

عنوان مقاله:

شناسایی نفوذ در شبکه های کامپیوتری بر اساس ایده ای مبتنی بر شناسایی جرم در جوامع انسانی

محل انتشار:

پانزدهمین کنفرانس مهندسی برق ایران (سال: 1386)

تعداد صفحات اصل مقاله: 6

نویسندگان:

حمیدرضا شجاع مودب - پژوهشگر پردازش هوشمند علائم، دانشکده مهندسی کامپیوتر و فناوری اطل

محمد مهدی همایونپور - پژوهشگر پردازش هوشمند علائم، دانشکده مهندسی کامپیوتر و فناوری اطل

مهدی شجری - پژوهشگر پردازش هوشمند علائم، دانشکده مهندسی کامپیوتر و فناوری اطل

خلاصه مقاله:

در این مقاله ما اقدام به معرفی مدلی برای تشخیص نفوذ در شبکه های کامپیوتری می کنیم که بر اساس ایده ای مبتنی بر اصول اولیه برای جرمشناسی در جوامع انسانی می باشد. اصل اول اصل برائت است و اصل دوم اصل تصریح مجرمانه بودن یک عمل در قانون می باشد. که اصل دوم عملا از اصل اول حاصل می شود. ضمنا ناهنجاری های که وقوع آنها در جامعه مسبوق به سابقه نبوده و جدیداً رخ داده در صورتیکه برای جامعه مضر باشند با یک رویه قانونی به عنوان جرم معرفی می شوند که از این فرایند نیز ما در مدل پیشنهادی ایده گرفته ایم. برای پیاده سازی مدل مورد بحث از ماشین بردار پشتیبان که یک طبقه بندی کننده تمایزی است استفاده کردیم لیکن می توان از هر طبقه بندی کننده یا ابزار دیگری نیز به این منظور استفاده کرد و مدل پیشنهادی مستقل از ابزار مورد استفاده برای پیاده سازی است. نتایج آزمایشات بر روی پایگاه تهیه شده بوسیله برنامه ارزیابی تشخیص نفوذ DARPA نشان داد که روش پیشنهادی در شناسایی نفوذ توانایی بیشتری نسبت به بسیاری از روشهای تشخیص نفوذ دارد.

کلمات کلیدی:

شبکه های کامپیوتری ، تشخیص نفوذ ، فرضهای جرمشناسی ، ماشین بردار پشتیبان

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/25350>

