عنوان فارسی مقاله:
رویکردی نوین برای شناسایی نفوذ با استفاده از شبکه‌های عصبی مصنوعی و خوشه‌بندی فازی

عنوان انگلیسی مقاله:
A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering

توجه!
این فایل تنها قسمتی از ترجمه می‌باشد. برای تهیه مقاله ترجمه شده کامل با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، اینجا کلیک نمایید.
5. Conclusions and future directions

Prevention of security breaches completely using the existing security technologies is unrealistic. As a result, intrusion detection is an important component in network security. IDS offers the potential advantages of reducing the manpower needed in monitoring, increasing detection efficiency, providing data that would otherwise not be available, helping the information security community learn about new vulnerabilities and providing legal evidence.

In this paper, we propose a new intrusion detection approach, called FC-ANN, based on ANN and fuzzy clustering. Through fuzzy clustering technique, the heterogeneous training set is divided to several homogenous subsets. Thus complexity of each sub training set is reduced and consequently the detection performance is increased. The experimental results using the KDD CUP 1999 dataset demonstrates the effectiveness of our new approach especially for low-frequent attacks, i.e., R2L and U2R attacks in terms of detection precision and detection stability. In future research, how to determine the appropriate number of clustering remains an open problem. Moreover, other data mining techniques, such as support vector machine, evolutionary computing, outlier detection, may be introduced into IDS. Comparisons of various data mining techniques will provide clues for constructing more effective hybrid ANN for detection intrusions.

To conclude, we have proposed a new intrusion detection approach, called FC-ANN, based on ANN and fuzzy clustering. The experimental results using the KDD CUP 1999 dataset demonstrate the effectiveness of our approach especially for low-frequent attacks. In future research, determination of the appropriate number of clustering remains an open problem. Moreover, other data mining techniques, such as support vector machine, evolutionary computing, outlier detection, may be introduced into IDS. Comparisons of various data mining techniques will provide clues for constructing more effective hybrid ANN for detection intrusions.