عنوان مقاله:
ارائه یک روش جدید و ترکیبی برای وارسی هشدارها در سیستم های همبسته ساز

محل انتشار:
بیستمین کنفرانس مهندسی برق ایران (سال: 1391)

تعداد صفحات اصل مقاله: 6

نویسندگان:
سیدفخرالدین نوربهبهانی - *دانشگاه صنعتی اصفهان، دانشکده مهندسی برق و کامپیوتر، مرکز تخصصی آپا*

سیدرسول موسوی - *دانشگاه صنعتی اصفهان*

خلاصه مقاله:
امروزه سیستم های تشخیص نفوذ اهمیت فوق العاده ای در تامین امنیت رایانه ها و شبکه های رایانه ای بر عهده دارند. سیست مهای همبسته ساز در کنار سیستم های تشخیص نفوذ قرار گرفته و با تحلیل و ترکیب هشدار های دریافتی از آن ها گزارش های مناسب برای بررسی وانجام اقدامات امنیتی تولید می نمایند. یکی از مشکلاتی که سیستم های تشخیص نفوذ با آن روبرو هستند، تولید حجم زیادی از هشدارهای غلط است. بنابراین یکی از مهمترین مسائل در سیستم های همبسته ساز، وارسی هشدارهای دریافت شده از سیستم تشخیص نفوذ به منظور تشخیص هشدارهای مثبت کاذب از هشدار های مثبت صحیح می باشد . در این مقاله یک روش جدید و ترکیبی برای وارسی هشدارها با استفاده از قوانین انجمنی، خوشه بندی و دسته بندی ارائه شده است. تمرکز اصلی این پژوهش بر روی بهین هسازی روش دسته بندیK نزدیکترین همسایه به منظور استفاده در وارسی هشدارها می باشد. روش ارائه شده روی یک مجموعه داده تست معتبر آزمایش شده و نتایج حاصل بیانگر کارایی مطلوب روش بهینه سازی دسته بندیK نزدیکترین همسایه و به تبع آن دقت بالای روش وارسی پیشنهادی می باشد

کلمات کلیدی:
انتخاب ویژگی، خوشه بندی، دسته بندی ، وارسی هشدار، همبسته سازی هشدار