عنوان مقاله:
راهکاری نوین جهت تشخیص نفوذ در شبکه های کامپیوتری به عنوان یک مساله نامتوازن

محل انتشار:
اولین کنفرانس بین المللی دستاوردهای نوین پژوهشی در مهندسی برق و کامپیوتر (سال: 1395)

تعداد صفحات اصل مقاله: 12

نویسندگان:
مجتبی رفعت - *کارشناس ارشد مهندسی فناوری اطلاعات دانشگاه شیراز*

منصور ذوالقدری جهرمی - *استاد، بخش مهندسی کامپیوتر، دانشکده برق و کامپیوتر، دانشگاه شیراز*

فاطمه پیرمرادیان - *کارشناس ارشد مهندسی فناوری اطلاعات دانشگاه شیراز*

خلاصه مقاله:
یکی از چالش های اصلی در مدیریت شبکه های پرسرعت و بزرگ تشخیص ناهنجاری های شبکه است که اینچالش منجر به طراحی سیستم های تشخیص نفوذ شده است. در سیستم های تشخیص نفوذ روشهای سواستفاده/ امضاروش هایی هستند که تشخیص نفوذ را با تطبیق یک نمونه با الگوهای نرمال و ناهنجار انجام میدهند و جز مسائل دسته-بندی محسوب می شوند. در سیستم های تشخیص نفوذ بر پایه امضاء بطور معمول از یک الگوریتم دسته بندی جهتتشخیص مهاجم استفاده میشود. الگوریتم نزدیکترین همسایه از روش های مطرح و پر کاربرد دسته بندی و انتخاب مناسبیبرای یک سیستم تشخیص نفوذ بر پایه امضاء می باشد. در یک سیستم تشخیص نفوذ با یک مجموعه داده نامتوازن روبروهستیم بطوریکه تعداد الگوهای کاربران عادی بسیار بیشتر از الگوهای مهاجمان می باشد. در این مقاله یک الگوریتمیادگیری نوین برای بهبود کارایی الگوریتم نزدیکترین همسایه در کاربرد تشخیص نفوذ، به عنوان یک مساله نامتوازنپیشنهاد شده است.

کلمات کلیدی:
سیستم تشخیص نفوذ، دسته بندی، نزدیکترین همسایه، داده های نامتوازن