کنفرانس بین المللی پژوهش های کاربردی در فناوری اطلاعات، کامپیوتر و مخابرات
International Conference on Information Technology, Computer & Communication
19 November 2015 ۲۸ آبان ماه ۱۳۹۴

چالش های امنیتی شبکه های 5G

سعید ترکمانی[۱] ، سید حسین شاهرخی[۲]
۱-دانشگاه آزاد اسلامی واحد الکترونیکی
۲-دانشگاه آزاد اسلامی واحد الکترونیکی

چکیده

می توان گفت که در نسل پنجم شبکه های موبایل به دلیل سرعت بالا و سرویس های جدید مخاطب از کاربر به سوی انواع دستگاه های متصل به شبکه تغییر پیدا می کند یعنی همان اینترنت اشیاء . نسل پنجم شبکه های موبایل فقط برای دستگاه های موبایل یا در نهایت تبلت یا نوت بوک نیست و هر چیزی که به اینترنت وصل می شود به طور خودکار کاربر شبکه خواهد بود .تصویر سازی استفاده از نسل پنجم شبکه های موبایل مانند این است که سعی در پیش بینی ظهور آی فون پنج سال قبل از رونمایی داشته باشیم. اکنون دوباره در چنین وضعیتی قرار گرفته ایم و باید ۱۰ سال آینده را تصویر سازی و دوباره تلاش کنیم چشم اندازی از جهان پس از ارائه نسل پنجم شبکه های موبایل به دست آوریم تا براساس آن استاندارد سازی شود. می توان گفت برای پیاده سازی نسل پنجم شبکه های موبایل با چالش های فراوانی رو به رو هستیم که یکی از این چالش ها، چالش های امنیتی است. در این نوشتار پس از معرفی نسل پنجم شبکه های موبایل و امواج میلیمتری به بررسی چالش ها آن می پردازیم اما بیشتر بر روی چالش های امنیتی این شبکه ها تمرکز می کنیم و راه حل های ارائه شده را بررسی خواهیم کرد .

واژگان کلیدی : 5G،امواج میلیمتری،SDN(software defined networks)،امنیت،device۲ device communication

ISBN: 978-600-7461-60-0

مقدمه :

هر نسل شبکه های موبایل سعی کرده است کمبود ها و نقایص نسل پیش از خود را برطرف کند. GSM سعی کرده مشکلات و ضعف های امنیتی شبکه های تلفن آنالوگ را مرتفع کند. ۳G سعی کرد تبادل اطلاعات را به شبکه های موبایل وارد کند وسرعت را هم افزایش دهد که چندان موفق نبود و ۴G تلاش کرد تجربه ناخوشایند استفاده از اطلاعات روی موبایل را بهبود بدهد. ۵G در حال ظهور است وارزیابی ها و تحلیل بازار این اتفاق بزرگ را تایید می کند، اما ۵G قرار است چه کمبود ها و مشکلاتی از نسل قبلی خود را برطرف کند؟در حال حاظر سه معیار اصلی برای استاندارد ۵G مطرح شده است:۱-این شبکه باید بتواند به سرعت دانلودی برابر یک گیگابایت بر ثانیه به دست بدهد و درآینده به سرعت چند گیگابایت بر ثانیه برسد. ۲- این شبکه باید تاخیر را به زیر یک میلی ثانیه برساند. ۳- این شبکه باید مصرف انرژی موثرتری نسبت به نسل پیشین داشته باشد. با وجود این که نمی توان پیش بینی های دقیقی درباره نسل بعدی شبکه های موبایل داشت و نیازمندی های کاربران باید توسط این شبکه پاسخ داده شود، صنعت موبایل به یک اجماع کلی درباره ۵G رسیده است. ارتباطات ماشین به ماشین یکی از کاربرد های ۵G است. همچنین قرار است ۵G اینترنت اشیاء را فعال کند مفهومی که می گوید در آینده در همه جا هر شیء آنلاینی می تواند بی سر وصدا با اشیاء آنلاین دیگر ارتباط داشته باشد ۵G می خواهد تسهیلاتی را فراهم کند تا بتوان از طریق شبکه های موبایل به خودروها متصل شد و از راه دور روبات های صنعتی را کنترل کرد. دسترسی از راه دور سیستم های پزشکی و زیر ساخت های شهر های مدرن آینده نیز جزء الویت های ۵G هستند. همه این ها تصویر بزرگتری از این نسل شبکه های موبایل می سازند. اگر بخواهیم مثال های عینی و قابل درک تری از کاربرد های فوق ارائه داد، باید به دانلود ویدیوهای۴K و۸K با سرعت بالا و بدون هیچ تاخیری اشاره کرد. تمام موارد فوق مشکلات امنیتی مخصوص به خود را دارند. برای مثال در بحث دسترسی از راه دور سیستم های پزشکی باید حفظ حریم خصوصی و سلامت بیمار در نظر گرفته بشود. مفهوم گره در شبکه های ۵G ذاتا بر مبنای انتقال بی سیم است که دارای آسیب پذیری می باشد.هنوز استاندارد های امنیتی شبکه های ۵G به درستی تعریف نشده اند که در واقع یکی از مولفه های کلیدی است که کل سیستم را پوشش می دهد. ارتباطات D۲D (device to device)که در شبکه های۵G مطرح است می تواند چالش های امنیتی داشته باشد به این صورت که طرفین ارسال کننده ودریافت کننده باید اطمینان داشته باشند که اطلاعات آنها برای رله ها قابل دسترسی نیست. درشبکه های ۵G نیاز به یک مدل بنیادی امنیتی احساس شده تا انعطاف پذیری بیشتری را فراهم کند. امنیت در شبکه های مجازی وخدمات آنها باید در نظر گرفته شود. مقاومت در برابر حملات و امنیت داده ها باید یک معیار اصلی در طراحی پایه پروتکل های جدید باشند. برای مقابله با این چالش های امنیتی ابزار های جدیدی مانندnetwork slicing- trusted computing و ابزار های دیگر نیاز است. در ادامه به معرفی چالشهای امنیتی و راه حل های ارائه شده می پردازیم.

ISBN: 978-600-7461-60-0

۱-تعریف یک استاندارد:

ابتدا استاندارد ها باید برای هر فناوری جدید موبایل تعریف و ساختاردهی شوند. این کار از چند سال قبل از استفاده و فراگیر شدن این فناوری آغاز می شود، زیرا پس از اجرا قرار است این استاندارد ها برای یک دهه یا بیشتر در کل صنعت و سراسر جهان باقی بمانند و مبنای هر ارتباطی باشند. برای۵G به ساختن استاندارد نیاز داریم که تا سال ۲۰۳۰ و حتی فراتر از آن قابلیت استفاده داشته باشند. ۵G یک نامی بی معنا است زیرا هنوز استانداردی وجود ندارد. سال ها است که این نام مطرح شده است، درحالی که هنوز تعریف درستی از آن نداریم.در همین حال، سازمان ها، دانشگاه ها، دولت ها، مراکز تحقیقاتی وآزمایشگاها در حال کار روی فناوری هایی هستند که استاندارد نسل بعدی شبکه های موبایل را تشکیل دهد. اما امروز ۵G چیزی بیشتر از یک مفهوم نیست ویک نیاز برای رفتن از یک فضای مه آلود و هاله مانند به یک فضای واقعی تا شش سال آینده است.براساس نشانه های تاریخی، نخستین شبکه ساخته شده بر اساس استاندارد۵G در سال ۲۰۲۰ راه اندازی خواهد شد. در این فرصت باقی مانده تا رسیدن به این نقطه تاریخی، سال های سختی برای استاندارد سازی ۵G خواهد بود. موسسه هایی مانند ۳GPP ITU ، IEEE، FCC دو تا سه سال فرصت دارند تا استانداردهای لازم برای راه اندازی شبکه های ۵G را تکمیل و نهایی کنند. همچنین، تمام مراکز تحقیقاتی و آزمایشگاهی، دولت ها ، سازمان ها و دانشگاه ها درگیر این قضیه خواهند بود و باید به این سازمان های استاندارد ساز کمک رسانی کنند یا حمایت های لازم مادی را به عمل آورند. حتی خود این مراکز نیز اذعان دارند هنوز هیچ استاندارد نهایی تهیه نشده است. با این حال، تمام این آزمایش ها و همکاری ها به پایه ریزی یک استاندارد مقدماتی وپایه ای منجر می شود که شروعی برای فعالیت و تخصیص بودجه در سراسر جهان به جهت توسعه پروژه های فناوری ۵G باشد. راه اندازی شبکه های آزمایشی و مراکز ارزیابی فناوری های ۵G نشان می دهد که با وجود نداشتن استانداردی در این زمینه، صنعت موبایل به راه خود ادامه می دهد و در حال ساخت نسل بعدی شبکه های موبایل است. درواقع ۵G مشکلاتی که امروزوجود ندارد ولی در طی چند سال آینده بروز خواهند کرد، حل کند. می توان گفت آن ها می خواهند از پیش مشکلات احتمالی آینده را حدس بزنند و راه کار ارائه بدهند و ما را برای سال های آینده آماده کنند.

شکل ۱- محققان شرکت سامسونگ در حال آزمایش راه اندازی شبکه های ۵G

ISBN: 978-600-7461-60-0

۲-طیف های فرکانسی :

هر استاندارد جدید موبایل نیازمند طیف های فرکانسی بیشتر است. شبکه های 5G نیز از این قاعده مستثنی نیستند.اگر اپراتور های موبایل می خواهند با ظرفیت های بسیار بیشتری پاسخ گوی کابران باشند، به همان اندازه نیازمند طیف های فرکانسی بی سیم بیشتری هستند تا به خدمت گرفته شوند. به طور قطع 5G از الگو های قدیمی تخصیص طیف فرکانسی تبعیت نخواهد کرد، ولی با یک دردسر جدید هم روبه رو است و آن این است که به اندازه کافی طیف فرکانسی آزاد وجود ندارد. تحلیل گران حوزه شبکه های بی سیم اعتقاد دارند به طور ویژه مسئله ای مانند رومینگ روی 5G مشکل ساز خواهد بود طیف های فرکانسی عمده ترین چالش کنونی و آینده بر سر اجرای اولیه با موفقیت شبکه های 5G هستند. به طور عمومی به اندازه کافی طیف های فرکانسی برای 5G نداریم واین فناوری به بهینه سازی گسترده ای روی طیف های موجود نیاز دارد. به وضوح تخصیص طیف های بیشتر به 4G وپس از آن به5G می تواند کمک کننده باشد، ولی به یک چالش عمومی تبدیل خواهد شد.به علاوه چالش دیگر یافتن باند های هارمونیک عمومی برای رومینگ 5G است، به طوری که تمام این طیف ها قابلیت استفاده در نقاط مختلف جهان توسط اپراتور را داشته باشند. یک راه کار می تواند تقسیم بندی و خرد کردن طیف های فرکانسی بالاتر به طیف های فرکانسی پایین ترباشد مثلا طیف های فرکانسی ۷۰۰ مگاهرتز و ۲/۶ گیگا هرتز که در حال حاضر توسط بیشتر اپراتورها استفاده می شوند. راه کار دیگر می تواند حرکت به سوی طیف های بالاتر مانند:۶ گیگاهرتز، ۲۸ گیگا هرتز،۳۸ گیگاهرتز باشد که به عنوان موج میلی متری شناخته می شوند.

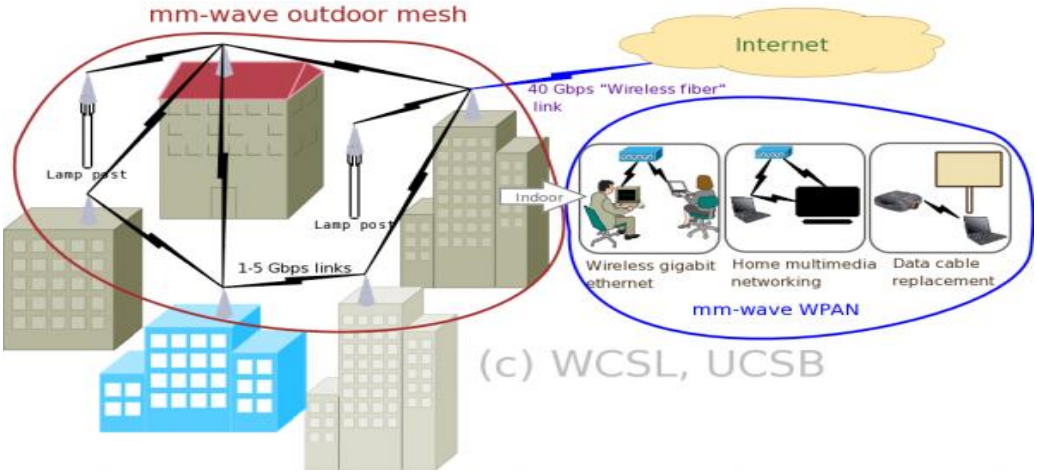
۳- اموج میلی متری:

به طور قطع می توان گفت نسل پنجم شبکه های موبایل بر روی امواج میلی متری کار می کنند. اپراتورها برای استفاده از این شبکه های جدید به طیف فرکانسی تازه ای نیاز دارند، اما چنین چیزی را از کجا باید یافت؟ مطابق تعاریف اتحادیه بین المللی مخابرات ITU باند موج میلی متری که به آن باند (ابرفرکانس) نیز گفته می شود، در محدوده ۳۰ تا ۳۰۰ گیگا هرتز قرارمی گیرند. هر چند دیگر رده های فرکانسی خیلی بالا که در مجاورت این محدوده قرار دارند نیز از ۱۰ تا ۳۰ گیگاهرتز شامل این دسته هستند، زیرا امواج در این محدوده نیز خواص مشابهی با امواج میلیمتری از خود نشان می دهند. تخمین زده می شود رگولاتورهای دولتی برای استفاده ارتباطات موبایلی به ایجاد طیفی شامل ۱۰۰ گیگاهرتز از این امواج قادر هستند.این میزان حدود صد برابر پهنای باندی است که شبکه های سلولی امروزی به آن دسترسی دارند. مدت ها است شرکت های اپراتور موبایل از استفاده طیف موج میلیمتری سر باز می زنند، زیرا تجهیزات رادیویی مورد نیاز برای این طیف فرکانسی گران قیمت است و علاوه بر آن اعتقاد دارند که ارتباط امواج میلیمتری بین دکل های سنتی و تجهیزات دستی به کندی صورت خواهد گرفت. همچنین، اپراتور ها نگرانی دیگری نیز داشتند که بخش زیادی از امواج میلی متری توسط اتمسفر، باران و گیاهان جذب و با از مسیر خود منحرف شوند و به این ترتیب، راهی به داخل ساختمان ها پیدا نکنند.امروز این نظر ها به سرعت در حال محو شدن هستند چند گروه تحقیقاتی به طور خاص روی اصول اولیه استفاده از امواج میلی متری در حال مطالعه وفعالیت هستند. در این تحقیقات موضوع هایی مانند مدل کانال ها،مدل انتشار، چگونگی آنتن های امواج میلی متری، شکل طراحی گوشی های تلفن همراه، تاثیر طراحی های خاص گوشی وآنتن روی تقویت امواج وتاثیر این امواج روی بدن انسان و.... مطرح هستند.

ISBN: 978-600-7461-60-0

مانند هر فناوری جدید نیازمند ساختن یک اکو سیستم در اطراف این امواج وفناوری های مرتبط با آن احساس می شود.شرکت های سازنده تجهیزات شبکه باید دست به کار شوند وشروع به ساخت کیت های شبکه مناسب استفاده از این امواج کنند واز سوی دیگر گوشی های تلفن همراه مناسب برای کار با این کیت های شبکه ساخته شوند.

شرکت های مختلفی توانستند اطلاعات را با سرعت ۱۱۵ گیگابیت برثانیه در فاصله ۱۵ متری روی طیف فرکانسی ۷۰ گیگاهرتز منتقل کنند برای مثال شرکت سامسونگ مدعی است نخستین سخت افزار امواج میلی متری را ساخته است، که شامل یک گیرنده و فرستنده ۶۴ بیتی است. این دستگاه روی فرکانس ۲۸ گیگا هرتز کار می کند و می تواند انتقال اطلاعات با سرعت بیش از یک گیگابیت بر ثانیه را در طول مسافتی دو کیلومتری انجام دهد.



شکل۲- نمایش ارتباطات داخلی وخارجی امواج میلیمتری

٤- چالش تاخیر:

نسل پنجم شبکه های موبایل از مجموعه ای از فناوری ها جدید بهره خواهد گرفت و امکان استفاده از هر فناوری دیگری که اکنون مطرح نیست، وجود دارد. این موضوع مخاطرات این شبکه را افزایش می دهد. برای مثال خودرویی که از یک سیستم خودکار مبتنی برفناوری های کلاود روی 5G استفاده می کند، اگر سیگنال دریافتی دچار اختلال و گم شدن شود،سیستم ترمز ماشین چگون عمل خواهد کرد؟ پس می توان گفت نیاز به کاهش حداکثری تاخیر در شبکه روی چگونگی توسعه این شبکه تاثیر دارد.نرخ خطای بسته ها نیازمند مرتب سازی و محاسبه تمام عوامل درونی وبیرونی شبکه است. در حال حاضر اپراتورها نمی توانند یک شبکه بی درنگ ارائه دهند که بتواند در لحظات حیاتی یک سیگنال مناسب با وضعیت موجود ارائه دهد یا مجموعه ای از راه کارها برای رانندگی در جاده های دور در اختیار رانندگان بگذارند، زیرا امکان رخ دادن هر گونه مشکل پیش بینی نشده ای برای اتصالات میان شبکه و خودرو قابل روئیت نیستند. زمان دسترسی به شبکه باید به طور چشم گیر کاهش یابد. برای مثال کنترل های شبکه باید به مراتب بیش تر از اکنون بشوند، شاید در هریک کیلومتر یک نقطه دسترسی و کنترل شبکه نیاز باشد.SDN به طور موثر اجازه می دهد اپراتورها بهتر از گذشته مسیر های عبور اطلاعات و انتخاب کمترین مسیریابی را در مقایسه با مسیریابی غیرهوشمند وناآگاه به نوع داده امروزی انجام دهند، ولی شاید تنها راه کار مورد نیاز نباشد یا هنوز به

ISBN: 978-600-7461-60-0

اندازه کافی توسعه داده نشده باشد. مشکل اینجاست که ابزار و معیار برای اندازه گیری فناوری۵G نداریم. تاخیر کمتر نیازمند افزایش محاسبات لبه(edge computing) است. تاخیر یکی از تهدیدات اصلی شبکه های ۵G است اگر به این امر به خوبی توجه نشود،خودروها و دیگر بخش های صنعت درگیر یا وابسته به ۵G بایک مشکل اصلی وجدی برخورد می کنند.

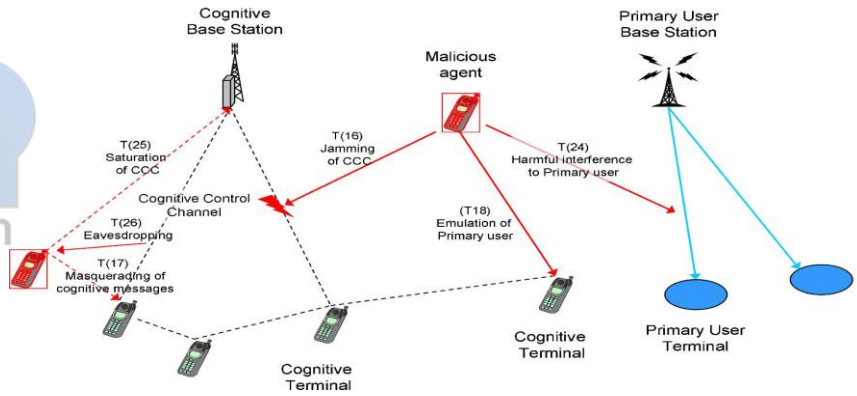
۵- چالش های امنیتی:

در این قسمت به بررسی چالش های امنیتی و راه حل های ارائه شده توسط محققان در نسل پنجم شبکه های موبایل می پردازیم. می خواهیم آسیب پذیری هایی از قبیل cognitive radio ویا بحث امنیت در ارتباطات D۲D ، تصدیق هویت handover و حفاظت از حریم خصوصی با استفاده از SDN ، حفاظت از امنیت نسل پنجم شبکه های مخابراتی با استفاده از امنیت لایه فیزیکی، ارائه یک معماری امنیتی مطابق با EU METIS ۵G project بپردازیم.

۵-۱- آسیب پذیری های cognitive radio:

مطالعه وتوسعه بر روی نسل پنجم شبکه های موبایل شروع شده وبسیاری از محققان معماری های بالقوه و وتکنیک های امیدوار کننده ای را که میتواند در شبکه های ۵G به کار برده شود را معرفی کرده اند. این تکنیک ها می توانند شامل : دسترسی چند گانه غیر متعامد(NOMA)، سیستم های چند ورودی و چند خروجی (MIMO)، تعاون ارتباطات و کدینگ شبکه، ارتباطات full duplex ، ارتباطات D۲D ، ارتباطات بر پایه امواج میلیمتری، شبکه های خودکار و cognitive radio می باشد. در بحث cognitive radio که سیستم های هوشمند رادیویی هستند و با استفاده از فیدبک به طور هوشمند از کانال های موجود استفاده می کنند می توان به این نکته اشاره کرد که نسبت به حمله هایی که در اثر اشتراک فرکانس روی می دهد آسیب پذیر است. رفتار حملات می تواند به صورت عمدی و غیر عمدی کلاس بندی شود.۱- malicious PUs emulation attack: در اینجا مهاجم به عنوان یک Pus برای انتقال سیگنال قوی به منظور تشخیص تداخل SUs ها نقش بازی می کند.۲- unintentional PUs attack : در اینجا Pus با نقص انتقال سیگنال قوی برای ارتباطاتی که SUs مسبب آنها هست باعث ایجاد خطا می شود.۳-malicious SUs emulation attack : در اینجا مهاجم به عنوان SUs برای گزارش اطلاعات نادرست در انتخاب طیف عمل می کند. ۴-unintentional SUs attack : SUs با نقص گزارشات سبب سنجش اطلاعات نادرست می شود.۵- selfish SUs attack : SUs اطلاعات نادرستی از سنجش اطلاعات برای استفاده از حداکثر از دامنه طیف ارائه می دهند. برای حملات مبتنی بر Pus/SUs تکنیک های تایید اعتبار پیشنهاد می شود. برای حملات unintentional PUs/SUs باید ابتدا کاربران شناسایی شده ودر مرحله بعد تجهیزات عوض بشوند وبرای حملات selfish SUs مکانیزم های اجتناب در نظر گرفته شده است.

ISBN: 978-600-7461-60-0

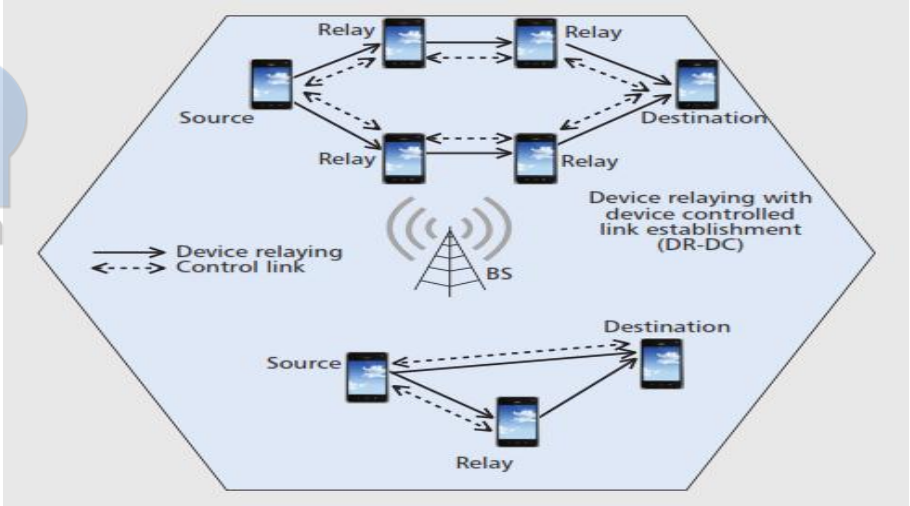


شکل ۳- آسیب پذیری cognitive radio

۵-۲ امنیت در ارتباطات device۲ device (D۲D) در نسل پنجم شبکه های مخابراتی

نسل پنجم شبکه های مخابراتی در ارتباطات device۲ device (D۲D) Device های مبدا ومقصد بدون هیچ کنترل کننده ای با هم ارتباط مستقیم دارند. وdevice های مبدا و مقصد باید بدون دخالت device دیگر از منابع هم استفاده کنند. از آنجایی که داده های کاربر از طریق دستگاه های کاربرمسیر یابی می شوند. امنیت و حریم خصوصی باید حفظ بشود. یک راه حل برای اطمینان از امنیت closed access برای device ی می باشد که می خواهیم در ردیف device ها قرار بدهیم. در closed access به این صورت است که device لیستی از device های قابل اعتماد را دارد و device ی که در لیست نیست باید از ردیف macro cell برای برقرای ارتباط استفاده کند. برای مثال کاربرانی که در همسایگی هم قرار دارند یا در یک محل کار می کنند و یکدیگر را می شناسند. یا کاربرانی که از طریق یک trusted party تصدیق هویت می شوند مثل یک سازمان می توانند به طور مستقیم با یکدیگر ارتباط برقرار کنند و سطح رضایت بخشی از حریم خصوصی را داشته باشند.device ها می توانند یک کدگذاری مناسبی بین خودشان برای جلوگیری از افشای اطلاعات تنظیم کنند. از سوی دیگر درclosed access هر device می تواند به عنوان رله برای دیگری عمل کند بدون اینکه هیچ محدودیتی داشته باشد واز آنجایی که هیچ نظارتی وجود ندارد امنیت یک مشکل چالش برانگیز به حساب می آید. مسائل مربوط به امنیت که در ارتباطات D۲D وجود دارند شامل : شناسایی پتانسیل حملات، تهدید و آسیب پذیری سیستم ها می باشد. آثار اولیه بر روی مسائل امنیتی در ارتباطات ماشین به ماشین می تواند سبب مسائل امنیتی در open access در ارتباطات D۲D شود. برای مثال کار های صورت گرفته توسط محققان که یک محیط قابل اعتماد برای ایجاد یک ارتباط امن وقابل اعتماد در میان تجهیزات M۲M برقرار می کند و همچنین مسیر یابی امن، نرم افزار های مبتنی بر کلید رمز نگاری متقارن وتشخیص حملات بالقوه را نیز مورد بررسی قرار داده اند.

ISBN: 978-600-7461-60-0



شکل٤-تصویر سازی از دستگاه ارتباطی رله با دستگاه ایجادکننده کنترل لینک. در اینجا device های منبع و مقصد بدون استفاده از لینک کنترل از اپراتور ها با یک دیگر تماس حاصل می کنند

۵-۳ تعریف یک چهارچوب امن برای همکاری device۲device در نسل پنجم شبکه های مخابراتی

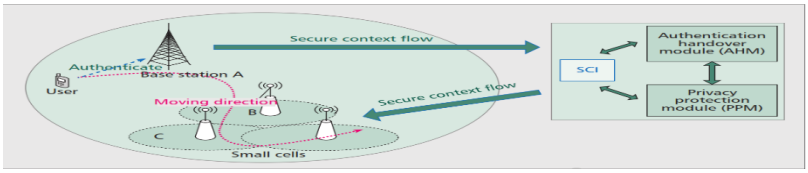
ارتباطات device۲device در نسل پنجم شبکه های مخابراتی می تواند تکنیکی را فراهم کند که نرخ بالاتری از داده را بتوان انتقال داد. امنیت انتقال داده برروی شبکه های بیسیم مبتنی بر cloud می تواند برای device ها محدودیت ایجاد کند. بنابراین هدف محققان این است که یک چهار چوب تحلیلی برای امنیت در لایه فیزیکی ارائه دهند و همچنین یک الگوریتم توزیع شده را ارائه داده اند که device ها برای انتخاب پیشنهاد همکاری با سایر device ها بتوانند خودمختار باشند و برای انطباق تخصیص بهینه قدرت خود بر اساس یک چهار چوب همکاری انتخاب کنند. محققان یک تعریفی از محدودیت فاصله را بین device ها در شبکه های بیسیم مبتنی بر cloud کردند که می تواند به عنوان یک چالش برای همکاری بین deviceها در نظر گرفته شود. واین محدودیت مسبب تعریف حالت تطبیقی برای همکاری device۲ device واختصاص قدرت تطبیقی بر این اساس شده است. برای انتقال امن داده در بحث همکاری device۲ device باید این نوع همکاری به صورت تطبیقی وتوزیع شده باشد. در واقع باید یک الگوریتم مبتنی بر cloud وجود داشته باشد زمانی که با حجم عظیمی از انتقال، تداخل و استراق سمع توسط شخص ثالث رو به رو هستیم. در کل از دیدگاه امنیتی باید یک چهار چوبی برای همکاری وجود داشته باشد که برای برنامه ها قابل تنظیم باشد.

٥-٤ تصدیق هویت handover و حفاظت از حریم خصوصی با استفاده از SDN (Software-Defined Networking)

استقرار سلول های کوچک همراه با محیط های ناهمگون به عنوان راه حلی برای شبکه های ۵G در نظر گرفته شده. با این حال این معماری چند لایه با الزامات سخت گیرانه در شبکه های ۵G چالش های جدیدی در تامین امنیت با توجه به پتانسیل

ISBN: 978-600-7461-60-0

hand over و احراز هویت در سلول های کوچک ۵G و Het nets به همراه دارد. در واقع می توان گفت با گسترش معماری چند لایه وظهور سلول های کوچکتر در شبکه های ۵G تامین امنیت و حفظ حریم خصوصی به یک چالش تبدیل شده است. در این زمینه محققان ابتدا به مطالعه و بررسی SDN برای شبکه های ۵G به عنوان یک پلتفرمی که قادر به تصدیق هویت موثر وحفاظت از حریم خصوصی hand over می باشد پرداختن. هدف محققان این است که یک تصدیق هویت ساده hand over را در ۵G Het nets به وسیله اطلاعات زمینه امنیتی کاربر در میان نقاط دستری به انجام برسانند. راه حل های امنیتی SDN بسیار کارآمد هستند و از طریق آن می توان قابلیت کنترل را متمرکز کرد که برای تاخیر در ارتباطات ۵G نیز می تواند ضروری باشد. باید به این نکته اشاره کرد که امنیت handover در شبکه های ۵G باید سریع وبدون کمترین پیچیدگی و همراه با کاهش اندازه سلول ها انجام شود. SDN به عنوان یک راه حل نه تنها یک پلتفرم مدیریت شبکه را فراهم می کند بلکه یک تصدیق هویت ساده handover که با کاهش تاخیر نیز همراه است را ارائه می دهد. بسیاری از موضوعات مرتبط مانند: پیچیدگی شبکه، عملکرد امنیتی تحت انواع حملات مختلف و استفاده موثر از اطلاعات در زمینه امنیت می تواند در مکانیزم های فعال سازی SDN در شبکه های ۵G مورد پژوهش قرار گیرد.



شکل ۵-SDN یک انتقال امن بین بین UE ۵G وAPs وAHM را در کنترلر SDN فعال می کند

۵-۵ حفاظت از امنیت نسل پنجم شبکه های مخابراتی با استفاده از امنیت لایه فیزیکی

نسل پنجم شبکه های مخابراتی میزان انتقال داده، پوشش رادیویی، زمان تاخیر خیلی پایین را دارا می باشند. اما یک مسئله مهمی که در اینجا وجود دارد این است که انتقال در شبکه های بی سیم ذاتا آسیب پذیر می باشد. بعضی از محققان تمرکز خود را بر روی امنیت لایه فیزیکی قرار دادن که محرمانه گی اطلاعات را تضمین می کند. در بین فناوری های مختلف سه بحث مختلف وجود دارد که عبارتند از : شبکه های ناهمگون، موج میلیمتری و بحث massive MIMO براساس اصول کلیدی هر یک از این فناوری ها محققان فرصت های غنی و چالش های برجسته ای را شناسایی کردن که طراحان امنیتی باید آن را مهار کنند. مانند identification که درک درستی از آینده امنیت لایه فیزیکی را به ما می دهد. شبکه های ۵G اساسا تاثیر عمیقی برروی طراحی امنیت لایه فیزیکی گذاشته است. یکی از مواردی را که در این قسمت بررسی خواهیم کرد massive MIMO می باشد این تکنولوژی در شبکه های ۵G می تواند از تعداد زیادی آرایه آنتن در فرستنده وگیرنده استفاده کند. و درآینده در شبکه های سلولی که با massive MIMO کار می کنند تعداد آرایه های آنتن در BS ها به طور چشم گیری افزایش پیدا می کند نسبت به مقدار جریان داده ای که برای تمام کاربران در هر سلول اختصاص داده می شود. در مقاسیه با سیستم های فعلی تکنولوژی massive MIMO قدرت بیشتر وطیف های گسترده تری را ارائه می دهد که با بهره برداری از طیف گسترده ای از gain آرایه ها میسر می شود. و طراحی سیستم انتقال با پیچیدگی کمتری را ایجاد

ISBN: 978-600-7461-60-0

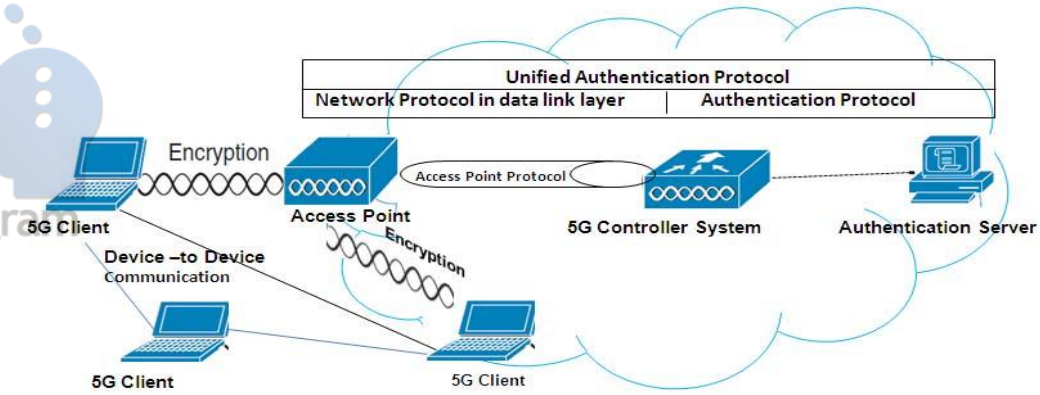
می کند. علاوه بر این اختلالات تصادفی مانند small scale ونویز می تواند به صورت متوسط باشد در صورتی که تعداد زیادی از آنتن ها در BS مستقر باشند. در massive MIMO می توان عملکرد امنیت را با کاهش مصرف انرژی افزایش داد. این افزایش را به دو علت عمده نسبت داده می شود: ۱- از آنجا که سطح انتقال قدرت قطع می شود دریافت نرخ سیگنال به نویز (SNR) در اسراق سمع به طور چشم گیری کاهش می یابد و این امر به طور قابل توجهی منجر به کاهش ظرفیت کانال استراق سمع می شود.۲- هنگامی که تعداد آنتن ها افزایش پیدا می کند با توجه به انتقال قدرت و نرخ امنیت انتظار می رود در فرستنده احتمال کاهش امنیت کم باشد. در بحث تکنولوژی امواج میلیمتری که در قسمت های قبل به آن اشاره کردیم و جزئی از شبکه های ۵G می باشند ودر فرکانس های ۳۰ تا ۳۰۰ گیگاهرتز کار می کنند وبه عنوان یک راه حل برای از بین بردن محدودیت ها وافزایش ظرفیت هزار برابر به رسمیت شناخته شده. امواج میلیمتری BS ها را می توان با ماکروویو ها در BS ها گسترش داد تا اطمینان حاصل شود که انتقال داده به صورت سریع و قابل اعتماد انجام می شود. نکته ای که در اینجا مطرح است امنیت و حریم خصوصی باید در سیستم های ارتباطی میلیمتری اجرایی شود. بسیاری از محققان باور دارند که تحقیقات در زمینه امنیت لایه فیزیکی درسیستم های ارتباطی امواج میلیمتری با توجه به معیار هایی از قبیل:۱-پهنای باند بیشتر۲- برد کوتاه انتقال۳-جهت۴- آرایه های آنتن های بزرگ بسیار امیدوار کننده و با ارزش می باشد.

۶-۵ ارائه یک معماری امنیتی برای نسل پنجم شبکه های مخابراتی مطابق با EU METIS ۵G project

با وجود اینکه شبکه های ۵G درآینده نزدیک در صنعت گسترش پیدا خواهد کرد اما استانداردهای امنیتی در آن نامشخص است. هدف محققان این است که یک طرح حفاظت عمومی برای دو طیف زیرساخت و برخی از اجزاء مهم ارائه دهند که سربار کمتری نیز داشته باشد. برهمین اساس معماری امنیتی یکپارچه ای را برای رفع نیاز های امنیتی ارائه دادند. این معماری برای استانداردهای جدید در مقابله با تهدیدات از جانب WLAN ها و تجهیزات تلفن همراه بسیار کارآمد می باشد واین معماری شامل اقداماتی متفاوت

برای مقابله با این تهدیدات می باشد. به طور خاص این معماری امنیتی از ادغام ۶ ماژول حاصل شده است :۱- اهراز هویت واحد و یک پارچه(unified authentication) ۲-اهراز هویت اضافی(additional authentication) ۳- رمزگذاری(encryption) ۴- دسترسی واحد ویک پارچه(unified access) ۵- دسترسی اضافی(additional access) ۶-امنیت یک پارچه (unified integrated security)

ISBN: 978-600-7461-60-0



شکل ٦-توپولوژی امنیت شبکه ٥G

همان طور که در شکل ۶ مشاهده می کنید اجزاء فیزیکی برای یک توپولوژی امنیت شبکه های ۵G شامل ۵G client- Access Access point (AP)- ۵G Network Controller(۵GNC)- Authentication server می باشد. در طراحی معماری امنیتی ۵G، Authentication server باید با ۵G Network Controller در ارتباط باشد. authentication server می تواند در زیر ساخت های WLAN استفاده شده و خدماتی از قبیل: سرویس های احراز هویت محلی، پشتیبانی از احراز هویت محلی، AAA (Authentication, Authorization and Accounting) و... را ارائه دهد. این معماری مطابق با هدف EU METIS ۵G project می باشد.

٦- نتیجه گیری:

برای متصل کردن دستگاه ها به شبکه که بخشی از اینترنت اشیاء محسوب می شود به سطح جدیدی از اتصالات بی سیم به اینترنت نیاز است به عبارت دیگر با نگاهی به سال ۲۰۲۰ یعنی تا ۵ سال دیگر اجرای پروژه هایی نظیر خودروهای خودران ، هواپیماهای بدون سرنشین تنها با استفاده از شبکه های ۵G میسر خواهد بود. طبق تخمین های زده شده توسط شرکت هایی نظیر سامسونگ نرخ انتقال اطلاعات در شبکه های ۵G ممکن است به ۱۰ گیگا بیت بر ثانیه برسد و نرخ دانلود برابر ۸۰۰گیگابیت بر ثانیه را داشته باشیم در حال حاضر چنین سرعتی در دسترس نیست وبه صورت آزمایشی به دست آمده. در این مقاله سعی کردیم که به معرفی نسل پنجم شبکه های مخابراتی بپردازیم و چالشهای پیش رو برای راه اندازی این نوع از شبکه از قبیل نبودن استاندارد واحد، طیف فرکانسی، تاخیر و چالش امنیت را بررسی کردیم. بیشتر بر روی چالش های امنیتی تمرکز کردیم وبه معرفی این چالش ها و راه کارهای ارائه شده توسط محققان پرداختیم. یک نکته ای که باید به آن اشاره کنیم امواج میلیمتری می باشد که به عنوان یکی از

ارکان ۵G در نظر گرفته می شود، امواج میلیمتری چالش های امنیتی مربوط به خود را دارند که به عنوان کار آینده گان در نظر گرفته می شود.

ISBN: 978-600-7461-60-0

منابع:

محمدی زاده،میثاق، ۱۳۹۴،پرونده ویژه 5G، شماره ۱۶۹، ماهنامه شبکه

تحویل داری، هومن،۱۳۹۴،پرونده ویژه 5G، شماره ۱۶۹، ماهنامه شبکه

[۱] Nan Yang, Lifeng Wang, Giovanni Geraci, Maged Elkashlan, Jinhong Yuan, and Marco Di Renzo "Safeguarding ۵G Wireless Communication Networks Using Physical Layer Security" IEEE april ۲۰۱۵

[۲] Samah A. M. Ghanem*, Munnujahan Ara "Secure Communications with D۲D Cooperation" Mobile Communications Department, Eurecom, Sophia Antipolis, France, Khulna University, Khulna-۹۲۰۸, Bangladesh,۲۰۱۵

[۳] Xiaoyu Duan and Xianbin Wang "Authentication Handover and Privacy Protection in ۵G HetNets Using software – defined networking" IEEE Communications Magazine • April ۲۰۱۵

[۴] Qi Fang, Zhang WeiJie, Wang Guojun , Fang Hui" Unified Security Architecture Research for ۵G Wireless System" School of Information Science and EngineeringCentral South University, nstitute for Infocomm Research, Agency for Science, Technology and Research Singapore ۲۰۱۴

[۵] Mohsen Nader Tehrani, Murat Uysal, and Halim Yanikomeroglu" Device-to-Device Communication in ۵G Cellular Networks: Challenges,Solutions, and Future Directions" IEEE Communications Magazine, may ۲۰۱۴

[۶] Gianmarco Baldini, Taj St urman, Abdur Rahim Biswas, Ruediger,Leschhorn, Gy¨oz¨oG´odor, Michael Street" Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead" Member, IEEE,۲۰۱۲

[۸] MA Zheng, ZHANG ZhengQuan ,DINGZhiGuo,FANPingZhi &LIHengChao "Key techniques for ۵G wireless communications:network architecture, physical layer,and MAC layer perspectives" Provincial Key Lab of Information Coding and Transmission,

ISBN: 978-600-7461-60-0

Southwest Jiaotong University, Chengdu ۶۱۰۰۳۱,Chin, Department of Communication Systems, Lancaster University, Lancaster LA۱ ۴YW,UK , ۲۰۱۵

[۹] Kashif Faheem, Dr Khalid Rafique "securing ۴G /۵G wireless networks" Pakistan Telecommunication Company ,۲۰۱۵

[۱۰] R. Guerzoni, R. Trivisonno, D. Soldani "SDN-Based Architecture and Procedures for ۵G Networks" Huawei, European Research Institute (ERI) Munich, Germany,۲۰۱۴

ISBN: 978-600-7461-60-0