فهرست

فصل ۱ مقدمه ۱

۱-۱- پیشگفتار ۲

۱-۲- مروری بر کارهای انجام شده ٤

۱-۳- هدف از انجام پایان‌نامه ۷

۱-۴- ساختار پایان‌نامه ۸

فصل ۲ سیستم‌های SCADA در شبکه قدرت ۹

۲-۱- مقدمه ۱۰

۲-۲- تاریخچه سیستم SCADA ۱۰

۲-۲-۱- نسل اول (MONOLITHIC) ۱۱

۲-۲-۲- نسل دوم (Distributed) ۱۳

۲-۲-۳- نسل سوم (Networking) ۱٤

۲-۳- سیستم SCADA در شبکه قدرت ۱۵

۲-۳-۱- مرکز کنترل (MTU) ۱۵

۲-۳-۲- ایستگاه راه دور (RTU) ۱۸

۲-۳-۳- تجهیزات ارتباطی در سیستم SCADA ۱۹

۲-۴- نرم‌افزارهای مربوط به سیستم SCADA ۲۰

۲-۵- ساختار سیستم اتوماسیون یک پست برق ۲۲

۲-۵-۱- حفاظت ۲۳

۲-۵-۲- کنترل ۲۳

۲-۵-۳- اندازه‌گیری ۲٤

۲-۵-٤- مانیتورینگ ۲٤

۲-۶- پیغامهای داده‌ای در یک پست برق ۲۵

۲-۷- سیستم‌های اندازه‌گیری ناحیه گسترده ۲۷

۲-۷-۱- تأخیر در سیستم‌های اندازه‌گیری ناحیه گسترده ۲۸

۲-۷-۲- عوامل مؤثر بر تأخیرها در WAMS ۳۰

۲-۷-۳- محاسبه تأخیرهای ارتباطی ۳۳

فصل ۳ شبکه‌های ارتباطی و پروتکل TCP/IP ۳۵
۳-۱- مقدمه ۳۶
۳-۲- تعریف پروتکل ارتباطی ۳۷
۳-۳- مدل مرجع OSI ۳۸
۳-۴- پروتکل TCP/IP ۴۱
۳-۵- لایه‌های پروتکل TCP/IP ۴۲
۳-۵-۱- لایه کاربرد (Application) ۴۳
۳-۵-۲- لایه انتقال (Transport) ۴۴
۳-۵-۳- لایه اینترنت (Internet) ۴۴
۳-۵-۴- لایه واسط شبکه (Network Interface) ۴۵
۳-۶- تشخیص برنامه‌ها با استفاده از TCP/IP ۴۶
۳-۶-۱- آدرس IP ۴۶
۳-۶-۲- درگاه TCP/UDP ۴۶
۳-۶-۳- سوکت ۴۷
۳-۷- همزمانی در TCP/IP ۴۷
۳-۷-۱- پروتکل زمانی شبکه ۴۸
۳-۷-۲- زمان مهرشده در لایه کاربرد SNTP/NTP ۵۰
۳-۷-۳- زمان مهرشده در لایه نرم‌افزاری اترنت ۵۱
۳-۷-۴- زمان مهرشده در لایه فیزیکی/ لایه داده‌ای اترنت ۵۱
۳-۸- تجهیزات شبکه ارتباطی ۵۳
۳-۸-۱- تکرارکننده‌ها ۵۳
۳-۸-۲- پل‌ها و سگمنت ۵۳
۳-۸-۳- مسیریابها ۵۴
۳-۸-۴- سوئیچ‌ها ۵۴
فصل ۴ سیستم‌های SCADA مبتنی بر TCP/IP ۵۶
۴-۱- مقدمه ۵۷
۴-۲- شبکه‌های ارتباطی مدرن در شبکه قدرت ۵۷

۴-۳- شبکه ارتباط مستقیم ۵۹
۴-۳-۱- شبکه اترنت (استاندارد IEEE 802.3) ۶۰
۴-۳-۲- شبکه‌های حلقه- نشانه (استاندارد IEEE 802.5) ۶۳
۴-۳-۳- شبکه کنترل‌نت (ControlNet) ۶۳
۴-۳-۴- شبکه دیوایس‌نت (DeviceNet) ۶۴
۴-۴- پروتکل شبکه‌ای پشت به پشت ۶۵
۴-۵- استفاده از فن‌آوری اطلاعات در سیستم‌های قدرت ۶۶
۴-۶- فن‌آوریهای نرم افزاری ۶۸
۴-۶-۱- فن‌آوری سرویس‌دهنده/مشتری ۶۸
۴-۶-۲- برنامه‌های تحت شبکه ۶۹
۴-۶-۳- فن‌آوری XML ۷۰
۴-۶-۴- زبان برنامه‌نویسی جاوا ۷۰
۴-۶-۵- برنامه‌نویسی بانک اطلاعاتی ۷۱
۴-۷- الگویی از یک سیستم SCADA مبتنی بر وب ۷۳
۴-۷-۱- تابع JavaCON ۷۵
۴-۷-۲- بانک‌های اطلاعاتی ۷۵
۴-۷-۳- تابع مشتری ۷۶
۴-۷-۴- واسط انسان- ماشین (MMI) ۷۶
فصل ۵ بررسی اثر تأخیر در شبکه‌های ارتباطی ۷۷
۵-۱- مقدمه ۷۸
۵-۲- اثر تأخیر زمانی بر عملکرد سیستم SCADA ۷۸
۵-۳- مدل تحلیلی رگرسیون خودکار ۸۰
۵-۴- اثر تأخیر زمانی در طراحی کنترل کننده ۸۳
فصل ۶ مدل اطلاعاتی سیستم قدرت و شبیه‌سازی ۸۸
۶-۱- مقدمه ۸۹
۶-۲- مدل کلاسیک سیستم قدرت ۸۹
۶-۲-۱- مدل اطلاعاتی سیستم قدرت بدون اختلال (Unperturbed) ۹۰

٦-٢-٢- مدل اطلاعاتی سیستم قدرت با اختلال (Perturbed) ٩١
۶-۳- مدل غیرخطی سیستم اطلاعاتی ۹۳
٦-٣-١- مدل غیرخطی سیستم اطلاعاتی بدون اختلال ٩٣
٦-٣-٢- مدل غیرخطی سیستم اطلاعاتی با اختلال ٩٤
۶-۴- پیاده‌سازی مدل اطلاعاتی شبکه قدرت ۹۵
٦-٤-١- مدل پایدارساز سیستم قدرت (PSS) ٩٦
٦-٤-٢- ارسال اطلاعات بر روی شبکه محلی (LAN) ٩٧
٦-٤-٣- ارسال اطلاعات با استفاده از خط Dial ١٠٤
فصل ۷ نتیجه‌گیری و پیشنهادات ۱۰۷
۷-۱- نتیجه‌گیری ۱۰۸
۷-۲- پیشنهادات ۱۰۸
مراجع ۱۱۰
واژه‌نامه انگلیسی - فارسی ۱۱۶

فهرست شکلها

شکل ۱-۱ چرخه اندازه‌گیری، اطلاعات و تصمیم گیری در یک شبکه قدرت ۳

شکل ۱-۲ شمای سیستم اطلاعاتی در سیستم قدرت ٤

شکل ۲-۱ نسل اول سیستم SCADA ۱۳

شکل ۲-۲ نسل دوم از سیستم SCADA ۱٤

شکل ۲-۳ نسل سوم از سیستم SCADA ۱۵

شکل ۲-۴ بلاک دیاگرام یک مرکز کنترل ۱٦

شکل ۲-۵ بلاک دیاگرام یک RTU ۱۹

شکل ۲-۶ معماری پست برق مدرن ۲۲

شکل ۲-۷ مدل مرجع واسط جهت یک پست برق ۲۵

شکل ۲-۸ ساختار WAMS به همراه کاربردهای PMUها ۲۸

شکل ۲-۹ بلاک دیاگرام تأخیر در سیستم قدرت ۳۰

شکل ۳-۱ مدل هفت لایه‌ای OSI ۳۸

شکل ۳-۲ پروتکل‌های مربوط به TCP/IP ٤۳

شکل ۳-۳ مقایسه‌ای بین مدل مرجع OSI و پروتکل TCP/IP ٤٤

شکل ۳-۴ فرآیندهای مربوط به درگاه TCP ٤۷

شکل ۳-۵ زمان مهر شده در لایه کاربرد SNTP/NTP ۵۰

شکل ۳-۶ یک پیاده‌سازی همزمانی در TCP/IP ۵۱

شکل ۴-۱ معماری ارائه شده توسط UCA ۵۸

شکل ۴-۲ یک الگوی معماری سرویس‌دهنده/مشتری سه ردیفه ٦۹

شکل ۴-۳ پیکربندی POWERNET در سیستم SCADA ۷٤

شکل ۴-۴ توابع مربوط به سرویس‌دهنده WSDS ۷۵

شکل ۴-۵ فرآیند تولید دیاگرام تک- خطی ۷۶
شکل ۵-۱ توپولوژی درختی یک سیستم SCADA ۷۹
شکل ۵-۲ میزان اندازه خطای تأخیر مربوط به انتشار ۸۰
شکل ۵-۳ خطای اندازه‌گیری به صورت تابعی از تأخیر سیستم ارتباطی و پهنای باند ۸۳
جدول ۵-۱ ضرایب تابع تبدیل PADÉ ۸۶
شکل ۵-۴ ارتباط دو سیستم فضای حالت ۸۶
شکل ۶-۱ پاسخ پله ولتاژ رویت شده ۹۱
شکل ۶-۲ مدل پیاده‌سازی‌شده با استفاده از SIMULINK-MATLAB ۹۵
شکل ۶-۳ ارسال داده‌های اندازه‌گیری بر روی شبکه محلی (LAN) ۹۷
شکل ۶-۴ ولتاژ آنالیز ترتیبی (V_{ps}) بر روی شبکه محلی (LAN) ۹۸
شکل ۶- ۵ توان اکتیو (P) بر روی شبکه محلی (LAN) ۹۹
شکل ۶- ۶ مشتق زاویه فاز ماشین ($\dot{\theta}$) بر روی شبکه محلی (LAN) ۱۰۰
شکل ۶- ۷ فرکانس ماشین (ω) بر روی شبکه محلی (LAN) ۱۰۱
شکل ۶- ۸ توان مکانیکی ماشین (P_a) بر روی شبکه محلی (LAN) ۱۰۲
شکل ۶- ۹ ولتاژ ترمینال ماشین (V_t) بر روی شبکه محلی (LAN) ۱۰۳
شکل ۶- ۱۰ تأخیر در شبکه محلی (LAN) ۱۰۴
شکل ۶- ۱۱ تأخیر بر روی خط DIAL ۱۰۵
شکل ۶- ۱۲ ولتاژ آنالیز ترتیبی(V_{ps}) در خط DIAL ۱۰۵
شکل ۶- ۱۳ تأخیر بر روی خط DIAL ۱۰۶

فهرست جداول

جدول ۲-۱ زمان مورد نیاز برای توزیع پیغامهای داده‌ای در پست برق ۲۵

جدول ۲-۲ سرعت توزیع پیغامهای داده‌ای در پست برق ۲۶

جدول ۲-۳ تأخیر در برخی از رسانه‌های ارتباطی ۳۴

جدول ۴-۱ برخی از فن‌آوریهای مربوط به شبکه ارتباط مستقیم ۶۱

فصل ۱

مقدمه

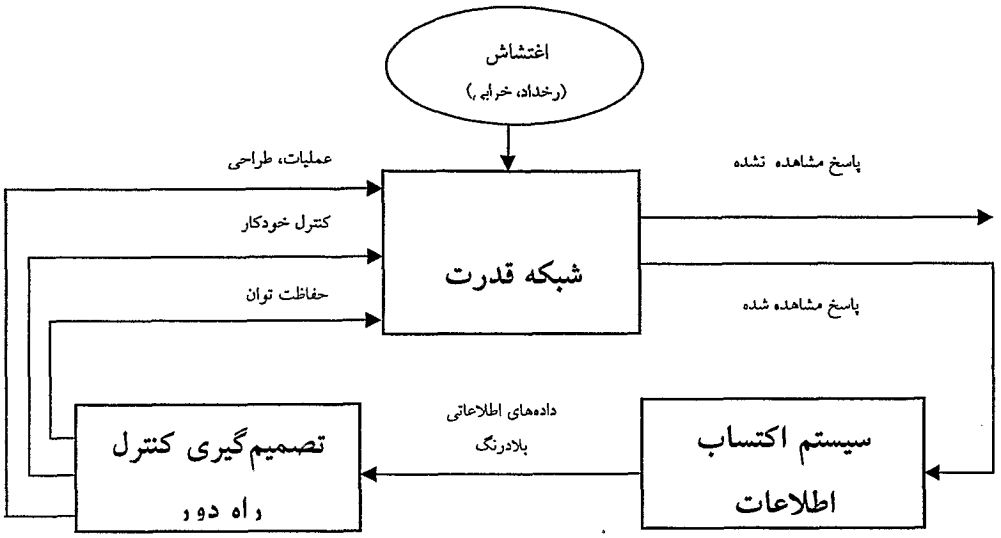
۱-۱- پیشگفتار

امروزه سیستم‌های کنترل نظارتی و اکتساب داده‌ای (SCADA[1]) در سیستم‌های قدرت، ساختار اصلی بخشهایی همچون سیستم مدیریت توزیع (DMS[2]) و سیستم مدیریت انرژی (EMS[3]) را تشکیل می‌دهند[۱]. مقررات‌زدایی[4]، یکپارچگی اطلاعات و دسترسی باز[5] به سیستم‌های قدرت را به‌گونه‌ای مهیا ساخته، تا تبادل اطلاعات داده‌ای، تجمع و انتشار آنها جهت مطالبات درون سازمانی و برون‌سازمانی با دقت بالایی فراهم شوند. در یک سیستم SCADA، داده‌های مورد نیاز و به‌هنگام، بایستی به صورت بلادرنگ جهت پردازش توسط فرآیندهای توزیعی و نیز فرمانهای کنترلی درسطح جغرافیایی گسترده‌ای در اختیار مرکز کنترل قرار گیرند تا اپراتورهای عملیاتی قادر به پاسخگویی به تمامی شرایط رخ داده در شبکه قدرت باشند.

دریافت داده‌های اطلاعاتی بلادرنگ با سرعت بالا و انتقال این داده‌ها به‌صورت گسترده، از عوامل کلیدی جهت کنترل بهینه یک شبکه قدرت محسوب می‌شوند[۲]. همانطور که درشکل ۱-۱ نشان داده شده، چرخه میان داده‌های اندازه‌گیری، اطلاعات مربوط به شبکه قدرت و همچنین تصمیم‌گیری در خصوص پاسخگویی به یک فرآیند مشاهده می‌شود[۳]. در اینجا با داشتن داده‌های اندازه‌گیری به صورت بلادرنگ و با سرعت بالا، جهت فراهم نمودن قابلیت اطمینان در شبکه قدرت در صورت بروز اختلال، اعمال کنترلی و حفاظتی مناسبی را خواهد داشت.

---

1 Supervisory Control And Data Acquisition
2 Distributed Management System
3 Energy Management System
4 Deregulation
5 Open Access



شکل ۱-۱ چرخه اندازه‌گیری، اطلاعات و تصمیم گیری در یک شبکه قدرت[۳]

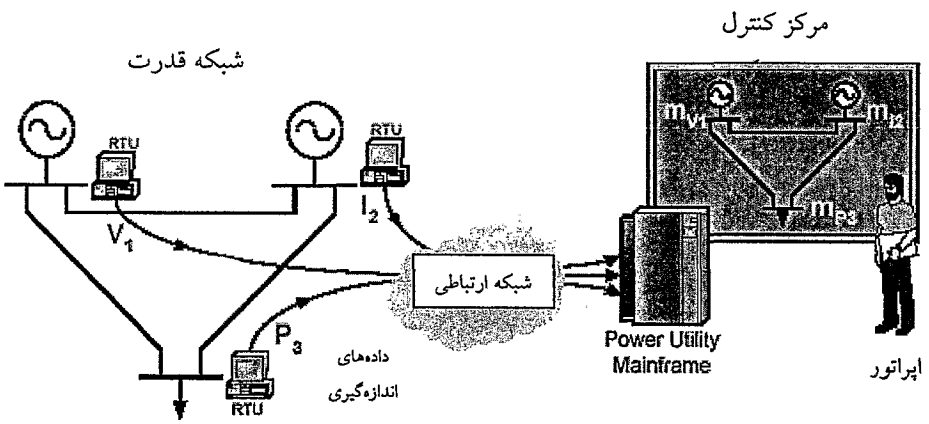
امروزه با گسترش خدمات شبکه‌ای همچون کنترل گسترده به‌صورت بلادرنگ، ادوات FACTS[1] و دسترسی به داده‌های اطلاعاتی مورد نیاز، وجود یک شبکه ارتباطی با پهنای باند بالا احساس می‌شود[٤]. هم‌اکنون بیشتر واحدهای برق، رسانه‌های ارتباطی مختلفی را جهت برآوردن خواسته‌های مورد نیاز خود به خدمت گرفته‌اند.

تا گذشته‌ای نه چندان دور یک سیستم SCADA به صورت یک سیستم یکپارچه بود که به‌صورت مستقل کار می‌کرد و شبکه‌های ارتباطی نقش کمرنگی را در آن ایفا می‌نمود. امروزه این سیستم‌ها برای بهره‌گیری هرچه بیشتر از امکانات صوت، داده و کنترل جریان داده‌ای[2] مستلزم استفاده از شبکه‌های محلی و گسترده می‌باشند تا بگونه‌ای قابلیت انعطاف‌پذیری بیشتری درشبکه‌های ارتباطی را از خود نشان دهند. در پیاده‌سازی سیستم امروزی SCADA، هدف پایین‌آوردن هرچه بیشتر تأخیرزمانی درجهت پاسخگویی به یک فرمان مورد نظر است و این موضوع از اهمیت خاصی برخوردار بوده، که پاسخ به یک آلارم با چه سرعت و مدت زمانی به مرکز کنترل می‌رسد و اپراتور را از وجود آن آگاه می‌نماید.

---

[1] Flexible AC Transmission System
[2] Control Data Stream

امروزه سیستم اطلاعاتی توسعه یافته در شبکه قدرت مدرن به گونه‌ای طراحی می‌شود که بتواند در مقایسه با شبکه‌های قدرت سنتی مواردی همچون مانیتورینگ، کنترل و قابلیتهای ارتباطی گسترده‌تری را فراهم نماید. همانگونه که در شکل ۱-۲ مشاهده می‌شود، فرآیند ارتباطی در یک سیستم اطلاعاتی در شبکه قدرت که شامل شبکه قدرت، سیستم اندازه‌گیری، شبکه ارتباطی و مرکز کنترل می‌باشد نشان داده شده است.



شکل ۱-۲ شمای سیستم اطلاعاتی در شبکه قدرت

در این فرآیند، کامپیوترهای RTU اندازه‌گیریهای مربوط به شبکه قدرت را ثبت نموده و به‌صورت بلادرنگ از طریق شبکه ارتباطی به مرکز کنترل ارسال می‌دارند. مرکز کنترل نیز قابلیت ارسال پیام به کامپیوترهای RTU را به‌منظور کنترل اعمالی از قبیل باز و بسته نمودن بریکرها، تغییر تپ ترانسفورمر و کنترل تولید ... برعهده دارد. در این فرآیند برخی مشخصه‌های تصادفی مربوط به شبکه کامپیوتری را خواهیم داشت که بر دقت اندازه‌گیریهای ارسالی اثر گذاشته و نیز مقادیر زیاد ترافیک در شبکه ارتباطی امکان بروز خطاهای بزرگ اندازه‌گیری را باعث می‌شود که ممکن است به‌صورت موقت بخشهایی از شبکه قدرت را بدون مشاهده باقی گذارد.

۱-۲- مروری بر کارهای انجام شده

در شبکه‌های قدرت سنتی، روشهای رؤیت‌پذیری [۷-۵] جهت چگونگی وضعیت قابل اندازه‌گیری یک شبکه قدرت مورد استفاده قرار می‌گرفت که در صورت رؤیت‌پذیر بودن، الگوریتم‌های تخمین حالت[۱۰-۸] قابلیت انجام محاسبه وضعیت غیرقابل اندازه‌گیری سیستم را خواهد داشت. این روشها

به‌طور گسترده‌ای در مراکز کنترل و مانیتورینگ موارد استفاده دارند بدین‌صورت که یک شبکه قدرت را با شرایط عملیاتی در حالت پایدار در نظر گرفته و خطاهای مربوط به اندازه‌گیریها را به دلایل تأخیر در ارسال و تحویل داده‌ها نادیده فرض می‌نمود. به‌عبارت دیگر در روشهای مانیتورینگ سنتی حالت شبکه قدرت در طول فرآیند اندازه‌گیری بدون تغییر باقی می‌ماند.

در اینجا هدف بررسی مشخصه‌ی خطاهای اندازه‌گیری به علت تأخیرهای تصادفی(MDE[1]) مربوط به ارسال و تحویل داده‌های اندازه‌گیری می‌باشد که در هنگام استفاده از توابع کنترل مدرن در یک مرکز کنترل از اهمیت خاصی برخوردار بوده، که خود امکان دقت بیشتری جهت مدلهای مربوط به شبکه قدرت را به‌صورت بلادرنگ در مقیاس زمانی بهتری فراهم می‌نماید.

در سالهای اخیر تلاشهای تحقیقاتی فراوانی در زمینه بررسی اثرات تأخیر در شبکه‌های کامپیوتر- کنترل آغاز گردیده است که چگونگی خطاهای ارسال و تحویل داده‌های اندازه‌گیری در امتداد شبکه ارتباطی را مورد بررسی قرار می‌دهند. یک مطالعه شبیه‌سازی با استفاده ازMatlab توسطF. L. Lian، J. R. Moyne و D. M. Tilbury [۱۱] صورت گرفته است که هدف آنها تعیین پارامترهای کلیدی مربوط به انواع مختلف شبکه‌های کامپیوتری ارتباط- مستقیم[2] می‌باشد. این پارامترها شامل فرآیند شبکه‌ای[3]، میزان تأخیرهای زمانی قابل قبول و همچنین مشخصه‌های مربوط به این تأخیرها می‌باشد. شبکه‌های تحلیل شده در اینجا شامل اترنت[4]، کنترل‌نت[5] و دیوایس‌نت[6] می‌باشند که نتایج این شبیه‌سازیها سطح ترافیک شبکه‌ای مربوط به اندازه بسته‌های داده‌ای را تعیین می‌کند. نویسندگان این مقاله قصد ارائه تحلیل و مقایسه تأخیر زمانی پیامها را داشته که این مسئله جهت طراحان سیستم‌های کنترل- کامپیوتری بسیار مفید می‌باشد.

---

[1] Measurement Delay Errors
[2] Direct Link
[3] Network Utilization
[4] Ethernet
[5] ControlNet
[6] DeviceNet

S. Johannessen, T. Skeie و C. Brunner [۱۲] در مقاله خود تحقیق کرده‌اند که آیا شبکه اترنت مشخصه‌های اجرائی کافی جهت تقاضاهای بلادرنگ اتوماسیون یک پست برق[1] را دارا می‌باشد که در اینجا با استفاده از نرم افزار شبیه‌سازی OPNET، پیاده‌سازی را با استفاده از پروتکلهای TCP و UDP به‌صورت بلادرنگ انجام داده‌اند. آنها بررسی کرده‌اند که آیا شبکه اترنت سریع[2] مبتنی بر سوئیچ قابلیت اجرای پیکربندی اتوماسیون یک پست برق را تحت شرایط بار آزمایشی داشته، و به این نتیجه رسیده‌اند که پروتکلهایTCP و UDP قادر به برآوردن مطالبات زمانی سیستم بوده و این در صورتی جوابگو خواهد بود که میزبانهای نهایی ماشینهایی با کارایی بالایی را به خدمت گرفته باشند.

مقاله‌ای تحت عنوان یک مدل تحلیلی جهت ارتباط میان خطاهای اندازه‌گیری و تأخیر زمانی توسط J. Luque, J. I. Escudero و F. Perez [۱۳] انجام شده است. آنها میزان اندازه‌گیریهای مربوط به شبکه قدرت را توسط فرآیند AR[3] مرتبه اول مدل نموده‌اند که این مدل خطای مربوط به اندازه‌گیری‌ها را به صورت تابعی از تأخیر در شبکه ارتباطی و پهنای باند مخابراتی مربوطه ارزیابی نموده است.

C. L. Su و C. N. Lu [۱۴] در مقاله خود با استفاده از یک فیلتر کالمن توسعه یافته اتفاقی(SEKF[4]) قصد فراهم نمودن تخمینهای بهینه‌ای از حالات شبکه ارتباطی را در صورت وجود تأخیر در شبکه قدرت نشان داده‌اند. روش کار بدین‌صورت است که میزان تأخیرهای مربوط به داده‌های مبادله شده به‌صورت آماری ثبت شده است که هر کدام از این اندازه‌گیریها به‌همراه تأخیرهای مربوطه در مرکز

---

[1] Substation
[2] Fast Ethernet
[3] Autoregressive
[4] Stochastic Extended Kalman Filter

کنترل نمونه‌برداری می‌شوند. در اینجا با استفاده از یک تکنیک استاندارد تخمین حالت شبکه قدرت به‌نام حداقل مربعات وزنی(WLS[1]) این نتایج را مقایسه نموده‌اند.

S. P. Carullo و C. Nwankpa [۱۵] نیز در مقاله خود یک مدل از شبکه قدرت را به همراه سیستم اطلاعاتی ارائه داده‌اند که مطالعات خطای اندازه‌گیریهای مربوط به سیستم‌ارتباطی را در اثر ترافیک موجود بر روی یک شبکه اترنت نشان داده است. در اینجا با استفاده از پروتکلهای TCP/IP و UDP و همچنین مدلهای بیان شده جهت سیستم اطلاعاتی، شبیه‌سازی ولتاژ اندازه‌گیری شده و همچنین خطای اندازه‌گیری از سوی کامپیوتر RTU به مرکز کنترل را نشان داده‌اند.

۱-۳- هدف از انجام پایان‌نامه

استفاده از شبکه‌های ارتباطی مدرن در شبکه قدرت امروزی، انگیزه مطالعه و بررسی اثرات ترافیک بر روی شبکه‌های ارتباطی را ایجاد کرده، بگونه‌ای که تاکنون تحقیقات زیادی در زمینه تحلیل چگونگی اثرات تأخیرهای تصادفی (به دلیل ترافیک شبکه ارتباطی) بر روی سیستم‌های اطلاعاتی انجام شده است. این تأخیرها می‌توانند بر میزان دقت اندازه‌گیری‌های مربوط به شبکه قدرت اثرات فراوانی داشته باشند.

درسالهای اخیر فن‌آوری TCP/IP محدودیت‌های موجود در شبکه‌های ارتباطی را از میان برداشته و به شبکه‌ها این توانایی را داده است تا با پیکربندی وگسترش ارتباطات، انعطاف‌پذیری بیشتری از خود نشان دهند. یکی از مزایای مهم کاربرد پروتکلTCP/IP استفاده از آن در شبکه‌های ارتباطی امروزی سیستم SCADA می‌باشد که سعی بر آن است تا با پیاده‌سازی سیستم‌های SCADA مبتنی بر این پروتکل ارتباطی، عملیات مربوطه را با همان کیفیت عملیاتی سیستمهای معمول داشت. در این پایان‌نامه با ارائه و پیاده‌سازی مدلی از سیستم اطلاعاتی شبکه قدرت، هدف شبیه‌سازی و تخمین

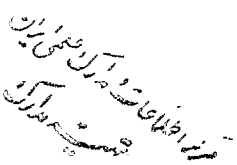
---

[1] Weighted Least Square

میزان اثر تأخیرهای مربوط به داده‌های ارسالی بر روی شبکه ارتباطی مربوط به یک سیستم SCADA می‌باشد. در نهایت، نتایج این شبیه‌سازی با مدلی از یک شبکه قدرت واقعی مقایسه می‌گردد.

۱-۴- ساختار پایان‌نامه

در فصل اول مقدمه‌ای بر سیستم‌های اطلاعاتی در شبکه قدرت ارائه می‌شود که شامل مروری بر کارهای انجام شده در خصوص اثرات تأخیر در شبکه ارتباطی می‌باشد. فصل دوم ساختار سیستم SCADA و اجزاء مرتبط با آن را بررسی می‌نماید. در فصل سوم تعریف شبکه‌های ارتباطی و پروتکل TCP/IP در شبکه‌های ارتباطی بررسی می‌گردد. فصل چهارم سیستم‌های SCADA را مبتنی بر پروتکل TCP/IP بررسی می‌نماید که در این فصل استفاده از فن‌آوری اطلاعات در شبکه‌های قدرت امروزی نیز بیان می‌گردد. در فصل پنجم اثرات تأخیر در سیستم‌های ارتباطی با ارائه چند مدل بررسی می‌شود. یک مدل تخمینی جهت بررسی اثر تأخیر در اندازه‌گیریهای ارسالی در شبکه قدرت با پیاده‌سازی عملی بر روی شبکه کامپیوتری محلی و خطوط ارتباطی تلفنی در فصل ششم ارائه خواهد شد. نتایج شبیه‌سازی و پیاده‌سازی در این فصل بحث و تحلیل خواهد گردید. سرانجام در فصل هفتم بحث و نتیجه‌گیری پایان‌نامه و پیشنهادات در خصوص کارهای آینده آورده شده است.



فصل ۲

سیستم‌های SCADA در شبکه قدرت

۲-۱- مقدمه

مؤسسه ملی استانداردهای آمریکا (ANSI[1]) یک سیستم SCADA را به‌صورت یک سیستم عملیاتی با سیگنال‌های کدشده بر روی کانال‌های مخابراتی تعریف می‌نماید که این سیستم جهت فراهم نمودن کنترل از راه دور تجهیزات در یک واحد صنعتی مورد استفاده قرار می‌گیرد[۱۶]. یک سیستم SCADA دارای یک سیستم نظارتی و نیز شامل یک سیستم اکتساب داده‌ای می‌باشد که با تجمع سیگنالهای کدشده بر روی کانالهای مخابراتی، اطلاعات دقیقی در مورد انجام یا ثبت اعمال مربوط به تجهیزات راه دور در اختیار مرکز کنترل قرار می‌دهد. مرکز کنترل نیز معمولاً شامل ایستگاه اصلی (MTU[2]) است که توسط سیستم ارتباطی با تعداد زیادی ایستگاه راه دور (RTU[3]) در تماس می‌باشد. همچنین مجموعه‌ای از استانداردهای نرم‌افزاری جهت مانیتورینگ و کنترل از راه دور تجهیزات واحد صنعتی را شامل می‌شود. امروزه سیستم‌های SCADA مشخصه‌های کنترلی حلقه-باز را به‌طور گسترده‌ای برای مسافتهای بسیار دور مورد استفاده قرار می‌دهند که اگر چه ممکن است بیشتر این مشخصه‌ها به‌صورت کنترل حلقه- بسته و یا در مسافتهای کوتاه قرار داشته باشند. به عبارت دیگر سیستم‌هایSCADA گستره وسیعی را پوشش داده که جهت ارتباطات خود از سیستم‌های ارتباطی بهره می‌گیرند.

۲-۲- تاریخچه سیستم SCADA

تا قبل از سال ۱۹۹۰ میلادی در یک سیستم SCADA از RTUهایی استفاده می‌شد که با استفاده از کنترل‌کننده‌هایی به همراه ماژولهای I/O[4] در مکانهایی دور از مرکز کنترل داده‌های مورد نیاز

---

[1] American National Standards Inistitute
[2] Master Terminal Unit
[3] Remote Terminal Unit
[4] Input/Output

اطلاعاتی را از طریق شبکه Telemetry به مرکز کنترل ارسال می‌نمود[۱۷]. در دهه‌ی ۸۰ میلادی استفاده از فن‌آوری سیستم کنترل توزیع‌شده (DCS[1]) جهت کنترل یک فرآیند صنعتی آغاز گردید که این فن‌آوری یک سیستم کنترلی به‌صورت توزیع شده را فراهم می‌نمود و در حالیکه اعمال متمرکزی را انجام می‌داد دارای زیر سیستم‌های کوچکتری بود که این زیر سیستم‌ها به‌طور مستقل و دور از هم قرار داشتند. با توسعه سیستم‌های DCS و استفاده از کنترل کننده‌های قابل برنامه‌ریزی (PLC[2]) که هوشمندی بیشتری نسبت به RTUهای نسل گذشته داشتند کنترل یک فرآیند به‌طور مستقل و بدون آنکه با مرکز کنترل تماسی داشته باشد انجام می‌گرفت. در اواخر دهه ۹۰ شباهتهای یک سیستم SCADA و DCS بیشتر به هم نزدیک شد بگونه‌ای که سیستم‌های SCADA قابلیتهای DCS را داشت و بالعکس. امروزه این سیستم‌ها توسط طراحان با اهدافی مشخص در جهت کنترل بهینه‌تر یک فرآیند کنترلی موارد استفاده دارند به‌طوریکه که بتوانند جهت ارتباطات داده‌ای، با بهره‌گرفتن از سیستم‌های ارتباطی توسعه یافته‌ی امروزی از قبیل پروتکلهای ارتباطی(TCP/IP وUDP) و شبکه اینترنت را با دسترسی بیشتری به خدمت گیرند[۳]. در ادامه موارد گفته شده برای درک بهتر از نحوه عملکرد سیستم‌های امروزی SCADA مبتنی بر پروتکل TCP/IP نیازمند آن هستیم که توسعه سیستم SCADA را طی سه نسل مختلف معماری مورد بررسی قرار دهیم که این امر باعث می‌گردد تا با دانش بیشتری نسبت به تغییر سیستم فعلی آن به‌سیستم‌های جدیدتر اقدام نموده و ارتباطات مورد نیاز آن را با مسائل تجاری و صنعتی امروزی سازگار نمائیم.

۲-۲-۱- نسل اول (Monolithic)

در ابتدای شروع کار سیستم‌های SCADA، محاسبات بر روی یک سیستم یکپارچه همچون Mainframeها انجام می‌شد. عموماً شبکه‌ای وجود نداشت و سیستم‌ها به صورت منفرد کار

---

[1] Distributed Control System
[2] Programmable Logic Controllers

می‌کردند. هنگامیکه استفاده از شبکه‌های گسترده (WAN[1]) جهت ارتباطات شبکه‌ای طراحی و پیاده‌سازی شدند RTUها جای بیشتری را در صنعت برای خود باز نمودند و لذا قادر به ارتباط با MTU از طریق شبکه‌های گسترده شدند. البته پروتکل‌های مربوط به شبکه‌های گسترده درآن زمان به گستردگی امروزی نبوده است[۱۸].

پروتکل‌های استفاده شده در شبکه‌های SCADA توسط تجهیزات RTU به صورت اختصاصی طراحی و پیاده‌سازی می‌شدند. این بدان معنا بود که پروتکل‌های RTU همواره متناسب با نوع محصول، کارخانه، نحوه دسترسی و ارتباطات آماده‌سازی می‌شدند. لذا یک سری محدودیت در به‌کارگیری آنها در کاربردها و یا شرایط متفاوت مشاهده می‌شد. از طرف دیگر این پروتکل‌ها، خیلی متکی به پشتیبانی مجازی و عوامل محدود کننده دیگر نیز بودند. لذا امکان‌پذیر نبود که انواع مختلفی از ترافیک داده‌ای ناشی از ارتباطات RTU را بر روی یک شبکه با هم ادغام نمود. اتصال به ایستگاه MTU بسیار محدود بود و اتصالات معمولاً از نوع Level Bus بوده و نیز از آداپتورها و یا کنترل‌کننده‌های خاص جهت اتصال به پردازنده مرکزی استفاده می‌شد.

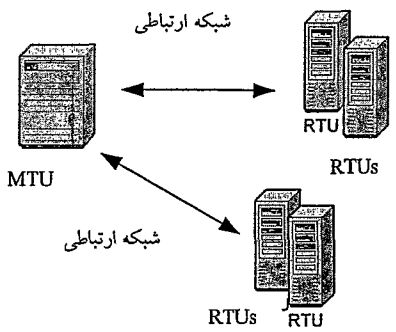
مسئله Redundancy- و اجتناب از بروز خطا در سیستم‌های نسل اول بوسیله استفاده از دو سیستم Mainframe یکسان متصل شده به باس اصلی، تا حدودی مطرح و حل شده بود. یکی از سیستم‌ها به صورت سیستم اصلی[2] و سیستم ثانویه به عنوان سیستم آماده‌بکار[3]، تنظیم می‌شد. سیستم ثانویه نیز به‌گونه‌ای تنظیم می‌گردید که قادر به مانیتور کردن و در اختیار گرفتن مسئولیت‌های سیستم اصلی در صورت بروز خطا بود.

در این حالت برای اتصال با سیستم‌های خارجی از ارتباطات سریال با سرعت پایین همچون استاندارد RS232 استفاده می‌شد. به‌طور خلاصه می‌توان گفت که نسل اول سیستم‌هایSCADA به

---

[1] Wide Area Network
[2] Primary System
[3] Standby System

سخت افزار، نرم‌افزار و دستگاه‌های جانبی محدود می‌شد که توسط سازندگان تولید می‌شدند. شکل ۲-۱ یک معماری نسل اول سیستم SCADA را نشان می‌دهد.



شکل ۲-۱ نسل اول از سیستم SCADA

۲-۲-۲- نسل دوم (Distributed)

نسل دوم سیستم SCADA با پیشرفت و توسعه فن‌آوری شبکه‌های محلی (LAN[1]) و حرکت به‌سوی هرچه کوچکتر کردن سیستم و توزیع پردازش‌ها توسط چندین سیستم شکل گرفت. هرکدام از ایستگاه‌های چندگانه[2]، توابع خاص خود را داشتند و نهایتاً به شبکه‌های LAN مربوطه متصل می‌شدند و اطلاعات خود را به صورت بلادرنگ در اختیار دیگران قرار می‌دادند. این ایستگاه‌ها در حقیقت نوعی ریز کامپیوتر بودند که نسبت به نسل اول کوچکتر و ارزان قیمت‌تر تمام می‌شدند[۱۸].

در اینجا می‌توان دو دسته ایستگاه توزیع شده را تعریف نمود:

۱- ایستگاه ارتباطی[3]: از این ایستگاه‌های توزیع‌شده به‌عنوان پردازنده‌های ارتباطی، استفاده می‌شد و ارتباط اصلی با دستگاه‌هایی همچون RTUها را برقرار می‌کردند.

۲- ایستگاه اپراتوری[4]: این ایستگاه به‌عنوان فراهم‌کننده یک واسط جهت کاربران سیستم مورد استفاده قرار می‌گرفت که به آن واسط انسان- ماشین (HMI[5]) می‌گفتند.

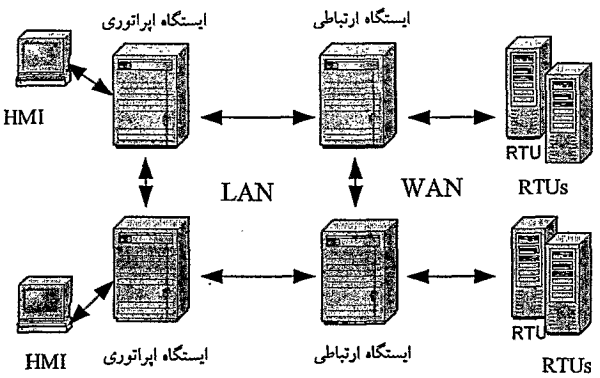
---

[1] Local Area Network
[2] Multiple Stations
[3] Communications Station
[4] Operator Station
[5] Human Machine Interface

در شبکه‌های مورد استفاده در اینگونه سیستم‌ها معمولاً از پروتکل‌های LAN استفاده می‌شد، البته خود این موضوع به دلیل محدود بودن مسافت مورد استفاده، یک محدودیت بشمار می‌رفت که معمولاً فاصله بین ایستگاه‌ها بر روی شبکه حداکثر ۱۸۰ متر بود.

از مزایای این نسل نسبت به نسل اول می‌توان به توسعه Redundancy و قابلیت اطمینان سیستم‌ها و افزایش قدرت پردازش اشاره نمود. به عنوان مثال اگر یک ایستگاه HMI دچار خرابی گردد، ایستگاه HMI دیگری بدون هیچ وقفه‌ای بجای آن انجام وظیفه خواهد نمود. بر خلاف نسل اول، در این معماری تمامی ایستگاه‌ها بر روی شبکه و به صورت Online مشغول به فعالیت بودند.

این نسل نیز همانند نسل اول سیستم‌هایSCADA همچنان وابسته بود به سخت‌افزار، نرم‌افزار و دستگاه‌های جانبی که توسط سازندگان تهیه می‌شدند. شکل ۲-۲ یک سیستم SCADA نسل دوم را نشان می‌دهد.

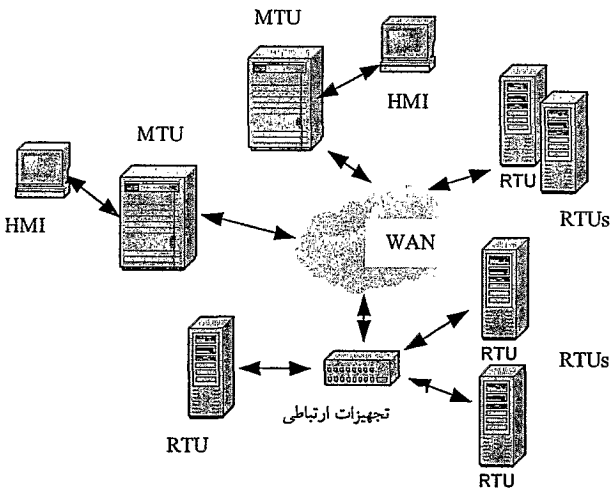


شکل ۲-۲ نسل دوم از سیستم SCADA

۲-۲-۳- نسل سوم (Networking)

نسل سوم سیستم‌هایSCADA ارتباط بسیار نزدیکی با نسل دوم دارد. شاید از جمله تفاوتهای اصلی بین آنها به معماری سیستم باز، کنترل‌های اختصاصی مربوط به سازندگان و محیطهای اختصاصی بتوان اشاره نمود. همانند نسل قبلی، در اینجا سیستم‌های شبکه‌ای چندگانه و به صورت منابع مشترک بین ایستگاه‌ها و پروتکل‌های اختصاصی مربوط به RTUها توسط سازندگان را داریم. شاید پیشرفت اصلی در نسل سوم، استفاده از معماری سیستم باز و به‌کارگیری استانداردها و پروتکل‌های ارتباطی و نیز امکان استفاده از توابع مربوط به سیستم SCADA به صورت توزیع‌شده و منطبق بر

سیستم‌های شبکه‌ای گسترده علاوه بر شبکه محلی باشد[۱۹]. در اینجا بخشی از ایستگاه اصلی که مسئول ارتباطات شبکه‌ای می‌باشد می‌تواند به صورت مستقل به فعالیت خود ادامه دهد. در شکل۲-۳ نسل سوم از سیستم SCADA را می‌توان مشاهده نمود.



شکل ۲-۳ نسل سوم از سیستم SCADA

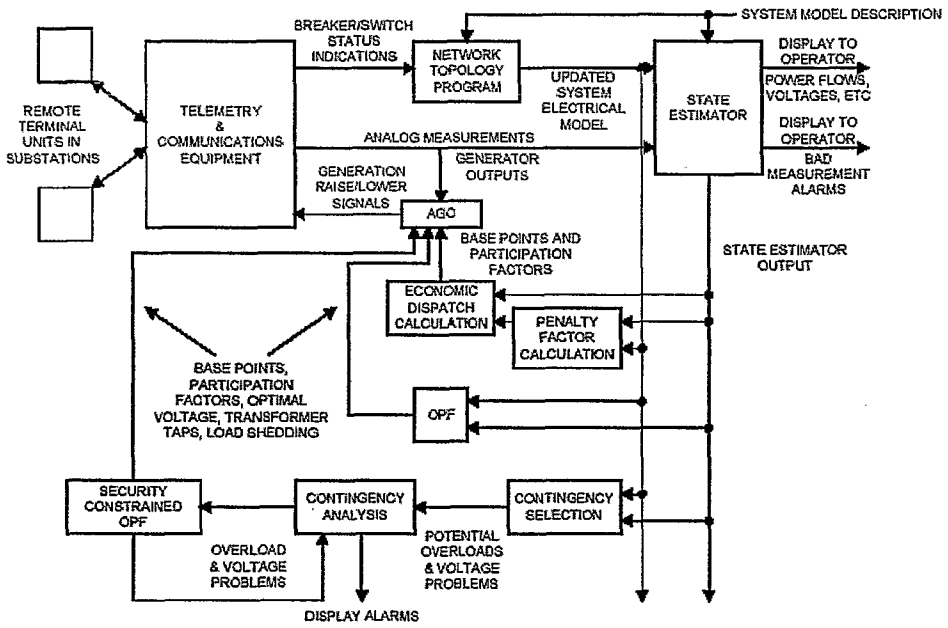
۲-۳- سیستم SCADA در شبکه قدرت

یک سیستم SCADA که امروزه در شبکه قدرت مورد استفاده قرار می‌گیرد شامل ٤ جزء مرکز کنترل، ایستگاه راه دور (RTU)، تجهیزات ارتباطی و نرم‌افزارهای مربوط به سیستم SCADA در شبکه قدرت می‌باشد که شرح هر کدام از آنها از نظر گذرانده می‌شود.

۲-۳-۱- مرکز کنترل (MTU)

مرکز کنترل معمولاً به‌عنوان جزء اصلی یا قلب یک سیستم SCADA می‌باشد و به‌طور مجازی واسطی است میان اپراتور و سیستم ارتباطی که اپراتور را از طریق آن با عملیات انجام شده در واحد صنعتی به‌صورت از راه دور آگاه می‌سازد. همانگونه که می‌دانیم در صنعت برق یک سیستم SCADA وظیفه مانیتورینگ، کنترل به‌صورت از راه دور پستهای برق و تجهیزات تولیدی را بر عهده دارد. داده‌های ارسالی به‌صورت بلادرنگ از طرف RTU در یک بانک اطلاعاتی در مرکز کنترل ذخیره می‌شوند تا جهت بسیاری از برنامه‌های کاربردی شبکه قدرت مورد استفاده قرارگیرند. در این

بانک‌اطلاعاتی برنامه‌های گوناگونی از قبیل تخمین حالت یک سیستم قدرت، عملیات مربوط به سیستم اقتصادی مطمئن[1] و برنامه تشخیص امنیت سیستم در مواقع بروز خطا در تجهیزات شبکه قدرت و یا خروج از مسیر یک خط انتقال قرار دارد[۲۰]. شکل ۲-٤ بلاک دیاگرام یک مرکز کنترل را به‌طور نمونه نشان می‌دهد. در این شکل برخی از فرآیندهای مربوط به چگونگی ارسال داده‌های اندازه‌گیری از کامپیوترهای RTU به مرکز کنترل در طول مسیر یک شبکه ارتباطی مشاهده می‌گردد.



شکل ۲-۴ بلاک دیاگرام یک مرکز کنترل[۲۰]

به‌عنوان مثال در یک مرکز کنترل داده‌های اندازه‌گیری ورودی از سوی خروجی یک ژنراتور می‌توانند به‌طور مستقیم توسط برنامه کنترل تولید خودکار (AGC[2]) مورد استفاده قرارگیرند. تمامی داده‌های وارد شده قبل از استفاده توسط برنامه‌های کاربردی، نیازمند آن است که توسط تخمینگر حالت پردازش شوند. نتایج بدست آمده به صورت تخمین حالت می‌توانند به‌عنوان پایه‌ای جهت توابع مربوط به امنیت یک سیستم قدرت به صورت بلادرنگ استفاده شوند. در مرکز کنترل تخمین حالت،

---

[1] Ensure Economic System
[2] Automatic Generation Control

یک تابع کلیدی جهت ساختار بلادرنگ در شبکه قدرت می‌باشد. برای مثال مدل بلادرنگ-Quasi Static Mathematical شرایط جاری مربوط به یک شبکه قدرت از قبیل ولتاژهای باس مربوطه و زوایای فاز را نشان می‌دهد[۲۱]. این مدل در فواصلی که اندازه‌های اطلاعاتی بلادرنگ (آنالوگ و/یا وضعیت) ارسالی به سیستم SCADA می‌رسند می‌تواند مورد استفاده قرارگیرد.

با پیشرفت وسایل کنترلی دیجیتال جدید مورد استفاده در شبکه‌های قدرت، نیاز بیشتری به این می‌باشد که این تجهیزات در فواصل زمانی کوتاه‌تری جهت کنترل مقاوم[۱]، "تجدید"[۲] و یا "به‌هنگام"[۳] گردند. در اینجا پهنای باند بالای شبکه‌های مخابراتی جهت فراهم نمودن نرخ نمونه‌برداری سریعتر به مدل این اجازه را خواهد داد تا در فواصل زمانی کمتری به هنگام گردد[۲۱].

پیش ازآنکه تخمینگر حالت اجرا شود بایستی همبندی[۴] شبکه قدرت معین باشد که این همبندی اتصالات فیزیکی مربوط به شبکه قدرت و همچنین چگونگی اطلاعات مربوط به اتصال خطوط انتقال به بار و باسهای تولید را شامل می‌شود. بنابراین هرگونه تغییری در کلیدها[۵] و سوئیچها در هر پست برق بر همبندی شبکه تأثیر خواهد گذاشت که در اینجا برنامه‌ای مورد نیاز است تا وضعیت نشانگرهای کلید/سوئیچ مخابره‌شده را خوانده و نیز مدل الکتریکی سیستم را دوباره‌سازی نماید[۲۰]. این برنامه در شکل ۲-۴ به‌صورت "برنامه همبندی شبکه"[۶] نمایش داده شده است که می‌تواند شامل توصیف کاملی از هر پست برق و چگونگی اتصال خطوط انتقال با تجهیزات پست برق باشد. همانگونه که در شکل ۲-۴ مشاهده می‌شود خروجی برنامه همبندی شبکه به‌همراه اندازه‌گیریهای مربوطه، به برنامه تخمینگر حالت ارسال می‌شود. در اینجا تخمین حالت به صورت تکنیکی جهت بیان وضعیت یک شبکه قدرت است که عملیات مربوطه را به‌صورت بلادرنگ بر روی

---

[1] Robust Control
[2] Refreshed
[3] Updated
[4] Topology
[5] Breakers
[6] Network Topology Program

اندازه‌گیریهای ثبت شده اجرا می‌نماید[۲۲]. در اینجا دو نمونه از داده‌های بلادرنگ مورد استفاده جهت تخمین حالت به صورت زیر می‌باشند:

۱- داده‌های اندازه‌گیری آنالوگ، که شامل ولتاژ باس‌ها، توان تزریقی حقیقی و راکتیو و همچنین پخش بارهای حقیقی و راکتیو می‌باشند.

۲- داده‌های وضعیت، نیز شامل موقعیتهای بریکر و سوئیچ می‌باشند.

داده‌های آنالوگ معمولاً از طرف ترانسدیوسرها ارسال می‌گردند و داده‌های وضعیت نیز ممکن است از سوی سوئیچها، اتصالات مربوط به کلیدها و یا دیگر وسایل الکترونیکی فرستاده شوند.

۲-۳-۲- ایستگاه راه دور (RTU)

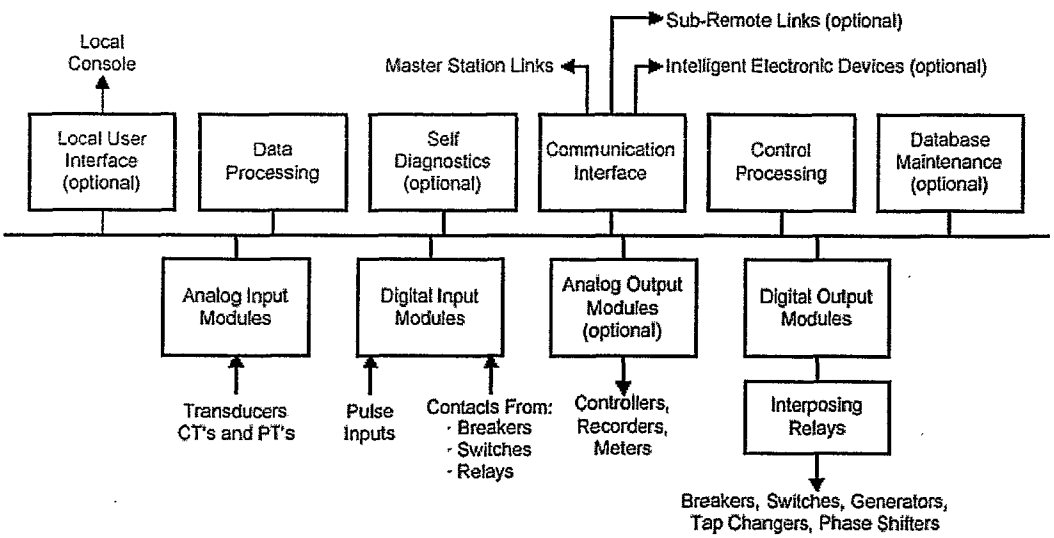
در سیستم SCADA، RTUها در آخرین نقطه از سیستم ارتباطی قرار گرفته‌اند و اعمال مختلفی از قبیل پردازش داده‌های مربوط به تجهیزات و ارسال این داده‌ها بر روی سیستم‌های ارتباطی طی فرآیندی به مرکز کنترل می‌باشد. امروزه اکثر RTUهای مورد استفاده در صنعت برق مبتنی بر طراحی‌های Embedded Microprocessor و یا PLC می‌باشند بدین معنی که گاهی بدون نیاز به MTU فرمان مربوطه را پاسخ می‌دهند. امروزه کامپیوترهای شخصی نیز جهت برخی از RTUها استفاده می‌گردند که این کامپیوترها با بهره‌گرفتن از فن‌آوریهای سطح بالا در پردازش توان عملیاتی و هزینه پایین‌تر قابلیت اجرای توابع عملیاتی زیادی را خواهند داشت[۲۳].

RTUها داده‌های دریافتی را پردازش نموده و توسط پروتکل‌هایی مانند Modbus، TCP/IP و یا یک پروتکل خاص[۲٤] بر روی شبکه ارتباطی می‌فرستند. در اینجا هر RTU جهت ارتباط یک آدرس به خود تخصیص می‌دهد. همانگونه که در شکل ۲-۵ آمده است مؤلفه‌های مختلف یک RTU را نشان می‌دهد که برخی از زیرسیستم‌های ارتباطی آن از قبیل خود تشخیص[1]، پردازش کنترل[2] و بانک

---

[1] Self Diagnostic
[2] Control Processing

اطلاعاتی نگهداری و تعمیرات[1] را نشان داده است. زیر سیستم پردازش داده شامل انتخاب و گزارش مربوط به داده‌های فیلد می‌باشد. داده‌های دیجیتال معمولاً از طرف سوئیچها، اتصالات کلیدها و یا دیگر وسایل الکترونیکی دریافت می‌گردند و داده‌های آنالوگ نیز از طرف ترانسدیوسرها ارسال می‌شوند[۲٤].



شکل ۲-۵ بلاک دیاگرام یک RTU [۲۴]

۲-۳-۳- تجهیزات ارتباطی در سیستم SCADA

امروزه فن‌آوریهای ارتباطی و داده‌ای در یک شبکه قدرت بایستی بگونه‌ای پیاده‌سازی گردند تا بتوانند دریافت و ارسال داده‌های اطلاعاتی را به‌صورت بلادرنگ با کیفیت بالایی فراهم نمایند. به‌طور خلاصه ساختار یک سیستم ارتباطی در شبکه قدرت می‌بایست شرایط زیر را دارا باشد:

۱- دارای پهنای باند بالا جهت مانیتور کردن حجم زیادی از اطلاعات اندازه‌گیری شده باشد.

[1] Maintenance

۲- تأخیرهای قابل قبولی در ارسال و دریافت داده‌ها[1] جهت کنترل و حفاظت بلادرنگ را بر روی شبکه‌های محلی و گسترده فراهم نماید.

امروزه استفاده از رسانه‌های ارتباطی متعددی در شبکه‌های ارتباطی مربوط به سیستم SCADA بکاربرده می‌شوند. این رسانه‌ها می‌بایست قادر باشند یک ارتباط بدون وقفه[2] و دوطرفه[3] را میان RTU و MTU جهت اعمال صحیح دریافت و ارسال داده‌ها برقرار نمایند. به‌طور مثال برخی ار رسانه‌های پرکاربرد مورد استفاده در سیستم‌های SCADA از قبیل خطوط سیمی خصوصی[4]، کابلهای زیر خاکی[5]، خطوط تلفن، رادیو، مودم، دیشهای مایکروویو، ماهواره‌ها و دیگر وسایل اتمسفری را نام برد که در بیشتر مواقع ممکن است ترکیبی از سیستم‌های مخابراتی را نیز جهت برقراری ارتباط از راه دور به خدمت گیرند. مثلاً از ارتباط Dial-up و یا خطوط تلفن اختصاصی، DSL[6]، ISDN[7]، کابل، فیبر نوری، WiFi و همچنین خدمات پهنای باند گسترده[8] جهت کاربردهای خود استفاده کنند[۱۷].

۲-۴- نرم افزارهای مربوط به سیستم SCADA

با روند توسعه سیستم‌های سخت‌افزاری و همچنین روشهای تولید نرم‌افزاری، استفاده ازتکنیک‌های زیر در یک سیستم قدرت امروزی ضروری می‌نماید[۲۵]:

۱- استفاده از فن‌آوری سرویس‌دهنده/ مشتری[9] بر پایه کامپیوتر.

۲- استفاده از استانداردهای مورد نیاز جهت نرم‌افزارها و پروتکلهای مورد استفاده.

---

1 Latency
2 Uninterrupted
3 Bidirectional
4 Private Wire Lines
5 Buried Cable
6 Digital Subscriber Line
7 Integrated Service Digital Network
8 Broadband
9 Server/Client Technology

۳- ضرورت استفاده از نرم افزارهای شئ‌گرا.

بیشتر نرم‌افزارهای مورد استفاده در سیستم SCADA بر پایه ماژولهای مستقل عمل می‌نمایند. بدین‌گونه که برنامه‌های مربوط به پروتکل‌های ارتباطی به نرم‌افزارهای استفاده شده این اجازه را می‌دهند که به‌طور جداگانه و نیز به صورت ترکیبی از یک عملیات یکپارچه قابل اجرا باشند.

به‌طور کلی می‌توان گفت یک سیستم SCADA با استفاده از یک واسط انسان- ماشین (HMI)، ارتباط اپراتور با توابع عملیاتی را در یک سیستم صنعتی فراهم می‌نماید به گونه‌ای که این اپراتور بتواند در شرایط بحرانی اخطارها و آلارم‌ها را براحتی مشاهده نموده، به فرمانهای کنترلی در محیط عملیاتی دسترسی داشته باشد و همچنین از طریق HMI قادر به تغییر نقاط تنظیم[1] مورد نیاز باشد.

امروزه نرم‌افزارهای HMI به‌صورتهای متنوعی ارائه می‌شوند که قادر به نصب بر روی کامپیوترهای شخصی بوده و تحت سیستم‌عاملهای مختلف از قبیلWindows، Unix و ... قابل اجرا می‌باشند. از انواع بسته‌های نرم‌افزاری کاربردی در این زمینه می‌توان Cimplicity (GE-Fanuc)، RSView (Rockwell Automation)، IFIX (Intellution) و InTouch (Wonderware)را نام برد[۲۵]. تمامی این بسته‌های نرم‌افزارهای از ابزارهای Manipulation/Presentation داده‌ای استاندارد جهت گزارش‌گیری و آرشیو داده‌ها استفاده می‌کنند و با کمک گرفتن از نرم‌افزارهای Microsoft Excel، Microsoft Word،Microsoft Access ، SQL و ... می‌توان جهت کاربردهای مربوطه استفاده نمود.

در سیستم‌های توسعه‌یافته امروزی استفاده از فن‌آوریهای مبتنی بر وب[2] در سیستم‌های SCADA نیز مورد استفاده قرار گرفته است که در این فرآیند داده‌های مورد نظر از طرف سیستم SCADA به سرویس‌دهنده‌های وب[3] که به‌طور دینامیکی به‌صورت صفحه‌های نوشته شده به صورت زبان نشانه گذاری فرامتنی (HTML[4]) می‌باشند فرستاده می‌شوند. سپس اطلاعات از طریق این صفحات به

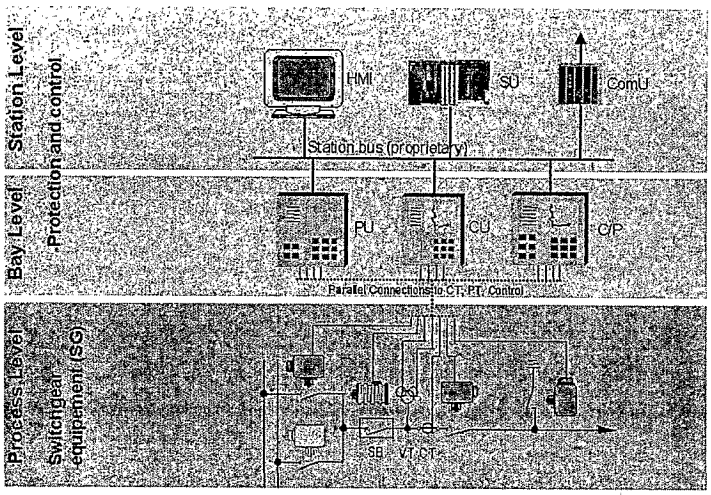
---

[1] Set-points
[2] Web-Based
[3] Web Servers
[4] Hyper Text Markup Language

شبکه محلی واقع در سایت محل اپراتور و یا به‌طور گسترده‌تر به شبکه جهانی اینترنت ارسال می‌گردند.

۲-۵- ساختار سیستم اتوماسیون یک پست برق

در شکل ۲-٦ پیکربندی یک پست برق مدرن مشاهده می‌شود. این پست برق می‌تواند شامل سه سطح پردازش، سطح میانه[1] و سطح ایستگاهی باشد[٢٦].



شکل ۲-۶ معماری پست برق مدرن [۲۶]

در یک پست برق مدرن، IEDها[2] از جمله وسایلی هستند که امروزه کاربردهای فراوانی داشته و بیشتر اعمال مربوط به پست برق توسط آنها صورت می‌گیرد. اتصالات فیزیکی تجهیزات به IEDها به صورت موازی بوده و جهت ارتباط IEDها با واحدهای ایستگاهی (SUs[3]) و ایستگاه HMI از ارتباطات سریال استفاده می‌شود. در اینجا یک واحد ارتباطی (ComU[4]) نیز موجود است که جهت کنترل ارتباط میان تجهیزات و IEDها به صورت یک ارتباط سریال با مرکز کنترل شبکه (NCC[5]) در

---

1 Bay Level
2 Intelligent Electronic Devices
3 Station Units
4 Communications Unit
5 Network Control Centre

تماس می‌باشد. IEDها شامل واحدهای ایستگاهی، واحدهای حفاظت (PUs[1])، واحدهای کنترل (CUs[2]) و گاهی نیز به صورت ترکیبی از هر دو واحد حفاظت و کنترل (C/Ps) می‌باشند[۲۶].

توابع عملیاتی در یک پست برق به‌طور نمونه شامل توابع حفاظت، کنترل، داده‌های اندازه‌گیری، مانیتورینگ، ثبت اغتشاشات رخ‌داده، اکتساب داده‌های مورد نیاز و نیز همزمانی این توابع با یکدیگر می‌باشد که به‌طور اختصار شرح اعمال مربوط به برخی از این توابع عملیاتی به‌صورت زیر آورده شده اند[۲۷].

۲-۵-۱- حفاظت

تمامی توابع مربوط به حفاظت در شبکه قدرت (از جمله حفاظتهای مربوط به خط، ترانسفورماتور، ژنراتور و باس‌بار) در واحد حفاظت (PU) کنترل و اجرا می‌گردند. این حفاظت‌ها شامل حفاظت فاصله[3]، حفاظت جریان بالا (O/C[4])، حفاظت دیفرانسیلی، حفاظت حرارتی، حفاظت باس‌بار و حفاظت خطای مربوط به کلید می‌باشند.

۲-۵-۲- کنترل

توابع کنترلی در یک پست برق به سه کلاس متفاوت شامل توابع "پایه‌ای"، "توسعه‌یافته" و "واحدایستگاهی" تقسیم می‌شوند که در واحدهای کنترل (CUs) و/یا در یک واحد ایستگاهی(SU) اجرا می‌گردند. به‌طور نمونه برخی از توابع کنترلی پایه‌ای از جمله کنترل مدار کلید(CB)، کنترل ایزولاتور(IS)، کنترل سوئیچ زمین (ES[5])، کنترل مربوط به تپ ترانسفورماتور، چک همزمانی (SC[6]) قبل از بسته شدن CB و کنترل ارتباط با NCC می‌باشد. توابع کنترلی توسعه یافته نیز شامل ترتیبهای

---

[1] Protection Units
[2] Control Units
[3] Distance Protection
[4] Overcurrent Protection
[5] Earthing Switch
[6] Synchrocheck

مربوط به سوئیچ‌ها[1]، ایزولاسیون خودکار بخشهای خطا، کلید خودکار هوشمند[2]، Load Shedding هوشمند و ذخیره‌سازی انرژی هوشمند است. توابع کنترل سطح ایستگاهی نیز شامل اتصالات به صورت ایستگاه‌های گسترده[3]، همزمانی مربوط به گستردگی در ایستگاه‌ها، ذخیره داده‌ها در ایستگاه‌های گسترده و انتخاب فایلهای ثبت شده مربوط به اغتشاش، تشخیص و تحلیل آنها می‌باشد.

۲-۵-۳- اندازه‌گیری[4]

در یک پست برق واحدهای کنترل و حفاظت دقت لازم را جهت اهداف اندازه‌گیری نداشته، به همین منظور در اینجا از یک سیستم اندازه‌گیری استفاده می‌شود که با داشتن سخت‌افزار و نرم‌افزار مجزا به صورت مستقل عمل می‌نماید. تجهیزات اندازه‌گیری به هسته‌های مربوط به ترانسفورماتورهای جریان (CT[5]) و ولتاژ (VT[6]) متصل می‌باشند. معمولاً CTها وVTهایی که جهت کنترل و حفاظت مورد استفاده قرار می‌گیرند دقت لازم برای صدور صورتحساب‌ها را نداشته، به همین دلیل از سیستم اندازه‌گیری مربوط به CTها و VTهای مستقل استفاده می‌شود که می‌توانند توسط افراد دیگری که با سیستم اتوماسیون پست برق سر و کار دارند مورد استفاده قرار گیرند.

۲-۵-٤- مانیتورینگ[7]

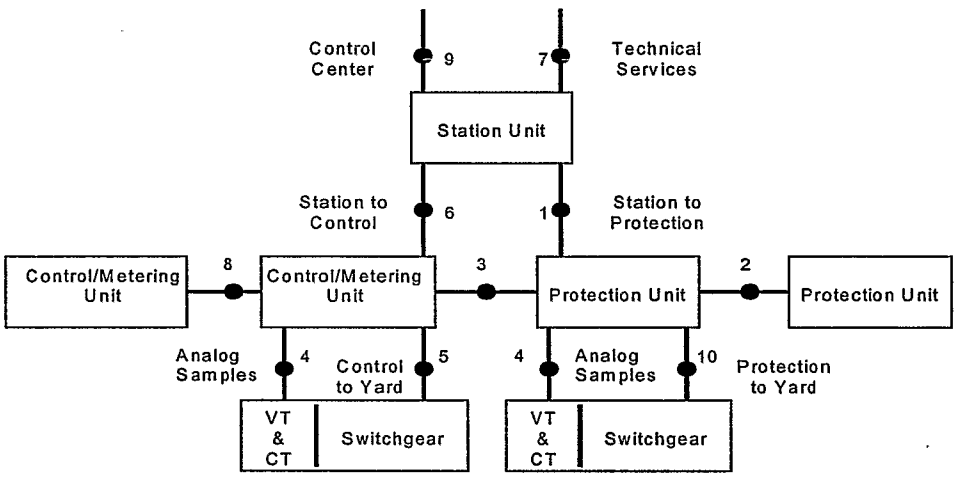
توابع مانیتورینگ در یک پست برق به دو کلاس "پایه‌ای" و "توسعه‌یافته" تقسیم می‌شوند. که به‌عنوان مثال توابع مانیتورینگ کلاس پایه شامل نشانگر وضعیت سوئیچها، اندازه‌گیریها، لیست مربوط به رخدادها و اخطارها می‌باشد. توابع مانیتورینگ کلاس توسعه‌یافته نیز شامل ثبت خرابیها، ثبت اغتشاشات، Trend Curves، محاسبات مربوط به اندازه‌گیریها و شرایط موجود جهت مانیتورینگ می‌باشد.

---

[1] Switching Sequences
[2] Intelligent Auto Reclose
[3] Stationwide Interlocking
[4] Metering
[5] Current Transformers
[6] Voltage Transformers
[7] Monitoring

۲-۶- پیغامهای داده‌ای در یک پست برق

پیرو موارد گفته شده در بخش قبل، شکل ۲-۷ یک مدل مرجع واسط جهت داده‌های اطلاعاتی میان توابع مربوط به یک پست برق را نشان می‌دهد. جدول ۲-۱ نیز زمان مورد نیاز برای توزیع داده‌های اطلاعاتی داخلی و خارجی جهت هر یک از کاربردهای مربوطه در یک پست برق را آورده است.



شکل ۲-۷ مدل مرجع واسط جهت یک پست برق[۲۶]

جدول ۲-۱ زمان مورد نیاز برای توزیع پیغامهای داده‌ای در پست برق[۲۶]

نوع داده‌های اطلاعاتی	داده‌های داخلی پست برق	داده‌های خارجی پست برق
داده‌های حفاظتی- سرعت بالا	۱ ms	٤ ms
داده‌های مانیتورینگ و کنترل- سرعت متوسط	١٦ ms	۱ s
داده‌های عملیاتی و نگهداشت- سرعت پایین	۱ s	۱۰ s
رشته‌های متنی	۲ s	۱۰ s
فایلهای داده‌ای پردازش شده	۱۰ s	۳۰ s
فایلهای برنامه‌ای	٦۰ s	۱۰ min
فایلهای تصویری	۱۰ s	٦۰ s
داده‌های صوتی و ویدئویی	۱ s	۱ s

انتشار و توزیع داده‌ها به صورت بلادرنگ نیازمند آن است که هر کدام از IEDهای پست برق بتوانند با توجه به ترافیک موجود داده‌های مورد نیاز را با یک زمان مشخص ارسال و دریافت نمایند. گاهی تأخیرهای غیر مجاز بر روی شبکه ارتباطی باعث وجود اختلال در اجرای توابع پست برق می‌گردد که هر کدام از عملیات داده‌ای می‌بایست با یک سرعت توزیع مشخص انتقال داده‌ها را در پست برق انجام دهند. در مدل مرجع آورده شده در شکل ۲-۷ همانطور که مشاهده می‌شود هر کدام از واسطهای نشان داده شده دارای سرعت توزیع پیغامهای داده‌ای متفاوتی می‌باشند که به صورت جدول ۲-۲ آورده شده‌اند[۲۶].

جدول ۲-۲ سرعت توزیع پیغامهای داده‌ای در پست برق[۲۶]

واسط ارتباطی	شماره واسط شبکه	سرعت توزیع پیغام (ms)
از کامپیوتر پست برق به حفاظت	۱	۱۰۰>
اطلاع رخداد جهت حفاظت	۲	۲ تا ۱۰
انتقال داده جهت حفاظت		۱۰ تا ۱۰۰
از کنترل به حفاظت	۳	۱۰ تا ۱۰۰
آنالوگهای CT و VT	۴	۲>>
اندازه‌های Synchrophasor		۱۰ تا ۱۰۰
از کنترل به Switchgear	۵	۱۰۰ تا ۲۵۰
از کامپیوتر پست برق به کنترل	۶	۱۰۰ تا ۲۵۰
از کامپیوتر پست برق یا IDE به خدمات فنی	۷	۱۰۰>
از کامپیوتر پست برق یا IDE به مرکز کنترل	۸	۱۰۰>
از کنترل به کنترل	۹	۱۰ تا ۱۰۰
از حفاظت به Switchgear .	۱۰	۲<<

۲-۷- سیستم‌های اندازه‌گیری ناحیه گسترده

امروزه در سیستم‌های SCADA، استفاده از سیستم‌های اندازه‌گیری ناحیه گسترده (WAMS[1]) سناریوی مانیتورینگ و کنترل شبکه قدرت را به‌طور دینامیکی دگرگون نموده است. در بیشتر کنترل‌های به‌صورت بلادرنگ، WAMS نوسانات و ناپایداریهای گذرای شبکه قدرت را کنترل می‌کند. به‌طور یقین تأثیر بیشتر WAMS بستگی به استفاده از فن‌آوریهای جدیدتر همچون FACTS، فن‌آوری اطلاعات و توجه به تأخیرهای مربوط به سیستم ارتباطی در شبکه اطلاعاتی دارد. انواع مختلف رسانه‌های ارتباطی استفاده شده، طول پیغام‌ها و پردازش‌های داده‌ای در شبکه اطلاعاتی، تأخیرهای زمانی را باعث شده که توانایی آن جهت واکنش به خروج از مدار[2] شبکه قدرت را به صورت گذرا نشان می‌دهد. اگر خروج از مدار اتفاق افتاده به صورت محلی و به طور مؤثر کنترل نشود می‌تواند باعث بروز خروج‌های زنجیروار[3] در شبکه قدرت گردد که در نتیجه در ناحیه گسترده‌ای از شبکه قدرت خرابی[4] به بار خواهد آمد[۲۷].

در شبکه‌های قدرت معمول عملیات مربوط به مراکز کنترل محلی برای کنترل خروج‌های زنجیروار به صورت بهینه نمی‌باشد که امروزه استفاده از مراکز حفاظتی ناحیه گسترده (WAPS[5]) باعث افزایش کیفیت و قابلیت اطمینان در شبکه قدرت شده است. در گذشته سیستم‌های SCADA/EMS معمول در مواقع بحرانی قادر به برآوردن کنترل بهینه و پایداری شبکه قدرت در صورت بروز خروج‌های زنجیروار نبودند که با افزایش نیازهای مربوط به داده‌های اطلاعاتی در سیستم امروزی SCADA و همچنین مقررات‌زدایی در شبکه‌های قدرت امروزی، کاربردهای بیشتر استفاده از WAMS نمایان شده است. به عبارت دیگر، WAMS در مقایسه با سیستم‌های SCADA/EMS

---

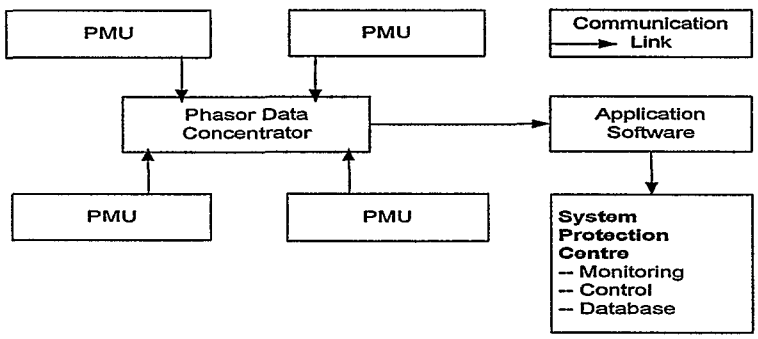
[1] Wide Area Measurement Systems
[2] Outage
[3] Cascaded Outage
[4] Blackout
[5] Wide Area Protection Centers

معمول یک پوشش دینامیکی نسبت به شبکه قدرت ناحیه گسترده جهت برآوردن اعمال پایداری بهینه و هماهنگ، در صورت بروز خروج‌های زنجیروار فراهم می‌نماید[۲۷].

در WAMS از واحدهای اندازه‌گیری فازوری (PMUs[1]) جهت فراهم نمودن اندازه‌گیریهای دینامیکی سیستم‌های توزیع و انتقال شبکه قدرت استفاده می‌گردد.PMUها به پیاده‌سازی شماتیک کنترل و اندازه‌گیری ناحیه گسترده کمک می‌کنند. اعمال اولیه یک PMU شامل اندازه‌های فازوری (ولتاژ/جریان/فرکانس) توسط نمونه‌برداری و پردازش سیگنالهای آنالوگ می‌باشد. تکنیکی که یک PMU جهت تبدیل سیگنالهای آنالوگ به نمونه‌های گسسته مورد استفاده قرار می‌دهد به نام تابع تبدیل فوریه گسسته (DFT[2]) می‌باشد.

۲-۷-۱- تأخیر در سیستم‌های اندازه‌گیری ناحیه گسترده

شکل ۲-۸ ساختاری از WAMS را به همراه کاربردهای PMUها نشان داده است. در اینجا PMUها با استفاده از DFT، فازورهای ولتاژ، جریان و فرکانس را اندازه‌گیری کرده و با سرعتی در حدود چند میلی ثانیه، پردازش و محاسبات مربوطه را بر روی آنها انجام می‌دهند[۲۸].



شکل ۲-۸ ساختار WAMS به همراه کاربردهای PMUها

PMUها جهت انتقال داده‌های اندازه‌گیری به مرکز کنترل از فرمت داده‌ای همزمانی به نام استاندارد IEEE۱۳۴۴ استفاده می‌کنند. در اینجا تأخیرهای انتشار[3] می‌تواند مربوط به فرمت داده‌ای PMU

---

1 Phasor Measurement Units
2 Discrete Fourier transform
3 Propagation Delays

باشد که نرخ داده‌ای سیستم ارتباطی، تأخیرهای مربوطه را تعیین می‌کند. علاوه بر این یک تأخیر پردازشی مربوط به ویندو سایز (WS[1]) DFT نیز خواهیم داشت که WS معادل تعداد نمونه‌های مورد نیاز جهت محاسبه فازورهای DFT بوده و در اینجا نقشی اساسی در جهت تعیین مقدار تأخیر بازی می‌کند. بر طبق فرمت استاندارد IEEE۱۳٤٤ پیغامهای انتقالی PMU دارای سه نوع فریم به صورت زیر می‌باشند[۲۸]:

۱- **فریم داده‌ای**[2]: این نوع فریم مربوط به اطلاعات داده‌های فازوری و حالت ورودیهای دیجیتالی بر روی هر کانال ارتباطی می‌باشد.

۲- **فریم سرآیند**[3]: فریم سرآیند به صورت یک فایل ASCII می‌باشد که شامل اطلاعات مربوط به شناسه PMU، منبع داده‌ای، الگوریتم‌ها و فیلترهای آنالوگ استفاده شده می‌باشد.

۳- **فریم پیکربندی**[4]: این فریم به صورت یک فایل باینری قابل خواندن برای ماشین است که شامل کد شناسه PMU، میزان فازورها، میزان کانال‌های دیجیتال، نام کانال‌ها و فازورها، فرکانس نامی خط[5] و پریود زمانی انتقال فازورها می‌باشد.

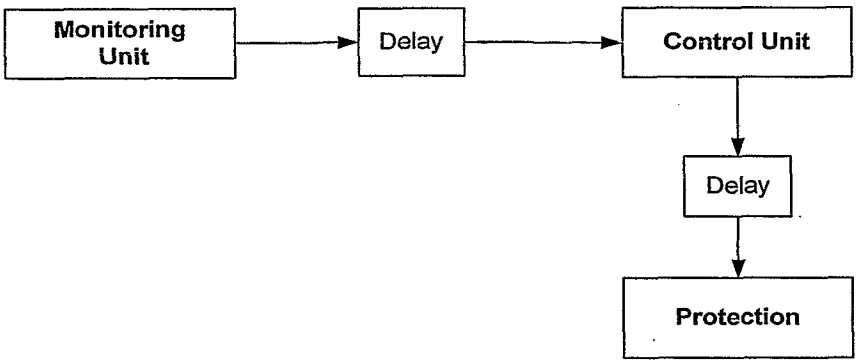
رسانه‌های ارتباطی استفاده شده در WAMS می‌توانند شامل خطوط تلفن، فیبرنوری، PLC[6] و ارتباطات بی‌سیم و ماهواره‌ای باشند. تأخیرهای زمانی مربوط به هر یک از رسانه‌های استفاده شده می‌توانند نقش تعیین کننده‌ای بر میزان زمان تلف شده[7] قبل از آنکه شروع انجام یک عمل بر روی WAMS اتفاق افتد، داشته باشند[۲۸].

---

[1] Window Size
[2] Data Frame
[3] Header Frame
[4] Configuration Frame
[5] Nominal Line Frequency
[6] Power Line Carrier
[7] Time Lag

۲-۷-۲- عوامل مؤثر بر تأخیرها در WAMS

تأخیرهای زمانی اجتناب ناپذیر در سیستم‌های کنترل توزیع‌شده بر ناپایداری سیستم کنترل تأثیر خواهند گذاشت به‌طوریکه ممکن است بر اجرای تمامی قابلیتهای سیستم کنترل اثر گذارند[۲۹]. تأخیرهای سیستم ارتباطی به‌طور اولیه می‌تواند بستگی به نوع رسانه ارتباطی و طول پیغامهای استفاده شده در انتقال اطلاعات جهت اهداف مانیتورینگ و کنترل، همچنین پردازش داده‌های اطلاعاتی مربوطه داشته باشد. شکل ۲-۹ بلاک دیاگرام تأخیر در شبکه قدرت را نشان می‌دهد.



شکل ۲-۹ بلاک دیاگرام تأخیر در سیستم قدرت

در حالتی که PMU از فرمت داده‌ای IEEE۱۳٤٤ استفاده می‌کند تأخیرهای سیستم ارتباطی می‌توانند به دلایل زیر رخ دهند[۲۹]:

۱- تأخیرهای ترانسدیوسر فازور[1] و ترانسدیوسر ولتاژ[2]: ترانسدیوسر یک وسیله پردازش است که به‌طور لحظه‌ای نقاط شکل موج سیگنال آنالوگ را به ترمهای قابل اندازه‌گیری همچون ولتاژ مؤثر(RMS[3])، جریان مؤثر، توان مؤثر، فرکانس شکل موج و زوایای نسبی ولتاژ و جریان تبدیل می‌کند. به‌عبارت دیگر ترانسدیوسرها برای اندازه‌گیری ولتاژها و جریانهای مؤثر در زمان

---

[1] Phasor Transducer
[2] Voltage Transducer
[3] Root Mean Square

نمونه‌برداری استفاده می‌شوند. امروزه از ترانسدیوسرهای دیجیتال به دلیل ایمن بودن آنها در مقابل نویز، بیشتر استفاده می‌شود.

۲- ویندوسایز DFT: ویندوسایز تعداد نمونه‌های مورد نیاز برای محاسبه فازورهای استفاده شده مربوط به DFT می‌باشد. هر چه میزان ویندوسایزها کوچکتر باشد تأخیر کمتری را باعث می‌گردند ولی مسئله‌ای که در اینجا مطرح می‌شود کوچک بودن ویندوسایزها منجر به این می‌شود که ناحیه بزرگتری در محاسبات مقادیر فازور به صورت نامعلوم باقی بماند. ویندوسایزهای بزرگتر بدون شک مقادیر تأخیر را افزایش نمی‌دهند درصورتیکه مقادیر فازور نامعلوم مربوطه، به صورت می‌نیمم خواهند بود.

۳- زمان پردازش: زمان پردازش نیازمند تبدیل اطلاعات ترانسدیوسر به اطلاعات فازور به کمک DFT می‌باشد. پردازش اساساً شامل استفاده از DFT در محاسبه مؤلفه فرکانسی پایه ولتاژ نمونه یا جریان نمونه می‌باشد. در اینجا فیلترهایی که قبل و بعد از پردازش استفاده می‌شوند نیز مقداری تأخیر را باعث می‌شوند.

۴- اندازه داده‌های[1] خروجی PMU: اندازه داده‌ای پیغام مربوط به PMU معادل اندازه بیت‌های اطلاعاتی است که شامل فریم داده، فریم سرآیند و فریم پیکربندی می‌باشد. طول پیغام بر مقدار تأخیر مؤثر خواهد بود به‌طوریکه یک پیغام با اندازه بزرگ‌تر می‌تواند تأخیر بیشتری را باعث شود و بالعکس.

۵- کدینگ خطای[2] داده‌ای: داده یا پیغام داده‌ای انتقالی جهت اطمینان از دریافت صحیح آن توسط ایستگاه دریافت‌کننده، با استفاده از بررسی افزونگی دوره‌ای(CRC[3]) کدگذاری می‌شود. از دیگر فرمهای کدگذاری می‌توان کدهای Reed-Solomon را نام برد که جهت ماهواره‌ها برای کاهش نرخ

---

[1] Data size
2 Error-coding
[3] Cyclic redundancy check

خطای بیت (BER[1]) در سیستم‌های ارتباطی استفاده می‌شوند. در اینجا کدگذاری و کدگشایی داده‌ای نیز مقداری تأخیر را باعث می‌شود[۲۹].

۶- **انتقال داده‌ها بین سیستم‌های ارتباطی و تجهیزات پردازش داده‌ای:** انتقال داده‌ها میان سیستم‌های ارتباطی و تجهیزات پردازش داده‌ای نیز باعث تأخیر می‌شوند خصوصاً در لحظه‌ای که داده‌ها به وسیله سیستم‌های ارتباطی بازیافت یا منتشر می‌گردند. انتقال میان شبکه‌های سوئیچ‌شده بسته‌ای[2] و شبکه‌های سوئیچ‌شده مداری[3] همچنین می‌تواند به تأخیر انتقال اضافه شود. امروزه فن‌آوری ترکیبی، تنگناهای موجود را در صورت استفاده از شبکه‌های دیجیتالی مانند کابل‌های فیبرنوری که در خطوط تلفن آنالوگ به کار برده می‌شوند را از میان برداشته است.

۷- **سیستم‌های ارتباطی:** نوع رسانه ارتباطی استفاده شده و همچنین فاصله فیزیکی بین خروجی PMU و واحد پردازش مرکزی (CPU[4]) مقداری تأخیر را باعث می‌گردد. جهت فواصل طولانی و تقویت سیگنالها به دلایل اتلاف سیگنال و تضعیف[5] آنها در طول مسیر از تکرارکننده‌ها استفاده می‌گردد که افزایش تعداد تکرارکننده‌ها نیز مقداری تأخیر را باعث می‌شود.

۸- **متمرکز کننده‌های داده‌ای:** متمرکزکننده‌های داده‌ای در ابتدا موقعیت مراکز تجمع داده‌ها را در CPU انتخاب نموده، سپس به تمامی داده‌های PMU که بر روی سیستم ارتباطی منتقل می‌شوند پاسخ می‌دهند. متمرکزکننده‌های داده‌ای، داده انتخابی مورد نظر را جهت مانیتورینگ و الگوریتم‌های کنترل مربوطه به مرکز کنترل برای اهداف آنالیز و تصمیم‌گیری ارسال می‌دارد.

---

[1] Bit Error Rate
[2] Packet Switched Networks
[3] Circuit Switched Networks
[4] Central Processing Unit
[5] Attenuation

۲-۷-۳- محاسبه تأخیرهای ارتباطی

محاسبه مربوط به تأخیرها یکی از جنبه‌های اصلی در WAMS می‌باشد. مقدار زیاد تأخیر اعمال مربوط به کنترل‌کننده‌ها را که پایداری و عدم نوسان شبکه قدرت را باعث می‌شوند، کند می‌نماید. تأخیرهای ارتباطی در WAMS به صورت رابطه زیر بیان می‌گردد.

$$\tau = \tau_f + \tau_p + \frac{L}{R} + \theta \qquad (۱-۲)$$

که τ زمان کل تأخیر، τ_f تأخیر ثابت[1] که برابر با مجموع زمانهای تأخیر مربوط به ترانسدیوسر استفاده شده، پردازش DFT، تمرکز داده‌ها و مالتی‌پلکس کردن آنها می‌باشد. τ_p، تأخیر انتشار، L مقدارداده‌های منتقل شده، R نرخ داده‌ای ارتباط و θ در اینجا معادل مجموع تأخیر بی‌ثبات تصادفی[2] است.

تأخیر انتشار بستگی به نوع رسانه ارتباطی دارد و بنابراین می‌تواند تابعی از هر دو عامل رسانه ارتباطی و فاصله فیزیکی میان مؤلفه‌های جداگانه WAMS باشد[۳۰]. به عنوان مثال رسانه‌های ارتباطی همچون فیبرنوری، PLC و خطوط تلفن به‌طور میانگین تأخیر انتشاری معادل ۲۵ ms دارند. در حالتی که از ماهواره‌های LEO[3] استفاده شده باشد این تأخیر حدوداً برابر ۲۰۰ms می‌باشد. مقداری تأخیرهای اضافی نیز مربوط به میزان داده‌هایی است که بر روی رسانه ارتباطی منتقل می‌شوند که بستگی به نرخ داده‌ای رسانه ارتباطی استفاده شده دارد. در صفحه بعد جدول ۲-۳ زمان کل تأخیر محاسبه شده جهت برخی از رسانه‌های ارتباطی مورد استفاده در WAMS را نشان می‌دهد[۳۰].

---

1 Fixed Delay
2 Random Delay Jitter
3 Low Earth Orbit

جدول ۲-۳ تأخیر در برخی از رسانه‌های ارتباطی [۳۰]

رسانه ارتباطی	میزان تأخیر - یک طرفه (ms)
کابلهای فیبر نوری	۱۰۰ — ۱۵۰
ارتباطات مایکروویو دیجیتال	۱۰۰ — ۱۵۰
PLC	۱۵۰ — ۳۵۰
خطوط تلفن	۲۰۰ — ۳۰۰
ارتباطات ماهواره‌ای	۵۰۰ — ۷۰۰

فصل ۳

شبکه‌های ارتباطی و پروتکل TCP/IP

۳-۱- مقدمه

با گسترش استفاده از کامپیوترها، نیاز به برقراری ارتباط و انتقال اطلاعات میان کامپیوترها جهت به اشتراک گذاشتن داده‌های مورد نیاز به‌صورت دو طرفه احساس گردید که این منجر به طراحی فن‌آوریهای شبکه‌ای گردید. همزمان با رشد شبکه‌ها نیاز به روشی جهت ارتباطات شبکه‌های ناهمگون با یکدیگر احساس می‌شد که این فن‌آوری تحت عنوان فن‌آوری بین شبکه‌ای[1] معروف می‌باشد. یکی از سازمانهای مهم که نیاز به قابلیتهای بین شبکه‌ای را در ابتدا احساس می‌کرد، آژانس پروژه‌های تحقیقاتی پیشرفته ایالات متحده[2] بود. یکی از مهمترین فن‌آوریهای طراحی شده توسط ARPA، فن‌آوری سوئیچینگ- بسته‌ای[3] (شبکه مبتنی بر ارسال بسته‌های اطلاعاتی) بود. شبکه‌های پیام‌رسانی سوئیچینگ- بسته‌ای ذاتاً برای ارتباطات بین شبکه‌ای مناسب می‌باشند و به همین دلیل ARPA سرمایه‌گذاری زیادی در فن‌آوری پیام‌رسانی سوئیچینگ- بسته‌ای در ارتباط دادن سایتهای کامپیوتری خود به دانشگاه‌ها، انستیتوهای تحقیقاتی دولتی و دیگر مراکز اطلاعاتی نمود که این شبکه تحت عنوانARPANET معروف شد. با پیشرفته‌تر و بزرگتر شدن ARPANET، توجه مراکز مختلف علاقه‌مند به فن‌آوریهای بین شبکه‌ای معطوف گردید. این مراکز شروع به کار مشترک برای تبدیل فن‌آوری ARPANET به یک پروتکل شبکه‌ای استاندارد به نام پروتکل کنترل انتقال/پروتکل اینترنت (TCP/IP[4]) کردند.

---

[1] Internetworking
[2] ARPA
[3] Packet - Switching
[4] Transport Control Protocol/ Internet Protocol

۳-۲- تعریف پروتکل ارتباطی

فرآیند به اشتراک گذاشتن اطلاعات، نیازمند ارتباط همزمان شده‌ای بین کامپیوترهای شبکه دارد. برای ایجاد سهولت در این فرآیند، برای هر یک از فعالیتهای ارتباط شبکه‌ای، مجموعه‌ای از دستورالعمل‌ها تعریف شده‌اند. هر دستورالعمل ارتباطی یک پروتکل یا قرارداد نام دارد که تأمین کننده توصیه‌هایی برای برقراری ارتباط بین اجزای نرم‌افزاری و سخت‌افزاری در انجام یک فعالیت بین شبکه‌ای می‌باشد.

امروزه پروتکلهای مختلفی با ویژگیهای خاص خود وجود دارند. بعضی از آنها ساده هستند، بعضی نیز قابلیت اعتماد بیشتری دارند و بعضی دیگر سریع‌تر عمل می‌نمایند. انتخاب یک پروتکل در شبکه‌های محلی آزاد بوده و بسته به زمینه فعالیت و نوع آن می‌توان از پروتکل‌های مختلفی استفاده نمود، ولی وقتی یک پروتکل به‌عنوان پروتکل ارتباطی یک شبکه انتخاب می‌شود تمامی کامپیوترها برای ارتباط در آن شبکه ملزم به استفاده از همان پروتکل هستند. یک پروتکل و یا همان قانون بین شبکه‌ای تعیین کننده موارد زیر است[۳۱]:

۱- تعیین زمان برقراری و زمان قطع ارتباط.

۲- تعیین ولتاژ سیگنال.

۳- تعیین نحوه رسیدن پیام به مقصد.

۴- هماهنگی و تنظیم سرعت انتقال اطلاعات بین یکدیگر.

۵- تنظیم و استاندارد کردن زمان انتقال اطلاعات جهت قابل استفاده بودن توسط تمامی سیستم‌ها.

۶- کنترل صحت ارسال و دریافت اطلاعات.

۷- تعیین نحوه فشرده‌سازی اطلاعات.

۳-۳- مدل مرجع OSI

به منظور شناخت مناسب نحوه عملکرد یک پروتکل ارتباطی در شبکه می‌بایست با برخی از مدل‌های رایج شبکه‌های ارتباطی آشنا گردید. مدل ارتباطی سیستمهای باز (OSI[1]) یک مدل مرجع مناسب در این زمینه است. این مدل در سال ۱۹۸٤ توسط سازمان استاندارد بین الملل (ISO[2]) ارائه گردید. مدل OSI به‌عنوان یک مدل مرجع و راهنما برای شناخت عملیات مربوط به ارتباطات استفاده می‌گردد. این مدل شامل تعدادی مؤلفه است که به لایه‌هایی تقسیم شده‌اند. هر لایه یک کار خاص در انتقال داده‌ها بر روی شبکه ارتباطی انجام می‌دهد. در زمان ارسال داده‌ها، هر لایه داده‌های قالب‌بندی شده توسط لایه بالاتر را گرفته و آنرا اداره می‌کند. سپس به لایه زیرین خود می‌فرستد. در زمان دریافت داده، لایه‌ها همین فرآیند را به‌طور معکوس انجام می‌دهند. مدل OSI همانطور که در شکل ۳-۱ آمده است شامل لایه‌های زیر می‌باشد (از پایین به بالا لیست شده است)[۳۲]:

Application
Presentation
Session
Transport
Network
Data Link
Physical

شکل ۳-۱ مدل هفت لایه‌ای OSI

[1] Open Systems Interconnection
[2] International Standard Organization

۱- لایه فیزیکی (Physical)

لایه فوق در ارتباط مستقیم با سخت افزار بوده و خصایص فیزیکی شبکه نظیر اتصالات، تعیین ولتاژ برای شناسایی صفر و یک‌ها، تشخیص نوع شبکه ارتباطی، تبدیل اطلاعات به بسته‌های داده‌ای[1] و تبدیل سیگنالهای دیجیتال و آنالوگ و زمانبندی آنهاست.

۲- لایه ارتباط داده‌ای (Datalink)

این لایه، مسئول تقسیم‌بندی اطلاعات به واحدهای منطقی، کنترل صحت آدرس فیزیکی و کنترل کننده سرعت ارسال اطلاعات و طریقه دسترسی به خط می‌باشد. در این لایه نوع شبکه ارتباطی و وضعیت بسته‌های اطلاعاتی نیز تعیین می‌گردند.

۳- لایه شبکه (Network)

این لایه مسئول تعیین مسیر حرکت اطلاعات، پردازش آدرس‌ها و حرکت داده‌ها بر روی یک شبکه پیچیده است. پروتکل‌های منطقی، مسیریابی و آدرس‌دهی در این لایه انجام خواهد شد.

۴- لایه انتقال (Transport)

لایه فوق مسئول پشتیبانی، کنترل جریان داده‌ها و بررسی خطا و بازیابی اطلاعات بین دستگاه‌های متفاوت است. کنترل جریان داده‌ها، بدین‌معنی است که این لایه در صورتیکه اطلاعاتی از چندین برنامه ارسال شده باشد، داده‌های مربوط به هر برنامه را به یک Stream آماده تبدیل کرده تا در اختیار شبکه فیزیکی قرار داده شوند.

---

[1] Packets

۵- لایه جلسه (Session)

لایه فوق مسئول ایجاد، پشتیبانی و ارتباطات مربوط با دستگاه دریافت کننده اطلاعات است. همچنین مدیریت برقراری ارتباط و نحوه ارسال اطلاعات را بر عهده دارد.

۶- لایه نمایش (Presentation)

مسئول کدگذاری اطلاعات به‌روش استاندارد می‌باشد. ترتیب فرستادن بیت‌ها و بایت‌ها و تبدیل کدهای مختلف و تبدیل فرمت فایل سیستم‌ها به هم، از دیگر وظایف این لایه می‌باشد.

۷- لایه کاربرد (Application)

این لایه با سیستم عامل و یا برنامه‌های کاربردی ارتباط دارد. کاربران با استفاده از نرم‌افزارهای کاربردی متفاوت قادر به انجام عملیات مرتبط با شبکه خواهند بود. این لایه حاوی مجموعه‌ای از پروتکلهایی است که به‌صورت واسطهای برنامه‌نویسی کاربردی (API[1]) ارائه می‌گردند.

ارسال و دریافت اطلاعات از طریق لایه‌های مربوط در کامپیوترهای فرستنده و گیرنده انجام می‌شود و داده‌ها توسط یک برنامه و توسط کاربر تولید خواهند شد. شروع ارسال داده‌ها از لایه کاربرد می‌باشد که در ادامه و با حرکت به سمت پایین، در هر لایه عملیات مربوطه انجام شده، داده‌هایی به بسته‌های اطلاعاتی اضافه خواهند شد. در آخرین لایه (لایه فیزیکی) با توجه به محیط انتقال استفاده شده، داده‌ها به سیگنالهای الکتریکی، پالس‌هایی از نور و یا سیگنالهای رادیویی تبدیل و از طریق کابل و یا هوا برای کامپیوتر مقصد ارسال خواهند شد. پس از دریافت داده در کامپیوتر مقصد، عملیات مورد نظر (معکوس عملیات ارسال) توسط هر یک از لایه‌ها انجام و در نهایت با رسیدن داده به لایه کاربرد و به‌کمک یک برنامه، امکان استفاده از اطلاعات ارسالی فراهم خواهد شد.

---

[1] Application Programming Interfaces

۳-۴- پروتکل TCP/IP

یک پروتکل پشته‌ای[1]، شامل مجموعه‌ای از پروتکل‌ها است که با یکدیگر فعالیت نموده تا امکان انجام یک عملیات خاص را برای سخت‌افزار و یا نرم‌افزار فراهم نماید[۳۲]. پروتکل TCP/IP نمونه‌ای از پروتکل‌های پشته‌ای می‌باشد که برقراری ارتباط از طریق پروتکل‌های متعددی که در چهار لایه مجزا سازماندهی شده‌اند، میسر می‌گردد. هر یک از پروتکل‌های موجود در پشته TCP/IP، دارای وظیفه‌ای خاص در زمینه برقراری ارتباط می‌باشند. در زمان ایجاد یک ارتباط، ممکن است در یک لحظه تعداد زیادی از برنامه‌ها، با یکدیگر ارتباط برقرار نمایند که پروتکل TCP/IP، دارای قابلیت تفکیک و تمایز یک برنامه موجود بر روی یک کامپیوتر با سایر برنامه‌ها بوده و پس از دریافت داده‌ها از یک برنامه، آنها را برای برنامه متناظر موجود بر روی کامپیوتر دیگر ارسال می‌نماید. برقراری ارتباط مبتنی برTCP/IP، با فعال شدن یک برنامه بر روی کامپیوتر مبدأ آغاز می‌گردد. برنامه فوق، داده‌های مورد نظر جهت ارسال را بگونه‌ای آماده و فرمت می‌نماید که برای کامپیوتر مقصد قابل خواندن و استفاده باشند. در ادامه آدرس کامپیوتر مقصد، به داده‌های مربوطه اضافه می‌گردد. پس از انجام عملیات فوق، داده بهمراه اطلاعات اضافی، در طول شبکه به‌حرکت درآمده تا به مقصد مورد نظر برسد. عملیات فوق، ارتباطی به محیط انتقال شبکه به منظور انتقال اطلاعات نداشته، و تحقق این عملیات با رویکردی مستقل نسبت به محیط انتقال، انجام خواهد شد. امروزه اکثر شبکه‌های‌کامپیوتری بزرگ و اغلب سیستم‌های‌عامل موجود از پروتکل TCP/IP، استفاده و حمایت می‌نمایند. امروزه TCP/IP، امکانات لازم به‌منظور ارتباط سیستم‌های غیرمشابه را فراهم آورده است. از ویژگی‌های مهم پروتکل فوق، می‌توان به مواردی همچون قابلیت اجراء بر روی محیطهای متفاوت، قابلیت اطمینان بالا، قابلیت گسترش و توسعه آن، اشاره کرد. از پروتکل فوق، به‌منظور دستیابی به اینترنت و استفاده از سرویس‌های متنوع آن نظیر وب و یا پست الکترونیکی

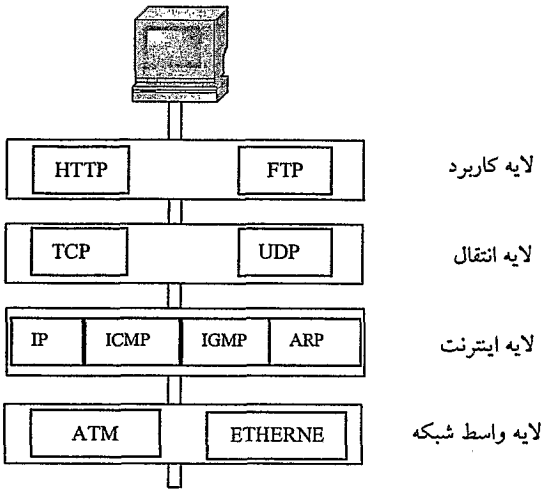
---

[1] Stack Protocol

استفاده می‌گردد. تنوع پروتکل‌های موجود در پشته TCP/IP و ارتباط منطقی و سیستماتیک آنها با یکدیگر، امکان تحقق ارتباط در شبکه‌های کامپیوتری را با اهداف متفاوت، فراهم می‌نماید. فرآیند برقراری یک ارتباط، شامل فعالیت‌های متعددی نظیر تبدیل نام کامپیوتر به آدرس IP معادل، مشخص نمودن موقعیت کامپیوتر مقصد، بسته‌بندی داده‌های اطلاعاتی، آدرس‌دهی و مسیریابی بسته‌های اطلاعاتی به‌منظور ارسال موفقیت آمیز به مقصد مورد نظر، که توسط مجموعه‌ی پروتکل‌های موجود در پشته TCP/IP انجام می‌گیرد[۳۲].

۳-۵- لایه‌های پروتکل TCP/IP

پروتکل TCP/IP، فرآیندهای لازم به منظور برقراری ارتباط را سازماندهی کرده و در این راستا از پروتکل‌های متعددی در پشته TCP/IP استفاده می‌نماید. به منظور افزایش کارایی در تحقق فرآیندهای مورد نظر، پروتکل‌ها در لایه‌های متفاوتی سازماندهی شده‌اند. اطلاعات مربوط به آدرس‌دهی در انتها قرار گرفته و بدین ترتیب کامپیوترهای موجود در شبکه قادر به بررسی آن با سرعت مطلوب خواهند بود. در این راستا، صرفاً کامپیوتری که به‌عنوان کامپیوتر مقصد معرفی شده‌است، امکان باز نمودن بسته‌های اطلاعاتی و انجام پردازش‌های لازم بر روی آن را دارا خواهد بود. TCP/IP، از یک مدل ارتباطی چهار لایه به‌منظور ارسال اطلاعات از محلی به محل دیگر استفاده می‌نماید[۳۳]. همانگونه که در شکل ۳-۲ مشاهده می‌شود هر یک از پروتکل‌های وابسته به پشته TCP/IP، با توجه به رسالت خود، در یکی از این لایه‌ها قرار می‌گیرند.



شکل ۳-۲ پروتکل‌های مربوط به TCP/IP

۳-۵-۱- لایه کاربرد (Application)

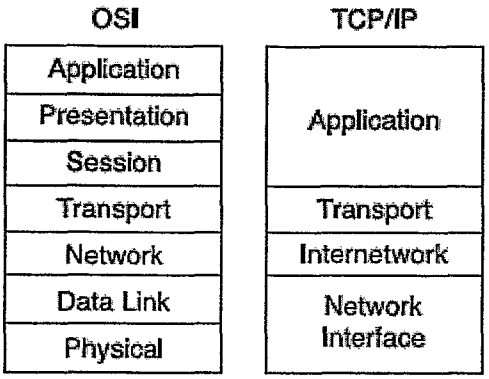
همانطور که در شکل ۳-۳ آورده شده است مقایسه‌ای بین مدل مرجع OSI و پروتکل TCP/IP مشاهده می‌شود. لایه کاربرد مطابق شکل ۳-۳ متناظر با لایه‌های Session ,Presentation و Application در مدل OSI است. تمامی برنامه‌ها و ابزارهای کاربردی با استفاده از این لایه قادر خواهند بود به شبکه دستیابی داشته باشند. پروتکل‌های موجود در این لایه به‌منظور فرمت‌دهی و مبادله اطلاعات کاربران استفاده می‌گردند. دو نمونه از پروتکل‌های موجود در این‌لایه به‌صورت زیر می‌باشند:

۱- **پروتکل انتقال فرامتن (HTTP[1])**، از این پروتکل به‌منظور ارسال فایل‌های صفحات وب استفاده می‌گردد.

۲- **پروتکل انتقال فایل(FTP[2])**، این پروتکل نیز جهت ارسال و دریافت فایل‌ها کاربرد دارد.

---

[1] Hypertext Transfer Protocol
[2] File Transfer Protocol



شکل ۳-۳ مقایسه‌ای بین مدل مرجع OSI و پروتکل TCP/IP

۳-۵-۲- لایه انتقال (Transport)

لایه فوق متناظر با لایه Transport در مدل OSI است. این لایه، قابلیت ایجاد نظم و ترتیب و تضمین ارتباط بین کامپیوترها و ارسال داده به لایه Application (لایه بالای خود) و یا لایه اینترنت (لایه پایین خود) را بر عهده دارد. لایه فوق، همچنین مشخصه منحصر بفردی از برنامه‌ای که داده را عرضه نموده است، ارائه می‌دهد. این لایه دارای دو پروتکل اساسی است که نحوه توزیع داده را کنترل می‌نمایند و به‌صورت زیر می‌باشند:

۱- **پروتکل TCP**، این پروتکل مسئول تضمین صحت توزیع اطلاعات است.

۲- **پروتکل داده‌گرام کاربری (UDP[1])**، این پروتکل امکان عرضه سریع اطلاعات بدون پذیرفتن مسئولیتی را در رابطه با تضمین صحت توزیع اطلاعات برعهده دارد.

۳-۵-۳- لایه اینترنت (Internet)

لایه فوق متناظر با لایه Network در مدل OSI است. لایه اینترنت[2]، با استفاده از آدرس IP (شامل یک مشخصه شبکه و یک مشخصه میزبان)، آدرس دستگاه مورد نظر را برای ارتباط مشخص

---

[1] User Datagram Protocol
[2] Internet Layer

می‌نماید لایه اینترنت، مسئول آدرس‌دهی، بسته‌بندی و مسیریابی داده‌ها است. که شامل چهار پروتکل اساسی به صورت زیر می‌باشد:

۱- **پروتکل اینترنت (IP)**[1]، پروتکل اینترنت مسئول آدرس‌دهی داده‌ها به‌منظور ارسال به مقصد موردنظر است.

۲- **پروتکل وضوح آدرس (ARP)**[2]، این پروتکل مسئول مشخص نمودن آدرس MAC[3] آداپتور شبکه بر روی کامپیوتر مقصد است.

۳- **پروتکل ICMP**[4]، این پروتکل نیز مسئول ارائه توابع عیب‌یابی و گزارش خطا در صورت عدم توزیع صحیح اطلاعات است .

۴- **پروتکل IGMP**[5]، این پروتکل مسئول مدیریت Multicasting در TCP/IP را برعهده دارد.

۳-۵-٤- لایه واسط شبکه (Network Interface)

لایه فوق، لایه‌های فیزیکی و داده‌ای را تشکیل می‌دهد که داده‌های مربوط به دستگاه‌های موجود در یک شبکه را مسیریابی می‌کند لایه واسط شبکه، مسئول استقرار داده بر روی محیط انتقال شبکه و دریافت داده‌ها از محیط انتقال شبکه است این لایه شامل دستگاه‌های فیزیکی نظیر کابل شبکه و آداپتورهای شبکه می‌باشد. لایه واسط شبکه، شامل پروتکل‌های مبتنی بر نرم‌افزار مشابه لایه‌های قبل، نمی‌باشد. پروتکل‌های اترنت[6] و ارسال به‌صورت مد غیر همزمان (ATM[7])، نمونه‌هائی از پروتکل‌های موجود در این لایه می‌باشند. پروتکل‌های فوق، نحوه ارسال داده‌ها در شبکه را مشخص می‌نمایند.

---

[1] Internet Protocol
[2] Address Resolution Protocol
[3] Media Access Control
[4] Internet Control Message Protocol
[5] Internet Group Management Protocol
[6] Ethernet
[7] Asynchronous Transfer Mode

۳-۶- تشخیص برنامه‌ها با استفاده از TCP/IP

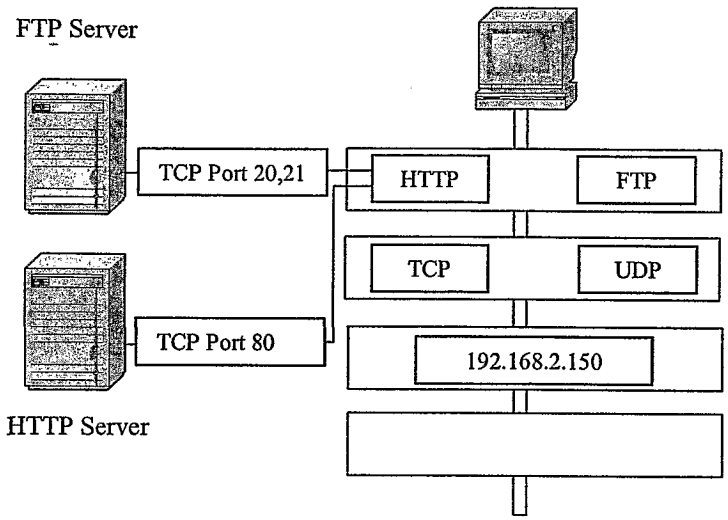
در شبکه‌های کامپیوتری، برنامه‌های متعددی در یک زمان با یکدیگر مرتبط می‌گردند. زمانیکه چندین برنامه بر روی یک کامپیوتر فعال می‌باشند پروتکل TCP/IP می‌بایست از روشی به منظور تمایز یک برنامه از برنامه دیگر، استفاده نماید. بدین منظور، از آدرس IP، پورت TCP/UDP وسوکت جهت مشخص نمودن یک برنامه خاص، استفاده می‌نماید[۳۳].

۳-۶-۱- آدرس IP

برقراری ارتباط در یک شبکه، مستلزم مشخص شدن آدرس کامپیوترهای مبدأ و مقصد است. آدرس هر یک از دستگاه‌های درگیر در فرآیند ارتباطی توسط یک عدد منحصربفرد که آدرس IP نامیده می‌شود مشخص می‌گردد. آدرس فوق می‌تواند به هریک از کامپیوترهای موجود در شبکه نسبت داده شوند[۳۳].

۳-۶-۲- درگاه TCP/UDP

یک درگاه معمولاً به صورت مشخصه‌ای برای یک برنامه است و مربوط به یک کامپیوتر خاص می‌باشد. درگاه با یکی از پروتکل‌های لایه انتقال (TCP و یا UDP) مرتبط می‌باشد که به آن درگاه TCP و یا درگاه UDP گفته می‌شود. درگاه می‌تواند عددی بین صفر تا ٦٥٥٣٥ را شامل شود. درگاه‌ها برای برنامه‌های TCP/IP سمت سرویس‌دهنده، به‌عنوان درگاه‌های "شناخته شده" نامیده شده و به اعداد کمتر از ١٠٢٤ ختم و رزو می‌شوند تا هیچگونه تعارض و برخوردی با سایر برنامه‌ها بوجود نیاید. مثلاً برنامه سرویس‌دهنده FTP از پورت TCP ۲۰ و ۲۱ استفاده می‌نماید. شکل ۳-۴ فرآیندهای مربوط به درگاه TCP را نشان می‌دهد[۳۳].



شکل ۳-۴ فرآیندهای مربوط به درگاه TCP

۳-۶-۳- سوکت

سوکت، ترکیبی از یک آدرس IP و درگاه TCP و یا درگاه UDP است. یک برنامه، سوکتی را با مشخص نمودن آدرس IP مربوط به کامپیوتر و نوع سرویس (TCP برای تضمین توزیع اطلاعات و یا UDP) و درگاهی که نشان‌دهنده برنامه است، مشخص‌می‌نماید. آدرس IP موجود در سوکت، امکان آدرس‌دهی کامپیوتر مقصد را فراهم و درگاه مربوطه، برنامه‌ای را که داده‌ها برای آن ارسال می‌گردند را مشخص می‌نماید[۳۴].

۳-۷- همزمانی در TCP/IP

همزمانی ارتباط داده‌ای میان دو سیستم کامپیوتری که قصد ارتباط داده‌های اطلاعاتی را با هم دارند به آسانی صورت نمی‌گیرد. در اینجا مسئله تأخیر در ارسال و دریافت داده‌های اطلاعاتی میان دو سیستم کامپیوتری مورد بحث می‌باشد که این بستگی به نوع معماری شبکه‌ای، میزان بار داده‌ای و پروتکل ارتباطی استفاده شده دارد. در شبکه‌های ارتباطی، مسئله تأخیر بدین‌معنی می‌باشد که

داده‌های خام[1] فرستاده شده از یک نود ارسالی، و دریافت آن توسط نود دیگر به دلایلی با تأخیرهای زمانی همراه باشد. این مسئله در صورتی قابل حل است که داده‌های خام ارسالی با یک زمان مهرشده[2] ارسال شده باشند یعنی یک همزمانی بین فرستنده و گیرنده برقرار شده باشد. به‌عنوان مثال صحت زمانی[3] برای یک شبکه اترنت به موارد زیر بستگی دارد[۳۴]:

۱- زمان مهرشده مربوط به زمان ورود و خروج بسته‌ها.

۲- تأخیرهای شبکه‌ای متغیر که بستگی به بار شبکه، افت سرعت ارتباط، اندازه بسته‌ها و معماری مورد استفاده دارد.

۳- نوع پروتکل استفاده شده که قادر است موارد مربوطه را جهت همزمانی بین فرستنده و گیرنده برقرار نماید. از پروتکل‌هایی که در این زمینه به‌صورت یک استاندارد باز و مناسب شناخته شده است می‌توان SNTP/NTP را نام برد.

۳-۷-۱- پروتکل زمانی شبکه

پروتکل زمانی شبکه (NTP[4]) و پروتکل زمانی شبکه ساده (SNTP[5]) به‌صورت پروتکل‌های عمومی و استاندارد جهت TCP وUDP مورد استفاده قرار می‌گیرند که با استفاده از تکنیکهای فیلترینگ توسعه‌یافته، تأخیر متغیر میان کامپیوتر سرویس‌دهنده و مشتری را به صورت بهینه فیلتر نموده، پشته‌های پروتکلی هر کدام را دریافت و سپس منتقل می‌نماید. یک پیاده‌سازی SNTP/NTP در معماری سرویس‌دهنده/ مشتری مبتنی بر توزیع یکتا[6] و توزیع چندگانه[7] می‌باشد که زمانهای به‌هنگام هر کدام به‌صورت زیر آورده شده است[۳۴]:

---

[1] Raw Data
[2] Time Stamped
[3] Timing Accuracy
[4] Network Time Protocol
[5] Simple Network Time Protocol
[6] Unicast
[7] Multicast

۱- زمانهای به‌هنگام توزیع یکتا [1]: زمان به‌هنگام در توزیع یکتا معادل یک زمان درخواست (TReq[2]) است که در ابتدا از طرف یک مشتری آغاز شده و سرویس‌دهنده نیز در جواب آن یک زمان پاسخ (TRep[3]) می‌فرستد. زمان مربوط به مشتری یک زمان مهرشده مرجع[4]، T_0، تولید می‌کند که این زمان مهرشده در بسته TReq قرار می‌گیرد. زمان مهرشده به عنوان ترکیبی از زوج TReq و TRep استفاده می‌گردد. مشتری همچنین دو زمان مهرشده دیگر را که بر پایه کلاک محلی می‌باشد در خود ذخیره می‌کند. T_1، یعنی زمان محلی هنگامیکه TReq فرستاده می‌شود و زمان محلی T_4 وقتی که TRep دریافت می‌گردد. سرویس‌دهنده نیز یک زمان مهرشده تولید می‌کند یعنی زمانیکه TReq دریافت می‌گردد، T_2 ، وقتی که TRep فرستاده می‌شود، T_3. زمانهای مهرشده در داخل TRep جای می‌گیرند. مشتری قادر است زمان تأخیر انتشار[5]، t_{pd}، و افست کلاک محلی[6] ، t_{offset}، را بر پایه چهار زمان مهرشده به‌صورت فرمول زیر محاسبه نماید:

$$t_{pd} = ((T_4 + T_1) - (T_3 - T_2))/2 \qquad (۱-۳)$$

$$t_{offset} = ((T_2 - T_1) + (T_3 - T_4))/2 \qquad (۲-۳)$$

۲- زمانهای به‌هنگام توزیع چندگانه[1]: زمانهای به‌هنگام چندگانه SNTP/NTP بر پایه TRep مربوط به بسته‌هایی است که در فواصل زمانی منظمی به یک گروه از آدرس‌های IP توزیع چندگانه ارسال می‌شوند. یک سرویس‌دهنده توزیع چندگانه انتظار هیچگونه درخواستی از مشتری ها ندارد. در اینجا یک مشتری توزیع چندگانه به گروه آدرس‌های IP توزیع چندگانه می‌پیوندد و منتظر شنیدن پاسخ می‌ماند. در اینجا مشتری‌ها قادر به محاسبه t_{pd} نیستند مگر آنکه سرویس‌دهنده توزیع چندگانه، TReqهای توزیع یکتا را پذیرفته باشد. صحت زمانی هنگامی رخ خواهد داد که زمان مهرشده و

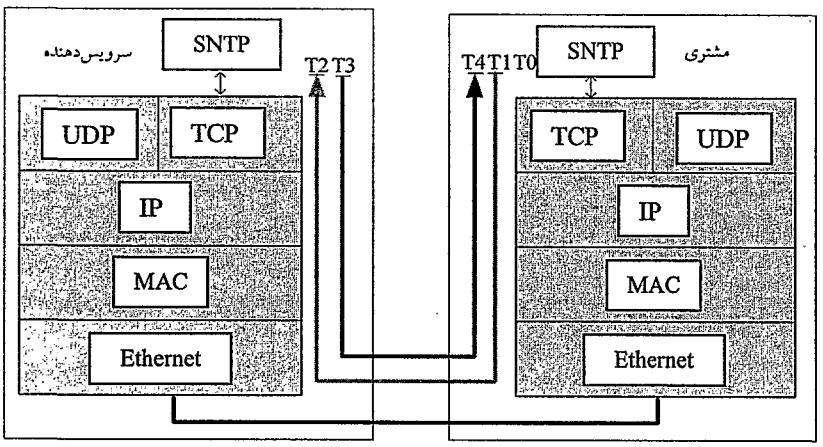
---

[1] Unicast Time Updates
[2] Time Request
[3] Time Reply
[4] Reference Time Stamp
[5] Popagation Delay
[6] Local Clock Offset

تغییرات مربوط به تأخیر شبکه صورت گرفته باشد. زمان مهرشده در لایه کاربرد SNTP/NTP، لایه نرم‌افزاری اترنت و یا در لایه فیزیکی/ لایه داده‌ای اترنت (سخت‌افزار) اجرا می‌گردد.

۳-۷-۲- زمان مهرشده در لایه کاربرد SNTP/NTP

زمان مهرشده در لایه کاربرد SNTP/NTP، همانطور که در شکل ۳-۵ نشان داده شده، بدین معنی است که از صحت زمانی مربوط به پشته TCP/IP با زمان تأخیر متغیر کاسته خواهد شد که این بستگی به نوع پیاده‌سازی شبکه، بارترافیکی آن و سیستم عامل بلادرنگ (RTOS[2]) دارد.



شکل ۳-۵ زمان مهر شده در لایه کاربرد SNTP/NTP

با استفاده از NTP و یا روشهای فیلترینگ مشابه آن از پیچیدگی موجود در شبکه ارتباطی کاسته می‌شود. مثلاً برای یک اتصال مستقیم با استفاده از کابل زوج سیم میان سرویس‌دهنده و مشتری صحت زمانی در حدود چند میلی‌ثانیه می‌باشد. سرویس‌دهنده هر دو زمان مهرشده دریافتی

---

[1] Multicast Time Updates
[2] Real Time Operating System

TReq، T_2، و زمان مهرشده انتقالی TRep ، T_3، را به بسته‌های TRep اضافه می‌کند. بنابر این زمان مهرشده T_3 قبل از آنکه ارسال شود در درون بسته قرار می‌گیرد.

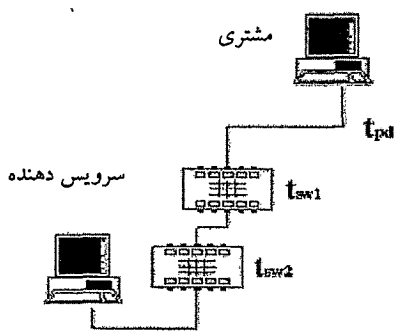
۳-۷-۳- زمان مهرشده در لایه نرم‌افزاری اترنت

زمان مهرشده اگر به‌صورت نرم‌افزاری اجرا شود می‌تواند باعث بهبودی صحت زمانی گردد. زمانهای مهرشده دریافتی T_2 و T_4 در ISR[1] اترنت اجرا می‌گردند و این وقتی اجرا می‌گردد که زمان مهرشده مربوط به مشتری (T_1) جهت نرم‌افزار اترنت اجرا شده باشد. صحت زمانی که مشتری‌ها با اجرای زمان مهرشده در لایه نرم‌افزاری اترنت انجام می‌دهند در حدود ده‌ها تا صدها میلی‌ثانیه می‌باشد.

۳-۷-٤- زمان مهرشده در لایه فیزیکی/ لایه داده‌ای اترنت

اگر زمان مهرشده در لایه فیزیکی/ لایه داده‌ای اترنت اجرا شده باشد قادر است تأخیرهای مربوط به پشته‌های پروتکل را کمتر نموده و همچنین در اینجا همزمانی می‌تواند با دقت بسیار بالایی در حدود میکروثانیه صورت پذیرد.

در شکل۳-۶ یک پیاده‌سازی همزمانی معمول در TCP/IP نشان داده شده است. در اینجا بسته‌های اطلاعاتی از طرف یک سوئیچ اترنت ارسال می‌شوند و تأخیرهای شبکه‌ای بستگی به بار شبکه، افت سرعت ارتباط، اندازه بسته‌های اطلاعاتی، معماری شبکه و تعداد سوئیچهای استفاده شده میان سرویس‌دهنده و مشتری دارند.



شکل ۳-۶ یک پیاده‌سازی همزمانی در TCP/IP

---

[1] Interrupt Service Routine

تأخیر مربوط به سوئیچها ممکن است از ده‌ها میکروثانیه تا چندین میلی‌ثانیه باشد. امروزه بیشتر سوئیچهای اترنت بر پایه فن‌آوری "ذخیره و حرکت به جلو[1] " عمل می‌نمایند یعنی یک بسته قبل از آنکه برروی درگاه ورودی برای خطاهای بیت و مقایسه با FCS[2] در انتهای بسته چک شود می‌بایست کاملاً دریافت گردیده سپس به طرف درگاه مورد نظر ارسال گردد، بنابراین در اینجا میزان تأخیر بستگی به افت سرعت ارتباط و اندازه بسته‌های اطلاعاتی دارد. یک ماکزیمم اندازه بسته اطلاعاتی(۱۵۲۲بایت) بر روی اترنت با سرعت 10Mbps تأخیری معادل ۱,۲ میلی‌ثانیه خواهد داشت که این میزان تأخیر بر روی اترنت با سرعت 100Mbps برابر با ۱۲۲ میکروثانیه می‌باشد[۳۴].

در صورت استفاده از اینترنت جهت محیط انتقال داده‌های اطلاعاتی عوامل مختلفی هستند که سبب تأخیر زمانی در انتقال داده‌ها می‌شوند و به‌طور کلی این عوامل را می‌توان به‌صورت زیر نام برد[۳۴]:

۱- تأخیر پشت به پشت[3] (T_{ed}): این تأخیر معادل زمان مورد نیاز جهت ارسال یک بسته‌ی داده از سوی کامپیوتر فرستنده به کامپیوتر گیرنده می‌باشد.

۲- تأخیر انتقال[4] (T_{td}): برابر با زمان مورد نیاز برای ارسال یک بسته به‌صورت فیزیکی می‌باشد. بدین معنی که مدت زمان لازم جهت ارسال بیت اول تا بیت پایانی مربوط به یک بسته‌ی داده‌ای به چه میزان می‌باشد.

۳- تأخیر انتشار[5] (T_{pd}): مدت زمان انتظار یک بسته جهت ارتباط فیزیکی می‌باشد.

۴- تأخیر پردازش بسته[6] (T_{ppd}): زمان مورد نیاز جهت ارسال یک بسته بر روی مسیریاب می‌باشد. در این قسمت مسیریاب بسته را از صف[7] برداشته و بر روی سیستم ارتباطی ارسال می‌نماید که در اینجا تأخیر مربوط به صف را شامل نمی‌شود.

---

[1] Store-and-Forward
[2] Flow Control Sequence
[3] End to End Delay
[4] Transmission Delay
[5] Propagation Delay
[6] Packet Processing Delay
[7] Queue

۵- تأخیر صف[1] (T_{qd}): مدت زمان انتظار مربوط به صف در مسیریابها می‌باشد. در صورتیکه یک سیستم ارتباطی تراکم[2] بسته‌ها را نداشته باشد، تأخیر صف در اینجا تقریباً معادل صفر می‌باشد. بدین معنی که بسته‌ها در صف منتظر نمی‌مانند.

رابطه میان تأخیرهای زمانی آورده شده در بالا را می‌توان به‌صورت زیر بیان نمود:

$$T_{ed} = T_{td} + T_{pd} + T_{ppd} + T_{qd} \qquad (۳-۳)$$

۳-۸- تجهیزات شبکه ارتباطی

تولید کنندگان تجهیزات شبکه، دستگاه‌های متفاوتی را به‌منظور غلبه بر مشکلات و محدودیت‌های گفته شده، طراحی و عرضه نموده‌اند. اغلب این تجهیزات در سایر فن‌آوری‌های مرتبط با شبکه نقش مهمی را ایفاء می‌نمایند[۳۴]. در زیر برخی از این تجهیزات آورده شده‌اند.

۳-۸-۱- تکرارکننده‌ها

تکرارکننده‌ها[3]، سگمنت‌های متفاوت یک شبکه ارتباطی را به یکدیگر متصل می‌کنند. در این حالت تکرارکننده سیگنال ورودی خود را از یک سگمنت اخذ و با تقویت سیگنال، آن را برای سگمنت بعدی ارسال خواهد کرد. بدین ترتیب با استفاده از چندین تکرارکننده و اتصال کابل‌های مربوطه توسط آنان، می‌توان ابعاد یک شبکه را افزایش داد.

۳-۸-۲- پل‌ها و سگمنت

شبکه‌های ارتباطی همزمان با رشد (بزرگ شدن حجم ارتباطات) دچار مشکل تراکم می‌شدند. در صورتیکه تعداد زیادی ایستگاه به یک سگمنت متصل شوند، هر یک دارای ترافیک خاص خود خواهند بود. در چنین وضعیتی تعداد تصادم در شبکه افزایش یافته و عملاً کارایی شبکه افت خواهد

---

[1] Queueing Delay
[2] Congestion
[3] Repeater

کرد. یکی از راه حل‌های موجود به‌منظور برطرف نمودن مشکل تراکم در شبکه ارتباطی، تقسیم یک سگمنت به چندین سگمنت است. با این کار برای تصادم‌هائی که در شبکه بروز خواهند داد، دامنه وسیعتری ایجاد می‌گردد. راه حل فوق باعث بروز یک مشکل دیگر می‌گردد که سگمنت‌ها قادر به اشتراک اطلاعات با یکدیگر نخواهند بود.

به‌منظور حل مشکل فوق، پل‌ها[1] در شبکه ارتباطی پیاده‌سازی شده‌اند. عملکرد پل از نظر افزایش ابعاد شبکه نظیر تکرارکننده است، با این تفاوت که پل قادر به ایجاد نظم در ترافیک شبکه نیز خواهد بود. پل نظیر سایر دستگاه‌های موجود در شبکه قادر به ارسال و دریافت اطلاعات بوده ولی عملکرد آنها دقیقاً مشابه با یک ایستگاه نمی‌باشد.

۳-۸-۳- مسیریابها

زمانیکه تعداد زیادی از ایستگاه‌های موجود در شبکه‌های مبتنی بر پل، فریم‌های Broadcast را ارسال می‌نمایند، تراکم اطلاعاتی بوجود آمده به‌مراتب بیشتر از زمانی خواهد بود که تمامی دستگاه‌ها در یک سگمنت قرار گرفته باشند. مسیریاب[2] یکی از دستگاه‌های پیشرفته در شبکه ارتباطی بوده که قادر به تقسیم یک شبکه به چندین شبکه منطقی مجزا است. مسیریاب‌ها یک محدوده منطقی برای هر شبکه ایجاد می‌نمایند. مسیریاب‌ها بر اساس پروتکل‌هائی که مستقل از فن‌آوری خاص در یک شبکه است، فعالیت می‌نمایند. ویژگی فوق این امکان را برای مسیریاب فراهم خواهد کرد که چندین شبکه با فن‌آوری‌های متفاوت را به یکدیگر مرتبط نمایند. امروزه استفاده از مسیریاب‌ها در شبکه‌های محلی و گسترده امکان پذیراست.

۳-۸-٤- سوئیچ‌ها

مهمترین تحول ایجاد شده در شبکه‌های اترنت امکان استفاده از سوئیچ‌های اترنت است. سگمنت‌ها توسط سوئیچ به یکدیگر متصل می‌گردند. نظیر پل با این تفاوت عمده که امکان اتصال چندین

---

[1] Bridges
[2] Router

سگمنت توسط سوئیچ فراهم می‌گردد. برخی از سوئیچ‌ها امکان اتصال صدها سگمنت به یکدیگر را فراهم می‌نمایند. تمام دستگاه‌های موجود در شبکه، سوئیچ و یا ایستگاه می‌باشند. قبل از ارسال فریم‌های اطلاعاتی برا ی هر ایستگاه، سوئیچ فریم مورد نظر را دریافت و پس از بررسی، آن را برای ایستگاه مقصد مورد نظر ارسال خواهد کرد. عملیات فوق مشابه پل است، ولی در مدل فوق هر سگمنت دارای صرفاً یک ایستگاه است و فریم صرفاً به دریافت‌کننده واقعی ارسال خواهد شد. بدین ترتیب امکان برقراری ارتباط همزمان بین تعداد زیادی ایستگاه در شبکه‌های مبتنی بر سوئیچ فراهم خواهد شد.

فصل ۴

سیستم‌های SCADA

مبتنی بر TCP/IP

۴-۱- مقدمه

همزمان با رشد فن‌آوری اطلاعات (IT[1]) و دانش‌های مرتبط با آن، استفاده از شبکه‌های ارتباطی در سیستم‌های صنعتی جهت ارتباطات و کنترل فرآیندهای مورد نیاز به‌صورت گسترده‌ای بکار برده می‌شد. امروزه در این سیستم‌ها بنا به دلایل محیطی حاکم، نیاز به یک شبکه ارتباطی با استانداردها و پروتکل‌های خاص ضروری می‌نماید. در سیستم‌های صنعتی خصوصاً شبکه قدرت لازم است که فرمانهای کنترلی به صورت بلادرنگ با دقت بالایی بر روی شبکه اطلاعاتی ارسال و سپس قطعیت دریافت آن توسط ایستگاه مورد نظر تأیید گردد[۳۵]. امروزه سیستم‌های SCADA به‌طور گسترده‌ای در شبکه‌های اطلاعاتی مربوط به شبکه قدرت بکار گرفته شده‌اند که هدف بیشتر واحدهای برق به خدمت گرفتن فن‌آوریهای جدید سیستم‌های ارتباطی، استانداردها و پروتکل‌های ارتباطی مربوطه در سیستم‌های SCADA می‌باشد. در این فصل استفاده از پروتکل TCP/IP بر روی شبکه‌های ارتباطی مربوط به سیستم اطلاعاتی شبکه قدرت و همچنین فن‌آوری اطلاعات و تا حدودی نیز کاربردهای آن در سیستم‌های SCADA بحث و بررسی خواهد شد.

۴-۲- شبکه‌های ارتباطی مدرن در شبکه قدرت

در دهه‌های اخیر تلاشهای فراوانی در جهت استاندارد نمودن پروتکلهای ارتباطی در شبکه‌های قدرت از سوی بیشتر واحدهای برق صورت گرفته است. به همین منظور در سال ۱۹۹۰ مؤسسه EPRI[2] مفهومی بنام UCA[3] را معرفی نمود [۱] که هدف آن همسو نمودن پروتکلهای ارتباطی استفاده‌شده در شبکه قدرت بوده و آنکه این پروتکلها به چه میزان توانایی ترکیب با یکدیگر را داشته و با هم سازگاری خواهند داشت. همچنین به چه میزان قادرند نیازهای آینده شبکه‌های

---

[1] Information Technology
[2] Electric Power Research Institute
[3] Utility Communication Architecture

ارتباطی مربوط به شبکه قدرت را برآورده سازند. همانگونه که در شکل ۴-۱ نشان داده شده است این معماری شامل اترنت بر روی لایه فیزیکی و لایه ارتباط داده‌ای (توسط کابل زوج سیم یا فیبر نوری)، TCP/IP و OSI –ISO[1] بر روی لایه شبکه و همچنین MMS[2] بر روی لایه کاربرد می‌باشد. به این علت که هزینه‌های پیاده‌سازی اترنت پایین بوده همچنین همبستگی لازم میان سخت‌افزارهای مربوط به شبکه (همانند هابها، پلها و مسیریابها) در آن وجود دارد این برتری باعث انتخاب لایه فیزیکی/ارتباط داده‌ای برای آن می‌باشد.

Manufacturing Messaging Specification (MMS)		لایه کاربرد
International Standards Organization – OSI Networking Stack	TCP/IP Networkoing Stack	لایه شبکه
10M,100M,1000M Ethernet 10Base T and 10BaseFL Media (کابلهای زوج سیم یا فیبر نوری)		لایه فیزیکی و ارتباط داده‌ای

شکل ۴-۱ معماری ارائه شده توسط UCA

در اینجا TCP/IP بر پایه پروتکل کنترل انتقال/اینترنت بوده و در لایه شبکه بر روی اینترنت استفاده می‌گردد. TCP/IP به‌صورت یک پروتکل جاری[3] عمل می‌نماید بدین معنی که انتقال بسته‌های داده‌ای در صورتی اتفاق می‌افتد که قبل از آن جریانی از داده‌ها بافر را پر کرده باشد[۳۳]. این نوع انتقال داده ممکن است در حین انتقال، تأخیر اندکی در ارسال بسته‌های کوچکتر را باعث شود که در مجموع می‌توان گفت استفاده از پروتکل TCP/IP مبتنی بر کنترل تراکم داده‌ها در صورت ترافیک بر روی شبکه ارتباطی می‌باشد که این مورد در ارسال داده‌های بلادرنگ دور از انتظار نیست. در این

---

[1] Open Systems Interconnect
[2] Manufacturing Messaging Specification
[3] Streaming

معماری، OSI -ISO نیز بر روی لایه شبکه می‌باشد و تا حدودی شبیه TCP/IP عمل می‌نماید با این تفاوت که اشکالات اساسی‌تری نسبت به ارتباطات داده‌ای خواهد داشت. لایه کاربرد نیز مجموعه‌ای از خدمات مربوط به عملیات داده‌ها را شامل می‌شود که به‌صورت نرم‌افزاری توسط کاربران صورت می‌گیرد.

امروزه در شبکه قدرت مشخصه‌های تصادفی مربوط به شبکه‌های ارتباطی مدرن می‌تواند تأثیر بسزایی بر حالات رؤیت‌پذیری شبکه قدرت داشته باشد. برای مثال پخش زمانهای مربوط به تحویل بسته‌های داده‌ای تحت شرایط مختلف ترافیک شبکه‌ای ممکن است اثرات زیادی بر محاسبات تخمین حالت به‌صورت بلادرنگ داشته و یا باعث بروز خطاهای دور از انتظار گردد و یا ممکن است داده‌های اندازه‌گیری ارسالی از سوی کامپیوتر RTU با تأخیر زمانی به تخمینگر حالت واقع در مرکز کنترل ارسال شوند که این خود می‌تواند باعث عدم رؤیت بسیاری از باسهای یک شبکه قدرت در طول یک یا چند فاصله محاسباتی گردد.

ارتباطات داده‌ای همواره نقش اساسی در اجرای عملیات و کنترل فرآیندهای مربوط به یک شبکه قدرت ایفا نموده‌اند. امروزه دو مدل شبکه‌ای را که توسط مؤسسه EPRI در شبکه‌های ارتباطی واحدهای برق جهت تبادل داده‌های مورد نیاز به‌صورت استاندارد شناخته شده‌اند[۳۲] یکی پروتکل شبکه‌ای ارتباط مستقیم و دیگری پروتکل شبکه پشت به پشت می‌باشد که در بخشهای بعدی شرح آنها آورده شده است.

۴-۳- شبکه ارتباط مستقیم

شبکه‌های ارتباط مستقیم[1] یکی از ساده‌ترین پیکربندیها برای تبادل داده‌های اطلاعاتی در سیستم‌های صنعتی می‌باشد که در این پیکربندی هر یک از میزبانها قادرند مستقیماً توسط برخی از رسانه‌های

[1] Direct Link

فیزیکی به این شبکه ارتباطی متصل شوند. در اینجا یک رسانه فیزیکی به‌عنوان مثال می‌تواند شامل یک سیم مسی یا کابل فیبرنوری باشد. یک شبکه ارتباط مستقیم ممکن است ناحیه کوچکی را در برگرفته باشد و گاهی نیز به‌صورت ناحیه وسیعی (مثلاً گستره جهانی) گسترده شده باشد. گام نخست در پیاده‌سازی یک شبکه ارتباط مستقیم اتصال دو یا چند گره به همدیگر با استفاده از یک رسانه ارتباطی مناسب می‌باشد و برای آنکه بسته‌های اطلاعاتی به‌طور موفقیت آمیز ارسال گردند می‌بایست پیش از آدرس‌دهی موارد زیر بر روی داده‌ها انجام شوند.

۱- کدگذاری[1]

۲- قاب‌گذاری[2]

۳- حفاظت خطا[3]

۴- توزیع داده‌ها با قابلیت اطمینان[4]

۵- دسترسی به رسانه[5]

پنج مورد فوق از جمله موارد مهمی هستند که هر فن‌آوری شبکه‌ای ارتباط مستقیم جهت انتقال بسته‌های داده‌ای از آن بهره می‌برد. در ادامه موارد آورده شده در بالا، در این بخش برخی از فن‌آوری‌های شبکه‌ای که امروزه به‌طور معمول جهت شبکه‌های اطلاعاتی مدرن شبکه قدرت مورد استفاده قرار می‌گیرند بررسی می‌گردد. جدول ۴-۱ برخی از فن‌آوریهای شبکه ارتباط مستقیم به همراه پارامترهای مهم آن‌را نشان داده است.

---

[1] Encoding
[2] Framing
[3] Error Detection
[4] Reliable Delivery
[5] Access Mediation

٤-٣-١- شبکه اترنت (استاندارد IEEE 802.3)

شبکه اترنت در ابتدا به‌صورت یک فن‌آوری مربوط به شبکه محلی بود که اخیراً با توجه به توسعه امکانات مخابراتی و محیط انتقال، زمینه استقرار دستگاه‌های موجود در یک شبکه اترنت با مسافت‌های بالاتر از چند کیلومتر نیز فراهم شده است. امروزه شبکه‌های اترنت با سرعتهای مختلفی از قبیل ۱۰ Mbps، ۱۰۰ Mbps، ۱۰۰۰ Mbps ارائه می‌گردد. سرعتهای ۱۰۰ Mbps (اترنت سریع[1]) و ۱۰۰۰ Mbps (گیگا بایت اترنت) امروزه جهت ارتباطات دوطرفه به‌طور همزمان[2] و نقطه به نقطه[3] نیز موارد استفاده دارند[۳۳].

جدول ۴-۱ برخی از فن‌آوریهای مربوط به شبکه ارتباط مستقیم [۳۰]

	Ethernet	Token Ring	ControlNet	DeviceNet
Data rate (Mbs)	10	4/16	5	0.5
Bit time (µs)	0.1	0.25/0.063	0.2	2
Max. length (m)	2500	250/segment	1000	100
Max. data size (bytes)	1500	4500/17800	504	8
Min. data size (bytes)	64	96	7	47/8
Max. number of hosts	1024	260	99	64
Typical prop speed (m/s)	Coax: $2x10^8$			

پروتکل‌های مربوط به اترنت مجموعه قوانین لازم برای ایجاد فریم‌ها را مشخص می‌کنند. در اینجا اندازه یک فریم به‌صورت محدود بوده و می‌بایست مجموعه‌ای از اطلاعات ضروری و موردنیاز در یک فریم وجود داشته باشند. مثلاً یک فریم بایستی دارای آدرس‌های مبدأ و مقصد باشد که آدرس‌های فوق هویت فرستنده و دریافت‌کننده یک پیغام را مشخص خواهند کرد و این آدرس

---

[1] Fast Ethernet
[2] Full-Duplex
[3] Ponit-to-Point

مشخصه اختصاصی مربوط به یک گره را مشخص می‌نماید. دو دستگاه متفاوت در اترنت نمی‌توانند دارای آدرس‌های یکسانی باشند.

یک سیگنال اترنت بر روی محیط انتقال به هر یک از گره‌های متصل‌شده در محیط انتقال خواهد رسید. بنابراین در اینجا مشخص شدن آدرس مقصد، به‌منظور دریافت پیام نقشی حیاتی ایفا می‌نماید. هرفریم اترنت می‌تواند طولی به میزان ۵۱۲ بیت (٦٤ بایت) داشته باشد که جهت حداقل اندازه یک بسته ۵۱۲ بیتی حداکثر طولی برابر با ۲۵۰۰ متر برای شبکه اترنت (۱۰ Mbps) فرض می‌شود. در اینجا میزان تأخیر بین میزبانها معادل ۵۱,۲ میکروثانیه می‌باشد[۳۳].

در اترنت فن‌آوری CSMA/CD[1]، مسئولیت تشریح و تنظیم نحوه ارتباط گره‌ها را با یکدیگر برعهده داشته، همچنین شروع انتقال و ارسال اطلاعات را قانونمند و تنظیم می‌نماید. در اینجا مفهوم "دسترسی چندگانه"[2] بدین منظور است که تمامی ایستگاه‌های موجود (متصل) در محیط انتقال قادر خواهند بود از انتقال اطلاعات آگاه شوند. در پروتکل اترنت وضعیت "حس حامل"[3] یعنی قبل از آنکه ایستگاهی قادر به ارسال اطلاعات باشد می‌بایست بررسی نماید که آیا محیط انتقال برای ارسال اطلاعات آزاد است و در صورت مثبت بودن جواب، ایستگاه مورد نظر قادر به استفاده از محیط انتقال و ارسال اطلاعات خواهد بود. در شبکه اترنت ممکن است دو ایستگاه به طور همزمان قصد استفاده از محیط انتقال و ارسال اطلاعات را داشته باشند. در صورت پدید آمدن این اتفاق که به آن پدیده تصادم[4] گویند هر یک از ایستگاه‌های مربوطه به مدت زمانی کاملاً تصادفی در حالت انتظار مانده و پس از اتمام زمان انتظار و بررسی شرط آزاد بودن محیط انتقال می‌توانند ارسال اطلاعات را آغاز نمایند[۳۲].

---

[1] Carrier Sense Multiple Access with Collision Detection
[2] Multiple Access
[3] Carrier Sense
[4] Collision

٤-٣-٢- شبکه‌های حلقه- نشانه (استاندارد IEEE 802.5)

شبکه‌های حلقه - نشانه[1] از روش ارسال و عبور نشانه بهره‌گرفته و همچنین از توپولوژی حلقه‌ای استفاده می‌کنند. البته در عمل معمولاً از توپولوژی حلقه- ستاره استفاده می‌شود که در این آرایش کامپیوترها به یک هاب[2] مرکزی متصل هستند و علامت یا نشانه در یک حلقه مجازی بین کامپیوترها حرکت می‌کند. در این آرایش کاربران جزئی از حلقه هستند، اما اتصال آن‌ها به این حلقه از طریق هاب صورت می‌گیرد که هاب نیز به صورت فیزیکی به شبکه متصل است. سرعت انتقال داده در شبکه‌های حلقه- نشانه بین ٤ Mbps تا ١٦ Mbps است[٣٣].

٤-٣-٣- شبکه کنترل‌نت (ControlNet)

شبکه ControlNet در سیستم‌های صنعتی مثالی از یک شبکه باس عبور- نشانه[3] می‌باشد که همانند یک شبکه حلقه- نشانه داده‌ها را به اشتراک می‌گذارد. باس- نشانه (استاندارد IEEE 804.4) یک پروتکل خطی، افت چندگانه[4] و به‌صورت یک توپولوژی درختی شکل و یا سگمنت می‌باشد[١١]. در یک شبکه ControlNet تمامی میزبانها به یک باس مشترک وصل می‌باشند. معماری باس ControlNet تا حدودی شبیه شبکه اترنت است و به‌صورت منطقی همانند یک شبکه حلقه- نشانه عمل می‌کند. در ControlNet نشانه‌ها بر پایه آدرس‌های فیزیکی عمل می‌کنند که بجای میزبانهای مجاور در شبکه حلقه- نشانه می‌باشند و نشانه عبوری مربوط به آدرس‌ها از بالا به پایین است. بدلیل آنکه معماری ControlNet از نوع باس مشترک بوده و در هر زمان فقط یک میزبان در حال انتقال داده می‌باشد پس هیچکدام از فریمها در اینجا با یکدیگر تصادم نخواهند داشت[١١].

---

[1] Token Ring
[2] Hub
[3] Token-Passing Bus
[4] Multidrop

٤-٣-٤- شبکه دیوایس‌نت (DeviceNet)

شبکه DeviceNet (CAN Bus[1]) در حقیقت پروتکلی استاندارد جهت لایه‌های فیزیکی و ارتباط داده‌ای می‌باشد که به‌صورت ارتباطات سریال جهت کاربردهای صنعتی خودکار موارد استفاده دارد. معماری CAN به‌گونه‌ای است که داده‌های انتقال‌یافته از هر ایستگاه شامل آدرس مبدأ و یا مقصد نمی‌باشند و در واقع این ماهیت فریم است که برای دیگر ایستگاه‌ها اهمیت داشته و به همین دلیل گاه این معماری را محتواگرا[2] نیز گویند[۱۱]. در اینجا محتوای هر پیغام توسط شناسه‌های انحصاری مشخص‌می‌شود.

در وضعیت‌هایی که دو یا چند ایستگاه می‌کوشند تا به‌طور همزمان انتقال داده را انجام دهند، در اینجا نیز با استفاده از مکانیزم CSMA/CD تعیین می‌کند که کدام پیغام برروی شبکه منتشر شود، بگونه‌ای که پیغامهای ارسالی هدر نروند. نکته مهم در این نوع پروتکل‌ها این‌است که داده‌های منتشر شده با یک‌بار انتشار بر روی شبکه به‌دست ایستگاه‌های مقصد می‌رسند. در اینجا ایستگاه‌های مقصد ممکن است یک، چند و یا تمامی ایستگاه‌های شبکه را شامل شوند که این رفتار ترافیک شبکه‌ای را به حداقل می‌رساند[۱۱].

۴-۴- پروتکل شبکه‌ای پشت به پشت

در بخش قبلی شرحی بر فن‌آوریهای مربوط به لایه ارتباط داده‌ای[3] آورده شد که خدمات تحویل و توزیع بسته‌های داده‌ای را از سوی یک میزبان به دیگر میزبانها نشان می‌داد. در این بخش پروتکل پشت به پشت[4] مربوط به لایه انتقال[1] ارائه می‌شود، بدین معنی که این معماری ارتباط میان برنامه‌های

---

[1] Control Area Network
[2] Content Oriented
[3] Data Link Level
[4] End-to-End

کاربردی را فراهم می‌سازد. یک معماری پشت به پشت می‌بایست موارد زیر را جهت یک انتقال بهینه فراهم نماید[۳۲].

۱- تحویل یک پیغام را تا رسیدن به مقصد تضمین نماید.

۲- پیغامهای دریافتی در مقصد به همان منظور ارسال، تحویل داده شوند.

۳- جهت هر پیغام بیشتر از یک نسخه پشتیبانی، کپی برداشته شود.

۴- همزمانی میان فرستنده و دریافت‌کننده را در نظر گیرد.

۵- فرآیندهای کاربردی چندگانه[1] جهت هرکدام از میزبانها را حمایت کند.

در اینجا پروتکل‌های انتقال بگونه‌ای طراحی شده‌اند تا قادر به تغییر خصوصیات مورد نیاز، با استفاده از برنامه‌های کاربردی و بدون در نظر گرفتن زیر لایه شبکه، سطح بالایی از خدمات را فراهم سازند. پروتکل شبکه‌ای پشت به پشت دارای محدودیت‌هایی نیز می‌باشند که برخی از این محدودیتها به‌صورت زیر آورده شده‌اند.

۱- پیغامهایی که در مسیر انتقال از بین می‌روند.

۲- پیغامهای ناقصی که به علت عدم ارسال کامل می‌بایست دوباره ارسال شوند.

۳- همسان نمودن کپی‌یک پیغام ارسالی با پیغام اصلی.

۴- محدود بودن برخی از پیغامها از نظر اندازه.

دو پروتکل رایج پشت به پشت در شبکه‌های ارتباطی که در اینجا بیشترین کاربرد را دارند می‌توان TCP و UDP را نام برد.

---

[1] Multiple Application Processes

۴-۵- استفاده از فن‌آوری اطلاعات در سیستم‌های قدرت

یکی از نیازهای اساسی جهت تبادل اطلاعات، استفاده هر چه بیشتر از فن‌آوری اطلاعات در تمامی زمینه‌های کاربردی شبکه قدرت می‌باشد که اهمیت آن روز به‌روز بیشتر احساس می‌گردد. امروزه با به خدمت گرفتن فن‌آوری اطلاعات در سیستم اطلاعاتی شبکه قدرت، دسترسی و اشتراک زیادی از داده‌های اطلاعاتی فراهم گردیده است[۳۵]. هم‌اکنون بیشتر واحدهای برق جهت برآوردن نیازهای اطلاعاتی خود قصد پیاده‌سازی سیستمی را دارند که توان تجمعی و تبادل هر چه سریعتر داده‌های اطلاعات را داشته و قادر باشد از یک روش یکسان برای جبران‌سازی اطلاعات، مبادله و اشتراک آنها استفاه نماید[۳۶]. هر چند در اینجا ممکن است عدم سازگاری برخی از فرمت‌های داده‌ای چندگانه[۱] با همدیگر و نیز نبود یک استاندارد مناسب جهت تبادل داده‌ها میان استفاده‌کنندگان مختلف وجود داشته باشد.

در گذشته‌ای نه چندان دور استانداردهای متعددی جهت مدیریت اطلاعات در شبکه قدرت استفاده می‌شد که امروزه برخی از این استانداردها یا اشباع شده‌اند و یا اینکه با سیستم‌های امروزی سازگاری ندارند. جهت رفع این مشکلات، استفاده از استانداردی یکسان را می‌طلبید تا واسطی میان انواع مختلف سیستم‌ها بوده و نیز توانایی تبادل اطلاعات میان سایر تجهیزات مربوط به شبکه قدرت را داشته باشد که این نیز به نوبه خود بسیار مشکل، وقت‌گیر و هزینه‌بر می‌باشد. در آینده نزدیک در صنعت برق استفاده هرچه بیشتر از یک معماری اطلاعاتی جهانی[۲] به صرفه‌تر به نظر می‌رسید که به عنوان مثال می‌توان مدل استاندارد تبادل داده‌های اطلاعاتی و شبکه‌های ارتباطی از قبیل اینترنت را نام برد. این مدل قادر به پاسخگویی جهت سایر نیازهای مربوط به نرخهای انتقال اطلاعات و همچنین کیفیت‌های جریان داده‌ای مربوط به سایر سیستم‌های اطلاعاتی می‌باشد[۳۶].

---

[1] Multiple Data Formats
[2] Universal Information Architecture

امروزه کاربرانی که در سازمانهای مختلف شرکتهای برق مشغول به‌کار هستند نیازمند دسترسی به اطلاعات مربوط به سیستم SCADA در نقاط مختلف می‌باشند. مسئله‌ای که در اینجا مطرح می‌شود چگونگی دسترسی به این داده‌ها با کمترین هزینه و یک روش ایمن[1] می‌باشد. همانطور که از نظر گذشت، یک سیستم SCADA قادر است گستره وسیعی از سطح جغرافیایی را پوشش داده بگونه‌ای که سایر فرمانهای کنترلی و داده‌های اطلاعاتی را جهت مطالبات درون سازمانی و برون سازمانی با هماهنگی‌های خاص خود فراهم نماید. تبادل داده‌های اطلاعاتی به خصوص در زمانهای بحرانی[2] نیازمند دسترسی هرچه سریع‌تر و به صورت ایمن می‌باشد که امروزه پیشرفتهای مربوط به شبکه‌های ارتباطی همچون فن‌آوری‌های مبتنی بر اینترنت و وب امکان دسترسی به اطلاعات و توسعه سیستم SCADA را با هزینه‌های اجرائی پایین‌تر و همچنین به‌صورت دیاگرامهای تک- خطی[3] تسهیل نموده است[۳۷].

در گذشته ایجاد دیاگرامهای تک- خطی جهت کاربردهای مربوط به EMS،SCADA و DMS در بیشتر پیاده‌سازیها به‌صورت دستی صورت می‌گرفت که این فرآیند بسیار خسته‌کننده، با صرف زمان زیاد و گاهی نیز با خطا[4] مواجه می‌شد. امروزه با استفاده از واسطهای کاربری-گرافیکی (GUI)[5] برای شبیه‌سازیها و اجرای نمایش دینامیکی سیستم‌های قدرت توسعه یافته‌اند که بیشتر آنها به صورت برنامه‌های مستقل[6] عمل می‌کنند[۳۷]. پیاده‌سازی سیستم SCADA مبتنی بر وب که در سال ۱۹۹۰ توسط محققان مطرح گردید در ابتدا مفهوم آن بسیار پیچیده می‌نمود، امروزه با به خدمت گرفتن فن‌آوری سرویس‌دهنده/مشتری، استفاده از نرم‌افزارهای جاوا و XML در سیستم‌های بلادرنگ، این پیاده‌سازیها را آسانتر نموده است.

---

[1] Secure
[2] Critical times
[3] One-Line Diagrams
[4] Error-prone
[5] Graphical User Interfaces
[6] Stand-alone

۴-۶- فن‌آوریهای نرم افزاری

با توسعه سیستم‌های نرم‌افزاری و GUIهای متعدد، پیاده‌سازی هر چه بهتر فن‌آوری‌های شبکه‌ای در سایر جنبه‌های سیستم امروزی SCADA مشاهده می‌شود. به‌عنوان نمونه برخی از این فن‌آوریهای نرم‌افزاری به صورت زیر آورده شده‌اند:

٤-٦-١- فن‌آوری سرویس‌دهنده/مشتری

در گذشته برنامه‌های کاربردی که در سیستم‌های سنتی SCADA مورد استفاده قرار می‌گرفتند فقط جهت برخی از سیستم‌های عامل و بانک‌های اطلاعاتی خاص قابل استفاده بودند که این خود نیز محدودیت‌هایی را باعث می‌گردید. برای مثال در برخی موارد این برنامه‌ها نیازمند تغییرات تابعی ساده‌ای بودند که در درون برنامه می‌بایست دوباره‌نویسی، تبدیل و یا از نو آزمایش گردند. امروزه استفاده از ساختار سرویس‌دهنده/مشتری دسترسی به نیازهای فوق را تسهیل نموده، خصوصاً که استفاده از برنامه‌های کاربردی را در شرایط بحرانی جهت استفاده هزاران کاربر به‌طور همزمان مهیا ساخته‌است. ساختار سرویس‌دهنده/مشتری به صورت شئ‌گرا و مبتنی بر سرویس‌دهنده[1] و بانکهای اطلاعاتی است که جهت راه‌حلهای مبتنی بر وب نیز مناسب می‌باشد. در شکل ٤-٢ یک الگوی معماری سرویس‌دهنده/مشتری سه‌ردیفه[2] مشاهده می‌شود که ردیف‌های آن به ترتیب شامل[۳۸]:

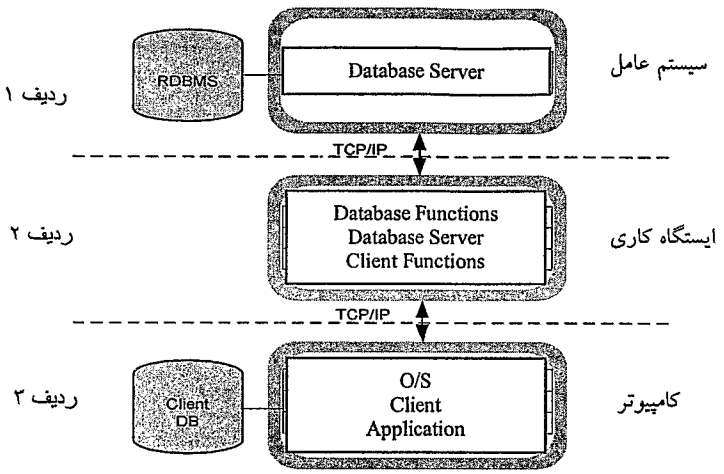
۱- ردیف خدمات[3]

۲- ردیف ذخیره داده‌ها[4]

۳- ردیف واسط انسان- ماشین(MMI[5])

---

[1] Server-Based
[2] Tier
[3] ServiceTier
[4] Data Store
[5] Man-Machine Interface



شکل ۴-۲ یک الگوی معماری سرویس‌دهنده/مشتری سه ردیفه

٤-٦-٢- برنامه‌های تحت شبکه

برنامه‌های شبکه‌ای این قابلیت را داشته که اطلاعات ذخیره‌شده را در هر کجای دنیا بازیابی نموده، همچنین کاربران قادر خواهند بود با استفاده از برنامه‌های شبکه‌ای بر روی شبکه ارتباطی با یکدیگر تبادل اطلاعات داشته باشند. امروزه برنامه‌های تحت شبکه در سیستم SCADA کاربردهای زیادی را جهت تبادل داده‌های اطلاعاتی بر عهده دارند که با استفاده از آنها دسترسی به داده‌های بلادرنگ سیستم SCADA در هر کجا می‌تواند برای افراد مجاز فراهم شود. همچنین چون هزینه‌های زیادی جهت دسترسی به اینترنت مورد نیاز نمی‌باشد تمامی کاربران با استفاده از یک مرورگر وب که جهت اتصال به سرویس‌دهنده سیستم SCADA مبتنی بر وب جهانی(WSDS[1]) نیاز دارند و با توجه به مجوز کاربری خود قادر خواهند بود به تمامی داده‌های مورد نیاز دسترسی پیدا کنند[۳۸].

٤-٦-٣- فن‌آوری XML

رشد روزافزون شبکه اینترنت باعث دسترسی هرچه سریع‌تر به اطلاعات، توزیع آنها و نیز مبادله بهتر این اطلاعات را فراهم نموده است. هر چند که در آغاز محدودیتهایی در مقیاسهای بزرگ تبادل

---

[1] Web-Based SCADA Display Systems

داده‌ای از قبیل گسترش، ساخت و شناسایی داده‌ها با توجه به داشتن یک پلت‌فرم چندگانه وجود داشت که با استفاده از فن‌آوریهای مبتنی بر شبکه تارگستر جهانی (WWW[1]) جهت تبادل اطلاعات توزیعی و پردازش آنها، زبان نشانه‌گذاری توسعه‌یافته (XML[2]) این مسئله را تسهیل نموده است. فن‌آوری XML به‌صورت ساختار سلسله مراتبی عمل می‌کند بدین معنی که یک ساختار درختی یا مدل داده‌ای مناسب را برای برنامه‌های کاربردی ارائه داده و آنها را به‌صورت متنی نمایش می‌دهد که استفاده از آن را برای انسانها و نیز ماشینها قابل فهم می‌نماید[۳۹]. امروزه فن‌آوری XML شرایطی را فراهم آورده است تا تبادل اطلاعات میان سایر کاربردهای موجود سیستم‌های قدرت به صورت مجزا برآورده گردد، همچنین با حداقل اصلاحات بر روی این کاربردها تبادل اطلاعات صورت پذیرد.

٤-٦-٤- زبان برنامه‌نویسی جاوا

سیستم‌های نرم‌افزاری در شبکه قدرت سنتی و استفاده از آنها در سیستم‌های قدرت امروزی، رویکردهای جدیدی را به سمت استفاده از ابزارهای برنامه‌نویسی شئ‌گرا[3] و زبانهای جدید برنامه‌نویسی همانند جاوا[4] با شعار معروف خود "نوشتن برای یکبار، اجرا در همه جا" و نیز فن‌آوری جدید آن یعنی J2EE و زبان نشانه‌گذاری فرامتنی (HTML[5]) برای کاربردهای مبتنی بر جاوا را در محیط اینترنت جهت مدیریت، استقرار و توسعه آسان داده‌ها فراهم نموده است[۴۰]. زبان برنامه‌نویسی جاوا به‌گونه‌ای طراحی شده‌است تا بدون در نظر گرفتن ریزپردازنده یا سیستم عامل مورد استفاده، در هر کامپیوتر یا ابزارهای محاسباتی دیگر قابل اجرا باشد. از جاوا می‌توان جهت تولید برنامه‌های کوچکتر به‌نام اپلت‌ها[6] استفاده نمود که برای قرار گرفتن در کامپیوتر سرویس‌دهنده شبکه متمرکز طراحی شده‌اند. با استفاده از اپلت‌های جاوا در شبکه، کاربر می‌تواند تابع برنامه و

---

[1] World Wide Web
[2] eXtensible Markup Language
[3] Object-oriented
[4] Java
[5] Hyper Text Markup Language
[6] Applets

داده‌های مورد نیاز را فراخوانی کرده و کارهای خاص مربوطه را بر روی آن انجام دهد و دیگر نیازی به نگهداری فایل داده‌ها و برنامه‌های نرم‌افزاری حجیم در کامپیوتر خود ندارد و در صورت نیاز به این داده‌ها می‌تواند آنها را از کامپیوتر سرویس‌دهنده فراخوانی نماید.

جاوا نرم‌افزار بسیار قدرتمندی است که قادر است متن، داده، گرافیک، صدا و ویدئو را در یک برنامه مدیریت کند. از کاربردهای بیشتر جاوا طراحی برنامه‌های کاربردی بزرگتر در محیط اینترنت یا شبکه‌های ارتباطی خاص می‌باشد. همانگونه که بیان شد زبان جاوا به‌عنوان یک زبان برنامه‌نویسی است که جهت استفاده در محیطهای شبکه‌ای مناسب شناخته شده است. در حالیکه کاربردهای اینترنت گسترش می‌یافت به طبع آن سازگاری این زبان بیشتر نمایان می‌شد بگونه‌ای که این زبان راه‌حلهای متعددی جهت رفع مشکلات در آدرس‌دهی زبانهای دیگر را نیز فراهم نموده است. سطح ایمنی اپلت‌های جاوا نسبت به دیگر نرم‌افزارها بسیار بالا بوده و به‌طور نسبی کاربردها و اپلتهای آن برای ارسال و دریافت داده‌ها بر روی اینترنت حرکتی رو به جلو داشته است[۴۱] و به همین خاطر استفاده از زبان جاوا در سیستم‌های SCADA با توجه به گستردگی آن مناسب شناخته شده است.

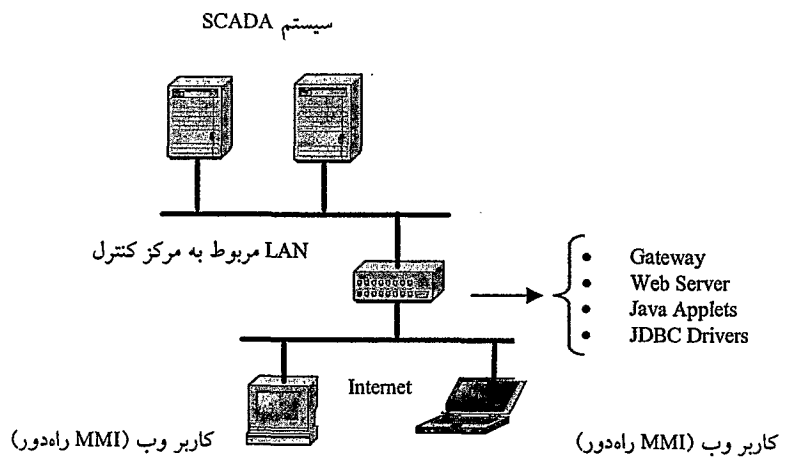
٤-٦-٥- برنامه‌نویسی بانک اطلاعاتی

جهت بایگانی و ذخیره داده‌های اطلاعاتی شبکه قدرت امروزه نرم‌افزارهای بانکهای اطلاعاتی کاربردهای زیادی پیدا کرده‌اند. در سیستم‌های جدید، بانک‌های اطلاعاتی همچون SQLJ[1] مورد استفاده قرار می‌گیرند که به‌صورت یک روش استفاده از زبان SQL[2] تحت برنامه‌های جاوا می‌باشند و برای کاهش هزینه‌های نگهداری و توسعه برنامه‌های جاوا جهت اتصال به بانک اطلاعاتی مورد استفاده قرار می‌گیرند. SQLJ یک مدل ساده برای کد جاوا فراهم نموده که شامل تمامی عملیات مربوط به SQL است همچنین یک برنامه واسط کاربردی بسیار ساده و به‌نام رابط بانک اطلاعاتی

---

[1] Structured Query Language Java
[2] Structured Query Language

جاوا (JDBC[1]) ارائه می‌دهد که برای توسعه کاربردهایی که به داده‌های نسبی دسترسی داشته و نیز می‌توانند با بانک‌های اطلاعاتی multi-vendor و راه‌اندازهای SQLJ استاندارد استفاده نمایند را شامل می‌شود[۴۲]. در شکل ۴-۳ یک پیاده‌سازی سیستم SCADA مبتنی بر اینترنت نشان داده شده‌است. در این پیاده‌سازی سیستم SCADA داده‌های اطلاعاتی بلادرنگ و داده‌های ذخیره‌شده از قبل[2] را در بانک‌های اطلاعاتی مربوطه که شامل داده‌های اخطار (آلارم)، رخدادها، پیکربندی سیستم و ... می‌باشند را در خود جای داده‌است. در اینجا دروازه[3] به‌صورت یک نود تابع چندگانه عمل می‌نماید بدین معنی که نه فقط به‌عنوان یک دروازه ارتباطی جهت ارتباط شبکه مربوط به سیستم SCADA به اینترنت بوده بلکه قادر است توابع سرویس‌دهنده وب جهت کاربران راه‌دور را فراهم نموده، همچنین واسطهای برنامه کاربردی (APIs) مربوط به JDBC و اپلت‌های جاوا نیز در اینجا بارگذاری می‌شوند.



شکل ۴-۳ یک سیستم SCADA مبتنی بر اینترنت

سرویس‌دهنده‌های وب توسط کاربران راه‌دور قابل دسترسی[4] هستند که هر کاربر با استفاده از آدرس سایت اینترنتی مورد نظر به آن دسترسی دارد. هنگامیکه ارتباط یک کاربر با این آدرس برقرار می‌شود

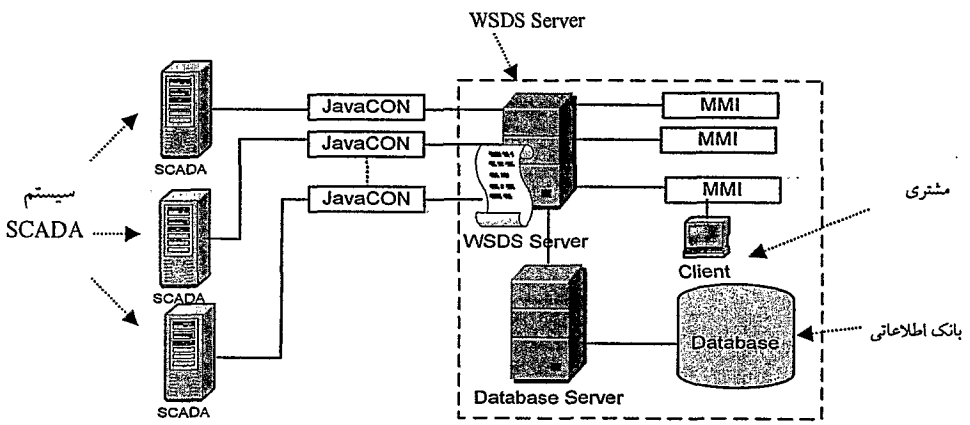
---

[1] Java Database Connectivity
[2] Historic Data
[3] Gateway

راه‌اندازهای[1] JDBC و اپلت‌های جاوا بر روی کامپیوتر کاربر بارگذاری می‌شوند که با استفاده از GUIهای مختلفی به‌عنوان توابع مربوط به مرورگرهای وب بارگذاری منابع و همچنین واسطهای مورد نیاز کاربری فراهم می‌گردند.

۴-۷- الگویی از یک سیستم SCADA مبتنی بر وب

بر پایه طراحی معماری سه- ردیفه شکل ٤-۲، در اینجا توسعه یک نرم‌افزار نمونه به‌نام PowerNet بیان می‌گردد. PowerNet یک نرم افزار workflow بوده که قادر است برخی از توابع SCADA همچون تولید دیاگرام تک- خطی و اجرای اعمال مربوط به داده‌ها را به‌صورت بلادرنگ مدلسازی نماید[۳۸]. شکل۴-۴ پیکربندی از PowerNet را توصیف می‌کند.



شکل ۴-۴ پیکربندی PowerNet در سیستم SCADA

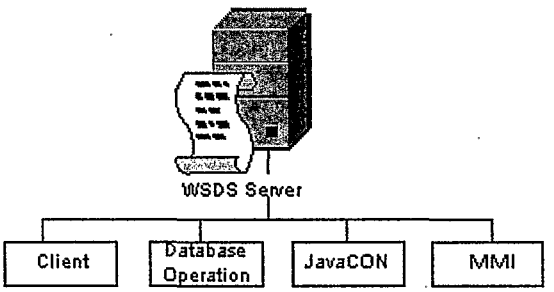
در شکل۴-۴، واسط نرم‌افزاری JavaCON جهت اتصال جاوا به سیستم SCADA می‌باشد که به عنوان یک پل ارتباطی میان سیستم SCADA و سرویس‌دهنده WSDS عمل می‌نماید. سرویس‌دهنده WSDS نیز توسط JavaCon پیغامها را از سیستم SCADA دریافت نموده و سپس آنها را جهت استفاده در اختیار MMI قرار می‌دهد. MMI نیز از طریق یک مرورگر شبکه از داده‌های مورد نیاز

---

[1] Drivers

سیستم SCADA استفاده نموده که این داده‌ها را در اختیار مهندسان، طراحان و مدیران رده بالای واحدهای برق قرار می‌دهد. MMI در طرف سایت مشتری همان شکل GUI مربوطه در سایت سرویس دهنده را دارد که اینگونه طراحی‌ها، به‌عنوان مثال کاربر را قادر خواهد ساخت تا جزئیات مربوط به یک پست برق را مشاهده نموده و وقتی که کاربر به سرویس دهنده WSDS دسترسی پیدا کرد با استفاده از یک مکامیزم امنیتی فقط به کاربران مجاز این اجازه را داده تا به داده‌های اطلاعاتی سیستم SCADA دسترسی داشته باشند.

یک سرویس‌دهنده WSDS به‌طور کامل توسط کدهای جاوا نوشته شده‌است که نیاز به یک مفسر جاوا جهت تجزیه بایت کد[1] مربوطه در هر زمانی که سرویس‌دهنده WSDS اجرا می‌شود دارد. به طوریکه در شکل۴-۵ نشان داده شده، سرویس‌دهنده قادر است چهار تابع مربوطه را از قبیل تابع مشتری، تابع JavaCON، تابع MMI و عملیات مربوط به بانک اطلاعاتی را حمایت کند که در زیر شرح آنها باختصار آورده شده است.



شکل ۴-۵ توابع مربوط به سرویس دهنده WSDS

٤-۷-۱- تابع JavaCON

JavaCON با یک سیستم SCADA به‌صورت از راه دور و مبتنی بر پروتکل TCP/IP و سوکتها در ارتباط می‌باشد. سرویس‌دهنده WSDS، داده‌های آنالوگ، اطلاعات مربوط به وضعیت بریکرها و تغییر تپهای تراتسفورماتور را به‌صورت بلادرنگ از سیستم SCADA دریافت کرده و آنها را بر روی

---

[1] Bytecode

صفحه وب نشان می‌دهد. در اینجا جهت پردازش JavaCONهای چندگانه از Multi-threading استفاده می‌شود. هنگامیکه یک JavaCON با سرویس‌دهنده WSDS ارتباط برقرار می‌کند یک thread برای پردازش داده‌های انتقالی از JavaCON مورد استفاده قرار می‌گیرد.

٤-٧-٢- بانک‌های اطلاعاتی

عملیات مربوط به بانک اطلاعاتی در طرف سایت سرویس‌دهنده و بر روی JDBC و SQLJ صورت می‌گیرد. JDBC به‌صورت یک برنامه واسط کاربردی مبتنی بر جاوا جهت اجرای اعمال مربوط به SQL می‌باشد و به برنامه جاوا این اجازه را داده تا اعمال مربوط به SQL را به بانک اطلاعاتی مورد نظر ارسال نماید. دو مجموعه از راه‌اندازهای JDBC مختلف برای عملیات مربوط به دو بانک اطلاعاتی متفاوت مورد استفاده قرار می‌گیرند. یکی راه‌انداز خالص JDBC-Net می‌باشد که JDBC نامیده شده و می‌تواند درون یک پروتکل شبکه‌ای مستقل DBMS را ترجمه کرده و در نهایت آن را توسط سرویس‌دهنده در درون یک پروتکل DBMS جای دهد. این راه‌انداز اساساً جهت استفاده در بانک های اطلاعاتی تحت شبکه Oracle کاربرد دارد. راه‌انداز دیگری به‌نام JDBC-ODBC[1] می‌باشد که به‌صورت یک پل ارتباطی به راه‌اندازODBC اضافه می‌شود که این پل ارتباطی دسترسیJDBC را بر حسب راه‌اندازهای ODBC برای استفاده بانک‌اطلاعاتی میزبان فراهم می‌نماید.

٤-٧-٣- تابع مشتری

در اینجا برنامه جاوا ارتباط میان مشتری و سرویس‌دهنده را تسهیل نموده است. ارتباط بین سرویس دهنده و مشتری شامل سه بخش برنامه سایت سرویس‌دهنده، برنامه سایت مشتری و پروتکل استفاده شده مربوط به هر یک آنها می‌باشد. هنگامیکه برنامه سایت مشتری شروع به کار می‌کند، در ابتدای کار به سرویس‌دهنده WSDS متصل شده، سرویس‌دهنده WSDS نیز آماده ارائه خدمات مورد نیاز به آن مشتری می‌باشد. برنامه سایت سرویس‌دهنده نیز یک thread جهت هدایت این مشتری را

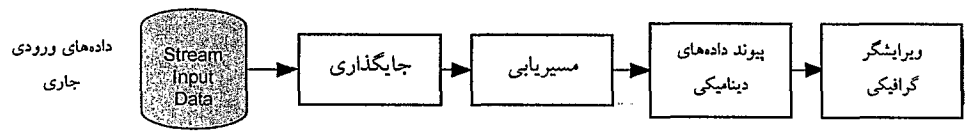
---

[1] Open Database Connectivity

شروع به ارسال می‌نماید. در اینجا هر مشتری می‌بایست دارای یک نام کاربری و یک شماره شناسه‌ای مجاز جهت دسترسی به اطلاعات مورد نیاز سیستم SCADA باشد.

٤-٧-٤- واسط انسان- ماشین (MMI)

در اینجا MMI بوسیله GUI و دیاگرامهای تک- خطی خود تولید، حمایت می‌شود. همانگونه که در شکل ۴-۶ مشاهده می‌شود دیاگرامهای تک- خطی خود تولید شامل داده‌های ورودی جاری[1]، جایگذاری، مسیریابی، پیوند داده‌های دینامیکی و ویرایشگر گرافیکی می‌باشند. در اینجا داده‌های ورودی جاری، اطلاعات مربوط به سایر مؤلفه‌های پست برق را جهت ایجاد توپولوژی (هم‌بندی) پست برق به کار می‌برد.



شکل ۴-۶ فرآیند تولید دیاگرام تک- خطی

[1] Stream Input Data

فصل ۵

بررسی اثر تأخیر در شبکه‌های ارتباطی

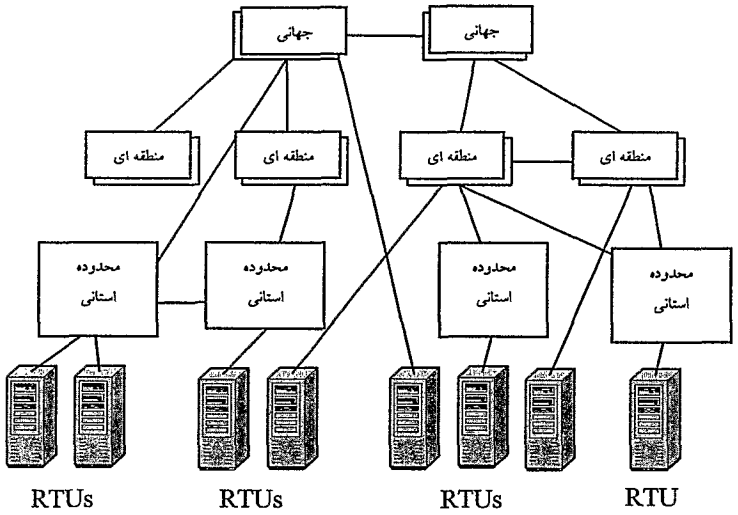
۵-۱- مقدمه

پروتکل‌ها و سیستم‌های ارتباطی در سیستم قدرت به دلایل مختلفی همچون محدودیتهای سرعت انتقال، انتقال مجدد در گره‌های ارتباطی و زمانهای مربوط به پردازش اطلاعات، باعث تأخیر در ارسال داده‌های اندازه‌گیری از RTU به مرکز کنترل می‌شوند. RTUها معمولاً داده‌های اندازه‌گیری را به‌صورت دیجیتالی پردازش و ذخیره می‌نمایند[۴۳]. اگر چه ممکن است گاهیRTUها به‌صورت محلی توابع کنترلی را برعهده داشته باشند ولی در بیشتر مواقع انتقال داده‌های اندازه‌گیری در فواصل دور با تأخیرهای زمانی همراه می‌باشد، این تأخیرها می‌تواند ناشی ازکاهش سرعت انتقال داده‌ها، تأخیرهای مربوط به توزیع داده‌ها و سرعت پردازش در تجهیزات ارتباطی باشند و یا ممکن است در اثر ترافیک در شبکه ارتباطی بدلیل انتقال داده‌های اطلاعاتی مختلف روی دهند[۴۴].

۵-۲- اثر تأخیر زمانی بر عملکرد سیستم SCADA

در سیستم‌های SCADA ممکن است عمل نظارت و کنترل داده‌های اندازه‌گیری به‌صورت گسترده بر شبکه ارتباطی در موقعیت‌های جغرافیایی متفاوتی انجام گردد که این اطلاعات ممکن است از مراکز کنترل مختلفی عبور نمایند، مثلاً از یک سطح پایین‌تر در محدوده استانی به سطح بالاتری در محدوده منطقه‌ای ارسال شوند و یا این اطلاعات در گستره جهانی دریافت گردند. همانگونه که در شکل ۵-۱ مشاهده می‌شود تبادل داده‌ها از طرف RTUها از طریق شبکه ارتباطی به مراکز کنترل به صورت سلسله مراتبی نشان داده شده است که به آن توپولوژی درختی گفته می‌شود.

با توجه به این توپولوژی هر کدام از سطوح مراکز کنترل قادرند با سطح مشابه خود در ارتباط باشند و یا می‌توانند به‌طور مستقیم با سطح بالاتر خود تماس داشته باشند. همچنین یک RTU می‌تواند مستقیماً با هر یک از سطوح مختلف مرکز کنترل با استفاده از شبکه ارتباطی در تماس باشد.

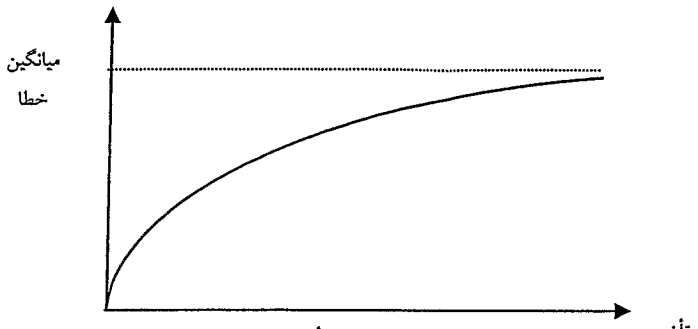


شکل ۵-۱ توپولوژی درختی یک سیستم SCADA

این ساختار سیستم ارتباطی، پروتکل‌هایی را شامل می‌شود که ارتباط بین هر یک از RTUها را به مراکز کنترل برقرار نماید. انتقال اطلاعات اندازه‌گیری از طرف یک نود به نود دیگر با تأخیرهای زمانی همراه می‌باشد که این زمان می‌تواند از چند ثانیه جهت مراکز کنترلی که به‌طور مستقیم به RTUها متصل هستند، باشد و یا برای مراکز کنترلی در گستره جهانی که اطلاعات را با واسطه دریافت می‌نمایند داده‌های اطلاعاتی زمانهای بیشتری را طی کنند. در فرآیند ارسال داده‌ها تأخیرهای موجود در سیستم ارتباطی، خطای اندازه‌گیری مربوط به اندازه‌های رؤیت شده در مرکز کنترل را سبب خواهند شد[٤٥]. در این فرآیند ارسال داده‌ها اگر $x(t)$ به‌صورت یک مقدار اندازه‌گیری شده ارسالی از طرف یک RTU فرض شود، r_x شدت تغییرات آن و T نیز تأخیر مربوط به سیستم ارتباطی باشد. مقدار e_T یعنی خطای اندازه‌گیری مربوط به مقدار رؤیت‌شده در مرکز کنترل به‌صورت معادله زیر می‌باشد[۴۵]:

$$e_T = f(T, r_x) \qquad (۱-۵)$$

معادله فوق تابع مشخصه‌های آماری مربوط به پارامتر $x(t)$ می‌باشد. با وجود این، در صورتیکه میزان تأخیر برابر صفر باشد میانگین خطا صفر می‌شود. زمانی که میزان تأخیر زیاد گردد، میانگین خطا به‌طور صعودی بالا می‌رود که این مطلب در شکل ۵-۲ نشان داده شده است.



شکل ۵-۲ میزان اندازه خطای تأخیر مربوط به انتشار[۴۵]

۵-۳- مدل تحلیلی رگرسیون خودکار

ارتباط میان میزان تأخیرهای سیستم ارتباطی و میانگین خطای اندازه‌گیری با داشتن ساختار آماری داده‌های اطلاعاتی بیان می‌گردد. با داشتن داده‌های اندازه‌گیری (m_x میانگین آماری داده‌ها، s_x واریانس داده‌ها)، ساختار آماری داده‌ها به‌صورت یک مدل تحلیلی رگرسیون خودکار بیان می‌شود[۴۴].

در اینجا با استفاده از عبارت $y(t)=x(t)-m_x$ یک مقدار داده جدید با همان خاصیت $x(t)$ و میانگین صفر بدست می‌آید. با فرض آنکه بتوان $y(t)$ را با استفاده از مدل رگرسیون خودکار (AR[1]) بیان کرد، معادله خطای اندازه‌گیری به‌صورت زیر بدست می‌آید:

$$\dot{y}(t)+Ay(t)=e(t) \qquad (۲-۵)$$

که در آن پارامتر $A>0$ و $e(t)$ خطای اندازه‌گیری می‌باشد.

در اینجا یک پیش‌بینی کننده جهت تخمین $y(t+T)$ به صورت زیر محاسبه می‌شود:

$$y(t+T\,|\,t)=e^{-AT}y(t) \qquad (۳-۵)$$

همچنین

$$x(t+T\,|\,t)=m_x+y(t+T\,|\,t)=m_x+e^{-AT}y(t) \qquad (۴-۵)$$

$$x(t+T\,|\,t)=m_x+e^{-AT}(x(t)-m_x) \qquad (۵-۵)$$

---

[1] Auto-Regressive

که واریانس پیش‌بینی کننده به‌صورت زیر بدست می‌آید.

$$s_T^2 = s_x^2(1-e^{-2AT}) \qquad (۵-۶)$$

در معادله (۵-۶) نسبت واریانس پیش‌بینی‌کننده به واریانس داده‌ها به میزان تأخیر زمانی در سیستم‌های ارتباطی (T) و پارامتر A بستگی دارد.

برای بدست آوردن این مدل تحلیلی می‌بایست مفهوم شدت تغییرات $x(t)$ بیان گردد. با فرض داشتن یک نمایش موقت از $x(t)$، شکل طیفی[1] آن به‌صورت $X(\omega)$ خواهد شد. نتایج بدست آمده نشان می‌دهد[۴۴] که جهت شدت تغییرات بالاتر، نیاز به پهنای باند بیشتری بر روی سیستم ارتباطی می‌باشد. با توجه به این نتایج، پهنای باند سیستم ارتباطی (B)، به‌عنوان پارامتری جهت اندازه‌گیری شدت تغییرات $x(t)$ استفاده می‌گردد. در نتیجه معادله (۵-۱) را می‌توان به‌صورت زیر نوشت:

$$e_T = f(T,B) \qquad (۵-۷)$$

فرض می‌شود که $P_y(\omega)$ طیف تابع چگالی توان (PDF)[2] برای $y(t)$ و $R(T)$ نیز کوواریانس مربوط به آن باشد. در مدل رگرسیون خودکار می‌توان نوشت:

$$R(T) = e^{-A|T|} \qquad (۵-۸)$$

و از طرف دیگر تابع چگالی توان از رابطه زیر بدست می‌آید:

$$P_y(\omega) = F[RR(T)] = F[s_y^2.R(T)] = F[s_y^2.e^{-A|T|}] \qquad (۵-۹)$$

که در آن $F[.]$، تابع تبدیل فوریه است. در نتیجه:

$$P_y(\omega) = \frac{2As_y^2}{A^2+\omega^2} \qquad (۵-۱۰)$$

که برای بدست آوردن پهنای باند به‌صورت زیر بدست می‌آید:

---

[1] Spectrum Form
[2] Power Density Function

$$\left[\frac{P_y(2\pi B)}{P_y(0)}\right]_{dB} = 10\log\left(\frac{P_y(2\pi B)}{P_y(0)}\right) \qquad (۱۱-۵)$$

که نتیجه می‌دهد:

$$\frac{2As_y^2}{A^2+4\pi^2B^2} = \frac{1}{2}\frac{2s_y^2}{A} \qquad (۱۲-۵)$$

و یا

$$A = 2\pi B \qquad (۱۳-۵)$$

در معادلات بیان شده در بالا مقدار پهنای باند فرآیند $y(t)$ مشخص شده است. هر چند که $y(t)$ با افزایش یک مقدار ثابت ($-m_x$) به $x(t)$ بدست می‌آید، ولی چون تفاوت $P_y(\omega)$ با $P_x(\omega)$ در فرکانس صفر می‌باشد تغییری در پهنای باند نخواهند داشت. بنابراین B همچنان که پهنای باند فرآیند $y(t)$ است، پهنای باند فرآیند $x(t)$ نیز می‌باشد.

وقتی که یکبار رابطه میان پارامترهای مدل رگرسیون و پهنای باند فرآیند بدست آمد، یک پیش‌بینی‌کننده را می‌توان با جایگذاری مقادیر مربوطه طراحی کرد، بدین‌صورت که:

$$x(t+T\,|\,t) = m_x + e^{-2\pi BT}(x(t)-m_x) \qquad (۱۴-۵)$$

در نتیجه خطای اندازه‌گیری به‌صورت معادله زیر بدست می‌آید:

$$e(t+T) = |x(t+T)-x(t)| \qquad (۱۵-۵)$$

که مقدار دقیق این خطا مشخص نمی‌باشد، هرچند که یک تخمین از آن را می‌توان توسط معادله زیر بیان نمود:

$$e(t+T\,|\,t) = |x(t+T\,|\,t)-x(t)| = \left(1-e^{-2\pi BT}\right)|x(t)-m_x| \qquad (۱۶-۵)$$

در معادله فوق برای یک مقدار داده شده از T، خطای تخمین محاسبه شده با زمان تغییر می‌کند. با میانگین‌گیری از دو طرف معادله (۵-۱۶) میانگین خطای ناشی از تأخیر در سیستم ارتباطی به صورت زیر است:

$$e_T = E[e(t+T\,|\,t)] = \left(1-e^{-2\pi BT}\right)E[|x(t)-m_x|] \qquad (۱۷-۵)$$

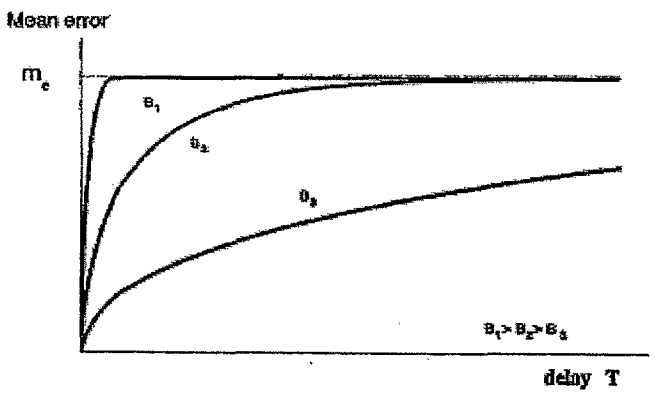
با تعریف پارامتر آماری، مقدار $x(t)$ به‌صورت $m_e = E[|x(t)-m_x|]$ بدست آمده است:

$$e_T = (1 - e^{-2\pi BT})\, m_e \qquad (۱۸-۵)$$

به‌عبارت دیگر می‌توان واریانس تخمین خطای ناشی از تأخیر سیستم ارتباطی را به صورت زیر نوشت:

$$s_T^2 = E\left[\left(e(t+T \mid t) - e_T\right)^2\right] = \left(1 - e^{-2\pi BT}\right)^2 \left(s_x^2 - m_e^2\right) \qquad (۱۹-۵)$$

همانطور که نشان داده شد، مدل AR(1) جهت ارزیابی خطاهای مربوط به اندازه‌گیریها در سیستم‌های SCADA مورد استفاده قرار گرفته است. با این فرض یک پیش‌بینی‌کننده مناسب جهت تخمین داده‌های اندازه‌گیری ارسالی طراحی شده است که این مدل تحلیلی مشخصه نمایی مربوط به خطای اندازه‌گیری را همانطور که در شکل ۵-۳ آورده شده است به‌صورت تابعی از تأخیر سیستم ارتباطی و پهنای باند مربوطه نشان می‌دهد.



شکل ۵-۳ خطای اندازه‌گیری به صورت تابعی از تأخیر سیستم ارتباطی و پهنای باند[۴۵]

۵-۴- تأخیر زمانی در طراحی کنترل کننده

امروزه یک شبکه قدرت مدرن بگونه‌ای طراحی می‌شود که در آن منابع تولید توان و بارها به‌صورت پراکنده در سطح وسیعی نسبت به هم واقع شده‌اند. ژنراتورها و بارها ممکن است صدها کیلومتر و یا بیشتر از همدیگر فاصله داشته باشند که معمولاً جهت کنترل و پایداری مربوط به شبکه‌های قدرت

به صورت یک شماتیک کنترل توزیع‌شده استفاده می‌گردد. به‌عنوان مثال در پایدارسازهای سیستم قدرت (PPS[1]) و رگولاتورهای ولتاژ از یک شماتیک کنترل توزیع‌شده استفاده شده است[۴۶].

برای حل مسائل مربوط به طراحی شماتیک کنترل توزیع‌شده در شبکه‌های قدرت، این شماتیک کنترل در نواحی گسترده به‌صورت متمرکز تعریف می‌شود که جهت سازگاری با دینامیک غیر خطی شبکه قدرت با استفاده از روش LMI[2] حل بهینه‌ی مسائل مربوطه با شرایط خطی و قیود نیمه معین[3] شامل ماتریسهای متقارن، انجام می‌شود [٤٧].

برای درک بهتر شماتیک کنترل متمرکز، داده‌های اندازه‌گیری ارسالی شامل سیگنالهای ولتاژ، جریان و زوایای فاز از طرف نواحی مختلف به مرکز کنترل ارسال می‌شوند. مرکز کنترل نیز سیگنالهای کنترلی مربوطه را به کنترل‌کننده‌های قدرت محلی می‌فرستد. در این فرآیند ارتباطی، رسانه‌های مختلفی مورد استفاده قرار می‌گیرند که خود ممکن است باعث بروز تأخیر زمانی در ارسال و دریافت داده‌ها شوند. این تأخیر زمانی می‌تواند معادل چند میلی ثانیه تا چندین ثانیه و یا بیشتر تغییر نماید. تأخیر زمانی برای یک سیگنال پسخور در سیستم‌های قدرت در حدود ۱۰۰ میلی ثانیه تخمین زده شده است.[٤٧].

در حوزه لاپلاس یک تأخیر زمانی ایده‌آل به‌صورت e^{-sT} بیان می‌گردد. در اینجا e^{-sT} به‌صورت یک عبارت گویا نمی‌باشد، بنابراین نمی‌تواند در ابعاد محدود تحقق پذیر باشد که می‌توان جهت تحلیل و سهولت انجام محاسبه، آنرا با استفاده از یک تقریب نسبی با بعد محدود در حوزه فرکانسی جایگزین نمود. در گذشته این تقریبهای نسبی جهت تأخیر زمانی با استفاده از توابع بسل[4]، تقریبهای Padé،

---

[1] Power System Stabilizers
[2] Linear Matrix Inequalities
[3] Semi-Definite Constraints
[4] Bessel Functions

چند جمله‌ایهای لاگرانژ[1] و توابع هذلولی صورت می‌گرفت که با توجه به دقت بالای تقریب Padé در شبکه‌های قدرت، امروزه این تقریب بیشتر موارد استفاده دارد.

در شبکه‌های قدرت همانطور که قبلاً بیان شد، تأخیرهای زمانی و تحلیلهای مربوط به آن، بیشتر مربوط به ناحیه پردازش سیگنال و رسانه‌های ارتباطی می‌باشد که در اغلب موارد از تأخیرهای زمانی ناحیه کنترلی چشم پوشی می‌گردد. در مجموع این تأخیرها می‌تواند بدلیل مدلاسیون و دی‌مدلاسیون مربوط به داده‌ها در سیستم‌های ارتباطی باشند.

در نواحی گسترده‌تر شبکه‌های قدرت، کاربرد استفاده از ماهواره‌ها بدلیل قابلیت اطمینان بیشتر جهت سیستم‌های ارتباطی بیشتر نمایان می‌شود که در این ارتباط تأخیر انتقال داده‌ها در حدود ۲۵۰ میلی‌ثانیه می‌باشد. با توجه به فاصله‌ی ماهواره‌ها از زمین این تأخیر زمانی نیز تغییر می‌کند. در نواحی کوچکتر نیز کابلها، مایکروویوها و فیبرهای نوری استفاده می‌گردند که در اینجا زمان تصمیم‌گیری برای دریافت یک پیغام شامل مدلاسیون، دی‌مدلاسیون، تأیید و تأخیر ارتباط جهت یک مودم با سرعت انتقال داده‌ای ٤٨٠٠bps حدوداً ۱۰۰ میلی ثانیه تخمین زده شده است[٤٨].

جهت طراحی یک کنترل‌کننده و تحلیل اجرای سیستم کنترل بهتر است تابع نمائی e^{-sT} با استفاده از یک تابع تبدیل گویا[2] به‌صورت زیر جایگزین شود:

$$p(x)=\frac{a_0+a_1x+\ldots+a_lx^l}{b_0+b_1x+b_mx^m} \qquad (۲۰-۵)$$

که در آن مقادیر a_iها و b_jها ($i=0,1,\ldots,l$ و $j=0,1,\ldots,m$) به‌صورت ضرایب تقریب Padé می‌باشند و با استفاده از معادله زیر بدست می‌آیند:

$$p^{(l,m)}(z)=\frac{\sum_{j=0}^{l}\frac{(l+m-j)!\,j!\,z^j}{(l+m)!+j!(l-j)!}}{\sum_{j=0}^{m}\frac{(l+m-j)!\,m!\,z^j}{(l+m)!\,j!(m-j)!}} \qquad (۲۱-۵)$$

---

[1] Laguerre Polynomials
[2] Rational Transfer Function

در اینجا $z=-sT$ می‌باشد. در معادله (۵-۲۱) هر چه مقادیر l و m افزایش یابند تقریب $P(x)$ به مقدار e^{-sT} نزدیکتر خواهد شد. اگر مقادیر l و m به سمت بی‌نهایت میل کنند $P(x)$ به سری مکلورن e^{-sT} به صورت زیر تبدیل می‌شود:

$$e^{z}=\sum_{i=0}^{\infty}c_i z^i \qquad (۵-۲۲)$$

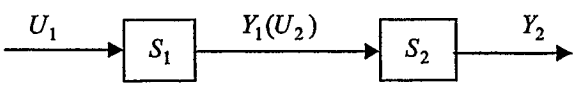
ضرایب تابع تبدیل Padé برای مقادیر $l=0,1,2$ و $m=0,1,2$ در جدول ۵-۱ آمده است.

جدول ۵-۱ ضرایب تابع تبدیل Padé

l / m	0	1	2
0	$\frac{1}{1}$	$\frac{-sT+1}{1}$	$\frac{\frac{1}{2}s^2T^2-sT+1}{1}$
1	$\frac{1}{sT+1}$	$\frac{-\frac{1}{2}sT+1}{\frac{1}{2}sT+1}$	$\frac{\frac{1}{6}s^2T^2-\frac{2}{3}sT+1}{\frac{1}{3}sT+1}$
2	$\frac{1}{\frac{1}{2}s^2T^2+sT+1}$	$\frac{-\frac{1}{3}sT+1}{\frac{1}{6}s^2T^2+\frac{2}{3}sT+1}$	$\frac{\frac{1}{12}s^2T^2-\frac{1}{2}sT+1}{\frac{1}{12}s^2T^2+\frac{1}{2}sT+1}$

در محیط MATLAB، زمان تأخیر مربوط به یک سیستم را می‌توان به‌صورت فضای حالت نشان داد. همانطور که در شکل ۵-۴ آمده است ارتباط میان دو سیستم فضای حالت نشان داده شده است. معادلات ریاضی مربوط به این سیستم به‌صورت زیر بیان می‌گردد:

$$\begin{aligned}\dot{X}_1 &= A_1X_1+B_1U_1\\ Y_1 &= C_1X_1+D_1U_1\\ \dot{X}_2 &= A_2X_2+B_2U_2\\ Y_2 &= C_2X_2+D_2U_2\end{aligned} \qquad (۵-۲۳)$$



شکل ۵-۴ ارتباط دو سیستم فضای حالت

در شکل ۵-۴، S_2 بلوک تأخیر زمانی مربوط به سیستم می‌باشد که مشخصه‌های آن به‌صورت زیر بیان می‌شود:

$$A_2=\begin{bmatrix} a & 0 & .... & 0 \\ 0 & a & .... & 0 \\ : & : & : & : \\ : & : & : & : \\ 0 & 0 & .... & a \end{bmatrix}، B_2=\begin{bmatrix} b & 0 & .... & 0 \\ 0 & b & .... & 0 \\ : & : & : & : \\ : & : & : & : \\ 0 & 0 & .... & b \end{bmatrix}، C_2=\begin{bmatrix} c & 0 & .... & 0 \\ 0 & c & .... & 0 \\ : & : & : & : \\ : & : & : & : \\ 0 & 0 & .... & c \end{bmatrix} و D_2=\begin{bmatrix} d & 0 & .... & 0 \\ 0 & d & .... & 0 \\ : & : & : & : \\ : & : & : & : \\ 0 & 0 & .... & d \end{bmatrix} \quad (۲۴-۵)$$

در ماتریسهای D, C, B, A آرایه‌های d , c, b, a به ترتیب، تأخیر زمانی به‌صورت نمایش تبدیل لاپلاس می‌باشند. در اینجا فرض بر این است که تأخیر مربوط به هر سیگنال یکسان بوده که در غیر اینصورت ترتیب مقادیر قطری نیاز به تغییر دارند. بنابراین در شکل ۵-۴ ، $U_2=Y_1$،

$$\dot{X}_2=A_2X_2+B_2(C_1X_1+D_1U_1)$$
$$Y_2=C_2X_2+D_2(C_1X_1+D_1U_1) \quad (۲۵-۵)$$

$$\begin{bmatrix}\dot{X}_1\\ \dot{X}_2\end{bmatrix}=\begin{bmatrix}A_1 & 0\\ B_2C_1 & A_2\end{bmatrix}\begin{bmatrix}X_1\\ X_2\end{bmatrix}+\begin{bmatrix}B_1\\ B_2D_1\end{bmatrix}U_1$$
$$Y_2=\begin{bmatrix}D_2C_1 & C_2\end{bmatrix}\begin{bmatrix}X_1\\ X_2\end{bmatrix}+D_2D_1U_1 \quad (۲۶-۵)$$

ماتریسهای D, C, B, A برای سیستم متصل شده نیز به‌صورت زیر می‌باشند.

$$A=\begin{bmatrix}A_1 & 0\\ B_2C_1 & A_2\end{bmatrix} \quad B=\begin{bmatrix}B_1\\ B_2D_1\end{bmatrix}$$
$$C=\begin{bmatrix}D_2C_1 & C_2\end{bmatrix} \quad D=D_2D_1 \quad (۲۷-۵)$$

برای طراحی یک کنترل‌کننده مقاوم جهت یک شبکه قدرت از معادلات حالت بدست آمده از سیستم متصل شده استفاده می‌گردد. برای جزئیات بیشتر به [۴۶] مراجعه شود.

فصل ۶

مدل اطلاعاتی سیستم قدرت و شبیه‌سازی

۶-۱- مقدمه

در این فصل جهت بررسی اثرات تأخیر در اندازه‌گیریهای ارسالی در یک سیستم SCADA، مدلی از شبکه قدرت را که شامل ترکیبی از هر دو ساختار فیزیکی شبکه قدرت و شبکه اطلاعاتی مربوط به آن می‌باشد، بررسی می‌گردد. ابتدا مدل کلاسیک شبکه قدرت بیان می‌شود سپس یک مدل اطلاعاتی مربوط به داده‌های اندازه‌گیری در شبکه قدرت در دو حالت بدون اختلال و با اختلال در شبکه ارتباطی ارائه می‌گردد. در بخش‌های بعدی نیز جهت مدل تخمین تأخیر بر روی شبکه TCP/IP، با استفاده از مدل اطلاعاتی آورده شده، شبیه‌سازی یک مدل از شبکه قدرت به‌صورت عملی بر روی شبکه LAN وخط Dial پیاده‌سازی می‌شود.

۶-۲- مدل کلاسیک سیستم قدرت

مدل رفتاری یک سیستم قدرت به‌صورت زیر بیان می‌شود:

$$\dot{x} = f(x, y) \quad \text{و} \quad 0 = g(x, y) \tag{۶-۱}$$

در اینجا x حالت دینامیکی سیستم و y حالت جبری شبکه قدرت می‌باشد که با کاهش معادلات جبری فوق تحت فرضیات متغیرهای جبری به‌صورت زیر بیان می‌گردد:

$$\dot{x} = f(x) \tag{۶-۲}$$

در صورت بروز نوسانات بار معادله ۶-۲ تبدیل به یک معادله دیفرانسیل اتفاقی به‌صورت زیر می‌گردد:

$$\dot{x}_\varepsilon = f(x_\varepsilon) \tag{۶-۳}$$

در اینجا x_ε حالت اختلال اتفاقی سیستم قدرت را نشان می‌دهد که میانگین نویزهای گاوسی افزوده برای آن فرض شده است. این نویزها می‌تواند شامل واریانس نوسانات بار از قبیل واریانس ولتاژ، جریان و توان تزریقی در یک باس و یا خطاهای مربوط به تأخیر در اندازه‌گیریها بر روی شبکه ارتباطی باشد. در مرکز کنترل متغیرهای اندازه‌گیری رؤیت شده با میزان واقعی ارسالی از سوی RTU

متفاوت بوده، که ممکن است بدلیل تأخیرهای تصادفی در شبکه ارتباطی مقدار دیگری را نشان دهند.

٦-٢-١- مدل اطلاعاتی سیستم قدرت بدون اختلال (Unperturbed)

متغیرهای اطلاعاتی سیستم قدرت از قبیل مقدار ولتاژ، جریان و توان تزریقی مربوط به هر باس برای یک سیستم کلاسیک m-machine n-bus به‌صورت زیر بیان می‌گردد[١٥]:

$$\dot{\delta}_i = \omega_i$$

$$\dot{\omega}_i = -\frac{D_i}{M_i}\omega_i + \frac{1}{M_i}\left[P_{mi} - P_{ei}(V,\delta)\right]$$

$$\dot{m}_{Vk} = \frac{1}{r_k}(V_k - m_{Vk})$$

$$\dot{m}_{Ik} = \frac{1}{r_k}(I_k - m_{Ik}) \qquad i = 2,\ldots,m \quad k = 1,\ldots,n$$

$$\dot{m}_{Pk} = \frac{1}{r_k}(P_{Ik} - m_{Pk})$$

$$P_{ei}(V,\delta) = |V_i|^2|Y_{ii}|\cos\theta_{ii} + \sum_{\substack{j=1 \\ j\neq i}}^{n}|V_i||V_j||Y_{ij}|\cos(\theta_{ij} - \delta_i + \delta_j) \qquad (۴-۶)$$

پارامترها و مقادیر فوق به‌صورت زیر بیان می‌گردند:

$\dot{\delta}_i$ = زاویه فاز

ω_i = فرکانس

M_i = ضریب اینرسی

D_i = ضریب میرایی

$P_{mi}(P_{ei})$ = توان ورودی مکانیکی (خروجی الکتریکی)

P_{Ik} = توان تزریقی حقیقی باس

I_k = جریان تزریقی باس

V_k = ولتاژ باس

$|Y_{ij}|(\theta_{ij})$ = مقدار (فاز) عنصر ij ام $Ybus$

m_{Vk} = اندازه ولتاژ باس رؤیت شده در مرکز کنترل

m_{Ik} = اندازه جریان باس رؤیت شده در مرکز کنترل

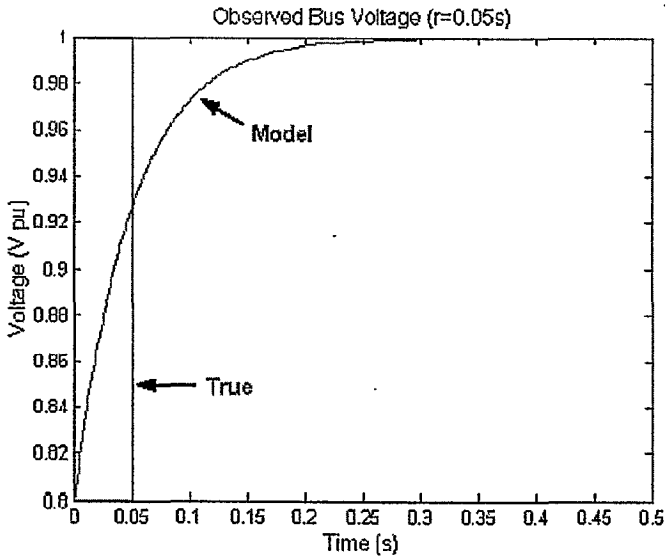
m_{Pk} = اندازه توان باس رؤیت شده در مرکز کنترل

r_k = ثابت زمانی شبکه ارتباطی رؤیت شده در مرکز کنترل

مدل اطلاعاتی فوق بر اساس مدل دینامیکی سیستم قدرت کلاسیک می‌باشد که در اینجا M_i ، D_i و P_{mi} مقادیر ثابتی فرض شده‌اند. بردار حالت، x، این مدل به‌صورت زیر بیان می‌گردد:

$$x = [\delta \;\; \omega \;\; m_V \;\; m_I \;\; m_P]^T \qquad (۵-۶)$$

جهت بدست آوردن متغیرهای اطلاعاتی، می‌بایست معادله دیفرانسیل فوق حل گردد. در این مدل فرض بر این است که ترافیک شبکه‌ای (نویز) وجود نداشته و میزان فاصله زمانی τ بسمت صفر میل می‌کند که مقدار متغیر با توجه به شکل ٦-١ در مرکز کنترل به‌صورت نمایی به مقدار واقعیش میل می‌کند[١٥]. همچنین تأخیر زمانی مربوط به داده‌های اندازه‌گیری جهت تمامی متغیرهای رؤیت‌شده در هر باس یکسان بوده، بدین‌گونه که مجموعه بسته‌های یکسانی را با همدیگر تشکیل می‌دهند. در اینجا میزان r_k برای همه باس‌ها یکسان است ($r_k = r \;\; for \;\; k = 1,...,n$).



شکل ۶-۱ پاسخ پله ولتاژ رویت شده [١٥]

٦-٢-٢- مدل اطلاعاتی سیستم قدرت با اختلال (Perturbed)

معادلات ۶-۴ جهت مواردی صادق است که پاسخ مرتبه اول با یک ثابت زمانی مشخص باشد. در بخش قبل شبکه ارتباطی بدون هیچگونه مؤلفه تصادفی از تأخیرهای مربوط به بسته‌های اندازه‌گیری

ارسالی در نظر گرفته شد که با فرض وجود ترافیک شبکه‌ای (نویز)، ثابت زمانی r_k به مقدار s_k تغییر می‌یابد که به‌صورت رابطه زیر بیان می‌گردد:

$$s_k = \frac{1}{r_k} \qquad (۶-۶)$$

و مؤلفه نوسانی[1] s_k را می‌توان به‌صورت زیر نوشت:

$$s_k \to s_k[1+\gamma_k \dot{w}(t)] \qquad (۶-۷)$$

در اینجا $\dot{w}(t)$، نویز گاوسی و γ_k پارامتر مقایسه‌ای جهت توصیف شدت نویز است (در باس k ام) که معادل نسبت انحراف معیار به مقدار میانگین s_k مربوط به آن باس می‌باشد که با توجه به میزان ترافیک شبکه‌ای در هر باس مانیتور شده تغییر می‌یابد. در اینجا فرض شده است تمامی RTU ها به شبکه یکسانی متصل می‌باشند و ترافیک یکسانی جهت هرکدام در نظر گرفته شده است، بدین معنی که مقادیر γ_k جهت تمامی باسها یکسان است. با جایگذاری معادله ۶-۷ در معادلات ۶-۴ معادلات دیفرانسیل اتفاقی زیر بدست می‌آیند:

$$\begin{aligned}
\dot{m}_{Vk} &= s_k(V_k - m_{Vk}) + s_k\gamma_k(V_k - m_{Vk})\dot{w}_{Vk} \\
\dot{m}_{Ik} &= s_k(I_k - m_{Ik}) + s_k\gamma_k(I_k - m_{Ik})\dot{w}_{Ik} \qquad k = 1,\ldots,n \\
\dot{m}_{Pk} &= s_k(P_{Ik} - m_{Pk}) + s_k\gamma_k(P_{Ik} - m_{Pk})\dot{w}_{Pk}
\end{aligned} \qquad (۶-۸)$$

که بردار حالت، x_ε، در صورت وجود اختلال به‌صورت زیر بیان می‌گردد:

$$x_\varepsilon = [\delta \ \omega \ m_{\varepsilon V} \ m_{\varepsilon I} \ m_{\varepsilon P}]^T \qquad (۶-۹)$$

در اینجا هدف محاسبه مقادیر s_k و γ_k می‌باشد که می‌توان پارامتر s_k را توسط اندازه‌گیریهای بدست آمده به‌صورت میانگین زمان تأخیر برای ارسال یک بسته از باس kام به مرکز کنترل بدون در نظر گرفتن هیچگونه نویز خارجی بر روی شبکه ارتباطی فرض نمود. γ_k نیز معادل نسبت انحراف معیار به مقدار میانگین زمان تأخیر در بسته ارسالی(از باس kام) می‌باشد. چون این پارامترها بشدت تحت

---

[1] Fluctuation

تاثیر ترافیک شبکه‌ای قابل تغییر هستند می‌توان این اندازه‌ها را برای سطوح مختلف ترافیک شبکه‌ای محاسبه نمود.

۶-۳- مدل غیرخطی سیستم اطلاعاتی

در صورتیکه یک تغییر ناگهانی در سیستم قدرت رخ دهد داده‌های اطلاعاتی بدست آمده یا متغیرهای رؤیت شده (m_{Vi} ، m_{Ii} و m_{Pi}) در مرکز کنترل دیگر همانند مدل نمایی بیان شده در بخش ۶-۲، به‌صورت نمایی به سمت متغیرهای واقعی خود (V_i ، I_i و P_i) میل نمی‌کنند. در اینجا متغیرهای اطلاعاتی در مقادیر اولیه خود مانده، سپس به‌طور غیرهمزمان به سمت مقادیر واقعی خود پرش می‌کنند که این در صورتی اتفاق می‌افتد که پس از بروز تأخیر در سیستم، اختلالی رخ داده باشد.

٦-۳-۱- مدل غیرخطی سیستم اطلاعاتی بدون اختلال

در اینجا همانند مدل بخش ۶-۲-۱، بر اساس مدل دینامیکی کلاسیک شبکه قدرت n-bus ،m-machine هر دو ساختار فیزیکی و اطلاعاتی مدل پیاده‌سازی می‌شوند. با استفاده از مدل Logistic Growth که قابلیت مدل‌سازی پاسخ متغیرهای اطلاعاتی برای یک تغییر ناگهانی در متغیرهای شبکه قدرت واقعی را دارد می‌توان این مدل را پیاده‌سازی نمود[۱۵]. در اینجا با استفاده از این مدل، نمایش متغیرهای اطلاعاتی یک سیستم کامل m-machine،n-bus به‌صورت زیر است:

$$\dot{m}_{Vk} = \frac{m_{Vk}}{a_k}\left(1-\frac{m_{Vk}}{V_k}\right) \qquad i=2,\ldots,m \quad k=1,\ldots,n$$

$$\dot{m}_{Ik} = \frac{m_{Ik}}{a_k}\left(1-\frac{m_{Ik}}{I_k}\right)$$

$$\dot{m}_{Pk} = \frac{m_{Pk}}{a_k}\left(1-\frac{m_{Pk}}{P_{Ik}}\right) \qquad (۶-۱۰)$$

که با حل معادلات فوق، متغیرهای اطلاعاتی بدست می‌آیند.

$$m_{Vk}(t) = \frac{m_{Vk}(0).V_k}{m_{Vk}(0)+(V_k-m_{Vk}(0))\exp(-\frac{t}{a_k})}$$

$$m_{Ik}(t) = \frac{m_{Ik}(0).I_k}{m_{Ik}(0) + (I_k - m_{Ik}(0))\exp(-\frac{t}{a_k})} \qquad (۱۱-۶)$$

$$m_{Pk}(t) = \frac{m_{Pk}(0).P_{Ik}}{m_{Pk}(0) + (P_{Ik} - m_{Pk}(0))\exp(-\frac{t}{a_k})}$$

در اینجا a_k، ماکزیمم نرخ رشد پاسخ مدل می‌باشد که تابعی از میانگین تأخیر زمانی مربوط به مقادیر متغیر تحویلی در یک شبکه قدرت واقعی به مرکز کنترل می‌باشد.

۶-۳-۲- مدل غیرخطی سیستم اطلاعاتی با اختلال

معادلات ۶-۱۰، جهت پاسخ شبکه ارتباطی با یک ثابت زمانی در مواقعی که هیچگونه مؤلفه تأخیر تصادفی وجود نداشته باشد معتبر است و موارد استفاده دارد. برای مدل غیرخطی شبکه قدرت مؤلفه تصادفی تأخیر به‌صورت یک مؤلفه نویز گاوسی افزوده به پارامتر a_k فرض می‌گردد که در اینجا تبدیل به یک متغیر جدید b_k ، به‌صورت زیر می‌شود:

$$b_k = \frac{1}{a_k} \qquad (۱۲-۶)$$

و مؤلفه نوسانی آن به‌صورت زیر می‌باشد:

$$b_k \to b_k[1 + \lambda_k \dot{w}(t)] \qquad (۱۳-۶)$$

در اینجا $\dot{w}(t)$، نویز گاوسی و λ_k پارامتر مقایسه‌ای جهت توصیف شدت نویز در باس kام می‌باشد. λ_k نیز با توجه به سطح ترافیک شبکه‌ای (نویز) جهت هر باسی که مانیتور می‌شود قابل تغییر است. در اینجا فرض می‌شود که همه کامپیوترهایRTU به شبکه‌ای یکسان متصل می‌باشند و ترافیک یکسانی جهت هریک از باسهای مانیتور شده در نظر گرفته می‌شود. بدین‌معنی که λ_k برای تمامی Kها مقدار یکسانی خواهد داشت. با جایگذاری ۶-۱۳ در معادلات ۶-۱۰ معادلات دیفرانسیل اتفاقی زیر را بدست می آیند:

$$\dot{m}_{Vk} = b_k m_{Vk}\left(1 - \frac{m_{Vk}}{V_k}\right) + b_k \lambda_k m_{Vk}\left(1 - \frac{m_{Vk}}{V_k}\right)\dot{w}_{Vk}$$

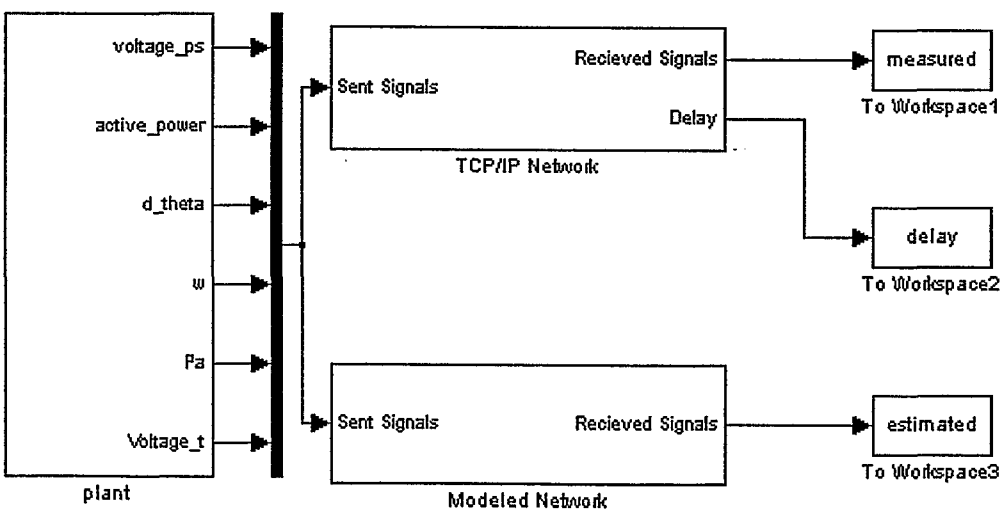
$$\dot{m}_{Ik} = b_k m_{Ik}\left(1 - \frac{m_{Ik}}{I_k}\right) + b_k \lambda_k m_{Ik}\left(1 - \frac{m_{Ik}}{I_k}\right)\dot{w}_{Ik} \qquad k = 1,\ldots,n$$

$$\dot{m}_{Pk} = b_k m_{Pk}\left(1-\frac{m_{Pk}}{P_{lk}}\right)+b_k\lambda_k m_{Pk}\left(1-\frac{m_{Pk}}{P_{lk}}\right)\dot{w}_{lk} \qquad (۱۴-۶)$$

در اینجا پارامتر λ_k با محاسبه γ_k بدست می‌آید.

۶-۴- پیاده‌سازی مدل اطلاعاتی شبکه قدرت

در این بخش پیاده‌سازی مدل اطلاعاتی شبکه قدرت با استفاده از نرم‌افزار Matlab به‌صورت شکل ٦-٢ پیاده‌سازی می‌شود که این پیاده‌سازی دارای سه بخش می‌باشد. بخش اول شامل شبیه‌سازی یک شبکه قدرت در Simulink-Matlab است که در شکل ٦-٢ با plant مشخص شده است. بخش دوم نیز شامل یک شبکه ارتباطی TCP/IP است که توسط رابط Matlab-Java و استفاده از توابع شبکه‌ای جاوا پیاده‌سازی شده است و در شکل ٦-٢ با TCP/IP Network مشخص می‌شود. در این آزمایشها برای بدست آوردن میزان دقیق زمان تأخیر، شبکه به‌صورت رفت و برگشت در نظر گرفته شده است و در اینجا فرض می‌شود که زمان تأخیر رفت با زمان تأخیر برگشت برابر است. بنابراین زمان تأخیر واقعی از نصف کردن زمان تأخیر بدست آمده محاسبه می‌شود. بخش سوم نیز شامل مدل تخمین تأخیر بر روی شبکه TCP/IP است که با توجه به معادلات آورده شده در بخش ٦-٢-٢، در Simulink-Matlab شبیه‌سازی شده است.



شکل ۶-۲ مدل پیاده‌سازی‌شده با استفاده از Simulink-Matlab

٦-٤-١- مدل پایدارساز سیستم قدرت (PSS)

جهت پیاده‌سازی مدلی از شبکه قدرت و ارسال داده‌های اندازه‌گیری آن بر روی شبکه ارتباطی، با استفاده از یک مدل آزمایشی پایدارساز سیستم قدرت کندر به صورت ۲ ناحیه و ٤ ماشین که در Simulink-Matlab آورده شده‌است، این پیاده‌سازی انجام می‌شود. این سیستم آزمایشی به‌صورت دو ناحیه کاملاً متقارن در فاصله ۲۲۰ کیلومتری و بر روی خط ۲۳۰ کیلو ولت قرار دارند. در اینجا این مدل به‌طور خاص جهت مطالعه نوسانات الکترومکانیکی فرکانس پایین در شبکه قدرت طراحی شده‌است که در هر کدام از این نواحی از ژنراتورهای ۹۰۰ MVA،۲۰ kv با پارامترهای یکسان استفاده شده‌است و در نهایت هدف آن تشریح راه‌حل فازوری با استفاده از سه PSS مختلف می‌باشد[۴۹][۵۰]. در اینجا هدف دریافت برخی از پارامترهای اندازه‌گیری‌شده از این مدل و سپس ارسال این داده‌ها بر روی شبکه TCP/IP و در آخر رؤیت این مقادیر در مرکز کنترل می‌باشد.

در این پیاده‌سازی می‌توان به‌طور همزمان تعداد زیادی از پارامترهای اندازه‌گیری را بر روی شبکه ارتباطی ارسال نمود. در اینجا به عنوان نمونه شش پارامتر از مدل فوق اندازه‌گیری و ثبت می‌شوند که این پارامترها به ترتیب عبارتند از ولتاژ آنالیز ترتیبی (V_{ps})، توان اکتیو (P)، مشتق زاویه فاز ماشین ($\dot{\theta}$)، فرکانس ماشین (ω)، توان مکانیکی ماشین (P_a)، ولتاژ ترمینال ماشین (V_t). در پایان با استفاده از معادلاتی که در بخش ٦-٢-٢ آورده شد، می‌توان میانگین و انحراف معیار تأخیر را محاسبه نمود که در اینجا میزان تأخیر اندازه‌گیری به‌صورت زیر محاسبه می‌شود:

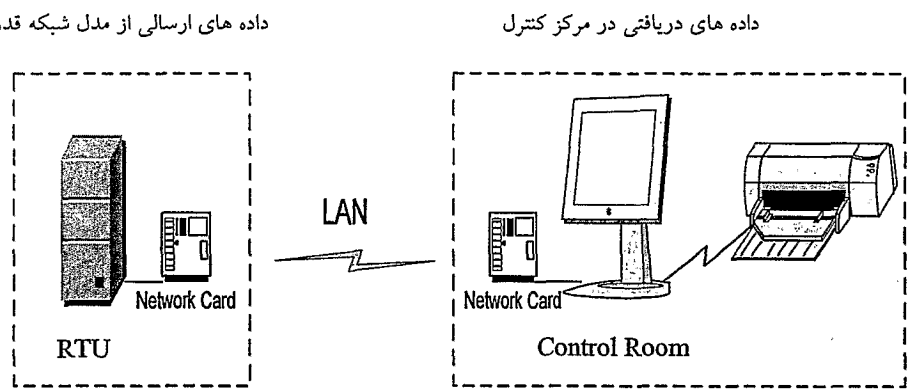
(میزان تأخیر = زمان ارسال پارامتر اندازه‌گیری شده- زمان رؤیت شده پارامتر اندازه‌گیری).

جهت درستی مدل‌های اطلاعاتی بیان شده، این پیاده‌سازیها بر روی یک شبکه واقعی انجام شده است. همانطور که در بخش دوم شکل ۶-۲ نشان داده شده است، داده‌های اندازه‌گیری از مدل شبکه قدرت یک‌بار بر روی شبکه محلی (LAN) دانشگاه ارسال گردیده و در محل دیگری به‌عنوان کامپیوتر مرکز کنترل این داده‌ها دریافت گردیدند. سپس به همان روش قبلی داده‌های اندازه‌گیری با استفاده از یک خط Dial ارسال شده و بر روی کامپیوتر مرکز کنترل دریافت می‌گردند. در بخشهای بعدی نتایج این شبیه‌سازی‌ها و میزان میانگین و انحراف معیار تأخیر، همچنین میزان تأخیر

اندازه‌گیری‌شده و مقایسه‌ای میان مدل اطلاعاتی و پیاده‌سازی عملی مدل شبکه قدرت بر روی شبکه ارتباطی واقعی آورده شده است.

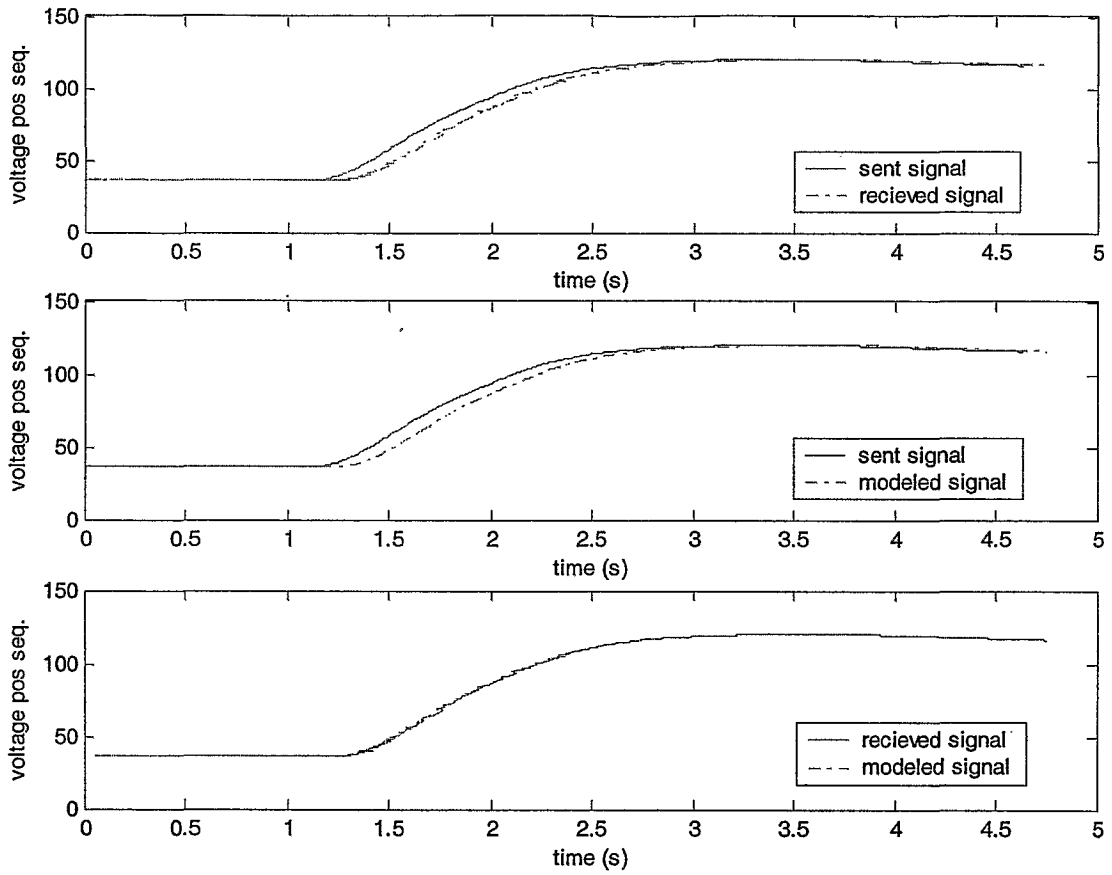
٦-٤-٢- ارسال اطلاعات بر روی شبکه محلی (LAN)

در این بخش همانطور که در شکل ۶-۳ نشان داده شده پیاده‌سازی بر روی LAN دانشگاه انجام گردیده است. بدین صورت که پارامترهای اندازه‌گیری شده مربوط به شبکه قدرت از طرف کامپیوتر RTU بر روی شبکه محلی ارسال شده، سپس این داده‌های اطلاعاتی در مرکز کنترل رؤیت گردیدند.



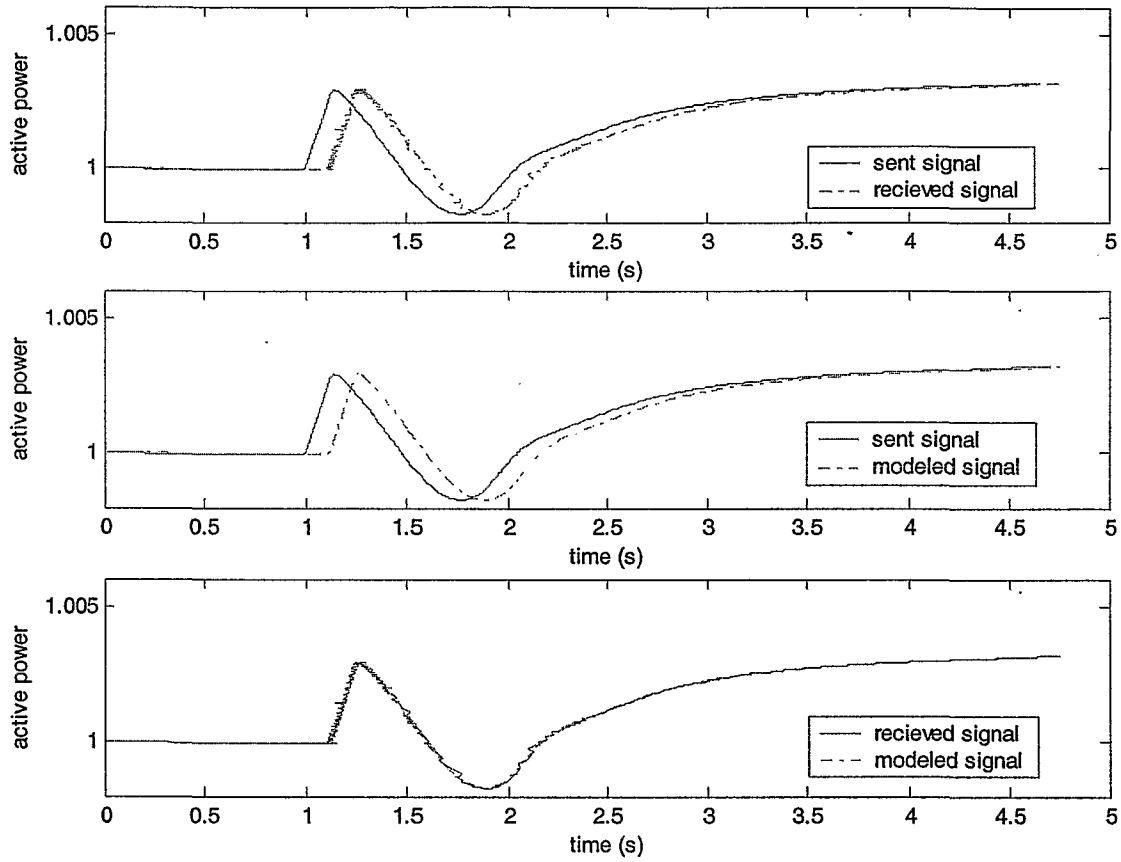
شکل ۶-۳ ارسال داده‌های اندازه‌گیری بر روی شبکه محلی (LAN)

برای هر یک از مقادیر داده‌های اندازه‌گیری شده ارسالی از مدل شبکه قدرت، به‌عنوان نمونه پارامترهای ولتاژ آنالیز ترتیبی (V_{ps})، توان اکتیو (P)، مشتق زاویه فاز ماشین ($\dot{\theta}$)، فرکانس ماشین (ω)، توان مکانیکی ماشین (P_a)، ولتاژ ترمینال ماشین (V_t) در کامپیوتر مرکز کنترل دریافت گردید. نتایج این شبیه‌سازی در شکل‌های ٦-۴ تا ٦-۹ به ترتیب برای هر کدام از این پارامترها آورده شده است.



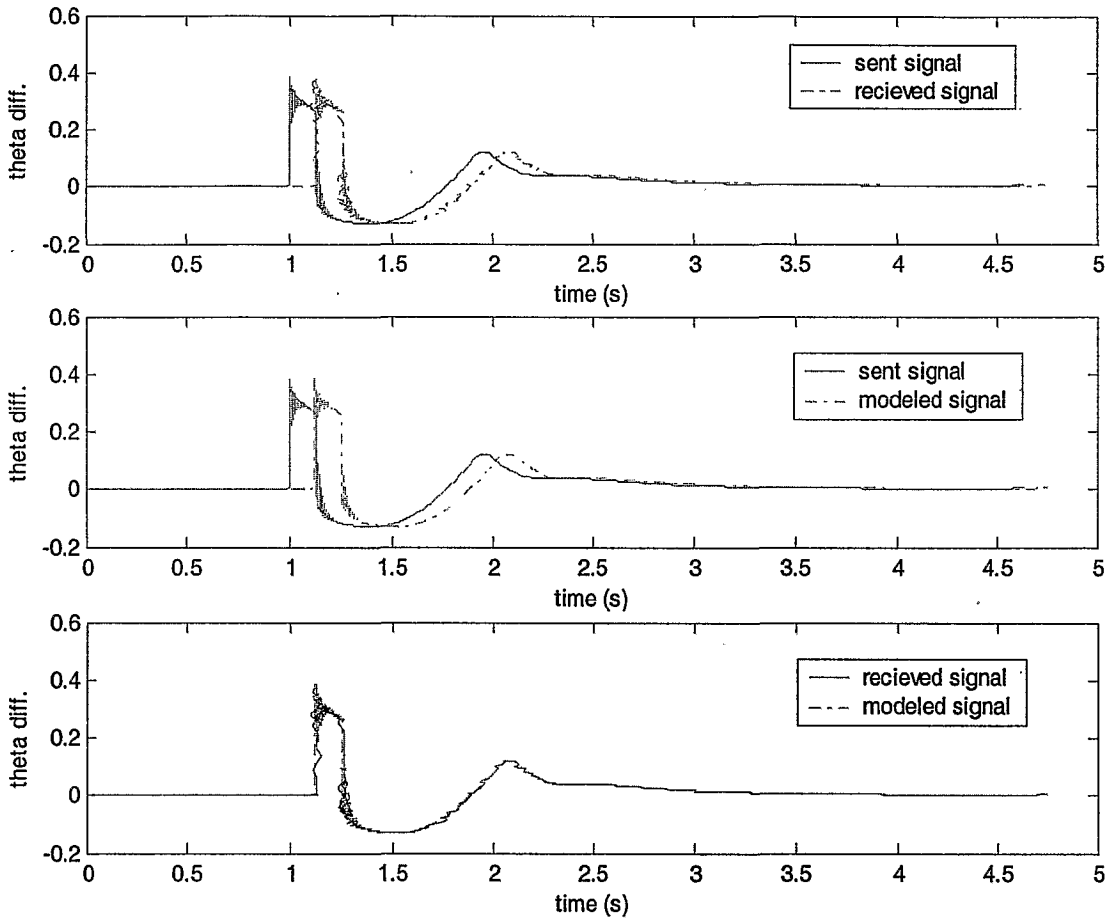
شکل ۶-۴ ولتاژ آنالیز ترتیبی (V_{ps}) بر روی شبکه محلی (LAN)

در قسمت اول شکل ٦-٤ مقدار اندازه‌گیری شده ولتاژ آنالیز ترتیبی(V_{ps}) ارسالی و همچنین مقدار رؤیت شده آن در مرکز کنترل بر روی شبکه ارتباطی مشاهده می‌شود. قسمت دوم نیز مقدار پارامتر اندازه‌گیری ارسالی را به همراه مدل تخمین‌زده شده نشان می‌دهد. در قسمت سوم مقایسه میان مقدار رؤیت شده و مدل تخمینی آن نشان داده شده است که در اینجا درستی مدل تخمین‌زده شده با مدل واقعی را نشان می‌دهد.



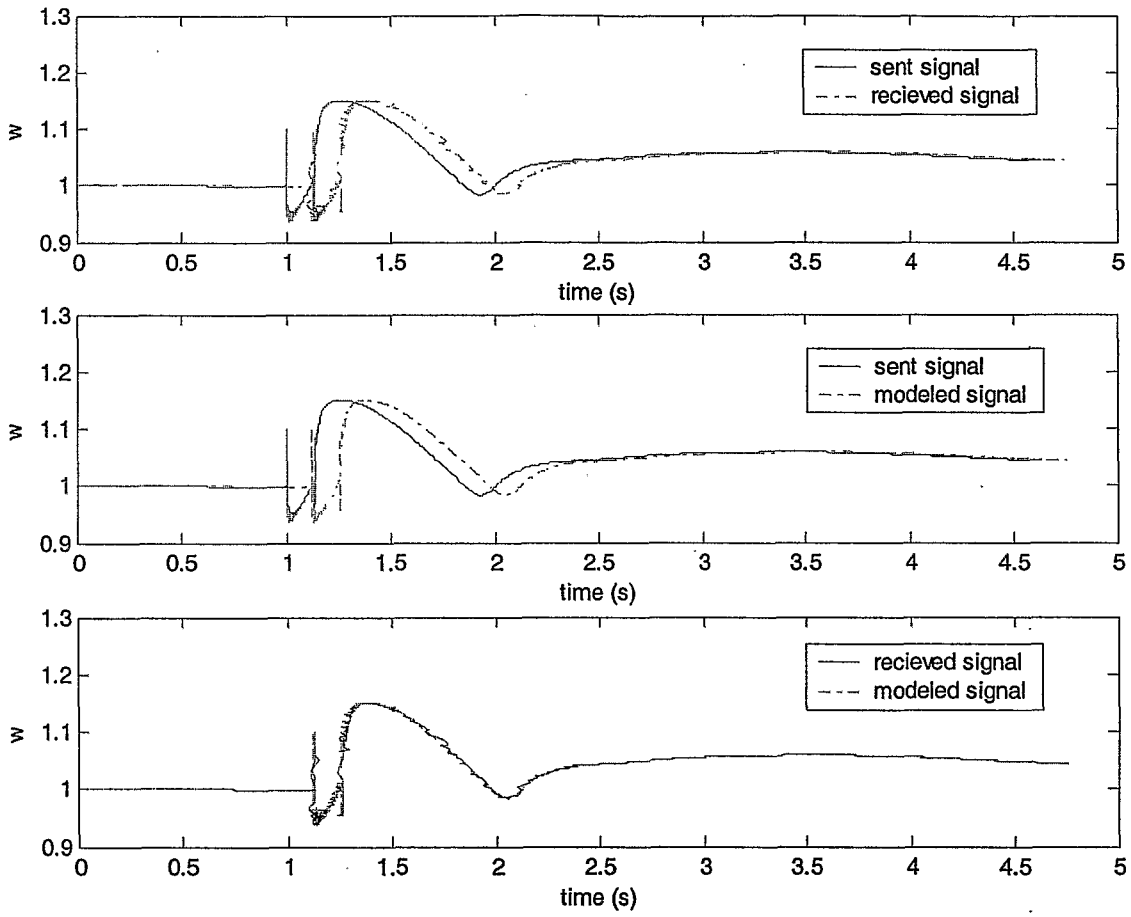
شکل ۶- ۵ توان اکتیو (P) بر روی شبکه محلی (LAN)

در شکل ۶-۵ پارامتر اندازه‌گیری‌شده ارسالی و رؤیت آن در کامپیوتر مرکز کنترل برای توان اکتیو (P) بر روی شبکه محلی مشاهده می‌شود. همانطور که در قسمت سوم شکل ۶-۵ نشان شده است مقایسه‌ای میان مدل تخمینی و مقدار رؤیت شده در مرکز کنترل مشاهده می‌شود که در اینجا صحت مدل اطلاعاتی بیان شده با پیاده‌سازی عملی آن را نشان می‌دهد.



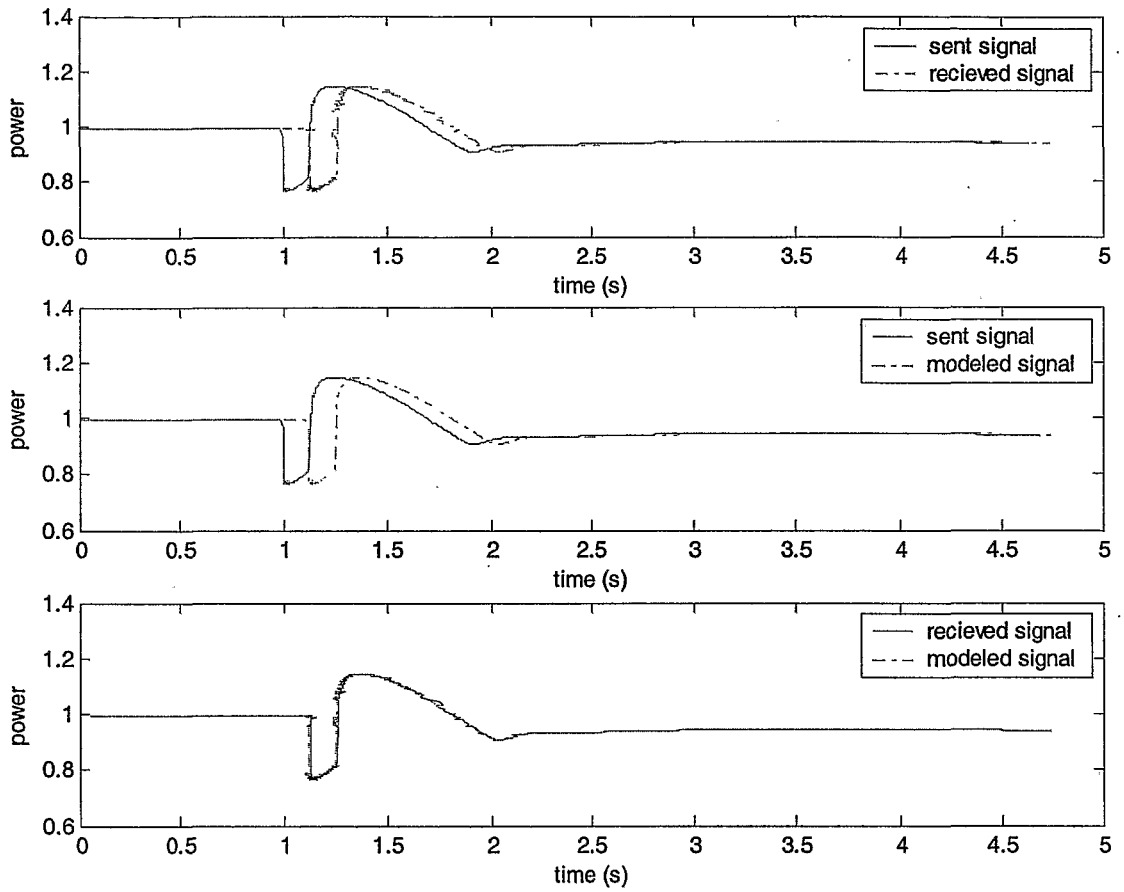
شکل ۶- ۶ مشتق زاویه فاز ماشین ($\dot{\theta}$) بر روی شبکه محلی (LAN)

در قسمت اول شکل ۶-۶ مقدار اندازه‌گیری شده مشتق زاویه فاز ماشین ($\dot{\theta}$) ارسالی و همچنین مقدار رؤیت شده آن در مرکز کنترل بر روی شبکه ارتباطی مشاهده می‌شود. قسمت دوم نیز مقدار پارامتر اندازه‌گیری ارسالی را به همراه مدل تخمین‌زده شده نشان می‌دهد. در قسمت سوم مقایسه میان مقدار رؤیت شده و مدل تخمینی آن نشان داده شده است که در اینجا درستی مدل تخمین زده شده با مدل واقعی را نشان می‌دهد.



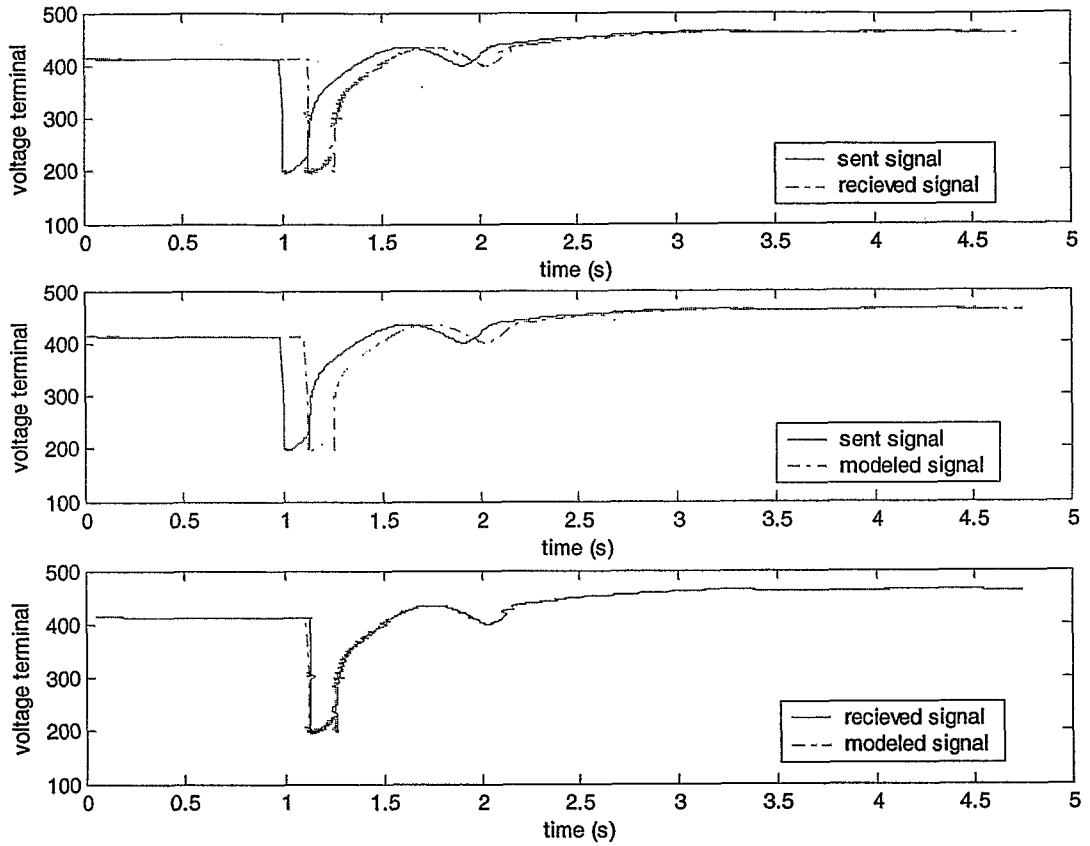
شکل ۶- ۷ فرکانس ماشین (ω) بر روی شبکه محلی (LAN)

در شکل ۶-۷ پارامتر اندازه‌گیری شده ارسالی و رؤیت آن در کامپیوتر مرکز کنترل برای فرکانس ماشین (ω) بر روی شبکه محلی مشاهده می‌شود. همانطور که در قسمت سوم شکل ۶-۷ آورده شده، مقایسه‌ای میان مدل تخمینی و مقدار رؤیت شده در مرکز کنترل نشان داده شده است. همچنین صحت مدل اطلاعاتی بیان شده با پیاده‌سازی مدل واقعی به‌صورت عملی در این قسمت آمده است.



شکل ۶- ۸ توان مکانیکی ماشین (P_a) بر روی شبکه محلی (LAN)

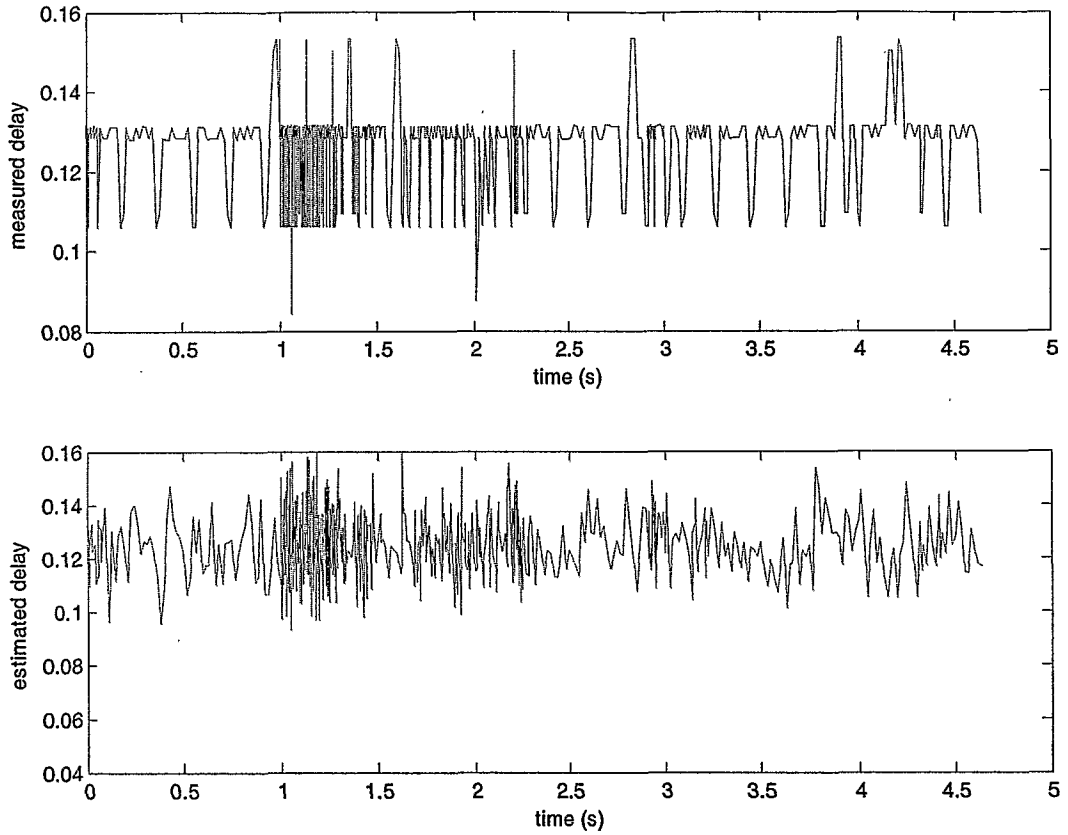
در قسمت اول شکل ۶-۸ مقدار اندازه‌گیری شده ارسالی پارامتر توان مکانیکی ماشین (P_a) و همچنین مقدار رؤیت شده آن در مرکز کنترل بر روی شبکه محلی مشاهده می‌شود. قسمت دوم نیز مقدار پارامتر اندازه‌گیری ارسالی را به همراه مدل تخمین‌زده شده نشان می‌دهد. در قسمت سوم مقایسه میان مقدار رؤیت شده و مدل تخمینی آن نشان داده شده است که در اینجا درستی مدل تخمین زده شده با مدل واقعی را نشان می‌دهد.



شکل ۶- ۹ ولتاژ ترمینال ماشین (V_t) بر روی شبکه محلی (LAN)

در شکل ۶-۹ پارامتر اندازه‌گیری شده ارسالی و رؤیت آن در کامپیوتر مرکز کنترل برای ولتاژ ترمینال ماشین (V_t) بر روی شبکه محلی مشاهده می‌شود. همانطور که در قسمت سوم شکل ۶-۹ آورده شده، مقایسه‌ای میان مدل تخمینی و مقدار رؤیت شده در مرکز کنترل نشان داده شده است. همچنین صحت مدل اطلاعاتی بیان شده با پیاده‌سازی مدل واقعی به‌صورت عملی در این قسمت آمده است.

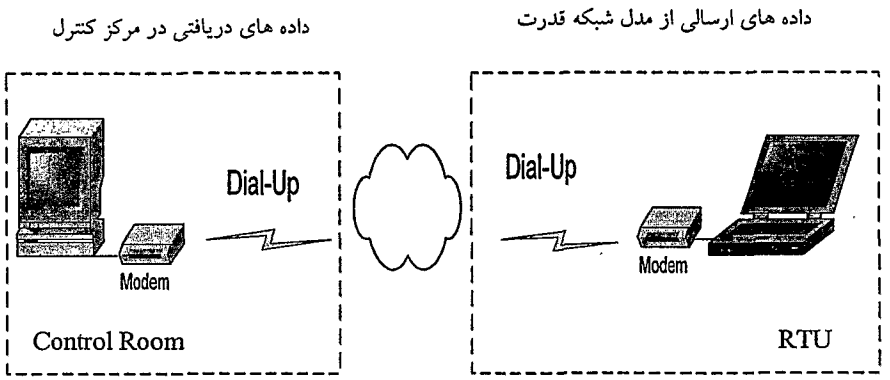
در شکل ٦-١٠ نیز تأخیر واقعی مدل اطلاعاتی شبکه قدرت به همراه تأخیر تخمین‌زده شده مشاهده می‌شود. در اینجا هر یک از مقادیر میانگین تأخیر، انحراف معیار و گامای تأخیر به ترتیب برابر با ۰,۱۲۵۵ ثانیه، ۰,۰۱۰۱ و ۰,۰۸۰۱ محاسبه شده‌اند. همانطور که در این شکلها نشان داده شده، روش تخمینی بیان شده در این پایان‌نامه، توانسته است به خوبی اثر تأخیر را بر روی شبکه محلی (LAN) مدل نماید.



شکل ۶- ۱۰ تأخیر در شبکه محلی (LAN)

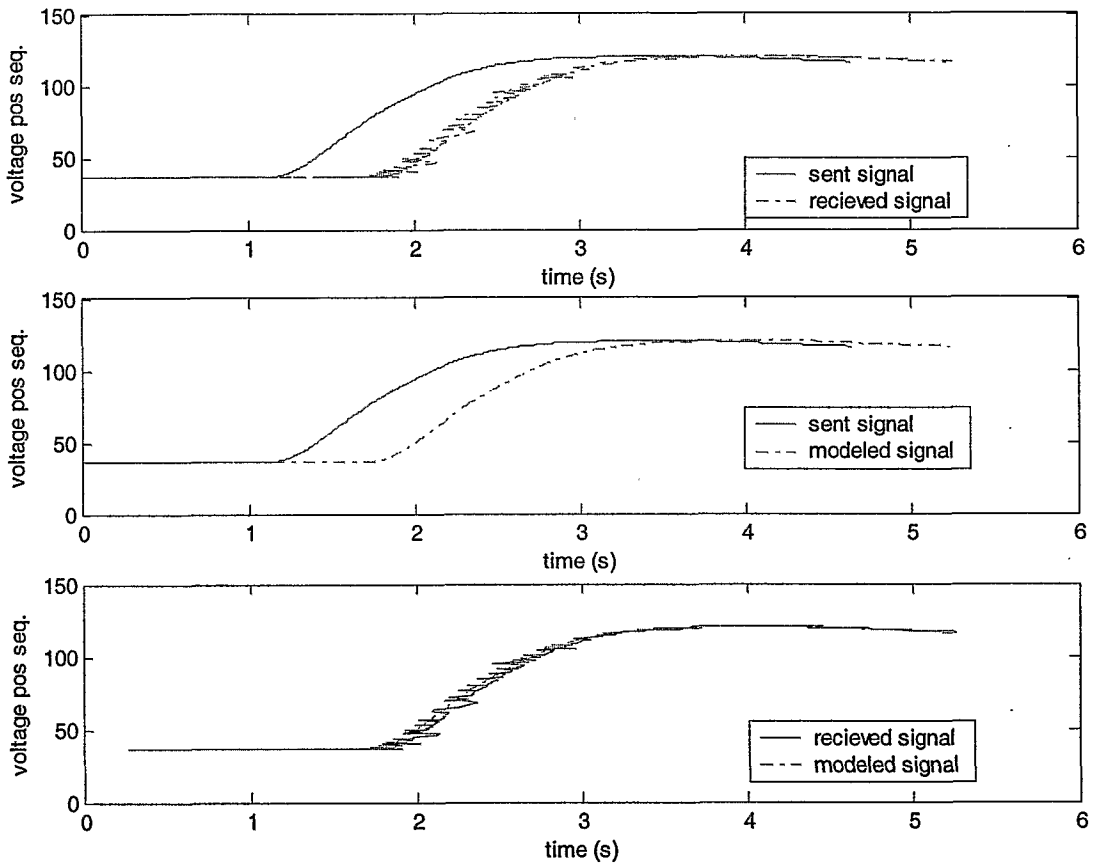
٦-٤-٣- ارسال اطلاعات با استفاده از خط Dial

در این بخش پیاده‌سازی مدل بر روی خط Dial انجام شده است. همانطور که در شکل ۶-۱۱ مشاهده می‌شود پارامترهای اندازه‌گیری شده مربوط به مدل شبکه قدرت از طرف کامپیوتر RTU بر روی خط Dial ارسال شده‌اند که در نهایت این داده‌های اطلاعاتی در مرکز کنترل رؤیت گردیدند.



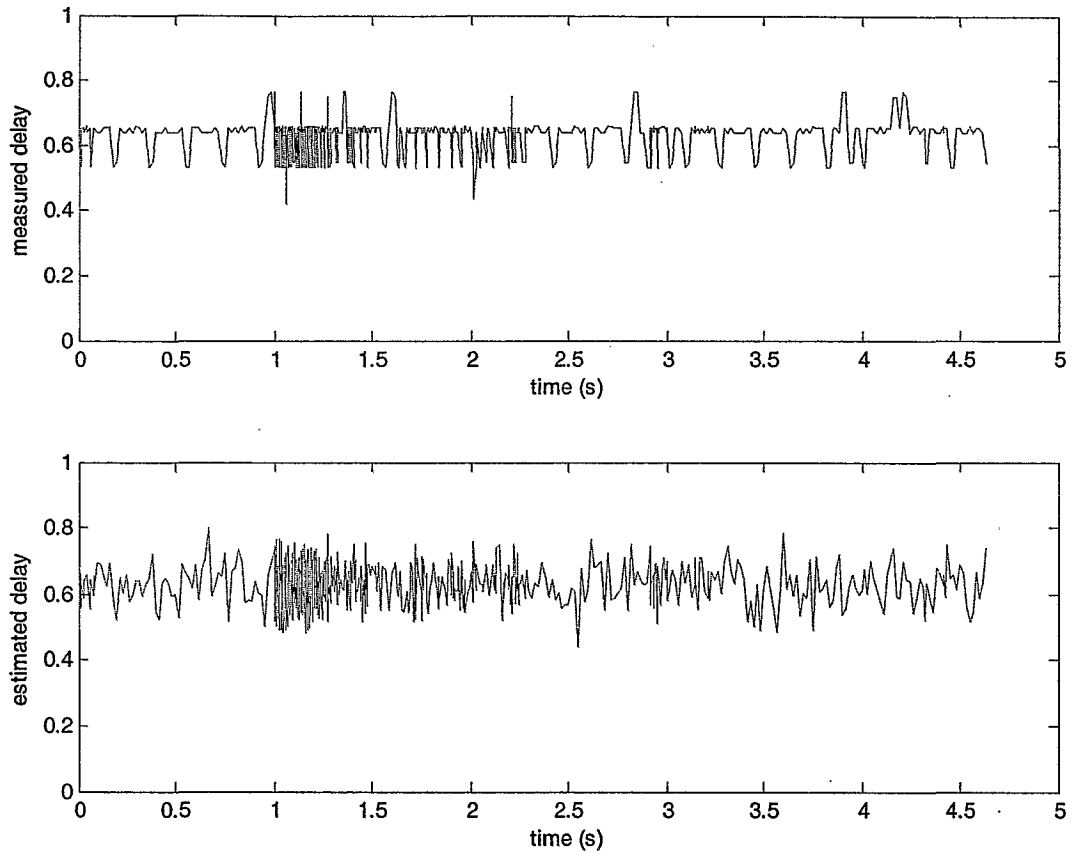
شکل ۶- ۱۱ تأخیر بر روی خط Dial

در این مرحله برای سایر مقادیر اندازه‌گیری‌های ارسالی همانند مرحله قبل انجام می‌شود که در اینجا به‌عنوان مثال همانطور که در شکل ٦-١٢ نشان داده شده، نتایج شبیه‌سازی برای ولتاژ آنالیز ترتیبی(V_{ps}) مشاهده می‌شود.



شکل ۶- ۱۲ ولتاژ آنالیز ترتیبی(V_{ps}) در خط Dial

در قسمت اول شکل ٦-١٢، مقدار ولتاژ آنالیز ترتیبی(V_{ps}) ارسالی و همچنین میزان ولتاژ رؤیت شده در مرکز کنترل بر روی شبکه ارتباطی مشاهده می‌شود. قسمت دوم نیز ولتاژ ارسالی را به همراه مدل تخمین‌زده شده نشان می‌دهد. در قسمت سوم مقایسه‌ای میان ولتاژ رؤیت شده و مدل تخمینی آن بدست آمده است. همچنین در شکل ٦-١٣ تأخیر واقعی مدل اطلاعاتی مربوط به شبکه قدرت به همراه تأخیر تخمین زده شده مشاهده می‌شود.



شکل ۶- ۱۳ تأخیر بر روی خط Dial

در اینجا مقادیر میانگین تأخیر، انحراف معیار و گامای تأخیر به ترتیب ۰,۶۲۷۶ ثانیه، ۰,۰۵۰۳ و ۰,۰۸۰۱ محاسبه شده‌اند. همانطور که در شکل‌های ٦-۱۲ و ۶-۱۳ نشان داده شده، روش تخمینی ارائه شده در این پایان‌نامه، توانسته است به خوبی اثر تأخیر را بر روی خط Dial مدل کند.

مدل اطلاعاتی بیان شده جهت شبکه قدرت در این فصل و اثبات درستی این مدل با پیاده‌سازی عملی یک مدل از شبکه قدرت بر روی شبکه محلی و خط Dial-up انجام گردید. همانطور که نتایج شبیه‌سازی در این پایان‌نامه جهت برخی از پارامترهای اندازه‌گیری شده ارسالی از مدل شبکه قدرت نشان می‌دهد این مدل تخمینی با مقایسه یک مدل واقعی از شبکه قدرت توانسته است اثر تأخیر را در سیستم اطلاعاتی مربوط به شبکه قدرت بخوبی نشان دهد و در اینجا نتیجه گرفت که پیاده‌سازی سیستم‌های SCADA مبتنی بر پروتکل ارتباطی همچون TCP/IP، تأخیر قابل قبولی نسبت به سیستمهای مرسوم SCADA [۲۶] با قابلیت اطمینان بیشتری را فراهم می‌نماید.

فصل ۷

نتیجه‌گیری و پیشنهادات

۷-۱- نتیجه‌گیری

سیستم‌های کنترل نظارتی و اکتساب داده‌ای (SCADA) در کنترل و مانیتورینگ سیستم‌های گسترده کاربردهای فراوان داشته، که این سیستمها دارای تأخیرهای ناشی از محدودیت سرعت انتقال داده، زمان پردازش و غیره می‌باشد. این تأخیرها می‌تواند باعث بروز خطاهایی در اندازه‌گیریهای ارسال شده از RTU به مرکز کنترل شود که میزان خطاهای اندازه‌گیری می‌تواند به تأخیر و شدت تغییرات داده‌های اندازه‌گیری شده بستگی داشته باشد.

در این پایان‌نامه با بیان یک مدل اطلاعاتی در شبکه قدرت، شبیه‌سازی تخمین تأخیر در شبکه‌های ارتباطی مبتنی بر TCP/IP بررسی گردید. جهت مشاهده اثر تأخیر در اندازه‌گیریهای ارسالی در یک سیستم SCADA، مدل شبکه قدرت را که شامل ترکیبی از هر دو ساختار فیزیکی سیستم قدرت و شبکه ارتباطی می‌باشد بر روی شبکه محلی (LAN) و خط Dial به صورت عملی پیاده‌سازی شد. مدل تأخیر در شبکه ارتباطی به صورت نویز گاوسی بیان شده است که تأخیر بدست آمده در این مدل با میزان تأخیر در پیاده‌سازی عملی مقایسه گردید. همانطور که میزان تأخیر در سیستم مرسوم SCADA در حدود ۱ ثانیه [۲۶] قابل قبول می‌باشد، با توجه به نتایج بدست آمده از شبیه‌سازی، مدل بیان شده توانسته است تأخیر قابل قبولی را بر روی شبکه ارتباطی مبتنی بر TCP/IP نشان دهد.

۷-۲- پیشنهادات

مجموعه کارهایی که در ادامهٔ این پایان‌نامه می‌تواند صورت گیرد در زیر آمده‌اند:

۱- در این پایان‌نامه، پیاده‌سازی بر روی شبکه محلی دانشگاه و خط Dial انجام شده است. در این دو پیاده‌سازی، مسافتهای منظور شده جهت فاصله میان RTU و مرکز کنترل کوتاه فرض شده‌اند. بهتر است که این پیاده‌سازی در یک مسافت زیاد که تجهیزات بیشتری از سیستم‌های ارتباطی (سوئیچها، مسیریابها...) در طی مسیر وجود دارند انجام شود تا بتوان نتایج را هر چه بیشتر در یک سیستم SCADA به‌صورت واقعی‌تر مشاهده نمود.