International Journal of Information Processing, 6(1), 76-83, 2012
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Comparison of Performance for Intrusion Detection System Using Different Rules of Classification

Nandita Sengupta[a], Jaya Sil[b] and Moumita Saha[b]

[a]Information Technology Program, University College of Bahrain, PO Box 55040, Manama, Kingdom of Bahrain

[b]Department of Computer Science and Technology, Bengal Engineering and Science University Shibpur, PO Botanic Garden, Howrah, Pin 711103,West Bengal, India

Classification is very important for designing intrusion detection system that classifies network traffic data. Broadly traffic data is classified as normal or anomaly. In the work classification performance using rules obtained by different methods are applied on network traffic and compared. Classifier is built based on rules of decision table, conjunctive rule, OneR, PART, JRip, NNge, ZeroR, BayesNet, Ridor from WEKA and using rough set theory. Classification performance is compared applying on KDD data set where the whole data set is divided into training and test data set. Rules are formed using training data set by different rule generation methods and later applied on test data set to calculate accuracy of classifiers.

Keywords: Classification, Intrusion Detection System, Rough Set Theory, Rules.

1. INTRODUCTION

Online classification of network traffic data is very important to develop Intrusion Detection System (IDS) that automatically monitors the flow of network packets. Existing works on intrusion detection have been carried out to classify the network traffic as anomaly or normal. A majority of current IDS follow signature based approach [1] in which similar to virus scanners, events are detected that match specific predefined patterns known as "signatures".

The limitation of these signature based IDS is their failure to identify novel attacks and even minor variation of patterns are not detected accurately. In addition, sometimes IDS generate false alarm for alerting network administrator due to failure of handling imprecise data which has high possibility to appear in network traffic data. Therefore, accuracy, computation time and system learning are the key issues to be addressed properly for classifying such data.

Classification is an important task in data mining research that facilitates analysis of huge amount of data. Rough Set Theory (RST) [2] is based on mathematical concept can handle vagueness in classification of data. However, prior to applying RST, the data is discretized and selection of discretization procedure has great impact on classification accuracy. In the paper, network traffic data [3] of KDD has been considered for generating training and testing patterns. In order to apply RST, the datasets are discretized and then a minimum subset of attributes of the data set is selected, called reducts by applying genetic algorithm [4]. Rules are generated from the reducts and classifiers are built using rule set classifier [5]. Finally, classification accuracy has been expressed in terms of correctly classified and incorrectly classified instances.

Other classifier rules, like decision table, conjunctive rule, OneR, PART, JRip, NNge, ZeroR, BayesNet, Ridor are applied on the same data set to find out correctly and incorrectly classified instances. These classifier rules are used by WEKA software [6] to measure corresponding classification accuracy and then compared based on the results achieved.

Table 7
Rough Set Classification Accuracy with Reduct

Reduct Set	% of Accuracy
Reduct 1	97.8
Reduct 2	92.5
Reduct 3	95.5
Reduct 4	92.6
Reduct 5	97.8
Reduct 6	90.0
Reduct 7	95.8
Reduct 8	92.2

Table 8
Comparison of Classification Performance with Reduct

Classifiers	Correctly Classified Instances(%)	Incorrectly Classified Instances(%)
Decision Table	90.2	9.8
Conjunctive Rule	85.3	14.7
OneR	90.2	9.8
PART	90.2	9.8
JRip	90.2	9.8
NNge	88.3	11.7
ZeroR	85.3	14.7
BayesNet	91.2	8.8
Ridor	93.2	6.8
RST	97.8	2.2

REFERENCES

1. S Neelakantan and S Rao. A Threat-Aware Signature based Intrusion-Detection Approach for Obtaining Network-specific useful Alarms, *in Proceedings of the Third International Conference on Internet Monitoring and Protection,* 2008.
2. T Beaubouef and F E Petry. Uncertainty Modeling for Database Design using Intuitionistic and Rough Set Theory, *in Journal of Intelligent and Fuzzy Systems: Applications in Engineering and Technology,* 20(3), August, 2009.
3. Nsl-KDD Data Set for Network-based Intrusion Detection Systems, *http://iscx.ca/NSL-KDD/.*
4. R N Shankar, T Srikanth, K B Ravi, A G Rao, Genetic Algorithm for Object Oriented Reducts Using Rough Set Theory, *In International Journal of Algebra,* 4(17):827-842, 2010.
5. S Kumar, S Atri, L H Mandoria. A Combined Classifier to Detect Landmines Using Rough Set Theory and Hebb Net Learning and Fuzzy Filter as Neural Networks, *In Proceedings of ICSPS,* 2009.
6. WEKA software Classifier Rules, *http://weka.sourceforge.net/ doc/weka/ classifiers/rules/ package-summary.html*
7. N Sengupta, J Sil. An Integrated Approach to Information Retrieval using RST, FS and SOM, *In Proceedings of ICIS,* Bahrain, 2008.
8. J Zhang, J Wang, D Li, H He, J Sun. A New Heuristic Reduct Algorithm base on Rough Sets Theory, *In Proceedings of Advances in Web-Age Information Management, WAIM, Lecture Notes in Computer Science,* vol. 2762, pages 247-253, 2003.
9. K Dembczynski, R Pindur, R Susmaga. Generation of Exhaustive Set of Rules within Dominance-based Rough Set Approach, *In Proceedings of International Workshop on Rough Sets in Knowledge Discovery and Soft Computing,* March, 2003.
10. H Lu, H Liu. Decision Tables: Scalable Classification Exploring RDBMS Capabilities, *In Proceedings of* 26th *International Conference on Very Large Databases,* Cairo, Egypt, 2000.

Nandita Sengupta has done her Bachelor of Engineering from Bengal Engineering College, Shibpur, Calcutta University. She completed Post Graguate Course of Management in Information Technology from IMT. Later on she passed M Tech (Information Technology) from Bengal Engineering and Science University Shibpur. she has worked in Design Department of Electrical Manufacturing Company Limited for 11 years. She is in academics and taught various subjects of IT over Last 9 years. Presently she is working as Lecturer in University College of Bahrain, Bahrain. Her area of interest is Analysis of Algorithm, Theory of Computation, Soft Computing Techniques, Network Computing. She achieved "Amity Best Young Faulty Award" on the occasion of 9th International Business Horizon INBUSH 2007 by Amity International Business School, Noida in February, 2007. She has around 17 publications in National and International conference and journals.

Dr. Jaya Sil an alumnus of BESUS(Bengal Engineering and Science University, Shibpur) and JU(Jadavpur University), completed her Ph.D. in Engineering from JU, Kolkata, India. She holds Masters in Computer Science and Engineering from JU and Bachelors in Electronics and Tele Communication Engineering from BESUS (formerly known as Bengal Engineering College). She has been in Academics for last 25 years. Presently she is working as Professor and Head of the Department of Computer Science and Technology Department and Director of School of VLSI Technology in BESUS. Under her leadership and guidance many sponsored projects have been successfully conducted. She has more than 80 publications in International Conferences and Journals. She has already supervised two Ph D theses and more than 10 Ph.D students presently working under her guidance. Dr. Sil worked as Post-Doc Fellow in Nanyang Technological University, Singapore on 2002-03 and visited Heidelburg University, Germany on 2007. Dr. Sil contributed a Book Chapter - Adaptive Agent Integration in Designing Object- Based Multiagent System. LNCS, Volume 3215/2004 Dr. Sil acts as Guest Editor in International Journal on Artificial Intelligence and Soft Computing and Editor of GA Issue Of Materials and Manufacturing Processes. Delivered Tutorial lectures in two Intl. Conferences NGMS 2006, 2008 and INDO US workshop in Kolkata. Her areas of research include Image Processing, Soft Computing Techniques, Multiagent Systems and Bio-Informatics.

Moumita Saha has completed her Bachelor of Technology from Meghnad Saha Institute of Technology, WBUT. She is pursuing Master of Engineering from Bengal Engineering And Science University(BESUS), Shibpur. She is performing her research work in the field of Soft Computing.