8TH REGIONAL CONFERENCE ON ELECTRICITY DISTRIBUTION
Tehran 21,22 Jan. 2020
CIRED IRAN NC
هشتمین کنفرانس منطقه‌ای سیـــــرد
تهران، ۱ و ۲ بهمن ماه ۱۳۹۸
انجمن صنفی کارفرمایی شرکت‌های توزیع نیروی برق

مطالعه، تحلیل و چالش های امنیت سایبری در شبکه های هوشمند برق

علیرضا رجبی
امور نظارت بر خدمات عمومی
شرکت توزیع نیروی برق
فارس ، ایران

رضا صداقتی
گروه مهندسی برق،
موسسه آموزش عالی غیرانتفاعی زند شیراز،
شیراز، ایران

امیر رضاقلی
گروه مهندسی برق،
موسسه آموزش عالی غیرانتفاعی زند شیراز،
شیراز، ایران

مجتبی پارسایی
دفتر سازماندهی و طبقه بندی مشاغل
شرکت توزیع نیروی برق
فارس ، ایران

وحید سینائی
امور نظارت بر خدمات عمومی
شرکت توزیع نیروی برق
فارس ، ایران

چکیده — شبکه هوشمند برق اساسا شبکه الکترونیکی مدرنی است که با استفاده از فناوری اطلاعات و ارتباطات، انرژی را از تولیدکنندگان به مصرف کنندگان منتقل می کند و اطلاعاتی نظیر چگونگی رفتار تولید کنندگان و مصرف کنندگان را به صورت خودکار جمع آوری و دنبال می کند تا با کنترل وسایل منازل مصرف کنندگان در مصرف انرژی صرفه جویی شود و در نتیجه قابلیت اطمینان، پایداری و ثبات تولید و توزیع برق بهبود یابد. هر چند شبکه های هوشمند کارایی شبکه را بهبود می بخشند اما استفاده از این فناوری ها، وابستگی شبکه برق به منابع سایبری را افزایش می دهد که ممکن است در مقابله حمله آسیب پذیر باشد. حمله به منظور سرقت انرژی یک حمله متداول در شبکه برق است. سرقت انرژی سالانه میلیاردها دلار به شبکه های برق در سراسر جهان خسارت وارد می کند. از اینرو لازم است تا روشهای مناسب جهت شناسایی سرقت انرژی در شبکه هوشمند توسعه داده شوند. در این مقاله سعی شده است تا با معرفی زیرساخت های فناوری در شبکه های انرژی، چالش های امنیتی آن مورد بررسی قرار گرفته و راه حلی جامع برای مشکلات امنیتی آن ارائه گردد.

واژه های کلیدی— شبکه هوشمند برق؛ حملات سایبری؛ امنیت؛ قابلیت اطمینان.

۱. مقدمه

تکامل و به روز شدن شبکه قدرت رایج باعث پیدایش شبکه هوشمند قدرت شده است که شامل نظارت پیشرفته، خودکار سازی و کنترل تولید، انتقال و توزیع برق می باشد. شبکه هوشمند قدرت از سه نظر قابل تعریف است[۱-۲]:

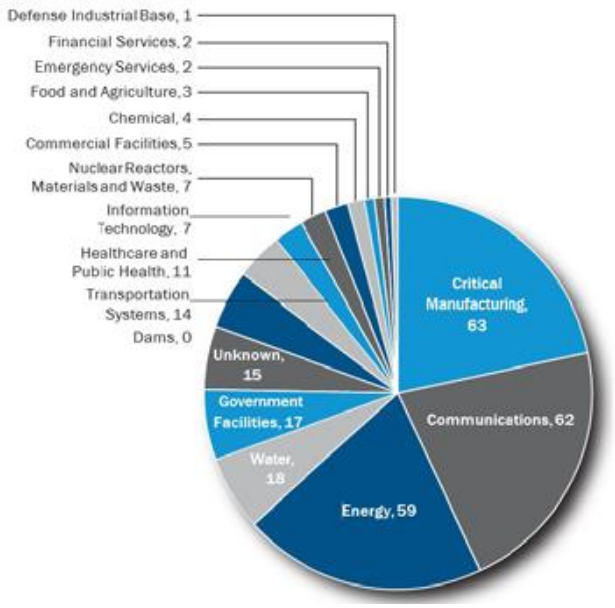
- شبکه هوشمند قدرت برای مصرف کننده بدین معنی است که آنها می توانند مصرف خود را بصورت هوشمندانه مدیریت کنند و در ساعات اوج مصرف که قیمت انرژی زیاد است هزینه کمتری را پرداخت کنند.
- این شبکه از دید کارشناسان محیط زیست به معنی استفاده از فناوری برای جلوگیری از آلودگی های زیست محیطی است.
- برای متخصصین صنعت برق، پایین آوردن سطح اوج مصرف و تصمیم گیری هوشمندانه و ارائه اطلاعات دقیق از وضعیت شبکه می باشد.

شبکه های تولید و توزیع برق از زیرساخت های حیاتی هر کشوری محسوب می شود، به ویژه اینکه هر گونه اختلالات در

دسترس پذیری آنها پیامدهای انتشاری بر روی زیر ساخت های حیاتی دیگر از قبیل شبکه های بانکی، ارتباطات، آب و ... به همراه خواهد داشت[۳]. در سال های اخیر رویکرد صنعت برق به شبکه های هوشمند به سرعت در جریان است. انگیزه این رویکرد، مزایای این شبکه ها از قبیل هوش توزیع شده، قابلیت پهنای باند و ... می باشد[۴-۵].

استفاده از زیرساخت های ارتباطی در شبکه برق باعث می شود که شبکه در معرض تهدیدها و آسیب های جدید قرار گیرد. از آنجا که اندازه گیرها در شبکه های هوشمند برق مقدار زیادی داده جمع آوری می کنند، که این داده ها شامل اطلاعات خصوصی مشتریان هم می شود ، از اینرو می تواند امنیت و حریم خصوصی مشترکان را به خطر بیندازد[۶]. از طرفی امکان دسترسی به تعداد زیادی دستگاه هوشمند که هر کدام می توانند به عنوان نقطه ورود مهاجم به شبکه باشند نیز یک آسیب پذیری دیگر است. در شبکه هوشمند توزیع برق ذی نفعان بیشتری داریم که داشتن ذی نفع بیشتر ، احتمال وقوع حمله های خطرناک را افزایش می دهد. مهاجمان می توانند با کشف و استفاده از این آسیب پذیری ها حمله های خود را به شبکه هوشمند توزیع برق پی ریزی کنند. مهاجمان در حمله به شبکه هوشمند توزیع برق اهدافی نظیر جمع آوری داده های مشترکین، حملات تروریستی و سرقت انرژی دارند. سرقت انرژی عبارتست از مجموعه اعمال مجرمانه ای که یک یا چند مصرف کننده انجام می دهند تا آمار مصرف انرژی ای که به شرکت های توزیع کننده گزارش می دهند را دستکاری کنند[۷]. یک گزارش بانک جهانی نشان می دهد که پنجاه درصد برق مصرفی در کشورهای در حال توسعه از طریق سرقت به دست می آید، حدود هشتاد درصد سرقت انرژی در سراسر جهان در مناطق مسکونی و بیست درصد باقیمانده در مناطق صنعتی و تجاری رخ می دهند[۸-۹].

امنیت یک معیار مهم موفقیت برای عملیات ایمن، کارآمد و قابل اطمینان شبکه هوشمند می باشد[۱۰]. مهم ترین هدف امنیت، حفاظت از تمامی دارائی های مرتبط در حیطه شبکه هوشمند از هر نوع خطر، همچون حملات امنیتی عمدی، اشتباهات پرعمدی، نقص تجهیزات، سرقت اطلاعات می باشد که هریک از آنها پیامدهای اجتماعی، سیاسی و اقتصادی ناگواری می تواند به دنبال داشته باشد. اما با ظهور ارتباطات مبتنی بر اینترنت و فناوری IP ، یوتیلیتی ها به منظور بهره برداری از منافع متعدد این شبکه های اطلاعاتی و ارتباطی، اجزا و منابع شبکه هوشمند را با شبکه های احتمالا ناامن اتصال می دهند. به این ترتیب حملات منعددی در سیستم های شبکه هوشمند رخ داده و گزارش شده است. بر طبق آخرین گزارش منتشر شده توسط "تیم واکنش اضطراری سایبری در سیستم های کنترل صنعتی" یا ICS-CERT در سال ۲۰۱۷، از ۲۹۰ نفوذ کشف شده به شبکه های زیرساخت های حیاتی(صنعتی و مالی)، ۵۹ حمله یعنی ۲۰٪ از آنها در بخش انرژی برق رخ داده است(شکل(۱)). همچنین انتشار اطلاعات فنی حمله به این سیستم ها در اینترنت و شبکه های اجتماعی، و روشن تر شدن کاستی های امنیتی مرتبط، شبکه هوشمند را نسبت به گذشته آسیب پذیر تر می کند[۱۱-۱۲].



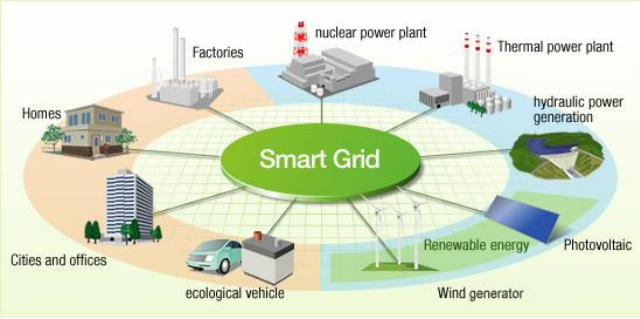
شکل ۱. نفوذ به شبکه های زیرساخت حیاتی به تفکیک بخش

شبکه بندی اجزای مختلف سیستم قدرت به هم، نیازمند فناوری های مختلفی در تعامل سازگار با یکدیگر است. این تعامل بین فناوری های مختلف می تواند به رخداد خطرات امنیتی جدیدی منجر شود[۱۳]. این بدان معناست که فناوری های جدید بکار رفته در شبکه هوشمند می تواند حاوی آسیب پذیری های احتمالی امنیتی باشند. اگر چه طراحی و اجرای شبکه هوشمند

برق کمک شایانی به حفظ منابع می کند اما از طرفی افزایش مسائل جدید و چالش هایی در مورد عملکرد موثر سیستم برق، آسیب پذیری هایی در مقابل شکاف های امنیتی برای شبکه به وجود می آورد. در این مقاله چالش های امنیتی در شبکه های هوشمند انرژی مورد بررسی قرار گرفته و راه حلی برای مقابله با حملات سایبری در آنها ارائه گرده است.

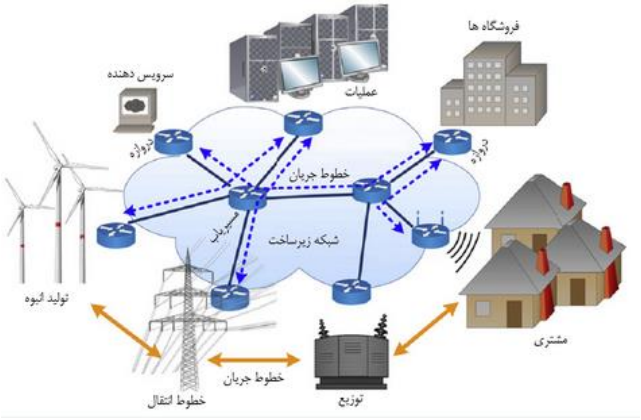
۲. شبکه هوشمند انرژی و اجزای آن

امروزه شبکه انرژی(Smart Grid) در هر کشوری، به منزله شاهراه‌های حیاتی برای توسعه پایدار به شمار می‌روند. تامین و توزیع مناسب و ارزان انرژی به مصرف کننده‌گان آن که صنایع بزرگ کشور هستند این قابلیت را می‌دهد تا با تولید محصولات، تولید ملی را افزایش دهند. امروزه زیرساخت شبکه اطلاعات لازمه‌ی شبکه توزیع انرژی به شمار می‌رود. نظارت بر تمامی اجزای شبکه به صورت متمرکز، قابلیت اعمال دستورات بر تمامی بخش‌ها، گزارش سریع مشکلات احتمالی جزو اولین نیازمندی ها به شمار میرود[۱۴].



شکل۲. شمایی از شبکه هوشمند انرژی

براساس مدل مفهومی موسسه‌ی استاندارد NIST شبکه هوشمند انرژی شامل ۷ دامنه‌ی منطقی است: تولید انبوه، انتقال، توزیع، مصرف، بازار، سرویس‌دهنده و عملیات. تصویری از این سیستم را در شکل(۳) مشاهده می‌کنیم.



شکل۳. اجزای گوناگون شبکه هوشمند انرژی

۳. ویژگیهای سیستم ارتباطی شبکه هوشمند برق

این موضوع واضح است که ارتباطات شبکه هوشمند از نظر پیچیدگی و ساختار سلسله مراتبی مانند اینترنت می‌باشد. اما تفاوت‌های ساختاری نیز باهم دارند:

- **معیارهای اندازه گیری کیفیت**

وظیفه‌ی اصلی اینترنت فراهم کردن خدمات داده‌ای (مرور وب، گوش کردن به موسیقی...) برای مصرف کننده است و دستیابی به توان عملیاتی و عدالت میان مصرف‌کننده دارای اهمیت بسیاری است. اما شبکه ارتباطی برق، برای ایجاد توان عملیاتی بالا ساخته نشده است بلکه معیارهای دیگری مانند اطمینان-پذیری، ارتباط بدون درنگ و امن و ارتباط غیر بلادرنگ برای سیستم‌های نظارتی و مدیریتی دارد. به‌عنوان مثال تأخیر در سیستم‌های قدرت دارای اهمیت بیشتری نسبت به توان عملیاتی است و همین اهمیت سیستم را به سمت طراحی بر اساس کاهش تأخیر هدایت می‌کند[۱۵].

- **مدل ترافیک**

مشخص است که بسیاری از جریان ترافیک در اینترنت دارای ویژگی خود تشابهی است، مانند ترافیک وب www . اما در ترافیک شبکه قدرت، مقدار بسیاری ار ترافیک حالت تناوبی دارد، دلیل این موضوع مونیتورینگ پیوسته داده‌های ایستگاه‌های توزیع و خواندن متناوب کنتورهای اندازه‌گیری در شبکه‌های خانگی است. علاوه بر این می‌توان انتظار داشت که اکثر ترافیک

در شبکه هوشمند انرژی با ترافیک اینترنت متفاوت باشد، زیرا از پروتکل‌های متنوعی در این شبکه در مقایسه با اینترنت استفاده می‌شود.

- **نیازمندی های زمانی**

بسیاری از ترافیک موجود در اینترنت فاقد محدودیت زمانی هستند و ترافیک حساس به تاخیر دارای نیازمندی ۱۰۰-۱۵۰ میلی ثانیه است که دارای کاربردهایی مانند VOIP و همچنین کاربردهای صوتی-تصویری هستند. این در حالی است که شبکه هوشمند انرژی دارای نیازمندی‌های زمانی متفاوتی از چند میلی‌ثانیه تا حدود دقیقه است. به عنوان مثال پیام‌های مربوط به trip protection ایستگاه‌های substation دارای نیازمندی تاخیری در حد ۳ میلی ثانیه هستند. بنابراین شبکه هوشمند انرژی دارای نیازمندی‌های زمانی بالاتری نسبت به اینترنت هستند[۱۶].

- **مدل ارتباطی**

اصل ارتباطی نقطه به نقطه پایه ارتباط در اینترنت به شمار می‌رود و بر همین اساس ارتباطات نقطه به نقطه (peer-to-peer) بین هر دو نقطه در اینترنت قابل برقراری است. در سیستم‌های فعلی و باقی مانده از گذشته در شبکه قدرت، بیشتر ارتباطات به صورت یک طرفه می‌باشند، بدین صورت که دستگاه‌ها به صورت پیوسته وضعیت خود را به مرکز کنترل ارسال می‌کنند. در مقایسه با این ساختار سنتی، در شبکه هوشمند انرژی مدل‌های ارتباط دوطرفه نیز وجود دارد: مانند بالا به پایین(مرکز به دستگاه) و پایین به بالا(دستگاه به مرکز). شبکه هوشمند همچنین از ارتباط نقطه به نقطه نیز پشتیبانی می‌کند، اما به دلایل امنیتی این روش محدود به شبکه‌های داخل منازل محدود می‌شود.

- **نوع پروتکل(Protocol Stack)**

تمامی اینترنت بر روی بستر پروتکل IP بنا شده است و در حال حاضر در حال حرکت به سمت IPv6 است. انتظار می‌رود که شبکه هوشمن انرژی نیز از IPv6 به عنوان لایه اصلی ارتباطی استفاده کند. در هر صورت شبکه هوشمند انرژی محدود به IPv6 نخواهد بود و می‌تواند با توجه به عملکرد شبکه و نیازمندی‌های موجود از پروتکل‌های متنوعی بهره ببرد. به عنوان مثال سوییچ‌های ATM برای تضمین کیفیت سرویس (Qualit of Service=QoS) برای ارسال پیام‌های حساس نسبت به تاخیر زمانی در سیستم ارتباطی قدرت استفاده می‌شود. در هر صورت، شبکه هوشمند انرژی از پروتکل‌های متنوعی برای کاربردهای مختلف استفاده می‌کند[۱۷-۱۸].

۴. اهمیت امنیت در شبکه هوشمند انرژی

رشد همه جانبه ارتباطات، شبکه ها(خصوصا شکل بی سیم آنها)، استفاده از فناوری های آنها در سیستم ها و شبکه های با گستردگی بالا، اهمیت راهبردی و حیاتی سیستم های زیر ساخت ملی(شامل شبکه هوشمند انرژی، سیستم های حمل و نقل، شبکه های پدافند و ...) ، جایگاه امنیت در این شبکه ها را بیش از پیش پر رنگ تر می کند.

انتشار بدافزارهایی مانند "استاکس نت" و "فلیم" ، امن سازی سیستم های کنترل صنعتی در برابر حملات سایبری بد رفتار مورد توجه قرار گرفته است. خرابی آنها ممکن است آسیب های جبران ناپذیری را به سیستم کنترل فیزیکی و مردم وابسته به آن وارد کند. به خطر افتادن امنیت این شبکه ها می تواند به از بین بردن ایمنی و سلامتی عمومی ، امنیت ملی و اقتصاد بینجامد. شبکه های انرژی به دلیل گستردگی و وابستگی تمام بخش ها به آن به عنوان یک شبکه صنعتی حیاتی به شمار می آیند. از اینرو ارتقای امنیت شبکه هوشمند با توجه به چالش های امنیتی خاص این شبکه از اهمیت بالایی برخوردار است.

۵. چالش ها و نیازمندی های امنیت سایبری در شبکه هوشمند انرژی

نقش سیستم ارتباطی در شبکه‌ی هوشمند انرژی بسیار حیاتی می‌باشد. برای اطمینان از قابل‌اعتماد و امن بودن این سیستم ارتباطی، ابتدا باید اهداف و نیازمندی‌های بحث امنیت را در این سیستم ارتباطی به‌صورت کامل شناسایی کنیم تا بتوانیم در ادامه

بر اساس آن یک راه حل همه‌جانبه را برای امنیت سایبری در حوزه انتقال و مدیریت انرژی داشته باشیم.

۱،۵. اهداف

گروه امنیت سایبری در موسسه‌ی استاندارد NIST یک نگرش جامع به موضوع امنیت در سیستم هوشمند انرژی را منتشر کرده‌اند[۸]. در ادامه سه سطح اصلی در موضوع امنیت سایبری را که در شکل (۴) نشان داده شده است را بیان می‌کنیم:

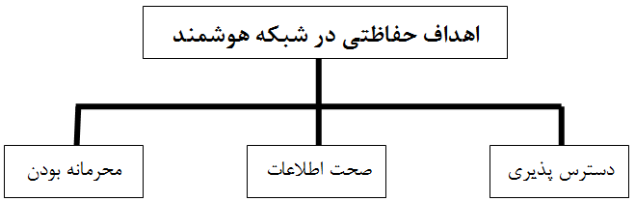
- **دسترس‌پذیری**: اطمینان از در دسترس بودن در زمان مورد نظر و استفاده از اطلاعات مورد نیاز یکی از مهم‌ترین موضوعات در شبکه‌ی هوشمند انرژی می‌باشد. این موضوع به این دلیل دارای اهمیت می‌باشد که اگر قابلیت استفاده از اطلاعات به علت قطع دسترسی از بین رود، ممکن است باعث اختلال در توزیع انرژی شود[۱۹].

- **صحت:** محافظت در برابر دست‌کاری نادرست در اطلاعات و یا تخریب آن که به معنای قابلیت عدم انکار و تأیید هویتآن است. از دست رفتن صحت که می‌تواند ناشی از تغییرات بدون اجازه و یا نابودی اطلاعات باشد، می‌تواند در آینده باعث اخذ تصمیمات نادرست در زمینه‌ی مدیریتی باشد.

- **حفظ اسرار:** حفظ محدودیت‌های مجاز در دسترسی و افشای اطلاعات برای حفظ حریم خصوصی افراد و اطلاعات اختصاصی می‌باشد. این موضوع به‌صورت اختصاصی جلوگیری از افشای بدون مجوز اطلاعاتی که برای عموم و افراد مجاز نیست اهمیت دارد.

از نظر چشم‌انداز سیستمی، قابل‌اطمینان بودن، دسترس‌پذیری و صحت از مهم‌ترین فاکتورهای امنیت در سیستم‌های هوشمند انرژی می‌باشند. حفظ اسرار در این زمینه دارای کمترین اولویت است اما از آنجایی که این سیستم شامل مصرف‌کننده‌گان می‌باشد، این موضوع اهمیت بسیاری پیدا می‌کند[۲۰].

در میان همه این ویژگی ها در امنیت شبکه هوشمند انرژی، کنترل و مدیریت توزیع شده دارای اهمیت ویژه ای خواهد بود که توسط چندین عامل مدیریت می شوند. هر عامل می تواند حرکت متفاوتی داشته باشد. کار با الگوریتم های کنترل در چارچوب شبکه هوشمند انرژی نیازمند سادگی، توزیع شده بودن، قوی بودن در مقابل اختلال و کارایی در بکارگیری منابع بوده و نیاز به فراهم ساختن پاسخ بلادرنگ صحیح دارد. بدلیل نبود ناظر متمرکز بر فعالیت گره های شبکه، راهبردهای کنترل توزیع شده، بیشتر در معرض حملات و خرابی اجزا هستند. بنابراین اهمیت آن برای تضمین محاسبات امن و قابل اعتماد با وجود دستگاههای بدرفتار افزایش می یابد. علاوه بر آن بیشترین تلاش کنونی برای ارتقای امنیت شبکه هوشمند انرژی(و سیستم های اسکادا) با تاکید بر روشهایی انجام شده است که محدود به امنیت پایگاه و ارتباط (به عنوان نمونه رمزنگاری و تشخیص هویت) می باشند. پس یک نگرانی ضروری برای محافظت از الگوریتم های کنترل از حملات سایبری بدخواه وجود دارد.



شکل۴. اجزای مختلف امنیت در شبکه هوشمند انرژی

۲،۵. نیازمندی ها

دسترس‌پذیری، صحت و حفظ اسرار همان طور که بیان شد سه موضوع سطح بالای امنیت در شبکه‌های هوشمند می‌باشند. علاوه بر چنین موضوعات کلی، در گزارش NIST نیازمندی‌های امنیتی اختصاصی برای شبکه‌ی هوشمند بیان شده است که شامل امنیت سایبری و امنیت فیزیکی می‌باشد. اختصاصاً در بخش امنیت سایبری شامل جزئیاتی از مشکلات و نیازمندی‌های مربوط به امنیت در شبکه‌ی هوشمند انرژی در مورد اطلاعات و شبکه می‌باشد. در زمینه‌ی امنیت فیزیکی شامل امنیت تجهیزات فیزیکی و حفاظت محیطی و همین‌طور سیاست های امنیتی مربوط به کارکنان و پیمانکاران می‌باشد[۱۷]. از

آنجایی که در این مقاله، موضوع مورد بحث ما امنیت سایبری می‌باشد، بنابراین نیازمندی‌های امنیت سایبری را در ادامه بیان می‌کنیم:

- **تشخیص حمله و عملیات تدافعی**: در مقام مقایسه با سیستم سنتی توزیع برق، شبکه‌ی هوشمند انرژی یک شبکه‌ی ارتباطی باز و توزیع‌شده در یک منطقه‌ی جغرافیایی وسیع می‌باشد. با توجه به این موضوع این غیرممکن است که بتوان اطمینان حاصل کرد که تمامی گره‌های این شبکه‌ی وسیع در برابر حملات مقاوم هستند. بنابراین شبکه‌ی ارتباطی نیازمند این است که ترافیک آن به‌صورت پیوسته تحت نظارت، آزمایش و سنجش قرار بگیرد تا بتوان فعالیت‌های غیرعادی که مربوط به حملات می‌باشند را در اسرع وقت شناسایی کرد. علاوه بر این شبکه باید دارای قابلیت خود ترمیمی باشد تا بتواند پس از وقوع حملات به فعالیت خود ادامه دهد. با توجه به اهمیت زیرساخت‌های قدرت، عملیات تدافعی در برابر حملات یک نیازمندی اساسی به شمار می‌رود تا در دسترس‌پذیری شبکه حفظ شود[۲۱].

- **شناسایی، تأیید هویت و کنترل دسترسی:** شبکه‌ی ارتباطی سیستم هوشمند شامل میلیون‌ها دستگاه الکتریکی و مصرف‌کننده می‌باشد. شناسایی و تأیید هویت یک فرآیند کلیدی برای تصدیق هویت یک ابزار یا مصرف‌کننده به‌عنوان یک پیش‌نیاز برای اعطای دسترسی به منابع در شبکه اطلاعاتی سیستم هوشمند انرژی می‌باشد. تمرکز کنترل دسترسی اطمینان از این موضوع است که منابع توسط کاربر صحیح که به‌صورت درست شناسایی شده است، در دسترس باشد. کنترل دسترسی باید به گونه‌ی سخت گیرانه باشد تا از دسترسی افراد غیر مجاز به اطلاعات حساس و کنترل زیرساخت‌ها جلوگیری به عمل بیاورد. برای دستیابی به این اهداف هر گره در شبکه هوشمند باید دارای سیستم‌های رمزگزاری پایه مانند سیستم‌های متقارن و نامتقارن برای تایید هویت و زمرنگاری داده‌ها باشد[۸].

- **پروتکل‌های ارتباطی امن و کارآمد**: برخلاف سیستم‌های ارتباطی سنتی، ارتباطات در شبکه‌ی هوشمند دارای محدودیت‌های زمانی و امنیتی می‌باشند، به خصوص در قسمت توزیع و انتقال. این دو محدودیت در گاهی مواقع حتی با یکدیگر دچار تداخل نیز می‌شوند. اگر در برخی از موارد دستیابی به هر دوی این نیازمندی‌ها به صورت کامل و همزمان ممکن نباشد، باید توازن بهینه‌ای میان امنیت اطلاعات و بهره‌وری ارتباطات در طراحی شبکه‌ی سیستم هوشمند ایجاد نمود.

۶. دسته بندی تهدیدات علیه شبکه هوشمند انرژی

حملات مخرب ممکن است باعث ایجاد آسیب‌های مصیبت بار در منابع تغذیه و قطع گسترده انرژی شوند که از موارد بسیار حساس در سیستم هوشمند انرژی است. برشمردن تمامی انواع حمله‌ها به علت گسترده و پیچیده بودن شبکه در سیستم هوشمند ممکن نمی‌باشد، به همین دلیل ما حملات مخرب را به سه دسته‌ی عمده با توجه به دسترس پذیری، صحت و حفظ اسرار، تقسیم‌بندی می‌کنیم:

- حملاتی که دسترس پذیری را مورد هدف قرار می‌دهند که انکار پاسخ دهی (Denial of Service=DoS) نیز خوانده می‌شود و تلاش می‌کنند تا باعث تاخیر، توقف و یا اختلال در ارتباطات سیستم هوشمند شوند[۲۱-۲۲].
- حملاتی که صحت را مورد هدف قرار می‌دهند و تلاش می‌کنند تا عمدا و به صورت غیر قانونی داده‌های موجود در سیستم را تغییر داده و یا دچار اختلال کنند.
- حملاتی که حفظ اسرار را مورد هدف قرار می‌دهند و سعی می‌کنند تا داده‌های غیر غیر مجاز را از منابع شبکه در سیستم هوشمند به دست آورند.

۷. روشهای تشخیص حملات سایبری در شبکه هوشمند انرژی

۱،۷. سیستم کنترل شبکه توزیع شده

سیستم کنترل شبکه توزیع شده یک سیستم کنترلی است که حلقه های کنترل یک شبکه بلادرنگ را محصور کرده است. امکانات ارتباطی و محاسباتی را با نظارت و کنترل موجودیت های فضای فیزیکی تکمیل می کند. این سیستم ها معمولا بوسیله عوامل شبکه شده ترکیب می شوند که شامل حسگرهای توزیع شده، محرک های توزیع شده، کنترل کننده های توزیع شده و شبکه ارتباطی هستند[۲۳].

ریشه سیستم های کنترل به سال ۱۸۶۸ بر می گردد، زمانیکه تحلیل های حرکتی گریز از مرکز گاورنر، توسط فیزیکدان مشهور جی.سی.ماکسول انجام شد. بیشترین دستاوردهای چشمگیر در سیستم های کنترل مرسوم، زمانی اتفاق افتاد که برادران رایت پرواز خودشان را در سال ۱۹۰۳ با موفقیت انجام دادند.

۲,۷. شبکه توافق

شبکه توافق دارای سه سیستم فیزیکی مستقل است. در این شبکه هر عامل یک کنترل کننده محلی و یک مدیر توافق دارد. کنترل کننده محلی به صورت ثابت وضعیت اطلاعاتش را به مدیر توافق گزارش کرده و با عوامل همسایه همراه با سایرین به وسیله شبکه ارتباطی مذاکره می کند. مدیر توافق یک نتیجه توافق را محاسبه کرده و آنرا به کنترل کننده محلی برمی گرداند و عمل خود را براساس نتیجه توافق تنظیم می نماید. سپس کنترل کننده محلی وضعیت جدید خودش را به مدیر توافق گزارش می دهد. مادامی که سیستم کار می کند، این روند ادامه می یابد[۱۸-۲۲].

۸. نتیجه گیری

از آنجاییکه شبکه های هوشمند انرژی، شبکه های به هم پیوسته و دوسویه می باشند که در آن اطلاعات نقش بنیادی در فرایند توزیع انرژی ایفا می کند ، لذا بایستی آسیب پذیری این شبکه ها در مقابل حمله های سایبری مورد توجه قرار گیرد. بنابراین در این مقاله سعی گردید ضمن مطالعه مختصر پیرامون شبکه هوشمند انرژی و تبیین ویژگی های آن، چالش های مرتبط با امنیت سایبری در شبکه هوشمند و انواع تهدیدات و روشهای تشخیص حملات سایبری در شبکه های هوشمند مورد ارزیابی و بررسی قرار گیرد.

منابع

[1] R. Langner, S. Stuxnet: Dissecting a cyberwarfare weapon. Security & Privacy, IEEE, 9(3), pp. 49-51, 2015.
[2] A.A. Cardenas, S. Amin, and S. Sastry, Secure control: Towards survivable cyber-physical systems. System, 1(a2), 2018.
[3] M. Amin, Security challenges for the electricity infrastructure. Computer, 35(4), pp. -10, 2012.
[4] W. Zeng, and M.-Y. Chow. A trade-off model for performance and security in secured Networked Control Systems. in Industrial Electronics (ISIE), ۲۰۱۱IEEE International Symposium on IEEE, 2014.
[5] F. Pasqualetti, A. Bicchi, and F. Bullo, Consensus computation in unreliable networks: A system theoretic approach. Automatic Control, IEEE Transactions on, 57(1), pp. 90-104, 2017.
[6] W. Ren, and R.W. Beard, Consensus algorithms for doubleintegrator dynamics. Distributed Consensus in Multi-vehicle Cooperative Control: Theory and Applications, pp. 77-104, 2018.
[7] A. Jadbabaie, J. Lin, and A.S. Morse, Coordination of groups of mobile autonomous agents using nearest neighbor rules. Automatic Control, IEEE Transactions on, 486), pp. 9-1001, 2013.
[8] L. Xiao, and S. Boyd, Fast linear iterations for distributed averaging. Systems & Control Letters, 53(1), pp. 65-78, 2016.
[9] A. Bartoli, J. Hern´andez-Serrano, M. Soriano, M., Dohler, A. Kountouris, D. Barthel, *"Secure Lossless Aggregation Over Fading & Shadowing Channels For Smart Grid M2M Networks*", IEEE Transactions on Smart Grid, Vol. 2, No. 4, 2011.
[10] S. Buchegger, J.L. Boudec, *"Performance Analysis of the CONFIDANT Protocol"*, In Proceedings of the 3rd ACM International Symposium on Mobile Ad hoc Networking & Computing, ACM, 2012.
[11] G.M. Coates, K.H. Hopkinson, S.R. Graham, S.H. Kurkowski, *"Collaborative Trust-Based Security Mechanisms for a Regional Utility Intranet"*, IEEE Transaction on Power Systems, Vol. 23, No. 3, 2008.
[12] C.H. Hauser, D.E. Bakken, I. Dionysiou, "*Security, trust, and QoS in next-generation control and communication for large power systems",* Journal of Critical Infrastructures, Vol. 4, No. 1, 2018.
[13] T. Jiang, I. Matei, J.S. Bara, *"A Trust Based Distributed Kalman Filtering Approach for Mode Estimation in Power Systems"*, First Workshop on Secure Control Systems, 2015.
[14] E. Johansson, T. Sommestad, M. Ekstedt, "*Issues of Cyber Security in SCADA Systems on the Importance of Awareness",* The 20th International Conference on Electricity Distribution (CIRED), 2019.

[15] Y.Yan, et al. "A survey on cyber security for smart grid communications." IEEE Communications Surveys & Tutorials (2018).
[16] A. Wang, G. Wenye, and K. Zhuo Lu. "Cyber security in the Smart Grid: Survey and challenges." Computer Networks, 57(5), pp.1344-1371, 2014.
[17] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," IEEE Communications Surveys & Tutorials, vol. 14, pp. 998-1010, 2018.
[18] ICS CERT Team, "ICS-CERT year in review", URL: https://ics-cert.uscert. Gov/Year-Review-2016, 2016.
[19] T. Sommestad, G. N. Ericsson, and J. Nordlander, "SCADA system cyber security: A comparison of standards," in IEEE Power and Energy Society General Meeting, pp. 1-, 2016.
[20] W. Jin, D. Kundur, and T. Zourntos",On the use of cyber-physical hierarchy for smart grid security and efficient control," 25th IEEE Canadian Conference in Electrical & Computer Engineering (CCECE), pp. 1-6, 2016.
[21] P. D. Ray, R. Harnoor, and M. Hentea, "Smart power grid security: A unified risk management approach", IEEE International Carnahan Conference on Security Technology ICCST 2010, pp. 276-285, 2018.
[22] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," IEEE Transactions on Smart Grid, vol. 2, pp. 326-333, 2017.
[23] A. Tóth, Á. Werner-Stark, and K.M. Hangos. "A structural decomposition-based diagnosis method for dynamic process systems using HAZID information." Journal of Loss Prevention in the Process Industries, pp. 97-104, 2019.