Whispering to Industrial IoT for converging multi-domain Network Programmability

Esteban Municio*, Steven Latré†, Johann M. Marquez-Barja*
*IDLab - Faculty of Applied Engineering, University of Antwerp - IMEC, Antwerp, Belgium
†IDLab - Department of Mathematics and Computer Science, University of Antwerp - IMEC, Antwerp, Belgium
{esteban.municio,steven.latre,johann.marquez-barja}@uantwerpen.be

***Abstract*—Industrial Internet of Things (IoT) calls for not only highly reliable, quasi-deterministic and low-power networks, but also for more flexible and programmable networks to cope with operator's dynamics demands. Software Defined Networking (SDN) offers the high levels of flexibility and programmability that traditional distributed protocols cannot offer. In between a fully centralized SDN-on-IoT management solution and a traditional fully distributed one, Whisper stands out as a trade-off solution that has the robustness, scalability and low-overhead of distributed solutions and the flexibility and programmability of centralized ones. In this demo we present a hands-on experience of how Whisper can be jointly used with traditional SDN solutions, such as ONOS, in order to extend the already existing network programmability in wired domains to 6TiSCH-based Industrial IoT segments. We deploy and test such architecture in real-world large-scale testbeds and demonstrate to be feasible and beneficial to provide an efficient and programmable end-to-end control over a heterogeneous network.**

***Index Terms*—IIoT, SDN, 6TiSCH, RPL, ONOS, Whisper**

I. Introduction

New advancements in Industrial IoT currently permit up to 99.999 reliability, latency of tens of milliseconds, and about a decade of battery life time, even in harsh and highly interfered environments [1]. However industrial networks also require to be flexible and programmable in order to cope with and be further tailored to the actual and dynamic industrial automation needs. This flexibility is already being provided in wired technologies through the use of SDN, and therefore, different solutions have sucessfully translated the SDN paradigm to the IoT domain [2]. However, the increase in in-band signaling overhead, and the uncoupling between the routing and scheduling layers remain as open challenges to extrapolate these solutions to the Industrial IoT. Whisper is one solution that aims to enable robust, scalable and low-overhead SDN-like capabilities in the Industrial IoT by centrally controlling the distributed routing and scheduling planes in the IoT network [3], [4].

The demo presented in this work experimentally shows how a 6TiSCH Industrial IoT network can be integrated with a traditional wired SDN architecture by using Whisper in the wireless segment. In order to do this, we show a representative use case in which end-to-end network control has to be exerted in both wireless and wired domains by a centralized entity.

Work partially funded by the EU's H2020 Fed4FIRE+ project no.723638.

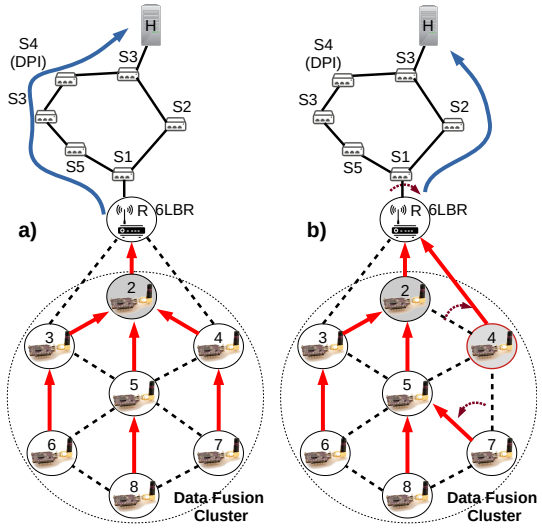

Fig. 1. In (a), the 6TiSCH network is aggregating data at node 2. In (b), network is end-to-end reconfigured to achieve lowest latency in node 4. Also, node 7's next hop is changed to continue aggregating its readings at node 2.

We use ONOS to perform network changes by user's demand in two real-world wired and wireless testbeds, reporting latency and reliability metrics for any of the resulting topologies.

II. Interconnecting Fed4FIRE testbeds for our use case

Let us assume we have a multi-domain industrial network as depicted in Figure 1. Critical sensor data (e.g., vibration level) from industrial assets are measured and centralized in node 2 to be aggregated, fused, and relayed to a Deep Packet Inspection (DPU) box located in the wired network before being stored in a local server H. In the event of abnormal readings in node 4, the operator may want to reduce the end-to-end latency for that sensor to closely monitor further anomalies and avoid possible damage. For this, the flow should be reconfigured by changing node 2's next hop in the wireless network and skipping the DPI box in the wired network.

We have deployed this use case in two geographically separated open large-scale Fed4FIRE+ federated testbed facilities [5], in Belgium (see Figure 2). First, we use the Citylab

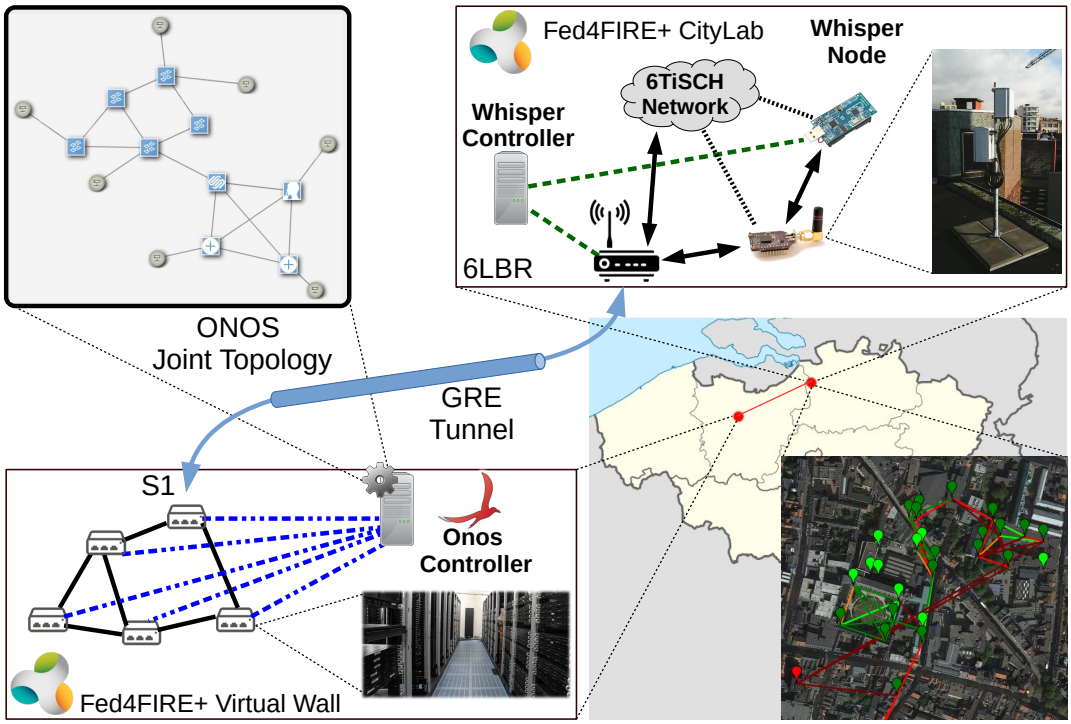

Fig. 2. Architecture of the multi-domain network deployed in two different Fed4FIRE+ testbeds to provide end to end control.

smartcity testbed [1] in Antwerp for the 6TiSCH segment, using OpenMotes-CC2538 nodes running OpenWSN Release 1.24 [2]. For the wired network and the ONOS controller, we use the Virtual Wall testbed [3] in Ghent, composed of barebone Openflow-enabled Open vSwitch 2.9 switches and a controller running a Whisper-integrated version of ONOS 2.1.0.

III. Demo

The demo consist in remotely controlling both the wired and wireless segments of both testbeds by interacting with the ONOS controller. By modifying the network topology in the ONOS dashboard, the corresponding routing and scheduling rules will be installed to modify the actual flow in both the OpenFlow-enabled wired network and the Whisper-enabled wireless network. Network state and performance metrics are gathered in real time to monitor the whole setup. For our use case, Figure 3 show the evolution of the latency for two sequential topology changes, a first change in the 6TiSCH network and subsequently a change in the wired network.

IV. Conclusion

In this demo we propose a solution to perform end-to-end control in a multi-domain industrial network. In order to jointly control the wired and 6TiSCH IoT wireless segments, we integrate Whisper, which offers robust, low-overhead SDN-like flexibility, with a traditional SDN solution. We deploy such architecture in real large-scale testbeds, demonstrating its feasibility and performance.

[1]https://www.fed4fire.eu/testbeds/citylab/

[2]Setup code available at https://github.com/imec-idlab/whisper-repository

[3]https://www.fed4fire.eu/testbeds/virtual-wall/

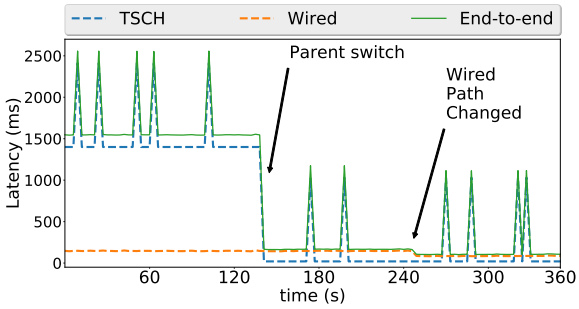

Fig. 3. Latency readings from node 4. First, a parent switch occurs in the 6TiSCH network. Secondly, the wired topology is modified as well to minimize the overall end-to-end latency.

References

[1] T. Watteyne, A. Mehta, and K. Pister, "Reliability through frequency diversity: why channel hopping makes sense," in *Proceedings of the 6th ACM symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*. ACM, 2009, pp. 116–123.

[2] S. Bera, S. Misra, and A. V. Vasilakos, "Software-defined networking for internet of things: A survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1994–2008, 2017.

[3] E. Municio, J. Marquez-Barja, S. Latré, and S. Vissicchio, "Whisper: Programmable and Flexible Control on Industrial IoT Networks," *Sensors*, vol. 18, no. 11, 2018. [Online]. Available: http://www.mdpi.com/1424-8220/18/11/4048

[4] E. Municio, N. Balemans, S. Latré, and J. M. Marquez-Barja, "Leveraging distributed protocols for full end-to-end softwarization in iot networks," in *2020 17th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2020, pp. 1–6.

[5] B. Vermeulen, W. Van de Meerssche, and T. Walcarius, "jFed toolkit, Fed4FIRE, federation," in *GENI Engineering Conference*, vol. 19, 2014.