

عنوان مقاله:

خوشه بندی شبکه های نرم افزار محور SDN با تشخیص نفوذ چندگانه برای بهبود امنیت آن

محل انتشار:

هفتمین کنفرانس ملی و اولین کنفرانس بین المللی محاسبات توزیعی و پردازش داده های بزرگ (سال: 1401)

تعداد صفحات اصل مقاله: 9

نویسنده:

فتانه طاهری آشتیانی - مربی، گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی دانشگاه آزاد اسلامی واحد بناب، بناب

خلاصه مقاله:

امروزه نوع جدیدی از معماری شبکه های بنام شبکه های مبتنی بر نرم افزار SDN به عنوان نیاز اساسی کاربران به شمار می رود. که در آن تمامی تجهیزات شبکه تحت مدیریت، کنترل و هدایت یک یا چند سرور مرکزی می باشد. برای تامین امنیت و تشخیص ناهنجاری ها و کنترل جریان ترافیک در این شبکه ها می توان از سیستم های تشخیص نفوذ چندگانه Multiple Intrusion Detection Systems که دارای چندین سیستم تشخیص نفوذ جداگانه است استفاده کرد. این سیستم ها با ارتباط و همکاری یکدیگر ناهنجاری های ترافیک را تشخیص داده و می توانند آنرا مدیریت کنند. برای تشخیص این ناهنجاری ها، حجم ترافیک مورد پردازش بین این سیستم ها به نحوی تقسیم، خوشه بندی و مدیریت می شوند در این سیستم ها از روش های مختلفی مانند روش های آماری، داده کاوی و غیره استفاده می شود. شبکه های عصبی، درخت تصمیم، رده بندی مبتنی بر قانون از روش های داده کاوی به شمار می رود که به منظور بهبود عملکرد این سیستم ها و رفع محدودیت های روش آماری براساس قواعد استفاده شده است. که ما در این مقاله به منظور بهبود عملکرد سیستم های تشخیص نفوذ در تشخیص حملات، از روش مبتنی بر داده کاوی و در ادامه برای تشخیص حملات و جداکردن آنها، از شبکه عصبی استفاده کرده ایم تا در ابتدا حملات تشخیص داده شده، سپس مجموعه عملکرد آنها در طی یک حمله در یک گراف رسم می شود. مجموعه داده مورد استفاده در این مقاله KDD99 و شبکه عصبی مورد استفاده از نوع پیشخور می باشد که الگوریتم یادگیری آن Back Propagation است. مجموعه داده KDD99 دارای پنج کلاس Normal, Dos, Probe, و RYL است. برای آموزش شبکه عصبی و تشخیص حمله از 10 نرون در لایه مخفی استفاده شده است، که ورودی آن شامل دنباله هایی از عملکرد می باشد. نتایج نشان می دهد که در الگوریتم پیشنهادی هر چقدر ضریب Target نزدیک عدد 1 باشد نشان دهنده خوب بودن آموزش می باشد، و با پیشرفت آموزش شبکه عصبی و تصحیح وزنها خطا کاهش و دقت افزایش می یابد.

کلمات کلیدی:

سیستم تشخیص نفوذ، داده کاوی، شبکه عصبی، مجموعه داده KDD99، یادگیری عمیق

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/1453913>

