Contribution ID: **166** Type: **Talk**

Cyber Physical Systems Security Using CPS-IoT Surveillance

Thursday, 1 December 2022 12:25 (20 minutes)

Cyber-Physical Systems (CPS) [1] are key building blocks of the fourth industrial revolution. They consist of ICT systems that are embedded in the physical objects we manipulate daily, as well as in our environment to provide an interface to the physical world. It is predicted that with the advances made in the Internet-of-Things, Next Generation Networking, Cloud computing and Artificial Intelligence, hundreds of thousands of islands of CPS which are currently geographically distributed in different countries and regions worldwide, will be federated to generate unprecedent datasets, which when submitted to emerging artificial intelligence (e.g. machine learning) models, will provide solutions to some of the key problems that the world could not solve till today. However, unlike traditional IT systems, CPS include a physical space and a cyber space and both need to be protected to avoid heavy economic damages and human lives losses resulting from potential cyber-attacks. On the other hand, recent literature on cybercrimes has revealed that the CPS-IoT, a key element of the CPS that manages its physical space, is the component which is most targeted by attackers to compromise the CPS operation through the IoT nodes. However, owing to their lightweight nature, the IoT nodes are often capable of implementing only limited security functions while IoT gateways are more powerful devices capable of implementing advanced security functions. Building upon this assumption, this talk revisits the issue of CPS security to propose a novel security model where computational resources are availed by IoT gateway devices to achieve "CPS-IoT surveillance" with the objective of detecting attacks launched on the CPS [5]. The proposed security model include i) a "Topology Replication Process" for detecting topology attacks and ii) a "Traffic Classification Model" using machine learning techniques to detect and classify traffic attacks. These two models can be used to detect topology and traffic attacks launched against two of the most widely IoT protocols, namely RPL and MQTT, as well as the least interference beaconing protocol (LIBP) [2,3,4,5] protocol

[1] Bagula A, Ajayi O, Maluleke H. Cyber physical systems dependability using cps-iot monitoring. Sensors. 2021 Apr 14;21(8):2761.

[2] A. Bagula, D. Djenouri, E. M. B. Karbab. Ubiquitous sensor network management: The least interference beaconing model. In proceedings of the 2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Pages 2352-2356, 2013.

[3] Antoine Bagula. Hybrid traffic engineering: the least path interference algorithm. In Proceedings of the SAICSIT 2004 Conference, Pages 89-96, 2004.

[4] A. Bagula and Z. Erasmus, IoT emulation with cooja, ICTP-IoT workshop, Trieste-Italy 2015.

[5] A. Bagula, L. Mbala & O. Ajayi. Cyber Physical Systems Using CPS-IoT Surveilleance. ISAT Technical Report, Tech-Report-03-October2022.

Primary author: BAGULA, Bigomokero Antoine (University of the Western Cape)

Presenter: BAGULA, Bigomokero Antoine (University of the Western Cape)

Session Classification: DIRISA

Track Classification: DIRISA