KnowNet : به سمت یک برنامه دانش برای مدیریت شبکه سازمانی

چکیده :

کارهای مدیریت شبکه امری خسته کننده و مستعد خطا است و اغلب نیازمند استدلال پیچیده از سمت مدیریت شبکه است. با KnowNet ما به بررسی چالش فنی استدلال در مورد مدیریت شبکه با استفاده از آن به صورت مجموعه ای از برنامه های مشارکتی اجرا شده در گراف دانش میپردازیم که معمولا شامل داده ها و اطلاعات در مورد شبکه و برنامه بوده و جهت مدیریت و استدلال استفاده می شوند. ما از رویکرد خود در مدیریت شبکه سازمانی با توسعه مجموعه ای از برنامه ها استفاده می کنیم که با مدیریت عملکرد برنامه در شبکه سازمانی محقق می شود.

1- مقدمه

علی رغم شناخت طولانی مدت اهمیت رویکرد های پیشرفته برای مدیریت شبکه و لزوم راه حل های خود کار توسط انجمن های تحقیقات شبکه ای، پیشرفت زیای هنوز برای مقاومت در برابر این تلاش ها وجود دارد. عملا مدیریت شبکه امری دستی، خسته کننده و مستعد خطا است و اغلب نیازمند استدلال پیچیده از طرف مدیریت شبکه است. خودکار سازی استدلال توسط کارشناسان دامنه یک چالش کلیدی در درک رویکرد سیستمی برای مدیریت شبکه است. این مسئله بسیار مشکل است زیرا این استدلال نیازمند مقادیر متنوعی از داده ها است. این داده ها از تعدادی از منابع مختلف جمع اوری شده است و به منظور تفسیر معنی دار، بایستی با حالت عملیاتی شبکه در زمان جمع اوری همبستکی داشته باشد. روابط پیچیده ای بین سخت افزار، پروتکل، سرویس ها و وضعیت عملیاتی وجود دارد و این وضعیت عملیاتی بایستی نیازمند درک اثرات و تغییرات در شبکه باشد.

استدلال ما این است که سیستم مدیریت شبکه می تواند از این عملکرد پشتیبانی کند و این نیازمند ابزاری برای پوشش دادن اطلاعات و دانش شبکه به طور جامع است که امکان تعامل آسان برنامه های مدیریت شبکه را با استدلال در مورد این دانش داده و منجر به تغییراتی در خود شبکه می شود. به این ترتیب ما از یک رویکرد عمل گرایانه برای درک این سیستم بهره می بریم. کلید اصلی این است که مدیران شبکه معمولا از چندین سیستم

برای پایش ومدیریت شبکه ها استفاده کرده و این که این مدیران معمولا به استدلال و منطقی می پردازند که با این سیستم ها ارتباط دارد. به جای تحمیل یک سیستم مدیریت شبکه جدید بر رو ی مدیران شبکه ای که نیازمند جایکزینی سیستم و ابزار های مورد استفاده هستند، ما یک چارچوبی را ارایه می کنیم که آن ها در کل سیستم استفاده می کنند و ما یک چارچوب را ارایه می کنیم که امکان خودکار سازی آسان کار های منطق و استدلال را می دهد.

برای رسیدن به این هدف ما KnowNet را ارایه می کنیم که یک سیستم مدیریت شبکه دانش محور است و موجب تسهیل کشف و تسهیم دانش می شود و اپراتور ها می توانند به طور موثر در مورد وضعیت شبکه استدلال کنند و اقدامات مناسب را تعیین کرده و شبکه را در صورت لزوم تغییر دهند. برنامه ها معمولا از گراف دانش در راس KnowNetبرای نماش داده های جمع اوری شده در مورد شبکه و دانش مشتق شده از شبکه استفاده می کنند. گراف های دانش محبوبیت زیادی را در میان تعدادی از دامین ها دارند و این به دلیل توانایی بیان و کشف روابط جالب در مجموعه داده های بزرگ است که امکان استدلال پیچیده در مورد داده های به هم پیوسته را می دهد. در مطالعه ما بر روی KnowNet، ما به بررسی استفاده از کراف دانش برای پوشش دادن اطلاعاتو دانش در شرایط مدیریت شبکه می پردازیم. در واقعف کار ما یک گام مهم به سمت مدیریت دانش است.

گراف دانش در KnowNet برای پوشش دادن چیزی فراتر از داد های شبکه استفاده می شود به خصوص برنامه های مدیریت شبکه با KnowNet تعامل داشته و از طریق کراف دانش نیز با خود شبکه تعامل دارد. به این ترتیب امکان پوشش دادن فعالیت های مدیریت دانش به عنوان بخشی از دیدگاه جامع شبکه در KnowNet وجود دارد. برای دست یابی به این سیستم مدیریت شبکه مشارکتی،ما یک گراف دانش موسوم به کیلو را برای کشف ویژکی های مفید در مدیریت شبکه توسعه داده ایم. به طور ویژه، کیلو شامل مجموعه ای از اشکال کراف دانش است که شامل: افزایش، پرس و جو و حذف است. علاوه بر این موارد، کیلو از مشترک شدن یا subscribe برای یادگیری در مورد رویداد های مربوطه پشتیبانی کرده وزمان را به دلیل اهمیت پوشش دادن شبکه در طی زمان در نظر می گیرد.

به منظور کشف اهمیت کاربردی معماری ارایه شده، ما مجموعه ای از برنامه های مدیریت شبکه را با هدف مدیریت شبکه سازمانی توسعه دادیم. ما یک شبکه سازمانی را پیش بینی می کنیم که در آن هر دو شبکه به

صورت کارکردی و نیز واحد های مدیریتی پیچیده در نظر گرفته می شوند و از این روی توسط برنامه های پشتیبانی شده با KnowNet فعال ساز یمی شود. بر اساس گزارشات اخیر بر روی چالش های شبکه ای، برنامه های مبتنی بر مدیریت امنیت و عملکرد تاکید می شود. ما نشان می دهیم که ابزار های موجودرا می توان در KnowNet قرار داد تا با عملکرد مدیریت شبکه جدید برای تحقق هدف مدیریت شبکه جامع تعامل داشته باشد.

مطالعه ما با استناد به تلاش های مدیریت شبکه ای قبلی(9-10-1-11-12-13-14)، از ابعاد مختلف منحصر به فرد است. اولا،ما بر این باوریم که که این مطالعه برای اولین بار به بررسی استفاده از خلاصه سازی گراف دانش برای پوشش دادن همه داده ها، دانش و اقدامات مربوط به مدیریت شبکه می پردازد. دوما، رویکرد ما برای حمله به مسئله مدیریت شبکه با یک مجموعه ای از برنامه های مشارکتی، یک توازن منحصر به فرد را بین انعطاف پذیری و سادگی ایجاد می کند. در KnowNet ما ساختار گراف دانش خود را برای تعریف ساختار بر طبق داده ها و شیوه های مدیریتی تحمیل نمی کنیم. از سوی دیگر این مسئله نیازمند پیشرفت بیشتر برنامه ها می باشد. در نهایت در KnowNet، ما یک رویکرد عمل گرایانه را برای مدیریت شبکه با استفاده از هر دوی آن ها و نیز برنامه های مدیریت شبکه در چارچوب جامع ارایه می کنیم.

اهداف این مقاله به شرح زیر است:

- طراحی و پیاده سازی KnowNet،که یک چارچوب مدیریت شبکه می باشد که مسئولیت پذیری ساتدلال در مورد شبکه در میان برنامه های مشارکتی را تقسیم می کند
- ما اقدام به طراحی و پیاده سازی kilo می کنیم که یک گراف دانشی است که مربوط به حوزه مدیریت دانش است
- برای بررسی و ارایه کاربرد KnowNet، ما مجموعه ای از برنامه های مدیریت شبکه مربوط به عملکرد و امنیت را برای شبکه های سازمانی ارایه می کنیم. برخی از برنامه ها در این مجموعه، یک استدلال پیچیده را نشان می دهند ضمن این که سایر برنامه ها از ابزار های مدیریت شبکه موجود استفاده می کنند. ما نشان می دهیم که چگونه KnowNet امکان می دهد تا این برنامه های موجود در یک سیستم مدیریت شبکه جامع قرار می گیرند

- ما اقدام به ارزیابی گسترده رویکرد خود در محیط شبکه سازمانی شبیه سازی شده خود می کنیم. این ارزیابی نشان دهنده توانایی شبکه پشتیبانی شده با KnowNet برای حفظ سلامت شبکه تحت شرایط متغیر و تنظیم مقیاس شبکه های با اندازه شرکتی است.

2-مقدمه و هدف

در فراتر از چشم انداز برنامه دانش، مطالعه ما الهام گرفته از نت سرچ(15) می باشد که یک ابزار بازیابی اطلاعات و جست و جو می باشد که از موتور های جست و جوی وب الهام گرفته است با این حال برای شبکه ها طراحی شده است. هدف نت سرچ سازمان دهی داده های شکبه برای مشخص کردن روابطی است که استنباط آن ها سخت است. درKnowNet ما اقدام به بازیابی اطلاعات برای ذخیره دانش پیشرفته می کنیم و یک بستر استدلال سیستماتیک را برای اپراتور ها ارایه می کنیم. برای انجام این کار، بستر به عنوان مبنایی برای خودکار سازی اقدامات مدیریت شبکه حلقه بسته در نظر گرفته می شود. اطلاعات کلیدی این است که رابطه کاوی با استفاده از یک گراف دانش بهبود می یابد که مدل اساسی آن بر مبنای این روابط است و این که پوشش دادن این روابط امکان خودکار سازی بخش های مدیریت شبکه را می دهد.

یک گراف دانش(kg)(5) یک ساختار داده ای مورد استفاده برای نمایش مجموعه ای از حقایق است که مجموعا تولید دانش می کنند. حقایق متشکل از مراکز گره و روابط(یال) بین آن ها است. این ها به صورت سه گانه نوشته می شوند برای مثال switchA has-interface if0. یک پرس و جو در برابر این گراف به شکل زیر گراف در نظر کرفته می شود(برای مثال همه زیرگراف ها به طوری کهa دارای سوییچ نوع و a دارای رابط B و Cاز رابط B استفاده می کند تا مسیر بین دو گره راجست و جو کند). سپس با باز گرداندن همه زیر گراف ها با مراکز مطابق با کوئری و باز گرداندن آن ها به جای متغیر ها، انجام می شود. استفاده از خلاصه سازی یا انتزاع گراف دانش به یک مدل محبوب برای تحلیل داده ها تبدیل شده است. با بیان داده ها به صورت یک شبکه ای از روابط، امکان کشف روابط و استنباط حقایق جدید از ارتباطات وجود دارد. گراف های دانش مطابق با دیتا سیت های بزرگ و کوئری های پیچیده هستند. در واقع کار ما بر توسعه برنامه های مدیریت شبکه و استفاده از آن در شرایط شبکه ای متوسط متمرکز است. از این روی مقیاس پذیری هدف کار فعلی مانیست.

بخش های زیر توجیه کننده تصمیم ما استفاده از گراف دانش به صورت هسته رویکرد KnowNetمی باشد:

الف: مدل سازی داده های شبکه

ما اقدام به تحلیل تعدادی از رویکرد های تمایش و مدل سازی داده های شبکه و ترکیب آن ها با تجربه خود برای شناسایی تعداد ملزومات کلیدی ای که بایستی در رویکرد جدید برطرف شود پرداختیم. استدلال ما این است که این ملزومات بایستی مطابق ب رویکرد مبنی بر گراف دانش باشد.

پشتیبانی ترکیب دانش: بیشتر داده های مدیریت شبکه دارای گرایش کلید-مقدار هستند. داده های SFLOW، هشدار هایIDS، پیگر بندی رابط، قواعد OPENFLOW و حتی بسته ها به خودی خود، مجموعه ای از جفت های کلید-مقدار هستند. اگرچه این نمایش داده ها مشخص واضح است، یک شیوه دست یابی و درک مستقیم جفت های خام وجود ندارد. از این روی در زمان نمایش این داده ها، هدف ما ویژگی های مرتبط با کلید ها و مقادیر می باشد.KnowNet به ما بررسی این ارتباطات و روابط را بین داده های مقدار- کلید می دهد.

آگونوستیک منبع داده ها: نمایش و مدل سای ها داده ها بایستی مستقل از ابزار هایی باشند که داده هایی را ارایه می کند.. بسیاری از ساختار های داده های پیشنهادی، منعکس کننده منبع داده ها می باشند. قرار دادن این منابع داده ها در مدل سازی موجب محدود شدن داده ها و ابزار های ساخته شده با استفاده از آن می شود. تبدیل داده های سطح پایین به کراف دانش،KnowNet به ما امکان ترکیب هر گونه داده را به یک مدل داده شبکه می دهد.

ب: مدیریت شبکه باگراف های دانش

در فراتر از نمایش داده ها، رویکرد مبتنی بر گراف دانش دارای ویژگی هایی است که موجب شده است تا جذابیت بالایی برای حوزه مدیریت شبکه پیدا کند.

ساختار انعطاف پذیری با سلسله مراتب: مدل داده های پیشنهادی توسط یک گراف دانش ساده است. و موجب ساده تر شدن انعطاف پذیری آن ها و ساختار های پیچیده در راس ان می شود. این ویژگیها به این معنی است که KnowNet نیازی به تحمیل طرح بر روی برنامه های نوشته شده ندارد. این موجب تسهیل توسعه انواع جدیدی از شبکه های مدیریت شبکه می شود. البته یک سری دسته های اشیا و سلسله مراتب های لایه بندی در شبکه و مجموعه ای از برنامه های پایه را در KnowNet بر اساس حقایق و با استفاده از مدل سلسله مراتبی می دهد.

برنامه های ما با مدل در کاربردی تعامل دارد. به این ترتیب امکان استنباط بین لایه های خلاصه سازی وجود دارد.

داده های موجود در گراف دانش توسط روابط آن سازمان دهی می شود خواه نوع داده ها و یا عناصر شبکه در نظر گرفته شود. بر عکس دیتابیس های موجود این داده ها در جداول متفاوت در نظر گرفته شده اند. این ابزاری برای پرس و جو به ازای همه اندازه گیری های عملکرد و همه هشدار های امنیتی است و سپس از طریق فیلیترینگ می توانیم نوع گره را مشخص کرده و همه دانش مرتبط با آن را به دست بیاوریم. این نه تنها تسهیل کننده پرس و جو های بزرگ می شود از این روی امکان کشف دانش با استفاده از برنامه های پرس و جو برای روابط متعدد مجعول بر اساس برنامه های آن ها وجود دارد.

اگرچه انعطاف پذیری یک طرح پویا مفید است، با این حال بیانگر یک سری چالش ها است. از آن جا که درک معنا و روابط نام سخت است، با این حال استفاده از منابع مختلف می تواند در نظر گرفته شود. در این نقطه، معنای مربوطه امکان درک بهتر روابط بین داده های شبکه را می دهد. هدف ما کشف استفاده از یک گراف دانش با ابزار های شبکه ای مربوطه یا تعبیه شده است.

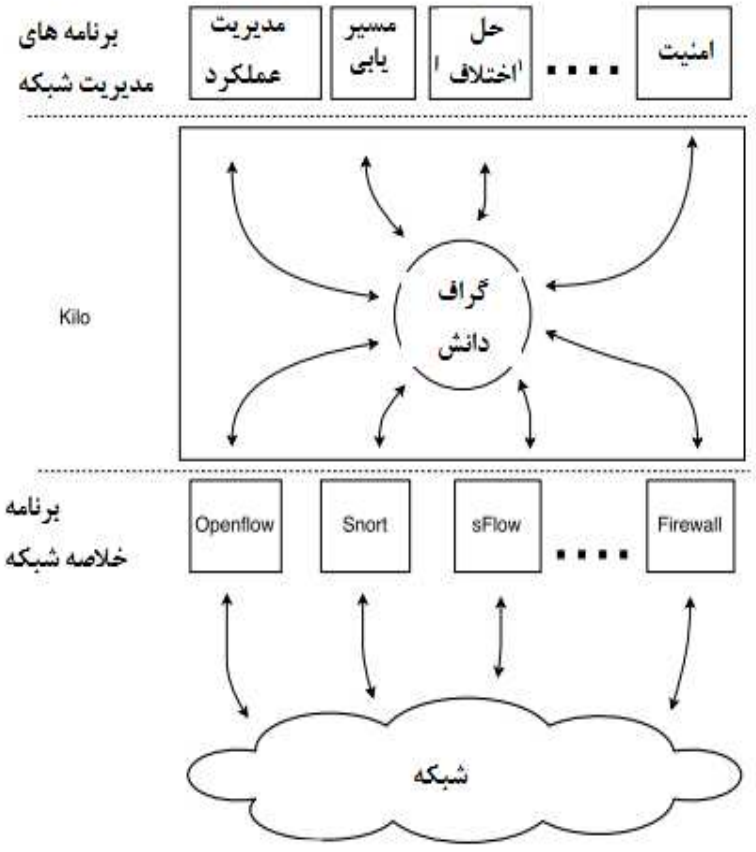
ساختار شبه شبکه: براز طبیعی شفاف بین یک گراف دانش و یک شبکه، مروبط به توپولوژی یک شبکه به صورت یک گراف نشان داده می شود. بسیاری از الگوریتم های شبکه رایج نظیر الگوریتم درخت حداقل و الکوریتم های مسیر یابی مختلف، بر اساس ساختار های گراف است. برنامه KnowNet یک عملکرد شبکه ای را ارایه می کند برای مثال ، مسیر یابی از این ویژکی ها استفاده می کند.

زنجیره های وابستگی: یک برازش مشهود بین گراف های دانش و حوزه مدیریت شبکه، در مدل سازی وابستگی ها وجود دارد. برای مثال، یک سرویس(نظیر وب سرور، فایل سرور یا ارتباط ip) بستگی به مسیر های شبکه ای دارد که بسته های خدماتی را تحویل می دهد. این مسیر به نوبه خود بستگی به پروتکل های اثبات گننده داشته و از این سخت افزار پیاده سازی کننده آن هاست. این وابستگی ها سلسله مراتبی نمی باشند: برای مثال، عملکرد مسیر مربوطه بستگی به سایر خدمات با استفاده از مسیر و هاپ در امتداد مسیر و وضعیت پویای آن ها دارد نظیر بار پیشنهادی، سطح ازدحام و خرابی ها. نشان دادن شبکه با استفاده از گراف دانش، امکان بررسی علت و معلول رفتار شبکه دارد.

3- معماری KnowNet

معماری KnowNet در شکل 1 نشان داده شده است. این به دو بخش تقسیم می شود: یک حافظه دانش مرکزی که به صورت گراف دانش kilo در نظر گرفته می شود و مجموعه ای از برنامه های هماهنگ سازی که از داده ها، اطلاعات و دانش در حافظه دانش برای انجام کار ها ی مدیریتی شبکه استفاده می کند

برنامه های مشارکتی KnowNet را می توان به مجموعه ای از برنامه های انتزاعی شبکه تقسیم کرد که با یک شبکه و مجموعه ای از برنامه های مدیریت شبکه ارتباط دارد و دستورات مدیریت مختلف شبکه راانجام می دهد. معماری KnowNet یک سری از چارچوب های مدیریت شبکه عمومی را ارایه می کند که قابل تعمیم به محیط مدیریت شبکه است.با این حال، دستور برنامه ها متناسب با یک محیط شبکه است که در آن یک سیستتم استفاده می شود. برای مثال در بخش 4 به توصیف برنامه هایتوسعه یافته متناسب با مدیریت شبکه سازمان می پردازیم.



شکل 1: معماری KnowNet

می توان دید که از دیدگاه انتزاعی، معماری KnowNet ساده از اقدامات مدیریتی شبکه پیروی می کند. مدیران شبکه از سیستم های خواندن و نوشتن مختلف در شبکه های خود استفاده می کنند و دلایل مربوط به خروجی را از برخی از سیستم های خواندن برای تصمیم گیری در مورد سیستم نوشتن دیگر تفسیر می کنند. هدف ما با KnowNet ایجاد یک سیستم مدیریت شبکه جامع است که امکان هماهنگ سازی این سیستم ها را برای تسهیل عملگر های شبکه در استدلال پیچیده و ب موقع در حالت شبکه می دهد

الف: یک گراف دانش مدیریت شبکه

سیستم های گراف دانش مرسوم نظیر ,[6] ,[3] Naga/Yago ,[2] Freebaseو ,[4] DeepDive برای کتترل دانش نسبتا استاتیک طراحی شده است.

دانش مرتبط با مدیریت شبکه پویا تر است. ما سه لازمه مرتبط با مدیریت شبکه خاص را شناسایی می کنیم که سیستم های گراف دانش موجود پشتیبانی خوبی ندارند.

کوئری های واکنشی: دستورات و بخش های مدیریت شبکه به شکل واکنشی اجرا می شوند برای مثال، اگر A رخ دهد، B اجرا می شود. این نشان دهنده نیاز به گراف دانش است که اطلاعاتی را در مورد برنامه ها ارایه می کند که دانش خاص به گراف افزوده می شود.

داده های متغیر زمانی: در یک سناریوی مدیریت شبکه، تغییرات دانش با گذشت زمان و مسیر یابی دانش به صورت تابعی از زمان است. این نشان دهنده لزوم برای گراف دانش یا مسیر یابی زمانی برای پشتیبانی از مدیریت شبکه است.

مهار داده ها: چون دانش با گذشت زمان در سناریوی مدیریت شبکه تغییر می کند، استفاده از حقایق وابسته به زمان است. حقایق می تواند تا حدودی گمراه کننده باشد. به علاوه توابع مدیریت شبکه تولید حجم زیادی از داده ها می کنند. این نشان دهنده نیاز به کنترل داده ها در پشتیبانی از مدیریت شبکه است.

ب: گراف دانش KnowNet: Kilo

به منظور انجام ازمایشات با ویژگی های ضروری و مفید برای مدیریت شبکه ، ما گراف دانشKnowNet را از اسکراچ پیاده سازی کردیم. این رویکرد به ما امکان بررسی دقیق تر گراف دانش را برای تسهیل مدیریت شبکه میدهد. Kilo بر کرفته از ناگا(3) است که یک گراف دانش برای کنترل حجم زیادی از دانش مبتنی بر متن استفاده

می شود. Kilo بر گرفته از الگوریتم های مرکزی دانش بوده و با افزایش و پرس و جو همراه است. ما یک رابط HTTP ار پیاده سازی می کنیم که از برنامه های مختلف برای کار با گراف دانش پشتیبانی می کند.

Kilo یک گراف دانش را نظیر افزایش، پرس و جو و حذف ارایه می کند. به علاوه، ما یک مدیریت شبکه خاص را در Kilo ارایه می کنیم که موسوم به ساب اسکریپشن می باشد. ما جزییات پیاده سازی دقیق و صریح مربوط به Kilo را در نظرمی گیریم.

زیرنویس ها و اشتراکات: بخش کلیدی مدیریت شبکه، واکنش به رویداد های خاص است. KILO این پویایی را با امکان دادن به برنامه ها برای دریافت نتایج جدید برای پرس و جو فراهم می کند زیرا گراف دانش از طریق اشتراکات به روز رسانی می شود. یکی از اهداف استفاده از این سیستم اولیه در گراف، اطمینان از برنامه هایی است که سریعا به تغییرات حالت شبکه واکنش می دهد. مکانیسم های خارجی نیازمند فنونی نظیر نظر سنجی است که می تواند موجب کاهش حالت های گذار می شود.

حذف: هر حافظه دانش نیازمند توانایی فراموش سازی یک قطعه از دانش است. دانش می تواند قدیمی، نامرتبط بوده و یا مدیریت آن سخت باشد. در Kilo ، می توان یک رویکرد مرجع را برای حذف در نظر گرفت.هر برنامه برای مقابله با این موضوعات نیاز است. زمانی که ما با یک مقدار صفر مواجه می شویم این مقدار از داده ها دیگر لازم نیست و بایستی آن ها را از گراف دانش فعال حذف کرد. ما از برنامه بایگانی پشتیبانی می کنیم که از ویژگی های پیاده سازی شده توسط برنامه های حذف برای انجام کنترل داده ها بر اساس سیاست ها و نیاز های شبکه سازمانی استفاده می کند.

زمان: ما زمان را به عنوان یک عامل مهم برای مهر زمانی پشتیبانی می کنیم. این امکان پرس و جو هایی را می دهد که شامل مهر های زمانی حداکثر و حداقل اختیاری است. با اجرای پرس و جو، حقایق بر اساس این پارامتر های زمانی فیلتر می شوند و به طور موثر گراف را ویرایش کرده و امکان استفاده از گراف را در هر مرحله زمانی می دهد.

4- برنامه های مدیریت انترپرایز

برنامه های نوشته شده برای KnowNet ساده هستند. جریان کار به صورت زیر است:1- پرس و جو یا اشتراک برای حقایق حاص : برای مثال، یک برنامه مسیر یابی که به دنبال حقایقی است که نشان می دهد رابط ها در

سطح پایین هستند و یا برنامه ای که اندازه گیری های فعال را انجام داد و به دنبال حقایقی است که بیان می دارد برنامه های دیگر نیازمند اندازه گیری یک مسیر خاص است. این چیزی فراتر از کوئری های داده های ساده است. اکوسیستم برنامه های مختلف اجرا شونده بر روی گراف دانش امکان ترکیب دانش سطحبالا و پیشرفته را در نتیجه درک نقاط داده های مختلف می دهد.2- تفسیر حقایق: این در جایی است که حجم کار های برنامه بالا باشد: رایانش مسیر ها، انجام اندازه گیری ها. این در جایی است که استفاده از گراف دانش بسیار مطلوب باشد. به این ترتیب امکان درک رفتار های شبکه به صورت یک عملگر با بررسی شبکه در سطح پایین برای تولید اطلاعات در سطح بالاتر وجود دارد. گراف دانش،برنامه هایی را ارایه می کند که متشکل از استدلال انسانی به شیوه ای رابطه محور است. این مرحله به معنی کاربرد دانش زمینه ای برای شبکه است که نتایج آن در یک گراف برای برنامه ها قرار داده شده است. افزودن هر گونه نتایج به گراف دانش: این حقایق موجب ایجاد استنباط دقیق از داده های موجود می شود و نشان دهنده نتایج اندازه گیری و احتمالات شبکه می باشدو می تواند شامل درخواست هایی برای برنامه های دیگر باشد. این دانش بر اساس دانش زمینه ای توصیه شده در تک تک برنامه ها است. به دلیل ماهیت باز گراف دانش، بیشتر برنامه ها بر یک کار ساده و متمرکز تاکید دارند که بر برنامه های ساده برای پشتیبانی از دانش غنی تکیه می کند. ما بر این باوریم که این رویکرد ساده موجب تسهیل فرایند پوشش و به کار گیری دانش شبکه می شود.

به منظور کشف توانایی KnowNet برای پشتیبانی از مدیریت شبکه، یک مجموعه ای از برنامه های نمونه را برای پشتیبانی از مدیریت شبکه دانش بنیان در شبکه سازمانی ارایه می کنیم.اگرچه این برنامه ها ساده هستند، بر چالش های موجود در مدیریت شبکه تاکید می کنند یعنی بوت استراپ و کاربرد شبکه، پایش عملکرد و مدیریت و مدیریت امنیت. ما بر این باوریم که پشتیبانی از چارچوب های موجود با در نظر گرفتن اندازه گیری های فعال در مسیر ها سخت است.

الف: عملکرد شبکه پایه

اولین مجموعه از برنامه ها، یک سطح پایه از کاربرد شبکه را ارایه می کند: ایجاد یک ارتباط IP که از هر شبکه انترپرایز انتظار می رود.

بوت استراپ: دوبرنامه در KnowNet با یک دیگر برای بوت استراپ عمل می کنند: برنامه توپولوژی که همه گره ها و سوییچ ها را پشتیبانی می کند و در بر گیرنده همه ویژگی های نگه داری و انوانتوری می باشند که نشان دهنده حالت رابط هستند و برنامه openflow که نشان می دهد OpenFlow می تواند رابطی را برای پیکر بندی کنترلگر ارایه کند. هر دوی این برنامه ها توسط سایر برنامه ها در اکوسیستم استفاده می شود. و این می تواند مجموعه ای از خلاصه ها را در اختیار می گذارد.

ارتباط IP: وقتی که ارتباط پشتیبانی شد، برنامه مسیر یابی را با مسیر یابی جهانی ارایه می کند. این خود از اطلاعات مربوط به توپولوژی برای محاسبه مسیر ها استفاده می کند و به برنامه openflow برای به روز رسانی جداول مسیر یابی تاکید می کند. اگر QoS بر روی شبکه پشتیبانی شود، برنامه مسیر یابی نیز در نصب مسیر قرار داد می شود.

مدیریت سرویس پایه: برنامه سرویس ما به عنوان یک مدیر QoS برای خدمات با پیگر بندی صفت ها از SLA عمل می کند.. این خود بر اساس اطلاعات قواعد و پشتیبانی توسط برنامه های بوت استراپ است.

حل اختلاف: ما یک روش اثبات مفهوم را پیاده می کنیم که دانش وابستگی به شبکه برای تشخیص روابط بین دستوراتی وجود دارد که در سطوح مختلف می تواند وجود داشته باشد برای مثال قادر به تعیین گراف دانشی است که می تواند رابط را در سطح شبکه و متناقض با تغییر سطح بالاتر در سطح مسیر حل کند. توجه کنید که معماری ما بستگی به حل اختلاف در این روش ندارد و می توان با رویکرد های حل اختلاف دیگر کار کرد.

ب: پایش عملکرد و مدیریت

مجموعه بعدی ما از برنامه ها به بررسی چیزی فراتر از حفظ ارتباط پرداخته و عملکرد شبکه را حفظ می کنند: با پایش فعالیت شبکه، مسیر یابی مجدد جریان برای رفع اهداف عملکردی و پیکر بندی مجدد شبکه در صورت لزوم برای حل مسئله و این با ترکیب دانش مربوط به شبکه از منابع مختلف در چارچوب گراف دانش صورت می گیرد.

اندازه گیری: ما یک سری برنامه هایی را برای منابع مورد استفاده داده های عملکرد شبکه نظیر sFlow-RT و ping ارایه می کنیم. این برنامه ها یک اندازه گیری دوره ای را از شبکه و افزایش آن ها به گراف دانش ارایه می کنند برنامه sflow به صورت منفعل است که اماره های جددی را از سوییچ جمع اوری می کند و امکان تحلیل

رجیان مبتنی بر تقاضا را می دهد. برنامه PING از اندازه گیری فعال تاخیر مسیر استفاده می کند. برنامه pingامکان اندازه گیری مسیر هایدلخواه را می دهد: این خود با برنامه مسیر یابی متناسب با بسته های ورودی به مسیر خاص تعامل دارد.

وضعیت شبکه: برنامه های iface و link برای پایش حالت رابط ها و لینک ها استفاده می شوند. آن ها به دنبال رابط هایی هستند که به طور کامل خراب می شوند و یا خطا را به صورت CRC بد پایش می کنند. در هر دو صورت برنامه از قابلیت خود برای کشف گراف دانش برای کشف مسیر و سرویس ها با استفاده از رابط ها استفاده کرده و از این روی نشان می دهد که سرویس ها بایستی مجددا مسیر یابی شوند و مسیر یابی مجدد واقعی قادر به پایش برنامه ها است.

مدیریت عملکرد: برنامه مسیر یاب عملکرد مسئول پایش عملکرد همه جریان های خدمات در شبکه است که کنترل می کند آیا SLAنقض شده است یا خیر و سپس تغییرات ضروری را اعمال می کند. رفع این نیاز ها مستلزم انواع مختلف اطلاعات پویا است. اولا برنامه بایستی به طور پیوسته ارتباط تازه و اندازه گیری های تاخیر را برای همه مسیر های شبکه دریافت کند. به علاوه، این نیازمند اطلاعات اندازه گیری دوره ای برای مسیر های غیر خدماتی است به طوری که به این مسئله پی ببرد که آیا مسیر های بهتری وجود دارد یا خیر. دوما،PT نیاز مند اطلاعاتی در مورد جداول پیشران است به طوری که مسیر های مورد استفاده در پایین تر از آستانه عملکرد قرار می گیرند. از این روی این برنامه می تواند کشف کند که ایا جریان های خدماتی تحت تاثیر مسیر هستند یا خیر. در نهایت PT بایستی بداند که آیا SLA منطبق بر اهداف است یا خیر.

همه اطلاعات مورد نیاز توسط PT، مبتنی بر برنامه عملکردی است که به صورت حقایق مرتبط با گره های مناسب در گراف دانش در نظر گرفته می شود. برنامه FLOW مسئول جریان های فردی محدود کننده سرعت فراتر از استانه های ترافیکی پیکر بندی شده با SLA است. این برنامه مطابق با Sflow می باشد که از آن اماره های جریان را دریافت می کند و برنامه open flow م که در پهنای باند دستور برنامه را برای نصب قواعد محدود کننده سرعت ارسال می کند.

پ: مدیریت امنیت

مجموعه برنامه های ما، امنیت شبکه را مدیریت می کند: آن ها از اجزای استاندارد نظیر سیستم های تشخیص تفوذ استفاده می کند. با این حال، چون آن ها قادر به بررسی حالت کامل شبکه هستند، از جمله بررسی رفتار، به این ترتیب می توان به نگرانی های عملی حاصل از شبکه های سازمانی رسیدگی کرد.

تشخیص و پیش گیری نفوذ: ما یک برنامه snort را برای KnowNet می نویسیم که به صورت ماژول خروجی برای Snort IDS عمل می کند و حقایقی را به صورت پایگاه دانش KnowNet تولید می کند.

با هشدار های snort در KnowNet ، سایر برنامه ها قادر به استفاده از اطلاعات و ترکیب آن ها بادانش مربوط به اطلاعات می باشند. از این روی می توان تعیین کرد که هر برنامه برای تفسیر snort برای هشدار و ترکیب با دانش توپولوژی از خط مشی اپراتور شبکه استفاده می کند. ما از این اطلاعات برای رایت قواعد فایر وال مبتنی بر هاست استفاده می کنیم. در این پیاده سازی، این قوانین توسط برنامه فایروال پیاده سازی می شود.

مدیریت آسیب پذیری و کشف رویداد: برای توسعه قابلیت های دانش برنامه هایامنیتی، میتوان از فنون کشف رویداد های استنباط رویداد های پیشرفته از حقایق ذخیره شده استفاده کرد. هر کشفی نظیر این، اهمیت زیادی در شبکه سازمانی برای شرایطی دارد که از آسیب پذیری استفاده می کند. این نوع کشف رویداد به آسانی با استفاده از گراف دانش قابل پیاده سازی است. با جست و جوی روابط می توان به حقایق ساده در خصوص ذخیره دانش رسید. این مجموعه از حقایق با ویژگی های مشترک نظیر زمان و مکان فیلتر سازی می شوند. پس از فیلتر سازیف حقایق باقی مانده قادر به تعریف دقیق یک رویداد پیشرفته در گراف هستند. این شکل با یک کوئری گراف نشان داده می شود. از دیدگاه عملیاتی، مدیر می تواند این حقایق را در نظر بگیرد. هر مجموعه از ویژگی های مطابق با این رویداد ها و حقایق تعریف شده توسط اپراتور شبکه مطلوب است. در این صورت KnowNet امکان رشد دانش را می دهد زیرا دانش جدید به صورت بخشی از دانش معلوم یا شناخته شده می باشد.

ما به بررسی توانایی رشد دانش KnowNet با توسعه برنامه کشف رویداد می پردزایم.از این روی یک ورودی از حقایق وجود دارند که بر اساس کشف مبتنی بر هاست هستند و حقایق ادرس IP بسیار مطلوب است. این برنامه اندازه گیری ها و رویداد ها را با این دسته از حقایق مرتبط می سازد. وقتی که نام نویسی انجام شد، برنامه سایر پرس و جو های گراف دانش را راایه می کند که مرتبط با حقایق موجود در پنچره زمانی است. این نتایج به مدیریت رویداد کمک می کنند. ما این برنامه رادر سناریوی تشخیص نفود بحش V-B ارایه می کتین.

5- ارزیابی

برای توسعه و تست برنامه ها در قالب KnowNet ، مایک شبکه انترپرایز را در Emulb را شبیه سازی می کنیم. این شبکه شبیه سازی شده متشکل از توپولوژی هاب و اسپوگ سلسله مراتبی دو لایه ای است. سوییچینگ در نرم افزار توسط Open vSwitch انجام می شود که یگ رابط پیکر بندی غنی را ارایه می کند که از open flow پشتیبانیمی کند.

شبکه با برنامه های topology و openflow بوت استراپ می شود. سه کلاس QoS پشتیبانی می شوند و مجموعه از خدمات با کم ترین صف اولویت تنظیم می شود. از این روی برنامه مسیر یابی یک ارتباط پایه را ایجاد می کند. همه آزمایشات برنامه ها بر اساس سوییچ های دسترسی هستند و آن ها هر دو مسیر غیر خدماتی و خدماتی را شامل می شود.

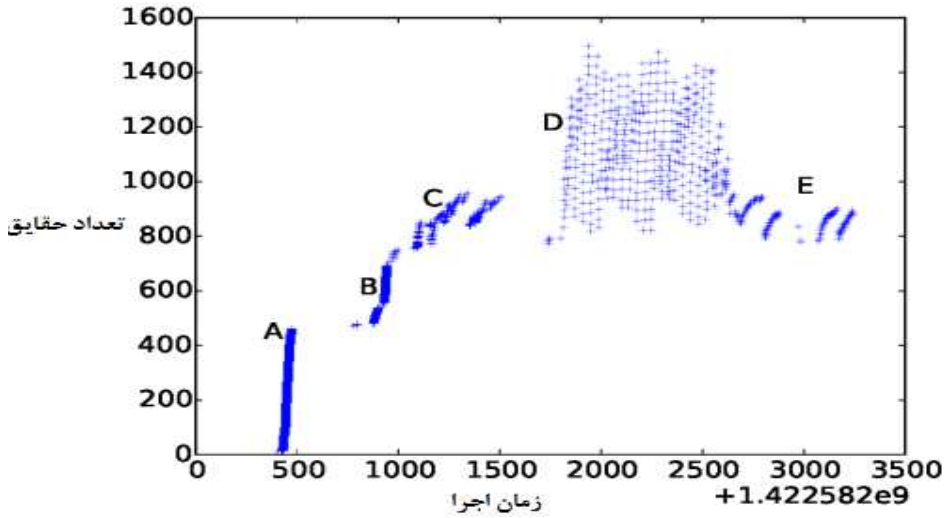
Primitive	Performance (ms)	
	Mean	Std. Dev.
Query	43	37
Subscription	52	38
Insert	0.1	0.2

جدول 1: زمان عملکرد

الف: ارزیابی عملکرد

به جز برخی از کوئری ها و اشتراکات، عملکرد به صورت قابل قبول باقی می ماند که ما داده ها را مدیریت می کنیم که نشان دهیم بیشتر اوقات، عملیات در ی چند هزارم ثانیه رخ می دهند. به خصوص برای پرس و جو ها، بدترین عملکرد با کوئری های بزرک تر رخ می دهد. با این حال بیشتر کوئری ها در برنامه ها از 4یا 5 متغیر استفاده می کنند

این معیار ها نشان می دهند که الگو های اولیه در کیلو می توانند عملکرد مناسبی در برنامه ها و شبکه های واقعی داشته باشند. این الگو به صورت نسخه ای از گراف دانش است و این نتایج نشان می دهند که مدل گراف دانش می تواند عملکرد قابل قبولی را ارایه کند



شکل 2: حقایق در سیستم به صورت تابعی از زمان اجرا

شکل 2 تعداد حقایق را در سیستم با گذشت زمان نشان می دهد و به طور کلی رفتار سیستم را باز گو می کند. در نقطه A، می توان شبکه، رابط های پیکر بندی و تفکیک اطلاعات رابط را بوت استراپ کرد. در B، ما شبکه را تتظیم می کنیم که شامل نصب و پیکر بندی OPEN FLOW نیز است. فاصله بین این حقایقAB ناشی از زمان نصب و شروع است. سپس vSwitch را باز کنید. در زمان C، ما می توانیم برنامه SNORT را پیاده سازی کنیم . این نشان می دهد که برنامه ارشیو مطابق با برنامه SNORT بوده و در این پیکر بندی استفاده می شود.در D، ما یک برنامه SFLOW را اجرا می کتیم که به طور معنی داری حقایق Sflow را جایکزین می کنیم که به نوع کنترل کمک می کند. از این روی snort هشدار هایی را در طی این دوره در d ارایه می کند. در نهایت E نشان می دهد که ما برنامه SFLOW را غیر فعال کرده و فراوانی اندازه گیری PING را روشن می کنیم. سیستم رفتار را به صورت C تثبیت می کند. این نشان دهنده و.اکنش سیستم به رفتار های شبکه ای نوسانی است.

ب:: ارزیابی کاربردی

ما مطالعات موردی را در نظر می گیریم که نشان می دهد چگونه برنامه ها در KnowNet قادر به حفظ عملکرد مطلوب شبکه تحت شرایط مختلف است.

پایش لینک و مسیر یابی انتخابی: ما توانایی برنامه ها را برای مسیر یابی انتخابی جریان های ترافیکی بر اساس سیاست شبکه در مواجهه با خطای نرم ارزیابی می کتیم. در این رابطه، ما نرخ خطای بیت را بر روی لینک نشان

می دهیم که شاخصی از خرابی تعویق است. این بسیار چالش بر انگیز است زیرا در سطح خدماتی، بسته های رد شده برای ازدحام اشتباه گرفته می شوند: همبستکی اطلاعات در سطوح مختلف برای درک عامل ریشه ای نیاز است. در این جا، برنامه لینک اطلاعیه ای را در مورد خطا های بیت بر وی لینک می دهد و نشان می دهد که خدمات از لینک استفاده می کند. یگی از سرویس ها اولویت بالایی دارند و از این روی به طور فعال برنامه LINK درخواست مسیر یابی مجدد سرویس را اطراف لینک خراب می دهد. گراف شکل 3 الف این مسیر یابی مجدد انتخابی را نشان می دهد.

تحلیل تاریخی برای مدیریت آسیب پذیری جدید: شکل 3ب ارزیابی ما را از برنامه vulnerability نشان می دهد. ما در گراف دانش نقاط را با خط چین نشان می دهیم. دو جریان در این زمان وجود دارد. برنامه vulnerability به بررسی داده های SFLOW در کراف دانش برای یک الگوی دسترسی مشترک برای گره جفاظت شده نی پردازد.برنامه های vulnerabilityایجاد یک کوئریبر اساس الگو می کند و می توان تنها جریان 1 را با الگو های دسترسی تاریخی مطابقت دهد.

حفاظت DOS:در این مثال، ما یک جریان ICMP را درون شبکه سازمانی به دلیل هاست در نظر می گیریم. اسنورت قادر به تشخیص این حملات است و ما می توانیم ترافیک را بلوکه کنیم. این دو مسئله هنوز وجود دارند1- ترافیک از طریق شبکه محلی حرکت می کند و منجر به کاهش عملکرد می شود 2- مشاهده هشدار اسنورت یک توجیه پیشرفته ای از حمله را می دهد. با استفاده از ترکیب برنامه های امنیتی، می توان KnowNet را در نظر گرفت که بر مسائل با شناسایی حمله PING با صحت بالا غلبه می کند.

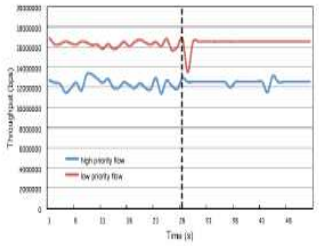
مسیر یابی جریان دانه ریز: ما یک برنامه مسیر یابی FLOW را برای پایش اماره های جریان و محدود سازی جریان فراتر از استانه های ترافیک پیکر بندی شده اجرا می کنیم. برنامه FLOW امکان استفاده از تحلیل SFLOW را می دهد. این جریان ها در کلاس های QOS قرار می گیرند که جریان خدماتی آن ها حفاظت شده است. شکل 3 پ برنامه های مطابق را با حفاظت از جریان در حدمات با اولویت بالا نشان می دهد. جریان در میانه گراف موجب شروع جریان دیگر می شود و به این ترتیب قبل از پایش برنامه می توان درخواست برنامه OPEN FLOW در محدود کننده سرعت داد.

کشف رویداد تشخیص نفوذ: برای نشان دادن اهمیت برنامه کشف رویداد، ما یک سناریو را در نظر می گیریم که در آن مدیر شبکه نگران کشف اختلالات در نرم افزار سرور در شبکه است که به نفوذی امکان دسترسی به دسترسید بالا را می دهد. به این ترتیب امکان تشخیص ارتباط از منبع ناشناخته وجود دارد و می توان تایید کرد که ایا نفوذ کننده قادر بوده است به اطلاعات دسترسی پیدا کند یا خیر. به این ترتیب به میزان اسیبپذیر به درجات نفوذ می توان رسیدگی کرد. در این صورت از برنامه nmap برای تعیین آسیب پذیری میزبان استفاده می شود. ما به ارزیابی برنامه کشف رویداد به صورت یک سناریو می پردازیم. این برنامه اصلی به کشف روابط تست شده با حقایق ادرس IP در شبکه کمک می کند و مجموعه ای از حقایق مربوط به فعالیت بدخیم را نشان می دهد.

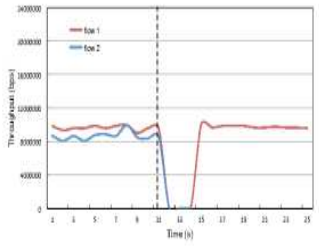
6- کارهای مربوطه

تا آن جا که می دانیم این اولین مطالعه ای است که نشان می دهد گراف دانش برای مدیریت شبکه موجب حفظ روابط بین رویداد ها و توپولوژی شبکه می شود. با این حال خود گراف دانش برای ذخیره روابط پس از استنباط آن ها استفاده می شود. و در فرایند استنباط واقعی استفاده نمی شود.

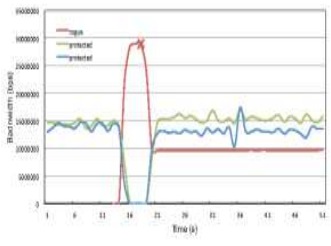
کار ما مربوط به تلاش های اخیر در مدیریت شبکه مرکز داده ها و خط مشی شبکه است. استیمن(14) بهب ررسی مجموعه ای از متغیر ها در برنامه های پیکربندی پرداخته است: از این روی امکان حفظ اینواریانت های قوی به صورت بخشی از چارچوب وجود دارد و از برنامه های ضعیف در هر یک از رابط ها پشتیبانی می کند. بر عکس KnowNet یک سری مدل هایانعطاف پذیر را از گراف شبکه ارایه می کند. امکان استفاده از ابزار های مدیریت شبکه در KnowNet وجود دارد. PGA(19) ازیک مدل گراف و خط مشی های شبکه برای ا حل اختلاف استفادهمی کند. KnowNet از رویکرد مکمل ما پیروی می کند به طوری که اطلاعات شبکه را در نظر گرفته و چارچوبی را ارایه می کند که از طریق آن می توان مدیریت شبکه را ترکیب کرد.



(a) مسیر یابی مجددجریان



(b) کنترل اسیب پذیری



(c) محدود سازی سرعت

شکل 3: الف: مسیر یابی مجدد انتخابی جریان ها در صورت خرابی نرم ب: دسترسی به گره حفاظت شده بلوکه می شود: دسترسی مشروع به الگوی احیا شده پ: برنامه ها موجب محدود شدن سرعت برنامه و حفاظت از جریان های با سرویس اولویت بالا می شود

فلو لاگ (16) یک ترکیب زمان اجرا و زبان برای مدیریت شبکه بر اساس پرو لوگ است. این به کاربران امکان دسترسی و ایجاد جداول ذخیره اطلاعات را در مورد شبکه می دهد. جداول سطح پایین به طور مستقیم در جریان OPENFLOW قرار گرفته و بر روی سوییچ ها نصب می شوند. این سیستم ها با مدیریت پیکر بندی شبکه مشابه با مجموعه ای از برنامه های شبکه سرو کار دارد/.بر عکس KNOWET امکان مدیریت شبکه را می دهد. سوفیا(9) یک برنامه اطلاعاتی توزیع شده است که اطلاعات را از تعدادی از سنسور ها جمع اوری کرده و به کار بر امکان ایجاد محرک های رایت را می دهد. این کنترل حلقه بسته در سوفیا مشابه با برنامه KNOWNET است. بر خلاف رویکرد انعطاف پذیر KNOWNET یک سری محدودیت هایی را بر برنامه ها وارد می کند، سوفیا بر اساس زبان منطق پرولوگ است که در آن هر دو سنسور ها و محرک ها با الگو های منطقی بیان می شود.

مشابه با قابلیت های کوئری ارایه شده توسط نمایش گراف دانش و اطلاعات، جست و جوی اطلاعات بر اساس زمینه بازیابی اطلاعاتو الگوی مبتنی بر جست و جوی مدیریت اطلاعات است. جست وجوی شبکه موجب محدود شدن صفحه جست و جوی بین شبکه و اپراتور می شود.

فناوری های موجود نظیر RDF، OWL و SWRL در این مرحله در نظر گرفته نمی شوند. ما به بررسی مدل مبتنی بر رابطه در ساده ترین شکل می پردازیم. با درک بهتر دانش شبکه، می توان سایر رویکرد های منطقی و توصیفی را ترکیب کمرد.

7- نتیجه گیری

KNOWNET یک چارچوب مبتنی بر گراف دانش برای نوشتن برنامه هایی است که شبکه را مدیریت می کند. گراف دانش در KNOWNET، کیلو به طور ویژه ای متناسب با حوزه مدیریت شبکه است از جمله توصیفات، داده های زمان محور و تخلیه مرجع. این الگو ها برای تسهیل شغل و کار اپراتور شبکه برای استدلال در مورد وضعیت شبکه مفید است. مااثبات کردیم که این بستر یک مبنای خوب برای توسعه طیف وسیعی از برنامه های مدیریت شبکه است. مطالعه آینده بایستی شامل کاربرد فنون یادگیری گراف دانش دیگر در حوزه مدیریت شبکه باشد.