دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۳، جلد ۲۲، شماره ۱ (۳۸-۶۰)
https://monadi.isc.org.ir

مروری بر روش‌های احراز اصالت لایه‌ی فیزیکی، معیارهای سنجش و حملات آن‌ها

پارسا رجبی[۱]، سید محمد رضوی‌زاده[۱،*]، و محمدحسام تدین[۲]

[۱] دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران، ایران
[۲] پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران

اطلاعات مقاله

تاریخچه مقاله:
تاریخ دریافت: ۱۱ فروردین ۱۴۰۳
تاریخ پذیرش: ۱۰ مرداد ۱۴۰۳
انتشار آنلاین: ۲۹ مرداد ۱۴۰۳

کلمات کلیدی:
احراز اصالت لایه‌ی فیزیکی
حملات لایه‌ی فیزیکی
رمزنگاری
معیارهای سنجش
ویژگی‌های فیزیکی

نوع مقاله: پژوهشی

چکیده

یکی از ابزارهای افزایش امنیت در شبکه‌های ارتباطی، احراز اصالت (یا همان احراز هویت) کاربران است که معمولاً در لایه‌ی کاربرد شبکه‌ها انجام می‌شود. اما در سال‌های اخیر، به منظور کاهش پیچیدگی و افزایش عملکرد، تمایل به سمت پیاده‌سازی این فرآیند در لایه‌های پایین‌تر شبکه در کنار روش‌های پیشین پدیدار شده است. یکی از راه‌حل‌های امیدوارکننده‌ی جدید، انجام فرآیند احراز اصالت در لایه‌ی فیزیکی است که در آن از ویژگی‌ها و نشانه‌های موجود در سیگنال‌های مبادله‌شده در این لایه برای احراز اصالت کاربران شبکه استفاده می‌شود. برخی از این ویژگی‌ها عبارتند از کانال ارتباطی، نویز، موقعیت و سرعت کاربران که این ویژگی‌ها به عنوان پارامترهایی همراه سیگنال استفاده می‌شوند. در این مقاله به مرور جامع روش‌های موجود در مقالات پیرامون احراز اصالت در لایه فیزیکی پرداخته می‌شود. در این رابطه علاوه بر دسته‌بندی روش‌های پیشنهادی در سال‌های اخیر، مقایسه‌ی آن‌ها با روش‌های موجود در سایر لایه‌ها نیز بررسی می‌شود. در ادامه یک معیار جدید برای دسته‌بندی بر مبنای میزان پنهانی برچسب هویتی در سیگنال مطرح می‌شود و همچنین حملات ممکن و راه‌های تشخیص و مقابله با آن‌ها بررسی می‌شود. در انتها نیز پیشنهادهایی برای پژوهش‌های بعدی در این حوزه ارائه می‌شود.

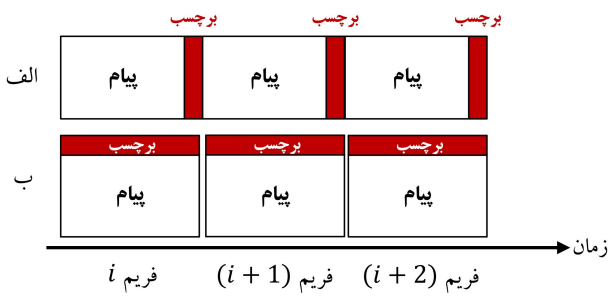
© ۱۴۰۳ انجمن رمز ایران

۱ مقدمه

یکی از ملزومات پایه‌ای امنیت سیستم‌ها، احراز اصالت است که می‌تواند از استفاده‌ی اشخاص ناشناس از سیستم جلوگیری کند. در واقع، احراز اصالت، بررسی درستی ادعای کاربری است که برای استفاده از یک سامانه، خود را معرفی می‌کند. برای احراز اصالت، می‌توان از روش‌های متفاوتی در لایه‌های مختلف استفاده کرد که یکی از آن‌ها روش‌هایی است که از لایه‌ی فیزیکی استفاده می‌کنند. در این روش‌ها، ویژگی‌های فیزیکی مانند کانال مخابراتی و یا خصوصیات سخت‌افزار مورد استفاده سنجیده می‌شود و با بهره‌گیری از این ویژگی‌ها، یک مشخصه‌ی هویتی برای آن کاربر ساخته می‌شود. این مشخصه مانند اثر انگشت[۱]، نشان‌دهنده‌ی هویت آن کاربر است. سپس این مشخصه‌ی هویتی در کنار سیگنالی که کاربر می‌خواهد ارسال کند همراه می‌شود تا طرف دیگر ارتباط بتواند با دیدن این مشخصه، به هویت فرستنده پی ببرد. به بیانی دیگر، سیگنالی که فرستنده ارسال می‌کند، از دو بخش تشکیل شده است: بخش داده‌ها که پیام[۲] نامیده می‌شود و بخش احراز اصالت که برچسب[۳] نام دارد. برای تخصیص منابع بین پیام و برچسب، محدودیت‌هایی مانند توان و تعداد برش‌های زمانی[۴] در نظر گرفته می‌شود که در ادامه توضیحاتی درباره‌ی آن آورده شده است. به عنوان نمونه، در شکل ۱، دو نوع از روش‌های

[1] Fingerprint [2] Message [3] Tag [4] Time slot

*نویسنده مسئول.
آدرس‌های رایانامه: parsarajabi1376@gmail.com (پارسا رجبی)، smrazavi@iust.ac.ir (سید محمد رضوی‌زاده)، tadayon@itrc.ac.ir (محمدحسام تدین)
© ۱۴۰۳ تمامی حقوق متعلق به انجمن رمز ایران است.



شکل ۱. سیگنال ارسالی متشکل از دو بخش پیام و برچسب هویتی

ارسال سیگنال داده به همراه برچسب نشان داده شده است که در (الف) پیام و برچسب در برش‌های زمانی مجزا ارسال شده‌اند و در (ب) پیام و برچسب هر دو همزمان با هم ارسال شده‌اند و ارتفاع مستطیلِ مربوط به پیام و برچسب، بیانگر توان اختصاص‌یافته به این دو بخش است.

در ادامه، ابتدا تاریخچه‌ای از احراز اصالت لایه‌ی فیزیکی ارائه می‌شود. پس از آن، مقدمه‌ای از احراز اصالت، کاربرد لایه‌ی فیزیکی برای این هدف و تفاوت‌ها با لایه‌های بالاتر گفته می‌شود و پس از آن به معرفی معیارهایی برای ارزیابی عملکرد، روش‌های احراز اصالت لایه‌ی فیزیکی و تقسیم‌بندی‌های متفاوت آن‌ها از دیدگاه‌های مختلف پرداخته می‌شود. سپس حملات و راه‌های تشخیص و مقابله با آن‌ها ارائه می‌شود. همچنین در انتها پیشنهادهایی برای پژوهش‌های بعدی در این حوزه، داده می‌شود.

۱.۱ مروری بر پژوهش‌های مرتبط

در حالی که همیشه تلاش برای بالا بردن سرعت انتقال اطلاعات در ارتباط بی‌سیم ادامه داشته است، مساله‌ی امنیت ارتباط امری ضروری بوده و همواره حملات جدیدی با هدف مختل کردن ارتباطات بی‌سیم انجام می‌شود. بخشی از این امنیت با استفاده از روش‌های رمزنگاری و در لایه‌های بالاتر انجام می‌شود، اما به عنوان مکملی برای برقراری امنیت، می‌توان از امنیت در لایه‌ی فیزیکی نیز استفاده کرد. زیرا به عنوان مثال، اگر شنودگری در لایه‌ی فیزیکی بتواند اطلاعات را شنود کند، احتمال آنکه پس از گذشت زمان بتواند رمز لایه‌های بالا را بشکند وجود دارد و یا گاهی برای تحلیل ترافیک شبکه و به دست آوردن مکان‌های پرتراکم، شنودگر حتی نیازی به رمزگشایی پیام‌های شنودشده نیز ندارد. روش‌هایی مانند نویز مصنوعی، شکل‌دهی امواج، استفاده از طیف گسترده و غیره ازجمله روش‌های امنیت لایه‌ی فیزیکی هستند که برای مقابله با شنود مطرح شده‌اند.

از طرف دیگر، گاهی کاربری غیرمجاز می‌خواهد که هویت خود را برای شبکه جعل کند و یا باعث اختلال در احراز اصالت کاربران مجاز شود. در این موارد، بحث دیگری راجع احراز اصالت در لایه‌ی فیزیکی به وجود می‌آید که می‌تواند در کنار لایه‌های دیگر، باعث امنیت بیشتر سامانه شود. در مرجع [۱]، احراز اصالت در سه دسته‌ی مبتنی بر رمزنگاری، مبتنی بر لایه‌ی فیزیکی و مبتنی بر چند لایه از شبکه بررسی شده است. لازم به ذکر است که تمرکز این مرجع، روی مخابرات وسایل نقلیه است. زیرا احراز اصالت لایه‌ی فیزیکی برای کاربران متحرک و ثابت، به دو مساله‌ی جداگانه منجر می‌شود، و یا به بیانی دیگر، احراز اصالت لایه‌ی فیزیکی، مبتنی بر ویژگی‌های فیزیکی است که در صورت حرکت کاربر، امکان تغییر ویژگی‌ها وجود دارد.

در ابتدا، اکثر روش‌های احراز اصالت لایه‌ی فیزیکی، تنها با استفاده از ویژگی‌های کانال مخابراتی و یا نقص سخت‌افزاری دستگاه‌ها مانند عدم دقت کلاک بود [۲]. اگر چه این نوع روش‌ها، یعنی استفاده از یک یا چند نشانه‌ی فیزیکی بدون هیچ پردازش و تغییری در آن‌ها، می‌تواند برای ارتباط موقت و در محیط ثابت مفید باشد، اما در حالتی که تنها از تعداد محدودی ویژگی‌های فیزیکی استفاده شود، بازدهی عملکرد در محیط متغیر با زمان کاهش می‌یابد و نیاز است تا از روش‌های دیگری مانند یادگیری ماشین برای تطبیق با تغییرات محیط استفاده کرد و یا ویژگی‌های فیزیکی را ترکیب کرد و یک نشانه‌ی هویتی دیگر به وجود آورد که دربرابر تغییرات محیط مقاوم باشد. بنابراین، در ادامه با گذشت زمان، از این ویژگی‌های فیزیکی استفاده شد و یک برچسب هویتی برای سیگنال ساخته شد.

در مرجع [۳] از لایه‌ی فیزیکی، برای احراز اصالت در سیستم‌های چندورودی–چندخروجی (MIMO [۱]) استفاده شده است و با اضافه کردن برچسب هویتی روی سیگنال داده عملیات احراز اصالت را انجام می‌دهد. در مرجع [۴] برای احراز اصالت در سیستم‌های MIMO، از تخمین کانال مخابراتی استفاده کرده است. در [۵] و [۶] این کار روی سیگنال مرجعی که برای هماهنگی بین فرستنده و گیرنده و تخمین کانال استفاده می‌شود و پایلوت [۲] نام دارد، انجام می‌شود و باعث می‌شود تا نرخ ارسال اطلاعات و توان ارسالی، نسبت به حالتی که برچسب هویتی روی سیگنال داده‌ها اضافه می‌شود بهتر باشد و دیگر نیازی به بازگرداندن سیگنال داده‌ها در گیرنده نباشد. در [۷]، از تغییرات زاویه‌ی برخورد (AoA [۳]) و زاویه‌ی خروج (AoD [۴]) استفاده شده است و برای سیستم‌های MIMO با در نظر گرفتن ویژگی فیزیکی چندمسیری [۵]، احراز اصالت را انجام می‌دهد.

در ادامه دیده می‌شود که پژوهش‌ها بر روی روش‌هایی برای پنهان کردن برچسب هویتی در سیگنال داده‌ها ادامه پیدا کرده است و برای تشخیص کاربر معتبر [۶]، از روش‌های یادگیری ماشین استفاده شده است. در [۸]، استفاده از روش‌های مختلف یادگیری ماشین برای احراز اصالت با استفاده از اطلاعات حالت کانال (CSI [۷])، بررسی شده است. در [۹]، چهار روش یادگیری بدون نظارت [۸] برای دسته‌بندی کاربران معتبر و مهاجمان بررسی شده است. همچنین در این مرجع، مساله برای چند مهاجم (نه لزوماً یک عدد) بررسی شده و برچسب هویتی، چندبعدی در نظر گرفته شده است. در مرجع [۱۰] برای محیط‌های پویا و متغیر با زمان که کاربران با سرعت‌های مختلفی حرکت می‌کنند، حالت کانال را

[1] Multiple-Input Multiple-Output [2] Pilot [3] Angle of Arrive [4] Angle of Departure [5] Multipath [6] Legitimate [7] Channel State Information [8] Unsupervised learning

در هر مرحله پیش‌بینی می‌کند. در مرجع [۱۱] با توجه به اینکه اندازه‌گیری کاربران معتبر در دسترس هست ولی اندازه‌گیری شنودگر در دسترس نیست، از یادگیری ماشین برای دسته‌بندی هویت کاربر استفاده کرده است. در مرجع [۱۲] از یادگیری برخط [1] استفاده کرده تا پایداری را در تغییرات محیط افزایش دهد و به جای انتخاب ویژگی‌های ثابت در همه‌ی زمان‌ها، انتخاب ویژگی‌ها را براساس تاثیر هر کدام انجام می‌دهد. در [۱۳] برای کاهش تأخیر و بار محاسباتی، هنگام دگرسپاری [2] در مخابرات سیار، از یادگیری انتقالی [3] استفاده کرده است. با توجه به اینکه احتمال حمله و فاش‌شدن کلید وجود دارد و یا نیاز است تا به تعداد زیادی کاربر خدمت‌رسانی شود، نیاز است تا نرخ تولید کلید را بالاتر برد، برای این کار می‌توان از روش‌هایی مانند صفحات هوشمند قابل تنظیم (RIS [4])، توابع فیزیکی تکثیرناپذیر (تفت) [5] و غیره استفاده کرد. این روش‌ها به ویژه در محیط‌هایی مناسب هستند که تغییرات ویژگی‌های فیزیکی زیاد نباشد و نتوان کلیدهای زیادی برای کاربران تولید کرد. در مراجع [۱۴] و [۱۵]، استفاده از RIS بررسی شده برای تولید کلید فیزیکی استفاده شده است و در مراجع [۱۶] و [۱۷] بالابردن نرخ تولید کلید فیزیکی با استفاده از تغییر کانال مخابراتی بررسی شده است. مرجع [۱۸]، همین مساله را از منظر مهاجم بررسی کرده و با تغییر ضرایب RIS، نرخ تولید کلید فیزیکی را کاهش می‌دهد. کاربرد دیگر RIS، در بالا بردن کنترل روی کانال مخابراتی و بیشتر کردن دقت سنجش ویژگی‌های فیزیکی است. زیرا در محیط نویزی بی‌سیم، ضرایب کانال بسیار متغیر است [۹] و سنجش آن نباید فاصله‌ی زمانی زیادی با استفاده از آن برای احراز اصالت داشته باشد تا اندازه‌گیری‌ها معتبر بماند. در مرجع [۱۹] نیز مروری جامع روی تولید کلید لایه‌ی فیزیکی انجام شده است و ارتباط آن با RIS و استفاده از آن برای MIMO بررسی شده و مراحل لازم برای تولید کلید فیزیکی نیز آورده شده است که در ادامه‌ی این مقاله نیز به آن اشاره‌ی مختصری می‌شود.

در مرجع [۲۰]، کاربردهای احراز اصالت لایه‌ی فیزیکی در نسل پنجم (5G) بررسی شده است و موضوعاتی که برای ادامه‌ی روند این پژوهش می‌تواند انجام شود، آورده شده است. در مرجع [۲۱] استفاده از RIS روی پهپاد بررسی شده است و از نظر امنیت لایه‌ی فیزیکی، آن را بررسی کرده است و توضیحاتی در مورد آسیب‌پذیری به حملات آورده شده است. همچنین در این مرجع، به نوعی از حمله به احراز اصالت لایه‌ی فیزیکی اشاره کرده است که در آن مهاجم، با تغییر ضرایب RIS، در فرآیند احراز اصالت اختلال ایجاد می‌کند. در مرجع [۲۲] نیز مساله‌ی احراز اصالت را در دو حالت تک‌پهپادی و دو پهپادی بررسی کرده است و کانال مخابراتی و موقعیت جغرافیایی را به عنوان ویژگی‌های فیزیکی انتخاب کرده است.

به عنوان کاربرد دیگر این نوع احراز اصالت در مخابرات، مرجع [۲۳] احراز اصالت لایه‌ی فیزیکی را در دسترسی چندگانه‌ی نامتعامد (NOMA [6]) بررسی کرده است. در این مرجع به دو دلیل احراز اصالت در NOMA پیشنهاد شده است. دلیل اول، امکان حمله در فضای باز بین فرستنده و گیرنده است و دلیل دوم، به این صورت بیان شده که با توجه به ارسال اطلاعات به چند کاربر از طریق NOMA، امکان تبانی برخی از کاربران با مهاجم و ایجاد اختلال در ارتباط هست. از طرف دیگر با توجه به تأخیر کمتر احراز اصالت در لایه‌ی فیزیکی و توانایی ایجاد لایه‌ی حفاظتی دیگری علاوه بر روش‌های احراز اصالت لایه‌های بالاتر، لایه‌ی فیزیکی را برای احراز اصالت در NOMA بررسی کرده است و سه طرح برای احراز هویت پیشنهاد داده است: طرح اول، احراز اصالت فیزیکی با برچسب هویتی مشابه [7] است که در آن برای تمامی کاربران از یک برچسب هویتی استفاده می‌کند. این طرح، دقت بالاتری از دو طرح دیگر دارد، اما امنیت آن کمتر است. طرح دوم، احراز اصالت فیزیکی با برچسب‌های هویتی مستقل تجمیعی [8] است که نسبت به طرح اول، نیاز به محاسبات بیشتری دارد ولی امنیت بالاتری دارد. طرح سوم، احراز اصالت فیزیکی با برچسب‌های هویتی جایگذاری‌شده در زمان‌های مختلف [9] است که باز هم نسبت به طرح اول نیازمند محاسبات بیشتری است اما امنیت بالاتری دارد. این طرح‌ها در مرجع [۲۴] نیز برای استفاده در دستگاه‌های بازپراکن [10] که محدودیت مصرف انرژی دارند، بررسی شده‌اند. مرجع [۲۵] نیز، الگوریتم رمزنگاری و رمزگشایی برای استفاده از احراز اصالت لایه‌ی فیزیکی در NOMA بررسی کرده است. در NOMA با توجه به اینکه سیگنال برای کاربران مختلفی همزمان ارسال می‌شود، نیاز است تا عدم تداخل برچسب‌های هویتی نیز بررسی شوند. از طرفی با توجه به اینکه کاربران به داده‌های دیگران دسترسی دارند، باید امنیت برچسب هویتی نیز بررسی شود. در ادامه در بخش معیارهای سنجش، در این مورد توضیحات بیشتری آورده شده است. از چالش‌های دیگری که برای استفاده از احراز اصالت فیزیکی در NOMA وجود دارد، تخمین مناسب کانال برای جلوگیری از تداخل برچسب‌های هویتی و تخصیص توان مناسب به آن‌ها است که می‌تواند به عواملی مانند فاصله‌ی کاربر، کیفیت کانال مخابراتی و یا نوع داده‌های ارسالی بستگی داشته باشد، به عنوان مثال داده‌های محرمانه برچسب هویتی متفاوتی از داده‌های معمولی نیاز دارند.

همچنین برای بالاتر بردن امنیت، می‌توان احراز اصالت لایه‌ی فیزیکی را با لایه‌های مختلف ترکیب کرد و از احراز اصالت چندلایه‌ای استفاده کرد [۲۶] و یا مشخصه‌ای جدید از این ویژگی‌ها ایجاد کرد که هنگام تغییر شرایط محیطی، ثابت بماند و بتوان هویت کاربر را با کمک آن تشخیص داد. از نظر حملات ممکن نیز، در [۲۷] برخی از حملات به لایه‌ی فیزیکی برای جعل هویت بررسی شده است، اما ارتباط آن با روش‌های متفاوت احراز اصالت لایه‌ی فیزیکی بررسی نشده است.

در ادامه‌ی این مقاله، مروری روی کارهای انجام‌شده در این حوزه آورده شده و روش‌های متفاوت احراز اصالت لایه‌ی فیزیکی از دیدگاه‌های متفاوتی تقسیم‌بندی شده‌اند و کاربرد و مزایا و معایب هر روش گفته شده است. تفاوت این مقاله با مرجع [۲۰] در این است که در این مرجع

[1] Online learning [2] Handover [3] Transfer learning [4] Reconfigurable Intelligent Surface [5] Physically Unclonable Functions (PUF) [6] Non-Orthogonal Multiple Access

[7] Shared tag [8] Superimposed independent tag [9] Time-division multiplexing tag [10] Backscatter devices

تمرکز بر روی استفاده از احراز هویت لایه‌ی فیزیکی برای نسل پنجم تلفن همراه است و مواردی مانند حملات ممکن و راه‌های تشخیص و مقابله با حملات بررسی نشده است. همچنین برای تقسیم‌بندی روش‌ها تنها از دو دسته‌ی ویژگی‌های سخت‌افزاری و کانال مخابراتی استفاده کرده است. اما در این مقاله سعی بر این بوده که دسته‌بندی روش‌ها کامل‌تر شود و معرفی جامعی از هر کدام از روش‌ها آورده شود. بنابراین روش‌های فعال و چالش و پاسخ نیز علاوه بر موارد ذکرشده در این مرجع، بررسی شده است. همچنین مقالات دیگری مانند مرجع [۱] دسته‌بندی برای احراز اصالت لایه‌ی فیزیکی ارائه داده‌اند که در این مقاله سعی شده تا این دسته‌بندی تکمیل شود و روش‌های متفاوت دیگری در این دسته‌بندی گنجانده شود که توضیحات بیشتر در این زمینه در بخش روش‌های گوناگون احراز اصالت لایه‌ی فیزیکی در ادامه‌ی این مقاله آورده شده است. در واقع در این مقاله سعی شده است که با توجه به گستردگی روش‌های متفاوت احراز اصالت لایه‌ی فیزیکی، دسته‌بندی روش‌ها به گونه‌ای باشد که روش‌هایی که اشتراک دارند در یک دسته باشند و از جدا کردن یک دسته برای هر حالت خاص پرهیز شود تا بتوان بررسی جامع‌تری روی روش‌های احراز اصالت لایه‌ی فیزیکی داشت و قواعد کلی‌تر و دقیق‌تری برای آن در نظر گرفت. همچنین تفاوت این مقاله با مراجع دیگری مانند [۲۸] و [۲]، در تقسیم‌بندی متفاوت روش‌های به کار رفته از نظر معیار پنهانی است. تفاوت‌های دیگری نیز در دسته‌بندی روش‌ها وجود دارد که در بخش روش‌های گوناگون احراز اصالت فیزیکی شرح داده شده است. همچنین معیارهایی که برای سنجش در مقالات مختلف استفاده شده‌اند، گردآوری شده و توضیحاتی در مورد آن‌ها ارائه شده است. با توجه به اینکه در مراجع دیده‌شده، مقاله‌ای که حملات به احراز اصالت در لایه‌ی فیزیکی را جمع‌آوری کرده باشد وجود ندارد، در این مقاله حملات ممکن و راه‌های تشخیص و مقابله با آن‌ها از مراجع مختلف جمع‌آوری و در کنار هم طبقه‌بندی شده‌اند تا بتوان دید بهتری از نقاط ضعف لایه‌ی فیزیکی برای احراز اصالت پیدا کرد و در آینده برای بهبود آن تلاش کرد.

۲.۱ احراز اصالت

در ارتباط مخابراتی گاهی نیاز است تا کاربران اثبات کنند که هویت معتبر دارند و مجاز به برقراری ارتباط هستند. برای این کار، باید دو مورد بررسی شود: احراز اصالت موجودیت [1]، احراز اصالت مبدأ داده [2].

در نوع اول، باید بررسی شود که فرد همانی است که ادعا می‌کند یا خیر. در حالی که مورد دوم، بررسی می‌کند که در این لحظه‌ی ارتباط، داده‌هایی که دریافت می‌شود از طرف همان فرد معتبر آمده یا از مبدأ دیگری فرستاده شده است. به عنوان مثال فرض کنید که آلیس می‌خواهد هویت خود را برای باب احراز کند. در این حالت، یک گواهی که نشان‌دهنده‌ی هویت خود باشد را برای باب می‌فرستد. حال باب این گواهی را نزد خود نگه می‌دارد و بعدا می‌خواهد از آن سوء استفاده کند و خود را به جای آلیس جا بزند. در این صورت می‌تواند گواهی ذخیره‌شده را برای شخص دیگری بفرستد. بنابراین در این حالت فقط احراز اصالت موجودیت بررسی شده و دیگر بررسی نمی‌شود که مبدأ داده چه کسی است. برای اینکه احراز اصالت کامل باشد، باید هر دو مورد بررسی شود. یعنی در مثال فوق، بررسی شود که کاربری که در آن لحظه دارد گواهی درستی را می‌فرستد، همان صاحب گواهی باشد نه اینکه فردی غیرمعتبر که فقط گواهی را به طریق نامعلومی به دست آورده و دارد از آن سوءاستفاده می‌کند [۲۹]. در بحث احراز اصالت لایه‌ی فیزیکی، می‌توان مورد اول یعنی موجودیت را به استفاده از ویژگی‌های مبتنی بر دستگاه و کلید هر کاربر ارتباط داد و مورد دوم یعنی مبدأ داده را به ویژگی‌های مبتنی بر کانال نسبت داد. زیرا ویژگی‌های مبتنی بر دستگاه برخواسته از خصوصیات سخت‌افزاری کاربر است در حالی که ویژگی‌های مبتنی بر کانال، نشان‌دهنده‌ی مواردی مانند موقعیت، جهت ارسال سیگنال توسط کاربر و شرایط محیطی کاربر است. جزئیات این روش‌ها در بخش‌های بعدی گفته می‌شود.

همچنین، می‌توان احراز اصالت را به دو نوع یک‌طرفه [3] و دوطرفه [4] تقسیم‌بندی کرد که در نوع یک‌طرفه، تنها یکی از طرف‌های ارتباط باید هویت خود را برای دیگری احراز کند، در حالی که در نوع دوطرفه، هر دو طرف ارتباط، باید هویت خود را برای طرف دیگر احراز کنند. به عنوان مثال، مرجع [۳۰] از احراز اصالت یک‌طرفه به وسیله‌ی RIS استفاده کرده و مراجع [۳۱]، [۳۲] و [۳۳] احراز اصالت دوطرفه با استفاده از کانال مخابراتی را بررسی کرده‌اند.

به طور کلی در حوزه‌ی امنیت، سه نوع کار می‌توان با ویژگی‌های فیزیکی انجام داد: امنیت لایه‌ی فیزیکی، تولید کلید فیزیکی، احراز اصالت لایه‌ی فیزیکی. هر کدام از این سه موضوع، محدودیت‌هایی دارند که در [۲۸] آمده است. به طور خلاصه امنیت لایه‌ی فیزیکی، استفاده از ویژگی‌های فیزیکی برای ارسال امن‌تر اطلاعات است. به عنوان نمونه، می‌توان از نویز مصنوعی، شکل‌دهی امواج، استفاده از طیف گسترده و غیره برای بالابردن امنیت ارسال اطلاعات استفاده کرد. اما در حوزه‌ی تولید کلید فیزیکی، هدف استخراج ویژگی‌های فیزیکی و تولید کلیدهای امن با نرخ بالا است. برای این‌کار، باید چهار مرحله را انجام داد: سنجش کانال، عددی‌کردن اندازه‌گیری‌ها [5]، اصلاح اطلاعات، بهبودبخشی به محرمانگی [۳۴]. در مرحله‌ی سنجش کانال، آلیس و باب با فرستادن سیگنال به یکدیگر، ویژگی‌های کانال را تخمین می‌زنند. سپس در مرحله‌ی عددی‌کردن، آن را با معیار مناسبی، با اعداد بیان می‌کنند. در قدم بعدی اطلاعات دریافتی را با توجه به بیت‌های توازن [6] و یا شماره‌ی بسته‌های دریافتی، اطلاعات دریافتی را که ممکن است به علت نویز، تداخل، خطای تخمین و غیره دچار خطا باشد، اصلاح می‌کنند. سپس در قدم آخر کلید را تغییراتی می‌دهند تا اگر شنودگری در میان راه توانسته باشد بخشی از اطلاعات را بفهمد، بی‌اثر شود [۱۵]. در مرجع [۱۹] نیز همین مراحل برای تولید کلید فیزیکی بررسی شده و در مورد استفاده از آن در MIMO و بکارگیری RIS برای تولید کلید فیزیکی توضیحاتی آورده شده است. با وجود این

[1] Entity Authentication (User Authentication) [2] Data Origin Authentication (Message Authentication)

[3] One-way [4] Two-way [5] Quantization [6] Parity bits

که تولید کلید فیزیکی در احراز اصالت لایه‌ی فیزیکی نیز کاربرد دارد، اما بررسی ارتباط این دو موضوع، هدف این مقاله نیست.

در این مقاله هدف بررسی احراز اصالت روی لایه‌ی فیزیکی است. احراز اصالت باعث بالابردن امنیت می‌شود و همچنین از کلیدهای فیزیکی استفاده می‌کند، اما در آن دیگر نحوه‌ی تولید کلید و یا تبادل کلید بررسی نمی‌شود و تمرکز روی مشخص کردن هویت کاربران معتبر و غیرمعتبر است.

۳.۱ تفاوت‌های استفاده از لایه‌ی فیزیکی با لایه‌های بالاتر در احراز اصالت

برای احراز اصالت می‌توان از روش‌ها و لایه‌های متفاوتی استفاده کرد. هر کدام مزایا و معایبی دارند که می‌توان بسته به نوع سامانه، از روش و لایه‌های مناسب استفاده کرد. احراز اصالت هرچه در لایه‌های نزدیکتر به لایه‌ی کاربرد [1] در شبکه انجام شود، استفاده از آن، ویژه‌ی یک برنامه‌ی خاص می‌شود، ولی اگر این کار در لایه‌ی فیزیکی انجام شود، برای تمامی داده‌های ارسالی از دستگاه، بدون در نظر گرفتن اینکه از طرف چه برنامه‌ای هستند، اعمال می‌شود. یعنی احراز اصالت روی کل داده‌های ارسالی که هر کدام می‌توانند برای کار و هدف متفاوتی باشند، انجام می‌گیرد. به عنوان مثال داده‌هایی که قرار است از طریق اینترنت ارسال شود، متشکل از پروتکل‌های متفاوت و یا حتی سایت‌های متفاوت است. همه‌ی این داده‌ها روی هم، در لایه‌ی فیزیکی می‌توانند به صورت یک بسته در نظر گرفته شود و احراز اصالت روی کل این بسته انجام گیرد. دلایل مختلفی که می‌تواند سازنده‌ی دستگاه را به سمت استفاده از احراز اصالت در لایه‌ی فیزیکی ببرد، عبارتند از:

اضافه شدن یک لایه‌ی حفاظتی دیگر: به طور کلی استفاده از لایه‌ی فیزیکی، یک لایه‌ی دیگر حفاظتی را به سیستم اضافه می‌کند. برخی مهاجم‌ها از طریق لایه‌ی کاربرد و یا لایه‌های دیگر غیر از لایه‌ی فیزیکی، حملات خود را انجام می‌دهند. با اضافه کردن احراز اصالت لایه‌ی فیزیکی، می‌توان به این نوع حملات مقاوم‌تر شد. به ویژه آنکه تشخیص ویژگی‌های فیزیکی مانند کانال مخابراتی کاربران، توسط مهاجم کار ساده‌ای نیست و حتی می‌توان تعداد ویژگی‌های فیزیکی مورد استفاده را بیشتر کرد تا امنیت بالاتر برود. همچنین در کاربردهایی که از احراز اصالت در لایه‌های بالاتر استفاده می‌شود، بخشی از بیت‌های پیام‌ها باید برای کاربرد امنیتی کنار گذاشته شوند، در نتیجه بخش مربوط به داده‌ها کمتر می‌شود. در این صورت اگر قرار باشد بخش امنیتی در پیام‌ها را کمترکرد و به جای آن بخش بیشتری برای داده‌ها گذاشت تا سرعت انتقال اطلاعات بالاتر رود، امنیت کمتر خواهد شد. در این حالت نیز می‌توان از لایه‌ی فیزیکی کمک گرفت [۳۵].

احراز اصالت تمامی داده‌های یک کاربر: لایه‌ی فیزیکی تمامی داده را احراز اصالت می‌کند و توجهی به اینکه داده‌ها از کدام برنامه‌ی لایه‌های بالاتر آمده‌اند ندارد. به عنوان مثال هنگام کار با اینترنت، در مرورگر یک صفحه برای کارهای بانکی باز است و یک صفحه هم برای بررسی اخبار روز باز هست. بخشی‌که برای کار بانکی است، نیاز به احراز اصالت دارد ولی مشاهده‌ی تارنمای خبری، نیازی به احراز اصالت ندارد. این کار در لایه‌ی کاربرد انجام می‌گیرد. به عنوان مثال کاربر با وارد کردن رمز و نام کاربری خود، احراز اصالت می‌شود. حال اگر قرار باشد که تمام داده‌های ارسالی از یک کاربر بدون در نظر گرفتن کاربرد آن، احراز اصالت شوند، در این صورت لایه‌ی فیزیکی، به کار می‌آید.

محاسبات ساده‌تر: معمولاً روش‌های رمزنگاری در لایه‌های بالا، محاسبات بیشتری نیاز دارند، در نتیجه سخت‌افزار بیشتری خواهند داشت. در حالی که در لایه‌ی فیزیکی، این‌کار با هزینه‌ی کمتری قابل انجام است. درکاربردهایی مانند ربات‌های کوچک و شبکه‌های نانو [2] در مهندسی پزشکی [۳۶]، وسایل مخابراتی که از انرژی بی‌سیم استفاده می‌کنند [۳۷]، ارتباط خودرو با همه‌چیز (V2X [3]) [۳۵]، که دستگاه قدرت پردازش بالایی ندارد، استفاده از لایه‌ی فیزیکی می‌تواند هزینه‌ی ساخت را پایین بیاورد. در [۳۷]، برای دستگاه‌هایی که از انرژی بی‌سیم استفاده می‌کنند، احراز اصالت لایه‌ی فیزیکی بررسی شده و علت آن را کمترکردن پیچیدگی، مصرف توان و بار محاسباتی بیان کرده است، به ویژه آنکه بخشی از فرآیند سنجش ویژگی‌های کانال، برای ارتباط بی‌سیم انجام می‌شود و می‌توان از آن اندازه‌گیری، برای احراز اصالت نیز استفاده کرد بدون اینکه نیاز به استفاده از محاسبات جدیدی برای رمزنگاری باشد.

تأخیر کمتر: برای دستگاه‌هایی که به تأخیر حساس هستند، نمی‌توان از روش‌های پیچیده‌ی رمزنگاری استفاده کرد، در این صورت نیز لایه‌ی فیزیکی، می‌تواند تأخیر کمتری از لایه‌های دیگر داشته باشد [۳۸]. زیرا بخشی از فرآیند، در حالت عادی در اکثر سیستم‌های مخابراتی انجام می‌شود (مانند سنجیدن کانال، تولید کلاک و غیره). در نتیجه بدون عملیات اضافه‌ای می‌توان از این بخش‌ها استفاده کرد و لایه‌ی حفاظتی دیگری اضافه‌کرد [۳۶].

احراز اصالت در تمامی لحظات: وقتی نیاز است که داده‌ها در تمام زمان ارتباط، احراز اصالت شوند، لایه‌ی فیزیکی نیز کاربرد خواهند داشت. به عنوان مثال اگر احراز اصالت تنها با نام کاربری و رمز عبور انجام شود، فقط در ابتدای ارتباط، احراز اصالت انجام می‌شود ولی در لایه‌ی فیزیکی، تمام زمان ارتباط، می‌توان بخش کوچکی از سیگنال را برای احراز اصالت اختصاص داد. این کار برای شبکه‌هایی مانند خودروهای هوشمند که دائما خودروهای همسایه‌ی آن‌ها در حال تغییر است، مناسب است. زیرا دیگر نیازی نیست هر بار نام کاربری و رمز فرستاده شود، در واقع در این حالت همیشه کنار داده‌ها، یک مشخصه‌ای برای احراز اصالت وجود دارد، مانند این است که داده‌ها همچون انسانی هستند که یک اثر انگشت دارند که آن را همه جا در اختیار دارند. در نتیجه احراز اصالت روی تمامی بیت‌های داده و تمامی لحظات ارتباط انجام

[1] Aplication layer

[2] Nano network

[3] Vehicle-to-Everything

می‌شود و اگر حتی حین ارتباط دستگاه دیگری خود را جایگزین دستگاه معتبر کند، گیرنده متوجه خواهد شد. در [۳۵] برای کم کردن پهنای باند اشغالی و پیام‌های کنترلی ارسالی در احراز اصالت خودروهای هوشمند، از ویژگی‌های فیزیکیِ توان سیگنال دریافتی، فاصله‌ی دو خودرو و سرعت نسبی دو خودرو، استفاده کرده و با استفاده از فیلتر کالمن [۱]، احراز اصالت را در شرایط محیطی متغیر با زمان انجام می‌دهد. در [۳۰] با استفاده از RIS، کانال مخابراتی را تحت کنترل قرار داده و با انتخاب المان صفحه و ترکیب تابع چکیده‌ساز [۲] با آن و سیگنال داده‌ها، در تمام زمان ارتباط کنار سیگنال داده، برچسب هویتی نیز فرستاده می‌شود. برای بهبود آن، می‌توان از روش پیشنهادی [۳۹] و [۱۱] استفاده کرد که به جای سیگنال داده، از پایلوت استفاده می‌کند تا نرخ انتقال اطلاعات، تحت تأثیر قرار نگیرد و نیازی به بازگردانی سیگنال بعد از جدا کردن برچسب نباشد.

نیاز شنودگر به SNR [۳] بیشتر: برای اینکه شنودگر بتواند عملیات شنود را انجام دهد، نیاز دارد تا سیگنال قوی‌تری از حالت عادی دریافت کند، زیرا بخشی که برای احراز اصالت استفاده می‌شود توان خیلی کمی از سیگنال را دارد و به صورت نویز دیده می‌شود و تشخیص آن راحت نخواهد بود [۲۸].

توانایی تشخیص دستگاه مورد استفاده‌ی کاربر و تعداد دستگاه‌های مورد استفاده: در این حالت حتی اگر کاربر در لایه‌های بالاتر بخواهد تعداد زیادی درخواست به شبکه بفرستد، همه‌ی این درخواست‌ها چون از یک دستگاه و یک موقعیت جغرافیایی ارسال می‌شوند، قابل تشخیص خواهند بود، حتی اگر کاربر بخواهد IP [۴] و یا MAC [۵] خود را جعل کند. همچنین اگر کاربر معتبر، بخواهد دستگاه خود را عوض کند قابل تشخیص است و در صورت لزوم می‌توان آن کاربر را مسدود کرد. در نتیجه می‌توان برای نوع و تعداد دستگاه‌های مورد استفاده‌ی یک کاربر معتبر محدودیت گذاشت [۲۸].

در انتها لازم به ذکر است که روش‌هایی که به کار گرفته می‌شود، بستگی به کاربردی دارد که از دستگاه مورد نظر انتظار می‌رود و تمامی روش‌های احراز اصالت می‌تواند به عنوان ابزار در جای مناسب، نقش مثبتی ایجاد کند و بنابر اهمیت و کاربرد، می‌توان هزینه‌های مختلفی کرد و در صورت لزوم حتی چندین لایه احراز اصالت در نظر گرفت.

۴.۱ معیارهای مورد استفاده

به طور کلی سه مورد در طراحی سامانه‌های احراز اصالت لایه‌ی فیزیکی باید در نظر گرفت [۲۸]:

امنیت [۶]: نشان‌دهنده‌ی میزان سختی تخمین برچسب سیگنال برای شنودگر است. برای آن معیار های متفاوتی مانند ابهام کلید [۷]، حداقل آنتروپی [۸] و توانایی تمایز برچسب از پیام توسط شنودگر [۹] می‌توان در نظر گرفت. ابهام کلید، نشان‌دهنده‌ی عدم قطعیت بعد از مشاهده‌ی متن رمزشده هست. ابهام کلید، معیاری است که میانگین را نشان می‌دهد. در صورتی که هدف به دست آوردن بیشترین احتمالی باشد که شنودگر می‌تواند کلید را درست حدس بزند، می‌توان از معیار حداقل آنتروپی استفاده کرد. همچنین برای اینکه شنودگر بتواند عملیات خود را بهتر انجام دهد، باید بتواند برچسب را از پیام جدا کند که این جدایی‌ناپذیری برچسب از داده‌ها، نیز می‌تواند برای سنجش امنیت به کار رود. در مقالات مختلف، معیارهای فوق را برای بررسی امنیت استفاده می‌کنند. به عنوان مثال در مرجع [۲۵] الگوریتم‌هایی برای رمزنگاری و رمزگشایی در احراز اصالت فیزیکی معرفی شده و بهبود امنیت از نظر ابهام کلید بررسی شده است.

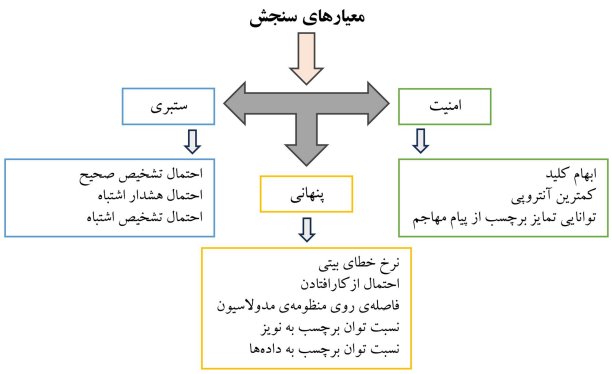
ستبری [۱۰]: نشان‌دهنده‌ی قابلیت مقابله با تغییر شرایط محیطی است. برای این بخش، می‌توان معیارهایی مانند احتمال تشخیص [۱۱]، احتمال هشدار اشتباه [۱۲]، احتمال تشخیص اشتباه [۱۳] را در نظر گرفت. به عنوان مثال در مرجع [۲۳] از ستبری برای بررسی مقاوم بودن نسبت به تداخل کاربران مختلف در NOMA استفاده کرده است و احتمال تشخیص صحیح و احتمال هشدار اشتباه را مشابه با مراجع [۲۴] و [۲۵] به دست آورده است. مراجع [۴۰] و [۲۲] نیز، احتمال تشخیص صحیح و هشدار اشتباه را برای ستبری در ارتباط پهپاد بررسی کرده است.

پنهانی سیگنال احراز اصالت در سیگنال داده [۱۴]: نشان‌دهنده‌ی میزان پنهان بودن برچسب نسبت به بخش داده‌ها است. یعنی هدف این است که تا حد امکان شنودگر متوجه نشود که اصلا بخشی برای احراز اصالت به سیگنال اضافه شده و تصور کند که همان نویز محیط است. برای این بخش، می‌توان از معیارهایی مانند فاصله‌ی اقلیدوسی در منظومه‌ی مدولاسیون، احتمال ازکارافتادن (احتمال قطع‌شدن) [۱۵]، نرخ بیت‌های خطا (BER [۱۶])، نسبت توان برچسب به توان سیگنال [۱۷] استفاده کرد. فاصله‌ی اقلیدوسی در منظومه‌ی مدولاسیون، نشان‌دهنده‌ی میزان سختی تشخیص برچسب اضافه‌شده به سمبل ارسالی است. احتمال ازکار افتادن، از این جهت کارایی دارد که اگر پنهانی برچسب هویتی از حدی بیشتر باشد، از فاصله‌ای دورتر نمی‌توان دیگر ارتباط برقرار کرد، زیرا SNR کمتری دریافت می‌شود. نرخ بیت‌های خطا، بیانگر این است که هر چقدر پنهان بودن برچسب در سیگنال بیشتر باشد، امکان دریافت خطا به علت نویز بیشتر می‌شود. نسبت توان برچسب به سیگنال نیز بیانگر این است که برچسب چه میزان قابل تشخیص برای شنودگر هست. بسته به نوع و کاربرد سیستم، می‌توان از معیارهای فوق برای بررسی پنهانی استفاده کرد. به عنوان نمونه، در مرجع [۲۴] از احتمال قطع‌شدن ارتباط، در مرجع [۴۱] از فاصله‌ی سمبل‌های برچسب در منظومه‌ی مدولاسیون و در [۳] از BER برای بررسی پنهانی استفاده شده است.

بنابراین معیارهای متفاوتی را می‌توان در قالب این سه دسته بررسی‌کرد. همچنین لازم به ذکر است که این معیارها لزوما در یک جهت عمل نمی‌کنند

[1] Kalman Filter [2] Hash function [3] Signal-to-Noise Ratio [4] Internet Protocol [5] Media Access Control [6] Security [7] Key equivocation [8] Min-entropy [9] Eve's distinguishing capability

[10] Robustness [11] Probability of detection [12] Probability of false alarm [13] Probability of missed detection [14] Covertness [15] Outage probability [16] Bit Error Rate [17] Tag-to-signal ratio



شکل ۲. معیارهای سنجش و مثال‌هایی از هر کدام

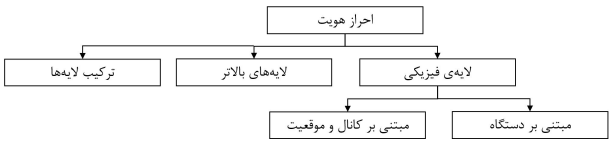
و باید مصالحه‌ای بین این سه معیار برقرارکرد [۴۲]. به عنوان مثال، هرچه برچسب پنهان‌تر باشد، ستبری کاهش می‌یابد زیرا تاثیرات نویز روی برچسب شدیدتر اثر می‌گذارد. از طرفی این پنهان‌تر بودن برچسب، باعث امنیت بیشتر می‌شود، زیرا شنودگر از ابتدا سخت‌تر می‌تواند برچسب را بیابد تا اینکه بخواهد بعدا آن را کدگشایی و تفسیر کند. بنابراین با توجه به نیاز سیستم، می‌توان این مصالحه را بین موارد فوق برقرار کرد.

شکل ۲، خلاصه‌ای از موارد فوق را نشان می‌دهد. همچنین باید دقت کرد که امنیت با پنهانی متفاوت است. امنیت یعنی اگر شنودگر برچسب هویتی را شنود کرد، نتواند آن را بفهمد، اما پنهانی یعنی اینکه از ابتدا شنودگر نفهمد که در سیگنال، بخشی به عنوان برچسب هویتی وجود دارد. در ادامه، روش‌های متفاوتی که برای احراز اصالت استفاده می‌شوند بررسی می‌شود و معیاری برای سنجش ترکیبی سه عامل فوق، گفته می‌شود.

۲ روش‌های گوناگون احراز اصالت لایه‌ی فیزیکی

برای استفاده از ویژگی‌های فیزیکی، می‌توان روش‌های متفاوتی را به کار برد. شکل ۳، دسته‌بندی قدیمی این روش‌ها طبق ویژگی‌های مورد استفاده و جایگاه آن در مقایسه با احراز اصالت در لایه‌های دیگر را نشان داده است. طبق این دسته‌بندی که مشابه مراجع [۲۰] و [۴۳] است، می‌توان روش‌های احراز اصالت لایه‌ی فیزیکی را با استفاده از ویژگی‌های سخت‌افزار مورد استفاده و کانال مخابراتی بین دو کاربر و یا موقعیت مکانی کاربران انجام داد. همچنین طبق شکل ۳ روش‌های دیگر احراز اصالت در لایه‌های بالاتر را می‌توان با لایه‌ی فیزیکی نیز ترکیب کرد.

در مرجع [۱] نیز در این زمینه یک طبقه‌بندی ارائه شده است که مشابه با شکل ۳ است، با این تفاوت که احراز اصالت لایه‌ی فیزیکی را به سه بخش احراز اصالت بدون کلید، مبتنی بر کلید و مبتنی بر برچسب هویتی تقسیم‌بندی کرده است که طبق این نوع دسته‌بندی، این ایراد به وجود می‌آید که با توجه به اینکه روش‌های مبتنی بر برچسب هویتی از کلید استفاده می‌کنند، به جدا کردن این دو دسته نیازی نیست. از طرفی دیگر روش‌هایی مانند چالش و پاسخ لزوما مبتنی بر کلید نیستند و به ویژگی‌های کانال نیز بستگی دارند.

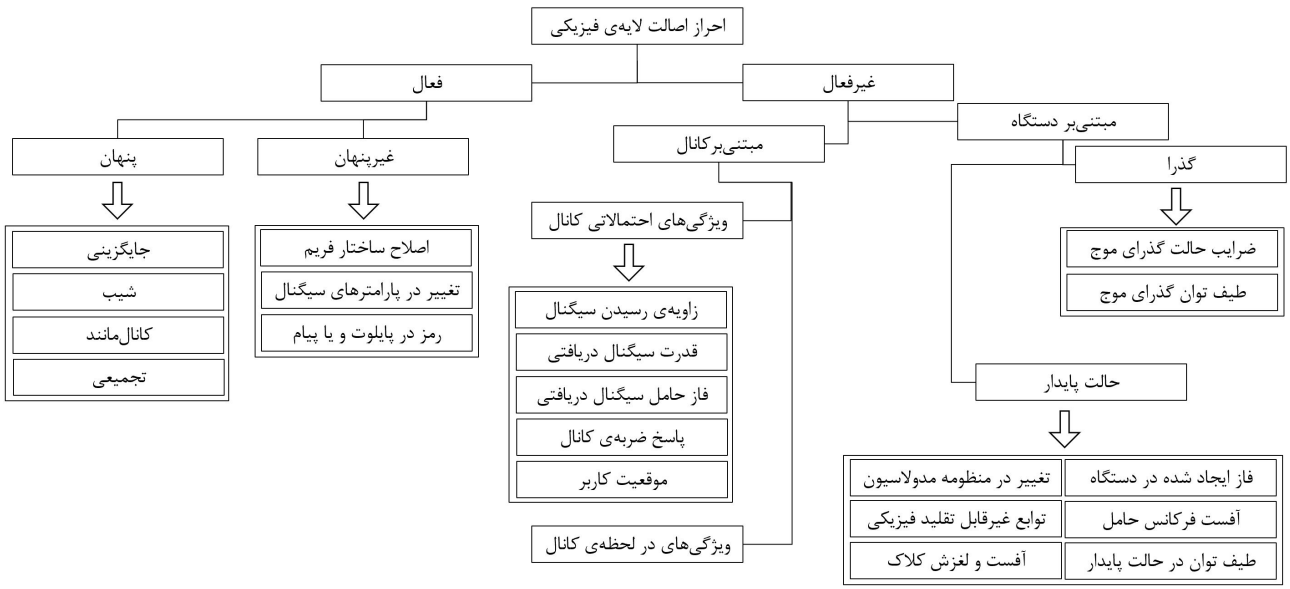


شکل ۳. تقسیم‌بندی روش‌های احراز اصالت

دسته‌بندی کامل‌تر از شکل ۳، در شکل ۴ آورده شده است. طبق شکل ۴، می‌توان احراز اصالت لایه‌ی فیزیکی را در دو دسته‌ی فعال [1] و غیرفعال [2] بررسی‌کرد. تفاوت اصلی روش‌های فعال و غیرفعال، اضافه‌کردن برچسب هویتی به سیگنال است. به عنوان مثال در روش‌های غیرفعال از ویژگی‌های سیگنال ارسالی و یا تنظیم پارامترهایی مانند فرکانس، فاز و غیره احراز اصالت انجام می‌شود ولی در روش‌های فعال فرستنده باید محاسباتی انجام دهد و یک برچسب ایجاد نماید و آن را به سیگنال اضافه کند. همچنین گیرنده نیز باید دوباره با محاسبات جدیدی، درستی این برچسب را بررسی‌کند. روش‌های غیرفعال، را می‌توان در دو نوع مبتنی بر دستگاه و مبتنی بر کانال و موقعیت بستگی کرد ولی روش‌های فعال، در دو دسته‌ی پنهان و غیرپنهان دسته‌بندی می‌شود.

برخلاف مرجع [۲۸] که روش‌هایی تحت عنوان روش‌های توسعه‌یافته در زیرمجموعه‌ی روش‌های غیرفعال آورده، و آن را به سه دسته‌ی روش‌های ترکیبی، یادگیری ماشین و نویز مصنوعی تقسیم کرده است، در این مقاله روش‌های غیرفعال تنها در دو دسته‌ی مبتنی بر کانال و دستگاه تقسیم‌بندی شده‌اند و استفاده از نویز مصنوعی در دسته‌ی روش‌های فعال قرار می‌گیرد، زیرا در این روش از ویژگی‌های کانال و دستگاه استفاده می‌شود و بخشی جدید به سیگنال اضافه می‌شود. بنابراین نمی‌تواند که روشی غیرفعال باشد. همچنین استفاده از یادگیری ماشین نیز می‌تواند به عنوان ابزاری برای هر کدام از روش‌ها مورد استفاده قرارگیرد. بنابراین نیازی به ایجاد دسته‌بندی جداگانه‌ای برای این روش وجود ندارد و اضافه کردن آن، تنها باعث می‌شود تا دسته‌بندی پیچیده‌تر شود. تفاوت دیگری که با این مرجع وجود دارد، در دسته‌بندی روش‌های ترکیبی [3] است. در این مرجع، روش‌های ترکیبی به عنوان روشی غیرفعال در نظر گرفته شده و ترکیبی از روش‌های مبتنی بر کانال و دستگاه معرفی شده است. در حالی که برخلاف این مرجع، در این مقاله سعی بر این بوده که دسته‌بندی بر اساس تفاوت‌های ذاتی روش‌ها باشد و دسته‌بندی در حداقل گروه‌های ممکن صورت گیرد تا بتوان با دیدی کلی همه‌ی روش‌ها را بررسی کرد و از بررسی به صورت حالت‌های خاص فراوان اجتناب کرد. بنابراین روش‌هایی که هم از ویژگی‌های کانال و هم از ویژگی‌های دستگاه استفاده می‌کنند، نیازی به دسته‌بندی جدا ندارند و می‌توانند در همان قالب بررسی شوند. از طرف دیگر در این مقاله، عنوان روش‌های ترکیبی، برای روش‌هایی به کار رفته که ترکیبی از روش‌های فعال و غیرفعال باشند، نه اینکه ترکیبی از روش‌های مبتنی بر کانال و دستگاه باشند. توضیحات بیشتر در این زمینه، در بخش روش‌های ترکیبی در ادامه گفته می‌شود. لازم به ذکر است که روش‌های ترکیبی (ترکیب روش‌های فعال و غیرفعال) در دسته‌بندی

[1] Active [2] Passive [3] Hybrid



شکل ۴. روش‌های متفاوت احراز اصالت لایه‌ی فیزیکی و مثال‌هایی از هر کدام

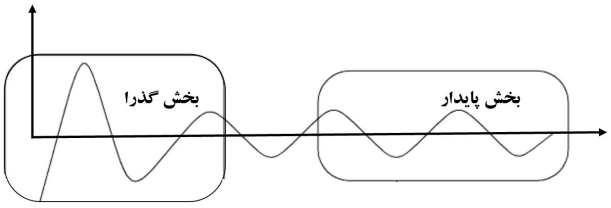
قرار نمی‌گیرند و در انتهای این مقاله به عنوان کاربردی برای موازنه‌ی بین معیارهای سنجش به صورت جداگانه شرح داده می‌شود.

دقت شود که از بین سه معیار سنجش گفته شده در بخش قبل، تنها معیار امنیت و ستبری برای روش‌های غیرفعال بررسی می‌شود ولی برای روش‌های فعال، هر سه مورد این معیارها بررسی می‌شود [۲۸]. علت اینکه معیار پنهان بودن برای روش‌های غیرفعال بررسی نمی‌شود، این است که روش‌های غیرفعال، کاملا پنهان هستند چون هیچ بخش جدیدی به سیگنال اضافه نمی‌شود که بخواهد غیرپنهان باشد.

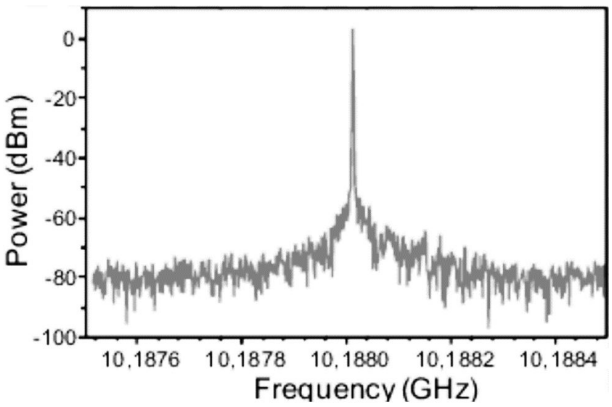
در ادامه، هر کدام از این بخش‌ها با جزئیات بیشتری بررسی خواهد شد و روش‌ها بر اساس میزان پنهانی، دسته‌بندی جدیدی خواهد شد. در انتها روش‌های ترکیبی بررسی می‌شود تا از مزایای هر دو روش فعال و غیرفعال بهره برد و معایب را نیز کاهش داد. همچنین برای این روش‌های ترکیبی، می‌توان از معیار سنجشی استفاده کرد که ترکیبی از سه معیار اصلی گفته شده است که در ادامه توضیحات آن آورده می‌شود.

۱.۲ روش‌های غیرفعال

این روش‌ها بسته به اینکه از چه نوع ویژگی استفاده می‌کنند، در دو دسته‌ی مبتنی بر دستگاه و مبتنی بر کانال قرار می‌گیرند. روش‌های مبتنی بر دستگاه از ویژگی‌هایی استفاده می‌کنند که به علت سخت افزار موجود در دستگاه و یا عدم دقت آن، به وجود آمده است. مثلاً یک اسیلاتور با فرکانس نامی مشخص، به دلایلی مانند نویز، عدم دقت در ساخت، شرایط محیطی و غیره نمی‌تواند دقیقاً همان فرکانس را تولید کند و مقداری خطا دارد. این خطا را می توان به عنوان یک ویژگی مبتنی بر دستگاه برای احراز اصالت استفاده کرد. ویژگی های مبتنی بر دستگاه را می‌توان دو



شکل ۵. بخش‌های پایدار و گذرای سیگنال



شکل ۶. طیف توان سیگنال ارسالی یک دستگاه، می‌تواند به عنوان برچسب هویتی در نظر گرفته شود.

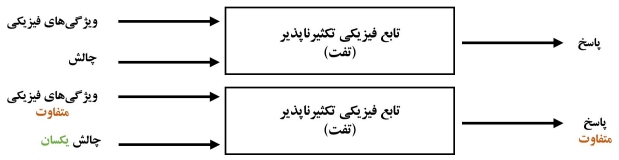
نوع در نظر گرفت. دسته ی اول، ویژگی های گذرا [1] هستند و دسته‌ی دوم ویژگی‌هایی هستند که در حالت پایدار [2] مشاهده می شود که در شکل ۵ نشان داده شده است. برای حالت گذرا می‌توان پارامترهایی مانند میرایی موج را بررسی کرد و یا مانند شکل ۶ طیف توانی را در نظر گرفت که در حالت گذرا به وجود می‌آید. همچنین در حالت پایدار مواردی مانند آفست فاز و فرکانس، تغییرات در منظومه‌ی مدولاسیون و غیره را در نظر گرفت.

[1] Transient [2] Steady state

ویژگی‌های مبتنی بر دستگاه، چالش‌هایی ایجاد می‌کنند. سنجش این ویژگی‌ها نیاز به سخت‌افزار اضافه‌ای دارد. همچنین در صورتی که شنودگر بتواند برچسب را تشخیص دهد و بیابد، دستگاه باید بتواند برچسب هویتی را عوض کند، ولی از طرفی تعویض برچسب برای این دسته دشوار خواهد بود. زیرا نمی‌توان ویژگی‌هایی که صرفا ناشی از نقص و عدم دقت سخت‌افزاری هستند را بدون تغییر سخت‌افزار عوض کرد. همچنین این ویژگی‌ها برای محیط های ثابت قابل استفاده هستند [۴۴]. زیرا در محیط های متحرک، با تغییر شرایط محیطی، عملکرد سخت‌افزارها نیز تغییر می‌کند. مثلاً مدارهای مجتمع در زیر نور خورشید و یا در زیر سایه، نویز متفاوتی دارند و این مساله کار را برای یافتن برچسب هویتی مناسب دشوار می‌کند. همچنین در این دسته ویژگی‌هایی هستند که ناشی از مشابه نبودن کلاک‌های ساخته‌شده در هر دستگاهی هست. این ویژگی‌ها مزیتی که دارند در فرستنده نیازی به تجهیزات اضافه‌تر ندارند ولی در عین حال این ایراد را دارند که در گیرنده نیاز است تا تجهیزاتی برای سنجش تفاوت کلاک در نظر گرفته شود [۴۳]. به عنوان مثال باید براساس یک کلاک با فرکانس بالاتری سنجیده‌شوند و یا از لایه‌های بالاتر استفاده کرد. به عنوان مثال از مهر زمانی [1] در پروتکل‌های TCP [2] و ICMP [3] استفاده کرد [۲۸]. نقطه‌ی ضعف دیگر این دسته، توانایی شنودگر برای تقلید این ویژگی‌ها است. زیرا شنودگر نیز می‌تواند طیف توان و کلاک و غیره را بسنجد. بنابراین این دسته فقط برای ارتباط های موقت مناسب خواهد بود که شنودگر زمان زیادی برای عملیات خود نداشته باشد. ایراد دیگر این دسته، عدم کنترل روی نرخ تولید کلید و تعویض کلید است که با توجه به منشأ سخت‌افزاری این روش، عوض کردن کلید و بالابردن نرخ تولید آن در ارتباط های دائمی عملا غیرممکن خواهد بود. با توجه به دلایل گفته‌شده به خصوص عدم کنترل روی تولید کلید، برای ارتباط های دائمی تلاش بر استفاده از روش‌های فعال خواهد بود که جلوتر توضیح داده می‌شود. در واقع با استفاده از روش‌های فعال می‌توان تغییراتی عمدی در منظومه‌ی مدولاسیون به وجود آورد و مانند نویزی عمدی سمبل ارسالی را در منظومه‌ی مدولاسیون جابه‌جا کرد و این تغییرعمدی، قابل کنترل خواهد بود و دیگر نیازی به استفاده از نقص و عدم دقت سخت‌افزاری نیست، اما باید توجه داشت که این تغییر عمدی، محدودیت‌هایی دارد تا از تشخیص برچسب هویتی توسط شنودگر، جلوگیری شود [۴۱].

راه دیگر، استفاده از ویژگی‌های مبتنی بر کانال است که براساس تفاوت کانال مخابراتی کاربران مختلف انجام می‌شود. بنابراین برای سامانه‌هایی مناسب است که کاربران با فاصله از یکدیگر باشند. مزیتی که استفاده از این روش دارد، توانایی شناسایی مکان تقریبی مهاجم است. زیرا می‌توان از ویژگی‌های اندازه‌گیری شده مانند توان سیگنال دریافتی و یا زاویه‌ی رسیدن سیگنال، فاصله‌ی تقریبی کاربری که غیرمجاز تشخیص داده شده را به دست آورد. از ویژگی‌های دیگری که می‌توان استفاده کرد، سرعت متحرک، فرکانس داپلر، پاسخ فرکانسی کانال و غیره است. به عنوان مثال‌هایی از این دسته، مرجع [۴] از تخمین کانال برای احراز اصالت در

[1] Time stamp [2] Transmission Control Protocol [3] Internet Control Message Protocol

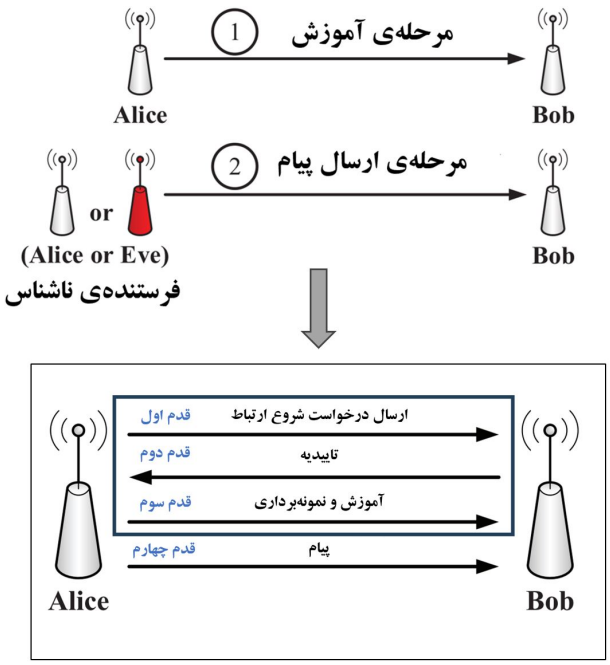


شکل ۷. تغییر پاسخ تفت با تغییر ویژگی‌های فیزیکی

سیستم‌های MIMO مبتنی بر پهپاد و مرجع [۴۵] از SNR برای احراز کردن هویت کاربران زمینی در پهپاد استفاده کرده است. همچنین مرجع [۲۲] از تفاوت SNR دریافتی و توجه به موقعیت و مختصات روی صفحه‌ی افقی، برای احراز اصالت کاربرانِ روی زمین استفاده کرده است. در [۴۶] از فرکانس داپلر و توان سیگنال دریافتی استفاده کرده و احراز اصالت ماهواره‌ها را بررسی کرده است. همچنین یکی از راه‌های تشخیص فریب در موقعیت‌یابی GPS [4] نیز توجه به SNR دریافتی و مقایسه‌ی آن با حالت‌های مختلف در محیط است. به عنوان مثال زیر درختان، در تونل‌ها، بین ساختمان‌های بلند و یا در مکان‌های روباز، مقادیر SNR ماهواره‌های GPS تغییراتی دارند که می‌توان از آن برای تشخیص فریب نیز استفاده کرد. برای امنیت بیشتر، می‌توان از هر دو نوع ویژگی‌های مبتنی بر کانال و مبتنی بر دستگاه استفاده کرد تا اگر مهاجمی از نوع سخت‌افزار مطلع بود یا از کانال مخابراتی مطلع بود، نتواند حمله انجام دهد. مرجع [۴۷] از CFO [5] علاوه بر CSI [6] استفاده کرده است تا بتواند عملکرد احراز هویت را بهبود دهد. همچنین موقعیت کاربر نیز می‌تواند در بسیاری از کاربردها راهگشا باشد. به عنوان مثال حداکثر سرعت یک کاربر تلفن همراه، در خودرو ممکن است در آزادراه‌ها رخ‌دهد، اما وقتی مشاهده شود که ناگهان موقعیت کاربر تغییر شدیدی کرده که از حداکثر سرعت آن بیشتر بوده، می‌توان پی‌برد که این کاربر قصد جعل موقعیت خود را دارد. در حالت‌هایی دیگر، می‌توان از روی تغییرات آرام توان سیگنال دریافتی، معتبر بودن کاربر را تشخیص داد. در واقع اگر مهاجمی بخواهد از محلی دیگر خود را به جای آن کاربر جا بزند، توان سیگنال دریافتی از مهاجم، متفاوت از کاربر معتبر خواهد بود. مرجع [۱۰] نیز از روش‌های یادگیری برای تخمین CSI استفاده کرده است تا بتواند احراز اصالت را در محیط متغیر با زمان پیاده‌سازی کند.

روش دیگری که می‌تواند در کنار این روش‌های غیرفعال استفاده شود، استفاده از تفت است. این توابع، تنها زمانی خروجی یکسانی خواهند داشت که هم ورودی تابع و هم خود تابع در هر دو حالت یکسان باشند. در غیر این صورت، خروجی متفاوت خواهد بود. این توابع مبتنی بر مشخصه‌های فیزیکی سخت‌افزار مانند دما، تأخیر، موقعیت و غیره هستند. شکل ۷ شمای این توابع را در کاربرد احراز اصالت نشان می‌دهد. مطابق شکل ۷، دستگاه غیرمعتبر تنها در صورتی می‌تواند پاسخ چالش را صحیح بدهد که ویژگی‌های فیزیکی کاربر معتبر را داشته باشد، به بیانی دیگر اگر یک دستگاه غیرمعتبر باشد، ویژگی‌های فیزیکی متفاوتی خواهد داشت، بنابراین برای چالشی که باید پاسخ دهد، نمی‌تواند پاسخ صحیح را بیابد، در نتیجه می‌توان متوجه شد که کاربر غیرمعتبر است.

[4] Global Positioning System [5] Carrier Frequency Offset [6] Channel State Information



شکل ۸. مراحل احراز اصالت غیرفعال [۲۸] (قدم ۱ تا ۳ برای مرحله‌ی آموزش و قدم ۴ برای مرحله‌ی ارسال پیام است [۲])

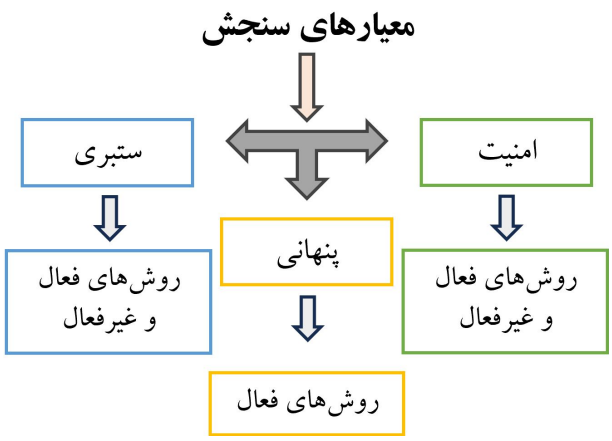
برای کاربردهایی مانند ارتباط پهپادهای ثابت در هوا که ویژگی‌های فیزیکی تغییرات زیادی نمی‌کنند، برای بیشتر کردن نرخ تولید کلید می‌توان از تفت استفاده کرد [۴۸]. روش دیگر، استفاده از روش‌های فعال خواهد بود که در ادامه توضیح داده شده است.

مراحلی که برای روش‌های غیرفعال استفاده می‌شود (شکل ۸)، از دو مرحله‌ی آموزش [1] و ارسال پیام [2] تشکیل شده است. خود مرحله‌ی آموزش نیز از سه قدم تشکیل شده است که در [۲] آمده است.

به طور خلاصه، در مرحله‌ی آموزش، ابتدا آلیس درخواست خود را برای باب ارسال کرده، باب برای آلیس تأییدیه‌ی درخواست را می‌فرستد. سپس آلیس سیگنال آموزشی را برای باب می‌فرستد. احراز اصالت در این مرحله با لایه‌های بالاتر انجام می‌شود [۲۸]. یعنی اگر هویت درست بود، داده‌ها به عنوان داده‌های هویت صحیح و اگر هویت احراز نشد، به عنوان داده‌های مهاجم ذخیره می‌شود.

در مرحله‌ی دوم، آلیس پیام را برای باب می‌فرستد. در این قدم آخر، احراز اصالت بر اساس لایه‌ی فیزیکی انجام می‌شود، یعنی باب ویژگی‌های فیزیکی سیگنال پیام را به دست می‌آورد و با ویژگی‌هایی که قبلا در دیتاست خود ذخیره کرده، مقایسه می‌کند. منظور از مقایسه، می‌تواند موارد مختلفی باشد، به عنوان مثال تساوی تقریبی ویژگی‌ها، پیوستگی (در کاربران متحرک)، بررسی تاثیرات محیط (دما، نویز، تغییر زاویه‌ی RIS) و پیش‌بینی حالت جدید ویژگی‌ها با توجه به‌ویژگی‌های قبلی می‌تواند به عنوان معیار مقایسه انتخاب شوند.

[1]Training stage [2]Message–transmission stage



شکل ۹. کاربرد معیارهای سنجش در روش‌های فعال و غیرفعال

۲.۲ روش‌های فعال

روش‌های فعال را در دو دسته‌ی غیرپنهان و پنهان می‌توان بررسی‌کرد. در روش‌های غیرپنهان، برچسب هویتی، با تمام توان در بخشی از برش‌های زمانی سیگنال قرارداده می‌شود. در نتیجه شنودگر می‌تواند به راحتی برچسب را تشخیص دهد. از طرفی با توجه به اینکه همواره بخشی‌از توان برای برچسب استفاده می‌شود، گذردهی داده‌ها و سرعت ارتباط کمتر می‌شود. همچنین گاهی از روش‌های طیف گسترده و پرش فرکانسی استفاده می‌شود که این روش‌ها نیز باعث اشغال پهنای باند می‌شود.

برای رفع این مشکلات، روش‌های پنهان درست شده‌اند. در روش‌های پنهان، برچسب سیگنال با توان کمتری ارسال می‌شود و یا حتی به حدی توان پایین خواهد بود که از دید ناظر بیرونی، شبیه نویز خواهد بود. بنابراین مزیت روش‌های پنهان، سرعت ارتباط بالاتر و امنیت بیشتر و پنهانی از شنودگر خواهد بود اما در عوض ستبری، کمتر می‌شود. زیرا اگر نویز محیط و یا فاصله‌ی فرستنده و گیرنده، از حدی بیشتر شود، گیرنده نمی‌تواند برچسب سیگنال را دریافت کند، چون با توان کمی ارسال شده است. در این مواقع، باید درصد پنهانی برچسب در سیگنال را کمتر کرد تا ستبری بیشتر شود ولی امنیت کمتر شود. بنابراین در روش‌های فعال، باید مصالحه‌ای بین سه معیار سنجش گفته‌شده در بخش قبلی انجام داد، در حالی که روش‌های غیرفعال، معیار پنهانی را ندارد و پنهان کامل در نظر گرفته می‌شود [۲۸]. شکل ۹ معیارهای سنجش را برای روش‌های فعال و غیرفعال تفکیک کرده است.

اکنون در ادامه‌ی این بخش روش‌هایی بررسی می‌شوند که به عنوان روش‌های غیرپنهان و پنهان استفاده می‌شوند. یک دسته از روش‌های غیرپنهان، اصلاح ساختار فریم [3] است. استفاده از TDM [4] و یا طیف گسترده و پرش فرکانسی، در این دسته هستند. روش دوم، اصلاح پارامترهای ارسالی [5] است. از مثال‌های این دسته، زاویه‌دادن و یا جابه‌جاکردن عمدی سمبل‌ها در منظومه‌ی مدولاسیون است. همچنین

[3]Modification of the frame structure [4]Time–Division Multiplexing

[5]Modification of the transmission parameters

می‌توان از بخش‌هایی از فریم برای قراردادن کد آن، استفاده کرد. دسته‌ی دیگر، رمزکردن در سیگنال پیام و پایلوت [1] هست که با استفاده از ویژگی‌های فیزیکی انجام شود. به طور کلی با توجه به نقاط ضعف روش‌های غیرپنهان، معمولاً برای ارتباط های مداوم، روش‌های پنهان به کار می‌روند. دقت شود که روش غیرپنهان در واقع حالتی حدی از روش پنهان است یعنی می‌توان دسته‌بندی را به گونه‌ای دیگر نیز بررسی کرد. مطابق شکل ۱۴، که توضیحات آن در ادامه خواهد آمد، می‌توان روش‌ها را بر اساس معیار پنهانی که از رابطه‌ی (۱) به دست می‌آید، طبقه‌بندی کرد.

$$c_t = \frac{\mathcal{P}_d}{\mathcal{P}_s} = 1 - \frac{\mathcal{P}_t}{\mathcal{P}_s} \qquad (1)$$

در رابطه‌ی (۱)، عبارات $\mathcal{P}_d$، $\mathcal{P}_s$ و $\mathcal{P}_t$، به ترتیب توان اختصاص داده شده در یک فریم برای داده‌ها، کل یک فریم سیگنال و برچسب هویتی هستند. در واقع می‌توان این طور نیز بیان کرد که $\mathcal{P}_d + \mathcal{P}_t = \mathcal{P}_s$. همچنین c_t ضریب آشکار بودن داده‌ها در سیگنال است که معیاری برای سنجش پنهانی است. این رابطه می‌گوید که میزان پنهانی، نسبت توان تخصیص داده شده به داده‌ها به روی توان کل یک فریم از سیگنال است. به عنوان نمونه، مراجع [۳۰] و [۴۹] از این معیار برای بیان پنهانی استفاده کرده‌اند، با این تفاوت که به جای محاسبه‌ی توان، از ضریب تخصیص توان استفاده کرده‌اند. در بخش توضیحات روش تجمیعی که در ادامه آمده، مختصری به ضریب تخصیص توان نیز پرداخته شده است.

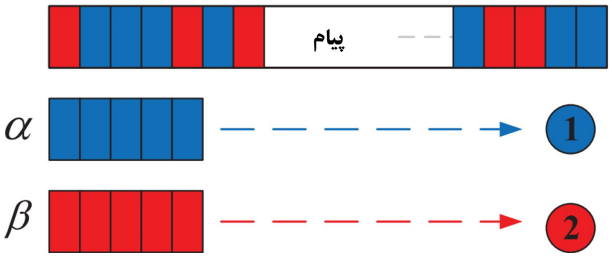
حال در این بخش، مهمترین روش‌ها یعنی روش‌های فعال پنهان به طور خلاصه بررسی می‌شوند. این روش‌ها خود در چهار دسته‌ی جایگزینی [2]، شیب [3]، کانال–مانند [4]، تجمیعی [5] قرار می‌گیرند.

در روش جایگزینی، تعدادی از بیت‌های پیام با بیت‌های برچسب هویتی، جایگزین می‌شوند. این جایگزینی، براساس کلید امنی صورت می‌گیرد. یعنی محل این بیت‌ها و خود ۰ یا ۱ بودن این بیت‌ها، با توجه به کلید انتخاب می‌شود.

روش دیگری که برای احراز اصالت فعال پنهان وجود دارد، روش شیب است. در این روش، پیام به دو گروه با ضریب توان متفاوت تقسیم می‌شود و مطابق با کلید توافق شده، هرلحظه بخشی از یکی از گروه‌ها را می‌فرستد. گیرنده با دریافت سیگنال، توان هر گروه را می‌سنجد و بررسی می‌کند که آیا ضریب توان دو گروه درست بوده یا خیر. به عنوان مثال، سیگنال پیام در شکل ۱۰ به دو گروه قرمز و آبی تقسیم شده (طبق کلید) و سیگنال s_1 و s_2 ساخته می‌شوند. سپس با ضریب توان طبق رابطه‌ی (۲)، دو سیگنال x_1 و x_2 ساخته می‌شوند و این دو سیگنال با هم ترکیب می‌شوند.

$$x_1 = \alpha s_1, \quad x_2 = \beta s_2 \qquad (2)$$
$$0 \le \beta < 1 < \alpha, \quad \frac{\alpha^2}{2} + \frac{\beta^2}{2} = 1$$

روش دیگری که برای احراز اصالت فعال پنهان استفاده می‌شود، روش کانال–مانند است. ایده‌ی این روش، قرار دادن برچسب هویتی در



شکل ۱۰. روش شیب (تقسیم پیام به دو گروه قرمز و آبی و تخصیص دو ضریب توان متفاوت) [۲۸]

سیگنال به گونه‌ای است که مشابه فیدینگ کانال شود. مطابق رابطه‌ی (۳)، می‌توان برای ارسال سیگنال پیام $X(t)$، آن را با ماتریس $A(t)$ به زیرفضای عمودی پایلوت (P) برد. همچنین در کنار ماتریس کانال $H(t)$، ماتریسی برای احراز اصالت به نام $F(t)$ را ضرب کرد و سیگنال دریافتی $Y(t)$ در گیرنده را به دست آورد. اگر گیرنده‌ای از احراز اصالت مطلع نباشد، متوجه $F(t)$ نخواهد شد و آن را مانند اثرات کانال فرض خواهد کرد ولی کاربر معتبر با توجه به اینکه کانال را سنجیده، می‌تواند درستی هویت فرستنده را تشخیص‌دهد. در مراجع [۶] و [۵] از این مورد استفاده شده است.

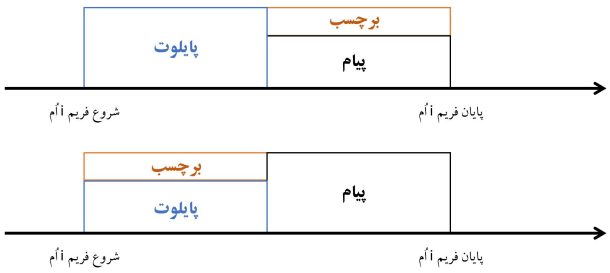
$$\begin{aligned} Y(t) &= H(t)F(t)U(t) + N(t) \qquad (3) \\ &= H(t)F(t)(X(t)A(t) + P) + N(t) \\ &= H(t)F(t)X(t)A(t) + H(t)F(t)P + N(t) \end{aligned}$$

روش دیگری که می‌توان برای احراز اصالت فعال پنهان استفاده کرد، روش تجمیعی است. این روش از روی هم قرار دادن سیگنال برچسب هویتی و سیگنال داده، سیگنال ارسالی را می‌سازد. مطابق رابطه‌ی (۴)، دو ضریب ρ_s و ρ_c به عنوان ضرایب تخصیص توان به دو سیگنال داده $(S(t))$ و برچسب هویتی $(C(t))$ در نظر گرفته می‌شوند و سیگنال ارسالی $X(t)$ از تجمیع این دو سیگنال به دست می‌آید. (لازم به ذکر است که باید ضریب تخصیص توان به برچسب بسیار کوچکتر از ضریب تخصیص توان به سیگنال داده باشد تا پنهانی رعایت شود.) همچنین دقت شود که سیگنال $C(t)$ که همان برچسب هویتی است، می‌تواند از خروجی تابع چکیده‌سازی به دست بیاید که به ورودی آن سیگنال پیام داده شده و کلید مورد استفاده k بوده است [۳]. در این صورت گیرنده باید سیگنال داده را به تابع چکیده‌ساز بدهد و بررسی‌کند که آیا برچسب هویتی دریافتی درست بوده یا خیر. به علاوه گیرنده می‌تواند به ضرایب تخصیص توان برای داده و برچسب نیز دقت کند تا بتواند شنودگر را دقیق‌تر تشخیص دهد. مراجع [۵۰] و [۳۰] از این مورد استفاده کرده‌اند.

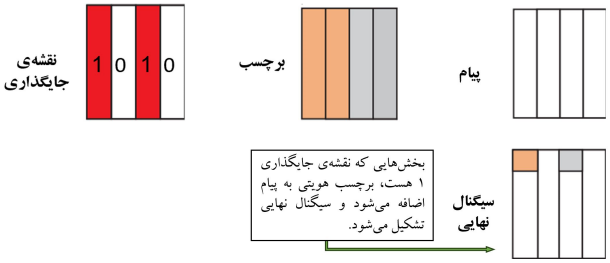
$$\begin{aligned} X(t) &= \rho_s S(t) + \rho_c C(t) \qquad (4) \\ p_c &\ll p_s \\ C(t) &= \mathrm{hash}_k(S(t)) \end{aligned}$$

این‌کار را می‌توان روی سیگنال پیام و یا حتی روی پایلوت انجام داد.

[1] Encoding of the pilot [2] Replacement [3] Slope [4] Channel–like [5] Superimposition



شکل ۱۱. اضافه‌کردن برچسب هویتی روی سیگنال پیام و یا سیگنال پایلوت (ارتفاع هر مستطیل، نشان‌دهنده‌ی ضریب تخصیص توان است.)



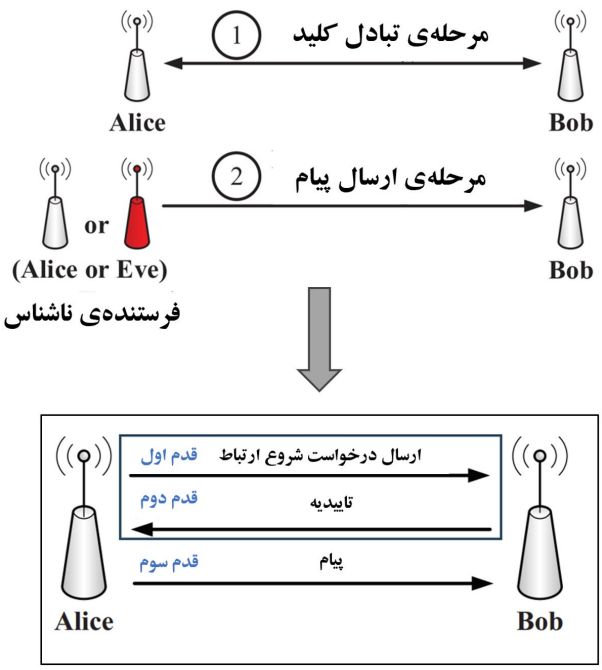
شکل ۱۲. اضافه‌کردن برچسب هویتی به کمک نقشه‌ی جایگذاری

شکل ۱۱ این مورد را نشان داده است. روشی که برچسب احراز اصالتی را روی سیگنال پیام استفاده می‌کند (رابطه‌ی (۴))، دو ایراد نسبت به اضافه‌کردن روی پایلوت دارد، اولا پردازش را زیاد می‌کند چون باید سیگنال پیام را کدگشایی کرد. ثانیاً ممکن است که ستبری را کاهش دهد، در حالی که اگر به پایلوت اضافه شود، سیگنال پیام می‌تواند با حداکثر توان ارسال شود و احراز اصالت نیز انجام شود [۲۸]. اما اضافه‌کردن به سیگنال پیام این مزیت را دارد که می‌تواند همزمان با ارسال داده‌ها، در تمامی لحظات، احراز اصالت را انجام دهد.

می‌توان این روش را با انجام تمهیداتی، بهتر کرد. به عنوان نمونه، در [۴۹] از ضریب توان متغیر به جای ρ_c در رابطه‌ی (۴) استفاده شده است و با توجه به مقادیر اندازه‌گیری‌شده از کانال و احتمال تشخیص، ضریب تخصیص توان را تغییر می‌دهد. همچنین می‌توان برداری تحت عنوان نقشه‌ی جایگذاری[1] برای تعیین محل برچسب هویتی در نظر گرفت تا بیت‌های برچسب هویتی را تنها در مکان‌های خاصی گذاشت که نقشه‌ی جایگذاری مشخص کرده است، در این حالت، توان ارسالی برای برچسب کاهش می‌یابد و پنهانی برچسب هویت در سیگنال نیز بیشتر می‌شود. برای این‌کار، مطابق شکل ۱۲ می‌توان در محل‌هایی که نقشه‌ی جایگذاری مشخص کرده است، برچسب هویتی را اضافه‌کرد [۵۰].

مراحل انجام احراز اصالت فعال، در شکل ۱۳ آمده است. به طور کلی دو مرحله‌ی تبادل کلید و ارسال پیام وجود دارد. مرحله‌ی تبادل کلید از دو قدم تشکیل شده است. در قدم اول آلیس برای باب درخواست شروع ارتباط می‌دهد. سپس باب تأییدیه‌ی شروع ارتباط را می‌دهد و از ویژگی‌های فیزیکی نمونه‌برداری می‌کند. سپس در قدم سوم، پیام ارسال می‌شود. دقت‌شود که تعداد قدم‌های روش فعال از غیرفعال کمتر است

[1] Mapping vector



شکل ۱۳. مراحل احراز اصالت فعال [۲۸] (مرحله‌ی تبادل کلید، شامل قدم ۱ و ۲ هست و مرحله‌ی ارسال پیام قدم ۳ هست [۲])

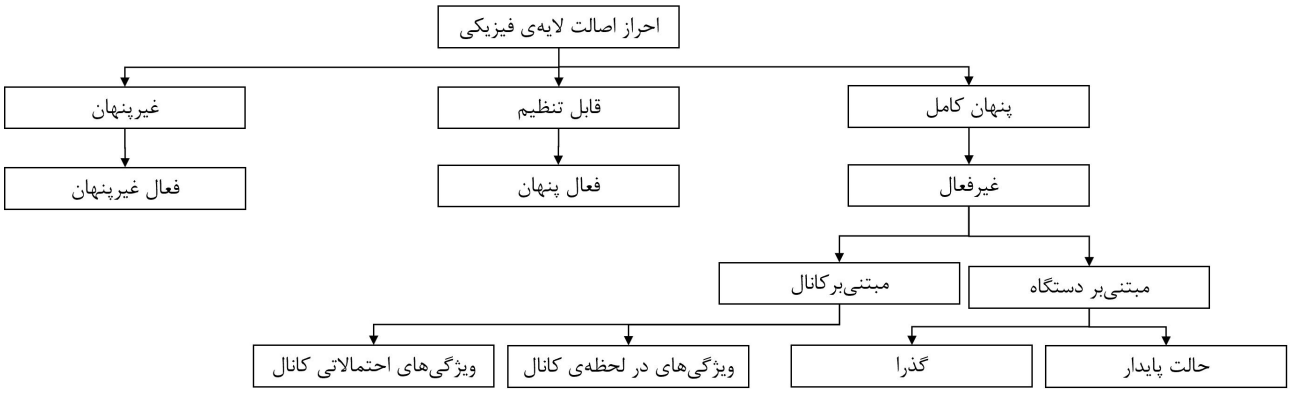
و از نظر سرعت وضعیت بهتری دارد.

۳.۲ تقسیم‌بندی از نظر پنهانی

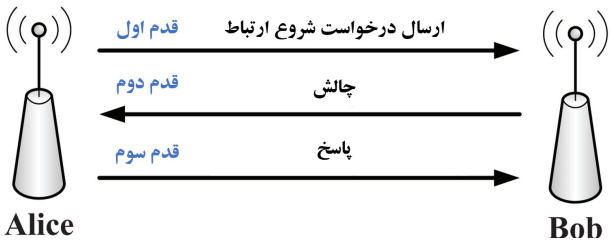
بنابر رابطه‌ی (۱)، می‌توان روش‌ها را از نظر معیار پنهانی تقسیم‌بندی کرد که این کار در شکل ۱۴ انجام شده است. روش‌های غیرفعال، پنهان کامل هستند، بعد از آن، روش‌های فعال پنهان، که میزان کمتری پنهان هستند و میزان پنهانی آن‌ها قابل تنظیم است. در آخر روش‌های غیرپنهان هستند که معیار پنهانی آن‌ها صفر درصد است. بنابراین کاربردی‌ترین دسته برای ارتباطات مداوم در این شکل، دسته‌ی دوم است که روش‌های فعال پنهان هستتند که می‌توان میزان پنهانی برچسب هویتی در سیگنال را تنظیم کرد و مصالحه‌ای بین معیارهای دیگر به وجود آورد.

۴.۲ روش‌های ترکیبی

این روش‌ها، ترکیبی از روش‌های فعال و غیرفعال هستند. همان طور که گفته شد روش‌های غیرفعال این مزیت را دارند که از نظر پنهانی برچسب هویتی، بهترین روش هستند. اما از طرفی ایرادی دارند که آن عدم کنترل روی تولید و تعویض کلید است. بنابراین می‌توان برای رفع این مشکل از روش‌های فعال نیز در کنار آن استفاده کرد تا بتوان کلید را در صورت نیاز تغییر داد. یکی از روش‌های ترکیبی، استفاده از چالش و پاسخ است. تفاوت این روش با روش‌های فعال این است که در این روش، هیچ برچسب هویتی به سیگنال اضافه نمی‌شود. یعنی به این صورت است که هر کسی درخواست احراز اصالت داشته باشد، باید بتواند پاسخ صحیح چالش ارسالی به خود را بدهد [۳۱]. به عنوان کاربردی از این



شکل ۱۴. طبقه‌بندی روش‌ها براساس معیار پنهانی



شکل ۱۵. مراحل روش ترکیبی چالش و پاسخ [۲]

روش، در مرجع [۵۱]، از روش چالش و پاسخ برای RFID استفاده شده است. مطابق شکل ۱۵، در این روش، آلیس درخواست شروع ارتباط را برای باب می‌فرستد و سپس باب یک چالش برای آلیس می‌فرستد. این چالش، می‌تواند یک عدد تصادفی باشد. آلیس این چالش را باید پاسخ دهد و پاسخ آن را برای باب بفرستد. سپس باب بررسی می‌کند که آیا پاسخ صحیح بوده یا خیر [۲].

مزیت این روش این است که نیازی نیست تا کاربر در مکان خاصی باشد و یا حتی نیازی نیست تا اندازه‌گیری CSI انجام شود. همچنین تعداد قدم‌های این روش، از روش غیرفعال کمتر است و می‌توان آن را سریع‌تر از روش غیرفعال انجام داد و روی تولید کلید نیز کنترل کرد. از طرفی نسبت به روش‌های فعال نیز، از این نظر بهتر است که پنهان کامل است، درحالی‌که روش‌های فعال، پنهان نسبی بودند. همچنین محاسبات کمتری از روش‌های فعال دارد. در واقع اگر فرض شود که کانال بین آلیس و باب در هر دو مسیر رفت و برگشت یکسان است ($H_{AB} \cong H_{BA}$) در این صورت محاسبات را می‌توان بسیار کاهش داد و طبق روابط (۵) و (۶) به دست آورد [۲]. مراحل کلی این نوع روش‌ها به صورت زیر هستند:

قدم ۱: فرض‌شود که باب درخواست شروع ارتباط را داشته و آلیس قصد دارد تا برای باب، چالشی بفرستد تا باب آن را پاسخ دهد. در واقع در اینجا هدف احراز اصالت باب برای آلیس هست (شکل ۱۶). همچنین فعلا فرض شود که رله‌های بین مسیر، وجود ندارند و فقط آلیس و باب هستند.

قدم ۲: آلیس یک عدد تصادفی مانند d تولید می‌کند و آن را برای باب می‌فرستد. سیگنال دریافتی توسط باب طبق رابطه‌ی (۵) خواهد بود. در این رابطه، d عدد تصادفی تولید شده توسط آلیس هست. y_B، سیگنال دریافتی در باب هست و H_{AB} پاسخ کانال از آلیس تا باب است. n_B نیز نویز دریافتی در باب است.

$$y_B = H_{AB} d + n_B \qquad (۵)$$

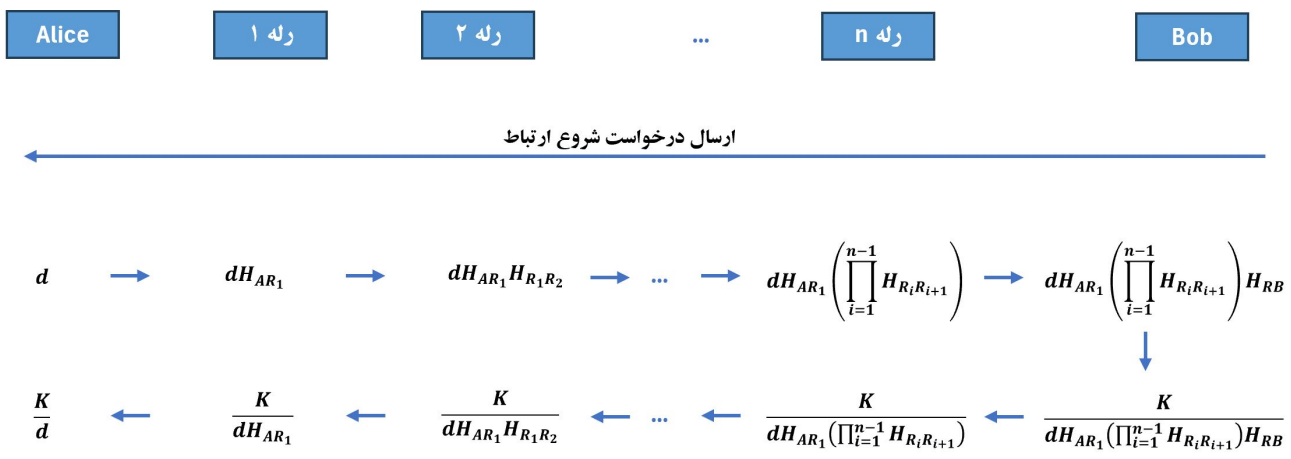
قدم ۳: باب طبق کلید امن K، پاسخ چالش را آماده می‌کند و سپس پاسخ را برای آلیس می‌فرستد. به عنوان مثال، پاسخ چالش را به صورت $\frac{K}{y_B}$ برای آلیس می‌فرستد که در آن K، کلید امن است. با توجه به اینکه در ابتدا فرض شده بود که $H_{AB} \cong H_{BA}$ برقرار است، رابطه‌ی (۶) به دست می‌آید که در آن، y_A، سیگنال دریافتی در آلیس هست و H_{BA} پاسخ کانال از باب تا آلیس است. n_A نیز نویز دریافتی در آلیس است.

$$y_A = H_B A \frac{K}{y_B} + n_A = \frac{H_{BA} K}{H_{AB} d + n_B} + n_A \cong \frac{K}{d} \qquad (۶)$$

اگر دو کلید شبیه به هم بود، هویت باب احراز می‌شود. منظور از شبیه به هم بودن کلید تخمینی با کلید اصلی، تساوی دقیق نیست، بلکه منظور همبستگی است. چون به علت وجود نویز در روابط (۵) و (۶)، مقدار نهایی تقریبی به دست آمده بود. بنابراین آلیس می‌تواند کلیدی که باب می‌دانسته را با رابطه‌ی (۷) تخمین بزند و با کلید خود مقایسه کند.

$$\hat{K} = y_A^H d \qquad (۷)$$

اکنون می‌توان این روش را تعمیم داد و بین آلیس و باب، از تعدادی رله استفاده کرد. شکل ۱۶ این مورد را نشان داده است [۳۲]. مشاهده می‌شود که کاملا مانند بدون حالت رله است، با این تفاوت که عمل ضرب در ماتریس کانال، برای هر رله تکرار می‌شود. در این شکل، باب درخواست شروع ارتباط را برای آلیس می‌فرستد و آلیس یک عدد تصادفی مانند d تولید می‌کند و آن را به رله‌ی اول می‌دهد. بنابراین این عدد در ماتریس کانال بین آلیس و رله‌ی اول، ضرب می‌شود. به همین ترتیب ادامه پیدا می‌کند تا به باب برسد. باب طبق کلید K پاسخ چالش را آماده می‌کند و دوباره مسیر رله‌ها طی می‌شود و با هر بار عبور از کانال، دوباره



شکل ۱۶. مراحل احراز اصالت به روش ترکیبی چالش و پاسخ برای چند رله

در ماتریس کانال ضرب می‌شود، در نتیجه صورت و مخرج کسر ساده می‌شوند تا به آلیس برسد. آلیس نیز $\frac{K}{d}$ را دریافت خواهد کرد. بنابراین می‌تواند متوجه شود که باب چه کلیدی را استفاده کرده بوده و به این ترتیب، هویت باب، برای آلیس احراز می‌شود.

در واقع، مزیت این روش ترکیبی چالش و پاسخ نسبت به روش فعال، دو مورد است: اولا پنهانی بیشتری دارد، چون از کانال بین آلیس و باب استفاده می‌کند و آن را هیچ جایی تحت عنوان برچسب هویتی نمی‌فرستد که شنودگری بخواهد آن را متوجه شود. ثانیاً محاسبات کمتری دارد، چون در روش‌های فعال، نیاز به انجام محاسباتی برای برچسب هویتی وجود دارد ولی در اینجا این‌کار به صورت خودکار با عبور از محیط انجام می‌گیرد و ماتریس‌های کانال خودبه‌خود ساده می‌شوند، یعنی دیگر نیاز به عملیات اضافه‌ای نخواهد بود. همچنین نسبت به روش‌های غیرفعال این مزیت را دارد که توانایی کنترل روی تولید و تغییر کلید بیشتر می‌شود، زیرا از اعداد تصادفی برای چالش و پاسخ استفاده کرده است. اما نقطه‌ی ضعف این روش نسبت به روش‌های فعال و غیرفعال، کمتر بودن ستبری است. زیرا از تقریب $H_{AB} \cong H_{BA}$ استفاده شده است و از n_B و n_A صرف‌نظر شده است، بنابراین به SNR بیشتری نیاز است. همچنین این روش برای ارتباط بدون پایلوت مناسب است، زیرا اگر پایلوت باشد، شنودگر می‌تواند کانال را تخمین بزند. در مرجع [۲] توضیحات کاملی از این روش آمده است.

علت اینکه روش فوق در دسته‌ی روش‌های ترکیبی آورده شده، این است که در روش فوق، استفاده از شرایط کانال، روشی غیرفعال مبتنی بر کانال به حساب می‌آید، از طرفی، تولید اعداد تصادفی و پاسخ دادن به چالش، نیازمند تغییرات در سیگنال است، بنابراین مشابه روش‌های فعال خواهد بود. در نتیجه روش چالش و پاسخ، هر دو نوع روش فعال و غیرفعال را در خود دارد و می‌توان مصالحه‌ای بین مزایا و معایب آن‌ها انجام داد.

به عنوان معیار سنجش برای روش ترکیبی می‌توان به جای استفاده از سه معیار سنجش گفته شده، از ترکیب آن‌ها استفاده کرد. احتمال احراز اصالت امن [1] (P_{SA}) معیاری است که مرجع [۴۲] استفاده کرده است. در این معیار، ترکیب هر سه معیار پنهانی، امنیت و ستبری وجود دارد و به صورت رابطه‌ی (۸) تعیین می‌شود.

$$P_{SA} = \max\left(P_{D,Bob} - P_{D,Eve}I_{Eve}, ۰\right) \qquad (۸)$$

$$I_{Eve} = ۱ - \frac{H(ky_{Eve})}{\log_۲ |\tau|} \qquad (۹)$$

در رابطه‌ی (۸)، $P_{D,Bob}$ احتمال تشخیص صحیح توسط باب است و بیانگر دقت احراز اصالت در باب و ستبری است. $P_{D,Eve}$ احتمال تمایز صحیح بین سیگنال معمولی و برچسب هویتی توسط شنودگر است و بیانگر معیار پنهانی است. در واقع شنودگر باید اول بتواند برچسب هویتی را از سیگنال معمولی تشخیص دهد تا بعدا بتواند کلید را بیابد. $H(ky_{Eve})$ ابهام کلید برای شنودگر است و $\frac{H(ky_{Eve})}{\log_۲ |\tau|}$ ابهام کلید نرمالیزه‌شده‌ی شنودگر است. I_{Eve} نسبت اطلاعاتی است که به شنودگر می‌رسد. یعنی بیانگر معیار امنیت است و از طریق رابطه‌ی (۹) به دست می‌آید. در این رابطه، y_{Eve} سیگنال دریافتی در شنودگر است و متشکل از برچسب هویتی و داده‌ها است. همچنین $|\tau|$ تعداد برچسب‌های هویتی ممکن است. اگر I_{Eve} صفر باشد، به معنای این است که هیچ اطلاعاتی به شنودگر نرسیده و اگر یک باشد، یعنی تمام اطلاعات لازم از کلید را شنودگر دارد. بنابراین هر سه معیار سنجش در این رابطه نهفته است. در نتیجه باید رابطه‌ی (۸) را بیشترین مقدار ممکن کرد. برای حداکثر کردن رابطه‌ی (۸) می‌توان قیودی مانند حداکثر مقدار برای هشدار اشتباه در نظر گرفت. به دلیل اینکه افزایش دقت تشخیص، سبب می‌شود تا هشدارهای اشتباه نیز بالاتر برود، این کار می‌تواند سودمند باشد و مدل بهتری از مساله بدهد.

بنابراین مساله‌ی بهینه‌سازی در مورد روش‌فوق به صورت رابطه‌ی (۱۰) به دست می‌آید.

[1] Probability of Security Authentication (PSA)

$$P_{SA} = \max\left(P_{D,Bob} - P_{D,Eve} I_{Eve}, 0\right) \quad (10)$$
$$\text{subject to } P_{FA,Bob} < \epsilon_{FA,Bob}, \quad P_{FA,Eve} < \epsilon_{FA,Eve}$$

۵.۲ تصمیم‌گیری درباره‌ی هویت

در انتهای هر روش، هدف نهایی تصمیم‌گیری در مورد مجاز بودن کاربر است [۵۲]. برای این‌کار، دو فرضیه مطابق رابطه‌ی (۱۱) وجود دارد که H_0 برای کاربر غیرمجاز و H_1 برای کاربر مجاز هست. به عنوان مثال در ساده‌ترین حالت در این رابطه، D می‌تواند تفاوت توان سیگنال دریافتی در لحظه‌ی کنونی با لحظات قبل باشد و θ_{th} سطح آستانه‌ی مورد نظر باشد که می‌توان در موارد مختلف، مقدار بهینه‌ی آن را نیز به دست آورد.

$$\mathcal{H}_0 : D \geq \theta_{th}, \quad (11)$$
$$\mathcal{H}_1 : D < \theta_{th}$$

حال برای اینکه به این تصمیم نهایی رسیده شود، می‌توان از راه‌های مختلف مانند تعیین سطح آستانه برای مقادیر اندازه‌گیری شده‌ای مانند تفاوت کانال در لحظه‌ی کنونی با لحظات قبل و یا یادگیری ماشین و دسته‌بندی با توجه به داده‌های آموزشی استفاده کرد. به عنوان مثال، [۵۳] از تفاوت تخمین کانال در لحظات قبل با پیش‌بینی آن استفاده کرده و برای پیش‌بینی و دنبال‌کردن بهتر تغییرات کانال، راه حلی پیشنهاد کرده است. همچنین در [۵۴] از این روش استفاده کرده و به جای D در رابطه‌ی (۱۱)، از سیگنالِ باقیمانده بعد از حذف برچسب هویتی استفاده کرده است. مرجع [۵۵] نیز یک امضا [1] متشکل از ویژگی‌های کانال و سخت‌افزار تعریف می‌کند و از رابطه‌ی (۱۱) برای تشخیص هویت استفاده می‌کند. برای به دست آوردن سطح آستانه نیز، مرجع [۵۶] از یادگیری عمیق [2] استفاده کرده و سطح آستانه‌ی مناسب را مقداری تعریف کرده که کمترین خطای تشخیص (شامل تشخیص [3] اشتباهیِ کاربر غیرمجاز و ردکردن [4] اشتباهیِ کاربر مجاز) را داشته باشد.

۳ حملات و راه‌های مقابله

همان‌طور که در بخش‌های قبلی گفته شد، احراز اصالت لایه‌ی فیزیکی جایگزین لایه‌های بالاتر نیست، بلکه برای حفاظت بیشتر می‌تواند مورد استفاده قرار گیرد [۵۷]. این نوع احراز اصالت نیز ممکن است مورد حملاتی قرار بگیرد که در این بخش، مختصری از این حملات در سه بخش فعال، غیرفعال و ترکیبی بررسی شده است و راه‌هایی برای تشخیص و مقابله با آن‌ها نیز ارائه شده است.

۱.۳ حملات غیرفعال

در این نوع حملات، مهاجم هیچ‌گونه سیگنالی را ارسال نمی‌کند و فقط محتوای اطلاعات ارسالی را دریافت می‌کند. در واقع این نوع حملات محرمانگی را به خطر می‌اندازند. شنود اطلاعات ارسالی برای یافتن برچسب هویتی، تحلیل ترافیک شبکه و تعیین نقشه‌ی شبکه از اهداف حملات غیرفعال است که در ادامه هر کدام توضیحات مختصری داده شده است.

شنود برای یافتن برچسب هویتی: در احراز اصالت لایه‌ی فیزیکی، حمله‌ی غیرفعالی که انجام می‌شود اکثراً برای شنود اطلاعات سیگنال است. این شنود، می‌تواند برای یافتن برچسب هویتی، تخمینی از کانال بین کاربران معتبر، پیدا کردن موقعیت تقریبی کاربران و یا استفاده‌ی دوباره از سیگنال برای احراز اصالت باشد. در این حالت شنودگر در زمان‌های مختلف داده‌برداری می‌کند و می‌تواند از روی این داده‌ها و با حذف سیگنال اصلی، برچسب هویتی را به دست آورد. همچنین در صورتی که از روش‌های احراز اصالت مبتنی بر دستگاه استفاده شود، شنودگر می‌تواند اطلاعات سخت‌افزار و یا حتی نرم‌افزار کاربران را به دست آورد و از آن در حملات بعدی خود به لایه‌های دیگر استفاده کند. به عنوان مثال اگر شنودگر تشخیص دهد سخت‌افزار مورد استفاده ساخت چه سالی است، می‌تواند نوع سیستم عامل و یا نرم‌افزارهای دیگر روی آن را نیز حدس بزند و در نتیجه می‌تواند از ضعف‌های آن نرم‌افزار برای حمله به لایه‌های بالاتر استفاده کند. برای جلوگیری از شنود، برچسب هویتی فیزیکی می‌تواند خروجی تابع چکیده‌سازی از اطلاعاتی مانند زمان ارسال پیام، شماره‌ی بسته‌ی ارسالی [5]، متن پیام، شماره‌ی شناسایی کاربر، کانال بین فرستنده و گیرنده، کلید تبادل‌شده از طریق لایه‌های بالاتر، موقعیت کاربر، پاسخ چالش ارسالی از فرستنده و غیره باشد و ویژگی‌های فوق بعد از اعمال تابع چکیده‌ساز، به عنوان برچسب هویتی به سیگنال اضافه‌شوند. در این حالت شنودگر داده‌ها را ذخیره می‌کند و با مقایسه با جدول خروجی تابع چکیده‌ساز برای حالت‌های مختلف، حتی اگر بتواند به ویژگی‌های فوق نیز برسد، با توجه به اینکه از ویژگی‌های دیگری مانند زمان ارسال، پاسخِ چالش، موقعیت و غیره نیز استفاده شده که تغییر کرده‌اند، شنودگر نمی‌تواند هویتی را جعل کند. مراجع [۳۰، ۴۱، ۴۹، ۵۰] از تابع چکیده‌ساز برای روش تجمیعی، [۵] از این نوع تابع برای روش کانال–مانند استفاده کرده‌اند. دقت‌شودکه تابع چکیده‌ساز، می‌تواند عمومی باشد و همه آن را بدانند، اما چون تابع چکیده‌ساز، کلید امن مخصوصی دارد، کسانی کلید را ندارند، نمی‌توانند خروجی تابع را پیدا کنند [۴۱] و تنها می‌توانند با چکیده‌سازی تمام پیام‌ها با تمام کلیدهای ممکن و ذخیره‌ی آن، قسمتی از پیام را به دست آورند (روش معمول شکستن خروجی تابع چکیده‌ساز) که آن هم با توجه به استفاده از ویژگی‌های فیزیکی مانند کانال مخابراتی و پنهان بودن برچسب هویتی، از آن جلوگیری می‌شود. همچنین می‌توان از راهی شبیه به راهی که در مرجع [۵۸] پیشنهاد شده است، استفاده کرد با این تغییر که به آن سیگنال برچسب هویتی را نیز اضافه کرد. در واقع، با ایجاد یک برچسب هویتی جعلی، شنودگر را به اشتباه انداخت و اطلاعات اشتباه را به آن داد. رابطه‌ی (۱۲) و (۱۳) این مورد را نشان می‌دهند.

$$X_A(t) = \rho_s S(t) + \rho_c C(t) + \rho_{spoof} C_{spoof}(t) \quad (12)$$
$$Y_U(t) = H(t) Y_A(t) + W(t) \quad (13)$$

[1] Signature [2] Deep learning [3] Detect [4] Reject

[5] Packet number

در رابطه‌ی (۱۲)، $X_A(t)$ سیگنالی است که آلیس برای باب می‌خواهد بفرستد (آلیس و باب هر دو کاربر مجاز هستند) و ρ_s، ρ_c، ρ_{spoof} به‌ترتیب ضرایب تخصیص توان به سیگنال داده‌ی $S(t)$، برچسب هویتی $C(t)$، برچسب هویتی فریبنده‌ی شنودگر C_{spoof} هستند. بنابراین آلیس سیگنال $X_A(t)$ را می‌فرستد و باب یا شنودگر، سیگنال $Y_U(t)$ را طبق رابطه‌ی (۱۳) دریافت می‌کنند که U می‌تواند E یا B باشد که نشان‌دهنده‌ی شنودگر و یا باب هست. $W(t)$ نیز نویز محیط است و $H(t)$ ماتریس کانال است. اگر ضریب توان اختصاص‌یافته به سیگنال برچسب هویتی کمتر از ضریب برچسب هویتی فریبنده باشد، شنودگر به اشتباه برچسب هویتی فریبنده را به عنوان برچسب واقعی، کدگشایی می‌کند و آن را ذخیره می‌کند.

تحلیل ترافیک شبکه و تعیین نقشه‌ی شبکه: در این حالت، شنودگر نیازی به فهمیدن دقیق اطلاعات ارسالی ندارد و می‌تواند تنها با اندازه‌گیری میزان پیام‌های رد و بدل شده، نقاط پراهمیت شبکه و یا مسیرهای عبور پیام را پیدا کند و در نتیجه تخمینی از موقعیت کاربران به دست می‌آورد. برای بالابردن امنیت در مقابل این حمله، روش‌های رمزنگاری در لایه‌های بالاتر کاربردی ندارد و باید از لایه‌ی فیزیکی استفاده کرد. نویز مصنوعی و فرستادن اطلاعات بیهوده برای فریب دادن شنودگر، روش‌هایی هستند که برای این کار استفاده می‌شود. اما در بحث احراز اصالت، باید تغییراتی روی آن‌ها انجام داد. به عنوان مثال، در یک سیستم که احراز اصالت فیزیکی وجود دارد، اگر یک فرستنده همراه داده‌ها، اطلاعات بیهوده برای فریب شنودگر بفرستد، باید حتماً آن را همراه برچسب هویتی فریبنده بفرستد، زیرا اگر اطلاعات بیهوده را بدون برچسب هویتی بفرستد، شنودگر می‌فهمد که این اطلاعات را نباید در تحلیل شبکه استفاده کند و این اطلاعات، فریبنده هستند، چون هیچ برچسب هویتی ندارند. این کار از نظر محاسبات و توان مصرفی مناسب نیست. بنابراین برای رفع این مشکل، می‌توان پنهان بودن برچسب هویتی را که در بخش‌های قبلی توضیح داده شد، رعایت‌کرد تا شنودگر نتواند هیچ برچسب هویتی (هم اصلی و هم فریبنده) را تشخیص دهد.

۲.۳ حملات فعال

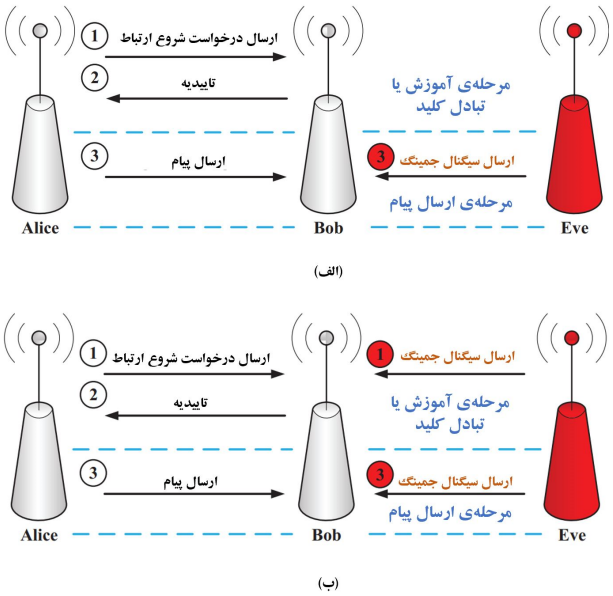
در این نوع از حملات، مهاجم اطلاعات سیگنال را تغییرمی‌دهد و یا سیگنال جدیدی ارسال می‌کند. یعنی یکپارچگی[1] و دسترسی[2] تحت‌تاثیر قرار می‌گیرد، در حالی که در حملات غیرفعال، محرمانگی[3] تحت‌تاثیر قرار می‌گیرد. در احراز اصالت لایه‌ی فیزیکی دو نوع حمله‌ی فعال جمینگ و فریب انجام می‌شود. حمله‌ی جمینگ باعث می‌شود تا هویت معتبر احراز نشود. همچنین حمله‌ی فریب باعث می‌شود تا هویت غیرمعتبر به اشتباه احراز شود.

حمله‌ی جمینگ: در این نوع، مهاجم تلاش می‌کند تا با ارسال سیگنال‌های مزاحم، در عملیات احراز اصالت اختلال ایجاد کند، یعنی هویت مجاز را نتواند احراز کند و یا هویت غیرمجاز را به اشتباه احراز کند. اهداف دیگری که مهاجم از این حمله دارد، می‌تواند کم‌کردن کیفیت ارسال و هدردادن انرژی کاربر به دلیل ارسال چندباره‌ی هر پیام باشد. همچنین گاهی می‌تواند مقدمه‌ای برای حملات بعدی باشد. به عنوان مثال اگر جمینگ باعث اختلال در احراز اصالت شود، کاربران غیرمجاز وارد سامانه می‌شوند و می‌توانند حملات منع سرویس[4] را انجام دهند. حمله‌ی جمینگ را می‌توان در ۲ دسته تقسیم‌بندی کرد: پیش‌نگر[5]، واکنشی[6]. در جمینگ پیش‌نگر، مهاجم بدون توجه به وضعیت ارسال، حمله می‌کند، اما در جمینگ واکنشی، مهاجم وضعیت ارسال را بررسی می‌کند و طبق آن حمله را انجام می‌دهد [۵۹]. به عنوان مثال، مهاجم در جمینگ واکنشی، ویژگی‌های فیزیکی کانال مخابراتی را بررسی می‌کند و طبق آن در عملیات احراز اصالت اختلال ایجاد می‌کند. ولی در جمینگ پیش‌نگر، مهاجم کار خود را طبق برنامه‌ی خود پیش می‌برد، مثلاً می‌تواند به صورت ثابت سیگنال جمینگ را در یک فرکانس خاص ارسال کند (جمینگ نقطه‌ای[7])، که این کار با توجه به اینکه ممکن است کاربری در آن لحظه و در آن فرکانس فعال نباشد، باعث هدر رفتن انرژی جمر می‌شود. همچنین کاربر می‌تواند برای مقابله با آن فرکانس خود را تغییر دهد. راه دیگر این است که جمر نیز فرکانس خود را مدام تغییر دهد و باعث هدررفت منابع کاربران معتبر در برخی از زمان‌ها شود (جمینگ جاروبی[8]). روش دیگر این است که در چند فرکانس مختلف این کار را همزمان انجام دهد (جمینگ رگباری[9]) که این کار نیز می‌تواند SNR کاربران را کاهش دهد. در این‌حالت، هرچه جمر فرکانس‌های بیشتری را همزمان بفرستد، مجبور است توان کمتری را برای هر فرکانس اختصاص دهد [۶۰]. در مرجع [۲۱] نیز، به استفاده از RIS برای جمینگ و تغییر ضرایب آن برای اخلال در احراز اصالت، اشاره شده است. برای تشخیص حمله‌ی جمینگ، مقاله‌ی [۶۱] دو روش پیشنهاد داده است که اگر جمینگ تنها در مرحله‌ی ارسال پیام باشد و در مرحله‌ی آموزش نباشد، می‌توان از مقایسه‌ی نویز در دو مرحله‌ی ارسال پیام و آموزش، فهمید که یک سیگنال جدید به محیط اضافه شده است که همان سیگنال جمینگ است. حال اگر جمینگ در هر دو مرحله باشد، می‌توان مقایسه‌ی نویز بین آلیس و باب را نیز به مقایسه‌ی قبلی اضافه کرد تا تفاوت دو محیط آلیس و باب را بفهمد.

حمله‌ی فریب: در این نوع، مهاجم تلاش می‌کند تا هویتی جعلی را به عنوان کاربر مجاز، به شبکه معرفی کند. برای این نوع حمله، نیاز است تا سیگنال‌های قانونی و معتبر توسط شنودگری ضبط شود و یا ویژگی‌های فیزیکی استخراج شود. سپس دو روش می‌توان در نظر گرفت: بازپخش سیگنال ضبط شده (حمله‌ی تکرار[10])، استفاده از ویژگی‌های فیزیکی برای ایجاد یک هویت جعلی [۲۷]. مورد اول، از نظر شناسایی بسیار ساده‌تر از مورد دوم است. زیرا معمولاً در برچسب هویتی، اطلاعاتی مانند زمان ارسال، موقعیت کاربر، شماره‌ی پیام نهفته است و با بازپخش سیگنال

[1] Integrity [2] Availability [3] Confidentiality

[4] Denial-of-Service (DoS) [5] Proactive [6] Reactive [7] Spot jamming
[8] Sweep jamming [9] Barrage jamming [10] Replay attack



شکل ۱۷. در (الف) سیگنال جمینگ تنها در مرحله‌ی ارسال پیام وجود دارد، اما در (ب) در هردو مرحله وجود دارد. [۶۱]

توسط شنودگر، می‌توان متوجه شد که این پیام منقضی شده است. به عنوان مثال، مرجع [۶۲] از زمان ایجاد پیام و فاصله، بازپخش سیگنال را تشخیص می‌دهد. اما مورد دوم که استفاده از ویژگی‌های فیزیکی و ساختن یک هویت جعلی است، شناسایی سخت‌تری دارد. همچنین، درصورتی‌که مهاجم اطلاعات شنود شده را تغییرات دهد و در زمان کوتاهی برای کاربر دیگر بفرستد نیز می‌تواند به عنوان حمله‌ی مرد میانی در نظر گرفته شود، اما اگر اطلاعات را ذخیره کند و ویژگی‌های فیزیکی را پیدا کند و آن‌ها را برای استفاده‌های دیگری نگه دارد، دیگر نمی‌توان آن را جزو حمله‌ی مرد میانی در نظر گرفت، مانند دادن برچسب هویتی جعلی به کاربرانی که قصد ورود به شبکه به عنوان کاربر مجاز را دارند. در این صورت حتی کاربران مجاز نیز نمی‌توانند وارد شبکه بشوند، چون برچسب هویتی که دریافت کرده‌اند، جعلی بوده است و فریب خورده‌اند. در این دسته، اگر برای احراز اصالت از روش‌های غیرفعال مبتنی بر کانال، مانند قدرت سیگنال دریافتی و موقعیت کاربر استفاده شود، شنودگر می‌تواند با تقلید این ویژگی‌ها، در حین ارتباط، خود را به جای کاربر مجاز جا بزند. علت اینکه در حین ارتباط باید این کار را بکند، این است که همان‌طور که در بخش‌های گذشته نیز گفته شد، مرحله‌ی اول احراز اصالت لایه‌ی فیزیکی، باید با استفاده از لایه‌های بالاتر انجام شود. بنابراین شنودگر باید صبر کند تا کاربری از طریق لایه‌های بالاتر احراز اصالت را شروع کند و سپس در حین ارتباط خود را به جای او جا بزند. همچنین اگر از روش‌های غیرفعال مبتنی بر دستگاه مانند عدم دقت کلاک، ویژگی‌های مدولاسیون و یا ویژگی‌های گذرای سیگنال استفاده شود، اگر شنودگر بتواند با کلاک بالاتری این عدم دقت کلاک و یا ویژگی‌های دیگر را پیدا کند، می‌تواند عیناً آن‌را بازتولید کند و یا روابط آن را بفهمد. دقت شود که در اینجا فرض بر این است که شنودگر از استخراج ویژگی‌ها و روش مورد استفاده در کاربران، آگاه است، در حالی که در بازپخش سیگنال ضبط شده این فرض نیازی نبود. بنابراین روش‌های غیرفعال احراز اصالت لایه‌ی فیزیکی، به این حملات آسیب‌پذیری دارند. در نتیجه می‌توان از روش‌های فعال استفاده کرد. در این روش‌ها با توجه به اینکه برچسب هویتی هم به ویژگی‌های فیزیکی و هم به کلید امن هر کاربر ربط دارد، کدگشایی آن به‌سادگی نخواهد بود. همچنین محل قرارگیری برچسب هویتی نیز مانند آنچه در روش جایگزینی در بخش‌های قبلی گفته شد، متغیر است و شنودگر نمی‌تواند بفهمد که برچسب هویتی در کدام بخش از سیگنال است. از طرف دیگر، کاربر معتبر نیز نمی‌داند که مهاجم چه تعدادی دارد و از کدام مدل استفاده می‌کند. به همین دلیل، مرجع [۹] از یادگیری بدون نظارت استفاده کرده و تشخیص فریب را برای تعداد زیادی مهاجم بررسی کرده است. مرجع [۶۳] نیز از توان سیگنال دریافتی استفاده کرده و با یادگیری بدون نظارت، حمله‌ی فریب را تشخیص می‌دهد. مرجع [۳۳] نیز حملات به دستگاه‌های بازپراکن را بررسی کرده و با توجه به اینکه دستگاه‌های بازپراکن انرژی مصرفی پایینی باید داشته باشند، امکان استفاده از لایه‌های بالاتر وجود ندارد و باید از لایه‌ی فیزیکی استفاده کرد. در این مرجع، برای فریب و جعل هویت، چهار حالت گفته‌شده و راه مقابله با آن را پیشنهاد داده است. حالت اول وقتی است که مهاجم رمز استفاده شده در لایه‌های بالاتر را داشته باشد. برای تشخیص این حالت، می‌توان با استفاده از توان سیگنال دریافتی و زاویه‌ی رسیدن سیگنال، موقعیت تقریبی را به دست آورد و هویت جعلی را تشخیص داد. حالت دوم ساخت سیگنال تقلبی (برچسب هویتی جعلی) است که آن نیز با همان روش موقعیت قابل تشخیص است. حالت سوم مهاجم سیگنال را بازپخش می‌کند. در این حالت با توجه به اینکه سیستم از توان تصادفی برای برش‌های زمانی متفاوت استفاده می‌کند قابل تشخیص است. حالت چهارم، وقتی است که مهاجم مانند رله عمل می‌کند. این حالت نیز با توجه به دریافت دو سیگنال مشابه از کاربر معتبر و مهاجم، حمله قابل تشخیص است.

یکی از روش‌های دیگری که برای حملات فریب که استفاده می‌شود، ایجاد در پشتی[1] است. در واقع گاهی حملات هدف مشخصی ندارند و صرفا فقط هدف کاهش دقت و بازدهی کلی سیستم است، اما گاهی هدف حملات مشخص است و به عنوان مثال هدف احراز اصالت جعلی خاصی است. با توجه به مطالب قبل، در احراز اصالت لایه‌ی فیزیکی، از دو مرحله‌ی آموزش (استخراج ویژگی‌های فیزیکی) و ارسال پیام استفاده می‌شود، بنابراین مهاجم می‌تواند با ایجاد داده‌های جعلی و تزریق آن در مرحله‌ی آموزش، مرحله‌ی ارسال پیام را نیز مختل کند. یعنی در مرحله‌ی آموزش که باید ویژگی‌های فیزیکی استخراج شود و یادگیری انجام شود، سیستم با داده‌های جعلی که مهاجم ایجاد کرده این کار را می‌کند و در نتیجه در مرحله‌ی ارسال پیام، هویت جعلی را نیز صحیح می‌پندارد. این روش درمواردی‌که یادگیری ماشین وجود ندارد نیز می‌تواند با ایجاد نویز مصنوعی، ویژگی‌های فیزیکی کانال را در مرحله‌ی استخراج ویژگی‌ها

[1] Backdoor

به دلخواه خود تغییر دهد که برای جلوگیری از آن باید هم از ویژگی‌های مبتنی بر دستگاه و هم از ویژگی‌های مبتنی بر کانال استفاده کرد.

دقت شود که برای ایجاد در پشتی، بازدهی سیستم از دید خودش، نباید کاهش یابد تا متوجه حمله نشود. زیرا اگر متوجه حمله بشود، می‌تواند این داده‌های جعلی را حذف کند. بنابراین باید مهاجم به گونه‌ای عمل کند تا خطای کدگشایی، عدم تطابق با داده‌های قبلی در سیستم به وجود نیاید. در مرجع [۶۴] تولید داده‌هایی برای فریب سیستم‌های دارای احراز اصالت لایه‌ی فیزیکی بررسی شده است. برای مقابله با این نوع حمله، راه‌هایی مانند نیاز به تاییدیه برای داده‌برداری می‌توان در نظر گرفت اما هنوز جای کار بسیاری وجود دارد و نیاز به تحقیقات بیشتر برای لایه‌ی فیزیکی است. اما به طور کلی اگر بحث پنهان بودن برچسب و امنیت آن رعایت شود، شنود آن توسط مهاجمان سخت‌تر خواهد شد و در نتیجه بازتولید داده‌های جعلی توسط مهاجمان نیز سخت‌تر خواهد شد.

۳.۳ حملات ترکیبی

در این نوع حملات، از ترکیب چند نوع از حملات فوق استفاده می‌شود و هر کدام بخشی از سیستم را آسیب می‌زنند. همچنین برای اینکه این حملات اثربخش شوند، بهتر است که توسط چند مهاجم انجام شود. به طور کلی راه تشخیص این حملات، مشاهده‌ی کاهش دقت احراز اصالت، افزایش نرخ خطا در کدگشایی (به علت بازپخش سیگنال‌های هویتی و قصد مهاجم برای جلوگیری از عمل‌کردن سیستم)، مشاهده‌ی تغییرات ناگهانی در ویژگی‌های فیزیکی کانال مخابراتی (به علت وجود جمر) است. مرجع [۶۵] یک حمله‌ی مشارکتی از طرف چند مهاجم را بررسی کرده که مهاجمان علاوه بر شنود اطلاعات ارسالی از فرستنده، با استفاده از حمله‌ی جمینگ، گیرنده‌ی مجاز را از فهمیدن برچسب هویتی فرستنده باز می‌دارند و سپس با استفاده از اطلاعات شنود شده، با توان کمی برچسب هویتی را برای گیرنده ارسال می‌کنند تا گیرنده نتواند آن را کدگشایی کند و پیغام عدم تایید برای فرستنده بفرستد. در نتیجه فرستنده مجبور به ارسال دوباره‌ی برچسب هویتی می‌شود و این فرآیند مدام تکرار پیدا کند. این مرجع برای مقابله با این حمله، راهی پیشنهاد کرده که فرستادن اطلاعات ویژگی‌های فیزیکی اندازه‌گیری‌شده به همراه پیام عدم تایید[1] هست. در این حالت فرستنده می‌تواند تغییرات ویژگی‌های فیزیکی در سمت گیرنده را بفهمد. به این ترتیب حمله را تشخیص می‌دهد. البته لازم به ذکر است که هدف اصلی از احراز اصالت، جلوگیری از ورود کاربران جعلی است. اما برای اخلال در احراز اصالت از حمله‌های دیگری مانند شنود و جمینگ و منع سرویس استفاده می‌شود [۵۷]. بنابراین برای مقابله با حملات احراز اصالت لایه‌ی فیزیکی، به مباحث امنیت لایه‌ی فیزیکی نیز نیاز است که مواردی مانند نویز مصنوعی و شکل‌دهی امواج را شامل می‌شود. در شکل ۱۸، خلاصه‌ای از بخش حملات و راه‌های تشخیص و مقابله با آن‌ها آورده شده است.

[1] Negative Acknowledgement (NACK)

۴ مسیر آینده‌ی پژوهش

احراز اصالت لایه‌ی فیزیکی را در دو نوع محیط می‌توان بررسی کرد: محیط ثابت، محیط متغیر با زمان. برای محیط های ثابت، روش‌های غیرفعال احراز اصالت لایه‌ی فیزیکی قابل قبول هستند. روش‌های ترکیبی نیز برای محیط‌های ثابتی که نیاز به تولید برچسب‌های بیشتر باشد، مناسب است. اما در محیط های متغیر با زمان نیاز است تا کنترل روی تولید برچسب هویتی بیشتر باشد تا بتوان با تغییرات محیط مقابله کرد. به همین دلیل باید به سراغ روش‌های فعال رفت. استفاده از RIS، یکی از روش‌هایی است که می‌توان با آن، تولید برچسب هویتی را کنترل کرد. به‌علاوه اینکه با فرستادن امواج در مسیرهای خاصی امنیت ارسال نیز بالاتر می‌رود. در زمینه‌ی استفاده از RIS برای احراز اصالت، پژوهش‌های اندکی انجام شده و فرصت برای پیشرفت وجود دارد. همچنین می‌توان از RIS در احراز اصالت متحرک‌ها مانند خودروهای هوشمند، پهپادها و یا به طور کلی در ارتباط V2X بهره برد.

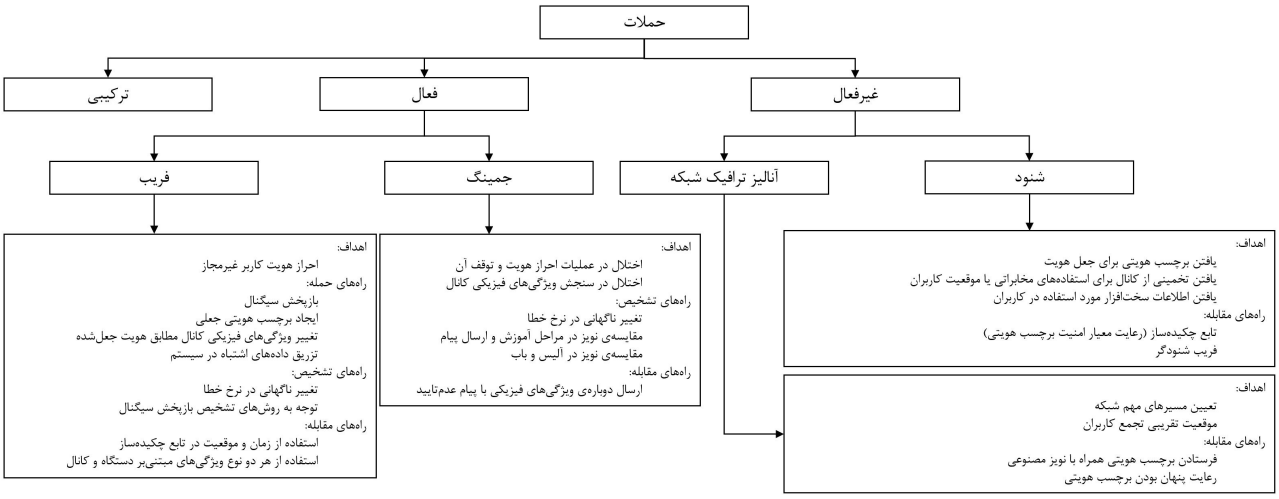
موضوع دیگری که فرصت پژوهش در آن وجود دارد، بحث مقابله با حمله‌ی درپشتی در احراز اصالت لایه‌ی فیزیکی است که با وجود آن که راه‌های مقابله برای این حمله در حالت‌های کلی وجود دارد، اما برای ارتباط بی‌سیم و لایه‌ی فیزیکی این موضوع به اندازه‌ی کافی بحث نشده است و به نظر می‌رسد که جای پیشرفت زیادی دارد.

۵ نتیجه‌گیری

استفاده از لایه‌ی فیزیکی برخلاف سایر لایه‌ها، روشی کم‌هزینه برای احراز اصالت است که می‌تواند برای افزایش امنیت شبکه‌های ارتباطی، در کنار روش‌های لایه‌های بالاتر شبکه استفاده شود. در این مقاله، ابتدا خلاصه‌ای از احراز اصالت آورده شده و سپس با ارائه‌ی دلایل و مثال‌هایی، نیاز به لایه‌ی فیزیکی در احراز اصالت مطرح شده است. سپس معیارهای اندازه‌گیری در سه دسته‌ی امنیت، پنهانی و ستبری آورده شده است. پس از آن خلاصه‌ای از روش‌های موجود برای لایه‌ی فیزیکی گفته شده و در سه دسته‌ی فعال، غیرفعال و ترکیبی، تقسیم‌بندی شده است. همچنین نموداری ارائه شده است که در آن روش‌ها براساس میزان پنهانیِ برچسب هویتی تقسیم‌بندی شده‌اند. در ادامه، خلاصه‌ای از حملات روی احراز اصالت لایه‌ی فیزیکی آورده شده و راه‌های تشخیص و مقابله با آن‌ها نیز بررسی شده است. در انتها مسیری برای آینده‌ی این پژوهش و پیشنهادهایی برای توسعه‌ی آن، ارائه شده است.

۶ سپاسگزاری

بدینوسیله از پژوهشگاه ارتباطات و فناوری اطلاعات و ستاد توسعه فناوری‌های اتصال‌پذیری و ارتباطات معاونت علمی، فناوری و اقتصاد دانش‌بنیان ریاست جمهوری، که طبق موافقتنامه شماره ۱۲۰۱۶ مورخ



شکل ۱۸. خلاصه‌ای از حملات و روش‌های تشخیص و مقابله

۱۴۰۲/۰۷/۲۳ از این پایان‌نامه حمایت کرده است و همچنین از راهبر پژوهش سرکار خانم اعظم عیدی سپاسگزاری می‌شود.

مراجع

[1] Shawky, Mahmoud A, Shah, Syed Tariq, Abdrabou, Mohammed, Usman, Muhammad, Abbasi, Qammer H, Flynn, David, Imran, Muhammad Ali, Ansari, Shuja, and Taha, Ahmad. How secure are our roads? an in-depth review of authentication in vehicular communications. *Vehicular Communications*, p. 100784, 2024.

[2] Xie, Ning, Zhang, Jiaheng, Zhang, Qihong, Tan, Haijun, Liu, Alex X, and Niyato, Dusit. Hybrid physical-layer authentication. *IEEE Transactions on Mobile Computing*, 23(2):1295–1311, 2023.

[3] Yan, Li, Wang, Junjie, He, Teng, Han, Gangtao, Li, Shuangzhi, and Liu, Guangyi. Two-user cooperative physical layer authentication in non-coherent massive mimo system. in *2022 IEEE 22nd International Conference on Communication Technology (ICCT)*, pp. 143–147. IEEE, 2022.

[4] Teng, Yulin, Shi, Huangwenqing, Niu, Mu, and Zhang, Pinchang. Identity authentication for ground control station based on mmwave mimo channel sparsity. *IEEE Communications Letters*, 2024.

[5] Goergen, Nate, Lin, W Sabrina, Liu, KJ Ray, and Clancy, T Charles. Extrinsic channel-like fingerprint embedding for authenticating mimo systems. *IEEE Transactions on Wireless Communications*, 10(12):4270–4281, 2011.

[6] Goergen, Nate, Lin, W Sabrina, Liu, KJ Ray, and Clancy, T Charles. Authenticating mimo transmissions using channel-like fingerprinting. in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, pp. 1–6. IEEE, 2010.

[7] Tang, Jie, Xu, Aidong, Jiang, Yixin, Zhang, Yunan, Wen, Hong, and Zhang, Tengyue. Mmwave mimo physical layer authentication by using channel sparsity. in *2020 IEEE International Conference on Artificial Intelligence and Information Systems (ICAIIS)*, pp. 221–224. IEEE, 2020.

[8] Enad, Eman Hani and Younis, Sedki. Machine learning based decision stratigies for physical layer authentication in wireless systems. in *2020 2nd Annual International Conference on Information and Sciences (AiCIS)*, pp. 114–118. IEEE, 2020.

[9] Meng, Rui, Xu, Xiaodong, Li, Gangyi, Xu, Bingxuan, Zhu, Fangzhou, Wang, Bizhu, and Zhang, Ping. Multi-dimensional fingerprints-based multi-attacker detection for 6g systems. *IEEE Internet of Things Journal*, 2023.

[10] Han, Jingyuan, Li, Yuxuan, Liu, Gang, Ma, Jingye, Zhou, Yi, Fang, He, and Wu, Xuewen. Model-driven learning for physical layer authentication in dynamic environments. *IEEE Communications Letters*, 2024.

[11] Senigagliesi, Linda, Cintioni, Lorenzo, Baldi, Marco, and Gambi, Ennio. Blind physical layer authentication over fading wireless channels through machine learning. in *2019 IEEE International Workshop on Information*

assisted ris communication networks. *IEEE Internet of Things Magazine*, 7(2):38–44, 2024.

[22] Zhou, Yi, Ma, Zheng, Liu, Heng, Yeoh, Phee Lep, Li, Yonghui, Vucetic, Branka, and Fan, Pingzhi. A uav-aided physical layer authentication based on channel characteristics and geographical locations. *IEEE Transactions on Vehicular Technology*, 2023.

[23] Xie, Ning, Zhang, Shengli, and Liu, Alex X. Physical-layer authentication in non-orthogonal multiple access systems. *IEEE/ACM Transactions on Networking*, 28(3):1144–1157, 2020.

[24] Li, Xingwang, Wang, Qunshu, Zeng, Ming, Liu, Yuanwei, Dang, Shuping, Tsiftsis, Theodoros A, and Dobre, Octavia A. Physical-layer authentication for ambient backscatter-aided noma symbiotic systems. *IEEE Transactions on Communications*, 71(4):2288–2303, 2023.

[25] Xie, Ning, Zhang, Qihong, Chen, Junjie, and Tan, Haijun. Privacy-preserving physical-layer authentication for non-orthogonal multiple access systems. *IEEE Journal on Selected Areas in Communications*, 40(4):1371–1385, 2022.

[26] Shawky, Mahmoud A, Bottarelli, Mirko, Epiphaniou, Gregory, and Karadimas, Petros. An efficient cross-layer authentication scheme for secure communication in vehicular ad-hoc networks. *IEEE Transactions on Vehicular Technology*, 72(7):8738–8754, 2023.

[27] Danev, Boris, Luecken, Heinrich, Capkun, Srdjan, and El Defrawy, Karim. Attacks on physical-layer identification. in *Proceedings of the third ACM conference on Wireless network security*, pp. 89–98, 2010.

[28] Xie, Ning, Li, Zhuoyuan, and Tan, Haijun. A survey of physical-layer authentication in wireless communications. *IEEE Communications Surveys & Tutorials*, 23(1):282–310, 2020.

[29] Annessi, Robert, Fabini, Joachim, and Zseby, Tanja. To trust or not to trust: Data origin authentication for group communication in 5g networks. in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pp. 1–7, 2018.

[30] Zhang, Pinchang, Teng, Yulin, Shen, Yulong, Jiang, Xiaohong, and Xiao, Fu. Tag-based phy-layer authentication for ris-assisted communication systems. *IEEE Transactions on Dependable and Secure Computing*, 20(6):4778–*Forensics and Security (WIFS)*, pp. 1–6. IEEE, 2019.

[12] Yin, Xinyu, Fang, Xiaojie, Zhang, Ning, Yang, Peng, Sha, Xuejun, and Qiu, Jinghui. Online learning aided adaptive multiple attribute-based physical layer authentication in dynamic environments. *IEEE Transactions on Network Science and Engineering*, 8(2):1106–1116, 2020.

[13] Wang, Shiji, Xia, Shida, Liu, Shan, Zhang, Yan, and Cao, Chang. Transfer learning-based physical layer authentication for wireless networks handover. in *2023 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, pp. 1–6. IEEE, 2023.

[14] Gao, Ning, Han, Yu, Li, Nannan, Jin, Shi, and Matthaiou, Michail. When physical layer key generation meets ris: Opportunities, challenges, and road ahead. *IEEE Wireless Communications*, 2024.

[15] Wan, Zheng, Huang, Kaizhi, Xu, Xiaoming, Yi, Ming, Wang, Hui-Ming, Zhu, Zhengyu, and Jin, Liang. Ris-assisted integration of communications and security: Protocol, prototyping, and field trials. *IEEE Internet of Things Journal*, 2024.

[16] Hu, Xiaoyan, Jin, Liang, and Huang, Kaizhi. Secret key generation assisted by intelligent reflecting surface with discrete phase shift in static environment. *Authorea Preprints*, 2023.

[17] Shahiri, Vahid, Behroozi, Hamid, and Kuhestani, Ali. Intelligent reflecting surface assisted secret key generation under spatially correlated channels in quasi-static environments. *arXiv preprint arXiv:2212.01563*, 2022.

[18] Hu, Lei, Li, Guyue, Luo, Hongyi, and Hu, Aiqun. On the ris manipulating attack and its countermeasures in physical-layer key generation. in *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*, pp. 1–5. IEEE, 2021.

[19] Xiao, Qingjiang, Zhao, Jinrong, Feng, Sheng, Li, Guyue, and Hu, Aiqun. Securing nextg networks with physical-layer key generation: A survey. *Security and Safety*, 3:2023021, 2024.

[20] Wang, Ning, Li, Weiwei, Wang, Pu, Alipour-Fanid, Amir, Jiao, Long, and Zeng, Kai. Physical layer authentication for 5g communications: Opportunities and road ahead. *IEEE Network*, 34(6):198–204, 2020.

[21] Mughal, Umair Ahmad, Alkhrijah, Yazeed, Almadhor, Ahmad, and Yuen, Chau. Deep learning for secure uav-

in uav-aided communication systems. in *2023 International Conference on Networking and Network Applications (NaNA)*, pp. 18–22. IEEE, 2023.

[41] Xie, Ning and Hu, TianXing. Improving the covertness in the physical-layer authentication. *China Communications*, 18(3):122–131, 2021.

[42] Xie, Ning, Chen, Changsheng, and Ming, Zhong. Security model of authentication at the physical layer and performance analysis over fading channels. *IEEE Transactions on Dependable and Secure Computing*, 18(1):253–268, 2018.

[43] Zeng, Kai, Govindan, Kannan, and Mohapatra, Prasant. Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]. *IEEE Wireless Communications*, 17(5):56–62, 2010.

[44] Bai, Lin, Zhu, Lina, Liu, Jianwei, Choi, Jinho, and Zhang, Wei. Physical layer authentication in wireless communication networks: A survey. *Journal of Communications and Information Networks*, 5(3):237–264, 2020.

[45] Zhou, Yi, Ma, Zheng, Liu, Heng, Yeoh, Phee Lep, Li, Yonghui, and Vucetic, Branka. Signal-to-noise ratio based physical layer authentication in uav communications. in *2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1–6. IEEE, 2023.

[46] Abdrabou, Mohammed and Gulliver, T Aaron. Threshold-based physical layer authentication for space information networks. in *2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, pp. 289–293. IEEE, 2022.

[47] Illi, Elmehdi, Qaraqe, Marwa, and El Bouanani, Faissal. A novel hybrid physical layer authentication scheme for multiuser wireless communication systems. *IEEE Internet of Things Journal*, 2023.

[48] Assaf, Tasneem, Al-Dweik, Arafat, Iraqi, Youssef, Jangsher, Sobia, Pandey, Anshul, Giacalone, Jean-Pierre, Abulibdeh, Enas E, Saleh, Hani, and Mohammad, Baker. High-rate secret key generation using physical layer security and physical unclonable functions. *IEEE Open Journal of the Communications Society*, 4:209–225, 2023.

[49] Tan, Haijun, Xie, Ning, Lu, Jian, and Niyato, Dusit. Generalized tag-based physical-layer authentication un-

4792, 2023.

[31] Shan, Dan, Zeng, Kai, Xiang, Weidong, Richardson, Paul, and Dong, Yan. Phy-cram: Physical layer challenge-response authentication mechanism for wireless networks. *IEEE Journal on selected areas in communications*, 31(9):1817–1827, 2013.

[32] Du, Xianru, Shan, Dan, Zeng, Kai, and Huie, Lauren. Physical layer challenge-response authentication in wireless networks with relay. in *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, pp. 1276–1284. IEEE, 2014.

[33] Wang, Pu, Yan, Zheng, and Zeng, Kai. Bcauth: Physical layer enhanced authentication and attack tracing for backscatter communications. *IEEE Transactions on Information Forensics and Security*, 17:2818–2834, 2022.

[34] Chen, Chen, Zhang, Junqing, Lu, Tianyu, Sandell, Magnus, and Chen, Liquan. Secret key generation for irs-assisted multi-antenna systems: A machine learning-based approach. *IEEE Transactions on Information Forensics and Security*, 19:1086–1098, 2023.

[35] Wang, Jian, Shao, Yameng, Wang, Yancong, Ge, Yuming, and Yu, Rundong. Physical layer authentication based on nonlinear kalman filter for v2x communication. *IEEE Access*, 8:163746–163757, 2020.

[36] Rahman, Muhammad Mahboob Ur, Abbasi, Qammer H, Chopra, Nishtha, Qaraqe, Khalid, and Alomainy, Akram. Physical layer authentication in nano networks at terahertz frequencies for biomedical applications. *Ieee Access*, 5:7808–7815, 2017.

[37] Xie, Ning, Tan, Haijun, Huang, Lei, and Liu, Alex X. Physical-layer authentication in wirelessly powered communication networks. *IEEE/ACM Transactions on Networking*, 29(4):1827–1840, 2021.

[38] Fang, He, Wang, Xianbin, and Hanzo, Lajos. Learning-aided physical layer authentication as an intelligent process. *IEEE Transactions on Communications*, 67(3):2260–2273, 2018.

[39] Xie, Ning and Zhang, Shengli. Blind authentication at the physical layer under time-varying fading channels. *IEEE Journal on Selected Areas in Communications*, 36(7):1465–1479, 2018.

[40] Teng, Yulin, Zhang, Pinchang, Liu, Yangyang, and Liu, Xin. Phy-layer authentication with hardware impairments

against eavesdropping attacks. *IEEE Systems Journal*, 17(1):1581–1590, 2022.

[59] Lu, Xiaozhen, Xiao, Liang, Li, Pengmin, Ji, Xiangyang, Xu, Chenren, Yu, Shui, and Zhuang, Weihua. Reinforcement learning-based physical cross-layer security and privacy in 6g. *IEEE Communications Surveys & Tutorials*, 25(1):425–466, 2022.

[60] Mpitziopoulos, Aristides, Gavalas, Damianos, Konstantopoulos, Charalampos, and Pantziou, Grammati. A survey on jamming attacks and countermeasures in wsns. *IEEE communications surveys & tutorials*, 11(4):42–56, 2009.

[61] Tan, Haijun, Li, Zhuoyuan, Xie, Ning, Lu, Jian, and Niyato, Dusit. Detection of jamming attacks for the physical-layer authentication. *IEEE Transactions on Wireless Communications*, 22(12):9579–9594, 2023.

[62] Avila, J, Prem, S, Sneha, R, and Thenmozhi, K. Mitigating physical layer attack in cognitive radio-a new approach. in *2018 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1–4. IEEE, 2018.

[63] Lu, Bingxian, Qin, Zhenquan, Yang, Mingyi, Xia, Xu, Zhang, Renjie, and Wang, Lei. Spoofing attack detection using physical layer information in cross-technology communication. in *2018 15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pp. 1–2. IEEE, 2018.

[64] Huang, Yunsong, Liu, Weicheng, and Wang, Hui-Ming. Hidden backdoor attack: A new threat to learning-aided physical layer authentication. in *2023 International Conference on Ubiquitous Communication (Ucom)*, pp. 310–314. IEEE, 2023.

[65] Cai, Yufeng, Wang, Wenya, Chen, Yicong, Tan, Haijun, Xie, Ning, and Wang, Jiangzhou. Multiple cooperative attackers for tag-based physical layer authentication. *IEEE Communications Magazine*, 61(7):165–171, 2023.

der frequency selective fading channels. *IEEE Transactions on Communications*, 71(5):2876–2890, 2023.

[50] Xie, Ning, Xiong, Wei, Sha, Mingrui, Hu, Tianxing, Zhang, Peichang, Huang, Lei, and Niyato, Dusit. Physical layer authentication with high compatibility using an encoding approach. *IEEE Transactions on Communications*, 70(12):8270–8285, 2022.

[51] Mehmood, Ahsan, Aman, Waqas, Rahman, M Mahboob Ur, Imran, Muhammad Ali, and Abbasi, Qammer H. Preventing identity attacks in rfid backscatter communication systems: A physical-layer approach. in *2020 International Conference on UK-China Emerging Technologies (UCET)*, pp. 1–5. IEEE, 2020.

[52] Zhang, YongBin, Jin, Liang, and Han, Qian. Physical layer authentication mechanism based on interpolated polynomial method. in *2021 International Conference on Advanced Computing and Endogenous Security*, pp. 1–5. IEEE, 2022.

[53] Han, Boliang, Gao, Zhenzhen, Liao, Xuewen, and Li, Kangze. One-class physical layer authentication under time-varying fading channels. in *2023 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 1–6. IEEE, 2023.

[54] An, Yongli, Bai, Haifei, Zhang, Shikang, and Ji, Zhanlin. Physical layer authentication of mimo-stbc systems based on constellation dithering. *Intelligent and Converged Networks*, 4(4):355–365, 2023.

[55] Afeef, Liza, Furqan, Haji M, and Arslan, Hüseyin. Physical layer authentication scheme in beamspace mimo systems. *IEEE Communications Letters*, 26(7):1484–1488, 2022.

[56] Wang, Shaoyu, Huang, Kaizhi, Xu, Xiaoming, Zhong, Zhou, and Zhou, You. Csi-based physical layer authentication via deep learning. *IEEE Wireless Communications Letters*, 11(8):1748–1752, 2022.

[57] Angueira, Pablo, Val, Iñaki, Montalban, Jon, Seijo, Óscar, Iradier, Eneko, Fontaneda, Pablo Sanz, Fanari, Lorenzo, and Arriola, Aitor. A survey of physical layer techniques for secure wireless communications in industry. *IEEE Communications Surveys & Tutorials*, 24(2):810–838, 2022.

[58] Topal, Ozan Alp and Kurt, Gunes Karabulut. Whispering lies to the eavesdropper: Physical layer spoofing

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2024, Volume 22, Number 1 (pp. 38–60)
https://monadi.isc.org.ir

An overview of physical-layer authentication methods, performance metrics, and their vulnerabilities to attacks

Parsa Rajabi [1], Seyed Mohammad Razavizadeh [1,*], Mohammad Hesam Tadayon [2]

[1] *Electrical Engineering, Iran University of Science & Technology, Tehran, Iran*
[2] *Iran Telecommunication Research Center, Tehran, Iran*

ARTICLE INFO.

Article history:
Received: March 30, 2024
Accepted: July 31, 2024
Published Online: August 19, 2024

Keywords:
Physical layer authentication
Physical layer attacks
Cryptography
Performance metrics
Physical layer features

Type: Research paper

ABSTRACT

Authentication plays a pivotal role in ensuring communication security. Cryptographic methods are frequently employed to fulfill this purpose. These methods, implemented at upper network layers, encounter challenges including complexity, power consumption, and overhead. Particularly for users with limited computational power, these methods encounter challenges. A novel solution to overcome these challenges is physical layer authentication (PLA), which involves utilizing physical layer features to embed a tag in the transmitted signal for authentication, leveraging various channel characteristics such as position, velocity, noise, etc. In this paper, a review of previous research is provided, highlighting the differences between physical layer and upper-layer authentication. Furthermore, existing categorizations for PLA and a novel classification based on covertness levels are provided. Moreover, possible attacks and corresponding countermeasures are investigated, followed by suggestions for future research in this area.

© 2024 ISC

* Corresponding author
Email addresses: h_norouzi@aut.ac.ir (Parsa Rajabi), h_norouzi@aut.ac.ir (Seyed Mohammad Razavizadeh), niksefat@aut.ac.ir (Mohammad Hesam Tadayon)
© 2024 ISC. All rights reserved.