عنوان مقاله:
کاهش نرخ خطای تشخیص نفوذ با استفاده از الگوریتم ژنتیک

محل انتشار:
اولین کنگره سراسری فناوریهای نوین ایران با هدف دستیابی به توسعه پایدار (سال: 1393)

تعداد صفحات اصل مقاله: 9

نویسندگان:
محبوبه جهازی - *دانشجوی کارشناسی ارشد مهندسی کامپیوتر-نرم افزارموسسه غیرانتفاعی میرداماد گرگان*

علی اکبر تجری سیامرزکوه - *دانشجوی دکتری علوم کامپیوتر دانشگاه تبریز*

خلاصه مقاله:
یکی از روش های اصلی برای رفع نفوذ سیستم های کامپیوتری،سیستمهای تشخیص نفوذ است روش های مختلفی ارائه شده است از جمله شبکه های عصبی،سیستم ایمنی بدن،الگوریتم ژنتیک و برنامه نویسی ژنتیک.هدف از تشخیصنفوذ نمایش، بررسی و ارائه گزارش از فعالیت شبکه است. به دلیل وجود محدودیت های اطمینان پذیری و تهدیدهای داخلی پیش گیری از نفوذ باید به بعضی از موارد مشکوک به حمله اجازه عبور دهد تا احتمال تشخیص های غلط (false positive) کاهش یابد. از طرف دیگر، روش هایIDSبا هوشمندی همراه هستند و از تکنیک های مختلفی برای تشخیص حملات بالقوه، نفوذها و سوء استفاده ها بهره می گیرند. یکIDSمعمولاً به گونه ای از پهنای باند استفاده می کند که می تواند بدون تأثیر گذاشتن روی معماری های محاسباتی و شبکه ای به کار خود ادامه دهد. تشخیص نفوذ با جستجو در مجموعه ای از فعالیت های کاربرشناسایی میشود. از آنجایی که این جستجوNP-completeاست نیاز به پایگاه داده ای از حوادث و حملات انجام شده دارد.الگوریتم ژنتیک میتواند اکتشافی مناسب با ارائه روش جستجو باشد.تابع مورد نظر در الگوریتم ژنتیک که تابع برازش نام دارد کمک می کند تاIDSبه طور قابل توجهی کاهش یابد

کلمات کلیدی:
الگوریتم ژنتیک،تشخیص نفوذ،سیستم های تشخیص نفوذ، شبکه، امنیت