عنوان مقاله:

An efficient modeling algorithm for intrusion detection systems using C5.0 and Bayesian Network structures

محل انتشار:

نویسندگان:

Fariba Younes Nia - *M. S. Student, dept. Computer and Informatics Eng. Payame Noor University Tehran, Iran*

Mehdi Khalili - *Assistant Professor, dept. Computer and Informatics Eng. Payame Noor University Tehran, Iran*

خلاصه مقاله:

although different models have been offered for intrusion detection systems (IDSs) in computer networks, it is difficult to distinct unauthorized connections from authorized ones because intruders act similar to normal users. In this paper we propose an efficient modeling algorithm for applying in IDSs to improve the quality of detections. In the proposed algorithm, the integration of Tree Augmented Naïve Bayes (TAN) in Bayesian Network (BN) and Boosting in C5.0 decision tree structures are used to take their advantages and avoid their weaknesses. These structures are adopted once individually. Then the agreements of their combination are considered. In addition, in implementation process, the KDDCUP'99 data set and the other widely-used measures in IDSs problem are used. The experimental results show that the proposed algorithm not only achieves satisfactory results in accuracy and false alarm rate, but also improves the existing works.

کلمات کلیدی:

intrusion detection systems; C5.0 decision tree; Bayesian Network; models integration; tree augmented naive bayes; boosting method

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/553144