Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Increment Feature Selection Approach for Intrusion Detection System in MANET

K. Rajesh Kambattan[1], R. Manimegalai[2], S. Ganapathy[3]
[1]*Department of CSE, Dhaanish Ahmed College of Engineering, Chennai, INDIA.*
[2]*Department of CSE, Park College of Engineering and Technology, Coimbatore, INDIA.*
School of Computing Science and Engineering, VIT University, Chennai, INDIA.

Abstract: ***Network security is very important in this internet world. Now, all kind of activities such as money transactions, buying and selling are done through internet only. Many security mechanisms have been introduced in the past decades in this direction. No one provides the sufficient detection accuracy on current internet attacks. Dynamics attacks are increasing daily due to the number of users increased in online. For providing better classification accuracy and detecting novel internet attacks, we propose an ideal intrusion detection system for improving the detection rate. The proposed system is the combination of Cuttle Fish Feature Selection algorithm, Extended Chi-square algorithm and the existing classification algorithm called IAEMSVM to build a better input sets to IDS. The experimental results of the proposed system show that the system is reduced the computation time with less features and better result when tested with KDD Cup 99 data set.***
Keywords: Intrusion Detection System, Feature Selection, CFA and Chi-square.

I. INTRODUCTION

The objective of intrusion detection model is detect various types of misbehave activity. The main function of IDS is monitoring the network activity. The traditional system like firewall and authentication was failed to detect malicious activity in mobile environment since lack of infrastructure, all nodes in MANET are mobile nature. IDS comes into two categories:. Network level IDS and . Host level IDS. In MANET, attacks can be identified by alert management system, which means alarms can be generated when anything went wrongly. But lack of technology still we are facing lot of problems like false alarm rate. Generally, IDS monitor and capture two type of behaviour namely known attacks and unknown attacks. The traditional methods are very easy to capture known attacks but any deviation from normal behaviour which is not already stored is difficult to capture. A significant amount of research has been taken to develop effective and intelligent intrusion detection system.

Feature is a method to remove irrelevant content and repeated features and selecting the best subset for attributes that produces better simplification of patterns belonging to dissimilar groups. Feature selection methods are divided into wrapper method and filter method. Due to continuous growth of data dimensionality, selecting relevant features through pre-processing could be a convenient one and avoids calculation overhead. For feature reduction, some techniques adopt feature adding concept and others they follow feature reduction. Based on problem nature any one of the techniques shall be adopted. The main advantage of feature selection process is to save time and yields better result rather than full data set.

The classification algorithms have been highly used in MANET for intrusion detection. Classification in the sense that data is classified or segregated according to its nature or behaviour. In mobile environment, due to heavy network usage, the messages are lost or not delivered properly to intensive recipient. These problems are identified by malicious or intruders. With the help of classification algorithm or technique, normal user and misbehave user can be segregated separately. Attackers can have a two type of classification such as passive attack, they gain knowledge without disturbing others, but active attacker gain knowledge and the same time, they disturb others like DoS. In this paper, a new intrusion detection system is proposed in this paper for detecting novel attacks. Moreover, a new feature selection algorithm called Incremental Feature Selection Algorithm (IFSA) is proposed for effective feature selection. The proposed feature selection algorithm is the combination of Cuttle Fish Feature Selection algorithm and Extended Chi-square algorithm . The proposed intrusion detection system uses the existing classification algorithm IAEMSVM [13] and the proposed feature selection algorithm. Rest of this paper is organized as follows: Section 2 provides the related works. Section 3 explains the proposed work. Section 4 provides the result and discussion. Section 5 gives conclusion and future works.

II. LITERATURE SURVEY

There are many intrusion detection systems have been proposed and implemented in this direction in the past decades. Among them,

Volume 5 Issue I, January 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Wei-Chao Lin et al proposed a novel feature selection procedure, namely the Cluster Center and Nearest Neighbor (CANN). Their work purely based on distance calculation between each data sample and its cluster center and doing same function on data and nearest neighbour in the same cluster. Then each data can be applied into intrusion detection process by k-NN classifier which produces high computational efficiency and detection rate is high. A new hybrid intrusion detection system was proposed by Yuk et al. In this work, they used intelligent dynamic swarm based rough set (IDS-RS) for feature selection and simplified for data classification. SSO performance can be improved here by adding new weighted local search for obtaining better result.

Fangjun et alwas proposed an intrusion detection by novel support vector machine model combining kernel principal component analysis and genetic algorithm. This proposed model was achieved higher predictive accuracy, faster convergence speed and better generalization. Mohammed et al was proposed mutual information based feature selection algorithm can solve all types of data. Here, Least Square Support Vector Machine based IDS was implemented for effective feature selection.

Aikaterini Mitrokotsa et al was proposed intrusion detection system for MANET using effective classification based on cost matrix and also how affects the classification by cost matrix. Here unknown attacks are identified by cross validation of tuned classifier. Seung et al was proposed optimal feature selection algorithm based on local search. According to this concept intrusion detection can be done easily by machine learning techniques, which gives better result. The network intrusion detection was enhanced by RS-ISVM by Yang et al. Concentric circle method was adopted here for picking up a sample data from reserved set for reducing computational timing. It achieves good performance and high reliability.

Veronica et al was dealt about unified pipeline for on-line learning for new coming huge new data set. Here they used three types of classical methods for promising results such as k-means discretizer, chi square filter and one layer artificial neural network. Shih et al was proposed an anomaly intrusion detection system with the help of support vector machine, decision tree and simulated annealing. Anomaly detection is tedious one to find by IDS. Here parameters are adjusted based on annealing by SVM and DT. A new ensemble classifier was proposed by Abdulla et al for effective intrusion detection. Their work relied on better accuracy by PSO, its generates weight to enable best classifier and Local unimodal sampling method is applied for behaviour identification. Ganapathy et al was proposed new hybrid feature selection method for intrusion detection in MANET.

III. SYSTEM ARCHITECTURE

The overall architecture of the proposed model is shown in figure 3.1. The main components of proposed is consists of five such as Intrusion Detection System, User Interface, KDD'99 cup data set, Classification module and Result.

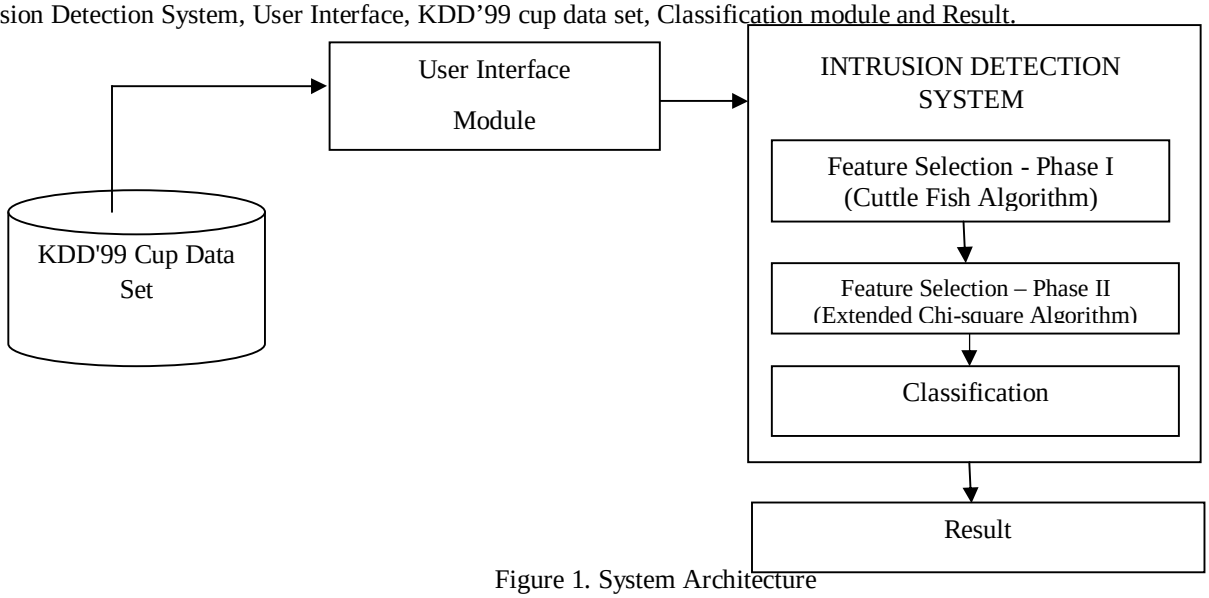

Figure 1. System Architecture

Data set is nothing but it is a collection of network traffic data collected by US Government and issued for research purpose. In IDS, two main sections are there namely feature selection phase I and II. These are used to filter relevant data for further processing and very helpful to identify attacks with efficient time consumption. At last, the classified details (normal and abnormal data) are sent to result.

IV. PROPOSED WORK

This section dealt about the proposed system. In this section, we have discussed in detail about cuttle fish algorithm (CFA) [12],

Extended Chi-square algorithm [11] and also explain the role of classification algorithm in this proposed system.

A. Feature Selection

We have used the existing cuttle fish algorithm [12] and Chi-square [11] for effective feature selection and classification. This cuttle fish algorithm is supporting dynamic decision over the feature selection process based on the environments and Extended chi-square algorithm to check the inconsistency level derived from previous level and allow the most relevant features to next level.

The adjacent two intervals of the set could be merged, that $\chi 2$ value is computed from the adjacent two intervals and the threshold value difference is also greater than other $\chi 2$ value. When two adjacent intervals have a maximal difference in the calculated $\chi 2$ value and threshold should be merged first.

Compute $\chi 2$ value by using the following formula,

$$\chi^2 = \sum\sum\left(\frac{Aij-Eij}{Eij}\right) \quad (1)$$

Where, m = 2 (the 2 intervals being compared), k = Number of classes, Aij = Number of examples in ith interval, jth class, Ri = Number of examples in ith class, Cj = Number of examples = $\sum$ j=1 Cj and Eij = Expected frequency of Aij = (Ri * Cj) / N.

Incremental Feature Selection Algorithm

Input : KDD Cup Dataset

Output: Dataset with Selected features

Initialize the necessary values

Compute the Chi-square value for the given set of records

Perform the Merging operation over the different two sub datasets

Find the inconsistency rate for the merger in merger

Perform the decreasing operation on significant level of records

Compute the finer of Chi-square value

Perform the Finer Merge operation over the dataset

Check whether the inconsistency rate is much finer for a merger.

Apply the Cuttle fish algorithm

List the selected features

B. Classification

We have used the existing and efficent classification algorithm called Intelligent Agent based Multiclass Support Vector Machine (IAEMSVM) algorithm [13] for effective classification. This technique uses the clustering technique, intelligent agent and decision tree for improving the classification accuracy.

V. RESULT AND DISCUSSION

This section discussed about the KDD'99 cup dataset which is used for evaluating the proposed system. Moreover, the experimental results also demonstrated with necessary justification over the achievement.

A. KDD'99 Cup Data Set

The KDD'99 Cup dataset [15] is used for carrying out the experiments. This dataset contains five million records and each connection record is described by 41 features. It has 22 categories of attacks from the following four classes such as DoS, R2L, U2R, and Probe. It has 391458 DOS attack records, 52 U2R attack records, 4107 Probe attack record, 1126 R2L attack records, and 97278 normal records only in this 10 percent of this data set.

B. Experimental Results

Five experiments have been conducted with different set of records. Here, we have used the three different feature selection

algorithms along with IAEMSVM. Table 1 shows the performance of the proposed feature selection technique and others.

Table 5.1 Performance of the proposed Intrusion Detection System

Ex. No.	CFA + IAEMSVM	ECSA + IAEMSVM	IFSA + IAEMSVM
1	99.35	99.32	99.52
2	99.29	99.22	99.49
3	99.17	99.13	99.77
4	99.26	99.17	99.66
5	99.21	99.12	99.52

From table 1, it can be seen that the performance of the proposed system is better with 9 features which are selected by IFSA. The reason for this difference in terms of accuracy of the proposed system is due to the uses of different number of features selected by IFSA. According to the IFSA, it can be considered the best detection accuracy produced by the proposed system with the use of particular subset among different subsets.

Figure 2 shows the comparative analysis between the proposed system (IFSA+IAEMSVM) and the existing systems (CFA+DT) [1] and IAEMSVM +CFA [12]. Here, we have considered three different sets which are contain 10, 15 and 20 features.

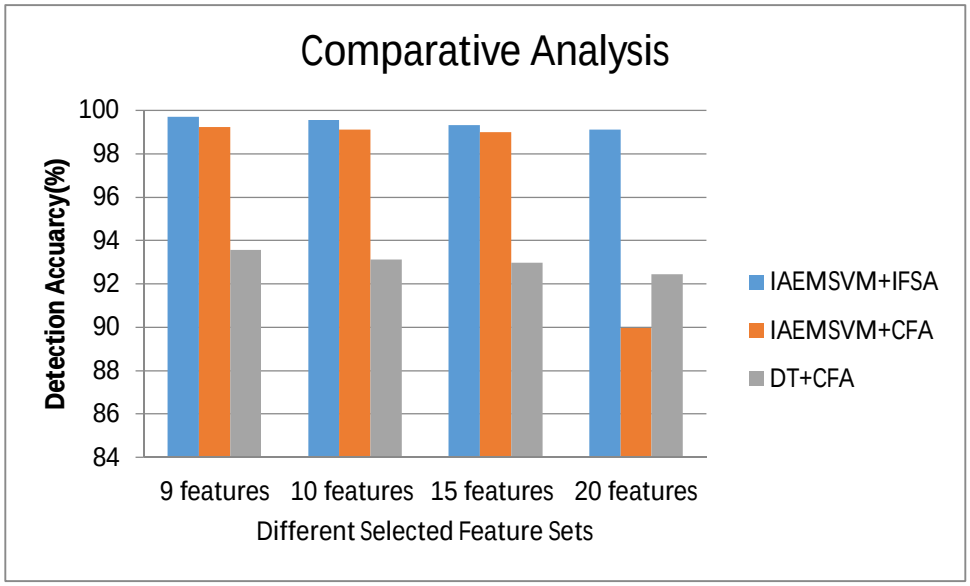

Figure 2 Comparative Analysis

From this figure, it can be observed that the performance of the proposed system is better than the existing system when we have considered all three different numbers of selected features for the experimental analysis. The reason for the better performance of the proposed system is the uses of effective classification algorithm.

VI. CONCLUSION AND FUTURE WORKS

In this paper, a new intrusion detection system is proposed in this paper for detecting novel internet attacks. Moreover, a new Incremental Feature Selection Algorithm (IFSA) is also proposed and implemented for effective feature selection. The proposed feature selection algorithm is the combination of Cuttle Fish Feature Selection algorithm and the Extended Chi-square algorithm. The experimental results shows the performance of the proposed system which are achieved above 99% detection accuracy in all types of attacks. Future works in this direction could be the introduction of new spatio-temporal fuzzy rules.

REFERENCES

[1] Wei-Chao Lin, Shih-Wen Ke and Shih-Fong Tsai, “CANN: An intrusion detection system based on combining cluster centers and nearest neighbors”, Knowledge-Based Systems, Elsevier, vol. 78, pg. 13-21, 2015.

Volume 5 Issue I, January 2017
ISSN: 2321-9653

[2] Yuk Ying Chung and Noorhaniza Wahid, “A hybrid network intrusion detection system using simplified swarm optimization (SSO)”, Applied Soft Computing, Elsevier, vol. 12, pg. 3014-3022, 2012.
[3] Fangjun Kuang, Weihong Xu and Siyang Zhang, “A novel hybrid KPCA and SVM with GA model for intrusion detection”, Applied Soft Computing, Elsevier, vol. 18, pg. 178-184, 2014.
[4] Mohammed A. Ambusaidi, Xiangjian He, Priyadarsi Nanda and Zhiuan Tan, “Building an intrusion detection system using a filter-based feature selection algorithm”, IEEE Transactions on Computers, 2014.
[5] Aikaterini Mitrokotsa and Christos Dimitrakakis, “Intrusion detection in MANET using classification algorithms: The effects of cost and model selection”, Ad Hoc Networks, Elsevier, vol. 11, pg. 226-237, 2013.
[6] Seung-Ho Kang and Naju, “A Feature Selection algorithm to find optimal feature subsets for Detecting DoS attacks” IEEE Conference of Decision Making, pp. 12-17, 2015.\
[7] Yang Yi, Jiansheng Wu and Wei Xu, “Incremental SVM based on reserved set for network intrusion detection”, Expert Systems with Applications, Elsevier, vol. 38, pg. 7698-7707, 2011.
[8] Veronica Bolon-Canedo, Diego Fernandez-Francos, Diego Peteiro-Barral, Amparo Alonso-Betanzos, Bertha Guijarro-Berdinas and Noelia Sanchez-Marono, “A unified pipeline for online feature selection and classification”, Expert Systems with Applications, Elsevier, vol. 55, pg. 532-545, 2016.
[9] Shih-Wei Lin, Kuo-Ching Ying, Chou-Yuvan Lee and Zne-Jung Lee, “An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection” Applied Soft Computing, Elsevier, vol. 12, pg. 3285-3290, 2012.
[10] Abdulla Amin Aburomman and Mamun Bin Ibne Reaz, “A novel SVM-KNN-PSO ensemble method for intrusion system”, Applied Soft Computing, Elsevier, vol. 38, pg. 360-372, 2006.
[11] Ganapathy S., Rajesh Kambattan K., Veerapandian N. and Pasupathy M, “An Intelligent Intrusion Detection System model for MANET’s based on Hybrid Feature Selection”, Artificial Intelligent Systems and Machine Learning, CiiT, vol. 3, pg. 13, 2011.
[12] Rajesh Kambattan K. and Manimegalai R, “An Effective Intrusion Detection System using CRF based Cuttlefish Feature selection algorithm and MSVM”, Asian Journal of Information Technology, vol. 15, pg. 891-895, 2016.
[13] Sannasi Ganapathy, Kanagasabai Kulothungan, Sannasy Muthurajkumar, Muthusamy Vijayalakshmi, Palanichamy Yogesh, Arputharaj Kannan, “Intelligent feature selection and classification techniques for intrusion detection in networks: a survey”, EURASIP Journal on Wireless Communications and Networking, Vol. 2013, No.1, pp. 1-16, 2013.