AI Adversarial approaches for maritime cybersecurity

Summary

Computer systems security is a struggle between attackers and defenders. Attacker and defender's actions are "intelligent", and they leverage on AI. Adversarial techniques are used to improve the resilience of defensive tools, by mimicking the attacker's adaptation. The aim of this thesis is to develop adversarial technique for maritime context.

Research field:	Information and communication technology
Supervisors:	Prof. Dr. Olaf Manuel Maennel Prof. Dr. Mohammad Reza Kave Salamatian
Availability:	This position is available.
Offered by:	Tallinn University of Technology Estonian Maritime Academy
Application deadline:	Applications are accepted between November 15, 2021 00:00 and December 15, 2021 23:59 (Europe/Zurich)

Description

Security of computer systems is an intrinsic struggle between attacker and defender. The attacker wishes to exploit vulnerabilities in the system, while the defender tries to counter the attacker's actions. Computer systems are complex artefacts with a large variety of components that are the playground of attacker and defender. Both attacker and defender increasingly leverage AI to monitor, detect, and manage the complexity of their tasks.

There are 5 interrelated frameworks for the use of AI in cybersecurity:

1. Static defensive AI
2. Static offensive AI
3. Defense considering dynamic AI based attacks
4. Attack considering dynamic AI based defense
5. Adaptive defensive and offensive dynamic AI

In this thesis we target the third and fourth frameworks that are assuming that the opponent can change and adapt their actions. In this context, adversarial techniques have been developed to improve robustness of defensive tools, by mimicking the attacker's adaptation. In these approaches, an AI system is calibrated to iteratively generate challenges and evolves by learning what is not well detected by the opponent.

In particular, we will investigate how an attacker can exploit their knowledge of the ML approaches used to defend a system in order to evade detection, and develop a game theoretic setting to design methods to counter such attacks in an adversarial setting. The study of adversarial system will heavily leverage on neural networks approaches and will targeted applications domains relative to maritime cybersecurity.

Supervisor: Prof. Dr. Mohammad Reza Kave Salamatian
Co-supervisor: Prof. Dr. Olaf Maennel

Applicants should fulfil the following requirements:

The applicant for the position must have a Master's degree and must fulfil the requirements for doctoral students at the Tallinn University of Technology. In addition, a competitive candidate for this role should demonstrate the following qualifications:

- A degree in computer science, or electrical engineering, or telecommunications, or mathematics another closely-related discipline.
- High level of interest on the topic.
- Good writing and communication skills, in particular in English language.

A lack of experience in the above skills could be compensated by evidence of research potential.

Appropriate training will be provided.

To get more information or to apply online, visit https://taltech.glowbase.com/positions/478 or scan the the code on the left with your smartphone.