ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

Importance of Multi-agents in Computational Intelligence: A Discussion

S. Sandosh B.E, M.Tech [I.S], (Ph.D),M.B.A., Dr. V. Govindasamy Ph.D, Dr. G. Akila Ph.D

Assistant Professor, Department of Computer Science & Engg, Sri Ganesh College of Engineering and Technology, Puducherry, India.

Associate Professor, Department of Information Technology, Pondicherry Engineering College, Pondicherry, India

Assistant Professor, Department of Computer Science & Engg, Pondicherry Engineering College, Pondicherry, India

ABSTRACT: Cyber frameworks are liable to intrusions and threats. The speed of the processes and a number of statistics for use in protecting the computer-generated area could not be treated by means of people without big computerization. It is obvious that protection in opposition to intelligent cyber weapons can be carried out through a wise software program. However, it's far tough to increase software with traditional constant procedures like hard-wired logic on decision making for efficiently protecting the dynamically changing attacks in the networks. Hence, there is a mandatory requirement for higher refined cyber protection framework that should be flexible and adaptable, and the framework is to be capable of handling huge kind of threats and to make intelligent real-time decisions. This state of affairs may be treated by making use of strategies of Artificial Intelligence which offers flexibility, also promotes to know the capability to software. The proposed work in this paper affords an efficient model with AI by way of combining smart cyber sensor agents (or computer-generated forces) a good way to hit upon, compare and do act to cyber threats in a timely mode and permit the group of agents to make decisions.

KEYWORDS: Cyber Space, Artificial Intelligence & Security, Intelligent Cyber Defense, Computer-generated forces, Computational Intelligence.

I. INTRODUCTION

Security is a very important issue for any People, Corporation, Organization and Nation in accordance to keep up growth and stability. Security threat provides rise to many issues like instability, economic setbacks, terror attacks causes loss of human lives, creates un-safety feelings. As a human being, the protection is difficult task as a result of the human has many restrictions on analyzing and process data at a time. This is often huge known issue within the current security system. This downside will overcome on the lot of sensible manner with the assistance of Artificial Intelligence (AI) techniques integration. The AI is that the method which machine acts just like the human. This strong feature permits AI operating in numerous fields simply. The operating nature of AI is analogous to the human brains. The AI looks to play the key role in security if the mixing of some AI techniques area finished the protection system, definitively enhances the protection infrastructure of any organization or nation. The protection system includes independent agency, DOS attack, Intrusion detection system, Cryptography, etc. Human process ability integrated with AI actually raise the protection at high extend.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

CYBER SECURITY

The process and ability of information and communications systems are protected or defended against damage of the information or the unauthorized use, modification, exploitation, etc. Strategies, policies and standards regarding the security and its operations in cyber area, and incorporating the complete range of vulnerability identification, risk reduction, preemption, world level engagement, accident response, recovery policy and actions, including the computer network procedures, information declaration, law enforcement, military, intelligence missions and diplomacy, as they relate to the security and steadiness of the global data and communication structure is to be properly constructed.

The goals of the cyber securities are:

1. To preserve the Integrity of the network system.
2. To regulate the usage of the network system.
3. To avoid extraction of software subcategories.
4. To secure the data in the network system data.
5. To secure the network access and to defend the unauthorized access attempts.
6. To make sure right and exact execution.
7. To make sure that the computations are perfect and efficeint.

II. ARTIFICIAL INTELLIGENCE IN SECURITY SYSTEM

Artificial intelligence is mandatory, for an immediate reaction to the conditions on the Internet. The security structure should be able to handle a huge volume of information in a fast manner in order to elaborate and evaluate events that occur in cyber area and also to make required real time decisions. The speed of this process and the quantity of data to be used cannot be easily handled by humans without significant automation.

The protection system includes independent agency, DOS attack, Intrusion detection system, Cryptography, etc. Human process ability integrated with AI actually raise the protection at high extend.

The Figure 3 (a) shows the traditional security system and also the real time security is depended on Artificial Intelligence techniques.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

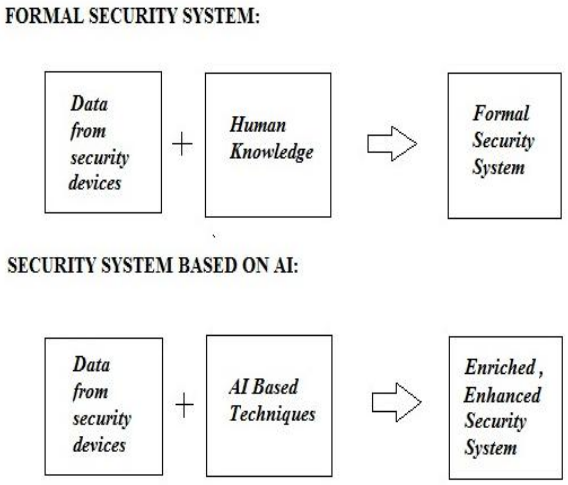


Figure 2 (a)

Various biological stimulated methods of Artificial Intelligence are increasingly playing an vital role in cybercrime discovery and avoidance.

Artificial Intelligence techniques are to be used to defend the cyber threats. A generic AI based model can be represented as,

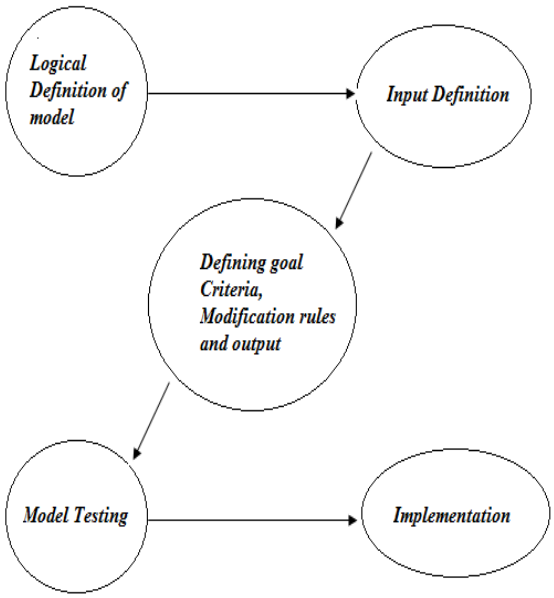


Figure 2 (b)

In the current state of fast developing intelligence of malware and complexity of cyber threats, it is necessary to improve intelligent cyber defense approaches.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

1. INTELLIGENT CYBER DEFENSE

In combined Artificial Intelligence grounded cyber defense scheme for the scattered nature of the Internet, the sensor gathers the statistics from the distributed ports and sends the investigated data to the condition awareness element.

The following are the probable elements of an Artificial Intelligence grounded cyber defense scheme,

1. Condition awareness (A procedure that converts identified data into a decision).
2. Sensors and Exploitation (the system to detect the challenger).
3. Command and Control (A procedure of hiding threats and achieving decisions).
4. Schemes and Strategies (an idea of what condition regulates a nice decision and organizing in accordance to the situations).
5. Defending Mechanism (A knowledge to identify and defend threat).
6. Engineering and Science (It is a basics of plan, arrangement, construction, and keep of cyber defense scheme).

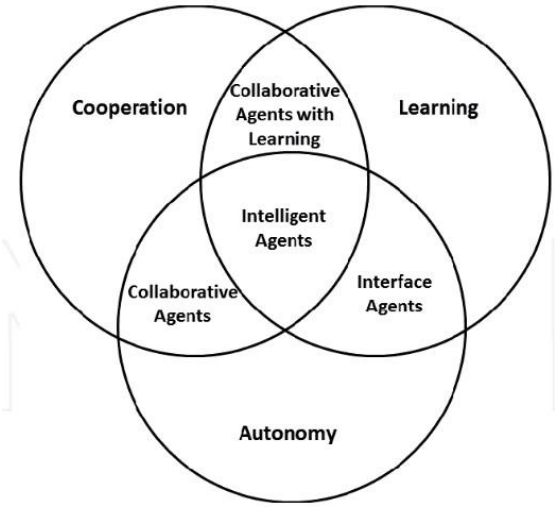


Figure 3

Intelligent cyber defense with human intervention and integrated software is not enough for efficiently protecting the dynamically changing attacks in the networks. Hence, there is a mandatory requirement for higher refined cyber protection framework that should be flexible and adaptable, and the framework is to be capable of handling huge kind of threats and to make intelligent real-time decisions.

This refined cyber defense scheme makes the decision to combine various agents to make the final decision to implement the defensive mechanism. A important situation of day by day network actions should be assigned to very intelligent agents also to be termed as Computer Generated Forces (CGFs).

2. COMPUTER-GENERATED FORCES

According to the defined human and integrated software boundaries, the point that intelligent software agents execute maximum cyber-attacks so that the internet atmosphere will be in need of automation agents to identify, evaluate, and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

respond to cyber-attacks. The purpose of intelligent agents is to travel and monitor over the network, concentrating on each node as much as possible to identify and analyze the node for its vulnerabilities and to address the node to make aware of its vulnerabilities. The intelligent agents should sense and evaluate the network activities for signature of the attack and if it is properly identified the agent should take some cyber-attack actions to defend. This defensive task is to launch and sustain a self-protective limit. The defensive task is to identify, evaluate, and to respond as applicable to cyber-attacks whether the attack is intentional or unintentional. On the defensive side, CGF's will be responsible for ensuring that access control mechanisms, firewalls, intrusion detection systems, and anti-virus and anti-pest software are appropriately deployed and enabled. CGF's will also scan for known vulnerabilities and assess risk.

On the protective side, the CGFs will detect the probable attacks, as individually or jointly examines the events in terms of feasible source, measure the value of probable opposing impacts and the agents develops required actions and finally respond to the attacks. The CGFs will define the kinds of attacks that are happening, the objectives of the attacks, the suitable responses to the attacks, the ranking of the responses, the creation of defenses on the subordinate attacks, the response to the main attacks, and for the whole supervision of the response.

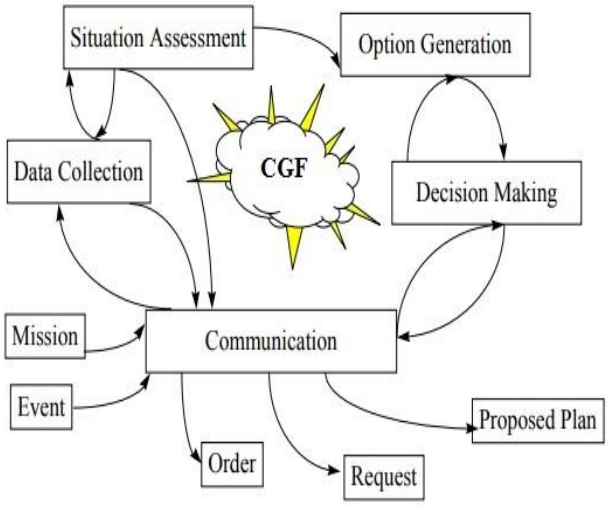


Figure 4

For the effective collection of known and unknown attacks, the CGFs are to be scattered on the entire network so that they collect information about the attack. The information collected by the cyber sensors promotes the cyber responsibilities (agents) to classify the attacks, regulate the probable strength of an attack, and deliver an entrance into the cyber combat that promotes the human observation of the event and the immediate response to the attacks. The Network bandwidth is keen to cyber sensor's information recording and Computer Generated Forces or agent's authentication. The cyber sensors shares the information among them in a secure way and that consumes network bandwidth and until now confirms that every cyber sensors accepts the information they require from other cyber sensors in the network, also at the time of a cyber-attack. Thus the cyber sensors who shares the information about the attack supports to bring in the suitable decision making in the network as a group. Synchronization between all the agents in a group tend to make a decision consumes many challenges. One among the main challenges is the management of the knowledge shared in the network. To overcome this challenge hierarchical knowledge management scheme named Computational Intelligence (CI) is applied in the decision making scheme.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

3. COMPUTATIONAL INTELLIGENCE

The computational Intelligence with the multi-agents or multiple sensors to offer a better decision is a crucial role. Quick status valuation and decision priority can be guaranteed only with the automatic knowledge management scheme.

In this paper, an idea of automatic knowledge management scheme for multi-agent systems is discussed and analyzed, which mainly promotes all real time agents to agree on a reliable decision that can be computed by one or more intelligent agents by sensible interaction between them for knowledge sharing. This idea simplifies work on multiple agents where the agents will have various confidence points in their different states.

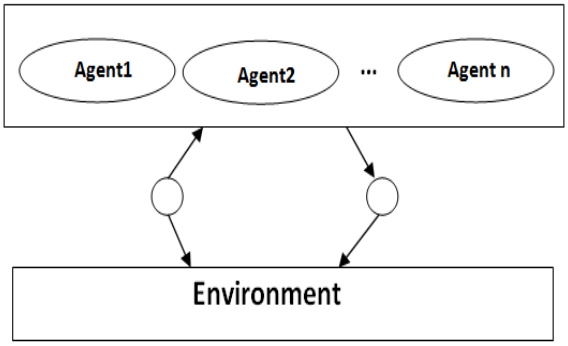
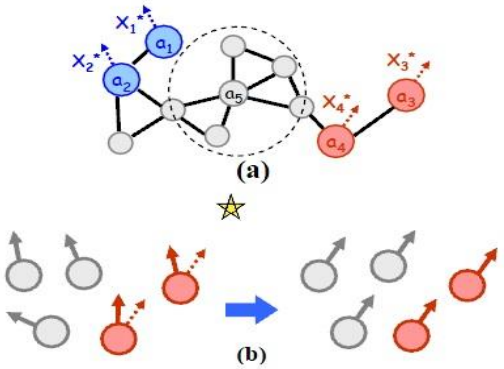


Figure 5 (a)

This idea of Computational Intelligence which regulates the knowledge management and sharing the information among the agents further signifies an extension that promotes for faster decision making in a continuously changing environment. This idea proves that the combination of intelligent agents following the decisions will come to a rapid global acceptance under required situations. This idea of Computational Intelligence with knowledge sharing and management also specifies the way of formal distributed agreement; hence a scheme is discussed to be successful in multi agent detection and decision which extends to handle threats or attacks though the agents may have different degrees of confidence in their present states.

Coordination will be a crucial task in large multi agents scheme where agents are efficiently distributed over the network, as because some important agents may easily tend to obtain important information but not accessible for other agents.



Figue 5(b) & 5(c)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

Figure 5(b) represents the group of agents with the group manager "a5" collects the alerts detected information from all the group agents and makes an appropriate decision and share the decision. Figure 5(c) represents the agents sharing the information with the others that an alert is detected and alert message conveyed in one direction.

These knowledgeable agents are essential to play a vital role when the knowledge sharing helps to achieve a reliable decision making. This idea of Computational Intelligence will help the informed agents to raise their level of confidence so that the entire group of agents would reach a single decision making accepted by all agents.

III. CONCLUSION

In this current situation of fast developing intelligence of malware and superiority of cyber attacks, it is mandatory to design and introduce intelligent cyber defense schemes. Hence the artificial intelligence based intelligent agents help to identify, analyze and respond to the cyber attacks. AI based Intelligent defense system and the Computer Generated Forces (CGF's) together constitutes the detection of cyber-attack efficiently and the alert messages are shared by the all the agents in the multi-agent group for the immediate decision-making process. Each agent defines the alert message or information and share with others through knowledge management scheme which jointly promotes the Computational Intelligence to make the appropriate decision making to respond the attacks. These reliable decisions by all the agents collectively agreed on a decision can be determined by one or a few better-informed agents.

IV. FUTURE WORK

Though the Computational Intelligence systems are planned to be widely used in network security, some ethical and legal problems obviously arises as the science and technology is quickly expanding. A few problems are privacy concerns and responsibilities on the ethical side. Further, the cyber sensor CGFs scheme must operate inside a network using various technologies should make ensure that the information about the security challenges and breaches reaching the knowledge management is very secure. The cyber sensors should be capable to share the information among them in a secure way and also they consume the network bandwidth. The CGF's agents must also guarantee that all the agents receive the information about the attack or threat from the other agents in the network, even at the time of other cyber-attacks happening in the network.

REFERENCES

[1] Mees.W , R. Mil. Acad., Brussels, Debatty, T. "Multi-agent System for APT Detection" IEEE 2014, page no : 401-406 DOI 10.1109/ISSREW.86.
[2]. H. Fu, X. Yuan, K. Zhang, X. Zhang, Q. Xie, (2007) "Investigating Novel Immune-Inspired Multi- Agent Systems for Anomaly Detection", The 2nd IEEE Asia-Pacific Service Computing Conference, pp. 466 472.
[3]. D. Dasgupta, (2006) "Computational Intelligence in Cyber Security", IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety (CIHSPS 2006), pp. 2–3.
[4]. Chih-Han Yu, Justin Werfel, Radhika Nagpal, "Collective Decision-Making in Multi-Agent Systems by Implicit Leadership" 9th Int. Conf. on Autonomous Agents and Multiagent Systems (AAMAS 2010)
[5]. D. Edwards, S. Simmons, N. Wilde, (2007) "Prevention, Detection and Recovery from Cyber-Attacks Using a Multilevel Agent Architecture", IEEE International Conference on System of Systems Engineering (SoSE '07),pp.1– 6.
[6]. Selma Dilek, Huseyin Cakır and Mustafa Aydın "Applications Of Artificial Intelligence Techniques To Combating Cyber Crimes: A Review. IJAIA.Vol. 6, No. 1, January 2015.
[7]. C. Czosseck, E. Tyugu, T. Wingfield "Artificial Intelligence in Cyber Defense" 2011 3rd International Conference on Cyber Conflict © 2011 by CCD COE.
[8]. Dinesh Kumar Saini and Vikas Singh "Soft Computing Techniques in Cyber Defense", International Journal of Computer Applications (0975 – 8887) Volume 50– No.20, July 2012.
[9]. "Agent-Based Control of Distributed Infrastructure Resources" Laurence Phillips, Hamilton Link, Randy Smith, and Laura Welland.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

[10]. Dinesh Kumar Saini and Hemraj Saini "Proactive Cyber Defense and Reconfigurable Framework for Cyber Security" International Review on computer and Software (IRCOS) Vol.2. No.2. March 2007, Pages 89-98. ITALY.
[11]. I. Kotenko, A. Konovalov, A.Shorov. Agent-Based modeling and Simulation of Botnets and Botnet Defence. In: C. Czosseck, K. Podins (eds.). Proc. Conference on Cyber Conflict. CCD COE Publications, Tallinn, Estonia, 2010.
[12].Swapnil Ramesh Kumbhar" An Overview on Use of Artificial Intelligence Techniques in Effective Security Management" Vol. 2, Issue 9, September 2014 IJIRCE.
[13].Laurence Phillips, Hamilton Link, Randy Smith, and Laura Welland "Agent-Based Control of Distributed Infrastructure Resources" SANDIA REPORT, SAND2005-7937 Unlimited Release, Printed Jan 2006