Technical Disclosure Commons

Defensive Publications Series

March 2020

SECURE AND FULLY TRANSPARENT ROAMING FOR LONG RANGE

Marcelo Yannuzzi

Carlos M. Pignataro

Bart Brinckman

SECURE AND FULLY TRANSPARENT ROAMING FOR LONG RANGE

AUTHORS:

Marcelo Yannuzzi
Carlos M. Pignataro
Bart Brinckman

ABSTRACT

Roaming with Long Range wide-area network (LoRaWAN) requires connections to home Network Servers (hNS), serving Network Servers (sNS) and forwarding Network Servers (fNS) across LoRa domains. Today, this entails a tedious manual process for generating the keys, certificates and configuration files to connect these servers on a peer-to-peer basis. This means that manual configurations grow quadratically with the number of LoRa networks involved. In addition, today there is no way to enable roaming across LoRa networks dynamically (i.e., not if these pre-configurations among the visited and the home/serving LoRa networks aren't in place). Accordingly, presented herein are techniques to scale LoRaWAN roaming linearly, while not only automating the entire roaming process, but also allowing the acceptance of dynamic roaming requests. Opposite to conventional arrangements, such as roaming hubs, where roaming partners need to adhere to the hub's rules for packet routing, service levels and trust, the techniques presented herein act transparently to the servers, keeping routing and data exchanges under the control of each peer.

DETAILED DESCRIPTION

The market shows that wireless technologies such as Wi-Fi®, private Long Term Evolution (LTE) (e.g., Citizens Broadband Radio Systems (CBRS)), public LTE, LPWAN and 5G will need to coexist in enterprise environments, as there is no one-size-fits-all winner—Wi-Fi® is a registered trademark of the Wi-Fi Alliance. This is mainly driven by the expansion of the Internet of Things (IoT) networks, which is progressively changing business segments such as supply chain, port operations, manufacturing, warehouses and transportation. These segments are seeking affordable solutions leveraging the benefits and operational cost of different licensed and unlicensed radios. That is, the wireless networks to be deployed in those segments will be heterogeneous in nature, and will need to be prepared to seamlessly combine various matrices of

access technologies and roaming scenarios. The capacity to locate and onboard assets on the move and provide visibility and predictability in real-time for decision makers is becoming a basic need.

To achieve this, the capacity for IoT devices to roam across administrative domains and spectrum is key (e.g., LoRa-LoRa; NB-IoT-NB-IoT, and for devices supporting multiple stacks, also exploit multiple radios, e.g., CBRS-Wi-Fi 6, CBRS-Public LTE, etc.). Long range (LoRa), in particular, is a low-power wide-area network (LPWAN) technology based on spread spectrum modulation techniques derived from chirp spread spectrum (CSS) technology. LoRa devices and wireless radio frequency technology is a long range, low power wireless platform that is widely used in Internet of Things (IoT) networks worldwide.

LoRa defines the lower physical layer, while LoRaWan defines the upper layers of the network. LoRaWAN is based on a medium access control (MAC) layer protocol, but acts mainly as a network protocol for managing communication between networks servers, LPWAN gateways and devices.

LoRa has very attractive features for customers. However, a number of things need to change first in order to turn LoRa into a professional solution capable of supporting massive roaming of assets across the world. In particular, recent publications, such as Johan Stokking, "5 x Why LoRaWAN Roaming Is Not A Solution", June 2019, have demonstrated that LoRa's roaming model is broken, where the main challenges include:

1. LoRaWAN roaming requires blind trust in roaming parties or hubs.
2. LoRaWAN Roaming requires many-to-many (peer-to-peer) pre-configurations.
3. LoRaWAN Roaming hubs centralize authority
4. LoRaWAN Roaming requires each party to operate a LoRaWAN Network Server (NS)
5. LoRaWAN Roaming does not support separating payload from metadata

The techniques proposed herein address the first four issues, above. In particular, the techniques proposed herein extend the OpenRoaming model and federation to the IoT space with the aim of improving and scaling out LoRaWAN roaming in a secure and non-disruptive way. That is, the solution described below requires changes neither to LoRa servers nor the messaging protocols that currently support passive roaming in LoRa.

The following example (use case) is used to illustrate aspects of the techniques presented herein. Figure 1, below, illustrates a LoRa sensor/actuator that roams from the Netherlands to Cape Town (both South Africa and the Netherlands use the EU863-870 ISM band for LoRa).

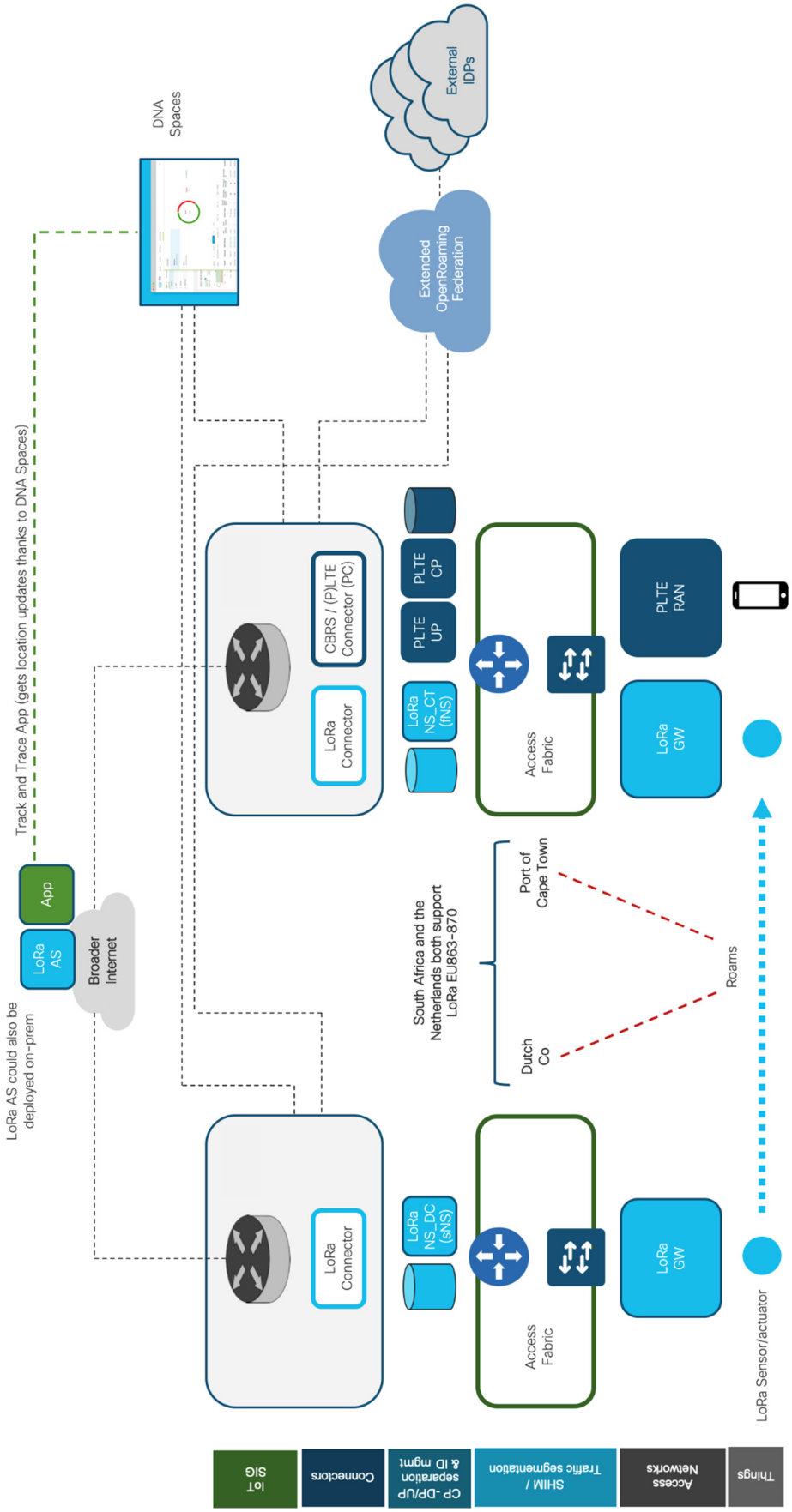
External IDPs
DNA Spaces
Extended OpenRoaming Federation
Track and Trace App (gets location updates thanks to DNA Spaces)
App
LoRa AS
Broader Internet
LoRa AS could also be deployed on-prem
CBRS / (P)LTE Connector (PC)
LoRa Connector
PLTE UP
PLTE CP
LoRa NS_CT (fNS)
Access Fabric
PLTE RAN
LoRa GW
South Africa and the Netherlands both support LoRa EU863-870
Port of Cape Town
Dutch Co
Roams
LoRa NS_DC (sNS)
LoRa Sensor/actuator
Things
Access Networks
SHIM / Traffic segmentation
CP-DP/UP separation & ID mgmt
Connectors
IoT SIG

Figure 1

In the example of Figure 1, it is assumed that:

- The access provider (i.e., the visited network) is port of Cape Town (CT). For instance, the port runs its own LoRa network.
- The LoRa sensor/actuator is attached to goods that need to be shipped from Port of Rotterdam (PoR) to port of Cape Town.
- PoR also runs its own LoRa network; PoR is just an intermediate (transit) location for the LoRa sensor/actuator (same role as Cape Town).
- The owner of those goods is a Dutch Company (DC).
- This company is the one that attached the LoRa sensor/actuator to the goods and is also the owner of the sensor/actuator.
- The LoRa sensor/actuator was activated by the owner on its own LoRa network.
- The Identity Provider (IDP) for the LoRa sensor/actuator in this case is the Dutch Co. (DC).

Figure 2, below, is a sequence diagram illustrating aspects of the techniques presented herein. In the example of Figure 2, it is assumed that the onboarding process in OpenRoaming both for the visited network (i.e., Port of Cape Town) and the IDP (DC) has already occurred (in day -1). That is, both parties are already part of the federation, which means that the certificates issued by OpenRoaming are in place, the DNS is already configured by the IDP and LoRa NSs were pre-configured through the connectors to send all traffic to their IoT Secure Internet Gateways (SIGs).

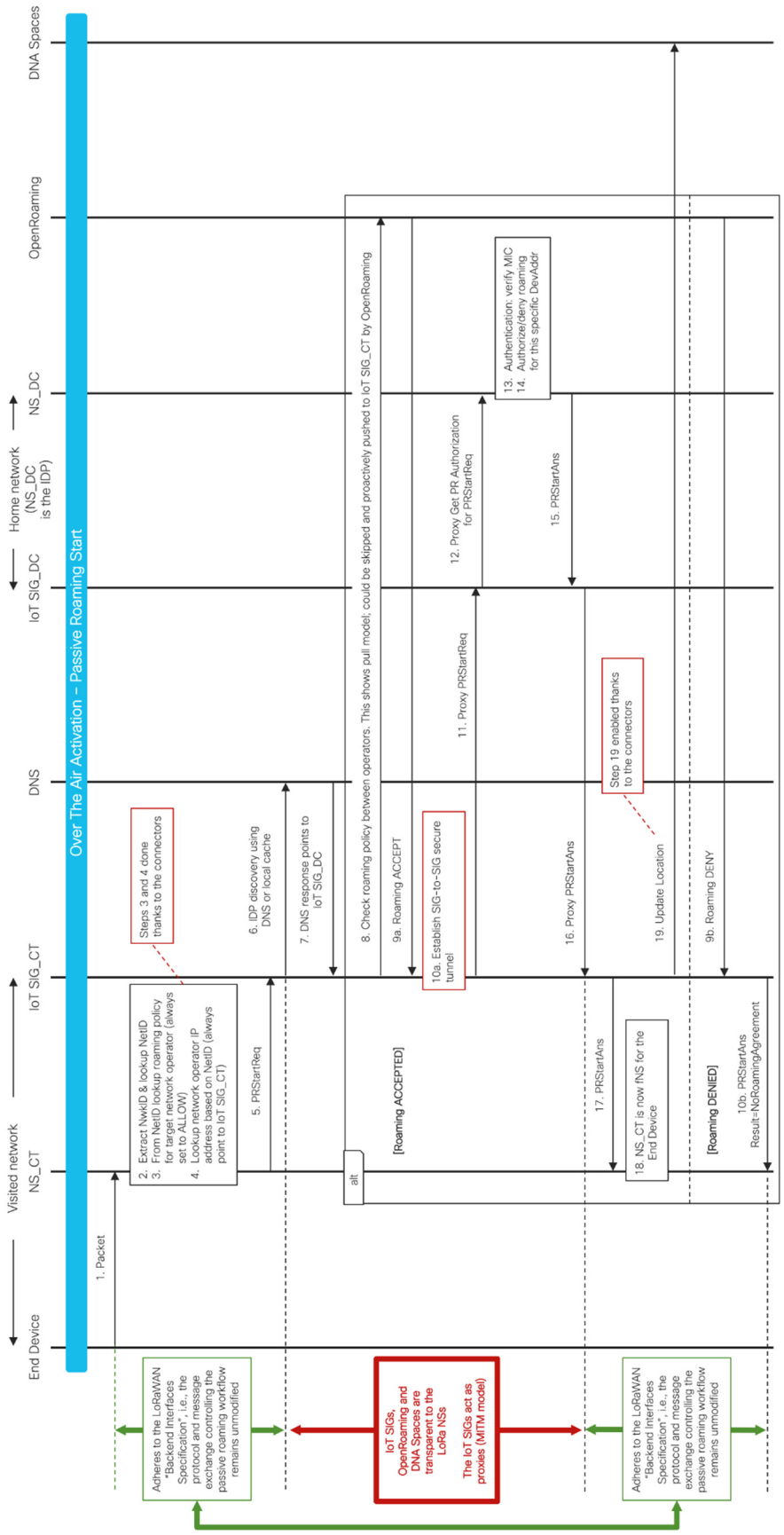
End Device
Visited network
NS_CT
IoT SIG_CT
DNS
IoT SIG_DC
Home network (NS_DC is the IDP)
NS_DC
OpenRoaming
DNA Spaces
Over The Air Activation – Passive Roaming Start
1. Packet
Steps 3 and 4 done thanks to the connectors
2. Extract NwkID & lookup NetID
3. From NetID lookup roaming policy for target network operator (always set to ALLOW)
4. Lookup network operator IP address based on NetID (always point to IoT SIG_CT)
5. PRStartReq
6. IDP discovery using DNS or local cache
7. DNS response points to IoT SIG_DC
8. Check roaming policy between operators. This shows pull model; could be skipped and proactively pushed to IoT SIG_CT by OpenRoaming
9a. Roaming ACCEPT
10a. Establish SIG-to-SIG secure tunnel
11. Proxy PRStartReq
12. Proxy Get PR Authorization for PRStartReq
13. Authentication: verify MIC
14. Authorize/deny roaming for this specific DevAddr
15. PRStartAns
16. Proxy PRStartAns
17. PRStartAns
Step 19 enabled thanks to the connectors
18. NS_CT is now fNS for the End Device
19. Update Location
9b. Roaming DENY
10b. PRStartAns Result=NoRoamingAgreement
alt
[Roaming ACCEPTED]
[Roaming DENIED]
Adheres to the LoRaWAN "Backend Interfaces Specification", i.e., the protocol and message exchange controlling the passive roaming workflow remains unmodified
IoT SIGs, OpenRoaming and DNA Spaces are transparent to the LoRa NSs
The IoT SIGs act as proxies (MITM model)
Adheres to the LoRaWAN "Backend Interfaces Specification", i.e., the protocol and message exchange controlling the passive roaming workflow remains unmodified

Figure 2

Today, roaming in LoRa requires many-to-many manual configurations to be maintained (LoRaWAN roaming is peer-to-peer). In particular, there are more than 110 commercial LoRaWAN networks at various stages of deployment across more than 55 countries worldwide. By some estimates, there are approximately 100 million LoRa end nodes. Currently, connecting an sNS and an fNS is a manual process (generating the keys, certificates and configuration files). With only 110 networks and a partial mesh, this already entails thousands of P2P manual configurations in total.

The techniques presented herein provide an opportunity for OpenRoaming, which includes:

- Scale linearly rather than quadratically.
- Enable grouping/clustering policies, e.g., allow a LoRa operator to aggregate multiple operators into the same bucket and solve roaming requests dynamically (i.e., without requiring pre-defined/static configurations among servers across different LoRa networks).

Steps 8 and 9 in Figure 2, above, avoid the P2P problem, thereby offering a new LoB for OpenRoaming. In any case, the checks carried out in steps 8 and 9 on the visited network can be performed by the NS_CT before the DNS lookup occurs (just as it is done today in LoRa).

The techniques presented are secure and provide the ability to scale out LoRa roaming in a fully distributed and decentralized way. The techniques presented herein also provide companies with the means to track and trace assets as they roam across different LoRa access networks.

The techniques presented herein have several benefits for end customers, including:

- Cost-effective roaming capabilities across the world using unlicensed bands. These capabilities can become even more prominent with the advent of 2.4 GHz LoRa.
- Location, traceability and insights available through cloud-based systems, such as DNA Spaces.

The techniques presented herein have several benefits for LoRa operators, including:

- Trusted SIGs and OpenRoaming help handling and scaling out the roaming process.
- Non-disruptive approach: requires changes neither to LoRa servers nor the messaging protocols supporting passive roaming.
- Easier to handle roaming agreements/policies through OpenRoaming than P2P.
- Overcomes issues 1-4 listed in the problem description section (e.g., no need for peering hubs).

The techniques presented herein have several benefits for hardware vendors, including:

- Market forecasts indicate that, some of the largest spending growth on IoT technologies between 2017 and 2023 will occur in the track-and-trace and inventory/supply chain sectors, with projected increases of 24.2%, and 20.2%, respectively (source: Forrester). Enterprises are looking for affordable solutions, since not everything can be endowed with cellular connectivity and roaming capabilities in licensed bands (cost, lack of public cellular coverage, etc.). The vendors with the most compelling technologies enabling mobility and roaming across heterogeneous access networks will be well positioned to capture this opportunity.
- Ability to offer a strategic point of control with benefits both for end customers and LoRa operators
- All traffic across domains goes through vendor control and data planes. Even within a single domain, traffic across spectrum can be proxied and forwarded by the IoT SIGs
- Assist in expanding the reach of the OpenRoaming Federation and value added services for the wireless networks