عنوان مقاله:
تشخیص هجوم در شبکه بر اساس ترکیبی از الگوریتم های میانگین و خوشه بندی

محل انتشار:
اولین کنفرانس ملی دانش پژوهان کامپیوتر و فناوری اطلاعات (سال: 1390)

تعداد صفحات اصل مقاله: 8

نویسندگان:
توماج پورایراندوست - *دانشگاه آزاد اسلامی زنجان-گروه کامپیوتر*

آیاز عیسی زاده - *دانشگاه تبریز-گروه علوم کامپیوتر*

احمد حیدری - *دانشگاه آزاد اسلامی زنجان-گروه کامپیوتر*

خلاصه مقاله:
اخیرا روشهای داده کاوی توجه زیادی را در موضوعات امنیت شبکه مانند تشخیص تحاجم به خود جلب کرده اند . سیستمهای تشخیص تحاجم ، قصد شناسایی حملات با نرخ تشخیصی بالا و نرخ اعلام نادرست پایینی را دارند. روشهای داده کاوی مبتنی بر دسته بندی برای تشخیص تهاجم ، اغلب در رویارویی با تغییرات پویا در ویژگی ها و الگوهای تشخیص ناکارآمد هستند. ار طرف روشهای آموزش غیر نظارتی ، کارایی بهتر در تشخیص حملات جدید دارند. در این مقاله ما ترکیبی از الگوریتم خوشه بندی با کاهش بر مبنای میانگین را به عنوان یم تکنین غیرنظارتی معرفی می کنیم. سیستم پیشنهادی ما ، ایتدا درصدی از داده ممیزی ترافیک شبکه را بر اساس میانگین روی فضاهای نرمال 0و1 و استاندارد بعنوان نمونه های بدیهی از رفتارهای نرمال و حملات حذف می کند. سپس خوشه بندی را بطور موثرتر روی نمونه های باقیمانده انجام می دهد . نتایج آزمایشی روی مجموعه داده تهیه شده از DARPA1999 نشان می دهد که تکنیک پیشنهادی ما ، زمان اجرای بسیار کمتر ، نرخ تشخیص بالاتر و اعلام نادرست پایین تری نسبت به تکنیک های غیرنظارتی مبتنی بر هوشه بندی پیشین دارد.

کلمات کلیدی:
تشخیص تهاخم ، داده کاوی ، خوشه بندی ، نرخ تشخیص ، نرخ اعلام نادرست