عنوان مقاله:
بهبود تشخیص نفوذ براساس کاهش ویژگی و با استفاده از دادهکاوی

محل انتشار:
هفتمین کنفرانس انجمن رمز ایران (سال: 1389)

تعداد صفحات اصل مقاله: 7

نویسندگان:
مریم معدنی پور - *تهران، دانشگاه صنعتی مالک اشتر، مجتمع پژوهشی فناوری اطلاعات، ارتباط*

حسن ابوالحسنی - *تهران، دانشگاه صنعتی شریف، دانشکده مهندسی کامپیوتر*

حسین شیرازی - *تهران، دانشگاه صنعتی مالک اشتر، مجتمع پژوهشی فناوری اطلاعات، ارتباط*

خلاصه مقاله:
در سیستمهای تشخیص نفوذ، با دادههای حجیم برای تحلیل مواجه هستند. بررسی مجموعه داده سیستمهای تشخیص نفوذ نشان میدهد که بسیاری از ویژگیها، ویژگیهای غیرمفید، بیتاثیر در سناریوهای حمله و یا ویژگیهای نامربوط هستند. بنابراین حذف ویژگیهای نامناسب از مجموعه ویژگی، به عنوان یک راهکار مناسب برای کاهش مجموعه داده سیستمهای تشخیص نفوذ معرفی میشود.نیازمندی دیگری که در سیستمهای تشخیص نفوذ مطرح میباشد، دانستن مجموعه ویژگی بهینه برای هر نوع حمله است. چرا که دراینصورت، سیستم تشخیص نفوذ قادر خواهد بود برای تشخیص هر نوع حمله، تنها از مجموعه ویژگی متناسب با آن حمله استفاده کند.در این تحقیق، روشی ارائه میشود که قادر است تمام نیازمندیهای فوق را پاسخگو باشد، علاوه براین، این روش نحوه ارتباط بین ویژگیها را برای تحلیل بهتر آنها نشان میدهد. روش پیشنهادی از مفاهیم دادهکاوی و تحلیل شبکههای اجتماعی استفاده مینماید

کلمات کلیدی:
کاهش ویژگی، انتخاب ویژگی، سیستمهای تشخیص نفوذ، دادهکاوی، تحلیل شبکههای اجتماعی