A Generative Adversarial Artificial Immune Network (GAAINet) for Distributed Intrusion Detection in Industrial IoT Systems

Siphesihle Sithungu

Supervisor: Prof. E.M. Ehlers

UNIVERSITY OF JOHANNESBURG

INTRODUCTION

IIoT is increasingly being applied in many important sectors, such as manufacturing, agriculture, military (Jaidka, Sharma & Singh 2020), energy, transport and health (Figueroa-Lorenzo, Añorga & Arrizabalaga 2020). The increased usage of IIoT – albeit to increase productivity and quality of life – raises security concerns. Generative Adversarial Network (GAN) approaches have been proposed for intrusion detection in IIoT (more specifically Cyber-Physical Systems (CPS)) in the literature (Belenko, Chernenko, Kalinin & Krundyshev 2018).

There is not a relatively large collection of work in the literature based on GANs for intrusion detection for IIoT. In addition, the works mentioned are relatively recent, which is reason to believe that this is an ongoing area of research. Therefore, in the aim of contributing to the ongoing research, current work proposes a novel Generative Adversarial Artificial Immune Network (GAAINet) for intrusion detection in IIoT systems.

BACKGROUND

This thesis investigates the realisation of an immunologically inspired generative model for intrusion detection in IIoT systems. The proposed model is a novel generative adversarial artificial immune network (GAAINet) which serves two purposes: (1) generating synthetic attack samples for IIoT intrusion detection to address class imbalance and (2) performing intrusion detection by training an immunologically inspired intrusion detector.

The typical use of artificial immune networks (AINs) is to learn the structure of a dataset for clustering or classification purposes. The research conducted in this thesis is the first body of work to originate and construct a standalone generative AIN model for generating synthetic samples. Furthermore, the generator AIN learns to generate synthetic samples without exposure to the original dataset in an adversarial fashion inspired by Generative Adversarial Networks (GANs).

This is achieved through adversarial training (with a discriminator AIN) inspired by generative adversarial networks (GANs). The GAAINet model is not trained through backpropagation, nor does it rely on artificial neural networks (ANNs). GAAINet consists of AINs, which are fundamentally unique to ANNs. Training is facilitated through immunologically inspired mechanisms such as clonal expansion, hypermutation and immune network dynamics (i.e. B Cell stimulation and suppression by neighbours).

Due to the latency requirements of IIoT environments, intrusion detector agents are deployed on edge devices to minimise the time it takes to detect intrusions. However, training takes place in the cloud due to the availability of computing resources. In addition, the ideal layer of abstraction for the proposed model is the application layer since it requires interaction with application layer technologies for training and intrusion detection.

Intrusion detector agents can leverage the nature of AINs to continuously improve and adapt over time. This is facilitated by the self-stabilizing and self-organising nature of AINs. Moreover, intrusion detector agents can share updated intrusion detection models (experience) by publishing them to the cloud. Doing so allows geographically dispersed agents to share knowledge and experiences autonomously.

GAAINet: OVERVIEW OF ARCHITECTURE

Supposed that an AIN is used as a classifier as described above. This work proposes that a generator AIN responsible for generating fake data samples can be constructed such that it learns an abstract representation of part of a latent space, which would allow it to generate examples potentially good enough to "fool" the discriminator. In order to achieve a working model, there must be an approach for training the discriminator and generator AINs. The generator and discriminator AINs are encapsulated into intelligent agents (Figure 2 and 4).

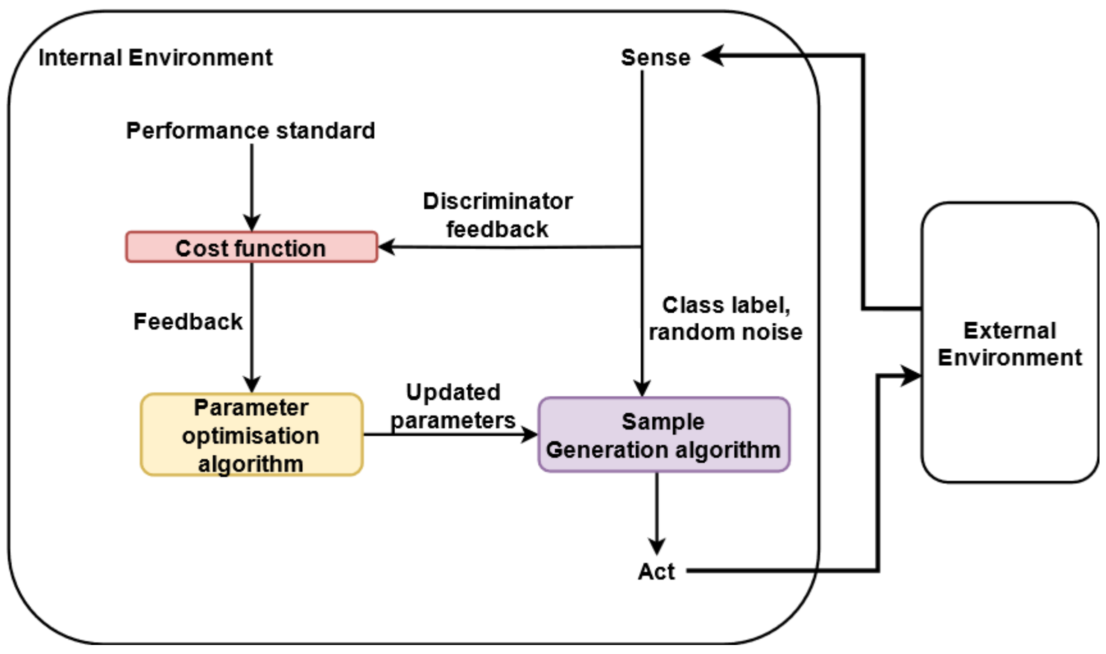

Figure 2 – Generator agent.

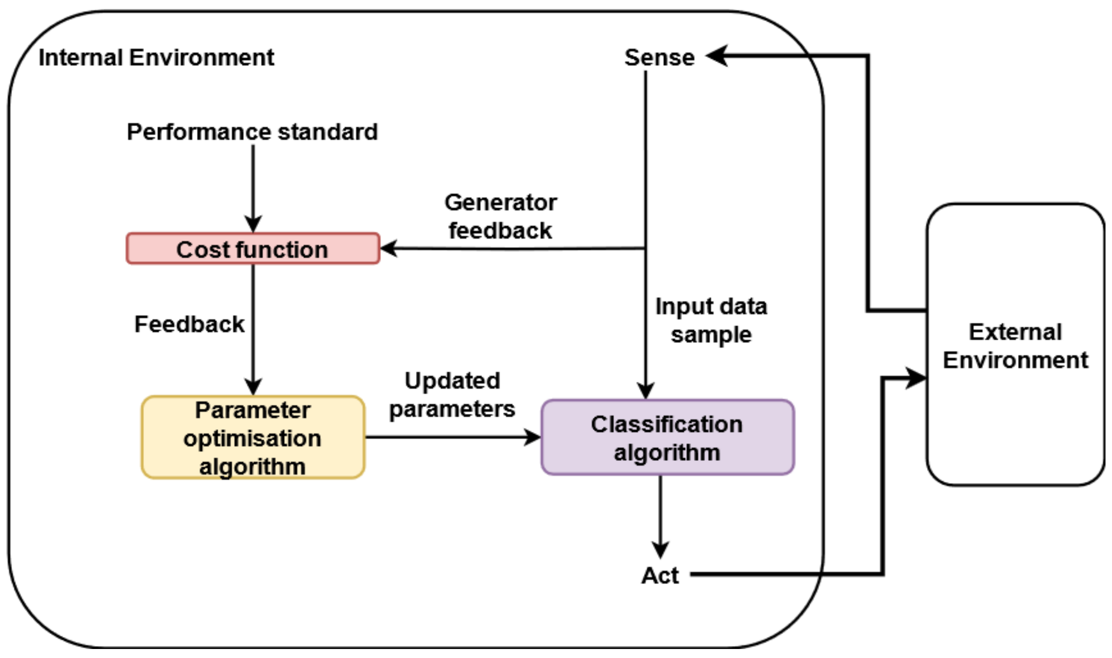

Figure 3 – Discriminator agent.

RESULTS AND CONCLUSION

A proof-of-concept prototype implementation demonstrated that the GAAINet model can be implemented in reality. The generator agent can be trained to generate synthetic samples for multiple datasets. In addition, the AIN intrusion detector was able to achieve state-of-the-art performance on intrusion detection.

REFERENCES

Jaidka, H., Sharma, N. & Singh, R., 2020, "Evolution of iot to iiot: Applications & challenges," Available at SSRN 3603739.

Figueroa-Lorenzo, S., Añorga, J. & Arrizabalaga, S., 2020, "A Survey of IIoT Protocols: A Measure of Vulnerability Risk Analysis Based on CVSS*," ACM Comput. Surv., 53(2).*

Belenko, V., Chernenko, V., Kalinin, M. & Krundyshev, V., 2018, "Evaluation of GAN Applicability for Intrusion Detection in Self-Organizing Networks of Cyber Physical Systems," *2018 International Russian Automation Conference (RusAutoCon), 1–7.*