عنوان مقاله:
سیستم جدید مدیریت هشدار برای سیستمهای تشخیص نفوذ با استفاده از ماشین بردار پشتیبان

محل انتشار:
همایش ملی کاربرد سیستم های هوشمند (محاسبات نرم) در علوم و صنایع (سال: 1392)

تعداد صفحات اصل مقاله: 18

نویسندگان:
عزت مرادپور - *کارشناس ارشد مهندسی نرمافزار دانشگاه آزاد اسلامی واحد شبستر-تبریز، ایران*

سعید پارسا - *دانشیار و عضو هیات علمی دانشگاه علم و صنعت تهران*

خلاصه مقاله:
با رشد روزافزون خطرات امنیتی برای سیستمها و شبکه های کامپیوتری ابزارها و شیوه های گوناگونی برای حفاظت کردن از آنها در مقابل تهدیدات فزاینده نفوذها و حملات پیشنهاد و توسعه داده شده است که سیستمهای تشخیص نفوذ یکی از این ابزارهای دفاعی امنیتی میباشد. این سیستمها جهت ایجاد هشدار، زمانیکه عملیات غیرنرمال و سوءاستفادهای صورت میگیرد، طراحی شده است. تولید هشدارهای زیاد، بیمورد و اشتباه یکی از بزرگترین مشکلات این سیستمها بوده و باعث سختی در درک و استفاده از این هشدارها برای مدیران امنیتی میباشد. لذا ارایه سیستم جدید و بهینه مدیریت هشدارها یکی از ضروریترین مسائل در این حوزه میباشد و ارائه شیوه ها و راهکارهای مناسب برای مدیریت و دسته بندی هشدارها امری اساسی در زمینه مدیریت هشدار میباشد. در این مقاله سیستم جدید مدیریت هشدار با تمرکز بر دسته بندی مناسب هشدارها ارائه شده است که مشکل سر و کار داشتن با مقدار زیادی از هشدارها را حل میکند. این سیستم جدید، هشدارها را با استفاده از ماشین بردار پشتیبان دسته بندی مینماید. نتایج پیاده سازی سیستم جدید نشان میدهد که این سیستم در مقایسه با سیستمهای مشابه که با راهکارهای دیگری هشدارها را دسته بندی میکنند، میزان هشدارهای اشتباه را بسیار کاهش داده و دسته بندی هشدارها با صحت، دقت و سرعت بالا انجام میگیرد. مزیت دیگر این سیستم، قابلیت استفاده فعال در سیستمهای تشخیص نفوذ میباشد.

کلمات کلیدی:
سیستم تشخیص نفوذ، مدیریت هشدار ، ماشین بردار پشتیبان