مجله محاسبات نرم، جلد ۱۰، شماره ۲ (پاییز و زمستان ۱۴۰۰)، صفحه ۱۶ـ۳۱
https://doi.org/10.22052/scj.2022.242847.0

مجله محاسبات نرم
SOFT COMPUTING JOURNAL
تارنمای مجله: scj.kashanu.ac.ir

دانشگاه کاشان
University of Kashan

مروری بر امنیت شبکه‌های مخابراتی مورد استفاده در شبکه‌های توزیع برق✧

فاطمه سعیدنژاد[۱]، دانشجوی کارشناسی ارشد، مهدی مجیدی[۱*]، استادیار
[۱] دانشکده مهندسی برق و کامپیوتر، دانشگاه کاشان، کاشان، ایران.

اطلاعات مقاله

تاریخچه مقاله:
دریافت ۲۴ مهر ماه ۱۴۰۰
پذیرش ۰۸ اردیبهشت ماه ۱۴۰۱

کلمات کلیدی:
شبکه هوشمند
شبکه‌های مخابراتی
امنیت
حملات سایبری
یادگیری عمیق

چکیده

صنایع برق با مشکلاتی مانند کاهش سوخت‌های فسیلی، انتشار گازهای گلخانه‌ای و فقدان آنالیز خودکار شبکه برق مواجه است. برای مقابله با چالش‌های موجود، ایجاد زیرساخت جدید ضروری است. مفهوم شبکه‌های هوشمند با هدف به‌روزکردن شبکه‌های برق کنونی با ادغام زیرساخت‌های مخابراتی پیشرفته با شبکه برق موجود، شبکه‌های برق را قابل‌اطمینان‌تر، بهینه و دوستدار محیط زیست می‌سازند. تجمیع شبکه‌های برق و شبکه‌های مخابراتی درحالی‌که فواید فراوانی دارد، دارای معایبی در زمینه‌ی امنیت سیستم و حفاظت است. در این مقاله، بعد از آشنایی با زیرساخت‌های مخابراتی شبکه هوشمند، ویژگی‌ها و کاربردهای آنها به معرفی تهدیدهای موجود علیه امنیت شبکه‌های مخابراتی و بررسی اقدامات مناسب شامل پیش‌گیری، شناسایی و مقابله با خطرات امنیتی پرداخته شده است. در مرحله پیش‌گیری از خطرات امنیتی، راه‌کارهایی مانند رمزنگاری و زنجیره بلوکی با هدف حفظ دسترسی به اطلاعات شبکه برای افراد مجاز، مطالعه و بررسی شده است. در زمینه شناسایی حملات در شبکه هوشمند به دلیل نیاز به راه حلی هوشمند و سریع، یادگیری عمیق به عنوان یکی از ابزارهای هوشمند، پویا و قدرتمند به همراه کاربردهای آن در بهبود امنیت شبکه هوشمند بررسی شده است.

۱. مقدمه

مشکلات ذخیره‌سازی انرژی، محدودیت ظرفیت تولید برق، ارتباط یک‌طرفه، کاهش سوخت‌های فسیلی، انتشار گازهای گلخانه‌ای توسط صنایع برق سنتی و افزایش منابع انرژی تجدیدپذیر پراکنده نیاز به یک زیرساخت جدید برای شبکه برق را ایجاد کرده است [۱، ۲]. شبکه هوشمند (SG)[1] زیرساختی جدید است که در نظر دارد فناوری‌های مخابراتی با سرعت بالا و دوطرفه را به میلیون‌ها دستگاه شبکه قدرت مانند زیرساخت‌های اندازه‌گیری پیشرفته (AMI)[2] متصل سازد تا یک زیرساخت پویا، با قابلیت‌های جدید در مدیریت انرژی ایجاد نماید. همچنین در این شبکه مصرف‌کنندگان نیز می‌توانند در تولید برق شرکت کنند [۳، ۴].

در شبکه SG فرآیند تولید، انتقال، توزیع، حفاظت، نظارت، تجزیه و تحلیل و کنترل برق انجام می‌گیرد. SG کاربردهای متفاوت را با استفاده از فناوری‌های مختلف انجام می‌دهد [۵]؛ بنابراین برای تامین نیازهای شبکه‌ی گسترده برق، SG باید همیشه در دسترس، قابل‌اطمینان، ایمن و دارای کمترین تاخیر

✧ نوع مقاله: مروری
* نویسنده مسئول
پست(های) الکترونیک: f.saeidnejad@grad.kashanu.ac.ir (سعیدنژاد)
m.majidi@kashanu.ac.ir (مجیدی)

[1] Smart Grid

[2] Advanced Metering Infrastructure

نحوه ارجاع به مقاله: سعیدنژاد، فاطمه، مجیدی، مهدی، «مروری بر امنیت شبکه‌های مخابراتی مورد استفاده در شبکه‌های توزیع برق»، مجله محاسبات نرم، جلد ۱۰، شماره ۲، ص۱۶ـ۳۱، پاییز و زمستان ۱۴۰۰.

باشد [۲، ۳]. واضح است که برای داشتن چنین ساختاری نیاز به شبکه‌های مخابراتی مناسب و کارآمد داریم. برای انتخاب شبکه‌های مخابراتی مناسب برای SG باید ویژگی‌های کلی که این شبکه‌ها دارند را بشناسیم، با فناوری‌های مخابراتی موجود و ویژگی‌های آنها آشنا شویم تا بهترین ترکیب را از میان فناوری‌های موجود برای SG انتخاب و پیاده‌سازی کنیم.

ریزشبکه‌ها (MG)[1] به‌عنوان یک عنصر سازنده SG در نظر گرفته می‌شوند. در واقع، MGها گروه‌های غیرمتمرکز از مولدهای الکتریسیته (مانند توربین‌های بادی و سلول‌های خورشیدی) و بارها هستند. آنها مسیرهای ارتباطی قابل اعتمادی در درون خود و بین خوشه‌های خود فراهم می‌کند. در [۶] محدودیت‌های فناوری‌های با سیم و بی‌سیم برای عملکرد موفقیت‌آمیز MG بررسی و مقایسه شده است. همچنین در این مقاله مطالعاتی در مورد وابستگی متقابل بین سلسله مراتب کنترل MG و شبکه مخابراتی، الزامات معماری MG برای یک ارتباط مطمئن، سریع، ایمن و زمان واقعی بدون تلفات بسته‌های داده و تاثیر شبکه مخابراتی بر عملکرد MG به‌صورت تجربی انجام شده است.

همان‌طور که بیان شد SG از سیستم انتقال برق و شبکه‌های مخابراتی برای ایجاد یک زیرساخت دوسویه از برق و اطلاعات تشکیل‌شده است؛ تجمیع این دو ساختار در حالی که فواید فراوانی دارد، دارای معایبی در زمینه‌ی امنیت سیستم و حفاظت است. شبکه‌های مخابراتی به‌طور گسترده‌ای در معرض حملات مخرب هستند؛ بنابراین SG آسیب‌پذیرتر است، زیرا علاوه بر حمله مستقیم به زیرساخت شبکه برق، با حمله به شبکه مخابراتی آن، به‌طور غیرمستقیم عملکرد SG تخریب می‌شود [۷]. نکته‌ای که در شبکه‌های مخابراتی در SG مهم است قابلیت اطمینان شبکه است [۸]. برای مثال، یک حمله سایبری ممکن است موجب یک خاموشی بزرگ شود یا اینکه وضعیت سیستم را از حالت بهینه اقتصادی خارج کند. برای اینکه بتوانیم امنیت را در شبکه‌های مخابراتی SG برقرار کنیم، پس از آشنایی با مفهوم امنیت در این شبکه‌ها و شناسایی تهدیدهای موجود می‌توانیم راهکارهای مناسبی برای داشتن یک شبکه مناسب برای SG ارائه دهیم. راهکارهای موجود برای مبارزه با حملات با توجه به هدف حملات متفاوت خواهد بود. برای مثال رمزنگاری، برای حملاتی با هدف دسترسی به اطلاعات موجود در شبکه انجام می‌شود. تمام حملات انجام‌شده علیه شبکه‌های مخابراتی در SG باید به بهترین نحو شناسایی شوند؛ بنابراین برای شناسایی حملات در شبکه‌ی پویایی مثل SG به راه‌حل هوشمند و سریع نیاز داریم.

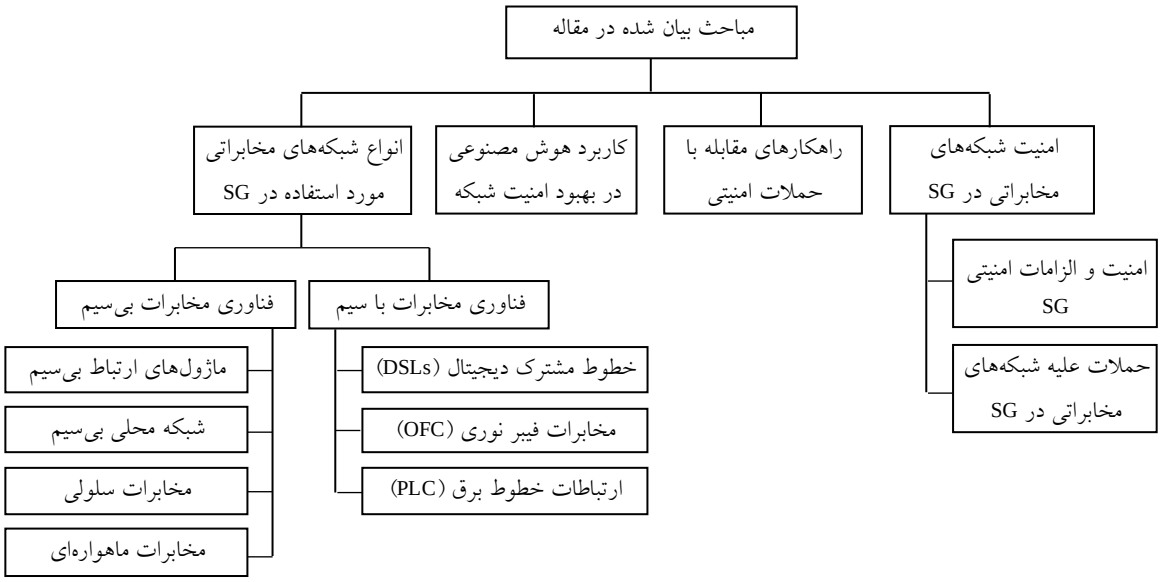
بسیاری از کشورهای جهان مانند ایالات‌متحده آمریکا، هلند، هند و ... تلاش خود را برای توسعه SG انجام داده‌اند. در ایران نیز طرح فراسامانه هوشمند اندازه‌گیری و مدیریت انرژی (فهام) به‌عنوان اولین قدم در زمینه هوشمندسازی سیستم قدرت در حال اجرا است؛ به نقل از پایگاه اطلاع‌رسانی وزارت نیرو در فاز اول این طرح استانداردها، مشخصات فنی و دانش فنی ساخت کنتورهای هوشمند داخلی تحقق یافت و مشترکان دیماندی برق که متقاضیان قدرت ۳۰ کیلووات یا بیشتر هستند به کنتورهای هوشمند مجهز شدند. در فاز دوم طرح فهام که وارد مرحله عملیاتی شده ۵ میلیون مشترک برق از جمله مشترکان کوچک صنعتی، تجاری، کشاورزی، مشترکان تک فاز تجاری، خانگی و سه فاز خانگی با اولویت مشترکان پرمصرف، طی دو سال به کنتورهای هوشمند مجهز خواهند شد که از این طریق رفتار مصرفی این دسته از مشترکان قابل مدیریت خواهد شد [۹].

در ادامه مقاله، در بخش دوم، بخشی از فناوری‌های مخابراتی مناسب برای SG را معرفی می‌کنیم و به بررسی ویژگی‌های این فناوری‌ها و معماری فناوری‌های مخابراتی پیاده‌سازی شده در فاز اول طرح فهام می‌پردازیم. در بخش سوم، الزامات و اهداف امنیتی شبکه‌های مخابراتی مورد استفاده در سیستم توزیع برق و تهدیدهای امنیتی علیه این شبکه‌ها را بررسی می‌کنیم و در بخش چهارم راهکارهای امنیتی در شبکه‌های مخابراتی مورد استفاده در شبکه‌های توزیع برق را بیان می‌کنیم؛ در این بخش، دو نوع رمزگذاری[2] را برای رسیدن به اهداف امنیتی شرح

[1] Microgrid

[2] Encryption

می‌دهیم. در بخش پنجم، یادگیری عمیق را به‌عنوان یک راه‌حل هوشمند و پویا برای شناسایی حملات علیه مخابرات SG معرفی می‌کنیم. در شکل (۱) ساختار کلی مقاله نشان داده شده است.



شکل (۱): ساختار مقاله

۲. انواع شبکه‌های مخابراتی مورد استفاده در SG

زیرساخت مخابرات SG ترکیبی از فناوری‌های مخابراتی متنوع برای دسترسی کارآمد و قابل اطمینان به اجزای مختلف SG در محیط‌های مختلف است. شبکه‌های مخابراتی SG باید مناطق جغرافیایی وسیعی را برای مراحل تولید، انتقال و توزیع برق پوشش‌دهی کنند. معماری مخابراتی SG شامل شبکه گسترده (WAN)[1]، شبکه محلی (LAN)[2] و شبکه خانگی (HAN)[3] است. شبکه HAN نزدیک‌ترین شبکه به کاربران است و جریان اطلاعات و ارتباطات بین لوازم خانگی را امکان‌پذیر می‌سازد. چند HAN به یک LAN متصل می‌شود. شبکه LAN اطلاعات را جمع‌آوری می‌کند و به WAN منتقل می‌کند که به شرکت‌های خدماتی انتقال داده شود [۱، ۸].

برای بهبود کارایی، قابلیت اطمینان و پایداری خدمات برق و همچنین به منظور بهینه‌سازی عملکرد نیروگاه‌های متصل‌شده، SG از ترکیب فناوری‌های مخابراتی برای تبادل داده‌ها و اطلاعات بلادرنگ[4] استفاده می‌کند. این فناوری‌ها در دو محیط با سیم و محیط بی‌سیم پیاده‌سازی می‌شوند [۸]. برای انتخاب فناوری مخابراتی مناسب با هدف رسیدن به عملکرد رضایت بخش ویژگی‌های مختلفی مانند میزان محافظت در برابر تداخل، مقیاس‌پذیری، هزینه ایجاد زیرساخت و نگهداری در نظر گرفته می‌شوند [۶، ۱۰]. در ادامه، انواع شبکه‌های مخابراتی با سیم و بی‌سیم مورد استفاده در شبکه برق معرفی می‌شوند.

۲،۱. فناوری مخابرات با سیم

فناوری‌های مخابراتی با سیم، ارتباطات را از طریق خطوط مشترک دیجیتال (DSLs)[5]، فیبر نوری و خطوط برق امکان‌پذیر می‌سازند. سیستم‌های مخابراتی سیمی مزایایی مانند پایداری و مقاومت در برابر تداخل دارند. همچنین سیستم‌های مخابراتی دیجیتال مدرن می‌توانند به میزان نرخ بیت 10 Gbps در تکنولوژی‌های DSL، 155 Mbps در کابل‌های کواکسیال و 160 Gbps بر روی کابل فیبر نوری دسترسی پیدا کنند [۱۰].

[1] Wide Area Network
[2] Local Area Network
[3] Home Area Network
[4] Real-time
[5] Digital Subscriber Lines

۲،۱،۱. خطوط مشترک دیجیتال (DSLs)

واژه DSL به‌طورمعمول به مجموعه‌ای از فناوری‌های مخابراتی اشاره دارد که داده‌های دیجیتال را روی خطوط تلفن منتقل می‌کنند. این مساله از هزینه اضافی استقرار زیرساخت مخابراتی برای SG جلوگیری می‌کند [۱۱]. با توجه به این که در انتقال صوت در زوج سیم، از باند فرکانسی پایین‌تر از چهار کیلوهرتز استفاده می‌گردد، در تکنیک DSL، برای انتقال داده در زوج سیم تلفن، از باند فرکانسی بالاتر استفاده می‌گردد.

در دسترس بودن گسترده، هزینه پایین و انتقال اطلاعات با پهنای باند بالا مهم‌ترین دلیل برای تبدیل فناوری DSL به اولین کاندیدای مخابراتی برای تامین‌کنندگان برق در اجرای مفهوم SG با کنتور هوشمند است؛ اما باید در نظر داشت که قابلیت اطمینان تکنولوژی DSL ممکن است برای برنامه‌های کاربردی در زمان‌های بحرانی قابل قبول نباشد [۲]. همچنین DSL برای فواصل کوتاه (حدود ۱/۲ کیلومتر برای VDSL[1]) مناسب است؛ زیرا با افزایش فاصله، بازده آن کاهش می‌یابد و برای مسافت‌های طولانی مناسب نیست [۱۱، ۱۲]. فناوری DSL برای اتصال لوازم‌خانگی هوشمند به SG و همچنین برای برنامه‌های کاربردی AMI و ... استفاده می‌شود [۱۰].

۲،۱،۲. مخابرات فیبر نوری (OFC[2])

سیستم‌های مخابراتی فیبر نوری، کیفیت سرویس (QoS)[3] خوبی را با پهنای باند بالا تامین می‌کنند. OFC یکی از زیرساخت‌های امیدوارکننده مخابراتی است که انتقال اطلاعات قابل اعتماد را ارائه می‌دهد [۱۳]. ظرفیت و پهنای باند این فناوری بسیار بیشتر از دیگر فناوری‌های بی‌سیم یا با سیم است و همچنین نرخ خطای کمی (BER)[4] را ارائه می‌دهد [۱۲، ۱۴]. OFC مؤثرترین روش برای ارتباط فواصل طولانی نسبت به سایر تکنولوژی‌ها است، زیرا برای تقویت داده‌ها به تعداد تکرارکننده‌های بسیار کمی نیاز دارد [۱۴]. هزینه اولیه این فناوری بالا است، اما قابلیت اشتراک OFC در بین کاربران مختلف می‌تواند این هزینه را در کوتاه مدت بازیابی کند [۱۳]. همچنین استقرار و نگهداری شبکه‌های فیبر نوری می‌تواند پرهزینه باشد [۱۱].

۲،۱،۳. ارتباطات خط برق (PLC[5])

در تکنیک PLC، از خطوط انتقال برق موجود برای انتقال سیگنال‌های داده از یک دستگاه به دیگری استفاده می‌شود [۲]. مهم‌ترین مزیت PLC کاهش هزینه ایجاد زیرساخت جدید است، چون خطوط برق موجود با چند ابزار جدید می‌تواند به‌عنوان کانالی برای انتقال سیگنال‌های ارتباطی بازسازی شود [۱۴، ۱۵]. در حال حاضر این فناوری دارای باند فرکانسی 0.3 KHz–250 MHz و نرخ انتقال داده 100 Bps–1.8 Gbps است. با کمک PLC ارتباطات در محیط‌های سخت که در آن هیچ فناوری نمی‌تواند در دسترس باشد نیز ممکن است [۱۶]، چراکه زیرساخت PLC می‌تواند مناطقی را پوشش دهد که در محدوده خدمات شرکت‌های خدماتی برق قرار دارند [۲].

استفاده از PLC برای انتقال داده همان طور که مزایایی دارد معایبی هم دارد؛ برای مثال نوع و طول کابل‌ها، ویژگی‌های ذاتی کابل‌های برق و غیره عملکرد کلی این فناوری را بسیار تحت تأثیر قرار می‌دهد [۱۵]. همچنین طبیعت باز و بدون حفاظ خطوط برق باعث ایجاد تشعشع الکترومغناطیسی می‌شود که می‌تواند از طریق گیرنده‌های رادیویی دریافت شود. این موضوع می‌تواند باعث دسترسی غیرمجاز به اطلاعات شود. با این حال، برای اجتناب از دسترسی غیرمجاز به اطلاعات خطوط انتقال، می‌توان از رمزنگاری[6] داده‌ها استفاده کرد [۱۴]. تعداد و نوع دستگاه‌های متصل به خطوط انتقال، فاصله اتصال بین فرستنده و گیرنده، به طور معکوس بر کیفیت سیگنال که از طریق شبکه، انتقال داده می‌شود تاثیر می‌گذارد. با این حال، راه‌حل‌های ترکیبی وجود دارند که در آن فناوری PLC با فناوری‌های دیگر یعنی GPRS[7] یا GSM[8] ترکیب می‌شود تا اتصال کاملی را که

[1] Very high speed Digital Subscriber Line
[2] Optical Fiber Communication
[3] Quality of Service
[4] Bit Error Rate
[5] Power Line Communication
[6] Cryptography
[7] General Packet Radio Service
[8] Global System for Mobile

توسط فناوری PLC امکان‌پذیر نیست فراهم کند [۲].

ماهیت PLC از نظر استانداردهای موجود در [۱۵] به طور جامع بررسی‌شده و تمام جنبه‌های سیستم‌های PLC، مانند فناوری‌های موجود، شبکه‌های مخابراتی، سطح ولتاژ و سایر جزئیات، با تمرکز ویژه بر جنبه‌های امنیتی سیستم‌های PLC از نظر تهدیدات امنیتی، آسیب‌پذیری‌ها، محدودیت‌ها و حملات و راه‌حل‌های امنیتی خاص در حوزه SG مطالعه شده است.

۲,۲. فناوری مخابرات بی‌سیم

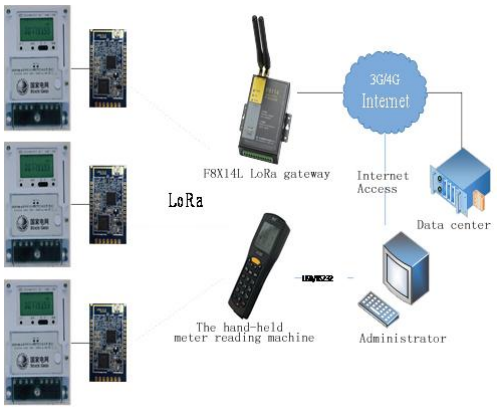
فناوری‌های مخابرات بی‌سیم هیچ محیط فیزیکی برای انتقال سیگنال ندارند. پیشرفت سریع در زمینه فناوری‌های مخابرات بی‌سیم، همراه با پیشرفت در فناوری پردازش سیگنال، راهی برای پیاده‌سازی گسترده آن در SG است [۱۰]. این فناوری مزایایی را مانند هزینه‌های پایین تجهیزات و نصب، استقرار سریع، دسترسی گسترده و انعطاف‌پذیری بیشتر ارائه می‌دهد [۱۷]. در ادامه چند فناوری بی‌سیم را بررسی می‌کنیم.

۲,۲,۱. ماژول‌های ارتباط بی‌سیم

فناوری ZigBee یک فناوری مخابرات بی‌سیم با استاندارد IEEE 802.15.4 است که مصرف توان، نرخ داده، پیچیدگی و هزینه راه‌اندازی به نسبت کمی دارد و در نتیجه، یک تکنولوژی ایده‌آل برای SG، نظارت انرژی، اتوماسیون خانه، قرائت خودکار کنتور و غیره است [۲]. باند فرکانسی این پروتکل، ۸۶۴ مگاهرتز برای اروپا، ۹۱۵ مگاهرتز برای ایالات متحده آمریکا و استرالیا و ۲/۴ گیگاهرتز در سراسر جهان است. از این رو، احتمال خراب شدن کل کانال ارتباطی به دلیل تداخل استانداردهایی مانند 802.11/b/g (WiFi) در مجاورت ZigBee افزایش می‌یابد؛ اما با استفاده از طرح‌های تشخیص و اجتناب از تداخل و پروتکل‌های مسیریابی، می‌توان عمر شبکه را افزایش داد و عملکردی قابل اعتماد و کارآمد برای شبکه‌های قدرت داشت [۱۳، ۱۸]. حافظه داخلی محدود و سرعت پردازش کم، از مشکلات عمده ZigBee هستند [۱۳].

فناوری Z-Wave یک فناوری بی‌سیم قابل اعتماد است که مصرف توان و هزینه پایینی دارد. این فناوری در اروپا در باند فرکانسی ۸۶۸ مگاهرتز و در آمریکا در باند ۹۰۸ مگاهرتز کار می‌کند. دامنه آن در محیط بسته ۳۰ متر است و تا ۱۰۰ متر در فضای باز افزایش می‌یابد و نرخ داده 9.6-40 Kbps را ارائه می‌دهد. Z-Wave با داشتن قابلیت‌های برد کوتاه و نرخ داده پایین، نامزد مناسبی برای کاربردهای SG در شبکه‌های خانگی است [۱۱].

محققان در [۱۹] استفاده از LoRa[1] را برای ارسال داده‌ها از کنتورهای هوشمند برق به متمرکزکننده داده پیشنهاد داده‌اند. LoRa که یک فناوری مخابرات بی‌سیم کم مصرف است برای انتقال داده در باند رادیویی ISM[2] برای برده‌های طولانی (حداکثر ۲۲ کیلومتر با توجه به شرایط محیطی) با نرخ بیت 27- 50 Kbps طراحی شده است. متمرکزکننده داده‌ها و کنتورهای هوشمند در مکان‌های مختلف و با فاصله از یکدیگر قرار دارند؛ بنابراین LoRa برای ارتباط میان این دو انتخاب مناسبی به نظر می‌رسد. شکل (۲) یک نمونه پیاده‌سازی ارتباط بی‌سیم با ماژول LoRa برای خواندن کنتور را نمایش می‌دهد.



شکل (۲): کاربرد ماژول LoRa برای خواندن کنتور از فواصل دور [۲۰]

۲,۲,۲. شبکه محلی بی‌سیم (WLAN[3])

شبکه WLAN یک اینترنت بی‌سیم با سرعت‌بالا است و ارتباطات ایمن، قابل اطمینان و با سرعت‌بالا را ارائه می‌دهد. نرخ داده آن از 2 Mbps تا 600 Mbps است و پوشش آن به

[1] Long Range
[2] Industrial, Scientific and Medical
[3] Wireless Local Area Network

بیش از ۱۰۰ متر می‌رسد. این شبکه بیشتر برای برنامه‌های کاربردی خانگی و محلی با نیازهای نرخ بیت به نسبت بالا مانند برنامه‌های نظارت ویدئویی مناسب است. با این حال، مصرف توان این شبکه برای بسیاری از دستگاه‌های SG بسیار بالا است [۱۱].

۲,۲,۳. مخابرات سلولی

در شبکه‌های سلولی، هر کاربر برای تبادل داده، از طریق تلفن همراه دارای سیم کارت خود به نزدیک‌ترین ایستگاه پایه همسایه‌اش متصل می‌شود. در مرکز هر سلول، یک ایستگاه پایه قرار دارد و تبادل داده ایستگاه‌های پایه مختلف، از طریق یک هسته مرکزی سوییچ برقرار می‌گردد. فناوری‌های 2G، 2.5G، 3G، 4G، LTE و 5G فناوری‌های مخابرات سلولی هستند که می‌توانند برای مخابرات SG انتخاب شوند [۱۰، ۱۷].

شبکه‌های سلولی از قبل وجود دارند بنابراین، صنایع همگانی نباید متحمل هزینه اضافی برای ایجاد زیرساخت مخابراتی مورد نیاز برای SG شوند. فناوری‌های سلولی از الگوریتم‌های امنیتی بیان شده در [۱۸] استفاده می‌کنند، بنابراین حریم خصوصی و امنیت این نوع شبکه‌ها به خطر نخواهد افتاد. نرخ داده بالا، پوشش گسترده، افزایش در قابلیت اطمینان و کیفیت، دلایل دیگری برای انتخاب این فناوری است [۱۰].

برخی کاربردهای حیاتی شبکه قدرت نیاز به دسترسی مستمر به ارتباطات دارند و از آنجا که سیستم سلولی به طور همزمان توسط بسیاری از کاربران استفاده می‌شود، گاهی نمی‌تواند پاسخگوی نیازهای برخی از برنامه‌ها که به خدمات بی‌وقفه نیاز دارند، باشد [۲، ۱۰].

۲,۲,۴. مخابرات ماهواره‌ای

پوشش جهانی توسط مخابرات ماهواره‌ای (SC)[1] بهترین راه‌حل برای کنترل دسترسی و نظارت از راه دور است. SC از فناوری‌های مؤثر برای ایستگاه‌های راه دور است که هیچ زیرساخت مخابراتی در آنجا وجود ندارد. سیستم موقعیت‌یاب جهانی (GPS)[2] برای به‌روزرسانی مکان دقیق و همزمان‌سازی استفاده می‌شود. در صورت قطعی لینک زمینی یا وضعیت اضطراری، SC می‌تواند به‌عنوان یک پشتیبان برای شبکه‌های مخابراتی مورد استفاده قرار گیرد [۱۳]. عیب اصلی این فناوری، تاخیر است. از آنجایی که سیگنال‌ها باید صدها کیلومتر را طی کنند، این تکنولوژی برای نظارت و کنترل بلادرنگ مناسب نیست [۱۰، ۱۳]. در جدول (۱) مقالات مطالعه شده در حوزه فناوری‌های مخابراتی به همراه کاربرد آنها در شبکه توزیع دسته‌بندی شده است.

جدول (۱): دسته‌بندی مقالات حوزه فناوری‌های شبکه‌های مخابراتی و کاربرد فناوری‌ها در شبکه توزیع

فناوری‌ها	کاربرد در شبکه توزیع	مراجع
فناوری مخابرات با سیم		
DSL	HAN, LAN	[۲]، [۸] و [۱۰-۱۳]
PLC	HAN, LAN, WAN	[۲] و [۸-۱۶]
OFC	LAN, WAN	[۸-۱۴]
فناوری مخابرات بی‌سیم		
ماژول ارتباط بی‌سیم	HAN, LAN	[۲]، [۸-۹]، [۱۱]، [۱۳-۱۴] و [۱۷-۱۸]
WLAN	HAN, LAN	[۸-۱۳] و [۱۷-۱۸]
مخابرات سلولی	HAN, LAN, WAN	[۲]، [۸-۱۴] و [۱۷-۱۸]
مخابرات ماهواره‌ای	HAN, LAN, WAN	[۸]، [۱۰] و [۱۲-۱۴]

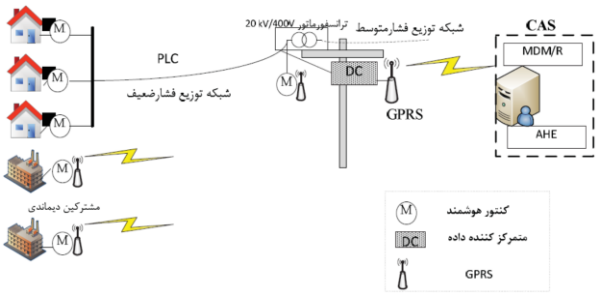
۲,۳. معماری فناوری‌های مخابراتی در طرح فهام

به‌طورکلی فناوری‌های سیمی پرهزینه هستند اما توانایی افزایش قابلیت ارتباطات، قابلیت اطمینان و امنیت را دارند. از سوی دیگر، فناوری‌های بی‌سیم می‌توانند هزینه‌های نصب را کاهش دهند، اما پهنای باند محدود و مشکلات امنیتی را فراهم می‌کنند [۲]. با ترکیب این فناوری‌ها با توجه به جغرافیای مناطق و ویژگی‌های فناوری‌های مختلف می‌توان یک شبکه مخابراتی همیشه در دسترس برای تمام مناطق تولید، انتقال و توزیع در شبکه‌های برق ایجاد کرد. شکل (۳) نمایی از ساختار فیزیکی

[1] Satellite Communication

[2] Global positioning system

یک شبکه توزیع است که بستر مخابراتی طرح فهام متشکل از فناوری‌های بی‌سیم و با سیم روی آن به شکل ساده نشان داده شده است. این معماری مربوط به فاز اول طرح فهام است [۲۱].



شکل (۳): معماری سیستم فهام [۲۱]

زیرساخت مخابراتی فاز اول طرح فهام شامل سیستم مرکزی، متمرکزکننده داده و کنتور است. کنتورها به سه نوع دیماندی، غیردیماندی و کنتورهای زیرترانسفورماتوری تقسیم شده‌اند. کنتورها میزان مصرف مشترکان را اندازه‌گیری و ثبت می‌کنند. اطلاعات ذخیره شده در کنتورهای دیماندی و کنتورهای زیرترانسفورماتور 400V/20kV به صورت مستقیم و در بستر GPRS به سیستم مرکزی ارسال می‌گردد. اطلاعات کنتورهای هوشمند غیردیماندی ابتدا به صورت محلی و در یک شبکه مش جمع‌آوری می‌گردد؛ بستر مخابراتی PLC باند باریک برای پیاده‌سازی لایه LAN انتخاب شده است. در صورت نیاز برخی از کنتورهای موجود در مسیر ارسال اطلاعات به متمرکزکننده داده نقش تکرارکننده را ایفا می‌نمایند. در نهایت نیز اطلاعات در بستر GPRS توسط مودم مخصوص موجود در متمرکزکننده داده برای سیستم مرکزی ارسال می‌گردد [۲۱].

۳. امنیت شبکه‌های مخابراتی در SG

امنیت SG برای حفاظت از شبکه‌های مخابراتی و شبکه برق ضروری است، چراکه این دو سیستم نیاز به تضمین دسترسی و حیات دائم در شرایط مختلف دارند [۲]. سیستم‌ها باید انعطاف‌پذیر باشند تا در صورت به خطر افتادن بخشی از امنیت آنها، بتوانند به شبکه خدمات ارائه دهند [۵]. مهم‌ترین چالش زیرساخت امنیت سایبری SG، یافتن و طراحی روش‌های بهینه برای ایمن‌سازی شبکه‌های مخابراتی بین میلیون‌ها دستگاه و واحد در سراسر تاسیسات برق، همراه با جلوگیری از حملات و دفاع از شبکه با روش‌های هوشمند، به منظور حفظ قابلیت‌های زیربنایی شبکه برق است [۲].

۳،۱. اهداف و الزامات امنیتی SG

اهداف و الزامات امنیتی SG در مراجع [۴، ۸، ۱۰] مشخص شده است، سه هدف مشترک به‌عنوان مهم‌ترین مسائل برای حصول اطمینان از عملکرد SG، عبارتند از:

- **دسترس‌پذیری:** اطمینان از دسترسی سریع و قابل اعتماد به اطلاعات، پهنای باند و تجهیزات برای صنایع همگانی و مصرف‌کنندگان است.
- **درستی یا یکپارچگی:** تضمین درستی، صحت و ثبات اطلاعات توزیع‌شده و محافظت از تغییر نادرست، درج، حذف یا بازپخش داده‌ها است. یکپارچگی داده‌ها با استفاده از روش‌های رمزنگاری می‌تواند تضمین شود.
- **محرمانگی:** داده‌ها به نحوی منتقل شوند که فقط برای افراد یا سیستم‌های مجاز افشا شوند و برای هر نهاد غیرمجازی قابل دسترسی نباشند. این امر به‌ویژه برای جلوگیری از افشای غیرمجاز اطلاعات خصوصی، ضروری است.

از دیدگاه قابلیت اطمینان سیستم، دو هدف اول حساس‌ترین و مهم‌ترین اهداف شبکه SG هستند. از آنجا که زیرساخت‌های سایبری، جریان برق را در زیرساخت‌های فیزیکی مدیریت می‌کنند، باید در هر زمانی در دسترس بودن برق را تضمین کنند. اطمینان از در دسترس بودن جریان برق و صحت اطلاعات شبکه در هرزمان، برای اکثر مشتریان مهم است. البته محرمانگی، در مخابرات شبکه خانگی و در ارتباط با مشتریان و در سیستم‌های AMI مهم و ضروری است [۸، ۱۰].

برای دستیابی به یک رویکرد جامع امنیت سایبری، علاوه بر اهداف امنیتی بیان شده، بعضی الزامات امنیتی نیز باید در SG تأمین گردند که این الزامات به اهداف امنیتی بیان شده مرتبط هستند. برخی از الزامات امنیتی SG که در [۵] با جزئیات شرح داده شده است شامل احراز هویت و شناسایی، تایید اصالت

کاربران، کنترل دسترسی سیستم، تنظیم میزان دسترسی کاربران به منابع، وجود حساب کاربری، حفظ حریم خصوصی، قابلیت اطمینان و حفظ ایمنی شبکه در شرایط غیرمنتظره هستند.

بر اساس فناوری‌های مورد استفاده، لایه‌ها، سیستم‌عامل‌ها و غیره، راه‌های بسیاری برای دسته‌بندی انواع مختلف از حملات مخرب علیه SG وجود دارد [۱۰]. طبقه‌بندی حملات سایبری با توجه به لایه‌های شبکه در مرجع [۵] شرح داده شده است. مقاله [۲۲] با تمرکز بر لایه فیزیکی، یک مدل فضای حالت برای بررسی جنبه‌های سایبری-فیزیکی در SG ارائه داده و سپس، مروری بر حملات و دفاع‌های متناظر انجام داده است. حملات را بر پایه عناصر هدفشان در شبکه، دسته‌بندی کرده است و روش‌های دفاعی جدید مانند دفاع هدف متحرک و علامت‌گذاری[1] را بررسی می‌نماید. یکی از حملات شبکه که بررسی می‌کند، استاکس‌نت است که در سال ۲۰۱۰ سیستم SCADA در تاسیسات هسته‌ای ایران را هدف قرار داد و فرکانس جریان الکتریکی سانتریفیوژها را تغییر داده و سپس در سرعت حرکت آنها اختلال ایجاد کرد. در ادامه، به معرفی چند مورد از حملات مخرب امنیتی که چالش‌های اساسی شبکه‌های مخابراتی در SG هستند، می‌پردازیم.

۳,۲. حملات علیه اهداف امنیتی شبکه‌های مخابراتی در SG

اندازه‌گیری‌ها و دستورات در SG به طور مداوم از طریق کانال‌های مخابراتی تولید و منتقل می‌شوند. در واقع، SG شامل دستگاه‌های فیزیکی، حسگرها، کانال‌های مخابراتی، مرکز کنترل، ردیاب داده‌های مخرب و سیستم‌های مدیریت انرژی است. ادغام این اجزای ناهمگن، SG را در معرض افزایش سطح تهدیدات سایبری قرار داده است. شبکه‌های مخابراتی در برابر مهاجمانی که می‌توانند سیگنال‌های کنترلی و اندازه‌گیری را دستکاری کنند، آسیب‌پذیر هستند [۲۲].

مسببین حملات امنیتی در شبکه‌های مخابراتی را می‌توان به دو نوع کاربران ناسالم و کاربران مخرب طبقه‌بندی کرد. کاربران ناسالم افرادی هستند که با نقض پروتکل‌های ارتباطی سعی در دستیابی به منابع شبکه بیشتر از کاربران مشروع دارند و کاربران مخرب با اهداف غیرشخصی به طور غیرقانونی اطلاعات شبکه را به دست می‌آورند و به تغییر اطلاعات و یا مختل کردن ارتباطات می‌پردازند که ممکن است باعث آسیب فاجعه‌بار به منابع برق و قطع برق گسترده شود [۴]. در این بخش سه نوع از حملات مخرب را بر اساس اهداف و نیازهای امنیتی سطح بالا، یعنی دسترس‌پذیری، یکپارچگی و محرمانگی، بررسی می‌کنیم.

۳,۲,۱. حملات به دسترس‌پذیری

این حملات، برای تخریب، مسدود کردن یا ایجاد تاخیر در مخابرات SG طراحی شده‌اند. این حملات را به طور معمول با نام انکار سرویس (DoS)[2] می‌شناسند [۱۰]. در واقع، DoS و DDoS[3] حملاتی هستند که در آنها نفوذگر با ارسال درخواست‌های زیاد به یک سرور منجر به خارج شدن آن از دسترس می‌گردد. مهاجم با هدف خاصی به وسیله یک یا چندین دستگاه که هر یک جریان‌های کوچکی را ارسال می‌کنند به ترافیک شبکه حمله می‌کند و دسترسی قابل اعتماد و به موقع به خدمات و اطلاعات شبکه را به خطر می‌اندازد (برای مثال با ایجاد پارازیت در ارتباط میان دو میزبان). همچنین معمولا این حملات با افشای اطلاعات و دستکاری شبکه همراه است [۲۳]. در حملات DoS نفوذگر از یک سیستم درخواست‌ها را ارسال می‌کند ولی در حملات DDoS که نوع توزیع‌شده DoS است، حملات از طریق چند سیستم صورت می‌گیرد. در این نوع حملات، نفوذگر امکان دارد که کنترل سیستمی را به دست گرفته و از آن برای حمله به دیگر سرویس‌ها استفاده کند.

تعامل شبکه قدرت و بخش سایبری و مخابراتی آن، بر قابلیت اعتماد کل شبکه تاثیرگذار است. در [۲۴]، آسیب‌پذیری سیستم قدرت در برابر حملات DOS به عنوان معیاری برای قابلیت اطمینان آن بررسی شده است. اثر حمله به صورت میانگین زمان غلبه بر سیستم (MTTC)[4] و میانگین زمان بازیابی (MTTR)[1] آن

[1] Watermarking

[2] Denial of Service
[3] Distributed Denial of Service
[4] Mean Time to Compromise

در نظر گرفته شده است. تابع هدف بهینه‌سازی آن شامل هزینه سرمایه‌گذاری و هزینه ناشی از وقفه حاصل از حمله سایبری و راه‌اندازی مجدد است و در ادامه، تعداد و محل قرار گرفتن بهینه آشکارسازهای خطا و ابزارهای سوئیچ جهت مقاومت بیشتر در برابر حملات سایبری، تعیین شده است.

با توجه به سازوکار و هدف حمله، حملات DoS و DDoS در لایه‌های مخابراتی مختلف و از راه‌های گوناگون انجام می‌شود. حملاتی مانند Ping of Death، TCP-SYN Flood، ICMP/UDP Flood از حملات انکار سرویس هستند [۴، ۲۵]. در ادامه دو نوع از این حملات شرح داده شده‌اند:

- حملات Ping of Death شامل یک بسته ICMP[2] ناهنجار است که اندازه بزرگی از داده را به هدف حمله ارسال می‌کند به طوری که میزبان را از کار می‌اندازد [۲۵].
- در حملات TCP-ACK Flood، حمله‌کننده تعداد زیادی بسته حاوی SYN به هدف ارسال می‌کند که به معنای تقاضای شروع ارتباط است. با توجه به درخواست، هدف، ارتباط را شروع کرده و در انتظار دریافت ACK از درخواست‌کننده می‌ماند، اما حمله‌کننده بدون ارسال ACK تعداد زیادی اتصال نیمه‌باز ایجاد می‌کند؛ بنابراین منابع به اتصال‌های نیمه‌باز اختصاص خواهد یافت و امکان پاسخ‌گویی به درخواست‌های جدید در شبکه از بین می‌رود [۲۵].

۳،۲،۲. حملات به یکپارچگی

انگیزه اصلی این نوع حملات این است که تبادل داده‌ها در شبکه‌های هوشمند با تغییر یا اضافه کردن غیرقانونی اطلاعات نادرست از بین برود [۲۶]. حملاتی مانند تزریق داده‌ی کاذب و دستکاری داده‌های حسگرها برای رسیدن به این اهداف انجام می‌شوند [۱۰]. علاوه بر حملاتی که اطلاعات را تغییر می‌دهند، حملات با هدف جعل هویت نیز به یکپارچگی آسیب می‌زنند [۵]. بدافزارها (Malicious Software) مانند Worms، Trojan و Backdoors نیز یکپارچگی SCADA[3] و در نتیجه SG را هدف قرار می‌دهند [۲۷].

۳،۲،۳. حملات به محرمانگی

در مقایسه با مهاجمین به یکپارچگی، مهاجمین به محرمانگی قصد تغییر اطلاعات شبکه برق را ندارند، بلکه مهاجمین فقط اطلاعات غیرمجاز را از منابع شبکه SG دریافت می‌کنند [۴]. کاربران مخرب با سوءاستفاده از اطلاعات به دیگران صدمه می‌زنند یا از اطلاعات به نفع خود سود می‌برند [۲۶]. حملاتی مانند تحلیل ترافیک، استراق سمع و Password Pilfering از این نوع حملات هستند [۱۰، ۲۷]. به عنوان مثال در حمله Password Pilfering یک نفوذگر با دستیابی به کلمه عبور، می‌تواند کنترل دسترسی را دریافت کند و محرمانه بودن شبکه را به خطر بیندازد [۲۷]. بنابراین حملات محرمانگی به حریم خصوصی مشترکین با انواع حملات و اقدامات مختلف مانند خواندن حافظه دستگاه‌ها به طور غیرقانونی، شنود رمزهای عبور و جعل هویت آسیب می‌زنند [۵].

۳،۳. طبقه‌بندی حملات براساس مدل معماری شبکه هوشمند

مدل معماری شبکه هوشمند (SGAM)[4] یک مدل مرجع تحت مجوز EU Mandate M/490 و یک معیار طبقه‌بندی برای حملات SG است. این مدل سه طبقه‌بندی برای لایه‌های اصلی در SG شامل لایه مخابرات، لایه کامپیوتر/فناوری اطلاعات و لایه سیستم‌های قدرت و انرژی را مشخص می‌کند. دقت کنید که ممکن است به هر کدام از این لایه‌ها حملاتی وارد شود [۲۵]. ما در این مقاله حملات علیه لایه مخابرات را بررسی می‌کنیم. در حالت کلی، حملات به لایه مخابرات در SG به دو دسته حملات علیه پروتکل‌های ارتباطی و حملات علیه شبکه تقسیم می‌شوند. در ادامه، به بیان جزئیات این حملات پرداخته خواهد شد.

[1] Mean Time to Recovery
[2] Internet Control Message Protocol
[3] Supervisory Control and Data Acquisition
[4] Smart Grid Architecture Model

۳،۳،۱. حملات علیه پروتکل‌های ارتباطی

هر چند در پروتکل‌های ارتباطی مورد استفاده در SG مانند پروتکل‌های ارتباطی Modbus، Profibus، DNP3 و ICCP راهکارهای امنیتی در نظر گرفته شده است، اما همچنان حملات امنیتی به آنها امکان‌پذیر است [۲۵]. پروتکل Modbus به طور گسترده‌ای در سیستم‌های کنترل صنعتی استفاده می‌شود. در این پروتکل یک master که ناظر و کنترل‌کننده است و یک یا چند واحد slave وجود دارد که از طریق مدار واسط سریال (مانند RS485) با هم ارتباط دارند. هر واحد slave اطلاعات دریافتی از field device ها را پس از درخواست master، ارسال می‌کند. هدف حملات محرمانگی در این پروتکل، شناسایی slave ها است زیرا آنها به اطلاعات field device ها دسترسی دارند. در این حملات، کنترل slave با ایجاد یک master مجازی برای کنترل یک یا چند field device انجام می‌شود. وجود یک master مجازی بین slave و master اصلی ممکن است باعث ایجاد تاخیر اطلاعات ارسالی به master اصلی شود که یکی از نشانه‌های تشخیص رخ دادن چنین حمله‌ای است [۲۵].

۳،۳،۲. حملات علیه شبکه

همانطور که می‌دانیم فناوری‌های شبکه در SG ناهمگون هستند. برای مثال حملات تزریق[1] و تغییر[2] به راحتی می‌توانند روی شبکه‌های بی‌سیم اثر بگذارند [۲۵]. حملات تزریقی به دسته گسترده‌ای از حملات اشاره دارد که مهاجم با بهره از ضعف‌ها و شکاف‌های امنیتی سیستم به روند ارتباطات وارد می‌شود و می‌تواند به سرقت داده‌ها، از بین بردن داده‌ها، انکار سرویس و... بپردازد. در حملات تغییر، مهاجم ضمن آنکه به داده‌های شبکه دسترسی پیدا می‌کند، توانایی تغییر اطلاعات را نیز دارد. همچنین نقص‌های امنیتی ذاتی در شبکه، ممکن است در برنامه‌هایی که با اینترنت کار می‌کنند، تاثیر بگذارد [۲۵]. در ادامه چند نوع حمله علیه زیر لایه شبکه در مدل SGAM آورده شده است.

- حملات DoS/DDoS
- حملات مرد میانی (MITM)[3]: این نوع حملات زمانی رخ می‌دهد که یک کابر غیرمجاز، دسترسی غیرقانونی به سیستم را به دست می‌گیرد. در این زمان، نفوذگر در شبکه‌ای مانند SCADA، برای سرور، خود را به عنوان کاربر هدف و برای کاربر هدف، خود را سرور جا می‌زند و به عبارتی در ارتباطات، با جعل هویت، عملیات شنود و یا حتی تغییر اطلاعات را انجام داده [۲۷] و هر سه هدف امنیتی دسترس‌پذیری، یکپارچگی و محرمانگی را به خطر می‌اندازد [۵]. برای مقابله با حملات MITM می‌توان از رمزنگاری کمک گرفت [۲۵].
- حملات بازپخش[4]: در این حملات اطلاعات شبکه به وسیله حملات MITM شنود می‌شوند؛ سپس به واسطه حملات بازپخش با تغییر یا بدون تغییر دادن داده‌های شنود شده، علیه قربانی استفاده می‌شود [۲۵].

۴. راهکارهای مقابله با حملات امنیتی

طبق تحقیقات انجام شده در مرجع [۲۷]، برای جلوگیری از حملات سایبری، به یک روند کاهش خطر برای رسیدن به سطح قابل قبولی از امنیت نیاز داریم. روند کاهش در سه مرحله تعریف شده است:

- **قبل از فرآیند کنترل کاهش:** در این مرحله، ارزیابی خطر برای شناسایی، تجزیه و تحلیل خطرات و رتبه‌بندی بر اساس اهمیت آنها، انجام می‌شود.
- **اجرای فرآیندهای کنترل کاهش:** در این مرحله، کنترل‌های امنیتی که خطر شناسایی شده در مرحله قبلی را تا سطح قابل قبولی کاهش می‌دهند، مانند سیستم‌های تشخیص نفوذ، مدیریت کلید و استانداردهای امنیتی.
- **پس از فرآیند کنترل کاهش:** در این مرحله، مداوم بررسی و نظارت انجام می‌شود تا هر خطر جدید را شناسایی و آنها را به زیرمجموعه ارزیابی خطر وارد کند.

[1] Injection
[2] Modification
[3] Man-in-the-Middle
[4] Replay

۴،۱. نمونه‌هایی از روش‌های مقابله با حملات

شناسایی حملات و کنترل آنها بر اساس اهداف امنیتی مختلف، متفاوت است. در ادامه، اقدامات امنیتی برای رسیدن به اهداف امنیتی سطح بالا را بررسی می‌کنیم.

۴،۱،۱. مقابله با حملات به دسترس‌پذیری

برای داشتن یک شبکه امن باید به اهداف امنیتی برسیم. شبکه برق باید همیشه در دسترس باشد و همان طور که پیش از این بیان شد حملات DoS جزو تهدیدهای اصلی برای امنیت SG هستند. راهکارهای مقابله با حملات DoS طبق تحقیقات انجام شده در [۴، ۱۰] به شرح زیر است:

- **تشخیص حمله با ۴ مکانیسم:** تشخیص مبتنی بر سیگنال، تشخیص مبتنی بر بسته داده، روش پیشگیرانه (الگوریتم‌های مبتنی بر ارسال بسته‌های کاوشگر) و روش ترکیبی.
- **تضعیف حمله با ۳ مکانیسم:** محدود کردن سرعت بسته‌های احتمالا مخرب، فیلتر کردن بسته از یک مقصد خاص پس از تشخیص حمله و تنظیم مجدد معماری شبکه.

۴،۱،۲. مقابله با حملات به یکپارچگی و محرمانگی

رویکردهای بیان شده برای حملات DoS برای تمام حملات از جمله حملات به محرمانگی و یکپارچگی کارایی ندارند. برای حفظ یکپارچگی شبکه راهکارهایی مانند روش اثرانگشت توان (PFP)[1] در [۲۸] پیشنهاد شده است. روش PFP مبتنی بر نظارت دقیق بر مصرف انرژی پردازنده هدف حملات و استفاده از روش‌های پردازش سیگنال و تشخیص الگو برای تشخیص ناهنجاری است. اقدامات دیگری نیز برای رسیدن به یکپارچگی و محرمانگی شبکه انجام می‌شود. برای نمونه در حملات MITM، به این دلیل که بسته‌های مخرب دارای جفت آدرس MAC[2] و IP[3] منطبق نیستند، تجزیه و تحلیل‌های عمیق بسته، مانند سیستم‌های تشخیص نفوذ[4] و سیستم‌های جلوگیری از نفوذ[5]، مفید است [۲۶]. در [۲۹] راهکاری ترکیبی و نوین برای تشخیص نفوذ در شبکه‌های کامپیوتری معرفی شده است. در [۳۰] امضای همریخت به‌عنوان راهکاری برای رفع نقاط ضعف شبکه‌های مستعد حمله تزریقی پیشنهاد شده است.

رویکردهای مبتنی بر رمزنگاری، علیه حملات به یکپارچگی و محرمانگی بسیار مؤثر هستند. سه موضوع کلیدی که در زمینه رمزنگاری انجام می‌شود شامل رمزگذاری[6]، احراز هویت و مدیریت کلید است [۴]. طرح‌های رمزگذاری می‌توانند بر اساس رمزگذاری کلید متقارن (به عنوان مثال AES[7]) یا رمزگذاری کلید نامتقارن (به عنوان مثال RSA[8]) باشند. رمزگذاری کلید متقارن از یک کلید برای رمزگذاری و رمزگشایی استفاده می‌کند ولی رمزگذاری نامتقارن یا رمزنگاری کلید-عمومی برای رمزگذاری و رمزگشایی به ترتیب از کلید عمومی و کلید خصوصی استفاده می‌کنند. تحقیقات انجام شده در مرجع [۴] نشان می‌دهد که رمزگذاری‌های متقارن برای ارتباطات بی‌درنگ در دستگاه‌های توزیع و انتقال مناسب‌تر از رمزگذاری‌های نامتقارن هستند، در حالی که رمزگذاری‌های نامتقارن (با اندازه کلید طولانی) دارای کاربردهای گسترده‌ای برای مدیریت کلید و محافظت از اطلاعات حساس مشتریان در AMI و HAN که ارتباطات بی‌درنگ نیاز ندارند، هستند؛ بنابراین در SG از ترکیب این دو نوع رمزگذاری برای رمزنگاری اطلاعات استفاده می‌شود.

در رمزگذاری‌ها می‌توان از پروتکل‌های مختلفی برای توزیع کلید استفاده کرد. برای مثال پروتکل‌های توزیع کلید کوانتومی همراه با رمزگذاری متقارن می‌توانند از کلیدهای توزیع‌شده بهتر محافظت کنند و محرمانه بودن و یکپارچگی داده‌های تبادل شده و ذخیره شده در SG را تضمین کنند. پروتکل‌های توزیع کلید کوآنتومی در SG در [۷] از زوایای مختلف بررسی شده است. رمزنگاری اطلاعات با انواع مختلفی از زبان‌های برنامه‌نویسی انجام می‌شود. برای رمزنگاری با زبان C می‌توان از کتابخانه

[1] Power Fingerprinting
[2] Media Access Control
[3] Internet Protocol
[4] Intrusion Detection System
[5] Intrusion Prevention System
[6] Encryption
[7] Advanced Encryption Standard
[8] Rivest–Shamir–Adleman

OpenSSL کمک گرفت که پیاده‌سازی متن باز را برای پروتکل‌های SSL[1] و TLS[2] فراهم می‌کند و از توابع پایه‌ای رمزنگاری مانند توابع تولید کلید، انجام رمزگذاری یا رمزگشایی و توابع کاربردی مختلف دیگری تشکیل شده است. هرچند که کتابخانه OpenSSL در اصل برای زبان برنامه‌نویسی C نوشته شده است، اما تعدادی کتابخانه در آن وجود دارد که از طریق آنها می‌توان در زبان‌های برنامه‌نویسی دیگری به غیر از C هم از آن استفاده کرد. این کتابخانه از انواع مختلفی از رمزگذاری‌ها از جمله RSA و AES پشتیانی می‌کند [۳۱]. اقدامات زیاد دیگری نیز علیه حملات موجود در شبکه‌های مخابراتی SG انجام شده که در [۱۰، ۲۶، ۲۷] به چند مورد از آنها اشاره شده است.

در بعضی از طرح‌های اعتبارسنجی، SG یک مرجع متمرکز برای مدیریت پایگاه داده و احراز هویت دارد که اگر پایگاه داده یا سرور متمرکز مورد حمله قرار گیرد، منجر به شکست سیستم می‌شود. اخیرا روش‌های امنیتی غیرمتمرکز مانند زنجیره بلوکی به عنوان گزینه‌ای جدید برای داشتن سیستم‌های ایمن استفاده می‌شوند، برخلاف مرجع امنیتی متمرکز، هر زنجیره بلوکی توسط یک گره غیرمتمرکز ناشناس مدیریت می‌شود که صحت گره‌ها و داده‌های جدید را با توافق شبکه تایید می‌کند؛ به عنوان مثال، دو منبع در SG می‌توانند بدون درگیر شدن واسطه‌ای، انرژی را با یکدیگر تبادل کنند [۲۳].

زنجیره بلوکی می‌تواند برای محافظت از حریم خصوصی داده‌ها، مدیریت هویت و مقاومت در برابر تهدیدهای سایبری مورد استفاده قرار گیرد. برای مثال، استفاده از رمزارزها برای پرداخت صورت‌حساب انرژی یکی از کاربردهای زنجیره بلوکی در حوزه انرژی است. یک راه‌حل امنیتی جدید استفاده شده در زنجیره بلوکی، رمزنگاری با توابع هش و احراز هویت مبتنی بر امضای دیجیتال است [۳۲]. در مرجع [۳۴] راه‌حل‌های امنیتی مبتنی بر زنجیره بلوکی برای AMI و کنتورهای هوشمند با هدف جلوگیری از حملات MITM و دستکاری داده‌ها از طریق شناسایی به موقع گره‌های متخاصم ارائه شده است. این الگوریتم‌های سبک برای کنتورهای هوشمند با قابلیت‌های محاسباتی پایین مناسب هستند. در مرجع [۳۵] راه‌حل‌هایی برای مشکلات احراز هویت در SG بررسی شده است و به کمک زنجیره بلوکی و رمزنگاری، یک پروتکل احراز هویت قابل اعتماد و کارآمد برای کنتورهای هوشمند و شرکت‌های خدماتی پیشنهاد شده است.

ایستگاه‌های شارژ خودروهای الکتریکی (EVCS)[3] متنوعی در دنیا وجود دارند که در تعامل با SG، وابستگی‌های متقابل سایبری-فیزیکی پیچیده‌ای ایجاد می‌کنند. مقاله [۲۳]، به راهکارهای امنیتی و همچنین حفره‌های امنیتی شبکه‌های EVCS می‌پردازد که با توجه به رشد فزاینده خودروهای هیبریدی و الکتریکی بسیار حیاتی می‌باشد؛ زیرا به هم خوردن امنیت سایبری آنها می‌تواند هم به خودروها و هم به EVCS ها آسیب برساند. این مقاله از مدل تهدید STRIDE که توسط مایکروسافت ایجاد شده، برای مدل‌سازی تهدیدات سایبری مانند فریب و نفوذ به شبکه، دستکاری اطلاعات و غیره استفاده می‌کند. در [۳۳] تحقیقات انجام شده در حوزه کاربردهای امنیتی زنجیره بلوکی تحلیل و بررسی شده است. در [۳۶] علاوه بر بیان اهداف و الزامات امنیتی SG و حملات امنیتی، مروری بر پیاده‌سازی زنجیره بلوکی در حوزه امنیت سایبری و حفاظت از داده‌ها در SG داشته است. زنجیره بلوکی علاوه بر بهبود امنیت، در حوزه‌های دیگر SG نیز استفاده می‌شود. مقاله [۳۷] کاربردهای زنجیره بلوکی در مدیریت و کنترل عملیات SG مانند تجزیه و تحلیل و مدیریت داده‌ها را بررسی می‌کند.

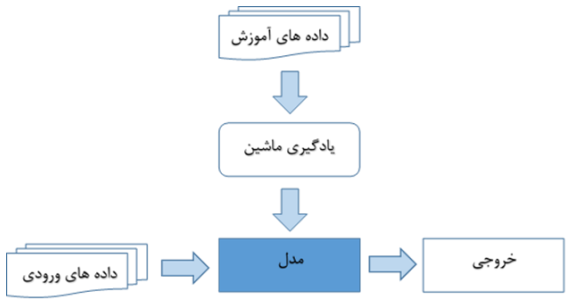
۵. کاربرد هوش مصنوعی در بهبود امنیت شبکه

پاسخ دقیق و سریع به حملات امنیتی، پیش‌شرط لازم برای حفظ امنیت شبکه SG است؛ بنابراین، شناسایی و طبقه‌بندی حملات در SG بسیار حیاتی است [۳۸]. فناوری‌های رایج، برای ارزیابی آسیب‌پذیری امنیت یک سیستم بلادرنگ و پویا مانند شبکه برق، از نقطه نظر محاسباتی گران و کند هستند. روش‌های یادگیری ماشین، با داشتن قابلیت‌های تشخیص الگو

[1] Secure Sockets Layer
[2] Transport Layer Security
[3] Electric Vehicle Charging Stations

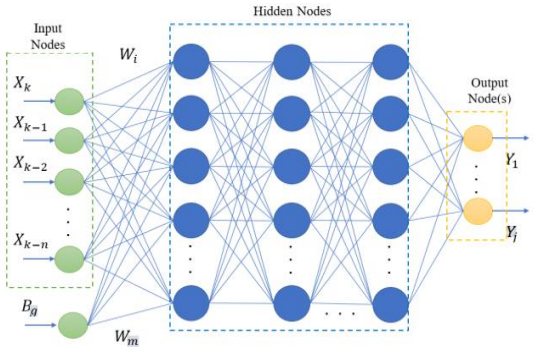
و یادگیری با سرعت بالا، مناسب‌ترین روش برای ارزیابی امنیت شبکه برق هستند [۳۹].

یادگیری ماشین از طریق مجموعه‌ای از روش‌های مبتنی بر این ایده است که ماشین می‌تواند با استفاده از داده‌های آموزش، مدل را به دست آورد و از آن مدل برای تصمیم‌گیری در مورد داده‌های واقعی استفاده کند؛ به عنوان مثال شبکه‌های عصبی و شبکه‌های عمیق عصبی (DNN)[1] از این نوع مدل هستند. این مفهوم در شکل (۴) نشان داده شده است. این بخشی از حوزه هوش مصنوعی است که از شناسایی الگو بهره می‌برد [۳۹، ۴۰]. درمراجع [۴۱-۴۳] به شرح و طبقه‌بندی تعدادی از الگوریتم‌های یادگیری ماشین مورد استفاده در سیستم‌های قدرت پرداخته شده است.



شکل (۴): مفهوم یادگیری ماشین [۴۰]

یادگیری عمیق (DL)[2] یک روش یادگیری ماشین است که از DNN استفاده می‌کند [۴۰] و محاسبات غیرخطی را روی داده‌ها از طریق نورون‌های مجازی چندلایه‌ای برای استخراج ویژگی‌های عمیق از نمونه‌ها انجام می‌دهد؛ بنابراین، در مقایسه با روش‌های رایج یادگیری ماشین، ویژگی‌های داده‌ها با احتمال زیاد به خوبی مشخص می‌شوند [۳۸]. DNN با الهام از عملکرد مغز انسان، از تعدادی دلخواه گره یا نورون تشکیل شده است و همان طور که در شکل (۵) نشان داده شده است، مجموعه یا لایه ورودی را با یک یا تعدادی لایه پنهان، به لایه خروجی ربط می‌دهد [۳۹، ۴۰، ۴۴، ۴۵]. DNN برخلاف شبکه‌های عصبی تک لایه محدودیت محاسبات خطی ندارد و قادر به یادگیری روابط پیچیده غیرخطی بین ورودی‌ها و خروجی‌ها است؛ هرچه واحدهای پنهان در شبکه عصبی بیشتر باشد پیچیدگی و دقت یادگیری بیشتر می‌شود [۳۹، ۴۴، ۴۵]. همچنین قابلیت پردازش موازی DNN، باعث افزایش سرعت در محاسبات و دقت بالا در ایجاد پیش‌بینی‌ها می‌شود [۳۹، ۴۴]. کاربردهای اصلی DL در SG شامل پیش‌بینی انرژی، امنیت سایبری، تشخیص خطا، پیش‌بینی و بهینه‌سازی الزامات فنی برای عملیات ایمن در سیستم قدرت می‌شود [۴۶].



شکل (۵): ساختار DNN [۳۹]

تشخیص ناهنجاری و نفوذ در شبکه، طبقه‌بندی، خوشه‌بندی داده‌های نادرست و احراز هویت کاربر، از نمونه کاربردهای DL و DNN در حوزه امنیت شبکه است [۳۹، ۴۴]. البته بیشترین تمرکز استفاده از DL روی تشخیص بدافزارها و شناسایی و طبقه‌بندی نفوذ در شبکه است [۴۴].

محققان در [۴۷] طبقه‌بندی بدافزارها را با استفاده از DNN با ۹ لایه با دقت ۹۷٪، با استفاده از ویژگی‌های حاصل از آنالیزهای ایستا و پویا انجام داده‌اند. در [۴۴] به کاری اشاره شده است که در آن DNN با ویژگی‌های به دست آمده از فایل‌های اجرایی، به خطای ۲/۹۴٪ در شناسایی بدافزارها و خطای ۰/۳۶٪ در طبقه‌بندی بدافزارها رسیده است. در [۴۸] با مقایسه مدل‌های یادگیری ماشین، بالاترین دقت تشخیص بدافزار در سیستم‌های اندرویدی با دقت ۹۶٪ به DNN تعلق یافت. همچنین پژوهشگران در [۳۸]، روشی را با استفاده از DNN پیشنهاد داده‌اند که با دقت ۹۶٪ خطرات سایبری موجود در SG را شناسایی می‌کند. در [۴۹]، یک شبکه عصبی عمیق ترکیبی برای تشخیص تقلب در مصرف برق پیشنهاد شده است. طبق نتایج این پژوهش این مدل در برخورد با مشکلات نامتعادل قوی

[1] Deep Neural Network
[2] Deep Learning

عمل می‌کند. در [۵۰]، یک معماری زنجیره بلـوکی همـراه بـا الگوریتم رمزگذاری مبتنی بر یادگیری تقویتی بـرای غلبـه بـر حملاتی مانند حمله تزریق داده کاذب پیشنهاد شده اسـت کـه حملات مخرب انجام شده علیه کنتورهای هوشمند را در حین انتقال داده، شناسایی و یک کانال ایمن برای انتقال داده‌های زمان واقعی ایجاد می‌کند. در [۵۱]، یک طرح مبتنـی بـر DL بـرای تشخیص حملات تزریق داده کاذب پیشنهاد شده است. نتـایج شبیه‌سازی دو سناریوی حمله واقعی با توجه به متغیرهای بهینه تعیین شده نشان می‌دهد که این طرح می‌تواند به‌طور مؤثر و با دقت خوبی حملات را شناسایی کند. در [۵۲]، محققـان یـک مدل یادگیری ماشین با دقت ۹۵/۴۴ درصد برای بهبود تشخیص حملات سایبری پیشنهاد داده‌اند. این مدل سلسله مراتبی دو لایه یک طبقه‌بندی برای شناسایی حملات سایبری یک سیستم SG فراهم می‌کند. این رویکرد لایه‌ای دقت مدل را بهبود می‌بخشد. همچنین در این پژوهش، روش‌هایی برای بهبود دقت مدل‌های تشخیص حمله ارائه شـده اسـت. در جـدول (۲) دسـته‌بنـدی موضوعی مراجع بررسی شده در این مقاله ارائه شده است.

۶. نتیجه‌گیری

امنیت SG برای حفاظت از شبکه‌های مخابراتی و شـبکه بـرق مورد نیاز است، چراکه این دو سیستم نیاز به تضمین دسترسی و حیات دائم در شرایط مختلف دارند. دسترس‌پذیری، محرمانگی و یکپارچگی، سه مورد از اهداف امنیتـی مهـم در شـبکه‌هـای مخابراتی مورد استفاده در SG هستند که درصورت برقراری این اهداف یک شبکه قابل اطمینان ایجاد می‌شود. یادگیری عمیق با داشتن برتری‌هایی مانند نداشتن محدودیت در محاسبات خطی و غیرخطی، قابلیت پردازش موازی و ... باعث افزایش سرعت در محاسبات و دقت بالا در ایجاد پیش‌بینی‌هـا مـی‌شـود، کـه می‌تواند یکی از ابزارهای کارآمد برای شناسایی حملات امنیتی علیه شبکه‌های مخابراتی SG باشد.

جدول (۲): دسته‌بندی موضوعی مقالات بررسی شده

مرجع	شبکه‌های مخابراتی SG	اهداف و الزامات امنیت SG	دسته‌بندی حملات امنیتی	راهکارهای مقابله با حملات	یادگیری ماشین در امنیت SG
[۸]	✓	✓			
[۱۰]	✓	✓	✓	✓	
[۲، ۱۱، ۱۳، ۱۴، ۱۷، ۱۸]	✓				
[۲۲، ۲۳]			✓	✓	
[۲۵]			✓		
[۲۶]		✓	✓	✓	
[۲۷]			✓	✓	
[۳۲، ۳۴، ۳۵، ۳۷]				✓	
[۳۶]		✓	✓	✓	
[۳۸، ۴۱، ۴۳–۴۵، ۴۷–۵۲]					✓

تعارض منافع: نویسندگان اعلام می‌کنند که هیچ تعارض منـافعی ندارند.

مراجع

[1] Abrahamsen F. E., Ai Y., and Cheffena M., "Communication Technologies for Smart Grid: A Comprehensive Survey", arXiv preprint arXiv: 11657, 2021.

[2] Gungor V. C., Sahin D., Kocak T., Ergut S., Buccella C., Cecati C., and Hancke G. P., "Smart Grid Technologies: Communication Technologies and Standards", IEEE Transactions on Industrial informatics, 7(4): 529-539, 2011.

[3] Isa N. B. M., Wei T. C., and Yatim A. H. M., "Smart Grid Technology: Communications, Power Electronics and Control System", in 2015 International Conference on Sustainable Energy Engineering and Application (ICSEEA), pp. 10-14, IEEE, 2015.

[4] Wang W. and Lu Z., "Cyber Security in the Smart Grid: Survey and Challenges", Computer Networks, 57(5): 1344-1371, 2013.

[5] Gunduz M. Z. and Das R., "Cyber-Security on Smart Grid: Threats and Potential Solutions", Computer Networks, 169:107094, 2020.

[6] Serban I., Céspedes S., Marinescu C., Azurdia-Meza

C. A., Gómez J. S., and Hueichapan D. S., "Communication Requirements in Microgrids: A Practical Survey", IEEE Access, 8: 47694-47712, 2020.

[7] Kong P.-Y., "A Review of Quantum Key Distribution Protocols in the Perspective of Smart Grid Communication Security", IEEE Systems Journal, 16(1): 41-54, 2020.

[8] Le T. N., Chin W.-L., and Chen H.-H., "Standardization and Security for Smart Grid Communications Based on Cognitive Radio Technologies—a Comprehensive Survey", IEEE Communications Surveys & Tutorials, 19(1): 423-445, 2016.

[۹] گروه اقتصاد و انرژی، آغاز فاز دوم طرح ملی فهام با هدف هوشمندسازی شبکه برق، تیر ۱۳۹۸. (آنلاین) قابل دسترس در: https://www.yjc.ir/00TPF5.

[10] Kabalci E. and Kabalci Y., Smart Grids and Their Communication Systems. Springer Singapore, 2018.

[11] Li Y., Cheng X., Cao Y., Wang D., and Yang L., "Smart Choice for the Smart Grid: Narrowband Internet of Things (Nb-Iot)", IEEE Internet of Things Journal, 5(3): 1505-1515, 2018.

[12] Refaat S. S., Ellabban O., Bayhan S., Abu-Rub H., Blaabjerg F., and Begovic M. M., "Smart Grid Communication Infrastructures", in Smart Grid and Enabling Technologies: John Wiley & Sons, 2021.

[13] Shaukat N., Ali S.M., Mehmood C.A., Khan B., Jawad M., Farid U., Ullah Z., Anwar S.M., and Majid M., "A Survey on Consumers Empowerment, Communication Technologies, and Renewable Generation Penetration within Smart Grid", Renewable and Sustainable Energy Reviews, 81(1): 1453-1475, 2018.

[14] Khan F., ur Rehman A., Arif M., Aftab M., and Jadoon B. K., "A Survey of Communication Technologies for Smart Grid Connectivity", in 2016 International Conference on Computing, Electronic and Electrical Engineering (ICE Cube), pp. 256-261, IEEE, 2016.

[15] Yaacoub J. P. A., Fernandez J. H., Noura H. N., and Chehab A., "Security of Power Line Communication Systems: Issues, Limitations and Existing Solutions", Computer Science Review, 39: 100331, 2021.

[16] Sharma K. and Saini L. M., "Power-Line Communications for Smart Grid: Progress, Challenges, Opportunities and Status", Renewable and Sustainable Energy Reviews, 67: 704-751, 2017.

[17] Anzar M., Nadeem J., and Sohail R., "A Review of Wireless Communications for Smart Grid", Renewable and Sustainable Energy Reviews, 41: 248-260, 2015.

[18] Mulla A., Baviskar J., Khare S., and Kazi F., "The Wireless Technologies for Smart Grid Communication: A Review", in 2015 Fifth International Conference on Communication Systems and Network Technologies (CSNT), pp. 442-447, IEEE, 2015.

[19] Cheng Y., Saputra H., Goh L. M., and Wu Y., "Secure Smart Metering Based on Lora Technology", in 2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA), pp. 1-8, IEEE, 2018.

[20] Lora Module Application for Remote Meter Reading Solution (online), 2016. Available: https://www.fourfaith.com/smartgrid/lora-module-application-for-remote-meter-reading-solution.html.

[۲۱] تکنولوژی‌های مخابراتی در سیستم‌های اندازه‌گیری هوشمند، سلسله گزارشات تخصصی شبکه هوشمند انرژی ایران، اردیبهشت ۱۳۹۲، شماره ۱۱.

[22] Zhang H., Liu B., and Wu H., "Smart Grid Cyber-Physical Attack and Defense: A Review", IEEE Access, 9: 29641-29659, 2021.

[23] Acharya S., Dvorkin Y., Pandžić H., and Karri R., "Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective", IEEE Access, 8: 214434-214453, 2020.

[24] Kapourchali M. H., Sepehry M., and Aravinthan V., "Fault Detector and Switch Placement in Cyber-Enabled Power Distribution Network", IEEE Transactions on Smart Grid, 9(2): 980-992, 2016.

[25] Elbez G., Keller H. B., and Hagenmeyer V., "A New Classification of Attacks against the Cyber-Physical Security of Smart Grids", in Proceedings of the 13th International Conference on Availability, Reliability and Security, ACM, 2018.

[26] Rawat D. B. and Bajracharya C., "Cyber Security for Smart Grid Systems: Status, Challenges and Perspectives", in SoutheastCon 2015, pp. 1-6, IEEE, 2015.

[27] Coffey K., Maglaras L. A., Smith R., Janicke H., Ferrag M.A., Derhab A., Mukherjee M., Rallis S., and Yousaf A., "Vulnerability Assessment of Cyber Security for Scada Systems", in Guide to Vulnerability Analysis for Computer Networks and Systems: Springer, pp. 59-80, 2018.

[28] Reed J. H. and Gonzalez C. R. A., "Enhancing Smart Grid Cyber Security Using Power Fingerprinting: Integrity Assessment and Intrusion Detection", in Future of Instrumentation International Workshop (FIIW) Proceedings, pp. 1-3, IEEE, 2012.

[۲۹] شیخان م. و عباسی ع.، «راهکار ترکیبی نوین برای تشخیص

Journal, 34(1): 106879, 2021.

[42] Kotsiopoulos T., Sarigiannidis P., Ioannidis D., and Tzovaras D., "Machine Learning and Deep Learning in Smart Manufacturing: The Smart Grid Paradigm", Computer Science Review, 40: 100341, 2021.

[43] Omitaomu O. A. and Niu H., "Artificial Intelligence Techniques in Smart Grid: A Survey", Smart Cities, 4(2): 548-568, 2021.

[44] Berman D. S., Buczak A. L., Chavis J. S., and Corbett C. L., "A Survey of Deep Learning Methods for Cyber Security", Information, 10(4), 2019.

[۴۵] لطیف م. و باطنی ز.، «بررسی و مقایسه روش‌های تشخیص نفوذ در شبکه‌های کامپیوتری»، همایش ملی فناوری در مهندسی کاربردی باشگاه پژوهشگران جوان و نخبگان دانشگاه آزاد اسلامی تهران، ۲۱ بهمن، ۱۳۹۵.

[46] Massaoudi M., Abu-Rub H., Refaat S. S., Chihi I., and Oueslati F. S., "Deep Learning in Smart Grid Technology: A Review of Recent Advancements and Future Prospects", IEEE Access, 9: 54558-54578, 2021.

[47] Cordonsky I., Rosenberg I., Sicard G., and David E. O., "Deeporigin: End-to-End Deep Learning for Detection of New Malware Families", in 2018 International Joint Conference on Neural Networks (IJCNN), pp. 1-7, IEEE, 2018.

[48] Yuan Z., Lu Y., Wang Z., and Xue Y., "Droid-Sec: Deep Learning in Android Malware Detection", in ACM SIGCOMM Computer Communication Review, 44(4): 371-372, ACM, 2014.

[49] Ullah A., Javaid N., Samuel O., Imran M., and Shoaib M., "Cnn and Gru Based Deep Neural Network for Electricity Theft Detection to Secure Smart Grid", in 2020 International Wireless Communications and Mobile Computing (IWCMC), 2020, pp. 1598-1602, IEEE.

[50] Shukla S., Thakur S., and Breslin J. G., "Secure Data Transmission in Smart Meters Using Q-Learning in Fog Computing Environment", in Proceedings of Sixth International Congress on Information and Communication Technology, 2022, pp. 667-678, Springer.

[51] Ding Y., Ma K., Pu T., Wang X., Li R., and Zhang D., "A Deep Learning-Based Classification Scheme for Cyber-Attack Detection in Power System", IET Energy Systems Integration, 3(3): 274-284, 2021.

[52] Farrukh Y. A., Ahmad Z., Khan I., and Elavarasan R. M., "A Sequential Supervised Machine Learning Approach for Cyber Attack Detection in a Smart Grid System", in 2021 North American Power Symposium (NAPS), 2021, pp. 1-6.

نفوذ در شبکه‌های کامپیوتری با استفاده از الگوریتم‌های هوش محاسباتی»، مجله محاسبات نرم، جلد ۶، شماره ۱، ص. ۶۵-۴۸، ۱۳۹۶.

[۳۰] بابامیر ف. و اسلامی ز.، «بهینه‌سازی پایداری داده‌های مفید و قابل اعتماد در شبکه‌های حسگر بی‌سیم بی‌ملازم»، مجله محاسبات نرم، جلد ۱، شماره ۱، ص. ۲۳-۱۶، ۱۳۹۱.

[31] Viega J., Messier M., and Chandra P., Network Security with Openssl: Cryptography for Secure Communications. O'Reilly Media, Inc, 2002.

[32] Andoni M., Robu V., Flynn D., Abram S., Geach D., Jenkins D., McCallum P., and Peacock A., "Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities", Renewable and Sustainable Energy Reviews, 100: 143-174, 2019.

[۳۳] برنگی ح.، راجی ف. و خاصه ع.، «تحلیل تحقیقات امنیت و حریم خصوصی حوزه بلاک‌چین: یک مطالعه علم سنجی»، مجله محاسبات نرم، جلد ۹، شماره ۱، ص. ۵۵-۴۰، ۱۳۹۹.

[34] Kamal M. and Tariq M., "Light-Weight Security and Blockchain Based Provenance for Advanced Metering Infrastructure", IEEE Access, 7: 87345-87356, 2019.

[35] Wang W., Huang H., Zhang L., and Su C., "Secure and Efficient Mutual Authentication Protocol for Smart Grid under Blockchain", Peer-to-Peer Networking Applications, 14(5): 2681-2693, 2021.

[36] Hasan M. K., Alkhalifah A., Islam S., Babiker N. B. M., Habib A. K. M. A., Aman A. H. M., and Hossain Md. A., "Blockchain Technology on Smart Grid, Energy Trading, and Big Data: Security Issues, Challenges, and Recommendations", Wireless Communications Mobile Computing, 2022.

[37] Aklilu Y. T. and Ding J., "Survey on Blockchain for Smart Grid Management, Control, and Operation", Energies, 15(1): 193, 2022.

[38] Zhou L., Ouyang X., Ying H., Han L., Cheng Y., and Zhang T., "Cyber-Attack Classification in Smart Grid Via Deep Neural Network", in Proceedings of the 2nd International Conference on Computer Science and Application Engineering, ACM, 2018.

[39] Dogaru D. I. and Dumitrache I., "Cyber Attacks of a Power Grid Analysis Using a Deep Neural Network Approach", Journal of Control Engineering and Applied Informatics, 21(1): 42-50, 2019.

[40] Kim F., MATLAB Deep Learning With Machine Learning, Neural Networks and Artificial Intelligence, Apress, 2017.

[41] Farhoumandi M., Zhou Q., and Shahidehpour M., "A Review of Machine Learning Applications in Iot-Integrated Modern Power Systems", the Electricity