detection which has a good identification accuracy with less false positives [30].

Devikrishna et al (2013) presented A Multi Layer Perception (MLP) for intrusion detection and used Knowledge discovery in Database (KDD) for classification of attacks [31].

Zhai (2014) proposed a multi-agent distributed IDS (DIDS) model based on BP neural network for intrusion detection with the advantages of reducing the amount mobile process of data, load balancing, detecting analysis neatly, better error-tolerating, and detecting distributed intrusion effectively [32].

5.2 Application of Intelligent agents against cyber crimes

Intelligent agents are autonomous computer-generated forces with the capability to communicate with each other to share data and they can cooperate with each other in order to plan and implement appropriate responses in case of unexpected events. The intelligent agents' characteristics like mobility, adaptability in the environments they are deployed in, and their collaborative nature, makes them suitable for combating cyber attacks.

Rowe (2003) developed a tool to systematically counter plan the ways to prevent particular cyber attack plans using multi-agent planning and some novel inference methods [33].

Helano (2006) introduced a system implemented in Prolog which is a synthesis based on a multi-agent systems (MAS) approach with a practical case used to fight cyber intrusions and with the ability to verify the properties of cybercrimes [34].

Mueen Uddin et.al (2010) proposed a new model called Dynamic Multi-Layer Signature based IDS using Mobile Agents, which can detect forthcoming threats with very high success rate by dynamically and automatically creating and using small and efficient multiple databases, with a mechanism to update these small signature databases at regular intervals using Mobile Agents [35] .

Mayank et al (2011) simulated dynamic mobile agent model using Colored Petri Nets (CPNs) which enables the owner of the agent to detect the malicious host. The simulation result clearly proves that owner can detect the malicious hosts and thus prevent Denial of service attack to occur in real world [36].

Akyazi et al (2012) proposed a distributed intrusion detection system to detect Distributed Denial of Service attacks in a special dataset. This method is tested in a simulated-real time environment, in which the mobile agents are synchronized with the timestamp given in the dataset [37].

Onashoga et al (2013) proposed a Multi agent-based architecture for Intrusion Detection System (IDS) to overcome the shortcoming of current Mobile Agent-based Intrusion Detection System, with three major phases namely: Data gathering, Detection and the Response phase [38].

M. Rajesh Kanna et al (2013) designed a wireless distributed Wireless Intrusion Detection System (WIDS) based on Intelligent agents which consist four major components: Intrusion detection module, Alert, Mobile agent platform, Test suit [20].

5.3 Application of artificial immune system against cyber crimes

Artificial Immune Systems (AIS) are a class of computationally intelligent systems which imitate the biological immune systems. Since the artificial immune system has techniques to solve complex computations, AIS plays an important role in the cyber security research.

Zhang et al (2011) proposed a hierarchical Distributed Intrusion Detection SGDIDS namely SGDIDS System that is applicable to identification of malicious network traffic and improving system security for improving cyber security of the Smart Grid with an intelligent module. This system uses AIS to detect and classify malicious data and possible cyber attacks [39].

Amit Kumar et al (2012) proposed a new general HTTP Botnet detection framework for real time network using Artificial Immune System (AIS) with no need for prior knowledge of Botnets [40].

Ismaila (2012) proposed a spam detection model based on negative selection algorithm that generates a new self (system) that randomly creates antibody against spam, by distinguishing self from non-self. The experimental result guarantees that the proposed model is able to establish a better true positive on an unknown spam [41].

Smera et al (2014) studied and compared two efficient spam filters namely Bayesian filters and Artificial Immunity filters and suggested Bayesian classifier has as an effective method to construct anti-spam filters [42].

Ibor et al (2015) proposed a highly efficient hybrid technique which is achieved using the combined features of three algorithms namely J48, Boyer Moore and K-NN for Malicious Network Traffic based on Active Response [43].

5.4 Application of genetic algorithm and fuzzy against cyber crimes

Liu et al (2010) to detect computer virus, the clustering method combining genetic algorithm and ant colony algorithm is adopted. From experimental results, it is clear that this method exhibits strong adaptability, shows better intelligence, and higher degree of automation in detecting virus [44].

Linda et al (2011) proposed a novel fuzzy based learning

algorithm for anomaly based network security cyber sensor together with its hardware implementation. The anomaly detection algorithm was specifically designed to allow for both fast learning and fast classification of attacks [45].

Hoque et al (2012) presented an Intrusion Detection System (IDS), by applying Genetic Algorithm (GA) to efficiently detect various types of network intrusions using the standard KDD99 benchmark dataset [46].

Ojugo et al (2012) presented a genetic algorithm based approach with its driver implementation. It employs a set of classification rule derived from network audit data [47].

Jitendra (2013) presented a genetic algorithm to detect email spam and the proposed idea is tested on 2248 mails and the overall efficiency is nearly 82% [48].

Jongsuebsuk et al (2013) depicted a network IDS based on a fuzzy genetic algorithm. Fuzzy rules are used to classify network attack data, whereas genetic algorithm optimizes the solution. The evaluation results showed that the proposed IDS can detect network attacks in real-time and within 2-3 seconds upon the arrival of data with the detection rate of over 97.5% [49].

Roshna et al (2013) presented a technique named as botnet detection using Adaptive Neuro Fuzzy Inference System (ANFIS) based on Anfis algorithm [50].

AI flexible features for IDPSs

AI techniques have numerous traits that make it suitable for the construction of the intrusion detection and prevention system (see Table 1)

Table 1: AI features for IDPS

Technology	Features
Artificial NeuralNetworks	i.Learning by example. ii. Resilience to noise and incomplete data. ii. Intuitiveness since it mimic biological neuron.
Intelligent Agents	i. Mobility. ii. Adaptability. ii. Collaboration.
Artificial Immune Systems	i. Self-adaptability. ii. self-organizing. ii. Dynamic nature.
Genetic Algorithms and fuzzy	i. Optimization. ii. Robustness. iii. Flexible.

Limitations of Existing Anomaly Detection and Prevention System

Today IDPS have become extremely valuable in enhancing the security of the networks and end hosts; they however have numerous key drawbacks [51]. They are:

- Encryption: Once the data packets are encrypted, the existing detection mechanisms may become completely futile in identifying the intrusions.
- Evasion of signatures: polymorphic worms which can automatically change their propagation characteristics thereby changing their signatures. Such worms also constitute a critical threat to the current detection system.
- False Positives: A false positive is an incident when a IDS falsely raises a security threat alarm for harmless traffic.
- Legal regulations: intrusion detection systems need to conform to legal regulations
- Attack to IDPS: may be disabled by attackers if they can learn how the system works.

Conclusion

As we are living in an online world, most of our everyday communications and commercial activities now take place via the Internet. However, it also caused issues that are difficult to manage such as the emergence of cyber crimes. Available academic resources show that AI techniques already have numerous applications in combating cyber crimes. This paper has briefly presented possibilities of AI techniques so far in cyber field for combating cyber crimes and their current limitations.

References

[1] Selma Dilek, Hüseyin Çakır and Mustafa Aydın, ”Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review”, International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, January 2015
[2] Manveer Kaur, Sheveta Vashisht, Kumar Saurabhi, “Adaptive Algorithm for Cyber Crime Detection”, International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 3 (3), 4381 – 4384, 2012
[3] Jheel Somaiya, Dhaval Sanghavi, Chetashri Bhadane, ”A Survey: Web based Cyber Crimes and Prevention Techniques”, International Journal of Computer Applications (0975 – 8887), Volume 105, November 2014
[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, ”Latest Face of Cybercrime and Its Prevention In India”, International Journal of Basic and Applied Sciences, Vol. 2, Pp. 150-156, 2013
[6] Advocate, Vivek Tripathi,” Internet Crime”, www.cyberlawsindia.net, Available: http://www.cyberlawsindia.net/internet-crime.html
[7] V. Rajaraman, ”JohnMcCarthy – Father of Artificial Intelligence”, in General Article Resonance, March 2014
[8] T N Shankar, Neural Networks, LAXMI Publications Pvt.Ltd, 2008

[9] J. S. Russell, P. Norvig, Artificial Intelligence: A Modern Approach, Upper Saddle River, Prentice Hall, New Jersey, USA, 2003
[10] G. Luger, W. Stubblefield, Artificial Intelligence: Structures and Strategies for Complex Problem Solving, Addison Wesley, 2004.
[11] Wikipedia, "Artificial Intelligence", en.wikipedia.org, Available: http://en.wikipedia.org/wiki/Artificial_intelligence
[12] Jacques Ferber, Multi-Agent System: An Introduction to Distributed Artificial Intelligence, Harlow: Addison Wesley Longman, 1999
[13] UKCI, "Workshop on Computational Intelligence", ukci.cs.manchester.ac.uk, Avaliable: http://ukci.cs.manchester.ac.uk/intro.html
[14] N. A. Alrajeh and J. Lloret," 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, Vo. 26, pp. 2105–2127.
[16] Wikipedia, "Intrusion detection system", en.wikipedia.org, Available: http://en.wikipedia.org/wiki/Intrusion_detection_system
[17] Gang Wang, Jinxing Hao, Jian Ma, and Lihua Huang, "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering", Elsevier Ltd 2010
[18] E. Tyugu, "Artificial intelligence in cyber defense", In Proceedings of the 3rd International Congress on Cyber Conflict (ICCC), pp. 1–11,2011.
[19] X. B. Wang, G. Y. Yang, Y. C. Li and D. Liu, "Review on the application of Artificial Intelligence in Antivirus Detection System", In Proceedings of the IEEE Congress on Cybernetics and Intelligent Systems, pp. 506- 509,2008
[20] M Rajesh Kanna, D. Hemapriya and C. Divya," 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, "Intelligent Intrusion Detection System Framework Using Mobile Agents", International Journal of Network Security & Its Applications (IJNSA), Vol 1, July 2009
[21] Yu Chen, "NeuroNet: Towards an Intelligent Internet Infrastructure", In Proceedings of the 5th IEEE Congress on Consumer Communications and Networking Conference (CCNC), pp. 543 547,2008
[22] Iftikhar Ahmad, Azween B Abdullah, and Abdullah S Alghamdi, "Application of Artificial Neural Network in Detection of Probing Attacks", In Proceedings of the IEEE Symposium on Industrial Electronics and Applications (ISIEA), 2009
[23] Ondrej Linda, Todd Vollmer and Milos Manic, "Neural Network Based Intrusion Detection System for Critical Infrastructures", In Proceedings of the International Joint Congress on Neural Networks, 2009
[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, "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, "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, "HTTP Botnet Detection Using Adaptive Learning Rate Multilayer Feed-Forward Neural Network", International Federation for Information Processing 2012
[30] Devikrishna K S and Ramakrishna B B, "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, Jul-Aug 2013
[31] ZhaiShuang-can, Hu Chen-jun and Zhang Wei-ming, "Multi-Agent Distributed Intrusion Detection System Model Based on BP Neural Network", International Journal of Security and Its Applications Vol.8, pp.183-192, 2014.
[32] N. C. Rowe, "Counterplanning Deceptions To Foil Cyber-Attack Plans", In Proceedings of the 2003
[33] IEEE Workshop on Information Assurance, pp. 203 210
[34] José Helan and Matos Nogueira, "Mobile Intelligent Agents to Fight Cyber Intrusions", International Journal of Forensic Computer Science , IJoFCS, pp 28-32,2006
[35] Mueen Uddin, Kamran Khowaja and Azizah Abdul Rehman, "Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents", International Journal of Network Security & Its Applications (IJNSA), Vol.2, October 2010
[36] Mayank Aggarwal, Nupur and Pallavi Murgai, "Simulation of Dynamic Mobile Agent Model to Prevent Denial of Service Attack using CPNS", International Journal of Computer Applications Volume 20, April 2011
[37] Ugur Akyazi , and A. Sima Uyar, "Distributed Detection of DDOS Attacks During the Intermediate Phase Through Mobile Agents", Computing and Informatics, Vol. 31, 759–778, 2012
[38] Onashoga, S. Adebukola, Ajayi, O. Bamidele and Akinwale, A. Taofik, "A Simulated Multiagent-Based Architecture for Intrusion Detection System", International Journal of Advanced Research in Artificial Intelligence (IJARAI), Vol. 2, 2013
[39] Y. Zhang, L. Wang, W. Sun, R. C. Green II, M. Alam, "Artificial Immune System based Intrusion Detection in A Distributed Hierarchical Network Architecture of

Smart Grid", IEEE Power and Energy Society General Meeting, pp. 1 – 8, 2011
[40] Amit Kumar Tyagi and Sadique Nayeem, "Detecting HTTP Botnet using Artificial Immune System (AIS)", International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 , Volume 2, May 2012
[41] Ismaila Idris," 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 , "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, "A Hybrid Mitigation Technique for Malicious Network Traffic based on Active Response", International Journal of Security and Its Applications Vol. 9, pp. 63-80, 2015
[44] Liu Guozhu and Shang Yanjun, "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", 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, "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, "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, "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," In Proceedings of the 10th International Congress on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), pp. 1-6, 2013
[50] Roshna R.S and Vinodh Ewards, "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

Author Profile

Jyothsna S Mohan received her B. Tech Degree in Computer Science and Engineering in 2009 from Cochin University of Science and Technology (CUSAT), and her M. Tech in Computer Science and Engineering in 2012 from SRM University, Chennai. She worked as a Lecturer in Computer Science in M.E.S, Arts and Science College, Villiappally. Now she is working as an assistant professor in Computer Science and Engineering, at College of Engineering Vadakara, Kozhikode, Kerala.

Nilina T received her B. Tech Degree in Computer Science and Engineering in 2009 from Cochin University of Science and Technology (CUSAT), and her M. Tech in Computer Science and Engineering in 2012 from SRM University, Chennai. She worked as an assistant professor in Computer Science and Engineering in College of Engineering, Vadakara, College of Engineering Thalassery. Now she is working as an assistant professor in Computer Science and Engineering, at Govt. College of Engineering Kannur.

.