Dynamically Aggregating Smart Community Sensors, Edge and Cloud Resources with Overlay VPNs

Renato Figueiredo, Ken Subratie, Saumitra Aditya, Vahid Daneshmand (University of Florida, USA); **Eiji Kawai, Hiroaki Yamanaka, Naomi Terada** (NICT, Japan); **Ryousei Takano** (AIST, Japan); Susumo Date, Yamada Takuya (Osaka University, Japan); **Pongsakorn U-chupala** (NAIST, Japan); **Hyuk-Jae Lee** (Seoul National U., South Korea)

Abstract

This project is part of CENTRA in collaboration with PRAGMA, and focuses on network virtualization middleware that allows edge and cloud resources to be logically connected, on-demand, into community virtual private networks (VPNs) with:

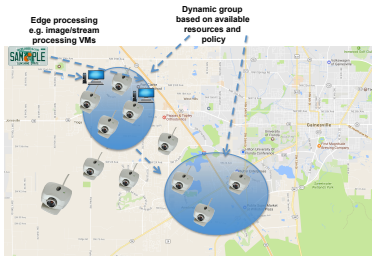
- Private IP addresses isolated from the public Internet
- Encryption of traffic between sensor/edge/cloud resources
- Peer-to-peer (P2P) overlay links for scalable communication
- Multiple different overlays on top of the physical infrastructure

Motivation and Goals

Recent technological breakthroughs enable a very large number of Internet of Things (IoT) devices, mobile/personal computers, and small-scale edge data centers to be deployed by citizens and government across a smart and connected community.

This presents new opportunities and challenges in the design of applications and middleware that can make effective use of highly-distributed edge resources, in additional to large-scale data centers at the core of cloud infrastructures.

Example use case scenarios that benefit from this model include video stream processing, where processing near cameras can reduce the data transfer requirements to a cloud infrastructure, and significantly reduce application-perceived latencies.



Future Work

Performance characterization of IoT overlay gateways

Infrastructure layer

SDN/overlay integration prototype and evaluation

Raspberry Pi, IPOP, OpenvSwitch, RISE testbed

Platform layer

Messaging, distributed stream processing (MQTT; Storm)

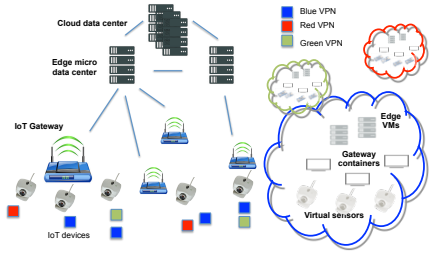
Applications layer

Image detection, target tracking, traffic control

Acknowledgements

This material is based upon work supported in part by the National Science Foundation under Grants No 1550126, 1527415, 1339737 and 1234983. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Towards an overlay/SDN hybrid architecture



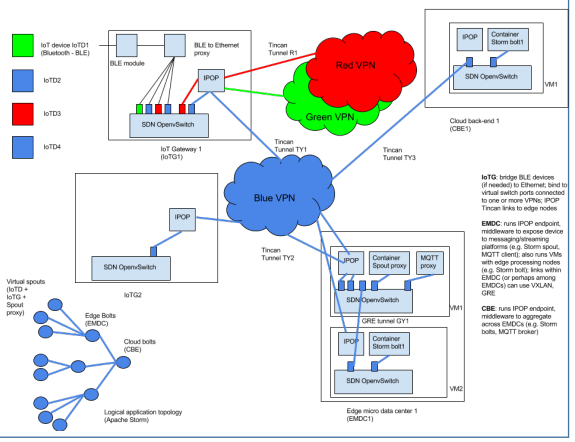
We envision an overlay network that dynamically aggregates, into the same logical virtual private network, resources including IoT gateways, VMs/ containers on edge resources near the gateways, as well as on cloud data center resources

Different user-defined virtual private networks (blue, red, green in this figure) can be deployed and managed dynamically to add/remove resources to support data processing workflows (e.g. stream processing) from sensors, to edge and cloud resources

The envisioned architecture includes SDN virtual switches (e.g. OpenvSwitch) on IoT gateways, and edge and cloud resources.

Ports in the SDN switches are connected by virtual links – overlay network tunnels with different encapsulation technologies depending on the environment and available (e.g., VXLAN within a data center; GRE across public Internet nodes; IPOP across Internet hosts behind NATs).

IoT devices bind to ports of the virtual switches at each IoT gateway, possibly with the help of a proxy (e.g. from Bluetooth Low Energy, BLE, to Ethernet)

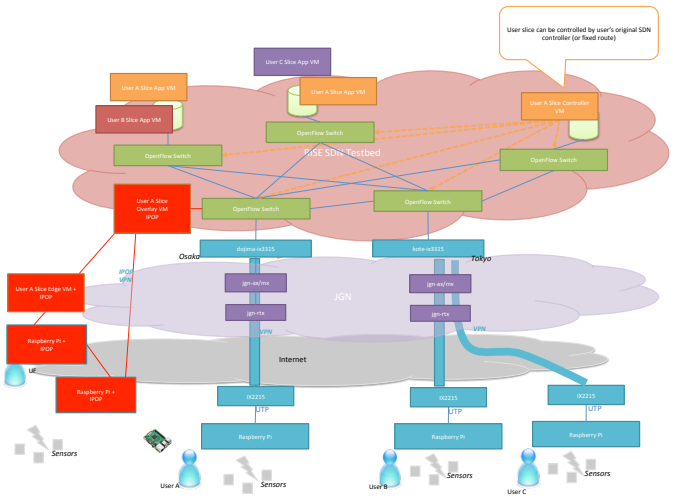


IoTG: bridge BLE devices (if needed) to Ethernet; bind to virtual switch ports connected to one or more VPNs; IPOP Tincan links to edge nodes

EMDC: runs IPOP endpoint, middleware to expose device to messaging/streaming platforms (e.g. Storm spout, MQTT client); also runs VMs with edge processing nodes (e.g. Storm bolt); links within EMDC (or perhaps among EMDCs) can use VXLAN, GRE

CBE: runs IPOP endpoint, middleware to aggregate across EMDCs (e.g. Storm bolts, MQTT broker)

Work in progress: Testbed



The team is collaborating on a testbed to prototype and evaluate system software, middleware, and applications

The testbed will include virtualized resources from the RISE SDN testbed, and external Raspberry Pi sensors and IoT gateways connected via different networking technologies (IPSEC, IPOP VPNs)