Int. J. Advanced Networking and Applications
Volume: 04, Issue: 04, Pages:71-73, Jan – Feb (2013)
Special Issue on "Computational Intelligence- A Research Perspective" held on "21st – 22nd February 2013"

Computational Intelligence Techniques in Intrusion Detection System for Critical Information Infrastructure Protection (CIIP)

J.Lekha
Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore
Email: saran.lekha@gmail.com
Dr.G.Padmavathi
Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore-
Email: ganapathi.padmavathi@gmail.com

ABSTRACT

Critical National Infrastructures (CNI) are important resources of the nation to be protected. Since all the operations are computer based the security of CNI are wholly dependent on security of Information systems. Many protection systems such as firewalls, cryptographic systems, Intrusion Detection Systems exists to provide Critical Information Infrastructure Protection (CIIP). Among them IDS play a significant role in analyzing and protecting huge volume of network traffic. Computational Intelligence Techniques can be implemented in IDS systems to handle complex real world threats to CNI. Some of the Computational Intelligence Techniques that can be applied to each layer of IDS are discussed.

Keywords – **Critical National Infrastructure (CNI), Critical Infrastructure Information Protection(CIIP), Intrusion Detection System(IDS), Computational Intelligence.**

I. INTRODUCTION

Today Critical National Infrastructures (CNI) such as Energy transmission and Distribution Networks, Telecommunication Networks, Transport Systems, Defense Infrastructures, Banking and Financial Organizations, National Health Care Services, Media and Information Networks [4] and many Government network whose operations are important for maintaining nation's resources. They are wholly or partly dependent on computer network information infrastructure for sharing, monitoring, controlling and securing data and information. But Information Infrastructures are targeted by cyber terrorism resulting in critical information infrastructure (CII). Since the CNI is interconnected to CII any potential damage to CII is also extended to CNI thereby causing both geographical and financial damage. Thus securing Critical Information Infrastructure has become a broader research field.

1.1 Threats on Critical Information Infrastructures

- Unauthorized access to data
- Clandestine alteration of data
- Identity fraud
- Denial of service

The result of these threats has given rise to security requirements [6] such as Data source authentication, Access control, Data confidentiality, Data integrity and non rejection. To ensure these security services CII needs a robust cyber defense system. Many cyber defense systems such as Firewall, Antivirus, End to End Encryption, Public Key Encryption, Host based Intrusion Detection Systems and Network Based Intrusion detection systems are available in market. Among these solutions HIDS and NIDS serve as powerful real time protection system. Both HIDS and NIDS follow a sequence of steps to identify whether the incoming traffic is an attack or not. Of the two IDS approaches, knowledge based IDS work with huge volume of network traffic.

They collect the raw data, subject it to preprocessing for converting raw data into meaningful format, reduce the large number of features into smaller set by selecting required features to reduce the load of the detection system. Then they construct rules to match the packet header and activate [5] pattern matching algorithms to match packet payload. If a match occurs then it finally raise an alarm. Thus preprocessing plays a vital role in determining the accuracy and throughput of the system. And that demanded some computational intelligence techniques to be used for reducing larger traffic to a small set of features.

When analyzing the data sets of IDS such as DARPA, KDD Cup, they contain enormous training and testing data. They also provide some intrinsic and non intrinsic features. So to test out IDS with existing benchmark datasets we need a computational system which learns feature modeling from existing data sets and classify the real time traffic, and that demanded Computational Intelligence.

II. COMPUTATIONAL INTELLIGENCE

In many complex cyber attacks the existing propositional modeling and probability modeling becomes insufficient.

Computational Intelligence is a set of nature inspired computational methodologies to address complex real world problems.

Computational Intelligence Techniques in IDS

- Soft Computing Techniques
- Machine Learning
- Artificial Immune Systems
- Agent Based Systems

2.1 Soft Computing Techniques

Soft Computing Techniques is a set of computational technique that overcomes some of the limitations of Hard Computing Techniques such as [7] tolerance of imprecision, uncertainty, partial truth and low approximation.

2.1.2 Neural Networks

Neural Networks is an interconnected group of artificial neurons. They can model complex relationship between given set of input and output. It can be effectively used for data filtering, data clustering, feature classification, feature selection and feature reduction and pattern recognition.

2.1.2 Fuzzy Logic

It maps knowledge represented in natural language to equivalent computer language. Fuzzy systems [1] can be used to build a fuzzy decision model trained with existing datasets and use fuzzy rules (fuzzier) to refer the inference engine to classify normal or anomalous traffic (defuzzy).

2.1.3 Evolutionary Computation

Evolutionary Computation can be used to perform iterative process to handle large population of data. Evolutionary computation methods such as evolutionary algorithms and Swarm Intelligence help to achieve this. Among many evolutionary algorithms Genetic Algorithm can act as detection [2] engine by calculating the fitness function to calculate the goodness of the incoming traffic by using crossover and mutation values. It can also be used for signature generation for new upcoming attacks perform patch updates.

2.1.4 Rough Set Theory

Rough sets are formal methods of preprocessing such as dimensionality reduction, feature selection and feature extraction, feature ranking [3] and rule generation. It works on the concept of reducts to identify hidden patterns in existing data. They can be combined with data mining techniques to classify normal and abnormal patterns of data. They can also be combined with ANN to improve system accuracy.

2.2 Machine Learning

Many machine techniques have been proposed for intrusion detection. Marcov model can be used to record sequence of network actions. Support Vector Machines can be used to classify normal and abnormal traffic. Self Organizing Map can be used to feature selection and dimensionality reduction. Decision tree with Naïve Bayes can be used to analyze various protocol headers.

2.3 Artificial Immune Systems

The theoretical human immune functions can be successfully applied to Intrusion Detection systems, thus making IDS and AIS based IDS. A self-non self non discrimination model uses change detection algorithms to detect misuse of files and system calls. Negative selection algorithms can be used to classify normal and abnormal sequences in the input and output traffic. Danger theory can be used to record unusual access to system files similar to unusual death of normal tissues without non self antigens.

2.4 Agent Based Systems

The limitation of Centralized IDS leads to Agent Based IDS. Agents are autonomous systems that can work independent of other systems on the network. Centralized IDS could not manage heavy traffic and hence multiple agents can be given the power of computation to handle huge traffic. Bayesian systems can be used in modeling framework of NIDS.

III. CONCLUSION

Critical Infrastructure Protection is a major research area to be focused. Even though many applications and systems have emerged IDS has a significant place in CIP. Computational Intelligence plays a vital role in each and every phase of IDS lifecycle. Moreover Soft Computing Techniques of CI can be used to increase the accuracy and throughput of IDS.

References

Journal Papers:

[1] R. Shanmugavadivu , Network Intrusion Detection System Using Fuzzy Logic , *Indian Journal of Computer Science and Engineering (IJCSE) Vol. 2 No. 1*, pp :101-111.

[2] Mohammad Sazzadul Hoque , An Implementation Of Intrusion Detection System Using Genetic Algorithm, *International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012*, pp: 109-120.

[3] Adebayo O. Adetunmbi, Network Intrusion Detection Based On Rough Set And K-Nearest Neighbour, *International Journal of Computing and ICT Research, Vol. 2 No. 1, June 2008*, pp: 60-66.

Books:

[4] Stefano AMICI, *Network Security in Critical Infrastructures, Stampa: PrintArt*

Chapters in Books:

[5] Asim Karim, Computational Intelligence for Network Intrusion Detection: Recent Contributions, *Springer-Verlag Berlin Heidelberg 2005*, pp. 170 – 175

Theses:
[6] Ondrej Linda, *Applications Of Computational Intelligence In Critical Infrastructures: Network Security, Robotics, And System Modeling Enhancements*, Masters Thesis, University of Idaho, 2009

Proceedings Papers:
[7] Witaya Siripanwattana1, Information Security based on Soft Computing Techniques, *Proceedings of the International Multi Conference of Engineers and Computer Scientists* 2008 Vol I

Biographies and Photographs

J. Lekha is working as Assistant Professor in Computer Science Department of Sri Krishna Arts and Science College. She has over 8 years of teaching experience in the field of computer science. She is currently pursuing her doctoral degree in Avinashilingam Institute for Home Science and Higher Education for Women under the guidance of Dr.G.Padmavathi. Her area of interest include Networks, Network Security, Knowledge based systems.

Dr.G.Padmavathi is the Professor and Head of computer science of Avinashilingam Deemed University for women, Coimbatore. She has 23 years of teaching experience and one year of industrial experience. Her areas of interest include Real Time Communication, Network Security and Cryptography. She has 140 publications in her reascher area .In presently she is guiding M.phil researcher and PhD's Scholar .She has been profiled in various Organizations her academic contributions. She is currently the principal investigator of four projects funded by UGC and DRDO.She is life member of many preferred organizations of CSI, ISTE, WSEAS, AACE, and ACRS.

Department. of Computer Science,
Avinashilingam Institute for Home Science and Higher Education for Women University,
Coimbatore