عنوان مقاله:
ترکیبی از روش های تفسیر پذیر برای تشخیص حملات شبکه

محل انتشار:
نهمین کنفرانس بین المللی وب پژوهی (سال: 1402)

تعداد صفحات اصل مقاله: 9

نویسندگان:
سیدمجتبی ابطحی - *دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ، تهران ایران*

حسین رحمانی - *دانشکد ه مهندسی کامپیوتر، دانشگاه علم و صنعت ، تهران ایران*

میلاد اله قلی - *دانشکد ه مهندسی کامپیوتر، دانشگاه علم و صنعت ، تهران ایران*

سجاد علیزاده - *دانشکد ه مهندسی کامپیوتر، دانشگاه علم و صنعت ، تهران ایران*

خلاصه مقاله:
امروزه اینترنت یکی از قسمت های اصلی جامعه را تشکیل می دهد. با توجه به فراگیر بودن اینترنت ، در دسترس بودن آن یک امر ضروری به شمار می رود. از طرفی مهاجمان به دنبال از دسترس خارج کردن خدمات اینترنتی و سوءاستفاده از شرکت های خدمات اینترنتی هستند. مهاجمان از ابزارها و روشهای مختلف جهت حمله به شبکه ها و زیرساخت های شرکت های ارائه کننده خدمات استفاده می کنند. به آن حملات، ناهنجاری در ترافیک شبکه نیز گفته می شود. به طورکلی ، ناهنجارها یا حملات، رویدادهای شبکه هستند که از رفتار عادی مورد انتظار، منحرف می شوند و از نظر امنیتی مشکوک هستند. روشهای بسیار متنوعی برای شناسایی حملات در شبکه ارائه شده اند. از مهم ترین چالش های روشهای پیشین می توان به دقت پایین و عدم تفسیر پذیری۱ اشاره نمود. در این مقاله ، ما سعی نمودیم که ترکیبی از روشهای پایه را برای شناسایی حملات به کار گیریم و دقت شناسایی حملات را در مجموعه داده متوازن شده به ۸۹ درصد برسانیم . این دقت در مقایسه با کارهای پیشین ۳ درصد رشد داشته است . به منظور حل چالش تفسیر پذیری، روشهای SHAP، LIME و درخت تصمیم را اعمال نموده و ویژگی های اثرگذار در شناسایی حملات راشناسایی نمودیم . روش پیشنهادی، علاوه بر دقت و تفسیر پذیری بالا، سرعت بالاتری نسبت به روشهای پیشین دارد.

کلمات کلیدی:
تشخیص ناهنجاری، یادگیری ماشین ، داده های شبکه ، بات نت ، داده کاوی، یادگیری گروهی ، تفسیرپذیری

لینک ثابت مقاله در پایگاه سیویلیکا: