Title:

“Towards a secure 5G and beyond vehicular network”

Context:

The last decade has seen to the emergence of increasingly sophisticated cyber-attacks targeting different network layers. Indeed, cyber threats and sources for vulnerabilities keep increasing. As a result, many organizations are now relying on the automation of security services based on machine learning and artificial intelligence techniques. This automation is necessary to, on the one hand, rapidly process and analyze huge amount of data on security beaches and detected anomalies. On the other hand, integration automated response is vital for effectively deployment of mitigation measures in order to deal with the various threats. There is therefore an obvious need to automate security measures, particularly in highly evolving environments such as 5G ecosystems, in order to adapt and adjust to real time changes in context. While these rapid changes in context are introducing new vulnerabilities, it is highly imperative and foremost important for cyber security experts to have intelligent responsive security measures in order to adapt mitigation measures to the nature of threats, without sacrificing QoS for legitimate users. One of the most prominent solutions lays in intrusion and anomaly detection/prevention schemes.

The deployment and management of solutions for the detection and prevention of anomalies are very complex in nature, especially in a V2X network in a 5G context. Thus, an effective solution requiring the convergence of several different and complementary expertise. In addition, the applied security policies depend highly to the provided service, application domain, and the physical nature of the underlying system. Undeniably, machine learning and deep learning techniques can improve the performance of an IDS by learning from past experiences without human intervention. Furthermore, IA-based solutions have shown promising results in addressing security challenges and concerns. Such solutions would integrate built-in security modules and services that combine enforcement and monitoring functions within the network infrastructure design.

Objectives:

This Phd proposal focuses on the study of cyber security and privacy related problems following the deployment of connected and autonomous cars in the context of 5G network and beyond. One of the subsequent challenges would be the deployment and integration of automated mitigation techniques along with classical security measures in order to address the new security concerns related to the highly evolving real-time nature of 5G enhanced vehicular network. The other major question that this project would tackle is using IA and machine learning techniques to provide adaptive security measures along with early detection of cyber threats and prominent attacks. Learning algorithms enhance the performance of an IDS through learning from past experiences without human intervention. A variety of machine learning algorithms would be investigated and explored for an IDS application.

This PhD is open for hiring in the area of Computer science. We are looking for applicants with a proven experience in applied machine learning and cybersecurity. The PhD student will be supervised by Pr. Sidi-Mohammed SENOUCI. (http://www.senouci.net)

Required Qualifications:

- An MSc degree (or equivalent) in Computer Science/Electrical and Computer Engineering related to the areas listed above.
- Relevant programming skills (C/C++, python, …)
- English writing and verbal skills.

Desirable Qualifications:

- Background in machine learning and artificial neural networks.
- Background in cybersecurity (IDS, encryption, authentication, etc.).
- Background in mobile networks (3G/4G/5G)

Submission details:

The following documents are required (CV, Motivation letter, transcripts of University transcripts and reference letters). Send them as attachments of an email, whose subject will be "Application for PhD position University of Bourgogne", which must be addressed to Sidi Mohammed Senouci (sidi-mohammed.senouci@u-bourgogne.fr).