UPIN – A shift in Network Control from operator to end user

Leonardo Boldrini[2], Rodrigo Bazo[1], Cristian Hesselman[1,3], and Paola Grosso[2]

[1]Design and Analysis of Communication Systems – University of Twente
[2]Multiscale Networked Systems – University of Amsterdam
[3]SIDN Labs

The UPIN (User-driven Path verification and control for Inter-domain Networks) project aims to increase the trust of end users in the Internet by effectively providing them with the necessary level of knowledge and control over how their traffic flows through the network. The UPIN project is a starting collaboration between the University of Twente and the University of Amsterdam and it is funded by NWO.

Currently, Internet users cannot verify nor control who processes their data when it travels across the network, for instance in terms of the service providers and network nodes that their data passes through and what jurisdictions apply. This lack of transparency and control is a risk for people's privacy (e.g., a malicious network compromising their data) and their safety (e.g., an untrusted network disrupting a remote surgery). It also increases costs, because organizations opt for setting up a "bypass network" to meet the transparency and control requirements of their applications rather than using a shared inter-network. Such problems are an increasing concern for critical service providers, such as healthcare or power supplying providers.

The goal of UPIN is to investigate methods for giving a certain degree of control over data routing to the user. We aim at achieving this through Path Control and Path Verification in both Single domain and Inter-domain networks. Other known efforts for solving the lack of control on the Internet exist, such as RINA [1] and SCION [2]. These two specific systems tackle the root of the problem, which is the current internet architecture. However, UPIN aims at a solution that can better blend into the current internet infrastructure, relying highly on Software-defined Networks (SDN).

The targeted impact is twofold: increased trust from users (individuals and organizations) in network services because they are able to verify how their data travels through the network, and more empowered users because they are able to control how their data travels through inter-domain networks, which increases self-determination, both at the level of individual users as well as at the societal level.

Traditionally, the operator has total control over the network. A first but important achievement is to find the relationship between the knowledge that users need of the network, and the control that they can have over it. Depending on the kind of control that we want to achieve, different levels of knowledge may be necessarily made transparent to the user, which may not be easy to deploy because it goes against what operators want. The way UPIN intends to accomplish this goal is by providing users with verifiable descriptions of the paths that their data took through the network and by allowing them to specify a set of required path attributes that UPIN enforces, for instance in terms of trusted network operators, geolocations of routers and application servers, and trusted router vendors.

Our novel contribution we will present at ICT.Open is the additional security the user can experience by allowing their decisions to act directly on the behaviour of the network. The architecture of UPIN introduces three main novel key components as shown in Fig. 1, showing the user's data being routed through networks according to specific operator descriptions and telemetry parameters. The first novel key component is the distributed Path Description, that is able to gather deep information on a multi domain network, the second is the Path Composition, that is responsible for translating into routing instructions

the intentions of the user, and the third is the Path Verification, which goal is to verify if everything the user asked actually happened along every node crossed in the network.

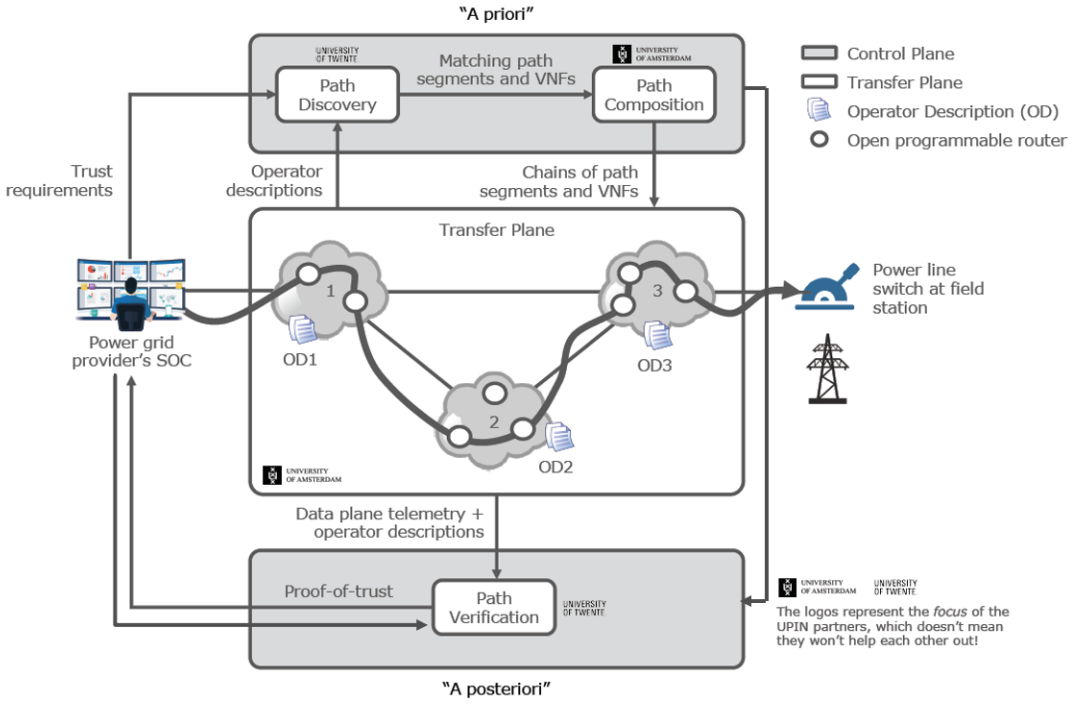

Fig. 1. The UPIN architecture.

UPIN advances the state of the art in these types of network control by combining various enabling technologies, for example, the new paradigm of Network Virtual Functions (NVF) and Segment Routing (SR). Both the IPv4 and IPv6 implementations of SR allow for the definition of a list of 'segments' that have to be traversed by the packets. In UPIN we investigate how SR can be adapted to support our use cases, and in particular we look at the integration of SR with NFV. A first research in this direction can be found in [4]. The UPIN prototype will be deployed and experimented on the 2STiC testbed [3], a national multi-domain setup of P4-programmable routers interconnected in a star-shaped optical network.

There are various challenges already encountered in this direction, as the already cited difficulty in finding a line between how much the user is interested in having control over how their traffic travels through the network, and how much information they need in order to improve it. Secondly, the idea behind the UPIN concept may not be well seen by operators who do not have intention to expose how their network is shaped. In conclusion, UPIN aims to study and analyze possibilities for managing the paths that data follows along the network, in order to empower users to achieve the level of security they want.

REFERENCES

[1] D. Barrera, L. Chuat, A. Perrig, R. M. Reischuk, and P. Szalachowski, "The SCION Internet Architecture", Communications of the ACM, Vol. 60, No. 6, June 2017.

[2] Vincenzo Maffione, Francesco Salvestrini, Eduard Grasa, Leonardo Bergesio, and Miquel Tarzan, "A software development kit to exploit RINA programmability", 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, May 2016.

[3] P. Grosso, C. Hesselman, L. Hendriks, J. Hill, R. van der Pol, V. Reijs, J. de Ruiter, C. Schutijser, and S. Konstantaras, "A National Programmable Infrastructure to Experiment with Next-Generation Networks", 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM 2021), experience track, Bordeaux, France, May 2021

[4] C. Portegies, L. Boldrini, M. Kaat, P. Grosso, "Experience with implementing VNF chains with Segment Routing and PCEP", 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM 2021), experience track, Bordeaux, France, May 2021