ACoPE : An adaptive semi-supervised learning approach for complex-policy enforcement in high-bandwidth networks

Oct 2019

Computer Networks (Elsevier)

1 citation

آکوپی: راهکار یادگیری تطبیق‌پذیر نیمه‌نظارتی برای اعمال سیاستهای امنیتی پیچیده در شبکه‌های پهن باند

در شبکه‌های امروزی با توجه به نرخ بالای تولید اطلاعات و حجم زیاد ، شاهد رفتارهای متفاوت در ترافیک شبکه‌ها هستیم ، لذا نیاز به یک رویکردی داریم که در سریعترین زمان ممکن این گونه تغییرات را تشخیص دهد و امکان اجرای سیاست های امنیتی بیشتری را فراهم آورد. نیاز به یک روشی داریم که ترافیک مدام در حال تغییر شبکه را به صورت لحظه‌ای(بلادرنگ) آنالیز و وضعیت شبکه را نیز بررسی کند. علاوه بر این برای شناسایی حملات مبتنی بر الگو و منع سرویس نیز وجود همچین سرویسی نیز الزامیست. همچنین شناسایی دقیق این که هر ترافیک مربوط به چه برنامه کاربردی هست، نیز لازم هست. مدیران امنیتی برای کنترل ترافیک شبکه خط مشی‌هایی را تعریف می کنند که در حالت کلی به این صورت هستند : اگر شرایطی برقرار بود ، فلان عمل را انجام بده.روشهای قدیمی آنالیز ترافیک برای به دست آوردن وضعیت سیستم و بررسی پیش شرط خط‌مشی‌ها که بر مبنای پورت یا محتوای بسته ها (DPI) بود، درمورد ترافیک‌های رمزشده جواب نمیداد و به همین دلیل استفاده از روش‌های مبتنی بر یادگیری ماشین پیشنهاد شد که این دسته از روشها به دلیل استفاده از خصوصیات آماری ، سربار کمتری نسبت بهDPI خواهندداشت. آکوپی از ارتباط بین جریانها(که سیاست های پیچیده بر اساس آن تعریف می شوند) استفاده می کند. از یک روش آماری برای بازرسی دقت استفاده می کند(مبتنی بر یادگیری ماشین نیمه نظارتی)، و هر موقع دقت پایین آمد به معنای تغییر در ترافیک است و از یک ماژول DPI برای اصلاح شرایط استفاده می کند.

آکوپی از یک داده‌ساختار به نام متافلو برای نگه داری وضعیت ترافیک‌های اخیر شبکه استفاده می‌کند. و هر متافلو می تواند سه وضع داشته باشد :دردست‌کنترل ، اخطار و خارج از کنترل. با استفاده از روش و پردازش کنترل آماری، وضعیت ترافیک را نظارت و کنترل می‌کند. از اپلیکیشن‌هایی که توسط DPI تشخیص داده شده است به عنوان یک سنگ صحت برای بروزرسانی متافلو استفاده می کند. تمام داده‌های موردنیاز برای بررسی شرایط خط‌مشی های پیچیده را توسط تنها یک مکانیزم خطی انباشت می‌کند(خاصیت جامع بودن).همچنین جریان‌های

اخیر را توسط تکنیک DPI برچسب‌گذاری می‌کند و وضعیت ترافیک شبکه را بروز می کند.(ویژگی سازگار پذیری
)

طراحی و شیوه‌کار: آکوپی اطلاعات جریانات اخیر شبیه به هم را در یک داده‌ساختار به نام متافلو ذخیره می‌کند. همه این متافلوها همراه با برچسب مطابق شان در یک داده ساختار به نام CPR ذخیره‌شده‌اند. هر متافلو می‌تواند در یکی از این سه حالت باشد: در دست کنترل، خارج از کنترل و اخطار.هر متافلو را با یک تاپل نشان می دهیم که شامل برخی از ویژگی‌های آن هست(c, r, b, ts, ld, σ i, pi).

شیوه‌کارش به این صورت هست که اگر جریان جدیدی به نام f_{new} در لحظه t وارد شود، در ابتدا سعی میکند متافلویی که بیشترین شباهت و نزدیکی به این جریان دارد را در رابطه CPR_t پیداکند. سپس به f_{new} نیز برچسب l` که متعلق به همان متافلو هست را می‌زند. پس از آن با استفاده از ابزار های DPI برچسپ صحیح l جریان $f_{new}$ را پیدا می‌کند. و حال تفاوت بین l و l` را محاسبه می‌کند و سپس طبق این اطلاعات به دست آمده وضعیت متافلو را به روز می‌کند(در ابتدا به صورت پیشفرض وضعیت متافلو در حالت اخطار هست):

- اگر متافلو در وضعیت در دست کنترل بود، بدین معناست که جریان‌های این متافلو به هم شبیه و منطقی هستند و همان برچسپ متافلو l` را به جریان f_{new} می زند.
- اگر متافلو در وضعیت خارج از کنترل بود، متافلو را از CPR حذف می‌کند و برچسپ l را به جریان f_{new} می زند
- اگر متافلو در وضعیت اخطار بود، برچسپ l را به جریان f_{new} می‌زند و این برچسب را به آرایه l_d مربوط به متافلو اضافه می‌کند.

اگر سایز یک متافلو نیز پرشد، می‌تواند آن را با یک متافلو جدیدتر ادغام کند. درآخر نیز اگر به یک متافلو اخیراً جریانی وارد نشده‌باشد، آن را از رابطه حذف می‌کند.

ارزیابی: در ابتدا کارایی آکوپی در دسته بندی ترافیک با چند تا از الگوریتم‌های دسته‌بندی دیگر با معیار های دقت ، صحت و یادآوری بررسی شده‌است.سپس ویژگی پردازش جامع و یادگیری تطبیقی آن که برای تحلیل‌گرهای ترافیک شبکه به منظور اعمال سیاست‌های‌امنیتی لازم هست، بررسی شده‌است. سپس در سه سناریوی مختلف(از جمله شناسایی حملات منع خدمت)، توانمندی آن در مدیریت نیازمندی‌های کاربر در زمینه های متفاوت با معیارهای : میزان استفاده از پردازشگر و حافظه و تعداد کل نشست‌ها و نشست‌های دورانداخته‌شده آزمایش شده‌است . در آخر نیز در یک شبکه پهن‌باند واقعی مورد بررسی قرار گرفته‌است.

ارتباط با موضوع پروژه :

چون که این روش گفته شده یک راهکار برای دسته بندی ترافیک شبکه هست و بررسی و اجرای خط‌مشی‌های امنیتی پیچیده(که با استفاده از آنها می توانند مکانیزم های دفاعی در برابر حملات منع خدمت تعریف کرد) را فراهم می‌سازد، پس می‌توان از آن به عنوان یک روش مطمئن و کاربردی برای دسته بندی ترافیک استفاده کرد. البته باید به کمک یک روشی این سیاستهای دلخواه مان را به صورت ارتباطات میان جریانی توصیف کرد.