Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 11, November 2019, pg.13 – 17

# A SURVEY ON AI WITH CYBER SECURITY

**Radha R**
Assistant Professor, Department of Computer Science and Engineering
Alliance University, Bangalore, India
radhaprasadnr@gmail.com

***Abstract— In today's digital era, the emerge of IOT and linked devices, cyber security experts come across a lot of encounters. The specialists require all the aid to overcome attacks, security cracks, its affects and respond to the attacks. A lot of linked workplaces lead to heavy traffic, high security attack vectors, security breaches and many more that the cyber environment cannot be handled by humans without sizeable automation. It is not easy to create software managed system with standard working algorithms (hard-wired logic on deciding level) for successfully cautious against the prominently growing attacks in networks. It is a evident fact that number of cyber security problems are now settled as an add on with progress only procedures of Artificial Intelligence techniques unit acquiring utilized. Cyber Security applications and analyses can now be moulded with AI applications and its existing methods.***

***KEYWORDS: Artificial Intelligence, Intelligent Agents, Cyber Security, Expert Systems.***

## I. INTRODUCTION

Establishment of mechanisms and technical means to maintain an up-to-date picture of possible threats of different scale, sources and character, trends in geopolitical context development and relevant national cyber picture analysis and development of capabilities to help identify attribution sources and take appropriate forms of protection and counteraction. Cyber Threats Intelligence is developed at three levels: strategic, operational, and tactical.

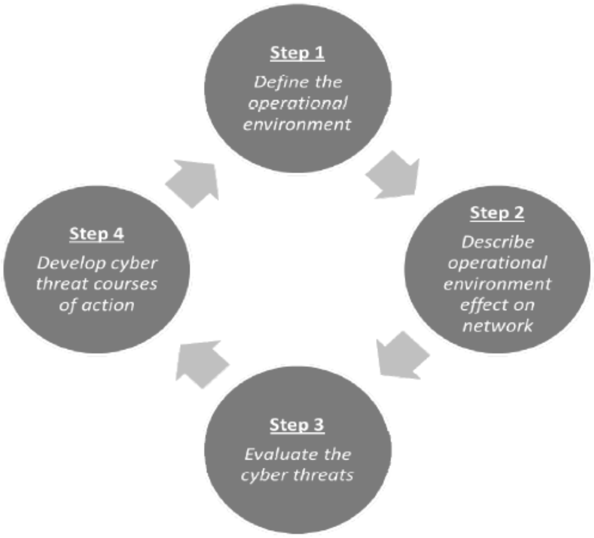

Step 1
Define the operational environment
Step 2
Describe operational environment effect on network
Step 3
Evaluate the cyber threats
Step 4
Develop cyber threat courses of action

Fig: Cyber threat intelligence cycle

AI enables us to develop autonomous computer solutions that adapt to their context of use, using self-management, self-tuning and self-configuration, self-diagnosis and self-healing. When it comes to the future of information security, AI looks like a very promising field of research that focuses on improving cyberspace security measures.

World practice has already noted a significant number of various Artificial Intelligence applications in computer security. Without trying for a comprehensive grouping, we could divide these methods into two main ways:

A. Conditionally named "distributed" methods:
A1. Multi-Agent Systems of Intelligent Agents;
A2. Neural Networks;
A3. Artificial Immune Systems and Genetic Algorithms.

B. Conveniently named "compact" methods:
B1. Machine Learning Systems, including: associative methods, inductive logic programming, Bayes classification;
B2. Pattern recognition algorithms;
B3. Expert Systems;
B4. Fuzzy logic.

## II. METHODS OF ARTIFICIAL INTELLIGENCE APPROPRIATE FOR FUNCTIONAL CYBER THREATS INTELLIGENCE

Features can be aggregated into a vector known as “feature vector”. Thus, feature extraction can be defined as an operation which transforms one or several signals into a feature vector. Identifying and extracting good features from signals is a crucial step, because otherwise the classification algorithm will have trouble identifying the class of these features, i.e., the behavioral state of the possible adversary.

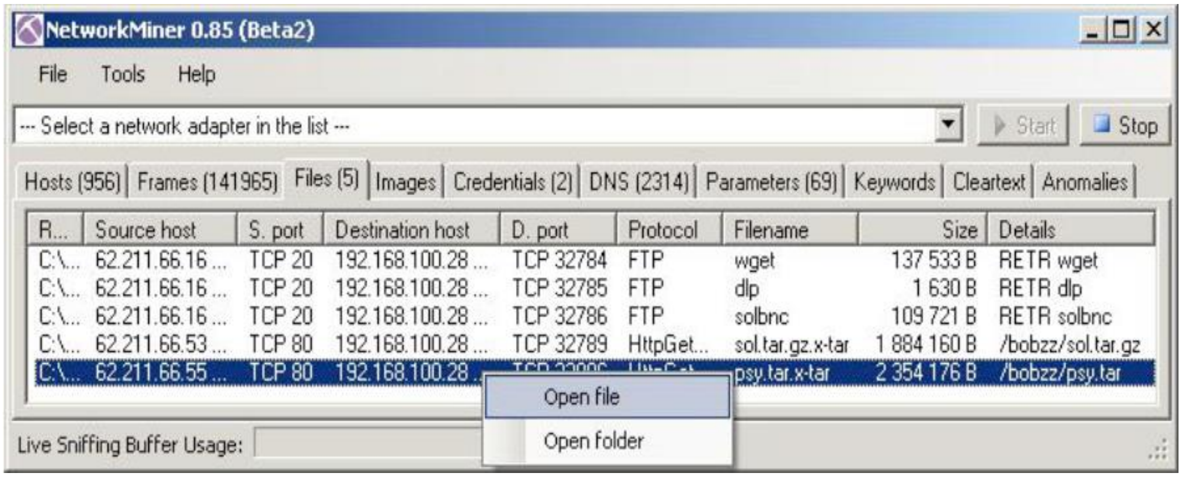
Therefore, following the analogy of the Brain-Computer Interface, two basic tasks have to be solved:

1. to find a suitable approach to selecting characteristics from which to derive features suitable for behavioral interpretation and validation. In doing so, the necessary inter-subject discrimination of the features for the subsequent classification must be ensured;

2. to build and optimize an ensemble of classifiers based on trained models to be used to assess behavior.

According to the researcher's scenario, design of the system of assessing the behavior of the supposed adversary can consist of two main phases: 1) offline training phase to calibrate the system and 2) online phase which uses the system to recognize the type of behavior states and translate them into the computer commands. Both offline and online phases follow a closed-loop process, generally composed of six steps:

a) Network activity measurement- this step consists in network surveillance of broadband Internet traffic (e-Mails, Web traffic, instant messengers, etc.) using methods, such Packet Capture appliances Fig in order to obtain signals reflecting the opponent’s intentions



| R... | Source host | S. port | Destination host | D. port | Protocol | Filename | Size | Details |
|---|---|---|---|---|---|---|---|---|
| C:\... | 62.211.66.16 ... | TCP 20 | 192.168.100.28 ... | TCP 32784 | FTP | wget | 137 533 B | RETR wget |
| C:\... | 62.211.66.16 ... | TCP 20 | 192.168.100.28 ... | TCP 32785 | FTP | dlp | 1 630 B | RETR dlp |
| C:\... | 62.211.66.16 ... | TCP 20 | 192.168.100.28 ... | TCP 32786 | FTP | solbnc | 109 721 B | RETR solbnc |
| C:\... | 62.211.66.53 ... | TCP 80 | 192.168.100.28 ... | TCP 32789 | HttpGet... | sol.tar.gz.x-tar | 1 884 160 B | /bobzz/sol.tar.gz |
| C:\... | 62.211.66.55 ... | TCP 80 | 192.168.100.28 ... | [illegible] | [illegible] | psy.tar.x-tar | 2 354 176 B | /bobzz/psy.tar |

Fig: Packet capturing appliances

b) Preprocessing - this step consists in cleaning and denoising input data to enhance the relevant information embedded in the signals;

c) Feature extraction – this extraction aims at relating the signals by a few applicable values called "features"

d) Classification - this step assigns a class to a set of features extracted from the signals, which corresponds to the kind of behavioral state identified. This phase can also be represented as "feature translation". Grouping algorithms are known as "classifiers"

e) Translation into a command/application - once the behavioral state is identified, a command is associated with this state in order to control a given application

Once the data have been acquired, they are pre-processed to clean (de-noise) the signals and to enhance relevant information embedded in these signals. The pre-processing step aims at increasing the signal-to-noise ratio of the input signals.

To perform this pre-processing, various spatial-spectrotemporal filters can be used. Naturally, numerous other pre-processing methods, which are more complex and more advanced, can be proposed and used. The most popular methods are namely, Independent Component Analysis (ICA) and Common Spatial Patterns (CSP) method. Based on a study of literary sources, the Echo State Network (ESN) method was proposed as a mechanism for feature selection – this is a class of Recurrent Neural Networks where the so-called "Reservoir Computing" approach for training is formulated.

## III. CONCLUSION

The process of introducing Artificial Intelligence methods at the different levels of Cyber Threat Intelligence is at very different stages: while in Tactical Intelligence, it has long gone out of the phase of research and experiments and is used for building real effective systems, In the field of Operational Intelligence, these studies are in a very initial phase and require the commitment of substantial resources. Furthermore, the question arises as to the application of possible outcomes of Operational Intelligence in the activity of Tactical Intelligence systems, which are intended to neutralize the immediate threats to computer systems and networks.

# REFERENCES

[1]. Anderson, Frivold, Valdes, "Next-Generation Intrusion Detection Expert System (NIDES)".

[2]. Rosenblatt. "The Perceptron-a perceiving and recognising automaton.Report 85-460-1, Cornell natural philosophy Laboratory, 1957.

[3]. "Logic Programming for Engineering", Bratko.I, Addison-Wesley, 2001.

[4]. B. Mayo, E. Tyugu, J. Penjam. Constraint Programming. Alignment ASI Series, v. 131, Springer-Verlag. 1994.

[5]. E. Tyugu. Algorithms and Architectures of Artificial Intelligence.IOS Press. 2007.

[6]. NabaSuroor and Syed Imtiyaz Hassan, "Identifying the factors of modern daystress using machine learning".

**[7].** Barika.F, K. Hadjar, and N. El-Kadhi, “ANN for mobile IDS solution” in Security and Management.
**[8].** TF. Lunt, R.Jagannathan. A Prototype Real-Time Intrusion-Detection Expert System.Proc.
**[9].** B. Iftikhar, A. S. Alghamdi, “Application of artificial neural network within the detection of dos attacks”, 2009.
**[10].** P. Norvig, S. Russell. “Artificial Intelligence: fashionable Approach”, 2000.