CPUH-Research Journal: **2018,** ***3(2),*** 140-145
ISSN (Online): 2455-6076
http://www.cpuh.in/academics/academic_journals.php

Artificial Neural Networks Plausibility to Deterred Cyber Criminals: A Review

Anurag Rana
Department of Computer Science and Engineering, Arni University (Indora) Kangra (H.P.) INDIA
E-mail: anuragrana.anu@gmail.com

ABSTRACT: Cyberspace is created by human beings, not in nature, has the unidentified hazards. Cyber warfare defined as "action by a nation-state to penetrate another nation's computer or networks". Cyber espionage and cyber attacks are types of threat. Cyber espionage caters information required to attacks. Cyber crime can now occur virtually anywhere through the work of experts and apprentices. Cyber criminals are rapidly discovering. The speed at which cyber crime occur leaves little bit hope for human interaction to endure without human error. The solution may be too advanced for human but doable for something created by humans: "Artificial Neural Networks".

Keywords: Cybercrime; ANN; IDS; cyber criminals

INTRODUCTION

Today, the world is interconnected; communications activities take place via the electronic devices and Internet. The dramatically growth of internet users and cyber communication, raises question about security of cyberspace information's. Cyberspace is the environment that is used for national wide communication by computer networks. Cyberspace domain is characterized in networked systems and associated physical infrastructures by the use of electromagnetic and electronics spectrum to save, alter, transfer of data. In consequence, cyberspace might be the intellection of interconnection of human with the computers and telecommunication, not including the heed to physical geography. As cyber space matures, International System has a new challenge in facing the use of force. To can create devastating real-world consequences using non-traditional weaponry, the Non-State Actors (NSA) continue to emerge, come by skill and proficiency required to the waging of conflict against an enemy. Cyberspace is endangered to threat. Cyberspace vulnerable threats are rapidly targeting citizens, financial houses and governments.

Cyber criminals are discovering new ways to threaten the citizens, corporate houses and governments. So, it's obvious hard for good guys to keep up with them. With the speed of cyber activity and high volume of data used, it is difficult to protect the cyber space by physical device or by intervention of human beings. It needs considerable automation to detect threats and to make intelligent real-time decisions. It is difficult to protect against evolving attacks by developing any software with conventional algorithms. It can be tackled by applying bio inspired computing methods of neural networks to software. Artificial Neural Networks functions with numbers of characteristics existent in human brain like problem solving, deduction, reasoning, social intelligence and creativity.

NATIONAL SECURITY

The fundamental requirements are security of humans, societies, and states. In INDIA, the DoIT (Department of Information Technology) exerted the CERT-In (India Computer Emergency Response Team) in the year 2004 to foil cyber attacks. In the year 2011, there were about 13,301 attack counted. After that, the government of India established a subdivision NCIIPC (National Critical Information Infrastructure Protection Centre) to foil attacks against defense, space, banking, telecom, energy power, transport and other sensitive's fields.

CYBER WAR AND CYBER CRIME

Cyber War: Cyber wars have been experienced by human beings since the dawn of history. The newness of cyber space and its lack of correspondence to the basic concepts of the world, there is no definition formulated to cyber war. Hostile action in cyber space graded according to the types of action undertaken and damage caused.

The proposed classification, arranged in descending order of severity:

1. The physical damage cause's by an attack on assorted civilian.
2. The physical damage cause's by the interruption of an attack on vital national information infrastructures.
3. Interruption of an attack on army targets in the state's sovereign territory.
4. Interruption of an attack on army targets outside the state's sovereign territory.
4. Insertion of hibernating attack tools, e.g.: Trojan horse or logic bomb that are for an attack.
5. Criminal Action, Industrial Reconnaissance.
6. Use of double purpose arm: Intelligence Gathering, Probing for common security exposure, penetration tests.

7. Organizing a media campaign propaganda, maltreat and disfiguration of official websites.

A cyber attack does not include kinetic damage to cyber space infrastructure. Cyber tools and its hardware and software weapons are use for attack in cyber space. The determination of an attack is not easy and simple. The ruling out the possibility of a technical flaw and determining an intrusion is not adequate. The entire spectrum of cyber threats is used by intrusion, and when an unauthorized move towards a computer resource occurs, it may be used for all kinds of activities, and it is difficult to identify the identity of the intruder and his impelling to action.

Cyber Crime: Cyber crime is crime that involves an electronic communication device and communication networks. The computer system may has used in the delegacy of a crime, or it can be the target. Debarati Halder and K. Jaishankar define cybercrime as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modem telecommunication networks such as INTERNET and mobile phone." Cybercrime circumscribes any criminal deed to dealing with computer systems and networks (known as hacking). Cybercrime also include traditional crimes conducted through the Internet. Internet fraud, hate crimes, telemarketing, credit card account thefts and determine theft are reckon to be cybercrimes, when the illegal activities are committed through the use of an Internet and computer. Cyber crimes may be defined as the unlawful deed where the computer system is used either as a tool or a target or both. Credit Card frauds, Bank Robbery, Phishing, Illegal down loading, industrial Espionage, Kidnapping Children, Children Pornography via cyber terrorism, scams, chat rooms, creation and /or distribution of viruses, spam and many other are general term that consider as crimes.

Types of Cybercrime: Cybercrimes can be classified in two ways:

1. Crimes where computer is target. DOS Attack, Virus attacks, hacking is examples.
2. Crimes include cyber terrorism, IPR violations, credit card frauds, EFT frauds, pornography etc. in which laptops, smart phones and computers are used as weapons.

ARTIFICIAL NEURAL NETWORK

An ANN is associate degree scientific discipline model that's galvanized by the approach biological system, resembling the human brain, method data. The keystone of this model is that the organization of data process system. It is composed of an oversized range of highly interconnected process components (neurons) operating in unison to resolve specific drawback. Artificial Neural Network may be a massively parallel distributed processor created from straightforward process units that includes a natural capability for storing experimental information and creating it out there to be used. A man-made neuron cell network (ANN) can be a procedure model supported the structure and functions of biological neural networks. A NN changes – or learns, in a very sense - supported that input and output, so, the flows of data affects the organization of ANN.

ANNs area unit thought of nonlinear applied math knowledge modeling tools wherever the complicated relationships between inputs and outputs area unit sculptured or patterns area unit found. ANN has many blessings however one in all the foremost recognized of those is that the proven fact that it will really learn from perceptive knowledge sets by victimization ANN as a stochastic perform approximation tool. These styles of tools facilitate calculate the foremost Cost-efficient and perfect ways for inward at solutions, whereas process computing functions or distributions. ANN takes knowledge instances instead of overall knowledge sets to make solutions, which save both cash and time. Artificial neural networks area unit thought of fairly straightforward mathematical model to reinforce current knowledge evaluation techniques. ANNs have three layers that are interconnected. Primary Layer consists of input neurons. Those neurons send knowledge to the second layer that successively sends the output neurons to the third layer. Coaching a man-made neural networks involve the selecting from allowed models that there are units many associated algorithms. ANN is additionally called a neural network.

INTRUSION DETECTION AND INTERFERENCE SYSTEM

Intrusion detection system (IDS) is intended to observe inward and outward networks activity. Also, establish any wary patterns that will indicate system or network attacks from somebody trying to disrupt into the system. IDS is taken into the account to be an inactive-monitoring system, since the most perform of associate degree IDS products are to admonish you of wary activity happening − not forestall them. Associate degree IDS basically reviews the network traffic and knowledge and can establish attacks, probes, exploits and different exposures.

Intrusion Detection System can be device or code that may give protection from outsider users and internal attackers, wherever traffic does not go past the firewall the least bit. Intrusion Detection System supervises network or system activities for vicious activi-

ties or policy violations and produces reports to a management node. The firewall defend a corporation from malicious attacks from the net if anyone tries to disrupt in with firewall or manage to disrupt within firewall security. Also, tries to access any system within sure aspect. It modify the supervisor in case any breach in security. IDS's are sort to smoke detector that raises associate degree alert if a particular thing happens. IDSs will reply to the suspicious event in one in all many ways in which, which incorporates displaying associate degree alert, work the event or maybe paging associate degree administrator. The IDS could also be prompted to reconfigure the network to cut back the consequences of the suspicious intrusion. IDS are two types one is Network-Based Intrusion Detection Systems (NIDS) and other is Host-Based Intrusion Detection Systems (HIDS).

An ID performs range of functions:

a) Observation system and users action.
b) Inspect system configuration for exposures and misconfigurations.
c) Assessing the integrity of important system and knowledge files.
d) Distinguish known attack in system action.
e) Distinguishing unknown action using applied mathematics evolutions.
f) Managing audit trials and lightness user violation of norms or traditional action.
g) Put in and operative traps to record data concerning intruders.
h) Correcting system configuration errors

ARTIFICIAL NEURAL NETWORKS TO DETERRED CYBER CRIMINALS

Artificial Neural Network could be a massively parallel distributed processor created of straightforward process units, that encompasses a natural capability for storing experimental data and creating it out there to be used [8]. Chen (2008) represented Neuro Net – a neural network system that's expert in observance the traffic, spot the traffic anomalies and it triggers countermeasures for it. The experiment leads to NS-2 showed that Neuro Net is effective against one form of hidden attack referred to as low-rate TCP-targeted distributed DoS attacks that are additionally called shrew attacks [22]. Iftikhar et al (2009) designed a system supported ANN to discover searching attacks. It adopted a supervised neural network development to examine the feasibleness of artificial neural network approach to searching attacks which are idea of others attacks in electronic net systems. The developed system is applied to totally different searching attacks and whereas examination its performance to alternative neural networks approaches and therefore the outcomes indicate the approach supported Multiple Superimposed Perceptron (MLP) design is a lot of precise and correct. Also, it shows optimum outcomes as comparison to alternative ways Linda et.al (2009) given a unique IDS-NNM-Intrusion Detection System victimization neural nets based model that use selected combination of two neural net learning algorithms particularly Levenberg-Marquardt and Error Back Propagation for modeling. Experimental results showing IDS-NN model rule is capable of capturing all intrusion makes an attempt given within the nets communication while not generating any false alarm [24]. Barika (2009) suggests Artificial Neural spec for deciding among intrusion detection systems with the goal of accumulated potency [25]. Iftikhar et al (2010) presents AN analysis of various neural network systems particularly Self-Organizing Map (SOM), Adaptive Resonance Theory (ART), on-line Back Propagation (OBPROP), Resilient Back Propagation (RPROP) and Support Vector Machine for Intrusion detection mechanisms victimization the multi- criteria deciding (MCDM) techniques. The outcomes show that in term of performance, inspected neural nets are higher, whereas relating to coaching overhead and power for managing wide-ranged and organized intrusion unattended NNs are higher. From this the conclusion is that Hybrid buttonhole of neural nets are the best resolution within space for intrusion detection [26]. Brij (2011) ANN is used to estimate variety of Zombies concerned in very flooding Distributed Denial of Services (DDoS) attack that are useful to conquer the outcome of attack [27]. Wu dialect (2009) given a hybrid methodology for spam filtering that uses rule-based process and back-propagation neural nets. Since the spamming behaviors could often modification, this methodology has evidenced to a greater extent sturdy examined to alternative spam sensing approaches which think about keywords [28]. Kufandirimbwa and Gotora (2012) given a way to spam filtering victimization Artificial Neural Networks, and therefore the perception learning methodology that produces favorable detection rates owing to the incorporation of never-ending learning feature as compared to alternative spam detection ways supported content and alternative characteristics of the message [29]. Venkatesh et al (2012) had given a Multi –layer feed forward neural net coaching framework victimization daring Driver Back-propagation learning rule for hypertext transfer protocol Botnet detection that encompasses smart determinations veracity with lesser extent to false positives [30]. Devikrishna et al (2013) had given A Multi Layer Perception (MLP) for intrusion detection and used data discovery in info (KDD) for classification of attacks [31]. Zhai (2014) projected multi-agent distributed intrusion detection system (DIDS) framework that supported Back-propagation neural nets for

intrusion detection with the benefits of reducing the number mobile method of knowledge, load equalization, detective work analysis showing neatness, and higher error-tolerating and detective work distributed intrusion effectively [32].

CONCLUSIONS

Today's, our most of communications and commercial activities now take place via the Internet. It caused various contents which are hard to negotiate. The emergences of cybercrimes and to deter cyber criminals are difficult. Available research and pedagogy assets demonstrate that ANN methods have applications for fight against to deter cyber criminals and cybercrimes. This review paper has concisely presented possibilities of ANN techniques so far in cyber field for combating to deter cyber criminals. In future, we can further go for practical implementation of intelligent system.

REFERENCES

[1] Selma Dilek, Hüseyin Çakýr and Mustafa Aydýn, **(2015)** "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes:A Review", *International Journal of Artificial Intelligence &Applications (IJAIA)*, Vol. 6, January.

[2] Manveer Kaur, Sheveta Vashisht, Kumar Saurabhi, **(2012)** "Adaptive Algorithm for Cyber Crime Detection", *International Journal of Computer Science and Information Technologies (IJCSIT)*, Vol. 3(3), 4381 –4384.

[3] Jheel Somaiya, Dhaval Sanghavi, Chetashri Bhadane, **(2014)** "A Survey: Web based Cyber Crimes and Prevention Techniques", *International Journal of Computer Applications* (0975 – 8887), Volume 105, November2014.

[4] Halder, D. Jaishankar, K, "Cyber crime and the Victimization of Women: Laws, Rights, and Regulations". *Hershey, PA, USA: IGI Global*. ISBN 978-1-60960-830-9

[5] Vineet Kandpal and R. K. Singh, **(2013)** "Latest Face of Cybercrime and Its Prevention In India", International Journal of Basic and Applied Sciences, Vol. 2, Pp. 150-156.

[6] Advocate,VivekTripathi,"InternetCrime",www.cyberlawsindia.net,Available:http://www.cyberlawsindia.net/internet-crime.html Cited on dated December 14th, 2017.

[7] V. Rajaraman, (2014) "JohnMcCarthy – Father of Artificial Intelligence", in General Article Resonance, March 2014.

[8] Anurag Rana, Ankur Sharma, **(2014)** "Optimization of Radial Basis Neural Network by Mean of Amended Fruit Fly Optimization Algorithm"*Journal Of Computer And Mathematical Sciences* Vol.5 (3): Pg.262-272.ISSN 0976-5727 (Print) ISSN 2319-8133 (Online).

[9] J. S. Russell, P. Norvig, (**2003)** Artificial Intelligence: A Modern Approach, Upper Saddle River, Prentice Hall, New Jersey, USA.

[10] G. Luger, W. Stubblefield, **(2004)** Artificial Intelligence: Structures and Strategies for Complex Problem Solving, Addison Wesley.

[11] Wikipedia, "Artificial Intelligence", en.wikipedia.org, Available: http://en.wikipedia.org/wiki/ Artificial_intelligence Cited on dated November 7th, 2017.

[12] Jacques Ferber, **(1999)** Multi-Agent System: An Introduction to Distributed Artificial Intelligence, Harlow: Addison Wesley Longman.

[13] UK-CI, "WorkshoponComputationalIntelligence", ukci.cs.manchester.ac.uk, Available: http://ukci.cs.manchester.ac.uk/intro.html.

[14] N. A. Alrajeh and J. Lloret, **(2013)** "Intrusion Detection Systems Based on Artificial Intelligence Techniques in Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, Vol.2013, Article ID 351047.

[15] S. Shamshirband, N. B. Anuar, M. L. M. Kiah, A. Patel, "An appraisal and design of a multiagent system based cooperative wireless intrusion detection computational intelligence technique," *Engineering Applications of Artificial Intelligence*, Vol. 26, pp. 2105–2127.

[16] Wikipedia, "Intrusion detection system", en.wikipedia.org, Available: http://en.wikipedia.org/wiki/ Intrusion detection system Cited on Dated December 27th, 2017.

[17] Gang Wang, Jinxing Hao, Jian Ma, and Lihua Huang, **(2010)** "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering", *Elsevier Ltd.*

[18] E. Tyugu, **(2011)** "Artificial intelligence in cyber defense", In Proceedings of the 3rd International Congress on Cyber Conflict (ICCC), pp. 1–11.

[19] X. B. Wang, G. Y. Yang, Y. C. Li and D. Liu, **(2008)** "Review on the application of Artificial Intelligence in Antivirus Detection System", In Proceedings of the IEEE Congress on Cybernetics and Intelligent Systems, pp. 506- 509.

[20] M Rajesh Kanna, D. Hemapriya and C. Divya, **(2013)** "Intelligent Agents For Intrusion Detection System (IAIDS)", *International Journal of Emerging Technology and Advanced Engineering*, ISSN 2250-2459, Volume 3, January 2013.

[21] N. Jaisankar, R. Saravanan, K.Durai Swamy, **(2009)** "Intelligent Intrusion Detection System Framework Using Mobile Agents", *International Journal of Network Security & Its Applications (IJNSA)*, Vol 1, July 2009.

[21]Yu Chen, **(2008)** "NeuroNet: Towards an Intelligent Internet Infrastructure", In Proceedings of the 5th IEEE Congress on Consumer Communications and Networking Conference (CCNC), pp. 543 547.

[22]Iftikhar Ahmad, Azween B Abdullah, and Abdullah S Alghamdi, **(2009)** "Application of Artificial Neural Network in Detection of Probing Attacks", In Proceedings of the IEEE Symposium on Industrial Electronics and Applications (ISIEA).

[23]Ondrej Linda, Todd Vollmer and Milos Manic, **(2009)** "Neural Network Based Intrusion Detection System for Critical Infrastructures", In Proceedings of the International Joint Congress on Neural Networks.

[24]F. A. Barika, K. Hadjar, and N. El Kadhi, "Artificial Neural Network for Mobile IDS Solution", Security and Management, pp 271–277.

[25] IftikharAhmad, AzeenAbdullah, and Abdullah Alghamdi, "Towards the selection of best neural network system for intrusion detection".

[26] Brij Bhooshan Gupta, Ramesh Chand Joshi, and Manoj Misra, **(2012)** "ANN Based Scheme to Predict Number of Zombies in a DDoS Attack", *International Journal of Network Security*, Vol.14, PP. 61–70, Mar 2012.

[27]C. H. Wu, "Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks", *Expert Systems with Applications*, Vol. 36, pp. 4321–4330.

[28]Owen Kufandirimbwa and Richard Gotora, **(2012)** "Spam Detection Using Artificial Neural Networks (Perception Learning Rule), *Online Journal of Physical and Environmental Science Research*, ISSN 2315-5027; Volume 1, pp. 22-29; June 2012.

[29] G Kirubavathi Venkatesh, and Anitha Nadarajan, **(2012)** "HTTP Botnet Detection Using Adaptive Learning Rate Multilayer Feed-Forward Neural Network", International Federation for Information Processing.

[30] Devikrishna K S and Ramakrishna B B, **(2013)** "An Artificial Neural Network based Intrusion Detection System" and Classification of Attacks", *International Journal of Engineering Research and Applications (IJERA)*, ISSN: 2248-9622 , Vol. 3, pp. 1959-1964.

[31] ZhaiShuang-can, Hu Chen-jun and Zhang Wei-ming, **(2014)** "Multi-Agent Distributed Intrusion Detection System Model Based on BP Neural Network", *International Journal of Security and Its Applications* Vol.8, pp.183-192.

[32]N. C. Rowe, **(2003)** "Counterplanning Deceptions To Foil Cyber-Attack Plans", In Proceedings of the IEEE Workshop on Information Assurance, pp. 203 210

[33] José Helan and Matos Nogueira, **(2006)** "Mobile Intelligent Agents to Fight Cyber Intrusions", *International Journal of Forensic Computer Science , IJoFCS*, pp 28-32.

[34]Mueen Uddin, Kamran Khowaja and Azizah Abdul Rehman, **(2010)**"Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents", *International Journal of Network Security & Its Applications (IJNSA)*, Vol.2.

[35]Mayank Aggarwal, Nupur and Pallavi Murgai, **(2011)** "Simulation of Dynamic Mobile Agent Model to Prevent Denial of Service Attack using CPNS", *International Journal of Computer Applications*, Volume 20.

[36] Ugur Akyazi , and A. Sima Uyar, **(2012)** "Distributed Detection of DDOS Attacks During the Intermediate Phase Through Mobile Agents", *Computing and Informatics*, Vol. 31, 759–778.

[37] Onashoga, S. Adebukola, Ajayi, O. Bamidele and Akinwale, A. Taofik, **(2013)** "A Simulated Multiagent-Based Architecture for Intrusion Detection System", *International Journal of Advanced Research in Artificial Intelligence (IJARAI)*, Vol. 2.

[38]Y. Zhang, L. Wang, W. Sun, R. C. Green II, M. Alam, **(2015)** "Artificial Immune System based Intrusion Detection in A Distributed Hierarchical Network Architecture of Paper ID: SUB155595 1722 *International Journal of Science and Research (IJSR)* ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438 Volume 4 Issue 6, June 2015.

[39]Amit Kumar Tyagi and Sadique Nayeem, **(2012)** "Detecting HTTP Botnet using Artificial Immune System (AIS)", *International Journal of Applied Information Systems (IJAIS)* – ISSN : 2249-0868 , Volume 2, May 2012.

[40] Ismaila Idris, **(2012)** "Model and Algorithm in Artificial Immune System for Spam Detection", *International Journal of Artificial Intelligence & Applications (IJAIA)*, Vol.3, January 2012.

[42] Smera Rockey and Rekha Sunny T , **(2014)** "A Hybrid Spam Filtering Technique Using

Bayesian Spam Filters and Artificial Immunity Spam Filters", *International Journal of Engineering Research & Technology (IJERT)* ISSN: 2278-0181,Vol. 3 , May – 2014.

[43] Ayei E. Ibor and Gregory Epiphaniou, **(2015)** "A Hybrid Mitigation Technique for Malicious Network Traffic based on Active Response", *International Journal of Security and Its Applications*, Vol. 9, pp. 63-80.

[44] Liu Guozhu and Shang Yanjun, **(2010)** "Unknown Virus Detection Method Amalgamation Genetic Algorithm into Ant Colony Algorithm", Journal of Computers, Vol. 5, June 2010.

[45] Ondrej Linda, Milos Manic, Todd Vollmer and Jason Wright,**(2011)** "Fuzzy Logic Based Anomaly Detection for Embedded Network Security Cyber Sensor ", In IEEE Symposium on Computational Intelligence in Cyber Security, 2011

[46] Mohammad Sazzadul Hoque, Md. Abdul Mukit and Md. Abu Naser Bikas, **(2012)** "An Implementation of Intrusion Detection System Using Fenetic Algorithm", *International Journal of Network Security & Its Applications (IJNSA)*, Vol.4, March 2012.

[47] A.A. Ojugo, A.O. Eboka, O.E. Okonta, R.E Yoro (Mrs) and F.O. Aghware, **(2012)** "Genetic Algorithm Rule-Based Intrusion Detection System (GAIDS)",*Journal of Emerging Trends in Computing and Information*, ISSN 2079-8407, Vol. 3, Aug 2012.

[48] Jitendra Nath Shrivastava and Maringanti Hima Bindu, **(2013)** "E-mail Classification Using Genetic Algorithm with Heuristic Fitness Function", *International Journal of Computer Trends and Technology (IJCTT)* – volume 4 August 2013.

[49] P. Jongsuebsuk, N. Wattanapongsakorn, and C. Charnsripinyo, "Real-time intrusion detection with fuzzy genetic algorithm, **(2013)** " In Proceedings of the 10th International Congress on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTICON), pp. 1-6.

[50] Roshna R.S and Vinodh Ewards, **(2013)** "Botnet Detection Using Adaptive Neuro Fuzzy Inference System", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 3, pp. 1440-1445, March -April 2013.