Developing Machine Learning-based Intrusion Detection Systems for Realistic IoT Systems

Summary

Machine learning-based intrusion detection has constituted one of the critical defences against cyber attacks, which requires huge adaptation to IoT systems. It is important to run the detection models on resource-constrained devices. When distinct learning models are developed for profiling specific device types, such models should be managed in the target IoT architecture. Transfer learning can be applied across different device types to minimize the burden of dealing with many models. The expectation from this position is to realize a complete machine learning-based solution that runs on a realistic IoT system. Smart city applications will be the primary target domain.

Research field:	Information and communication technology
Supervisors:	Prof. Dr. Sadok Ben Yahia Dr. Ants Torim
Availability:	This position is available.
Offered by:	School of Information Technologies Department of Software Science
Application deadline:	Applications are accepted between October 01, 2022 00:00 and October 23, 2022 23:59 (Europe/Zurich)

Description

IoT technologies have been increasingly incorporated into various application areas such as city management, transportation, energy, and health. The interaction of the field devices (i.e., sensors, actuators) with physical space initiates various complex data flows between these devices and edge networks/cloud systems. Using IoT systems, the malicious actors may resort to various cyber-attack techniques to induce physical harm to the victims. Therefore, it is imperative to design security functions and embed them into the relevant system assets. Intrusion detection has constituted one of the critical defensive functions as it enables identifying attacks as early as possible to pave the way for appropriate counteractions. As the malicious actors change their attack techniques in time, intrusion detection systems should adapt to those newly-evolved attacks.

A huge body of research demonstrated that machine learning could be applied to detecting cyber attacks [1]. It is highly needed to adapt these solutions to IoT environments. Although various studies have obtained high detection results [2]–[4] on some IoT intrusion datasets, they do not demonstrate the actual performance of the detection systems in realistic IoT systems. Besides the detection accuracy, it is crucial to establish automatic data pipelines that convert the raw system activity to model features and run the relevant detection models on resource-constrained devices. A system design may delegate some detection tasks to edge devices or cloud systems to utilize the resources efficiently. When distinct learning models (e.g., anomaly detection models) are developed for profiling specific device types, such models should be managed in the target IoT architecture. Transfer learning can be applied across different device types to minimize the burden of dealing with many models. In applications with privacy needs, federated learning can be adapted to reach a common model without sharing the whole data.

The expectation from this position is to realize and benchmark a complete machine learning-based analytical solution that runs on a realistic IoT system. Smart city applications will be the primary target domain.

Supervisors:

Main supervisor: Dr. Ants Torim
Co-supervisor: Prof. Dr. Sadok Ben Yahia

Support for Teaching and Supervising Activities

The candidate will take part in developing courses and supervising M.Sc. students regarding machine learning and its application to cyber security problems

Candidate's Background and Knowledge

Candidates must have a M.Sc. in computer engineering or related fields. This position requires a solid background in data analytics and machine learning concepts. An experience with IoT systems or familiarity with cyber security concepts is a plus.

References

[1] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surv. tutorials*, vol. 18, no. 2, pp. 1153–1176, 2015.

[2] Y. Meidan *et al.*, "N-baiot—network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, 2018.

[3] H. Bahşi, S. Nõmm, and F. B. La Torre, "Dimensionality reduction for machine learning-based IoT botnet detection," in *2018 15th International Conference on Control, Automation, Robotics and Vision (ICARCV)*, 2018, pp. 1857–1862.

[4] S. Nõmm and H. Bahşi, "Unsupervised anomaly-based botnet detection in IoT networks," in *2018 17th IEEE international conference on machine learning and applications (ICMLA)*, 2018, pp. 1048–1053.

To get more information or to apply online, visit https://taltech.glowbase.com/positions/596 or scan the the code on the left with your smartphone.