مرکزتخصصی آپا دانشگاه بیرجند

فرصت‌ها، تهدیدات و الزامات امنیتی 5G

شماره نگارش ۱/۰

طبقه‌بندی ..... عادی

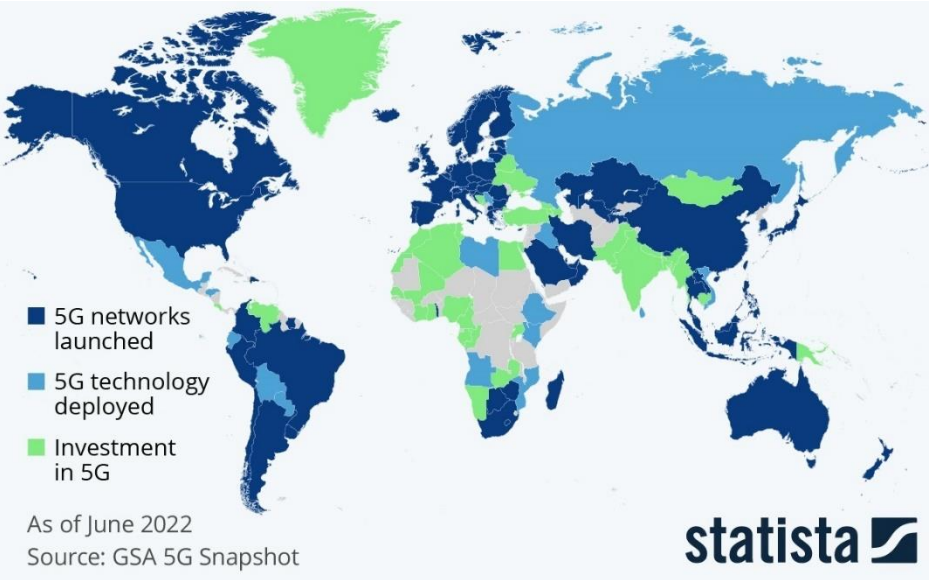
فهرست مطالب

۱. مقدمه

سیستم‌های بی‌سیم نسل پنجم (5G)، هم‌اکنون جدیدترین نسل سیستم‌های ارتباطات سیار سلولی هستند که نه تنها تکامل یافته شبکه‌های سلولی 4G می‌باشند، بلکه سرویس‌های جدید بسیاری نیز به آن افزوده شده است. هدف از تحقیق و توسعه 5G افزودن ویژگی‌های پیشرفته متعددی مانند ظرفیت بالاتر از 4G، تراکم بالاتر کاربران و پشتیبانی از ارتباطات دستگاه به دستگاه (D2D) و ارتباطات گسترده نوع ماشین است. همچنین به این موارد می‌توان تأخیر و مصرف انرژی کمتر 5G را برای پیاده‌سازی بهتر اینترنت اشیاء (IoT) اضافه نمود. به بیان دقیق‌تر، اتصالات ۱ تا ۱۰ گیگابیت بر ثانیه تا نقاط پایانی در میدان (برد رادیویی)، تأخیر ۱ میلی‌ثانیه، پهنای باند ۱۰۰۰ برابری در واحد سطح، ۱۰ تا ۱۰۰ برابر شدن تعداد دستگاه‌های متصل، ۹۹/۹۹۹ درصد دسترس‌پذیری، پوشش ۱۰۰ درصدی، کاهش ۹۰ درصدی مصرف انرژی شبکه و بیش از ۱۰ سال عمر باتری برای دستگاه‌های کم مصرف جزء ۸ ویژگی پیشرفته سیستم‌های بی‌سیم 5G هستند. برای دستیابی به این الزامات عملکردی، فناوری‌های مختلفی برای سیستم‌های 5G مانند شبکه‌های ناهمگن (HetNet)، چند ورودی - چند خروجی (MIMO)[1] گسترده، موج میلی‌متری (mmWave)، ارتباطات دستگاه به دستگاه (D2D)، شبکه نرم‌افزار محور (SDN)[2]، مجازی‌سازی توابع شبکه (NFV)[3] و تقسیم‌بندی شبکه[4] به کار گرفته شده‌اند.

امروزه با افزایش سرویس‌ها و حجم ترافیک، میل به سرعت بیشتر در شبکه‌های ارتباطی اجتناب‌ناپذیر است. شکل ۱ پوشش جهانی شبکه‌های ارتباطی و میزان توسعه 5G را در ژوئن ۲۰۲۲ نمایش می‌دهد. کشورهای چین و آمریکا در این حوزه پیش رو هستند.

[1] multiple-input multiple-output
[2] Software Defined Network
[3] Network Functions Visualization
[4] networking slicing



شکل ۱- نقشه پوشش جهانی 5G

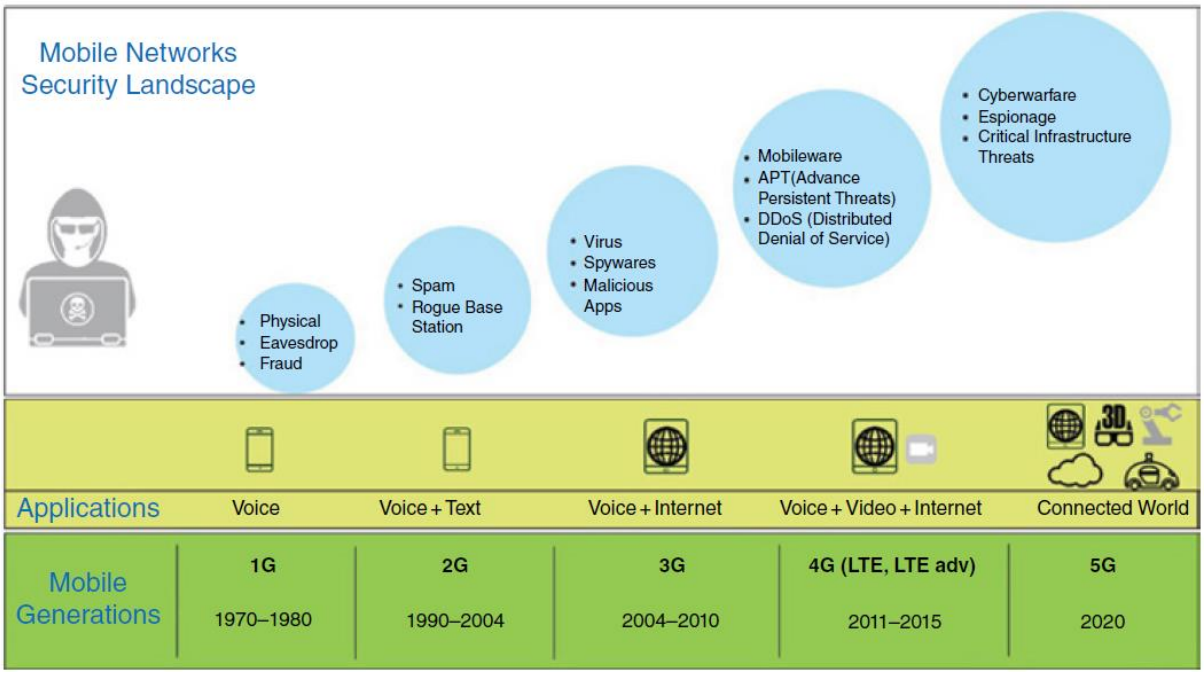
ظهور کسب‌وکارهای جدید، معماری متفاوت و فناوری‌های نوظهور موجود در 5G، چالش‌های نوینی را در توسعه آن به همراه داشته است. از جمله این چالش‌ها می‌توان به موارد زیر اشاره کرد:

- **محدودیت رنج فرکانسی در شبکه‌های 5G** – بسیاری از شبکه‌های 5G با فرکانس رادیویی بالا به نام امواج میلی‌متری کار می‌کنند که قابلیت حمل داده‌های زیادی را دارند (برای مثال، برای پخش سریع‌تر فیلم‌های HD اما در محدوده محدود اغلب کمتر از یک مایل مربع). داده‌های منتقل شده از طریق این طیف فرکانسی به راحتی توسط اشیاء معمول مانند درختان و ساختمان‌ها مسدود می‌شوند.
- **عدم سازگاری دستگاه‌ها** – اکثر تولیدکنندگان دستگاه‌های ارتباطی مانند تلفن‌ها، تبلت‌ها نسخه‌های سازگار با 5G را منتشر نکرده‌اند.
- **هزینه بالای توسعه** - پیش‌بینی می‌شود که شرکت‌های مخابراتی قبل از سال ۲۰۲۵ به اندازه ۲۷۵ میلیارد دلار در زیرساخت‌های 5G سرمایه‌گذاری کنند. یک اپراتور شبکه تلفن همراه باید قبل از راه‌اندازی 5G هزینه‌های زیر را متحمل شود:
  - مجوز طیف فرکانسی

- سخت‌افزار فیزیکی مورد استفاده در استقرار 5G
- استخدام نیروی متخصص برای نصب سخت‌افزار لازم
- تست و آزمایش مجدد شبکه

بدون شک یکی از مهم‌ترین چالش‌های فراروی کاربران، حفظ امنیت و حریم خصوصی است. کاربران در حال حاضر به اهمیت این دو موضوع واقف هستند، از این رو در محیط کسب‌وکار 5G، امنیت و حریم خصوصی جزء عوامل ضروری برای تداوم تجارت هستند.

چشم انداز امنیت شبکه‌های موبایلی (همان طور که در شکل ۲ نمایش داده شده است) باید در پرتو این مسئله مورد توجه قرار گیرد که نسل‌های مختلف موبایل چگونه تکامل یافته‌اند. رابطه مستقیمی بین تکامل تکنولوژی شبکه موبایل و تکامل نسبی تهدیدات امنیتی به لحاظ معماری، تکنولوژی، قابلیت‌های فنی، سرویس‌های ارائه شده و عوامل تهدید مربوطه وجود دارد.



شکل ۲- چشم انداز امنیت شبکه های موبایلی

شبکه‌های موبایل بلافاصله بعد از آغاز به کار اولین نسل تکنولوژی موبایل (که 1G نیز گفته می‌شود)، شاهد تهدیدات و چالش‌هایی بودند و علیرغم همین تهدیدات، با چشم اندازی پیچیده و چالش برانگیز به رشد

ادامه داده‌اند. 1G در درجه اول برای ارائه قابلیت جابجایی به کاربران صوتی عرضه شد. در این تکنولوژی مشتریان شاهد آزادی خود در برقراری تماس تلفنی ضمن جابجایی بودند. مجرمان نیز روش‌هایی کشف کردند که به واسطه آن‌ها دست به کلاهبرداری موبایلی و جا زدن خود به عنوان مشترکان قانونی می‌کردند تا از این طریق از تماس رایگان بهره‌مند شوند. از این رو به سرعت کلونینگ یا جعل تلفن‌های همراه با تولید و فروش تلفن‌های کلون شده غیرقانونی (تلفن جعل شده تلفنی است که برای انتقال ESN و MIN یک تلفن همراه مجاز دیگر برنامه نویسی شده است) به یک صنعت تبدیل شد. برخی هکرها راه‌های جدیدی برای استراق سمع تماس‌ها یافتند و به مکالمات خصوصی با انگیزه های مخرب گوش می‌دادند.

با 2G، دوره اسپمینگ پیام‌ها (spamming) در دنیای موبایل آغاز شد. اسپمینگ به عنوان حمله گسترده ای جهت تزریق اطلاعات اشتباه یا فرستادن تبلیغات ناخواسته به ابزارهای موبایل مورد استفاده قرار می‌گرفت. صندوق دریافت پیام‌ها پر از پیام‌های اسپمی می‌شد که گروه خاص یا عموم جامعه را مورد هدف قرار می‌دادند. کلاهبرداران از اسپمینگ موبایل برای نیت‌های پلید خود بهره می‌گرفتند.

با هوشمندتر و پیچیده تر شدن ابزارهای کاربری، اپلیکیشن‌های داده و اینترنت نیز به سرویس‌های اصلی ارائه شده توسط ارائه کنندگان خدمات موبایل در شبکه های 3G تبدیل شدند. سرعت یک اتصال داده 3G معمولی حدود ۵۰۰ تا ۷۰۰ کیلوبیت بر ثانیه بود که برای ارائه ارتباط اینترنت اپلیکیشن ها کافی بود. خط سیر تهدیدات در 3G به سرعت تلفن‌های کاربران، سیستم‌های کاربری و سیستم‌های عامل آن‌ها را مورد هدف قرار داد. از این رو هر از چند گاهی آسیب‌پذیری‌های سیستم عامل موبایل مورد استفاده قرار می‌گرفت، زیرا برنامه‌های کاربردی موبایلی دارای کدهای زیانبار برای کسب دسترسی غیرمجاز به اطلاعات حساس شخصی، مانند تماس‌ها، گذرواژه کاربران و داده‌های مکان بودند. با افزایش سرعت داده‌ها، تنوع بدافزارها و ابزارهای جاسوسی نیز بیشتر شد.

با LTE برای اولین بار شبکه موبایل به یک معماری انتها-به-انتهای (end-to-end) کاملا مبتنی بر IP تبدیل شد. این کار به ارائه کنندگان خدمات در رابطه با سرعت نوآوری کمک می‌کرد، مقیاس و سرویس های جدیدی عرضه می نمود و همچنین پتانسیل تهدید شبکه‌های 4G را نیز افزایش می‌داد. DDoS

(جلوگیری از سرویس توزیع شده) و APT (تهدیدات پیوسته پیشرفته) واقعیت‌های جدید برای شبکه موبایل بودند، چرا که ضربه آن ها به سرویس‌دهی شدید و همراه با خسارات مالی عظیم بود. حمله کنندگان سازمان یافته‌تر شده و شروع به دنبال‌کردن روشی سیستمی در اجرای تهدیدات خود بودند. از سوی دیگر شناسایی حضور مخفیانه آن‌ها در شبکه موبایل دشوارتر شده است، در حالی که به طور میانگین یک حمله، ماه ها زمان می برد.

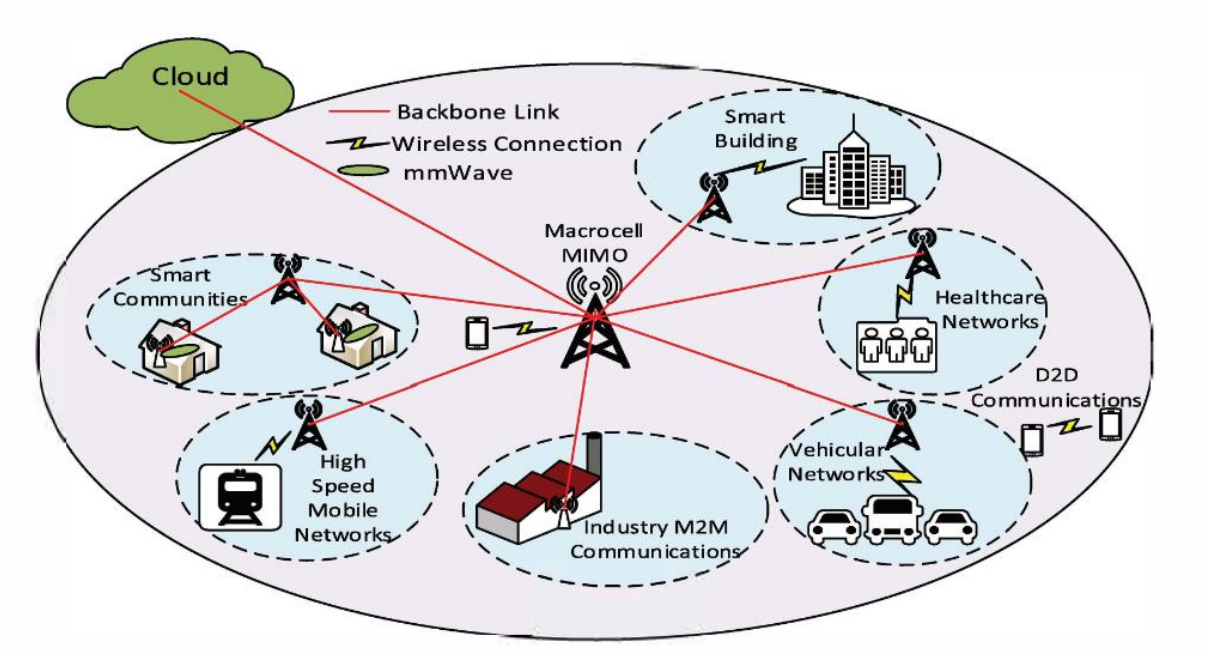
5G با وعده اتصال دادن میلیاردها ابزار و تلفن همراه با پهنای باندی بسیار قابل اطمینان و متراکم معرفی شد که دارای زیرساخت شبکه‌ای سریع و تحمل پذیر نسبت به نواقص بوده و چندین بخش و صنعت را سرویس‌دهی می‌کند. موارد کلیدی استفاده از 5G شامل زیرساخت‌های حیاتی، اینترنت اشیا، شهرهای هوشمند و دنیای کاملا متصل است. با این موارد کاربرد، 5G هدف ایده آل برای حمله کنندگانی خواهد بود که ممکن است به دنبال ایجاد اخلال گسترده اجتماعی و اقتصادی در یک بازه زمانی کوچک باشند. تهدیدات 5G حول محور انگیزه های مالی و منافع سیاسی خواهد بود که توسط گروه‌ها، افراد حرفه‌ای و مجرمان دارای دانش و منابع تکنولوژیکی گسترده صورت خواهد گرفت. چشم انداز تهدید 5G، پویا و مبتنی بر تهدیدات پیشرفته و پیچیده ای همچون بدافزارهای flame و استاکسنت (stuxnet) خواهد بود.

با توسعه فناوری بی‌سیم، مکانیزم‌های امنیتی سخت‌تری برای محافظت از سیستم‌های ارتباطی سیار امروزی به وجود آمده است. به‌عنوان مثال، احراز هویت یک طرفه در 2G به تأیید هویت متقابل در 3G و 4G ارتقاء یافته است. همچنین الگوریتم‌های رمز و طول کلید آنها در حال ارتقاء و قوی‌تر شدن هستند. معماری‌های امنیتی سنتی بر حفاظت از صدا و داده‌ها متمرکز می‌باشند و همه آنها در ویژگی‌های امنیتی زیر مشترک هستند:

- مدیریت هویت کاربر مبتنی بر (U)SIM
- احراز هویت متقابل بین شبکه ها و کاربران
- تأمین امنیت مسیر بین طرفین ارتباط به صورت hop-by-hop

۲. فرصت‌ها

امروزه جامعه و صنعت دستخوش یک تحول دیجیتالی شده‌اند و بدیهی است که شبکه‌های موبایل موجود قادر به برآورده کردن نیازهای ارتباطی در آینده نخواهند بود؛ بنابراین یک فناوری جدید مورد نیاز است. طبق مقاله‌ای که توسط Forbes منتشر شده است، بیش از ۸۰ درصد مدیران معتقدند که 5G پتانسیل ارائه طیف وسیعی از مزایا را دارد. انتظار می‌رود در آینده نه چندان دور، صد میلیارد اتصال در سراسر جهان بین مردم، اشیاء و سازمان‌ها وجود داشته باشد. شکل ۳، یک معماری کلی از سیستم‌های بی‌سیم 5G را نشان می‌دهد. سیستم‌های بی‌سیم 5G نه تنها می‌توانند ارتباطات صوت و داده سنتی را برقرار کنند، بلکه می‌توانند کاربردهای متعددی را فراهم کنند. موارد کاربرد مختلفی برای 5G مشخص شده‌اند که از جمله آنها می‌توان ارتباطات خودرو به خودرو و خودرو به زیرساخت، اتوماسیون صنعتی، خدمات سلامت، شهرهای هوشمند و خانه‌های هوشمند را نام برد.



شکل ۳- یک معماری کلی برای سیستم‌های بی‌سیم 5G

۱,۲. افزایش پهنای باند تلفن همراه

امروزه پهنای باند اینترنت تلفن همراه به سرعت توسعه یافته و دستگاه‌های هوشمند بسیار پرطرفدار شده‌اند. در نتیجه، ویدئوهای تلفن همراه حدود ۵۰ درصد از ترافیک شبکه اپراتور را تشکیل می‌دهند و این نسبت روز به روز در حال افزایش است. همچنین گرایش به سمت سرویس‌های فراگیر بر اساس تکنولوژی‌های جدید واقعیت افزوده و واقعیت مجازی وجود دارد و مصرف‌کنندگان می‌خواهند هر جا که هستند این سرویس‌ها را تجربه کنند؛ بنابراین آنها باید قادر به استفاده از فناوری بی‌سیم باشند. این سرویس‌ها برای پهنای باند تلفن همراه (MBB)[5] بسیار مهم خواهند بود. کاربردهای قابل توجهی در اینترنت وجود دارد که نیاز به پهنای باند بالا دارند و این امر باعث گسترش سریع 5G می‌شود.

۲,۲. شبکه هوشمند انرژی

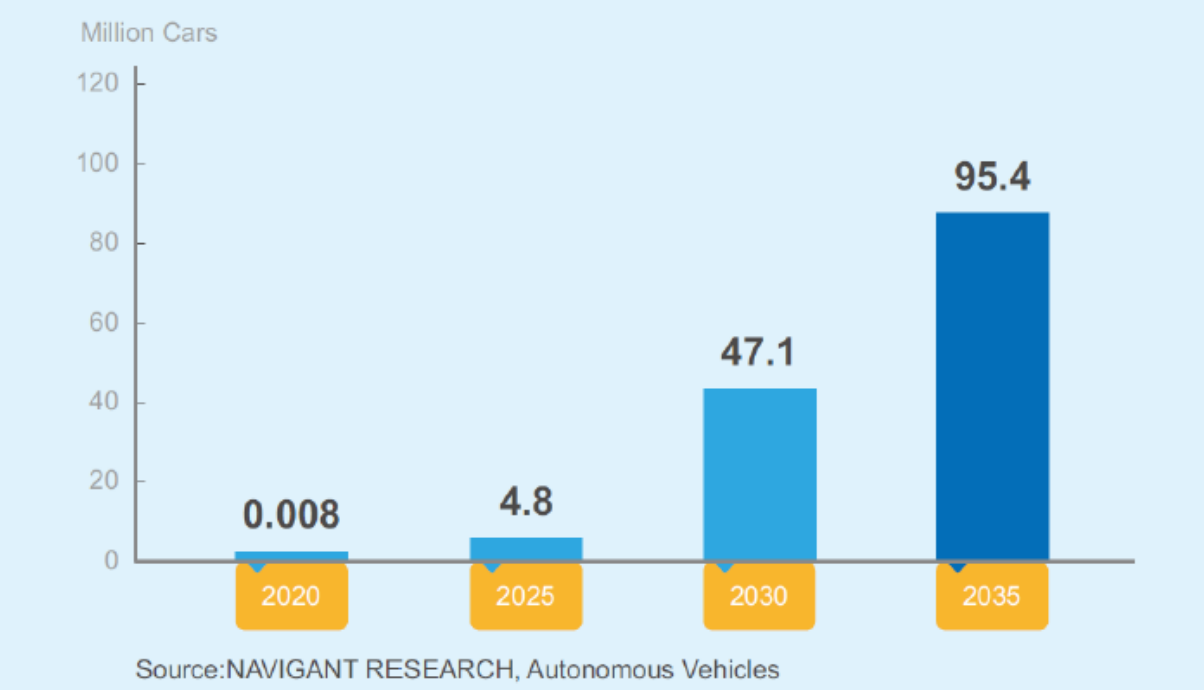
شبکه‌های هوشمند، اطلاعات، ارتباط از راه دور و اتوماسیون را در سیستم‌های سنتی نیرو ادغام می‌کنند و باعث تغییر در نحوه ذخیره‌سازی، توزیع و فروش انرژی می‌شوند. امروزه شبکه‌های هوشمند جزء ضروری استراتژی‌های ملی در زمینه انرژی در بسیاری از بازارها از جمله چین، اروپا و آمریکا محسوب می‌شوند. شبکه‌های هوشمند بر این اصل استوار هستند که همه چیز در شبکه به هم متصل و تحت نظارت و کنترل است. داده‌های مورد استفاده، وضعیت و عملکرد شبکه و تأمین انرژی از منابع تولید به صورت متمرکز جمع‌آوری می‌شوند؛ بنابراین، سیستم ارتباطات برای شبکه هوشمند یک جزء حیاتی است که تمام توان تولید، انتقال و توزیع برق و همچنین سیستم‌های مدیریت را به هم پیوند می‌دهد. این سیستم انتقال دو سویه داده‌ها بین حسگرها و سیستم‌های پایش، بین سیستم‌های کنترلی و تولید انرژی، ذخیره‌سازی و تجهیزات انتقال و بین سیستم‌های کنترلی و کنتورهای هوشمند کاربران نهایی را ممکن می‌سازد. یک شبکه هوشمند نیازمندی‌های مختلفی برای امنیت و قابلیت اطمینان، پهنای باند شبکه، تأخیر و پوشش در

[5] Mobile Broadband

پنج مرحله (تولید برق، انتقال، تبدیل، توزیع و مصرف) دارد. سیستم‌های ارتباطی موجود تمام الزامات فنی را برآورده نمی‌کنند. بی‌شک فناوری 5G راه‌حل و فرصتی بزرگ در این حوزه محسوب می‌گردد.

۳,۲. رانندگی هوشمند

صنعت اتومبیل در ابتدای راه تغییر و تحولی قرار دارد که تحقق آن ۱۵ تا ۲۰ سال طول خواهد کشید. میلیاردها دلار در ارتباط با فناوری‌های وسایل نقلیه پیشرفته سرمایه‌گذاری شده است که معرفی سیستم‌های ایمن جدید و در نهایت خودروهای بدون راننده را ممکن می‌سازد. نسل‌های آینده اتومبیل‌ها برای برقراری ارتباط با یکدیگر، با سیستم‌های کنترل ترافیک محلی، با تولیدکنندگان و با ارائه‌دهندگان سرویس شخص ثالث نیاز به ارتباطات بی‌سیم پیچیده‌ای خواهند داشت. همانطور که در شکل ۴ نشان داده شده است، تعداد وسایل نقلیه خودران تا سال ۲۰۳۵ به ۹۵/۴ میلیون خواهد رسید. همچنین طبق گزارش Accenture، همه خودروهای جدید تا سال ۲۰۲۵ به هم متصل خواهند شد.



شکل ۴- پیش‌بینی تعداد وسایل نقلیه خودران

۴٫۲. تولید هوشمند

در چشم‌انداز انقلاب صنعتی چهارم، کارخانجات آینده بر پایه سیستم‌های سایبری فیزیکی خواهند بود. آنها محاسبات، فرآیندهای فیزیکی و تحت شبکه را به منظور بهبود روش‌های اجرایی در کسب‌وکارهای تولیدی ادغام خواهند کرد. کل زنجیره تأمین تولید به هم متصل خواهند شد. داده‌هایی در مورد جنبه‌های کلیدی کسب‌وکار مانند طراحی، تولید و توزیع و اطلاعاتی درباره تجهیزات و محصولات و حتی داده‌های مربوط به مشتریان و تأمین‌کنندگان بین مکان‌های مختلف به اشتراک گذاشته می‌شوند تا عملیات در تمامی این حوزه‌ها بهبود یابند. همچنین کارخانه‌ها به ربات‌های تولیدی توانمندتر و حسگرها و سیستم‌های خودکار مجهز می‌شوند؛ بنابراین این امر منجر خواهد شد تا تقاضای تولید افزایش یافته و انعطاف‌پذیری تولید و بهره‌وری نیز بهبود یابد. همه این تحولات بر اساس اشتراک‌گذاری و تجزیه و تحلیل گسترده داده خواهد بود. این انتشار اطلاعات تنها در صورتی می‌تواند اتفاق بیفتد که زیرساخت مخابراتی بی‌سیم قوی وجود داشته باشد و طیف گسترده‌ای از تجهیزات (کنترل سیستم‌ها و محصولات) توانایی برقراری ارتباط را داشته باشند.

۵٫۲. سلامت

در حال حاضر، فشارهای وارده بر سیستم‌های بهداشت جهانی بسیار زیاد است. رشد و سالخوردگی جمعیت به این معنی است که تداوم ارائه خدمات مراقبت سلامت با روش‌های سنتی بسیار پرهزینه خواهد بود. دولت‌ها در پاسخ به این نیاز باید به دنبال روش‌های جدید و فناوری‌های مراقبت سلامت از راه دور باشند که می‌توانند منجر به کاهش هزینه‌ها، افزایش کارایی فرایندها و بهبود سلامت جمعیت شوند. در عین حال به افراد، مجموعه‌ای از خدمات مراقبت سلامت یا پایش سلامت از راه دور ارائه می‌شود؛ از این رو، امروزه بشریت در حال تحقق سلامت الکترونیکی برای افزایش دسترسی به خدمات پزشکی و کاهش هزینه‌های مربوط به آن می‌باشد. دستگاه‌های تلفن همراه هم‌اکنون به‌عنوان بخشی از فرایند تشخیص پزشکی یا درمانی در سراسر جهان مورد استفاده قرار می‌گیرند. طبق یک نظرسنجی صورت گرفته از ۱۵ هزار نفر در

۱۵ کشور جهان، ۴۴ درصد از مردم با پزشکانی برخورد داشته‌اند که در طول درمان یا تشخیص بیماری از دستگاه تلفن همراه استفاده می‌کنند. از جمله کاربردهای شبکه‌های 5G در حوزه سلامت عبارتند از:

خدمات مراقبت سلامت از راه دور: شامل تشخیص بیماری از راه دور و مشاوره از طریق ارتباط تصویری

پایش سلامت شخصی: استفاده از حسگرهای ناحیه بدن برای مدیریت سلامت افراد از جمله نظارت و مدیریت پزشکی هوشمند

اتوماسیون مراقبت خانگی/کمک زندگی: ترکیب اطلاعات ابری و حسگرها به منظور مدیریت و تغییر تنظیمات مراقبت به صورت خودکار

مدیریت دارایی: استفاده از فناوری‌های بی‌سیم برای ردیابی و نظارت بر تجهیزات

جراحی از راه دور: جراحان قادر به انجام عملیات از راه دور، با استفاده از ویدئو و رباتیک و در آینده با استفاده از واقعیت افزوده خواهند بود.

تجاری: دستگاه‌هایی که توسط مصرف‌کنندگان خریداری می‌شوند تا سلامت خود را پیگیری کنند یا فعالیت و رفتارهای خود را نظارت کنند.

۳. تهدیدات

احتمالا در سال نه چندان دور، شاهد رانندگی اتومبیل‌های بدون راننده و پرواز پهپادهای بدون خلبان زیادی خواهیم بود. برای کنار آمدن با هجوم این دسته از سرویس‌های جدید که از اینترنت استفاده می‌کنند قطعا به سطح جدیدی از ارتباطات بی‌سیم نیاز خواهد بود و تمام این دستگاه ها برای ارتباط مؤثر و سریع به فناوری ارتباطی نسل پنجم تلفن همراه نیاز خواهند داشت. نسل پنجم تلفن همراه روشی به مراتب هوشمندتر برای دستگاه‌ها محسوب خواهد شد تا به اینترنت دسترسی پیدا کنند. با توجه به این امر، دستگاه هایی که به این شبکه ارتباطی متصل می شوند نیز باید از هوشمندی مناسبی برخوردار باشند. 5G یا ظهور اشیای متصل به اینترنت هر چیزی از ماشین های لباسشویی گرفته تا مترهای هوشمند، دوربین های ترافیکی، اتومبیل های بدون راننده، جاده‌های هوشمند و حس‌گرهایی که به یک درخت متصل شده-

اند، به طور پیوسته اطلاعات را از طریق اینترنت با یکدیگر به اشتراک می‌گذارند. بر اساس پیش بینی‌ها، در سال ۲۰۲۵ بیش از ۲۷ میلیارد شی، به اینترنت متصل می‌شوند. به راحتی می توان متوجه شد که چه حجمی از اطلاعات باید منتقل شوند و اینترنت نسل پنجم این امیدواری را می‌دهد تا این دستگاه‌ها و اشیاء مختلف به راحتی کار کنند. شاید با داشتن این حجم از اشیاء و دستگاه‌های متصل به اینترنت که با استفاده از فناوری نسل پنجم تلفن همراه با یکدیگر متصل شده و اطلاعات را به اشتراک می گذارند، دیدن یک شهر هوشمند دیگر دور از انتظار نباشد. یکی از کاربردهای 5G دسترسی بی سیم ثابت (FWA) است که بطور کامل یا مقطعی جایگزین اتصالات اینترنتی کنونی خواهد شد. در اینجا «ثابت» به معنی خدمات بی‌سیمی می باشد که به موقعیت‌ها و ابزارهای ثابت در خانه‌ها و ادارات ارائه می شود. یک پایانه دسترسی بیسیم ثابت شامل موارد ذیل است که اغلب در یک جعبه فیزیکی متمرکز شده است: تجهیزات کاربری و نقطه دسترسی وای فای. تجهیزات کاربری، اتصال دسترسی بی سیم ثابت به شبکه را فراهم می‌کند، و نقطه دسترسی وای فای که به تجهیزات کاربری متصل است، ابزارهای خانگی را قادر می‌سازد به دسترسی بی-سیم ثابت متصل شوند. در نتیجه دسترسی بی سیم ثابت به عنوان یک دروازه بین هر ابزار متصل شده‌ای در خانه و شبکه خارجی عمل می‌کند.

شبکه‌های مخابراتی در حال حاضر رو به رشد هستند ولیکن تعداد وسایل متصل به شبکه با سرعت بیشتری افزایش پیدا می‌کند و در ضمن هنوز آن گونه که باید و شاید وارد دوران وسایل هوشمند نشده‌ایم. در دوران پیش رو، فقط گوشی و تبلت به شبکه متصل نیستند بلکه یخچال، ماشین لباس شویی، اجاق‌ها و مایکروفرها، قهوه جوش‌ها و سماورهای برقی، کولرها و دستگاه‌های تهیه مطبوع، لامپ‌ها و وسایل الکترونیکی منزل مثل تلویزیون و اسپیکر، همه و همه از طریق اینترنت با کاربر در ارتباط هستند. هر کجا که باشیم فرقی نمی‌کند، می‌توانیم با وسایل هوشمند منزل ارتباط برقرار کنیم و دستور دهیم و این چیزی است که به شبکه‌ای با بازدهی بالاتر، سرعت بیشتر و تأخیر کمتر نیاز دارد. در صنایع و کارخانه‌ها و همین طور وسایل هوشمند داخل شهر مثل اتوبوس‌ها، خودروها، چراغ‌های راهنمایی، دوربین های ترافیکی و حتی سیستم آبیاری خودکار پارک و فضای سبز هم می‌توان با هوشمندی بیشتر و دسترسی گسترده به اینترنت،

کارها را ساده کرد. به همین جهت است که شبکه‌ای سریع تر و بهینه‌تر می‌تواند همگام با دنیای هوشمند امروز، معرفی شده و رشد کند. اریکسون یکی از فعالان جهانی است که در پیاده سازی نسل پنجم تلفن همراه دخیل است که یکی از حوزه های فعالیتش دسترسی بی سیم ثابت است که به طور کامل یا تا حدی جایگزین اتصالات پهن باند ثابت مسکونی خواهد شد.

با توجه به فضایی که این روزها بر دنیا حاکم است، سرعت و پهنای باند بیشتر برای موبایل‌ها کم کم تبدیل به واقعیتی شده است و در نوک پیکان این فناوری، نسل چهارم شبکه تلفن همراه قرار گرفته است. LTE مخفف کلمات Long Term Evolution و به معنی «تحول طولانی مدت» هست. در حالی که LTE جدید رسما به عنوان نسل چهارم تلفن همراه نامیده می‌شود و پیشرفت‌های زیادی نسبت به نسل سوم تلفن همراه فعلی دارد، امکانات این شبکه نه تنها به نفع مصرف کننده است که برای سرویس دهنده‌های شبکه مخابراتی نیز کار آمد است.

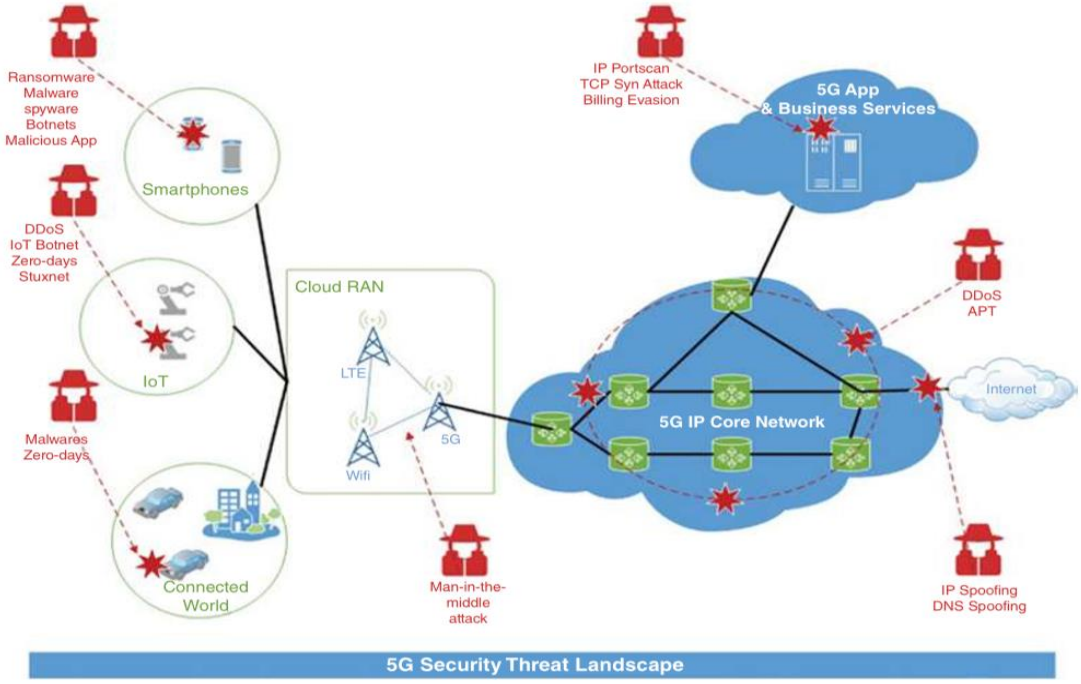
LTE در سرتاسر دنیا به عنوان اولین شبکه مخابراتی تلفن همراه مورد استفاده قرار گرفته است و نسل های گذشته با 2G و 3G به آرامی توانسته است شبکه LTE را گسترش دهد. این شبکه برای گسترش نیاز به زمان دارد و ممکن است از آنچه انتظار می رود نیز بیشتر زمان ببرد و تا آن زمان سایر فناوری‌ها نظیر CDMAو GSM نیز به حیات خود ادامه خواهند داد.

برنامه ریزی کمپانی‌های بزرگ عرضه مودم، شبکه و اینترنت به گونه‌ای است که به زودی شبکه های نسل پنجم به طور کامل عملیاتی شوند. به این ترتیب معرفی و کاربرد گسترده نسل پنجم تلفن همراه نزدیک است. الکس جینسونگ چوآ، مدیر فنی شرکت اس کا تلکام، در اظهار نظری گفت:« فناوری نسل پنج به شکل قابل توجهی زندگی مردم را تغییر خواهد داد». مت گراب، نایب رئیس اجرایی و مدیر فنی شرکت فناوری های کوالکام، در همایشی گفت: «مزایای فناوری نسل پنج بسیار فراتر از ارائه‌ی سرعت بیشتر است. این فناوری شکل جدیدی از خدمات را به همراه می‌آورد که ما تابه حال شاهد آن نبوده‌ایم؛ خدماتی که دنیای واقعی و مجازی را در یکدیگر ادغام می کند، انواع مختلف ترافیک داده‌ها را ترکیب می‌کند و برای رسیدن به بهترین عملکرد، طیف‌های رادیویی گوناگون را باهم یکپارچه می‌نماید.» ونو ژاکوب فویربورن،

مدیر فنی شرکت اس کا تلکام، نیز در همین زمینه افزود: «فناوری نسل پنج تنها شکل دیگری از اتصال نیست؛ بلکه این فناوری به مدیریت زندگی دیجیتال مصرف کنندگان مربوط می شود.» در کنار این موارد، والتر ویگل، نایب رئیس شعبه اروپایی مؤسسه تحقیقات هوآوی، نیز اصرار داشت که دنیا شاهد یک انقلاب خواهد بود.

با طیف گسترده‌ای از برنامه‌ها و خدمات 5G و نقش مهم آن در خدمت به جامعه برای رشد اجتماعی، اقتصادی و ایمنی عمومی، دامنه تهدید برای 5G می‌تواند بسیار گسترده باشد. انگیزه‌های تهدید و حمله به 5G اکنون از نسل‌های قبلی شبکه بیشتر خواهد بود. شانس بیشتری وجود دارد که 5G به عنوان یک هدف اصلی برای فعالیت‌های جنایی ناشی از انگیزه‌های مختلف، از جمله انگیزه‌های سیاسی تحت حمایت دولت، مخالفان، کارتل‌های جنایات سازمان یافته، جاسوسی و جنگ سایبری باشد.

دامنه تهدیدات 5G هیچگونه مرزی نخواهد داشت و از تجهیزات کاربر نهایی مانند تلفن های همراه، وسایل صنعتی، حسگرها، اتوماسیون منزل، اتومبیل‌های خودران، شبکه‌های سازمان یافته تا شبکه‌های تلفن همراه متغیر خواهد بود. با چنین چشم اندازی، همانطور که در شکل ۵ نشان داده شده است، انواع تهدیدات موجود در شبکه، مانند تهدید تلفن‌های هوشمند از طریق باج افزار، نرم‌افزارهای جاسوسی، ربات‌ها و ... را در بر می‌گیرد.



شکل ۵- چشم انداز تهدیدات امنیتی 5G

این یک چالش جدی برای تامین کنندگان امنیت است که سیستم دفاعی مناسبی جهت محافظت از شبکه های 5G ایجاد کنند. برنامه‌های کاربردی و خدمات برای شبکه‌های 5G ۱۰ برابر خواهد بود. 5G برای زیر ساخت‌های حیاتی، سلامت، مدیریت جامعه، امور مالی، تجارت و سیستم‌های صنعتی مورد استفاده قرار خواهد گرفت. این امر چشم انداز تهدید 5G را فراتر از هر شبکه ارتباطی دیگری که تاکنون وجود داشته بزرگ می‌کند.

در حال حاظر ما این درک را داریم که قرار است معماری 5G در بالای معماری مبتنی بر IP قرار گیرد و به ارث رسد و ویژگی‌های سنتی مبتنی بر شبکه‌های تلفن همراه را به ارث ببرد. 5G نه تنها نسل بعدی شبکه تلفن همراه خواهد بود، اما همچنان بستری برای معرفی نسل بعدی تهدیدات امنیتی خواهد بود.

پیش بینی شده است که تهدیدات امنیتی نسل بعدی ویژگی‌های زیر را دارا باشد:

- پیچیده - پیچیده بودن در ماهیت که از ترکیبی چند مرحله‌ای از مسیرها و ابزارهای مختلف حمله استفاده می‌شود.
- مبهم – حمله‌هایی که توسط چندین لایه مبهم شده‌اند و تشخیص آنها بسیار سخت است.

- مخفی - تشخیص سخت و توانایی پنهان کردن خود. به عنوان مثال، حمله باج افزار.
- مداوم - این حملات مداوم بوده و خود را بعد از هر تلاش ناکام تکامل می‌دهند.

APT حملاتی هستند که ویژگی‌های فوق را دارا می‌باشند، کاهش و محافظت از آنها دشوار است و در نهایت به تهدیدهای جدی تبدیل می‌شوند که خسارات بزرگی به همراه دارد. APT معمولا امکانات مهم زیرساختی را هدف قرار می دهد و باعث ایجاد اختلال اساسی و تأثیر چند بعدی می‌شوند.

۱,۳. سلامت و 5G

یکی از بخش‌های مهم و قابل توجه در راه‌اندازی 5G در کشورهای مختلف بالاخص کشورهایی با استاندارد سلامت بالا، ایجاد مشکلاتی از قبیل افزایش دمای پوست، تغییر ژن، ترویج تکثیر سلولی و سنتز پروتئین‌های مرتبط با استرس اکسیداتیو، فرآیندهای التهابی و متابولیک است که می‌تواند باعث ایجاد آسیب‌های چشمی شود و بر پویایی عصبی-عضلانی تأثیر بگذارد. در نظر گرفتن عواملی همچون SAR در فرکانس‌ها و شرایط مختلف و اثرات آن می‌تواند، عامل خوبی جهت انتخاب نوع فرکانس برای پیاده‌سازی در کشور باشد. وضع قوانین و مقررات لازم در خصوص میزان اثر، ضریب نفوذ، محل‌های نصب دکل و زوایای آنها می‌بایست با دقت و بر اساس استانداردهای سلامت دنیا پیاده‌سازی گردد تا حداقل Side Effect را در پی داشته باشد. امروزه شهرهایی در دنیا وجود دارند که مردم با اعتراضات خود از راه‌اندازی این شبکه‌ها جلوگیری نموده‌اند، که این حوزه نیز نیاز به تحقیقات منطقه‌ای و رعایت آن دارد.

۲,۳. امنیت در 5G

5G مزایای برجسته‌ای همچون بهبود سرعت و کارایی، تأخیر کم، عمر باتری طولانی‌تر، ظرفیت بیشتر و راندمان بالاتری را به ارمغان می‌آورد. علاوه بر این، شبکه‌های 5G نه تنها برای نرخ داده‌ها با سرعت بالاتر دارای برتری هستند، بلکه یک ستون فقرات را برای بسیاری از سرویس‌های جدید در شبکه‌هایی مانند IoT و اینترنت صنعتی به وجود می‌آورند. این سرویس‌ها قابلیت اتصال را برای خودروهای بدون راننده و وسایل

نقلیه هوایی بدون سرنشین (پهپادها)، نظارت بر سلامت از راه دور از طریق حسگرهای متصل به بدن، لجستیک هوشمند از طریق ردیابی اقلام و تشخیص از راه دور فراهم می‌کنند. با این حال، افزایش بی‌اندازه تعداد دستگاه‌ها و استفاده زیاد از مجازی‌سازی و ابر منجر به تهدیدات، خطرات و حملات امنیتی چند وجهی در رابطه با 5G خواهد شد. علاوه بر این، برای تحقق ارتباطات قوی و سالم در آینده، صنعت باید استاندارد امنیتی بالایی را برای 5G فراهم نماید.

۴. الزامات امنیتی در 5G

به خاطر ماهیت پخشی محیط بی‌سیم، انتقال اطلاعات به صورت بی‌سیم، مستعد مواجه شدن با تهدیدات مخرب متعددی است. در این بخش، ۴ نوع حمله در شبکه‌های بی‌سیم 5G یعنی استراق سمع و تحلیل ترافیک، Jamming، DoS[۶] و DDoS[۷] و MITM[۸] بررسی می‌شود. همچنین چهار سرویس امنیتی شامل احراز هویت، محرمانگی، دسترس‌پذیری و جامعیت را معرفی می‌کنیم.

۱,۴. حملات در شبکه‌های بی‌سیم 5G

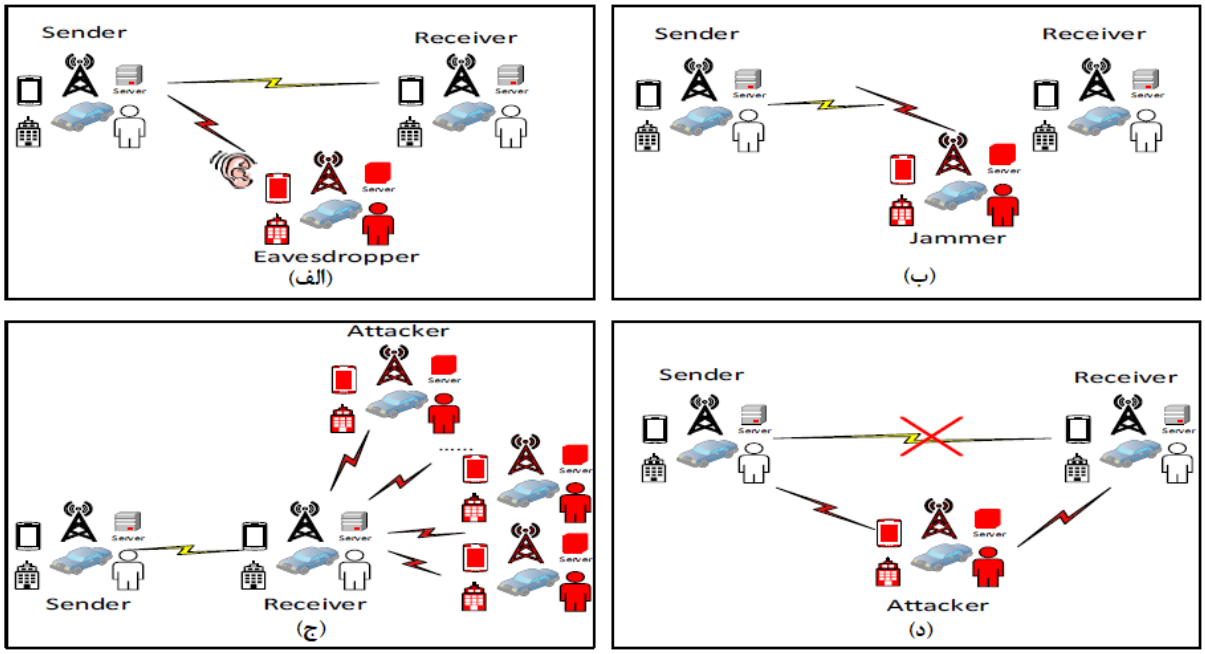
شکل ۴، هر ۴ حمله را نشان داده است که هرکدام از آنها به تفکیک از سه جنبه مورد بررسی قرار می‌گیرند: نوع حمله (فعال یا غیرفعال)، سرویس‌های امنیتی فراهم شده برای مقابله با این حمله و روش‌های متناظر به کار گرفته شده برای جلوگیری یا اجتناب از این حمله. ما بر حملات امنیتی در لایه فیزیکی و لایه MAC تمرکز می‌کنیم، جایی که در آن تفاوت‌های امنیتی بین شبکه های بی‌سیم و سیمی رخ می‌دهد.

۱,۱,۴. حمله استراق سمع و تحلیل ترافیک

[۶] Denial of Service
[۷] Distributed Denial of Service
[۸] Man in the Middle

استراق سمع، حمله‌ای است که توسط یک گیرنده غیرمجاز، برای شنود یک پیام از دیگران استفاده می‌شود. استراق سمع، یک حمله غیرفعال است؛ زیرا همان گونه که در شکل ۶ (الف) نشان داده شده است، ارتباطات معمول به وسیله استراق سمع، تحت تأثیر قرار نمی‌گیرند. به خاطر ماهیت غیرفعال بودن آن، تشخیص استراق سمع دشوار است. رمزنگاری سیگنال‌ها بر روی لینک رادیویی، پرکاربردترین روش برای مقابله با حمله استراق سمع است. استراق سمع‌کننده نمی‌تواند مستقیماً سیگنال‌های دریافتی را مشاهده کند که این امر به خاطر رمزنگاری است. تحلیل ترافیک، دیگر حمله غیرفعال است که یک گیرنده غیرمجاز برای مشاهده اطلاعات مانند مکان و هویت طرف‌های مبادله با تحلیل ترافیک سیگنال‌های دریافتی بدون درک محتوای خود سیگنال، به کار می‌رود. به بیان دیگر، حتی اگر سیگنال رمزنگاری شده باشد، تحلیل ترافیک را هنوز می‌توان برای آشکارسازی الگوهای طرف‌های مبادله مورد استفاده قرار داد. حمله تحلیل ترافیک بر خود ارتباطات اصلاً تأثیر نمی‌گذارد.

روش رمزنگاری استفاده شده برای جلوگیری از استراق سمع شدیداً به قدرت الگوریتم رمزنگاری و همچنین به توان محاسباتی استراق سمع‌کننده بستگی دارد. به خاطر رشد سریع توان محاسباتی و بهبود فناوری‌های تحلیل داده پیشرفته، استراق سمع‌کنندگان می‌توانند از فناوری‌های جدید در حملات خود استفاده کنند. مکانیزم‌های موجود برای جلوگیری از استراق سمع با چالش بزرگی مواجه شده‌اند؛ زیرا بسیاری از آنها تعداد اندکی استراق سمع کننده همزمان با توان محاسباتی کم و قابلیت تحلیل داده کم را در نظر می‌گیرند.



شکل ۶- حملات در شبکه‌های بی‌سیم 5G (الف) استراق سمع، (ب) Jamming، (ج) DDoS، (د) MITM

علاوه بر این، چند فناوری برای شبکه‌های بی‌سیم 5G مانند HetNet به کار گرفته شده است که می‌تواند دشواری مقابله با استراق سمع را افزایش دهد. به طور کلی، ویژگی‌های جدید شبکه‌های بی‌سیم 5G ممکن است منجر به سناریوهای بسیار پیچیده‌تری برای مقابله با استراق سمع شوند، برای مثال، اخیراً استراق سمع‌کنندگان با چند آنتن در نظر گرفته شده‌اند. روش‌های رمزنگاری برای جلوگیری از استراق سمع به طور گسترده در گذشته مورد بررسی قرار گرفته‌اند؛ اما اخیراً، پژوهش‌های امنیت لایه فیزیکی برای مقابله با استراق سمع، توجه بیشتری را به خود جلب کرده‌اند.

۲,۱,۴. حمله Jamming

برخلاف استراق سمع و تحلیل ترافیک، Jamming می‌تواند به طور کامل ارتباطات بین کاربران مجاز را مختل کند. شکل ۶ (ب) مثالی از حمله Jamming را نشان می‌دهد. گره مخرب می‌تواند تداخل عمدی ایجاد کند تا ارتباطات داده‌ای بین کاربران مجاز را مختل کند. همچنین Jamming می‌تواند مانع دسترسی کاربران مجاز به منابع رادیویی شود.

روش‌های طیف گسترده مانند DSSS[9] و FHSS[10] به‌عنوان روش‌های ارتباطات امن هستند که برای مقابله با Jamming در لایه فیزیکی با انتشار سیگنال بر روی یک پهنای باند طیفی گسترده‌تر مورد استفاده قرار می‌گیرند؛ اما روش‌های ضد Jamming مبتنی بر DSSS و FHSS ممکن است مناسب برخی از کاربردهای شبکه‌های بی‌سیم 5G نباشند.

۳٫۱٫۴. حملات DoS و DDoS

حملات DoS می‌توانند منابع شبکه را توسط یک مهاجم، کاملاً مصرف کنند. DoS یک حمله امنیتی است که دسترسی به شبکه‌ها را مختل می‌کند. Jamming را می‌توان برای اجرای یک حمله DoS مورد استفاده قرار داد. DDoS را می‌توان هنگامی انجام داد که بیش از یک مهاجم توزیع شده وجود داشته باشد. شکل ۶ (ج) یک مدل DDoS را نشان می‌دهد. DoS و DDoS هر دو حمله فعال هستند که در لایه‌های مختلف قابل اجرا می‌باشند. به دلیل حجم زیاد تعداد دستگاه‌های متصل در شبکه‌های بی‌سیم 5G، حملات DoS و DDoS احتمالاً به یک تهدید جدی برای اپراتورها تبدیل می‌شود. حملات DoS و DDoS در شبکه‌های بی‌سیم 5G می‌توانند دسترسی شبکه از طریق تعداد بسیار زیادی از دستگاه‌های متصل را مورد هدف قرار دهند. با توجه به هدف حمله، یک حمله DoS را یا می‌توان به‌عنوان یک حمله DoS به زیرساخت شبکه و یا به‌عنوان یک حمله DoS به دستگاه/کاربر شناخت. حمله DoS به زیرساخت شبکه می‌تواند سطح سیگنال‌دهی، سطح کاربر، سطح مدیریت، سیستم‌های پشتیبان، منابع رادیویی و منابع منطقی و فیزیکی را مورد حمله قرار دهد. حمله DoS به دستگاه/کاربر نیز می‌تواند باتری، حافظه، دیسک، CPU، رادیو، محرک و حسگرها را مورد هدف قرار دهد.

[9] direct sequence spread spectrum
[10] frequency hopping spread spectrum

۴,۱,۴. حمله MITM

در حمله MITM، مهاجم به صورت مخفی کنترل کانال ارتباطی بین دو کاربر مجاز را در دست می‌گیرد. مهاجم MITM می‌تواند پیام‌های ارتباطی بین دو شخص مجاز را شنود، تغییر یا جایگزین کند. شکل ۶ (د) یک مدل حمله MITM را نشان می‌دهد. MITM یک حمله فعال است که در لایه‌های مختلف قابل اجرا می‌باشد. به خصوص اینکه، هدف حملات MITM در معرض خطر قرار دادن محرمانگی، جامعیت و دسترس‌پذیری داده‌ها می‌باشد. بر اساس گزارش Verizon، حمله MITM یکی از رایج‌ترین حملات امنیتی می‌باشد. در شبکه‌های سلولی قبلی، حمله MITM مبتنی بر ایستگاه پایه جعلی، حمله‌ای است که در آن مهاجم یک کاربر مجاز را وادار به ایجاد یک اتصال با یک ایستگاه فرستنده گیرنده جعلی می‌کند. احراز هویت دو طرفه بین دستگاه موبایل و ایستگاه پایه معمولاً برای جلوگیری از حمله MITM مبتنی بر ایستگاه پایه جعلی استفاده می‌شود.

۲,۴. سرویس‌های امنیتی در شبکه‌های بی‌سیم 5G

معماری جدید، فناوری‌های جدید و موارد کاربرد در شبکه‌های بی‌سیم 5G، ویژگی‌ها و الزامات جدید در سرویس‌های امنیتی را به وجود می‌آورند. در این بخش، عمدتاً چهار نوع سرویس امنیتی را معرفی می‌کنیم: احراز هویت (احراز هویت موجودیت، احراز هویت پیام)، محرمانگی (محرمانگی داده‌ها، حریم خصوصی)، دسترس‌پذیری و جامعیت

۱,۲,۴. احراز هویت

دو نوع احراز هویت وجود دارد: احراز هویت موجودیت و احراز هویت پیام. هر دو مورد در شبکه‌های بی‌سیم 5G برای مقابله با حملاتی که قبلاً ذکر شد، مهم هستند. احراز هویت موجودیت، برای تضمین این است که آیا موجودیت ارتباطی، همان است که ادعا می‌کند. در شبکه‌های سلولی قبلی، احراز هویت دو طرفه بین تجهیزات کاربر (UE)[۱۱] و موجودیت مدیریت سیار (MME)[۱۲] قبل از اینکه دو طرف با هم مبادله پیام داشته

[۱۱] user equipment

باشند، اجرا می‌شود. احراز هویت‌های دو طرفه بین UE و MME، مهم‌ترین ویژگی امنیتی در چارچوب امنیت سلولی سنتی است. احراز هویت و توافق کلید (AKA)[۱۳] در شبکه‌های سلولی 4G LTE بر پایه کلید متقارن است؛ اما، 5G نه تنها نیاز به احراز هویت بین UE و MME دارد، بلکه بین اشخاص ثالث دیگر مانند ارائه‌دهنده سرویس نیز نیاز است. از آنجایی که مدل اعتماد با مدل اعتماد استفاده شده در شبکه‌های سلولی سنتی فرق دارد، نیاز به مدیریت احراز هویت ترکیبی و انعطاف‌پذیر در 5G وجود دارد. احراز هویت ترکیبی و انعطاف‌پذیر UE را می‌توان به سه روش مختلف پیاده‌سازی کرد: احراز هویت فقط با استفاده از شبکه، احراز هویت فقط با استفاده از ارائه‌دهنده سرویس و احراز هویت توسط شبکه و ارائه‌دهنده سرویس. به خاطر سرعت نرخ داده بسیار بالا و تأخیر بسیار کم در شبکه‌های بی‌سیم 5G انتظار می‌رود که احراز هویت در 5G بسیار سریع‌تر از گذشته باشد.

با توجه به کاربردهای جدید متنوع در شبکه‌های بی‌سیم 5G، احراز هویت پیام بیش از پیش اهمیت یافته است. علاوه بر این، به دلیل وضع الزامات سخت‌گیرانه‌تر در مورد تأخیر، بازده طیفی و بازده انرژی در 5G، احراز هویت پیام با چالش‌های جدیدی مواجه شده است.

۲،۲،۴. محرمانگی

محرمانگی از دو منظر محرمانگی داده‌ها و حریم خصوصی قابل توجه است. محرمانگی داده‌ها با محدود کردن دسترسی داده‌ها فقط برای کاربران مدنظر و جلوگیری از دسترسی کاربران غیرمجاز یا افشای داده‌ها برای آنها، از انتقال داده‌ها در نتیجه حملات غیرفعال محافظت می‌کند. حریم خصوصی نیز از کنترل و تأثیرگذاری بر روی اطلاعات مرتبط با کاربران مجاز جلوگیری می‌کند. برای مثال، حریم خصوصی از هرگونه تحلیل جریان ترافیک توسط مهاجم ممانعت به عمل می‌آورد. الگوهای ترافیک را می‌توان برای تشخیص اطلاعات حساس مانند مکان فرستندگان/گیرندگان مورد استفاده قرار داد. با توجه به کاربردهای مختلف

[12] mobility management entity
[13] authentication and key agreement

5G، داده‌های گسترده‌ای مرتبط با حریم خصوصی کاربر مانند داده‌های مسیریابی خودرو، داده‌های نظارت بر سلامت و غیره وجود دارند.

رمزنگاری داده‌ها به طور گسترده برای ایمن‌سازی محرمانگی داده‌ها با ممانعت کاربران غیرمجاز برای استخراج هرگونه اطلاعات مفید از اطلاعات منتشر شده استفاده می‌شود. روش رمزنگاری کلید متقارن را می‌توان برای رمزنگاری و رمزگشایی داده‌ها با اشتراک یک کلید خصوصی بین فرستنده و گیرنده به کار گرفت. برای اشتراک کلید بین فرستنده و گیرنده یک روش توزیع کلید امن لازم است. روش‌های رمزنگاری سنتی با این فرض طراحی شده‌اند که مهاجمان توان محاسباتی محدودی دارند؛ بنابراین، جدال با مهاجمانی که توان محاسباتی بالایی دارند، دشوار خواهد بود. به جای اتکا به مکانیزم‌های رمزنگاری لایه بالاتر عمومی، امنیت لایه فیزیکی می‌تواند از سرویس محرمانگی در برابر حملات Jamming و استراق سمع پشتیبانی کند.

علاوه بر سرویس‌های داده‌ای 5G، کاربران به اهمیت استفاده از سرویس حفظ حریم خصوصی پی برده‌اند. سرویس حریم خصوصی در 5G به توجه بیشتری نسبت به شبکه‌های سلولی قبلی نیاز دارد که این به خاطر اتصالات داده‌ای گسترده است. سرویس گمنامی، یکی از الزامات امنیتی پایه در موارد کاربرد بسیاری است. در بسیاری از موارد، نقض حریم خصوصی می‌تواند باعث پیامدهای جدی شود. برای مثال، داده‌های نظارت بر سلامت، اطلاعات سلامت شخصی حساسی را آشکار می‌کنند و یا داده‌های مسیریابی خودرو می‌توانند حریم خصوصی موقعیت جغرافیایی را در معرض خطر قرار دهند. شبکه‌های بی‌سیم 5G، نگرانی‌های امنیتی جدی در مورد نقض حریم خصوصی به وجود می‌آورند. در HetNets، به خاطر تراکم بالای سلول‌های کوچک، الگوریتم انجمنی می‌تواند حریم خصوصی در رابطه با موقعیت جغرافیایی کاربران را نقض کند.

۳،۲،۴. دسترس‌پذیری

دسترس‌پذیری به قابل دسترس بودن و قابل استفاده بودن یک سرویس برای هر کاربر مجاز، در هر زمان و هر مکانی که لازم باشد، گفته می‌شود. دسترس‌پذیری ارزیابی می‌کند که سیستم تا چه حدی در هنگام مواجهه با حملات مختلف مقاوم است و یک معیار عملکردی کلیدی در 5G می‌باشد. حمله به دسترس-پذیری یک حمله فعال عادی است. یکی از حملات اصلی به دسترس‌پذیری حمله DoS است که می‌تواند

باعث منع دسترسی به سرویس برای کاربران مجاز شود. Jamming یا تداخل می‌توانند لینک‌های ارتباطی بین کاربران مجاز را با استفاده از تداخل سیگنال‌های رادیویی مختل کنند. با وجود گره‌های IoT ناامن گسترده، شبکه‌های بی‌سیم 5G با یک چالش بزرگ در جلوگیری از حملات Jamming و DDoS برای تضمین سرویس دسترس‌پذیری مواجه می‌شوند. برای دسترس‌پذیری در لایه فیزیکی، DSSS و FHSS دو راهکار امنیت لایه فیزیکی کلاسیک وجود دارد.

۴,۲,۴. جامعیت

اگرچه احراز هویت پیام، تایید منبع پیام را حاصل می‌کند؛ اما حفاظت در برابر تکثیر یا تغییر پیام وجود ندارد. هدف 5G برقراری اتصال در هر زمان، هر مکان، به هر نحو و پشتیبانی از کاربردهای مرتبط با زندگی روزمره انسان مانند سنجش کیفیت آب آشامیدنی می‌باشد. جامعیت داده‌ها یکی از الزامات امنیتی کلیدی در کاربردهای مشخصی است.

جامعیت از دستکاری یا تغییر اطلاعات توسط حملات فعال و به واسطه موجودیت‌های غیرمجاز جلوگیری می‌کند. جامعیت داده‌ها می‌تواند توسط حملات مخرب داخلی مانند تزریق پیام یا تغییر داده‌ها نقض شود. از آنجا که مهاجمان داخلی شناسه‌های معتبری دارند، تشخیص این حملات دشوار است. موارد کاربردی مانند کنتورهای هوشمند در شبکه هوشمند، مستلزم ارائه سرویس جامعیت داده‌ها برای مقابله با دستکاری است. در مقایسه با ارتباطات صوت، داده‌ها را می‌توان آسان‌تر مورد حمله و تغییر قرار داد. سرویس‌های جامعیت را می‌توان با استفاده از احراز هویت دو طرفه ارائه نمود. سرویس جامعیت اطلاعات سلامت شخصی نیز لازم است. جامعیت پیام را می‌توان در راهکارهای احراز هویت فراهم نمود.

۳,۴. چالش‌های امنیتی پیش روی 5G

در ادامه به برخی چالش‌های امنیتی 5G اشاره شده است:

۱،۳،۴. مدل‌های جدید کسب‌وکار

در شبکه‌های سنتی ارتباطات سیار، هدف اصلی ارتقاء سطح زندگی مردم از طریق ارتباطات است. در این شبکه‌ها کاربران می‌توانند از طریق پیام‌های متنی، تماس‌های صوتی و تماس‌های ویدئویی، گشت‌وگذار در اینترنت و یا دسترسی به خدمات برنامه‌های کاربردی با استفاده از تلفن‌های هوشمند ارتباط برقرار کنند. با این حال، 5G دیگر محدود به مشتریان خاص و یا داشتن شبکه موبایل سریع‌تر یا عملکردهای غنی‌تر در تلفن‌های هوشمند نیست، بلکه هدف اصلی 5G ارائه سرویس به صنایع عمودی است که انواع خدمات جدید از آنها ناشی می‌شود. در زمینه صنایع عمودی، تقاضاهای سطح امنیتی مورد نیاز سرویس‌ها می‌تواند بسیار متفاوت باشد. به‌عنوان مثال، دستگاه‌های اینترنت اشیاء (IoT) موبایل نیاز به امنیت سبک دارند؛ در حالیکه سرویس‌های موبایل پر سرعت، امنیت موبایل بسیار کارآمد را می‌طلبند؛ بنابراین رویکرد امنیتی hop-by-hop ممکن است به اندازه کافی برای ایجاد امنیت انتها به انتها (E2E) برای سرویس‌های مختلف کارآمد نباشد و یا برای جلوگیری از دسترسی غیرمجاز به دستگاه‌های IoT، نیاز به یک روش دقیق‌تر تأیید هویت وجود دارد (به‌عنوان مثال، شناسایی بیومتریک می‌تواند بخشی از تأیید هویت در خانه‌های هوشمند باشد).

۲،۳،۴. معماری شبکه IT محور

فناوری‌های جدید IT، مانند مجازی‌سازی و شبکه‌های SDN و NFV، به‌عنوان راهی برای تبدیل شبکه 5G، به شبکه‌ای کارآمد و در عین حال کم‌هزینه‌تر دیده می‌شوند. با این حال امنیت برای خدمات 5G امکان‌پذیر نیست، مگر اینکه اصلاحات لازم در زیرساخت شبکه انجام گیرد.

۳،۳،۴. دسترسی ناهمگن

ناهمگنی یکی از ویژگی‌های شبکه‌های دسترسی نسل بعدی خواهد بود. ماهیت ناهمگن نه تنها ناشی از استفاده از فناوری‌های مختلف دسترسی (مانند WiFi و LTE) می‌باشد، بلکه از محیط‌های چندشبکه‌ای نیز نشأت می‌گیرد. دستگاه‌های IoT گزینه‌های مختلفی برای دسترسی به شبکه‌ها دارند. به‌عنوان مثال آنها می‌توانند به طور مستقیم یا از طریق درگاه خروجی و روش‌های دیگر به شبکه متصل شوند.

۴،۳،۴. حفظ حریم خصوصی

با پیشرفت اینترنت موبایل، صنایع عمودی از جمله مراقبت‌های بهداشتی، خانه‌های هوشمند و حمل‌ونقل هوشمند به شبکه‌های 5G متوسل می‌شوند. از این رو شبکه‌های 5G نگرانی‌های جدی درباره نقض حریم خصوصی ایجاد می‌کنند. در بسیاری از موارد، نقض حریم خصوصی می‌تواند عواقب جدی ایجاد کند. به‌عنوان روش اصلی برای دسترسی به شبکه، شبکه‌های تلفن همراه دارای داده‌ها و سیگنال‌هایی هستند که حاوی بسیاری از اطلاعات مربوط به حریم خصوصی افراد (به‌عنوان مثال اطلاعات هویتی، موقعیتی و محتواهای خصوصی) می‌باشند. بر این اساس محافظت از حریم خصوصی در 5G موضوعی چالش‌برانگیز است.

۵،۳،۴. حملات DDoS در صدر نگرانی‌های امنیتی 5G

با افزایش تعداد دستگاه‌ها و با توسعه شبکه 5G، تهدیدات DDoS می‌تواند گسترش یابد.

۴،۴. دیدگاه‌ها و پیشنهادات امنیتی 5G

دیدگاه‌های متفاوتی جهت تأمین امنیت در 5G مطرح شده است که در ادامه به برخی از آنها اشاره می‌شود:

۱،۴،۴. ارائه مدل‌های اعتماد و مدیریت هویت

شبکه‌های Telecom وظیفه تأیید اعتبار کاربر را فقط برای دسترسی به شبکه بر عهده دارند. یک مدل اعتماد با دو عنصر، بین کاربران و شبکه‌ها شکل می‌گیرد. تأیید اعتبار بین کاربر و خدمات، تحت پوشش شبکه‌ها نیست. با این حال، در شبکه‌های 5G، یک مدل اعتماد با یک عنصر اضافی که همان استفاده از ارائه‌دهنده خدمات عمودی است، یک مدل احتمالی موفق خواهد بود. در این حالت شبکه ممکن است با ارائه‌دهندگان خدمات همکاری کنند تا یک مدیریت هویت مطمئن و کارآمد را فراهم سازند.

۲،۴،۴. امنیت سرویس‌گرا

سیستم‌های 5G به صورت سرویس‌گرا می‌باشند. این بدان معناست که تأکید ویژه‌ای بر الزامات امنیتی که ناشی از دیدگاه سرویس است، وجود خواهد داشت. به‌عنوان مثال، مراقبت از راه دور به امنیت انعطاف‌پذیر نیاز دارد؛ در حالیکه IoT به امنیت سبک نیاز دارد. از این رو ارائه امنیت متمایز برای خدمات متفاوت کاملاً منطقی به نظر می‌رسد.

۵. جمع‌بندی

آنچه مشخص است 5G فرصت‌های بی‌شماری به همراه خود به ارمغان می‌آورد که از همین امر می‌توان به راحتی نتیجه گرفت که به زودی این فناوری در تمام جهان گسترش خواهد یافت. حال چه بهتر قبل از ورود و گسترش آن در کشور، اقدامات ساختار یافته و با پشتوانه علمی در حوزه تهدیدات و الزامات امنیتی این پدیده نوظهور صورت گیرد تا مخاطرات و تهدیدات امنیتی این فناوری از قبل پیش‌بینی و راه حل‌هایی برای آن اتخاذ گردد.

منابع

Araniti, G., Campolo, C., Condoluci, M., Iera, A., & Molinaro, A. (2013). LTE for vehicular networking: a survey. IEEE communications magazine, 51(5), 148-157.

Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.

Cao, J., Li, H., & Ma, M. (2015, June). GAHAP: A group-based anonymity handover authentication protocol for MTC in LTE-A networks. In 2015 IEEE International Conference on Communications (ICC) (pp. 3020-3025.(

Di Ciaula, A. (2018). Towards 5G communication systems: Are there health implications? International Journal of Hygiene and Environmental Health, 221(3), 367-375. doi: https://doi.org/10.1016/j.ijheh.2018.01.011

Ericsson press, 2014. URL: https://www.ericsson.com/en/press-releases/2014/7/ericsson-5g-delivers-5-gbps-speeds

Fang, D., Qian, Y., & Hu, R. Q. (2017). Security for 5G mobile wireless networks. IEEE Access, 6, 4850-4874.

Gazzah, L., & Najjar, L. (2019). Enhanced cooperative group localization with identification of LOS/NLOS BSs in 5G dense networks. Ad Hoc Networks, 89, 88-96. doi: https://doi.org/10.1016/j.adhoc.2019.03.004

Ghendir, S., Sbaa, S., Al-Sherbaz, A., Ajgou, R., & Chemsa, A. (2019). Towards 5G wireless systems: A modified Rake receiver for UWB indoor multipath channels. Physical Communication, 35, 100715. doi: https://doi.org/10.1016/j.phycom.2019.100715

Huawei. (2016). 5G Opening up New Business Opportunities.

Hussain, R., Hussain, F., & Zeadally, S. (2019). Integration of VANET and 5G Security: A review of design and implementation issues. Future Generation Computer Systems, 101, 843-864. doi: https://doi.org/10.1016/j.future.2019.07.006

Internet source – scm-fallersleben.ciando.com

Internet source – www.worldtimezone.com

Kumar, A., & Om, H. (2019). Design of a USIM and ECC based handover authentication scheme for 5G-WLAN heterogeneous networks. Digital Communications and Networks. doi: https://doi.org/10.1016/j.dcan.2019.07.003

Lemstra, W. (2018). Leadership with 5G in Europe: Two contrasting images of the future, with policy and regulatory implications. Telecommunications Policy, 42(8), 587-611. doi: https://doi.org/10.1016/j.telpol.2018.02.003

Li, S., Xu, L. D., & Zhao, S. (2018). 5G Internet of Things: A survey. Journal of Industrial Information Integration, 10, 1-9. doi: https://doi.org/10.1016/j.jii.2018.01.005

Liyanage, M., Ahmad, I., Abro, A. B., Gurtov, A., & Ylianttila, M. (Eds.). (2018). A Comprehensive Guide to 5G Security. John Wiley & Sons.

Matinmikko, M., Latva-aho, M., Ahokangas, P., & Seppänen, V. (2018). On regulations for 5G: Micro licensing for locally operated networks. Telecommunications Policy, 42(8), 622-635. doi: https://doi.org/10.1016/j.telpol.2017.09.004

Morgado, A., Huq, K. M. S., Mumtaz, S., & Rodriguez, J. (2018). A survey of 5G technologies: regulatory, standardization and industrial perspectives. Digital Communications and Networks, 4(2), 87-97. doi: https://doi.org/10.1016/j.dcan.2017.09.010

Oughton, E. J., & Frias, Z. (2018). The cost, coverage and rollout implications of 5G infrastructure in Britain. Telecommunications Policy, 42(8), 636-652. doi: https://doi.org/10.1016/j.telpol.2017.07.009

Serrano Mamolar, A., Pervez, Z., Alcaraz Calero, J. M., & Khattak, A. M. (2018). Towards the transversal detection of DDoS network attacks in 5G multi-tenant overlay networks. Computers & Security, 79, 132-147. doi: https://doi.org/10.1016/j.cose.2018.07.017

Temesvári, Z. M., Maros, D., & Kádár, P. (2019). Review of Mobile Communication and the 5G in Manufacturing. Procedia Manufacturing, 32, 600-612. doi: https://doi.org/10.1016/j.promfg.2019.02.259

Wen, F., Wymeersch, H., Peng, B., Tay, W. P., So, H. C., & Yang, D. (2019). A survey on 5G massive MIMO localization. Digital Signal Processing. doi: https://doi.org/10.1016/j.dsp.2019.05.005

Zhang, S., Wang, Y., & Zhou, W. (2019). Towards secure 5G networks: A Survey. Computer Networks, 162, 106871. doi: https://doi.org/10.1016/j.comnet.2019.106871

Zhang, S., Wu, Q., Xu, S., & Li, G. Y. (2016). Fundamental green tradeoffs: Progresses, challenges, and impacts on 5G networks. IEEE Communications Surveys & Tutorials, 19(1), 33-56.