عنوان مقاله:
بهبود عملکرد سیستم تشخیص نفوذ با استفاده از تکنیک ماشین بردار پشتیبان

محل انتشار:
کنفرانس بین المللی پژوهش های کاربردی در فناوری اطلاعات، کامپیوتر ومخابرات (سال: 1394)

تعداد صفحات اصل مقاله: 18

نویسندگان:
حسن سمیعی درونه - *دانشگاه آزاد کرمان، دانشجوی کارشناسی ارشد، مهندسی فناوری اطلاعات*

حمید میروزیری - *عضو هیئت علمی گروه کامپیوتر دانشگاه شهید باهنر کرمان ، دانشگاه آزاد اسلامی ،کرمان*

خلاصه مقاله:
امروزه امنیت شبکه و اطمینان از ارتباط امن، بر بستر شبکه از اهمیت بیشتری برخوردار می باشد. لذا برای حفاظت از اطلاعاتحساس لازم است از روش های تشخیص نفوذ برای شناسایی و پیشگیری از حمله استفاده شود. هدف ما ارائه روشی جهتتشخیص و دسته بندی نفوذ به شبکه با استفاده از تکنیک ماشین بردار پشتیبان می باشد. استخراج ویژگی ها بخش کلیدی ازیک سیستم تشخیص نفوذ است که می توانیم با استفاده از آن حالات سیستم را توصیف نماییم، در اینجا از مجموعه داده هایNSL-KDDCPP استفاده شده است. برای تامین هدف اصلی سیستم تشخیص نفوذ، فعالیت های سیستم بوسیله تکنیکماشین بردار پشتیبان به دو دسته عادی و غیر عادی (حمله شده) برای تشخیص نفوذ دسته بندی شده و در تصمیم گیری نهاییوع نفوذ مشخص گردید. پس از اینکه نفوذ شناسایی شد، ما با استفاده از تکنیک ماشین بردار پشتیبان حملات را بر اساسویژگی های آن در چهار دسته مختلف قرار خواهیم داد. الف) حملات DOS ، ب) حملات U2R ج) حملات R2L د)حملات PROBE

کلمات کلیدی:
ماشین بردار پشتیبان، سیستم های تشخیص نفود، دسته بندی، دیتاست NSL-KDD