dAuth - Decentralizing LTE Authentication and Roaming

Sudheesh Singanamalla, Esther Jang, Nick Durand, Matthew Johnson, Spencer Sevilla, Kurtis Heimerl

University of Washington, Seattle
The Case for Rural Community Networks and Rural Connectivity

- ~1 Billion people live outside mobile broadband coverage
- 400 Million people live outside any mobile coverage
- Telecom operators have rolled out 2G/3G networks as far as economically and commercially viable.

Source: The State of Mobile Internet Connectivity 2019, GSMA
Rural Community Networks

Advantages:
- Built by and for their users
- Run cooperatively
- Optimized for local needs
- Sustainable in rural areas
- Leverages local resources
- Provides local services
Rural Community Networks

Constraints:
- Backhaul satellite connectivity
- Localized Radius of connectivity
- Intermittent power supply
Why can’t Telcos set up infrastructure and improve connectivity in rural areas? What happens when users in community cellular networks move outside network range?
Challenges with Traditional LTE Networks

- Not economically viable to extend and deploy infrastructure to remote rural areas.
- Primarily profit driven and cannot cater to local desires (e.g. free calls within communities)
- Roaming between telecom operators is a business decision, managed by physical agreements between network operators
Exponential Complexity of Roaming Agreements

Every single large telecom operator needs to have a roaming agreement with at least with one mobile network in each country to allow their users to roam.

(Many countries still do not allow national roaming)

This might only be possible for large telcos like Verizon/AT&T/T-Mobile.

Verizon Roaming: https://ss7.vzw.com/is/content/VerizonWireless/available-international-travel-services.pdf
Can we provide Cellular data access in rural remote areas?

Can we enable these users to roam between different communities?
Primer into LTE Networks

A. LTE Network is called an Evolved Packet System (EPS) and is an end-to-end all IP network comprising of 2 parts
   a. E-UTRAN (Radio Access Network)
A. LTE Network is called an Evolved Packet System (EPS) and is an end-to-end all IP network comprising of 2 parts
   a. E-UTRAN (Radio Access Network)
   b. Enhanced Packet Core Network
LTE Network Reference Architecture
User Equipment

UE or User Devices are the wide array of LTE compatible devices which are available with the users and comply to the 3GPP standard.
eNode B (eNB)

Provides the radio link interface and performs radio resource management and scheduling along with cell interference coordination.
LTE Network Architecture: Mobility Management

MME

Performs necessary roles in User Authentication, signaling along with session and mobility management. (e.g., cell tracking, handover management, etc.)
LTE Network Architecture: Serving Gateway

Serving Gateway (S-GW)

Routes and forwards user data packets and allows traffic management between LTE and other 2G/3G systems to P-GW.

Manages and stores state/context of different UEs
Packet Data Network Gateway (P-GW)

PDN Gateway that provides connectivity from the UE to external packet data networks (Internet) and performs policy enforcement and lawful interception, packet screening.
LTE Network Architecture: Home Subscriber Server

HSS

Central Database that contains user related and subscription related information such as SIM card keys, type of subscription, data limits, etc.,
Stripping down LTE Network Architecture

Open5Gs - An open source implementation of EPC

Moves the data center EPC to the edge!

Cheapest computer we could buy. Currently is actively running in Bokondini, Indonesia supporting hundreds of active users.
Traditional LTE Authentication

**Authentication:** Check if the user device with the SIM card is actually owned by the network which it is trying to connect to.

Bidirectional authentication

1. UE authenticates and validates the network
2. Network authenticates and validates the UE
Technical Complexities of Roaming

Telecom operators perform roaming in multiple ways posing different challenges:

1. The roaming core network requests subscribers’ home network for necessary authentication values needing reliable connectivity between operators.
   a. Users experience higher latencies since all requests are tunnelled home.
2. The symmetric key and state corresponding to the user could be exchanged between operators over an encrypted channel.
   a. Raises security concerns

Current Roaming Practices - Fully connected networks

1. UE Connects to the Roaming eNB
2. Roaming MME asks Home HSS to authenticate the phone.
Current Roaming Practices - Fully connected networks

Challenges/Limitations:

- The EPC cores need to be fully available for allowing roaming users to connect to the network
- All the network traffic is tunneled from the roaming EPC to the Home EPC resulting in higher latencies for data usage
- The architecture would not work in disconnected settings like in community cellular networks challenged by power outages, failure of backhaul connectivity
SIM Cards & Milenage

- Inexpensive to manufacture / get SIM cards printed
- Standardized authentication algorithms (Milenage) using symmetric key AES 128 bit encryption.

SIM Cards and HSS contain the following to make authentication happen using symmetric key cryptography:

- Symmetric key (K)
- AMF (Authentication Management Field)
- SEQ (Sequence Number)
- IMSI (International Mobile Subscriber Identity)

SIM Sequences and SQN construction from SEQ

- 4 Octet sequences which are single use and monotonically increasing
  - SQN = SEQ (27 bits) + IND (5 bits)

The SQN state is maintained in the HSS database.

SIM Cards use the SEQ numbers from a specific row as sequence numbers

Usage of a SEQ invalidates unused SEQ values before that in a given row.
Milenage Function outputs

- \( f_1 \): Computes MAC_A
- \( f_{2345} \): Computes XRES, CK, IK, AK
- KDF: Computes \( K_{asme} \) from
  - IMSI, SQN, PLMN, CK, IK, RAND

**Integrity** Algorithms [IK]:
- 0000: EIA0 Null Integrity Protection Algorithm
- 0001: 128-EIA1 SNOW 3G
- 0010: 128-EIA2 AES

**Cipher** Algorithms [CK]:
- 0000: EEA0 Null Ciphering Algorithm
- 0001: 128-EEA1 SNOW 3G based algorithm
- 0010: 128-EEA2 AES based algorithm
Steps in Authentication: Attach, Identity Requests

Communication between the User Device and the eNB which is registered with the MME

The UE Identifies network capabilities, algorithms to use and session identifiers

UE → eNB → MME
Steps in Authentication: Authentication Info. Request

AIR happens between the MME and the HSS where the MME requests the HSS for Authentication Vectors and validation for a specific user trying to connect.

MME → HSS/AuC
The HSS responds to the request for authentication from the MME with a RAND challenge, expected response XRES, AUTN value and K_{asme}.

HSS/AuC → MME
Steps in Authentication: Authentication Request

The MME signals the UE with an Authentication Request and provides the RAND and AUTN as a challenge to compute the RES.

Downlink Transport

MME → UE
The MME signals the UE with an Authentication Request and provides the RAND and AUTN as a challenge to compute the RES.

**Uplink Transport:**
Compares XRES == RES

UE → MME
Steps in Authentication: Security Mode

- Initialize signaling security between the UE and the MME
- UE derives corresponding CK, IK keys for encryption and Integrity algorithms

- Completes Authentication and UE successfully attaches to the network.
Precomputing LTE Authentication Vectors (AV)

- \( \text{AUTN} = (\text{SQN} \oplus \text{AK}) + \text{AMF} + \text{MAC}_A \)
- \( \text{AV} = \{\text{RAND}, \text{XRES}, \text{AUTN}, K_{asme}\} \)

- The Home HSS creates the required authentication vectors (AVs) and publishes the vectors to other EPC nodes over a blockchain network.
- The SQN construction matrix allows us to dedicate specific row(s) for roaming.
- One time usage of SEQ to create an AV prevents replay attacks and the AVs remain valid until they are used by the UE.
- Any EPC participating in the blockchain network can allow users to roam.
The need for decentralization

- Multiple community cellular networks EPC cores become participants in a blockchain network
- Home network pre-computes authentication vectors and shares it with the rest of the network as a transaction
- Communities choose who they can connect to and pre-pay for total data associated with an authentication vector.
- Never share symmetric keys needed for authentication
  - Subscriber trusts Home network provider
- Design for high network outages and high latency communication between communities
- Common policy for operation agreed upon by network operators
Implementation

- Built currently with Hyperledger Sawtooth as the blockchain layer running PoET consensus
- Generate authentication vectors (AV) with a sliding window of X usable AVs in the network
- Roaming nodes consuming the vector for user authentication report the consumption and corresponding billing/payment workflows take over
- Integrated into Open5Gs fork (uw-ictd/nextepc) in dAuth branch

https://github.com/uw-ictd/nextepc/tree/dAuth
Lab Experiments

- 1x 8GB RAM Zotac Mini Computers
- 1x 4GB RAM Zotac Mini Computer
- 1x 8GB RAM Dell workstation

Running Open5GS and Hyperledger Sawtooth with corresponding transaction processors.

2 USRP B200 mini SDRs behaving as 2 cellular networks allowing users.
~4 tx/s with heavy network usage (~13x more than block sizes)
Challenges & Future Work

- Blockchain consensus protocols (PoET/PBFT) are chatty and consume lots of bandwidth
- Need for tuning networking parameters to minimize the chattiness and operate better in high latency and bandwidth constrained networks
- Improving current experiments with batching
- Real world deployment experiments with the Othello Network in Seattle
THANKS!
Any questions?
You can find me at
@sudheesh001 & sudheesh@cs.washington.edu

https://ictd.cs.washington.edu/