IJRSET 2015 SPL Volume 2, Issue 11 Pages: 17-23
ISSN 2394-739X
International Journal for Research in Science Engineering and Technology

SOFT COMPUTING TECHNIQUES TO DETECT CYBER ATTACK

[1] LEKHA. J, [2] MOHAMAD IMRANKHAN. A, [3] ROHINI. R,
[1, 2, 3] Assistant professor, student , student.
[1, 2, 3] Department of computer science and application,
[1, 2, 3] Bharathiyar University,

Abstract:-

Cyber attack is one of the challenging tasks in today's computer era. Many cyber security mechanisms have been proposed by many researchers. But still all these countermeasures are challenged by cyber attacks thrown by hackers. All the existing solutions should be reframed by upcoming researchers to face the upcoming cyber attacks. Of many existing techniques available Intrusion Detection Systems play a vital role in handling the attacks in a network. Soft Computing techniques are aln upcoming technique to handle problems with imprecision and accuracy. This paper discusses some of the soft computing techniques that can be applied in Intrusion Detection System to handle network traffic in detecting attacks with increased efficiency and accuracy.

KEYWORDS: - Cyber attack, countermeasures, Detection System, detecting attacks, network traffic.

1. INTRODUCTION

Computer security also called as cyber security or IT security. Cyber security can be applied in computing devices such as computers and smartphones, as well as in both private and public computer networks, including world Internet. All the fields are protected from unplanned or unpermitted access through cyber security[5]. Information security protects the files on an independent system, a LAN or a WAN.

Computer security is the process of applying security measures to ensure confidentiality, integrity, and availability of data. According to computer security experts "physical security breach is one of the worst kinds of security breaches as it generally allows full access to both data and equipment". But Cyber Security also plays an important role in security measures. The aim of cyber security is to protect data both in static and dynamic states. Counter measures can be used to increase the data security. Some of the measures are access control, awareness training, audit and accountability, risk assessment, penetration testing, vulnerability management, and security assessment and authorization. Some of the methods to implement these measures are Intrusion Detection Systems (IDS), Intrusion Detection and Prevention Systems (IDPS) and Extrusion Detection Systems.

2. SINS OF SECURITY

There are some sins that should be strictly avoided to protect attacks. They are,

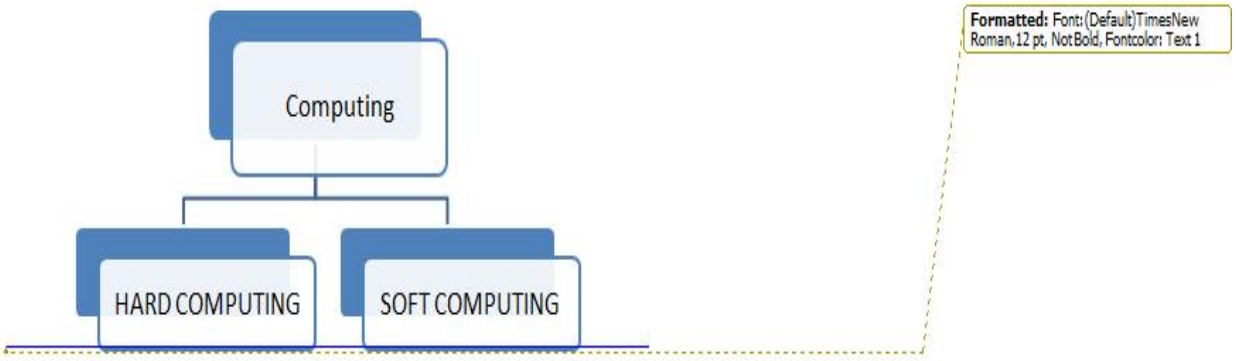
- Weak passwords
- Phishing spam
- Lack of data back up
- Insecure Internet Browsing
- Use of pirated software
- Misuse of Portable storage devices.
- Lack of proper encryption
- Lack of regular updates

- Using Wireless Hotspots
- Lack of awareness/ proper training.

3. COMPUTING TECHNIQUES AN OVERVIEW

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

There are two types of computing as shown in Fig 1.



Formatted: Font:(Default)TimesNew Roman,12 pt, NotBold, Fontcolor: Text 1

Figure 1: Types of Computing

4. HARD COMPUTING

Hard Computing requires a precisely state analytic model and it is based on binary logic, crisp system and numerical analysis .Hard computing has the characteristics of precision and categoricity and it requires programs to be written. Hard computing uses two-valued logical methods. It is deterministic and requires perfect input data to produce precise answer. Hard computing is strictly sequential.

5. SOFT COMPUTING

Soft computing gives an exact solution to computationally hard tasks like NP-complete problems, for which there is no known algorithm that can compute a correct solution in polynomial time. Soft computing is disguised from conventional computing in that, unlike hard computing, it is tolerant of imprecision, contingency, sectional truth and approximation. There are many techniques in Soft computing [4] as shown in Fig 2. Software Human mind is a role pattern of soft computing. Soft computing solutions are unpredictable, uncertain and between 0 and 1.soft computing is a formal area of study in computer science in early 1990's [1]. recent trends tend to involve evolutionary and swarm intelligence based algorithms and bio-inspired computation.[2][3] soft computing are complementary rather than competitive. Furthermore, soft computing is a foundation component for the emerging field of conceptual intelligence.

6. IMPORTANCE OF SOFT COMPUTING

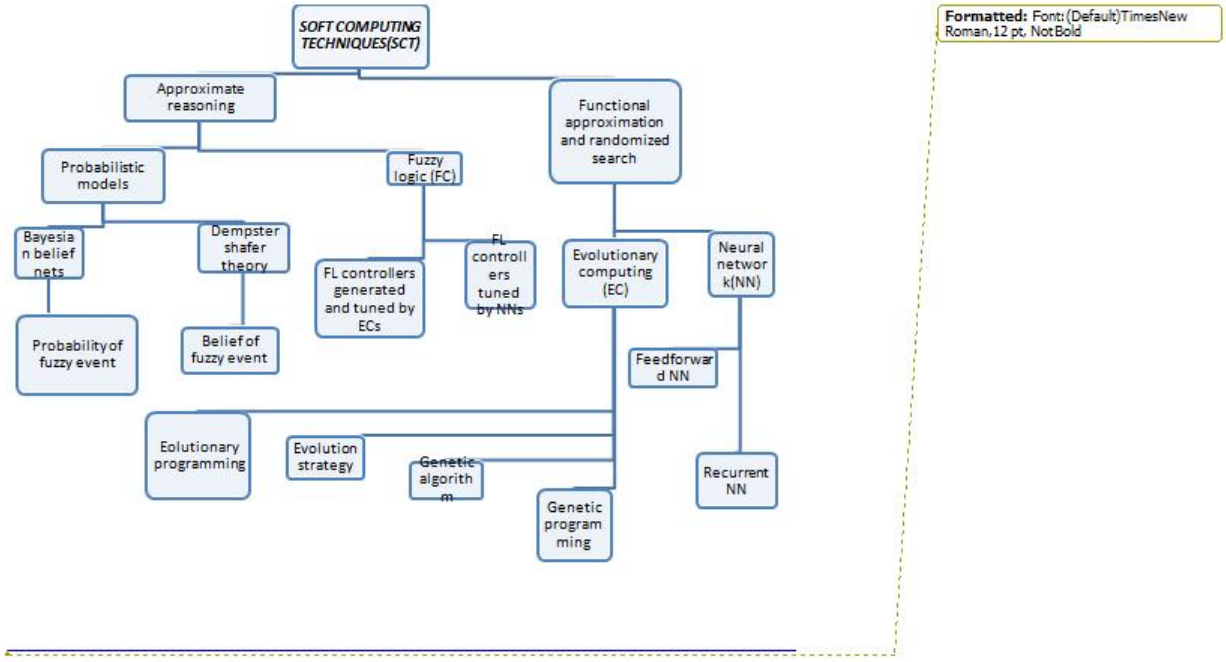
The effective combination of soft computing is known as “neuro fuzzy systems” these systems have high machine intelligence significant. They have both consumer products and industrial systems. The products are employed in soft computing technique quotient. The conceptual structure of soft computing suggests the students in many ways especially, they should not be trained just in FUZZY LOGIC, NEURO COMPUTING, GENETIC PROGAMING or PROBABILISTIC REASONING[4]. At present BISC group (Berkeley Initiative on Soft Computing) comprises close to 600 students, professors, and employees of private and non-private organisation.

Currently BISC has 50 institutions with high ranks. In BISC freshers are allowed with supportive environment. Many members are interested to join in BISC.

7. APPLICATIONS OF SOFT COMPUTING

- Handwriting recognition
- Automotive systems and manufacturing
- Image processing and data compression
- Architecture
- Decision-support
- Systems power systems
- Neuro fuzzy systems
- Fuzzy logic control

The detailed diagram of soft computing techniques are,



Formatted: Font: (Default)TimesNew Roman,12 pt, Not Bold

Figure 2: Soft computing techniques (sct)

8. INSTRUSION DETECTION SYSTEM (IDS)

An intrusion detection system (IDS) is a hardware or software application used to monitor the system activities for malicious activities and produces reports to a management station. IDS have a variety of "flavours" and it aims to detect suspicious traffic in different ways.Intrusion detection and prevention systems (IDPS) are mainly focused on identifying possible incidents, logging information and reporting attempts. As well as, IDPS was used by organization to identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPS have become a necessary addition to the security infrastructure.[6] They use several techniques, which includes the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content[7].

9. TYPES OF IDS

There are different types of IDS based on three characteristics. They are,

Formatted: Font: (Default) Times New Roman, 12 pt, Fontcolor: Text 1

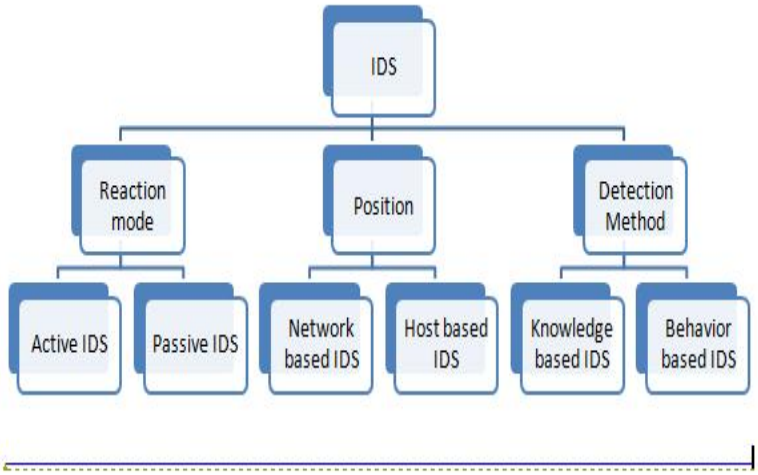


Figure 3: Types of IDS

10. ACTIVE IDS

An active Intrusion Detection Systems (IDS) is also named as Intrusion Detection and Prevention System (IDPS). Intrusion Detection and Prevention System (IDPS) is constructed to automatically block suspected attacks without any command required by an user. Intrusion Detection and Prevention System (IDPS) has the advantage of providing real-time corrective action to an attack.

11. PASSIVE IDS

A passive IDS is a system that is constructed only to check for the network traffic activity and alert an operator to potential vulnerabilities and attacks. A passive IDS is not capable of performing any protective and preventing functions by itself.

12. NETWORK BASED IDS

Network Intrusion Detection Systems (NIDS) usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in erratic mode and a separate management interface. The IDS will work along a network segment , monitoring of all other segments.

13. HOST BASED IDS

A Host Intrusion Detection Systems (HIDS) is a software application installed on hosts in workstations. The agents monitor the operating system and write data to log files.HIDS can onlymonitor the individual host on the workstations by the agents are installed and it cannot able to monitoring the whole network. These systems are used to monitor any intrusion attempts on critical servers.

14. KNOWLEDGE BASED IDS

A Knowledge-Based Intrusion Detection Systems is also referred as “signature based intrusion detection system”. It references a database of previous attack signatures and known system vulnerabilities. The meaning of word signature means a recorded evidence of the intrusion or attacks in IDS. Each attack leaves a footprint behind (e.g., nature of data packets, failed attempt to run an application, failed logins, file and folder access etc.). These footprints are called as signatures and it can be used to know and prevent the same attacks in the future. Based on these

signatures Knowledge-based (Signature-based) IDS checks intrusion attempts. They are also called as Misuse Based Detection Systems.

15. BEHAVIOR BASED IDS

An Anomaly-Based Intrusion Detection System is also known as behavior based intrusion detection system. It is a system for detecting computer attacks and misuse by monitoring system activity. It can be classified as either normal or anomalous. The classification is based on algorithmic or rules. This is as antonym to signature-based systems, which can only detect attacks for which a signature has been previously created. Determining what is attack traffic, the system must be thought to analyze normal system activity. This can be accomplished in such ways, most commonly with artificial intelligence techniques. Systems using neural network shares a great effect to do. Another thing, normal usage of the system comprises using a strict mathematical model, and flag any deviation from this attack. This is known as strict anomaly detection.

17. ATTACKS HANDLED BY IDS

Many types of attacks can be handled by IDS. Of them some of the primary attacks handled by IDS are illustrated in the following table.

Attack Type	Service	Mechanism	Effect of the attack
Ipsweep	ICMP	Abuse of feature	Identifies active machines
Mscan	Many	Abuse of feature	Looks for known vulnerabilities
Nmap	Many	Abuse of feature	Identifies active ports on a machine
Saint	Many	Abuse of feature	Looks for known vulnerabilities
Satan	Many	Abuse of feature	Looks for known vulnerabilities
SYN Stealth	Multiple	Abuse of feature	Identifies active machines
FIN Stealth	Multiple	Abuse of feature	Identifies active services
Ping Sweep	ICMP	Abuse of feature	Identifies active machines
Scan	Multiple	Abuse of feature	Identifies active UDP services
Null Scan	Multiple	Abuse of feature	Identifies active services
IP Scan	Multiple	Abuse of feature	Identifies active protocols
ACK Scan	Multiple	Abuse of feature	Identifies the firewall mechanism (stateful or simple network filter)
Window Scan	Multiple	Mis-configuration	Identifies active services
RCP Scan	Multiple	Abuse of feature	Identifies active remote procedure call ports (RPC)

Formatted Table

16. SOFT COMPUTING TECHNIQUES IN IDS

There are some techniques to be used to detect cyber attacks. Some basic techniques are,

Support Vector Machine (SVM)
Neural Network (NN)
Fuzzy logic (FL)
Evolutionary computation (EC).

18. SUPPORT VECTOR MACHINE (SVM)

support vector machines is also called as support vector networks[10].are developed learning models with given learning algorithms that analyze data and patterns, used for classification and regression. Some training examples, each marked for belonging to one of two decision method, Support vector networks training algorithm to builds a model that assigns new

examples into some category or the other, making it a non-probabilistic binary linear classifier. An SVM model is focused of the example, the examples of the separate categories are divided by a clear gap that is as wide as possible. New examples are then mapped into that same space and belonged to the category based on they fall on which side of the gap have it.

19. DEFINITION

A support vector machine constructs a set of hyper planes in a high- or infinite-dimensional space, which can be used for classification, regression, and such other tasks. A good separation is achieved by the hyper plane that has the largest distance to the nearest training point of any class. It is called as functional margin.

20. PROPERTIES

SVMs belong to a family of linear classifiers and can be interpreted as an extension of the perceptron. They can also be referred as important case of Tikhonov regularization.

Minimize the empirical classification error.

Maximize the geometric margin hence it is also called as maximum margin classifiers.

21. ARTIFICIAL NEURAL NETWORK (ANN)

In machine learning and biological science, artificial neural networks are a species of statistic learning models inspired by biological neural networks (the central nervous systems of animals, particularlybrain) and are used to accurate functions that can depend on a large number of inputs and basically unknown thing[11]. Neural Networks are generally presented as systems of interconnected "neurons" conversation with each other. The connections have numeric weights that can be tuned based on experience, making neural nets and capable of learning.

22. APPLICATION

Uses of artificial neural network models can be used to refer a function from observations. This is particularly useful in applications where the complexity of the data makes the design of such a function of hand unworkable.

23. FUZZY LOGIC (FL)

Fuzzy logic is a form of group-valued logic.the truth values of fuzzy logic is of real number between 0 and 1.Boolean logic, the truth values of variables are only 0 or 1. Fuzzy logic has been extended to concept of partial, where the truth value may range between completely true and false[8].The linguistic variables are used, when degrees may be managed by some specific functions[9].

- Propositional fuzzy logics are
- Monoidal t-norm-based propositional fuzzy logic
- Basic propositional fuzzy logic
- Łukasiewicz fuzzy logic
- Gödel fuzzy logic
- Product fuzzy logic
- Fuzzy logic with evaluated syntax

The general classification of soft computing technique metaheuristics is shown below,

Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Text 1

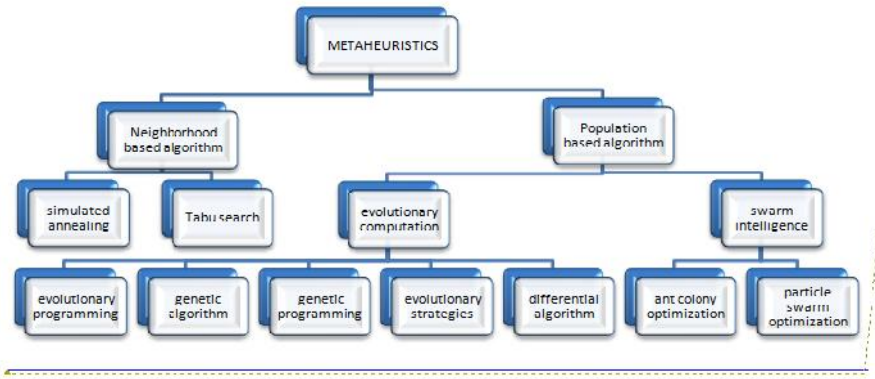


Figure 4: Met aheuristics

CONCLUSION & FUTURE SCOPE

The main objective of this study is to have a detailed knowledge on various tools and techniques required to handle cyber attacks. some of the soft computing techniques that can be applied to intrusion detection system has been summarized.

The present study can be extended to a detailed study on soft computing technique that can be applied to each layer in the instruction detection system.

REFERENCE

[1].Zadeh, Lotfi A., "Fuzzy Logic, Neural Networks, and Soft Computing," Communication of the ACM, March 1994, Vol. 37 No. 3, pages 77-84.

[2].X. S. Yang, Z. H. Cui, R. Xiao, A. Gandomi, M. Karamanoglu, Swarm Intelligence and Bio-Inspired Computation: Theory and Applications, Elsevier, (2013).

[3].D. K. Chaturvedi,Soft Computing: Techniques and Its Applications in Electrical Engineering, Springer, (2008).

[4].A Definition of Soft Computing - adapted from L.A. Zadeh

eliance spells end of road for ICT amateurs", May 07, 2013, The Australian

[5]. Abdullah A. Mohamed, "Design Intrusion Detection System Based On Image Block Matching", International Journal of Computer and Communication Engineering, IACSIT Press, Vol. 2, No. 5, September 2013.

[6].Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)" (PDF). Computer Security Resource Center (National Institute of Standards and Technology) (800–94). Retrieved 1 January 2010.

[7].Novák, V., Perfilieva, I. and Močkoř, J. (1999) Mathematical principles of fuzzy logicDodrecht: Kluwer Academic. ISBN 0-7923-8595-0

[8].Ahlawat, Nishant, AshuGautam, and Nidhi Sharma (International Research Publications House 2014) "Use of Logic Gates to Make Edge Avoider Robot." International Journal of Information & Computation Technology (Volume 4, Issue 6; page 630) ISSN 0974-2239 (Retrieved 27 April 2014)

[9].Cortes, C.; Vapnik, V. (1995). "Support-vector networks". Machine Learning20 (3): 273. doi:10.1007/BF00994018

[10].Hertz J., Krogh A., Palmer, R. G. (1991) "Introduction to the Theory of Neural Computation," Addison –Wesley.