International Journal of Electronics Signals and Systems

Volume 1 | Issue 2 Article 4

September 2011

An Intelligent Agent Based Intrusion Detection System Using Fuzzy Rough Set Based Outlier Detection

N. Jaisankar
Department of Information Science and Technology, College of Engineering Guindy, Anna University, Chennai-25, India, jaisasi_win@yahoo.com

M Ganapathy
Department of Information Science and Technology, College of Engineering Guindy, Anna University, Chennai-25, India, ganapathy.sannasi@gmail.com

A Kannan
Department of Information Science and Technology, College of Engineering Guindy, Anna University, Chennai-25, India., kannan@annauniv.edu

K Anand
KTH University, Swedan, anand01oct@gmail.com

Recommended Citation

Jaisankar, N.; Ganapathy, M; Kannan, A; and Anand, K (2011) "An Intelligent Agent Based Intrusion Detection System Using Fuzzy Rough Set Based Outlier Detection," *International Journal of Electronics Signals and Systems*: Vol. 1 : Iss. 2 , Article 4.
DOI: 10.47893/IJESS.2011.1018
Available at: https://www.interscience.in/ijess/vol1/iss2/4

Available online at www.interscience.in

An Intelligent Agent Based Intrusion Detection System Using Fuzzy Rough Set Based Outlier Detection

N Jaisankar[1], M Ganapathy[2] , A Kannan[3] , K Anand[4]

[1,2,3] Department of Information Science and Technology, College of Engineering Guindy, Anna University, Chennai-25, India.

[4] KTH University, Swedan.

Email: jaisasi_win@yahoo.com[1], ganapathy.sannasi@gmail.com[2] , kannan@annauniv.edu[3], anand01oct@gmail.com[4]

Abstract - Since existing Intrusion Detection Systems (IDS) including misuse detection and anomoly detection are generally incapable of detecting new type of attacks. However, all these systems are capable of detecting intruders with high false alarm rate. It is an urgent need to develop IDS with very high Detection rate and with low False alarm rate. To satisfy this need we propose a new intelligent agent based IDS using Fuzzy Rough Set based outlier detection and Fuzzy Rough set based SVM. In this proposed model we intorduced two different inteligent agents namely feature selection agent to select the required feature set using fuzzy rough sets and decision making agent manager for making final decision. Moreover, we have introduced fuzzy rough set based outlier detection algorithm to detect outliers. We have also adopted Fuzzy Rough based SVM in our system to classify and detect anomalies efficiently. Finally, we have used KDD Cup 99 data set for our experiment, the experimental result show that the proposed intelligent agent based model improves the overall accuracy and reduces the false alarm rate.

Keywords - *Intrusion Detection System (IDS), Outlier Detection, Fuzzy Rough Set, Feature Selection, EC4.5, Fuzzy Rough Set Based SVM*

.

I. INTRODUCTION

The internet becomes unavoidable essential tool in every bodies day to life. It helps business, entertainment etc. the information security of using internet is an important issue need to be addressed. There are various security systems have been proposed by the researchers [12] particularly, Intrusion detection systems helps the network to detect various malicious attacks [13] which cannot be detected by connectional firewall. These IDS can be divided into two major catagories based on their detection approaches misuse detection and anomaly detection. Misuse detection is the ability to identify intrusions based on known signature patterus for the malicious activity and anomoly detection is the attempt to identify traffic on deviation from network traffic patterns [14]. Recently, Researchers focusing on data mining techniques to analyze and apply in developing efficient IDS, But still there major problem with current IDS is that they fail to detect new types of attacks without known signature patterns. However, another main issue in the current IDS models is its failure to reduce the false alarm rate.

In this paper data mining technologies such as classifiers, outlier detection using fuzzy roughsets and fuzzy roughset based SVM has been proposed in developing IDS to address the some pf the exsisting issues such as to improve the detection accuracy and to reduce the false alarm rate.

The main aim of this paper is first, we select the feature set from KDD Cup99 Data set using fuzzy rough set and then we introduced new fuzzy rough outlier factor for efficient outlier detection which wil be included as one component in the proposed intelligent agent based IDS, another component called fuzzy rough set based SVM to classify the data efficiently and finally we introduced decision manager who will analyse all the outputs announce the final decision of the system.

The rest of this paper organised as follows, section 2 discuss about literature survey, section 3 discuss about architecture of the proposed model, section 4 discuss and analyse the experimental results and finally conclusion is drawn and suggested some feature work in section 5.

II. LITERATURE SURVEY

Hua TANG and Zhuolin CAO [1] proposed a machine learning based algorithm for intrusion detection which uses a combination of nural networks and support vector machines. However, they have used all the features of KDD cup dataset. Lee et.al [2] has proposed a data-mining framework for designing intrusion detection models by mining normal patterns from audit data. S. Peddabachigan et.al [3] investigated some new techniques for intrusion detection and evaluated their performance based on the KDD Cup 99 Intrusion data.

S.Sun et.al [4] proposed a hybrid intelligent system that uses a new algorithm called weighted support vector clustering algorithm, which is, applied it to the anomaly detection problem. Their experimental results show that their method achieves high detection rate with low false alarm rate.

Eric C.C Tsang et.al [5] in their work defines attributed reduction with fuzzy rough sets and analyzes its structure in details and they have developed a formal definition of reduction with fuzzy rough sets. Richard Jensen and Quiang Shen [6] have presented a fuzzy-rough method for attribute reduction, which alleviate important problems encountered by traditional methods. Fabrizio Angiulli et. al [7] have proposed a distance based outlier detection method, which is to find the top outliers in an unlabeled data set and provide a subset of it, called the outlier detection solving agent. Solving agent can investigate the accuracy in separately outliers from inliers. Faizah Shaari et.al. [8] have used rough sets for outlier detection is to discover Non-Reduct from Information Systems. Didier Dubois et.al [9] proposed an idea to combine rough set with fuzzy sets. It enables several independent approaches to approximation models to be unified. They also proposed another idea is to turn the equivalence relation into fuzzy similarity relation. Zdzislaw Pawlak [10] has described some propertis of rough sets and investigated approximate operations on sets, approximate quality of sets and approximate inclusion of sets. Degang Chen et.al. [11] have applied fuzzy transitive kernals as fuzzy similarity relations and develop a fuzzy transitive kernal based fuzzy rough sets, they also proved that SVM and Fuzzy Sets are connected.

III. INTELLIGENT AGENT BASED APPROACH

A. System Architecture

The Fig.1 shows that overall archtecture of the intelligent agent based system. The functionality of various components of the system can be described as follows.

B. Feature Selection Agent

The main aim of feature selection agent is to determine a minimal feature subset that can represent data as a whole is essential to the success of an intrusion detection system if both accuracy and speed are to be achieved. The agent uses fuzzy rough set and its potential for selecting an optimum feature subset.

C. Fuzzy Rough Set Based Outlier Detection

The following definition for fuzzy rough membership function based outliers detection has been presented. We no need to detect outliers just by checking all the elements in the universal set U. Instead we can consider subset X of U and detect outliers with respect to X. Here we define a fuzzy rough outlier is a weight function such that for any $F_i \in X$

$$W_X^{\{a\}}(F_i) = \frac{|[x]_R \cap X|}{|[x]_R|}$$

Where $[x]_R =$ **{ u∈ U: ∀ a∈C(f(u,a) = f (x,a))** denotes the indescernibility class of relation IND(C) that contains element Fi. factor which indicates the degree of outlierness for every object with respect to subset of universe U.

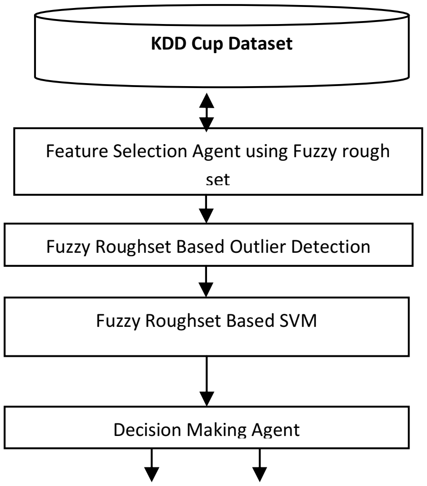
KDD Cup Dataset
Feature Selection Agent using Fuzzy rough set
Fuzzy Roughset Based Outlier Detection
Fuzzy Roughset Based SVM
Decision Making Agent

Fig 1. System Architecture

Definition 1

Let the 4-tuples (U, A, V, f) be an Information System (IS), $X \subseteq U$ and $X \neq 0$. For any Fi X, The fuzzy rough outlier factor of Fi With respect to X in IS is defined as

$$\textbf{FROF}\ (\mathbf{F_i}) = \mathbf{1}- \frac{\sum_{a\in A}(\mu_X^{\{a\}}(F_i) \times W_X^{\{a\}}(F_i)}{|\mathbf{A}|}$$

Where $\sum_{a\in A}(\mu_X^{\{a\}}(F_i)$: $X \longrightarrow (0, 1]$ is a fuzzy rough membership function whose domain is set X. For every singleton subset {a} of A, and for every singleton subset of A

$$W_X^{\{a\}}(F_i) : \mathbf{X} \longrightarrow \mathbf{[0, 1]}$$

D. Fuzzy Fuzzy RMS based Outlier Detection Algorithm:

Input: Information System IS = (U,A,V, f) and a subset X of U where |U| = n and |X| = n_x <n and |A| = m; threshold value α

```
Output:  A set S of outliers based on fuzzy RMF
For every a∈ A
{
    Sort all oblets from uviverse U and X based on given order on domain value Va of attribute element a,
    For every $F_i$ ∈ X
    {
        Compute the indescernibility class  $[x]_{\{a\}}$
        Compute $\mu_X^{\{a\}}(F_i)$, the value of fuzzy rough membership function of $F_i$ w.r.t. X under indiscernibility relation IND(X).
        Assign a weight $W_X^{\{a\}}(F_i)$ to $F_i$
} }
For every $F_i$ ∈ X
{
    Compute fuzzy rough outlier of $F_i$
    FROF ($F_i$) > α then S = S U {$F_i$}
}
Return S.
```

E. Decision Manage

The decision manager first will collect the output of classifiers. Then analyze the results and investigate whether the intrusion detection accuracy of the combined classifier is improved when compared with the results of the individual classifiers.

F. Fuzzy Rough Set Based SVM (FRSVM)

According to Degang Chen et. Al. [11] In FRSVM the membership of every training sample is computed using fuzzy rough set, so that hard marging of SVM can be combined with fuzzy rough sets [9] . Here for classification we use a lower approximation operation in fuzzy transitive kernal based fuzzy rough sets to compute the membership of every training set. Clearly there are two classifications FRSVM and FSVM. FSVM mainly deals with the importance of the training samples when FRSVM consider inconsistency between conditional feature and decision lable, so they involve different motivations and formalisms to compute the cuzzy membership, and different motivations and reformulations of SVM.

IV. RESULTS AND DISCUSSION

Accuracy of the various attacks refers to the proportion that the types of data are correctly classified and there are four types compared in this paper. The following table 1 illustrate the comparison results of accuracy of various attacks by using rough Set based outlier detection IDS and Intelligent agent based IDS using fuzzy rough set based outlier detction

Table 1 Detection Accuracy Comparison between RS_IDS and Fuzzy RS_IDS

Attack Type	RS_IDS	FuzzyRS_IDS
U2R	69	41
R2L	84.7	34.5
DOS	96.99	99.95
Prob	99.99	96.9
Normal	99.8	99.7

The experimental result show that for DOS, U2R and R2L attacks the detection accuracy of an intelligent agent based IDS using fuzzy rough set based outlier detection is better than the IDS using rough set based outlier detection

V. CONCLUSION

In this paper, we proposed preprocessing techniques for an IDS called feature selection algorithm that uses Fuzzy Rough Set theory and a classification module for classifying the data set. The results obtained from preprocessing module indicate that the feature subset obtained by fuzzy Rough set is robust and has provides a better performance when compared with classification using full data set. We used the KDD Cup 99 Intrusion Detection Data set for carrying out the experiments. In this paper, We have constructed intelligent agent based intrusion detection system using fuzzy rough set based outlier detection by introducing new algorithm called fuzzy rough set based outlier detection algorithm to detect outliers and the classifier fuzzy rough set based SVM have been adapted and used . It has been observed that the proposed system provides better accuracy for all classes used when compared with IDS using rough set based outliers. Furthermore, it has been proved that the detection accuracy for PROBE and R2L classes of attacks is 99.9%. Furtherworks in this direction could be the use of spatio temporal constraints in the rough sets based outlier detection which can be a effective first level preprocessing.

REFERENCES

[1] D Hua TANG, and Zhuolin CAO. Machine Learning-based Intrusion Detection Algorithms. In Journal of Computational Information Systems, Vol.5, No.6, pages 1825-1831, 2009.

[2] Lee W, and Stolfo S. Datamining approaches for intrusion detection. In Proceedings of the 7th USENIX security symposium,1998.

[3] S.Peddabachigari, A.Abraham, C.Grosan, and J.Thomas. Modeling intrusion Detection system using hybrid In intelligent systems Journal of Network and Computer Applications 30, pages 114–132, 2007.

[4] S. Sun, and Y. Wang. A Weighted Support Vector Clustering Algorithm and its Application In Network Intrusion Detection In First International Workshop on Education Technology and Computer Science Vol. 1, pages 352-355, 2009.

[5] Eric C.C. Tsang, Degang Chen, and D.S.Yeung. Attributes Reduction using Fuzzy Rough Sets In IEEE Transaction on Fuzzy Systems Vol. 16 No 5, pages 1130- 1140,Oct.2008.

[6] Richard Jensen and Quiang, " Fuzzy Rough Attribute Reduction with Application to Web Categorization, Vol.22, Febraury 2008

[7] Fabrizio Angiulli, Stefano Basta, and Clara Pizzuti, "Distance based Detection and prediction of Outliers", IEEE Transactions on Knowledge and Data Engineering, Vol.18, No.2, February 2006.

[8] Faizah Shaari, Azuraliza Abu Bakar and Abdul Razak Hamdan, " Outlier Detection Based on Rough Sets Theory", Intelligence Data Analysis NO.13, pp. 191 -206, 2009.

[9] D.DuboisandH.Prade,"Roughfuzzysetsandfuzzyroughsets," International Journal of General Systems,vol.17, no.2–3, pp.191–209,1990.

[10] Zdzislaw Pawlak, Rough Sets", International Journal of Computer and Information Sciences, Vol.11, No.5, pp. 341-356,1982.

[11] Degang Chen, Qiang He and Xizhao Wang " FrSVMs: Fuzzy rough set based Support Vector Machinie, Fuzzy Sets and Systems, Vol.161, pp. 596-607, 2010.

[12] Ahmed Patel, Qais Qassim, and Christopher Wills. A survey of intrusion detection and prevention systems. In Information Management & Computer Security, Vol. 18 Issue: 4, pages 277 - 290, 2010.

[13] Chih-Fong Tsai, and Chia-Ying Lin, A Triangle area based nearest neighbors approach to Intrusion Detection. In Pattern recognition, Vol. 43 Issue: 1, pages 222-229, 2010.

[14] Mohammadreza.E Sara.M, Fatinah.S,Lilly Suriani.A. Intrusion Detection using Data Mining Techniques In IEEE International Conference on Information Retrievel and knowledge management (CAMP). pages 200-203, 2010.