فصلنامه رویکردهای پژوهشی نوین در
مدیریت و حسابداری
سال ششم، شماره ۸۶، پاییز ۱۴۰۱، ص ۹۷۸-۹۵۹

Journal of New Research Approaches
in Management and Accounting
ISSN: 2588-4573
http://www.majournal.ir

انواع روش های تامین امنیت در شبکه های بی سیم

احد تفضلی [۱]

تاریخ دریافت: ۱۴۰۱/۰۷/۰۴ تاریخ چاپ: ۱۴۰۱/۰۹/۲۵

چکیده

رشد افزاینده استفاده از شبکه های بی سیم در جهان، لزوم استفاده از روش های افزایش امنیت در آن ها را چند برابر می کند. در این مقاله یک مرور کلی از حملات امنیتی که در شبکه‌های بی‌سیم با آن مواجه می‌شوند، با توجه به معماری پروتکل شبکه ارائه می‌شود که در آن تهدیدات امنیتی بالقوه در هر لایه پروتکل مورد بحث قرار می‌گیرد. ما همچنین بررسی پروتکل‌ها و الگوریتم‌های امنیتی موجود را که در استانداردهای شبکه بی‌سیم موجود، مانند بلوتوث، وای‌فای، وایمکس و سیستم‌های تکامل بلندمدت (LTE) اتخاذ شده‌اند، ارائه می کنیم.

واژگان کلیدی

شبکه های بی سیم، امنیت، فضای مجازی، حملات سایبری.

۱. کارشناسی ارشد مهندسی فناوری اطلاعات-مدیریت سیستم های اطلاعاتی، دانشگاه غیاث الدین جمشید کاشانی، قزوین، ایران.

مقدمه

توسعه سریع شبکه های بی سیم، امکانات و آسایش زیادی را برای زندگی انسان ها فراهم کرده است ولی مشکلاتی را نیز به همراه داشته است که در این میان، امنیت ارتباطات از جمله مهم ترین مشکلات آن ها است. مسائل امنیتی شبکه های بی سیم نه تنها به حریم خصوصی افراد بلکه به امینت سازمان ها، ادارات دولتی و امنیت دفاع ملی مرتبط است. کلید حل مشکلات امنیتی و ارتباطات شبکه های بی سیم در استفاده از الگوریتم های رمز گذاری و رمز گشایی نهفته است. دو روش رمز گذاری سنتی متقارن و نامتقارن وجود دارد، روش متقارن اولین بار توسط سازمان استاندارد ایالات متحده آمریکا ارائه گردید. در این روش فرستنده و گیرنده از یک کلید برای رمز گذاری و رمز گشایی استفاده می کنند. در روش نامتقارن از ۲ کلید جداگانه برای رمزگذاری و رمز گشایی استفاده

می گردد. کلید رمز گذاری، کلید عمومی و کلید رمز گشایی، خصوصی نامیده می شود. مشکل این روش پردازش زیاد برای CPU در زمان رمز نگاری و رمز گشایی است. شبکه‌های بی‌سیم معمولاً معماری پروتکل OSIرا اتخاذ می‌کنند که شامل لایه برنامه، لایه انتقال، لایه شبکه [۶]، لایه MACو لایه فیزیکی است [۱, ۲]. لایه ها معمولاً به طور جداگانه در هر لایه محافظت می شوند تا الزامات امنیتی از جمله اعتبار، محرمانه بودن، یکپارچگی و در دسترس بودن را برآورده کنند[۳]. گرچه رمزنگاری محرمانه بودن ارتباطات قابل دستیابی را بهبود می بخشد، اما به توان محاسباتی اضافی نیاز دارد و تأخیر را تحمیل می کند، زیرا زمان معینی برای رمزگذاری و رمزگشایی داده ها مورد نیاز است [۴]. شبکه های بی سیم معمولا از ۷ لایه طبق استاندارد OSI[۱] تشکیل شده اند که شامل: ۱- لایه فیزیکی[۲]، ۲- لایه پیوند داده[۳]، ۳- لایه شبکه[۴]، ۴-لایه انتقال[۵]، لایه نشست[۶]، لایه نمایش (ارائه)[۷] و لایه کاربردی[۸] می شوند. وظیفه لایه فیزیکی، انتقال بیت ها بر روی کانال مخابراتی است و امروزه این لایه مهم ترین لایه برای ارتقاء امنیت شبکه های بی سیم شناخته شده است. این لایه تعامل با سخت افزار واقعی و سیگنال رسانی را دارد و تجهیزات سخت افزاری، کابل ها، فرکانس ها و پالس های مورد استفاده برای نشان دادن سیگنال های باینری را مشخص می کند و همچنین خدمات و سرویس هایی را به لایه پیوند داده می دهد. لایه پیوند داده قالب های اطلاعاتی را با لایه فیزیکی مبادله کرده و لایه فیزیکی، آن ها را به پالس های الکتریکی تبدیل می کند و توسط ابزارات بی سیم و یا با سیم ارسال می کند. وظیفه لایه پیوند داده این است که با استفاده از مکانیزم های کنترل خطا داده ها را روی یک کانال انتقال بدون خطا و ایمن به مقصد ارسال کند. همچنین، لایه پیوند داده، بسته های اطلاعاتی را از لایه شبکه گرفته و آن ها را تبدیل به فریم های اطلاعاتی می کند. در واقع

---

۱ Open System Interconnection
۲ Physical Layer
۳ Data Link Layer
۴ Network Layer
۵ Transport Layer
۶ Session Layer
۷ Presentation Layer
۸ Application Layer

وظیفه اصلی این لایه، ارائه سرویس به لایه شبکه است و داده ها را از لایه شبکه میدا به لایه شبکه مقصد منتقل می کند. فریم[۹]، واحد اطلاعات در لایه پیوند داده است. کشف خطا در این لایه می تواند از طریق بیت های کنترل خطا مثل بیت های توازن[۱۰] انجام شود. وظیفه لایه شبکه، مسیریابی است. ه عبارتی هرگاه یک قطعه داده دارای هویت و شناسنامه (در این لایه "بسته" گفته می شود) تحویل این لایه در یک ماشین شود، در صورتی که مقصد نهایی همین ماشین باشد محتوای بسته به لایه بالاتر (لایه انتقال)تحویل داده می شود در غیر اینصورت برای رسیدن به مقصد نهایی خود از طریق کانالی دیگر به بیرون ارسال می شود. هر مسیریاب می تواند هم به صورت ایستا هم به صورت پویا و هوشمند بسته ها را مسیریابی کند. در این لایه تمام ماشین های شبکه نیاز به یک آدرس جهانی یکتا[۱۱] هستند. هر مسیریاب بر اساس این آدرس ها اقدام به هدایت بسته ها به مقصد خواهند کرد. لایه انتقال که چهارمین لایه در مدل OSI است، وظیفه نگهداری و کنترل ریزش اطلاعات را بر عهده دارد. این لایه، اطلاعات مربوط به هر نرم‌افزار در سیستم عامل را دریافت و آن‌ها را در قالب یک رشته تکی درمی‌آورد. لایه نشست، وظیفه ایجاد، مدیریت و نگهداری و در نهایت خاتمه یک نشست[۱۲] را با کامپیوتر مقصد بر عهده دارد. در هنگام برقراری یک ارتباط بین دو کامپیوتر اصطلاحا یک جلسه یا نشست برقرار می شود. عملیاتی که در لایه نمایش انجام می گیرد عموما بر روی محتوا و مفهوم پیام ها متمرکز است. از این عملیات می توان به تبدیل قالب[۱۳] پیام ها, فشرده سازی[۱۴], رمزنگاری[۱۵] و رمزگشایی پیام ها, تبدیل کدها به یکدیگر اشاره کرد. لایه کاربرد را می توان مجموعه ای از استانداردها و پروتکل هایی دانست که برای تبادل پیام بین نرم افزار های کاربردی تعریف شده اند[۵, ۶].

شبکه های بی سیم، دستگاه های بدون سیم را قادر می سازند تا بدون اتصال فیزیکی با یکدیگر ارتباط برقرار کنند، اما عدم وجود اتصال با سیم، خطرات امنیتی را در این دستگاه ها زیاد می کند. در مورد یک شبکه بی سیم اگر امنیت به صورت کافی تامین نشده باشد، دسترسی به آن بسیار راحت است و کاربران موجود در آن را برای حملات سایبری آسیب پذیر تر می کند. بدین منظور برای تضمین اصالت گیرنده، شبکه های بی سیم موجود معمولاً از چندین روش احراز هویت به طور همزمان در لایه های پروتکل مختلف، از جمله تأیید هویت لایه MAC و تأیید هویت لایه شبکه استفاده می کنند. لایه MAC یا لایه نظارت بر دسترسی به رسانه انتقال[۱۶] در شبکه های فراگیر که از یک کانال مشترک با دسترسی های چند گانه استفاده می کنند مسئول نظارت بر دسترسی به کانال است. به طور خاص، در لایه MAC،

---

[۹] Frame
[۱۰] Parity
[۱۱] Global Address
[۱۲] Session
[۱۳] Format
[۱۴] Data Compression
[۱۵] Encryption
[۱۶] Media access control

آدرس MAC یک کاربر باید احراز هویت شود تا از دسترسی غیرمجاز جلوگیری شود. WEP[۱۷] قدیمی ترین و رایج ترین پروتکل امنیتی وای فای[۱۸] است که امروزه از آن استفاده نمی شود و دارای سطح امنیتی بسیار پائینی است.

انتخاب یک پروتکل رمزگذاری به عوامل زیادی از جمله اهمیت داده‌های شبکه، میزان دسترسی کاربران، قابلیت‌های مودم دو بانده یا تک بانده و پهنای باند بستگی دارد. دو مورد از پروتکل‌های امنیتی شبکه‌های وای‌فای که امروزه متداول هستند، WPA[۱۹]

و WPA2 نام دارند که دو پروتکل احراز هویت لایه شبکه هستند که معمولاً مورد استفاده قرار می گیرند[۷-۹]. WPA در سال ۲۰۰۳ میلادی برای رفع مشکلات WEP ارائه گردید. TKIP[۲۰] روش مورد استفاده در رمزگذاری های WPA است. TKIP دارای امنیت بالاتری از WEP بود ولی در سال ۲۰۱۲ میلادی، در زمان ارتقاء " Wi-Fi 802.11" به دلیل آشکار شدن ضعف ها و خطاهای امنیتی اش که نفوذ را برای مخربان امنیتی به آسانی ایجاد می کرد منسوخ شد.TKIP مجموعه‌ای از الگوریتم‌ها است که به عنوان یک "پوشش" برای WEP کار می‌کند که به کاربران تجهیزات WLAN قدیمی اجازه می‌دهد تا بدون تعویض سخت‌افزار به TKIP ارتقا دهند. TKIP از برنامه‌نویسی اصلی WEP استفاده می‌کند، اما کدهای اضافی را در ابتدا و انتها برای کپسوله‌سازی و اصلاح آن می‌پیچد؛ مانند WEP، TKIP از الگوریتم رمزگذاری جریان RC4 به عنوان اساس خود استفاده می کند. پروتکل جدید، با این حال، هر بسته داده را با یک کلید رمزگذاری منحصر به فرد رمزگذاری می کند و کلیدها بسیار قوی تر از کلیدهای قبلی خود هستند[۱۰, ۱۱]. برای افزایش قدرت کلید، TKIP شامل چهار الگوریتم اضافی است:

- بررسی یکپارچگی پیام رمزنگاری برای محافظت از بسته ها
- یک مکانیسم توالی بردار اولیه که شامل هش است، برخلاف انتقال متن ساده WEP
- یک تابع اختلاط کلید در هر بسته برای افزایش قدرت رمزنگاری
- مکانیزم کلیدگذاری مجدد برای تولید کلید هر ۱۰۰۰۰ بسته.

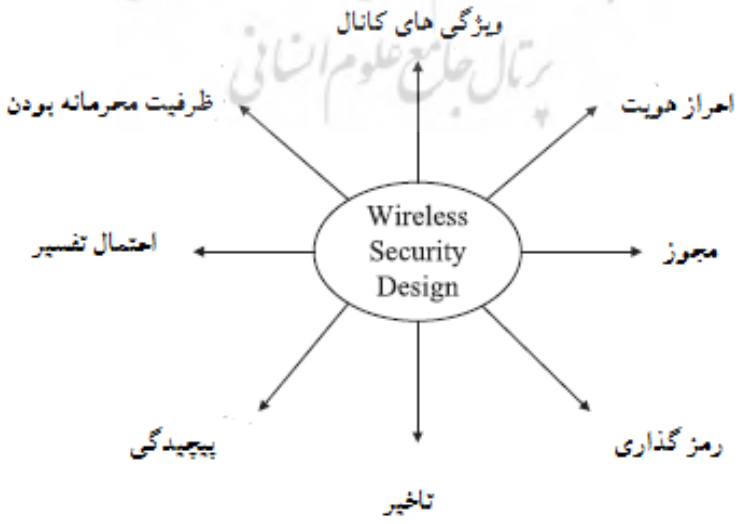
استاندارد رمزگذاری دیگری که امروزه استفاده می شود AES[۲۱]

است که در سال ۲۰۰۱ میلادی توسط NIST[۲۲] ارائه شد و از خانواده الگوریتم های متقارن محسوب می شود[۱۲, ۱۳]. روش های مختلفی تاکنون برای رمزگذاری و ایمن سازی شبکه های وای فای ارائه شده و همچنان در حال تکمیل هستند. سیر تکامل استانداردهای رمزگذاری در شبکه‌های بی‌سیم به صورت زیر است:

Wired Equivalent Privacy[۱۷]
Wi-Fi[۱۸]
[19] Wi-Fi Protected Access
Transient Key Integrity Protocol[۲۰]
Advanced Encryption Standard[۲۱]
National Institute of Standards and Technology[۲۲]

- شبکه باز (خطرناک): شبکه بی‌سیم باز شبکه‌ای است که در آن رمز عبور وجود ندارد. در این حالت هیچ یک از ترافیک‌های شبکه رمزگذاری نمی‌شود، به این معنی که داده‌های شبکه برای هر کسی قابل‌نمایش است.
- WEP 64 (خطرناک): استاندارد قدیمی رمزگذاری WEP منسوخ شده و بسیار آسیب‌پذیر است.
- WEP 128 (خطرناک): این استاندارد نیز همان WEP است فقط دارای کلید رمزگذاری طولانی‌تر بوده، اما باز هم از امنیت بالایی برخوردار نیست.
- WPA-PSK از نوع TKIP: این استاندارد در اصل همان رمزگذاری استاندارد WPA یا WPA1 است. این استاندارد نیز در حال حاضر ایمن نیست.
- WPA-PSK از نوع AES: این استاندارد، پروتکل قدیمی‌تر WPA را با روش رمزگذاری مدرن‌تر AES ادغام کرده است. سخت‌افزارهایی که از AES پشتیبانی می‌کنند قادر به رمزگذاری بر اساس استاندارد WPA2 هستند.
- WPA2-PSK از نوع TKIP: این روش از استاندارد مدرن WPA2 با رمزگذاری قدیمی TKIP استفاده می‌کند. این گزینه خیلی ایمن نیست و فقط تنها برای دستگاه‌های قدیمی که از WPA2 از نوع AES پشتیبانی نمی‌کنند، استفاده می‌شود.
- WPA2-PSK از نوع AES: این استاندارد برای همه شبکه‌های بی‌سیم توصیه می‌شود. در حال حاضر این استاندارد امن‌ترین روش رمزگذاری بی‌سیم است.

بدیهی است که بهره‌برداری از مکانیسم‌های احراز هویت چندگانه در لایه‌های پروتکل مختلف می‌تواند امنیت بی‌سیم را دوباره به قیمت پیچیدگی محاسباتی و تأخیر بالا افزایش دهد. روش‌های اصلی امنیت بی‌سیم شامل احراز هویت، مجوز و رمزگذاری است که برای آن عوامل مختلف طراحی، به عنوان مثال، سطح امنیت، پیچیدگی پیاده‌سازی و تأخیر ارتباط باید متعادل شوند. در شکل ۱ چالش های طراحی امنیت یک شبکه بی سیم نشان داده شده است[۱۴].



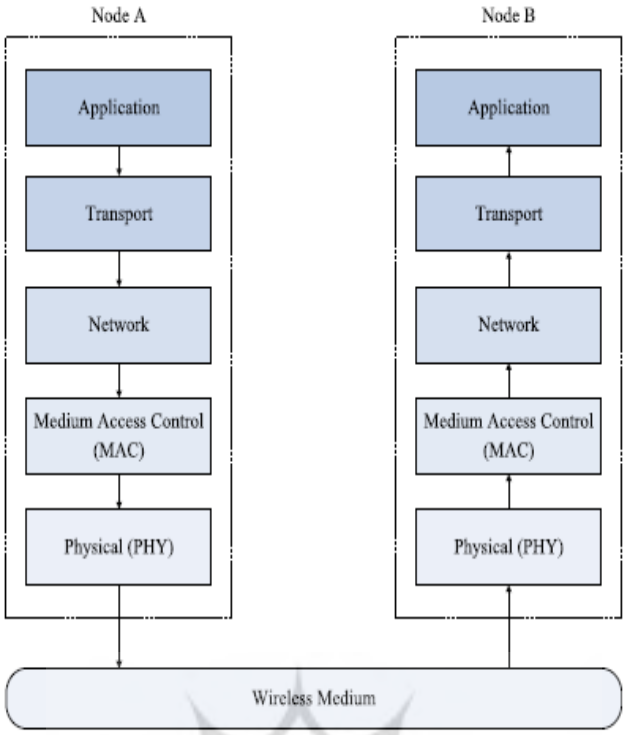
شکل ۱ چالش های طراحی امنیت یک شبکه بی سیم[۱۴].

در شبکه های سیمی، گره های ارتباطی به صورت فیزیکی از طریق کابل به هم متصل می شوند. در مقابل، شبکه های بی سیم به دلیل ماهیت پخش رسانه بی سیم بسیار آسیب پذیر هستند. به صراحت، شبکه‌های بی‌سیم مستعد حملات مخربی از جمله حملات شنود[۱۵]، حملاتDoS [۱۶]، حملات جعل [۱۷]، حملات [۱۸]MITM و غیره هستند. اخیراً، امنیت لایه فیزیکی به عنوان وسیله ای امیدوارکننده برای محافظت از ارتباطات بی سیم برای دستیابی به امنیت تئوری اطلاعات در برابر استراق سمع در حال ظهور است.

۲- انواع حملات ممکن در شبکه های بی سیم

به طور معمول، یک گره شبکه مجهز به کارت رابط شبکه بی سیم است و دارای یک آدرس MAC منحصر به فرد است که می تواند برای اهداف احراز هویت استفاده شود. مجدداً، علاوه بر احراز هویت MAC، روش‌های احراز هویت بی‌سیم دیگری از جمله تأیید هویت لایه شبکه، تأیید هویت لایه حمل‌ونقل و تأیید هویت لایه برنامه وجود دارد. همانطور که در شکل ۲ نشان داده شده است، یک گره شبکه (که با گره A مشخص می شود) ازیک سری پروتکل ها برای انتقال بسته های داده خود به گره شبکه دیگر (به عنوان مثال، گره B) استفاده می کند. به طور خاص، بسته داده در گره A ابتدا با سربارهای پروتکل، از جمله سربار لایه برنامه، سربار لایه انتقال، سربار لایه شبکه، سربار MAC و سربار لایه فیزیکی گسترش می یابد که منجر به یک بسته محصور شده می شود. سپس، بسته داده حاصل از طریق رسانه بی سیم به گره B منتقل می شود که کپسوله کردن یا بسته بندی بسته را انجام می دهد، از لایه فیزیکی شروع شده و به سمت لایه کاربردی پیش می رود تا بسته داده اصلی را بازیابی کند. تفاوت بین شبکه‌های سیمی و بی‌سیم عمدتاً در لایه‌های فیزیکی و MAC نهفته است، در حالی که لایه‌های کاربردی، انتقال و شبکه شبکه‌های بی‌سیم معمولاً با شبکه‌های سیمی یکسان هستند. در نتیجه، شبکه های سیمی و بی سیم به دلیل کاربرد، حمل و نقل و لایه های شبکه، آسیب پذیری های امنیتی مشترکی دارند. با این وجود، آنها همچنین از حملات انحصاری متقابل رنج می برند، زیرا شبکه های سیمی و بی سیم دارای لایه های مختلف PHY و MAC هستند، جدول ۱ پروتکل های اصلی و مشخصات پیاده سازی شده در هر یک از لایه های OSI بی سیم را نشان می دهد. به عنوان مثال، لایه کاربردی از HTTP[۲۳] به منظور ارائه خدمات وب پشتیبانی می کند، در حالی که FTP[۲۴] برای انتقال فایل های بزرگ استفاده می شود وSMTP[۲۵] برای ارسال نامه الکترونیکی (ایمیل) و غیره فراخوانی می شود [۱۹].

23 Hyper text transfer protocol
24 File Transfer Protocol
25 Simple mail transfer protocol



شکل ۲ معماری پروتکل لایه ای OSI بی سیم عمومی شامل لایه برنامه، لایه انتقال، لایه شبکه، لایه MAC و لایه فیزیکی.

جدول ۱ – پروتکل های هر یک از لایه های OSI

پروتکل های اصلی	لایه های OSI
HTTP,FTP,SMTP	لایه کاربردی
TCP,UDP,	لایه انتقالی
IP,ICMP	لایه شبکه
CSMA/CA,ALOHA,CDMA,OFDMA	لایه MAC
محیط انتقال، مدوله سازی و کد	لایه فیزیکی

TCP[۲۶] یا پروتکل کنترل انتقال که در لایه انتقالی استفاده می شود استانداردی است که نحوه برقراری و حفظ یک مکالمه شبکه ای که برنامه ها از طریق آن بتوانند داده ها را مبادله کنند، تعریف می کند.TCP با پروتکل اینترنت (IP) که چگونگی ارسال بسته های داده توسط رایانه ها به یکدیگر را تعریف می کند، کار می کند و تحویل مطمئن بسته های داده را تضمین می کند، در حالی که UDP[۲۷] هیچ تضمینی برای چنین تحویل قابل اطمینان و سفارشی ندارد.

[26] Transmission Control Protocol
[27] User Datagram Protocol

UDP یک پروتکل ارتباطی جایگزین برای پروتکل کنترل انتقال (TCP) است که در درجه اول برای برقراری اتصالات کم زمان و تحمل ضرر بین برنامه ها در اینترنت استفاده می شود. برخلاف TCP، UDP یک مدل انتقال ساده‌تر را اتخاذ می‌کند، از این رو هزینه پروتکل را کاهش می دهد. در لایه شبکه، پروتکل‌های مختلفی داریم، مانند IP[۲۸] که شیوه‌ای استاندارد برای ارسال و مسیریابی بسته‌های داده در شبکه‌های کامپیوتری است و این کار را با استفاده از آدرس‌های آی‌پی انجام می‌دهد آدرس آی‌پی، شناسه منحصربه‌فردی است که هویت هر یک از کامپیوترها یا دیگر تجهیزات (گره‌های) متصل به شبکه را مشخص می‌کند. در شبکه‌های مبتنی بر پروتکل اینترنت (آی‌پی)، هر کامپیوتر یا دستگاه متصل به شبکه، یک آدرس آی‌پی دارد که آن را از دیگر کامپیوترهای تحت شبکه متمایز می‌کند. وقتی داده‌ای روی اینترنت ارسال می‌شود، آن داده به قطعات کوچکی به نام بسته[۲۹] تبدیل می‌شود. بسته، حاوی آدرس آی‌پی فرستنده و نیز آدرس آی‌پی گیرنده است. وقتی بسته‌ها به مقصد می‌رسند، با کمک پروتکل دیگری موسوم به TCP، با ترتیب صحیح‌شان به هم می‌پیوندند و به‌شکل یک‌پارچه اولیه درمی‌آیند.

در رابطه با لایه MAC، پروتکل های مختلف متعددی وجود دارد که توسط شبکه های بی سیم مختلف پذیرفته شده است، مانند CSMA/CA[۳۰] مورد استفاده در شبکه های Wi-Fi، ALOHA[۳۱] شکاف دار که در شبکه های ماهواره ای تاکتیکی توسط نیروهای نظامی استفاده می شود، CDMA درگیر در شبکه های تلفن همراه و OFDMA[۳۲] در شبکه های پیشرفته LTE و LTE اتخاذ شده است [۲۰-۲۲]. دسترسی چندگانه با قابلیت شنود سیگنال حامل/پیشگیری از تصادم (CSMA/CA) در شبکه‌های کامپیوتری، روش دسترسی چندگانه در شبکه‌های بیسیم می‌باشد. زمانیکه اطلاعات بر روی بستر شبکه های کامپیوتری در حال حرکت به سوی مقاصد خود میباشند احتمال بروز تصادم و برخورد بین این اطلاعات و پکت ها وجود دارد. از این رو برای جلوگیری از این تصادم و برخورد ها در شبکه دو پروتکل اساسی وجود دارد. این پروتکل ها CSMA/CD[۳۳] یا و دیگری CSMA/CA یا نام دارند. پروتکل دسترسی چندگانه ALOHA برای انتقال داده ها از طریق یک کانال شبکه عمومی استفاده می شود و دسترسی به کانال شبکه ارتباطی مشترک را می توان با استفاده از سیستم ALOHA هماهنگ و داوری کرد. این پروتکل در دهه ۱۹۷۰ در دانشگاه هاوایی توسط نورمن آبرامسون[۳۴] و همکارانش ایجاد شد. این سیستم در ابتدا برای پخش رادیویی زمینی طراحی شده بود، اما اکنون سیستم های ارتباطی ماهواره ای از آن استفاده می کنند. هنگامی که دو یا چند سیستم به دنبال انتقال همزمان در یک کانال هستند، یک سیستم ارتباطی مشترک مانند ALOHA به راهی برای رسیدگی به برخوردها نیاز دارد[۲۳, ۲۴]. علاوه بر این، لایه فیزیکی ویژگی های فیزیکی انتقال اطلاعات را مشخص می کند، از جمله رسانه انتقال،

28 Internet Protocol
29 Packet
30 Carrier Sense Multiple Access/Collision Avoidance
31 Advocates of Linux Open-source Hawaii Association
32 Orthogonal frequency-division multiple access
33 Carrier-sense multiple access with collision detection
34 Norman Abramson

مدولاسیون، کدگذاری خط، چندگانه سازی، سوئیچینگ مدار، شکل دهی پالس، تصحیح خطای رو به جلو، درهم آمیختن بیت و سایر عملیات کدگذاری کانال. هر لایه OSI چالش‌ها و مسائل امنیتی منحصر به فرد خود را دارد، زیرا لایه‌های مختلف به پروتکل‌های مختلف متکی هستند، بنابراین آسیب‌پذیری‌های امنیتی متفاوتی را نشان می‌دهند. در زیر طیف وسیعی از حملات بی سیم را که به طور بالقوه توسط لایه های پروتکل مختلف با آن مواجه می شوند، خلاصه می کنیم.

الف. حملات لایه فیزیکی

لایه فیزیکی پایین ترین لایه در معماری پروتکل OSI است که برای مشخص کردن ویژگی های فیزیکی انتقال سیگنال استفاده می شود. ماهیت پخش ارتباطات بی‌سیم، لایه فیزیکی آن را در برابر حملات شنود و پارازیت که دو نوع اصلی حملات لایه فیزیکی بی‌سیم هستند، بسیار آسیب‌پذیر می‌کند، به طور خاص، حمله استراق سمع به تلاش کاربر غیرمجاز اشاره دارد رهگیری انتقال داده بین کاربران قانونی [۲۵] یک گره مخرب در شبکه‌های بی‌سیم می‌تواند به آسانی تداخل عمدی را برای ایجاد اختلال در ارتباطات داده بین کاربران قانونی ایجاد کند که از آن به عنوان یک حمله پارازیت (همچنین به عنوان حمله DoS شناخته می‌شود) یاد می‌شود. هدف مسدود کننده جلوگیری از دسترسی کاربران مجاز به منابع شبکه بی سیم است و این امر دسترسی شبکه را برای کاربران قانونی مختل می کند. برای این منظور، تکنیک‌های طیف گسترده به‌عنوان وسیله‌ای مؤثر برای دفاع در برابر حملات DoS با پخش سیگنال ارسال بر روی پهنای باند طیفی وسیع‌تر از باند فرکانسی اصلی آن شناخته می‌شوند.

ب. حملات لایه MAC

لایه MAC چندین گره شبکه را قادر می‌سازد تا به یک رسانه مشترک با کمک مکانیسم‌های کنترل دسترسی کانال هوشمند مانند CSMA/CA، CDMA، OFDMA و غیره دسترسی پیدا کنند. به طور معمول، هر گره شبکه مجهز به یک NIC[۳۵] و یک آدرس MAC منحصر به فرد است که برای احراز هویت کاربر استفاده می شود. مهاجمی که سعی می کند آدرس MAC اختصاص داده شده خود را با قصد مخرب تغییر دهد، MAC spoofing نامیده می شود که تکنیک اصلی حملات MAC است[۲۶-۲۸]. ربودن IP یکی دیگر از فعالیت های غیرقانونی است که توسط رباینده‌گان به منظور تصاحب آدرس IP یک کاربر قانونی دیگر راه اندازی شده است. اگر مهاجم موفق به ربودن آدرس IP شود، قادر به قطع ارتباط کاربر قانونی و ایجاد یک اتصال جدید به شبکه با جعل هویت کاربر قانونی و در نتیجه دسترسی به اطلاعات محرمانه است. انواع دیگری از تکنیک‌های ربودن IP وجود دارد، از جمله ربودن پیشوند، ربودن مسیر و ربودن پروتکل دروازه مرزی [۲۹, ۳۰].

[35] Network interface card

ج. حملات لایه حمل و نقل

این بخش به طور خلاصه فعالیت های مخرب در لایه انتقال را با تاکید بر حملات TCP و UDP[۳۶] خلاصه می کند. به طور خاص، TCP یک پروتکل حمل و نقل اتصال گرا است که برای پشتیبانی از انتقال مطمئن بسته های داده طراحی شده است که معمولاً برای تحویل ایمیل ها و برای انتقال فایل ها از یک گره شبکه به گره دیگر استفاده می شود. برخلاف TCP، UDP یک پروتکل حمل و نقل بدون اتصال است که با کاهش سربار پروتکل و تاخیر همراه است، حملات TCP شامل حملات TCP flooding و حملات پیش‌بینی شماره دنباله [۳۱] است. حمله TCP که به عنوان ping flooding نیز شناخته می‌شود، یک حمله DoS در لایه انتقال است، جایی که مهاجم تعداد زیادی درخواست پینگ، مانند درخواست‌های اکو ICMP[۳۷] را به یک گره قربانی ارسال می‌کند که سپس با ارسال پاسخ‌های پینگ پاسخ می‌دهد؛ مانند پاسخ های اکو ICMP. این کار هم بافرهای ورودی و هم خروجی گره قربانی را پر می‌کند و حتی ممکن است اتصال آن به شبکه هدف را زمانی که تعداد درخواست‌های پینگ به اندازه کافی زیاد باشد به تاخیر بیاندازد. تکنیک پیش‌بینی توالی TCP یکی دیگر از حملات TCP است که تلاش می‌کند تا شاخص توالی بسته‌های TCP یک گره فرستنده را پیش‌بینی کند و سپس بسته‌های TCP گره را بسازد. لایه کاربردی از HTTP برای سرویس های وب، FTP برای انتقال فایل و SMTP برای انتقال ایمیل پشتیبانی می کند. هر یک از این پروتکل ها مستعد حملات امنیتی هستند. به طور منطقی، حملات لایه کاربردی ممکن است به عنوان حملات HTTP، حملات FTP و حملات SMTP طبقه بندی شوند.

حملات اصلی HTTP شامل حمله بدافزار (به عنوان مثال، اسب های تروجان، ویروس ها، کرم ها، درهای پشتی، کی لاگرها و غیره)، حمله تزریق زبان ساختاریافته (SQL[۳۸]) و حمله اسکریپت بین سایتی است [۳۲].

اصطلاح «بدافزار» به نرم‌افزار مخربی اشاره دارد که به شکل کد، اسکریپت و محتوای فعال برنامه‌ریزی شده توسط مهاجمانی است که تلاش می‌کنند انتقال‌های مجاز را مختل کنند یا اطلاعات محرمانه را رهگیری کنند. تزریق SQL معمولاً برای حمله به برنامه‌های مبتنی بر داده با درج عبارات سرکش SQL در تلاش برای دسترسی غیرمجاز به وب‌سایت‌های قانونی مورد سوء استفاده قرار می‌گیرد. آخرین نوع از حملات HTTP که ذکر می شود، به عنوان حملات اسکریپت بین سایتی نامیده می شود که معمولاً در برنامه های کاربردی وب رخ می دهد و هدف آنها دور زدن برخی از اقدامات کنترل دسترسی (به عنوان مثال، همان خط مشی مبدا) با تزریق اسکریپت های سمت مشتری به صفحات وب است.[۳۳-۳۶].

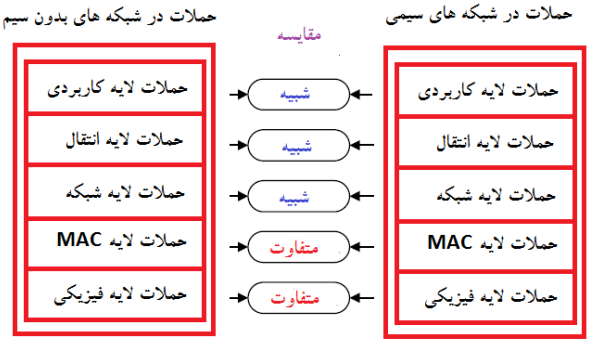
همانطور که در شکل ۳ نشان داده شده است، حملات لایه کاربرد، انتقال و شبکه شبکه های بی سیم مانند حملات شبکه های سیمی است، زیرا شبکه های بی سیم و سیمی پروتکل های مشترکی را در لایه های برنامه، حمل و نقل و شبکه به

[36] User Datagram Protocol

[37] internet control message protocol

Structured Query Language[۳۸]

اشتراک می گذارند. در مقابل، شبکه های بی سیم از نظر حملات PHY و MAC با شبکه های سیمی متفاوت هستند. به طور کلی، تنها لایه های PHY و MAC در استانداردهای شبکه های بی سیم (مانند Wi-Fi، بلوتوث، LTE و غیره) مشخص شده اند. علاوه بر این، لایه بی سیم PHY کاملاً متفاوت از همتای مبتنی بر سیم است. به دلیل ماهیت پخش انتشار رادیویی، لایه PHY بی سیم در برابر حملات شنود و پارازیت بسیار آسیب پذیر است. برای این منظور، امنیت لایه فیزیکی به عنوان وسیله ای مؤثر برای ایمن سازی ارتباطات بی سیم در برابر استراق سمع در حال ظهور است



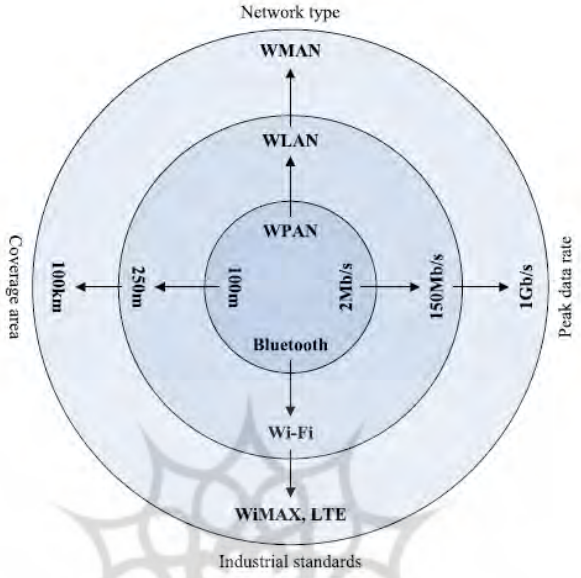
شکل ۳- مقایسه بین شبکه های بی سیم و سیمی از نظر حملات امنیتی در لایه های مختلف OSI

۳- روش ها و نمونه های دفاعی امنیتی برای شبکه های بی سیم

در این بخش به بررسی روش های ارتقاء امنیت شبکه های بی سیم پرداخته شده است. در مقایسه با شبکه های سیمی، شبکه های بی سیم دارای مزیت عدم نیاز به استقرار زیر ساخت های کابلی پر هزینه هستند. در شکل ۴ خانواده ای از شبکه های بی سیم مشاهده می شود که به ارائه مقایسه ای بین تکنیک های WLAN[۳۹]، WPAN[۴۰] و WMAN[۴۱] از نظر استاندارد ها، منطقه تحت پوشش و نرخ داده آن ها می پردازد. به عنوان مثال یک WPAN برای اتصال به دستگاه های شخصی (صفحه کلید، هدست صوتی، چاپگر و غیره) با سرعت داده کم و در یک منطقه تحت پوشش کوچک استفاده می شود. یا به عنوان مثال، بلوتوث یک استاندارد رایج در WPAN است که از زیر پوشش رادیویی برد کوتاه در باند ۲۴۰۰- ۲۴۸۰ مگاهرتز استفاده می کند که می تواند حداکثر سرعت داده ۲ مگابیت بر ثانیه و بردی تا ۱۰۰ متر را فراهم کند. شکل ۴ همچنین نشان می دهد که یک WLAN به طور کلی دارای نرخ داده بالاتر و منطقه پوشش وسیع تری نسبت به WPAN است که برای اتصال دستگاه های بی سیم از طریق یک AP در یک منطقه تحت پوشش محلی استفاده می شود. به عنوان مثال، IEEE 802.11 (همچنین به عنوان Wi-Fi شناخته می شود) از یک سری استانداردهای WLAN صنعتی تشکیل شده است. استانداردهای مدرن Wi-Fi قادر به پشتیبانی از حداکثر سرعت داده ۱۵۰ مگابیت بر ثانیه و حداکثر برد ۲۵۰ متر هستند [۸۸]. در نهایت، یک MAN معمولاً برای اتصال یک کلان شهر با نرخ بالاتر و در یک منطقه تحت پوشش بزرگتر از WPAN و WLAN استفاده می شود[۳۷-۳۹]. به

[39] wireless LAN
[40] wireless personal area network
[41] Wireless metropolitan area network.

عنوان مثال، در شکل ۴، ما دو نوع استاندارد صنعتی برای WMAN، یعنی WiMAX و LTE را نشان می دهیم. در ادامه، مروری بر روش های امنیتی مورد استفاده در استانداردهای بی سیم فوق الذکر (یعنی بلوتوث، وای فای، وایمکس و LTE) برای حفاظت از صحت، محرمانه بودن، یکپارچگی و در دسترس بودن انتقال های قانونی از طریق بی سیم ارائه خواهیم کرد.



شکل ۴- خانواده شبکه های بی سیم متشکل از WPAN، WLAN و WMAN.

الف- بلوتوث

بلوتوث یکی از استاندارد های شبکه های بی سیم با برد کوتاه و کم مصرف است که به طور گسترده در دستگاه های محاسباتی و ارتباطی و همچنین در تجهیزات جانبی مانند تلفن های همراه، صفحه کلید، هدست های صوتی و غیره پیاده سازی شده است. با این حال، دستگاه های بلوتوث مشمول ی تعداد زیادی از تهدیدات امنیتی بی سیم شده و ممکن است به راحتی در معرض خطر قرار گیرند. به دلایل امنیتی، هر دستگاه بلوتوث دارای چهار موجودیت است، از جمله آدرس دستگاه بلوتوث (BD_ADDR)، کلید احراز هویت خصوصی، کلید رمزگذاری خصوصی و یک عدد تصادفی (RAND) که به ترتیب برای احراز هویت، مجوز و رمزگذاری استفاده می‌شوند. به طور خاص، BD_ADDR حاوی ۴۸ بیت است که برای هر دستگاه بلوتوث منحصر به فرد است. کلید احراز هویت خصوصی ۱۲۸ بیتی برای احراز هویت و کلید رمزگذاری خصوصی که طول آن از ۸ تا ۱۲۸ بیت متفاوت است برای رمزگذاری استفاده می شود[۴۰-۴۲].

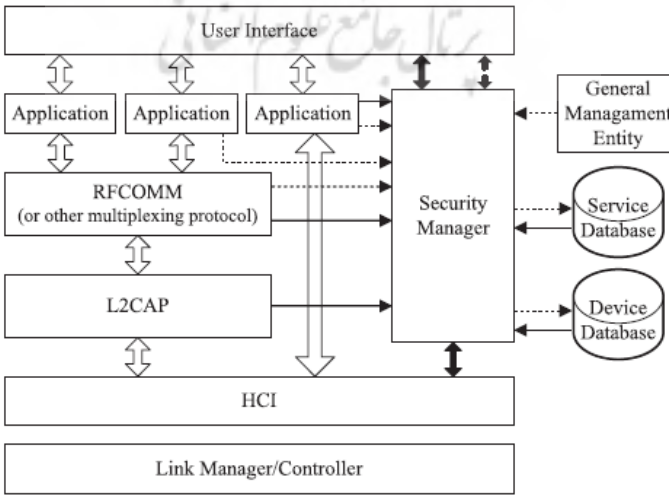
علاوه بر این، RAND یک عدد شبه تصادفی ۱۲۸-b است که اغلب توسط خود دستگاه بلوتوث تولید می شود. شکل ۵ معماری امنیتی بلوتوث را نشان می دهد که در آن جزء کلیدی، مدیر امنیتی مسئول احراز هویت، مجوز و رمزگذاری است. همانطور که در شکل ۵۶ نشان داده شده است، پایگاه داده سرویس و پایگاه داده دستگاه عمدتاً به ترتیب برای

ذخیره اطلاعات مربوط به امنیت در سرویس ها و دستگاه ها استفاده می شوند که می توانند از طریق رابط کاربری تنظیم شوند. این پایگاه‌های اطلاعاتی نیز می‌تواند توسط نهاد مدیریت عمومی اداره شود. هنگامی که یک دستگاه بلوتوث درخواست دسترسی از دستگاه دیگری دریافت می کند، ابتدا با کمک RFCOMM یا سایر پروتکل های مالتی پلکسی، از مدیر امنیتی خود سؤال می کند. سپس، مدیر امنیتی باید با بررسی پایگاه داده سرویس و پایگاه داده دستگاه، به این سؤال پاسخ دهد که آیا اجازه دسترسی را می دهد یا خیر. نمایه دسترسی عمومی بلوتوث سه حالت امنیتی را تعریف می کند:

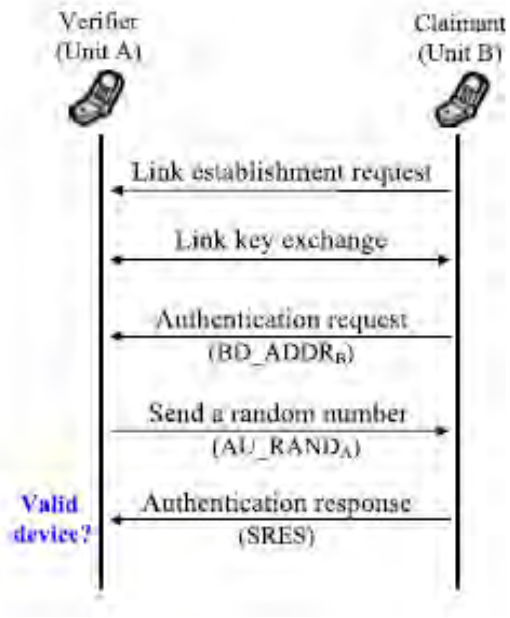
۱) حالت امنیتی ۱ (غیر ایمن) که در آن هیچ امنیتی آغاز نمی شود.

۲) حالت امنیتی ۲ (امنیت اجباری در سطح سرویس) که در آن رویه امنیتی پس از ایجاد پیوند بین فرستنده بلوتوث و گیرنده آغاز می شود.

۳) حالت امنیتی ۳ (امنیت اجباری سطح پیوند) که در آن رویه امنیتی قبل از ایجاد پیوند آغاز می شود. در سیستم‌های بلوتوث، یک دستگاه به یکی از سه دسته طبقه‌بندی می‌شود: دستگاه قابل اعتماد، غیرقابل اعتماد، دستگاه احراز هویت شده، غیر احراز هویت و دستگاه ناشناخته. دستگاه مورد اعتماد به این معنی است که دستگاه به عنوان یک رابطه مطمئن و ثابت احراز هویت شده و مجاز شده است، بنابراین دسترسی نامحدود به همه خدمات دارد. احراز هویت نشان دهنده فرآیند تأیید هویت دستگاه های بلوتوث بر اساس BD_ADDR و کلید پیوند است. همانطور که در شکل ۶ نشان داده شده است، احراز هویت بلوتوث از "طرح چالش-پاسخ" استفاده می کند که در آن تایید کننده (واحد A) مدعی (واحد B) را به چالش می کشد و سپس به خاطر احراز هویت پاسخ می دهد. فرآیند مجوز برای تصمیم گیری در مورد اینکه آیا یک دستگاه بلوتوث حق دسترسی به یک سرویس خاص را دارد یا خیر استفاده می شود. به طور معمول، دستگاه‌های مورد اعتماد مجاز به دسترسی به همه سرویس‌ها هستند، اما دستگاه‌های غیرقابل اعتماد یا ناشناخته قبل از اعطای دسترسی به خدمات، نیاز به مجوز دارند.



شکل ۵ معماری امنیتی بلوتوث[۴۳].



شکل ۶- فرآیند احراز هویت بلوتوث.

ب. وای فای

خانواده شبکه‌های وای‌فای که عمدتاً مبتنی بر استانداردهای IEEE 802.11 b/g هستند، در حال گسترش هستند. رایج ترین پروتکل های امنیتی در وای فای به عنوان WEP و WPA نامیده می شوند. WEP در سال ۱۹۹۹ به عنوان یک اقدام امنیتی برای شبکه‌های Wi-Fi پیشنهاد شد تا انتقال داده‌های بی‌سیم را مانند شبکه‌های سیمی سنتی ایمن کند. اولین استاندارد IEEE 802.11 که مورد تائید گسترده قرار گرفت IEEE 802.11b بود. اگرچه محصولات IEEE 802.11b را بر اساس استانداردی مشابه ساخته‌اند؛ اما همیشه یک نگرانی وجود داشت که آیا محصولات فروشندگان مختلف با یکدیگر تعامل‌پذیر خواهند. برای نیل به این هدف اتحادیه بی سیم (WECA[۴۲]) یک کنسرسیوم صنعتی، در سال ۱۹۹۹ تشکیل شد این سازمان بعداً به اتحادیه Wi-Fi تغییر نام داد و مجموعه‌ای آزمایشی برای تائید تعامل‌پذیری برای محصولات IEEE 802.11b ایجاد کرد. اصطلاح Wi-Fi برای محصولاتی به کار می‌رود که این گواهی را دریافت کرده‌اند.

با این حال، نشان داده شده است که WEP یک پروتکل امنیتی نسبتا ضعیف است که دارای نقص های متعدد است. WPA به عنوان یک جایگزین، در سال ۲۰۰۳ برای جایگزینی WEP معرفی شد، به طور معمول، WPA و WPA2 ایمن تر از WEP هستند و بنابراین به طور گسترده در شبکه های Wi-Fi مدرن استفاده می شوند. در زیر، فرآیندهای احراز هویت و رمزگذاری پروتکل های WEP، WPA و WPA2 را به تفصیل شرح می دهیم. پروتکل WEP از دو بخش اصلی احراز هویت و رمزگذاری تشکیل شده است، احراز هویت WEP از یک بخش احراز هویت چهار مرحله ای "چالش-پاسخ" بین مشتری Wi-Fi و نقطه دسترسی که با کمک یک کلید WEP مشترک کار می کند، استفاده

[42] Western Electrical Contractors Association

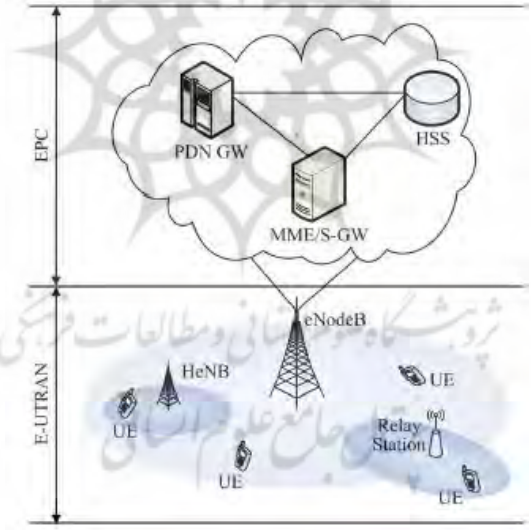
می کند. سپس متن رمزگذاری شده دریافتی را با کمک کلید WEP از پیش به اشتراک گذاشته شده رمزگشایی می کند و سعی می کند متن رمزگشایی شده را با متن اصلی مقایسه کند. اگر مطابقت پیدا شود، نقطه دسترسی یک نشانگر احراز هویت موفق برای مشتری ارسال می کند. در غیر این صورت، احراز هویت ناموفق تلقی می شود. مزیت اصلی WPA نسبت به WEP این است که WPA از رمزگذاری داده های قوی تری استفاده می کند که به آن TKIP گفته می شود که توسط یک MIC به منظور محافظت از یکپارچگی داده ها و محرمانه بودن شبکه های Wi-Fi کمک می شود. وایمکس (همچنین با نام IEEE 802.16 شناخته می شود) استانداردی است که برای WMAN توسعه یافته است و سیستم اولیه وایمکس برای ارائه حداکثر سرعت داده ۴۰ مگابیت بر ثانیه طراحی شده است. به منظور برآورده کردن الزامات ابتکار بین المللی مخابرات سیار-پیشرفته، IEEE 802.16m به عنوان یک نسخه به روز شده از وایمکس اصلی پیشنهاد شد که قادر به پشتیبانی از حداکثر سرعت داده ۱ گیگابیت بر ثانیه برای دریافت ثابت و ۱۰۰ مگابیت بر ثانیه است[۷, ۴۴, ۴۵]؛ مانند سایر سیستم‌های بی‌سیم، وایمکس نیز با حملات بی‌سیم مختلف مواجه می‌شود. زیرلایه امنیتی یک پروتکل به اصطلاح PKM[۴۳] را تعریف می کند که استفاده از گواهی دیجیتال X.509 را همراه با الگوریتم کلید عمومی RSA[۴۴] و الگوریتم AES برای احراز هویت کاربر و همچنین برای مدیریت کلید و انتقال ایمن در نظر می گیرد. نسخه اولیه PKMv1 همانطور که در استانداردهای اولیه وایمکس مشخص شده است (به عنوان مثال IEEE 802.16a/c) از مکانیزم احراز هویت یک طرفه پیچیده استفاده می کند و از این رو در برابر حملات MITM آسیب پذیر است. برای پرداختن به این مشکل، یک نسخه PKM به روز شده (PKMv2) در نسخه های پیچیده تر استاندارد وایمکس (به عنوان مثال، IEEE 802.16e/m) [104] پیشنهاد شد که بر احراز هویت دو طرفه متکی است. احراز هویت در وایمکس توسط پروتکل PKM به دست می آید که از دو رویکرد احراز هویت اصلی پشتیبانی می کند، یعنی احراز هویت مبتنی بر RSA و احراز هویت مبتنی بر EAP.. گواهی X.509 شامل کلید عمومی و آدرس MAC گره شبکه مرتبط با آن است. در طول فرآیند احراز هویت مبتنی بر RSA که در شکل ۱۳ نشان داده شده است، هنگامی که یک SS یک درخواست احراز هویت از یک WiMAX BS دریافت می کند، گواهی دیجیتال X. 509 خود را به BS می فرستد که سپس تأیید می کند که آیا گواهی معتبر است یا خیر. اگر گواهی معتبر باشد، SS تایید شده در نظر گرفته می شود. در مقابل، یک گواهی نامعتبر به این معنی است که SS نمی تواند احراز هویت شود.

ج- تکامل بلند مدت (LTE)

LTE یک از جدیدترین استانداردهایی است که توسط پروژه مشارکت ۴G برای شبکه های تلفن همراه نسل بعدی توسعه یافته است که برای ارائه پوشش یکپارچه، سرعت داده بالا و تأخیر کم طراحی شده است [۴۶] از سوئیچینگ بسته

[43] Privacy and key management
[44] Rivest–Shamir–Adleman

برای کار متقابل یکپارچه با سایر شبکه های بی سیم پشتیبانی می کند. از سال ۲۰۱۹ میلادی این استاندارد در حال جایگزینی با نسل چهارم ارتباطات است. شبکه LTE معمولاً از یک EPC[45] و یک E-UTRAN تشکیل شده است، همانطور که در شکل ۷ نشان داده شده است [۳۷] EPC شامل یک MME[46]، یک دروازه سرویس دهی، یک دروازه شبکه داده بسته (PDN GW) و یک HSS[47] است. FTP و SSH هر دو پروتکل هایی تحت شبکه هستند که درست مانند HTTP بالای لایه TCP/IP اجرا می گردند. علاوه بر این، E-UTRAN شامل یک ایستگاه پایه (که در LTE نیز eNodeB نامیده می شود) و چندین UE[48] است. اگر شرایط کانال بین UE و eNodeB ضعیف باشد، ممکن است یک ایستگاه رله برای کمک به ارتباطات داده آنها فعال شود. علاوه بر این، هم در دفاتر کوچک و هم در محیط های مسکونی، یک HeNB ممکن است برای بهبود پوشش داخلی با افزایش ظرفیت و قابلیت اطمینان E-UTRAN نصب شود. اگرچه معرفی این عناصر به LTE می‌تواند پوشش و کیفیت شبکه را بهبود بخشد، اما آسیب‌پذیری‌ها و تهدیدات امنیتی جدید خود را دارد. به منظور تسهیل تبادل بسته ایمن بین UE و EPC، یک پروتکل به اصطلاح EPS-AKA برای دفاع از شبکه های LTE در برابر حملات مختلف، از جمله حملات تغییر مسیر، حملات ایستگاه پایه سرکش و حملات MITM پیشنهاد شد. یک فرآیند احراز هویت دو طرفه بین UE و EPC فراخوانی شد که در پروتکل EPS-AKA که مسئول تولید هر دو CK[49] و IK[50] است، پذیرفته شده است[۴۷, ۴۸].



شکل ۷ ساختار معماری LTE.

45 Evolved packet core
46 Mobility management entity
47 Home subscriber server
48 User equipment.
49 Ciphering key
50 Integrity key

۴- نتیجه گیری:

در این مقاله، ما یک بررسی از چالش‌های امنیتی بی‌سیم و مکانیسم‌های دفاعی برای حفاظت از صحت، محرمانه بودن، یکپارچگی و در دسترس بودن انتقال‌های بی‌سیم در برابر حملات مخرب ارائه کرده‌ایم. ما در مورد طیف وسیعی از حملات بی‌سیم و تهدیدات امنیتی که بالقوه در لایه‌های پروتکل مختلف از لایه برنامه تا لایه فیزیکی تجربه می‌شوند، بحث کرده‌ایم که به حملات لایه برنامه و لایه انتقال، لایه شبکه، لایه MAC و همچنین فیزیکی طبقه‌بندی می‌شوند. حملات لایه ای سپس، پارادایم‌ها و پروتکل‌های امنیتی موجود که برای محافظت در برابر حملات لایه‌های پروتکل مختلف طراحی شده‌اند، در زمینه چندین شبکه بی‌سیم به طور گسترده مستقر شده، از جمله بلوتوث، وای‌فای، وایمکس و LTE بررسی شده‌اند. با در نظر گرفتن اینکه انتقال بی سیم به دلیل ماهیت پخش رادیویی در برابر حملات استراق سمع بسیار آسیب پذیر است، ما همچنین وضعیت فناوری امنیت لایه فیزیکی را مورد بحث قرار داده ایم که به عنوان یک پارادایم امیدوارکننده برای دفاع از انتقال بی سیم در برابر استراق سمع در حال ظهور است.

منابع

۱. Foukalas, F. V. Gazis, and N. Alonistioti, *Cross-layer design proposals for wireless mobile networks: a survey and taxonomy.* IEEE Communications Surveys & Tutorials, 2008. 10(1): p. 70-85.

۲. Jurdak, R. C.V. Lopes, and P. Baldi, *A survey, classification and comparative analysis of medium access control protocols for ad hoc networks.* IEEE Communications Surveys & Tutorials, 2004. 6(1): p. 2-16.

۳. Ganesh, D.E. *Analysis of Wireless Sensor Networks Through Secure Routing Protocols Using Directed Diffusion Methods.* International Journal of Wireless Network Security, 2022. 7(1): p. 28-35.

۴. Xiao, Y. et al. *MAC security and security overhead analysis in the IEEE 802.15. 4 wireless sensor networks.* EURASIP Journal on Wireless Communications and Networking, 2006. 2006: p. 1-12.

۵. Wu, Y. et al. *A survey of physical layer security techniques for 5G wireless networks and challenges ahead.* IEEE Journal on Selected Areas in Communications, 2018. 36(4): p. 679-695.

۶. Fu, B. et al. *A survey of cross-layer designs in wireless networks.* IEEE Communications Surveys & Tutorials, 2013. 16(1): p. 110-126.

۷. Reddy, B.I. and V. Srikanth, *Review on wireless security protocols (WEP, WPA, WPA2 & WPA3).* International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2019: p. 28-35.

۸. Lashkari, A.H. M.M.S. Danesh, and B. Samadi. *A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i).* in *2009 2nd IEEE international conference on computer science and information technology*. 2009. IEEE.

۹. Tews, E. and M. Beck. *Practical attacks against WEP and WPA*. in *Proceedings of the second ACM conference on Wireless network security*. 2009.

.۱۰ Tews, E. R.P. Weinmann, and A. Pyshkin. *Breaking 104 bit WEP in less than 60 seconds*. in *International Workshop on Information Security Applications*. 2007. Springer.
.۱۱ Schepers, D. A. Ranganathan, and M. Vanhoef. *Practical Side-Channel Attacks against WPA-TKIP*. in *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*. 2019.
.۱۲ Akkar, M.L. and C. Giraud. *An implementation of DES and AES, secure against some attacks*. in *International Workshop on Cryptographic Hardware and Embedded Systems*. 2001. Springer.
.۱۳ Bonnetain, X. M. Naya-Plasencia, and A. Schrottenloher, *Quantum security analysis of AES.* IACR Transactions on Symmetric Cryptology, 2019. 2019(2): p. 55-93.
.۱۴ Zou, Y. et al. *A survey on wireless security: Technical challenges, recent advances, and future trends.* Proceedings of the IEEE, 201 .۶104)9 :(p. 1727-1765.
.۱۵ Yu, J. et al. *An indirect eavesdropping attack of keystrokes on touch screen through acoustic sensing.* IEEE Transactions on Mobile Computing, 2019. 20(2): p. 337-351.
.۱۶ Cetinkaya, A. H. Ishii, and T. Hayakawa, *An overview on denial-of-service attacks in control systems: Attack models and security analyses.* Entropy, 2019. 21(2): p. 210.
.۱۷ Monteiro, J. J. Alam, and T.H. Falk, *Generalized end-to-end detection of spoofing attacks to automatic speaker recognizers.* Computer Speech & Language, 2020. 63: p. 101096.
.۱۸ Al-shareeda, M.A. et al. *Review of prevention schemes for man-in-the-middle (MITM) attack in vehicular ad hoc networks.* International Journal of Engineering and Management Research, 2020. 10.
.۱۹ Zhang, J. et al. *Future Internet: trends and challenges.* Frontiers of Information Technology & Electronic Engineering, 2019. 20(9): p. 1185-1194.
(۲۰ Mishra, D. and E. Natalizio, *A survey on cellular-connected UAVs: Design challenges, enabling 5G/B5G innovations, and experimental advancements.* Computer Networks, 2020. 182: p. 107451.
.۲۱ Stanczak, J. et al. *Enhanced unmanned aerial vehicle communication support in LTE-advanced*. in *2018 IEEE Conference on Standards for Communications and Networking (CSCN)*. 2018. IEEE.
.۲۲ Balteanu, F. et al. *Envelope tracking system for high power applications in uplink 4G/5G LTE advanced*. in *2018 Asia-Pacific Microwave Conference (APMC)*. 2018. IEEEv
.۲۳ Yavascan, O.T. and E. Uysal, *Analysis of slotted ALOHA with an age threshold* .IEEE Journal on Selected Areas in Communications, 2021. 39(5): p. 1456-1470.
.۲۴ Munari, A. *Modern random access: An age of information perspective on irregular repetition slotted ALOHA.* IEEE Transactions on Communications, 2021. 69(6): p. 3572-3585.
.۲۵ Huanan, Z. X. Suping, and W. Jiannan, *Security and application of wireless sensor network.* Procedia Computer Science, 2021. 183: p. 486-492.
.۲۶ Liu, S. *Mac spoofing attack detection based on physical layer characteristics in wireless networks*. in *2019 IEEE International Conference on Computational Electromagnetics (ICCEM)*. 2019. IEEE.

.۲۷ Ullas, S. and J. Sandeep, *Reliable Monitoring Security System to Prevent MAC Spoofing in Ubiquitous Wireless Network*, in *Advances in Big Data and Cloud Computing*. 201 ,۹Springer. p. 141-153.

T۲۸ Jiang, P. et al. *Virtual MAC spoofing detection through deep learning*. in *2018 IEEE International Conference on Communications (ICC)*. 2018. IEEE)

.۲۹ Ponmaniraj, S. R. Rashmi, and M.V. Anand. *IDS based network security architecture with TCP/IP parameters using machine learning*. in *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*. 2018. IEEE.

.۳۰ Dwivedi, A. P. Tiwari, and S. Pandey, *TCP/IP: Security Issues & Solution.* International Journal of Scientific Research in Modern Science and Technology, 2022. 1(1): p. 50-56.

.۳۱ Mishra, A. S. Sharma, and A. Pandey. *A review on DDOS attack, TCP flood attack in cloud environment*. in *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*. 2020.

.۳۲ Alenezi, M. M. Nadeem, and R. Asif, *SQL injection attacks countermeasures assessments.* Indonesian Journal of Electrical Engineering and Computer Science, 2021. 21(2): p. 1121-1131.

.۳۳ Zhu, Z. et al. *SQL Injection Attack Detection Framework Based on HTTP Traffic*. in *ACM Turing Award Celebration Conference-China (ACM TURC 2021)*. 2021.

.۳۴ Dhanapal, A. and P. Nithyanandam, *The HTTP Flooding Attack Detection to Secure and Safeguard Online Applications in the Cloud* .International Journal of Information System Modeling and Design (IJISMD), 2019. 10(3): p. 41-58.

.۳۵ Schoenborn, J.M. and K.D. Althoff. *Detecting SQL-Injection and Cross-Site Scripting Attacks Using Case-Based Reasoning and SEASALT*. in *LWDA*. 2021.

.۳۶ Singh, T. and B. Aksanli. *Real-time traffic monitoring and SQL injection attack detection for edge networks*. in *Proceedings of the 15th ACM International Symposium on QoS and Security for Wireless and Mobile Networks*. 2019.

.۳۷ Cao, J. et al. *A survey on security aspects for LTE and LTE-A networks.* IEEE communications surveys & tutorials, 2013. 16(1): p. 283-302.

H۳۸ Suliaman, A.G. and Z.M.T. Alkattan, *Survey on Vulnerability of 4G/LTE Network Security and Improvements*. 2021.

.۳۹ Singh, U. et al. *A survey on LTE/LTE-A radio resource allocation techniques for machine-to-machine communication for B5G networks.* IEEE Access, 2021. 9: p. 107976-107997.

‘۴۰ Venkata Bhaskara Sastry, T. and P. Amritha, *Bluetooth Low Energy Devices: Attacks and Mitigations*, in *Advances in Electrical and Computer Technologies*. 2021, Springer. p. 381-389”

.۴۱ Daudov, I. M. Orobey, and I. Ignatev. *Bluetooth based technology for industrial personnel local positioning*. in *IOP Conference Series: Materials Science and Engineering*. 2 .۰۲۱IOP Publishing.

.۴۲ Cäsar, M. et al. *A survey on Bluetooth Low Energy security and privacy.* Computer Networks, 2022. 205: p. 108712.

.۴۳ Sun, J.Z. et al. *Design, implementation, and evaluation of Bluetooth security*, in *Wireless Lans And Home Networks: Connecting Offices and Homes*. 2001, World Scientific. p. 121-130.

.۴۴ Hegde, S.B. et al. *WPA2 Based Wireless Enterprise Configuration*. in *2021 IEEE International Conference on Mobile Networks and Wireless Communications (ICMNWC)*. 2021. IEEE.

.۴۵ Ahson, S.A. and M. Ilyas, *WiMAX: Standards and security*. 2018: CRC press.

.۴۶ Jarwan, A. et al. *LTE-based public safety networks: A survey.* IEEE communications surveys & tutorials, 2019. 21(2): p. 1165-1187.

.۴۷ Chow, M.C. and M. Ma, *A secure blockchain-based authentication and key agreement scheme for 3GPP 5G networks.* Sensors, 2022. 22(12): p. 4525.

.۴۸ Vali Mohamad, N.M. et al. *Development of an enhanced secured authentication and key agreement procedure for UMTS network.* Wireless Personal Communications, 2020. 110(1): p. 467-483.