پایان‌نامه‌ی کارشناسی ارشد: نرگس اندیشمند، ۱۳۹۷

استفاده از کلاس بندی ترکیبی برای تشخیص نفوذ به شبکه

هم زمان با رشد شبکه‌های کامپیوتری، حملات و نفوذ به آنها نیز افزایش چشمگیری داشته است. واضح است که امروزه اقدامات و ابزارهای امنیتی اولیه مانند دیواره آتش یا ضد ویروس‌ها برای فراهم کردن سطح مناسبی از امنیت شبکه‌های سازمانی و همچنین جلوگیری از کاربران مخرب که به داخل سیستم‌ها نفوذ می‌کنند، به اندازه کافی کارآمد نیستند.یکی از راه‌حل‌ها در جلوگیری از نفوذ و کم‌کردن فعالیت‌های مخرب، توسط سیستم‌های تشخیص نفوذ شبکه فراهم می‌شود. در پایان نامه حال حاضر، با توجه به اطلاعات ورود کاربران در شبکه و نیز احتمال نفوذ آنها در سیستم‌های پردازشی، راهکاری موسوم به روش تشخیص نفوذ خودکار پیشنهاد شده که از مجموعه راهبردهای یادگیری ماشین در شناسایی استفاده می‌کند. مجموعه الگوریتم یکپارچه متشکل از پیش پردازش داده‌ها، انتخاب ویژگی و طبقه‌بندی به روش ترکیبی است. در مرحله پیش پردازش، مقادیر از دست رفته بازیابی می‌شوند، هنجارسازی داده‌ها صورت می‌پذیرد و جهت دستیابی به بایاس مطمئن از خروجی و افزایش سطح ثبات، خوشه‌بندی به روش بیشینه امید ریاضی پیاده‌سازی می‌گردد. در گام بعدی، توسط الگوریتم تکاملی ازدحام ذرات از ابعاد بردار ویژگی‌ها کاسته می‌شود تا دقت تشخیص نفوذ افزایش یابد و سطح پردازش اطلاعات کمتر شود. طبقه‌بند ترکیبی، روشی است مرکب از سه الگوریتم شبکه عصبی مدل تغذیه شونده رو به جلو، مدل احتمالاتی و مدل آبشاری که از طریق هم‌بندی رای‌گیری، نتایج با یکدیگر ترکیب می‌شوند. داده‌های نمونه، زیرمجموعه‌ای 40000 عضوی از داده‌های تشخیص نفوذ KDD99 است که از UCI دریافت شده و شامل 42 ویژگی مجزاست. نتایج حاصل از پیاده‌سازی الگوریتم حاکی از دستیابی به دقت بالاتر از 98/5% است و تا حد چشمگیری بروز خطاهای مثبت در تشخیص مرتفع گردیده است. با تکرار آزمایش، میزان پراکندگی در میان پاسخ‌های مرحله پیش‌بینی کمینه بوده که نشان از حل مسئله عدم قطعیت دارد. پیشنهاد آن است که مجموعه راهکار پیشنهادی به واسطه انتخاب ویژگی و هم‌بندی در طبقه‌بندی به عنوان ابزار تشخیص نفوذ استفاده گردد

کلیدواژه‌ها: تشخیص نفوذ، پیش پردازش، خوشه‌بندی، انتخاب ویژگی و طبقه‌بند هم‌بندی شده

شماره‌ی پایان‌نامه: ۱۲۷۴۱۰۰۶۹۵۱۰۰۷
تاریخ دفاع: ۱۳۹۷/۰۳/۰۹
رشته‌ی تحصیلی: مهندسی کامپیوتر- نرم افزار
دانشکده: فنی و مهندسی
استاد راهنما: مهندس حسام حسن‌پور
استاد مشاور: مهندس یاسر علمی‌سولا

M.A. Thesis:

Using ensemble classification for network intrusion detection

The growth of computer networks has been concomitant with a dramatic rise in computer attacks and intrusion. It is clear that today's basic security measures such as firewalls or anti-virus are not sufficiently effective in providing a decent level of security for organizational networks, and in preventing the infiltration of malicious users in the system.
One way to preclude the intrusion and mitigate malicious activity is using network intrusion detection systems. In this paper, based on input data of user in the network and the possibility of their infiltration on the processing systems, a solution called the auto-infiltration detection method is proposed that employs a set of machine learning strategies for identification. An integrated algorithm set consists of data pre-processing, feature selection, and ensembling classification. In the pre-processing stage, the lost values are recovered, data are normalized, and to achieve a reliable bias of the output and increase the stability level, the clustering is implemented using the Expectation-Maximization (EM) method.
In the next step, the particle swarm optimization algorithm is utilized to reduce the dimensions of the feature vector in order to enhance the accuracy of intrusion detection and reduce the processing level of information. Ensemble learning is a method composed of three algorithms of Feed Foeward neural network (FFNN), Probabilistic neural network (PNN) model, and Cascade-forward neural network (CFNN) model that combine the results through Voting learning. Sample data is a 40000-connection subset of the KDD99 infiltration detection data received from the UCI that contains 42 distinct features. The results of algorithm implementation indicated an accuracy of above 98.5% as well as significant improvement of false positive in diagnosis. By repeating the experiment, the dispersion rate of responses in the predictive stage was minimal, indicating that the uncertainty was resolved.
It is suggested that the proposed set of solutions be used as an intrusion detection tool by selecting the attribute and classification bonding as the infiltration detection device