IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-5, Issue-12 E-ISSN: 2347-2693

Machine Learning in Cyber Defence

Namita Parati[1*], Pratyush Anand[2]

[1*]Department of CSE, BRECW, Hyderabad, India
[2]Functional Consultant, Fujitsu Pvt. Ltd., Hyderabad, India

[*]*Corresponding Author: namianand006in@gmail.com*

Available online at: www.ijcseonline.org

Received: 09/Nov/2017, Revised: 21/Nov/2017, Accepted: 06/Dec/2017, Published: 31/Dec/2017

Abstract: Whether we realize it or not, machine learning touches our daily lives in many ways. When you upload a picture on social media, for example, you might be prompted to tag other people in the photo. That's called image recognition, a machine learning capability by which the computer learns to identify facial features. Other examples include number and voice recognition applications. From an intrusion detection perspective, analysts can apply machine learning, data mining and pattern recognition algorithms to distinguish between normal and malicious traffic. One way that a computer can learn is by examples. With the advances in information technology (IT) criminals are using cyberspace to commit numerous cyber crimes. Cyber infrastructures are highly vulnerable to intrusions and other threats. Physical devices and human intervention are not sufficient for monitoring and protection of these infrastructures; hence, there is a need for more sophisticated cyber defense systems that need to be flexible, adaptable and robust, and able to detect a wide variety of threats and make intelligent real-time decisions. Numerous bio-inspired computing methods of Machine Learning have been increasingly playing an important role in cyber crime detection and prevention. The purpose of this study is to present advances made so far in the field of applying ML techniques for combating cyber crimes, to demonstrate how these techniques can be an effective tool for detection and prevention of cyber attacks, as well as to give the scope for future work.

Index Terms—Intrusion Detection; Machine Learning

I. THE NEED FOR INTELLIGENT IDS

An intrusion detection system (IDS) monitors the network traffic looking for suspicious activity, which could represent an attack or unauthorized access. Traditional systems were designed to detect known attacks but cannot identify unknown threats. They most commonly detect known threats based on defined rules or behavioural analysis through baselining the network.

A sophisticated attacker can bypass these techniques, so the need for more intelligent intrusion detection is increasing by the day. Researchers are attempting to apply machine learning techniques to this area of cybersecurity.
The foundation of any intelligent IDS is a robust data set to provide examples from which the computer can learn.

Today, however, very little security data is publicly available. That's why I conducted an experiment in which I created a small, new data set with discernible features that can help analysts train computers to detect the most serious threats, even zero-day attacks.

II. LITERATURE REVIEW

A. Intrusion Detection System

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 [1] [2] [3].

Intrusion detection system only can identify intrusions, and it cannot prevent the system from attacks [4] [5]. 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.

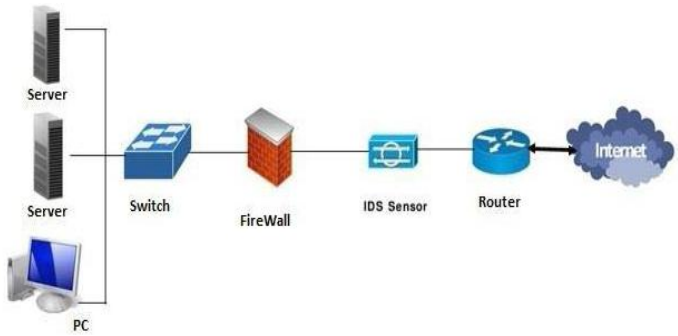

Figure 1: Intrusion detection system

B. 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 [2]. 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.

The IPS should work properly, as it one of the main frontline components used to avoid the degrading of network performance. It must also work fast because exploits could be caused in real-time. The IPS must also spot and react precisely, so it can eliminate threats and false positives. Figure 02 indicates how an IPS is placed in a networking environment.

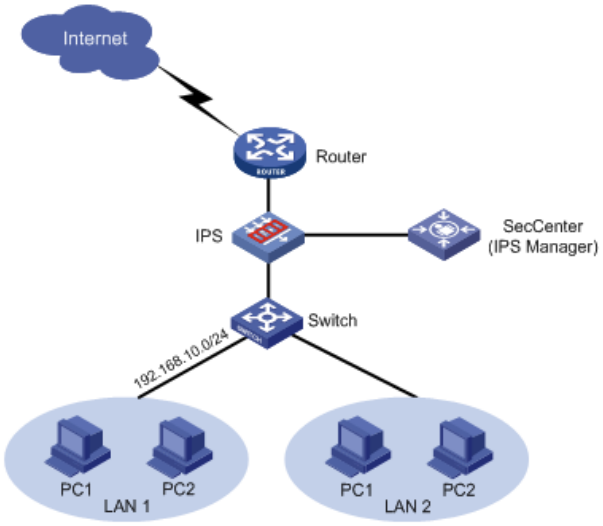

Figure 2: Intrusion prevention system

C. Machine Intelligence/Learning

AI (also called machine intelligence in the beginning) emerged as a research discipline at the Summer Research Project of Dartmouth College in July 1956. AI can be described in two ways:

(i) as a science that aims to discover the essence of intelligence and develop intelligent machines;

(ii) as a science of finding methods for solving complex problems that cannot be solved without applying some intelligence (e.g. making right decisions based on large amounts of data).

In the application of ML to cyber defense, we are more interested in the second definition.

Research interest in AI include ways to make machines (computers) simulate intelligent human behavior such as thinking, learning, reasoning, planning. The general problem of simulating intelligence has been simplified to specific sub-problems which have certain characteristics or capabilities that an intelligent system should exhibit. The following characteristics have received the most attention:

a) Deduction, reasoning, problem solving (embodied agents, neural networks, statistical approaches to AI);

b) Knowledge representation (ontologies);

c) Planning (multi-agent planning and cooperation);

d) Learning (machine learning);

e) Natural Language processing (information retrieval – text mining, machine translation);

f) Motion and Manipulation (navigation, localization, mapping, motion planning);

g) Perception (speech recognition, facial, recognition, object recognition);

h) Social Intelligence (empathy simulation);

i) Creativity (artificial intuition, artificial imagination);

j) General Intelligence (Strong AI).

Classic AI approaches focus on individual human behavior, knowledge representation and inference methods. Distributed

Artificial Intelligence (DAI), on the other hand, focuses on social behavior, i.e. cooperation, interaction and knowledge-sharing among different units (agents). The process of finding a solution in distributed resolution problems relies on sharing knowledge about the problem and cooperation among agents. It was from these concepts that the idea of intelligent multi-agent technology emerged. An agent is an autonomous cognitive entity which understands its environment, i.e. it can work by itself and it has an internal decision-making system that acts globally around other agents. In multi-agent systems, a group of mobile autonomous agents cooperate in a coordinated and intelligent manner in order to solve a specific problem or classes of problems. They are somewhat capable of comprehending their environment, making decisions and communicating with other agents.

The lack of exactness and inconsistency in the network traffic patterns has encouraged a number of attempts towards intrusion detection based on 'Soft Computing'. 'Soft Computing' techniques attempt to devise inexact and approximate solutions to the computationally-hard task of detecting abnormal patterns corresponding to an intrusion

D. intrusion detection and prevention system

An intrusion detection and prevention system (IDPS) (See Fig. 3) is software or a hardware device placed inside the network, which can detect possible intrusions and also attempt to prevent them. IDPSs provide four vital security functions: monitoring, detecting, analyzing, and responding to unauthorized activities.

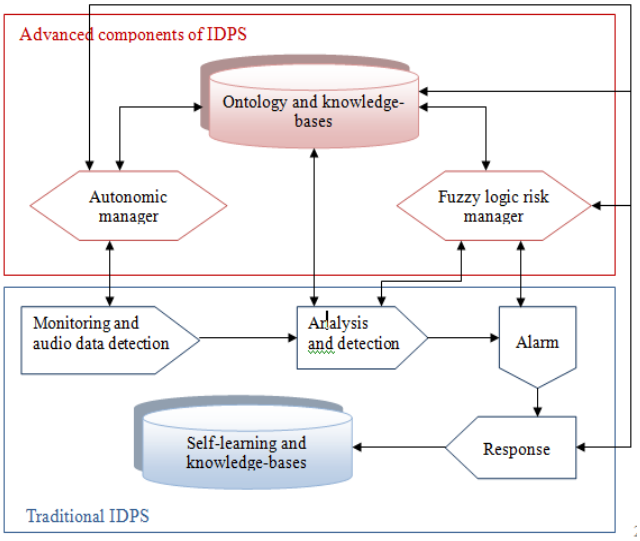

Figure 3: Intrusion prevention system

D. Desired Characteristics of an IDPS

An IDPS should have certain characteristic in order to be able to provide efficient security against serious attacks.

Those characteristics include the following:

- Real-time intrusion detection – while the attack is in progress or immediately afterwards,
- False positive alarms must be minimized,
- Human supervision should be reduced to minimum, and continuous operation should be ensured,
- Recoverability from system crashes, either accidental or those resulting from attacks,
- Self-monitoring ability in order to detect attackers' attempts to change the system,
- Compliance to the security policies of the system that is being monitored, and
- Adaptability to system changes and user behavior over time.

III. APPLICATIONS OF AI TO DEFENSE AGAINST CYBER CRIMES

After surveying the papers available about AI applications in CD, we are able to conclude that numerous useful applications already exist in this field. They belong, first of all, to applications of artificial neural nets in perimeter defense. On the other hand – it has become obvious that many more CD problems can be solved successfully only when AI methods are used. Wide knowledge usage is necessary in decision making, and the intelligent decision support is one of the yet unsolved problems in CD. A large number of methods have been developed in the artificial intelligence field for solving hard problems that require intelligence from the human perspective. Some of these methods have reached a stage of maturity where precise algorithms exist that are based on these methods. Some methods have even become so widely known that they are not considered belonging to artificial intelligence any more, but have become a part of some application area, for instance, data mining algorithms that have emerged from the learning subfield of AI. It would be impossible to try to give more or less complete survey of all practically useful AI methods in a brief survey. Instead, we have grouped the methods and architectures in several categories: neural nets, expert systems, intelligent agents, search, machine learning, data mining and constraint solving. We outline these categories here, and we give references to the usage of respective methods in cyber defence. We are not going to discuss natural language understanding, robotics and computer vision which we consider specific applications of AI. Robots and computer vision have definitely impressive military applications, but we have not found anything specific to CD there.

A. Neural nets

Neural nets have a long history that begins with the invention of perceptron by Frank Rosenblatt in 1957 – an artificial neuron that has remained one of the most popular elements of neural nets [6]. Already a small number of perceptrons combined together can learn and solve interesting problems. But neural nets can consist of a large number of artificial neurons. Therefore neural nets provide a functionality of massively parallel learning and decision-making. Their most distinguished feature is the speed of operation. They are well

suited for learning pattern recognition, for classification, for selection of responses to attacks [7] etc. They can be implemented either in hardware or in software.

A reason for the popularity of neural nets in cyber defense is their high speed, if implemented in hardware or used in graphic processors. There are new developments in the neural nets technology: third generation neural nets – spiking neural networks that mimic biological neurons more realistically, and provide more application opportunities. Good opportunities are provided by the usage of FPGA-s (field programmable gate arrays) that enable rapid development of neural nets and their adjustment to changing threats.

B. Expert systems

Expert systems are unquestionably the most widely used AI tools. An expert system is software for finding answers to questions in some application domain presented either by a user or by another software [8]. It can be directly used for decision support, e.g. in medical diagnosis, in finances or in cyberspace. There is a great variety of expert systems from small technical diagnostic systems to very large and sophisticated hybrid systems for solving complex problems. Conceptually, an expert system includes a *knowledge base*, where expert knowledge about a specific application domain is stored. Besides the knowledge base, it includes an *inference engine* for deriving answers based on this knowledge and, possibly, additional knowledge about a situation. Empty knowledge base and inference engine are together called *expert system shell* -- it must be filled with knowledge, before it can be used. Expert system shell must be supported by software for adding knowledge in the knowledge base, and it can be extended with programs for user interactions, and with other programs that may be used in hybrid expert systems. Developing an expert system means, first, selection/adaptation of an expert system shell and, second, acquiring expert knowledge and filling the knowledge base with the knowledge. The second step is by far more complicated and time consuming than the first. There are many tools for developing expert systems. In general, a tool includes an expert system shell and has also a functionality for adding knowledge to the knowledge repository. Expert systems can have extra functionality for simulation [7], for making calculations etc. There are many different knowledge representation forms in expert systems, the most common is a rule-based representation. But the usefulness of an expert system depends mainly on the quality of knowledge in the expert system's knowledge base, and not so much on the internal form of the knowledge representation. This leads one to the *knowledge acquisition problem* that is crucial in developing real applications.

Example of a CD expert system is one for security planning [9]. This expert system facilitates considerably selection of security measures, and provides guidance for optimal usage of limited resources. There are early works on using expert systems in intrusion detection [10, 11].

C. Intelligent Agent Applications

Intelligent agents are autonomous computer-generated forces that communicate with each other to share data and cooperate with each other in order to plan and implement appropriate responses in case of unexpected events. Their mobility and adaptability in the environments they are deployed in, as well as their collaborative nature, makes intelligent agent technology suitable for combating cyber-attacks.

D. Artificial Immune System Applications

AISs, just like the biological immune systems which they are based on, are employed to uphold stability in a changing environment. The immune-based intrusion detection comprises the evolution of immunocytes (self-tolerance, clone, variation, etc.) and antigens detection simultaneously. An immune system produces antibodies to resist pathogens and the intrusion intensity can be estimated by variation of the antibody concentration. Therefore, AISs play an important role in the cyber security research [12].

VI. CHALLENGES IN INTELLIGENT CYBER DEFENSE

When planning the future research, development and application of AI methods in CD, one has to distinguish between the immediate goals and long-term perspectives. There are numerous AI methods immediately applicable in CD, and there are immediate CD problems that require more intelligent solutions than have been implemented at present. Until now we have discussed these existing immediate applications.

In the future, one can see promising perspectives of the application of completely new principles of knowledge handling in situation management and decision making. These principles include introduction of a *modular and hierarchical knowledge architecture* in the decision making software. This kind of architecture has been proposed in [14]. A challenging application area is the knowledge management for net centric warfare [15]. Only automated knowledge management can guarantee rapid situation assessment that gives a decision superiority to leaders and decision makers on any C2 level. As an example, the paper [14] describes an idea of the hierarchical and modular knowledge architecture in the Joint Command and Control Information System of the Bundeswehr. Expert systems are already being used in many applications, sometimes hidden inside an application, like in the security measures planning software [19].

However, expert systems can get wider application, if large knowledge bases will be developed. This will require considerable investment in knowledge acquisition, and

development of large modular knowledge bases. Also further development of the expert system technology will be needed: modularity must be introduced in the expert system tools, and hierarchical knowledge bases must be used.

Considering a more distant future -- at least some decades ahead, perhaps we should not restrict us to the "narrow AI". Some people are convinced that the grand goal of the AI -- development of artificial general intelligence -- AGI can be reached in the middle of the present century. The first conference on AGI was held in 2008 at the University of Memphis. The Singularity Institute for Artificial Intelligence (SIAI), founded in 2000, warns researchers of a danger that exponentially faster development of intelligence in computers may occur. This development may lead to Singularity, described in [16] as follows: "The Singularity is the technological creation of smarter-than-human intelligence. There are several technologies that are often mentioned as heading in this direction. The most commonly mentioned is probably Artificial Intelligence, but there are others ... -- several different technologies which, if they reached a threshold level of sophistication, would enable the creation of smarter-than-human intelligence. ... A future that contains smarter-than-human minds is genuinely different in a way that goes beyond the usual visions of a future filled with bigger and better gadgets." A futurist Ray Kurtzwell has extrapolated the development to come up with.

Singularity in 2045 [17]. One need not to believe in the Singularity threat, but the rapid development of information technology will definitely enable one to build considerably better intelligence into software in coming years. (Consider the recent impressive performance of IBM-s Watson program [18].) Independently of whether the AGI is available or Singularity comes, it is crucial to have the ability to use better AI in cyber defense than the offenders have it.

V. CONCLUSION

Fast development of information technology considerably impacts to human life styles. However it also generates issues such as emergence of cyber-crimes. Application of artificial agent is a new trend to combating cyber-crimes as they provide features such as mobility, rationality, adaptability and collaboration. This paper has briefly presented about the cyber-crimes and advances made so far in the field of applying Machine Learning techniques in collaboration with Intrusion Prevention Systems, Intrusion Detection Systems in order to combat cyber-crimes.

VI. ACKNOWLEDGMENT

It is not only customary but necessary for a researcher to mention her indebtedness to those who had helped in carrying out and enhance the research work.

REFERENCES

[1] 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]

[2] 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]

[3] I. Ionita and L. Ionita, "An agent-based approach for building an intrusion detection system",RoEduNet International Conference 12th Edition: Networking in Education and Research, pp. 1-6, 26-28, 2013 [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6714184. [Accessed: 11- Feb- 2016]

[4] S. Dilek, H. Çakır and M. Aydin, "APPLICATIONS OF ARTIFICIAL INTELLIGENCE TECHNIQUES TO COMBATING 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]

[5] A. Cerli and D. Ramamoorthy, "Intrusion Detection System by Combining Fuzzy Logic with Genetic Algorithm", Global Journal of Pure and Applied Mathematics (GJPAM), vol. 11, no. 1, 2015 [Online]. Available: http://ripublication.com/gjpamspl/gjpamv11n1spl_20.pdf. [Accessed: 09- Feb- 2016]

[6] F. Rosenblatt. The Perceptron -- a perceiving and recognizing automaton. Report 85- 460-1, Cornell Aeronautical Laboratory, 1957.

[7] G. Klein, A. Ojamaa, P. Grigorenko, M. Jahnke, E. Tyugu. Enhancing Response Selection in Impact Estimation Approaches. Military Communications and Information Systems Conference (MCC), Wroclaw, Poland, 2010.

[8] http://en.wikipedia.org/wiki/Expert_system. Expert System. Wikipedia.

[9] J. Kivimaa, A. Ojamaa, E. Tyugu. Graded Security Expert System. Lecture Notes in Computer Science, v. 5508. Springer, 2009, 279-286.

[10] D. Anderson, T. Frivold, A. Valdes. Next- generation intrusion detection expert system (NIDES). Technical Report SRI-CSL-95-07, SRI International, Computer Science Lab (1995).

[11] TF. Lunt, R. Jagannathan. A Prototype Real-Time Intrusion-Detection Expert System. Proc. IEEE Symposium on Security and Privacy, 1988, p. 59.

[12] L. Rui, L. Wanbo, (2010) "Intrusion Response Model based on AIS", International Forum on Information Technology and Applications (IFITA), Vol. 1, pp. 86 – 90.

[13] U. Kaster, B. Kuhiber. Information and Knowledge Management in C2 Systems – The Gap Between Theory and Practice is not all that big. In: M.- Amanovicz. Comcepts and Implementations for Innovative Military Communications and Information Technologies. Military University of Technology Publisher, Warsaw, 2010, pp. 98 – 107.

[14] J. Kaster. Combined Knowledge Management and Workflow Management in C2 Systems – a user centered approach. Fraunhofer Institute for Communication, Information Processing and Ergonomics. Report ID # 197, 2009.

[15] http://singinst.org/overview/whatisthesingularity/
[17] R. Kurtzwell. The Singularity is Near. Viking Adult. 2005.
[18]http://www.ted.com/webcast/archive/event/ibmwatson
[19] J. Kivimaa, A. Ojamaa, E. Tyugu. Pareto-Optimal Situation Analysis for Selection of Security Measures. Proc. MilCom, 2008.

ABOUT THE AUTHOR

Namita Parati is working as Assistant Professor at Bhoj Reddy Engineering College for Women, Hyderabad, INDIA. She has received B.E, M.Tech Degree in Computer Science and Engineering. Her main research interest includes intrusion detection using hybrid network.

Pratyush Anand is working asIT Functional Consultant at, Fujitsu Pvt Ltd, Hyderabad, INDIA. He has received B.E Degree in Computer Science and Engineering and MBA in IT and Marketing. He main research interest includes Cloud computing and Machine Learning.

