ISSN:0975-9646

Hostility Cyber Crime Using Artificial Representative Systems

P.Nagarani[1],O.Naga Kumari[2],G.Archana[3]

[1]*Assistant Professor in Department of Information Technology in Teegala Krishna Reddy Engineering College,Telangana,India.*
[2]*Assistant Professor in Department of Information Technology in Teegala Krishna Reddy Engineering College,Telangana,India.*
[3]*Assistant Professor in Department of Information Technology in Teegala Krishna Reddy Engineering College,Telangana,India.*

Abstract- Information technology (IT) is something that is being evolved day by day. As a negative aspect of IT, with the help of technological advancements, criminals are using cyberspace to commit numerous cyber-crimes. Since people are connected to the cyber space with their own devices, they are all vulnerable to intrusions and other various kinds of threats. Basic protection methods, such as internet security suits, are not just enough to protect the data and devices. Introducing effective and highly advanced cyber defense systems has become essential. As of today, with the technology, the globe is moving towards the artificial intelligence (AI). AI plays a major role in technology and has been involved with many technological aspects as well. Creating cyber defense systems, using intelligent Representatives has become a trend by today. Basically, an intelligent Representative is a software component which can be emerged in an environment, take decisions, and has the ability of noticing and representing. The purpose of this study is to introduce a sophisticated cyber-crime defense system which involves intelligent Representatives that are based on artificial intelligence.

Keywords :Artificial Intelligence, Cyber Crime Expert Systems, Intelligent Representatives, Neural nets,.

1. INTRODUCTION

With the advances in information technology (IT) criminals are using cyberspace to commit numerous cyber crimes. Growing trends of complex distributed and Internet computing raise important questions about information security and privacy. Cyber infrastructures are highly vulnerable to intrusions and other threats. Physical devices such as sensors and detectors are not sufficient for monitoring and protection of these infrastructures; hence, there is a need for more sophisticated IT that can model normal behaviors and detect abnormal ones. These cyber defense systems need to be flexible, adaptable and robust, and able to detect a wide variety of threats and make intelligent real-time decisions [1, 2]. With the pace and amount of cyber attacks, human intervention is simply not sufficient for timely attack analysis and appropriate response. The fact is that the most network-centric cyber attacks are carried out by intelligent representatives such as computer worms and viruses; hence, hostility them with intelligent semi-autonomous representatives that can detect, evaluate, and respond to cyber attacks has become a requirement. These so called computer-generated forces will have to be able to manage the entire process of attack response in a timely manner, i.e. to conclude what type of attack is occurring, what the targets are and what is the appropriate response, as well as how to prioritize and prevent secondary attacks [3].AI offers this and various other possibilities. Numerous nature-inspired computing methods of AI (such as Computational Intelligence, Neural Networks, Intelligent Representatives, Artificial Immune Systems, Machine Learning, Data Mining, Pattern Recognition, Fuzzy Logic, Heuristics, etc.) have been increasingly playing an important role in cyber crime detection and prevention. AI enables us to design autonomic computing solutions capable of adapting to their context of use, using the methods of self-management, self-tuning, self-configuration, self-diagnosis, and self healing.

2. CYBER CRIMES:

DEFINITION, ISSUES the rapid development of computing technology and internet had a lot of positive impact and brought many conveniences in our lives. However, it also caused issues that are difficult to manage such as emergence of new types of crimes. For instance, common crimes such as theft and fraud attained new form of “Cyber Crimes” through information technology. Moreover, as this technology continues to evolve, criminal cases change correspondingly. Every day we are faced with increasing number and variety of cyber crimes, since this technology presents an easy way for criminals to achieve their goals. Furthermore, information technology facilitates globalization of these crimes by erasing country borders and making it much harder to monitor, detect, prevent or capture cyber criminals [4, 5, 6].

3. ARTIFICIAL INTELLIGENCE (AI) TECHNIQUES FOR CYBER SECURITY

3.1 Expert Systems An Expert System is a computer system that copies the decision making ability of a human. This is a best example of Knowledge based system. These knowledge-based systems are composed of two sub-systems: the Knowledge Base and the Inference Engine. The knowledge base represents the illustrations and assertions in the real world. The Inference Engine is an automatic reasoning system. It evaluates the current situation of the knowledge base and applies the rules relevant to that, then asserts new knowledge in to it. CSIA - Cyber Security Artificial Intelligence Expert System has the following components in Knowledge base and

Inference Engine. Expert Systems Knowledge Base Malicious IP Address Known Malware Known Virus Approved Applications Approved IP Addresses End Point Usage Statistics. Inference Engine IP Address Geographical Location Connection Attempts Connection Patterns Frequency of Program Use Document Usage Login Timestamps Login Attempts Port Communication File/Folder Access Patterns A. Security Expert System The Security expert system follows a set of rules to battle cyber-attacks. It checks the process with the knowledge base if it is good known processes then the security system ignore otherwise the system would terminate the process. If there is no such process in knowledge base, then using inference engine algorithms (rule sets), the expert system finds out the machine state. The machine state has been composed into three states namely safe, moderate and severe. According to the machine state, the system alerts the administrator or the user about the status, and then the inference has been feed to Knowledge base.

3.2 Neural Nets Neural Nets is also known as deep learning. It is an advanced branch of AI. It is inspired by the functions and working of the human brain. Our brain has several neurons, which are largely general purpose and domain-independent. It can learn any type of data. In 1957 Frank Rosenblatt created an artificial neuron (Perceptron) which paved the way for neural networks. These perceptron can learn and tackle absorbing issues by combining with other nerves i.e., perceptron. Perceptron learn on their own to identify the entity on which they are trained by learning and processing the high level raw data, as our brain learns in its own from the raw data using our sensory organ's inputs. When we apply this deep learning (trained) to cyber security, the system can identify whether a file is malicious or legitimate without human interference. This technique yields a strong result in detecting the malicious threats, compared with classical machine learning systems. The triumph of neural nets in cyber security is their speed. When they enforced in hardware or graphical processors it processes faster. Neural nets can permit the exact detection of new malware threats and fill in the dangerous gaps that leave organizations wide open to attacks.

3.3 Intelligent Representatives Intelligent Representative (IA) is an independent entity which recognizes movement through sensors and follows up on an environment using actuators (i.e. it is an representative) and directs its activity towards accomplishing objectives. Intelligent representatives may likewise learn or use knowledge base to accomplish their objectives. They might be extremely simple or very complex. A reflex machine, for example, thermostat is an intelligent representative. It has the behavior like understanding representative interaction language, pro-activeness and reactivity. They can adapt to real time, learn new things rapidly through communication with environment, and have memory based standard storage and recovery abilities. Intelligent representative is created in showdown against Distributed Denial of Service (DDoS) attacks. In case if there is any legal or business issue, it should be manageable to develop a "Cyber Police". Cyber Police should have mobile intelligent representatives. For this we should device the infrastructure to support the quality and interaction between the intelligent representatives. Multi-representative tools will give a lot of full-fledged operative appearance of the cyber police.

4. ARTIFICIAL INTELLIGENCE & CYBER SECURTY APPLICATIONS

4.1 CYBER ATTACKS The main aim of maintaining Security in Cyber environment is to protect the system from Hackers and also Software errors and Failures. There is a need for the development of the system that can detect and correct errors and also to defend against many types of incoming Network attacks. So integrating Artificial intelligence techniques in Cyber Security could lead to the development of such systems which could search and repair errors before they enter in to the Cyber area.

Figure 1: Hackers & Cyber Attack

4.2 CRIME PREVENTION: An early form of Artificial Intelligence called Computer Statistics was used to prevent certain cyber-crimes in Cyber environment. It is using a tool called Predictive Policing, where in artificial intelligence is combined with game theory to prevent Cyber-crime under Cyber area.

Figure 2: Cyber-crime and AI

PRIVACY PROTECTION: Privacy is one of the major concern of issue in today's complex world. Certain automation algorithms involving Artificial Intelligence have been used to improve privacy in and around us.

Figure 3: Privacy Protection with AI

4.3. IDENTIFY, RESEARCH AND COLLECT IDEA

Cyber attacking, it is a common word used in the present world. Daily thousands of computer networks or computer systems get attacked by an unknown systems or hackers in order to damage or destroy the system. In order to prevent and detect such attacks many systems are being developed. A background study was done in order to identify the available technologies, mechanisms etc.

5. INTRUSION DETECTION SYSTEM :

5.1 An Intrusion Detection System or IDS is a network security technology originally built for spotting vulnerabilities that exploit against a targeted application or a computer system. It is the process of monitoring the events occurring in a computer system or in a network and analyzing them for possible incidents indications, which are violations or impending threats of destruction of computer security strategies, suitably used policies, or common security practices. An ID system gathers and analyzes information from various sources within a computer or a network to identify possible security breakings, which include both intrusions and attacks from the outsiders the organization and does not use them properly or attacks within the organization. Particular intruders can be pin pointed and shown through an algorithm [7] [8] . Intrusion detection system only can identify intrusions, and it cannot prevent the system from attacks [9] . It should be fast enough to identify the intruders (external or internal intruders) as soon as the attack is going on. In IDSs efficiency is a more important feature. Intrusion Detection System (IDS) technologies are not very effective as there are several limitations, such as performance, scalability and flexibility. Intrusion Prevention System (IPS) is a new approach to defense networking systems. Figure 01 indicates how an IDS is placed in a system.

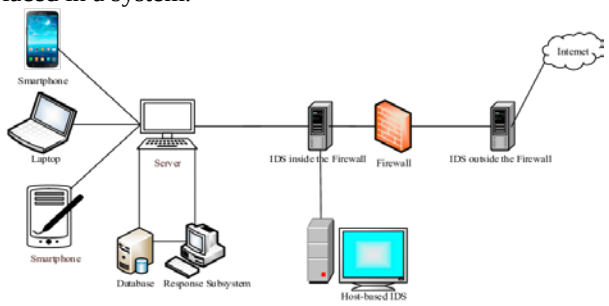

Figure 4: Intrusion detection system

5.2 Intrusion Prevention System

Intrusion prevention systems or IPS, also known as intrusion detection and prevention systems or IDPS, are network security appliances that monitor networks and system activities for malicious activities. The IPS often lies directly behind the firewall and provides a complementary or integral layer of analysis that selects for dangerous contents. Intrusion prevention is a preemptive approach in network security which is used to identify potential threats and respond to them swiftly. Like an intrusion detection system (IDS), an intrusion prevention system (IPS) checks and controls network traffic. However, because an exploit may be carried out quickly after the attacker gains access, intrusion prevention systems also have the ability to take immediate actions, it's about a bunch of rules created by the network administrator. As an example, IPS might drop a packet that it determines to be malicious and block all further traffic from that IP address or port [9]. Legitimate traffic, meanwhile, it should be sent forward to the recipient with no sudden interruption or delay of service. Unlike its predecessor the Intrusion Detection System (IDS) is known to be a passive system that scans traffic and alerts back the threats the IPS is placed intact with (in the direct communication path between source and destination), automated actions will be taken on entire traffic flows that enter the network by actively analyzing them. Specifically, these actions include:

- Dropping the malicious packets;
- Sending an alarm to the administrator;
- Blocking traffic from the source address;
- Resetting the connection.

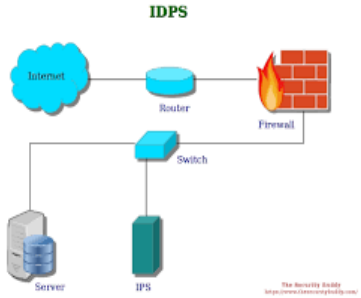

Figure 5: Intrusion prevention system

5.3 Cyber Security System / Cyber Attack Detection Systems (CADS):

Cyber Attack Detection Systems (CADS) and its generic framework perform well for all the classes. This is based on Generalized Discriminate Analysis algorithm (GDA) for feature decrement of the cyber-attack datasets and a collective approach of classifiers for classification of cyber-attacks [1]. Cyber Attack Detection System is having improved detection accuracy for all the classes of attacks. Cyber Attack Detection Systems are of two types [2]. Host Intrusion Detection Systems (HIDS) and Network Intrusion Detection Systems (NIDS). Host intrusion detection refers to the class of intrusion detection systems that reside on and monitor an individual's host machine.

5.4 Detects denial-of-service (DOS) attacks

A DoS attack is an attack type which is used to make a computer or a network resource unavailable to the users, such as to temporarily or permanently interrupt or suspend services of a host connected to a network. By targeting user's computer and its network connection, or the computers and network of the sites the user is trying to use, an attacker may be able to prevent the user from accessing email, websites, online accounts (banking, etc.), or other products and services that reside on the affected computer. The most common type of DoS attack is a situation where an attacker floods a network with information. When the user types an URL for a particular

website into web browser, he is sending a request to that site's server to view the page. Only a certain amount of requests will be processed by the server at a time, therefore requests will not be processed if an attacker swamps the desired server with. This is known as a "Denial of Service" because the user will not be able to access that site.

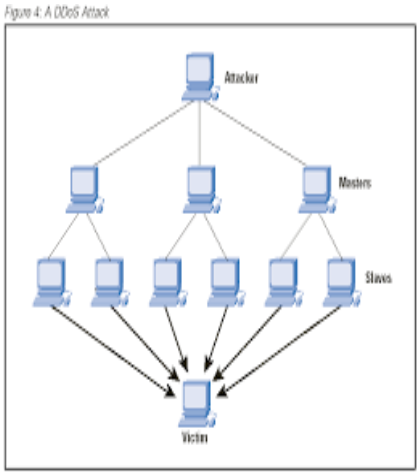

Figure 3: Typical DOS Attack

5.5 Representative Based / Artificial Representative

An entity that can be activated, autonomous and has the capability of formulating inner judgment can identify as an representative. An representative is a software program that gives assistance to user to complete some tasks or activities. Representatives in a multi-representative system (MAS) must be able to cooperate and work together with every user of the system [4] [8]. Therefore, a common language is requisite for the purpose of communication, an Representative Communication Language, or ACL can be used for this. Intelligent representatives are software components which have special features of intelligent behavior such as pro-activeness, understanding of an representative communication language [2] [3]. They may also possess features such as mobility, adaptability and collaboration. Multi-representative system is a system which consists of multiple representatives interacting with each other to learn or exchange experience [4] [8]. Consequently more complete operational picture of the cyber space can be provided by these multi-representative tools.

5.6 Algorithms

An algorithm can be identified as a procedure or a formula which helps in solving a problem. A computer program can be viewed as an implementation of an algorithm. In mathematics and computer science, an algorithm usually means a procedure that helps to solve a recurrent problem. New approaches can be made by combining set of algorithms in order to detect and defeat cyber-attacks [5] [9]. Combining Fuzzy logic and Genetic Algorithm (GA) for identify intrusions has being developed since there is an essentiality of a high security approach to safe and confident communication of information between different organizations [7]. In creating new approaches FUZZY LOGIC algorithm and GENETIC algorithm are being used. Genetic Algorithm is an optimization algorithm that helps in finding appropriate fuzzy rules. Fuzzy rule is a machine learning algorithm. Fuzzy logic along with genetic based approach gives more powerful performance.

5.7 Data sharing between representatives

Representatives share its data with other representatives in the system. In sharing data, the system has used wide varieties of sharing schemes such as, centralized data reporting on one side and decentralized sharing on the other. This article present a theoretical concept and framework based on peer-to-peer computing in order to integrate a multi-representative system. But this is sharing results in a scalability bottleneck due to the high volumes of incoming data; these systems often have slow performance or slow reaction

5.8 Data mining

Data mining /data or knowledge discovery is the process of analyzing data from different perspectives and transforming it to useful information. It allows users to analyze data from many different dimensions, categorize it, and summarize the identified relationships. Typically, data mining is the process of identifying correlations or patterns among fields in large relational databases. Data mining concept can be used to analyze a multi-representative based approach in intrusion detection. Analyzing previous cyber attacking details using data mining techniques predictions regarding the future attacks can be done.

6. Advantages Of AI Techniques

I. Expert Systems - Decision Support - Intrusion Detection - Knowledge Base - Inference Engine

II. Neural Nets - Intrusion Detection and Prevention System - High speed of operation - DoS Detection - Forensic Investigation

III. Intelligent Representatives - Proactive - Representative Communication Language - Reactive - Mobility - Protection against DDoS.

7. Conclusion

AI is considered as a standout amongst the most encouraging advancement in the information age and cyber security. New techniques, algorithm, tools and enterprises offering AI based services are always rising with respect to the worldwide security showcase. Contrasted with traditional cyber security solutions, these frameworks are more adaptable, flexible and robust, therefore enhancing security execution and better protect system from an expanding number of refined cyber threats. Right now, profound learning procedures are potentially the most encouraging and effective tools in the domain of AI. There is additionally an earnest requirement for use of intelligent cyber defense methods in a various areas where the most appropriate technology is not only neural nets. As of recently, neither individuals nor AI alone have demonstrated general achievement in cyber security. Regardless of the immense change that AI has conveyed to the domain of cyber security, related

frameworks are not yet ready to alter completely and consequently to changes in their condition. In addition a holistic view on the cyber environment of associations is required.

8. SCOPE FOR FUTURE WORK

Cyber security needs much more attention. Given human limitations and the fact that representatives such as computer viruses and worms are intelligent, network-centric environments require intelligent cyber sensor representatives (or computer-generated forces) which will detect, evaluate and respond to cyber attacks in a timely manner [3]. International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, No. 1, January 2015 34 Application of AI techniques in cyber defense will need planning and future research. One of the challenges is knowledge management in network-centric warfare, hence a promising area for research is introduction of modular and hierarchical knowledge architecture in the decision making software. Rapid situation assessment and decision superiority can only be guaranteed with automated knowledge management. It is also foreseeable that the grand goal of AI research – development of artificial general intelligence - can be reached in not so distant future which would lead to Singularity described as "the technological creation of smarter-than-human intelligence". Nevertheless, it is of crucial importance that we have the ability to use better AI technology in cyber defense than the one offenders possess [5]. Furthermore, a lot more research needs to be done before we are able to construct trustworthy, deployable intelligent representative systems that can manage distributed infrastructures. Future work must search for a theory of group utility function to allow groups of representatives to make decisions . For future work in enhancing IDPSs, unsupervised learning algorithms and new techniques will be considered together to create hybrid IDPS which will improve the performance of anomaly intrusion detection . Moreover, combining all kinds of AI technologies will become the main.development trend in the field of anti-virus technology [7]. or power issues on the ethical side or questions of due process on the legal side. A wide range of both ethical and legal questions come up in the light of the human judgment", "to what degree do we want to allow technology to take human roles" or "what legal precedent can be applied to machines" will need to be answered .

REFERENCES

[1] H. Chen, F. Y. Wang, (2005) "Guest Editors' Introduction: Artificial Intelligence for Homeland Security", IEEE intelligent systems, Vol. 20, No. 5, pp. 12–16. International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, No. 1, January 2015 35

[2] D. Dasgupta, (2006) "Computational Intelligence in Cyber Security", IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety (CIHSPS 2006), pp. 2–3

[3] M. R. Stytz, D. E. Lichtblau, S. B. Banks, (2005) "Toward using intelligent representatives to detect, assess, and counter cyberattacks in a network-centric environment", Ft. Belvoir Defense Technical Information Center, 1. Edition, Alexandria, VA.

[4] J. Helano, M. Nogueira, (2006) "Mobile Intelligent Representatives to Fight Cyber Intrusions", the International Journal of Forensic Computer Science (IJoFCS), Vol. 1, pp. 28-32.

[5] E. Tyugu, (2011) "Artificial intelligence in cyber defense", 3rd International Conference on Cyber Conflict (ICCC 2011), pp. 1–11.

[6] A. Patel, M. Taghavi, K. Bakhtiyari, J. Celestino Júnior, (2012) "Taxonomy and Proposed Architecture of Intrusion Detection and Prevention Systems for Cloud Computing", Y. Xiang et al. (Eds.), Springer-Verlag Berlin Heidelberg, pp. 441 458.

[7] S. Singh and S. Silakari, "A Survey of Cyber Attack Detection Systems", IJCSNS International Journal of Computer Science and Network Security, vol. 9, no. 5, 2009 [Online]. Available: http://paper.ijcsns.org/07_book/200905/20090501.pdf. [Accessed: 08- Feb- 2016].

[8] S. Simmons, D. Edwards, N. Wilde, J. Just and M. Satyanarayana, "Preventing Unauthorized Islanding: Cyber-Threat Analysis", 2006 IEEE/SMC International Conference on System of Systems Engineering, pp. 5, 24-26 [Online]. Available: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=165229&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1652294. [Accessed: 11- Feb- 2016].

[9] S. Dilek, H. Çakır and M. Aydın,"APPLICATIONS OF ARTIFICIAL INTELLIGENCE TECHNIQUES TO HOSTILITY CYBER CRIMES: A REVIEW", International Journal of Artificial Intelligence & Applications (IJAIA), vol. 6, no. 1, 2015 [Online]. Available: http://arxiv.org/ftp/arxiv/papers/1502/1502.03552.pdf. [Accessed: 13- Feb- 2016].