به نام خدا

دانشگاه صنعتی امیرکبیر(پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

گزارش سمینار کارشناسی ارشد

رشته مهندسی فناوری اطلاعات گرایش شبکه‌های کامپیوتری

عنوان

ارائه روشی برای سرویس امن چند پخشی در شبکه های ارتباطی ناهمگون شبکه های هوشمند

A secure multicast service in heterogeneous in smart grid networks

استاد راهنما:

جناب آقای دکتر خرسندی

وحید ذوالفقاری

۹۰۱۳۱۰۲۲

مهر ۱۳۹۱

چکیده

با گسترش روز افزون شبکه برق و تقاضا برای تامین توان الکتریکی نیاز به یک سیستم مدیریت یکپارچه‌ی متمرکز در شبکه برق را ضروری ساخت. در چند سال اخیر تلاشهای بسیار زیادی برای ایجاد چنین ساختار مدیریتی مناسبی انجام شده است که این تلاشها منتج به مفهومی به نام *Smart Grid* شده است. جوهره اصلی *Smart Grid* به زعم کارشناسان این حوزه همانا استفاده از فناوریهای پیشرفته اطلاعات و ارتباطات *ICT* برای مدیریت سریعتر و دقیق تر شبکه برق است. در حوزه زیر ساخت ارتباطی شبکه *Smart Grid* سرویسهای مختلفی باید ارائه شود که یکی از مهمترین و کلیدی ترین این سرویس ها سرویس چند پخشی است. عنوان این گزارش گویای مطالبی که در این گزارش دیده خواهد شد است : ارائه روشی برای سرویس امن چند پخشی در شبکه های ارتباطی ناهمگون شبکه های هوشمند . در این گزارش ابتدائاً مقدمه ای درباره خود شبکه های هوشمند و *vison* ای که ما برای آینده مان از آن برای خود تصویر کردیم ارائه داده ایم. سپس وضعیت فعلی شبکه برق در ایران را بررسی کرده ایم و بطور اجمالی بخشهایی از آن را که باید تغییرات عمده کند تا به هوشمندی لازم برای یک شبکه *Smart Grid* برسد بررسی کرده ایم.

در فصل سوم از گزارشی که حاصل سه تز دکترا ویک پایان نامه دوره ارشد است مطالبی را تحت عنوان زیرساخت ارتباطی شبکه های هوشمند آورده ایم. در این فصل سعی شده است پاسخ این سوال داده شود که : چه داده هایی قرار است در زیرساخت ارتباطی شبکه های هوشمند رد و بدل شود. در فصل چهارم به بخش " امن " عنوان گزارش پرداخته شده است، بدین معنی که امنیت در شبکه های هوشمند بعنوان اصلی ترین نیاز آن بررسی شده است. سپس کاربردهای چند پخشی در شبکه *Smart Grid* بطور کامل بررسی شده است و پروتکلهای مخصوص شبکه هوشمند که برای تبادل داده بین بخشهای مختلف طراحی شده است آورده شده است. بدلیل اینکه مبحث شبکه های هوشمند مبحث جدیدی است و هنوز در مرحله طراحی سرویسهایی که قرار است روی آن داده شود می باشد روال کار در بخش داده آن این است که از فناوریهایی که در شبکه های داده معمولی قبلاً پیشنهاد شده و استفاده شده است در شبکه جدید *Smart Grid* بکار گرفته شود. البته این بکارگیری می بایست ویژگیها و خصوصیات ویژه‌ی شبکه *SG* را در نظر بگیرد. از همین رو در فصل پنجم مروری بر الگوریتمهایی که در شبکه داده قبلاً ارائه شده است را آورده ایم. در انتها هم نتیجه گیری کار برای جمع بندی مطلب آورده شده است.

کلید واژگان:*شبکه های هوشمند برق، شبکه های ناهمگون، چند پخشی، امنیت در شبکه های هوشمند*

فهرست مطالب

فهرست شکل‌ها

فصل ۱

مقدمه

Smart grid گونه ای از فناوریهای دیجیتال مورد استفاده در شبکه های برق است. یک *SG* برق را از تولید کننده به مصرف کننده از طریق ارتباطات دیجیتال دوطرفه برای کنترل دستگاه های برقی در منازل مشتریان می رساند. با این کار در مصرف انرژی صرفه جویی می شود و هزینه ها کاسته و قابلیت اتکا و شفافیت افزوده می شود. در این نوع شبکه، شبکه‌ی برق با سیستمهای اندازه گیری و جمع آوری اطلاعات که شامل *smart meter* ها هستند تلفیق می شود. دولتهای بسیاری در این زمینه کار می‌کنند و از آن به عنوان راهی برای حل مشکل استقلال انرژی، گرمایش جهانی، و مسائل مقاومت در حالات بحرانی استفاده می‌کنند.

این مطلب مورد توافق همه است که شبکه های برق امروزی در جهان صنعتی تحت فشار زیادی است. این مطلب دلایل زیادی دارد از آنجمله فقدان خطوط انتقال جدید برای همراه شدن با رشد بار مصرفی و تولیدی برق، اپراتورهای در حال بازنشستگی، یکپارچه شدن با منابع انرژی تجدیدپذیر که خصوصیات توان و مسائل مختلف آن هنوز بخوبی شناخته نشده است. این فشارها ضرورت استفاده از سنسورهای داده که در کاربردهای متعددی مثل *power application*، *geographic scopes*، *patterns of consume* و غیره استفاده می شود را گوشزد می کند.

Smart grid می خواهد عملکردهای جدیدی را به شبکه ی برق فعلی اضافه کند. اگرچه این کار ریسکهای امنیتی جدیدی را ایجاد می کند. ما امروزه به مقدار زیادی به شبکه ی تامین برق مان وابسته هستیم که این وابستگی شبکه‌ی برق را به یک دارایی حیاتی برای ما تبدیل کرده است. اختلال در تامین توان الکتریکی تاثیرات اجتماعی بسیاری در بر خواهد داشت. امنیت شبکه‌ی برق یک مسئله‌ی بسیار مهم است. یکی از ابعاد مهم شبکه‌ی *smart grid* زیرساختهای ارتباطی آن است که امنیت آن از حوزه های فعال در پژوهش می‌باشد. خصوصاً موقعی که همه‌ی *component* ها شبکه می شوند تعداد نقاطی که می توان به سیستم شبکه ی برق دسترسی داشت افزایش می یابد. **[1]**

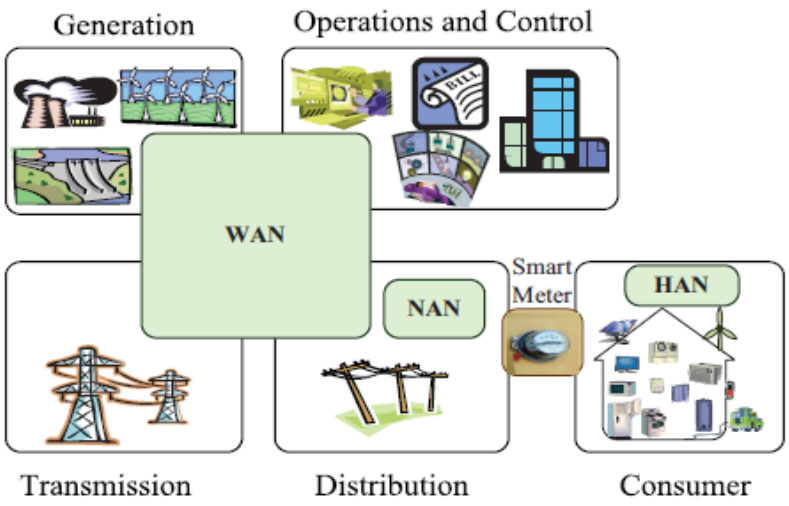
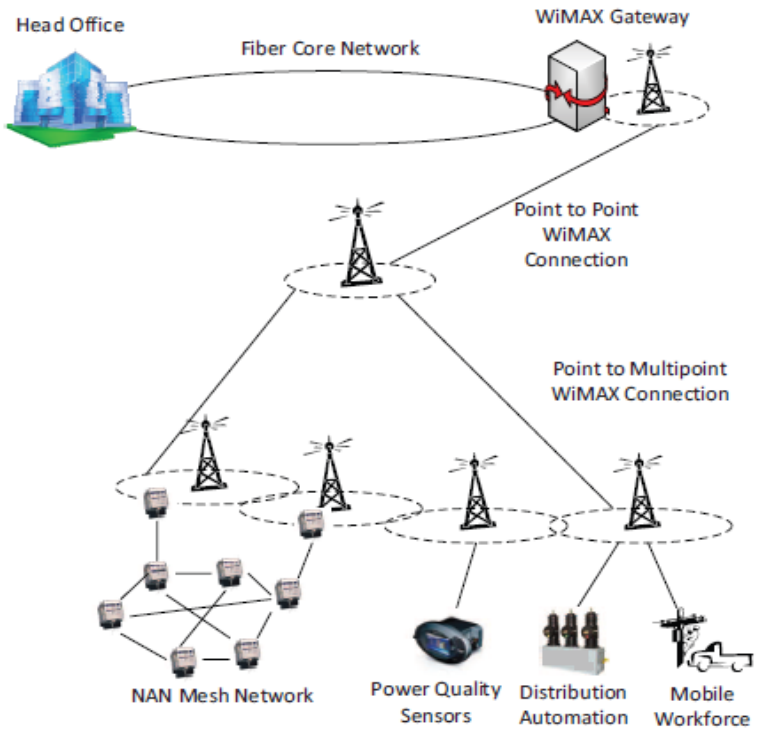


Fig. 1. Smart grid multi-tier network.



شکل ۱- شمای کلی از شبکه برق هوشمند

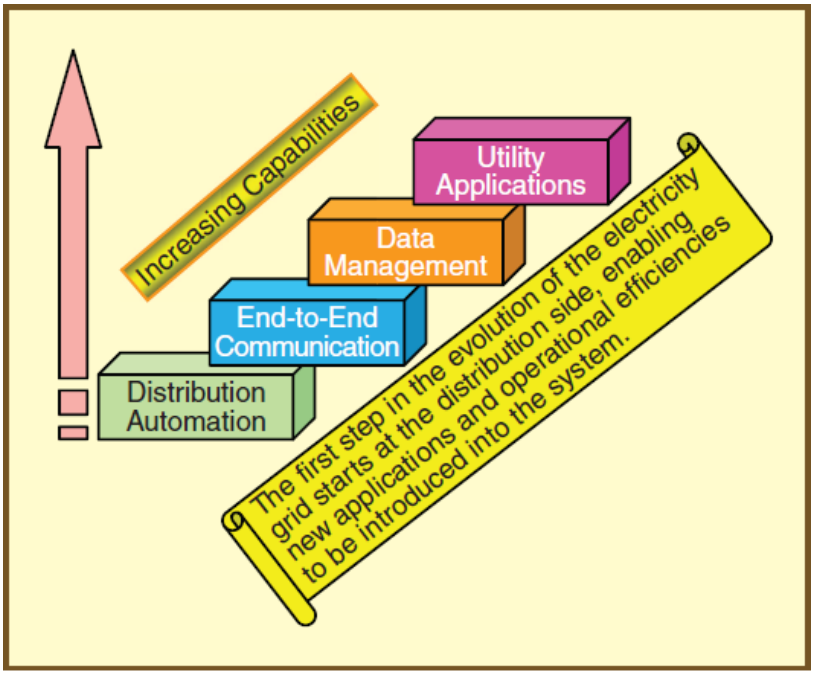
۱-۱ شبکه برق هوشمند

برای داشتن دید کامل و کنترل فراگیر، شبکه برق هوشمند باید فناوری اطلاعات و ارتباطات را در کنار سیستم برق قرار دهد. شکل [۲] ویژگی های برجسته شبکه برق جدید را در مقایسه با شبکه برق نسل قبل نشان می دهد.

Existing Grid	Intelligent Grid
Electromechanical	Digital
One-Way Communication	Two-Way Communication
Centralized Generation	Distributed Generation
Hierarchical	Network
Few Sensors	Sensors Throughout
Blind	Self-Monitoring
Manual Restoration	Self-Healing
Failures and Blackouts	Adaptive and Islanding
Manual Check/Test	Remote Check/Test
Limited Control	Pervasive Control
Few Customer Choices	Many Customer Choices

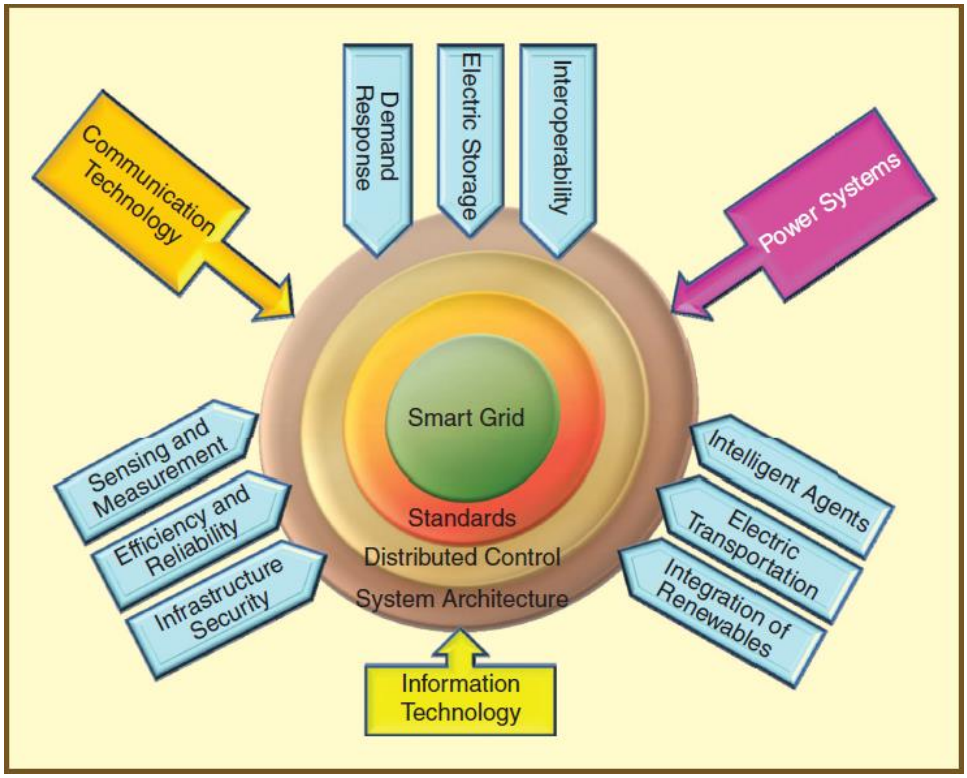
شکل ۲ - مقایسه شبکه برق هوشمند با شبکه سنتی موجود

با توجه به این که منشا مشکلات شبکه برق از سیستم توزیع برق ناشی می شود، نقطه عطف تعمیرات اساسی شبکه در انتهای زنجیر قرار می گیرد. شکل ۳ هم نشان می دهد که کارخانه های تولید برق باور دارند که سرمایه گذاری روی سیستم های توزیع برق گنجایش آنها را با گذشت زمان افزایش خواهد داد.



شکل ۳ - قابلیت های مورد انتظار از تامین کنندگان

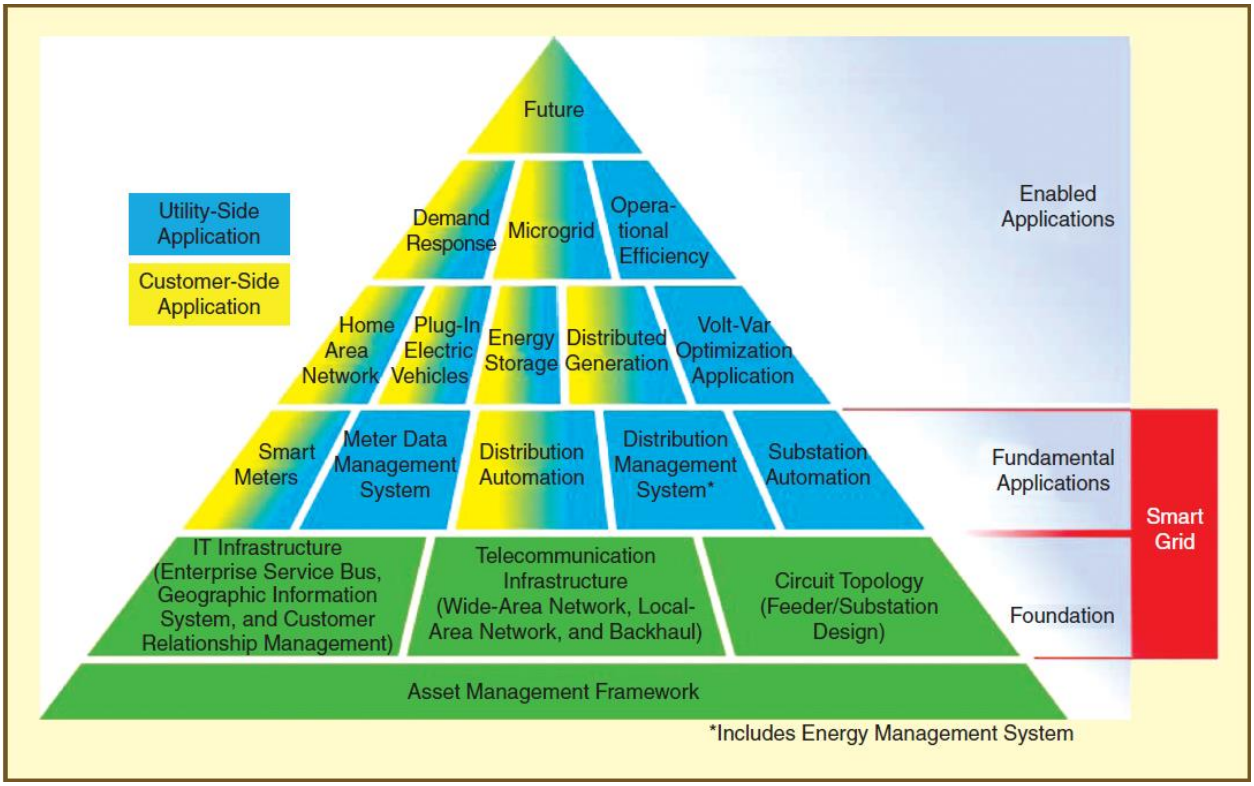
ارتباطات و مدیریت داده با توجه به ظرفیت هایی که دارند نقش مهمی را در مسیر پیشرفت شبکه برق ایفا می کنند. این ظرفیت ها و ویژگی های اساسی و پایه ای به صنعت برق اجازه می دهد که که لایه ای از هوشمندی را روی تجهیزات حال حاضر خود قرار دهند و کاربرد ها و پردازش های جدیدی را در تجارت خود تعریف کنند. همانطور که در شکل [۴] می بینیم، همگرایی تکنولوژی ارتباطات و اطلاعات با قدرت مهندسی سیستم، در کنار دستاوردها، تکنولوژی ها و کاربردهای جدید، به شبکه برق حاضر این اجازه را می دهد که پروتکل ها و استاندارد های جدید را برای پیشرفت خود به کار ببندد.



شکل ۴ - اجزای اصلی شبکه برق هوشمند

۲-۱ مشوق های شبکه برق هوشمند

به عنوان زیرساخت صنعت برق، در حال حاضر شبکه الکتریکی روی فن آوری های همه فن حریف تمرکز کرده است. شرکت های تامین برق در شمال آمریکا و سراسر جهان قدم های سخت و دشواری را در مسیر استفاده از تکنولوژی های جدید برای بهبود عملکردها و زیر ساخت های خود برداشته اند. استفاده کاراتر از تجهیزات حاضر را می توان به عنوان هسته تغییرات تکنولوژیکی در نظر گرفت. هرم شکل ۵ نشان می دهد که کدام یک از روش های مدیریت تجهیزات در توسعه شبکه برق هوشمند پایه ای تر است. می توان دید که پایه ای ترین کار ساخت یک زیربنا برای شبکه برق هوشمند بر اساس IT، ارتباطات است.



شکل ۵ - هرم شبکه برق هوشمند

همانطور که بحث شد رشد لایه هوشمند روی تجهیزات شبکه برق باعث فعال شدن کاربردهای اساسی شبکه برق هوشمند می شود. جالب است که به این نکته توجه کنیم که هرچند که اساس شبکه برق هوشمند بر پایه ادغام عرضی تجهیزات اساسی و پایه ای است، اما قابلیت ها و تجهیزات صحیح و درست شبکه برق هوشمند بر اساس ادغام کاربردهای لایه های بالاتر است. به عنوان مثال یک قابلیت ضروری مانند قابلیت پاسخ بلادرنگ ممکن است بدون ادغام شبکه های خانگی و دستگاه های اندازه گیری هوشمند نتواند محقق شود.

به این ترتیب، می توان ادعا کرد که با توجه به اندازه و ارزش تجهیزات می توان شبکه برق را هوشمند تر کرد. به عنوان تجهیزات با ارزش تر می توان مشاهده و کنترل توزیعی استراتژیک را در کنار شبکه برق حاضر قرار داد و به رشد آن کمک کرد. پس رشد عملکردی و تکنولوژیکی این سیستم نوظهور در طول زمان آن را به عنوان بسته بزرگ توزیعی هوشمند در سرتاسر جهان مطرح می کند. این رشد اورگانیک به سیستم ها اجازه می دهد که بار و عملکرد بسیاری از سیستم های قدیمی را روی این سیستم جدید منتقل کنند و سرویس های خورد را بهبود و گسترش دهند.

این شبکه های نوظهور هوشمند برق تولید انرژی را تسهیل می بخشند. همچنین این سیستم ها منابع انرژی جایگزین را باهم یکپارچه می کنند و مدیریت تولید گازهای گلخانه ای را آسان تر می کنند و در نهایت آنها صنایع را قادر می سازند که از تجهیزات حاضر خود به بهترین نحو استفاده کنند و بهترین کارایی را در زمینه های مختلفی مثل پاسخ بلادرنگ، کاهش بار و کنترل کیفیت داشته باشند.

مشکل بزرگی که اکثر صنایع تامین کننده در سرتاسر جهان با آن مواجه هستند این است که چطور می توانند به کارایی مورد نیاز در کمترین زمان ممکن، با کمترین هزینه و بدون به خطر انداختن سرویس های حیاتی که در حال حاضر فراهم کرده اند برسند. علاوه بر این، تامین کنندگان باید در مورد استراتژی ها و مسیر راهی که باید برای رسیدن به بالاترین بازگشت سرمایه طی کنند، تصمیم گیری کنند.

مانند هر موجودیت دارای فناوری جدید، تامین کنندگان نیز در دنیای در حال توسعه برتری قابل توجه و انکارناپذیری در مقایسه با سایر همتایان خود دارند. همچنین تامین کننده ای که با مشکلات قانونی کمتری مواجه باشد می تواند جهش بلندتری رو به جلو داشته باشد.

فصل ۲

وضعیت فعلی شبکه برق در ایران

نیروی الکتریکی در یک شبکه سراسری تقریباً به هم پیوسته از محل تولید تا محل مصرف از مراحل مختلفی گذر می کند. این مراحل با توجه به ساختار فعلی شبکه برق به شرح ذیل می باشد : [۲]

شبکه تولید (نیروگاه های بخاری، گازی و آبی)
شبکه انتقال (۴۰۰ و ۲۳۰ و بعضاً ۱۳۲ کیلو ولت)
شبکه فوق توزیع (۶۳ و بعضاً ۱۳۲ کیلو ولت)

شبکه توزیع (۳۳ ، ۲۰ و ۱۱ کیلوولت)

شبکه فشار ضعیف (۴۰۰ و ۲۲۰ ولت)

بدلیل خصوصیات کاملاً متفاوت هر یک از شبکه های فوق توسط گروه های مجزایی نظارت و بهره برداری می شود.

۲-۱ ساختار سیستمهای دیسپاچینگ

دیسپاچیگ ملی

دیسپاچینگ منطقه ای

دیسپاچینگ محلی

دیسپاچینگ توزیع

۲-۲ دیسپاچینگ ملی

با توجه به اینکه فرکانس یک مفوم متمرکز می باشد، کنترل فرکانس شبکه به مرکز ملی سپرده شده است. ابزار مرکز کنترل ملی جهت تثبیت فرکانس شبکه، مدیریت تولید واحدهای بزرگ می باشد. سیستم دیسپاچینگ ملی با نصب تجهیزات اسکادا در نیروگاه های بزرگ، ضمن قرائت تولید هر واحد و وضعیت آنها با استفاده از نرم افزارهای پیشرفته بار واحدها را متناسب با فرکانس شبکه کنترل می نماید.

تجهیزات اسکادای نصب شده در نیروگاه ها اطلاعات مربوط به مربوط به واحدها و بی واحدها (اطلاعات مربوط به مقادیر *MW, MVar , MWhr , KV* ناخالص واحد، وضعیت کلیدها و سکسونرهای بی واحد و وضعیت *Run/Stop* واحد، آلارمهای واحد و ...) را مستقیماً از نیروگاه ها به مرکز دیسپاچینگ ملی منتقل می‌کنند. کنترل بار واحدهای بزرگتر از ۹۰ مگاوات نوسط دیسپاچینگ ملی انجام می گیرد. دیسپاچینگ کلی در عین حال هماهنگی دیسپاچینگهای پایین دست خود را نیز بعهده دارد.

۲-۳ دیسپاچینگهای منطقه ای

دیسپاچینگ منطقه ای کنترل ولتاژ و بار شبکه انتقال را بر عهده دارد. با توجه به اینکه ولتاژ یک مفهوم غیر متمرکز می باشد و شبکه انتقال کشور بسیار گسترده می باشد، لذا شبکه انتقال به مناطق کوچکتری تقسیم شده است تا کنترل بار و ولتاژ هر منطقه به صورت غیر متمرکز انجام گیرد.

هم اکنون شبکه انتقال کشور به شش قسمت تبدیل شده و توسط شش مرکز دیسپاچینگ منطقه ای *(AOC)* کنترل می شود. شش منطقه عبارتند از :

منطقه شمالشرق که مرکز دیسپاچینگ آن در مشهد می باشد. *(NEAOC)*
منطقه شمالغرب که مرکز دیسپاچینگ آن در تبریز می باشد. *(NWAOC)*
منطقه تهران که مرکز دیسپاچینگ آن در تهران می باشد. *(TAOC)*
منطقه مرکزی که مرکز دیسپاچینگ آن در اصفهان می باشد. *(CAOC)*
منطقه جنوبشرق که مرکز دیسپاچینگ آن در کرمان می باشد. *(SEAOC)*
منطقه جنوبغرب که مرکز دیسپاچینگ آن در اهواز می باشد. *(SWAOC)*

محدوده عملکرد دیسپاچینگهای منطقه ای به شرح زیر است :

الف) کنترل و بهره برداری از پستهای نیروگاه ها

در اینگونه پستها وضعیت بریکر و سکسیونرهای واحد، وضعیت *stop/Run* واحد و مقدار *MW,MVar* خالص بعد از ترانس واحد به دیسپاچینگ منطقه ای ارسال می شود و بقیه تجهیزات پست مانند آنچه که در قسمت ج توضیح داده شده کنترل و نظارت می شوند.

ب) کنترل و بهره برداری از پستهای *400 KV* ، *230 KV* و نیز شبکه انتقال *400 KV* ، *230 KV*

اطلاعات پستهای *400 KV* ، *230 KV* هر منطقه به مرکز دیسپاچینگ آن منطقه ارسال شده و دستورات کنترلی نیز برای اینگونه پستها از مرکز مربوطه ارسال می شود. البته بایستی یادآوری کرد که در پستهای

400/63 , *230/63* کیلو ولت اطلاعات خطوط *63KV* به این مراکز ارسال نمی شود. اطلاعاتی که از طرف *63KV* ارسال می شود عبارتست از :

MVar, MW ثانویه ترانسها
کنترل وضعیت بریکر ترانسها
وضعیت سکسیونرهای ترانسها
وضعیت و کنترل بریکرهای باس سکشن، باس کوپلر
ولتاژ باسها
آلارمهای باسهای *63 KV*

در مورد پستهای *33(KV)* *132/20* منترل و بهره برداری از طرف *132 KV* و نیزمقادیر *MW,MVar,KV* ثانویه ترانسها، کنترل بریکرهای ثانویه ترانسها، باس سکشن و باس کوپلر در سه منطقه جنوبشرق، شمالشرق و شمالغرب بعهده دیسپاچینگ های منطقه ای خواهد بود.

تقسیم بندی اطلاعات لازم از پست یا نیروگاه

اطلاعات لازم از یک پست و یا نیروگاه برای ارسال به مرکز دیسپاچینگ را می توان به ۴ دسته ذیل تقسیم بندی نمود:

الف – کنترل های مورد نیاز مانند کنترل کلیدها، تپ چنجر ترانسها، بار واحدها و ...
ب- وضعیت های مورد نیاز مانند وضعیت کلیدها، تپ چنجر ترانسها، سکسیونرها و ...
ج - آلارمهای مورد نیاز مانند آلارمهای خط، ترانس، واحد و ...
مقادیر اندازه گیری مورد نیاز مانند مگاوات و مگاوار خط، ترانس، ولتاژ خط یا باس و ...

فصل ۳

بررسی زیر ساخت ارتباطی در شبکه *Smart Grid*

۳-۱زیر ساخت ارتباطی

مدل مفهومی ای که از شبکه ارتباطی شبکه هوشمند می خواهیم در این گزارش بدان اشاره کنیم توسط کمیته معماری شبکه هوشمند [۱] توسعه داده شده است. شکل۶ دیاگرام مرجع [3]این مدل مفهومی را نشان می دهد. این شکل که در مرجع آورده شده است از چندین دامنه تشکیل شده است که هرکدام توسط یک جعبه نمایش داده شده اند. این دامنه ها تشکیل شده اند از *بازیگران*[۲] و *کاربردها*[۳]. *بازیگران* شامل دستگاه ها، سیستمها یا برنامه هایی می شوند که وظیفه تصمیم گیری را دارند و اطلاعات ضروری را برای انجام *کاربردها* تبادل می کنند. کنتورهای هوشمند، ژنراتور های خورشیدی و سیستمهای کنترل نمونه هایی از این دستگاه ها و سیستمها هستند. از طرف دیگر، *کاربردها* وظیفه هایی هستند که توسط یک یا چند *بازیگر* در محدوده یک دامنه انجام می شوند. بعنوان مثال اتوماسیون خانگی[۴] ، تولید انرژی خورشیدی، ذخیره انرژی یا مدیریت انرژی. ضمناً این شکل ابزاری است برای شناسایی *بازیگران* و مسیرهای ارتباطی محتمل در شبکه هوشمند. همچنین این شکل یک روش مناسب برای شناسایی تعاملات داخل دامنه و بین دامنه ای و کاربردهای بالقوه و قابلیتهایی که با این تعاملات فعال می شوند را نشان می دهد.

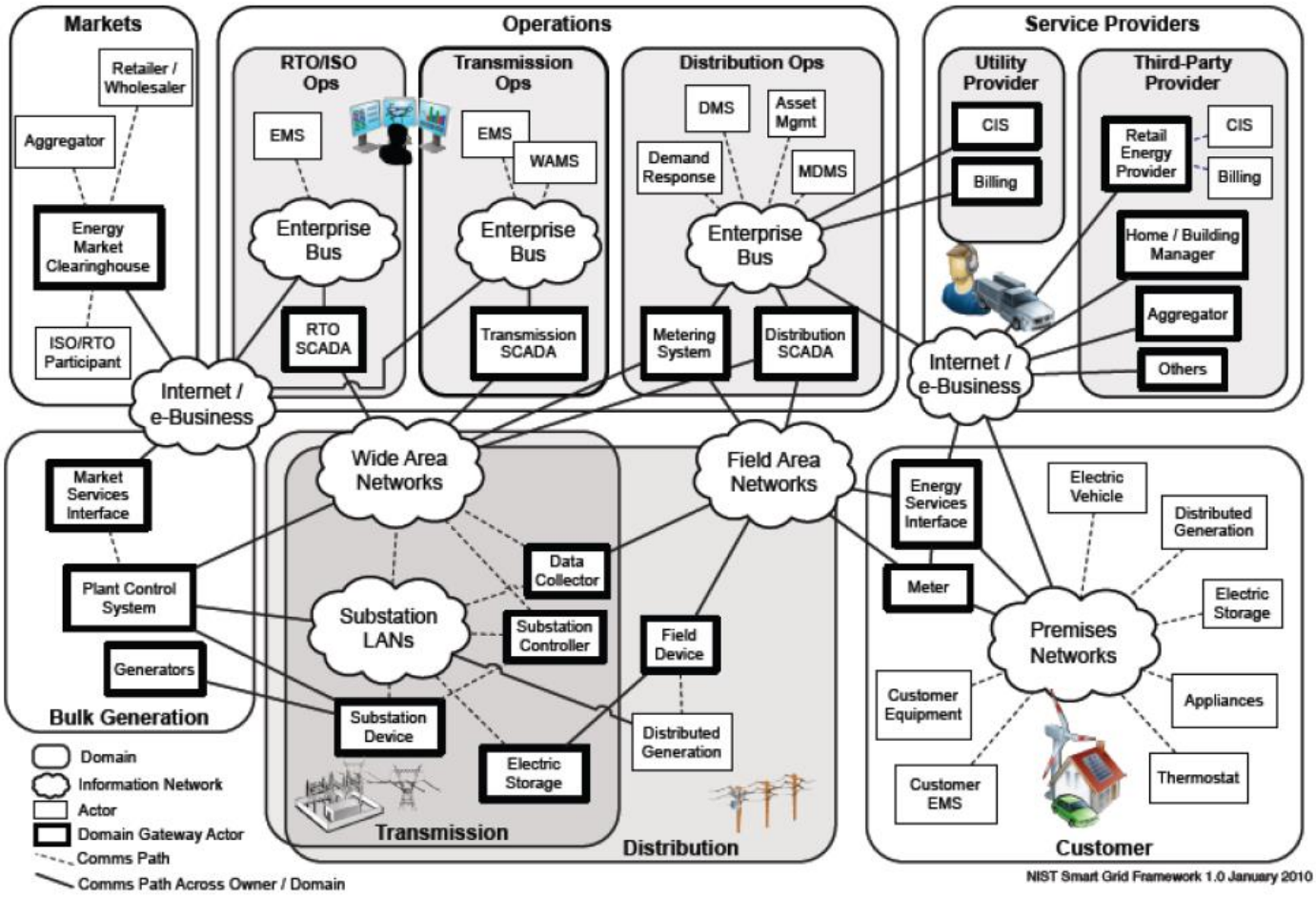
---

[۱] *Smart Grid Architecture Committee (SGIP)*

[۲] *Actors*

[۳] *Applications*

[۴] *Home automation*



شکل۶ دیاگرام مدل مفهومی مرجع برای شبکه داده ***Smart grid***

جدول زیر توصیفی از هر دامنه و بازیگران آن آورده است:

دامنه	توصیف	بازیگران	کاربردهای معمول
عملیات	بازیگران این عرصه مسئول عملکرد یکنواخت و آرام سیستم برق هستند. امروزه، بخش عمده ای از این مسئولیتها بر دوش مدیریت برق هر کشور است. شبکه هوشمند قابلیت واگذاری بخشی از این مسئولیتها به بخش خصوصی را فراهم می کند. البته فارغ از اینکه بخش خصوصی و بازار رقابتی	*Engineering department, control center, EMS, ...*	*Network operation,monitoring, control, fault management, ...*

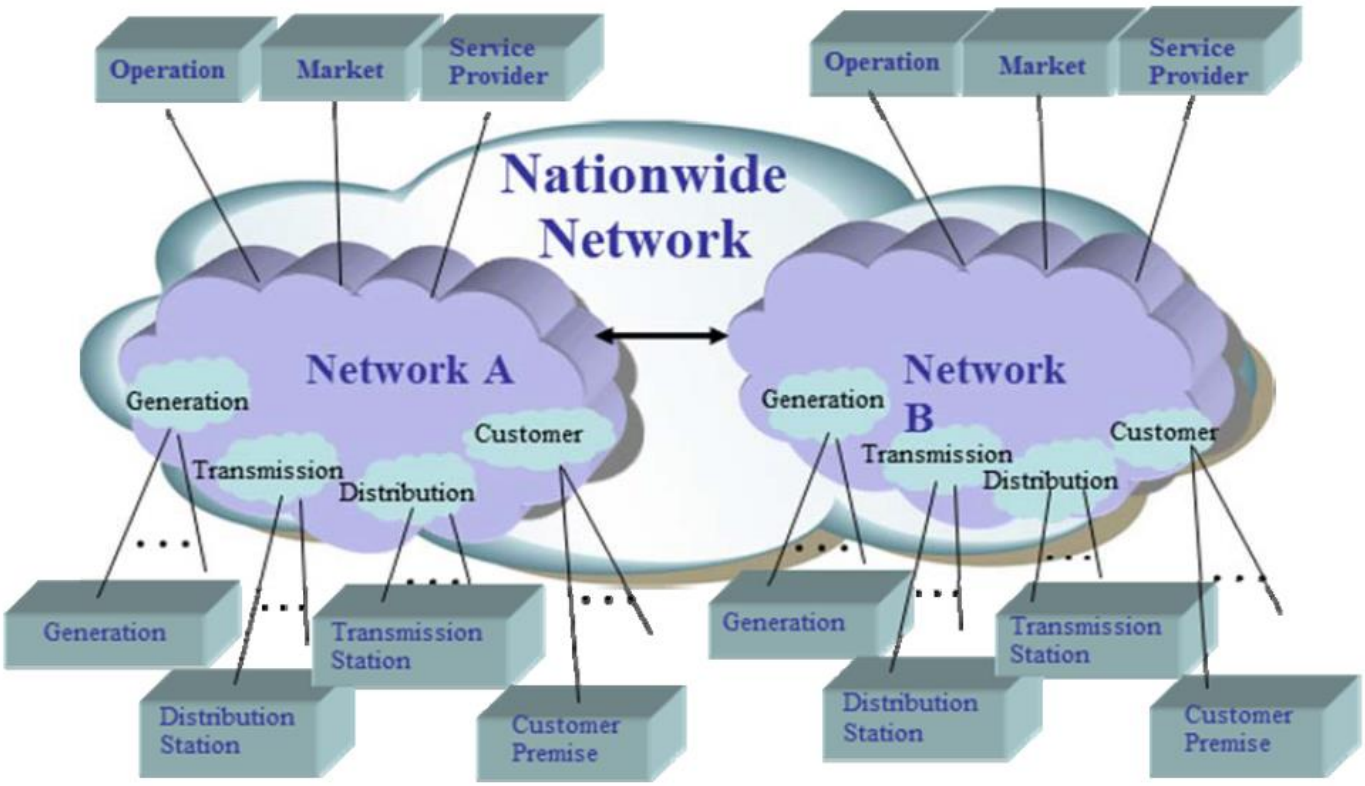
	شرکتهای برق چقدر پیشرفت کرده اند، همچنان بخشی از وظایف پایه ای بر دوش دولتها خواهد ماند.		
انتقال	بخش انتقال وظیفه اش انتقال مقدار زیادی برق از منابع تولید کننده به بخش توزیع از طریق چندین *substation* است. یک شبکه انتقال برق معمولاً توسط یک عملگر انتقال محلی [۱] یا عملگر سیستم مستقل [۲]*(RTO/IOS)* که وظیفه اصلی شان حفظ پایداری در شبکه برق با ایجاد توازن بین تولید و بار مصرفی در شبکه انتقال است مدیریت می شود.	*remote terminal units , substation meters , protection relays, power quality monitors, phasor measurement units, sag monitors, fault recorders, and substation user interfaces,…*	*Substation automation, system protection, control, maintenance, …*
توزیع	دامنه توزیع دامنه واسط بین دامنه انتقال، دامنه مشتری و نقاط اندازه گیری مصرف، ذخیره سازی توزیع شده، و تولید توزیع شده می باشد که می تواند توپولوژی های مختلفی داشته باشد مثل شعاعی [۳]، حلقوی یا مش.	*Capacitor banks, sectionalizers, reclosers, protection relays, storage devices and distributed generators, …*	*Outage management, asset management, measuring , …*
مشتری	مشتری آخرین عنصر زنجیره ای است که همه بخشهای آن هدفشان رساندن برق به مشتری است. اینجا دامنه ای است که برق را مصرف می کند. بازیگران دامنه مشتری او را قادر می کنند تا میزان مصرف و احیاناً تولیدش را کنترل کند. همچنین در این دامنه جریان اطلاعات بین مشتری و سایر دامنه ها توسط بازیگران آن کنترل می شود.		*Building/Home Automation, Industrial Automation, Micro-generation , …*

[۱] *Regional Transmission Operator*

[۲] *Independent System Operator*

[۳] *Radial*

۳-۱-۱معماری کلی ارتباطی



شکل۷ شبکه ارتباطی کلی ***Smart Grid***

شکل۶ شکل مرجع مفهومی برای شبکه های اطلاعاتی شبکه هوشمند است که یک دید سطح بالا درباره ارتباطات در این شبکه ارائه می دهد توسط *SGAC* پیشنهاد شده است. ابرهای کشیده شده بیانگر این مطلب است که شبکه داده ارتباطات داده بین نقاط انتهایی هفت دامنه مختلف – همانهایی که بصورت مستطیل نشان داده شده اند – را باید برقرار کند. هر دامنه یک محیط محاسباتی توزیع شده را دارد و ممکن است برای برآوردن نیازهای ارتباطی دامنه خود زیر شبکه هایی را هم ایجاد کند. در داخل هر شبکه، یک ساختار سلسله مراتبی متشکل از فناوریهای شبکه ای همچون *Home Area Network, Personal Area Network, Wireless Access Network, Local Area Networks, Wide Area Networks* ممکن است پیاده شود.

۳-۱-۲ نگاشت زیر ساخت های ارتباطی به کاربردهای *SG*

پیاده سازی کاربردهای *SG* نیازمند تزریق دستگاه های کنترلی، ارتباطات و اندازه گیری های جدید به سیستم است.یک زیرساخت ارتباطی مناسب باید همه نیازمندیهای کاربردهای انتخاب شده را به همراه چالشهای عملی همچون هزینه و چرخه حیات را در نظر بگیرد. جنبه های مختلف راه حلهای ارتباطی باید در نظر گرفته شود. جنبه هایی همچون : مشخصه های فنی، هزینه، چرخه حیات دارائی ها، استراتژیهای بکارگیری، استاندارد سازی، قابلیت همکاری متقابل و تاثیر بر روی کارایی *utility*.

سه گام برای ایجاد یک متدولوژی برای نگاشت کاربردها به زیرساخت های ارتباطی باید برداشته شود:

۱) ارزیابی عمیق نیازهای ارتباطی که نیازهای فیزیکی ای همچون سرعت ارتباط، حجم داده ها، مسائل کنترل خطا ونیازمندیهای امنیتی سایبری و غیره را به دنبال دارد.
۲) ارزیابی همپوشانی داده ها و نیازهای ارتباطی کاربردهای مختلف با هم.این ارزیابی به مطالعه درباره بخشهایی که در آنها امکان تجمیع داده و ایجاد مسیرهای ارتباطی مشترک برای کاربردهای مختلف در *SG* هست می پردازد.
۳) انتخاب رسانه های ارتباطی، توپولوژی، پهنای باند و بقیه فاکتورها بر اساس نیازمندیهای اساسی کاربردها که انتخاب مشخصه های طراحی مناسب را برای برآوردن نیازمندیهای کاربردها ممکن می‌سازد.

نیازمندیهای ارتباطی شامل:

- میزان داده هایی که باید منتقل شود، هرچند وقت باید این انتقال انجام شود و با چه سرعتی ؟
- اینکه آیا داده باید بصورت همزمان یا غیر همزمان باید منتقل شود ؟

- اینکه آیا جریان داده یکطرفه است ی دوطرفه ؟
- چه سطحی از کنترل خطا و امنیت سایبری مورد نیاز است ؟
- اینکه یک کاربرد در کجای شبکه برق و زیرساخت ارتباطی آن قرار دارد؟

۳-۲ کاربردهای سطح انتقال کاربردهای *Smart Grid*

این بخش کاربردهای جدید سطح انتقال شبکه هوشمند که برای این مطالعه انتخاب شده اند را مورد بحث قرار می دهد. کاربردها به شکل مورد کاربردی[۱] توصیف شده اند. بازیگران، فرآیندها و جریان داده ها ارائه شده‌اند و در ادامه مبحثی پیرامون این کاربردهای جدید و مزایای آن و تفاوتهای آن با نمونه های قبلی ارائه شده است.

۳-۲-۲ کاربردهای انتخاب شده:

چهار کاربرد انتخاب شده است که سیستمهای عملیات، کنترل، محافظت و نگهداری را پوشش می دهد. این کاربردهای جدید شامل: پردازش هشدار پیشرفته[۲]، مکان یابی خودکار خطا[۳]، تشخیص و تخفیف رویداد آبشاری[۴] و نگهداری برمبنای شرایط مدارقطع کن ها [۵]. در ادامه مقداری درباره جزئیات این کاربردها صحبت می کنیم.

۳-۲-۳ پردازش هشدار پیشرفته

همچنان که سیستم برق از نظر عملیاتی به مرزهای توانایی خود نزدیک می شود و شرایط عملکرد آن روز به روز پیچیده تر می‌شود، اپراتورها اغلب با دریافت تعداد بسیار زیادی پیامهای هشدار تولید شده توسط رویدادها روبرو هستند. یک اختلال عمده در سیستم برق می تواند منشا صدها یا گاهاً هزاران هشدار یا رویداد باشد. امروزه، بسیاری از سیستمهای *SCADA* سیستم پردازش هوشمند هشدار *(IAP)*[۶] را بکار بسته اند تا به آنها در کار کردن

---

[۱] *Use Case*

[۲] *Advanced Alarm processing*

[۳] *Automated Fault Location*

[۴] *Cascaded Event Detection and Mitigation*

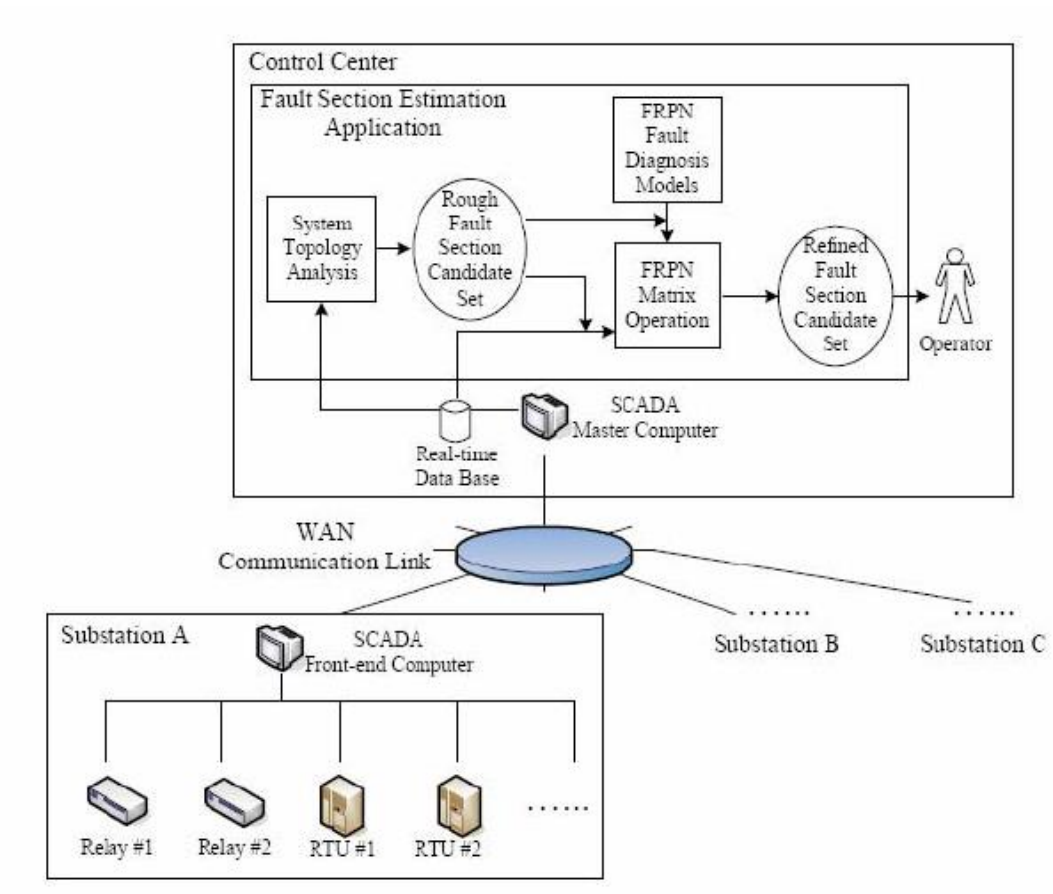
[۵] *Condition based Maintenance of Circuit Breakers*

[۶] *Intelligent Alarm Processing*

با هشدارهای بی شماری که دریافت می کنند کمک کند. سیستم پردازش هشدار پیشرفته که در منبع **[4]** پیشنهاد شده است بر سایر *IAP* های پیشنهاد شده بخاطر وجود مزایای زیر برتری یافته است:

- تعداد هشدارهایی که به اپراتور می رسد را کاهش می دهد.
- شرایطی که تحت آن سیستم هشدار تولید می کند را واضح تر بررسی کرده است.
- عملهای تصحیحی مناسب را در شرایطی که اپراتور نیاز دارد به آن پیشنهاد می کند.

شکل ۸ ساختار پیاده سازی را نشان می دهد. همانطور که در این شکل مشاهده می کنید، مزیت اصلی سیستم پردازش هوشمند هشدار جدید برمی گردد به استفاده از داده های *substation* که از *IED* ها می‌آیند بجای اینکه از *RTU*ها بیایند. همچنین این سیستم تحلیل داده‌ی اضافی‌ای را انجام می‌دهد که به شناسایی بهتر رابطه علت و معلولی بین رویدادها در سیستم برق و هشدارهای مربوطه می‌انجامد.



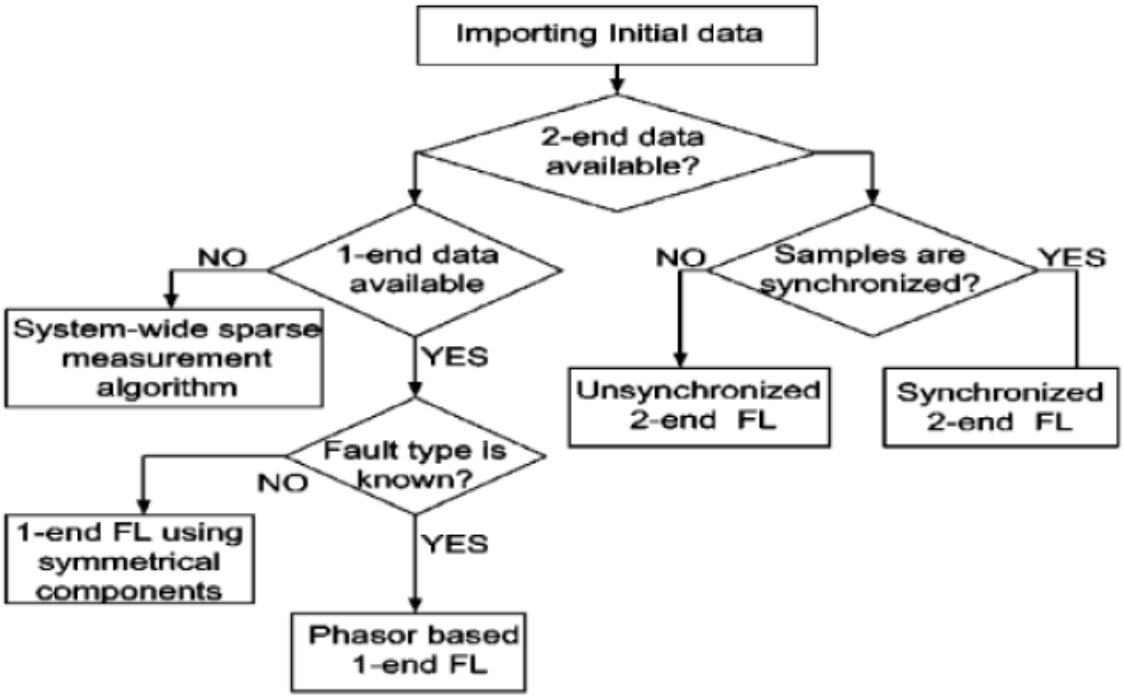
شکل۸پیاده سازی ساختار پردازش هشدار پیشرفته

۳-۲-۴ مکان یابی خودکار خطا

خطاهای خط انتقال ممکن است یا توسط مولفه های فرکانس برق ولتاژ و جریان یا از روی افزایش زودگذر فرکانس تولید شده توسط خطا محاسبه شود. نیازمندیهای داده الگوریتمهای مختلف متفاوت است، این مطلب درباره دقت این الگوریتمها نیز صادق است. یک روش مکان یابی خطای بهینه که مناسبترین الگوریتم مکان یابی خطا را بر اساس آمادگی [۱] و موقعیت داده اندازه گیری شده انتخاب می کند در مرجع *[10]* پیشنهاد شده است. الگوریتم مکان یابی خودکار بهترین نتیجه را از بین الگوریتمهای زیر با استفاده از *flowchart* ای که در شکل ۹ نشان داده شده است پیدا می کند:

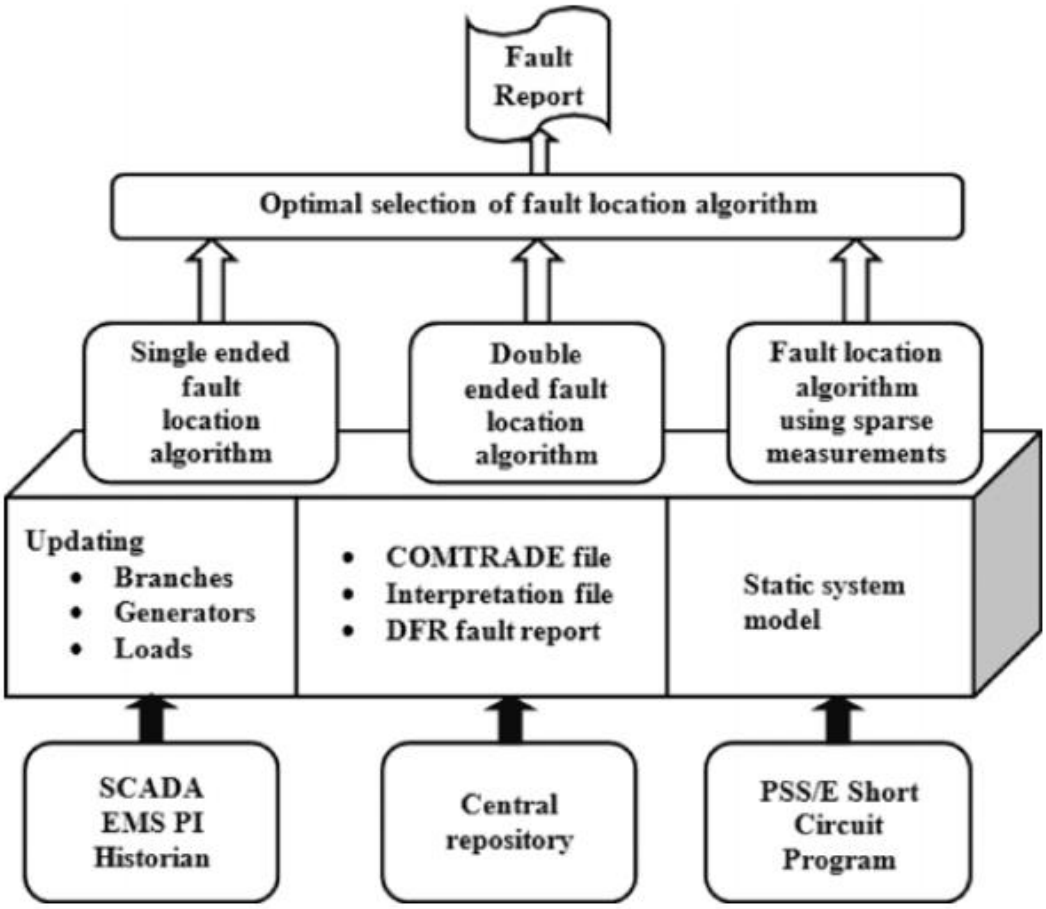
- *Single-End Method*
- *Double-End Methods*
- *Sparse Measurement Method*

[۱] *Availability*



شکل۹فلوچارت مکان یابی خودکار خطا

شکل ۱۰ معماری پایه ای برای روش مکان یابی خودکار خطا را نشان می دهد. توصیف داده و گامهای پردازشی در این شکل نشان داده شده است.



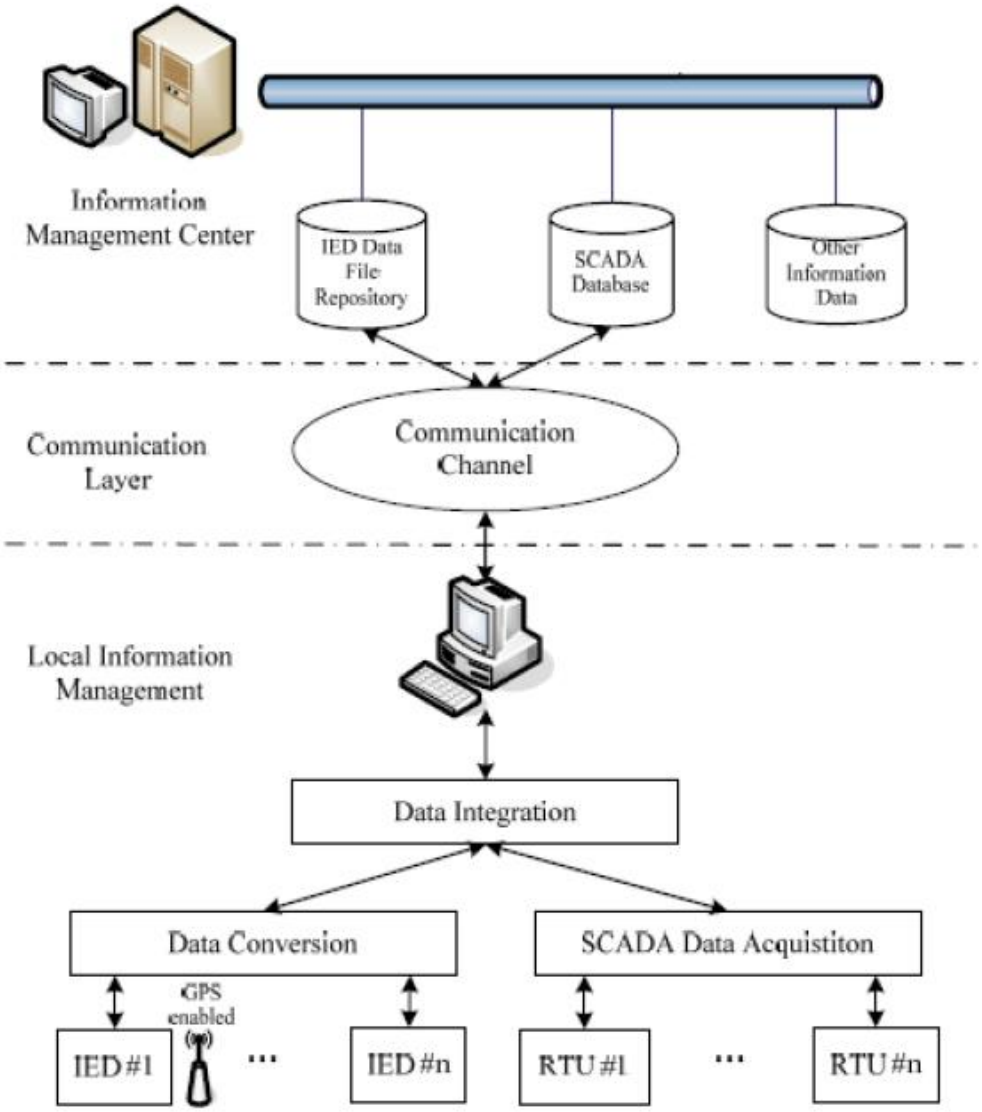
شکل۱۰معماری الگوریتم بهینه یافتن خطا

مزیت اصلی این رویکرد در مقام مقایسه با رویکردهای قبلی این است که این روش بر اساس داده های موجود بهترین الگوریتم در سیستم موجود پیشنهاد می شود و به همین دلیل است که نتایج این الگوریتم نسبت به بقیه دقیق تر و قابل اطمینان تر است.

۳-۲-۵ تشخیص و تخفیف رویداد آبشاری

ابزارهای این سیستم شامل آنالیزورهای امنیتی روتین و برپایه رویداد است که شالوده آن بر روشهای جریان توان و پردازش توپولوژی استوار است. همچنین در این روش مدل کنترلهای امنیتی برای رویداد های پیش بینی شده و نشده اعمال می شود. چهارچوب کلی تبادل اطلاعات در شکل ۱۱ نشان داده شده است.

مزیت این رویکرد نسبت به همه رویکردهای موجود این است که این روش قادراست رویدادهای آبشاری را به محض وقوع تشخیص و تخفیف دهد. این قابلیت بخاطر این است که این الگوریتمها از داده های *real-time* برای شناسایی وضعیت سیستم برق و مولفه هایش استفاده می کند و قادر است اپراتور را از تغییراتی که حتی *SCADA* قادر به تشخیص آنها نیست مطلع سازد.



شکل۱۱چهارچوب کلی برای تبادل اطلاعات

۳-۲-۶ نگهداری بنا به شرایط مدار قطع کن ها [۱]

مرجع **[5]** یک استراتژی سطح سیستم برای مدار قطع کن ها برپایه مدلهای نگهداری احتمالی پیشنهاد داده است. این روش از یک رویکرد "پایین به بالا " استفاده می کند و و داده های تاریخچه و نظارت *real-time* برپایه شرایط را در تخمین نرخ خرابی بکار می گیرد.

۳-۲-۷ خلاصه ای از بازیگران

جدول زیر خلاصه ای از بازیگران مطرح شده در *use case* ها و دامنه های گفته شده ارائه می دهد.

بازیگر	دامنه ها	توصیف
IED	انتقال	یک دستگاه دارای ریزپردازنده که در کنترل و نظارت بر تجهیزات شبکه برق و نیز در برقراری ارتباط با *SCADA* استفاده می شود. همچنین کاربردهای هوشمند توزیع شده ی هوشمندی بر روی آن اجرا می شود که برخی عملیات را بصورت خودکار انجام می دهند.
Substation Application	عملیات	*Substation* ها نقاطی در بخش انتقال و توزیع هستند که در آنها ولتاژ به کمک ترانسفورماتورها از مقادیر بالا به پایین یا بالعکس تبدیل می شود. توان الکتریکی ممکن است در گذر ار منبع تولید به مشتری از چندین *substation* عبور کند. یعنی سطح ولتاژ ممکن است در چندین گام تغییر کند. کاربردهای *substation* بر روی کامپیوترهای *substation* اجرا می شوند.
SCADA	عملیات	یک سیستم کامپیوتری که عملیات در سیستم برق را کنترل و نظارت می کند. پایگاه داده *SCADA* توسط داده هایی که *Remote Terminal Unit* ها جمع آوری می شوند بروز رسانی می شود. سرعت و دقت در اندازه گیری داده ها از نتایج این سیستم است و امکان نظارت[۲] و کنترل حلقه- بسته نیز پشتیبانی می شود.

[۱] *Condition Based Circuit Breaker Maintenance*

[۲] *supervisory*

Wide Area Monitoring and Control System	عملیات	اندازه گیری های انجام شده از *phasor measurement unit* ها که در *substation* های پخش شده در کل سیستم برق قرار داده شده اند و عملهایی که توسط عملگرهای انتقال بر اساس آن انداره گیریها انجام می شود این سیستم را تشکیل می دهند.
Metering system	مشتری	سیستمهایی که برای جمع آوری داده های مصرف و سایر داده های مور نیاز اپراتور استفاده می شود.
GIS	عملیات	یک سیستم اطلاعاتی که وظیفه ی تجمیع، ذخیره سازی، ویرایش، تحلیل، به اشتراک گذاری و نمایش اطلاعات جغرافیایی را دارد.
Power System Control Center	عملیات	مرکزی برای کنترل متمرکز عملیات در سیستم برق
EMS	عملیات	یک سری ابزارهای کامپیوتری که توسط اپراتورها در شبکه برق برای نظارت، کنترل و بهینه سازی کارایی سیستم تولید و انتقال. *EMS* همچنین ورودی *DMS*[1] را بصورت اشیاء ، محدودیتها و داده های ورودی از سایر نرم افزار های *EMS* تامین می‌کند.

[1] *Data Management System*

فصل ۴

روشهای موجود

۴-۱امنیت در *smart grid*

سیستمهای کامپیوتری سه نیازمندی اصلی امنیتی دارند که عموماً به آنها *CIA (Confidentiality, Integrity, and Availability)* گفته می شوند :

قابلیت اعتماد: محافظت از داده های ارسالی در برابر فاش شدن (مثلاً جلوگیری از استراق سمع آنچه که ارسال می شود.) بعنوان مثال برای ایجاد اعتماد در کاربردهای *e-commerce*، تراکنشهای کارتهای اعتباری بین مرورگر وب و *Web Server* رمزنگاری می شود.

Integrity یا تمامیت: حفاظت در برابر دستکاری تبادلات; حال این دستکاریها عمدی باشد یا سهوی و تضمین اینکه تغییرات قابل شناسایی باشد. که شامل دو بخش است : یکی درباره ی داده ها و دیگری درباره‌ی نظیرها (*peer*)

۲-۱ نظیرها می بایست تایید کنند که اطلاعاتی که به نظر می رسد از یک نظیر معتمد دریافت شده اند واقعاً از آن نظیر باشند، که این *data origin authentication* نامیده می شود.

۲-۲ نظیرها باید تصدیق کنند که محتوای داده های تبادل شده دستکاری نشده اند. این موضوع *data integrity* اطلاق می شود.

*Availability*یا آمادگی: تضمین اینکه سرویس دهنده ها همیشه در دسترس خواهند بود و سیستم در برابر حملات *Denial of service (DOS)* ایمن است.

اهداف امنیتی که در این حوزه بیشتر مد نظر هستند قابلیت اعتماد، جامعیت و دسترس پذیری هستند. در بیشتر حوزه ها جامعیت و قابلیت اتکا مقدم بر دسترس پذیری هستند ولی در شبکه‌ی برق مسئله مهم این است که توان همیشه باید در دسترس باشد، بنابراین دسترس پذیری مهمترین هدف امنیتی شبکه قرار می گیرد. جامعیت و قابلیت اتکا در جایگاه های بعدی از نظر اهمیت قرار دارند.

*Availability*مهمترین هدف امنیتی در *SG* است. سیستمهای *real-time* حیاتی در *SG* تخمین زده شده است که حداکثر ۴ میلی ثانیه تاخیر را تحمل می کنند. این سیستمها بطور پیوسته بر وضعیت شبکه ی برق نظارت می کنند و هر گونه اختلالی در شبکه‌ی ارتباطی آن می تواند به قطع شدن برق بیانجامد. جدول *1.1* تخمینی از حداکثر تاخیر قابل قبول بخشهای مختلف *SG* را نشان می دهد.

Maximum Latency	Communication Type
≤ 4 ms	Protective relaying
Sub-seconds	Wide area situational awareness monitoring
Seconds	Substation and feeder supervisory control and data acquisition (SCADA)
Minutes	Monitoring noncritical equipment and marketing pricing info
Hours	Meter reading and longer-term pricing info
Days/Weeks/Months	Collecting long-term usage data

شکل ۱۲ -تخمینی از حداکثر نیازمندیهای تاخیر ارتباطات مختلف

در *SG* علاوه بر فاکتورهای *CIA* ملاحظات دیگری را هم باید در نظر گرفت. تاخیر اضافی، پیچیدگی محاسباتی و اندازه ی بسته ها نیز بسیار مهم هستند. در بسیاری موارد قابلیت اعتماد بسیار کمتر از دو مورد دیگر اهمیت دارد: در *SG* اینکه یک حمله کننده بتواند محتویات یک پیام را ببیند برایش ارزش بسیار پایین تری دارد نسبت به اینکه بتواند پیغامهای غلط در شبکه بفرستد و رسیدن بسته های قانونی را به تاخیر بیاندازد. *[6]*

۲-۴ چند پخشی در *smart grid*

چندپخشی ارتباطات یک به چند را بگونه‌ای موثر فراهم می کند. اگرچه چندپخشی بطور گسترده ای در اینترنت و اخیراً در شبکه‌ی حسگر بیسیم *[7]* و شبکه های تحمل پذیر اختلال *[8]*مورد بررسی گرفته است،

ولی کاربرد آن در زیرساختهای حیاتی همچون *smart grid* زیاد مورد توجه قرار نگرفته است *[9]*. در *smart grid* عمل *multicast* کاربردهای زیادی دارد. بعنوان مثال در *wide area protection* واحدهای اندازه گیری *phasor* یا *(PMU)* می تواند برای اندازه گیری پارامترهای سیستم همچون ولتاژ و جریان و سپس *multicast* کردن داده ها به مراکز کنترل استفاده شود. بر اساس داده های دریافتی مراکز کنترل می توانند عکس العمل مناسبی در قبال ازکارافتادگیهای پی درپی[۱]نشان دهند. بعنوان مثالی دیگر در طول دوره‌ی اوج [۲]مصرف انرژی، مراکز تامین کننده[۳] می توانند یک دستور درخواست- پاسخ [۴]به گروه بزرگی از دستگاه های خانگی صادر کنند و از آنها بخواهند که به طور موقت خاموش شوند یا میزان مصرف خود را کاهش دهند. کاربردهای دیگری هم هستندکه از *multicast* برای انجام عملیات و کنترل خود در *smart grid* استفاده می‌کنند. بیشتر تحقیقات در زمینه‌ی ارتباطات امن گروهی بیشتر بر روی معماری گروه های امن و مسئله‌ی مدیریت کلید متمرکز شده است. اگر چه تحقیقات جدید بر روی روشهای تایید هویت موثر بسته ها متمرکز شده است.

تامین کننده ها[۵]از تکنولوژی مختلف شبکه های *WAN* برای جمع آوری اطلاعات و کنترل بخشهای مختلف مثل نیروگاه ها، ادارات و سیستم *SCADA* و نیز کنترل و نظارت شبکه‌ی برق استفاده می کنند. این شبکه های فناوریهای مختلفی همچون *PLC*[۶]، فیبر نوری، خطوط اجاره ای و تکنولوژیهای مختلف بی سیم را با یکدیگر ترکیب کرده اند.یک شبکه‌ی *smart grid WAN* از اتصال دو شبکه تشکیل شده است. شبکه‌ی هسته و شبکه‌ی توزیع[۷]. شبکه‌ی هسته ادارات مرکزی و *substation* ها را به هم متصل می کند و در آن از فیبر نوری استفاده می شود که نرخ داده ی بالا و تاخیر کمی را ارائه می دهد. جایی که استفاده از فیبر ممکن نباشد یا خیلی گران باشد استفاده از تکنولوژیهای دسترسی بیسیم مانند *WiMAX* بخاطر راحتی استفاده و قابلیت اعتماد [۸]تایید شده پیشنهاد می شود. برای شبکه های توزیع یا *backhaul* که شبکه های *NAN(Neighbor Area Network)* را به هم متصل می کند از فناوریهای همچون فیبر نوری، *WiMAX*، *PLC*، ارتباط از طریق ماهواره و شبکه

---

[۱] *cascaded failure*
[۲] *peak*
[۳] *utility*
[۴] *demand-response*
[۵] *utility*
[۶] *power line communication*
[۷] *backhaul*
[۸] *reliability*

های سلولی استفاده می شود. بنابراین این نیاز وجود دارد که ارتباطات بین شبکه های ناهمگون وجود داشته باشد. چون ممکن است در یک قسمت از شبکه از یک رسانه‌ی ارتباطی و در جای دیگر رسانه ی دیگری استفاده شده باشد و در عین حال نیاز باشد که بین این نودهای در شبکه های مختلف ارتباط *multicast* وجود داشته باشد. مسئله‌ی اصلی در این ارتباط قابل اعتماد [۱]بودن این ارتباط است.

۳-۴ پروتکلهای شبکه *smart grid*

در سال ۱۹۹۴ زیر کمیته های جمع آوری، نظارت و کنترل داده‌ی *IEEE Power Engineering Society* گروه ضربتی [۲]را برای بازبینی پروتکل های ارتباطی ای که بین *Intelligent Electronic Devices (IEDs)*[۳] و *Remote Terminal Units (RTUs)* در *substation* ها وجود دارد تشکیل داد.

گروه ضربت *IEEE* محیط سیستم *SCADA* را سیستمی مرتب در حال تغییر و بسیار گیج کننده یافت که هزینه و زمان اجرای سیستمهای *SCADA substation* را بشدت افزایش می داد. این گروه اطلاعات مربوط به تقریباً ۱۴۰ پروتکل را جمع آوری کرد و آنها را با لیستی از نیازمندیهای یک پروتکل ارتباطی مقایسه نمود.

این مقایسه منتج به لیست کوتاهی از پروتکل‌ها شد که اکثر نیازمندیها را برآورده می کردند. سپس از بین این لیست قرعه کشی شد و دو پروتکل *SCADA* بعنوان مرجع انتخاب شدند. *IEC 60870-5-101* و *DNP3*.

*IED*ها داده ها را از سنسورها و تجهیزات برق می‌گیرند و می توانند دستورات کنترلی صادر کنند، مثلاً اگر یک ناهنجاری را در ولتاژ، جریان، یا فرکانس احساس کنند به *circuit breaker* ها دستور لازم را صادر می‌کنند. این دستورها می بایست به کمک سرویس *multicast* به *circuit breaker* ها داده شود.

---

[۱] *reliable*

[۲] *Task Force*

[۳] یک *Intelligent Electronic Device (IED)* عبارتی است که در صنعت برق برای توصیف کنترل کننده های دارای *microprocessor* اطلاق می‌شود.

چندپخشی نقش مهمی را در شبکه‌ی *SG* بازی می کند. همانطور که قبلاً هم اشاره شد چندپخشی در *Phasor Measurement Units (PMUs)*برای تحویل داده‌های وضعیت سیستم بصورت دوره‌ای در یک ناحیه جغرافیایی بزرگ استفاده می شود. *UDP Multicast*در *DNP3* برای *reset* کردن همزمان شمارنده‌ها یا مقدارچندین دستگاه کنترل از راه دور استفاده می شود. در پروتکل *IEC 61850* پروتکلهای لایه پیوند داده‌ای همانند *Generic Object Oriented Substation Events (GOOSE)* و *Sampled MeasuredValue (SMV)* برای جمع آوری داده های وضعیت *real time*، بروزرسانی وضعیت*IED*ها و رساندن دستورات کنترلی استفاده می‌شود.

IEC 61850 توصیفی است بر چگونگی طراحی و پیکربندی خودکار عملکردهای یک *substation*. این استاندارد از یک مجموعه کامل از عملکردهای *substation* پشتیبانی می‌کند و ویژگیهای ارتباطی مورد نیاز یک *substation* را بیان می‌دارد. همچنین آنقدر توسعه پذیر هست که تکامل مکرر سیستم را پوشش دهد. *IEC 61850* از مدل داده‌ای شی‌گرا برای توصیف اطلاعات تجهیزات اصلی و عملکردهای خودکار *substation*استفاده می‌کند. آن همچنین واسط [۱] ارتباطی بین*IED* ها و چگونگی نگاشت آنها به تعدادی پروتکل قابل اجرا بر روی *TCP/IP* و اترنت پرسرعت را توصیف می‌کند.

GOOSE یک پروتکل *multicast* لایه پیوند داده است که در *IEC 61850* برای ارسال پیامهای حساس به زمان استفاده می شود; پیامهای همچون وقایع [۲]*substation*، دستورات [۳] و هشدارهای داخل شبکه‌ی *substation*. به دلیل اینکه *GOOSE* مستقیماً به فریمهای اترنت نگاشت می شوند، می تواند از *high-speed switched Ethernet* سود برد و قادر است نیازمندیهای زمانی خود را برآورده سازد.

درحوزه ی امنیت *multicast* هم تحقیقات زیادی انجام شده است. مرجع *[10]* به مسائل مختلف در امنیت *multicast* پرداخته است. در مرجع *[11]* یک روش توزیع کلید جدید برای *multicast* ارائه شده است که هدفش کاهش پیچیدگی محاسباتی است. بخشی از تحقیقات در این زمینه درباره امنیت سیستم *SCADA* است.

---

[۱] *Interface*

[۲] *Events*

[۳] *commands*

روش *ASKMA*[1] یکی از روشهای مطرح در این حوزه است که به بحث مدیریت کلید در *SCADA* می-پردازد*[12]*. در مرجع *[13]* روش *ASKMA* که باوجود پشتیبانی از *multicast* کارایی کمی دارد، بهبود یافته و روش *AKAMA+* را پیشنهاد کرده است که پیچیدگی محاسبات *ASKMA* و نیز تعداد کلیدهای ذخیره شده در نودها را کاهش می دهد.

---

[1] *Advanced SCADA Key Management Architecture*

فصل ۵

الگوریتمهای مسیریابی چندپخشی در شبکه های داده

۵-۱ چند پخشی

چند پخشی یک الگوی ارتباطی است که یک میزبان مبدا پیامی را به گروهی از میزبانهای مقصد ارسال می کند. اگرچه اینکار می تواند با ارسال پیامهای *unicast* مختلف به هر کدام از مقاصد انجام پذیرد اما دلایل زیادی وجود دارد که استفاده از قابلیت چند پخشی را اجتناب ناپذیر می کند. اولین مزیت عمده استفاده از چند پخشی کاهش بار شبکه است. همانطور که قبلاً اشاره شد چند پخشی کاربردهای زیادی در *smart grid* دارد. از آنجا که چند پخشی نیازمند ارسال تنها یک بسته از طرف منبع و تکثیر این بسته در صورت نیاز (بر اساس درخت چند پخشی) است چند پخشی می تواند در مصرف پهنای باند مورد نیاز شبکه صرفه جویی کند.

بخش دیگری که چند پخشی می تواند بسیار مفید باشد کشف منبع [۱] است. در شبکه اینترنت کاربردهای زیادی وجود دارد که در آن یک میزبان می خواهد بداند آیا یک سرویس خاص در شبکه وجود دارد یا نه ؟ پروتکلهای اینترنتی همچون *Bootstrap Protocol (BOOTP)* و *Open Shortest Path First (OSPF)* مثالهایی از این کاربردها هستند. به کمک پیامهای چند پخشی و ارسال درخواست [۲] به آن میزبانها که پتانسیل داشتن این قابلیت را دارند می توان سرویسهای مورد درخواست را پیدا نمود.

خاصیت مهم دیگر چند پخشی پشتیبانی از کاربردهای *datacasting* است. در سالهای اخیر انتقال داده های چند رسانه ای روز به روز بیشتر مورد استفاده قرار می گیرند. سیگنالهای صوتی و تصویری گرفته شده، فشرده می شوند وسپس به گروهی از *station* های گیرنده ارسال می کند. بجای استفاده از مجموعه ای از ارتباطات نقطه به نقطه بین نودهای مشارکت کننده چند پخشی می تواند برای توزیع داده های چند رسانه ای بین گیرنده ها مورد استفاده قرار گیرد. در دنیای واقعی *station* ها می توانند به یک *audio-cast* یا *video-*

---

[۱] *Resource discovery*

[۲] *Query*

cast متصل شده یا جدا شوند. انعطاف پذیری اتصال و ترک یک گروه چند پخشی می تواند تغیّر در عضویت نودها را راحت تر کنترل نماید.

مفهوم گروه یک مفهوم اساسی در چند پخشی است. بنا به تعریف یک پیغام چند پخشی از یک منبع به گروهی از میزبانهای مقصد ارسال می شود. در *IP multicasting* گروهای چند پخشی یک *ID* بنام *multicast group ID* دارند. هرگاه که یک پیغام چند پخشی ارسال می شود، *multicast group ID* آن گروه مقصد را مشخص می کند. این *group ID* ها در اصل مجموعه ای از آدرسهای *IP* که کلاس *D* خوانده می شوند است. بنابراین اگر یک میزبان می خواهد یک در خواست چند پخشی را که به یک گروه خاص فرستاده می شود دریافت کند نیازمند آن است که بگونه ای به همه پیامهایی که به یک گروه خاص ارسال می شود گوش دهد. اگر مبدا و مقصد یک بسته چند پخشی بر روی یک باس مشترک باشند (مثلاً *Ethernet Bus*) کار ساده است و همه بسته ها را دریافت می کنند و فقط گیرنده بسته را برمی دارد. اگر فرستنده و گیرنده بر روی یک *LAN* نباشند، ارسال بسته های چند پخشی به سمت مقاصد پیچیده تر می شود. برای حل مسئله مسیریابی بسته های چند پخشی در سطح اینترنت میزبانها می بایست با مطلع کردن روتر چند پخشی در زیر شبکه خود به گروه مورد نظر ملحق[1] شوند. *The Internet Group Management Protocol (IGMP)* برای این منظور استفاده می شود. ترک یه گروه هم از طریق *IGMP* انجام می شود. از این طریق می توان روترهای چند پخشی در شبکه اعضای گروه های چند پخشی در شبکه خودشان را می شناسند و می توانند بر اساس آن تصمیم بگیرند که یک پیام چند پخشی را در شبکه خودشان هدایت کنند یا نه؟ هرگاه یه مسیریاب چند پخشییک بسته چند پخشی را دریافت می کند *group ID* بسته را بررسی می کند و بسته را صورتی هدایت می کند که عضوی از آن گروه در شبکه متصل به خود داشته باشد. *IGMP* اطلاعات مورد نیاز در آخرین گام هدایت بسته های چند پخشی به سمت مقصد استفاده می‌شود.اگرچه برای تحویل یک بسته چند پخشی از منبع به نودهای مقصد در شبکه های دیگر روترهای چند پخشی می بایست اطلاعاتی مربوط به عضویت نودهای متصل به خود در گروه های چند پخشی را تبادل کنند. الگوریتمهای مختلفی همچون *flooding*، *spanning tree*، *reverse path forwarding*، *reverse path multicasting* ، برای تبادل اطلاعات مسیریابی بین روترها استفاده می شود.

[1] *join*

بعضی از این الگوریتمها در پروتکلهای مسریابی چند پخشی پویا همچون *DVMRP*[۱] ، پروتکل *MOSPF*[۲] و *PIM*[۳] استفاده شده اند. بر اساس اطلاعات مسیریابی بدست آمده از طریق این پروتکلها، هرجا که یک بسته چند پخشی به یک گروه چند پخشی فرستاده می شود، مسیریابهای چند پخشی تصمیم خواهند گرفت که آیا آن بسته را به شبکه شان بفرستند یا نه ؟ نهایتاً مسیریاب پایانی نگاه خواهد کرد که ببیند بر اساس اطلاعات *IGMP* آیا عضوی از آن گروه خاص بصورت فیزیکی به شبکه اش متصل است یا نه ؟ و باید آن را هدایت کند یا نه ؟

در بخش بعدی می خواهیم آدرسهای چند پخشی را بررسی کنیم و بحث کنیم که چگونه این آدرسها می‌توانند به آدرسهای لایه *MAC* نگاشت داده شوند. سپس ما درباره *IGMP* و اینکه چه توسعه هایی برای چند پخشی *IP* در میزبانها مورد نیاز است بحث می کنیم. الگوریتمهای مسیریابی هم بعنوان پایه ای برای پروتکلهای مسیریابی چندپخشی بررسی می‌شود.

۵-۲ گروه های چند پخشی

در *IPv4* سه نوع آدرس داریم: تک پخشی [۴] همه پخشی [۵] و چند پخشی [۶]. آدرسهای تک پخشی برای انتقال یک پیام به یک نود مقصد استفاده می شود. آدرسهای همه پخشی هنگامی استفاده می شوند که یک بسته قرار است به همه نودهای یک زیرشبکه ارسال شوند. برای تحویل یک بسته به گروهی از نودهای مقصد که لزوماً در همان زیر شبکه نیستند آدرسهای چند پخشی استفاده می شوند. در حالیکه آدرسهای *IP* کلاس *A, B* و *C* برای پیامهای تک پخشی استفاده می شوند. آدرسهای کلاس *D(224.0.0.0 – 239.255.255.255)* توسط پیامهای چند پخشی استفاده می شوند.

---

[۱] *Distance Vector Multicast Routing Protocol*

[۲] *Multicast extension Open Shortest Path First*

[۳] *Protocol Independent Multicast*

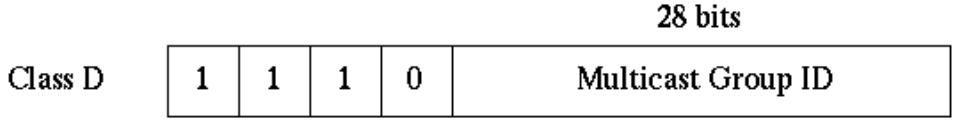
[۴] *Unicast*

[۵] *Broadcast*

[۶] *Multicast*

۵-۲-۱ آدرس چند پخشی

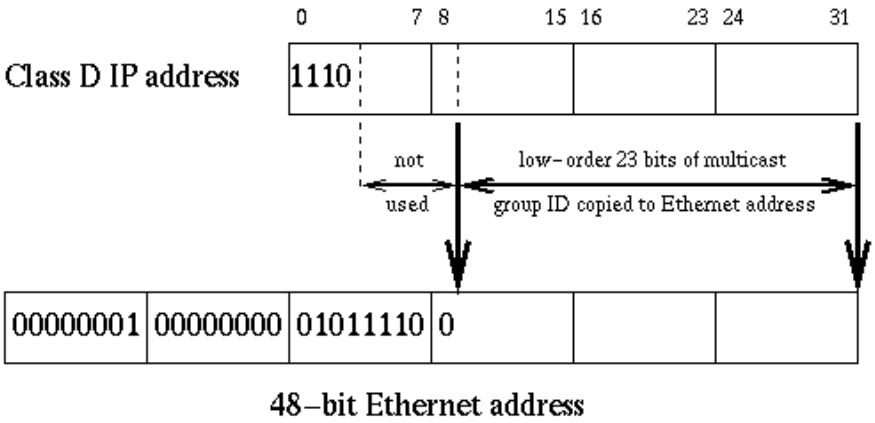
آدرسهای *IP* کلاس *D* به گروهی از نودها که یک گروه چند پخشی را تعریف می کنند اختصاص می یابد. ۴ بیت با ارزش از کلاس *D*مقدار *"1110"* دارند. ۲۸ بیت باقیمانده بعد از حذف این ۴ بیت *Multicast Group ID* نامیده می شوند. بعضی از آدرسهای کلاس *D* توسط *Internet Assigned Numbers Authority (IANA)* برای مصارف خاص رزرو شده اند. بلوکی از آدرسهای چند پخشی شامل آدرسهای رنج *224.0.0.1* تا *224.0.0.255* برای استفاده در پروتکلهای مسیریابی و سایر پروتکلهای سطح پایین کشف توپولوژی و نگهداری استفاده می شوند. آدرسهای بین ۲۳۹,۰,۰,۰ تا ۲۳۹,۲۵۵,۲۵۵,۲۵۵ برای استفاده کاربردهای محلی و داخلی شبکه رزرو شده اند و در سطح اینترنت استفاده نمی‌شوند. چندی دیگر از آدرسهای کلاس *D* برای بعضی گروه های شناخته شده همچون " همه روترها در این *subnet* " یا " همه روترهای *DVMRP* " و " همه روترهای *OSPF* ". فرمت آدرسهای کلاس *D* در شکل زیر نشان داده شده است :



شکل ۶ فرمت آدرسهای کلاس ***D***

یک بسته چند پخشی با همان سطح قابلیت اعتماد *best-effort* که برای یک بسته تک پخشی *IP* وجود دارد به اعضای گروه تحویل داده می شود. از دست رفتگی بسته ها و دریافت خارج از ترتیب بسته ها امکان دارد. همانند بسته های تک پخشی، باید یک آدرس لایه *MAC*باشد که آدرس چند پخشی به آن نگاشت یابد. *IANA* مجموعه ای از آدرسهای لایه *IEEE-802.11 MAC-layer* را برای بسته های چند پخشی رزرو کرده است که شامل رنج *01:00:5E:00:00:00* تا *01:00:5E:7F:FF:FF* می شود.

یک آدرس *IP* چند پخشی می تواند با جایگذاری ۲۳ بیت کم ارزش آدرس *IP* چند پخشی در ۲۳ بیت کم ارزش آدرس لایه *MAC*بدست آید. این نگاشت در شکل زیر نشان داده شده است :



شکل ۱۳- نگاشت آدرسهای ***IP*** کلاس ***D*** به آدرسهای چند پخشی اترنت

۲-۵ پروتکل مدیریت گروهی اینترنت *(IGMP)*

میزبانهایی که مایلند بسته های چند پخشی را دریافت کنند باید روترهای نزدیک بدون واسط خود را از اینکه علاقمند دریافت پیامهای چند پخشی ارسال شده در یک گروه چند پخشی خاص هستند آگاه سازند. بدینگونه، هر نود می تواند عضو یک یا بیشتر گروه چند پخشی شوند و پیغامهای ارسالی در آن گروه را دریافت کنند. پروتکلی که میزبانها این اطلاعات را با روترهای همسایه شان به کمک آن تبادل می کنند پروتکل مدیریت گروهی اینترنت[۱] نامیده می شود.

*IGMP*همچنین توسط روترها به منظور بررسی دوره ای اینکه اعضای گروه یک گروه شناخته شده همچنان فعال هستند یا نه استفاده می شود. درحالتی که بیش ازیک روتر چند پخشی بر روی یک زیر شبکه *(LAN)* یک روتر بعنوان "پرسشگر "[۲] انتخاب می شود. این روتر وظیفه پیگیری وضعیت اعضای گروه های چند پخشی ای که در این زیر شبکه عضو فعال دارند را دارد. بر اساس اطلاعات بدست آمده از *IGMP* روتر تصمیم می‌گیرد که آیا پیام چند پخشی را درزیر شبکه خود ارسال کند یانه ؟ بعد از دریافت یک بسته چند پخشی ارسال شده به یک گروه چند پخشی خاص روتر بررسی می کند که آیا حداقل یک عضو از آن گروه در زیر شبکه خود دارد یا نه ؟

---

[۱] *Internet Group Management Protocol (IGMP)*

[۲] *querier*

اگر اینگونه باشد بسته را به زیر شبکه اش هدایت می کند و در غیر اینصورت بسته را دور می ریزد. نیازی به گفتن نیست که این آخرین مرحله از مراحل تحویل یک بسته چند پخشی است.

۵-۳ الگوریتمهای مسیریابی چند پخشی

چندین الگوریتم برای ساختن درخت چند پخشی پیشنهاد شده است. این الگوریتمها می توانند بصورت بالقوه در پیاده سازی پروتکل مسیریابی چند پخشی استفاده شوند. برای شروع از دو الگوریتم ساده *flooding* و *Spanning trees* استفاده می کنیم. سپس درباره الگوریتمهای پیچیده تری مانند *Reverse Path Forwarding (RPF)* ، *Truncated Reverse Path Forwarding (TRPF)*، *Steiner Trees (ST)* و *Core-Based Trees (CBT)*را به بحث می گذاریم.

۵-۳-۱ *Flooding*

الگوریتم *flooding* که در حال حاضر در پروتکلهایی همچون *OSPF* استفاده می شود ساده ترین تکنیک برای ارسال بسته های چند پخشی به مسیریابهای یک *internetwork* است. در این الگوریتم وقتی یک روتر یک بسته چند پخشی را دریافت می کند ابتدا بررسی می کند که آیا قبلاً این بسته را دریافت کرده است یا نه ؟ اگر اولین بار است که این بسته را دریافت می کند، روتر بسادگی بسته را بر روی همه *interface* های خود – بجز *interface* ای که بسته را از آن دریافت کرده است – هدایت[1] می کند. در صورت تکراری بودن بسته آن را دور می اندازد. با این شیوه می توانیم مطمئن شویم که همه روترها در *internetwork* حداقل یک نسخه از بسته را دریافت کرده اند.

اگر چه این الگوریتم بسیار ساده است ولی مشکلات عدیده ای دارد. الگوریتم *flooding* تعداد زیادی بسته تکراری در شبکه تولید می کند که باعث هدر رفتن پهنای باند شبکه می شود. علاوه بر این، چون هر روتر باید وضعیت بسته هایی که دریافت می کند را نگهداری کند تا بر اساس آن بررسی کند که آیا هر بسته را قبلاً دریافت

[1] *Forward*

کرده است یا نه ، روتر نیازمند آن است که یک مدخل برای هر بسته دریافتی در جدول خود نگهداری کند. بنا براین، الگوریتم *flooding* از منابع حافظه ای روترها استفاده نامناسب می‌کند.

۵-۳-۲ درختهای پوشا [۱]

الگوریتم بهتری که ارائه شده است الگوریتم درختهای پوشا است. این الگوریتم که در حال حاضر توسط پروتکل *IEEE-802 MAC* استفاده می شود الگوریتمی قدرتمند و از نظر اجرا ساده است. در این الگوریتم، یک زیر مجموعه از لینکهای شبکه برای ساخت یک درخت بین نودها انتخاب می شوند. در این درخت تنها یک مسیر فعال بین هر دو روتر وجود دارد. بدلیل اینکه این درخت همه نودهای شبکه را پوشش می‌دهد به آن درخت پوشا گفته می‌شود. هرگاه یک روتر یک بسته چند پخشی را دریافت می کند بسته را تنها بر روی لینکهایی هدایت می کند که عضو درخت پوشا هستند، - البته بجز لینکی که بسته را از آن دریافت کرده است. –اینکار تضمین می کند که همه روترها در شبکه بسته را دریافت کنند. خوبی این الگوریتم این است که تنها اطلاعاتی که یک روتر نیاز به نگهداری دارد یک متغیر بولین به ازای هر *Interface* است که نشان دهد این لینک متعلق به درخت پوشا هست یا نه ؟

البته این الگوریتم دو مشکل دارد : همه ترافیک را بر روی مجموعه کوچکی از نودها توزیع می کند که می تواند باعث ازدحام در این لینکها شود. دوم اینکه عضویت روترها در گروه های چند پخشی را در نظر نمی‌گیرد.

۵-۳-۳ *Reverse Path Broadcasting (RPB)*

الگوریتم *RPB* که هم اکنون در پروتکل *MBone*[۲] استفاده می شود بهبودی است بر الگوریتم درخت پوشا. در این الگوریتم بجای ساختن یک درخت پوشای در سطح شبکه، یک درخت پوشای ضمنی برای هر منبع ساخته می‌شود. بر اساس این الگوریتم هرگاه یک روتر یک بسته چند پخشی را بر روی لینک L و از منبع S دریافت می

---

[۱] *Spanning Tree*

[۲] *Multicast Backbone*

کند، روتر بررسی می کند که آیا لینک L به کوتاهترین مسیر به سمت S است یا نه؟ اگر اینگونه است بسته بر روی همه لینکها بجز L هدایت می شود. در غیر اینصورت بسته دور انداخته می شود.

این الگوریتم در عین سادگی در پیاده سازی، کارآمد نیز می باشد. علاوه بر این چون بسته ها از طریق کوتاهترین مسیر از نود مبدا به مقاصد می رسد بسیار سریع نیز می باشد. الگوریتم *RPB* به هیچ مکانیزمی برای اینکه بداند به چه لینکهای نباید بفرستد نیاز ندارد. روتر نیاز ندارد که کل درخت پوشا را نگه دارد و بدلیل اینکه بسته ها از درختهای پوشای مختلفی (نه الزاماً یک درخت پوشای منحصر بفرد) ارسال می شوند ترافیک در شبکه پخش می شود و مشکل تمرکز بسته ها بر روی لینکهای خاص وجود ندارد. با این وجود، الگوریتم *RPB* یک مشکل عمده دارد : درخت توزیع خود را فارغ از اطلاعات عضویت روترها در گروه‌های مختلف چندپخشی می سازد.

۴-۳-۵ *Truncated Reverse Path Broadcasting (TRPB)*

الگوریتم *TRPB* برای غلبه بر بعضی محدودیتهای الگوریتم *RPB* پیشنهاد شده است. پیشتر ذکر شد که به کمک پروتکل *IGMP*، یک روتر می تواند تعیین کند که آیا یک گروه چندپخشی خاص در زیر شبکه متصل به آن عضوی دارد یا نه ؟ اگر این زیرشبکه یک زیر شبکه انتهایی یا برگ باشد (هیچ روتر بعد از آن وجود ندارد) روتر درخت چندپخشی را قطع می کند. البته باید ذکر کرد *TRPB* همانند *PRB* بسته را به روتر همسایه ارسال نخواهد کرد اگر این روتر بر روی کوتاه ترین مسیر از مبدا تا آن نباشد.

اگرچه عضویت روترها در گروه چند پخشی در الگوریتم *TRPB* استفاده می شود و زیر شبکه های برگ از درخت پوشا حذف می شوند ولی ترافیک غیر ضروری بر روی زیرشبکه های غیر برگ که عضوی از گروه در آنها نیست همچنان وجود دارد.

۵-۳-۵ *Reverse Path Multicasting*

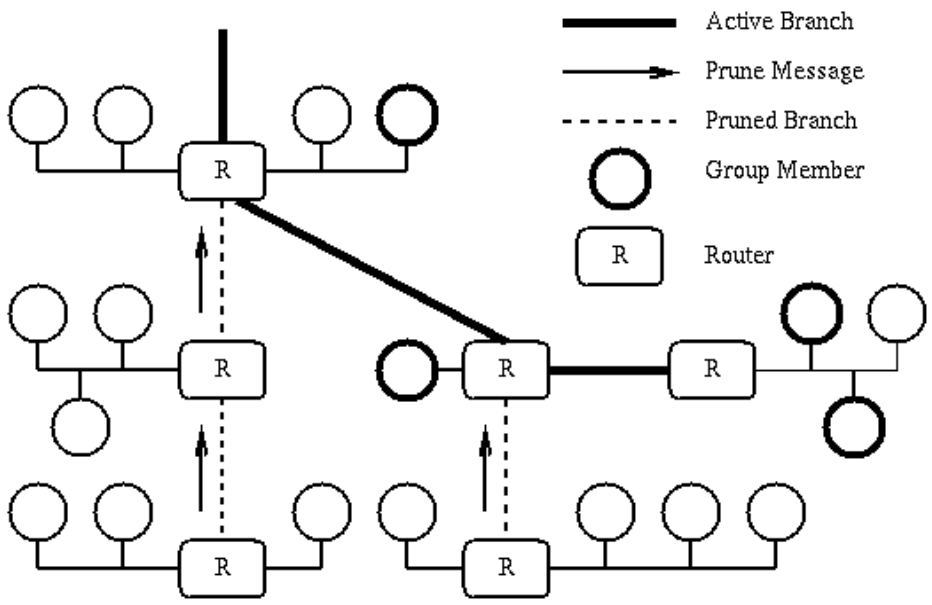
الگوریتم *TRPB* (که بعنوان *RPB* همراه با هرس نیز شناخته می شود) توسعه است بر الگوریتمهای *RPB* و *TRPB*. *RPM* درختی برای تحویل بسته ها می سازد که تنها نودهایی زیر را می پوشاند:

۱) زیر شبکه های شامل اعضای گروه یا

۲) روترها و زیر شبکه هایی که در مسیر کوتاهترین مسیر به زیر شبکه ای هستند که شامل اعضای گروه است.

درخت RPM می‌تواند بگونه ای هرس شود که یک بسته چند پخشی بتواند بر روی لینکهایی که آن را به اعضای گروه مقصد می رساند هدایت شود. برای یک زوج (مبدا، گروه) اولین بسته چند پخشی با الگوریتم $TRPB$ ارسال می‌شود. روترهایی که که هیچ روتر پایین دستی [۱]در درخت $TRPB$ ندارند روترهای برگ نامیده می شوند. اگر یک روتر برگ یک بسته چندپخشی را برای یک زوج (مبدا، گروه) دریافت کند و هیچ عضوی از آن گروه در زیر شبکه خودش نداشته باشد، یک پیغام '' هرس '' برای روتری که بسته چند پخشی را از آن دریافت کرده است می فرستد. دریافت یک پیغام هرس بر روی یک لینک نشان دهنده این است که یک بسته چند پخشی که برای آن زوج (مبدا، گروه) باشد نباید بر روی آن لینک ارسال شود. نکته مهم این است که پیغامهای هرس تنها یک گام به عقب به سمت مبدا فرستاده می‌شوند. روتر بالادستی می بایست اطلاعات هرس دریافتی را در حافظه اش نگهداری کند. از طرف دیگر، اگر روتر بالادستی هیچ عضوی از آن گروه در زیر شبکه محلی خود نداشته باشد و از همه فرزندان خود در درخت $TRPB$ پیغام هرس را دریافت کرده باشد او هم به نوبه خود پیغام هرس را به روتر پدر خود در درخت $TRPB$ می فرستد. به همین صورت پیغامهای هرس به صورت آبشاری درخت $TRPB$ را به گونه ای هرس می‌کند که بسته های چند پخشی تنها بر روی لینکهایی ارسال می‌شوند که نهایتاً به یک مقصد منتهی می‌شوند. شکل زیر هرس و درخت RPM بدست آمده را نشان می دهد.

[۱] *downstream*



شکل ۱۴- الگوریتم ***RPM*** و درخت حاصل از آن

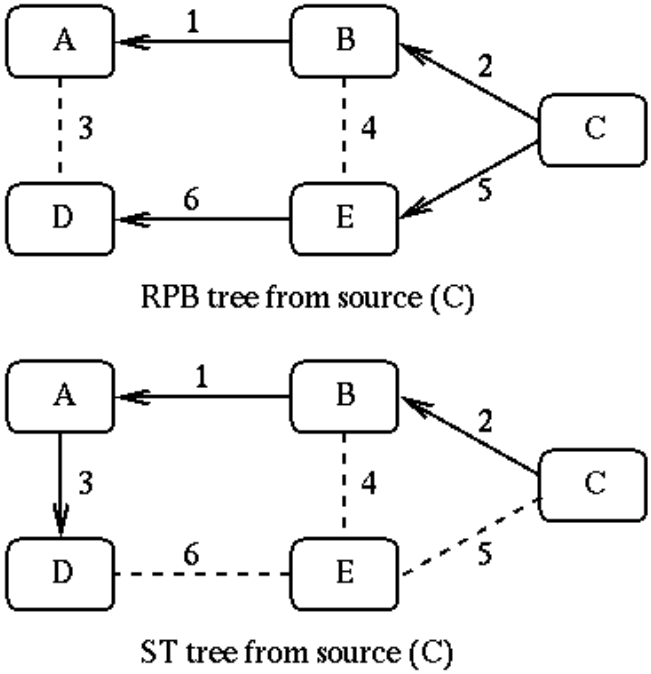
توپولوژی شبکه و عضویت نودها در گروههای چند پخشی دائماً در حال تغییر است و وضعیت هرس درختهای تحویل [۱] باید در بازه های زمانی منظم تازه سازی شود. بنابراین، در الگوریتم *RPM* اطلاعات هرس در روترها بصورت دوره ای حذف می شوند و بسته بعدی مربوط به زوج (مبدا، گروه) دوباره به همه روترهای برگ فرستاده می شود. این اساسی ترین مشکل *RPM* است. همچنین فضای حافظه مورد نیاز نسبتاً بزرگ مورد نیاز این الگوریتم برای نگهداری اطلاعات وضعیت همه زوج های (مبدا، گروه) مشکل دیگری است که مقیاس پذیری این الگوریتم را به خطر می اندازد. – که در نتیجه آن را برای شبکه های خیلی بزرگ نامناسب می‌کند. -

۶-۳-۵ *Steiner Trees (ST)*

در خانواده الگوریتمهای *RPB* (*RPB* ، *TRPB* و *RPM*) کوتاهترین مسیر بین نود منبع و هر نود مقصد برای تحویل بسته های چند پخشی استفاده می‌شود که باعث می شود این بسته ها به سریع ترین شکل ممکن به مقصد برسند. اگرچه هیچ کدام از این الگوریتمها تلاشی برای استفاده حداقلی از منابع شبکه ندارند. در شکل

[۱] *Delivery trees*

۷ درخت RPB و درخت تحویل دیگری برای شبکه مورد نظر نشان داده شده است. فرض این است که C منبع است و A و D گیرندگان بسته هستند.



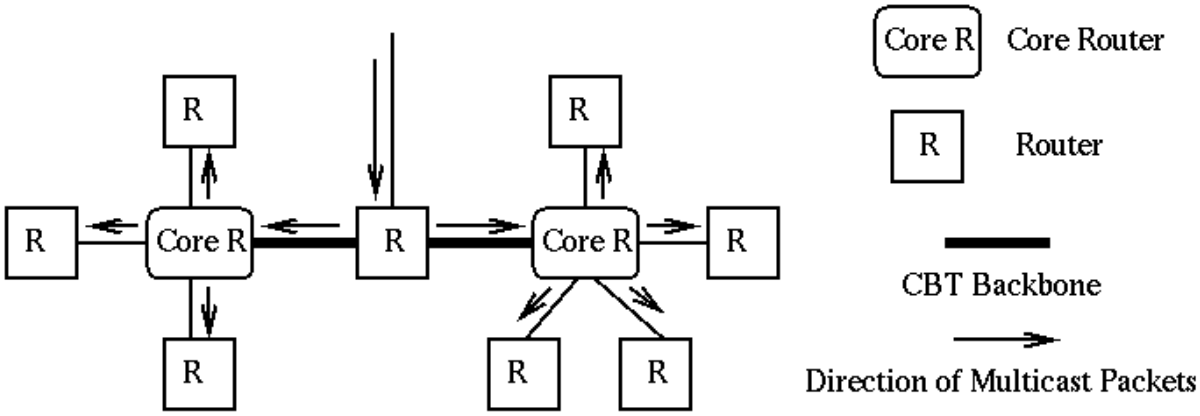
شکل ۱۵- درختهای ***steiner***

براحتی مشاهده می شود که دومین درخت تعداد لینکهای کمتری را به کار می گیرد. اگرچه این درخت از درخت RPB کندتر است – چرا که بسته ها می بایست ۳ گام را بپیمایند تا به D برسند در حالیکه این تعداد در درخت RPBدو گام بود.) این نوع درخت ها درخت اشتاینر خوانده می‌شوند. اگر چه درختهای اشتاینر تعداد لینکهای استفاده شده برای ساخت درخت تحویل را کمینه می‌کنند، پیچیدگی محاسباتی این درختها آنها را از نظر عملی کم اهمیت کرده است. همچنین بدلیل اینکه شکل ST با اضافه شدن یا ترک گروه توسط یک نود تغییر می کند درختهای اشتاینر بسیار ناپایدار نیز می باشند.

۷-۳-۵ *Core-Based Trees (CBT)*

آخرین الگوریتم پیشنهاد شده برای ساخت درختهای تحویل چند پخشی الگوریتم درخت برپایه هسته نامیده می شود. برخلاف سایر الگوریتمهایی که پیشتر بحث کردیم، CBT تنها یک درخت تحویل برای هر گروه می

سازد. به عبارت بهتر، درخت استفاده شده برای هدایت بسته های چند پخشی یک گروه خاص، تنها یک درخت است که فارغ از موقعیت نود مبدا ساخته شده است. یک روتر یا مجموعه ای از روترها بعنوان روترهای هسته درخت تحویل انتخاب می‌شوند. همه پیامهای به یک گروه خاص همانند یک پیام تک پخشی به سمت روترهای هسته ارسال می شوند تا اینکه به روتری برسند که عضو درخت تحویل مربوط به آن گروه هستند. سپس بسته بر روی همه *interface* های خروجی که بخشی از درخت تحویل آن گروه هستند - بجز آنی که بسته از آن دریافت می شود. – ارسال می‌شود. این فرآیند در شکل زیر نشان داده شده است.



شکل ۱۶- درختهای برپایه هسته

بدلیل اینکه *CBT* تنها یک درخت تحویل برای هر گروه چند پخشی می‌سازد، روتر های چند پخشی نیازمند اطلاعات کمتری درمقایسه با سایر الگوریتمهای مسیریابی دارد. *CBT* خیلی در مصرف پهنای باند صرفه جویی می‌کند چرا که نیاز ندارد هیچ بسته چند پخشی ای در شبکه *flood* شود. اگرچه استفاده از تنها یک درخت برای هر گروه ممکن است منجر به تمرکز ترافیک و ایجاد گلوگاه[1] بر روی روترهای هسته کند. داشتن تنها یک درخت تحویل ممکن است منتج به مسیرهای غیر بهینه و بنابراین تاخیر در تحویل بسته ها شود.

[1] *Bottleneck*

الگوریتمهای بحث شده دراین بخش می تواند برای توسعه پروتکلهای مسیریابی استفاده شود. هرکدام از این الگوریتمها نسبت به بقیه مزایا و معایبی دارد که باعث می‌شود استفاده از آن در بعضی موقعیتها موثرو در سایر موقعیتها کم کارآمدتر باشد.

فصل ۶

نتیجه گیری و چشم‌اندازهای آتی

در این گزارش سعی بر آن شده است یک بررسی کلی از الگوریتمهای چند پخشی در شبکه های داده معمولی آورده شود. دلیل این کار این است که ماهیت شبکه هوشمند همان شبکه داده معمولی است. با این تفاوت که نیازمندیهای تاخیر و پهنای باند و غیره *application* های مختلف متفاوت است . این شبکه داده باید همه این نیازمندیها را بصورت متمرکز برآورده کند. ولی این الگوریتمها که در فصل پنجم مروری بر آنها آورده شده است واجد بیشتر این نیازمندیها نیستند. مشکل عمده ای که این الگوریتمها از آن رنج می برند امنیت است. همانطور که در بحث ۴-۱ مطرح شد امنیت در زیرساخت شبکه هوشمند مسئله بسیار مهمی است و الگوریتمهایی که برای چند پخشی مطرح شده اند یا مسئله امنیت را در نظر نگرفته اند یا اینکه بار محاسباتی بالایی بر دوش نودها می گذارند. در شبکه های هوشمند عموماً نودها توان محاسباتی و ظرفیت ذخیره سازی کمی دارند. مسئله دیگری نیز که در شبکه های هوشمند باید در نظر گرفته شود ناهمگونی این شبکه ها است. نودها در شبکه هایی با رسانه های ناهمگونی به سیستم مرکزی کنترل *SCADA* متصل هستند و این مسئله پیاده سازی سرویسهای مختلف از جمله چند پخشی را بر روی آن مشکل می سازد.

مراجع

[1] T. Baumeister, "Literature Review on Smart Grid Cyber Security," 2010.

*[2]*ورهراممحمدهادی, ناهیسعید, داوریفرمهرداد *and* ,داوریابوالفضل, "سیستمهایدیسپاچینگمدرنواتوماسیونشبکههادرایران. ".

[3] National Institue of Standards and Technology, "WebHome<SmartGrid<TWiki."[Online].Available:

http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WebHome. [Accessed: 22-Sep-2012].

[4] M. Kezunovic, "Intelligent Alarm Processor." [Online]. Available: http://www.ercot.com/content/meetings/ros/keydocs/2006/0810/11._Intelligent_Alarm_Processor_Kezunovic_July_24_2006.pdf. [Accessed: 22-Sep-2012].

[5] S. Natti and M. Kezunovic, "Transmission System Equipment Maintenance: On-line Use of Circuit Breaker Condition Data," in IEEE Power Engineering Society General Meeting, 2007, 2007, pp. 1 –7.

[6] C. H. Hauser, T. Manivannan, and D. E. Bakken, "Evaluating Multicast Message Authentication Protocols for Use in Wide Area Power Grid Data Delivery Services," in 2012 45th Hawaii International Conference on System Science (HICSS), 2012, pp. 2151–2158.

[7] L. Su, B. Ding, Y. Yang, T. F. Abdelzaher, G. Cao, and J. C. Hou, "oCast: Optimal multicast routing protocol for wireless sensor networks," 2009, pp. 151–160.

[8] W. Gao, Q. Li, B. Zhao, and G. Cao, "Multicasting in delay tolerant networks: a social network perspective," in Proceedings of the tenth ACM international symposium on Mobile ad hoc networking and computing, New York, NY, USA, 2009, pp. 299–308.

[9] Qinghua Li and Guohong Cao, "Multicast Authentication in the Smart Grid With One-Time Signature," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 686–696, Dec. 2011.

[10] Z. Begic and M. Bolic, "Security in Multicast Networks," in IEEE International Symposium on Signal Processing and Information Technology, 2008. ISSPIT 2008, 2008, pp. 352–356.

[11] LihaoXu and Cheng Huang, "Computation-Efficient Multicast Key Distribution," IEEE Transactions on Parallel and Distributed Systems, vol. 19, no. 5, pp. 577–587, May 2008.

[12] Donghyun Choi, Hakman Kim, Dongho Won, and Seungjoo Kim, "Advanced Key-Management Architecture for Secure SCADA Communications," IEEE Transactions on Power Delivery, vol. 24, no. 3, pp. 1154–1163, Jul. 2009.

[13] Donghyun Choi, Sungjin Lee, Dongho Won, and Seungjoo Kim, "Efficient Secure Group Communications for SCADA," IEEE Transactions on Power Delivery, vol. 25, no. 2, pp. 714–722, Apr. 2010.