کارگاه های آموزشی مرکز اطلاعات علمی جهاد دانشگاهی

کارگاه آنلاین آشنایی با پایگاه های اطلاعات علمی بین المللی و ترفند های جستجو

کارگاه آنلاین
پروپوزال نویسی و پایان نامه نویسی

کارگاه آنلاین
بررسی مقابله ای متون (مقدماتی)

No. F-15-AAA-0000

ارائه معماری‌ای جهت پایش امنیتی طرح فهام با استفاده از سیستم‌های تشخیص نفوذ به همراه برآورد اقتصادی اجرای آن

هانیه خسروی[۱]، سوفیا آهنج[۲]
گروه زیرساخت مخابراتی
پژوهشگاه نیرو
تهران، ایران
h.khosravi@aut.ac.ir[1], sahanj@nri.ac.ir[2]

چکیده — سیستم زیرساخت اندازه‌گیری پیشرفته (AMI) یک سیستم یکپارچه شامل نرم‌افزارها، سخت‌افزارهای دیجیتالی، شبکه و بستر مخابراتی است که قابلیت‌هایی نظیر امکان ارتباط دو طرفه با مشترکین، قرائت، نظارت و کنترل از راه دور دستگاه‌های اندازه‌گیری، جمع‌آوری، مدیریت، پردازش و تحلیل اطلاعات جمع‌آوری شده و تولید گزارش‌های لازم را فراهم می‌آورد. امنیت AMI مسئله‌ای بسیار با اهمیت است. به منظور جلوگیری از حملات، سوءاستفاده از آسیب‌پذیری‌های سیستم و هزینه‌های سنگین ناشی از آن‌ها باید راه‌حلی جامع ایجاد شود؛ که بخشی از آن توسعه روش‌های نظارتی است. در این مقاله، به بررسی نیازمندی‌های عملی برای نظارت بر طرح فراسامانه هوشمند اندازه‌گیری و مدیریت انرژی (فهام) از طریق جانمایی سیستم تشخیص نفوذ می‌پردازیم و در نهایت به برآورد هزینه‌های این معماری پیشنهادی خواهیم پرداخت.

واژه‌های کلیدی — سیستم تشخیص نفوذ؛ زیرساخت اندازه‌گیری پیشرفته؛ امنیت سایبری؛ دستگاه‌های اندازه‌گیری هوشمند.

۱. مقدمه

با گسترش روز افزون استفاده از انرژی الکتریکی و با افزایش درخواست مصرف کنندگان برای داشتن انرژی با کیفیت و با قابلیت اطمینان بالا و با گسترش کاربران این نوع انرژی، طیف وسیعی از مصرف‌کنندگان و دستگاه‌های اندازه‌گیری وارد شبکه‌های توزیع برق شده‌اند. مدیریت این پهنه وسیع مشترکان، نیاز به قرائت دستگاه‌های اندازه‌گیری، صدور صورت‌حساب، مدیریت قطع و وصل شدن اتصال مشترکان، مدیریت شبکه در ساعات اوج مصرف و نیاز به ویژگی‌های خاص برای کنترل مصرف کاربران و مشترکان، همچنین نیاز به نظارت دقیق و بلادرنگ بر نحوه مصرف کاربران، مدیران این حوزه را بر آن داشته تا از سیستم‌های هوشمند برای برآورده کردن اهداف خود بهره جویند. به این منظور امکانات لازم برای ایجاد AMI[1] در جهت ایجاد شبکه هوشمند در ایران در حال فراهم آمدن و پیاده‌سازی است. تحقق این مسئله در پروژه‌ای با عنوان فراسامانه هوشمند اندازه‌گیری و مدیریت انرژی (فهام) صورت گرفته که پیاده‌سازی آن بر عهده سازمان بهره‌وری انرژی ایران (سابا) می‌باشد.

۱.۱. اجزای طرح فهام

شکل ۱ اجزا و واسط‌های ارتباطی مورد نیاز طرح فهام را نشان می دهد. اجزای اصلی به شرح زیر هستند:

الف) کنتور برق/هاب مخابراتی: این دستگاه برای مقاصد نگه‌داری و بهره‌برداری از طریق واسط ارتباطی MI3 به تجهیز عملیات و تعمیر و نگه‌داری متصل می‌شود. این تجهیز علاوه بر اندازه‌گیری برق به عنوان یک هاب مخابراتی عمل می‌کند و از طریق واسط MI4 برای ذخیره‌سازی و انتقال اطلاعات کنتورهای آب و گاز به کار گرفته می‌شود. ارتباط آن با

[1] Advanced Metering Infrastructure

تجهیز انتهایی سمت مشترک نیز از طریق واسط ارتباطی MI5 برقرار می‌شود. کنتور برق/هاب مخابراتی به صورت از راه دور توسط سیستم مرکزی مدیریت می‌شود که این مدیریت می‌تواند به صورت مستقیم از طریق شبکه WAN و توسط واسط ارتباطی MI2 انجام شود یا به صورت غیر مستقیم از طریق جمع‌کننده داده و واسط ارتباطی MI1 صورت پذیرد.

ب) تجهیزات عملیات و تعمیر و نگه‌داری: تجهیزات دستی و قابل حملی هستند که به منظور تبادل اطلاعات با تجهیزات در زمان نصب آن‌ها یا در فرآیند نگه‌داری آن‌ها به کار می‌روند. این تجهیزات از طریق واسط ارتباطی MI3 و CI4 به صورت محلی به ترتیب به کنتور برق و جمع کننده داده متصل می‌شوند. هم‌چنین این تجهیزات در زمانی که دسترسی از راه دور به تجهیزات اندازه‌گیری وجود ندارد برای عملیات تعمیر و نگه‌داری یا قرائت آن‌ها به کار می‌روند.

ج) کنتورهای متصل به کنتور برق/هاب مخابراتی: تجهیزات هوشمند اندازه‌گیری هستند که برای اندازه‌گیری میزان مصرف آب و گاز مورد استفاده قرار می‌گیرند. این کنتورها از طریق واسط ارتباطی MI4 به کنتور برق/هاب مخابراتی متصل شده و به این ترتیب با سیستم مرکزی ارتباط برقرار می‌کنند.

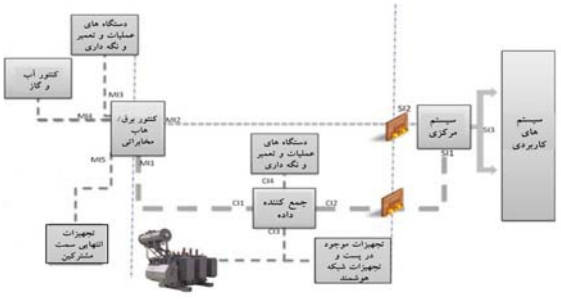
د) تجهیزات انتهایی سمت مشترکین: تجهیزات کمکی هستند که می‌توانند به کنتور برق/هاب مخابراتی متصل شوند و با آن تبادل اطلاعات کرده یا مقادیر مصرف و سایر اطلاعات را به مشترک نشان دهند. این ارتباط از طریق واسط ارتباطی MI5 برقرار می‌شود.

ه) جمع کننده داده: تجهیز واسطی است که بین کنتور برق/ هاب مخابراتی و سیستم مرکزی قرار می‌گیرد. هدف اصلی از به کارگیری آن جمع‌آوری و مدیریت اطلاعات دریافتی از کنتورهای برق/هاب مخابراتی به صورت مستقیم و کنتورهای آب و گاز و تجهیزات انتهایی سمت مشترکین به صورت غیر مستقیم می‌باشد. این اطلاعات از طریق واسط ارتباطی CI1 جمع‌آوری شده و سپس از طریق واسط ارتباطی CI2 مربوط به شبکه WAN به سیستم مرکزی ارسال می‌شوند. فرمان‌های کنترلی، برنامه‌ریزی، پیکربندی مجدد و سایر دستوراتی که از سیستم مرکزی صادر می‌گردند با استفاده از CI1-MI1 به کنتور برق/هاب مخابراتی می‌رسند. هم‌چنین جمع‌کننده داده دارای واسط ارتباطی CI4 برای اتصال به تجهیزات عملیات و تعمیر و نگه‌داری نیز می‌باشد. همچنین، یک اتصال به تجهیزات موجود در پست توزیع و تجهیزات شبکه هوشمند نیز با استفاده از واسط ارتباطی CI3 وجود دارد.

و) تجهیزات موجود در پست و تجهیزات شبکه هوشمند: این تجهیزات با استفاده از واسط ارتباطی CI3 به جمع کننده داده متصل می‌شوند. آن‌ها می‌توانند برای عملکرد آینده شبکه هوشمند که نیازمند کنترل، نظارت و ارتباط با حسگرهای مختلف است به کار گرفته شوند.

ز) سیستم مرکزی: این سیستم از طریق واسط ارتباطی SI3 با سیستم‌های کاربردی ارتباط برقرار می‌کند و مسئولیت مدیریت تمام اطلاعات و داده‌های مرتبط با فهام مانند پیکربندی، کنترل و بهره‌برداری از تمام اجزای سیستم با استفاده از واسط‌های ارتباطی SI1 و SI2 را بر عهده دارد. عملیات بر روی رویدادها و هشدارها و مدیریت بهره‌برداری ارتباطات سیستم نیز بر عهده آن می‌باشد. در بسیاری از موارد سیستم مرکزی دستوراتی را از سیستم‌های کاربردی دریافت می‌کند که باید عملکرد صحیح و به موقع آن‌ها تضمین شود. این دستورات شامل قرائت پارامترهای مختلف، پیکربندی اجزای تشکیل دهنده دستگاه‌های میدانی، قطع از راه دور و غیره می‌باشند. ممکن است سیستم مرکزی برخی از وظایف خود را به جمع کننده داده محول کند. سیستم مرکزی شامل دو زیرسیستم AHE[۲] و MDM[۳] می‌باشد. AHE مدیریت اطلاعات و شبکه مخابراتی WAN و LAN، مدیریت تمام تجهیزات موجود در شبکه، ثبت تجهیزات موجود در شبکه و مدیریت تعمیر و نگه‌داری آن‌ها را بر عهده دارد. MDM تمام اطلاعات به دست آمده از AHE را مدیریت و بایگانی می‌کند.

ح) سیستم‌های کاربردی[۴]: شامل سیستم‌های فنی و تجاری هستند که یا در حال حاضر وجود دارند یا برنامه‌ای برای ایجاد آن‌ها موجود است. این سیستم‌ها عبارتند از سیستم ثبت کنتورها، سیستم تنظیم تعرفه، سیستم صدور صورت‌حساب، سیستم مدیریت انرژی، سیستم مدیریت خاموشی و غیره که فرآیندهای موردنیاز بهره‌برداران انرژی را انجام می‌دهند. ارتباط این سیستم‌ها با سیستم مرکزی از طریق واسط ارتباطی SI3 انجام می‌شود. [۱]



شکل ۱: اجزا و واسط‌های ارتباطی طرح فهام.

[2] AMI Head End
3 Meter Data Management
[4] Legacy Systems

۱.۲. نیازمندی‌های نظارت بر AMI

نصب AMI افزایش قابل‌توجهی در میزان تهدیدات امنیتی ایجاد می‌کند. افزوده شدن زیرساخت مخابراتی و توانایی‌های پردازشی دستگاه‌های AMI همراه با دسترسی فیزیکی به دستگاه‌های اندازه‌گیری هوشمند راه‌های جدیدی برای نفوذ به سیستم ایجاد می‌کنند. از میان اهدافی که مهاجمین در حمله به AMI دنبال می‌کنند می‌توان به سرقت اطلاعات حساس، سوءاستفاده از زیرساخت مخابرات و اختلال در سرویس‌ها به منظور اخاذی، خرابکاری و فعالیت‌های تروریستی اشاره کرد. [۲]

۱.۲.۱. مهم‌ترین نگرانی‌های امنیتی درباره AMI

مهم‌ترین نگرانی بیان شده توسط صنایع مختلف در فازهای متفاوت نصب AMI – در حال برنامه‌ریزی، در آغاز کار و در مرحله تکمیل شده – پایین بودن امکان کنترل بر روی دستگاه‌های AMI است. در حقیقت، دستگاه‌های اندازه‌گیری به همراه جمع کننده‌ها آسیب‌پذیرترین مولفه‌ها در مقابل نفوذ سایبری به وسیله یک مهاجم خارجی هستند و این در حالی است که سیستم‌های نقطه ابتدایی (AHE)[5] و دسترسی فروشندگان آسیب‌پذیرترین نقاط در برابر حملات داخلی هستند. صنایع مختلف نگرانی‌های خود درباره AMI را با توجه به رویدادهای امنیتی که در ادامه بیان شده‌اند توضیح می‌دهند:

- قطع گسترده از راه دور بدون مجوز.
- دستکاری دستگاه‌ها: تزریق کد مخرب و بدافزار (مثلا از طریق حملات سرریز بافر)، الصاق دستگاه‌های سرکش، دستکاری دستگاه‌های اندازه‌گیری، دسترسی به کلمه عبور سفت‌افزارها و حملات روز-صفر به دستگاه‌های AMI.
- مسائل رمزنگاری: دسترسی به کلیدهای رمزگشایی یا کشف معایب رمزنگاری.
- حمله منع خدمت (DoS)[6] به مسیریاب‌ها و رله‌های سلولی.
- اصلاحات بدون مجوز بر روی پیکربندی سیستم و مولفه‌های فیزیکی.

امکان ایجاد رویدادهای امنیتی فوق و پیامدهای سیاسی، اجتماعی و اقتصادی آن نیاز به ارائه یک راه‌حل جامع امنیت به منظور جلوگیری از این تهدیدات را الزامی می سازد. استفاده از راه‌حل جامع نظارت می تواند گامی موثر در رفع این نگرانی‌ها باشد. این راه‌حل جامع نظارتی می‌تواند با استفاده از حسگرهای تشخیص نفوذ (IDS) و پایش مرکزی آن‌ها صورت گیرد. مسلما پایش کامل شبکه و رسیدن به یکپارچگی و سلامت کامل دستگاه‌های AMI نیازمند نظارت بر تمامی دستگاه‌ها است که ممکن است هزینه بالایی داشته باشد. در ادامه ابتدا درباره IDS، انواع آن و نحوه عملکرد آن به طور مختصر توضیحاتی ارائه می‌شود. سپس به بررسی چگونگی برخورد صنایع با این فناوری پرداخته خواهد شد و در نهایت راه‌حلی جامع برای طرح فهام ارائه خواهد شد. [۲]

۲. سیستم تشخیص نفوذ

تشخیص نفوذ به فرآیند نظارت بر رویدادهایی که در سیستم رایانه یا شبکه رخ می‌دهند و تجزیه و تحلیل آن‌ها به منظور یافتن مشخصاتی از حوادث محتمل گفته می‌شود. [۳] یک IDS از قسمت‌های مختلفی تشکیل شده است که عبارتند از: ۱) حسگرها یا عوامل برای نظارت بر فعالیت‌ها و تجزیه و تحلیل آن‌ها؛ ۲) یک کارگزار[7] مدیریت برای متمرکز کردن اطلاعات جمع‌آوری شده به وسیله حسگرها یا عوامل و مدیریت این اطلاعات؛ ۳) یک کارگزار پایگاه داده برای ذخیره تمامی داده‌های جمع‌آوری شده به وسیله حسگرها و تولید شده توسط کارگزار مدیریت؛ و ۴) یک کنسول به منظور فراهم آوردن واسطی برای کاربران و مدیران، به این ترتیب مدیران خواهند توانست وضعیت سیستم تحت نظارت، هشدارها، رویدادهای تحت بازرسی را بررسی و سیستم را پیکربندی کنند.

فرآیند تشخیص فعالیت‌های مخرب بر مبنای سه روش مجزا انجام می‌شود:

۱. شناسایی مبتنی بر امضا: این روش شامل جست‌وجوی الگوهای رفتار مخرب با استفاده از یک پایگاه داده از امضاهای از قبل تعریف شده حملات است؛

۲. شناسایی بر مبنای ناهنجاری: در این روش انحراف از پروفایل‌های از قبل تعریف شده رفتار عادی با استفاده از اندازه‌گیری‌های آماری تشخیص داده می‌شود؛

۳. شناسایی بر مبنای مشخصات: این روش شامل شناسایی انحراف از پروفایل‌های از قبل تعریف شده از رفتار صحیح است. این پروفایل‌ها با استفاده از مشخصات منطقی تعریف می‌شوند.

5 AMI Head end
6 Denial of Service
7 Server

۲.۱. سیستم‌های تشخیص نفوذ مبتنی بر شبکه و میزبان

یک IDS مبتنی بر شبکه در قسمت‌های خاصی از شبکه بر ترافیک نظارت دارد و با هدف شناسایی فعالیت‌های مشکوک به تجزیه و تحلیل پروتکل‌های شبکه، انتقال و کاربرد می‌پردازد. اصولا NIDSها با محدودیت‌هایی روبرو هستند که از آن جمله می توان به موارد زیر اشاره نمود: ۱) عدم توانایی در تجزیه و تحلیل ترافیک رمزنگاری شده شبکه؛ ۲) در صورت قرار گرفتن تحت شرایط بار سنگین نمی‌توانند تجزیه و تحلیل کاملی انجام دهند یا به طور کلی از کار می‌افتند. [۳]

حسگرهای تشخیص نفوذ می‌توانند علاوه بر ترافیک شبکه بر اطلاعات یک رایانه میزبان نیز مانند یکپارچگی فایل‌ها، رویدادنگارهای برنامه‌های کاربردی و فراخوانی‌های سیستم نظارت داشته باشند که در این صورت به آن‌ها سیستم‌های تشخیص نفوذ مبتنی بر میزبان (HIDS)[8] گفته می‌شود. در مقایسه با NIDSها، HIDSها غالبا دارای این مزیت هستند که می‌توانند به علت اصلی حملات دسترسی پیدا کنند. اما این IDSها دو محدودیت مهم دارند: ۱) معمولا سربار قابل توجهی به رایانه میزبان تحت نظارت می‌افزایند، و ۲) این امکان وجود دارد که سیستم عامل رایانه میزبان را پشتیبانی نکنند. به دلیل این دو محدودیت این نوع IDSها می‌توانند به صورت مجزا بر روی لوازم نیز نصب شوند و بلافاصله در جلوی رایانه میزبان تحت نظارت قرار بگیرند.

۳.راه‌حل‌های صنعتی

اگرچه از قبل راه‌حل‌های نظارتی نظیر هشدار ضد دستکاری و قابلیت‌های رویدادنگاری توسط دستگاه‌های اندازه‌گیری هوشمند صورت می‌گرفت، ولی در کنار آن صنایع مختلف در حال سرمایه‌گذاری بر روی تکمیل این راه‌حل‌های نظارتی بوده‌اند. در حال حاضر شرکت‌های مختلفی بر روی ارتقاء این راه‌حل‌های نظارتی فعالیت می‌کنند. یک برآورد از ۱۵ فروشنده امنیتی پیشرو در این خصوص نشان می‌دهد که بیش‌تر این محصولات در دو گروه زیر جای می‌گیرند (شکل ۲):

۱- حسگرهای متمرکز تشخیص نفوذ مبتنی بر شبکه.

۲- مدیریت کننده‌های امنیتی رویدادها و اطلاعات (SIEM)[9].

شکل۲: درصد فروشندگان IDS برای محیط‌ها و فناوری‌های مختلف.

بیش‌تر این محصولات برای نظارت بر SCADA[10] طراحی شده‌اند؛ اما تعداد روزافزونی از آن‌ها امروزه قابلیت‌های تجزیه و تحلیل پروتکل‌های AMI و روش‌های داده‌کاوی برای پردازش رویدادهای AMI را نیز دارند. از آنجایی که در شبکه AMI بخش قابل‌توجهی از ترافیک از دستگاه‌های اندازه‌گیری به سمت نقطه ابتدایی (AHE) در جریان است لذا قرار دادن محصولات نظارتی در این دستگاه‌ها دارای اهمیت بسزایی است. اما با وجود اهمیت قرار دادن این محصولات برای نظارت در این بخش همواره ایده کاهش دادن هزینه‌ها با نصب تنها یک راه‌حل متمرکز به طور مثال در جمع کننده‌های داده در مقابل محدودیت دید نداشتن نسبت به رویدادهایی که در لبه شبکه (کنتورها) رخ می‌دهند، مطرح است. در صورت استفاده از راه‌حل‌های متمرکز کنونی تهدیداتی چون قطع ارتباط راه دور بدون مجوز که از منطقه میدانی سرچشمه می‌گیرند نمی‌توانند تشخیص داده شوند. وجود وقایع امنیتی مختلف نظیر حمله به دستگاه‌های اندازه‌گیری هوشمند در سال ۲۰۰۹ که منجر به دزدی گسترده برق شد [۴]، نیاز صنایع را برای راه‌حل‌های امنیتی‌ای که قابلیت فراهم آوردن آگاهی نسبت به تمامی قسمت‌های زیر ساخت را داشته باشند بیش از پیش مشخص نمود. در حال حاضر این شکاف امنیتی، یعنی نبود حسگرهای تشخیص نفوذ مبتنی بر میزبان جاسازی شده در دستگاه‌های AMI، وجود دارد و صنایع مختلف بر آن تاکید دارند؛ به همین علت بررسی یکپارچگی سفت‌افزار از راه دور و شناسایی دستگاه‌های در خطر امکان‌پذیر نیست.

به منظور یافتن دلایل عدم استفاده از حسگرهای تشخیص نفوذ مبتنی بر میزبان جاسازی شده در دستگاه‌های اندازه‌گیری AMI، پرسشنامه‌ای درباره "دستورالعمل و بهترین شیوه‌ها در پاسخ به حادثه AMI" تدوین گردید. پاسخ‌های صنایع به این پرسشنامه نشان می‌دهند که دلایل اصلی صنایع برای استفاده از راه‌حل‌های نظارت متمرکز و عدم استفاده از IDSهای توزیع شده در منطقه میدانی در این موارد خلاصه می‌شوند: مقرون به صرفه بودن، نبود امنیت کامل برای AMI، دشوار بودن یکپارچه‌سازی پروتکل‌های اختصاصی مخابرات (مثلا بیش‌تر فناوری‌های مخابرات در لایه‌های پایین‌تر اختصاصی هستند.). [۲]

8 Host-based Intrusion Detection System
9 Security Information and Event Manager

10 Supervisory Control And Data Acquisition

۴. دستورالعمل‌هایی برای یک IDS جامع و مقیاس‌پذیر برای AMI

بررسی مدل تهدید، نیازهای بیان شده توسط صنایع مختلف، راه‌حل‌های موجود که از سوی تامین کنندگان امنیت طرح شده‌اند و تحقیقاتی که اخیرا درباره نظارت بر AMI انجام شده است، بینشی درباره مشخصات یک IDS جامع برای AMI فراهم می‌آورد. این مشخصات عبارتند از:

۱- نصب IDS مبتنی بر میزبان در نقطه ابتدایی (AHE): قرار دادن تنها یک IDS مبتنی بر میزبان در نقطه ابتدایی (AHE) از نظر اقتصادی بسیار مقرون به صرفه است. این حسگر می‌تواند حملاتی که از شبکه AMI سرچشمه می‌گیرند و شبکه utility را هدف قرار می‌دهند و بالعکس و هم‌چنین حملات داخلی‌ای که در رویدادنگارها ردپایی به جا می‌گذارند را شناسایی کند. از میان حملاتی که این IDS قادر به تشخیص آن‌ها نخواهد بود می‌توان به نصب بدافزار بر روی دستگاه‌های اندازه‌گیری و استراق سمع ترافیک NAN[11] اشاره کرد. علت ناشناس ماندن این حملات عدم دسترسی به اطلاعاتی چون یکپارچگی سفت‌افزار دستگاه‌های اندازه‌گیری، محتوای حافظه آن‌ها، ترافیک NAN بین دستگاه‌های اندازه‌گیری و چگونگی استفاده از پهنای باند شبکه می‌باشد. ارسال اطلاعات محرمانه مشترکین و داده‌های خصوصی صنعت برق بر روی شبکه AMI، مخابرات امن بین مولفه‌های این شبکه و رمزنگاری را به مسئله‌ای ضروری تبدیل کرده است. بنابراین، با توجه به دسترسی نقطه ابتدایی (AHE) به تمامی کلیدهای رمزگشایی، یک مزیت به کارگیری این معماری این است که حسگر IDS نصب شده در نقطه ابتدایی (AHE) نیز می‌تواند بر روی ترافیک رمزگشایی شده تجزیه و تحلیل انجام دهد. [۵]

۲- نصب IDS مبتنی بر میزبان در دستگاه‌های اندازه‌گیری: نظارت بر سیستم عامل‌های جاسازی شده در دستگاه‌های نصب شده در منطقه میدانی با استفاده از سیستم‌های تشخیص نفوذ مبتنی بر میزبان حیاتی است. با به کارگیری این معماری بینشی جامع از ترافیکی که در شبکه AMI جریان دارد فراهم می‌آید. به علاوه، حسگرهای جاسازی شده می‌توانند حملاتی که از درون شبکه خانگی (HAN)[12] (مثلا از طریق یک دستگاه هوشمند به خطر افتاده) آغاز می‌شوند را شناسایی کنند. حملاتی که به طور مستقیم سیستم مرکزی یا مولفه‌های کنار دستگاه‌های اندازه‌گیری را هدف قرار می‌دهند، توسط حسگرهای دستگاه‌های اندازه‌گیری قابل شناسایی نیستند. هم‌چنین لازم است به این نکته نیز توجه شود که دستگاه‌های اندازه‌گیری توان پردازشی، ذخیره‌سازی و قابلیت‌های مخابراتی بسیار محدودی دارند. توان پردازشی محدود میزان تجزیه و تحلیلی که می‌تواند در هر حسگر انجام شود را محدود می‌کند. صنایع مختلف نیز تمایلی به پرداخت یک هزینه اضافی برای ارتقا سخت‌افزار میلیون‌ها دستگاه اندازه‌گیری هوشمند ندارند. بنابراین این حسگرها به صورت متناوب به بررسی یکپارچگی نرم‌افزار و سفت‌افزار دستگاه‌های اندازه‌گیری، محتوای حافظه و سطح سیگنال می‌پردازند و گزارش سلامتی خود را برای جمع کننده‌ها ارسال می‌کنند. [۵]

۳- نصب IDS مبتنی بر شبکه در جمع کننده‌های داده: یک حسگر IDS مبتنی بر شبکه با توان پردازشی و حافظه کافی برای پشتیبانی از فناوری‌های تشخیص مبتنی بر مشخصات حالت‌دار[13] نصب شود. این IDS می‌تواند هشدارهای ارسال شده از سوی دستگاه‌های اندازه‌گیری را تجمیع کند.

۴- نظارت با کمک لیست سفید: سیستم‌های تشخیص نفوذ مبتنی بر شبکه باید از طبیعت قطعی-یقینی مخابرات سیستم انرژی جهت پیاده‌سازی یک لیست سفید به منظور به دست آوردن دقت در شناسایی حملات ناشناخته استفاده نمایند. به این طریق نیاز به به‌روزرسانی‌های دوره‌ای تا حد زیادی کاهش خواهد یافت.

۵- تایید رسمی سیاست‌ها: توسعه‌دهندگان سیستم تشخیص نفوذ باید ابزارهای تایید کننده رسمی را برای اعتبارسنجی سیستم‌های تشخیص نفوذ مبتنی بر میزبان و شبکه به کار بگیرند. این ابزارها در بررسی طراحی سخت‌افزارهای سیستم‌های حیاتی استفاده می‌شوند و می‌توانند تضمین کنند که سیستم‌های تشخیص نفوذ نیازمندی‌های سیستم AMI را برآورده می‌نمایند.

۶- روش‌های تشخیص توزیع شده، هم‌بستگی و تجمیع مقیاس‌پذیر: معماری ناظر باید برای AMIها که از میلیون‌ها دستگاه ساخته شده‌اند مقیاس شود. این نیازمندی به مقیاس‌پذیری بالا به این معناست که فناوری‌های تشخیص توزیع شده نیز باید علاوه بر نقشه‌های جمع‌آوری هوشمند داده مورد توجه قرار بگیرند. نقشه‌های جمع‌آوری هوشمند داده عملگران را قادر می‌سازند که بدون دریافت تعداد زیادی هشدار از شرایط آگاهی پیدا کنند.

11 Neighborhood Area Network
12 Home Area Network
13 Stateful specification-based detection technology

۷- عملی بودن: در پایان، هر راه‌حل امنیتی که در محیط شبکه هوشمند نصب می‌شود باید با تقویت لایه‌های امنیتی و بدون تاثیر بر ماموریت هسته‌ای که همان تحویل انرژی است عملی باشد. [۲]

با مطالعه رهنمودهای ارائه شده در [۲]، یک معماری ناظر برای AMI می‌تواند به مولفه‌های زیر تجزیه شود:

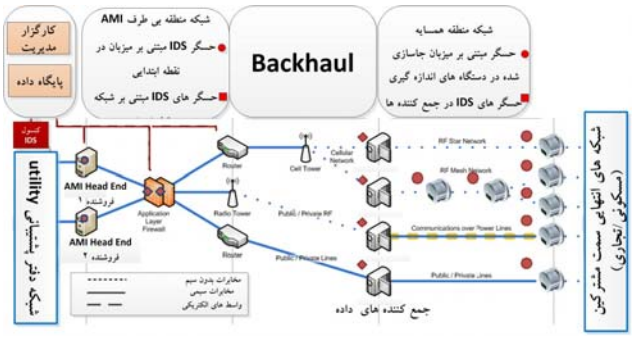
۱- حسگرها: مولفه‌های سخت‌افزاری و نرم‌افزاری برای دریافت، تجزیه و تحلیل فعالیت شبکه یا سیستم هستند. برای یک AMI، حسگرها باید در نقطه ابتدایی (AHE)، جمع کننده‌ها (DC)[۱۴] و دستگاه‌های اندازه‌گیری (کنتورها) نصب شوند. حسگرهای نقطه ابتدایی (AHE) حجم زیادی از ترافیک را پردازش می‌کنند و این در حالی است که حسگرهای درون دستگاه‌های اندازه‌گیری کمینه نیازمندی‌های محاسباتی را دارند.

۲- کارگزارهای مدیریت: اطلاعات تولید شده به وسیله حسگرها باید به یک یا چند کارگزار مدیریت ارسال شود. نقش کارگزارهای مدیریت ذخیره داده‌ها در یک پایگاه داده و اجرای فرآیند هم‌بسته‌سازی و تجمیع به منظور تشخیص نفوذهایی که به صورت موضعی قابل شناسایی نیستند، می‌باشد.

۳- کارگزار پایگاه داده: مخزنی برای اطلاعات مربوط به رویدادهایی که به وسیله حسگرها یا کارگزارهای مدیریت ضبط شده‌اند. ترکیب کارگزار مدیریت و کارگزار پایگاه داده غالبا مدیریت امنیتی رویدادها و اطلاعات (SIEM) نامیده می‌شود. یک SIEM می‌تواند رویدادهای امنیتی را از سایر حسگرها علاوه بر آن‌هایی که در AMI نصب شده‌اند رویدادنگاری کند.

۴- کنسول: واسطی که مدیران امنیتی می‌توانند برای پیکربندی سیستم‌های تشخیص نفوذ و نظارت بر وضعیت امنیتی AMI از آن استفاده کنند.

توپولوژی معماری نظارت همراه با موقعیت مولفه‌های مختلف AMI در شکل ۳ نشان داده شده است.



شکل ۳: شبکه AMI تجهیز شده با مولفه‌های IDS.

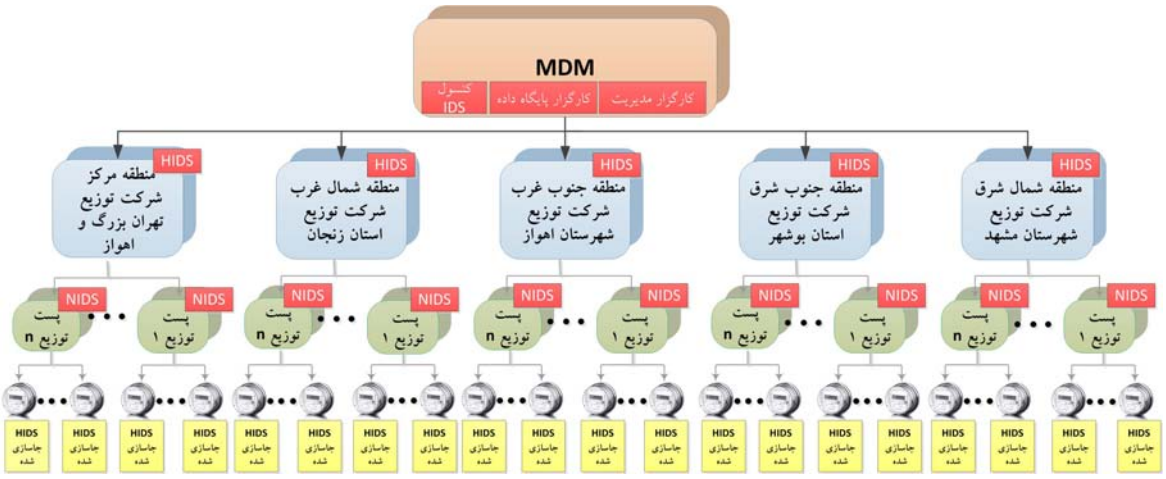
14 Data Collector

۵.معماری پیشنهادی نظارت بر طرح فهام با استفاده از IDS

معماری پیشنهادی نظارت بر طرح فهام در شکل ۴ نشان داده شده است. مطابق طرح فهام مشترکین در سطح کشور به پنج ناحیه شمال شرق، شمال غرب، جنوب شرق، جنوب غرب، تهران و البرز تقسیم شدند. بر اساس این طرح در هر یک از این مناطق یک AHE برای جمع‌آوری اطلاعات و برقراری ارتباط با دستگاه‌های اندازه‌گیری و جمع کننده‌های داده نصب خواهد شد. هر یک از این مراکز وظیفه کنترل و نظارت بر پست‌ها را در شبکه توزیع بر عهده دارند. در هر یک از پست‌ها یک جمع کننده مستقر می‌شود. بر اساس طرح فهام و مطالب ارائه شده در بخش ۴، در طرح پایش امنیتی فهام پیشنهاد می‌شود که بر روی هر یک دستگاه‌های اندازه‌گیری (کنتورها) یک IDS مبتنی بر میزبان جاسازی شده با قابلیت‌های پردازشی، ذخیره‌سازی و مخابراتی محدود نصب شده و بر روی هریک از جمع کننده‌های داده یک IDS مبتنی بر شبکه قرار گیرد. در هر یک از AHEها یک IDS مبتنی بر میزبان و یک IDS مبتنی بر شبکه در مسیر ارتباطی بین DC و AHE قرار داده شود.

با توجه به آمار تفصیلی سال ۹۱، تعداد مشترکین (دستگاه‌های اندازه‌گیری یا کنتور) در سراسر کشور ۲۷۱۵۸۰۰۰ و تعداد پست‌های توزیع ۵۱۰۵۰۵ پست گزارش شده است. بنابراین به منظور پایش امنیتی فهام با به کارگیری IDS، در سراسر کشور به پنج سیستم تشخیص نفوذ مبتنی بر میزبان با قابلیت پردازش بالا، ۵۱۰۵۰۵ سیستم تشخیص نفوذ مبتنی بر شبکه و ۲۷۱۵۸۰۰۰ دستگاه اندازه‌گیری (کنتور) تجهیز شده با سیستم تشخیص نفوذ مبتنی بر میزبان جاسازی شده و پنج سیستم تشخیص مبتنی بر شبکه با قابلیت پردازش بالا نیازمند خواهد بود.

بر اساس مطالعات انجام شده هزینه هر دستگاه اندازه‌گیری هوشمند ۷۶ دلار (۲۵۸۴۰۰ تومان) و هزینه‌های مربوط به نصب زیرساخت مخابراتی در بازه ۱۵۰~۱۲۵ دلار (تقریبا ۵۱۰۰۰۰~۴۲۵۰۰۰ تومان) برای هر دستگاه اندازه‌گیری تخمین زده شده است [۶] و هزینه‌های مربوط به امنیت سایبری حدود ۲۰٪ هزینه‌های AMI ارزیابی شده است که بر اساس گزارشات مربوطه بخش عمده این هزینه‌ها مربوط به پیاده‌سازی زیرساخت IDS و SIEM به وسیله صنایع مختلف در AMI است [۷]، در این صورت هزینه ایجاد امنیت سایبری شامل پیاده‌سازی IDS برای هر دستگاه اندازه‌گیری معادل ۴۰.۲~ دلار (تقریبا ۱۵۳۰۰۰~۱۳۶۰۰۰ تومان) و هزینه تجهیز تمامی دستگاه‌های اندازه‌گیری در سطح کشور ۱۲۲۷۵۴۱۶۰۰~۱۰۹۱۷۵۱۶۰۰ دلار



شکل ۴: معماری پیشنهادی به منظور پایش امنیتی طرح فهام .

(۴۱۵۵۱۷۴۰۰۰۰۰۰~۳۶۹۳۴۸۸۰۰۰۰۰۰ تومان) خواهد بود.

هم‌چنین بر اساس آمار ارائه شده در سال ۹۱ میزان انرژی برق فروخته نشده در اثر حادثه، ۲۱۹۷۵۰۰۰۰ کیلووات ساعت و هزینه تقریبی خاموشی در همین سال ۳۰۸۳ تومان به ازای هر کیلو وات ساعت برآورد شده است. بنابراین در این سال هزینه تلف شده ناشی از خاموشی در اثر حادثه ۶۷۷۴۸۹۲۵۰۰۰۰ تومان بوده است.

بنابراین از آنجا که با پیاده‌سازی تجهزات امنیتی بر روی دستگاه‌های اندازه‌گیری نه تنها امکان تشخیص حملات سایبری، خاموشی‌های ناشی از آن و جلوگیری از انتشار این حملات وجود دارد؛ بلکه با ایجاد یک سیستم نظارتی بر وضعیت سلامت دستگاه‌های اندازه‌گیری و تولید هشدار در صورت بروز هر گونه اختلال در عملکرد آن‌ها، جلوگیری یا برطرف کردن سریع‌تر خاموشی‌های رخ داده به علل مختلف امکان‌پذیر خواهد بود. بنابراین، حتی اگر تمام هزینه‌های مربوط به پیاده‌سازی امنیت به IDS مربوط باشد، با در نظر گرفتن هزینه‌های ناشی از خاموشی در اثر حادثه در یک سال، هزینه‌های پیاده‌سازی IDS بر روی تمامی دستگاه‌های اندازه‌گیری در سطح کشور حداقل در مدت حدود ۶ سال قابل بازگشت خواهد بود. این برآورد اقتصادی نشان می‌دهد که پیاده‌سازی این طرح نه تنها از لحاظ سیاسی و اجتماعی مثمر ثمر خواهد بود، بلکه به لحاظ اقتصادی نیز توجیه‌پذیر است.

۶. نتیجه‌گیری

در این مقاله اجزای طرح فهام، نیازمندی‌های نظارت بر AMI و راه‌حل‌های صنعتی موجود برای انجام این کار توضیح داده شدند. هم‌چنین به طور مختصر انواع سیستم تشخیص نفوذ، مزایا و معایب هر نوع بررسی شد. سپس به منظور پیاده‌سازی یک معماری ناظر بر AMI پیشنهاداتی ارائه شد، که از مهم‌ترین آنان می‌توان به ضرورت وجود IDSهای جاسازی شده در دستگاه‌های اندازه‌گیری (کنتورها) اشاره کرد. در پایان، با در نظر گرفتن مشخصات کمی و کیفی طرح فهام یک معماری ناظر بر این طرح با به کارگیری IDS به همراه برآورد اقتصادی ارائه شد.

منابع

[1] Available at: http://www.iransg.com/saba_content/media/image/2011/06/2203_orig.pdf
[2] Available at: http://www.energycollection.us/ Energy-Metering/ Intrustion-Detection-System.pdf
[3] K. Scarfone and P. Mell, “Guide to intrusion detection and prevention systems (idps),” NIST SP 800-94, vol. 800, pp. 94, 2007
[4] Avilable at: http://www.gao.gov/assets/600/592508.pdf
[5] D. Grochocki, “Deployment considerations for intrusion detection systems in advanced metering infrastructure,” Master thesis, University of Illinois, 2013.
[6] Available at: http://www.ferc.gov/eventcalendar/Files/20070423091846-EPRI%20-%20Advanced%20Metering.pdf
[7] Available at: https://www.smartgrid.gov/files/Estimating_Costs_Benefits_Smart_Grid_Preliminary_Estimate_In_201103.pdf

کارگاه های آموزشی مرکز اطلاعات علمی جهاد دانشگاهی

کارگاه آنلاین آشنایی با پایگاه های اطلاعات علمی بین المللی و ترفند های جستجو

کارگاه آنلاین
پروپوزال نویسی و پایان نامه نویسی

کارگاه آنلاین
بررسی مقابله ای متون (مقدماتی)