عنوان مقاله:
تشخیص نفوذ در شبکه های رایانه ای با استفاده از درخت تصمیم و کاهش ویژگی ها

محل انتشار:
فصلنامه پدافند الکترونیکی و سایبری, دوره 9, شماره 3 (سال: 1400)

تعداد صفحات اصل مقاله: 11

نویسنده:
علی اکبر تجری سیاه مرزکوه - *استادیار دانشگاه دولتی گلستان ،گرگان گروه علوم کامپیوتر*

خلاصه مقاله:
امروزه نیاز به سیستم‌های تشخیص نفوذ مبتنی بر ناهنجاری به دلیل ظهور حملات جدید و افزایش سرعت اینترنت بیشتر از قبل احساس می شود. معیار اصلی برای تعیین اعتبار یک سیستم تشخیص نفوذ کارآمد، تشخیص حملات با دقت بالا است. سیستم‌های موجود علاوه بر ناتوانی در مدیریت رو به رشدحملات،دارای نرخ‌های بالای تشخیص مثبت و منفی نادرست نیز می‌باشند. در این مقاله از ویژگی-هایدرخت تصمیمID۳ برای سیستم‌های تشخیص نفوذ مبتنی بر ناهنجاری استفاده می‌شود. همچنین از دو روش انتخاب ویژگی برای کاهش میزان داده‌های استفاده شده برای تشخیص و دسته‌بندی استفاده می‌شود. برای ارزیابی الگوریتم پیشنهادی از مجموعه داده KDD Cup۹۹ استفاده شده است. نتایج آزمایش نشان دهنده میزان دقت تشخیص برای حملهDoS به میزان۸۹/۹۹% و به طورمیانگین میزان دقت ۶۵/۹۴% برای کلیه حملات با استفاده از درخت تصمیم است که بیانگر مقادیر بهتر نسبت به کارهای قبلی است.

کلمات کلیدی:
تشخیص نفوذ, درخت تصمیم, خوشه بندی k-means, حمله ی DoS, مجموعه داده KDD Cup۹۹