IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 6, No. 4, December 2017, pp. 166~173
ISSN: 2252-8938, DOI: 10.11591/ijai.v6.i4.pp166-173

Neural KDE Based Behaviour Model for Detecting Intrusions in Network Environment

V. Brindha Devi[1], K.L. Shunmuganathan[2]
[1]Sri Sairam Institute of Technology, Tamil Nadu, India
[2]Department of Computer Science, R.M.K. Engineering College, Kavaraipettai

Article Info

Article history:

Received Aug 26, 2017
Revised Oct 28, 2017
Accepted Nov 11, 2017

Keyword:

Firefly algorithm
Fuzzy approach
SVC placement

ABSTRACT

Network intrusion is one of the growing concern throughout the globe about the information stealing and data exfiltration. In recent years this was coupled with the data exfiltration and infiltration through the internal threats. Various security encounters have been taken in order to reduce the intrusion and to prevent intrusion, since the stats reveals that every 4 seconds, at least one intrusion is detected in the detection engines. An external software mechanism is required in order to detect the network intrusions. Based on the above stated problem, here we proposed a new hybrid behaviour model based on Neural KDE and correlation method to detect intrusions. The proposed work is splitted into two phases. Initial phase is setup with the Neural KDE as the learning phase and the basic network parameters are profiled for each hosts, here the neural KDE is generated based on the input and learned parameters of the network. Next phase is the detection phase, here the Neural KDE is computed for the identified parameters and the learned KDE feature value is correlated with the present KDE values and correlated values are calculated using cross correlation method. Experimental results show that the proposed model is robust in detecting the intrusions over the network.

Corresponding Author:

V. Brindha Devi,
Sri Sairam Institute of Technology,
Tamil Nadu, India.

1. INTRODUCTION

Today's networks are compromised to advanced range of cyber-attacks and context with all sort of intrusion in networks. Advanced operating systems are evolving for the purpose of VA/PT. Since those are widely used for hacking purposes unethically. Recent attacks such as stuxnet have destructed the main resources of the country. The compromised host within the organization shall be a victim to play the malicious attacks as insider threat. Today's network security credentials such as IDS, IPS helps in identifying and preventing the attacks. Most of the traditional security solutions are signature based systems, since these system are to be updated periodically/intervally to endure for the real time attacks. If the system with the existing security measures is compromised to any form of attacks other than in the set of lists, then the system is not able to handle those attacks. This was stated as the serious challenge, hence in order to detect an anomaly, an optimal IDS is to be developed to identify the real time intrusions.

Since there are various types of IDS evolved in recent years. Some of those are optimal in sequence, a good example of signature based IDS is 'SNORT'. In this paper an optimal IDS has been designed with the behavioural model to detect anomalies in the active networks. Some of the anomalies are password escalation, ARP poisoning, DNS poisoning attacks etc., these types of attacks are well established anomalies which utilize the existing legal communication protocols such as TCP/IP, UDP, HTTP, HTTPS etc.

The basic organisation of this paper is splitted into various sections such that section (1) details about the IDS – state-of-the-art.

An 'IDS' is a term defined for detecting intrusions, reporting, correlating and to mitigate the risks which are attempted as privilege escalation event. There are mainly two active types of IDS available, namely Host based and Network based.

According to Susan et al the IDS is termed as 'Intrusion Detection' which denotes the clearly view of definition about IDS and Rafeez stated the characteristics of IDS into five basic models namely Host based, Network based, Application based, Signature based and Anomaly based. Present day IDS are basically termed as signature based IDS. Since an intelligent IDS has to develop for detecting advanced range of insider attacks, threats etc.

Network based IDS

Network based IDS are implemented in the gateway interface to monitor entire network traffic

Host based IDS

Host based IDS are used to monitor and analyse each host in the network. Though they can be implemented to monitor single host, multiple host, connected host. These types of IDS are used to analyse the encrypted network traffic.

Application based IDS

Application based IDS are implemented in the individual application program. IT monitors each and every events occurring within the application.

Signature based IDS

Signature based IDS can analyse the on-going network traffic of the known pattern; these kinds of IDS needs periodical updation of the signature.

Anomaly based IDS

Intelligent IDS systems are usually anomaly based one, these kinds of IDS are used to learn the attacker pattern and frames its own rule based on attacker behaviour and then predicts the suspicious events.

Some of the key concerns reported in this paper are

1) If the attacker is subjected to unobserved, the attack may be sustained on long term basis and it is highly vulnerable.
2) Entire data with strong knowledge about organization is subjected to any leakage or damage.
3) The network can be used as promising host for compromised attacks.
4) The associated host of the networks within the organization can be used as the launch pad for activating attacks.

2. RELATED WORK

Initial level of Intrusion detection system for detecting anomalies was led by the author Salem et. al who provides a vast range of research in designing anomaly model. Next attempt for modelling anomaly based behaviour model was achieved by Bivens et. al at 2002, using neural network. This IDS model plays an important role in detecting network anomalies. In 2005, Salvatore et. Al designed a hardware based IDS which was proficient in nature and deployed in FPGA based embedded circuits. The main anomaly detector was designed by Laheeb at 2007, this was the first attempt made to detect the anomalies which are running as an internal threat. A new strategy of profiling scheme was proposed by the author Akaninyene who developed an IDS to detect the network abnormality using K-means unsupervised clustering scheme.

Various authors demonstrated the taxonomy of Various IDS proposed for Wired and Wireless environment; out of them some are benchmarked with its reliable efficacy and deployed in real time designated security tools. Here we proposed a robust methodology using neural KDE function and cross correlation function which differs from the above mentioned models. The detailed approach of the proposed IDS has been clearly demonstrated in the following sections. Result analysis shows the efficacy of the proposed algorithm.

2.1. Proposed model – A Theoretical Prototype

The proposed solution for the above stated problem is implementing wide range of security policies, product based policy, business policy and user level security policies to avoid insider attacks and external gateway policies to evaluate infiltration packets into the network premises. Present day attack detection model and signature based models are not in active up to the level and lack in detection of vulnerabilities/threats. Another approach is to build an effective intelligent behaviour model based IDS to detect these kinds of attacks by learning the behaviour pattern of the attacker and live network behaviours. The detailed study of behaviour based approach is explained clearly in [4], since they are limited in feature adaptation and not equipped for identifying anomalies.

In this paper, a new behaviour model for IDS has been developed to detect network anomalies. The proposed model is robust in nature due to its learning capabilities of real time live feed of network data

and cross correlating it with the addressed pattern in order to detect the anomalies. Robust nature of the behaviour model proposed in this paper is initially to learn the network traffic patterns using neural KDE function. Neural KDE is a kernel function which works on basis of neural model. Each input is tested with the possible output and the learned data is computed with KDE values. Firstly in learning phase all the network parameters are learnt and profiled specifically with neural KDE values and approximate KDE values are computed. Secondly in detection phase the KDE values of the live feed are compared with learnt KDE values and correlation is applied in order to detect the intrusions.

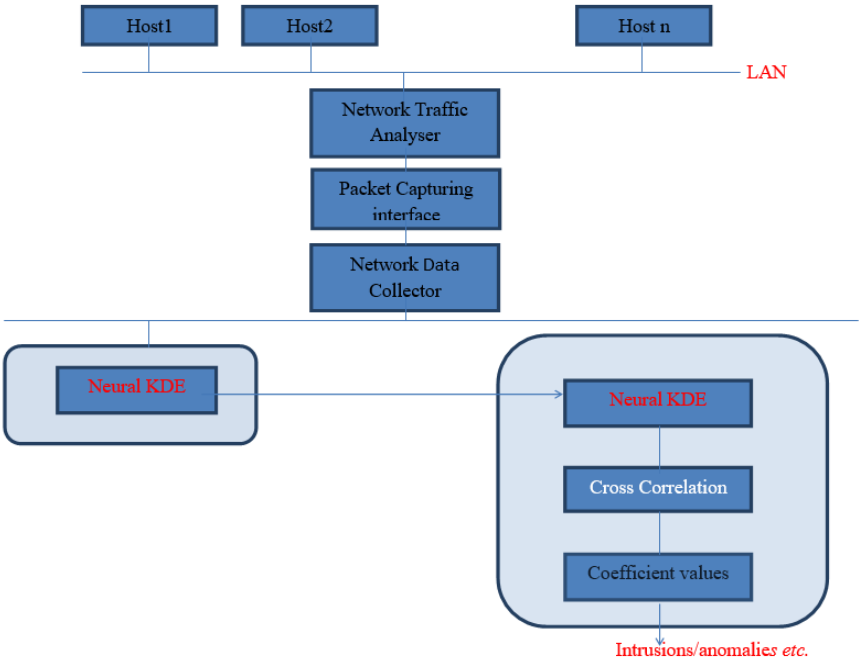

Figure 1. Architecture of Proposed model

Here, Neural KDE values are computed for learnt phase using specific network patterns such as CPU utilization, Memory usage, Memory utilization, Incoming Packet buffer, Outgoing Packet buffer, Cached Bytes etc. Network packet analysers are used to analyse the network packets. Packet capturing interface is widely used to capture all the packets and network data collector acts as the serialization interface for all the network inputs.

The main contribution of this paper

1) Concocting a behaviour model to detect anomalies in the network.
2) Implementing Neural KDE for Learning phase and live feed.
3) Intending the robust algorithm for detecting anomalies.
4) Bestowing the results of the proposed behavioural model.
5) Network packet analyser
6) Uniqueness is comparing all the network parameters to detect anomalies
7) Utilizing all the system/host resource for effective analysis
8) Cross correlation of Learnt KDE values with the live KDE values

2.2. Network Packet analyser

Network packet analysers are used to analyse the network packets based on three main criteria namely Normal packets, wary packets (Suspicious packets) and malicious packets. Table 1 clearly denotes the packet definition for various protocol based data packets. Packet analyser structure is clearly stated:

Protocol	IP	Port	Direction	IP	Port	Action

Figure 2. Additional structure of proposed packet analyser

Normal packets

Data packets which belongs to the homeland premises. Some of the homeland protocols utilized by any organization are TCP, IP, UDP, DNS, POP3, IPsec, SSL, FTP etc.

Wary packets

The packets may be uneven at the sequence and the results always in odd mode. The packets are suspicious but not cause any vital damage to the premises.

Malicious packets

Any data packets which could cause the damage to the organization and its network component and results in negative impact for security credentials within the organization.

Table 1: packet definition for data packets; HTTP, SSL, Kerberos, SMB, SNMP

S.No	Service	port number	Model	Security credential
1	HTTP	80	WEB	High
2	SSL	23	Security	High
3	MySQL	3306	DB	Average
4	Kerberos	81	Windows PowerShell	Low
5	SMB	445	Windows PowerShell	Low
6	SNMP	25	Network	Average

Learning phase

In this phase, the values have been collected from the network parameters which are related to the network for each connected host. Each host are profiled into system and network parameters and each value are utilized to compute Neural KDE. A detailed process was illustrated in the algorithm 1 which runs in all hosts for 5 working days with all network and system credentials.

Algorithm 1 Learning phase

Begin
Initiate learning and profiling
Profile each host
Collect network credentials
Do feature selection
Compute Neural KDE
Compute KDE parameters
End

Detection phase

In this phase as off the learning phase is cloned to compute neural KDE values for the hosts of same parameters in several time periods. Then the Comparison process is carried out for the present Neural KDE values with the learnt KDE values.

Defined Hypothesis

According to the hypothesis, the correlation values always a probability and lies between 0 and 1.

General Assumption: *KDE values always lies between 0 to 1. If the values are nearest circumstance of 1, then the relationship possessed by the parameters is in strong relationship*

Theory: *Based on assumption, the threshold value of each parameter is fixed to its intense level (refer KDE plots)*

Hypothesis 1: *if the threshold value lies between 0.5 – 1, then it is a normal behaviour*

Hypothesis 2: *if the threshold value lies between 0 - 0.5, then it is abnormal behaviour or anomaly*

Correlation phase

Based on the hypothesis defined above the cross correlation values are computed. The detection phase is exhibited by considering, analysing and comparing all the defined network and system parameters. According to the discussion defined in previous section's anomalies are the specific event based, so that the proposed methodology computed here yields the promising results by utilizing the network parameters for identification.

Algorithm 2 Detection phase

Use learnt data
Procure the live feed
Do feature selection
Compute Neural KDE
Use KDE values of Learnt data and live feed
Apply cross correlation
Compare cross correlation value for each network parameter
If the threshold (correlation) < 0.5 then
Caption: Intrusion detection
Trigger Alarm
End

---

3. RESULT ANALYSIS OF OUR MODEL

Analysis of the proposed model is clearly tested experimentally with 5 active running host with Linux platform and single server host with the same. This section is splitted into two with 2 phases. Initial phase deals with experimental setup and secondly with result analysis of the proposed methodology

Experimental Setup

The proposed model has been developed and data has been collected from 5 hosts which were running on Ubuntu, Backtrack etc. In this phase using the data collector, the entire host behaviour is learnt by its network parameters such as RAM memory utilization, CPU usage, incoming bytes, outgoing bytes, incoming packets, outgoing packets, memory usage, control block and data block.

Result analysis

Secondly, in detection phase the system profiles all the network parameters of each host in the network. Each hosts are profiled as of learning phase, the attack pattern is performed by initiating Backtrack operating system. Here various attacks have been performed and the data has been collected and refined. Now the learnt data and live feed with attack sequence is given as the input and analysed in the MATLAB R2013b version.

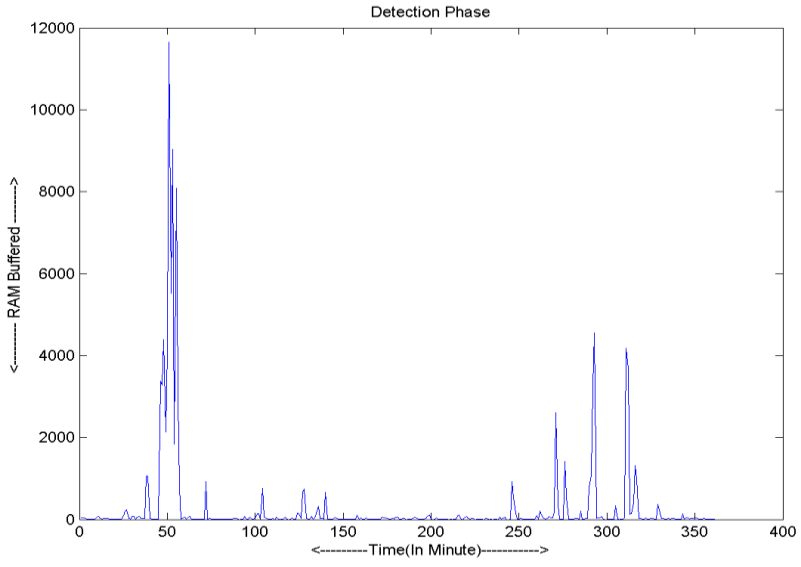

Figure 3. Detection phase for attack sequence

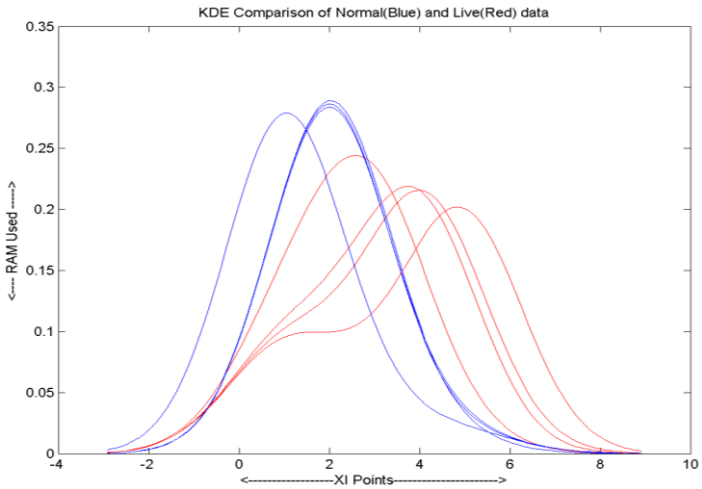

Figure 4. Computed Neural KDE value for RAM usage

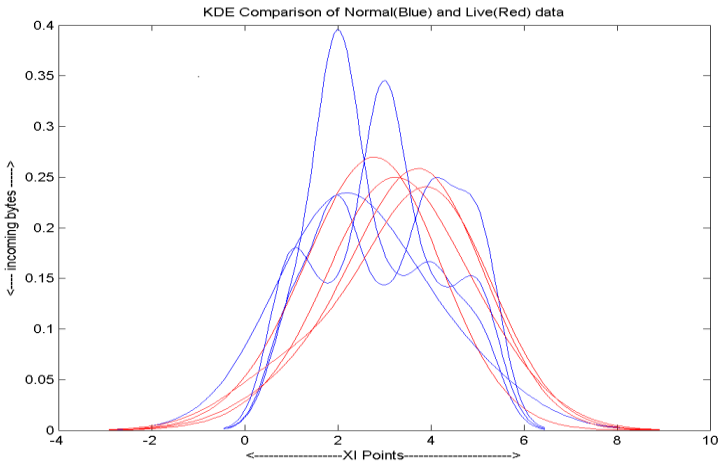

Figure 5. Computed Neural KDE value for incoming bytes

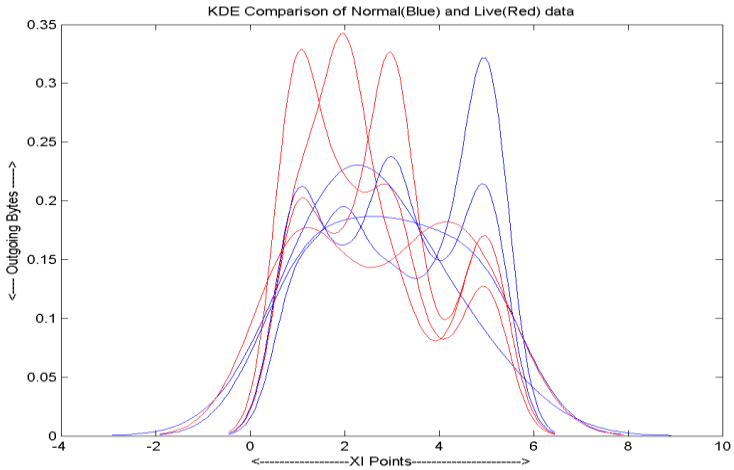

Figure 6. Computed Neural KDE value for outgoing bytes

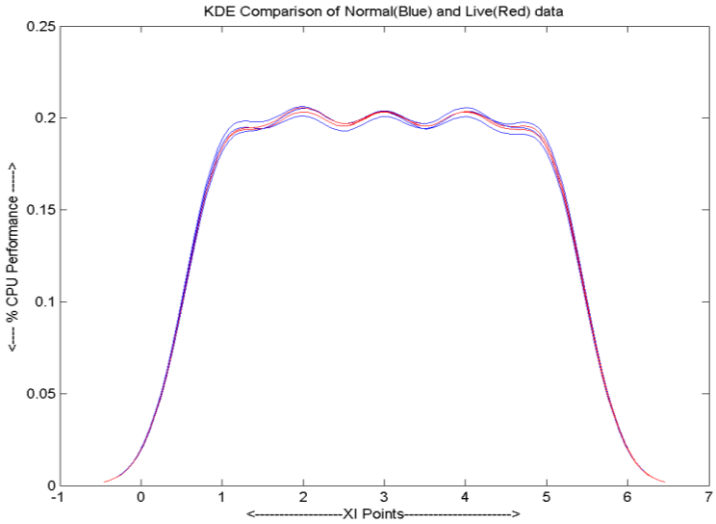

Figure 7. Computed Neural KDE value for CPU usage

The analysis of the proposed model is fully based on the comparison of cross correlation values with the network parameters such as CPU usage, RAM usage, incoming bytes, outgoing bytes, incoming traffic and outgoing traffic. This correlation value shows the deviation range and the proposed methodology yields the promising results by detecting intrusions. By this method all the attacks performed at several time periods were identified/detected and auspicious results were achieved. The cross correlation values of attack sequence are clearly defined in the Table 2.

Table 2. Cross correlation values of attacking sequence

S.No	Time	CPU	RAM	Outgoing packets	Incoming packets
1	1:16:59	1179339978	892986	896046	636809
2	1:17:10	1179339978	896119	896046	636809
3	1:18:28	1179611728	898952	898952	639716
4	1:19:26	1179791914	898231	901233	641997
5	1:20:27	1179972352	900347	903479	644243
6	1:21:27	1180153141	902466	905726	646491
7	1:22:27	1180376311	904659	908039	648815
8	1:23:11	1211149803	926499	937182	664802
9	1:24:4	1262468314	962392	937182	664802
10	1:25:26	1380740088	1043522	1022047	709688
11	1:26:22	1420838212	1071513	1071466	735810

4. CONCLUSION

Hence the paper is concluded by proposing a robust behavioural model for IDS to detect anomalies in the network domain. The main research motivation in our proposed model is utilizing Neural KDE based computational technique with cross correlation values. The experimental results demonstrated in Figure 3-7 shows the optimality of the proposed algorithm. In the present model is adapted for any IDS and can be implemented over any layer of OSI model. In future, the proposed IDS is extended to detect the covert communications in Application tier protocols.

REFERENCES

[1] Frederick, K.K. (2001) *Network Intrusion Detection Signatures, Part One* Receive on 14 January from http://online.securityfocus.com/infocus/1524.html.

[2] Roesch, M. (1990) Snort- *Lightweight Intrusion Detection for Networks* Receive from 14 January from http//www.snort.org.

[3] Susan, Y., John, D.T., Dave, A., & Felix, L. (2001) *The Hacker's Handbook*, CRC Press. Receive on 14 January from http://books.google.com.my/books?id=AO2fsAPVC34C&pg=PA174&lpg=PA174&dq=signature+based+network&source=web&ots=LeRC4cdZK7&sig=jZW2o68ViZdm nb4PSPR0zAgTtxI&hl=en#PPA173, M1.

[4] Yixue Wang, A Sort of Multi-Agent Cooperation Distributed Based Intrusion Detection System, Modem computer, 2008.
[5] Jianchun Jiang, Hengtai Ma, Dangen Ren, Network Security Intrusion Detection, *Journal of Software*, 2000.
[6] JMarin, D.Ragsdale, and JSurdu, A hybrid approach to the profile creation and intrusion detection, *Proc.of DARPA Information Survivability Conference & Exposition* 11, 2001.
[7] Ming Tan, Xiaolong Hu, Liancheng Liu, Based on multi-examination technology invasion examination system model, *Computer project and design*, 2008.
[8] Ming Xiao, Distributed Intrusion Detection System Design, *Electronic Science and Technology University*, 2002.
[9] Xiren Xie, "Computer Network," Publishing House of Electronics Industry, pp.110-111, 2005.
[10] U.S. National Security Agency Releases, "The Technical Framework of Information Assurance,"Beijing China Electronical Software publishing house, pp.46-57, 2004.
[11] Julia Allen, Alan Christie, et a1.State of the Practice of Intrusion Detection Technologies.Technical Report, *Networked Systems Survivability Program*, pp.47-85, 2000.
[12] Congwei Zheng, Tianfa Jiang."Research on Inetanet network security technology based on intelligent firewall,"*Computer Engineering and Applications*, pp.156-158, 2005.
[13] Xiaoping Yang, Jing Su. "Research on Intrusion Detection technology based on Protocol Analysis," *Computer Application Research*, pp.108-110, 2004.
[14] Chen A A, Common Intrusion Detection Framework.http://seclabs. Cs.ucdavis.edu/cidf,2002-01-17.
[15] Xiaoqun Du, Scott A.Smolka, Rance Cleaveland, "Local Model Cheeking and Protocol Analysis," *Software Tools for Technology Transfer*.
[16] D. Barbara, J. Couto, S. Jajodia, L. Popyack and N. Wu "ADAM: Detecting intrusions by data mining", *Proc. IEEE Workshop Inf. Assurance and Security*, pp.11 -16 2001.
[17] N. Ye, S. Emran, X. Li and Q. Chen "Statistical process control for computer intrusion detection", *Proc. DISCEX II*, vol. 1, pp.3 -14 2001.
[18] N. Ye , S. Vilbert and Q. Chen "Computer intrusion detection through EWMA for auto correlated and uncorrelated data", *IEEE Trans. Rel.*, vol. 52, no. 1, pp.75 -82 2003.
[19] N. Ye , S. Emran , Q. Chen and S. Vilbert "Multivariate statistical analysis of audit trails for host-based intrusion detection", *IEEE Trans. Comput.*, vol. 51, no. 7, pp.810 -820 2002.
[20] W. Lee and S. Stolfo "A framework for constructing features and models for intrusion detection systems", *ACM Trans. Inf. Syst. Secur.*, vol. 3, no. 4, pp.227 -261 2000.
[21] Zhong Shaochun, Song Qingfeng, Cheng Xiaochun, Zhang Yan (2003). "A Safe Mobile Agent System for Distributed Intrusion Detection." *Proceedings of the Second International Conference on Machine Learning and Cybernetics IEEE*.
[22] Lin Zhaowen, Ren Xingtian, Ma Yan (2006). "Agent-based Distributed Cooperative Intrusion Detection System." *IEEE*.
[23] Sartid Vongpradhip, Wichet Plaimart (2007). "Survival Architecture for Distributed Intrusion Detection System (dIDS) using Mobile Agent". *Sixth IEEE international Symposium on Network Computing and Application (NCA 2007)*.
[24] Wang Jun, Wang Chong-jun, Xie Jun-yuan, Chen Shi-fu (2006). "Research on Agent-based Intrusion Detection Technique". *COMPUTER SCIENCE*, Vol. 33, No. 12, pp. 65-69.
[25] Dalila Boughaci, Habiba drias, Ahmed Bendib, etc (2006). "A Distributed Intrusion Detection Framework based on Autonomous and Mobile Agents". *Proceedings of the International Conference on Dependability of Computer Systems IEEE*.
[26] Abdelhamid Belmekki, Abdellatif Mezrioui (2005). "Using Active Agent for Intrusion Detection and Management." *Proceeding of the 2005 Conference IEEE*.

BIOGRAPHIES OF AUTHORS

V. Brindha Devi,B.E.,M.E., is a Research scholar at Anna University, Chennai. Currently working in Sri Sairam Institute of Technology .She has more than 13 years of teaching experience and her areas of specializations are Wireless Networks, Fuzzy computation, Artificial Intelligence.

Dr. K.L. Shunmuganathan,B.E,M.E.M.S,Ph.D is working as the Professor & Head of CSE Department of R.M.K. Engineering College, Chennai, Tamil Nadu, India. He has more than 23 years of teaching experience and his areas of specializations are Networks, Artificial Intelligence.