15th International Conference on
Information Technology,Computer&Telecommunication

تشخیص ترافیک ناهنجاری شبکه با استفاده از ماشین بردار پشتیبان

خالد دورقی

دانشجوی دکتری مهندسی کامپیوتر نرم افزار و الگوریتم

چکیده:

آسیب‌پذیری‌های جدید و حملات شبکه‌ای که همیشه در حال تکامل هستند، تهدیدات بزرگی برای امنیت فضای سایبری امروزی هستند. تشخیص ناهنجاری در ترافیک شبکه یک تکنیک امیدوارکننده و موثر برای افزایش امنیت شبکه است. علاوه بر تجزیه و تحلیل آماری سنتی و تکنیک‌های تشخیص مبتنی بر قانون، مدل‌های یادگیری ماشین برای تشخیص هوشمند داده‌های ترافیک غیرعادی معرفی شده‌اند. در این مقاله، روش با استفاده از ماشین بردار پشتیبان و خوشه‌بندی برای تشخیص ناهنجاری در ترافیک شبکه پیشنهاد شده است. لینک‌ها در گزارش ترافیک شبکه از طریق قوانین آماری و طرح‌ریزی خطی به بردارهای ویژگی تبدیل می‌شوند. بردارهای ویژگی بدست‌آمده به طبقه‌بندی‌کننده ماشین بردار پشتیبان وارد می‌شوند و به عنوان عادی یا غیرعادی طبقه‌بندی می‌شوند. بر اساس ایده ماشین بردار پشتیبان و خوشه‌بندی، یک مدل بهینه‌سازی برای آموزش پارامترهای روش استخراج ویژگی و طبقه‌بندی کننده ترافیک ایجاد می‌شود. تست‌های عددی نشان می‌دهند که مدل پیشنهادی در تمام مجموعه داده‌های آزمایش‌شده بهتر عمل می‌کند.

کلید واژه‌ها: ترافیک شبکه، ناهنجاری، ماشین بردار پشتیبان (SVM)، خوشه‌بندی، استخراج ویژگی