
بسم الله الرحمن الرحيم

دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

بررسی و تحلیل زیر لایه امنیت استاندارد IEEE 802.16

پایان نامه کارشناسی ارشد رشته مهندسی برق- مخابرات

نوید نصیری زاده

استاد راهنما

دکتر مهدی برنجکوب

۱۳۸۶

دانشگاه صنعتی اصفهان
دانشکده برق و کامپیوتر

پایان نامه کارشناسی ارشد رشته مخابرات آقای نوید نصیری زاده

تحت عنوان

بررسی و تحلیل زیر لایه امنیت استاندارد IEEE 802.16

در تاریخ ۸۶/۲/۱۱ توسط کمیته تخصصی زیر مورد بررسی و تصویب نهایی قرار گرفت.

۱ـ استاد راهنمای پایان نامه — دکتر مهدی برنجکوب

۲ـ استاد مشاور پایان نامه — دکتر پژمان خدیوی

سرپرست تحصیلات تکمیلی دانشکده — دکتر علی محمد دوست‌حسینی

این پایان‌نامـه بـا حمایـت **مرکـز تحقیقـات مخـابرات ایران** (قرارداد شماره ۵۰۰/۲۹۰۷/ت مورخ ۸۳/۳/۲۴) بـه اتمام رسیده است

تشکر و قدردانی

حمد و سپاس پروردگار هستی بخشی که از وجود خود در من دمید و مرا از نعمتهای خود بهره‌مند ساخت. چگونه من حقیر می‌توانم از زبان قاصرم شکر این همه نعمت را به درگاه او بجای آورم؟

از دست و زبان که برآید　　کزعهده شکرش به درآید

برخود لازم می‌دانم از استاد بزرگوارم جناب آقای دکتر **مهدی برنجکوب** که با رهنمودها و توصیه‌های ارزشمند خود مرا در به انجام رساندن این پایان نامه راهنمائی کردند، تشکر و قدردانی کنم. بدون نصایح راهنمائی‌ها و دلسوزیهای ایشان و صبر و حوصله و زمان فراوانی که این بزرگوار در به انجام رسانیدن این پژوهش صرف نمودند اتمام این پایان نامه امکان پذیر نبود. از زحمات جناب آقای دکتر پژمان خدیوی که با راهنمائیها و نظرات خود مرا در هرچه بهتر به انجام رسیدن این تحقیق کمک کردند سپاسگزاری می‌کنم.

از خانواده‌ام مخصوصاً **پدر** و **مادر** عزیزم که صبورانه و فداکارانه سالیان متمادی زحمات بسیار زیادی را کشیدند که شاید جبران لحظه‌ای از آن برایم ممکن نباشد و مشوق و راهنمایم در عرصه های مختلف زندگی بودند صمیمانه کمال امتنان و سپاس را دارم. از **همسر** عزیز، دلسوز و مهربانم و نیز خانواده همسرم که با درک موقعیتی که در آن بودم مشوق، همراه و حامی من بودند بسیار سپاسگزارم.

از کلیه اساتیدی که از محضرشان استفاده کرده‌ام و دوستانی که از نعمت همراهی و مصاحبت با آنان برخوردار بوده‌ام و کلیه عزیزانی که مجال آن نشد که آن‌ها نامی بیاورم کمال تشکر و امتنان را دارم و سلامتی و تائیدات روز افزون همگی را از درگاه ایزدمنان خواستارم.

چکیده

به‌دنبال توسعه شبکه‌های بی سیم محلی، نیاز به شبکه‌های بی سیم شهری روز به روز افزون‌تر گردید. تا آنجا که برای اولین بار استاندارد شبکه بی سیم شهری در سال ۲۰۰۱ تدوین گشت و با نام تجاری WiMAX و با استفاده از استاندارد IEEE 802.16-2001 وارد بازار گردید. شبکه بی سیم شهری دارای دو قسمت اصلی بی سیم و باسیم است. قسمت بی‌سیم این شبکه از استاندارد IEEE 802.16 تبعیت می‌کند. از آنجا که چالش اصلی در شبکه بی سیم شهری، قسمت بی‌سیم آن است، لذا پیشرفت و کارآمدترشدن شبکه مذکور کاملا وابسته به استاندارد IEEE 802.16 است. در استاندارد مذکور، از یک زیر لایه به نام زیر لایه امنیت استفاده شده است، که تمام مکانیزم‌های امنیتی مربوط به حوزه کانال رادیوئی در آن پیاده‌سازی می‌گردد. استاندارد IEEE 802.16 دارای نسخه‌های متفاوتی است که دو نسخه اخیرآن در سال های ۲۰۰۴ و ۲۰۰۶ به ترتیب با عنوان نسخه‌های ۲۰۰۴ و e انتشار یافتند. در این پایان‌نامه مکانیزم های امنیتی دو نسخه ۲۰۰۴ و e مورد بررسی می‌گیرد و ضمن معرفی سرویس‌های امنیتی مورد نیاز در این استاندارد و ارزیابی سرویس های امنیتی پیاده‌سازی شده، در حد امکان سناریوهای حمله متناظر ارائه می‌شود. در پایان با پیشنهاد مقدماتی یک معماری جامع امنیتی سعی می‌شود تا تمام حوزه های امنیتی مطرح در شبکه بی‌سیم شهری اعم از بخش‌های بی‌سیم و باسیم آن بیان و سرویس‌های امنیتی مورد نیاز در هر یک از حوزه‌ها معرفی شوند.

فصل اول
مقدمه

۱-۱ مقدمه

با توسعه شبکه‌های بی سیم محلی، نیاز به شبکه‌های بی سیم شهری[1] (WMAN) روز به روز افزون‌تر گردید. تا آنجا که برای اولین بار استاندارد شبکه بی سیم شهری در سال ۲۰۰۱ تدوین گشت و با نام تجاری WiMAX[2] و با استفاده از استاندارد IEEE 802.16-2001 وارد بازار گردید. استاندارد IEEE 802.16 دارای نسخه‌های متفاوتی است که دو نسخه اخیر آن در سال‌های ۲۰۰۴ و ۲۰۰۶ به ترتیب با نام نسخه ۲۰۰۴ و e انتشار یافتند.

شبکه بی سیم شهری دارای دو قسمت اصلی بی سیم و با سیم است. قسمت بی‌سیم این شبکه، اتصال ما بین تجهیزات کاربر تا اولین نقطه متصل به شبکه سیمی (BS[3]) را انجام می‌دهد. اتصال مذکور با استفاده از استاندارد IEEE 802.16 انجام می‌شود. قسمت دیگر شبکه، قسمت با سیم شبکه می‌باشد که وظیفه آن برقراری اتصال ما بین BSها به یکدیگر و یا به دیگر شبکه‌ها، نظیر شبکه اینترنت و شبکه PSTN[4] است. از آنجا که چالش اصلی در شبکه بی سیم شهری، قسمت بی‌سیم آن است، لذا پیشرفت و کارآمد ترشدن شبکه مذکور کاملا وابسته به استاندارد IEEE 802.16 است.

---

[1] Wireless Metropolitan Area Network
[2] Worldwide interoperability for Microwave Access
[3] Base Station
[4] Public Switched Telephone Network

۱-۲ تاریخچه

شبکه‌های بی سیم شهری با سرعت در حال گسترش می‌باشند و در آینده ای نه چندان دور از پرکاربردترین شبکه‌های مورد استفاده خواهند شد. اولین نسخه استاندارد IEEE 802.16، در سال ۲۰۰۱ انتشار یافت و هم اکنون بعد از گذشت کم تر از شش سال بیش از چهار نسخه متفاوت از آن عرضه شده است. جدول ۱-۱ روند تکامل این استاندارد به همراه بعضی از ویژگی‌های شاخص آن را نشان می‌دهد [۱-۳].

جدول ۱-۱. روند تکامل استاندارد IEEE 802.16 [۱]

سال	نام نسخه استاندارد	پهنای باند ارائه شده	ویژگی
۲۰۰۱	IEEE 802.16-2001	32-134 Mbps	LoS[1]
۲۰۰۳	IEEE 802.16-2003	100 Mbps	NLoS[2]
۲۰۰۴	IEEE 802.16-2004	32-134 Mbps 100 Mbps	LoS NLoS
۲۰۰۵	IEEE 802.16-e	*15 Mbps	NLoS حمایت از جابجائی کاربر

در نسخه‌های اولیه استاندارد، کاربرد شبکه WiMAX فقط برای اتصال یک شبکه محلی به شبکه‌های دیگری همچون شبکه اینترنت استفاده می‌شد. برای مثال اتصال به اینترنت شبکه محلی یک دانشگاه یا یک شرکت با استفاده از شبکه WMAN تامین می‌گردید. با گذشت زمان و پیشرفت سریع تکنولوژی، نسخه e استاندارد مذکور عرضه گردید. در این نسخه از جابجائی کاربر در سطح شبکه پشتیبانی می‌گردید، این امر موجب شد تا شبکه WiMAX برای اشخاص حقیقی نیز قابل ارائه باشد، بطوریکه کاربر قادر است با استفاده از رایانه قابل حمل خود در سطح شهر به شبکه WMAN متصل شده و از طریق آن به دیگر شبکه‌ها، نظیر شبکه اینترنت و اینترانت متصل گردد.

از آنجاکه شبکه WiMAX قادر به عرضه پهنای باند وسیعی است، لذا می‌تواند خدماتی همچون اینترنت پرسرعت، VoIP[3]، پخش تصاویر زنده، کنفرانس و ارتباطات تصویری و ... را به کاربرهای خود ارائه نماید و

---

[1] Line of Sight

[2] None Line of Sight

* در [۴]، یک نمونه واقعی نسخه e استاندارد IEEE 802.16 پیاده‌سازی شده است. در [۴] آمده که BS قادر می‌باشد به کل کاربرهایش در یک سلول تا 320 Mbps پهنای باند ارائه دهد و هر SS حداکثر می تواند تا 32 Mbps پهنای باند دریافت نماید.

[3] Voice over IP

از طرف دیگر به علت آن که زیر ساختار کل شبکه در دست شرکت ارائه دهنده سرویس می‌باشد، لذا این شبکه قادر به ارائه پهنای باند وسیع، همراه با کیفیت سرویس تضمین شده به مشترکین خود است [۴].

مشترکین شبکه بی سیم شهری با استفاده از کانال رادیوئی به شبکه مذکور متصل می‌شوند و از آنجا که همه افراد به کانال مذکور دسترسی دارند، لذا مقوله امنیت در قسمت بی سیم شبکه WMAN دارای اهمیت به سزائی است و استاندارد در یک فصل مستقل مکانیزم‌هائی را برای حفظ سرویس‌های امنیتی مختلف معرفی و بیان نموده است.

استاندارد IEEE 802.16 در دولایه فیزیکی و پیوند داده پیاده سازی شده است. لایه پیوند داده به نوبه خود دارای سه زیر لایه می‌باشد، که یکی از آن‌ها، زیر لایه امنیت است. در زیر لایه مذکور انواع مکانیزم‌های امنیتی پیاده سازی شده است.

۱-۳ هدف پایان‌نامه

تحقیقات محدودی بر روی امنیت نسخه‌های مختلف IEEE 802.16 منتشر شده است. از آنجا که نسخه e استاندارد در سال ۲۰۰۶ منتشر شده است و با توجه به گذشت زمان کمی از انتشار آن، هنوز پژوهشی در رابطه با ارزیابی امنیت این نسخه ارائه نشده است. اما در زمینه امنیت نسخه ۲۰۰۴ استاندارد، تحقیقاتی منتشر شده، که طی آن‌ها حملاتی به مکانیزم‌های امنیتی این نسخه انجام شده است [۵-۶]. در هیچ یک از تحقیقات مذکور، به امنیت به صورت جامع نگریسته نشده است. هدف این پایان‌نامه آن است که در حد امکان به امنیت شبکه‌های بی‌سیم شهری به صورت جامع پرداخته شود. لذا در ابتدا به دلیل اهمیت حوزه کانال رادیوئی، سعی شده، تمام سرویس‌های امنیتی در حوزه مذکور بیان و سپس در ادامه مکانیزم‌های امنیتی پیاده سازی شده در دو نسخه مورد بررسی و ارزیابی قرار گیرند و در صورتی که حمله جدید قابل اجرائی بر روی مکانیزم‌های مذکور یافته شود، آن حملات تشریح گردند و در ادامه، سرویس‌های امنیتی ارائه شده در دو نسخه مذکور، با یکدیگر مقایسه شوند.

در پایان با پیشنهاد مقدماتی یک معماری امنیتی جامع سعی می‌شود تا تمام حوزه‌های امنیتی موجود در شبکه بی‌سیم شهری بیان و با معرفی سرویس‌های امنیتی مورد نیاز در هر یک از حوزه‌ها، معماری امنیتی مذکور ارائه گردد.

۱-۴ ساختار پایان نامه

در فصل دوم این پایان‌نامه زیرلایه امنیتی نسخه ۲۰۰۴ استاندارد IEEE 802.16 [۷] و مکانیزم‌های امنیتی آن معرفی می‌شوند. در این فصل در ابتدا انواع لایه‌های این استاندارد بیان و سپس چگونگی برقراری اتصال در قسمت بی سیم شبکه معرفی خواهد شد. در نهایت انواع کلید و مکانیزم‌های رمزنگاری جریان داده‌ها در نسخه مذکور شرح داده خواهد شد.

در فصل سوم به معرفی زیر لایه امنیتی نسخه e استاندارد IEEE 802.16 [۸] و مکانیزم‌های امنیتی آن پرداخته می‌شود. از آنجاکه در نسخه مذکور از پروتکل EAP به عنوان یک پروتکل احراز اصالت استفاده شده، لذا در ابتدای این فصل، پروتکل EAP معرفی می‌گردد. همانطور که ملاحظه خواهد شد مکانیزم‌های امنیتی بکارگرفته شده در نسخه e استاندارد، سرویس‌های امنیتی به مراتب بیشتری را نسبت به اسلاف خود ارائه می‌دهند.

در فصل چهارم، ابتدا سرویس‌های امنیتی مورد نیاز در حوزه کانال رادیوئی شبکه‌های بی سیم شهری معرفی خواهند شد و سپس ارائه یا عدم ارائه سرویس‌های مذکور در دو نسخه ۲۰۰۴ و e مورد ارزیابی قرار گرفته و در صورت یافتن رخنه[1] امنیتی در آن‌ها، تلاش می‌شود سناریوی حمله متناظر ارائه گردد.

در فصل پنجم، انواع حوزه‌های امنیتی مطرح در شبکه بی سیم شهری معرفی و در ادامه سرویس‌های امنیتی مورد نیاز در این حوزه‌ها معرفی خواهند شد. در ادامه با پیشنهاد مقدماتی یک مدل امنیتی جامع برای این شبکه سعی می‌شود تا نیازمندیهای امنیتی در سطح کل شبکه پوشش داده شود.

در فصل ششم نیز ضمن جمع بندی مطالب، نتایج حاصل از این تحقیق آورده می‌شود و در پایان پیشنهاداتی برای ادامه کار ارائه خواهد شد.

---

[1] flaw

فصل دوم
معرفی استاندارد IEEE 802.16 و زیر لایه امنیتی نسخه ۲۰۰۴ آن

۲-۱ مقدمه

اولین نسخه استاندارد IEEE 802.16 در سال ۲۰۰۱ توسط سازمان IEEE طراحی شد و با نام تجاری WiMAX وارد بازار گردید. کاربرد این استاندارد در شبکه‌های بی سیم شهری (WMAN) می‌باشد. WiMAX شبیه به شبکه WIFI[1] برای برقراری اتصال و ایجاد شبکه بین کامپیوترها کاربرد دارد، با این تفاوت که شبکه‌های WIFI برای حداکثر چند ده متر استفاده می‌گردد، در صورتیکه شبکه‌های WiMAX تا شعاع چندین کیلومتر و باپهنای باندی وسیع جواب می‌دهد. استاندارد 802.16، دو لایه فیزیکی و پیوند داده قسمت بی سیم شبکه WMAN را پیاده سازی می‌نماید. لایه پیوند داده مربوط به این استاندارد، دارای سه زیر لایه می‌باشد، که یکی از آنها، زیر لایه امنیت است. وظیفه این زیر لایه، پیاده سازی امنیت در قسمت بی سیم شبکه WMAN می‌باشد.

در این فصل، ابتدا استاندارد 802.16 و لایه‌های آن معرفی خواهد شد و در ادامه مکانیزم‌ها و ساختار امنیتی زیر لایه امنیت نسخه ۲۰۰۴ این استاندارد، اعم از پروتکل توزیع کلید، روش‌های رمزنگاری و ساختار گواهینامه دیجیتالی استفاده شده در این نسخه از استاندارد معرفی می‌شوند.

---

[1] Wireless Fidelity

۲-۲ آشنائی با استاندارد IEEE 802.16

استاندارد IEEE 802.16 برای اولین بار در سال ۲۰۰۱ توسط موسسه IEEE طراحی شد. در این استاندارد از فرکانس حامل 10-66 GHz استفاده شده و اتصال[۱] مابین ایستگاه مشتری[۲] (SS) و ایستگاه ثابت[۳] (BS) به صورت دید مستقیم[۴] (LoS) می‌باشد. سرعت انتقال داده در این نسخه از استاندارد 32 Mbps تا 134 Mbps است. در سال ۲۰۰۳، نسخه a این استاندارد طراحی و تدوین گردید. در این نسخه، فرکانس حامل 2-11 GHz کاهش یافته بود و این امر موجب شده بود تا اتصال ما بین SSو BS به صورت دید غیر مستقیم[۵] (NLoS) امکان پذیر گردد. علاوه بر هم بندی[۶] ستاره، هم بندی Mesh Mode و نیز مدولاسیون OFDM[۷] برای اولین بار در این نسخه از استاندارد، به کار گرفته شد و سرعت انتقال داده به حداکثر 100 Mbps محدود شد. نسخه بعدی استاندارد، در سال ۲۰۰۴ و با نام ۲۰۰۴ طراحی شد. در این نسخه از استاندارد تمام ویژگی‌های استانداردهای قبلی حفظ شده، بطوریکه از سه فرکانس حامل متفاوت حمایت شده است. در این نسخه از استاندارد طرفین قادر می‌باشند، بر اساس نیازشان یکی از مدل‌های ارتباطی LoS و یا NLoS را ایجاد نمایند. جدیدترین نسخه استاندارد IEEE 802.16، به نام نسخه e در سال ۲۰۰۵ طراحی و تدوین گردید. این نسخه از استاندارد علاوه بر داشتن تمام قابلیت‌ها و ویژگی‌های نسخه‌های قبلی، از جابجائی کاربر نیز حمایت می‌نماید.

۲-۲-۱ آشنائی با لایه‌های استاندارد IEEE 802.16

برای طراحی یک شبکه کامپیوتری، مسائل و مشکلات بسیار گسترده و متنوعی وجود دارد که باید به نحوی حل شود تا بتوان یک ارتباط مطمئن و قابل اعتماد بین دو ماشین در شبکه برقرار کرد. این مسائل همگی از یک سنخ نیستند و پاسخ وراه حل مشابهی نیز نداشته و بخشی از آنها توسط سخت افزار و بخش دیگر با تکنیک‌های نرم افزاری قابل حل هستند. به عنوان مثال نیاز برای ارتباط بی سیم بین چند ایستگاه در شبکه، طراح شبکه را مجبور به استفاده از مدولاسیون آنالوگ در سخت افزار مخابراتی خواهد کرد ولی مسئله هماهنگی در ارسال بسته‌ها از مبدا به مقصد یا شماره گذاری بسته‌ها برای بازسازی پیام و اطمینان از رسیدن یک بسته، با استفاده از تکنیک‌های نرم افزاری قابل حل است. طراح یک شبکه باید تمام مسائل شبکه

---

[1] Connection
[2] Subscriber Station
[3] Base Station
[4] Line of Sight
[5] Non Line of Sight
[6] Topology
[7] Orthogonal Frequency Division Multiplexing

را تجزیه و تحلیل کرده و برای آنها راه حل ارائه کند ولی چون این مسائل دارای ماهیتی متفاوت از یکدیگرهستند، بنابراین طراحی یک شبکه باید به صورت لایه به لایه انجام شود.

برای آنکه طراحی شبکه‌ها سلیقه ای و نامتجانس نشود سازمان جهانی استاندارد[۱] (ISO) مدلی هفت لایه ای به نام OSI[۲] را برای شبکه ارائه کرد. در مدل مرجع OSI، هفت لایه تعریف شده است که هر کدام از لایه‌ها دارای قوانین و پروتکل‌های مخصوص به خود می‌باشد. در جدول ۲-۱، لایه‌های مدل مرجع OSI به همراه وظایف هریک به طور خلاصه آمده است [۹].

جدول ۲-۱. لایه‌های مدل مرجع OSI به همراه وظایف هر لایه

نام لایه	وظیفه
لایه کاربرد	انواع سرویس‌های کاربردی سطح بالا شامل: پروتکل‌های انتقال نامه‌های الکترونیکی، انتقال فایل، انتقال صدا و تصویر و صدها سرویس کاربردی دیگر
لایه ارائه	فشرده سازی و بازگشائی فایل، رمزنگاری و..
لایه جلسه	فراهم آوردن شرایط یک جلسه همانند ورود به سیستم از راه دور، احراز اصالت طرفین و ..
لایه انتقال	شکستن پیام‌های بزرگ به قطعات دارای هویت، ایجاد اتصال‌های انتها به انتها، حفظ ترتیب بسته‌ها و جریان بایت‌ها، هویت بخشیدن به فرآیندها و ..
لایه شبکه	مسیریابی و هدایت بسته‌ها بر اساس آدرس جهانی، پیشگیری از ازدحام و کنترل ترافیک
لایه پیوند داده	انتقال فریم‌های اطلاعات بین دو گره متصل به یک کانال فیزیکی بر اساس آدرس محلی، کشف و کنترل خطا، کنترل جریان داده‌ها
لایه فیزیکی	انتقال بیت‌ها برروی کانال فیزیکی و حل مسائل مرتبط با کانال

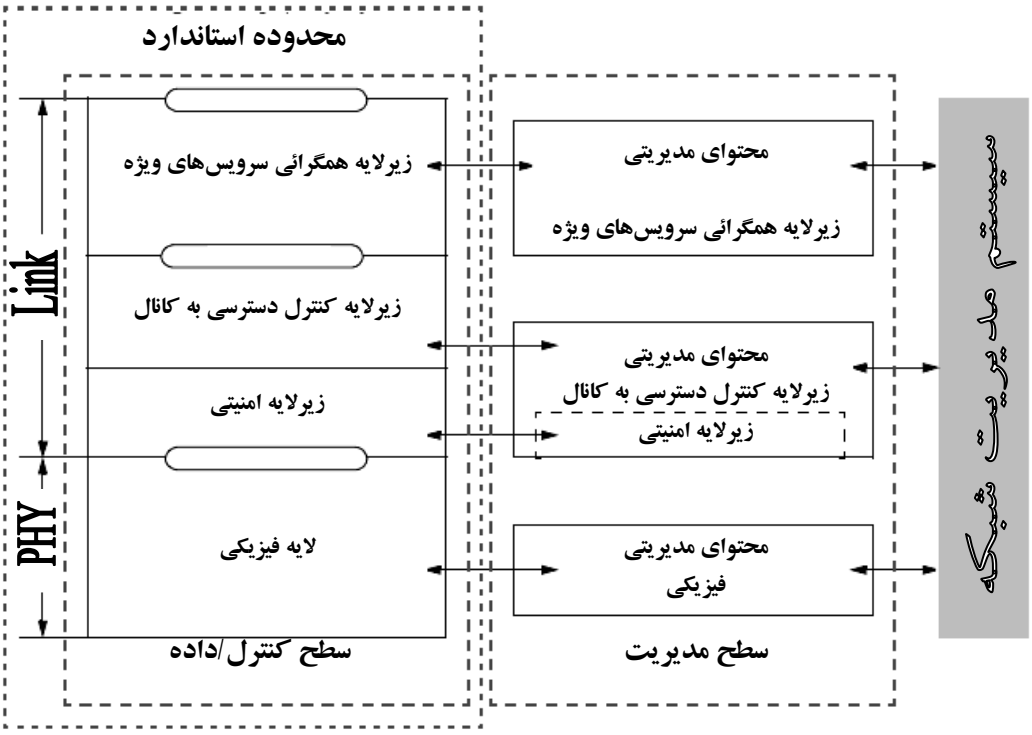
انجمن بین المللی مهندسین برق و الکترونیک[۳] (IEEE) به عنوان بزرگترین موسسه علمی و تحقیقاتی جهان در زمینه برق، الکترونیک و کامپیوتر در بسیاری از زمینه‌ها اقدام به تدوین استانداردهای جهانی نموده که در این بین سری استاندارد IEEE 802.x در ارتباط با شبکه‌های کامپیوتری تدوین شده است. این استانداردها در خصوص انتقال اطلاعات روی کانال مشترک و مدیریت کانال هستند، لذا در لایه اول و دوم از مدل OSI مطرح می‌شوند. از آنجائی که کل استانداردهای IEEE 802.x دو لایه فیزیکی و پیوند داده مدل مرجع OSI را پیاده سازی می‌نماید، لذا وابسته به نوع هم بندی شبکه، نوع استاندارد و پروتکل قالب بندی[۴] داده در آن‌ها متفاوت می‌باشند. برای مثال استاندارد IEEE 802.3 برای شبکه با هم بندی BUS و استاندارد

[1] International Standard Organization
[2] Open System Interconnection
[3] Institute of Electrical & Electronics Engineers
[4] Framing

IEEE 802.5 برای شبکه‌های محلی حلقه می‌باشد و هر کدام از این دو شبکه از نوع قالب بندی خاص خودشان پیروی می‌نمایند.

استاندارد IEEE 802.16 برای برقراری ارتباط در قسمت بی سیم شبکه WMAN طراحی شده (ارتباط ما بین SS و BS) و همانند سایر استانداردهای IEEE 802.x، لایه اول و لایه دوم مدل مرجع OSI را پیاده سازی می‌نماید. شکل۲-۱ زیر لایه‌های مربوط به لایه پیوند داده ولایه فیزیکی استاندارد IEEE 802.16 را نشان می‌دهد. ساختار کلی این لایه‌ها, شبیه به شبکه‌های دیگر سری 802 است. سه زیر لایه مربوط به لایه پیوند داده آن عبارتند از:

۱. **زیر لایه امنیتی**[1]: این زیر لایه با مسائل مرتبط با امنیت و نیز محرمانه نگاهداشتن اطلاعات سر و کار دارد که برای شبکه‌های عمومی‌در محیط‌های باز مانند شبکه‌هائی همچون شبکه بی سیم، به مراتب حیاتی تر از شبکه‌های خصوصی بسته مثل Ethernet است. این زیر لایه، عملیات رمز گذاری, رمزگشائی و مدیریت کلیدها را بر عهده دارد.



شکل۲-۱. لایه‌ها و زیرلایه‌های استاندارد IEEE 802.16 [۷]

[1] Security Sublayer

۲. زیر لایه کنترل دسترسی به کانال[1] **(MAC)**: این زیرلایه پروتکل‌های مدیریت کانال را در بر می‌گیرد. در این مدل مبنا آن است که ایستگاه ثابت (BS), سیستم را کنترل می‌کند. این ایستگاه می‌تواند "جریان اطلاعات از ایستگاه ثابت به مشتری‌ها"[2] را به صورت کاملا متفاوت و متمایز زمان بندی نماید و نیز نقش بسیار مهمی‌در مدیریت "جریان اطلاعات از مشتری‌ها به ایستگاه ثابت"[3] ایفا می‌کند.

۳. "زیر لایه همگرائی وابسته به سرویس"[4]: وظیفه این زیر لایه ایجاد واسطی متناسب با لایه شبکه است.

در ادامه این بخش، ابتدا، مراحل ایجاد یک اتصال در قسمت بی سیم شبکه WMAN بررسی شده و سپس زیرلایه امنیتی و مکانیزم‌های امنیتی پیاده سازی شده در این زیر لایه معرفی می‌شوند.

۲-۲-۲ مراحل برقراری اتصال در قسمت بی سیم شبکه

SS برای برقراری اتصال با BS مراحل مختلفی را طی می‌نماید، که در ادامه شرح هر یک از این مراحل به صورت خلاصه آورده شده است.

الف- جستجو برای یافتن کانال DL[5]**:** BS برای اعلام موجودیت خود در یک سلول و همزمان سازی خودش با SS پیغام DL-MAP را مکررا در سطح سلول منتشر می‌نماید. SS با دیدن این پیغام متوجه می‌شود که در سلول متناظر با BS قرار دارد و با دریافت پیغام DCD[6]، ابتدا خودش را با آن همزمان و سپس کانال‌های DL موجود و مجموعه ای از پارامترهای مربوط به این کانال‌ها را بدست می‌آورد. SS تا زمانی که پیغام‌های DL-MAP و DCD مربوط به کانال DL را به طور کامل دریافت ننماید از این مرحله خارج نمی‌گردد.

ب- گرفتن پارامترهای مربوط به کانال UL[7]**:** بعد از پایان عملیات همزمان سازی و گرفتن پارامترهای مربوط به کانال DL، SS منتظر دریافت پیغام UCD[8] می‌ماند تا با دریافت این پیغام بتواند مجموعه ای از پارامترهای مربوط به کانال UL را بدست آورد. پیغام‌های UCD مکررا توسط BS ارسال می‌گردد تا بواسطه آن، کانال‌های UL موجود اعلام گردد.

ج- انجام دادن عملیات دامنه یابی[9]**:** عملیات دامنه یابی، تنظیمات توان و Offsetهای زمانی ما بین SS و BS را را انجام می‌دهد. برای انجام دادن عملیات تنظیم توان، SS پیغامی‌با نام RNG-REQ[10] را با کمترین توان

---

[1] Medium Access Control Layer
[2] Downstream
[3] Upstream
[4] Service Specific Convergence Sublayer
[5] Downlink
[6] Downlink Channel Descriptor
[7] Uplink
[8] Uplink Channel Descriptor
[9] ranging
[10] Ranging Request

ممکن ارسال می‌نماید. اگر پاسخی از سوی BS دریافت ننمود سطح توان پیغام ارسالی را به صورت پلکانی افزایش می‌دهد تا آنجائی که پیغام RNG-RSP[1] از سوی BS دریافت شود. بدین ترتیب BS متوجه می‌شود که توان ارسالی پیغام RNG-REQ کافی بوده است.

د- مذاکره نمودن در رابطه با قابلیت‌های اصلی: بعد از به اتمام رسیدن عملیات دامنه یابی، SS از طریق پیغام SBC-REQ[2] قابلیت‌ها و توانائی‌های خودش را برای BS ارسال می‌نماید و BS با دریافت این پیغام، قابلیت‌های مشترک میان خودش و SS را شناسائی نموده و با استفاده از پیغام SBC-RES[3]، به ایستگاه مشتری مشتری مربوطه اطلاع می‌دهد.

ه- مبادله کلید و احراز اصالت ss: بعد از به اتمام رسیدن مذاکره در رابطه با کانال، نوبت به انجام عملیات احراز اصالت SS می‌رسد. در این مرحله ابتدا BS، هویت SS را وارسی نموده و سپس در صورت تائید آن، کلیدهای خصوصی مربوط به عملیات رمزنگاری کلید TEK[4] و رمزنگاری داده را توزیع می‌نماید.

و- انجام عملیات ثبت نام: پس از انجام مبادله کلید و احراز اصالت، عملیات ثبت نام انجام می گردد و در ادامه این عملیات، یک IP محلی یکتا با استفاده از مکانیزم DHCP[5] به هر SS ثبت نام شده، اختصاص داده می‌شود می‌شود و بدین ترتیب SS و BS قادر می‌شوند تا داده‌هایشان را در قسمت بی سیم شبکه WMAN رد و بدل نمایند.

۲-۳ معماری زیر لایه امنیتی استاندارد IEEE 802.16

همانطور که بیان شد، استاندارد 802.16، دو لایه فیزیکی و پیونددداده را در قسمت بی سیم شبکه WMAN پیاده سازی می‌نماید. لایه پیوند داده در این استاندارد دارای یک زیر لایه به نام زیر لایه امنیت می‌باشد که وظیفه آن پیاده سازی ویژگی‌های امنیتی در قسمت بی سیم شبکه می‌باشد. امنیت در این زیر لایه با استفاده از دو پروتکل پیاده سازی شده است:

الف- یک پروتکل ساده که قالب‌های[6] داده در لایه MAC را رمز نگاری می‌نماید و سپس از قسمت بی سیم شبکه عبور می‌دهد. این پروتکل در دو قسمت تعریف گردیده شده است:

- مجموعه الگوریتم‌های رمز نگاری[7]: شامل الگوریتم رمزنگاری داده والگوریتم رمزنگاری کلید TEK

---

[1] Ranging Response
[2] SS Basic Capability Request
[3] SBC Responsilble
[4] Traffic Encrypion Key
[5] Dynamic Host Configuration Protocol
[6] Frame
[7] Cryptographic Suite

- قوانینی که برای پیاده سازی الگوریتم‌های رمزنگاری بر روی قالب‌های داده در لایه MAC بکار می‌رود.

ب- پروتکل "مدیریت کلید محرمانگی"[1] (PKM) که توزیع و همزمان سازی کلیدهای توافق شده را از ایستگاه ثابت به ایستگاه مشتری به صورت امن انجام می‌دهد.

۲-۳-۱ مروری بر پروتکل رمزنگاری قالب‌های داده در زیرلایه امنیت

خدمات رمزنگاری به عنوان مجموعه ای از توانایی‌ها در لایه امنیتی MAC تعریف گردیده و در "سرآیند MAC"[2] (GMH)، اطلاعات مربوط به نوع الگوریتم رمز نگاری بکار رفته در هر قالب، ذکر می‌گردد. فقط بخش داده هر قالب رمز می‌شود و سرآیند قالب رمز نخواهد شد (شکل ۲-۲). لازم به توضیح است که همه پیغام‌های مدیریتی، به صورت شفاف و بدون عملیات رمزگذاری ارسال می‌گردد.

هنگامی‌که یک قالب داده، بر روی یک اتصال انتقال می‌یابد تا در لایه MAC، از تجهیزات کاربر به ایستگاه ثابت و یا بالعکس ارسال گردد، ابتدا یک "شناسه تداعی گر امنیتی"[3] (SAID) به این اتصال اختصاص داده می‌شود و سپس فرستنده عملیات رمزنگاری و دیگر عملیات‌ها را بر روی این قالب داده، بر اساس محتوای تداعی گر امنیتی (SA) اختصاص داده شده انجام می‌دهد. در گیرنده نیز، در هنگام دریافت قالب داده، دقیقا روند مشابهی طی می‌شود، بدین ترتیب که با دریافت قالب داده، ابتدا گیرنده، SA مربوط به آن اتصال را شناسایی نموده و سپس عملیات رمز گشائی و دیگر عملیات‌های امنیتی را بر روی آن، بر اساس همان SA شناسایی شده انجام می‌دهد.

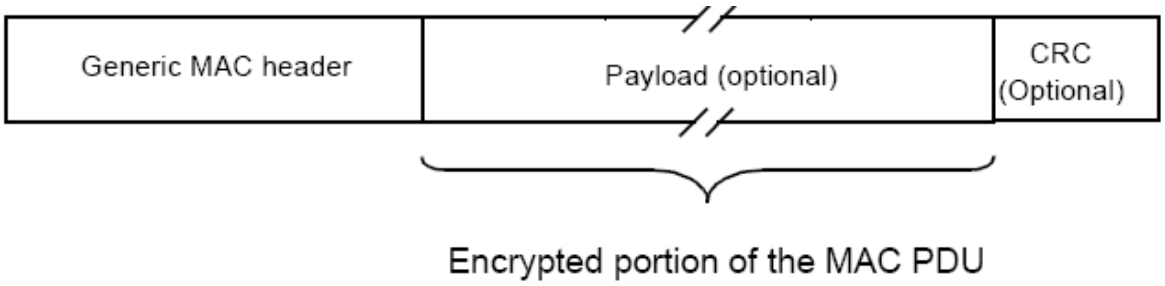
SA, مجموعه ای از اطلاعات امنیتی مشتمل بر الگوریتم‌های قابل قبول، پارامترهای مربوطه، طول کلیدها و ... می‌باشد که BS با یک یا چند SS به صورت مشترک قرارداد نموده تا بواسطه آن بتواند یک اتصال امن در شبکه IEEE 802.16 ایجاد نماید.

سرآیند MAC که به صورت آشکارا مبادله می‌شود، شامل همه اطلاعات رمزنگاری می‌باشد. این اطلاعات شامل "شناسه اتصال"[4] (CI)، "شماره سریال کلید رمزنگاری"[5] (EKS) و فیلد "کنترل رمزنگاری"[6] (EC) هستند که برای رمزگشایی داده در گیرنده لازم خواهند بود. ایستگاه ثابت در اتصال با هر ایستگاه

---

[1] Privacy Key Management
[2] Gneric MAC Header
[3] Security Association Identifier
[4] Connection Identifier
[5] Encryption Key Sequence(EKS)
[6] Encryption Control

مشتری دارای یک SA با شناسه منحصر به فرد می‌باشد، که تمام اطلاعات مربوط به سرآیند MAC در آن SA نیز وجود دارد.



شکل ۲-۲. رمزگذاری قالب داده در لایه MAC [۷]

۲ بیت از سرآیند MAC، متعلق به شماره کلید رمزنگاری (EKS) می‌باشد. با استفاده از این فیلد کلید TEK، مربوط به رمزنگاری جریان قالب داده مشخص می‌شود.

رمزنگاری داده با استفاده از بیت EC مشخص می‌گردد به نحویکه اگر مقدار این فیلد برابر یک باشد بدین معنی است که داده رمزگذاری گردیده و مقداردرون فیلد EKS نشان دهنده شماره سریال کلید مرتبط با داده رمزشده می‌باشد و اگر مقدار این فیلد برابر صفر باشد، بدین معنی است که داده موجود در قالب، رمز نشده است. این نکته نیز قابل توجه است که اگر داده ای بدست طرفین اتصال برسد که رمز نشده ولی بر اساس SA باید عملیات رمزگذاری برروی آن انجام شده باشد، حذف می‌گردد.

۲-۳-۲ مروری بر پروتکل مدیریت کلید محرمانگی

با استفاده از پروتکل مدیریت کلید محرمانگی تمام اطلاعات کلیدی به صورت امن بین ایستگاه ثابت و ایستگاه‌های مشتری توزیع و همزمان می‌گردد. در این بخش ساختار این پروتکل به صورت خلاصه آورده شده و در بخش (۲-۴) ساختار این پروتکل به صورت کامل بیان می‌شود.

هرSS[۱]، از پروتکل مدیریت کلید محرمانگی استفاده می‌نماید تا بتواند کلید جواز و " کلید رمز جریان داده‌ها" [۲] (TEK) را از ایستگاه ثابت بدست آورد. این پروتکل برای انجام این مهم، از گواهینامه دیجیتالی

[۱] هر ایستگاه مشتری از کاربر و تجهیزات کاربر تشکیل شده است.

[2] Traffic Encryption Key

X.509 [١٠]، الگوریتم رمزنگاری کلید عمومی RSA[1] [١١] و الگوریتم‌های رمزنگاری متقارن استفاده می‌کند.

پروتکل PKM، از مدل "کارفرما/سرویس دهنده"[2] پیروی می‌نماید. SS به عنوان کارفرما تقاضای کلید می‌نماید و BS به عنوان سرویس دهنده پاسخ به درخواست وی می‌دهد و تضمین می‌نماید که SS فقط کلیدی را دریافت نماید که مجوزش را دارد. این پروتکل برای انجام عملیاتهای مربوطه از پیغام‌های مدیریتی MAC مانند پیغام‌های PKM-REQ, PKM-RSP استفاده می‌نماید.

پروتکل PKM با استفاده از رمز گذاری کلید عمومی‌یک کلید مشترک را بین BS و SS برقرار و از آن برای امن کردن مبادله کلید TEK استفاده می‌نماید. استاندارد IEEE 802.16 این کلید را کلید جواز[3] (AK) می‌نامد. پروتکل PKM برای مبادله کلید TEK بیشتر از الگوریتم رمزنگاری متقارن استفاده می‌نماید. یکی از دلایل استفاده از کلید AK و الگوریتم رمزنگاری متقارن برای مبادله کلیدهای TEK، کاهش یافتن سر بار محاسباتی ناشی از رمزنگاری کلید عمومی‌می‌باشد.

BS، SS را در طول مبادلات "راه اندازی جوازدهی"[4]، احراز اصالت[5] می‌کند. هر SS دارای یک گواهینامه دیجیتال X.509 می‌باشد که بوسیله سازنده SS و یا یک CA معتبر، صادر شده است. این گواهینامه دیجیتال شامل آدرس MAC و کلید عمومی SS می‌باشد که ابتدا به BS ارائه و سپس از آن کلید جواز درخواست می‌گردد. BS با دریافت گواهینامه دیجیتالی SS، آن را وارسی نموده و در صورت تایید آن، کلید جواز را با استفاده از کلید عمومی‌موجود درگواهینامه دیجیتال SS رمزگذاری و به سمت SS ارسال می‌نماید.

۲-۳-۳ مجموعه رمزنگاری

مجموعه رمزنگاری شامل روش‌هائی برای رمزنگاری داده‌ها، انجام شدن عملیات احراز اصالت و رمزنگاری کلید TEK می‌باشد. این مجموعه شامل ۳ بایت است. بایت با ارزش آن، الگوریتم رمزنگاری داده را معرفی می‌نماید (جدول ۲-۲)، بایت وسطی مشخص می‌کند که آیا داده‌های رد و بدل شده احراز اصالت می‌گردند و یا خیر و در انتها، بایت کم ارزش الگوریتم رمزنگاری TEK را مشخص می‌کند (جدول ۲-۳). لذا برای هر SA بواسطه این ۳ بایت خصوصیات مجموعه رمزنگاری SS با BS بدست می‌آید (جدول ۲-۴). برای مثال اگر مجموعه رمز نگاری با مقدار 0x010001 انتخاب گردد، بیانگر مطالب زیر می‌باشد:

---

[3] حروف ابتدائی نام‌های این سه نفر: Rivest، Shamir و Adelman

[2] Client/Server
[3] Authorization Key
[4] initial authorization
[5] Authenticate

الف- رمز نگاری داده‌ها با استفاده از روش رمزنگاری DES به شیوه CBC[1]، انجام می گردد.

ب- احراز اصالت داده انجام نمی‌شود.

ج- TEK با استفاده از روش 3-DES,128 رمزنگاری می گردد.

[1] Cipher Block Chaining