عنوان مقاله:
ارائه روشی ترکیبی مبتنی بر استخراج ویژگی عمیق و شبکه های باور عمیق برای تشخیص نفوذ سایبری و طبقه بندی حملات مبهم

محل انتشار:
چهارمین کنفرانس ملی دانش و فناوری مهندسی برق کامپیوتر و مکانیک ایران (سال: 1399)

تعداد صفحات اصل مقاله: 13

نویسندگان:
ایمان عطارزاده - *استادیار گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی ، دانشگاه آزاداسلامی واحد تهران مرکزی، تهران، ایران.*

مریم رستگارپور - *استادیار گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی ، دانشگاه آزاداسلامی واحد ساوه، ساوه، ایران.*

محمدرضا اسدزاده - *کارشناسی ارشد در رشته مهندسی فناوری اطلاعات گرایش تجارت الکترونیکی دانشگاه آزاد اسلامی واحد الکترونیک، تهران، ایران.*

خلاصه مقاله:
در دنیای امروز، امنیت شبکه های کامپیوتری از اهمیت بسیار بالایی برخوردار است. سیس‌تمهای تش‌خیص نف‌وذ مبتنی بر یادگیری ماشین قادر به شناسایی حملات ناشناخته هستند، اما مشکل روشهای موجود این است که، ب‌ا استفاده از فنون مختلف حمله، در هنگام تشخیص دچار اشتباه میشوند یا اینکه دقت تش‌خیص آنه‌ا ک‌م اس‌ت. بعلاوه، یک مهاجم که دارای دانش حیاتی در مورد یک سیستم حفاظتی است میتواند به راحتی سامانه تش‌خیص نفوذ را دور بزند. بنابراین با توجه به چالش های فراوانی که در حوزه تشخیص نفوذ وجود دارد، بررسی راهکاره‌ای جدید میتواند در راستای ارتقای سامانه های تشخیص نفوذ نقش مهمی ایفا نماید. هدف اصلی این پژوهش، بهبود دقت تشخیص نفوذ با استفاده از یادگیری عمیق است. برای این منظور، ابتدا با استفاده از فنون مهندسی ویژگ‌ی، عملیات تعریف و انتخاب ویژگی انجام شده و سپس در جهت کاهش تع‌داد ویژگیه‌ا از روش خودرمزنگ‌ار ب‌رای استخراج ویژگی استفاده شده است. در نهایت، با استفاده از طبقه‌بندیکننده باور عمیق و درخت تصمیم عملی‌ات تشخیص نفوذ و طبقه بندی انواع حملات انجام شده است. در مدل پیشنهادی، هر دو الگوریتم استخراج ویژگ‌ی و طبقه بندی باور عمیق، از ماشین بولتزمن محدود شده به‌ره برده ان‌د. ب‌رای ارزی‌ابی اثربخش‌ی روش پیش‌نهادی، مجموعه‌ای از آزمایشها انجام شده و روش پیشنهادی با روشهای شبکه عصبی، ماش‌ین ب‌ردار پش‌تیبان و ش‌بکه عصبی عمیق مورد مقایسه قرار گرفته و برای ارزیابی از معیارهای دق‌ت و فراخ‌وانی اس‌تفاده ش‌ده اس‌ت. نت‌ایج حاصل از انجام آزمایشها برتری مدل پیشنهادی را نسبت ب‌ه س‌ایر روشه‌ای م‌ورد مقایس‌ه ب‌ا می‌زان دق‌ت در تشخیص نفوذ 99.52% و معیار فراخوانی 98.58% نشان داده است.

کلمات کلیدی:
تشخیص نفوذ شبکه، خودرمزنگار، باور عمیق، طبقه بندی حملات مبهم.