عنوان مقاله:
مروری بر تشخیص نفوذ از دیدگاه مجموعه دادهها و تکنیکهای یادگیری ماشین چالشها مزایا معایب

محل انتشار:
چهاردهمین کنفرانس بین المللی فناوری اطلاعات،کامپیوتر و مخابرات (سال: 1400)

تعداد صفحات اصل مقاله: 20

نویسندگان:
شهرزاد رحیمی - *دانشجو کارشناسی ارشد، دانشکده مهندسی، دانشگاه آزاد اسلامی، واحد مشهد*

یحیی فرقانی - *استادیار، دانشکده مهندسی، دانشگاه آزاد اسلامی، واحد مشهد*

خلاصه مقاله:
با افزایش استفاده از اینترنت، حجم زیادی از اطلاعات بین دستگاه های ارتباطی مختلف رد و بدل می شود. داده ها باید بهطور ایمن بین دستگاه های ارتباطی منتقل شوند و بنابراین، امنیت شبکه یکی از حوزه های تحقیقاتی غالب برای سناریو یشبکه فعلی است. بنابراین سیستم های تشخیص نفوذ به طور گسترده همراه با مکانیسم های امنیتی دیگر مانند فایروال وکنترل دسترسی استفاده میشوند. ایدههای تحقیقاتی زیادی در رابطه با سیستم های تشخیص نفوذ با استفاده از تکنیکهاییادگیری ماشین، تکنیکهای یادگیری عمیق و الگوریت مهای گروهی و تکاملی ارائه شدهاند.این روش ها بر روی مجموعه داد ههایی مانند KDD CUP ، DARPA ۹۹ ، و NSL-KDD با استفاده از ویژگی های شبکه برای طبقه بندی انواع حمله آزمایششده اند. از سویی دیگر تکامل در سناریوهای حمله به گونه ای بوده است که یافتن سیستم های تشخیص نفوذ ک ارآمد و بهین هشبکه) NIDS (با به روز رسانی های مکرر به یک چالش بزرگ تبدیل شده است. پیاده سازی NIDS با استفاده از تکنیک هاییادگیری ماشین و مجموعه داده های نفوذ بروز شده یکی از راه حلهای مدل سازی موثر NIDS است. این مقاله شرحمختصری از مجموعه دادههای نفوذ برچس بگذاری شده در دسترس عموم و تکنیکهای ML را ارائه میکند . سپس توضی حمختصری در مورد آثار ادبی ارائه میشود که در آن تکنیکهای یادگیری ماشین برای پیادهسازی NIDS در سناریوهایشبک ههای مختلف مانند شبکههای سنتی، شبکههای ابری، WSN ، Ad-Hoc و شبکههای IoT استفاده میشوند. از این رو، اینمقاله مجموعه دادههای نفوذ در دسترس عموم و تکنیکهای یادگیری ماشینی را که در سیستمهای تشخیص نفوذ اخیر مورداستفاده قرار گرفتهاند، گرد هم میآورد تا چالشهای امروزی و مسیرهای آینده را آشکار کند . این مقاله همچنین مشکلاتمرتبط با NIDS را توضیح می دهد. این به محققان کمک میکند تا مدلهای NIDS موجود را تقویت کنند و همچنی نمدلهای موثر جدیدی را توسعه دهند.

کلمات کلیدی:
مجموعه داده نفوذ، امنیت، یادگیری ماشین، ناهنجاری