ORIGINAL RESEARCH PAPER
VOLUME-6 | ISSUE-6 | JUNE-2017 | ISSN No 2277 - 8179 | IF : 4.176 | IC Value : 78.46
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

A HYBRID METHOD FOR FEATURE SELECTION IN INTRUSION DETECTION SYSTEM BASED ON DCA AND PCNN NETWORK

Computer Science

Brajesh Kumar M.Tech. Scholar, IES college of Technology, Bhopal

Prof. Aishwarya Mishra Associate Professor, Department, IES college of Technology, RGPV Bhopal, India

ABSTRACT

No matter how large or small your company is, you need to have a plan to ensure the security of your information assets. Such a plan is called a security program by information security professionals. A security program provides the framework for keeping your company at a desired security level by assessing the risks you face, deciding how you will mitigate them, and planning for how you keep the program and your security practices up to date. Feature selection is always beneficial to the field like Intrusion Detection, where vast amount of features extracted from network traffic needs to be analyzed. All features extracted are not informative and some of them are redundant also. A hybrid method using DCA and PCNN network algorithm are useful for reduced feature selection in IDS.

KEYWORDS:

Information Security, Feature selection, Swarm Intelligence, DCA algorithm, PCNN network.

INTRODUCTION

With the wide and quick development of network technology, in the field of social networking, e-business, e-learning and online shopping, Security is a big issue for all networks in today's enterprise environment. Hackers and intruders have made many successful attempts to bring down high-profile company networks and web services. Many methods have been developed to secure the network infrastructure and communication over Internet. Some of them are the use of firewalls, encryption, and virtual private networks. Intrusion detection is a relatively new addition to such techniques. Intrusion detection methods with machine intelligence started appearing in the last few years. Using intrusion detection methods, you can collect and use information from known types of attacks and find out if someone is trying to attack your network or particular hosts. An Intrusion Detection System (IDS) is the device (or application) that monitors network/system activities and the analyzing of data for potential vulnerabilities and attacks in progress; it also raises alarm or produces report. Different sources of information and events based on information are gathered to decide whether intrusion has taken place. This information is gathered at various levels like system, host, application, etc. Based on analysis of this data, we can detect the intrusion based on two common practices – Misuse detection and Anomaly detection. Misuse detection IDS models function in very much the same sense as high-end computer anti-virus applications. That is, misuse detection IDS models analyze the system or network environment and compare the activity against signatures (or patterns) of known intrusive computer and network behavior. Anomaly detection takes the normal observation model and uses statistical variance or expert systems to determine if the system or network environment behavior is running normally or abnormally. Reduce the search space by removing irrelevant variables so that

(a) Only interrelated variables with the class label are selected,
(b)The intelligent algorithm is able to come up with results based on the available computing resources. This often happens when we filter out massive numbers of variables in the input dataset because of a necessity to minimize the data dimensionality.

RELATED WORK

In the past few years, a swarm intelligence feature selection algorithm was proposed based on the initialization and update of only a subset of particles in the swarm by Martinez, Gene doublets concept was introduced by Chopra, based on the gene pair combinations. A new ensemble gene selection method was applied by Liu, to choose multiple gene subsets for classification purpose, where the significant degree of gene was measured by conditional mutual information or its normalized form.

ATTRIBUTE SELECTION AND CLASSIFICATION TECHNIQUES

Intrusion detection can be thought of as a classification problem: we wish to classify each audit record into one of a discrete set of possible categories, normal or a particular kind of intrusions. Given a set of records, where one of the features is the class label (concept), classification algorithms can compute a model that uses the most distinguishing (unique) feature values to describe each concept. So, classification tasks typically require the construction a function (classifier) that assigns a class label to each data item described by a set of attributes. The term data mining is frequently used to designate the process of extracting useful information from large databases. There are a wide variety of data mining algorithms, drawn from the fields of statistics, pattern recognition, machine learning, and databases. Several types of algorithms are particularly relevant to intrusion detection.

a) PULSE COUPLED NEURAL NETWORK

A PCNN is a two-dimensional neural network. Each neuron in the network corresponds to one pixel in an input image, receiving its corresponding pixel's color information (e.g. intensity) as an external stimulus. Each neuron also connects with its neighboring neurons, receiving local stimuli from them. The external and local stimuli are combined in an internal activation system, which accumulates the stimuli until it exceeds a dynamic threshold, resulting in a pulse output. Through iterative computation, PCNN neurons produce temporal series of pulse outputs. The temporal series of pulse outputs contain information of input images and can be used for various image processing applications, such as image segmentation and feature generation. Compared with conventional image processing means, PCNNs have several significant merits, including robustness against noise, independence of geometric variations in input patterns, capability of bridging minor intensity variations in input patterns, etc.

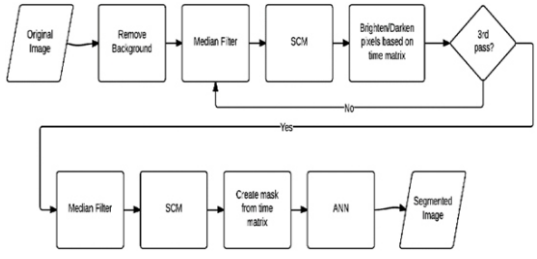

Fig: PCNN network

b)DENDRITIC CELL ALGORITHM

DCA (DC Algorithm), an innovative approach in nonconvex programming is then developed to solve the resulting problem.

Pseudocode for the Dendritic Cell Algorithm.
Input: Input Patterns, $iterations_{max}$, $cells_{num}$, $Migration Thresh_{bounds}$

Output: Migrated Cells
Immature Cells $\left arrow$ Initialize Cells($cells_{num}$,
$Migration Thresh_{bounds}$)
Migrated Cells $\left arrow$ $\empty set$

For ($i=1$ **To** $iterations_{max}$)
P_i $\left arrow$ Select Input Pattern(Input Patterns)
k_i $\left arrow$ (Pi_{danger} – 2 $\times$ Pi_{safe})
cms_i $\left arrow$ (Pi_{danger} + Pi_{safe})
For ($Cell_i$ $\in$ Immature Cells)
Update Cell Output Signals($Cell_i$, k_i, cms_i)
Store Antigen($Cell_i$, $Pi_{antigen}$)
If ($Celli_{lifespan}$ $\leq$ 0)
Reinitialize Cell($Cell_i$)
ElseIf ($Celli_{csm}$ $\geq$ $Celli_{thresh}$)
Remove Cell(Immature Cells, $Cell_i$)
ImmatureCells $\leftarrow$
CreateNewCell($MigrationThresh_{bounds}$)
If ($Celli_{k}$ < 0)
$Celli_{type}$ $\left arrow$ Mature
Else
$Celli_{type}$ $\left arrow$ Semi mature
End
Migrated Cells $\left arrow$ $Cell_i$
End
End
End

Return (Migrated Cells)

CONCLUSIONS

In this paper, a survey on intelligent techniques for feature selection and classification techniques used of Intrusion Detection has been presented and discussed. In addition, a new feature selection algorithm called DCA and PCNN network algorithm. In this paper, intelligent algorithms for feature selection and classification have been proposed to design an effective intrusion detection system. The scope of this paper includes neural networks, fuzzy systems, genetic algorithm and particle swarm intelligence. The advantages and disadvantages of these intelligent techniques have been analyzed. The contributions of various research works in IDS are systematically summarized and compared, which allows us to clearly define existing research challenges and highlight promising new research directions. In addition the need for the new intelligent feature selection also called DCA algorithm has been highlighted based on experimental results. In addition, the advantage of proposing the new classification also called PCNN network has been discussed in detail so that the proposed system can be used to provide security to networks effectively.

REFERENCES:

[1] Shi-Jinn Horng, Ming-Yang Su, Yuan-Hsin Chen, Tzong-Wann Kao, Rong-Jian Chen, Jui-Lin Lai and Citra Dwi Perkasa "A novel intrusion detection system based on hierarchical clustering and support vector machines", Elsevier, 2011, Pp 306-313.
[2] Gaby Abou Haidar and Charbel Boustany "High Perception Intrusion Detection Systems Using Neural Networks", IEEE, 2015, Pp 497-501.
[3] D. P. Gaikwad and Ravindra C. Thool "Intrusion Detection System Using Bagging Ensemble Method of Machine Learning ", IEEE, 2015, Pp 291-295.
[4] Shelly Xiaonan Wu and Wolfgang Banzhaf "The Use of Computational Intelligence in Intrusion Detection Systems: A Review", Applied Soft Computing, 2010, Pp 2-42.
[5] Preeti Singh and Amrish Tiwari "An Efficient Approach for Intrusion Detection in Reduced Features of KDD99 using ID3 and classification with KNNGA", IEEE, 2015, Pp 445-452.
[6] Asaf Shabtai, Uri Kanonov and Yuval Elovici "Intrusion detection for mobile devices using the knowledge-based, temporal abstraction method", The Journal of Systems and Software, 2010, Pp 1524–1537.
[7] Monowar H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita "Network Anomaly Detection: Methods, Systems and Tools", IEEE, 2014, Pp 303-336.
[8] S. Revathi and Dr. A. Malathi "A Detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques for Intrusion Detection", IJERT., 2013, Pp 1848-1853.
[9] Mahbod Tavallaee, Natalia Stakhanova and Ali A. Ghorbani "Towards Credible Evaluation of Anomaly-based Intrusion Detection Methods", IEEE, 2010, Pp 1-10.
[10] Shaik Akbar, Dr.K .Nageswara Rao and Dr. J.A. Chandulal "Intrusion Detection System Methodologies Based on Data Analysis", International Journal of Computer Applications, 2010, Pp 10-20.
[11] Jayveer Singh and Manisha J. Nene "A Survey on Machine Learning Techniques for Intrusion Detection Systems", International Journal of Advanced Research in Computer and Communication Engineering, 2013, Pp 4349-4355.
[12] A. M. Chandrashekhar and K. Raghuveer "FORTIFICATION OF HYBRID INTRUSION DETECTION SYSTEM USING VARIANTS OF NEURAL NETWORKS AND SUPPORT VECTOR", IJNSA, 2013, Pp 71-90.
[13] Álvaro Herrero, Martí Navarro, Emilio Corchado and Vicente Julián "RT-MOVICAB-IDS: Addressing Real-Time Intrusion Detection",Elsevier, 2013, Pp 1-24.
[14] Bharanidharan Shanmugam and Norbik Bashah Idris "Hybrid Intrusion Detection Systems (HIDS) using Fuzzy Logic", Intrusion Detection Systems, 2011, Pp 1-21.
[15] S. Saravana kumar, Uma maheshwari , D. Jayalakshmi and R.Sugumar "Development and Implementation of Artificial Neural Networks for Intrusion Detection in Computer Network ", IJCSNS, 2010, Pp 271-275.