Title: Multi-agent trust management for the Web of Things

Supervisors: Laurent Vercouter (LITIS, Rouen), Jean-Paul Jamont (LCIS, Valence)

Duration: 6 months

Salary: about 500 euros per month

Context:

The master internship is part of the ANR MaestrIoT (*Multi-Agent Trust Decision Process for the Internet of Things*) project which will start in January 2022. **It may continue as a thesis funded by the project from October 2022**.

The main objective of the MaestrIoT project is to develop an algorithmic framework for ensuring trust in a multi-agent system handling sensors and actuators of a cyber-physical environment. Trust management [1] has to be ensured from the perception to decision making and integrating the exchange of information between WoT devices. The MaestrIoT framework will cover three aspects: (i) definition and recognition of security contexts to evaluate the risks associated to data coming from an agent's own sensors and from other agents; (ii) definition of a trust management system integrating these security contexts to build and share trust assessments; (iii) sequential decision making processes adapted to information having various trust assessments. MaestrIoT will consider two privileged application domains: Industry 4.0 and Connected Cooperative Automated Mobility.

Work description for the master internship:

When applied to a web of things, implementing a trust management system raises new challenges requiring the development of new models and algorithms. Yan et al [2] point out that to have a trustworthy IoT, a trust management system must cover several aspects. It has to allow each entity to evaluate and decide the level of trust for neighboring entities. The way data is perceived, as well as the way it is transmitted and merged, must also be taken into account. Additionally, trust should be ensured in privacy preservation and during interactions with human users. At last, an original point is that the identity of entities is not necessarily ensured if the implementation of a robust authentication mechanism is not realistic [3]. This challenges a strong assumption of existing trust management models that use to attach trust values to identities. A new approach for trust management systems in IoT is therefore needed to realistically meet these constraints.

The expected work is to define and **develop a decentralized multi-level trust management system adapted to the IoT specificities**. The system will have to consider two levels as different targets will be considered: the agent's own sensors/actuators, and other agents. The work will have a theoretical part in the definition of the models and a practical part for experimentation on the platforms of the MaestrIoT project for which the use of trust management is not yet common [4] and/or has shortcomings [5]. The proposal may be based on the exploitation of work in progress that will be used in the project [6].

[1] J. Sabater-Mir, and L. Vercouter (2013). Trust and reputation in multiagent systems. Multiagent systems, 381.
[2] Z. Yan, P. Zhang, and A. V. Vasilakos. "A survey on trust management for Internet of Things". In: Journal of Network and Computer Applications 42 (2014), pp. 120–134. issn: 1084-8045. doi: https://doi.org/10.1016/j.jnca.2014.01.014.
[3] L. Vercouter and J.-P. Jamont. "Lightweight trusted routing for Wireless Sensor Networks". In: Progress in Artificial Intelligence 1.2 (Apr. 2012), pp. 193–202.
[4] Boudagdigue, C., Benslimane, A., Kobbane, A., Liu, J. . Trust management in industrial Internet of Things. IEEE Transactions on Information Forensics and Security, 15, 3667-3682, 2020.
[5] Hussain, R., Lee, J., Zeadally, S. (2020). Trust in VANET: A survey of current solutions and future research opportunities. IEEE transactions on intelligent transportation systems, 22(5), 2553-2571.
[6] Liévin, R., Jamont, J. P., Hély, D. (2021). CLASA: a Cross-Layer Agent Security Architecture for networked embedded systems. In 2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS) (pp. 1-8). IEEE.