Network
securité-IIOT

Postdoc
2023

Cybersecurity and Anomaly Detection in the Industrial Internet of Things

Lieu	Networks research team, ICube (UMR CNRS 7357)
Supervisor	Fabrice Theoleyre (fabrice.theoleyre@cnrs.fr)

Mots-clés

Cybersecurity ; Anomaly Detection ; attacks ; Industrial Internet of Things ; Predictions ;

Context

We are looking for an excellent, motivated, post-doctoral researcher to work in the area of cybersecurity and wireless networking. The position is available for one plus one year after a successful review evaluation. The post-doctoral fellow shall be involved in the supervision of PhD and master students, and will be fully integrated in the networks research team @ICube.

The Industrial Internet of Things is now highly popular, both in the academic and industrial worlds. Small devices are connected to the Internet, and need to save their energy by optimizing the radio transmissions [1]. Industrial environments are complex, very noisy, and time-evolving. In these conditions, providing high reliability is a major challenge [2].

While IoT is a key enabler for Industry 4.0, we have to provide the same level of trust / security :
— measure the efficiency of the network. A collection of Service Level Objectives (SLO) are commonly defined for critical applications [3] ;
— identify unexpected behaviors. These anomalies [4] may come from e.g., an attack [5], a configuration error, or a time-variant characteristic ;

Skills

The candidate has ideally :
— A PhD degree in Electrical or Computer Engineering, Computer Science, or a related discipline ;
— strong skills in wireless networking (protocols and algorithms) ;
— good knowledge in machine learning ;
— willingness to deploy prototypes, conduct real experiments in our testbed, collect measurements ;
— Excellent writing, communication and presentation skills in English ;
— Strong coding skills in Python, and C.

Remuneration

3,186€ gross salary / month

Application

Please send to fabrice.theoleyre+postdoc@cnrs.fr :
— a detailed CV ;
— the list of your publications ;
— an estimated date for your PhD defense (if not yet defended) ;
— a cover letter.

Références

[1] V. C. Gungor and G. P. Hancke. Industrial wireless sensor networks : Challenges, design principles, and technical approaches. IEEE Transactions on Industrial Electronics, 56(10) :4258–4265, Oct 2009.

[2] Maria Rita Palattella, Nicola Accettura, Xavier Vilajosana, Thomas Watteyne, Luigi Alfredo Grieco, Gennaro Boggia, and Mischa Dohler. Standardized Protocol Stack for the Internet of (Important) Things. IEEE Communications Surveys & Tutorials, 15(3) :1389–1406, 2013.

[3] Guillaume Gaillard, Dominique Barthel, Fabrice Theoleyre, and Fabrice Valois. Service level agreements for wireless sensor networks : A wsn operator's point of view. In 2014 IEEE Network Operations and Management Symposium (NOMS), pages 1–8, 2014.

[4] Xiaodan Yan, Yang Xu, Xiaofei Xing, Baojiang Cui, Zihao Guo, and Taibiao Guo. Trustworthy network anomaly detection based on an adaptive learning rate and momentum in iiot. IEEE Transactions on Industrial Informatics, 16(9) :6182–6192, 2020.

[5] Keping Yu, Liang Tan, Shahid Mumtaz, Saba Al-Rubaye, Anwer Al-Dulaimi, Ali Kashif Bashir, and Farrukh Aslam Khan. Securing critical infrastructures : Deep-learning-based threat detection in iiot. IEEE Communications Magazine, 59(10) :76–82, 2021.