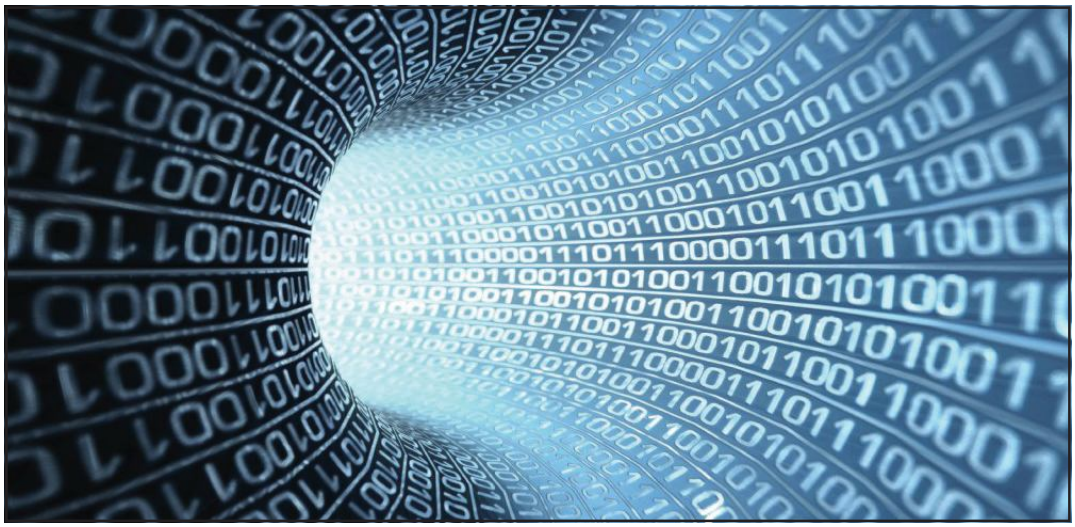
تکیه بر روش‌های امنیت مبتنی بر لایه فیزیکی،

راهبردی برای حفظ امنیت در عصر پساکوانتومی



علی رحمان‌پور | rahmanpour@teyf.ir
rahmanpour@ieee.org

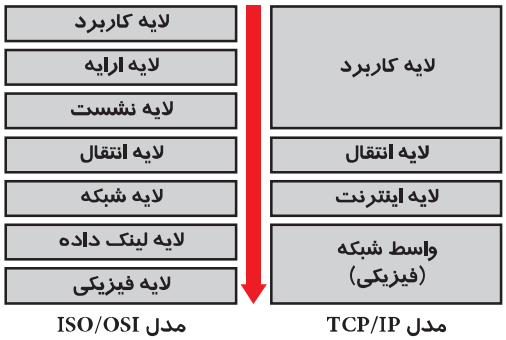
مقدمه

در سال‌های اخیر، باتوجه‌به رشد روزافزون قدرت محاسباتی رایانه‌ها و ابررایانه‌ها و زمزمه ورود پردازشگرهای کوانتومی، کارایی الگوریتم‌های رایج رمزنگاری (مبتنی بر پیچیدگی محاسباتی)، به‌طور گسترده‌ای با ابهام روبرو شده است. از طرفی چالش‌های موجود در پیاده‌سازی مطمئن الگوریتم‌های رمزنگاری مانند مسایل مربوط به مدیریت و تبادل کلید نیز همچون گذشته به‌صورت جدی مطرح می‌باشند. ازاین‌رو چند سالی است توسعه راهکارهای امنیتی مبتنی بر لایه فیزیکی، برای مقابله با چالش‌های بیان شده موردتوجه گسترده‌ای قرار گرفته است؛ هم‌اکنون این شاخه در حال تبدیل‌شدن به راهبردی قدرتمند است و رفته‌رفته درکنار روش‌های امنیت سنتی جای می‌گیرد.

تا پیش از سال ۱۹۷۵، غالب روش‌های حفاظت اطلاعات بر اساس نظریه سیستم‌های ارتباطی محرمانه شانون[1] و مبتنی بر رمزنگاری در لایه‌های بالا بود. بر این اساس، گره فرستنده بدون درنظر گرفتن تفاوت کانال‌ها و با فرض یکسان‌بودن شرایط برای هر دو گیرنده قانونی و شنودگر، تلاش می‌کرد تا با بکارگیری روش‌های مبتنی بر رمزنگاری، دسترسی به اطلاعات اصلی را برای مخاطب غیرقانونی ناممکن نماید.

در سال ۱۹۷۵ مقاله معروف واینر[2] پیرامون کانال شنود[3] منتشر شد؛ واینر در این مقاله که به نوعی نقطه آغاز امنیت لایه فیزیکی به حساب می‌آید، با واردکردن نویز به مدل ارتباطی، بحث امنیت ارتباط را از زاویه‌ای جدید مورد بررسی قرار داده و ایده امکان انتقال امن اطلاعات با بهره‌گیری از راهکارهای مبتنی بر لایه فیزیکی را ارایه کرد. این راهبرد همچنین منجر به پدیدآمدن معیاری جدید برای سنجش میزان امنیت کانال با عنوان "ظرفیت محرمانگی"[4] شد.

اگرچه اهمیت ایده ارایه شده پیرامون امنیت لایه فیزیکی از همان ابتدا مشخص بود و در سال‌های پس از آن، مقالات متعددی برای تکمیل این مفهوم منتشر شد، اما تا چند دهه بعد، این حوزه همچنان به‌عنوان یک روش فرعی و زیر سایه روش‌های متداول رمزنگاری باقی ماند. تا سال‌های اخیر که باتوجه‌به آنچه در مقدمه گفته شد، این راهبرد مجددا موردتوجه گسترده محافل تحقیقاتی قرار گرفت و امروزه زمزمه بکارگیری آن در نسل پنجم ارتباطات سیار به‌گوش می‌رسد.



شکل ۱- نمایی از جایگاه امنیت لایه فیزیکی از منظر لایه‌بندی شبکه

معیارهای متفاوت در سنجش امنیت

معیارهای سنجش امنیت همواره یکی از چالش‌برانگیزترین مسایل در حوزه انتقال امن اطلاعات است. امنیت لایه فیزیکی در این حوزه که یکی از بنیادین‌ترین مسایل امنیتی است نیز با معرفی ظرفیت محرمانگی، قواعد بازی را تغییر داد. ظرفیت محرمانگی به بیانی ساده بیانگر "حداکثر ظرفیت موجود برای انتقال اطلاعات به گیرنده موردنظر، بدون امکان شنود آن از سوی گره غیرقانونی" است. امروزه ظرفیت محرمانگی به‌عنوان یکی از معیارهای اصلی سنجش امنیت و درکنار پیچیدگی محاسباتی مطرح شده است؛ به‌گونه‌ای که ظرفیت محرمانگی برای سنجش امنیت در لایه فیزیکی بکارگرفته می‌شود و پیچیدگی محاسباتی بیشتر برای سنجش امنیت مبتنی بر رمزنگاری بکار می‌رود.

مقایسه امنیت مبتنی بر لایه‌های بالا و لایه فیزیکی

شیوه‌های حفاظت از امنیت یک لینک ارتباطی را می‌توان از دیدگاه‌های متفاوتی بررسی کرد. همان‌طور که اشاره شد، یکی از این تقسیم‌بندی‌ها بر اساس لایه‌ای از شبکه است که حفاظت اطلاعات در آن تامین می‌شود:

حفظ محرمانگی در لایه فیزیکی: در روش‌های بهبود محرمانگی مبتنی بر لایه فیزیکی، اصل بر این است تا شنودگر غیرمجاز نسبت به گیرنده قانونی به میزان اطلاعات کمتری دسترسی یابد. در این روش درصورتی امنیت کامل بدست خواهد آمد که شنودگر به هیچ سطح از اطلاعات انتقالی در کانال ارتباطی اصلی دسترسی نداشته باشد؛ یا به‌صورت کاربردی شاید بتوان این‌گونه تعریف نمود که با میزان اطلاعاتی که در دسترس وی قرا می‌گیرد عملا قادر به فهم و استخراج پیام نباشد.

حفظ محرمانگی در لایه‌های بالا: در این روش‌ها، فرض می‌شود شنودگر دارای توان دست‌یابی به همه آنچه گیرنده قانونی در لایه فیزیکی بدان دسترسی دارد را داراست، ازاین‌رو سعی می‌شود با به‌کارگیری شیوه‌هایی چون رمزنگاری در لایه‌های بالا (عموما لایه کاربرد در مدل TCP/IP) امکان استخراج اطلاعات اصلی توسط شنودگر ناممکن گردد. درحقیقت در این روش، نوعی تونل محرمانه در دل لایه فیزیکی زده شده و اطلاعات حقیقی از داخل آن منتقل می‌شود.

حال سؤالی که ضروری است بدان پاسخ داده شود این است که با وجود روش‌های سنتی حفظ محرمانگی مبتنی بر رمزنگاری لایه‌های بالا، چه ضرورتی برای بهره‌گیری از روش های امنیتی مبتنی بر لایه فیزیکی وجود دارد؟

اگرچه در مقدمه نیز به‌طور گذرا به این مسأله اشاره شد، پاسخ این سؤال را می‌توان به‌صورت دقیق‌تر در موارد ذیل بیان کرد:

- در روش‌های مبتنی بر لایه فیزیکی، تلاش می‌شود تا شنودگر به هیچ سطحی از اطلاعات دسترسی نیابد، چه اینکه حفظ محرمانگی در پایین‌ترین لایه رخ می‌دهد. بدیهی است این روش نسبت به ایجاد یک تونل ارتباطی امن در داخل لایه فیزیکی دارای امنیت بیشتری است. این مسأله به‌ویژه در کاربردهای حساس بسیار مهم است.

- روش‌های مبتنی بر رمزنگاری در لایه‌های بالا، غالبا درجه‌ای از امنیت را باتوجه‌به پیچیدگی محاسباتی لازم برای شکستن رمز فراهم می‌کنند، ازاین‌رو امکان شکستن رمز با روش‌هایی چون موازی‌کردن پردازنده‌ها و یا استفاده از رایانه های قوی‌تر در دراز مدت، میسر است. به این مسأله نیز باید توجه شود که طرفین اصلی ارتباط از توان محاسباتی شنودگر اطلاعات قطعی ندارند، هرچند این اطلاعات در حال‌حاضر نزدیک به واقعیت است، اما احتمال ورود رایانه‌های بسیار پرسرعت کوانتومی را نیز باید درنظر گرفت که در آن صورت بحث پیچیدگی محاسباتی تقریبا ازمیان‌رفته و باید به‌دنبال روش‌های جایگزین برای حفظ امنیت قطعی ارتباطات (و نه صرفا بر حسب پیچیدگی محاسباتی) گشت.

- مسأله دیگر این است که در بحث پیرامون امنیت لایه فیزیکی، برخی روش‌های بالا بردن امنیت از طریق همکاری بین‌لایه‌ای موردنظر است. در این روش‌ها از ویژگی‌های چون محوشدگی[5] در کانال‌های بی‌سیم و تصادفی‌بودن آن، به‌منظور بهبود درجه امنیت روش‌های مبتنی بر رمزنگاری و به‌عنوان بخشی از معماری امنیت سنتی شبکه استفاده می‌شود. بدین‌ترتیب مسایلی چون تصادفی‌بودن کانال که چه‌بسا در حالت عادی به‌عنوان یک چالش در ارتباطات بی‌سیم مطرح باشند، به‌منظور بهبود امنیت نقشی سازنده ایفا می‌کنند.

- بسته به نوع شبکه، دلایل بیشتری را نیز می‌توان برشمرد، ازجمله استفاده از امنیت لایه فیزیکی به‌منظور حفاظت از محرمانگی موقعیت جغرافیایی فرستنده، مشکلات ناشی از مدیریت، تعویض و نابودی کلید در سیستم‌های مبتنی بر رمزنگاری سنتی و....

البته دو راهبرد کلی بیان شده (برقراری امنیت در لایه‌های بالا و لایه فیزیکی)، دارای تفاوت‌های کاربردی نیز می‌باشند که بسته به هدف، ممکن است یکی بر دیگری برتری یابد. ازجمله این تفاوت‌ها می‌توان به موارد ذیل اشاره نمود:

- هر چه امنیت در لایه‌ای بالاتر صورت پذیرد، تغییرات اعمالی در شبکه به‌گونه‌ای خواهند بود که کاربر آنها را بیشتر حس خواهد کرد و درمقابل، هر چه امنیت در لایه‌های پایین‌تر صورت گیرد، از دید کاربر ناپیداتر است.

- امنیت در لایه‌های بالا، توانایی تمرکز بیشتر به‌منظور انتخاب سطح امنیت متفاوت برای نوع کاربردهای گوناگون (و همچنین برای کاربران مختلف) را داراست، اما در لایه‌های پایین‌تر، امکان این انتخاب تقریبا از بین می‌رود، به‌خصوص در لایه فیزیکی که با سیگنال‌ها سروکار داریم و اطلاعی از محتوای آنها در دست نیست.

- روش‌های محرمانگی مبتنی بر لایه فیزیکی هنوز از لحاظ پژوهشی درحال‌توسعه می‌باشند. باتوجه‌به هزینه

پیاده‌سازی زیاد آنها، همچنان نیاز است تا بیشتر در نقشی مکمل و درکنار روش‌های سنتی حفظ امنیت اطلاعات بکارگرفته شوند.

امنیت لایه فیزیکی با امنیت فیزیکی سیستم متفاوت است

همان‌طور که اشاره شد، امنیت لایه فیزیکی مفهومی است که گرچه پایه‌هایش چهار دهه قبل گذاشته شد، اما اخیرا موردتوجه گسترده قرار گرفته؛ همین مسأله نیز موجب بروز سوءتفاهماتی در درک آن شده است. ازجمله اشتباهات متداولی که پیرامون امنیت لایه فیزیکی وجود دارد، یکسان‌دانستن آن با مباحثی چون امنیت فیزیکی سیستم و مقابله با تهدیداتی مانند حملات کانال جانبی[6] است. اگرچه در برخی موارد (همچون استفاده از مشخصه‌های سیگنال ارتباطی برای احراز اصالت و...) مرز میان راهکارهای امنیت لایه فیزیکی و امنیت فیزیکی بسیار نزدیک شده و بعضا محو می‌شود، اما این دو راهبرد اصولا با یکدیگر متفاوت می‌باشند. امنیت لایه فیزیکی باید از دیدگاه لایه‌بندی شبکه مورد بررسی قرار گیرد. با این زاویه نگاه، امنیت لایه فیزیکی برخلاف امنیت در لایه‌های بالا که با بیت‌ها و بسته‌های داده سروکار دارد و امنیت در حوزه تجهیزات که با سیستم فیزیکی مواجه است، بر روی سیگنال و توان ارسالی آن متمرکز است.

جمع‌بندی

درنهایت لازم است به این مسأله اشاره شود که نظر به پیچیدگی‌های عملی که پیش روی امنیت مبتنی بر لایه فیزیکی است، شاید هنوز نتوان (و یا حتی نیازی نباشد) که محرمانگی را به‌طور کامل به این لایه بسپاریم، به‌خصوص باتوجه‌به اینکه در بسیاری از کاربردهای عمومی نیاز به این سطح از امنیت وجود ندارد؛ به‌عنوان نمونه برای یک کاربر شبکه سیار عمومی، باتوجه‌به نوع خدمات مورداستفاده از یک‌سو و وجود تهدیدات متعدد در لایه‌های بالاتر از سوی دیگر، اعمال کامل امنیت در لایه فیزیکی، حداقل در شرایط کنونی، ضروری نیست. اما حتی در همین مورد نیز روش‌های مکمل مبتنی بر لایه فیزیکی بسیار مؤثر خواهد بود و پیش‌بینی می‌شود در آینده نزدیک مورداستفاده قرار گیرد. برای نمونه، در بسیاری از موارد برای انتقال کلیدهای اولیه به یک کانال امن نیاز است که یکی از کاربردهای مکمل امنیت لایه فیزیکی، فراهم‌کردن بستری برای انتقال و تعویض امن کلید است. همچنین روش‌های ارایه شده پیرامون احراز اصلات مبتنی بر لایه فیزیکی نیز از سایر راهکارهایی است که در کاربردهای عمومی قابل استفاده است. از سوی دیگر امروزه روش‌های پیچیده‌تر امنیتی در لایه فیزیکی همچون استفاده از نویز مصنوعی و شکل‌دهی پرتو برای انتقال امن اطلاعات، به‌منظور کاربردهای حساس‌تر نظامی و امنیتی نیز درحال‌توسعه می‌باشند که در اینجا مجالی برای پرداختن به آنها نیست.

برای کسب اطلاعات بیشتر پیرامون این حوزه می‌توانید به بخش مقدمه [1] مراجعه نمایید. ■

منبع:

[1] رحمان‌پور، علی، (۱۳۹۳)، "بهبود امنیت لایه فیزیکی در سیستم‌های مخابرات بی‌سیم چندآنتنی، مبتنی بر نویز مصنوعی گره مقصد"، پایان‌نامه کارشناسی ارشد، اساتید راهنما: دکتر وحید طباطباوکیلی و دکتر سید محمد رضوی‌زاده، دانشکده برق دانشگاه علم و صنعت ایران.

پی‌نوشت‌ها:

1- Shannon
2- Wyner
3- Wiretap Channel
4- Secrecy Capacity
5- Fading channel
6- Side-channel attack