Network automation: opportunities for Industrial Internet of Things
Jean-Philippe Georges

To cite this version:
Jean-Philippe Georges. Network automation: opportunities for Industrial Internet of Things. 2019. hal-02419104

HAL Id: hal-02419104
https://hal.science/hal-02419104
Submitted on 19 Dec 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Network automation: opportunities for Industrial Internet of Things

IFAC Blog

Dr. Jean-Philippe GEORGES
VC TC 3.3 Telematics: Control via Communication Networks
Université de Lorraine, CNRS, CRAN, F-54000, Nancy, France
jean-philippe.georges@univ-lorraine.fr
July 22, 2019

TC 3.3 – Telematics: Control via Communication Networks – (from CC3 – Computers, Cognition and Communication) leads attempts to strengthen the synergy of sound control theory and automation/information technology (with engineering and software for implementation). Remote control applications benefit from increasing capabilities among others in telecommunication and machine-to-machine communication. The 5th IFAC Symposium on Telematics Applications\(^1\) to be organized in September 25-27, 2019, in Chengdu, China will gather the recent research and application of telematics, enlarged with the concepts of Cyber Physical Systems, Industrial Internet and of Internet of Things. Telecommunications, and networks in wide-sense, are playing a core role in the support of networked control systems and cyber physical systems. Considering the advances in Internet of Things and Industrial Internet, they are even facing new challenges and require the definition of new control strategies. The issue is to develop networks capable of reconfiguring themselves more efficiently, whether in terms of Quality of Service, spatial and temporal constraints or dependability. It corresponds to the advent of the concept of network automation or software-defined networking and could be seen as a new evolution of control of the network.

1 Network automation

Network automation might be introduced where networks parameters (like routing or scheduling) are dynamically configured and algorithms are orchestrated in order to match the QoC requirements. A special attention has been paid regarding the orthogonal experience needs and objectives between end users and network providers. To ensure that the full architecture (network, computing, storage) will be able to support flexibility and dynamics reconfigurations will require facilities (network automation) and guarantees (performance evaluation)

\(^1\)https://ifactelematics2019.swjtu.edu.cn
whatever it would be achieved through centralised or distributed algorithms. In fact, it is on the trend of Roberto Saracco’s future vision for 2030-2050 of 6G:

6G networks will embed planning into the network itself, meaning that the network will become aware of the way it is being used, what is actually required by its users at this specific moment and what it is likely to be required at a later time and it will be able to plan for its evolution by reconfiguring its resources and by “asking” vested parties to provide additional resources coming up with a convincing reason and a convincing business plan.

This renewed interest of network automation is engaging since it comes over the years after that full-integrated protocols like ATM (with a full support of the QoS support and the control, data, management planes) were forsaken for the benefit of the basic (best-effort) IP. During the last decades and complementary to over-provisioning techniques, efforts have been pushed to add tricks over IP to retrieve QoS support. However it has lead to unsound architectures that suffer from a non native understanding of the network management over the layers. The recent development have reemphasised the needs for (centralised) automatic control. It is based on the framework of Software-Defined Networking (SDN) that is defined, by Open Network Foundation (ONF), as a new network architecture where the network control, directly programmable, is separated from the data plane. It is based on software for implementations and algorithms such that it may leads to full-autonomic network management (reaching the concept of Intelligent-Defined Networking).

Figure 1: Evolution of network management

The purpose of SDN is hence to abstract the network in order to simplify its use and its configuration. Preliminary research has thus focused on SDN as an enabler for industrial control and production engineering [1] and spatial launchers as well [4]. We are not looking for a single protocol stack, but instead,
for (centralised or distributed) algorithms that will both evaluate the overall performance of the networked systems and support automatic reconfigurations of the architecture regarding the users/providers’ needs. The change is even more deep since it will require more engineering for graduates students and it will led to software robots for configuring network devices (whereas it might be still achieved by technicians, device per device). And it is above all the role of the IFAC community to take the lead in these necessary efforts. We are here convinced that control and network specialists should work together early in the design at it occurs in the past with the networked control systems research field.

2 Industrial Internet of Things

One of the current move in network architecture is related to the support of Internet of Things (IoT). It is an important topic since networks are here one of the foundation to develop smart things (Global e-Sustainability Initiative (GeSI) SMARTer 2030 report) and Future Internet, Industry 4.0 or Industrial Internet (of Things). Generally speaking, it is related to the digital transformation of industrial process. It encompasses national (as well as European and international) Future Industry efforts and in AI as novel business plans for Internet actors like Cisco.

It is interesting to note here that it has reached sectors traditionally poor in automation technology like mining. It was one of outcome of the doctoral course for future automation systems in context of process systems and minerals engineering (MIDICON 2018) organized by Aalto University in 2018. 5G and data analytics techniques start to be used here in mine to support remote control and vehicle traffic control.

Industrial automation will use more and more the IIoT networks (we are gathering here the notion of Industrial Internet, Machine-to-Machine, Internet of Everything, embedded Internet, Web of Things, Smart Things). The idea is not here to work on the usage of IoT (and even to rethink factories, grid, logistics), but to work on the core of IoT itself, since it faces challenges that let future usages probably unsure. It is interesting to note that the notion of IoT is even not well defined. We can mention from IEEE “A network of items—each embedded with sensors—which are connected to the Internet”, from ETSI “Machine-to-Machine (M2M) communications is the communication between two or more entities that do not necessarily need any direct human intervention. M2M services intend to automate decision and communication processes” and from ITU “Available anywhere, anytime, by anything and anyone”.

Industrial networks have been through different battles (or even fieldbus war – IEC 61158/61784, 62439 and ARINC 664 – [3] and more recently, industrial Ethernet war [2]). In wired local area networks, the trend is the study of the so-called Time-Sensitive Networking (TSN) that gathers several stan-
standards (IEEE 802.1AB, AS, ASbt, AQ, CB, Qca, Qaz, Qat, Qav, Qbv, Qch, Qci, Qbn, Qcc, Qbp, Qbz, ...). The main interests of these standards is to provide actuation capabilities largely extending the control plane and hence supporting a more precise network automation. It is interesting to note that actually, a quite similar kind of battle seems to occur for wireless local area sensor networks between the de facto standard, the IEEE 802.15.4 (and its extensions IEEE 802.15-e, 6TiSCH and specifics ones like IEC 62591 (WirelessHART), IEC 62734 (ISA100.11a), and IEC 62601 (WIA-PA) or even the Wifi 802.11ah/ax amendments. Investigations about the real-time performance are still required and the challenge of exploiting network-related effects on the automation control is still going on. For wide area wired network, one may cite the ongoing standardisation activities of IETF DetNet: deterministic networking over Internet. For wireless communications, remote control is currently considering LPWAN technologies like LoRa and Sigfox as cellular technology LTE and the ongoing 5G.

Therefore, rather than focusing on a particular communication technology (wired as wireless, Ethernet TSN, 5G, etc.), it is a question of looking for algorithms enabling to tackle the interoperability between those ecosystem vendor solutions and to monitor and optimise theirs performances. A final objective could be to achieve Internet at the speed of light (as defined by ACM in 2013) or Tactile Internet network (as defined by ITU in 2014 – end-to-end latencies to 1 ms) without over-provisioning the network at least 50 percent link utilisation for deterministic traffic flows (as ruled out by IETF).

The final point deals with the deployment at data analysis (and storing) on edge and fog nodes in distributed networks rather than into the cloud as natively introduced for remote monitoring applications. As detailed in the following, it is likely that IIoT needs tools to simplify development, deployment and operation of processing storage, analytics, or any combination of micro-services and to decrease the energy usage (through optimised workflows) over the (local and external) infrastructure. The challenge is to decide where that data should go and be analysed (to power better business decisions) and it claims for the ability to apply rules to data in motion (with taking care of data ownership, privacy and security). It needs an architectural framework to extend fog processing to multiple tiers: east-west (fog to fog) and north-south (hierarchical processing leveraging network topology). It can be coupled with virtualisation in order to deploy virtual services faster and at lower cost. It aims here at automating network fabric provisioning for both virtual and physical infrastructures.

Among the different needs for IIoT infrastructures, 6 hot topics are usually mentioned. The first one consists on determining the optimal frequency (avoid unnecessary data pulls high frequency when the data will be consumed at low frequency and hence avoid network congestion). Algorithms to identify automatically the needs and to adapt the polling have to be defined as well to sleep down the network usage (think of duty cycles in wireless communications). Then, prioritisation (or classification of service) is required to ensure integrity of critical/sensitive traffic. Next, it is important to determine the right place for data processing according to the real-time and constrained data requirements. Decoupling hardware from operating systems and hardware (virtualisation) is also a huge topic since resources (processing, storing, networking) have to be

https://datatracker.ietf.org/wg/detnet/documents/
adjusted to the data requirements in order to guarantee a relevant service level. The mapping of those resources should be also orchestrated in a consistent way, aware to the machine/process control logic. Finally, it is important nowadays to be able to report online (visibility/observability) on the current operation states of the network, enabling to identify correctly the plant.

To summarise, advanced network automation (centralised or distributed) is the missing technology to bring the ability for IIoT to adapt plant floor network (provision devices for timeliness, security, reliability, scalability and deploy policies) to industrial business varying requirements (assurance and compliance), to contain costs, to decrease the infrastructure complexity, to simplify the management (0-touch deployment), to support the various protocols (converged plant network through a common control/data plane) and to enable supervision and visibility (observability) of the infrastructure state. Nevertheless, separating the design of the controllers and coders can be very sub-optimal, incurring some severe performance losses and significant additional costs. We will aim at a strong cooperation (co-design) and composability of control and network logics, since we are turning in aligning the network to operational technology and finding the best equilibrium between those.

References


