عنوان مقاله:
بهبود الگوریتم K-Means برای سیستم های تشخیص نفوذ دارای ویژگی های اسمی و پیوسته

محل انتشار:
هفتمین کنفرانس ملی و اولین کنفرانس بین المللی مدیریت دانش (سال: 1394)

تعداد صفحات اصل مقاله: 10

نویسندگان:
سیدوحید فرهی - *دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات شبکه، دانشگاه صنعتی شیراز، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، ایران*

محمدمهدی معصومی - *دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات شبکه، دانشگاه صنعتی شیراز، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، ایران*

مرضیه احمدزاده - *دکتری مهندسی نرم افزار، دانشگاه صنعتی شیراز، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، ایران*

خلاصه مقاله:
با گسترش شبکه جهانی اینترنت و ارتباط شبکه های کامپیوتری با دنیای خارج، برقراری امنیت از مسائل اصلی شبکه های کامپیوتری می باشد. سیستم های تشخیص نفوذ در خط دوم دفاع سعی دارند تهدیدهای امنیتی را تشخیص دهند. الگوریتم های خوشه بندی یکی از روش های مهم استخراج دانش از مجموعه داده ها می باشد. الگوریتم K-Means یکی از الگوریتم های خوشه بندی است که می تواند در سیستم های تشخیصنفوذ و استخراج و کشف دانش بسیار مفید باشد. تا کنون این الگوریتم در تحقیقات بسیاری مورد استفاده قرار گرفته است. اما توجه به این نکته الزامی است که این الگوریتم برای مجموعه داده هایی که فقط شامل ویژگی -های پیوسته هستند مطرح است و بر اساس فاصله هندسی کار می کند. مجموعه داده ها در سیستم های تشخیص نفوذ علاوه بر ویژگی های پیوسته شامل ویژگی های اسمی نیز می باشند. تا کنون در سیستم های تشخیص نفوذ این مساله مورد توجه قرار نگرفته که مجموعه داده های مورد استفاده در سیستم های تشخیص نفوذ شامل ترکیبی از ویژگی های پیوسته و اسمی هستند. در این پژوهش الگوریتم خوشه بندی K-Means با توجه به این مساله که مجموعه داده ها در سیستم های تشخیص نفوذ دارای ترکیبی)پیوسته و اسمی(از ویژگی ها هستند توسعه داده شده است.

کلمات کلیدی:
سیستم های تشخیص نفوذ، خوشه بندی، ویژگی های ترکیبی، بهبود K-Means ،داده کاوی