PROPOSING BPN BASED IDS FOR SECURITY IN CLOUD

[1]Vaibhav Kant Singh, [2]Devendra Kumar Singh
Department of Computer Science & Engineering, Institute of Technology
Guru Ghasidas Vishwavidyalaya, Central University, Bilaspur, (C.G.), India
Email: [1]vibhu200427@gmail.com , [2]devendra.singh170@gmail.com

Abstract— The network is flood with huge amount of information. With the advancement in Internet Technology there is transmission of data from source to destination. A new concept of Cloud is introduced which enable user to have a platform utilizing which a number of facilities can be utilized at the client end without the facilities actually present in the system. In this paper we have proposed the construction of IDS using BPN to control the access of Intruders in the Cloud.

***Index Terms*—Intrusion Detection System (IDS), Cloud, Back Propagation Network (BPN), Infrastructure as a Service (IAAS), Software as a Service (SAAS), Platform as a service (PAAS), Network as a Service (NAAS), Storage as a Service (STASS).**

I. INTRODUCTION

Cloud provides an environment where the user present in the client machine is able to have access on various resources present in the other machine. Cloud provides an environment to the user where he can run his program on a system which is not having configuration desired to run the program.

II. CLOUD

Cloud computing is not a new technology it is existing for some time in the recent past. Currently the technology is used in a wide extent. In yester years only a few companies were making use of it. Now, even individuals are using the concept in day to day life. Looking to the reliability given by the cloud computing paradigm now all small and large companies are adopting it in their framework. When Internet came into existence the number of people making use of the technology was less. But as time passed the utility of the cloud concept has increased. Previously internet was mainly utilized for providing information. But now the focus has changed. Now websites not only provide information it also provide platform for submitting information for others. Now even social sites are present which are keeping people up to date with their family and friends. As the number of users had increased in internet the amount of data accumulated has increased, this advancement had resulted an increase in the number of server to process the user requests. Now various clusters of server are formed which manage Pentabyte of space for processing. The formed clusters had taken the form of Grid. Various clusters are collaborated to form Grid. In environment where thousands of servers are connected and deployed form a datacenter. Big Companies have their own data center. The Data centers possed by these companies want to have communication with each other. The technology which could be utilized to perform the above objective is Cloud Computing. Cloud computing is a collection of various technologies like remote access, virtualization, network virtualization etc. Cloud computing is a group of cluster and grid which have many computers or server forming a infrastructure. The framework we use according to our flexibility. Cloud service provider provides various services to the user like some user may demand for space, some user may ask for remote access, some user may ask for some type of software, some may require some network utility or device etc. The Cloud service provider require internet for providing the facilities to the user. As already discussed various big companies are maintaining their own cloud. Example of clouds include Google Cloud, Amazon web service, Microsoft ozure, IBM cloud, Rackspace, NASA's open source project-Openstack. The companies having cloud work as cloud service providers to the various users on internet. Cloud are basically of three types Public Cloud, Private Cloud and Hybrid Cloud. There are five classification representing the set of services provided by cloud. The five services are IAAS, SAAS,PAAS,NAAS and STASS.

A. IAAS

In this type of service the Cloud service provider provides the whole infrastructure for the user. This is indeed very powerful service provided by the Cloud service provider. In this service a highly configured operating system is provided to the user. In this category Amazon ranked first. Virtualization concept is utilized for availing the service to the user. Using virtualization on a single server several operating systems are made to run. IBM also supports various companies by providing the infrastructure service.

B. SAAS

Under this category the Cloud service provider provides software to the cloud user. In this type the user need not install the software in its machine. Using the X-Window system from any server the software can be made available to the user. In the current time the biggest example of SAAS is the Gmail service which is on an average used by every fifth person. Beside this Google docs, Microsoft Online Office etc. are some of the online developing tools.

C. PAAS

This category deals with providing Platform to the user. The provided platform is used by the software developers for creating various customized softwares. Some example include Google app Engine, Twitter API or Facebook API. Engine yard for used application developing using ruby on rail, PHP and node is Red Hat openshift.

D. NAAS

In this category users are provided high speed network for their data transfer. In this category various service comes like virtual private network (VPN), Bandwidth on demand, Mobile network virtualization, AWS provide service bandwidth on demand.

E. STASS

In this category the Cloud is responsible for giving storage space to the users. This is of two types namely Block storage and Object storage. Block storage is unformatted partition which is made available to the cloud user by the cloud service provider. The user may use the storage space as a native space or may format the space and may specify its own file system. Examples of this include AWS and E2S service. Object storage is file system which is flexible storage directly mounted in the users system. This is like a drive in Computer System. Examples of this include Google Drive, Drop box, UC Cloud etc. Now a day's almost all companies are providing this service. Block storage is provided through SCSI protocol whereas Object storage is provided through NFS or SSHFS.

III. INTRUSION DETECTION SYSTEM

The types of intruders include Masquerador, Misfeasor and Claridestine users. Intrusion Detection System is a Software Application that tracks network or system policy violations and produces reports to a management console. There are two types IDS i.e. Network Based IDS and Host Based IDS. The basic components of IDS technology types Host-based IDS, Network-based IDS, Wireless-based IDS, Network behavior Analysis BA and Mixed IDS. The components in IDS include sensor and agent, where the former in typically used for NIDS, WIDS and NBA systems to monitor networks and HIDS uses the latter to monitor and analyze activities. Intrusion Detection and Prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them and reporting attempts. Classification of IDPS technologies are Network based IDPS, Wireless based IDPS, Network based analysis and Host based. Detection Classification is basically of three types namely computation depended approach, artificial intelligence and biological concepts. Beside the basic approaches there are new detection approaches also namely statistics based, pattern based, rule based, state based and heuristic based approach.

IV. PROBLEM STATEMENT

Several users are making access to the same cloud. When several users are running in the same area there is always a chance of one user trying to make an access in the area of other user to have an advantage of some type. This gave the rise for the notion of an Intrusion Detection System (IDS).

V. LITERATURE SURVEY

In [1] post processing filter is proposed to reduce false positives in **network based** intrusion detection. The filter comprises three components, each one of which is based upon statistical properties of the input alert set. Special characteristics of alerts corresponding to true attacks are exploited. These alerts may be observed in batches, which containing similarities in the source of destination IPs, they may produce abnormalities in the distribution of alerts of the same signature. False alerts can be recognized by the frequency with which is their signature triggers false positive. In this paper apply approach can significantly reduce the number and percentage of false positive produced by “Snort”. In [2] MANETs are vulnerable to a of network layer attacks such as Black hole, Gray hole, sleep derivation and Rushing attacks. In this paper, intrusion detection and adaptive response mechanism for MANETs that detect a range of attacks and provides an effective response with low network of degradation. We consider the deficiencies of a fixed response to an intrusion and we overcome these deficiencies with a flexible response scheme that depends on the measured confidence is the attack , the severity of attack and the degradation in network performance. In these scheme shows that it allows a flexible approach to management of threats attacks demonstrates improved network performance with a low network overhead.In [3] IDS deals with huge amount of network traffic and uses large feature set to discriminate normal p attern and intrusive pattern. However, most of existing real-time anomaly detection. In this paper propose a 3-Tier iterative Feature Selection Engine (IFSEng) for feature subspace selection. Principal Component Analysis (PCA) technique is used for the pre-processing of data. Problems are huge amount of network traffic. Find the normal pattern and intrusive pattern. Lack the ability to process data for real-time anomaly detection. Provide solution for problem 3-Tier iterative feature selection engine (IFSEng) for feature subspace selection.In [4] their objective is to protect against attempts to violate defense mechanisms. Indeed, IDSs themselves are part of the computing infrastructure, and thus they may be attacked by the same adversaries they are designed to detect. This is a relevant aspect, especially in safety-critical environments. Such as hospitals, aircrafts, nuclear power plants etc. they are giving an overview on adversarial attacks against IDSs. An extensive description of how such attacks can be implemented by exploiting IDS weakness at different abstraction levels. For each attack implementation a critical investigation to the proposed solution and open points. Provide solution for the problem highlight the most promising research directions for the design of adversary-aware, harder to defeat IDS solution.In [5] The deployment of wireless sensor networks and mob ad-hoc network in applications such as emerging services, warfare as e and health monitoring poses the threat of various hazards cyber hazards, intrusions and attacks as a consequence of these network’s openness. Among the most significant research difficulties in such liable target is to distingvuuish between misuse and abnormal behavior so as to ensure secure, reliable networks operations and services. In [6] Artificial Neural Network (ANN) can improve the performance of IDS when compared with traditional methods for ANN based IDS, detection precision, especially for low-frequent attacks and detection stability are still needed to be enhanced. For the solution they are applying new approach FC-ANN, based on ANN and Fuzzy cluster to solve the problem and help IDS achieve higher detection rate, less false positive rate and stronger stability. In FC-ANN, firstly fuzzy clustering technique is used to generate different training subsets. Subsequently, based on different training subset, different ANN models are trained to formulate different base models.ANN is one of the widely used techniques and has been successful in solving many complex practical problems. And ANN has been successfully applied into IDS. In [7] The kind of users and the injection of network packets into the internet sectors are not under specific control. There is no clear description as to what packets can be considered normal or abnormal. An IDS is designed to classify by the incorporation of enhanced rules as learnt from the network behavior with less computational complexity of O(n). The machine learning algorithms were applied to the audit records and processed according to the feature definitions to generate intrusion detection rules. Machine learning techniques and rule based method will be implemented in cloud computing IDS environment by considering the time complexity and the detection rate parameters.In [8] One of the effective ways to achieve higher security is to use IDS, which are software tools used to detect abnormal activities in the computer or network. One technical challenge in IDS is the curse of high dimensionality. They propose a "feature selection phase", which can be generally implemented in any IDS. They are using feature selection algorithms and study the performance of using these algorithms compared to mutual information based feature selection method. These feature selection algorithm require the use of a feature goodness measure. We investigate using both a liner and a non-liner measure linear correlation coefficient and mutual information, for feature selection. Further, we introduce an IDS that uses an improved Machine Learning based method, least squares support vector machine. Machine learning and data mining techniques have recently been used in research to remove the manual and ad-hoc elements from the process of building IDS. Machine learning techniques have the ability to build a system that improves its performance based on nearly acquired information.In [9] Most of existing Intrusion Detection (ID) models with a single level structure can only detect either misuse or anomaly attack. A hierarchical ID model using principal component analysis (PCA) neural networks is proposed to overcome such shortages. In the PCA is applied for classification and neural networks are used for online computing. Hierarchical ID model is presented based on the PCANN, which is suitable for adaptive online computing for both misuse detection and anomaly detection. In [10] Cloud computing represents a new paradigm where computing resources are offered as services in the world via communication internet. As many new type of attacks are arising at a high frequency, the cloud computing services are exposed to an increasing to amount of security threats. To reduce security risk, two approaches of the network traffic anomaly detection in cloud communications have been presented, which analyze dynamic characteristics of the network traffic based on the synergetic neural networks and the catastrophe theory. A synergetic dynamic equation with a group of the order parameter is used to describe the complex behaviors of the network traffic system in cloud communications. The anomaly can be detected. Detect the network traffic anomaly and achieve the high detection probability and the low false alarms rate. In [11] Agent based approach using artificial immune system (AIS) paradigms as a successful mechanism for distributed IDS. The AIS paradigms are negative selection, clonal selection, danger theory, and immune network. This paradigms are very successful for anomaly IDS. The AIS paradigms are inspired by the powerful human immune system (HIS) and are promising candidate for design of an IDS.The proposed AIS based against are capable of learning, self adaption, platform mobility, autonomy and collaboration. The system (MAIS-IDS) was designed using this powerful and collaborative agent. This system has mobile and static agents with detector agents as the main actors in MAIS-IDS. MAIS-IDS is a hybrid system that analyzes both system settings and network traffic. In [12] Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends information Technology's (IT) existing capabilities. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. A new model targeting at improving features of an existing model must not risk or threaten other important feature of the current model the architecture of cloud poses such a threat to the security of the existing technologies when deployed in cloud environment. In [13] This is a survey paper. In this survey different intrusions affecting availability, confidentiality and integrity of cloud resources and services. Incorporating IDS and IPS in cloud are examined. IDS/IPS positioning in cloud environment to achieve desired security in the next generation networks. Cloud computing aims to provide convenient, on-demand, network access to a shared pool of configurable computing resources (e.g. network, servers, storage, applications, and services), which can be rapidly provisioned and released with minimal management effort or service provider interactions. In [14] central to this are the issues of data security and the lack of trust that users have in relying on cloud services to provide the foundation of their IT infrastructure. This is a high complex issue, which covers multiple inter-related factors such as platform integrity, Robust service guarantees, that have yet to be overcome in a meaningful way. A concept for an innovative integrated platform to reinforce the integrity and security of cloud services and we apply this in the context of critical infrastructures to identify the core requirements, components and features of this infrastructure. In [15] The long term potential benefits through reduction of cost of services and improvement of business outcomes make cloud computing an attractive proposition these days. To make it more marketable in the wider IT user community one needs to address a variety of information security risk. Cloud computing with the main focus on gaps and security concerns. We identify the top security threats and their existing solutions. We also investigate the challenges/obstacles in implementing threat remediation. In [16] In this paper they propose a framework integrating network IDS in the cloud. Our NIDS module consists of Snort and signature apriori algorithm. It generates new rules from captured packets. These new rules are appended in the Snort configuration file to improve efficiency of Snort. It aims to detect known attacks and derivative of known attacks in cloud by monitoring network traffic, while ensuring low false positive rate with reasonable computational cost. We also recommend the positioning of NIDS in cloud. In [17] cloud computing presents existing opportunities to foster research for scientific communities; virtual machine technology has a profound role in this. Virtual machine technology enables cloud to offer large scale and flexible computing infrastructure that are available on demand to address the diverse requirements of scientific research. Cloud introduce novel security challenges which need to be addressed to facilitate widespread adoption. In [18] we believe that one way to raise it is to address challenging real-world problems whose solution offers a clear benefit to the viticulturist. They propose a system for the detection and location, in t he natural environment, of bunches of grapes in color images. This system is able to distinguish between white and red grapes, and at the same time, it calculates the location of the bunch stem. In [19] Monitoring of the system performance in highly distributed computing environments is a wide research are: In today's computational Grids (CGs) and cloud computing (CCs), the end users may define the special personal requirements and preferences in the resource and service selection, service functionality and data access. Such requirements may refer to the special individual security conditions for the protection of the data and application codes. Therefore, solving the scheduling problems in modern distributed environments remains still challenging for most of the well known schedulers, and the general functionality of the monitoring systems must be improved to make them efficient as schedulers supporting modules. In [20] The vulnerabilities in the communication (TCP/IP) protocol stack and the availability of more sophisticated attack breed and more and more network hackers to attack the network intentionally or unintentionally, leading to Distributed Denial of Service (DDoS) attack. The DDoS attacks could be detected using the existing machine learning techniques such as neural classifiers. These classifiers lack generalization capabilities which result in less performance leading to high false positive. In this paper, evaluates the performance of a comprehensive set of machine learning algorithms for selecting the base classifier using the publically available KDD CUP 99 dataset. Based on the outcome of the experiments, Resilient Back propagation (RBP) was chosen as base classifier for our research. The improvement in performance of the RBP classifier is the focus of this paper. Proposed classification algorithm RBP Boost is achieved by combining ensemble of classifier outputs and Neyman person cost minimization strategy, for final classification decision.

VI. PROPOSED WORK

In this paper we have proposed the use of BPN the most widely used learning algorithm for training in Artificial Neural Network. Artificial Neural Network is the field of Computer Science which deals with the construction of computer programs that are having resemblance with the working of human brain. In ANN we try to exploit the feature of human brain to deal with uncertain and inconsistent data. Artificial Neural Network comprises of three basic elements namely learning algorithm, neuron and network topology. In this paper we will implement IDS using the concept of BPN. The implemented IDS will be installed in the Cloud used to serve various client systems. The implemented IDS trace all the coming users. The behavior of the user is assessed by the IDS implemented using BPN.

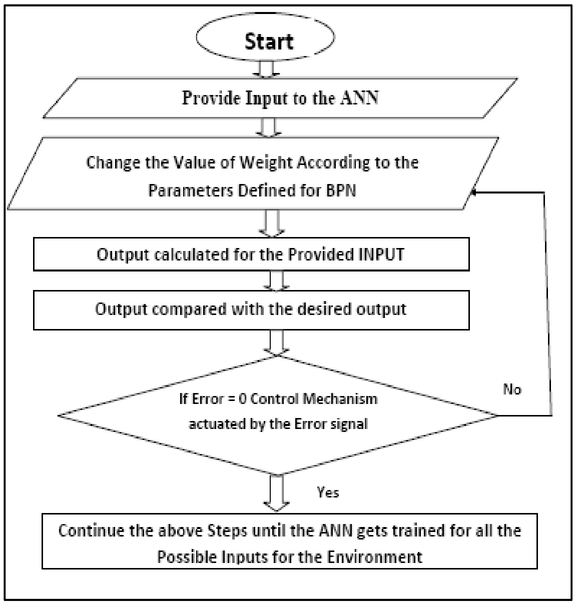
Start
Provide Input to the ANN
Change the Value of Weight According to the Parameters Defined for BPN
Output calculated for the Provided INPUT
Output compared with the desired output
If Error = 0 Control Mechanism actuated by the Error signal
No
Yes
Continue the above Steps until the ANN gets trained for all the Possible Inputs for the Environment

Figure1:-Flowchart representing the working of BPN implemented in the ANN used as an IDS in Cloud

BPN Algorithm

Step1:-Randomly select a vector pair (IP,DP) from the training set and call it (I,D).

Step2:-Use I as Input to the BPN and successively compute the Outputs of all neurons in the network (Bottom-up) until you get the Network output Y.

Step3:-Compute the “error” E of the network i.e. the difference between the desired output D and the actual output Y.

Step4:-Apply the BPN learning rule to update the weights in the Network so that its output Y for input I is closer to the desired Output D.

Step5:-Repeat steps (i) to (iv) for all vector pairs in the training set; this is called a training epoch

Step6:-Run as many epochs as required to reduce the network error E to fall below a threshold that you set before hand.

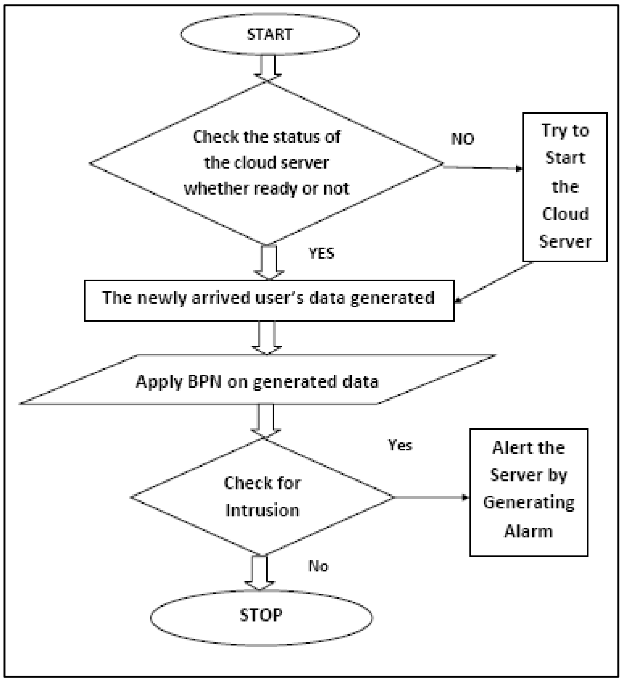
START
Check the status of the cloud server whether ready or not
NO
Try to Start the Cloud Server
YES
The newly arrived user's data generated
Apply BPN on generated data
Check for Intrusion
Yes
Alert the Server by Generating Alarm
No
STOP

Figure2:-Flowchart representing the proposed IDS

VII. Conclusion

The conclusion that we draw from the study that we made in the field of IDS is that IDS is a system that enables the cloud to have generation of alarm by virtue of which the intruder is disallowed to use the cloud and thus helps the other user to get intruded.

REFERENCES

[1] George P. Spathoulas, Sokratis K, Katsikas: “Reducing false positive in intrusion detection system”, July-2009, Published in Science Direct, Elsevier Ltd, P. 35-44.

[2] Adnan Nadeem , Michael P. Howarth : “An intrusion detection and adaptivet response mechanism for MANETs“, published in Science Direct, Elsevier, Sept 2013, p-368-380.

[3] Arun Jamdagni, Zhiyuan Tan, Xiangjian He, Priyadarsi Nanda, Ren Ping Liu : RePIDS : “A multi tier Real – Time Payload – based Intrusion Detection System”, Publised in Journal Science Direct, Elsevier, Jan- 2012-13, p-811-824.

[4] Igino Corona, Giorgio Giacinto, Fabio Roli: “Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues”, published in Science Direct, Elsevier, March-2013.

[5] Shahaboddin Shamshirband, Nor Badrul Anuar, Miss Laiha Mat Kiah, Ahmed Patel : “A

apprarisal and Design of a multi-agent system based computational intelligence techniques", published in Science Direct, Elsevier, May-2013, P-2105-2127.

[6] Gang Wang, Jinxing Hao, Jian Ma, Lihua Huang : "A new approach to intrusion detection using Artificial Neural Networks and Fuzzy clustering", published in Science Direct, Elsevier, 2010, p-6225-6232.

[7] G. Gowrison , K. Muneeswaran, T. Revathi: "Minimal complexity attack classification detection system ",published in Science Direct, Elsevier, 2013, p-921-927.

[8] Fatemeh Amiri, Mod. Mahdi Rezaei Yousefi, Caro Lucas, Azadeh Shakery, Naseer Yazdani : "Mutual information-based feature selection for IDS", published in Science Direct, Elsevier, Jan-2011, p-1184-1199.

[9] Guisong Liu, Zhang Yi, Shangming Yang: "A hierarchical intrusion detection model based on the PCA neural networks",published in Science Direct, Elsevier, Dec-2006-07, p-1561-1568.

[10] Wei Xiong, Hanping Hu, Naixue Xiong, Laurence T. Yang, Wen-Chih Peng, Xiaofei Wang, Yanzhen Qu :"Anomaly secure detection methods by analyzing dynamic characteristics of the network traffic in Cloud Communications", published in Science Direct, Elsevier, April-2013-14, p-403-415.

[11] Neda Afzali Seresht, Rezai: "MAID-IDS : A distributed IDS using multi-agent AIS approach". published in Science Direct, Elsevier, 2014, p-286-298.

[12] S. Subhashini, V. Kavitha: "A survey on security issues in service delivery models of cloud computing", published in Science Direct, Elsevier, July- 2010-11,p-1-11.

[13] Chirag Modi, Dhiren Patel, Bhavesh Borisanya, hiren Patel, Avi Patel, Muttukrishnan Rajaranjan: "A survey of intrusion detection techniques in Cloud", published in Science Direct, Elsevier, May-2012-13, p-42-57.

[14] M. Mackay, T. Baker, Al-Yasiri :"security –oriented cloud computing platform for critical infrastructures", published in Science Direct, Elsevier, 2012, p-679-686.

[15] Md. Tanzim Khorshed, A.B.M. Shawkat Ali, Saleh A. Wasimi: "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing", published in Science Direct, Elsevier, Jan- 2012, p-833-851.

[16] Chirag N. Modi, Dhiren R. Patel, Avi Patel, Muttukrishnan Rajarajan :"Integrating Signature Apriori based Network IDS in Cloud Computing", published in Science Direct, Elsevier, 2012, p-905-912.

[17] Junaid Arshad, Paul Townend, Jie Xu: "A novel intrusion severity analysis approach for clouds": published in Science Direct, Elsevier, 2011, 416-428.

[18] M.J.C.S. Reis, R. Morais, E. Peres, C. Pereira, O. Contente, S. Soares, A. Valente, J. Baptisa, P.J.S.G. Ferrwira, J. Bulas Cruz: "Automatic detection of bunches of grapes in natural environment from color images", published in Science Direct, Elsevier, Jul-2012, p(285-290).

[19] Daniel Grzonka, Joanna Kolodeziej, Samee Ullah Khan : " Artificial neural network support to monitoring of the evolutionary driven security aware scheduling in computational distributed environments", published in Science Direct, Elsevier, Article in Press, Oct 2014, p(1-15)

[20] P. Arun Raj Kumar, S. Selvakumar : " Distributed denial of service attack detection using an ensemble of neural classifier", published in Science Direct, Elsevier, Feb-2011, p(1328-1341).