ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

Intrusion Detection System Based on Fuzzy Association Rule with Genetic Network Programming

Harinee.k [1], Veeramuthu.A [2]

P.G. Student, Department of Information Technology, K.L.N College of Information Technology, Sivagangai, Tamilnadu, India[1]

Associate Professor, Department of Information Technology , Sathyabama University, Chennai,Tamilnadu, India[2]

Abstract: Intrusion detection which classifies the attacks on the Internet from usual behaviour of usage on the Internet. Here intrusion detection systems are vital tool in the cluster environment fight to keep its computing resources secure .It is an unavoidable portion of the information security system. Emerging variety of network behaviours and the rapid development of attack scenarios, it is vital to develop fast machine-learning-based intrusion detection algorithms with high detection rates and low false positive and false negative -alarm rates with the help of association rule mining. In this course of work a fuzzy class-association rule mining method based on genetic network programming (GNP) for intrusion detection. GNP is an evolutionary optimization technique, which uses directed graph structures leads for enhancing the representation ability .In combination with fuzzy set theory and GNP, the proposed work can deal with mixed database that contains both discrete and continuous attributes and also extract many important class association rule .Therefore, the proposed method can be flexibly applied to both misuse and anomaly detection in network-intrusion-detection .It can extract important rules using these tuples and this mechanisms can calculate measurements of association rules directly using GNP which provides detection rate for prediction based approach.

Keywords: GNP, fuzzyclass ,Intrusion detection, false positive negative alarm

I INTRODUCTION

Enormous application oriented system over the Internet such as online shopping, net banking, trading stocks and foreign exchange and online auction have been developed. However, open access platform of the Internet, computer systems and data is always at risk under some security issues. Abundant growth of the Internet has prompted network intrusion detection to create a vital component of infrastructure protection mechanisms. Network intrusion detection can be identified by a set of malicious actions which may threaten the availability of a network resource, integrity, confidentiality,security.

Intrusion detection conventionally categorized in to misuse detection and anomaly detection. Misuse detection mainly focuses for specific patterns or sequences of programs and user behaviours that match well-known intrusion scenarios. Anomaly detection develops a system of normal network behaviours, and intrusions are detected by evaluating significant deviations from the normal behaviour of the user. The advantage of anomaly detection is that it may detect rare intrusions that have not been observed yet.

An extended algorithm for important class association rule mining from incomplete databases using GNP. An incomplete database includes missing data in some tuples. For example, the database of questionnaire probably includes missing data. In case plural databases are joined, missing data would also appear because attributes in each database which are seems to be same. usually, conventional rule extraction methods indicates the database as complete,

While accuracy is the essential requirement of an intrusion-detection system (IDS), its extensibility and adaptability are also critical in today's network computing environment. Currently, building effective IDS is an effective task. IDS system developers depends on their intuition and experienced to select the statistical behaviour or stratagies for anomaly detection.Attacks scenarios,system vulnerabilities have been analysed and implement corresponding rules and patterns for misuse detection. Because of the manual and adhoc nature of the development process, such IDS have limited extensibility and adaptability.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

The remaining sections discuss as follows.section2 reviews multimodality image fusion. In section3 reviews fusion of spectral factorization .in section 4 fusion rule for fusion of detail and approximation .in section4 reviews fused result The remainder of this paper is organized as follows. In Section II related work is discussed, followed by elaborate description proposed work in Section III. Subsequently, in Section IV described our experimental setup, with the data sets used and tool used. In Section V presented the results followed by a discussion and a conclusion in Section VI.

II RELATED WORK

An basic premise for intrusion detection is that when audit mechanisms are enabled to record system events, distinct evidence of legitimate activities and intrusions will be manifested in the audit data [4]. Because of the large amount of audit records and the variety of system features, efficient and intelligent data analysis tools are required to discover the behavior of system activities. KDD99Cup [5] dataset and the Defense Advanced Research Projects Agency (DARPA) datasets provided by MIT Lincoln Laboratory are widely used as training and testing datasets for the evaluation of IDSs [4], An evolutionary neural network is introduced in and networks for each specific system-call-level audit data (e.g., ps, su, ping, etc.) are evolved. Parikh and Chen discussed a classification system using several sets of neural networks for specific classes and also proposed a technique of cost minimization in the intrusion-detection problems.

Data mining generally refers to the process of extracting useful rules from large stores of data. The recent rapid development in data mining contributes to developing wide variety of algorithms suitable for network-intrusion-detection problems. Intrusion detection can be thought of as a classification problem: we wish to classify each audit record into one of discrete sets of possible categories, normal or a particular kind of intrusion.

As one of the most popular data mining methods for wide range of applications, association-rule mining is used to discover association rules or correlations among a set of attributes in a dataset. The relationship between datasets can be represented as association rules. An association rule is expressed by X . Y , where X and Y contain a set of attributes. This means that if a tuple satisfies X, it is also likely to satisfy Y . The most popular model for mining association rules from databases is the a priori algorithm . This algorithm measures the importance of association rules with two factors: support and confidence. However, this algorithm may suffer form large computational complexity for rule extraction from a dense database.

III.METHODOLOGY

The main aim of this project is to detect the Intrusion in Network by using Data Mining.This work describes a novel fuzzy class-association-rule mining method based on GNP and its application to intrusion detection. By combining fuzzy set theory with GNP, the proposed method can deal with the mixed database that contains both discrete and continuous attributes. Such mixed database is normal in real-world applications and GNP can extract rules that include both discrete and continuous attributes consistently

- Network Creation and Communication module
- Fuzzy class-association-rule formation module
- GNP module
- Enhancement module
- Comparison module

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

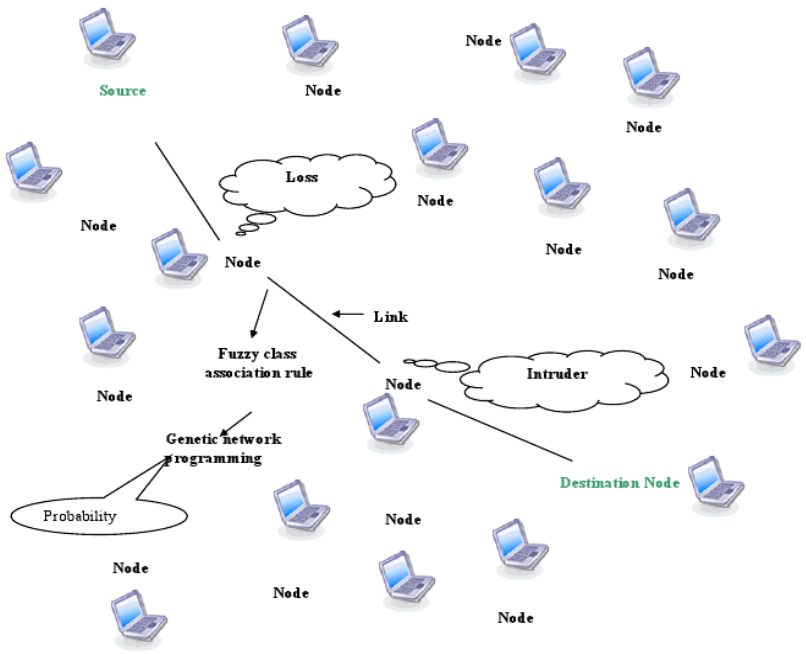


Figure 1. Architecture for intrusion detection system

The above fig1 Architecture of ids gives a clear idea of detecting the intrusions occurred in wireless network in the issue of transmission of packets.Packet transfer is occurred from the source to destination via processing nodes.So there may be possibility of packet loss because of processing node or nodes in clusters.The goal is to detect the intrusion happening in adhoc nature by applying fuzzy rule.

A.NETWORK CREATION AND COMMUNICATION MODULE

Network Creation and communication module is done in ad-hoc.In this these five process/modules have been carried out.As a result intrusion in this network can detected. Create the Network.Then form Source and Destination.Upload files in Source. Destination Send Data Request to Source. Source Calculate the shortest path using dijistra's algorithm Source Send the Advertisement Message to the path Nodes (GNP basis). Path Nodes are divided three two parts at the time of transformation.The network created is in adhoc nature or wireless.So transferring of packets containing datas via the shortest path containing processing nodes.

B .FUZZY CLASS-ASSOCIATION-RULE FORMATION MODULE

The judgment node applies the fuzzy class association rule in the process node.There are four rules performed by this module.Each rule consists of two sub attributes.Attributes like A1,A12.Based upon the attributes statistical or probablity values can be obtained.These four rules are used in the existing system for intrusion detection.These fuzzy rules are mined by using association rule mining.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

C. GNP MODULE

The node requests for a packet from source node to the destination node. The transaction is through the processing node if the the packet is getting transferred In workflow via the processing node.In this case each processing node will act as a jundgement node and transfers the packet to another processing node..The Judgment node Transfer the packet to processing node and receive the ACK. Then Apply GNP.Attributes Matching Probability produce Misuse Detection & Probability.Then Calculate Detection

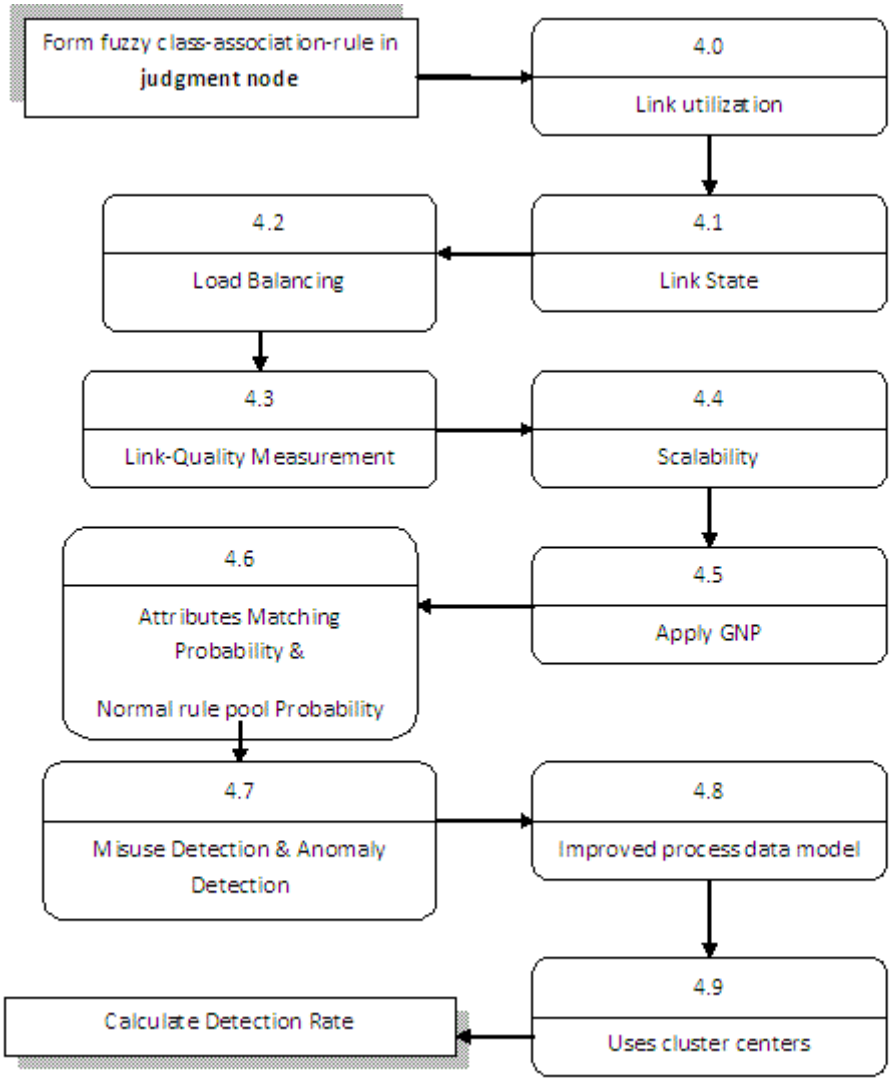


Fig. 1 Flow diagram of intrusion detection system

D .ENHANCEMENT MODULE

Enhancement module below the application of seven rules along with the four fuzzy rules.This module gives more exposure than the existing four rules.Transaction includes processing node act as judgement node. Judgment node Transfer the packet to processing node and receive the ACK.Then Apply GNP Attributes Matching Probability produce

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

Misuse Detection. Normal rule pool Probability produce Anomaly Detection.Then Calculate Detection Rate and fitness value calculation according to the implementation of rules and Gnp.

- Link utilisation

In this rule it will give the statistical value how much the link is utilised for the transaction.

- Link state

In this rule it will show the capability of the link size whether it is capable to transfer the packet.

- Link quality measurement

In this rule it will give the strength of the link. somecase it may get weaker of continuous transaction.

- Scalability

This rule gives the possibility of stretching up of the path to connect nodes may get packet loss of adhoc-nature.

- Load balancing

This rule provides capability of the link which can transfer only a limited packets based apon their size.

- Improved process Data model

This rule is based on the normal behaviours of processing node in the datamodel.

- Cluster centers

In this rule the neighboring node which in the cluster.

E. FUZZY CLASS ASSOCIATION RULE MINING

First, minimum support is applied to find all frequent packets in a database.Second, these frequent packets minimum confidence constraint are used to form rules.Sub attribute utilization-Network connection have thier own characterstics such as discrete and continues attribute and these attribute values are important informations that cannot be loss.In this process introduce a sub attribute utilization mechanism concerning binary and simbolic and continues attribute to keep the completness of data information.Binary attributes are divided into two sub attributes corresponding to judegement function.for eg.Binary attribute A1(=Land) was divided into A'11(representing Land=1)and A'12(representing Land-=0) The symbolic attribute was divided into several sub attributes while the continues attribute was also divided in the three sub attributes.

Conserning the values represented by lingustic terms (low,middle and high)of fuzzy membership function perdefined for each continues attributes.J1,J2,....Jm(m is the total number of judgment functions),serve as decision functions that return judgment results so as to determine the next node.Processing nodes,P1,P2,...Pn(n is the total number of processing functions),serve as action/processing functions.Three kinds of genetic operators i.e,selection,mutation and crossover are implemented in GNP.

- Selection

Individuals are selected according to their fitness.

- Crossover

Two new offsprings are generated from two parents by exachanging the genetic information the selected nodes and their connections are swapt by each other by crossover.

- Mutation

One new individual is generated from one original individual by the following operators.Each node branch selected with the probability and reconnected to another node.Each node function is selected with the probability and changed to another one.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

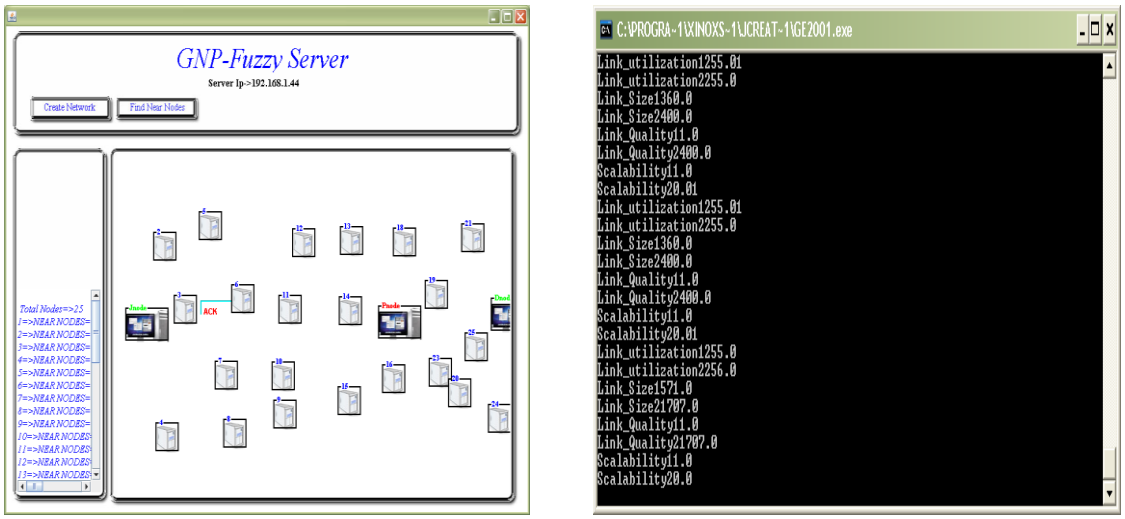
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

IV EXPERIMENTAL SET UP

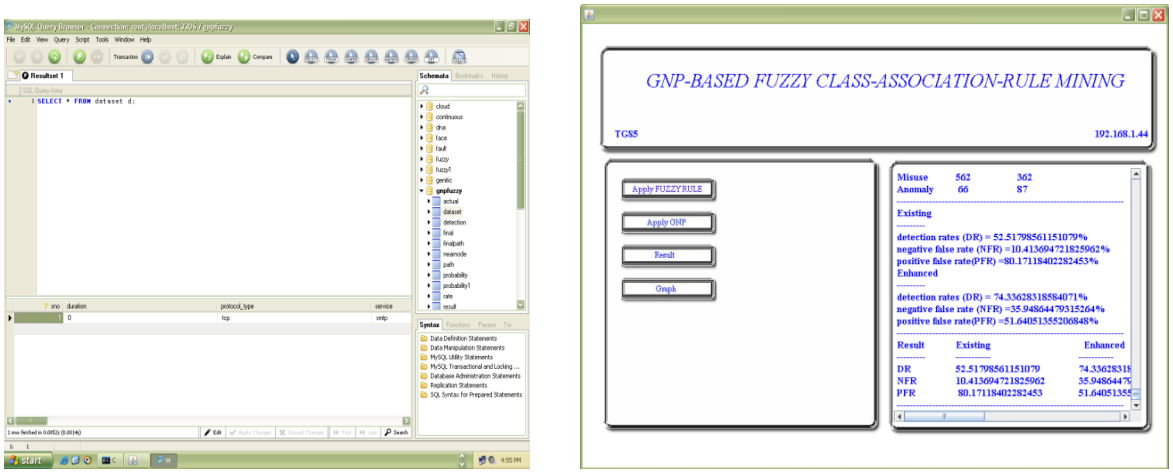
GNP-based fuzzy class-association-rule mining can deal with both discrete and continuous attributes in the database, which is practically useful for real network-related databases.The proposed fitness function contributes to mining more new rules with higher accuracy.The proposed framework for intrusion detection can be flexibly applied to both misuse and anomaly detection with specific designed classifiers.Experienced knowledge on intrusion patterns is not required before the training.High detection rates (DRs) are obtained in both misuse detection and anomaly detection.

V RESULTS AND DISCUSSION



(a) (b)

Fig2 (a) The above fig which provides a environment of 20 nodes with possible shortest path based on destination node and transmission node stimulates the transmission and receiving ack (b) the above provides the assessment of rule minied based on fuzzy and gnp.



(C) (d)

Fig. 2. (c) the above database creation with my sql with kddcup and darpa dataset. (d) the above which provides the detection rate ,false detection rate ,positive detection rate after gnp.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

VI CONCLUSION

In this paper, a GNP-based fuzzy class-association-rule mining with sub attribute utilization and the classifiers based on the extracted rules have been proposed, which can consistently use and combine discrete and continuous attributes in a rule and efficiently extract many good rules for classification.As an application,intrusion-detection classifiers for both misuse detection and anomaly detection have been developed and their effectiveness is confirmed using KDD99Cup and DARPA98 data. The experimental results in the misuse detection show that the proposed method shows highDR and lowPFR,which are two important criteria for security systems.In the anomaly detection, the results show high DR and reasonable PFR even without pre experienced knowledge,which is an important advantage of the proposed method

REFERENCES

[1] Shingo Mabu, *Member, IEEE, Ci Chen, Nannan Lu, Kaoru Shimada,*and Kotaro Hirasawa*, Member, IEEE ,"A*n Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming".January 2011.

[2] Kddcup99data[Online].Available:kdd.ics.uci.edu/databases/kddcup 99/kddcup99.html

[3] J. G.-P. A. El Semaray, J. Edmonds, and M. Papa, "Applying data mining of fuzzy association rules to network intrusion detection," presented at the IEEE Workshop Inf., United States Military Academy, West Point, NY, 2006. A. Criminisi, P. Perez, and K. Toyama, "Region filling and object removal by exemplar-based image inpainting.", IEEE Transactions on Image Processing, vol. 13, no.9, pp. 1200–1212, 2004.

[4] W. Hu, W. Hu, and S. Maybank, "Adaboost-based algorithm for network intrusion detection," *IEEE Trans. Syst.,Man, Cybern. B, Cybern.*, vol. 38, no. 2, pp. 577–583, Apr. 2008.