ARTIFICIAL INTELLIGENCE APPROACH TO ENSURING THE CYBER SECURITY OF CRITICAL INFRASTRUCTURE

[1]Petar Čisar , [2]Sanja Maravić Čisar and [2]Igor Fürstner

1 University of Criminal Investigation and Police Studies, Belgrade, Serbia
petar.cisar@kpu.edu.rs

2 Subotica Tech – College of Applied Sciences, Subotica, Serbia
sanjam@vts.su.ac.rs, ifurst@vts.su.ac.rs

Introduction

Critical infrastructure is the basis of systems, networks and properties in a country that are so crucial that their continued operation is required to ensure the national security, economy, and the public's health and/or safety.
Although critical infrastructure is similar in most of countries due to the basic requirements of life, this infrastructure can vary according to a nation's needs, resources and development level.
The functioning of critical infrastructure is of particular importance during emergencies related to public health and safety e.g. COVID-19. Certain industries within the critical infrastructure at this time have a special responsibility to continue to operate.
Artificial intelligence (AI) can provide many benefits in order to raise cyber security levels for critical infrastructure.

Benefits of AI for cyber security

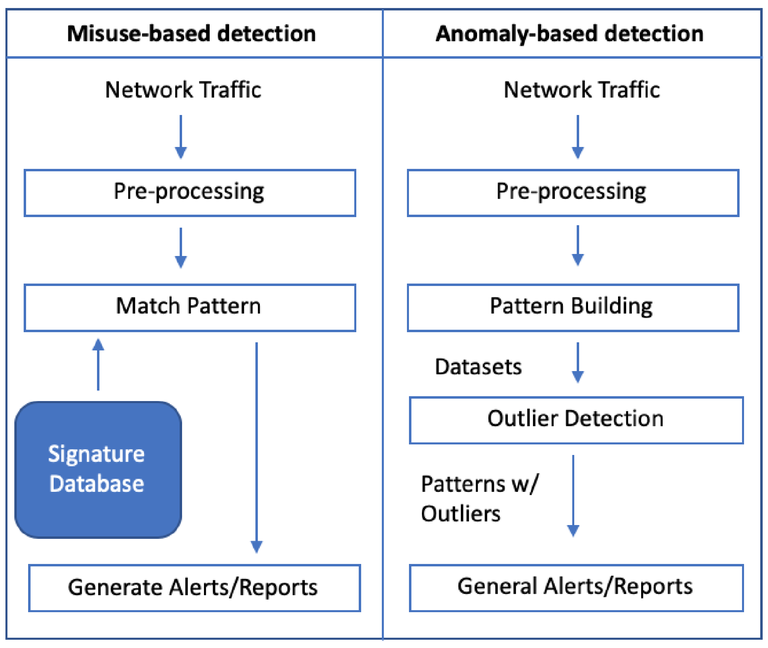
In addition to application in many areas, AI systems are increasingly being used to ensure a sufficient level of cyber security. Some successful applications in security sphere are:
Biometric logins
- ❑ Detection of threats and other malicious activities
- ❑ Natural language processing
- ❑ Multi-factor authentication

Drawbacks and limitations of AI for cyber security

The benefits elaborated above are only part of the wide possibilities of AI in improving cyber security. But, there are disadvantages which prevent AI from becoming a basic tool in this field. In order to build and maintain an AI system, a large amount of resources are required including memory, data, and CPU power. Additionally, because AI systems are trained through learning data sets, it is necessary to use many different data sets of malware codes, usual (non-malicious) codes, and anomalies. Obtaining all of these data require a lot of time and significant resources.
Another drawback is that hackers can also use AI to improve and test efficiency of their malware.

Implementation of systems with AI in intrusion detection

The goal of intrusion detection is to identify malicious entities. The intrusion detection system (IDS) has the role of detecting unwanted manipulations. IDS should detect all types of malicious network traffic and computer use, which cannot be detected by a conventional firewall. The general architecture of an IDS system is shown in the following figure.



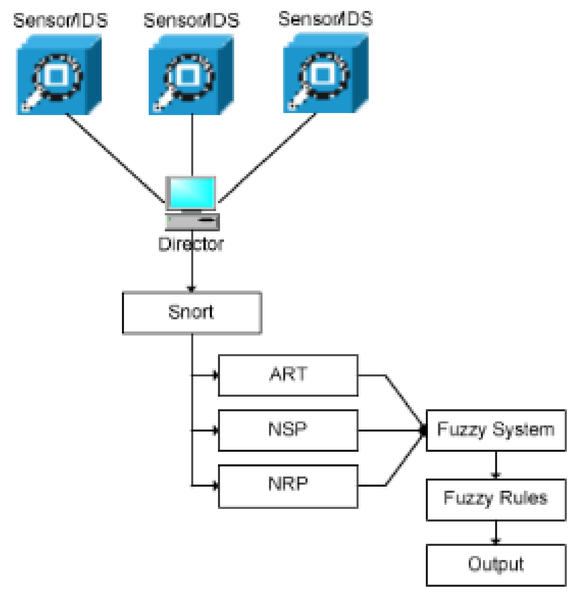
Architecture of an IDS

The goal of applying AI in IDS / IPS (intrusion prevention system) is to automate the correlation process, which otherwise the human brain can do very well based on the repetition of a large number of cases.
The types of artificial intelligence systems that are often used for intrusion detection are:
- ❑ expert systems
- ❑ fuzzy logic
- ❑ artificial neural networks

Expert systems are intelligent computer programs that contain "expert" knowledge, ie. knowledge that an expert in that field would have. Expert system has three components: knowledge base, inference engine and control engine.
These systems are modeled in such a way as to separate the phase of harmonization of rules from the phase of action. E.g. NIDES (Next-Generation Intrusion Detection Expert System). NIDES applies hybrid intrusion detection technique - combines anomaly-based (monitoring of system activities) and signature-based approaches (detection of known attack sequences). It generates user profiles based on several different criteria, while misuse detection component encodes known scenarios and attack patterns.

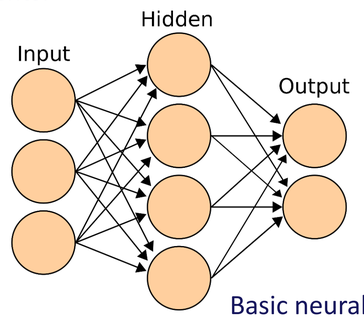
Fuzzy logic

Unlike formal logic in which two values are used in reasoning (true-false, 0-1), fuzzy logic uses real numbers from the interval [0, 1], which is much closer to reality, human thinking and expression.
Using fuzzy logic it is possible to conclude on the basis of incomplete and insufficiently precise information - approximate reasoning. Fuzzy logic systems (fuzzy systems) are used in diagnostics, management and prediction.
One of the various possibilities of application of fuzzy logic in function of intrusion detection is fuzzy-based Snort (popular open source IDS/IPS software).



Fuzzy-based Snort (ART - Average time between Received Packets, NSP - Number of Sent Packets, NRP - Number of Received Packets)

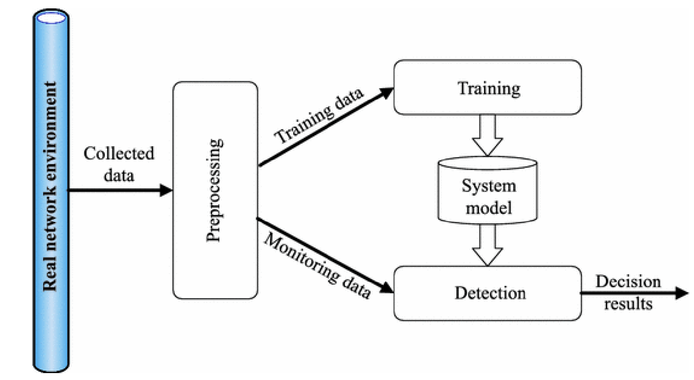
Artificial neural networks are creations that mimic biological nervous systems in performing functions, such as learning from a limited set of examples and pattern recognition. They provide some remarkable possibilities such as the ability to learn, adapt, and generalize. They are also successfully applied in many areas, including pattern recognition, classification and process control.
An artificial neural network is a system composed of several simple processor units - neurons, connected by communication channels - connections with weight coefficients.



Basic neural network model

The goal of neural networks is the idea to train them to predict the next action or user command, keeping in mind a window of n previous actions.
Neural networks in the security sphere, in addition to numerous advantages, also have certain disadvantages. Advantages of neural networks are:
- ❑ They work with data having noise.
- ❑ Their success does not depend on any statistical assumptions about the nature of the underlying data.
- ❑ They are easier to change for new user communities.

Neural networks have to be trained, ie. undergo a set of trainings using simulated or actual attacks and legal approaches to "learn" what regular approaches are and what intrusions are, and to keep decision-making mechanisms up and running.



Impact of training data on the detection result

Conclusions

Bearing in mind all the stated characteristics of AI, it can be concluded that it is quite far from becoming the universal cyber security solution. The best approach in the meantime would be combining current proven security methods with AI tools.

ICCECIP 2020
2nd International Conference on Central European Critical Infrastructure Protection
November 16-17, 2020. Budapest, Hungary
ÓBUDA UNIVERSITY
BÁNKI DONÁT FACULTY OF MECHANICAL AND SAFETY ENGINEERING