encrypts output with the key (undoes first step)	
Encrypts output with the key	

มุมมองเกี่ยวกับการเข้ารหัสแบบ TDES (Perspective on TDES)

หากพิจารณาในแง่ของการรักษาความมั่นคงปลอดภัยสารสนเทศแล้วการเข้ารหัสแบบ TDESถือว่าเป็นการเข้ารหัสแบบกุญแจสมมาตรที่มีความแข็งแกร่งเพียงพอแต่หากพิจารณาในแง่ของการดำเนินการใช้งานจริงแล้วการที่ต้องผ่านกระบวนการรหัสถึง 3 รอบทำให้เกิดเป็นภาระของการประมวลผล(Processing Intensive) [17] ซึ่งถึงแม้ว่า TDES จะนับว่าเป็นการเข้ารหัสแบบสมมาตรที่มีความปลอดภัยเพียงพอก็ตามแต่ก็เป็นการเข้ารหัสที่ค่อนข้างช้าต้องการพลังในการประมวลผลสูงและต้องการหน่วยความจำสำรอง (RAM) ที่มากเพียงพอซึ่งไม่เหมาะกับสิ่งอุปกรณ์แบบพกพา (Hand-held Devices) แม้แต่กับเครื่องคอมพิวเตอร์ส่วนบุคคลแบบตั้งประจำที่ (Client PCs) เองก็ยังถือว่าไม่ค่อยเหมาะสมต่อการใช้งานจริงสักเท่าใด

3. Advanced Encryption Standard - AES

เนื่องมาจากความเริ่มล้าสมัยของการเข้ารหัสมาตรฐานDES รวมไปถึงข้อจำกัดความต้องการทรัพยากรในการประมวลผลที่ค่อนข้างสูงของการเข้ารหัสแบบ TDESสถาบันกำหนดมาตรฐานและเทคโนโลยีแห่งชาติของประเทศสหรัฐอเมริกา(The National Institute of Standards and Technology – NIST)จึงได้เสนอมาตรฐานใหม่ของการเข้ารหัสลับขั้นสูงชื่อว่าAES (Advanced Encryption Standard) [15] AES มีประสิทธิภาพดีเพียงพอทั้งในแง่ของพลังในการประมวลผลและความต้องการหน่วยความจำสำรอง (RAM)ที่เหมาะสมสามารถประยุกต์ใช้ได้กับสิ่งอุปกรณ์หลากหลายประเภทรวมไปถึงเครื่องโทรศัพท์มือถือระบบเซลลูล่าร์และเครื่องมือประเภทเลขาส่วนตัวดิจิตอลที่สมัยนี้อาจจะเรียกกันว่ามือถืออัจฉริยะหรือพีดีเอโฟน (PDAs) นั่นเอง ลองพิจารณาตารางสรุปเปรียบเทียบระหว่างการเข้ารหัสแบบDES, 3DES, และAES ดังแสดงไว้ในตารางที่ 6 [19]

ตาราง 6 ตารางสรุปเปรียบเทียบกรรมวิธีการเข้ารหัสแบบใช้กุญแจสมมาตรระหว่างDES, TDES, และAES

	DES	**TDES**	**AES**
Key Length (bits)	56	112 or 168	128, 192, 256
Strength	อ่อนแอ	เข้มแข็ง	เข้มแข็ง
Processing Requirements	ปานกลาง	สูง	ปานกลาง
RAM Requirements	ปานกลาง	สูง	ปานกลาง

ตามตารางที่ 6 คือมาตรฐานการเข้ารหัสลับขั้นสูงแบบ AES นั้นมีรูปแบบความยาวของกุญแจรหัสให้เลือกใช้อยู่ 3 ขนาด คือ กุญแจรหัสขนาด 128 บิต, 192 บิต, และ 256 บิตซึ่งขึ้นอยู่กับความจำเป็นให้สอดคล้องกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ(Security Threats) ซึ่งจะเห็นว่าAES ใช้กุญแจรหัสแบบสมมาตรที่มีขนาดเกิน 100 บิตทั้งหมด [20] จึงถือได้ว่า AES เป็นมาตรฐานการเข้ารหัสลับขั้นสูงที่มีความแข็งแกร่งมากเพียงพอ ซึ่งพบต่อมาว่าการเจาะรหัสลับด้วยวิธีการแบบบรู๊ทฟอร์ส (Brute-Force) สามารถถอดรหัสข้อความจากการเข้ารหัสแบบ DES ได้ภายในเวลาไม่กี่วินาทีนั้นจะต้องใช้เวลาถึงกว่า 100 ล้านล้านปี (Trillion Years) ในการถอดรหัสลับขั้นสูงมาตรฐานAES ขนาด 128 บิตสำหรับข้อมูลการเปลี่ยนในทางธุรกรรมแล้วการใช้กุญแจรหัสขนาด 192 บิตและ 256 บิตถือเป็นสิ่งจำเป็นโดยในปัจจุบันมีการกำหนดใช้งานมาตรฐานการเข้ารหัสลับขั้นสูงแบบ AES ในระบบการรหัส (Cryptographic Systems) หลายๆ ประเภทกันอย่างแพร่หลาย

ประเด็นความอ่อนแอและความแข็งแกร่งของกุญแจรหัสแบบสมมาตร ในกระบวนการเข้ารหัสที่ใช้กุญแจแบบสมมตรนี้ถ้าใช้กุญแจรหัสที่มีความยาวน้อยกว่า 100 บิตจะยังถือว่าเป็นกุญแจรหัสที่ยังคงมีความอ่อนแอ (Weak Keys) อยู่ซึ่งไม่ควรนำมาใช้ใน

กระบวนการพาณิชย์อิเล็กทรอนิกส์(e-Commerce) ซึ่งแน่นอนว่ากุญแจรหัสขนาด 56 บิตก็ย่อมพิจารณาว่ายังไม่มีความเข็มแข็งเพียงพอด้วยเช่นกัน

ถึงแม้ว่าในปัจจุบันนี้กุญแจรหัสแบบสมมาตรที่มีความยาวตั้งแต่ 100 บิตขึ้นไปจะนับว่าเป็นกุญแจรหัสที่มีความเข้มแข็งแล้วก็ตามแต่ถ้าข้อมูลที่ต้องส่งผ่านนั้นมีความสำคัญหรือมีความอ่อนไหวสูง (Sensitive Transactions) ข้อมูลด้านธุรกรรมต่างๆกุญแจรหัสที่ใช้ก็ควรต้องมีความยาวบิตมากขึ้นเพื่อให้มีความปลอดภัยเพียงพอและเหมาะสมกับข้อมูลเหล่านั้นและด้วยเทคโนโลยีระบบคอมพิวเตอร์สมัยใหม่ที่ทำให้เครื่องคอมพิวเตอร์สามารถประมวลผลได้อย่างรวดเร็วมากขึ้นเรื่อยๆกุญแจรหัสขนาด 100 บิตอาจจะไม่ถือว่าเป็นกุญแจรหัสแบบสมมาตรที่มีความแข็งแกร่งเพียงพออีกต่อไปแล้วในอนาคต

อย่างไรก็ตามในระบบคอมพิวเตอร์หลายๆ ระบบ สิ่งที่ผู้ใช้ต้องทำอาจเป็นเพียงแค่การจดจำรหัสผ่านแบบสั้นๆ (Brief Passwords) และข้อความในการพิสูจน์ตัวตน (Pass Phrases) เพื่อนำมาสร้างกุญแจรหัสซึ่งถ้าหากว่ารหัสผ่านและข้อความในการพิสูจน์ตัวตนนั้นไม่มีความปลอดภัยเพียงพอ (ซึ่งมีแนวโน้มที่จะเป็นแบบนั้นถ้าไม่มีการควบคุมที่ดีพอในการสร้างรหัสผ่าน) ก็ย่อมจะส่งผลให้กุญแจรหัสที่สร้างขึ้นมาใหม่นั้นไม่มีความแข็งแกร่งอย่างเพียงพอตามไปด้วย

B. Asymmetric Key Encryptions

อัลกอริทึมนี้จะใช้กุญแจสองตัวเพื่อทำงาน ตัวหนึ่งใช้ในการเข้ารหัสและอีกตัวหนึ่งใช้ในการถอดรหัสข้อมูลที่เข้ารหัสมาโดยกุญแจตัวแรก อัลกอริทึมกลุ่มสำคัญในแบบอสมมาตรนี้คือ อัลกอริทึมแบบกุญแจสาธารณะ (Public keys Algorithms) ซึ่งใช้กุญแจที่เรียกกันว่า กุญแจสาธารณะ (Public keys) ในการเข้ารหัสและใช้กุญแจที่เรียกกันว่า กุญแจส่วนตัว (Private keys) ในการถอดรหัสข้อมูลนั้น กุญแจสาธารณะนี้สามารถส่งมอบให้กับผู้อื่นได้ เช่น เพื่อนร่วมงานที่เราต้องการติดต่อด้วย หรือแม้กระทั่งวางไว้บนเว็บไซต์เพื่อให้ผู้อื่นสามารถดาวน์โหลดไปใช้งานได้ สำหรับกุญแจส่วนตัวนั้นต้องเก็บไว้กับผู้เป็นเจ้าของกุญแจส่วนตัวเท่านั้นและห้ามเปิดเผยให้ผู้อื่นทราบโดยเด็ดขาด

อัลกอริทึมแบบกุญแจสาธารณะ ยังสามารถประยุกต์ใช้ได้กับการลงลายมือชื่ออิเล็กทรอนิกส์ (ซึ่งเปรียบเสมือนการลงลายมือชื่อของเราที่ใช้กับเอกสารสำนักงานทั่วไป) การลงลายมือชื่อนี้จะเป็นการพิสูจน์ความเป็นเจ้าของและสามารถใช้ได้กับการทำธุรกรรมต่างๆ บนอินเทอร์เน็ต เช่น การซื้อสินค้า เป็นต้น วิธีการใช้งานคือผู้เป็นเจ้าของกุญแจส่วนตัวลงลายมือชื่อของตนกับข้อความที่ต้องการส่งไปด้วยกุญแจส่วนตัว แล้วจึงส่งข้อความนั้นไปให้กับผู้รับ เมื่อได้รับข้อความที่ลงลายมือชื่อมา ผู้รับสามารถใช้กุญแจสาธารณะ (ที่เป็นคู่ของกุญแจส่วนตัวนั้น) เพื่อตรวจสอบว่าเป็นข้อความที่มาจากผู้ส่งนั้นหรือไม่

อัลกอริทึมแบบกุญแจสาธารณะ แบ่งตามลักษณะการใช้งานได้เป็น 2 ประเภท คือ

- ใช้สำหรับการเข้ารหัส
- ใช้สำหรับการลงลายมือชื่ออิเล็กทรอนิกส์

โดยอัลกอริทึมที่นำมาใช้ในการ Authentication ใน Wimaxในปัจจุบันคือ RSA

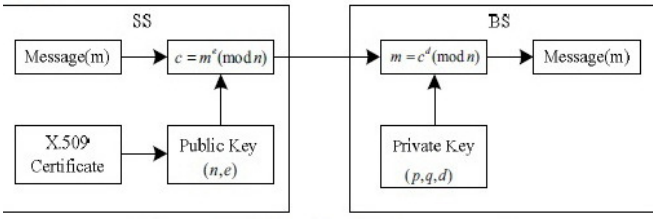
RSA

RSA เป็น encryption บนอินเตอร์เน็ตและระบบการรับรองที่ใช้อัลกอริทึมที่พัฒนาในปี 1977 โดย Ron Rivest, Adi Shamir และ LoonardAdleman อัลกอริทึม RSA มีการใช้โดยทั่วไปในการ encryption [21] และการรับรองซึ่งได้ร่วมเป็นส่วนหนึ่งของ web browser จาก Netscaps และ Microsoft รวมถึง Lotus Notes, Intuit Quicken และผลิตภัณฑ์อื่นๆ ระบบ encryption เป็นของ RSA Security [22] บริษัทต้องขออนุญาตการใช้เทคโนโลยีอัลกอริทึมและการขายชุดพัฒนาโปรแกรมเทคโนโลยีเป็นส่วนของมาตรฐานเว็บอินเตอร์เน็ตและการคำนวณ

การทำงานของ RSA

รายละเอียดทางคณิตศาสตร์ของอัลกอริทึมใช้ในการเก็บ public key และ private key มีให้ที่เว็บ RSA โดยย่ออัลกอริทึมนี้ใช้ผลคูณของprime number ขนาดใหญ่ (prime number หารลงตัวได้โดยตัวเลขและ1) และผ่านกระบวนการเพิ่มเติมที่มาจากกลุ่มของ2 จำนวนที่เก็บpublic key และอีกชุดเก็บprivate key เมื่อมีการพัฒนา key จำนวนprime number ดังเดิมจะไม่มีความสำคัญและถูกลบทิ้งทั้งkey สาธารณะและส่วนตัว [23] ต้องการสำหรับ encryption/decryption แต่เฉพาะเจ้าของ private key ที่ต้องการทราบการใช้ระบบ RSA, private key ไม่ต้องมีการสั่งข้ามอินเตอร์เน็ต private key ใช้decrypt ข้อความที่ได้รับการ encrypted ด้วย public key ถ้ามีการส่งข้อความผู้ส่งสามารถค้นหาpublic key ของผู้รับจากผู้บริหารกลางและ encrypt ข้อความไปให้ผู้รับด้วย public key ของผู้รับซึ่งผู้รับสามารถรับรองตัวเองกับผู้ส่งโดยการ

ใช้ private key ในการ encrypt การรับรองดิจิตอลเมื่อผู้ส่งได้รับแล้วผู้ส่งสามารถใช้ public key ของผู้รับเพื่อ decrypt

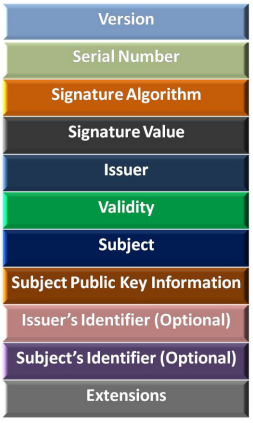


รูปที่ 13 ขั้นตอนการตรวจสอบ RSA [3]

มีการใช้ RSA ร่วมกับ X.509 เพื่อให้เกิดประสิทธิภาพมากขึ้น

1. X.509 Authentication Service

ระบบ X.509 เป็นระบบการพิสูจน์สิทธิ์ที่สำคัญมากในระบบเครือข่ายโดยX.509 เป็นอนุกรมย่อยของ X.500 ซึ่งกำหนดมาตรฐานโดย ITU-T โดยในขณะที่ X.500 เป็นตัวกำหนดโครงสร้างในลักษณะที่เป็นDirectory หรือ Hierarchy Tree นั้น X.509 จะทำหน้าที่ในการพิสูจน์สิทธิ์ให้กับส่วนต่างๆ ของ Directory นั้นสำหรับรูปแบบการใช้งานเมื่อเทียบกับ Kerberos แล้วการใช้งาน Kerberos จะเน้นไปที่การพิสูจน์สิทธิ์เพื่อเข้าใช้บริการซึ่งมักจะเป็นการพิสูจน์สิทธิ์ภายในองค์กรเดียวกันแต่X.509 จะเน้นไปที่การพิสูจน์ตัวบุคคลเพื่อยืนยันการติดต่อมากกว่า [25]



รูปที่ 14 X.509 Certificate [24]

การทำงานของX.509 จะมีโครงสร้างการทำงานที่เป็น Directory โดยในที่นี้Directory จะทำหน้าที่เป็นที่เก็บข้อมูลที่ใช้ในการยืนยันซึ่งโดยทั่วไปจะอยู่ในรูปของCertificate ซึ่งในCertificate จะบรรจุPublic Key ของผู้ใช้ที่Signed โดยPrivate Key ขององค์กรที่จ่ายใบCertificate มาให้สำหรับการทำงานของX.509 นั้นจะมีขอบเขตการนำไปใช้งานที่กว้างขวางมากเช่นใช้ในการทำMail Security ใช้ในการทำIP Security ใช้ในการทำWeb Security หรือหากจะกล่าวว่าเมื่อใดที่ต้องการการพิสูจน์หรือยืนยันบุคคลหรือยืนยันเครื่องคอมพิวเตอร์แล้วก็มักจะอยู่ในขอบข่ายการทำงานของ X.509 เสมอ [24]

X.509 ได้ถูกนำเสนอเมื่อปี1988 จากนั้นได้ผ่านการปรับปรุงเป็นลำดับขั้นในประเด็นต่างๆรวมทั้งเรื่องของความปลอดภัยด้วยจากนั้นก็ได้ออกมาเป็นข้อเสนอที่ปรับปรุงแล้วในปี 1993 และปรับปรุงอีกครั้งในปี1995 โดยการทำงานของX.509 จะใช้การเข้ารหัสแบบPublic Key และใช้มาตรฐานDigital Signature ในการSigned สำหรับอัลกอริทึมนั้นไม่ได้ระบุแน่นอนโดยสามารถเลือกใช้ได้หลายตัวแต่ที่แนะนำคือRSA สำหรับDigital Signature ก็เช่นกันที่ไม่ได้กำหนดมาตรฐานของอัลกอริทึมHash เอาไว้ [26]

2. Certificate

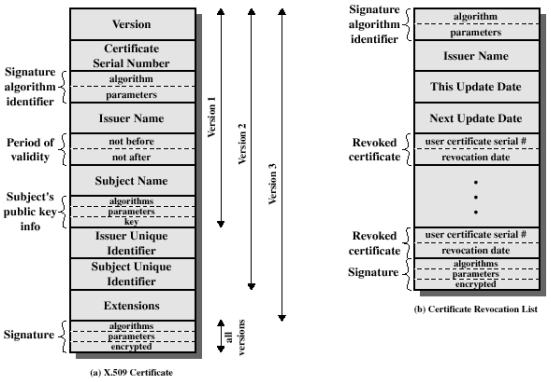
เนื่องจาก X.509 นั้นจะเปรียบเสมือนกับโครงสร้างที่ทำหน้าที่เก็บ Certificate ซึ่งทำหน้าที่เป็นใบรับรอง Public-Key ของแต่ละบุคคลหรือแต่ละเครื่องว่าเป็น Public Key ที่ทำหน้าที่เป็นตัวแทนของบุคคลนั้นหรือเครื่องนั้นจริงโดย Certificate จะสร้างขึ้นโดย Certificate Authority หรือ CA ที่เชื่อถือ (Trust) ได้จากนั้นก็จะนำมาเก็บใน CA ซึ่งอาจเป็น CA ที่สร้างCertificate หรือไม่ก็ได้ดังนั้นจุดเริ่มแรกที่เราจะต้องศึกษาคือโครงสร้างของCertificate โดยในรูปที่ 15 จะแสดงรูปแบบทั่วไปของ Certificate โดยมีรายละเอียดดังนี้

- Version แสดงหมายเลขเวอร์ชันเพราะในแต่ละเวอร์ชันจะมีรูปแบบของข้อมูลที่ไม่เหมือนกันก็ได้โดยปกติจะเป็นเวอร์ชัน 1 แต่หากใน Certificate มีการใช้Initiator Unique Identifier หรือ Subject Unique Identifier แล้วค่าเวอร์ชันจะต้องเป็น2 และหากมีการใช้Extension ใดๆ ค่าของเวอร์ชันจะต้องเป็น3
- Serial Number เป็นเลขจำนวนเต็มโดยจะต้องไม่ซ้ำกันใน CA ที่จ่ายใบ Certificate มาโดยเลขนี้จะเป็นเลขที่จะใช้อ้างถึงแต่ละ Certificate ในแต่ละ CA ที่ได้สร้างขึ้นมา
- Signature Algorithm Identifier เป็นฟิลด์ที่ระบุอัลกอริทึมที่ใช้ในการ Sign Certificate พร้อมด้วยพารามิเตอร์ที่ใช้แต่เนื่องจากค่านี้จะระบุอีกครั้งในฟิลด์ Signature ฟิลด์นี้จึงไม่มีการใช้งานมากนัก
- Issue Name เป็นชื่อของ CA ที่สร้างและ Sign Certificate ใบนี้
- Period of Validity เป็นตัวบอกว่าให้ใช้ Certificate นี้ตั้งแต่เมื่อไรถึงเมื่อไร

- Subject Name เป็นชื่อของบุคคลที่ Certificate ใบนี้อ้างถึงหรือแทนบุคคลนั้นซึ่งหมายความว่าใน Certificate นี้จะเก็บ Public Key ที่มีบุคคลในฟิลด์นี้เป็นผู้เก็บ Private Key ที่คู่กันอยู่

- Subject's Public Key Information เป็นฟิลด์ที่เก็บ Public Key และระบุถึงอัลกอริทึมที่ใช้ที่ใช้กับ Key นี้และพารามิเตอร์อื่นๆ

- Issuer Unique Identifier เป็นฟิลด์ Option ที่ใช้ในการระบุถึง CA ในกรณีที่ X.500 Name มีการนำไปใช้กับส่วนอื่นๆ



รูปที่ 15 แสดง Format ของ X.509

- Subject Unique Identifier เป็นฟิลด์Option ที่ใช้ในการระบุถึงบุคคลในกรณีที่X.500 Name มีการนำไปใช้กับส่วนอื่น

- Extension เป็นกลุ่มของฟิลด์ที่เพิ่มเติมข้อมูลอื่นๆเข้ามาด้วย

- Signature จะบรรจุ MD ของข้อมูลในทุกฟิลด์ที่เข้ารหัสด้วย Private Key ของ CA เพื่อเป็นการยืนยันว่า Certificate นี้สร้างมาจากCA จริงๆโดยจะมีข้อมูลที่ระบุวิธีการ Hash และวิธีการเข้ารหัสด้วย [27]

ข้อดีและข้อเสียของ RSA

ข้อดี - จะมีการใช้Key ในการร้องขอการเข้าใช้งาน ซึ่ง Key มีการเข้ารหัสอีครั้งหนึ่ง ทำให้ปลอดภัยมากยิ่งขึ้น

ข้อเสีย - ความน่าเชื่อถือของหน่วยงานกลางที่มีหน้าที่เก็บ Key

- ต้องใช้วิธีการอื่นร่วม เพราะอาจเกิดกรณีการดัก Key กลางทาง เช่น Man in the Middle Attack

เมื่อเปรียบเทียบการเข้ารหัสแบบ Symmetric Key Encryptions และ AsymmetricKey Encryptions ในเชิงการทำงาน สามารถสรุปได้ดังตารางที่ 7

ตาราง 7 เปรียบเทียบการเข้ารหัสแบบ Symmetric Key Encryptions และ AsymmetricKey Encryptions ในเชิงการทำงาน

No	Symmetric Key Encryptions	Asymmetric Key Encryptions
1. Number of keys	1 key	2 keys แยกPublic Key และPrivate Key
2. Key Distribution	ยากเนื่องจากว่าถ้ามีหลาย Party ที่ต้องการใช้ ก็จะต้องหา Secured Channel ส่งไปหา	ง่ายเนื่องจากว่าสามารถกระจาย Public Key ได้เลย ไม่ได้เป็นความลับ
3. Chain of trus	ขึ้นอยู่กับตอนทำ Key Distribution	มี Certificate Authority (CA) เป็นตัวกลางช่วยVerify แต่ละParty
4. Digital Signature Properties	ไม่สามารถทำ Digital Signature ได้	สามารถทำDigital Signature ได้
5. Key Revocation	ทำไม่ได้หรือทำได้ยาก	ทำได้โดยใช้CRL หรือ OCS

เมื่อเปรียบเทียบประสิทธิภาพของการเข้ารหัสแบบ Symmetric Key Encryptions และ AsymmetricKey Encryptions สามารถสรุปได้ดังตารางที่ 8

ตาราง 8 เปรียบเทียบประสิทธิภาพการทำงานของSymmetric Key Encryptions และ AsymmetricKey Encryptions

Appoaches	Asymmetric	Symmetric
Encryption	Slower	Faster
Descryption	Slower	Faster
Key Descryption	Easy	Difficult
Security	Highest	Moderate

C. EAP based

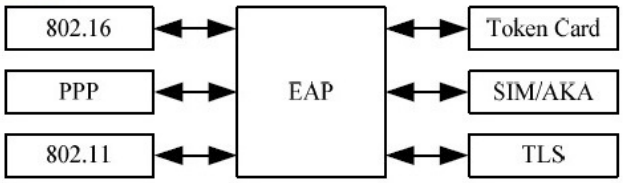
Extensible Authentication Protocol (EAP) คือ โปรโตคอลสำหรับเครือข่ายไร้สายที่ขยายบนวิธี authentication ที่ใช้โดย Point-to-Point Protocol (PPP)สามารถสนับสนุนกลไกของ

authentication ต่าง ๆ ได้ เช่น tokencards, smartcards, certificates, one-time passwords และ public key encryption authentication

การทำงานโดยทั่วไป ของ EAP Protocolคือ EAP ผู้ใช้ขอการเชื่อมต่อกับเครือข่ายไร้สายผ่านจุดเข้าถึง (สถานีที่ส่งผ่านและรับข้อมูล บางครั้งเรียกว่า transceiver) จุดเข้าถึงขอข้อมูลระบุตัว (ID) จากผู้ใช้และส่งผ่านข้อมูลนั้นไปยังแม่ข่าย authentication จากนั้นแม่ข่าย authentication จะขอให้จุดเข้าถึงสำหรับการพิสูจน์การดำรงอยู่ของ ID หลังจากนั้นจุดเข้าถึงบรรจุการตรวจสอบจากผู้ใช้และส่งกลับไปที่ แม่ข่าย authentication ผู้ใช้จึงจะเชื่อมต่อกับเครือข่ายตามคำขอ

การ Authentication ในรูปแบบ EAP Based จะกระทำผ่านสิ่งที่โอเปอเรเตอร์ออกให้ ไม่ว่าจะเป็น SIM หรือ X.509 ซึ่งมีหลายแบบ เช่น EAP-SIM ใช้ SIM, EAP-AKA ที่ใช้ USIM ของเครือข่าย 3G, EAP-TLS และ EAP-TTLS เป็นต้น โดยจะทำการตรวจสอบกับเครือข่ายเอง เช่น AAA Server หรืออุปกรณ์เครือข่ายที่เก็บข้อมูลลูกค้าไว้

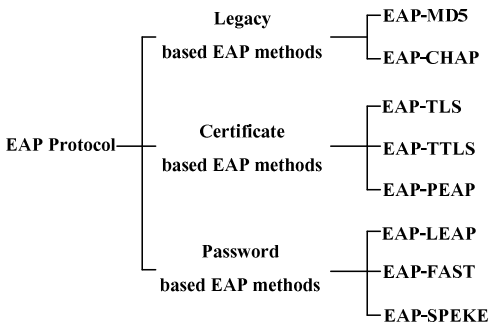
ข้อดีของวิธีการ EAP basedมีความสะดวก เพราะเป็นการร้องขอเข้าใช้งานกับ AAA Server โดยตรง



รูปที่ 16 สถาปัตยกรรมของ Protocol EAP

EAP แยกเป็น3 ประเภทตามวิธีการทำงาน ดังนี้ [24]

- Legacy based EAP methods
- Certificate based EAP methods
- Password based EAPmethods



รูปที่ 17 ประเภทของ EAP Protocol

1. Legacy based EAP methods

EAP-MD5

ข้อมูลที่ส่งผ่านไปยัง RADIUS เซิร์ฟเวอร์ คือ username และ password ซึ่งจะถูกเข้ารหัสด้วยเทคนิคที่เรียกว่า MD5 การใช้กลไก EAP-MD5 ช่วยแก้ไขปัญหาเรื่องการตรวจสอบผู้ใช้ในเครือข่าย WLAN ให้มีความปลอดภัยมากขึ้น แต่ไม่ได้ช่วยแก้ไขปัญหาเรื่องความไม่ปลอดภัยของการใช้รหัสลับเครือข่าย (WEP Key) ซึ่งมีความคงที่ (static) ดังนั้นผู้โจมตียังคงสามารถดักฟังและเจาะรหัสลับของเครือข่ายซึ่งมีความคงที่ได้ถึงแม้จะมีการใช้ EAP-MD5 เมื่อผู้โจมตีทราบรหัสลับของเครือข่ายแล้วก็จะสามารถเข้าใจข้อมูลที่รับส่งอยู่ในเครือข่ายและอาจทราบ username และ password โดยอาศัยเทคนิคต่างๆสำหรับการเจาะรหัส MD5 ได้ในที่สุดนอกจากนี้ข้อบกพร่องในกลไก EAP-MD5 อีกอย่างหนึ่งคือผู้ใช้ไม่สามารถตรวจสอบอุปกรณ์แม่ข่าย ซึ่งทำให้ผู้โจมตีอาจจะสามารถหลอกลวงให้ผู้ใช้ต่อเชื่อมเข้ากับอุปกรณ์แม่ข่ายของผู้โจมตีได้และสุดท้ายคือ Microsoft Vista, Microsoft ไม่สนับสนุน EAP-MD5 ทำให้ไม่เป็นที่นิยมใช้ในเวลาต่อมา [28]

EAP-CHAP

Challenge-Handshake Authentication Protocol (CHAP)เป็นโปรโตคอลhandshake 3 ทางที่ยอมรับกันว่ามีความปลอดภัยสูงกว่า Password Authentication Protocol สามารถใช้ได้สำหรับชนิดของการตรวจสอบความถูกต้อง TTLS เท่านั้น [2]

สิ่งที่น่าจะเป็นประโยชน์มากที่สุดของ EAP-LEAP คือ ค่าใช้จ่ายที่ต่ำ เพราะไม่มี public keyจึงทุ่นค่าใช้จ่ายและลดความยุ่งยากในการบริหาร นอกจากนี้การใช้ username/password มั่นใจได้ว่าเป็นการรับรองความถูกต้อง รวดเร็วและใช้เวลาน้อยในการตรวจสอบซึ่งกันและกัน

ข้อเสียของการ EAP-CHAP ก็คือว่าไม่มีวิธีที่จะสร้าง PMK สำหรับการเข้ารหัสของข้อมูลในอนาคตทำให้ วิธีนี้ไม่นิยมใช้

2.Certificate based EAP methods

EAP-TLS

EAP-TLS Protocol (Transport Layer Security) ได้รับการพัฒนาขึ้นโดยบริษัท Microsoft ซึ่งในโพรโตคอลนี้จะไม่มีการใช้ username และpassword ในการตรวจสอบผู้ใช้แต่จะใช้ X.509 certificates แทนซึ่งการทำงานของโพรโตคอลนี้จะอาศัยการส่งผ่าน PKI ผ่านSSL (Secure Sockets Layers) มายังEAP เพื่อใช้

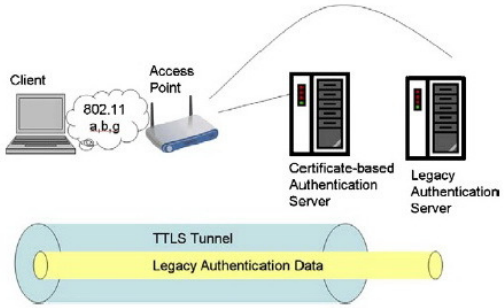
กำหนด WEP Key สำหรับผู้ใช้แต่ละคน EAP-TLS กำหนดให้มีการตรวจสอบทั้งเครื่องแม่ข่ายและผู้ใช้ (Mutual Authentication) [29] ด้วยเช่นเดียวกับ LEAP แต่อย่างไรก็ตามปัญหาหลักของ EAP-TLS ความยุ่งยากและค่าใช้จ่ายในการติดตั้งจัดการและบริหารระบบ PKI Certificate

ข้อดี ใช้ X.509 certificates ในการตรวจสอบผู้ใช้

ข้อเสีย ความยุ่งยากและค่าใช้จ่ายในการติดตั้งจัดการและบริหารระบบ PKI Certificate

EAP-TTLS

EAP-TTLS Protocolถูกเริ่มพัฒนาโดยบริษัท Funk Software ซึ่งการทำงานของ EAP-TTLS คล้ายกับ EAP-TLS คือจะมีการตรวจสอบเครื่องแม่ข่ายโดยใช้ Certificate แต่ผู้ใช้จะถูกตรวจสอบโดยการใช้username และ password [20] ซึ่งความปลอดภัยของ EAP-TTLS จะน้อยกว่า EAP-TLS และที่สำคัญ EAP-TTLS อาจไม่ได้รับความนิยมมากนักในเวลาต่อไปเนื่องจาก Microsoft และ Cisco ได้ร่วมมือกันพัฒนาโพรโตคอลขึ้นมาใหม่ชื่อว่า PEAP (Protected EAP) ซึ่งมีการทำงานเช่นเดียวกับ EAP-TLS ที่กล่าวมาแล้วข้างต้น



รูปที่ 18 TTLS Authentication

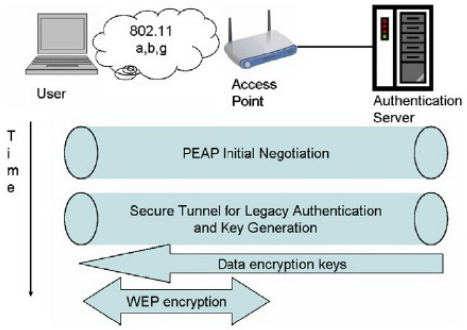
ข้อดี - มีการตรวจสอบเครื่องแม่ข่ายโดยใช้ Certificate

ข้อเสีย - ความปลอดภัยของ EAP-TTLS จะน้อยกว่า EAP-TLS

- ไม่ได้รับความนิยมมากนักในเวลาต่อไปเนื่องจากได้พัฒนาโพรโตคอลขึ้นมาใหม่ชื่อว่า PEAP

EAP-PEAP

PEAP เป็นการตรวจสอบความถูกต้อง Extensible Authentication Protocol (EAP) IEEE 802.1X ชนิดใหม่ที่ออกแบบมาเพื่อใช้ประโยชน์จาก EAP-Transport Layer Security (EAP-TLS) ด้านของเซิร์ฟเวอร์และสนับสนุนวิธีการตรวจสอบความถูกต้องหลายๆวิธีรวมทั้งรหัสผ่านของผู้ใช้และรหัสผ่านป้อนครั้งเดียวและ Generic Token Cards [28]



รูปที่ 19 PEAP Authentication

3. Password based EAPmethods

EAP- LEAP

LEAP หรือEAP-Cisco Wireless โพรโตคอล LEAP (Lightweight Extensible Authentication Protocol) ได้รับการพัฒนาขึ้นโดยบริษัท Cisco ซึ่งในโพรโตคอลนี้นอกจากจะมีกลไกในการส่งผ่านข้อมูลเกี่ยวกับusername และpassword ของผู้ใช้ไปยัง RADIUS เซิร์ฟเวอร์เพื่อทำการตรวจสอบแล้วLEAP ยังมีการจัดการและบริหารรหัสลับของเครือข่าย (WEP Key) ให้มีการเปลี่ยนแปลงค่านั่นคือเมื่อผู้ใช้ผ่านการตรวจสอบเรียบร้อยแล้วจะได้รับ WEP Key เพื่อใช้ในการเข้ารหัสข้อมูลสำหรับผู้ใช้นั้นๆ [1] ซึ่งหมายความว่า WEP Key ของแต่ละผู้ใช้สามารถมีความแตกต่างกันออกไปได้

ข้อเสีย คือ ในปัจจุบันLEAP ยังถูกจำกัดอยู่แต่ในผลิตภัณฑ์ของCisco เท่านั้น

EAP-FAST

EAP-FAST คล้ายกับ EAP-TTLS มาก EAP-FAST อาศัยหลักการใช้งานของ TLS เพื่อสร้างอุโมงค์ระหว่าง Client และ Server ที่สามารถนำมาตรวจสอบ client ผ่านการใช้รหัสผ่านในการตรวจสอบ แต่ความแตกต่างระหว่าง Certificate-based EAP methods และ EAP-FAST คือ ไม่ต้องใช้ server ที่มี public key แต่ EAP-FAST จะใช้ Protected Access Credential (PAC) เพื่อสร้างอุโมงค์ TLS

ฉะนั้นEAP-FAST จึงเป็นเพียงสิ่งที่มาแทน EAP-LEAP และถูกจัดกลุ่มในกลุ่ม Password-based methods

หนึ่งในข้อดีที่ใหญ่ที่สุดของ EAP-FAST คือมันให้ความปลอดภัยมากคล้ายกับ EAP-TTLS หรือ PEAP ไม่มีค่าใช้จ่ายเกี่ยวกับ Public key อย่างไรก็ตามการรักษาความปลอดภัยที่เกี่ยวข้องกับ PKI ก็ยังคงอยู่ เพราะไม่มี CAที่ดูแลเฉพาะ ข้อดีของวิธีการนี้คือ มันรองรับการเชื่อมต่อใหม่ได้อย่างรวดเร็วที่กำหนดโดย RFC 3748

ข้อเสียที่ใหญ่ที่สุดของวิธีนี้คือ ต้องมีการ round Trip หลายๆ รอบในการเชื่อมต่อระหว่าง client และ server อีกทั้งเมื่อมี automatic PAC ที่เปิดใช้ EAP-FAST มีช่องโหว่ตรงผู้โจมตีสามารถดัก PAC และสามารถใช้สิทธิของ user อย่างไรก็ตาม EAP-FAST ก็ยังเป็นทางเลือกที่ดีของ Cisco ที่จะใช้แทน EAP-LEAP [28]

EAP- SPEKE

SPEKE or Simple Password Exponential Key Exchange SPEKE จะวิธีการใช้ความรู้ร่วมกันของรหัสผ่านทั้งในauthenticatorและclientเพื่อสร้างชุดของข้อความที่จะแลกเปลี่ยนของเนื้อหาแบบสุ่มคีย์เซสชันต้นแบบจะใช้ร่วมกันระหว่างอุปกรณ์เพื่อเพิ่มความแข็งแกร่งของการป้องกัน

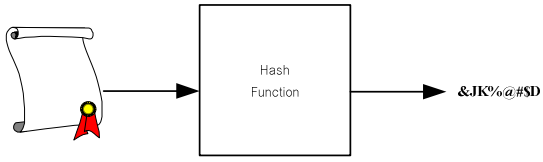
EAP-SPEAK อาศัยการยกกำลังเลขสุ่มขนาดใหญ่ ซึ่งเป็นจำนวนเฉพาะขนาดใหญ่ การคำนวณค่าชี้แจงจะถือเป็นฟังก์ชั่นทางเดียว ตั้งแต่ขั้นตอนการlogarithmic ในการคำนวณค่าเดิมที่มีความซับซ้อน ดังนั้นคนที่ไม่มีค่าชี้แจงจะไม่สามารถที่จะไม่สามารถกำหนดฐานหรือเลขชี้กำลังได้ [28]

ตารางที่ 9 เปรียบเทียบ EAP แต่ละวิธี [28]

	Legacy	EAP-TLS	EAP-TTLS	EAP-PEAP	EAP-LEAP	EAP-FAST	EAP-SPEKE
RFC 4017 requirement							
Mutual Auth.	No	Yes	Yes	Yes	Yes	Yes	Yes
Session Keys	No	Yes	Yes	Yes	Yes	Yes	Yes
Dict.Attack Immunity	No	Yes	Yes	Yes	No	Yes	Yes
Man-in-Mid. Immunity	No	Yes	Yes	Yes	No	Yes	Yes
Practical Issues							
User Authentication	Yes	Not if cert is on disk	Not if cert is on disk	Not if cert is on disk	Yes	Not if cert is on disk	Yes
Forward Secrecy	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Efficient	Yes	No	No	No	Yes	No	Yes
Low Cost	Yes	No	No	No	Yes	Yes/No	Yes
Broad AP Support	Yes	Yes	No	Yes	No	No	Yes
Fast Reauthentication	No	Yes	Yes	Yes	No	Yes	No

D. Algorithm Hash

Hash หมายถึงการนำเอาตัวเลขหรือข้อความมาผ่านกรรมวิธีอย่างใดอย่างหนึ่งแล้วได้ผลลัพธ์ออกมาเป็นตัวเลขชุดฟังก์ชั่นHash (Hash Function) มีบทบาทอย่างมากต่อการรักษาความมั่นคงปลอดภัยในเครือข่ายจากคุณสมบัติที่สำคัญหลายๆ ประการพบว่ามีคุณสมบัติหลักในการตรวจสอบการคงสภาพของข้อมูลโดยที่ค่า Hash ของข้อความใดๆ (Message Digest) จะถูกแนบไปด้วยกันกับข้อความนั้นและส่งออกไปยังเครือข่ายหากข้อความถูกแก้ไขแล้วจะทำให้ค่าMessage Digest นั้นไม่เหมือนเดิมฟังก์ชั่นHash ถูกใช้เพื่อตรวจสอบว่าข้อความที่ส่งได้ถูกแก้ไขระหว่างทางหรือไม่นั่นเอง [8]



รูปที่ 20 แสดงการทำงานของ Hash

กรรมวิธีการ Hash ที่ว่านี้โดยส่วนใหญ่จะเป็นฟังก์ชันทางคณิตศาสตร์โดยฟังก์ชัน Hash ที่ดีจะต้องมีคุณสมบัติการกระจายที่ดีกล่าวคือข้อความเดียวกันเมื่อผ่าน Hash ฟังก์ชันแล้วจะต้องได้ผลลัพธ์เหมือนเดิมเสมอและหากข้อความที่ต่างกันเพียงเล็กน้อยผ่าน Hash ฟังก์ชันควรจะต้องได้ผลลัพธ์ที่ต่างกันมากและที่สำคัญก็คือ

ไม่ควรมีข้อความใดๆ ตั้งแต่ 2 ข้อความขึ้นไปที่ผ่าน Hash ฟังก์ชันแล้วจะได้ผลลัพธ์ที่เหมือนกันนอกจากนั้นแล้วฟังก์ชัน Hash ที่ดีควรมีคุณสมบัติดังต่อไปนี้

- ฟังก์ชัน Hash ควรสามารถใช้งานกับข้อมูลที่มีความยาวใดๆ

- ฟังก์ชัน Hash จะต้องสามารถสร้างผลลัพธ์ที่มีความยาวเพียงค่าเดียว (คือผลลัพธ์ยาวเท่ากันหมด)

- ฟังก์ชัน Hash ควรเป็นฟังก์ชันที่ไม่ซับซ้อนสามารถสร้างโดยฮาร์ดแวร์และซอฟต์แวร์ได้ง่าย

- ฟังก์ชัน Hash ไม่ควรเป็นฟังก์ชันที่ย้อนกลับได้คือเมื่อทราบผลลัพธ์แล้วไม่มีทางทราบข้อมูลเลย

- ฟังก์ชันHash ไม่ควรสร้างผลลัพธ์เดียวกันจากข้อมูลที่ต่างกันy <> x เมื่อH (x) = H (y)

ในทุกอัลกอริทึมของฟังก์ชันHash มักใช้หลักการทำงานเดียวกันนั่นคือการแบ่งข้อมูลออกเป็นบล็อกละเท่าๆกันโดยสมมติว่ามีความยาวn บิตจากนั้นจะเริ่มทำงานตั้งแต่บล็อกข้อมูลแรกโดยนำมาผ่านฟังก์ชัน Hash ซึ่งจะได้ผลลัพธ์ออกมาชุดหนึ่งจากนั้นโดยใช้ผลลัพธ์ที่ได้กับข้อมูลในบล็อกถัดไปเมื่อนำมาผ่านฟังก์ชันHash ก็จะได้ผลลัพธ์ใหม่จากนั้นก็จะทำแบบเดิมกับบล็อกข้อมูลถัดไปเรื่อยๆจนหมดก็จะได้ผลลัพธ์สุดท้ายซึ่งก็คือ Message Digest นั่นเองเช่นหากฟังก์ชันHash คือการทำ XOR ของทุกบิตในบล็อกแล้วจะสามารถเขียนเป็นสมการทำงานได้ดังนี้

$$Ci = bi1 + bi2 + \ldots + bim$$

จากสมการด้านบนจะแสดงการทำงานโดยจะเป็นการหาค่า Parity ของแต่ละบิตที่เรียกว่า Longtitude Redundancy Check ซึ่งจะได้ข้อมูลผลลัพธ์ความยาวn บิตเท่ากับบล็อกของข้อมูลอย่างไรก็ตามเนื่องจากวิธีการนี้เป็นวิธีการง่ายๆ จึงอาจเกิดความผิดพลาดขึ้นได้ง่ายเพราะการใช้วิธี Parity นั้นหากมีบิตที่ผิดพลาดหลายบิตก็อาจทำให้ได้ MD ที่มีค่าเท่ากันได้ง่ายซึ่งไม่เป็นไปตามคุณสมบัติข้อที่ 5 ดังนั้นจึงไม่มีการนำไปใช้งานจริงแต่ใช้ในการอธิบายหลักการพื้นฐานเท่านั้น [30]

	bit 1	bit 2	. . .	bit *n*
block 1	b_{11}	b_{21}		b_{n1}
block 2	b_{12}	b_{22}		b_{n2}
	. . .	. . .	. . .	. . .
block *m*	b_{1m}	b_{2m}		b_{nm}
hash code	C_1	C_2		C_n

รูปที่ 21 Simple hash function Using Bitwise XOR

- Approaches to Message Authentication

ในการเข้ารหัสนั้นแม้ว่าจะสามารถป้องกันความลับไม่ให้ถูกดักจับ (Eavesdropping) ซึ่งเป็นการโจมตีในลักษณะ Passive แล้วยังมีการโจมตีในลักษณะ Active ได้แก่การเปลี่ยนแปลงข้อมูลซึ่งในบางครั้งเราก็ไม่ได้ต้องการที่จะรักษาความลับของข้อมูลมากนักด้วยว่าเป็นข้อมูลที่เปิดเผยแต่ต้องการการรับรองว่าเป็นเอกสารฉบับจริงซึ่งในโลกของเอกสารจริงเรามักใช้การเซ็นชื่อรับรองและการพิสูจน์ลายมือชื่อในการพิสูจน์ว่าเป็นเอกสารฉบับจริงหรือพิสูจน์ว่าได้รับรองเอกสารจริงซึ่งอาจหมายถึงว่าเป็นเอกสารหรือข้อมูลที่เป็นข้อมูลจริงหรือจากแหล่งข้อมูลที่ถูกต้อง

กระบวนการในการรับรองเอกสาร (Message Authentication) คือกระบวนการที่ยอมให้คู่ที่มีการรับส่งเอกสารกันสามารถจะพิสูจน์ได้ว่าเอกสารหรือข่าวสารที่ได้รับนั้นเป็นเอกสารที่รับรองความถูกต้องโดยมีเป้าหมายอยู่ 2 ประการคือรับรองว่าเนื้อความในเอกสารฉบับนั้นยังคงเป็นเนื้อความเดิมที่ส่งมาแบบนั้นโดยไม่ได้มีการเปลี่ยนแปลงระหว่างการส่งและรับรองว่าเอกสารฉบับนั้นส่งมาจากต้นทางที่อ้างถึงจริงๆเช่นหากเป็นการส่ง Mail ก็คือการรับรองว่า Mail ฉบับดังกล่าวส่งมาจากผู้ส่งตามชื่อจริงและเนื้อความก็คือเนื้อความที่ผู้ส่งเขียนขึ้นทั้งหมดนอกจากนั้นยังอาจรับรองด้วยว่าเอกสารนั้นเป็นเอกสารที่ส่งมาตามกำหนดไม่มีการล่าช้าจนเกินการใช้งานและไม่ได้เป็นเอกสารที่เกิดจากการส่งซ้ำ(Replay A ttack)

- Authentication Using Conventional Encryption

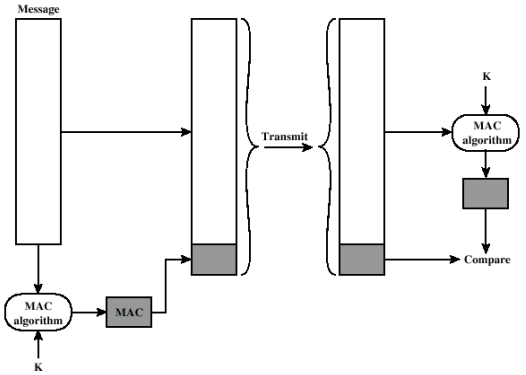
การรับรองเอกสารที่ง่ายที่สุดวิธีหนึ่งก็คือการเข้ารหัสเอกสารด้วยConventional Encryption โดยหากเราสมมติว่ามีเฉพาะผู้ส่งและผู้รับที่รู้และใช้Key เดียวกันดังนั้นเมื่อผู้ส่งทำการส่งเอกสารก็จะมีเฉพาะผู้รับเท่านั้นที่สามารถถอดรหัสเพื่ออ่านเอกสารได้ดังนั้นจึงถือเป็นการรับรองเอกสารได้วิธีหนึ่งและหากในการส่งเอกสารมีการตรวจสอบความผิดพลาดและมีการกำหนดหมายเลขลำดับ(Sequence Number) ก็ยิ่งทำให้แน่ใจได้ว่าเอกสารไม่มีความผิดพลาดและมีลำดับการส่งที่ถูกต้องไม่สามารถทำReplay Attack ได้และหากมีการทำTimestamp ด้วยแล้วก็จะตรวจสอบเวลาที่ใช้ในการส่งได้อีกด้วย

- Message Authentication without Message Encryption

ในการรับรองเอกสารนั้นในบางครั้งก็ไม่มีความจำเป็นต้องเข้ารหัสเอกสารเพราะเอกสารบางอย่างเป็นเอกสารที่เปิดเผยอยู่แล้วเช่นเอกสารประเภทสัญญาประกาศหรือกฎระเบียบต่างๆเพราะการเข้ารหัสเอกสารนั้นทำให้ทุกครั้งที่มีการเปิดเอกสารออกอ่านจะต้อง

มีการถอดรหัสทุกครั้งซึ่งนับเป็นการสิ้นเปลืองเวลาที่ใช้ในการประมวลผลส่วนนี้ดังนั้นหากมีความจำเป็นต้องรับรองเอกสารที่สามารถเปิดเผยได้ก็ไม่ควรใช้วิธีการเข้ารหัสเพราะการเข้ารหัสเป็นคนละเรื่องกับการรับรองเอกสาร

ในการสร้างการรับรองเอกสารที่สามารถตรวจสอบได้นั้นอาจใช้ฟังก์ชันทางคณิตศาสตร์และรหัสลับ (Secret Key) เพื่อสร้างบล็อกของข้อมูลขนาดเล็กที่เรียกว่า Message Authentication Code หรือ MAC จากนั้นก็จะแนบ MAC ไปกับเอกสารและส่งไปยังผู้รับ โดยเมื่อผู้รับได้รับเอกสารและ MAC ก็จะนำเอกสารที่ได้รับนี้ไปผ่านฟังก์ชันทางคณิตศาสตร์เดียวกันโดยใช้รหัสลับเดียวกันเช่นหากส่งจาก A ไปยัง B ก็จะเรียกว่ารหัสลับ AB เพราะรหัสลับที่ต่างกันก็จะสร้าง MAC ที่ต่างกันดังนั้นในรหัสลับแต่ละรหัสลับก็จะใช้ในการส่งเอกสารเฉพาะคู่ใดคู่หนึ่งเท่านั้นโดยหากเอกสารที่ได้รับมีเนื้อความเหมือนกับที่ส่งมาเมื่อผ่านฟังก์ชันทางคณิตศาสตร์แล้วก็ควรจะได้ MAC ที่มีค่าเท่ากันด้วยดังนั้นก็จะนำค่าMAC ที่ได้จากการคำนวณไปเปรียบเทียบกับ MAC ที่แนบมากับเอกสารว่าเป็นค่าเดียวกันหรือไม่โดยหากมีค่าเดียวกันก็สามารถอนุมานได้ว่าเนื้อความเป็นเนื้อความเดียวกันดังรูปที่ 22



รูปที่ 22 Message Authentication Using a Message Authentication Code (Mac)

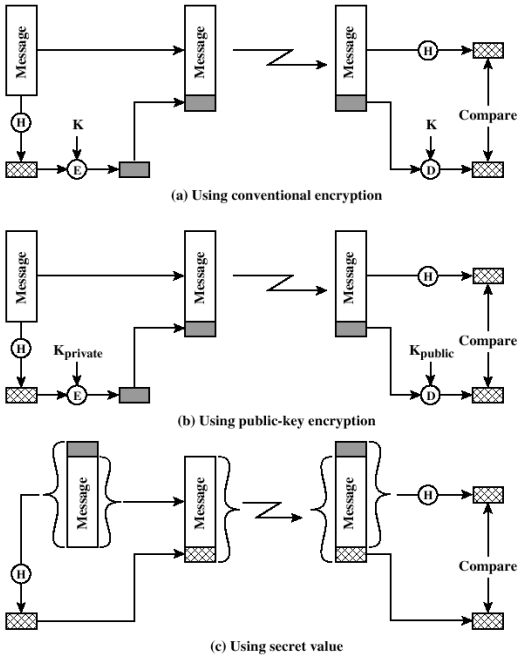
จากรูปหากมีการเปลี่ยนแปลงเนื้อความเกิดขึ้นก็จะทำให้ค่า MAC ที่คำนวณใหม่ที่ปลายทางไม่เท่ากับค่าMAC ต้นทางหรือหากมีการเปลี่ยนค่าMAC ด้วยก็จะไม่สามารถสร้างค่าMAC เดียวกันได้เพราะผู้อื่นจะไม่ทราบถึงรหัสลับที่ใช้งานอยู่ดังนั้นจะเห็นได้ว่ากระบวนการนี้สามารถรับรองเอกสารได้โดยไม่จำเป็นต้องเข้ารหัสข้อมูลเลยและหากใช้งานร่วมกับการกำหนดหมายเลขลำดับและการใช้Timestamp แล้ววิธีนี้ก็จะมีความปลอดภัยในการใช้งานพอสมควร

- การใช้ One-Way Hash Function

ในการสร้าง MAC โดยใช้ MAC Algorithm นั้นเนื่องจากลักษณะของการใช้งานจะเป็นการเข้ารหัสหรือการสร้าง MAC ในทิศทางเดียวโดยไม่มีความจำเป็นต้องถอดรหัสกลับมาได้และเนื่องจากค่า MAC ที่ต้องการควรจะมีขนาดความยาวคงที่และเกิดจากการประมวลผลเนื้อความทั้งหมดซึ่งการทำงานในลักษณะนี้จะเหมาะกับการทำงานที่เรียกว่า Hash โดยฟังก์ชัน Hash จะรับข้อความ M ที่มีความยาวใดๆ และสร้างรหัสที่มีความยาวคงที่ H(M) ออกมาโดยจะเรียกรหัสนี้ว่า Message Digest หรือ MD ออกมาโดย Hash จะต่างจาก MAC ตรงที่ Hash ไม่จำเป็นต้องใช้ Secret Key [31] โดยการทำงานของ Hash สามารถแสดงในรูปที่ 22

จากรูปที่ 23 ในรูป (a) จะแสดงการใช้งานฟังก์ชันHash ร่วมกับ Secret Key โดยหลังจากที่สร้าง MD ออกมาแล้วก็จะนำเอา MD นี้มาเข้ารหัสโดยใช้ Secret Key จากนั้นจึงแนบ MD ที่เข้ารหัสแล้วไปกับเอกสารแล้วจึงส่งเมื่อเอกสารไปถึงปลายทางก็จะมีการแยกเอกสารออกมาแล้วสร้าง MD โดยใช้อัลกอริทึมเดียวกันขึ้นมาใหม่แล้วเปรียบเทียบกับ MD ที่ส่งมาพร้อมเอกสารว่าเท่ากันหรือไม่ซึ่งวิธีนี้จะคล้ายกับวิธีการในรูปที่ 23 โดยสมมติว่า Secret Key จะทราบเฉพาะผู้ส่งและผู้รับเท่านั้น

อย่างไรก็ตามในโลกแห่งความเป็นจริงนั้นเป็นเรื่องยากที่จะใช้ Key จำนวน 1 คีย์สำหรับการสื่อสาร 1 คู่เพราะในการสื่อสารในวงกว้างก็จะต้องสร้างคีย์ขึ้นมามากมายอันทำให้ยากต่อการจดจำและการจัดเก็บนอกจากนั้นยังมีปัญหาในการส่ง Key ให้กันอีกด้วยดังนั้นในทางปฏิบัติแล้วในการรับรองเอกสารนี้มักจะนำคีย์ที่เรียกว่า Public Key มาใช้งานมากกว่าโดยระบบของPublic Key จะมีการสร้าง Key ขึ้นมา 2 Key โดยคีย์แรกจะเก็บไว้กับผู้สร้างเรียกว่า Private Key และคีย์ที่ 2 จะแจกจ่ายออกไปเรียกว่า Public Key โดยข้อความที่เข้ารหัสโดยคีย์ใดคีย์หนึ่งจะต้องถอดโดยคีย์คู่ของมันเช่นหากเข้ารหัสด้วย Private Key ก็ต้องถอดด้วยPublic Key ซึ่งรายละเอียดของการเข้ารหัสแบบ Public Key จะกล่าวถึงต่อไป



รูปที่ 23 แสดง Message AuthenticationUsinga One-Way

Hash Function

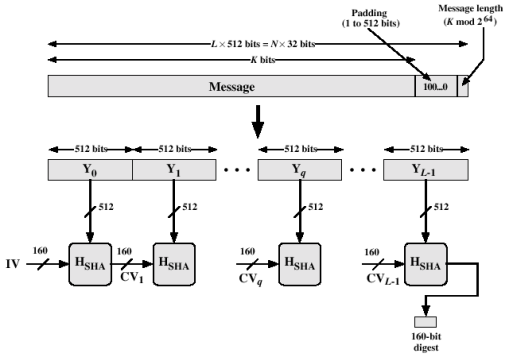
ในรูป (a) และ(b) นั้นจะมีการใช้การเข้ารหัสเพื่อเข้ารหัสข้อมูลในส่วนของ MD ทั้งนี้เพื่อไม่ให้ผู้ดักจับข้อมูลกลางทางสามารถจะปลอมโดยการสร้าง MD ขึ้นมาใหม่ได้อย่างไรก็ตามการเข้ารหัสจะทำให้เสียเวลาในการทำงานเพิ่มขึ้นหรือหากให้ทำงานด้วยฮาร์ดแวร์ก็จะเป็นการเพิ่มค่าใช้จ่าย นอกจากนั้นในอัลกอริทึมการเข้ารหัสบางตัวก็มีสิทธิบัตรอยู่ เช่น RSA ซึ่งต้องเสียค่าใช้จ่ายเพิ่มหรือบางอัลกอริทึมก็จะติดขัดในเรื่องของกฎหมายของการส่งออกรหัสลับเช่น DES ดังนั้นหากไม่ใช้อัลกอริทึมในการเข้ารหัสเลยก็สามารถทำได้ดังในรูป C โดยการเพิ่มสิ่งที่เรียกว่ารหัสลับเข้าไปในข้อมูลก่อนจะมีการคำนวณค่า MD ดังนั้นค่า Hash ที่ได้ก็จะเป็นค่า Hash ของข้อมูลกับรหัสลับจากนั้นในการส่งจะส่งเฉพาะข้อมูลกับ Hash โดยไม่ส่งรหัสลับไปด้วยโดยถือว่ารหัสลับจะต้องทราบทั้ง 2 ฝ่ายจากนั้น เมื่อข้อมูลส่งถึงปลายทางก็จะนำรหัสลับมาเพิ่มเข้าไปก่อนที่จะคำนวณค่า Hash ก็จะป้องกันการแก้ไขระหว่างทางได้โดยไม่จำเป็นต้องใช้อัลกอริทึมในการเข้ารหัสใดๆ เลย

ฟังก์ชัน Hash นั้นอันที่จริงแล้วสามารถสร้างได้ง่ายเช่นอาจนำเอาข้อความมาบวกกันทั้งหมดแล้วกลายเป็นค่า Hash ก็ได้แต่ฟังก์ชัน Hash ในลักษณะดังกล่าวมีข้อเสียคือจะเกิดการซ้ำกันของผลลัพธ์ได้ง่ายดังนั้นในโลกนี้จึงมีผู้ค้นคิดฟังก์ชัน Hash เอาไว้มากมายแต่ฟังก์ชั่น Hash ที่นิยมนำมาใช้ในการเข้ารหัสใน Wmax ในปัจจุบันมี 2 ฟังก์ชั่นคือ SHA-1และ HMAC [3]

SHA-1

ในบรรดาฟังก์ชัน Hash ทั้งหลายฟังก์ชัน SHA-1 จัดว่าเป็นฟังก์ชันหนึ่งที่เป็นมาตรฐานและมีการใช้งานกันอย่างกว้างขวางโดย SHA ได้รับการพัฒนาโดย NIST โดยได้รับการประกาศเป็นมาตรฐานที่FIPS PUB 180 ในปี1993 โดยหลังจากนั้นมีการปรับปรุงเป็นSHA-1 ในปี1995 โดยประกาศเป็นมาตรฐานที่ FIPS PUB 180-1 [16]

ฟังก์ชัน SHA-1 จะใช้บล็อกข้อมูลขนาด512 บิตโดยสร้างผลลัพธ์MD ความยาว160 บิตคงที่โดยการทำงานของฟังก์ชันนี้แสดงในรูปที่ 24



รูปที่ 24 Message Digest Generation Using SHA-1

1 เติมบิต (padding) โดยจะมีการเติมบิตข้อมูลเพิ่มเติมโดยจะเพิ่มเป็นจำนวนเท่ากับ 512-เศษที่ได้จากการหาร512 แล้วลบออก64 บิตเนื่องจากจะมีการเพิ่มความยาวอีก 64 บิตในขั้นตอนที่ 2 ดังนั้นแม้ว่าบล็อกข้อมูลที่หารด้วย 512 ลงตัวก็จะต้องมีการเติมบิตด้วยเช่นกัน

2 จะมีการเพิ่มข้อมูลความยาว 64 บิตโดยจะเป็นข้อมูลที่ระบุความยาวของข้อมูลก่อนที่จะมีการเติมบิตเข้าไปโดยการเพิ่มข้อมูลความยาวบิตเท่ากับ 64 บิตนี้จะทำให้ความยาวของข้อมูลที่รวมกับการเติมบิตและเพิ่มอีก 64 บิตจะมีความยาวที่หารด้วย 512 ลงตัวพอดีซึ่งหมายความว่าจะแบ่งเป็นบล็อกละ 512 บิตได้อย่างลงตัว

3 จะมีการกำหนดค่าเริ่มต้นของ MD Buffer โดยมีความยาวเท่ากับ160 บิตโดยบัฟเฟอร์นี้จะเก็บค่าเริ่มต้นของ MD จะแทนด้วยรีจิสเตอร์จำนวน5 ตัวตัวละ32 บิตโดยมีชื่อเป็นA,B,C,DและE โดยมีค่าเริ่มต้นคงที่ดังนี้ [32]

A= 67452301 (เป็นเลขฐาน16 มีความยาว32 บิต)

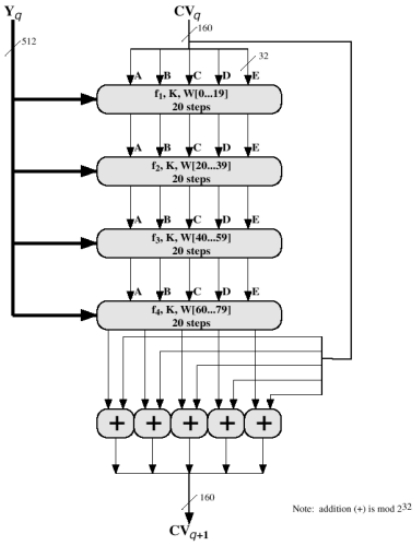
B=EFCDAB89

C=98BADCFE

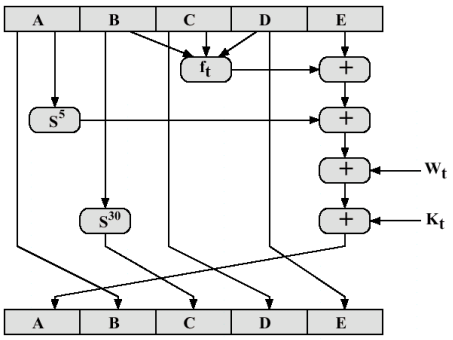
D=10325476

E= C3D2E1F0

4 ซึ่งถือเป็นหัวใจของการทำงานทั้งหมดโดยจะมีการประมวลผลข้อมูลเป็นบล็อกครั้งละ 512 บิตโดยกระทำเป็นรอบๆ จนกว่าข้อมูลจะหมดโดยแสดงขั้นตอนการทำงานไว้ในรูปที่ 24 โดยจะมีการทำงานทั้งหมด 4 รอบโดยในแต่ละรอบจะประกอบด้วย20 ขั้นตอนย่อยจากนั้นเมื่อผลลัพธ์ของทั้ง 4 รอบออกมาก็จะมีการนำไปบวกเข้ากับข้อมูล CV ที่เข้ามาอีกทีก็จะได้เป็น Message Digest ของบล็อกนั้นจากนั้น MD ก็จะใช้ในการประมวลผลข้อมูลในบล็อกถัดไปจนหมดก็จะได้ MD สุดท้ายที่ความยาว160 บิตออกมา



รูปที่ 25 SHA-1 Processing of a Single 512 bit Block



รูปที่ 26 Elementary SHA Operation (single step)

สำหรับการทำงานในแต่ละรอบ จะมีรายละเอียดของการทำงานตามรูปข้างต้นโดยเครื่องหมาย S จะหมายถึงการ Shift ตามจำนวนบิตที่กำกับไว้สำหรับ K คือค่าที่นำมาบวกโดยค่าที่กำหนดไว้สำหรับบวกแต่ละรอบ คือ 5A827999, 6ED9EBA1, 8F1BBCDC และ CA62C1D6 สำหรับค่า W เป็นข้อมูล 32 บิตที่ดึงมาจากส่วนของ 512 บิตจาก Input Block โดยคำนวณจากสูตร Wt = S1 (Wt-16 + Wt-14 + Wt-8 + Wt-3) โดย W ได้มาจาก Word ในแต่ละรอบของ t ซึ่งจะมีทั้งหมด 16 Word สำหรับ Ft นั้นเป็นฟังก์ชันที่จะใช้ในแต่ละรอบของการทำงาน

จากอัลกอริทึมจะเห็นได้ว่าผลลัพธ์ที่ได้ในแต่ละบิตจะเกิดจากอินพุตในแต่ละบิตโดยในแต่ละรอบการทำงานมีการทำงานที่ซับซ้อนซึ่งจะต่างกับการใช้ฟังก์ชันง่ายๆ อย่าง XOR โดย SHA-1 จะมีความเป็นไปได้ที่ข้อความ 2 ข้อความที่มี MD เดียวกันเท่ากับ 2 ยกกำลัง 80 และมีความยากในการหาข้อความที่มี MD ที่ได้เท่ากับ 2 ยกกำลัง 160 ซึ่งถือว่ามีความปลอดภัยในการใช้งานมากเพียงพอ

ข้อดี - ทำงานได้เร็ว

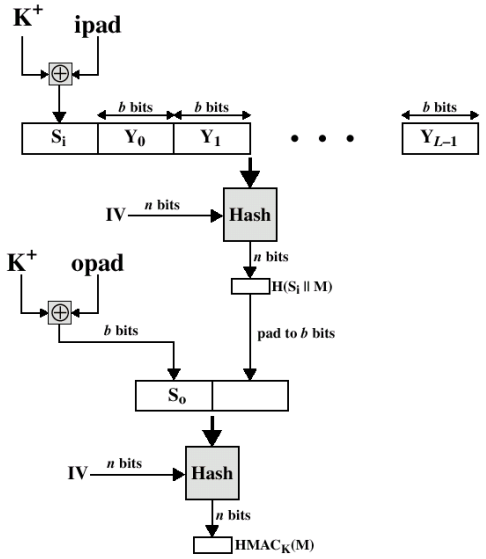
- ผลลัพธ์หรือข้อความย่อยที่ได้ไม่เกิดการชนกัน

HMAC

ชื่อ HMAC ย่อมาจากรหัสพิสูจน์ตัวจริงของข้อความโดยใช้ค่าแฮชเป็นหลัก (Has-basedMessage Authentication Code) [3] อัลกอริทึม HMAC ได้รับการพัฒนาขึ้นในปีคริสต์ศักราช1996 [BELL96a,b] โดยมีแนวคิดในการนำฟังก์ชันแฮชทางเดียวที่มีอยู่ในปัจจุบันเช่น MD5 หรือ SHA-1 มาใช้ประโยชน์ให้มากที่สุด [25]

ในปัจจุบันได้มีการนำเอาอัลกอริทึม HMAC มาใช้เป็นมาตรฐานในการรักษาความปลอดภัยของข้อมูลที่ส่งผ่านเครือข่ายอินเทอร์เน็ตโดยจะอยู่ในส่วนของโพรโทคอลอินเทอร์เน็ต (InternetProtocol, IP) และโพรโทคอล SSL (Secure Socket Layer) เป็นต้น [33]

แผนผังการทำงานของอัลกอริทึม HMAC ได้แสดงไว้ในรูปที่ 27



รูปที่ 27 แสดงแผนผังการทำงานของอัลกอริทึมHMAC

ข้อเสียของ HMAC

- ยังคงมีปัญหาเดิมคือ การแลกเปลี่ยนกุญแจ

-สมมุติให้ไม่มีปัญหาการแลกเปลี่ยนกุญแจก็ตาม การใช้ขั้นตอนวิธีนี้ก็ไม่สามารถใช้ได้กับกรณีที่มีจำนวนผู้รับมากกว่า1 คน

- ผู้รับไม่สามารถมั่นใจได้ว่าข้อความที่ส่งมาจากผู้ส่งจริงๆ ไม่ใช่มาจากผู้รับคนใดคนหนึ่งในกลุ่ม เพราะผู้รับคนอื่นๆ ก็ทราบกุญแจสมมาตรตัวเดียวกันนี้เช่นกัน

- กรณีที่สามารถแก้ปัญหาดังกล่าวข้างต้น ทั้ง 2ฝ่ายรับทราบกุญแจสมมาตรด้วยกัน ดังนั้น จะพิสูจน์ได้อย่างไรว่าค่า MAC ที่ได้เกิดจากผู้ส่ง หรือ ผู้รับกันแน่ที่ดำเนินการขึ้นมา และก็เป็นไปได้ที่ทั้ง 2 ฝ่ายรู้ข้อความต้นฉบับและค่า MA

V. สรุป

มาตรฐานIEEE 802.16หรือ Wimaxเป็นมาตรฐานใหม่สำหรับ MAC Layer เมื่อผู้ใช้ต้องการเข้าใช้งานเครือข่าย WLAN จะต้องมีการแสดงหลักฐานสำหรับประกอบการตรวจสอบ (credential) ต่ออุปกรณ์แม่ข่ายหลังจากนั้นอุปกรณ์แม่ข่ายจะส่งผ่านหลักฐานดังกล่าวต่อไปยัง RADIUS เซิร์ฟเวอร์ซึ่งเป็นระบบสำหรับตรวจสอบผู้ใช้โดยเฉพาะที่ใช้กันอยู่ทั่วไปโดยการแลกเปลี่ยนข้อมูลกันระหว่าง RADIUS เซิร์ฟเวอร์และอุปกรณ์WLAN โดยในเอกสารนี้จะแนะนำวิธีการ Authentication 4 ชนิดคือ Symmetric Key Encryptions , Asymmetric Key Encryptions , EAP (Extensible Authentication Protocol) และ กรรมวิธีการ Hash

Symmetric Key Encryptions คือการที่ทั้งสองฝ่ายจะให้กุญแจรหัสที่เหมือนกันคือใช้กุญแจรหัสเดียวกันทั้งในกระบวนการเข้ารหัส(Encryption) และการถอดรหัส(Decryption) โดยแต่ละฝ่ายจะทำการเข้ารหัสข้อมูลที่ต้องการส่งด้วยกุญแจรหัสนี้และในทางกลับกันเมื่อได้รับข้อมูลที่ส่งมาจากอีกฝ่ายก็จะใช้กุญแจรหัสเดียวกันนี้ในการถอดรหัสออกมาเป็นข้อความดั้งเดิมที่ถูกส่งมาจากอีกฝ่ายหนึ่งได้หรือกล่าวได้อีกนัยหนึ่งก็คือกุญแจรหัสที่ใช้ทั้งในการเข้ารหัสและถอดรหัสเป็นกุญแจรหัสตัวเดียวกันนั่นเอง Symmetric Keyที่นำมาใช้ใน Authentication ใน Wimaxนั้นมี 3 ชนิดคือ DES,3DES และ AES

Asymmetric Key Encryptions คือ Algorithm ที่ใช้Key ที่แตกต่างกันในการทำEncrypt และDecrypt ซึ่งKey ที่แตกต่างกันนี้จะเรียกว่าPrivate Key และPublic Key โดย Private Key จะต้องอยู่กับเจ้าของPrivate Key เท่านั้นแต่Public Key คนอื่นสามารถทราบได้Asymmetric Keyที่นำมาใช้ใน Authentication ใน Wimaxนั้นมี 1 ชนิดคือ RSA โดยนำมาใช้งานร่วมกับ X.509

EAP (Extensible Authentication Protocol)วิธีการของ EAP คือจะ กระทำผ่านสิ่งที่โอเปอเรเตอร์ออกให้ไม่ว่าจะเป็นSIM หรือ X.509 ซึ่งมีหลายแบบเช่นEAP-MD5, EAP-PEAP, EAP-TLS, EAP-TTLS, EAP-LEAP,EAP-FAST และ EAP-SPEAK เป็นต้น โดยจะทำการตรวจสอบกับเครือข่ายเองเช่นAAA Server

กรรมวิธีการ Hash คือการนำเอาตัวเลขหรือข้อความมาผ่านกรรมวิธีอย่างใดอย่างหนึ่งแล้วได้ผลลัพธ์ออกมาเป็นตัวเลขชุดหนึ่ง กรรมวิธีการ Hash นี้โดยส่วนใหญ่จะเป็นฟังก์ชันทางคณิตศาสตร์ โดยฟังก์ชันHash ที่ดีจะต้องมีคุณสมบัติการกระจายที่ดีกล่าวคือข้อความเดียวกันเมื่อผ่าน Hash ฟังก์ชันแล้วจะต้องได้ผลลัพธ์เหมือนเดิมเสมอและหากข้อความที่ต่างกันเพียงเล็กน้อยผ่านHash ฟังก์ขันควรจะต้องได้ผลลัพธ์ที่ต่างกันมากและที่สำคัญก็คือไม่ควรมีข้อความใดๆตั้งแต่2 ข้อความขึ้นไปที่ผ่าน Hash ฟังก์ชันแล้วจะได้ผลลัพธ์ที่เหมือนกันอัลกอลิทึ่ม Hash ที่นำมาใช้งานในการ Authentication ใน Wimaxนั้นมี 2 ชนิดคือ SHA-1 และ HMAC

โดยในแต่ละวิธีที่นำมาใช้ในการ Authentication ใน Wimax นั้น สามารถป้องกันภัยคุกคามได้ต่างกันชนิดกัน

ตารางที่ 10 สรุปผลลักษณะลักษณะภัยคุกคาม และ Algorithm(S) และ Technique ที่ใช้การป้องกันภัยคุกคามแต่ละวิธี [19]

Threat	Algorithm(S)
Jamming	AES
Man in the middle attack	AES, RSA
Eavesdropping Traffic	DES-CBC, AES-CCM, 3DES
BS or MS Masquerading	X.509 , EAP
Management massage modification	SHA-1, MAC, AES,HMAC
Data traffic modification	AES
DoS on BS or MS	EAP, SHA-1, AES, MAC, HMAC, RSA

VI. อ้างอิง

[1] K.Etemad, M-Y.Lai, Kamran Etemad, J.Lee and Y.Chang, "Overview of WiMAX Network Architecture and Evolution" the Institute of Electrical and Electronics Engineers, 2011.

[3] Lang Wei-min, Zhong Jin-li, Li Jian Jun et.al., "Research on the Authentication Scheme of WiMAX" in Proc 4th International Conference on Wireless Communications, Networking and Mobile Computing, 12-14 October 2008,Dalian, China PR. pp. 1–4.

[4] M.N.Khan and S.Ghauri, "The WiMAX 802.16e physical layer model," Proc. of International Conference on Wireless, Mobile and Multimedia Networks (IET), 2008. pp. 117 – 120.

[5] S.S.Hasan and M.A. Qadeer, "Security concerns in WiMAX," Proc. of Int. Conf. on First Asian Himalayas (AH-ICI), 2009, pp. 1-5.

[6] P.Daan, P.Viktor, L.Bart, T.Emmeric, J.Wout, M.Ingrid, D.Piet and M.Luc "A Throughput Analysis at the MAC Layer of Mobile WiMAX," Proc. of Wireless Communications and Networking Conference (WCNC), 2010, pp. 1 – 6.

[7] A.Bestetti, G.Giambene and S.Hadzic, "WiMAX: MAC layer performance assessments," Proc. of 3rd International Symposium on Wireless Pervasive Computing ISWPC, 2008, 490 – 494.

[8] Y.Zhu, J.He ,Q.Zhang and H.Huang, "Research on Packet Convergence Sublayer Classifier in WiMAX System," Proc. of 5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009, pp.1 – 4.

[9] S Kim, O Lee, S Choi and SJ Lee, "MAC-aware routing metric for 802.11 wireless mesh networks," Proc. of 20TH International Symposium on Personal, Indoor and Mobile Radio Communications, 2009 , pp 47-51.

[10] Y.Chuang, H.Tseng and S.Sheu, "A Performance Study of Discrete-error-checking Scheme (DECS) with the Optimal Division Locations for IEEE 802.16-based Multi-hop Networks," IEEE Transactions on Computers, 2012, Issue 99, pp.1.

[11] M.Barbeau, "WiMax/802.16 threat analysis," Proc. of 1ST Int.Conf. Quality of service & security in wireless and mobile networks, 2005, pp. 8-15.

[12] M.Nasreldin, H.Asian, M.El-Hennawy and A.El-Hennawy, "WiMax Security," Proc. of 22nd International Conferenceon Advanced Information Networking and Applications - Workshops, 2008, pp. 1335 – 1340.

[13] K. Ritesh Kumar, Mayank Raj, K. Balakrishnan and D.Das "WEBS: WiMAX emulation testbed to benchmark streaming multimedia QoS," Proc. of 3rd International Conference on Internet multimedia services architecture and applications (IMSAA), 2009, pp. 193-198.

[14] Zibideh, W.Y., "Modified-DES encryption algorithm with improved BER performance in wireless communication," Proc. Of Radio and Wireless Symposium (RWS), 2011 , pp. 219 – 222.

[15] L.Cuilan, "A Simple Encryption Scheme Based on WiMAX," Proc. of International Conference on E-Business and Information System Security (EBISS '09), 2009, pp. 1-4.

[16] D.Johnston, and J.Walker, "Overview of IEEE 802.16 security," Security & Privacy Mag, 2004, v.3, pp. 40-48.

[17] L Nazaryan, N Khan, EA Panaousis and C Politis. "Performance Evaluation of IPsec over WiMAX," Wireless World Research Forum meeting 23; 20-22 Oct 2009, Beijing, China.

[18] C.Jenkins, M.Schulte and J.Glossner "Instruction set extensions for Triple DES processing on a multi-threaded software-defined radio platform," Proc. of Conference on Signals, Systems and Computers (ASILOMAR), 2010 , pp. 1387–1391.

[19] M.Barbeau "WiMax/802.16 Threat Analysis," Proc. of 1st international workshop on ACM Quality of service & security in wireless and mobile networks, 2005, pp. 8-15.

[20] T.Nguyen "A survey of WiMAX security threats," http://www.cse.wustl.edu/~jain/cse571-09/ftp/wimax2. Washington University Engineering & Applied Science, 2009.

[21] J.Al-Zaabi, N.Chilamkurti, S.Zeadally, and K.Jongsung "A Proposed Authentication Protocol for Mobile Users of WiMAX Networks," Proc. of 3rd International Conference on Human-Centric Computing (HumanCom), 2010 , pp. 1-6.

[22] A.M.Taha, A.T.Abdel-Hamid and S.Tahar, "Formal Verification of IEEE 802.16 Security Sublayer Using Scyther Tool," Proc. of International Conference on Network and Service Security (N2S '09), 2009, pp. 1-5.

[23] K.Bongkyoung, C.P.Lee, Y.Chang, and J.A.Copeland, "A Security Scheme for Centralized Scheduling in IEEE 802.16 Mesh Networks," Proc. of Conference on Military Communications (MILCOM), 2007, pp. 1-5.

[24] A.Wu, J-h.Zhu, Y.Ma and Y-L.Li "Research on PHY layer supporting MESH model in IEEE 802.16," Proc. of 2nd International Conference on Computer Engineering and Technology (ICCET), 2010, pp. V7-395 -V7-398.

[25] S.Xu , M.Matthews and C.T.Huang, "Security issues in privacy and key management protocols of IEEE 802.16," Proc. of 44th Conference on the annual Southeast regional, 2006, pp. 113-118.

[26] S.Xu and C.T.Huang, "Attacks on PKM Protocols of IEEE 802.16 and Its Later Versions," Proc. of 3rd International Symposium on Wireless Communication Systems (ISWCS '06), 2006. pp. 185 – 189.

[27] L.Harn and J.Ren, "Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications," In IEEE Transactions on Wireless Communications, 2011, pp 2372 – 2379.

[28] D.Q. Liu, and M. Coslow, "Extensible authentication protocols for IEEE standards 802.11 and 802.16", in Proceedings of the international Conference on Mobile Technology, Applications, and Systems, Mobility 2008, pp. 1-9.

[29] L.Yi, K.Miao and A.Liu, "A comparative study of WiMAX and LTE as the next generation mobile enterprise network," Proc. of 13th International Conference on Advanced Communication Technology (ICACT), 2011, pp. 654-658.

[30] M.C.Vuran and I.F.Akyildiz, "Cross-Layer Error Control Optimization in WiMAX," Proc. of 3rd International Conference on ensor and Ad Hoc Communications and Networks (SECON '06), 2006, pp. 585-594.

[31] F.A.Ibikunle, "Notice of Violation of IEEE Publication Principles Security Issues in Mobile WiMAX (802.16e)," Proc. of Symposium on Mobile WiMAX (MWS '09), 2009, pp.117-122.

[32] A.Frank, "Security Issues in Mobile WiMAX (IEEE 802.16e)," Proc. of Symposium on IEEE Mobile WiMAX, 2009, pp. 117-122.

[33] B.Sikkens, "Security issues and proposed solutions concerning authentication and authorization for WiMAX (IEEE 802.16e)," Proc. of 8th Conference on IT Enschede University of Twente, 2008.