عنوان مقاله:
تشخیص نفوذ در شبکه های کامپیوتری به کمک الگوریتم ژنتیک

محل انتشار:
اولین همایش ملی پژوهش های مهندسی رایانه (سال: 1393)

تعداد صفحات اصل مقاله: 13

نویسنده:
هدی پوررجبی - *کارشناس ارشد مهندسی فناوری اطلاعات , دانشگاه شیراز*

خلاصه مقاله:
سیستم تشخیص نفوذ یک سیستم محافظتی است که خرابکاری های در حال وقوع در شبکه را شناسایی می کند. در این سیستم ها بااستفاده اطلاعاتی مانند پویش پورتها و تشخیص ترافی غیر متعارف، نفوذخرابکاری ها را می توان کشف و به مسئول شبکه گزارش داد. برایآنکه سیستم های تشخیص نفوذ قدرت کشف و تشخیص نفوذهای از قبل تعریف نشده را داشته باشند، به نوعیهوشمندی نیاز دارند. در اینحالت، این سیستم ها قابلیت یادگیری دارند و می توانند بر روی بسته های وارد شده به شبکه تحلیل انجام داده و کاربران عادی و غیر عادی را تشخیص دهند. روش های هوشمند متداول شامل شبکه های عصبی؛ منطق فازی؛ تکنی های داده کاوی و الگوریتم های ژنتیک می باشند. در این مقاله با تشریح الگوریتم ژنتی و ارتباط ان با سیستم های تشخیص نفوذ، پیاده سازی این سیسکتم هکا را به کمک الگوریتم ژنتیک بیان شده و مکانیزم هایی به منظور بهبود عملکرد سیستم های تشخیص نفوذ توسط این الگوریتم بیان می گردد. علاوه بر این مکانیزم ها الگوریتم تطبیقRBNDMبا استفاده از مجموعه دادهKDD99ارزیابی می شود. این آزمایش نشان می دهد که این مدل می تواند نرخ مثبت و واقعیIDSارا افزایش دهد.

کلمات کلیدی:
امنیت شبکه های کامپیوتری، سیستم های تشخیص نفوذ، الگوریتم ژنتیک ، KDD99