ADDING EXPERT KNOWLEDGE TO TAN-BASED INTRUSION DETECTION SYSTEMS

S. Benferhat
CRIL-CNRS, Faculté Jean Perrin, Rue Jean Souvraz
Lens, France

A. Boudjelida, H. Drias
Institut National d'Informatique (INI), Alger, Algérie

Keywords: Intrusion detection, TAN.

Abstract: Bayesian networks are important knowledge representation tools for handling uncertain pieces of information. The success of these models is strongly related to their capacity to represent and handle (in)dependence relations. A simple form of Bayesian networks, called naive Bayes has been successively applied in many classification tasks. In particular, naive Bayes have been used for intrusion detection. Unfortunately, naive Bayes are based on a strong independence assumption that limits its application scope. This paper considers the well-known Tree Augmented Naïve Bayes (TAN) classifiers in the context of intrusion detection. In particular, we study how additional expert information such that "it is expected that 80% of traffic will be normal" can be integrated in classification tasks. Experimental results show that our approach improves existing results.

1 INTRODUCTION

Intrusion detection is an essential part of a complete security policy in information systems. Its function consists in analyzing information collected by security audit mechanisms in order to find possible attacks. Two main approaches are used to seek intrusions trace: Misuse detection and Anomaly detection.

Misuse detection approach uses attacks signatures knowledge. These systems are very precise to detect known attacks. Though, their detection capacities are limited to attacks which appear in their signatures data base. Thus, continuous updates are required each time new attacks are discovered.

Anomaly detection systems adopt an opposed approach. It first defines a profile for normal traffic, then checks deviations from this normal behaviour. Thus, attacks, including new ones, are detected when they deviate from the normal profile. However, attacks having a profile close or similar to the normal one can not be detected. Then often legitimate users change their manners, the normal behaviour should be redefined.

IDS have three common problems: temporal complexity, correctness and adaptability. The temporal complexity problem results from the extensive quantity of data that the system must supervise in order to perceive whole situation.

Positive false rate and negative false rate are usually used to evaluate the correctness of IDS. Positive false can be defined as alarms which are triggered from legitimate activities. Negative false are attacks, which are not detected by the system. An IDS is more precise if it detects more attacks and gives few false alarms. In case of misuse detection systems, security experts must examine new attacks to add their corresponding signatures. In anomaly detection systems, human experts are necessary to define relevant attribute for defining the normal behaviour.

This leads us to the adaptability problem. The currents IDS aptitudes to be adapted are very limited. This makes them ineffective for new or

Benferhat S., Boudjelida A. and Drias H. (2009).
ADDING EXPERT KNOWLEDGE TO TAN-BASED INTRUSION DETECTION SYSTEMS.
In *Proceedings of the International Conference on Security and Cryptography*, pages 61-64
DOI: 10.5220/0002262200610064

unknown attacks detection or to be adapted to an evolutionary environment.

Machine learning approaches provide a potential solution to adaptation and correctness problems in intrusion detection context. Many classification approaches try to construct an explicit function from common set of features values to obtain instances labels (category of attacks or normal).

Since (Denning D. E., 1987), several approaches based on statistical learning were proposed for intrusion detection. Among works which use TCP packets analysis that of (Bykova, M. et al., 2001) who have used simple statistics and (Ben Amor et al., 2004) who have compared performances of Bayesian networks and decision trees. (Valdes, A., Skinner, K., 2000) have used directly Bayesian networks to model attacks and their temporal evolution. Concerning Bayesian networks learning for systems resources and users logs analyses we can mention works of (Kruegel, C. et al, 2003, Scott, S. L., 2004, John G., 1997).

The most adapted Bayesian classification model for intrusion detection is naive Bayes. They present several advantages due to their simple structure.

Bayesian naive networks construction is very simple; it is always easy to consider new scenarios (updates facility). Inference is polynomial, while inference in Bayesian networks with general structures is known to be a hard problem (Cooper, G. F., 1990). However, naive Bayes networks consider a very strong features independence assumption: detection features are independent in a session class context. Such hypothesis is not always true in real applications.

This paper proposes an event classification which uses TAN classifiers. This will enable us to represent dependences between variables and to integrate additional data, in order to improve decision and detection process performances.

Section 2 shows how general expert information can help in improving the detection rate of attacks, while Section 3 presents comparative studies between TAN and other classification approaches. Finally, section 4 concludes the paper.

2 HANDLING EXPERT INFORMATION

This section suggests a new procedure to deal with this problem is to use additional information on connections type. For example, we have information that, on normal connections, usually there is X % of these connections which are actually attacks and we have to determine these connections.

In Bayesian networks, in order to determine these connections, we need to sort classified connections as normal according to probability that they represent attacks (or according to another sort function such difference between probability that they represent attacks and probability that they are normal), then the X % first connections will be taken in order to be considered as attacks.

This information can be also related to several attacks classes (Normal, Dos, R2L, U2R and Probing in KDD'99 data set case), by making for example assumption that on obtained normal connections, there is X % of connections which are actually DOS attacks and Y % which are R2L attacks, thus it remains to determine normal connections who represent these attacks. To do this operation, we precede similarly, by sorting classified connections as normal according to the probability that they represent DOS attacks, then we take X % first connexions.

The same thing for R2L attacks, but the sorting function will be related to the probability that they represent R2L attacks then the first Y % connections will be taken.

The main remark drawn from the additional information experiments results Table 1 is the considerable PCC improvement, because this rate have reached 96.69 % for five connections classes case against 92 90 % without using additional information and 97.40 % for two connections classes case against 94.07 % without using additional information.

As in (Ben Amor et al., 2004) we have used 10% of KDD' 99 set (KDD cup 99, 1999), which corresponds to 494019 training connections and 311029 test connections, with 18729 new attacks which do not appear in training set.

Each connection is described by 41 discrete and continuous features (for example connection duration, protocol type, etc.) and marked to be normal, or an attack, with only one attack type per line (for example Smurf, Perl, etc.).

Attacks are grouped in four classes:

Denial of Service (DOS). Make some machine resources unavailable or too busy to answer to legitimate users requests.

User to Root (U2R). Exploit vulnerability on a system to obtain a root access.

Remote to Local (R2L). Use vulnerability in order to obtain a local access like a machine user.

Probing. Collect useful information or known vulnerabilities about a network or a system.

A more detailed study of preceding results, more precisely negative false, shows that rest of selected connections (which have incorrect classification result) represent in their majorities another attacks class than the considered class, which reduces significantly number of negative false.

Table 1: TAN + Supplementary information results.

Five classes					
Normal	Dos	R2L	U2R	Probing	PCC
99.16%	99.46%	53.60%	31.43%	78.11%	**96.69%**
Two Classes					
Normal	Abnormal	PCC			
98.80%	97.07%	**97.40%**			

3 COMPARATIVE STUDY

A comparative study presented in Table 2 gathering tests results leaded by (Ben Amor et al., 2004), which have used the same experimental conditions as those used in our study, and results obtained previously, based on PCC, shows that considering all attacks, five attacks classes or only two attacks classes do not affect TAN classification quality.

We can also note that TAN results are generally better than those of the other strategies.

Table 2: PCC Comparison between Decision trees, Naive Bayes, TAN, TAN + Supplementary Information.

	All Attacks	Five Attacks Classes	Two Attacks Classes
Decision	91.41 %	92.28 %	93.02 %
Naive Bayes	91.20 %	91.47 %	91.45 %
TAN	91.27 %	**92.90 %**	**94.07 %**
TAN +	-	**96.69 %**	**97.40 %**

Another comparative study presented in Table 3 shows that TAN are competitive with the winning strategy in KDD' 99 and also share with this latter it failure to well classify R2L and U2R connections. We can even note that TAN give better results than the other strategy for Dos and R2L attacks detection.

The principal remark that we can draw from this table remains the significant improvements given by exploiting additional information with TAN.

This strategy has increased considerably R2L and U2R attacks detection rate and it has minimized false negative rate.

If we consider the global PCC, we can say that TAN + Supplementary information is better than the wining strategy in KDD' 99.

Table 3: Comparison between the wining strategy, TAN and TAN + Supplementary Information.

	Winning Strategy	TAN	TAN+ Suppl. Info.
Normal	99.50 %	98.10 %	99.16 %
Dos	97.10 %	97.86 %	99.46 %
R2L	8.40 %	18.57 %	53.60 %
U2R	13.20 %	9.11 %	31.43 %
Probing	83.30 %	73.28%	78.11 %
PCC	92.70 %	**92.90 %**	**96.69%**

4 CONCLUSIONS

Performances evaluation results of TAN strategy showed that it is better than naive Bayes. These results also showed that PCC obtained by TAN is better than that obtained by decision trees for the five connexions class case. Details of these results showed also that TAN is very competitive with the winning strategy in KDD competition.

This paper has also shown how to use a new procedure which exploits additional information. Evaluation results of this new approach showed that this approach provides better results than previous approaches.

REFERENCES

Ben Amor, N., Benferhat, S., Elouedi, Z.: Naive Bayes vs Decision Trees in Intrusion Detection Systems, ACM Symposium on Applied Computing. SAC’04 (2004)

Benferhat, S., Tabia, K.: On the combination of Naive Bayes and decision trees for intusion detection. The International Conference of Intelligencecontrol and Automation. CIMCA (2005)

Bykova, M., Ostermann, S., Tjaden, B.: Detecting network intrusions via a statistical analysis of network packet characteristics. In Proceedings of the 33rd South Eastern Symposium on System Theory (2001)

Chow, C. K., Liu, C. N.: Approximating discrete probability distributions with dependence trees. IEEE Trans on Info Theory 14. pp 462—467 (1968)

Cooper, G. F.: Computational complexity of probabilistic inference using Bayes belief networks. Artificial Intelligence. Vol. 42, pp. 393--405 (1990)

Denning D. E.: An intrusion-detection model. IEEE Transactions on software engeneering, SE-13. pp. 222--232 (1987)

Friedman, N., Geiger, D., Goldszmidt, M.: Bayesian network classifiers. Machine Learning, 29(2-3):131--163 (1997)

Geiger, D.: An entropy-based learning algorithm of Bayesian conditional trees. In UAI '92. pp. 92--97 (1992)

Hamine, V., Helman, P.: Learning Optimal Augmented Bayes Networks. Dept. of Computer Science. University of New Mexico. Albuquerque. New Mexico 87131 USA (2004)

John, G., Enhancements to the Data Mining Process. PhD thesis, Stanford University (1997)

KDD cup 99, intrusion detection dataset task description. University of California Department of Information and Computer Science, http://kdd.ics.uci.edu/databases/kddcup99/task.html (1999)

Kruegel, C., Mutz, Robertson, W., Valeur, F.: Bayesian Event Classification for Intrusion Detection" Reliable Software Group. University of California, Santa Barbara (2003)

Langley, P., Iba, W., Thompson, K.: An Analysis of Bayesian Classifiers. In Proceedings of the Tenth National Conference on Artificial Intelligence, pp. 223--228, AAAI Press and MIT Press (1992)

Scott, S. L.: A bayesian paradigm for designing intrusion detection system. Computational Statistics and Data Analysis (special issue on network intrusion detection). 45: 69--83 (2004)

Valdes, A., Skinner, K.: Adaptive Model-based Monitoring for Cyber Attack Detection. In proceedings of Recent Advances in Intrusion Detection (RAID). pp. 80--92. Toulouse, France (2000)