APJ. 4(2):60-69, Summer 2023

Arman Process Journal (APJ)

Homepage: armanprocessjournal.ir

Towards Integrated Management Approach of Distribution Networks

S. Soleimani [*,1]

[1] Electrical and Computer Engineering Department, Kurdistan University, Iran

Received: 28 June 2023
Accepted: 26 August 2023

KEYWORDS:
Network Management,
Security,
Error Handling,
Efficiency,
Resource Audit,

[1] Corresponding author
soleimani.wk@yahoo.com

ABSTRACT

Today, distributed network management frameworks are used to provide, operate, maintain and secure network infrastructures. Basically, the correct management of distribution networks requires a wide range of activities, methods, routines and the use of executive, operational and maintenance tools of computer systems. When the issue of security attacks lurking in the network is raised, the importance of comprehensive management and monitoring of the data exchanged in the network will be twofold. In order for the managers of such networks to be able to regularly monitor the system logs and its operational framework and to identify hardware, software and security attacks, an integrated management framework is needed to undertake the comprehensive and systematic management. An approach that analyzes security events, collects and categorizes system logs and enables de-centralized network management. The comprehensive and integrated management approach of distribution networks uses a set of communication hardware and user interface software and accessories as an integrated system to control network tools and equipments. The perspective of integrated management of distribution networks makes network resources available to users in an efficient and fast method. Therefore, network optimization is guaranteed using error analysis and performance management. By using comprehensive management frameworks, the best suitable tools for managing, monitoring and controlling the network can be used to respond to the challenges in the network if needed. In this article, we intend to research and examine the approach of achieving integrated management approach for distribution networks and its dimensions.

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
16	0	0

نشریه تخصصی آرمان پردازش، دوره ۴، شماره ۲، تابستان ۱۴۰۲

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir

به سوی دیدگاه مدیریت جامع شبکه های توزیعی

سعید سلیمانی*[1]

[1] کارشناسی ارشد مدیریت صنعتی، دانشکده مدیریت و حسابداری، دانشگاه شهید بهشتی، تهران، ایران.

چکیده

امروزه از چارچوب های مدیریت شبکه های توزیعی برای تهیه، بهره برداری، نگهداری و ایمن سازی زیرساخت های شبکه استفاده میشود. اساسا مدیریت صحیح شبکه های توزیعی نیازمند طیف وسیعی از فعالیت ها، روش ها، روال ها و استفاده از ابزارهای اجرایی، عملیاتی و نگهداری از سیستم های کامپیوتری می باشد. زمانی که موضوع حملات امنیتی در کمین شبکه مطرح می‌شود، اهمیت مدیریت جامع و نظارت روی داده هایی که در شبکه رد و بدل می‌شوند دوچندان خواهد بود. برای اینکه مدیران چنین شبکه هائی بتوانند به‌طور منظم روی لاگ‌های سیستم و چارچوب عملیاتی آن نظارت داشته باشد و مشکلات سخت‌افزاری، نرم‌افزاری و حملات امنیتی را شناسایی کند، نیاز به چارچوبی مدون است که مدیریت جامع و نظام مند شبکه را بر عهده بگیرد. چارچوبی که وقایع امنیتی را تجزیه‌وتحلیل کند، لاگ‌های سیستم را جمع‌آوری و دسته‌بندی کرده و در کل مدیریت و نظارت روی شبکه را به‌صورت متمرکز امکان‌پذیر کند. رویکرد مدیریت جامع شبکه های توزیعی مجموعه ای از سخت‌افزارهای ارتباطی و نرم‌افزارهای رابط کاربری و ملحقات را به صورت سامانه‌ای یکپارچه برای کنترل ابزارها و تجهیزات شبکه و نظارت بر عملکردها به خدمت میگیرد. دیدگاه مدیریت جامع شبکه های توزیعی منابع شبکه را به شکلی کارآمد، موثر و سریع در دسترس کاربران قرار میدهد. همچنین بهینه سازی شبکه با استفاده از تجزیه و تحلیل خطا و مدیریت عملکرد تضمین میشود. با استفاده از چارچوب های مدیریت جامع میتوان بهترین ابزارهای مناسب برای مدیریت، نظارت و کنترل شبکه را به کار گرفت تا در صورت نیاز، به چالش های پیش آمده در شبکه پاسخ دهند. در این مقاله قصد داریم درخصوص رویکرد دستیابی به مدیریت جامع شبکه های توزیعی و ابعاد آن تحقیق و بررسی نمائیم.

واژگان کلیدی:
مدیریت شبکه،
امنیت،
مدیریت خطا،
کارائی،
حسابرسی منابع،

تعداد جداول	تعداد شکل ها	تعداد مراجع
۰	۰	۱۶

مقدمه

امروزه بهره‌گیری از فن‌آوری سیستم‌های اطلاعاتی برای افزایش کارایی و بهره‌وری مناسب در اغلب زمینه‌ها به سرعت در حال گسترش است. شبکه‌های گستردهٔ کامپیوتری با انواع روش‌ها و ابزارهای دستیابی به اطلاعات، قدرت و توانایی کامپیوترهای موجود در شبکه را فارغ از مکان فیزیکی آن‌ها در دسترس استفاده‌کنندگان قرار داده است. از طرفی اتکای رو به تزاید به فن‌آوری اطلاعات، افزایش احتمال خطر ناشی از کاربرد آن را نیز در پی دارد. همزمان با پیشرفت و توسعهٔ قابل توجه فن‌آوری کامپیوتر در زمینه‌های مختلف نرم‌افزار و سخت‌افزار، زمینه کوشش جدی برای ایجاد امنیت لازم برای حفظ داده‌ها و سیستم‌ها فراهم شده است. درحال حاضر ضرورت حفظ امنیت داده‌ها و سیستم‌ها به این دلیل قابل توجه است که ره‌آوردهای فن‌آوری معاصر عموماً در تصمیم‌گیریهای مهم اتخاذ شده به وسیلهٔ حکومتها و همچنین سازمان‌های معتبر جهانی نقش اساسی را ایفا می‌کند. به علاوه فن‌آوری پیشرفته صنعتی نیز مبتنی بر سیستم‌های اطلاعاتی ایمن و قابل اطمینان، کارایی بهینه دارد. امروزه حجم قابل توجهی از مبادلات بازرگانی و مالی بین‌المللی با استفاده از فن‌آوری تبادل الکترونیکی داده‌ها انجام می‌شود. ایجاد کوچکترین خللی در این سیستم مبادلاتی، ضررهای هنگفتی را به طرفین مبادله تحمیل خواهد کرد که بعضاً ممکن است به ورشکستگی آنها بیانجامد [۱].

اساسا برای بررسی مسایل مرتبط با امنیت داده‌ها و سیستم ها ابتدا باید به طبقه‌بندی آنها پرداخت. این طبقه‌بندی را حول محورهای مسایل تکنیکی و غیر تکنیکی، سخت‌افزار، نرم‌افزار، محیط‌های تبادل اطلاعات، امنیت داده‌ها، نقش عوامل انسانی و نظایر آن می‌توان انجام داد. طبقه‌بندی و پرداختن به اجزای امنیت داده‌ها و سیستم‌ها شناخت ما را از مقولهٔ امنیت سیستم‌ها بیشتر می‌کند [۲]. در این حوزه، روش‌های حفاظتی عمدتا به دو بخش حفاظت فیزیکی و غیرفیزیکی تقسیم می‌شود. حفاظت‌های فیزیکی بیشتر به منظور جلوگیری از ورود و دسترسی غیر مجاز به محل استقرار و تاسیسات مرتبط با سیستم‌های کامپیوتری است. حفاظت‌های غیر فیزیکی شامل انواع روش‌ها و تمهیدات پیش‌بینی شده در نرم‌افزارها به منظور تامین اهداف مختلف امنیتی سیستم‌ها است [۳].

در چند دههٔ نخست پیدایش شبکه‌ها، محققین دانشگاه از شبکه ها برای ارسال پست الکترونیکی استفاده می‌کردند و کارمندان نیز برای اشتراک چاپگرها از آن استفاده می‌نمودند. تحت این شرایط امنیت مورد توجه نبود. اما اکنون، میلیونها شهروند از شبکه‌ها برای امور بانکی و مالیاتی استفاده می‌کنند و در نتیجه، امنیت شبکه از اهمیت خاصی برخوردار است. معیارهای ارزیابی امنیت سیستم‌ها، موضوعی است که از اوایل دههٔ ۱۹۸۰ میلادی به وسیلهٔ وزارت دفاع آمریکا، مطرح شد. هدف از معیارهای ارزیابی، ارایهٔ الگویی برای طبقه‌بندی سیستم‌های کامپیوتری بر اساس قابلیت‌های اشاره شده از سوی پنتاگون در چهار بخش و هفت رده به طبقه‌بندی سیستم‌های کامپیوتری می‌پردازند. معیارهای ارزیابی ابتدا برای سیستم‌های نظامی مطرح شد. امروزه در صحنهٔ بین‌المللی شاهد تلاش کشورها و مجامع مختلف برای ارایهٔ معیارهای مشترکی به منظور ارزیابی کلیه سیستم‌های کامپیوتری هستیم. در مورد امنیت تا آنجایی که مربوط به تعریف خود امنیت – اهمیت –خطرات تهدید کننده و روشهای مقابله با به خطر افتادن امنیت داده ها و سیستمها و همینطور محافظت شبکه و توزیعات جزئی در رابطه با پروتکلهای انتقال امن فایلها می باشد در نظر گرفته شود. بیشتر سیستم‌های کنترل حمل و نقل، نیروگاهها و کارخانجات بزرگ امروزی از پایگاه‌های اطلاعاتی خود به صورت لحظه‌ای و پیوسته استفاده می‌کنند. بدیهی است که یک لحظه توقف سیستم و یا بروز کوچکترین خطا در داده‌ها می‌تواند خسارات غیر قابل جبرانی در هر یک از این سیستم‌ها بوجود آورد. همچنین بروز اشکال در نرم‌افزار و یا سخت‌افزارهای به کار گرفته شده در تجهیزات مدرن پزشکی، به علت در نظر نگرفتن ضروریات امنیت داده‌ها و سیستم‌ها، ممکن است صدمات غیرقابل جبرانی به وجود آورد. به رغم توسعهٔ صنعت کامپیوتر، تلاش اندکی برای آگاه کردن کاربران از آسیب‌پذیری داده‌ها و سیستم‌ها (ناشی از تغییرات و تخریب‌های غیر مجاز عمدی و یا سهوی) صورت گرفته است. همچنان که حوادث و عوامل مخرب علیه سیستم‌های اطلاعاتی با وضوح بیشتری آشکار می شوند، کاربران این سیستم‌ها نیز تمایل بیشتری آشکار می‌شوند، کاربران این سیستم‌ها نیز تمایل بیشتری نسبت به حل مشکلات وابسته به تامین امنیت سیستم‌ها از خود نشان می‌دهند.

به طور معمول (در اغلب سیستم‌ها) مسأله امنیت تا قبل از مرحلهٔ تعریف نیازمندی‌های عملیاتی به طور جدی مد نظر قرار نمی‌گیرد و سیستم به طور مستقیم وارد مرحله پیاده‌سازی می‌شود. بدین ترتیب دستیابی به یک سطح مناسب امنیتی برای سیستم در حال اجرا به ندرت امکان پذیر است. حتی در صورت امکان عملی شدن چنین امنیتی، هزینه‌های ناشی از این امر در مقایسه با سیستم‌هایی که از ابتدای طراحی، ملاحظات امنیتی را در نظر گرفته‌اند، بسیار بالاتر خواهد بود. بنابر این ضروریات امنیتی هر سیستمی می‌بایست در مرحله تعریف و تبیین نیازمندی‌های کاربران آن سیستم در نظر گرفته شود و در طراحی سیستم لحاظ شود [۴].

به سوی دیدگاه مدیریت جامع شبکه های توزیعی

مدیریت برای سرویس‌های اطلاعات شبکه بندی شده، هم مدیریت منابع سیستم و هم مدیریت شبکه را طلب می‌کند. یعنی مدیریت در این زمینه مهم است. مدیریت جامع و همه جانبه شبکه های توزیعی شامل پنج زمینه اصلی به شرح زیر است [۸-۵]:

مدیریت پیکربندی

مدیریت پیکربندی شبکه، فرآیندی است که هر دستگاه در شبکه در طول چرخه عمر خود تحت آن قرار می‌گیرد. این مهم شامل کشف

دستگاه، نگهداری موجودی، پشتیبان گیری از پیکربندی، نظارت بر تغییرات پیکربندی و انطباق، ردیابی فعالیت کاربر و عیب یابی، با اجرای عملیات شبکه مناسب است. یکی از ارزشمندترین مزایای مدیریت پیکربندی شبکه، توانایی آن در کاهش زمان خرابی است. تغییرات ایجاد شده در شبکه، بلافاصله توسط مدیران سیستم شناسایی می‌شوند. مدیریت پیکربندی شبکه همچنین با امکان شناسایی آسان اجزا و نرم افزارهای فعال در شبکه، دید و مسئولیت پذیری را بهبود می‌بخشد. علاوه بر این، سازمان ها می توانند سیاست‌های ممیزی را با پیکربندی شبکه ایجاد و سفارشی کنید که این مهم از انطباق با استانداردهای صنعت پشتیبانی می‌کند.

مدیریت پیکربندی در مدیریت شبکه به طور طبیعی قبل از گزینش توپولوژی شبکه، کشیدن نقشهٔ شبکه وانتساب پارامترهای پیکربندی در نماینده های مدیریت و سیستم های مدیریت استفاده و مورد توجه قرار می‌گیرد. مدیریت پیکربندی صرفاً به نقطه نظرات عملیاتی نگاه نمی‌کند بلکه به نقطه نظرات مهندسی و طرح‌ریزی نیز توجه دارد. پیش‌بینی شبکه شامل طراحی و طرح‌ریزی شکبه است. لذا پیش بینی شبکه را می‌توان قسمتی از مدیریت پیکربندی فرض نمود.

پیش‌بینی شبکه در شبکه های توزیعی پیش‌بینی مسیر نامیده می شود که یک پردازش و فرآیند اتوماتیک است یک ترانک (مسیراز مرکز سوئیچ کننده اصلی به مرکز سوئیچ کننده مقصد) و مسیر سرویس مشخص (سفارشی کردن برای ملاقات مشخصات مشتری) به وسیله برنامه‌های نوشته شده در سیستم عامل، طراحی می‌شود. طرح‌ریزی و سیستم فهرست یا سیستم طراحی یکی شده و یک سیستم یکپارچه ایجاد می‌کنند، بنابر این مسیر طراحی شده به طور اتوماتیک مشتق خواهد شد و تاریخ نیز برای سیستم طرح ریزی روشن می‌شود و لذا اطمینان خواهد داشت که اجزاء در سیستم فهرست، معتبر و در دسترس است به طور مشابه در صورت قطع شدن یک مسیر با سیستم طرح‌ریزی دسترسی داشتن برای طراحی‌های بعدی آگاه می‌کند. در حالی که پیش‌بینی در شبکه‌های ارتباطی کامپیوتر دارای نیازمندیهای مختلف است به جای استفاده از اتصالهای Cricuit – Swutcing از – Packet Swithching در انتقال اطلاعات از مبدا تا مقصد استفاده می‌شود. در Packet – Swithching به صورت اتصال‌گرا و در مسیرهای شاید مختلف و مستقل از بسته های دیگر، عمل ارسال بسته‌ها صورت می‌گیرد و هر بسته به وسیله مسیریاب در گرههای مختلف و براساس بار روی اتصالهای سوئیچ می‌شود.

پیش‌بینی روی اتصالها بر اساس حداکثرو میانگین درخواست و تقاضا می‌باشد. در ارتباطات Store & Forward بسته‌های اضافی می‌تواند در بافر مسیریاب ذخیره شده و در صورت از دست دادن یا گم شدن دوباره ارسال شوند. در اتصالات مسیرهای اتصال‌گرا، مسیر درخواست به صورت مجازی سوئیچشده و به طور دائم و همیشگی تا انتهای اتصال موردنظر باقی می‌ماند ومناسب درخواستهای انتها به انتها اتصالهای مختلف در نظرگرفته می شود در حال که در پیش بینی شبکه سوئیچ کردن بسته‌ها در شبکه بر اساس آمارهای کارائی و کیفیت برای نیازمندیهای سرویس می باشد. پیش‌بینی شبکه در اتصالات WAN پهن باند با استفاده از تکنولوژی ATM بسیار پیچیده است و مفهوم مسیر مجازی همیشه مورد استفاده است و اساسا گزارش و حساب پیش‌بینی‌های پردازش‌ها را دارد و سوئیچ‌ها بر اساس سلول در مقابل سوئیچ کردن بسته‌ها بر اساس قالب و یا Frame قرار دارند. عموما هر سوئیچ ATM برای هر اتصال جلسه اطلاعات، راه مجازی – مسیر مجازی VP_VC را فقط برای گرههای همسایه خود دارد نه برای مسیر پیش فرض انتها به انتها [۹].

مدیریت پیکربندی شبکه روی علوم توپولوژی شبکه بنا نهاده شده است. یک شبکه هنگام تغییر پیکربندی، رشد و یا عوض شدن، نیازمند ارتقاء توپولوژی شبکه به صورت اتوماتیک است و هر ارتقاء به وسیله ترمیمهای کاربردها در سیستم مدیریت شبکه صورت می‌گیرد. به هر حال حوزه برای ترمیم پردازش‌ها نیازمند اجبار و تحمیل است. ترمیم به طور اتوماتیک به صورت پخش[1]کردن Ping روی هر قطعه و به وسیله دستورات و سئوالات پیشرفته SNMP انجام می‌گیرد و بیشترجزئیات روی سیستم جمع می‌شود. لازم به ذکر است، ناتوانی و درماندگی در نگاشت پیکربندی منطقی به پیکربندی فیزیکی، کارائی مدیریت شبکه را پیچیده‌تر می‌کند چرا که اولاً باید دو نقشه جدا از هم به طور مداوم نگهداری شده و به همدیگر عوض شوند، ثانیاً هنگام اضافه شدن یک جزء وترمیم خودکار توسط سیستم، یک رویه دستی نیاز است تا روی پیکربندی فیزیکی نیز پی‌گیری شود. مدیریت پیکربندی شبکه یک ابزار جامع مدیریت پیکربندی شبکه است که به شما کمک می‌کند تا کل چرخه عمر دستگاه‌ها و پیکربندی‌های شبکه خود را مدیریت کنید. این امر مهم راه حل‌هایی برای پیکربندی شبکه های توزیعی، تغییر و مدیریت انطباق در اختیار شما قرار می‌دهد. این ابزار همچنین به شما در عملیات حیاتی شبکه مانند خودکار کردن عملیات پیچیده شبکه، زمان بندی پشتیبان گیری، ردیابی فعالیت کاربر، تولید گزارش‌های دقیق و موارد دیگر کمک می‌کند [۱۰].

مدیریت خطا

خطا در شبکه‌های کامپیوتری به شرایطی گفته می‌شود که اطلاعات دریافتی با اطلاعات ارسالی مطابقت نداشته باشد. نویزها، مزاحمت زیادی برای سیگنال‌های دیجیتالی در طول زمان انتقال ایجاد می‌کنند یا به عبارتی خطاهایی را برای بیت‌های باینری در حال انتقال به وجود می‌آورند. در این صورت ممکن است یک بیت ۰ به بیت ۱ تغییر کند و یا بالعکس. خطا در یک شبکه به طور طبیعی وابسته به خطا در اجزاء شبکه و به پیامد آن از دست دادن اتصال است. مدیریت خطا، خواستار کشف یک خطا است که در شبکه پدید آمده است و تشخیص مکان خطا و جداسازی از مشکلات به پی‌آمد آن باید انجام گیرد. زمانی که یک خطا در یک شبکه توزیعی روی می‌دهد یا علت آن از عیب اجزاء

[1]Broad Cast

است یا از کارائی است و ممکن است، در بیشتر مکانها خود را نشان دهد لذا در یک سیستم مدیریت متمرکز شده، خطاها می‌توانند از مکانهای مختلف باشند. رخدادهای خطا با پیدا کردن علّت مشکل همانند یک جنگ تن به تن می‌ماند. امنیت شبکه به جلوگیری کردن از دسترسی‌های غیر مجاز به اطلاعات توسط پرسنل و اشخاص غیر مجاز مربوط می‌شود، امنیت شبکه علاوه بر اینکه خواستار بحث تکنیکی است نیازمند سیاستها و رویه‌های خوب تعریف شده می‌باشد. همچنین می‌توانیم رمزگذاری در ارتباط میان منبع و دریافت کننده بهره بگیریم بدون اینکه مانیتور و دستکاری غیر قانونی داشته باشیم. برای داشتن مدیریت جامع به محاسبه‌گری در مدیریت و گزارشات نیازمندیم که این عمل سلامت اقتصادی را در بر دارد، گزارش برای مدیریت به منظورهای مختلفی و به عنوان عملهای روزانه شبکه، انجام می‌گیرد. برای مثال عموما در این حوزه گزارشاتی برای اندازه‌گیری کیفیت سرویس‌ها مورد نیاز است که در توافقات پیش فرض سطح سرویس صورت گرفته وتهیه می‌گردد. اساسا مدیریت خطا، ۵ گام پردازش و فرآیند را به شرح زیر درخواست می‌کند [۱۳-۱۱]:

- کشف خطا (Fault Detection)
- مکان خطا (FaultLocation)
- اعاده و برگرداندن سرویس (Service Restoration)
- شناسائی علت اصلی مشکلات (1dentification Of The Problemäs Root Cause)
- تفکیک‌پذیری مشکل (problem Resolution)

خطا باید به طور سریع کشف شود و احتمالاً به وسیله سیستم مدیریت متمرکز انجام می‌گیرد و ترجیحاً قبل از اینکه کاربر متوجه آن شود باید انجام بگیرد. مکان خطا، درخواست مکان اتفاق افتادن آن را می‌کند ما این گام را از جداسازی مشکلات تمیز داده‌ایم که در عمل باید با هم یکسان باشند (جداسازی مشکلات با مکان خطا) اما دلیل برای این گونه انجام دادن این است که برگرداندن سرویس به کاربران بر اساس وبا استفاده از میانگین تناوبی به سرعت صورت می‌گیردو اعاده سرویس از یک اولویت بالاتر نسبت به تشخیص مشکل و حل آن برخوردار است، در حالی که ممکن است این امر همیشه امکان‌پذیر نباشد. شناسائی علت اصلی و ریشهٔ مشکلات جزء فرآیندها و پردازشهای پیچیده است بعد از اینکه منبع مشکل مشخص شد یک Trouble Ticket می‌تواند ایجاد و تولید شود تا مشکل را حل نماید. در خودکار نمودن مرکز عملیاتی شبکه، Trouble Ticket به طور اتوماتیک به وسیله سیستم مدیریت شبکه تولید می‌شود. کشف خطا با استفاده از موارد پائین صورت می‌گیرد:

ـ سرشماری Polling: که در این حالت سیستم مدیریت شبکه به طور متناوب از حالتهای نماینده‌های مدیریت سرشماری می‌کند.

ـ تله: trap: که نماینده‌های مدیریت که بر اساس اطلاعات از عناصر شبکه بنا نهاده شده‌اند خطاهای غیر درخواستی را به سیستم مدیریت شبکه می‌فرستند.

یک برنامه کاربردی یک دستور Ping را به طور متناوب تولید و منتظر پاسخ آن می‌ماند موقعی که یک تعداد از قبل معین شده از پاسخهای متوالی دریافت نشود، فعالیت تعریف شده شکسته واز بین می‌رود. تکرار کردن Ping به تعداد معین شده (Preset) برای کشف خطا به خاطر برقراری توازن میان ترافیک بالاسری (Over Head) و سرعت، انجام می‌گیرد و آن را بهینه می‌کند و با هزینه بهتری خطا را کشف می‌نماید. طرح کشف متناوب با استفاده از تله‌ها صورت می‌گیرد مثلاً تله Message Link Down و EgpneighborLoss در SNMP 71 می‌تواند در نماینده ست شده و رخدادها به سیستم مدیریت شبکه گزارش می‌شوند، که دارای نام عمودی درست و قانونی است یکی از مزایای تله‌ها به سرشماری این است که کشف خطا سریع‌تر و با کمترین بالاسری ترافیک انجام می‌گیرد.

کشف مکان خطا با یک روش ساده صورت می‌گیرد و به این نحو است که باید تمام اجزاء شبکه که خراب شده اند کشف شده و مشکل اصلی ردگیری گیری گردد که این به وسیله پیمایش به سمت پائین در درختهای توپولوژی انجام می‌گیرد تا شروع و مشکل شناسائی شود. بعد از اینکه مکان خطا را فهمیدیم و مشخص شد در گام بعدی باید خطا جدا شود (منبع مشکل توصیف شود) ابتدا ما باید مشخص و تعریف نمائیم که مشکل و ایراد از اجزاء است یا از اتصالهای فیزیکی چرا که ممکن است در مثال قبلی کارت رابط وظایف خود را خوب انجام می‌دهد ولی اتصال فیزیکی خود را از دست داده است لذا ما نیازمند ابزارهای تشخیص گوناگونی برای جداسازی علت هستیم. برای مدتی فرض می‌کنیم که اتصال، مشکلی ندارد و ایرات از کارت رابط است که در این هنگام اقدام به جداسازی مشکل در لایه‌هایی می‌کنیم که مسبب تولید آن مشکل هستند، گم شدن بی اندازه بسته‌ها ممکن است از قطع تماس ایجاد شود و گم شدن بسته ها را با استفاده از Ping می‌توانیم اندازه بگیریم، حتی می‌توانیم پرشهایی از پارامترهای MIB روی گره خودمان یا روی گرههای مرتبط انجام دهیم تا در آینده مسبب و علّت مشکل را محلی نمائیم. برای مثال نرخ خطا از پارامترهای گروهی رابط‌های همانند if In Discards و if In Erros و if Out Discards و if Our Errors با مراجعه به میزان و نرخ ورود و خروج بسته‌ها محاسبه می شود که ممکن است ما را در جداسازی مشکلات در کارت رابط کمک نماید. راه حل ایده‌آل برای مکان‌یابی و جداسازی خطا یک راه حل هوشمندانهٔ مصنوعی و ساختگی است که به وسیله مشاهده کردن تمام نشانه‌ها و علائم شاید که بتوانیم منبع مشکل را تشخیص دهیم [۱۴].

مدیریت کارائی

توصیف کردن کارائی در قسمتهایی از یک شبکه، مشکل تر از تعریف کردن قسمتهای آن می‌باشد. برای مثال ما زمانی مشاهده می‌کنیم که در قسمتی کارائی شبکه کند شده است، در آن صورت ما نیازمند تعریف کردن کندی هستیم مبنی بر اینکه قطعهٔ شبکه آهسته شده است که ممکن است از آهسته عمل کردن سروری باشد که کاربرد را روی خود

داشته و اجرا می‌کند. پارامترهایی که می‌توانیم به عنوان نشان کارائی شبکه در سطح عمومی تعریف کینم عبارتند از: توان عملیاتی[1]- زمان پاسخ – در دسترس بودن شبکه و قابلیت اطمینان.

شاخص از این پارامترها به این بستگی دارد که به چه علّت، کی وکجا بخواهیم اندازه‌گیری کنیم. پارامترها در سطح کلان می‌تواند در دوره‌ای از پارامترهای سطح زیر تعریف شود. همچنین بعضی از پارامترها که در روی توان عملیاتی شبکه تاثیر می‌گذارد عبارت هستند از:

پهنای باند با ظرفیت انتقال رسانه‌ها، سودمندی آنها، نرخ خطای کانال، حداکثر بار و متوسط بار ترافیک می‌باشد. که آنها در نقاط مشخصی از شبکه قابل اندازه‌گیری هستند. زمان پاسخ در یک شبکه نه تنها به توان عملیاتی شبکه بستگی دارد بلکه به کاربرد[2] هم مربوط می شود به عبارت دیگر آن هم به شبکه بستگی دارد و هم به کارائی شبکه، بنابر این در یک محیط خادم / مخدوم چنین به نظر می‌رسد گه ممکن است مخدوم آهسته کار کندو یا خادم خود استفاده، بیش از حد داشته باشد که بالاسری در ترافیک شبکه ایجاد می‌گردد ویا هر دو مورد به صورت ترکیبی وجود داشته باشند. زمان واکنش و پاسخ‌گویی کاربرد در یک شبکه بیش از دیگر موارد بر اعتراضات ونیازمندیهای کاربر نهائی تاثیر می‌گذارد برای اندازه‌گیری پاسخگوئی کاربرد عموما سه نوع شاخص می‌توانیم داشته باشیم:

- در دسترس بودن کاربرد
- زمان پاسخ میان کاربر و سرویس دهنده
- نرخ قالبهای پشت سر هم که نرخ داده‌ای موفق به سوی ایستگاه کاربر می‌باشد.

گروه کاری شبکه IETF چندین RFC روی اندازه‌گیری جریان ترافیک را توسعه داده است که RFC 2063 معماری اندازه‌گیری و گزارش دادن برای جریانهای ترافیک شبکه را تعریف می‌کند. شبکه‌های ستون فقرات به نوعی اتصال به سایر شبکه ها هستند و میزبانهای منفرد به آن وصل نمی‌شوند. یک شبکه منطقه‌ای شبیه به یک ستون فقرات است اما کوچک‌تر است که به آن امکان اتصال میزبانهای متصل هست ومیزبانهای آن ممکن است تصدیق کننده و مؤید شبکه ستون فقرات باشد. شبکه های Stub – Enterprise به LANها و میزبانها وصل می شوند و تصدیق کننده شبکه منطقه‌ای وشبکه ستون فقرات می شود میزبانها و سیستم‌های پایانی مؤید تمام این شبکه‌ها هستند.

همچنین راهکار دیگر مانیتورکردن داده در شبکه به خاطر رفتار غیر عادی کارائی است. آستانه و سرحدها، مجموعه‌ای از پارامترهای مهم مدیریت کارائی هستند که موقعی که شاخص از آستانه گذر کند شروع به تولید هشدار می‌کنند. داده‌ها جمع‌آوری و محاسبه می‌شوند و زمانی که حد مورد نظر پر شد برای آن سرویس خاص یک هشدار تولید می‌کنند. سیستم‌های مدیریت شبکه به طور عمومی تمامی رویدادهای انتخاب شده برای نمایش را که شامل هشدارها هستند را گزارش می‌دهند. هشدارها مجموعه‌ای برای بحرانها هستند که هشدار را بر طبق بحران عوض می‌کنند. وابستگی‌ها روی پیاده‌سازی یا هشدارها را به طور اتوماتیک پاک می‌کنند یا بر اثر شروطی از بین می‌برند یا به وسیله دستی وتوسط یک عمل پاک می‌کنند که حالت آخر برای پرسنل باهوش در مقابل آنچه که اتفاق می‌افتد مفید است.

لازم به ذکر است، مشکلات مرتبط به کارائی با توجه به نوع مشکل جدا می‌شوند. قبل از اینکه یک درصد بالا از بسته ها گم شود باید علّت گم شدن را برای فعالیت پیدا نمود که این عمل به صورت متناوب و غیر دائمی صورت می‌گیرد. در این حالت مانیتور کردن گم شدن بسته‌ها روی واحدهای متناوب، زمانی ممکن است که مشکلات را از هم جدا کنند مثال دیگر برای مشکلات کارائی، داشتن معاشرت با تاخیر طولانی است که چنین قابل توصیف است که بسته‌ها بیش از حد انداخته می‌شوند که در این هنگام می‌توانیم منبع تاخیر بسته‌ها را از طریق رویه ردگیری مسیریاب پیدا کنیم و بسته‌ها را کاوش کرده و گره راحذف نمائیم. در مدیریت خطا نیز بطور مشابه مشکلات ممکن است که درچندین مکان پدیدار شود که آنها توانمندی گزارش به سیستم مدیریت مرکزی را در رخداهای مستقل چندگانه داشته باشد. با فرض اینکه آنها به هم مرتبط نیز باشند. برای مثال انداختن بیش از حد بسته ها در یک اتصال ممکن است ترافیک سوئیچ و مسیر یاب را با تناوب رودررو کند. لذا باعث علت یک بالاسری در این شبکه شده و یک هشدار را باید گزارش کند. آمارهای کارائی در میزان سازی[3] یک شبکه مورد استفاده قرار می‌گیرد که می‌تواند معتبر بودن توافقات سطوح سرویس و تحلیل خواسته های مورد استفاده و طرح‌ریزی و بهینه سازی کارائی باشد. یک کاربرد برای نتایجی که شامل آمارهای کارائی است این است که شبکه را با کارائی بهتری میزان می‌کند. برای مثال دو قطعه در یک شبکه شاید یک درگاه[4] بهم متصل شوند و ترافیک مابین دو قطعه بیش از اندازه باشد که باعث تولید تاخیر بیش از اندازه می‌کند. آمارهای خطا در بسته‌های انداخته شده در روی رابط درگاه این مشکل را آشکار می‌کند. راه حل برای این مشکل چنین است که پهنای باند را برای درگاه افزایش دهیم که می‌تواند یا به وسیله افزایش ظرفیت صورت پذیرد یا با اضافه نمودن یک درگاه ثانویه میان دو قطعه انجام گیرد. البته یک درگاه اضافی باعث مشکلات مرتبط با پیکربندی می‌شود که نیازمند دوباره پیکربندی شدن ترافیک هستیم. آمارهای خطای مختلف در لایه‌های گوناگون جمع‌آوری شده و کیفیت برای سرویس اندازه‌گیری می‌شود و در صورت نیاز به ارتقاء کارائی راهنمایی می‌شود بعضی از سایر پارامترهای کارائی به وسیله مانیتور کردن آمارهای شبکه میزان می‌شود که پهنای باند برای اتصالات، میزان استفاده از اتصالها و کنترل کردن بهم حداکثر به میانگین از ترافیک داده‌های پشت سرهم که به طور ذاتی و اصلی انجام می‌گیرد به علاوه استفادهٔ و بکارگیری ترافیک ممکن است با توزیع نمودن دوباره بار در طول روز باعث پیشرفت گردد که با استفاده

[1] Through put
[2] Application
[3] Tuning
[4] Gateway

از ترافیکهای عمده در ساعات مشغول و ترافیکهای غیرعمده در ساعات کساد صورت می‌پذیرد.

یک آمار مهم، در سرویس‌های باند بالا، تغییر در تاخیر شبکه است که با Jitter (بی‌ثبات) شناخته می‌شود و تغییر در کیفیت سرویس رخ می‌دهد که برای مشتری به وسیله SLA تضمین شده که این تضمین تحت تاثیر قرار می‌گیرد. لذا مدیریت کارائی و ابعاد آن در شبکه های توزیعی از اهمیت ویژه ای برخوردار می باشد [۱۵و۸و۶].

مدیریت امنیت

مدیریت امنیت هم از لحاظ تکنیکی و هم از جنبه ملاحظات مدیریتی و اجرائی در مدیریت اطلاعات در شبکه های توزیعی مورد توجه قرار می‌گیرد. مدیریت امنیت متقاضی و خواهان امنیت داشتن دسترسی به شبکه و اطلاعات در جریان شبکه، دسترسی به داده‌های ذخیره شده در شبکه و دستگاری داده‌های ذخیره شده و در گردش سرتاسر شبکه است. نواحی مرتبط ممکن است که دارای ارتباطات سری با محلهای دیگر باشند که در این بین یک مزاحم ممکن است میان پیامها حائل شده و به طور زیرکانه تراکنش را مبادله کند و یا از آنها استفاده و فایده ببرد و یا به چیزهای ارسالی و دریافتی شخص صدمه وارد کند. برای حفظ امنیت یک سیستم شبکه ای توزیع شده، باید خطرات احتمالی زیادی را در نظر گرفت. به منظور کاهش این خطرات، می‌توان از استراتژی‌های رایج زیر استفاده کرد:

- الگوریتم‌های رمزگذاری که از داده‌ها در حین انتقال و در حالت استراحت محافظت می‌کنند.
- فایروال‌هایی که دسترسی به پورت‌ها/کابل‌های خاص را محدود می‌کنند.
- سیستم‌های تشخیص نفوذ که رفتار غیر عادی را در بین سرویس‌های شبکه شناسایی می‌کنند.
- سیستم‌های پیشگیری از نفوذ (IPS) که با شروع اقدامات دفاعی مانند مسدودسازی IP های مشکوک و حذف سرویس‌های آسیب‌دیده، به تلاش برای نفوذ پاسخ می‌دهند.

این اقدامات به تنهائی ممکن است بدون کمک سایر منابع، برای شناسایی حملات در سطح شبکه در راستای مدیریت جامع امنیت کافی نباشند. ما نه تنها می‌توانیم از دسترسی عوامل مخرب از ماشین‌های دیگر به ماشین‌های ما در همان فایروال جلوگیری کنیم، بلکه می‌توانیم اقدامات امنیتی را نیز نظارت کنیم. به اشتراک‌گذاری بی‌پروای داده‌ها می‌تواند آن‌ها را در معرض تهدیدات سایبری قرار دهد و هزینه محافظت از آن‌ها را بالا ببرد [۱۶].

مدیریت محاسبات

مدیریت شبکه در سه سطح و مدیریت سرویس در چهار سطح از سلسله مراتب بنا نهاده شده است که نه تنها شامل مفروضات تکنیکی است بلکه شامل تصمیمات سیاسی نیز می باشد. سیاستها عموما یکباره ایجاد شده و در سیستم‌ها پیاده‌سازی می شوند. برای مثال برای حل تراکم شبکه در ترافیکهای بالا ممکن است به طور اتوماتیک پارامترها را تنظیم نماید. به این معنی که پهنای باند را زیاد کرده تا ترافیک کاهش یابد. که قبلاً یکی از سیاستهای تصمیم‌گیری بود و در قسمتی از سیستم مدیریت پیاده‌سازی می‌شد. مدیریت سطوح سرویس در بخش مهمی از مدیریت محاسبات سیستم و شبکه مورئ توجه قرار می گیرد که به توافقات سطح سرویس میان مشتری‌ها وارائه کننده سرویس و به کیفیتی که از شبکه و سیستم انتظار داریم مربوط می‌شود و سرویس‌های کاربرد، اقتصادی ارائه و نگهداری می‌شوند. مدیریت محاسبات شبکه همچنین می تواند محاسبه و میزان استفاده از منابع توزیعی شبکه را مدیریت نماید [۱۷].

در پایان لازم به ذکر است، از بزرگ‌ترین مشکلاتی که مدیران شبکه با آن مواجه هستند، چگونگی دسته‌بندی و نظارت روی رویدادهای جاری در این بستر است. مخصوصا زمانی که موضوع حملات امنیتی در کمین شبکه مطرح می‌شود، اهمیت مدیریت جامع و نظارت روی داده هایی که در شبکه رد و بدل می‌شوند دوچندان خواهد بود. برای اینکه مدیر شبکه بتواند به‌طور منظم روی لاگ‌های سیستم و چارچوب عملیاتی آن نظارت داشته باشد و مشکلات سخت‌افزاری، نرم‌افزاری و حملات امنیتی را شناسایی کند، نیاز به محصولاتی دارد که مدیریت جامع و نظام مند شبکه را بر عهده بگیرد. محصولی که وقایع امنیتی را تجزیه‌وتحلیل کند، لاگ‌های سیستم را جمع‌آوری و دسته‌بندی کرده و در کل مدیریت و نظارت روی شبکه را به‌صورت متمرکز امکان‌پذیر کند [۱۸].

نتیجه گیری

صنعت و تجارت در دنیای امروز نیازمند بهره مندی از سیستم های نوین برای انجام فعالیت ها و خدمات مختلف است. یکی از سیستم های محبوب مورد استفاده در عصر حاضر که در آن تمرکزگرایی حذف می شود، شبکه های توزیعی است. شبکه های توزیع شده سیستم های مبتنی بر رایانش توزیعی می باشند که در آنها اجزای برنامه ها و داده‌ها به چندین منبع نامتمرکز وابسته هستند. مدیریت شبکه را می توان نوع و شکل تازه ای از ساختارها و زیرساخت های فعالیت سازمانی دانست که امروزه استفاده از آن برای سازمان های مختلف ضرورت دارد. در مدیریت شبکه باید از برنامه ها، ابزارها و فرآیند های لازم بهره برد. مدیریت به معنی به کارگیری منابع مادی و انسانی به شکلی موثر و کارآمد است. در حقیقت منابع و افراد برای رسیدن به اهداف مشخص شده در سازمان به کار گرفته میشوند. دیدگاه مدیریت جامع شبکه های توزیعی منابع شبکه را به شکلی کارآمد، موثر و سریع در دسترس کاربران قرار میدهد. همچنین بهینه سازی شبکه با استفاده از تجزیه و تحلیل خطا و مدیریت عملکرد تضمین میشود. با استفاده از چارچوب های مدیریت جامع میتوان بهترین ابزارهای مناسب برای مدیریت، نظارت و کنترل شبکه را به کار گرفت تا در صورت نیاز، به چالش های پیش آمده در شبکه پاسخ دهند. در این مقاله درخصوص رویکرد

دستیابی به مدیریت جامع شبکه های توزیعی و ابعاد آن تحقیق و بررسی نمودیم و الزامات و نیازمندی های ضروری را بیان کردیم.

تعارض منافع

«هیچ‌گونه تعارض منافع توسط نویسندگان بیان نشده است»

منابع و مآخذ

[1] Sarukhani S, Dabiran F, Ayatollahi Z. Integrated management in the communication service provider's network. In7'th International Symposium on Telecommunications (IST'2014) 2014 Sep 9 (pp. 641-645). IEEE.

[2] García AP, Oliver J, Gosch D. An intelligent agent-based distributed architecture for smart-grid integrated network management. InIEEE Local Computer Network Conference 2010 Oct 10 (pp. 1013-1018). IEEE.

[3] Poulkov V. Beyond the next generation access. Wireless world in 2050 and beyond: A window into the future!. 2016:17-39.

[4] Bellman K, Botev J, Diaconescu A, Esterle L, Gruhl C, Landauer C, Lewis PR, Nelson PR, Pournaras E, Stein A, Tomforde S. Self-improving system integration: Mastering continuous change. Future Generation Computer Systems. 2021 Apr 1;117:29-46.

[5] Klijn EH, Steijn B, Edelenbos J. The impact of network management on outcomes in governance networks. Public administration. 2010 Dec;88(4):1063-82.

[6] Boutaba R, Salahuddin MA, Limam N, Ayoubi S, Shahriar N, Estrada-Solano F, Caicedo OM. A comprehensive survey on machine learning for networking: evolution, applications and research opportunities. Journal of Internet Services and Applications. 2018 Dec;9(1):1-99.

[7] Kreutz D, Ramos FM, Verissimo PE, Rothenberg CE, Azodolmolky S, Uhlig S. Software-defined networking: A comprehensive survey. Proceedings of the IEEE. 2014 Dec 19;103(1):14-76.

[8] Chowdhury NM, Boutaba R. A survey of network virtualization. Computer Networks. 2010 Apr 8;54(5):862-76.

[9] Han B, Gopalakrishnan V, Ji L, Lee S. Network function virtualization: Challenges and opportunities for innovations. IEEE communications magazine. 2015 Feb 19;53(2):90-7.

[10] Cho JH, Swami A, Chen R. A survey on trust management for mobile ad hoc networks. IEEE communications surveys & tutorials. 2010 Oct 14;13(4):562-83.

[11] Zou Y, Zhu J, Wang X, Hanzo L. A survey on wireless security: Technical challenges, recent advances, and future trends. Proceedings of the IEEE. 2016 May 10;104(9):1727-65.

[12] Alemdar H, Ersoy C. Wireless sensor networks for healthcare: A survey. Computer networks. 2010 Oct 28;54(15):2688-710.

[13] Mohassel RR, Fung A, Mohammadi F, Raahemifar K. A survey on advanced metering infrastructure. International Journal of Electrical Power & Energy Systems. 2014 Dec 1;63:473-84.

[14] Bititci U, Garengo P, Dörfler V, Nudurupati S. Performance measurement: challenges for tomorrow. International journal of management reviews. 2012 Sep;14(3):305-27.

[15] Ghafir I, Prenosil V, Svoboda J, Hammoudeh M. A survey on network security monitoring systems. In2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) 2016 Aug 22 (pp. 77-82). IEEE.

Performance Distributed Computing (Cat. No. 98TB100244) 1998 Jul 31 (pp. 140-146). IEEE.

[18] Chopra A, Kumar R. Efficient resource management for multicast Ad hoc networks: survey. International Journal of Computer Network and Information Security. 2016 Sep 1;8(9):48.

[16] Lin H, Yan Z, Chen Y, Zhang L. A survey on network security-related data collection technologies. IEEE Access. 2018 Mar 21;6:18345-65.

[17] Raman R, Livny M, Solomon M. Matchmaking: Distributed resource management for high throughput computing. InProceedings. The Seventh International Symposium on High