
بسم الله الرحمن الرحیم

به نام خدا

دانشگاه فردوسی مشهد
دانشکده مهندسی – گروه کامپیوتر

پایان نامه کارشناسی ارشد

ارائه پروتکل ارتباطی امن برای کنتورهای هوشمند برق

تهیه کننده:

قربانعلی فروغ

استاد راهنما :

دکتر محمدحسین یغمایی مقدم

زمستان ۱۳۹۱

تعهدنامه

اینجانب **قربانعلی فروغ** دانشجوی دوره دکتری/کارشناسی ارشد رشته **کامپیوتر** دانشکده **مهندسی** دانشگاه فردوسی مشهد نویسنده پایان‌نامه **پروتکل ارتباطی امن برای کنتورهای هوشمند برق** تحت راهنمایی **دکتر محمد حسین یغمایی مقدم** متعهد می‌شوم:

- تحقیقات در این پایان‌نامه توسط اینجانب انجام شده و از صحت و اصالت برخوردار است.
- در استفاده از نتایج پژوهشهای محققان دیگر به مرجع مورد استفاده استناد شده است.
- مطالب مندرج در پایان‌نامه تاکنون توسط خود و یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ جا ارائه نشده است.
- کلیه حقوق معنوی این اثر متعلق به دانشگاه فردوسی مشهد می باشد و مقالات مستخرج با نام "دانشگاه فردوسی مشهد" و یا "Ferdowsi University of Mashhad" به چاپ خواهد رسید.
- حقوق معنوی تمام افرادی که در به دست آمدن نتایج اصلی پایان‌نامه تاثیرگذار بوده‌اند در مقالات مستخرج از رساله رعایت شده است.
- در کلیه مراحل انجام این پایان‌نامه، در مواردی که از موجود زنده (یا بافتهای آنها) استفاده شده است ضوابط و اصول اخلاقی رعایت شده است.
- در کلیه مراحل انجام این پایان‌نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته یا استفاده شده است، اصل رازداری، ضوابط و اصول اخلاق انسانی رعایت شده است.

تاریخ

امضای دانشجو

مالکیت نتایج و حق نشر

- کلیه حقوق معنوی این اثر و محصولات آن (مقالات مستخرج، کتاب، برنامه‌های رایانه‌ای، نرم‌افزارها و تجهیزات ساخته شده) متعلق به دانشگاه فردوسی مشهد می‌باشد. این مطلب باید به نحو مقتضی در تولیدات علمی مربوطه ذکر شود.
- استفاده از اطلاعات و نتایج موجود در پایان‌نامه بدون ذکر مرجع مجاز نمی‌باشد.

چکیده

کنتورهای هوشمند برق بخش اساسی سیستم‌های AMI است که به منظور قرائت مصارف برق استفاده می‌گردد. این کنتورها ارتباط دو طرفه بین مشتری و شرکت برق را فراهم می‌کند. کنتورهای هوشمند گزارش مصرف را به صورت لحظه‌ای، روزانه، هفته و ماهانه محاسبه نموده و برق را به صورت دو طرفه بین مصرف کننده و شرکت برق کنترل می‌کند. در ساختار ارتباطی سلسله مراتبی این شبکه، تعدادی از کنتورها توسط یک مرکز (BAN) مدیریت می‌شود. با افزایش تعداد کنتورها در یک مرکز زمان پاسخگویی نیز افزایش یافته و باعث تأخیر زمان رمزگشایی/تصدیق پیام‌ها و سرریز شدن حافظه می‌گردد. از طرف دیگر محدودیت‌های منابع در مرکز باعث افزایش زمان رمزگشایی و تصدیق پیام‌ها و همچنین باعث سرریز شدن حافظه می‌گردد. با توجه به کارایی متفاوت الگوریتم‌های رمز و روش‌های احرازهویت زمان رمزگشایی پیام‌ها توسط هر الگوریتم نیز متفاوت است. در این پایان نامه پروتکل ارتباطی امن جهت کاهش بار ترافیکی در مرکز و استفاده بهینه از منابع موجود ارائه شده است. در نتیجه، پروتکل پیشنهادی با پروتکل‌های قبلی و حالت نرمال مقایسه گردیده است. بعد از تحلیل پیام‌های مورد نیاز، حافظه استفاده شده، تأخیر زمان رمزگشایی/ تصدیق پیام‌ها در الگوریتم‌های مختلف با تعداد کنتورهای متفاوت ارزیابی گردیده است.

کلمات کلیدی

ساختار سلسله مراتبی، الگوریتم‌های رمز، تحلیل پیام‌ها، محدودیت منابع، کارایی، سربار پیام‌ها، سرریز شدن حافظه، مقیاس پذیری و رمزگشایی/تصدیق پیام‌ها

فهرست مطالب

==========

فهرست اشکال IV

فهرست جداول V

فصل اول: مرور بر شبکه هوشمند برق ..... - ۱ -

۱-۱- مرور بر شبکه‌های هوشمند برق ..... - ۲ -

2-1- قیمت گذاری پویا ..... - ۴ -

۱-۲-۱ . سیستم‌های زیر ساخت اندازه گیر پیشرفته ..... - ۵ -

1-2-2. کنتورهای هوشمند برق ..... - ٦ -

نتیجه گیری ..... - ۷ -

فصل دوم: امنیت شبکه هوشمند برق ..... - ۸ -

2-1- بررسی امنیت در شبکه‌های هوشمند برق ..... - ۹ -

۲-۲- ریسک‌های شبکه هوشمند قدرت ..... - ۱۰ -

2-3- دانستن تهدیدات ..... - ۱۲ -

2-4- فرصت‌ها و چالش‌های فن آوری مخابرات بی سیم برای کاربردهای شبکه هوشمند برق ..... - ۱۳ -

۲-٤-۱- فن آوری ZigBee ..... - ۱۳ -

۲-۵- میزان اثر محرمانگی، صحت و در دسترسی ..... - ۱٤ -

۲-۵-۱- میزان اثر ..... - ۱۵ -

۲-۵-۲- میزان تأثیر برای طبقه‌های محرمانگی، صحت و در دسترسی ..... - ۱٦ -

۲-٦- انتخاب نیاز های امنیت ..... - ۱۸ -

2-7- هفت ناحیه برای مدل مرجع منطقی ..... - ۱۹ -

۲-۸- امنیت شبکه‌های حسگر بی سیم در شبکه هوشمند قدرت ..... - ۲۱ -

۲-۹- کاربردهای WSNsدر شبکه برق قدرت ..... - ۲۲ -

۲-۹-۱- عوامل امنیتی و تهدید در WSNs ..... - ۲۲ -

فصل سوم: امنیت در کنتورهای هوشمند برق ..... - ۲۴ -

3-1- بررسی چالش‌ها و نیاز های امنیتی ..... - ۲۵ -

۳-۲- کار های انجام شده ..... - ۲٦ -

3-3-1- ارزیابی سیستم‌های رمز نگاری ..... - ۳۰ -

3-3-2- حساسیت کلید در روش‌های متقارن و نامتقارن ..... - ۳٤ -

3-3-3- آسیب پذیری های رمزنگاری متقارن ..... - ۳٤ -
3-3-4- شیوه‌های رمز و آسیب پذیری آن‌ها ..... - ۳٦ -

نتیجه گیری ..... **- ۴۸ -**

فصل چهارم: پروتکل ارتباطی امن برای کنتورهای هوشمند برق ..... **- ۴۹ -**

٤-١- پروتکل ارتباطی امن برای کنتورهای هوشمند برق ..... - ٤٩ -
2-4- طراحی پروتکل ارتباطی امن برای کنتورهای هوشمند برق ..... - ٥١ -
3-4- بخش‌های اساسی پروتکل ارائه شده ..... - ٥٥ -
4 -4- اندازه، زمان بندی و تعداد پیام‌ها ..... - ٦٠ -
۴-۵- پروتکل پیشنهادی ..... - ٦٤ -
٤-٦- تحلیل پیام‌ها ..... - ٦٦ -
7-4-تحلیل و شناسایی مدیریت ارتباط ..... - ٦٩ -
۴-۸- امنیت پروتکل پیشنهادی ..... - ۷۰ -
9-4- ارزیابی پروتکل پیشنهادی ..... - ۷٦ -

نتیجه گیری ..... **- ۸۳ -**

فصل پنجم: ارزیابی و مقایسه ..... **- ۸۴ -**

۵-۱- مدل پیشنهادی شبکه ..... - ۸۵ -
2-5- اهداف ..... - ۸٦ -
4-5-نتیجه گیری و ارزیابی‌ها ..... - ۸۷ -
5-5- فاکتورهای موثر در کارایی پردازنده ..... - ۸۸ -
۵-۶- نتایج و سناریوهای ارزیابی ..... - ۹۰ -
7-5- سناریوی تحلیل پیام‌های مورد نیاز ..... - ۹٦ -
7-5- تحلیل سربار پیام‌ها ..... - ۱۰۲ -
8-5- مقایسه زائد الگوریتم‌ها در پیام‌های 32 بایتی و 64 بایتی ..... - ۱۰۵ -
9-5- کارایی و عبور دهی الگوریتم‌ها ..... - ۱۱۰ -
10-5- مقایسه تأخیر رمزگشایی در پروتکل پیشنهادی با حالت نرمال ..... - ۱۱۲ -
11-5- مقایسه حافظه استفاده شده ..... - ۱۱۸ -

نتیجه گیری ..... **- ۱۲۱ -**

فصل ششم ..... **- ۱۲۲ -**

نتیجه گیری ..... **- ۱۲۲ -**

کارهای آتی ..... **- ۱۲۵ -**

منابع و مآخذ: ..... - ۱۲٦ -

فهرست اشکال

==========

شکل ۱- ۱: نمونه‌ی شبکه هوشمند برق ..... - ۳ -

شکل ۱- ۲: شبکه ارتباطی در AMI ..... - ٦ -

شکل ۲- 1: تعامل حامی‌ها در ناحیه‌های مختلف شبکه هوشمند از طریق ارتباط امن [] .....

..... - ۱۹ -

شکل ۳- ۱: ساختار و تقسیم بندی الگوریتم‌های رمز نگاری ..... - ۳۲ -

شکل ۵- ۱: مدل ارتباطی پیشنهادی با استفاده از فن‌آوری PLC ..... - ۸٦ -

شکل ۵- ۲: مقایسه بار ترافیکی در BAN مبتنی بر AES-128 (تعداد، مجموع اندازه و تأخیر رمزگشایی پیام‌ها) ..... - ۹۱ -

شکل ۵- ۳: مقایسه تأخیر رمز گشایی روش‌های قبلی با پروتکل پیشنهادی ..... - ۹۵ -

شکل ۵- ۴: الف- مقایسه سربار در پروتکل پیشنهادی و حالت نرمال مبتنی بر پیام‌های ۳۲ و ۶۴ بایتی ..... - ۱۰۸ -

شکل ۵- ۵: ب – مقایسه سربار با در نظر داشت ECDSA-256مبتنی بر پیام‌های ۳۲ و ۶۴ بایتی ..... - ۱۰۹ -

شکل ۵- ۶: مقایسه رمز گشایی مبتنی بر رمز و رمزگشایی اطلاعات روی تک هسته و دو هسته ..... - ۱۱۱ -

شکل ۵- ۷: مقایسه رمز گشایی مبتنی بر اجرای بینچ مارک روی تک هسته و دو هسته ..... - ۱۱۱ -

شکل ۵- ۸: مقایسه تأخیر پروتکل پیشنهادی با حالت نرمال و روش قبلی مبتنی بر پیام ..... - ۱۱۲ -

شکل ۵-۹: مقایسه پروتکل پیشنهادی و حالت نرمال در الگوریتم DES و 3DES ..... - ۱۱٦ -

شکل ۵-۱۰: مقایسه پروتکل پیشنهادی و حالت نرمال در الگوریتم AES-128 و CAMELLIA-128 ..... - ۱۱٦ -

شکل ۵- ۱۱: مقایسه پروتکل پیشنهادی و حالت نرمال در الگوریتم RC4 و AES-128..... - ۱۱۷ -

شکل ۵- ۱۲: مقایسه پروتکل پیشنهادی و حالت نرمال در الگوریتم ECDSA 256,192 ..... - ۱۱۷ -

شکل ۵- ۱۳: مقایسه حافظه استفاده شده مطابق به روش‌های قبلی، تمام پیام‌های شبکه و پروتکل پیشنهادی .... - ۱۱۸ -

شکل ۵ -14مقایسه دو حالت نرمال و پیشنهادی با روش ECDSA-256 ..... - ۱۱۹ -

شکل ۵- ۱۵: مقایسه حافظه استفاده شده مبتنی بر پروتکل پیشنهادی و حالت نرمال..... - ۱۲۰ -

فهرست جداول

==========

جدول ۲- ۱: انواع فن‌آوری‌های بی سیم با قابلیت‌ها، نرخ داده و فضای پوشش. [۴] ..... - ۱۳ -

جدول ۲- ۲: سطوح اثر با از دست دادن محرمانگی، صحت و در دسترسی در شبکه هوشمند قدرت [۵] ..... - ۱۷ -

جدول ۲- ۳: خلاصه نیازهای امنیتی واسطها [۵] ..... - ۲۰ -

جدول ۴- ۱: زمان بندی، داده اصلی، سربار پیام و تعداد پیام‌های شبکه BAN با فرض ۴۰۰ کنتور در ثانیه..... - ۶۱ -

جدول ۴- ۲: زمان بندی، داده اصلی، سربار پیام و تعداد پیام‌های اولویت اول با فرض ۴۰۰ کنتور در ثانیه ..... - ۶۲ -

جدول ۴- ۳: زمان بندی، داده اصلی، سربار پیام و تعداد پیام‌های اولویت دوم با فرض ۴۰۰ کنتور در ثانیه ..... - ۶۲ -

جدول ۴- ۴: مجموع بار ترافیکی با بلاک‌های ۳۲ بایتی پیام‌های اولویت دوم با فرض ۴۰۰ کنتور در ثانیه..... - ۶۳ -

جدول ۴- ۵: مجموع بار ترافیکی با بلاک‌های ۳۲ بایتی پیام‌های اولویت اول با فرض ۴۰۰ کنتور در ثانیه ..... - ۶۳ -

جدول ۴- ۶: جدول پیشنهادی پیام‌های اولویت دوم ..... - ۶۵ -

جدول ۴- ۷: جزئیات پیام‌های اولویت دوم با توجه به اندازه اولیه، نوع پیام و محتویات آن [۱۴, ۱۷-۱۹, ۳۵] ..... - ۶۸ -

جدول ۵- ۱: جدول ارزیابی کارایی ECDSA با طول کلیدهای متفاوت مبتنی بر پردازنده تک هسته‌ی ۲ گیگاهرتز ... - ۹۲ -

جدول ۵- ۲: جدول ارزیابی کارایی ECDSA با طول کلیدهای متفاوت مبتنی بر پردازنده ۱۶۰ میگاهرتز..... - ۹۳ -

جدول ۵- ۴: حد اقل پیام‌های مورد نیاز در شبکه BAN..... - ۹۷ -

جدول ۵- ۳: جدول میانگین رمزگشایی الگوریتم‌ها ..... - ۹۵ -

جدول ۵- ۵: پیام‌های اولویت دوم با فرض ۴۰۰ کنتور در یک ثانیه ..... - ۹۹ -

جدول ۵- ۶: پیام‌های اولویت دوم در بازه زمانی ۶۰ ثانیه ..... - ۱۰۰ -

جدول ۵- ۷: حد اقل پیام‌های مورد نیاز در شبکه BAN، در بازه زمانی ۶۰ ثانیه..... - ۱۰۰ -

جدول ۵- ۸: پیام‌های اولویت اول در شبکه BAN، برای پاسخگویی در زمان ۶۰ ثانیه ..... - ۱۰۲ -

جدول ۵- ۹: زائد برای اندازه‌های متفاوت پیام‌ها نظر به الگوریتم‌های مختلف ..... - ۱۰۳ -

جدول ۵- ۱۰: سربار برای پیام‌های ۳۲ بایتی مبتنی بر CAMELLIA-128، AES-128 و SEED..... - ۱۰۶ -

جدول ۵- ۱۱: سربار برای پیام‌های ۶۴ بایتی مبتنی بر CAMELLIA-128، AES-128 و SEED..... - ۱۰۷ -

جدول ۵- ۱۲: جدول زمان رمزگشایی مبتنی بر پیام ..... - ۱۱۲ -

فصل اول

مقدمه

صنعت نیروی برق مشابه به سکتورهای صنعتی دیگر، با بعضی از چالش‌ها درگیر است. شبکه هوشمند برق از یک سو درگیر افزایش تقاضا برای انجام عملیات سیستم‌های باهم متصل و پیچیده است. از سوی دیگر درگیر کنترل ساختار صنعت برق با توجه به انحصار در آوردن بازار برق می‌باشد. همه این پیچیده‌گی‌ها در روند شبکه هوشمند قدرت تأثیر گذاشته و امنیت آن را پیچیده‌تر ساخته است.

شبکه هوشمند قدرت شبکه‌های اتوماسیون[1] را از حالت منسوخ شده، اختصاصی و شبکه محصور[2] به عرصه فن آوری اطلاعات حاضر انتقال داده است.

همراه با پیاده سازی شبکه هوشمند برق اهمیت فن آوری اطلاعات[3] و زیر ساخت مخابرات در مطمئن ساختن و امنیت سکتور برق افزایش یافته است. بنابراین جهت امنیت شبکه هوشمند برق به امنیت سیستم‌ها، اطلاعات در فن آوری اطلاعاتی و زیر ساخت مخابرات پرداخته می‌شود. ممکن درگیر شدن فن‌آوری اطلاعات با سکتور مخابرات بعضی آسیب‌پذیری‌های امنیتی را بو جود آورد. امّا استانداردهای امنیتی سایبر برای شناخت و ارزیابی آسیب‌پذیری‌ها؛ راه حل‌های را معرفی می‌نماید.

تحقیقات نشان می‌دهد که احتمال آسیب پذیری امنیتی وجود دارد و بعضی خلاهای امنیتی در شبکه‌های هوشمند قدرت مشاهده شده است.

---

[1] Automation Networks
[2] Closed Network
[3] Information Technology (IT)

دانشمندان مرکز IOActive طی سال‌های گذشته تست‌های گسترده خود را روی دستگاه‌های شبکه هوشمند برق انجام دادند تا از احتمال آسیب‌پذیری امنیتی این شبکه مطلع شوند. به گفته «جاشوا پنل» مدیر مرکز IOActive، در پایان این بررسی‌ها دانشمندان حفره‌های زیادی را کشف کردند که به هکرها امکان می‌دهد به این شبکه دسترسی پیدا کرده و جریان برق را قطع کند[۱].

تهدیدات امنیتی به صورت عمده توسط پیچیده‌گی سیستم‌ها، گسترش داده‌ها، استفاده از افزایش دستگاه‌ها، افزایش نقاط ورودی در مسیرها و همچنان ممکن توسط بعضی نرم افزارهای بدخواه نیز معرفی گردد.

با توجه به تهدیدات علیه سیستم‌های هوشمند قدرت، یک هدف مهم توسعه استانداردهای امنیت سایبر است. با این حال، تجربه گذشته نشان می‌دهد که پروتکل‌های امنیتی متمایل به طراحی خطاها هستند و خطاها را مهیا می‌کند. شبکه هوشمند قدرت باید در برابر طیف گسترده‌ای از تهدیدهای امنیتی مانند هکرها، تروریست‌های سایبر، کشورهای سرکش و نیز از اقدامات غیر عمدی حفاظت شوند.

۱–۱– مرور بر شبکه‌های هوشمند برق

شبکه هوشمند قدرت، ابزارآلاتی به دستگاه‌های شبکه، پست‌ها و خطوط انتقال می‌افزاید تا حجم انبوهی از داده‌ها را جمع آوری، پردازش و در نهایت به صورت یک شبکه خودکار عمل کند. شبکه هوشمند قدرت با استفاده از فن‌آوری دیجیتال دو طرفه، انرژی را از تولید کنندگان به مشتریان منتقل می‌کند. هدف از این کار کنترل وسایل منازل مصرف کنندگان، صرفه جویی در مصرف انرژی است. علاوه بر این هزینه کاهش می‌یابد، قابلیت اطمینان و شفافیت نیز ارتقا می‌یابد.

شبکه هوشمند یک مسئله منفرد و مجزا نیست، بلکه مجموعه‌ای کامل از فن‌آوری‌های است که در ایجاد یا ارتقاء شبکه برق بکار می‌رود. این شبکه با استفاده از دستگاه‌های دیجیتال ردگیری مصرف و

نحوه مصرف در زمان اوج (پیک) را مراقبت می‌نماید. همچنین کنترل استفاده انرژی در خانه یا ساختمان به نحوی انجام می‌دهد که در صورت امکان دستگاه‌های پرمصرف در اوج مصرف خاموش شوند.

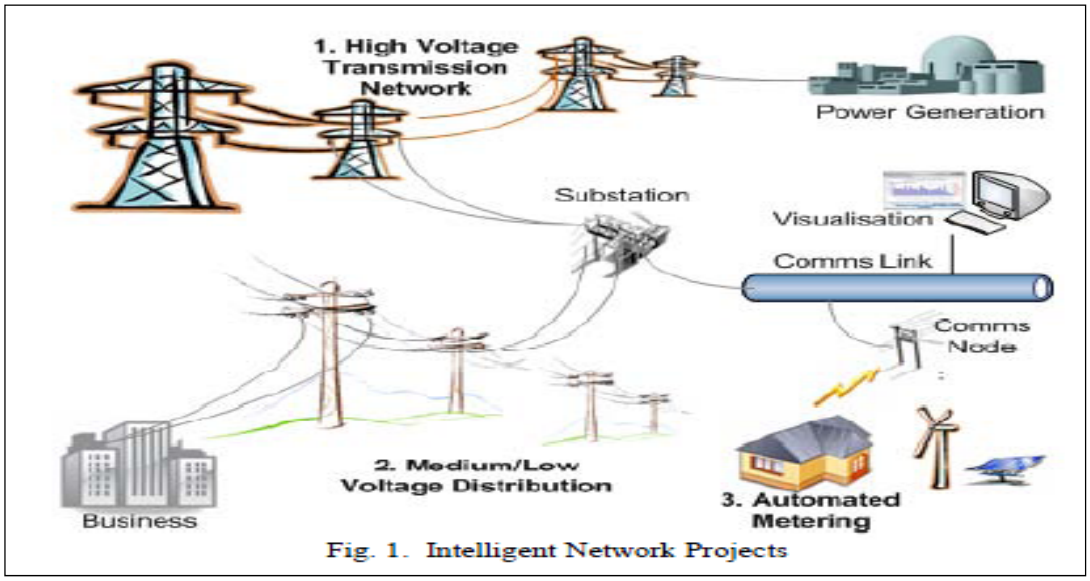


Fig. 1. Intelligent Network Projects

شکل ۱- ۱: نمونه‌ی شبکه هوشمند برق

شبکه هوشمند می‌تواند سیستم‌های مراقبتی در داخل ساختمان داشته باشد و به مصرف کنندگان اجازه دهد تا مصرف انرژی خود را بهتر مدیریت کنند. حتی امکان منابع انرژی مستقل برای شبکه‌های هوشمند وجود دارد. منابع انرژی مستقل مانند صفحه‌های شمسی خانه یا سیستم‌های زمین گرمایی منازل؛ اجازه می‌دهند تا انرژی خود را به شبکه تزریق نمایند. شکل ۱-۱ نمونه‌ی شبکه هوشمند برق را نشان می‌دهد.

اصلی‌ترین هدف تأمین برق مطمئن و پاسخ گوئی به نیازهای رو به رشد مشتریان با کمترین خسارت به محیط زیست است .فن آوری هوشمند توانایی ایجاد تغییرات اساسی در تولید، انتقال، توزیع و استفاده از انرژی الکتریکی همراه با منافع اقتصادی و محیطی دار. این شبکه با برآورده نمودن نیازهای مشتریان و

در دسترس بودن برق مطمئن و پایدار، استفاده از جمع آوری اطلاعات در زمان بحرانی، تصمیم‌گیری می‌نماید و از خاموشی‌های ناخواسته جلوگیری می‌کند.

ابعاد مختلفی در مورد منافع وجود چنین شبکه در نظر گرفته شده است. مصرف کننده مایل است بداند؛ چه زمانی قیمت برق بالاتر و چه زمانی پایین‌تر است و به این صورت مصرف خود را بهینه کند. مشتری مایل است در طول روز قیمت برق را بداند و تولید کننده برق تماس بگیرد که برق در خانه شما قطع است و یا این امکان را به مصرف کنندگان بدهد تا گام‌های اولیه را انجام دهد. مصرف کنندگان مایل است که قطع برق را یک‌بار هم تجربه نکند، چرا که شبکه هوشمند برق قدرت، پیش از اتفاق افتادن این امر، راه حل برای مدیریت آن دارد. مصرف کننده مایل است خودروهای برقی خود را در هر جا برق لازم را ذخیره کند. همه‌ی این چیزها با یک شبکه‌ی هوشمند مطمئن و امن در دسترس خواهند بود.

۱-۲- قیمت گذاری پویا

قیمت گذاری پویا یکی از انگیزه‌های اقتصادی و پاسخگویی به مصرف کننده است. همچنین جهت تشویق و انگیزه مشتریان به نام «تقاضا مشارکت« و یا پاسخ به درخواست‌ها است. قیمت گذاری پویا با استفاده از فن‌آوری است که مشتری با اطلاعات قیمت گذاری برای مدت زمان فعلی یا آینده تصمیم می‌گیرند. قیمت گذاری پویا برای مشتری امکان تغیر تقاضا را مطابق به اطلاعات قیمت گذاری می‌دهد.

بخش‌های قیمت گذاری پویا شامل:

- قیمت گذاری زمان استفاده[1]: قیمت انرژی از پیش تعیین شده نسبت به زمان اوج بیشتر است.

[1] Time-of-use pricing

- قیمت گذاری زمان اوج مصرف[1]: حساس‌ترین ساعت و اوج قیمت‌ها شناسایی شده و میزان قیمت‌ها بسیار بالاتر برای این ساعت‌ها تعیین شده است. با این حال قابل مقایسه با تعداد ساعت کمتر نسبت به قیمت گذاری زمان استفاده است.
- قیمت گذاری زمان واقعی[2]: قیمت انرژی در واحد زمان با توجه به مصرف ابزار متفاوت است.

دسترسی مصرف کنندگان به اطلاعات مربوط به انرژی: مصرف کنندگان به اطلاعات قیمت گذاری دسترسی دارند. شرکت‌های در حال توسعه ابزارهای نظارتی و برنامه‌های کاربردی نرم افزاری را در اختیار مصرف کنندگان قرار می‌دهند تا مصرف کنندگان قادر به نظارت مصارف خود از طریق این ابزارها باشند. نمونه‌ای این ابزارها شامل: Google's PowerMater, Microsoft's Hohm و GridPointهستند.

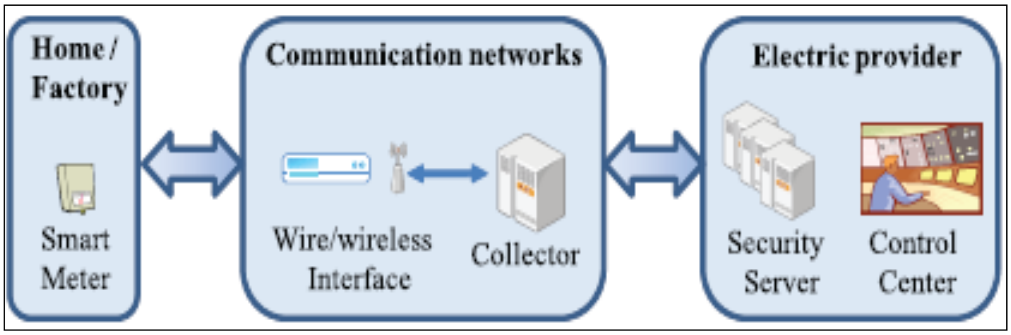
۱-۲-۱. سیستم‌های زیر ساخت اندازه گیر پیشرفته

سیستم زیرساخت اندازه گیر پیشرفته یکی از ساختارهای عمومی در شبکه‌های هوشمند برق است. این سیستم‌ها اطلاعات بهره‌وری و درخواست انرژی را به سرویس دهندگان و مصرف کنندگان فراهم می‌کند. مطابق شکل ۱-۲؛ مبادله داده در کنتورهای هوشمند از طریق شبکه‌های ارتباطی به صورت زمان واقعی انجام می‌گیرد. کنتورهای هوشمند و شبکه‌های ارتباطی سرویس‌های زیر ساخت اندازه گیر پیشرفته را فراهم می‌کند. کنتورهای هوشمند در سیستم‌های اندازه گیر پیشرفته چهار وظیفه اساسی زیر را انجام می‌دهد:

۱. نظارت و ثبت در خواست‌ها
۲. واقعه نگاری رخدادها در ارتباط به قدرت «مثلاً قطع برق»
۳. ارائه اطلاعات ورودی به سیستم و استفاده از اطلاعات تصدیق کننده بالا[1]

[1] Critical peak pricing
[2] Real-time Pricing

۴. تحویل و دریافت پیام‌های کنترل مثال، کنترل لوازم هوشمند خانگی، قطع از راه دور و غیره ((



شکل ۱- ۲: شبکه ارتباطی در AMI

۱-۲-۲. کنتورهای هوشمند برق

کنتور هوشمند برای این طراحی شده است که برق به صورت موثر و کار آمد انتقال داده شود. به بیان دیگر دستگاه گزارش در سایت هر مشتری بنام کنتور هوشمند یاد می‌شود. کنتورهای هوشمند بجای کنتورهای برقی کامپیوتری شده هستند و برای خروج اطلاعات چندین خانه، به بیرون متصل است.

هر کنتور هوشمند حاوی پردازنده، ذخیره گاه فراموش شده نی[۲] و سهولت‌های مخابراتی است. گرچه در بسیاری توصیه‌ها کنتور هوشمند و وظایف آن مشابه به نوع قبلی ساده گفته‌اند ولی این‌ها با روش‌های گذشته خیلی زیاد موثر ساخته شده است. کنتورهای هوشمند می‌تواند موارد استفاده روزانه را تعقیب کند، از طریق برنامه نرم افزاری مصرف کننده را قطع کند و یا در صورت مشکل اعلام خطر را به هردو سایت ارسال کند. همچنین کنتور هوشمند برای کنترل وسایل هوشمند برقی از واسط[۳] مستقیم استفاده می‌نماید. علاوه بر آن کنتورها تمام درخواست‌های مصرف کنندگان را در زمان مناسب به مرکز ارسال و پاسخ مربوطه را دریافت می‌نماید. گزارش خرابی، قطع، هشدارها، گزارش مصرف لحظه‌ای، ساعت، روزانه، ماهانه و غیره نیز توسط این دستگاه ارسال و دریافت می‌گردد. بنابراین داده‌ها و پیام‌های ارسالی توسط

---

[1] Verifier
[۲] Nonvolatile Storage
[3] Interface

این دستگاه به مرکز ارسال و از مرکز جواب مربوطه دریافت می‌گردد. علاوه بر آن پیام‌های نظارت و کنترل جهت امنیت و ارسال وضعیت‌های بحرانی به مرکز ارسال می‌شود. جزئیات بیشتر در مورد اندازه پیام‌ها، تعداد پیام‌ها و فیلدهای هر پیام‌ها در فصل چهارم بحث خواهد شد. با ارائه پروتکل ارتباطی امن برای کنتورهای هوشمند برق در نظر است، تعداد کنتورهای هوشمند در شبکه BAN، اندازه بار ترافیکی و منابع مورد نیاز را بررسی نمایم.

نتیجه گیری

ظهوری شبکه هوشمند برق با بعضی نیازمندی‌ها باعث تغیرات بنیادی گردید. این نیازمندی‌ها شامل: شبکه توزیع خود بازیاب، شبکه توزیع نیروی برق دوستدار محیط زیست، کنترل غیر متمرکز و فراگیر با استفاده از گسترش حسگرها و ابزارهای اندازه گیری و غیره است. یکی از اهداف دیگر بکار گیری اتوماسیون و کاهش عامل انسانی است که با فراهم شدن شبکه هوشمند برق لحاظ می‌شود.

منابع تجدید پذیر و کنترل غیر متمرکز از ویژگی‌های دیگر این شبکه است که شبکه را بیشتر قابل اعتماد ساخته است. هر مصرف کننده از طریق پورتال خانگی صورت مصرف و قیمت لحظه‌ی را ملاحظه می‌کند. شبکه توزیع نیرو با کمترین هزینه و استفاده بهینه از دارایی‌های با ارزش[1] با به‌کارگیری مفهوم پاسخ به در خواست علاقه‌مندی مشتریان را بیشتر می‌سازد.

[1] Asset

فصل دوم

امنیت در شبکه‌های هوشمند برق

مقدمه

همراه با پیاده سازی شبکه هوشمند برق اهمیت فن آوری اطلاعات و زیر ساخت مخابرات در مطمئن ساختن و امنیت سکتور برق افزایش یافته است. بنابراین امنیت شبکه هوشمند به امنیت سیستم‌ها، اطلاعات در فن آوری اطلاعات و زیر ساخت مخابرات بسته است. ممکن درگیر شدن فن آوری اطلاعات با سکتور مخابرات بعضی آسیب‌پذیری‌های امنیتی را در اول بو جود آورد. امّا استانداردهای امنیتی سایبر برای شناخت و ارزیابی آسیب‌پذیری‌ها برنامه‌ی را بو جود میاورد.

تحقیقات نشان می‌دهد که احتمال آسیب‌پذیری امنیتی وجود دارد و بعضی خلأهای امنیتی در شبکه‌های هوشمند قدرت مشاهده شده است. دانشمندان مرکز IOActive طی سال‌های گذشته تست‌های گسترده خود را روی دستگاه‌های شبکه هوشمند برق انجام دادند تا از احتمال آسیب‌پذیری امنیتی این شبکه مطلع شوند. «جاشوا پنل» مدیر مرکز IOActive در پایان این بررسی‌ها گفته‌اند که دانشمندان حفره‌های زیادی را کشف کردند که به هکرها امکان می‌دهد به این شبکه دسترسی پیدا کرده و جریان برق را قطع کند [۴] ،[۲]. تهدیدات امنیتی به صورت عمده توسط پیچیده‌گی سیستم‌ها، گسترش داده‌ها، استفاده از افزایش دستگاه‌ها، افزایش نقاط ورودی در مسیرها و همچنان توسط بعضی نرم افزارهای بدخواه نیز معرفی می‌گردد.

این فصل شامل بررسی امنیت در شبکه هوشمند برق، دانستن تهدیدات، انواع حملات، فرصت‌ها و چالش‌های فن آوری مخابرات بی سیم، اهداف امنیت سایبر، سطوح اثر، واسطهای منطقی و نیازهای امنیتی توصیه شده را بررسی می‌کنیم. همچنین امنیت شبکه حسگر در شبکه هوشمند در این فصل بحث گردیده است.

۲-۱- بررسی امنیت در شبکه‌های هوشمند برق

دستگاه‌های شبکه هوشمند قدرت در اصل کامپیوترهای کوچکی هستند که به کاربران و شرکت‌های تأمین کننده انرژی برق امکان می‌دهند که جریان برق مصرفی را بهتر کنترل کنند. در حال حاضر حدود 2میلیون عدد از این دستگاه‌ها مورد استفاده قرار گرفته است که پیش بینی می‌شود طی سال‌های آتی بر تعداد آن‌ها افزوده شود.

سازمان IOActiv و مرکز مستقل تحقیقات امنیتی"Travis Goodspeed"دریافتند که دستگاه‌های شبکه هوشمند قدرت می‌توانند کدهای مخرب را گسترش دهند. در زمینه هکرها کدهای مخرب را منتشر می‌کنند. در این صورت دستگاه‌های هوشمند برق مورد سوءاستفاده قرار گرفته و جریان برق از راه دور قطع می‌شود. از طرف دیگر امنیت باید در تمام چرخه حیات و مراحل توسعه سیستم شامل طراحی، پیاده سازی، نگهداری، تغیر مکان و غیره حفظ شود. یعنی در همه فازها باید به آن توجه شده و امنیت لازم بر قرار و پایدار بماند. امنیت سایبر نه تنها حملات عمدی کار بران داخل موسسه، عوامل جاسوسی صنعتی، تروریست‌ها دانسته شده است؛ بلکه حملات دیگر مانند سازش‌ها غیر عمدی از زیرساخت اطلاعات به دلیل خطاهای کاربر، خرابی تجهیزات و بلاهای طبیعی نیز است.

با پذیرش اطلاعات و فن‌آوری‌های مخابراتی در شبکه هوشمند و یکپارچگی سایبر و سیستم‌های اطلاعاتی، مسایل بی شماری امنیتی بر می‌خزد. هر سیستم پیچیده، آسیب پذیری و چالش‌های دارد؛

شبکه هوشمند قدرت نیز از این امر مستثنا نیست. در شبکه هوشمند قدرت افزایش تعامل و یکپارچگی سیستم‌ها تأثیر گذاشته است. بنابراین سیستم‌های اطلاعاتی، ارتباطات دو مسیره و حفاظتی امنیتی را بیشتر مشکل می‌سازد. همچنین فن آوری ارتباطی بی سیم مانند، GPRS /CDMA , 3G/4G, WiFi, WiMaxو ZigBee در سیستم‌های شبکه هوشمند قدرت وسیعاً پذیرفته شده بوده و یا پذیرفته شده خواهند بود. این فن‌آوری‌ها در کنتورهای هوشمند، دستگاه‌های هوشمند سیار و حسگرهای هوشمند وسیعاً استفاده شده است. تنوع این فن‌آوری‌ها محیط ارتباطات را زیاد پیچیده ساخته و مشکلات حفاظت امینی را افزایش می‌دهد. بعضی چالش‌های امنیت شبکه هوشمند بسیار مشابه به شبکه‌های سنتی است، امّا بیشتر درگیر پیچیده‌گی‌های اثر متقابل[1] است. بعضی فن‌آوری‌های جدید مانند شبکه‌های حسگر بی سیم، رایانش ابری[2] و معماری سرویس‌های تضمین شده (SOA[3])نیز باعث چالش‌های امنیتی شده است.

۲-۲- ریسک‌های شبکه هوشمند قدرت

پیچیدگی سیستم‌ها، استفاده از فن‌آوری‌های مختلف ریسک و تهدیدات امنیتی را افزایش داده است. علاوه بر آن تعداد سهامداران و عملیاتی حساس به زمان خطرات امنیتی را افزایش داده‌اند. در وسیع‌ترین مفهوم آن، امنیت سایبر برای صنعت برق پوشش دادن تمام مسائل اتوماسیون و مخابرات است. سیستم‌های اتوماسیون و مخابرات بر اساس عملیات سیستم‌های قدرت[4] است که در نتیجه عملکرد مدیریت آب، برق و فرآیندهای تجاری انجام می‌شود. البته در اصل همه موارد حمایت از مشتری است. در صنعت برق، تمرکز در اجرای تجهیزات باعث بهبودی سیستم قدرت شده است.

[1] Interaction
[2] Cloud Computing
[3] Service-oriented architecture
[4] Power Systems

تا این اواخر، مخابرات و تجهیزات فن آوری به طور معمول به عنوان حمایت کننده قابلیت اطمینان برای سیستم قدرت دیده می‌شد. با این حال این بخش به طور فزاینده‌ای برای قابلیت اطمینان سیستم‌های قدرت در حال حیاتی شدن است. با استثناء مشکلات اولیه اساساً تجهیزات قدرت شکست‌های مداوم و آبشار مربوط به مشکلات موجود است. همچنین شکست زیرساخت‌های فن آوری اطلاعات مربوطه به هر گونه حملات هکری، تروریستی و یا اینترنتی نه بوده است. شکست می‌تواند ناشی از حوادث غیر عمدی، اشتباهات، رعایت نکردن هشدارهای کلیدی و طراحی ضعیف باشد. بنابراین سازش غیر عمدی نیز باید نشانه گیری شود و روی همه رویکرد خطرات تمرکز شود. همچنین آسیب پذیری ممکن است به منظور نفوذ گری در شبکه، دسترسی به نرم افزارهای کنترلی و تغییر بی ثبات کردن شرایط بار[1] شبکه باشد. آسیب پذیری ممکن است هرگونه روش‌های غیر قابل پیش بینی را به مهاجم اجازه دهد. ریسک‌های اضافی شبکه شامل:

۱. افزایش پیچیده‌گی‌های شبکه ممکن آسیب‌پذیری‌ها را معرفی کند و افشاء بالقوه برای مهاجم و خطاهای غیر عمدی را افزایش دهد.

۲. وابستگی شبکه‌ها می‌تواند آسیب‌پذیری‌های متداول را معرفی کند

۳. افزایش آسیب پذیری ممکن است اختلال در ارتباطات و معرفی نرم افزار بدخواه[2] / فرم‌ویر و یا باعث سازش سخت افزار در نتیجه حمله DoSفراهم شود.

۴. افزایش تعداد نقاط ورودی و مسیرها باعث بهره برداری و دسترسی دشمنان می‌شود.

۵. سیستم‌های به هم پیوسته می‌تواند مقدار از اطلاعات خصوصی را در معرض افزایش ریسک قرار دهد. به ویژه زمانی که داده‌ها تجمیع[3] می‌شوند.

[1] Load Condition
[2] Malicious
[3] Aggregated

۶. استفاده از افزایش فن‌آوری‌های جدید می‌تواند آسیب‌پذیری‌های جدید را افزایش دهد.

۷. گسترش مقدار داده‌ها به صورت بالقوه باعث مصالحه و افشای داده‌های محرمانه می‌شود. در این صورت ممکن است باعث نقض حریم خصوصی مشتری شود.

۲-۳- دانستن تهدیدات

تطبیق سطح امنیتی مختص به سیستم ترکیبی و پیچیده یک چالش بزرگ است که ابزارهای امروز به آن روبرو است. این چالش‌ها به دلیل امنیتی افزایش داده شده است. همزمان با فراهم کردن سرویس رسانی به افراد غیر مسئول و لحاظ شدن امنیت کاری دشوار است. با این فطرت که امنیت همیشه یک بازی «گربه و موش» است که تهدیدات جدید نیازمند روش‌های جدید امنیتی است. ایجاد استراتژی امنیتی نیاز به عمل بالانس[1] دارد. هر روش محدود کردن دسترسی باید با ماهیت دارایی[2] و محدودیت‌های اعمال شده بر کاربران و کارمندان با حقوق دسترسی سایبر همراه با بالانس سازی باشد.

شناختن انواع تهدیدات امنیتی سیستم مهم و موثر است. هر نوع مهاجم می‌تواند توسط سه فاکتور مشخص شود. همچنین بزرگ‌ترین تهدید تخصص، شکیبایی و تأمین مالی دانسته شده است [۳]

۱). تخصص ۲). تأمین مالی ۳). زمان

تهدیدات اولیه در شبکه هوشمند برق شامل هکر، خرابکار[3]، تروریست، کارمند ناراضی، حکومت یا سازمان، حریفان اقتصادی و در بعضی حالت‌ها مشتری نیز دانسته شده است.

[1] Balancing
[2] Asset
[3] Vandal