به نام خدا

مؤسسه فرهنگی هنری
دیباگران تهران

امنیت شبکه های LTE

(شبکه های موبایل نسل جدید)

تألیف و تدوین:

مرکز تحقیقات فناوری اطلاعات و ارتباطات صدر

(محمد صابری، بهمن مددی، سید مرتضی پورعلی)

بهار ۱۳۹۵

سرشناسه: صابری، محمد، ۱۳۶۶

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

مشخصات نشر: تهران- دیباگران تهران ،۱۳۹۵

مشخصات ظاهری: ۲۰۹ ص.

شابک: ۹۷۸-۶۰۰-۱۲۴-۴۷۴-۲

وضعیت فهرستنویسی: فیپا

موضوع: تکامل بلند مدت (مخابرات)

موضوع: Long -term evolution(telecommunications)

شناسه افزوده: مددی بهمن،۱۳۶۴

شناسه افزوده: پورنقی سید مرتضی،۱۳۶۶

شناسه افزوده: مرکز تحقیقات و فناوری اطلاعات و ارتباطات صدر

رده بندی کنگره: ۱۳۹۵ ۸ الف ۲ ص/ TK ۵۱۰۳/۴۸۳۲۵

رده بندی دیویی: ۶۲۱/۳۸۴۵۶

شماره کتابشناسی ملی: ۴۳۷۱۸۵۸

امنیت شبکه های LTE

شبکه های سلولی نسل جدید

مؤلفان: محمد صابری
بهمن مددی
سید مرتضی پورنقی

ناشر: مؤسسه فرهنگی هنری دیباگران تهران

حروفچینی و صفحه‌آرایی: دیباگران تهران

طرح روی جلد: مجتبی حیدری

چاپ: دانشجو

نوبت چاپ: اول

تاریخ نشر: ۱۳۹۵

تیراژ: ۳۰۰ جلد

قیمت: ۴۳۰۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۱۲۴-۴۷۴-۲
ISBN: 978-600-124-474-2

نشانی واحد فروش: تهران، میدان انقلاب، خ کارگر جنوبی، روبروی پاساژ مهران، پلاک ۱۲۵۱
تلفن: ۶۶۴۱۰۰۴۶-۲۲۰۸۵۱۱۱ کد پستی: ۱۳۱۴۹۸۳۱۸۵

پست الکترونیکی: bookmarket@mftmail.com

فروش اینترنتی:
www.mftshop.com
www.mftbook.ir

نشانی تلگرام: @mftbook

نشانی اینستاگرام: Dibagaran_publishing

فهرست

مقدمه ناشر

خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب هایی 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 سطح 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.

گستردگی علوم و توسعه روزافزون آن، 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 و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر خود، رفع کمبودها و نیازهای موجود، منابعی پُربار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت **"محمد صابری،بهمن ماهر،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 می‌نماید جهت 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 می فرستیم 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 در ابعاد 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 زیر ساخت‌های ارتباطی هستند. رشد روز افزون شبکه‌های موبایل، ارزان شدن گوشی‌های تلفن همراه و تنوع کاربری‌ها و خدمات ارائه شده موجب شده که بخش بزرگی از کاربران، موبایل را به صورت روزانه استفاده نمایند. نسل‌های 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 سیستم‌های 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 و ارائه خدمات متنوعی که نیاز به پهنای باند بیشتر داشت، نسل چهارم موبایل طراحی و پیاده سازی 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 داده های 1Gb/s در جهت فروسو 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 می‌نماید. 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 پیش نیاز انجام اقداماتی است که در جهت رفع و یا کاهش تهدیدات باید انجام پذیرد. از همین رو، نگارش این کتاب قدمی مثبت در جهت ایجاد درک و شناخت در این حوزه و اتخاذ اقدامات مناسب در جهت افزایش ایمنی و امنیت استفاده از این شبکه‌ها خواهد بود.

محمدرضا پاکروان

دانشیار دانشکده برق

دانشگاه صنعتی شریف

تابستان ۱۳۹۵

تو برده پیش گرفتی و ز انشیاق جمالت

ز پرده‌ها به در افتاد رازهای نهانی

(سعدی)

مقدمه

علی‌رغم گسترش رو افزون 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 و 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 مرزی جهانی که مبتنی بر IP باشد امکاناتی مثل سرعت بالا، ظرفیت بالا، پشتیبانی از صوت و داده که همگی بر مبنای IP هستند را فراهم می‌کند. در پاییز سال ۲۰۰۴، TSC RAN برای اولین بار کارگاهی برای معرفی یک استاندارد جدید به نام LTE بر پا کرد. بعد از این کارگاه، شش ماه زمان صرف تشریح و توصیف اهداف کار 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 سنتی نسل 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 کردنناًخیراشاره 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 LTEهستیم. 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؛ به‌طوری 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 نحوه‌ی ارزیابی‌های آن را بیشتر می‌کند. اگر چه روشن است که شبکه‌های آتی IP از جمله LTE و LTE-A با 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 ارزیابی‌های امنیتی در آینده برای شبکه‌های تلفن همراه مرتبط می‌باشد، چند پروژه تحقیقاتی در سطح جهان و اروپا ارزیابی و بررسی این تهدیدات را به عهده گرفته اند.

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 زمانی تهدیدات ممکن است خواننده را به اندازه کافی قادر به تصمیم‌گیری آگاهانه بر مبنای اطلاعات موجود کند. بر این تصمیم گرفته شد برآوردی از ریسک‌های مرتبط با تهدیدها هم مورد بحث قرار گیرد. این مساله 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 پایه‌ای کتاب است، در فصل سوم تشریح می‌گردد. فصل چهارم به توضیح فرایند تماس و مکالمه در زیر فصل‌های: حالت‌های مختلف تماس، نمایش جریان تماس، فرآیند 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 تئوری 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 سرانجام رسیدن این کتاب از هیچ لطفی دریغ ننمودند، سپاس گزار باشیم. امید است تألیف این کتاب گامی ناچیز باشد که بتواند در راستای پیشبرد اهداف علمی انقلاب اسلامی ایران به حساب آید و مورد رضایت حضرت ولی عصر (عج) و مقام عظمای ولایت حضرت امام خامنه‌ای (حفظه الله) قرار گیرد.

مؤلفین

تابستان ۱۳۹۵