

عنوان مقاله:

ارائه یک روش ترکیبی جهت تشخیص نفوذ حملات DDOS در اینترنت اشیا

محل انتشار:

هفتمین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات (سال: 1398)

تعداد صفحات اصل مقاله: 11

نویسندگان:

امیرحسین حسنی - دانشگاه آزاد اسلامی واحد پرند

علی آذربر - دانشگاه آزاد اسلامی واحد پرند

علیرضا تقی زاده - دانشگاه آزاد اسلامی واحد پرند

خلاصه مقاله:

امروزه با رشد فناوری اطلاعات امنیت شبکه های کامپیوتری یکی از چالش های بزرگ می باشد. از این رو سیستم های تشخیص نفوذ یا IDSها در حال حاضر جزء اصلی ترین و کاملترین قسمت های یک سیستم پایش یا مانیتورینگ شبکه می باشند IDS ها فناوری های تقریباً جدیدی هستند و این نوید را به ما می دهند که به ما در جهت شناسایی نفوذ در تمامی انواع شبکه ها کمک خواهند کرد. تشخیص نفوذ در واقع فرآیندی است که در آن رویدادها و رخدادها را یک سیستم یا شبکه پایش شده و بر اساس این پایش ها وقوع نفوذ به آن شبکه با سیستم تشخیص داده می شود. یک نفوذ در واقع فعالیت یا عملی است که توسط آن محرمانگی، صحت و تمامیت و یا دسترسی پذیری به منابع دچار اختلال و یا تعرض می شود. در این پایان نامه ما یک چهارچوب کلی به منظور کشف حملات DDOS مبتنی بر روش های داده کاوی مطرح شده است. در ابتدا از دو مجموعه داده محک زنی NSL-KDD و ISCX 2012 استفاده شده است که این داده ها بدون برچسب فرض شده اند. سپس با استفاده از الگوریتم ازدحام ذرات چند هدفه انتخاب ویژگی بدون ناظر و در نتیجه کاهش بعد را خواهیم داشت. پس از کاهش بعد خوشه بندی داده ها با استفاده از الگوریتم ACO+Rough k-means انجام شده است که با تغییرات پیشنهادی عملکرد مطلوبی را به همراه داشته است. دقت حاصل شده برای خوشه بندی صحیح در روش پیشنهادی در مجموعه داده های ISCX و NSL-KDD به ترتیب برابر با 99.7 و 87 درصد بوده است که در مقایسه با روش های دیگر دقت بهتری را داشته است. در انتها نیز با استفاده از داده های برچسب خورده در مرحله خوشه بندی، سه مدل شبکه عصبی، ماشین بردار پشتیبان و درخت تصمیم آموزش دیده و تست شده اند.

کلمات کلیدی:

خوشه بندی، حملات DDOS، سیستم تشخیص نفوذ، ISCX2012، NSL-KDD

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/913343>

