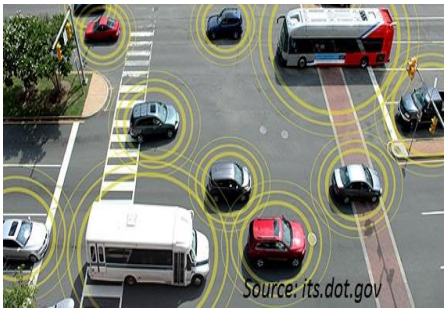
Post-Doc Research Proposal

System Theory Approach for Privacy preserving Cyberphysical systems

Advisors: Alain KIBANGOU and Hassen FOURATI
E-mail: alain.kibangou@gipsa-lab.fr
Team: NeCS (http://necs.inrialpes.fr)

Start: September 2016 Duration: 12 M
Candidate profile: Strong skills in Systems theory, optimization, and nonlinear filtering are required.

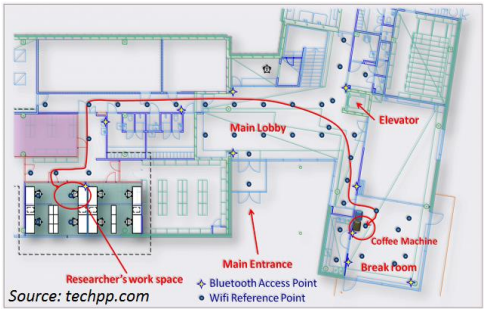
Context: NeCS is a joint Inria-GIPSA-Lab (Université Grenoble Alpes-CNRS) team. It is bi-located at INRIA (Montbonnot) and at the GIPSA-Lab (Grenoble main campus). This work will be achieved in the framework of a ProCyPhys, a project funded by the University Grenoble Alpes.



Topic description: For safer and less congested cities, ICTs offer a huge scope of services. These services involve users, physical infrastructures, and communication and computing tools. The success of such services depend on the quantity and the quality of the information obtained from users. However, users do not generally want to disclose their personal information but nonetheless hope to have efficient services. The proliferation of information sources and the use of communication networks increase the risk of privacy violation. One can think that it would suffice to overprotect the transmission of information between users and managers of cyber-physical systems by encrypting communications for example. It has been shown that by overlapping anonymous information from different sources, it is possible to recover the hidden information [Sweeney, 2002 ; Narayanan and Shmatikov, 2008]. However, this approach is not well indicated for time series resulting from dynamical systems.

In this project, we are interested with cyber-physical systems that can be viewed as systems of interconnected entities which are locally governed by difference equations of partial differential equations, namely intelligent transportation systems and indoor navigation. We adopt an analysis from a system theory point of view.

A first approach to analyze privacy preservation is to study observability of the overall system, see [Kibangou and Commault, 2014] where a large family of non-observable networks have been characterized for homogeneous systems of consensus type. In this approach, the network structure immunizes the overall system. However, such results are restricted to some specific families of networks and limited types of dynamics [Parlangeli and Notarstefano, 2012 ; O'Cleary et al. 2013]. A second approach, consists in adding information (noise) to the sensitive one: that is the differential privacy concept that leads to differential filtering where the aim is to develop an estimator that is robust enough according to the added noise [Le Ny and Papas, 2014].



In this project, the main goal is to make the system partially non-observable. The idea is to compress the state space while adding noise to the sensitive information in a smarter way. Due to state compression, the system becomes singular. The main challenge of this project is to synthesize the compression matrix and the noise sequence so that only the non-sensitive information belong to the observability subspace. Such a synthesis should be carried out in a distributed way. We will resort to low rank approximation tools and to distributed optimization techniques. Unlike standard low rank approximation problem we must guaranty a quality of estimation. For instance, the system must be able to provide a reliable estimation of the average speed in a transportation network while protecting the precise locations of the vehicles participating in the estimation process.

The obtained results will be validated using data from Grenoble city generated by the simulator developed by the team (http://necs.inrialpes.fr/pages/grenoble-traffic-lab.php). For indoor navigation, the MOCA experimental platform (http://www.gipsa-lab.grenoble-inp.fr/recherche/plates-formes.php?id_plateforme=79) at GIPSA-Lab will be used to collect data.

References:

S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, "Distributed optimization and statistical learning via the alternating direction method of multipliers", *Foundations and trends in Machine Learning*, vol. 3, No. 1, 2010.

B. Hoh, T. Iwuchukwu, Q. Jacobson, M. Gruteser, A. Bayen, J.-C. Herrera, R. Herring, D. Work, M. Annavaram, and J. Ban, "Enhancing privacy and accuracy in probe vehicle based traffic monitoring via virtual trip lines," *IEEE Trans. on Mobile Computing*, vol. 11, no. 5, May 2012.

A.Y Kibangou and C. Commault, "Observability in connected strongly regular graphs and distance regular graphs", *IEEE Trans. on Control of Network Systems*, vol. 1, no 4, Dec. 2014, pp. 360-369.

A.Y. Kibangou and A. Monin, "GPS based Land Vehicle positioning using Gaussian Sum Filters" *Proc. ICASSP 2008*, Las vegas, USA, pp. 3653-3656.

Le Ny and G. Pappas, "Differentially private filtering", *IEEE Trans. on Automatic Control*, vol. 59, no. 2, Feb. 2014, pp. 341-354.

A. Makni, A.Y. Kibangou, H. Fourati, and J. Dumon, "Descriptor approach for attitude estimation", *IEEE Multi-conference on Systems and Control*, 2015, Sydney, Australia.

A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets (how to break anonymity of the Netflix Prize dataset)," *in Proceedings of the IEEE Symposium on Security and Privacy*, 2008.

N. O'Cleary, Y. Yuan, G.-B. Stan, and M. Barahona, "Observability and coarse graining of consensus dynamics through the external quitable partition," *Physical Review E,* vol. 88, pp. 1-42, 2013.

B. A. Olshausen and D. J. Field. Sparse coding with an overcomplete basis set: A strategy employed by V1? *Vision Research*, vol. 37, no. 23, pp.3311–3325, Dec. 1997.

G. Parlangeli and G. Notarstefano, "On the reachability and observability of path and cycle graphs," *IEEE Trans. Automatic Control*, vol. 57, no. 3, pp. 743–748, Mar. 2012.

L. Sweeney, "k-anonymity : A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 5, pp. 557–570, 2002.