

۱۴۲۴۷۶۱
- ۱۵, ۱۶

به نام خدا

مؤسسه فرهنگی هنری
دیباگران تهران

امنیت شبکه های LTE

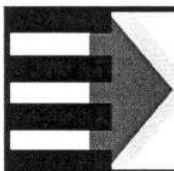
(شبکه های نسل اولی نسل جدید)

تألیف و تدوین:

مرکز تحقیقات فناوری اطلاعات و ارتباطات صدر

(محمد صابری، بهمن مددی، سید مرتضی پورعلی)

بهار ۱۳۹۵



هرگونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی
ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق
مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می گیرند.

برشنامه: صابری محمد، ۱۳۶۶

عنوان و نام پدید آور: امنیت شبکه های LTE (شبکه های سلولی نسل جدید) / مؤلفان: محمد صابری، مهدی سید مرتضی پورنقی، مرکز تحقیقات و فناوری اطلاعات و ارتباطات صابر.

مشخصات نشر: تهران - دیباگران تهران ۱۳۹۵

مشخصات ظاهری: ۴۰۹ ص.

شابک: ۹۷۸-۶۰۰-۱۲۴-۴۷۴-۲

وضعیت فهرست نویسی: فیا

موضوع: تکامل بلند مدت (مخابرات)

موضوع: Long-term evolution (telecommunications)

شماره افزوده: مهدی، ۱۳۶۶

شماره افزوده: پورنقی، سید مرتضی، ۱۳۶۶

شماره افزوده: مرکز تحقیقات و فناوری اطلاعات و ارتباطات صابر

رده بندی کنگره: ۱۳۹۵ A ۲ قف ۵۱ TK ۵۱-۳۱۴۹۸۲۱۸۵

رده بندی دیویی: ۶۲۱/۳۴۵۶

شماره کتابشناسی ملی: ۳۳۷۱۸۵۸

امنیت شبکه های LTE

شبکه های سلولی نسل جدید

مؤلفان: محمد صابری

مهدی

سید مرتضی پورنقی

ناشر: مؤسسه فرهنگی هنری دیباگران تهران

حروفچینی و صفحه آرایی: دیباگران تهران

طرح روی جلد: مجتبی حابری

چاپ: دانشجو

نوبت چاپ: اول

تاریخ نشر: ۱۳۹۵

تیراژ: ۳۰۰ جلد

قیمت: ۴۳۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۱۲۴-۴۷۴-۲

ISBN: 978-600-124-474-2

نشانی واحد فروش: تهران، میدان انقلاب، خ کارگر جنوبی، رویروی پاسار مهرسان، پلاک ۱۲۵۱

تلفن: ۰۲۲-۸۵۱۱۱۱۱-۶۶۴۱۰۰۴۶ کد پستی: ۱۳۱۴۹۸۲۱۸۵

فروش اینترنتی:

www.mftshop.com

www.mftbook.ir

پست الکترونیکی: bookmarket@mftmail.com

نشانی اینستاگرام: Dibagaran_publishing

نشانی تلگرام: @mftbook

فهرست

۱	امنیت شبکه های LTE
۱	(شبکه های سلولی نسل جدید)
۱	تألیف و تدوین
۱	مرکز تحقیقات فناوری اطلاعات و ارتباطات صدر
۱۵	پیشگفتار
۱۷	مقدمه
۲۰	فصل ۱
۲۰	مروری بر تاریخچه مخابرات سلولار
۲۱	۱-۱ دیپاچه
۲۱	تلفن همراه نسل اول (1G): صدای آنالوگ
۲۱	۱-۱ تاریخچه
۲۲	۱-۲ معماری
۲۴	تلفن همراه نسل دوم (2G): صدای دیجیتال
۲۴	تاریخچه
۲۶	معماری شبکه GSM
۳۳	نقش سیم کارت در سیستم GSM
۳۸	مکانیزم رمزگذاری سیستم GSM
۴۲	بررسی امنیت شبکه GSM
۴۴	تلفن همراه 2.5G
۴۴	تاریخچه

۴۸	معماری سیستم
۵۲	تلفن همراه نسل سوم (3G): صدای دیجیتال و داده
۵۲	تاریخچه
۵۶	معماری شبکه UMTS
۶۰	بررسی امنیت شبکه UMTS
۶۶	رمز گذاری محیط رادیویی
۶۶	ماین احراز اصالت مشترک SIM
۶۶	محرمانگی شناسه کاربر در محیط رادیویی
۶۷	فصل ۲
۶۷	مخابرات نسل چهارم (4G)
۷۵	تاریخچه
۷۶	LTE (تکامل بلند مدت - Long Term Evolution)
۷۷	بررسی امنیت در شبکه LTE
۷۸	سیر تکامل از LTE به LTE Advanced
۸۱	فصل ۳
۸۱	معماری شبکه ی LTE
۸۳	UE (User Equipment)
۸۴	E-UTRAN (Evolved UTRAN)
۸۷	EPC (Evolved Packet Core)
۹۱	پشتیبانی از دست به دست شدن
۹۲	تعامل با دیگر شبکه های رادیویی
۹۳	پشتیبانی از صوت و SMS
۱۰۹	سطوح پروتکل در شبکه LTE

۱۰۹	 پروتکل‌های سطح کاربر
۱۱۰	 پروتکل‌های سطح کنترل
۱۱۱	 کیفیت سرویس و حامل‌های EPS
۱۱۴	 فرایند انتقال صوت در شبکه LTE
۱۱۵	 IMS از طریق LTE
۱۱۸	 Circuit Switched Fallback (CSFB)
۱۱۸	 یکپارچه‌سازی Single Radio Voice Call Continuity (SRVCC)
۱۲۰	 Relay Node
۱۲۱	 RN در نقش یک UE
۱۲۱	 RN در نقش یک ایستگاه پایه
۱۲۲	 مراحل آغاز به کار RN
۱۲۳	 ایستگاه خانگی (HeNB)
۱۲۴	 سناریو استفاده از HeNB‌ها
۱۲۶	 پایانه امنیت SeGW
۱۲۷	 سیستم مدیریت HeNB (HeMS)
۱۲۹	 CSG
۱۲۹	 رابط X2
۱۲۹	 رابط S5
۱۲۹	 معماری امنیتی HeNB
۱۳۲	 فصل ۴
۱۳۲	 فرایند تماس و مکالمه
۱۳۳	 حالت‌های مختلف اتصال اولیه:
۱۳۴	 Unknown UE

۱۳۵	حالت اول پیوست
۱۳۵	حالت دوم پیوست
۱۳۶	Know UE
۱۳۹	نمایش ساده جریان تماس در حالت های مختلف
۱۴۰	Initial Attach with IMSI
۱۴۱	Initial Attach with GUTI
۱۴۲	Initial Attach Procedure
۱۴۳	IMSI Acquisition
۱۴۶	Authentication
۱۴۷	IMS Security Setup
۱۴۷	Location Update
۱۴۸	EPS Session Establishment
۱۵۷	EPS Entity Information
۱۵۸	قبل از پیوست اولیه
۱۵۸	بعد از پیوست اولیه
۱۵۹	Traffic Flow on the LTE Network
۱۶۰	Traffic flow in uplink direction: from UE to the Internet
۱۶۱	Traffic flow in downlink direction: from the Internet to UE
۱۶۱	IP Address: ID Necessary to Connect to a PDN
۱۶۲	LTE IP Address Allocation Schemes
۱۶۴	Dynamic IP Address Allocation
۱۶۷	Static IP Address Allocation
۱۷۲	فصل ۵

ویژگی‌ها و نیازمندی‌های امنیتی شبکه LTE.....	۱۷۲
مقدمه.....	۱۷۳
نگاهی به معماری امنیتی شبکه LTE.....	۱۷۶
ویژگی‌های امنیتی استفاده شده در EPS.....	۱۷۷
محرمانگی هویت دستگاه و کاربر.....	۱۷۷
تصدیق هویت بین UE و شبکه.....	۱۷۹
احراز هویت کاربر.....	۱۸۰
محرمانگی داده‌ی کاربر و داده‌ی سیگنالینگ.....	۱۸۱
الگوریتم‌های رمزنگار مورد استفاده در EPS.....	۱۸۱
یکپارچگی داده‌ی کاربر و داده‌ی سیگنالینگ.....	۱۸۲
مشاهده پذیری و پیکربندی امنیتی.....	۱۸۳
نشانه‌ای از رمزگذاری شبکه.....	۱۸۳
فعال و غیر فعال کردن احراز اصالت USIM کاربر.....	۱۸۳
مذاکره امنیتی الگوریتم‌ها.....	۱۸۳
حفاظت سیگنالینگ NAS.....	۱۸۵
خط مشی امنیتی eNodeB.....	۱۸۵
شنود قانونی.....	۱۸۶
تماس‌های اضطراری.....	۱۸۶
امنیت تعامل.....	۱۸۶
امنیت حوزه شبکه ((Network Domain Security (NDS)).....	۱۸۶
پرو فایل‌های گواهینامه.....	۱۹۰
رویکرد لایه بندی شده‌ی امنیت در شبکه LTE.....	۱۹۳
نیازمندی‌های امنیتی در eNB.....	۱۹۴

۱۹۵	نیازمندی‌های امنیتی در HeNB
۱۹۷	خصوصیات امنیتی HeNB
۱۹۷	مفاهیم احراز هویت
۱۹۸	احراز هویت با استفاده از IKEv2
۲۰۰	محیط مورد اعتماد و اجرای امن
۲۰۱	ماژول طرف میزبان
۲۰۱	امنیت فیزیکی
۲۰۱	امنیت مخابرات
۲۰۲	تصدیق مکان و زمان
۲۰۲	فرایندهای امنیت داخلی در دستگاه پایه خانگی
۲۰۲	راه‌اندازی امن و بررسی صحت دستگاه
۲۰۳	حذف ماژول طرف میزبان (HPM)
۲۰۳	از دست رفتن لینک بازگشتی
۲۰۴	پایه زمانی امن
۲۰۵	دستکاری اطلاعات گذاری داخلی
۲۰۶	فصل ۶
۲۰۶	معماری امنیتی شبکه LTE
۲۰۷	مقدمه
۲۱۰	فرایند احراز اصالت و توافق کلید AKA
۲۱۲	اهداف و پیش نیازهای EPS AKA
۲۱۴	توزیع بردارهای تصدیق EPS از HSS به MME
۲۱۷	احراز اصالت دوسویه و برقراری کلید به اشتراک گذاری شده بین Serving Network و UE
۲۲۱	بسته مخابراتی غنی و صوت از طریق LTE

۲۲۱		خصوصیات امنیتی برای RCS و VoLTE
۲۲۱		فرایند توزیع کلید در شبکه
۲۲۲		سلسله مراتب کلید
۲۲۳		استخراج کلید
۲۲۷		هدف کلیدهای سلسله مراتبی
۲۲۹		شناختی کلیدهای EPS
۲۳۰		فرایند دست به دست شدن
۲۳۳		پیش زمینه سازیم ترانزیت کلید (Handover keying)
۲۳۳		احراز اصالت و کالته داده شده
۲۳۳		درخواست کلید
۲۳۴		دسترسی خوشبینانه (Optimistic Access)
۲۳۶		مدیریت دست به دست شدن کلیدهای LTE
۲۴۰		Key Change on the Fly
۲۴۱		مکانیزم های امنیت صوت در شبکه LTE
۲۴۱		امنیت IMS در LTE
۲۴۲		امنیت سیگنال دهی IMS
۲۴۲		احراز هویت مشترک در فرایند ثبت نام کردن IMS
۲۴۶		محرمانگی و محافظت از یکپارچگی برای سیگنال دهی SIP در IMS
۲۵۰		امنیت سطح رسانه IMS
۲۵۱		امنیت Circuit Switched Fallback
۲۵۲		امنیت Single Radio Voice Call Continuity
۲۵۲		تحويل SRVCC از LTE به UTRAN
۲۵۳		Handover SRVCC از LTE به GERAN

۲۵۳ امنیت داخلی شبکه LTE

۲۵۳ ثبت نام کاربر در شبکه

۲۵۴ لغو کاربر در شبکه

۲۵۴ تحرک پذیری در حالت idle

۲۵۹ راه اندازی هم زمان فرایندهای امنیتی

۲۶۱ خدمات مکان (سکونت)

۲۶۴ خدمات پیام کوتاه (SMS)

۲۶۶ تصمیمات طراحی برای امنیت EPS

۲۶۶ وابسته سازی دانش امنیت

۲۶۶ واسطها در UE و SS/HLR

۲۶۷ استفاده دوباره از 3G USIM

۲۶۷ عدم استفاده از 2G SIM ها در EPS

۲۶۸ احراز اصالت و کالتهی

۲۶۸ جداسازی شبکه رمزنگاری و شبکه خدمت رسانی احراز اصالت

۲۶۹ نقطه انتهایی رمزگذاری و یکپارچگی

۲۷۱ سلسله مراتب جدید کلید در EPS

۲۷۲ جداسازی کلید در فرایند دست به دست شدن

۲۷۳ خط مشی امنیت همگن برای دسترسی به شبکه های ناهمگن

فصل ۷ ۲۷۵

ارزیابی خطر و بررسی تهدیدها ۲۷۵

۲۷۸ روش ارزیابی بکار گرفته شده در ASMONIA

۲۸۰ تعاریف

۲۸۴ دسته بندی تهدیدها

۲۸۶	دسته بندی تهدیدات
۲۹۱	ارزیابی خطر
۲۹۱	شبکه‌ی هسته
۳۰۸	تهدیدهای مرتبط با سیستم چند رسانه‌ای IP (IMS)
۳۱۱	ارزیابی تهدیدهای مرتبط با PCRF و سیستم شارژ
۳۱۵	ارزیابی تهدیدهای علیه خدمات مکان‌یابی
۳۱۶	ارزیابی تهدیدات علیه SMS
۳۱۸	زخم پذیری
۳۱۸	تهدیدهای مرتبط با آنتن همراه کاربر UE
۳۳۰	اقدامات متقابل علیه ردیابی UE مبتنی بر اعداد متوالی
۳۳۳	اقدامات مقابله با دست بردن فیزیکی
۳۳۶	تهدیدات مواجه با خود راه انداز محافظت شده و سیگنالینگ چندبخشی در LTE
۳۳۷	تهدیدهای مرتبط با پخش اطلاعات سیستم
۳۴۳	تهدیدهای مرتبط با eNB و long-haul transport links
۳۴۵	فرایند سیگنالینگ برای احراز هویت محلی دوره‌ای
۳۵۴	حملات حذف
۳۵۴	نتیجه گیری
۳۵۵	تهدیدات واسطه‌های ارتباطی شبکه LTE
۳۶۱	نتیجه گیری
۳۶۲	تهدیدات هسته شبکه
۳۶۷	زخم پذیری شبکه‌های Backhaul در LTE
۳۷۰	تهدیدات امنیتی در IMS
۳۷۶	تقلب

خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب فنی است که بتواند خواسته های به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.

حمد و سپاس ایزد منان را که با الطاف بیکران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای نشر عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گسترده‌گی علوم و تخصص‌ها، افزون‌آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش روشن می‌نماید.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران، محققان نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر خود در پاسخگویی به نیازهای موجود، منابعی پُر بار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت "محمد صابری، بهمن محمدی، سید مرتضی پورنقی، پژوهشگران مرکز تحقیقات و فناوری اطلاعات و ارتباطات صدر" و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

کارشناسی و نظارت بر محتوا: زهره قزلباش

در خاتمه ضمن سپاسگزاری از شما دانش‌پژوه گرامی درخواست می‌مائیم مراجعه به آدرس dibagaran.mft.info (ارتباط با مشتری) فرم نظرسنجی را برای کتابی که در دست دارید تکمیل و ارسال نموده، انتشارات دیباگران تهران را که جلب رضایت و وفاداری مشتریان را هدف خود می‌داند، یاری فرمایید.

امیدواریم همواره بهتر از گذشته خدمات و محصولات خود را تقدیم حضورتان نماییم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
Publishing@mftmail.com

پیشگفتار

حوزه فناوری اطلاعات و ارتباطات نقش مهمی در زندگی ما دارد مکالمات روزمره ما، پیام‌هایی که به صورت نوشتاری یا تصویری برای یکدیگر می‌فرستیم و اطلاعاتی که از شبکه اینترنت دریافت می‌داریم مثال‌هایی از کاربری روزانه فناوری اطلاعات و ارتباطات در زندگی ما هستند. دنیای امروز و آینده ما، دنیای اطلاعات است. کنترل جریان اطلاعات و تولید و مصرف اطلاعات نقشی مهم در توانایی، اقتدار و امنیت کشورها و ملت‌ها دارد. شبکه‌های مخابراتی، زیر ساخت و بستر تبادل اطلاعات را تشکیل می‌دهند. این شبکه‌ها انواع متعدد و در بسترهای مختلفی از قبیل فیبر نوری، زیرساخت‌های سیمی و شبکه‌های موبایل، راه‌های ارتباطی متعددی را شکل می‌دهند که در آن‌ها جریان اطلاعات روزمره کاربران برقرار می‌شود.

شبکه‌های موبایل یکی از مهمترین زیرساخت‌های ارتباطی هستند. رشد روز افزون شبکه‌های موبایل، ارزان شدن گوشی‌های تلفن همراه و تنوع کارهای خدمات ارائه شده موجب شده که بخش بزرگی از کاربران، موبایل را به صورت روزانه استفاده نمایند. سال‌های اول و دوم موبایل متمرکز بر ارائه خدمات صوتی بودند و ابزاری مناسب و کارآمد برای برقراری تماس در حال حرکت و بیرون از خانه و محل کار را فراهم می‌نمودند. در نسل سوم موبایل، ارائه خدمات دیتا و ارتباط با اینترنت به عنوان یک نیاز مهم کاربران مورد توجه قرار گرفت. از همین رو در طراحی این نسل از شبکه‌های موبایل، ارائه سرعت بالای دیتا یک اولویت تلقی شد و کاربران شبکه موبایل نسل سوم نرخ تبادل داده‌ای بسته‌ای تا محدوده بیش از ده مگابیت در ثانیه را تجربه نمودند. با افزایش تنوع کاربری‌های شبکه‌های دیتا، ارائه خدمات متنوعی که نیاز به پهنای باند بیشتر داشت، نسل چهارم موبایل طراحی و پیاده‌سازی گردید. در طراحی شبکه‌های نسل چهارم موبایل که به شبکه‌های LTE مشهور هستند، ارائه خدمات دیتا با کیفیت و سرعت بالا از ابتدا به عنوان مهمترین هدف برگزیده شد و نرخ‌های تبادل داده‌های در محدوده صد مگابیت در ثانیه مد نظر قرار گرفت. بعدها با توسعه فناوری، این نرخ افزایش یافت و در استانداردهای LTE-A نرخ تبادل داده‌های 1 Gb/s در جهت فرسو و 500 Mb/s در جهت فراسو ارائه گردیدند.

امنیت تبادل داده‌ها در شبکه‌های ارتباطی یکی از نیازهای مهم و حیاتی کاربران است. کاربران مایل نیستند که اطلاعاتی که مبادله می‌کنند در دسترس دیگر کاربران قرار گیرد. خدماتی جدید مانند بانکداری الکترونیکی یا خریدهای الکترونیکی در فضای مجازی، نیاز مبرمی به امنیت و صحت تبادل داده‌ها دارند تا بتوانند اعتماد کاربران را جذب نمایند. از همین رو، درک کیفیت عملکرد شبکه‌های

موبایل نسل جدید و داشتن نگرش خوبی در خصوص مفاهیم عملیاتی به کار رفته در تامین امنیت این شبکه‌ها و تهدیدات امنیتی قابل تصور برای این شبکه‌ها امری مفید و مطلوب است. کتاب حاضر در جهت تبیین جنبه‌های شایان توجه در خصوص امنیت شبکه‌های موبایل نسل چهارم LTE نگاشته شده است. در این کتاب، در فصل‌های اول تا چهارم مروری بر روند توسعه فناوری‌های موبایل در نسل‌های مختلف، معماری این شبکه‌ها و مکانیزم‌های برقراری ارتباط ارائه شده است. در فصل پنجم، ویژگی‌ها و الزامات امنیتی شبکه LTE مورد بررسی قرار گرفته است و فصل ششم معماری امنیتی شبکه LTE را توصیف می‌کند. فصل هفتم نیز به بررسی مخاطرات و تهدیدهای محتمل در این شبکه‌ها می‌پردازد و احتمال خطر، تاثیر و میزان اهمیت خطر را تحلیل می‌نماید. بررسی و فهم مباحث امنیتی در شبکه‌ها بیش نیاز از تمام اقدامات امنیتی است که در جهت رفع و یا کاهش تهدیدات باید انجام پذیرد. از همین رو، نگرش این کتاب قدم مثبتی در جهت ایجاد درک و شناخت در این حوزه و اتخاذ اقدامات مناسب در جهت افزایش ایمنی و قابلیت اعتماد این شبکه‌ها خواهد بود.

محمدرضا پاک‌روان

دانشیار دانشکده برق

دانشگاه صنعتی شریف

تابستان ۱۳۹۵

تورده پیش گرفتگی و اشتیاق جمالت

ز پرده‌ها به در افتاد رازهای نهانی

(سعدی)

مقدمه

علی‌رغم گسترش روزافزون مطالعات و پژوهش‌های جهانی در سیستم‌های LTE/SEA که توسط 3GPP به عنوان مسیری نزدیک برای رسیدن به استانداردهای مخابرات نسل چهارم تعیین شد، این موضوع در ایران آن چنان که باید مورد توجه قرار نگرفت. با توسعه‌ی چشم‌گیر نسل‌های مخابرات سلولی در سال‌های اخیر و همچنین نیازمندی عصر کنونی به آخرین نوع تکنولوژی ارتباطی، اهمیت بررسی سیستم LTE بیش از پیش ضروری به نظر می‌آید. LTE یا LTE-A یکی از پیشرفته‌ترین سیستم‌های مخابرات سلولی است که در بسیاری از کشورها راه‌اندازی شده است. هدف نسل جدید شبکه‌های تلفن همراه با یکی کردن شبکه‌های موجود و ایجاد یک شبکه‌ی مابین جهانی که مبتنی بر IP باشد امکاناتی مثل سرعت بالا، ظرفیت بالا، پشتیبانی از صوت و داده که ممکن بود با سیستم‌های IP هستند را فراهم می‌کند. در پاییز سال ۲۰۰۴، TSC RAN برای اولین بار کارگاهی برای معرفی یک استاندارد جدید به نام LTE برپا کرد. بعد از این کارگاه، شش ماه زمان صرف تشریح و توصیف اهداف، نیازها و نیازهای مقدماتی جهت ایجاد بستر تحقیقاتی آن شد. در واقع نام کامل سیستم، SAE/LTE می‌باشد. SAE امکان دسترسی ترکیبی را با استفاده از تکنولوژی پهنای باند بالای LTE و تکنولوژی سنتی‌تر GSM و 3G فراهم می‌کند. اصطلاح فنی برای سیستم SAE/LTE، EPS است. از مهمترین اهداف در نظر گرفته شده برای این سیستم می‌توان به نرخ داده بالا در مرز سلول‌ها و اهمیت کمینه کردن تأخیر اشاره کرد. در سال ۲۰۰۵ تصمیم گرفته شد که از OFDM در اتصال پایین سو و SC-FDMA در اتصال بالاسو استفاده شود. به طور کلی در هر نسخه از انتشارات 3GPP شاهد تکامل مخابرات همراه در قالب LTE هستیم. با مقایسه LTE نسبت به سایر شبکه‌های انتقال داده نظیر WiMAX می‌توانیم علاوه بر شاخصه‌های برتری مانند پهنای باند و نرخ داده بالاتر LTE توجهمان را به مدولاسیون جدید -SC-FDMA و فناوری MIMO به کار رفته در سیستم LTE منعطف کنیم که نظیر آن در سایر سیستم‌های انتقال داده مشاهده نمی‌شود.

به دلیل ویژگی‌های منحصر به فرد شبکه‌های LTE، چالش‌های جدیدی نیز در مکانیسم طراحی آن به وجود آمده و همین موضوع منجر به آسیب‌پذیری‌های امنیتی متفاوتی در این شبکه شده است.

شبکه‌های مخابراتی به‌طور فزاینده‌ای در معرض تهدیدات شناخته شده‌ی مختلفی قرار دارند. شکی نیست که حملات جدید و ناشناخته‌ای نیز انجام خواهد گرفت که عناصر و خدمات شبکه‌های ارتباطی را هدف قرار خواهند داد. این مساله در مورد شبکه‌های جدید با استانداردهای جدید که در محک تجربه قرار نگرفته‌اند بسیار حایز اهمیت می‌شود. افزایش سرعت و همچنین وسعت دادن شبکه‌های مخابراتی نسل جدید و ایجاد یک شبکه‌ی مرکزی جهانی، مساله تهدیدات این نوع از شبکه‌ها را برای کشورها برجسته می‌کند؛ به طره‌ی که می‌توان این مساله را در ارتباط مستقیم با امنیت ملی دانست. امکان استفاده از زیرساخت‌های این شبکه برای کاربردهای امنیت عمومی، نظامی و خصوصی، اهمیت شناخت امنیت این شبکه و معماری‌های آن را بیشتر می‌کند. اگر چه روشن است که شبکه‌های آتی IP از جمله LTE و LTE-A تهدیدات نوعی مواجه خواهند بود، اما روشن نیست که کدام تهدیدات از همه‌ی موارد چشمگیرتر بوده و کدام عناصر شبکه بیشتر در معرض خطر قرار دارند. از آنجایی که چنین دانش و اطلاعاتی تا حد زیادی به آگاهی‌یابی امنیتی در آینده برای شبکه‌های تلفن همراه مرتبط می‌باشد، چند پروژه تحقیقاتی در سطح جهن و جامعه ارزیابی و بررسی این تهدیدات را به عهده گرفته‌اند.

این کتاب با هدف تشریح زیرساخت شبکه LTE، نیازمندی‌ها و معماری امنیتی آن، ارائه و تحلیل تهدیدات مرتبط با شبکه LTE آماده شده است. با این حال تنها راه تهدیدات ممکن است خواننده را به اندازه کافی قادر به تصمیم‌گیری آگاهانه بر مبنای اطلاعات موجود نکند. بنابراین تصمیم گرفته شد برآوردی از ریسک‌های مرتبط با تهدیدها هم مورد بحث قرار گیرد. این کتاب می‌تواند منجر به درک بهتری از تهدیدهای منحصر به فرد در شبکه‌های مخابراتی نسل جدید گردد.

در فصل اول کتاب مروری بر تاریخچه و معماری مخابرات سلولار تا قبل از مخابرات نسل چهارم صورت می‌گیرد. در فصل دوم، مخابرات نسل چهارم و سیر پیشرفت آن بررسی می‌شود. تشریح معماری شبکه LTE، که از فصول پایدای کتاب است، در فصل سوم تشریح می‌گردد. فصل چهارم به توضیح فرایند تماس و مکالمه در زیر فصل‌های: حالت‌های مختلف تماس، نمایش جریان تماس، فرآید پیوست اولیه و روش‌های اختصاص‌دهی آدرس IP می‌پردازد. در فصل پنجم ویژگی‌ها و نیازمندی‌های امنیتی شبکه بیان می‌شود. در فصل ششم معماری امنیتی شبکه با تشریح فرایند احراز اصالت و توافق کلید، فرایند مدیریت و توزیع کلید، مکانیزم امنیت صوت، امنیت داخلی شبکه و در نهایت تصمیمات طراحی برای

امنیت EPS مورد بررسی قرار می‌گیرد. در فصل آخر انواع تهدیدات امنیتی در بخش‌های مختلف شبکه مورد بررسی قرار می‌گیرد و با تقسیم‌بندی تهدیدات در بخش‌های مختلف شبکه به ارزیابی خطر آن‌ها به صورت دقیق پرداخته می‌شود.

تلاش زیادی صورت گرفته است تا مطالب بیان شده در یک سطح مناسب و دور از پیچیدگی‌های نئوری جهت آشنایی با معماری امنیتی و تهدیدات شبکه LTE تنظیم گردد. اگرچه خواستگاه نهایی مؤلفین بیان تخصصی و جزئی مطالب در این حوزه است اما با توجه به عدم وجود کتابی مناسب در کلیات این موضوع، تصمیم به ارائه کتاب در این قالب و فصل بندی گردید. امید است در آینده نزدیک امکان ارائه این مطالب نیز محقق گردد.

در پایان سزاوار است از زحمات دکتر امیر مسعود امینیان مدرس، مهندس حجت الله جهانی و مهندس امین اسفندیار که در سوانح رسیدن این کتاب از هیچ لطفی دریغ ننمودند، سپاس گزار باشیم. امید است تألیف این کتاب گامی بسازد که یک در راستای پیشبرد اهداف علمی انقلاب اسلامی ایران به حساب آید و مورد رضایت حضرت ولی عهده (ع) و مقام عظمای ولایت حضرت امام خامنه‌ای (حفظه الله) قرار گیرد.

مؤلفین

تابستان ۱۳۹۵