ISSN: 2230-9926

Available online at http://www.journalijdr.com

IJDR

International Journal of Development Research
Vol. 07, Issue, 11, pp.16866-16872, November, 2017

ORIGINAL RESEARCH ARTICLE

Open Access

A SURVEY OF ARTIFICIAL INTELLIGENCE FOR ENHANCING THE INFORMATION SECURITY

***[1]Roumen Trifonov, [1]Georgi Tsochev, [1]Slavcho Manolov, [2]Radoslav Yoshinov and [1]Galya Pavlova**

[1]Faculty of Computer Systems and Technology, Technical University, Sofia 1000, Bulgaria
[2]Laboratory of Telematics at the Bulgarian Academy of Sciences, Sofia 1000, Bulgaria

ARTICLE INFO

Article History:
Received 16th August 2017
Received in revised form
08th September, 2017
Accepted 17th October, 2017
Published online 29th November, 2017

Key Words:
Intrusion detection/prevention systems,
Artificial intelligence,
Computer networks,
Information security,
Intelligent security.

****Corresponding author***

ABSTRACT

The analysis of the latest trends of threats to different types of attacks adequately reflects the radical changes over the last three or four years in the landscape of cyber-threat protection. The conventional network protection tools such as penetration detection and anti-virus focusing on the risk vulnerability component and traditional incident response methodology have become inadequate for certain players due to the evolution of the goals and complexity of the entry of computer networks. Therefore, the fight against them can happen with intelligent semi-autonomous or wholly autonomous agents that can detect, evaluate, and respond with the appropriate protection action. These intelligent methods will need to be able to manage the entire process in response to an attack. It is based on artificial intelligence and the use of its methods to protect from cybercrimes. The aim of this study is to present and compare different methods of artificial intelligence for fighting the crime in cyberspace, or rather their application in systems for detecting and preventing intrusions.

Citation: Roumen Trifonov, Georgi Tsochev, Slavcho Manolov, Radoslav Yoshinov and Galya Pavlova, 2017. "A survey of artificial intelligence for enhancing the information security", *International Journal of Development Research*, 7, (11), 16866-16872.

INTRODUCTION

It is very important for an organization is to develop mechanisms to secure to prevent unauthorized access to system resources and confidential company and government data (Roumen Trifonov, 2006). There are many ways to protect the network infrastructure of an enterprise, including also systems for detecting and preventing intrusions. Over the past two decades, the development of computer networks is scope for innovative improvements. The market has many varieties of type "Next Generation", which provide a relatively good set of tools (systems) interaction and prevention of network attacks. Physical devices such as sensors and detectors are not sufficient for monitoring, analysis and protection of the network infrastructure. It takes more complex information technology that can model proper behavior and identify abnormal. These systems cyber security need to be flexible, adaptable and clear, but at the same time able to discover the wide variety of threats and make smart choices. With the pace of cyber-attacks, the human factor is not sufficient for timely analysis and action under attack.

Human resources and lack of expertise were the main weakness of the organizations. The fact is that the intelligent agents carry out most network attacks, such as computer viruses and worms (Fig. 1). So fighting them can become smart semi-autonomous or fully autonomous agents that can detect, evaluate and respond with appropriate action for protection. These intelligent methods will need to be able to manage the whole process in response to an attack, i.e. to analyze and determine what type of attack happens, what is intended and what is the appropriate countermeasures, and not least how to prioritize and secondary prevention of attacks. It was in those difficult situations we need innovative approaches by applying methods of artificial intelligence. The aim of this study is to present and compare different methods of artificial intelligence for fighting the crime in cyberspace, or rather their application in systems for detecting and preventing intrusions.

Artificial Intelligence

As stated above, to provide a flexible and secure software that help people in fighting computer crime is necessary to use innovative technologies from artificial intelligence. In recent

years, artificial intelligence (AI) has become a tempting area for researchers. AI used to be breathed intelligence of a machine. The studies are highly technical and specialized; often fail to communicate with each other. Field of AI is based on the assertion that the intelligence of people (potential (innate) ability of a conscious individual to draw conclusions (deductions) on an information) can be described so precisely that a machine can simulate it. After several decades of research, AI is not only the subject of research or planning some movement, but also more complex depth and interrelated decisions.

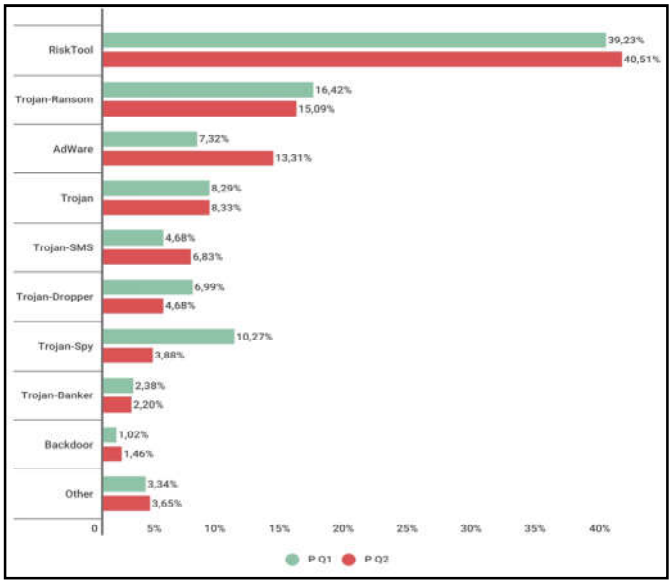

Figure 1. Threats during Q1 and Q2 in 2017

AI offers many opportunities, most of which are inspired by nature computational methods - intelligent agents, neurons networks, data mining, artificial immune systems, machine learning, pattern recognition, fuzzy logic, heuristic and others.

Applications in the field of AI are widely accepted by modern information society. This interdisciplinary initiative has created a joint connection between computer scientists and network engineers in the design, simulation and development of models for network penetration and their characteristics.

Intrusion Detection/Prevention System

Intrusion Detection/Prevention System (abbreviated as IDPS) is a security system that detects hostile activity on the network and tries to prevent it. The key is then to detect and possibly prevent actions that could jeopardize the security of the system, or attempt to break in the work, including the phases of exploration / collection of data that include, for example, a port scan (Fig. 2). One of the key features of intrusion detection/prevention systems is their ability to provide a view of the unusual activity and issue alarms notifies administrators and / or block the connection of the suspect (Kazienko and P. Dorosz, 2003). The classification of the typical IDPS systems is divided into three large groups (Host- vs, 2016) is given in Table 1.

Table 1. Intrusion Detection/Prevention Types

Name	Functionality
Host Based Intrusion Detection/Prevention System	collecting information about activity on a particular single system or host
Network Based Intrusion Detection/Prevention System	perform analysis of all traffic passing through a network segment or subnet
Application Based Intrusion Detection/Prevention System	focuses its monitoring and analysis on a specific application protocol or protocols in use by the computing system

IDPS consist of four major elements (Fig. 3) – data collection, feature selections, analysis and action. The data collection is a file in which is recorded the data that should be analyzed. In rule based IDPS the analysis is done by checking the data of compare it to a signature or pattern. Another method is anomaly based.

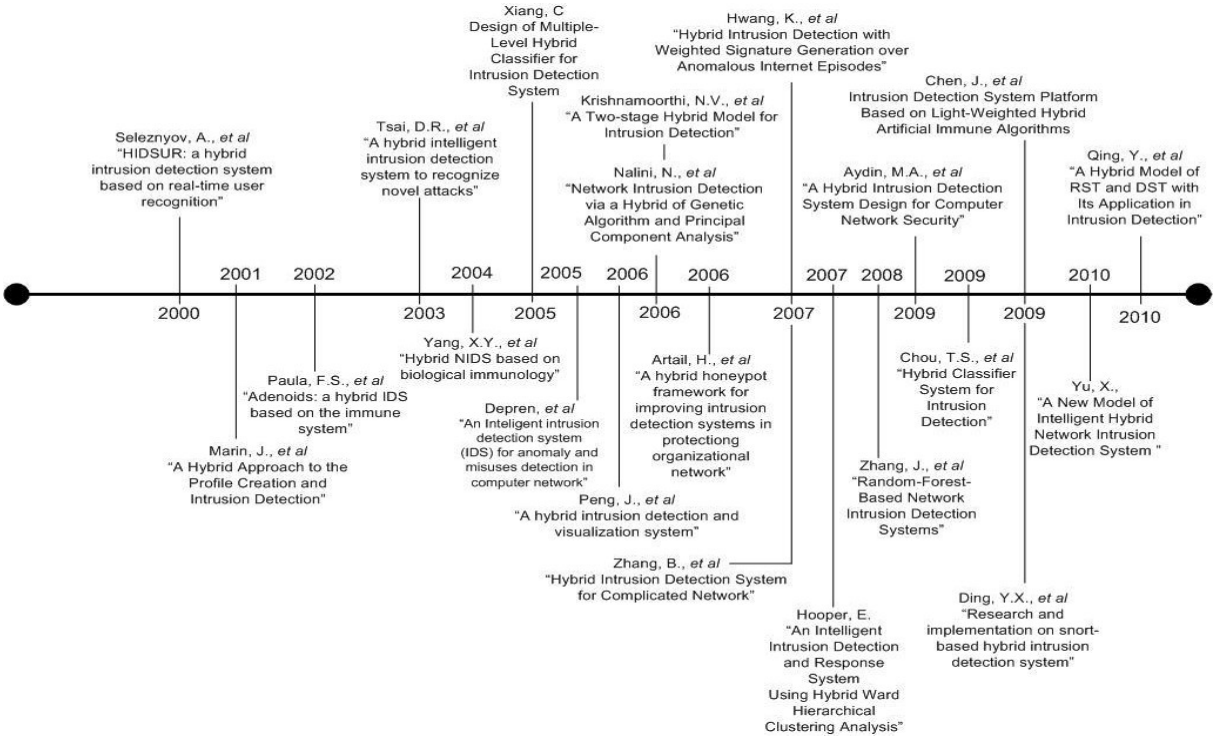

Figure 2. Roadmap intrusion early detection / prevention (Stiawan et al., 2011)

The action defines the attack and reaction of the system (Scarfone and Mell, 2007). Usually the information flow in IDPS starts with the row packet capture this involves not only capturing packets, but also passing the data to the next component of the system.

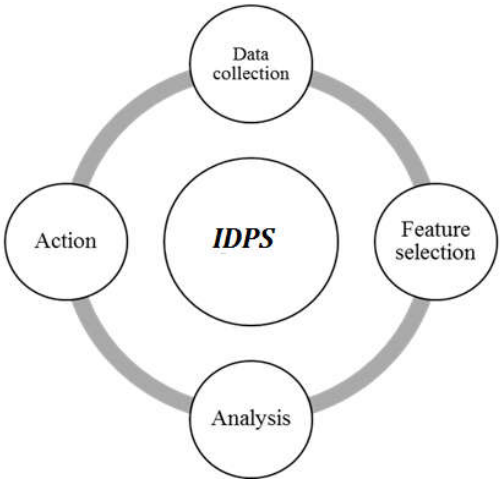

Figure 3. Functionality of IDPS

Filtering means limiting the packets that are captured according to a certain logic based on characteristics, such as type of packet, IP source address range, and others. Subsequently sending the packets to a series of decoder routines that define the packet structure for the layer two data that are collected through promiscuous monitoring. Once each packet is decoded, it is often stored either by saving its data to a file or by assimilating it into a data structure while, at the same time, the data are cleared from memory. Decoding "makes sense" out of packets, but this, in and of itself, does not solve all the problems that need to be solved for an IDPS to process the packets properly. Stream reassembly means taking the data from each TCP stream and, if necessary, reordering it (Kumar and Dhawan, 2012).

The typical components in an IDPS are sensor or agent, management server, database server and console (Scarfone, 2007). The role of the artificial intelligence is the development of the sensors or agents. Typically using the term sensor is for IDPSs that monitor networks, including network-based, wireless, and network behavior analysis technologies. In host-based IDPS technologies, the term agent is used. Some IDPS sensors have a learning or simulation mode that suppresses all prevention actions and instead indicates when a prevention action would have been performed (Scarfone, 2007). Artificial intelligence easily solve the problem of human factor. The primary difficulty of the IDPS is how accurately the system can in terms of whether non-hostile activity is flagged; false positive and whether malicious activity will be missed; false negative. Large volume of alerts is unmanageable and overwhelming to the human analyst. Inspecting thousands of alerts per day is unfeasible, especially if 99% of them are false alerts. Many approaches have been suggested, but artificial intelligence comes natural to solve this problem – machine learning, data mining etc.

Using artificial intelligence to protect against cybercrime

An intelligent, adaptive and cost-effective tool that is capable of detecting and preventing intrusions in real time is the purpose companies that deal with cybercrime.

Various methods in the field of AI has been used to automate the process of detecting intrusions while reducing human factor.

Artificial Neural networks (ANN)

An Artificial Neural Network is an information processing system that is inspired by the way biological nervous systems. Neural networks are models built from multiple processing elements (neurons), each of which perform simple numerical operations and share results with their neighbors through weighted connections. Most of the intrusion detection systems based on the ANN are using two kinds of neural networks: multilayered feedforward neural networks and Kohonen's self-organizing maps (Vesely, 2004).

ALAN BIVENS et all (BIVENS, 2012), developed a system that uses use self-organizing maps, as they have been shown to be effective in novelty detection, automated clustering and visual organization. Their system is modular based network IDS that analyses the tcpdump traffic and develop windowed traffic intensity trends. The learning process uses architectural learning period.

Dilip Kumar Barman and Guruprasad Khataniar (Barman, 2012) (Figure 4) used Artificial Neural Network (ANN) with back propagation as IDPS. The ANN based IDPS system will use the attributes (total of 41) of the intrusion signatures of the dataset KDD99.

Min-Joo Kang and Je-Won Kang proposed a novel IDS using a deep neural network (DNN) is proposed to enhance the security of in-vehicular network (Kang, 2016).

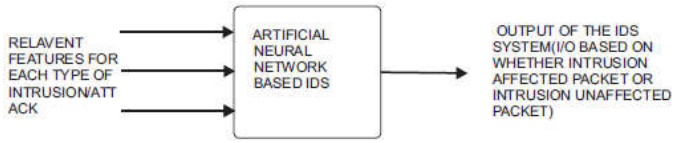

Figure 4. Application of ANN for detection of intrusion for a class of intrusion (Bivens et al., 2002)

Mehdi MORADI and Mohammad ZULKERNINE (MORADI, 2004), present A Multi-Layer Perceptron (MLP) is used for intrusion detection based on an off-line analysis approach. Their research aims to solve a multi class problem in which by the neural network the type of detected attack.

Artificial Immune Systems

The Artificial Immune Systems (AIS) were inspired by the Human Immune System that is robust, decentralized, error tolerant, and adaptive (Aziz, 2012). The HIS is made of molecules, cells, and tissues that establish human body's resistance to infections caused by viruses and etc. The AIS can distinguish and eliminate the different pathogens from self-cells. This provides a great source of inspiration for the security of computer systems, especially IDS.

The first who began researches in this field are Farmer, Packard, and Perelson. Their algorithm describes a method for change detection that is based on the generation of T-cells in the immune system. In 1994 Forrest and her group at the University of New Mexico began research to build an IDS based on AIS.

They proposed a negative selection algorithm to utilize the process of the HIS for a sophisticated anomaly-detection process (Forrest, 1997). Liu et al. propose method of intrusion detection for the IoT that simulates self and non-self-antigen. The Immature detector, mature detector and the memory detector evolve dynamically to prevent intrusion. Their algorithm provides a new way in the in the intrusion detection in IoT environment (Liu, 2011). Dutt et al. propose a methodology which results show the efficiency of the model for detecting intrusion after inducing malicious attacks on the host - based system (Dutt, 2016).

Machine Learning

Machine learning methodologies are being widely used by the researchers in the field of network intrusion detection due to their generalization capabilities that helps to understand the technical knowledge about the intrusions that do not have any predefined patterns (Panda, 2011). There are two types of machine learning techniques - single classifier and hybrid classifier. Juma et. al. (JUMA, 2015), are very well described the machine learning techniques in their paper. They say that the future of machine learning in intrusion detection prevention systems, are only beginning to develop and can be expected many more future scientific developments.

Fuzzy logic and fuzzy sets

Fuzzy set theory was introduced by Zadeh (RAJASEKARAN, 2003), for handling uncertainty. Fuzzy logic is a rule-based system that can rely on the practical experience of an operator, particularly useful to capture experienced operator knowledge (http://www.controleng.com/single-article/artificial-intelligence-fuzzy-logic-explained/8f3478c13384a2771ddb7e93 a2b6243d.html) The approach of FL imitates the way of decision making in humans that involves all intermediate possibilities ranges in degree between 0 and 1. Jongsuebsuk et al. (Jongsuebsuk, 2013), proposed a network IDS based on a fuzzy genetic algorithm. Fussy rules are used to classify network attack data, while a genetic algorithm is an optimization algorithm that can help finding appropriate fuzzy rule and give the best/optimal solution. Chimphlee et al. proposed the Fuzzy Rough C-means (FRCM) to clustering analysis (Li, 2004). The results they achieve with the performance are very good compared to the Kmeans methods.

Genetic Algorithms

Genetic Algorithms incorporate the concept of Darwin's theory. They were inspired by the biological evolution (development), natural selection, and genetic recombination (Aziz, 2012). Genetic algorithms can be used to evolve simple rules for network traffic. GA generates a set of rules, that later can be used to distinguish the normal and abnormal network traffic. The algorithms to create these data sets uses a chromosome-like data structure and evolve the chromosomes using selection, recombination and mutation operators. Li (Li,, 2004), proposed an IDS with 57 genes in chromosomes, where each gene represents single connection feature, like: source IP address, destination IP address, source port, destination port, duration, protocol, number of bytes sent by originator, number of bytes sent by responder, etc. Due to the effectiveness of the evaluation function, the succeeding populations are biased toward rules that match intrusive connection. Anup Goyal And Chetan Kumar (Forrest, 1997) suggested systematic learning method known as Genetic Algorithm (GA), to identify illegitimate nodes. The algorithm considers the varied features in network connectivity like protocol type, network service to destination and connection status to generate a type based rules. Ojugo, et. al. have used genetic algorithms to develop rule-based intrusion detection. their study, the genetic algorithm based approach, which uses a set of classification rules derived from the data network audit and support confidence framework to be used as a fitness function, to evaluate the quality of each rule. Implementation of the software aims to improve system security in the network settings to allow the confidentiality, integrity and availability of system resources (Ojugo, 2012). Immannavar et al. proposed A GNP based fuzzy membership for identifying threats, attacks or intrusions over the Internet (Immannavar,, 2015). There methods handle both discrete and continuous attributes and it can be flexibly applied to any kind of attacks.

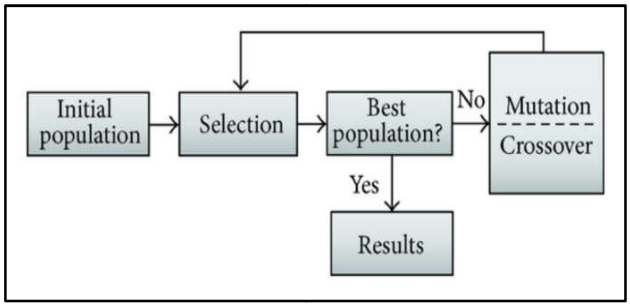

Figure 5. General architecture of genetic algorithm (Alrajeh et al., 2013)

Intelligent agents

Agents can be defined to be autonomous, problem-solving computational entities capable of effective operation in dynamic and open environments (Luck, 2003). Agents are often deployed in environments in which they interact, and may be cooperate, with other agents (including both people and software) that have possibly conflicting aims.

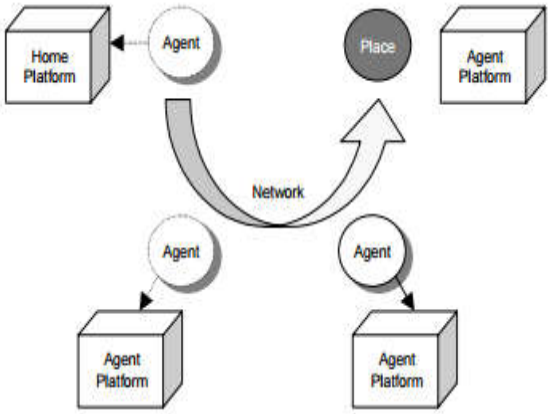

Figure 6. Model of Intelligent agent system

Ganpathy et al. in 2012 proposed a method that combines an intelligent agent-based weighted distance outlier detection (IAWDBOD) algorithm and intelligent agent-based enhanced multiclass support vector Machine (IAEMSVM) algorithm. The result for DoS, Probe, and other attacks are 99.77%, 99.70%, and 79.72%, respectively, when intelligent agents are added to the classifier.

The main advantage of this method is that it reduces the false positive rates (Ganapathy, 2012). Jain et al. in their article make detailed comparative analysis of different mobile agent based IDS (Jain, 2016).

Each record consists of 41 different attributes that describe the different characteristics of the link, categorized as follows: basic TCP features, content features, time-based traffic characteristics, and host-based functions.

Table 2. Advantages and disadvantages of the different AI methods used for IDPS

Technology	Advantages	Disadvantages
Artificial Neural Networks	learn by example or training, flexibility; multiple class classification; Parallel nature; able to work imprecise and incomplete data; speed; ability to "learn" the characteristics of misuse attacks and identify instances that are unlike any which have been observed before by the network (Devikrishna et al., 2013)	Indication of intrusions completely dependents on the training of the system and the the training data; training routine requires a large number of data to ensure that the results are statistically accurate.
Artificial Immune Systems	Decentralized; error tolerant; adaptive; highly efficient and versatile robustness distribution lightweight self-organizing, and self-adapting	Work well on small problems with medium sized testbeds; Hard implementation for distinguishing self from non-self pathogens
Machine learning	High Accuracy Able to model complex and nonlinear decision boundaries.	Difficulties with evaluation; Outlier detection
Fuzzy Logic/Sets	Reasoning is Approximate rather than precise; Effective (port scans and probes) Reconciles conflicting objectives fuzzy sets easily modified	High consumption of resources; Difficulty in relevant rule subset identification;
Genetic Algorithms	deriving best classification rules; Selecting optimal parameters solves the problems with multiple solutions intrinsic parallelism; highly re-trainable evolve over time by using crossover and mutation (Majeed, 2014)	Over-fitting; Complex representing of the problem; Complex configuration of the system; Converge premature to a solution;
Intelligent Agents	Mobility Adaptability Collaboration Autonomy agents are independently-running entities Inferential capability Pro-activeness: agents can take the initiative to act and response to their environment low cost and time saving approach Reducing Network Load Platform Independence (https://www7.informatik.tu-muenchen.de/um/courses/ seminar/ worm/WS0405/albag.pdf.)	The scalability is limited because the analysis is performed in one single. Hard to maintenance and control overhead; Tool are new and have unknown security bugs and vulnerabilities; Agents ability to travel introduces fault-tolerant properties (Karygiannis)
Expert Systems	automating some audit procedures automating some audit procedures knowledge base can be updated and extended contain a large amount of information	audit trail are translated in terms of if-then-else rules not able to learn from the mistakes cannot creatively come with new solutions for the issues not easily achievable to mimic the exact knowledge of an Expert(human)
Datasets	knowledge base can be updated and extended contain a large amount of information simplicity	Updating Adaptability Difficulty in relevant rule subset identification
Naïve Bayes	return not only the prediction but also the degree of certainty simplicity independence assumption	Problems with imbalanced Problems with data scarcity

Datasets

The Cyber Systems and Technology Group (DARPA Intrusion Detection Evaluation Group) of the MIT Lincoln Laboratory, under the sponsorship of the Defense Advanced Research Projects Agency (DARPA ITO) and the Air Force Research Laboratory (AFRL / SNHS), has collected, developed and disseminated the first standard evaluation of computer networks IDSes (http://www.ll.mit.edu/mission/ communications/cyber/CSTcorpora/ideval/data/). This happened in 1998 and 1999, resulting in the first data sets DARPA 1998 and DARPA 1999, with DARPA 1998 being more popular. KDD Cup is the annual Data Mining and Discovery Knowledge competition organized by the ACM Special Interest Group. The task of the competition is to develop a classifier capable of distinguishing between legitimate and illegal interactions in computer networks [35]. For this purpose, a DARPA 1998 [36] dataset was used during the race and subsequently became a common name under the name KDD'99. Both DARPA and KDD data sets consist of nearly 5 million learning paths (ie events) labeled "penetration" or "no penetration" and a separate set of data - tests consisting of visible and invisible attacks.

All forms of attack fall into one of the three categories: Remote-to-Local (R2L), User-to-Root (U2R), Denial of Service (DOS) or Drilling (Lee, 1999). As already mentioned, KDD'99 is based on DARPA 1998, which itself is strongly criticized by McHugh (McHugh, 2000), largely due to the fact that it has the characteristics of synthetic data. As a result, some of the existing problems in DARPA 1998 remain in KDD'99. One of the most important flaws in the two sets of data is the huge number of abbreviated records, so learning algorithms are made as frequent recordings, and thus prevent them from learning themselves (they are usually more harmful to networks like U2R and R2L). Since there are currently only a few public datasets, such as DARPA 1998 and KDD'99, many of the experimental work of scientists is based on non-public or proprietary datasets. According to many scientists, and according to Tsai's report (Tsai, 2009), it can easily be concluded that these two sets of data are recognized as a de facto standard in the field of penetration detection.

Expert systems

The Expert System (ES) is a computer program that contains knowledge and makes a logical conclusion about a specialized subject area for the purpose of solving certain tasks or giving

appropriate advice. The creator (developer) of the expert system must have a model to follow when seeking a solution. The model shows the properties and behavior of the system. It is important that it be simple and include only the most important features of the process. Although the analysis of the security of the expert systems is an audit problem, it is treated in isolation as it involves a wide range of problems. As noted below, there are very few specific studies in the field of security in expert systems. Here are the unique aspects of expert systems compared to other types of computer systems. The unique properties of ES have a direct impact on the security of these systems. Some controls can be used for all types of ES and all types of ES "shell" software. There are very few and limited ES security studies. Overall, the closest discussion is about EDP systems. Because expert systems are practically computer programs, they require the same security measures as other computer programs. Many of the concerns about security in traditional computer programs can be found in other sources (such as Halper *et al* [1985] and Weber [1988]) and are therefore beyond the scope of the subject. However, expert systems differ in many ways from other more traditional computer systems. These differences require investigation of additional security concerns. The approach here is to show some of the unique properties and control that can mitigate the risks. Stefan Axelsson's study (Axelsson, 1999), describes several types of expert systems in the field of intrusion detection and prevention systems. The overview gives a good idea of the novelties and trends in this area.

Naive Bayes

Naive Bayes is a simple technique for constructing classifiers: models that assign class labels to problem instances, represented as vectors of feature values, where the class labels are drawn from some finite set. It is not a single algorithm for training such classifiers, but a family of algorithms based on a common principle: all naive Bayes classifiers assume that the value of a particular feature is independent of the value of any other feature, given the class variable. Mr. Panda and M. Patra (Panda, 2007), suggest a framework of NIDS based on Naïve Bayes algorithm that builds patterns of network services over data sets labelled by the services. Compared to other methods of AI it has higher detection rate, less time consuming and low cost factor. S. Mukharjee and N. Sharma (Mukherjee, 2012). propose another approach in their investigation. They use Naïve Bayes with feature reduction. The results are very promising and the model has high accuracy.

Comparison of the different AI methods

AI have many advantages such as – precision and accuracy, fraud detection, lacking the emotional side, robots think logically, function without stopping (do not require sleep or breaks), the costs are minimized and controlled and etc. Of course, like any fast growing technology there are some problems – cannot act any different from what they are programmed to do, machines lack of common sense, eventually will replace humans in every field and will lead to unemployment, fear of robots superseding humans etc. Several algorithms for intrusion detection and prevention based on various methods were reviewed and the advantages and disadvantages of these algorithms are shown in Table 2.

Conclusion

AI gives us the opportunity to develop autonomous computing solutions that adapt to their context of use, using the methods of self-control, self-tuning and self-configuration, self-diagnostics and self-healing. When it comes to the future of information security, AI looks very promising area of research that focuses on improving the security of cyberspace. This article looks at some of the areas of AI, which have undergone significant changes over the last decade. It shows the progress that scientists have made in the fight against cybercrime. This area is fast growing and requires in-depth research, as there are many promising results that may be obtained from these algorithms, especially in their combined use.

Acknowledgement

This research is conducted and funded in relation to the execution of a scientific-research project № H07/56 “Increasing the level of network and information security using intelligent methods” of the Technical University of Sofia under the contract № D07-4/15.12.2016 with National Science Fund in Bulgaria.

REFERENCES

“DARPA Intrusion Detection Data Sets webpage on The MIT Lincoln Laboratory website.,” DARPA , 2014. [Online]. Available: http://www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/data/.

“Host- vs. 2016. Network-Based Intrusion Detection Systems,” SANS Institute 2000 – 2005.

Albag, H. “Network & Agent Based Intrusion Detection Systems,” [Online]. Available: https://www7.informatik.tu-muenchen.de/um/courses/seminar/worm/WS0405/albag.pdf.

Alrajeh, N. and Lloret, J. 2013. “Intrusion Detection Systems Based on Artificial Intelligence Techniques in Wireless Sensor Networks,” *International Journal of Distributed Sensor Networks,* 2013.

Axelsson, S. 1999. Research in Intrusion-Detection Systems: A Servey, Göteborg.

Aziz, A. S. A., Salama, M. and Hassanien, A. E. 2012. “Detectors Generation using Genetic Algorithm for a Negative Selection Inspired Anomaly Network Intrusion Detection System,” in Federated Conference on Computer Science and Information Systems, WROCŁAW.

Barman, D. K. and Khataniar, G. 2012. “Design of intrusion detection system based on artificial neural network and application of rough set,” *International Journal of Computer Science & Communication Networks*, vol. 2, no. 4, pp. 549-552.

Bivens, A., Palagiri, C., Smith, R., Szymanski, B. and M. Embrechts, 2002. “Network-Based Intrusion detection using neural,” in Intelligent Engineering Systems through Artificial Neural Networks ANNIE-2002, St. Louis.

Chimphlee, W. Abdullah, A. H. and Sap, M. N. M. 2006. “Anomaly-Based Intrusion Detection using Fuzzy Rough Clustering,” International Conference on Hybrid Information Technology.

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),* vol. 3, no. 4, pp. 1959-1964.

Dingle, N. “Artificial Intelligence: Fuzzy Logic Explained,” [Online]. Available: http://www.controleng.com/single-article/artificial-intelligence-fuzzy-logic-explained/8f3478c13384a2771ddb7e93a2b6243d.html.

Dutt, I., Borah, S. and Maitra, I. 2016. "Intrusion Detection System using Artificial Immune System," International Journal of Computer Applications, vol. 144, no. 12, pp. 19-22.

Forrest, S., S. A. Hofmeyr and A. Somayaji, "Computer Immunology," Commun. ACM, vol. 40, no. 10, p. 88–96, 1997.

Ganapathy, S., Yogesh, P. and Kannan, A. 2012."Intelligent Agent-Based Intrusion Detection System Using Enhanced Multiclass SVM," Computational Intelligence and Neuroscience, 2012.

Goyal, A. and Kumar, C. 2007. "GA-NIDS: A Genetic Algorithm based Network Intrusion Detection System,".

Immannavar, M. Pujar, P. M. and Suryavanshi, M. 2015. "AN Intrusion detection model based on fuzzy membership function using gnp," International Journal of Research in Engineering and Technology, vol. 4, no. 8, pp. 27-32, 2015.

Jain, C. and Saxena, A. K. 2016. "General Study of Mobile Agent Based Intrusion Detection System (IDS)," *Journal of Computer and Communications*, vol. 4, pp. 93-98.

Jongsuebsuk, P., Wattanapongsakorn, N. and Charnsripinyo, C. 2013. "Real-time intrusion detection with fuzzy genetic algorithm," 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology.

Juma, S., Muda, Z., Mohamed, M. A. and Yassin, W. 2015. "Machine learning techniques for intrusion DETECTION system: A REVIEW," *Journal of Theoretical and Applied Information Technology*, vol. 72, no. 3, pp. 422-429, 2015.

KDD CUP 1999, "Computer network intrusion detection webpage on SIGKDD website," 199. [Online]. Available: http://www.sigkdd.org/kdd-cup-1999-computer-network-intrusion-detection.

Kang, M.-J. and Kang, J.-W. 2016. "Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security," PLOS one, 7 Jun [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4896428/.

Karygiannis, T. "Network Security Testing Using Mobile Agents," National Institute of Standards and Technology, Gaithersburg,.

Kayacik, H. G. and N. Z. Heywood, 2005. "Analysis of three intrusion detection system benchmark datasets using machine learning algorithms," Proc. Intelligence and Security Informatics, pp. 362-367.

Kazienko, P. and Dorosz, P. 2003. "Intrusion Detection Systems (IDS) Part I - (network intrusions; attack symptoms; IDS tasks; and IDS architecture)," 7 April [Online]. Available: http://www.windowsecurity.com/articles-tutorials/intrusion_detection/Intrusion_Detection_Systems_IDS_Part_I__network_intrusions_attack_symptoms_IDS_tasks_and_IDS_architecture.html.

Kumar, Y. and Dhawan, S. 2012. "A review on information flow IN intrusion detection system," *IJCEM International Journal of Computational Engineering & Management,* vol. 15, no. 1, pp. 91-96,

Lee, W., Stolfo, S. and Mok, K. 1999. "Mining in a data-flow environment: Experience in network intrusion detection," in fifth ACM SIGKDD international conference on Knowledgediscovery and data mining.

Li, W. 2004. "Using Genetic Algorithm for Network Intrusion Detection," Proc. of the United States Department of Energy Cyber Security Group.

Liu, C., Yang, J., Y. Zhang, R. Chen and J. Zeng, "Research on immunity-based intrusion detection technology for the Internet of Things," Seventh International Conference on Natural Computation, 2011.

Luck, M., McBurney, P. and Preist, C. 2003. Agent Technology: Next Generation Computing, AgentLink II.

Majeed, P. G. and Kumar, S. 2014. "Genetic Algorithms in Intrusion Detection Systems: A Survey," *International Journal of Innovation and Applied Studies*, vol. 5, no. 3, pp. 233-240.

McHugh, J. 2000. "Testing intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory," ACM transactions on Information and system Security, vol. 3, no. 4, pp. 262-294.

Moradi, M. and Zulkernine, M. 2004. "A Neural Network Based System for Intrusion Detection and Classification of Attacks," Queen University, Canada.

Mukherjee, S. and Sharma, N. 2012. "Intrusion Detection using Naive Bayes Classifier with Feature Reduction," Procedia Technology, vol. 4, no. 10.1016/j.protcy.2012.05.017., pp. 119-128.

Ojugo, A., Eboka, A., Okonta, O., Yoro, R. and Aghware, F. 2012. "Genetic Algorithm Rule-Based Intrusion Detection System (GAIDS)," *Journal of Emerging Trends in Computing and Information Sciences,* vol. 3, no. 8, pp. 1182-1194.

Panda, M. and Patra, M. R. 2007. "NETWORK INTRUSION DETECTION USING NAÏVE BAYES," IJCSNS *International Journal of Computer Science and Network Security,* vol. 7, no. 12, pp. 258-263.

Panda, M., Abraham, A., Das, S. and Patra, M. R. "Network Intrusion Detection System: A Machine Learning Approach," Intelligent Decision Technologies, vol. 5, no. 4, 2011.

Rajasekaran, S. and Vijayalakshmi Pai, G. A. 2003. Neural Networks, Fuzzy logic and genetic algorithm: synthesis and applications, PHI Learning Pvt. Ltd.,

Roumen Trifonov, R. Y. 2016. "Some Security Issues of the Governmental Cloud," in 15th International Conference on ACE'16, Mallorca, Spain, August 19-21.

Scarfone, K. and Mell, P. 2007. Guide to Intrusion Detection and Prevention Systems (IDPS), National Institute of Standards and Technology.

Stiawan, D., Abdullah, A. H. and M. Y. Idris, 2011. "Characterizing Network Intrusion Prevention System," *International Journal of Computer Applications*, vol. 14, no. 1.

Tsai, C., Hsu, Y., Lin, C. and Lin, W. 2009. "Intrusion detection by machine learning: A review," Expert Systems with Applications, vol. 36, no. 10, pp. 11994-12000.

Vesely, A. and Brechlerova, D. 2004. "Neural networks in intrusion detection systems," Agric. econ. - Czech, vol. 50, pp. 35-39.

****