

شبکه‌های بی سیم نسل پنجم امنیت و حریم خصوصی

نویسندگان:

Dong FengFang, Yi Qian & Rose Qingyang Hu

مترجمان:

اسماعیل سندگل - رضا آذریان

سرشناسه	فانگ، دانگ فنگ
عنوان و نام پدیدآور	Fang, Dongfeng
مشخصات نشر: مشهد	شبکه‌های بی‌سیم نسل پنجم، امنیت و حریم خصوصی / نویسندگان دانگ فنگ فنگ، ئی کیان، رز کینگ یانگ هو؛ مترجمان اسماعیل سندگل، رضا آذریان.
مشخصات ظاهری	درخشش، ۱۴۰۳.
شابک	۹۷۸-۶۰۰-۵۱۰۶-۳۹-۸:
وضعیت فهرست نویسی	فیپا:
یادداشت	عنوان اصلی: 5G wireless network security and privacy, c2023.
موضوع	مخابرات -- نسل پنجم سیستم‌های سیار -- تدابیر ایمنی 5G mobile communication systems -- Security measures
شناسه افزوده	چیان، یی، ۱۹۶۲-م.
شناسه افزوده	- Qian, Yi, 1962:
شناسه افزوده	هو، رز چینگ یانگ
شناسه افزوده	Hu, Rose Qingyang:
شناسه افزوده	سندگل، اسماعیل، ۱۳۶۴- مترجم
شناسه افزوده	آذریان، رضا، ۱۳۴۴-، مترجم
رده بندی کنگره	۲۵/TK۵۱۰۳:
رده بندی دیویی	۳۸۴۵۶/۶۲۱:
شماره کتابشناسی ملی	۹۵۹۱۰۰۱:
اطلاعات رکورد کتابشناسی	فیپا



شبکه‌های بی‌سیم نسل پنجم، امنیت و حریم خصوصی

نویسندگان: دانگ فنگ فنگ، ئی کیان، رز کینگ یانگ هو

مترجمان: اسماعیل سندگل، رضا آذریان

ویراستار: محمدصادق امینی مقدم

نوبت / سال چاپ: اول ۱۴۰۳

شمارگان: ۲۰۰ نسخه

قیمت: ۲۲۰,۰۰۰ تومان

شابک: ۹۷۸-۶۰۰-۵۱۰۶-۳۹-۸

مشهد، خیابان سعدی، پاساژ مهتاب، شماره ۲۵ تلفن: ۰۵۱ ۳۲۲۵۱۹۲۳

www.derakhsheshbook.com @ derakhshesh.book

فهرست مطالب

فصل اول - مقدمه‌ای بر سیستم‌های بی‌سیم نسل پنجم ۱

۱-۱ انگیزه‌ها و اهداف شبکه‌های بی‌سیم نسل پنجم	۱
۲-۱ درایوهای امنیتی و الزامات	۳
۳-۱ معماری شبکه بی‌سیم نسل پنجم	۶
۱-۳-۱ مروری بر معماری شبکه بی‌سیم نسل پنجم	۶
۲-۳-۱ مقایسه بین شبکه سلولی قدیمی و شبکه بی‌سیم نسل پنجم	۸
۴-۱ نتیجه‌گیری	۹
فصل دوم - امنیت از سیستم‌های بی‌سیم قدیمی تا شبکه‌های نسل پنجم	۱۰
۱-۲ امنیت شبکه برای سیستم‌های قدیمی	۱۰
۲-۲ حملات امنیتی و خدمات امنیتی در شبکه‌های بی‌سیم نسل پنجم	۱۵
۱-۲-۲ حملات امنیتی	۱۵
۲-۲-۲ خدمات امنیتی	۱۸
۳-۲ تکامل معماری‌های امنیتی بی‌سیم از نسل سوم به نسل پنجم	۲۲
۱-۳-۲ معماری امنیتی نسل سوم	۲۲
۲-۳-۲ معماری امنیتی نسل چهارم	۲۴
۲-۳-۳ معماری امنیت بی‌سیم نسل پنجم	۲۵
۴-۲ خلاصه	۲۹
فصل سوم - مکانیسم‌های امنیتی در سیستم‌های بی‌سیم نسل پنجم	۳۰
۱-۳ رویکردهای رمزنگاری و امنیت لایه فیزیکی	۳۰
۲-۳ احراز هویت	۳۵
۳-۳ در دسترس بودن	۴۳
۴-۳ محرمانه بودن داده‌ها	۴۷
۵-۳ مدیریت کلید	۵۴
۶-۳ حریم خصوصی	۵۶
۷-۳ نتیجه‌گیری	۵۷
فصل چهارم - افزایش امنیت شبکه‌های نسل پنجم توسط نوین‌های مصنوعی و فرایند تداخل	۵۹
۱-۴ افزایش امنیت نسل پنجم از طریق استفاده از نوین مصنوعی و تداخل	۵۹
۲-۴ مثالی از مدل سیستم HetNet و تحلیل امنیتی آن	۶۱

۱-۱-۱	مدن سیسم و مدن بهدید	۶۱
۲-۲-۴	تجزیه و تحلیل امنیتی	۶۴
۱-۳-۴	حداکثر میزان رازداری	۶۶
۲-۳-۴	الگوریتم پیشنهادی	۶۷
۴-۴	نتایج عددی و شبیه سازی	۷۲
۵-۴	نتیجه گیری	۷۶
	فصل پنجم - طرح‌های امنیتی انعطاف پذیر	۷۷
۱-۵	معرفی	۷۸
۲-۵	بررسی ادبیات فنی	۸۱
۳-۵	چالش‌های امنیت و حریم خصوصی اینترنت اشیا	۸۳
۱-۳-۵	امنیت	۸۴
۴-۵	اینترنت اشیا	۸۵
۱-۴-۵	حریم خصوصی	۸۶
۲-۴-۵	قابلیت اشتراک گذاری داده و منابع بین دستگاه‌ها	۸۶
۳-۴-۵	آینده اینترنت اشیا	۸۸
۵-۵	حفاظت از رمز عبور ضعیف	۹۴
۱-۵-۵	فقدان پیچ‌ها و آپدیت‌های منظم و مکانیزم ضعیف به روز رسانی	۹۵
۲-۵-۵	رابطه‌های ناامن	۹۶
۳-۵-۵	حفاظت ناکافی از داده‌ها (ارتباطات و ذخیره سازی)	۹۷
۶-۵	مدیریت ضعیف تجهیزات اینترنت اشیا	۹۸
۷-۵	امنیت سایبری اینترنت اشیا از پایه	۱۰۲
۱-۷-۵	رسیدگی موثر به نگرانی‌های امنیتی IoT	۱۰۳
	فصل ششم - مدیریت انتقال ایمن و کارآمد در شبکه‌های بی سیم نسل پنجم	۱۰۴
۱-۶	مسائل و ملزومات ارتباط از طریق شبکه‌های بی سیم نسل پنجم	۱۰۴
۲-۶	یک مدل نسل پنجم CN و مدل سیستم HetNet	۱۰۵
۳-۶	سناریوها و رویه‌های انتقال نسل پنجم	۱۱۱
۲-۳-۶	رویه‌های تحویل	۱۱۱
۴-۶	یک پروتکل احراز هویت جدید برای شبکه‌های نسل پنجم	۱۱۶
۱-۴-۶	مفروضات	۱۱۶
۲-۴-۶	پیشن احراز هویت	۱۱۷

۱۱۹ احراز هویت کامل	۳-۴-۶
۱۲۱ احراز هویت سریع	۴-۴-۶
۱۲۳ تجزیه و تحلیل امنیتی پروتکل های جدید احراز هویت نسل پنجم	۵-۶
۱۲۴ ارزیابی عملکرد	۶-۶
۱۲۵ سربار ارتباط	۱-۶-۶
۱۲۵ سربار محاسبات	۲-۶-۶
۱۲۶ نتیجه گیری	۷-۶
۱۲۷ فصل هفتم - مسائل باز و دستورالعمل های تحقیقاتی آینده برای امنیت و حریم خصوصی	
۱۲۹ مدل های جدید اعتماد	۱-۷
۱۳۰ مدل های جدید حمله امنیتی	۲-۷
۱۳۰ حفاظت از حریم خصوصی	۳-۷
۱۳۱ مدیریت امنیت یکپارچه	۴-۷

فهرست تصاویر

- شکل ۱-۱ معماری کلی سیستم‌های بی‌سیم نسل پنجم ۳
- شکل ۱-۲ درایوهای امنیتی و الزامات امنیت بی‌سیم نسل پنجم ۴
- شکل ۱-۳ مدل اعتماد شبکه‌های بی‌سیم نسل چهارم و نسل پنجم ۶
- شکل ۱-۴ معماری عمومی شبکه بی‌سیم نسل پنجم ۸
- شکل ۱-۲ حملات در شبکه‌های بی‌سیم نسل پنجم (a) استراق سمع، (b) پارازیت، (c) DDoS، و (d) MITM ۱۷
- شکل ۲-۲ معماری امنیتی نسل سوم تعریف شده توسط نسل سوم PP TS 33.102 ۲۳
- شکل ۲-۳ معماری امنیتی نسل چهارم تعریف شده توسط نسل سوم PP TS 33.402 ۲۵
- شکل ۲-۴ معماری امنیتی شبکه بی‌سیم نسل پنجم ۲۷
- شکل ۱-۳ رمزگذاری و رمزگشایی با کلید متقارن ۳۲
- شکل ۲-۳ مدیریت کلید با KDC ۳۲
- شکل ۳-۳ رمزگذاری و رمزگشایی مبتنی بر کلید عمومی ۳۳
- شکل ۳-۴ امضای دیجیتال مبتنی بر کلید عمومی ۳۳
- شکل ۳-۵ یک مدل احراز هویت با قابلیت SDN [Duan and Wang, 2016] ۳۸
- شکل ۳-۶ فرآیند احراز هویت طرح ابطال برنامه امن RFID [فن و همکاران، 2015] ۴۰
- شکل ۳-۷ مدل سیستم m-health [ژانگ و همکاران، 2017a] ۴۱
- شکل ۳-۱۰ مدل تخصیص منابع [Labib et al. 2015] ۴۶
- شکل ۳-۱۱ مدل کلی سیستم با حملات شنود ۴۶
- شکل ۳-۱۲ مدل سیستم با لینک D2D و یک استراق سمع ۴۹
- شکل ۳-۱۳ سه طرح تبادل کلید در سدیدی و کومار [Sedidi and Kumar, 2016] ۵۵
- شکل ۴-۱ مدل سیستم دو لایه HetNet مورد مطالعه ۶۲
- شکل ۴-۲ نمودار جریان الگوریتم ۷۱
- شکل ۳-۴ میزان محرمانه بودن کاربر تحت حمله شنود ۷۳
- شکل ۴-۴ میزان پنهان کاری با تعداد متفاوت جفت D2D ۷۴
- شکل ۴-۵ توان انتقال SBS ۷۵
- شکل ۱-۶ مقایسه LTE CN و نسل پنجم CN ۱۰۶
- شکل ۲-۶ مدل سیستم هت نت نسل پنجم ۱۰۸
- شکل ۳-۶ مدل اعتماد در مدل سیستم مورد مطالعه ۱۰۹
- شکل ۴-۶ فرآیندهای انتقال UP از یک ماکروسل BS به یک سلول کوچک AP ۱۱۲

فصل اول

مقدمه‌ای بر سیستم‌های بی‌سیم نسل پنجم

شبکه‌های بی‌سیم نسل پنجم^۱، نوعی از ارتباطات بی‌سیم سیار، فراتر از سیستم‌های پیشرفته نسل چهارم^۲ هستند. این نوع شبکه‌ها (به اختصار 5G) نه تنها تکامل شبکه‌های سلولی قدیمی نسل چهارم‌اند، بلکه سیستم ارتباطی جدیدی هستند که می‌توانند بسیاری از قابلیت‌های خدمات جدید را پشتیبانی کند [۱]. در این فصل، پیشینه‌ای کلی از شبکه‌های بی‌سیم نسل پنجم و امنیت آن، از جمله انگیزه‌ها و اهداف، انگیزه‌ها، الزامات امنیتی و معماری کلی‌اش را معرفی می‌کنیم.

۱-۱ انگیزه‌ها و اهداف شبکه‌های بی‌سیم نسل پنجم

تحقیق و توسعه فناوری نسل پنجم بر دستیابی به ویژگی‌های پیشرفته‌ای مانند ظرفیت افزایش یافته برای پشتیبانی از تعداد بیشتری از کاربران با سرعت‌های بیشتر از نسل چهارم، افزایش تراکم کاربران پهنای باند تلفن همراه برای بهبود پوشش متمرکز، و پشتیبانی ارتباطات دستگاه به دستگاه (D2D)، ارتباطات عظیم از نوع ماشین، برنامه‌ریزی نسل پنجم همچنین با هدف ارائه عملکرد بهتر شبکه از نظر زمان، تأخیر کمتر و مصرف انرژی کمتر برای پشتیبانی بهتر از اجرای اینترنت اشیا است [۲]. به طور خاص، هشت ویژگی پیشرفته سیستم‌های بی‌سیم نسل پنجم به شرح زیر است:

- سرعت داده: ۱-۱۰ گیگابیت بر ثانیه در سمت کاربر.
- تأخیر کم: تأخیر ۱ میلی ثانیه برای درخواست‌ها.
- پهنای باند: ۱۰۰۰ برابر پهنای باند در واحد سطح.

^۱ 5 Generation

^۲ G4/International Mobile Telecommunications (IMT)

- قابلیت اتصال: ۱۰-۱۰۰ برابر تعداد دستگاه‌های متصل.
- در دسترس بودن: ۹۹/۹۹٪ در دسترس بودن.
- پوشش: ۱۰۰٪ پوشش.
- بهره‌وری انرژی شبکه: کاهش ۹۰ درصدی مصرف انرژی شبکه.
- بهره‌وری انرژی دستگاه: افزایش عمر باتری برای دستگاه‌های کم مصرف تا ۱۰ سال.

برای دستیابی به این هشت ویژگی پیشرفته عملکرد شبکه، فناوری‌های مختلفی برای سیستم‌های نسل پنجم، مانند شبکه‌های ناهمگن^۱ (HetNet)، چند خروجی چند ورودی عظیم^۲ (MIMO)، موج میلی‌متری^۳ (mmWave)، ارتباطات D2D، شبکه نرم افزاری تعریف شده^۴ (SDN)، مجازی سازی توابع شبکه^۵ (NFV)، و برش شبکه^۶، استفاده می‌شوند. فرآیند استاندارد سازی برای سیستم‌های بی‌سیم نسل پنجم انجام شده است [۳]. شکل ۱-۱ سیستم‌های بی‌سیم نسل پنجم عمومی را نشان می‌دهد.

¹ heterogeneous networks (HetNet)

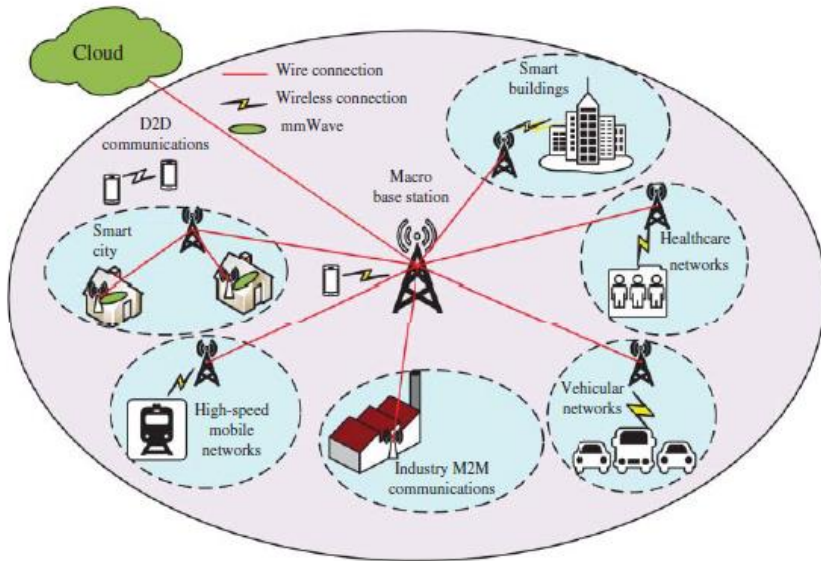
² multiple-input multiple-output (MIMO)

³ millimeter wave (mmWave)

⁴ software-defined network (SDN)

⁵ software-defined network (NFV)

⁶ network slicing



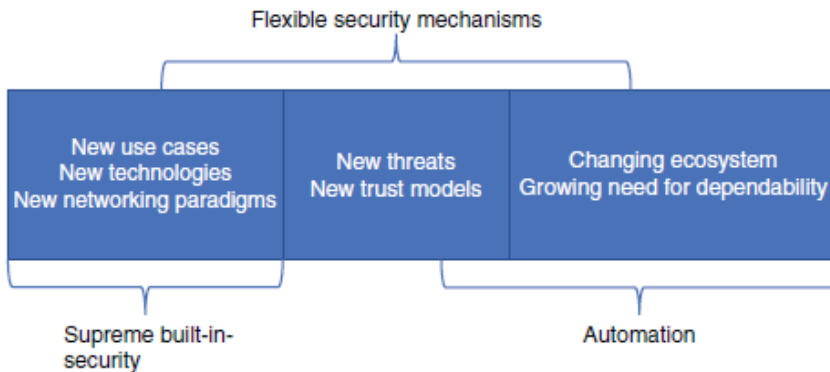
شکل ۱-۰ معماری کلی سیستم‌های بی‌سیم نسل پنجم

همانطور که در شکل ۱-۱ نشان داده شده است سیستم‌های بی‌سیم نسل پنجم نه تنها می‌توانند ارتباطات سنتی صوتی و داده‌ای، بلکه بسیاری از کاربردهای جدید مانند کاربردهای صنعتی جدید، و تعداد زیادی دستگاه و برنامه کاربردی برای اتصال جامعه را نیز فراهم کنند. در شکل ۱-۱ کاربردهای مختلف نسل پنجم، مانند ارتباطات وسیله نقلیه به وسیله نقلیه و وسیله نقلیه به زیرساخت، اتوماسیون صنعتی، خدمات بهداشتی، شهرهای هوشمند و خانه‌های هوشمند مشخص شده است. اعتقاد بر این است که سیستم‌های بی‌سیم نسل پنجم می‌توانند پهنای باند تلفن همراه را با خدمات حیاتی و برنامه‌های کاربردی عظیم اینترنت اشیا تقویت کنند [۴]. با معماری، فناوری‌ها و کاربردهای جدید در سیستم‌های بی‌سیم نسل پنجم، برای تأمین امنیت و حفاظت از حریم خصوصی این سیستم‌ها با چالش‌های جدیدی مواجه خواهند شد.

۲-۱ انگیزه‌های امنیتی و الزامات

برای دستیابی به اهداف شبکه‌های بی‌سیم نسل پنجم، محرک‌ها و الزامات امنیتی ضروری است. شکل ۲-۱ انگیزه‌های اصلی امنیت شبکه بی‌سیم نسل پنجم را به عنوان امنیت داخلی عالی، مکانیسم‌های امنیتی

ثابت و اتوماسیون نشان می‌دهد. از آنجایی که در نسل پنجم، کاربردهای جدید، فناوری‌های جدید و پارادایم‌های جدید شبکه معرفی شده‌اند، امنیت داخلی قوی‌ای نیاز است. کاربردهای دیگر می‌توانند الزامات خاصی مانند تأخیر بسیار کم در ارتباطات کاربر را معرفی کنند که به بهبود عملکرد مکانیسم‌های امنیتی فعلی نیاز دارد. فن‌آوری‌های جدید قابلیت‌های خدمات پیشرفته‌ای را ارائه می‌کنند و همچنین آسیب‌پذیری‌های جدیدی ایجاد می‌کنند و بنابراین الزامات امنیتی جدیدی را به نسل پنجم تحمیل می‌کنند [۵]. در HetNet، فناوری‌های دسترسی مختلف ممکن است نیازمندی‌های امنیتی متفاوتی داشته باشند و یک محیط چند شبکه‌ای ممکن است به احراز هویت مکرر با محدودیت‌های تأخیر نیاز داشته باشد. MIMO عظیم یک تکنیک حیاتی نسل پنجم برای دستیابی به راندمان طیفی و بازده انرژی بالاتر در نظر گرفته شده است. MIMO همچنین به عنوان یک تکنیک ارزشمند در برابر استراق سمع غیرفعال در نظر گرفته می‌شود. علاوه بر این، SDN و NFV در نسل پنجم از مدل‌های ارائه خدمات جدید پشتیبانی می‌کنند و بنابراین به جنبه‌های امنیتی جدید نیاز دارند. با ظهور پارادایم‌های شبکه نسل پنجم، یک معماری امنیتی جدید مورد نیاز است. برای رسیدگی به این مسائل، امنیت باید بخشی جدایی‌ناپذیر از معماری کلی در نظر گرفته شود و بایستی در طراحی سیستم به کار برده شود.



شکل ۲-۰ انگیزه‌های امنیتی و الزامات امنیت بی‌سیم نسل پنجم