Speeding-up Denial-of-Service Detection Rules Computation thanks to Genetic Algorithm

M. Grari[1], M. Nasri[1], G. Dequen[2]

1. Laboratory MATSI, University Mohammed I OUJDA,
m.grari@ump.ma nasri@est.ump.ma
2. Laboratory MIS, University Picardie Jules Verne
gilles.dequen@u-picardie.fr

Keywords : Denial-of-Service; Network Intrusion Detection; KDD99; Genetic Algorithm; Metaheuristic.

1 Introduction

Internet is expanding very quickly in recent years, mainly in terms of the services offered and of the mobility of users that make them more vulnerable to various attacks. Intrusion Detection Systems (short for IDS) identify unauthorized accesses to a system or a network. They are usually and typically classified with respect to placement such as: host-based or network-based. A host-based IDS monitors resources such as system logs, file systems and disk resources activities whereas a network-based IDS focuses its detection on data passing through the network. This work deals with IDS based on network detection (short for NIDS). Several ways can be used to tackle NIDS problem. Among them, you can find Statistics-based approaches applied to audit data, profiles user, disk and memory, Rule-based approaches (e.g. Data Mining[6]) or Heuristic-based approaches(e.g. Neural Networks [7], Fuzzy Logic, Swarm Intelligent or Genetic Algorithms(short for GA) [4,5]). Within the framework of this work we focused on the latter approach.

The use of GA within IDS has been previously studied. The reader can refer to [4,5]. As an illustration, the authors of [4] describe an implementation of rule based GA for intrusion detection system. They use 3 features from the state-of-the-art KDD99 data set benchmark (Duration, protocol_type and dst_host_srv_count) to classify four major types of attacks (Denial-of-Service, User to Root Attacks, Remote to user Attack and Probe attacks). Another similar work is presented in [4] where the authors propose to select 3 network features (Duration, src_byte and dst_host_srv_serror_rate) and 10 best rules selected for the classification of the intrusion and normal connections in KDD99. They are able to reach a detection rate of `smurf` attacks, a specific Denial-of-Service (short for DoS), equals to 99%. Nevertheless, this approach seems to be time consuming. As a contribution of this work we propose to reach a higher detection rate (i.e. greater than 99.9 %) with a computing time consumption reduced of an order of magnitude equals to 10 (within a sequentially implementation). One of the main principle we propose in this contribution is to select relevant features adapted to each type of attacks. We first focus our contribution to DoS attacks.

The paper is organized as follows. Section 2 provides an overview of the Genetic Algorithm principle. In section 3, we briefly describe KDD99 dataset benchmark [1] and its 10% subset used in our experiments. We also provide a short analysis of attacks belonging to this subset.

Section 4 describes the policy defining our dedicated GA approach (also named GADOSD) to reach high rate of Denial-of-Service `smurf` (and others) detection intrusion us in weak runtime consumption. Thus, we propose to use 3 features (among the 41 availables in KDD99). We then choose to replace protocol_type features used by S. Akbar in [4] by src_byte (i.e. Bytes sent from source to destination). We also replace dst_host_srv_serror_rate used by Z.Bankovicin [4] by dst_host_srv_count. We finally define the selection operator and its associated fitness function [2]. The complete principle of our NIDS approach is presented in the Fig. 1 inspired by works in [3,4,5]. The Fig. 2 presents the Evaluation function of the best chromosome in each generation.

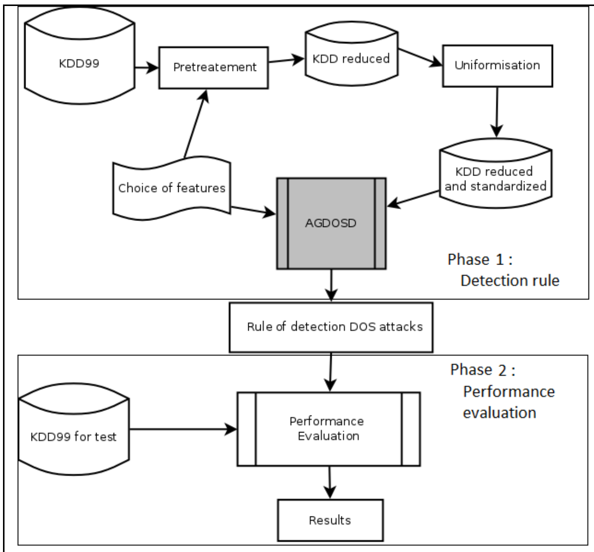

Fig. 1. Structure of the proposed model

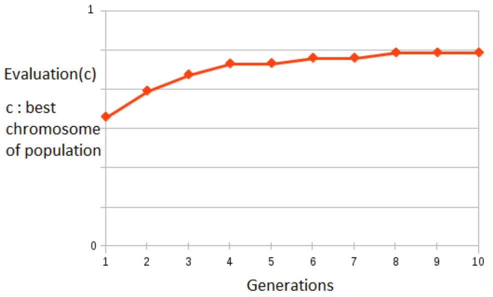

Fig. 2. Evaluation of the best chromosome in population in each generation

In section 5 we present, after describing our experimental context, some comparative results showing improvements of GADOSD on some specific DOS detection intrusion. Table 1 compares our approach with S. Akbar approach [6]. In particular we show the detection percentage and false positive rate, in this experiments our approach with 99.927 is the best in term of detection percentage and false positive rate.

Table 1. Comparisons between our approach and others approach for `smurf` attacks

	`smurf` attack		
	S. Akbar Approach	Z. Bankovic approach	Our approach
Detection percentage	73%	99%	**99.927%**
False positive Rate	27.3%	0%	**7.2%**

Finally, In section 6, we conclude that our approach generate rule by applying GA to network intrusion detection system to detect the Denial-of-Service attacks. This approach applied to the KDD99 benchmark data set, implemented in java, confirms that every features are specifics to categories of attacks, we obtained good percentage of detection of DOS attacks, up to 72% for only 1 rule of detection. We provide some perspectives and future works.

References

[1] KDD cup 1999 data http://kdd.ics.uci.edu/databases/KDD99/KDD99.html
[2] L. Jourdan, C. Dhaenens, and E-G. Talbi (2006) "Using datamining techniques to help metaheuristics: a short survey", International Workshop on Hybrid Metaheuristics (HM 2006). LNCS Vol. 4030, ISBN: 3-540-46384-4. Grenada, Spain.
[3] E-G. Talbi (2013). “Combining metaheuristics with mathematical programming, constraint programming and machine learning”, 4OR, Vol11, No.2, pp.101-150.
[4] Z Bankovic, D Stepanovic, S Bojanic, O Nieto-Taladriz (2007). “Improving network security using algorithm approach”, Computers and Electrical Engineering 33438-451.
[5] S. Akbar, K. Nageswara Rao, and J. A. Chandulal (2011). "Implementing rule based Genetic Algorithm as a solution for intrusion detection system." Int. J. Comput. Sci. Netw. Secur 11.8: 138.
[6] S. M. Bridges, R. B. Vaughn (2010). “Fuzzy Data Mining And Genetic Algorithms Applied ToIntrusion Detection”, Proceedings of 12th Annual Canadian Information Technology Security Symposium, pp. 109-122.
[7] M. Moradi, M. Zulkernine (2004). A neural network based system for intrusion detection and classification of attacks, in: Proceedings of the 2004 IEEE International Conference on Advances in Intelligent Systems–Theory and Applications, Luxembourg-Kirchberg, Luxembourg, 15–18 November 2004, IEEE Press.