Interactive session on

"Smart Grids for Smart Cities"

30th October 2018

India Habitat Centre, New Delhi

How To Scale Smart Grid Deployments

Sylvain Vittecoq

CTO - CyanConnode

Jointly Organized by

National Smart Grid Mission
Ministry of Power
Government of India

ieema
your link to electricity

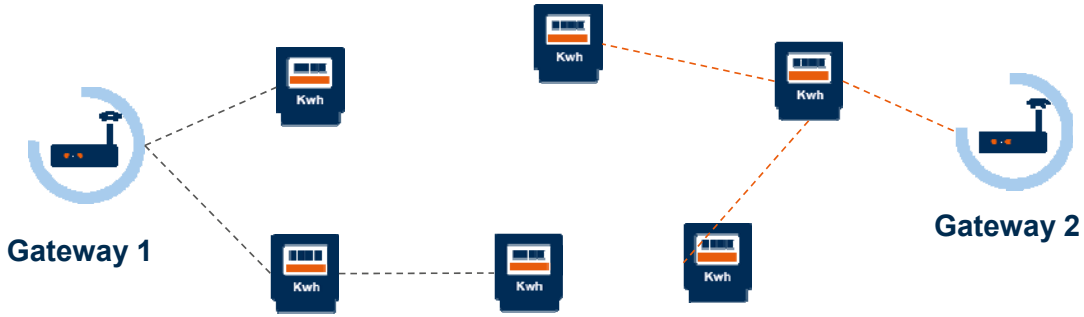
Communication 100% Cellular : Challenging !

- Coverage by Telco Operators : NOT COMPLETE
  - No Coverage Deep Within Buildings (Urban Areas)

- Cellular Network : NOT 100% AVAILABLE
  - Daily Drop-outs (Overload / Peak Demand)
  - DLMS Protocol : Not Best Fit

- Current Cellular Technology : CORE ISSUES FOR IoT
  - Meters Can Not Move For Better Signal
  - No Broadcast Capability (Mass Firmware Update)

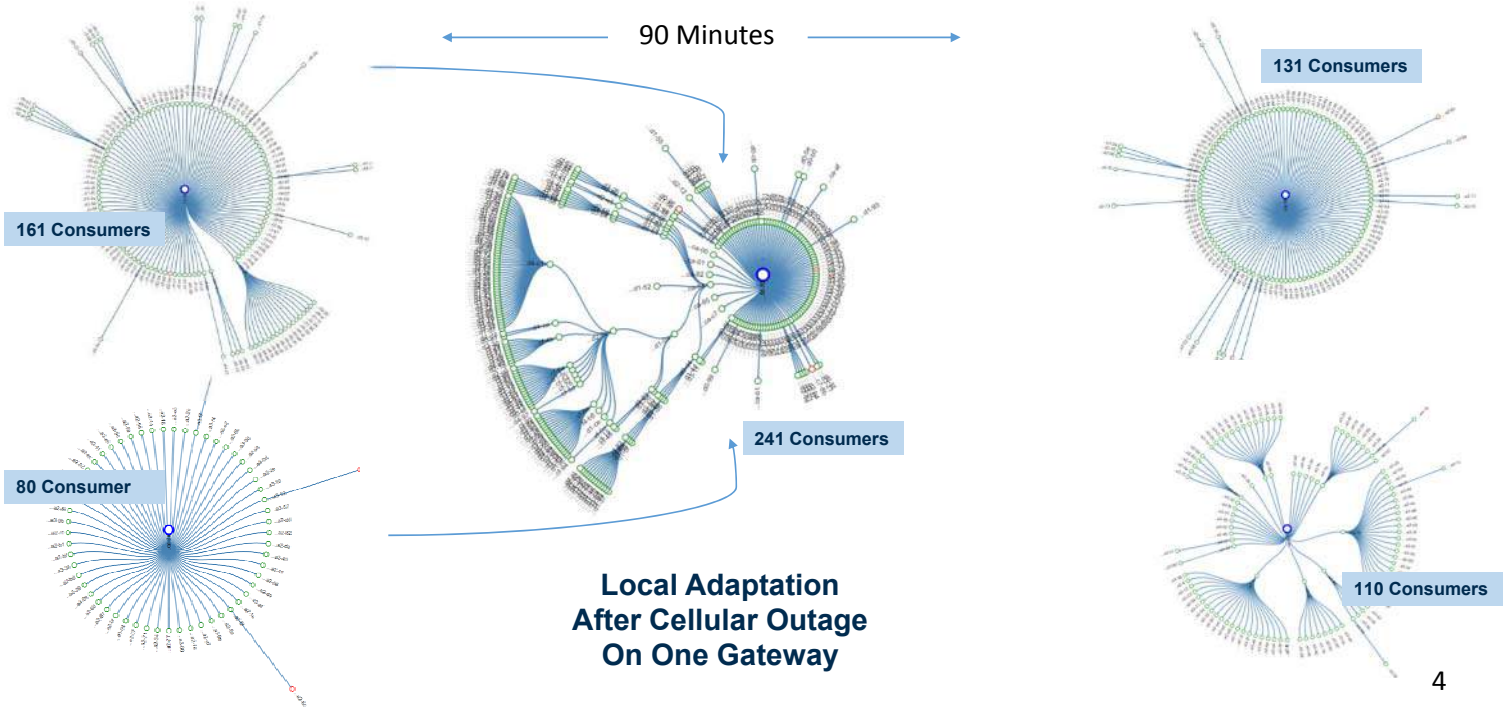
Mesh + Cellular : A Working Model !



- Gateways Within Cellular Coverage
  - Such locations always exist in any neighborhood
- Sub-GHz Radio
  - ISM Band - License Free
  - Great penetration into buildings & Good bandwidth
- Modern RF SOC
  - Signal processing : Very performant
  - Low cost & low power consumption

- RF Mesh Networks
  - Self-Forming & self-Healing
  - Constant adaptation to local conditions
  - Constant load-balancing
  - Always local decisions (no operator action)
  - 2 Way Traffic : Device ←→ Enterprise

Mesh Networks : How to Meet SLAs



Local Adaptation
After Cellular Outage
On One Gateway

Smart Cities : Which Networks ?

- Enable New IoT Devices
  - Device Management : Not Fully Standardized Yet
  - Communication Stack : Fully Standardized (RFCs)
  - Common Network Layer : IPv6
  - New Devices To Join Same Networks : ROI Infrastructure
- Enable New IoT Applications (15 – 20 years)
  - 5 B/Sec - 500 B/Sec
  - 2 Way Communication
    - Alarms & Data From Devices
    - Commands From Utilities & Users
  - Good Resiliency To Backhaul Instability
- How To Scale Smart City Networks
  - Security : Not An After Thought
  - Roll Out : Need To Be Streamlined

Smart City Networks : How To Secure Them ?

- Security Model : STANDARD-BASED !
  - Authorization : Only Authorized Devices Can Join
  - Authentication : Only Authenticated Devices Can Produce Data & Run Commands
  - Encryption : In-Flight Data Always Encrypted (AES128 - AES256)

- Device ←→ Enterprise System : END-TO-END !
  - Pre-Shared Keys
    - Complex To Provision
  - Public Key Infrastructure
    - Scale To Millions (Certificate Provisioning Before Deployment, Not After)
    - Ability To Black List Compromised Devices Once Identified …

Mesh IoT Devices : How To Secure Them ?

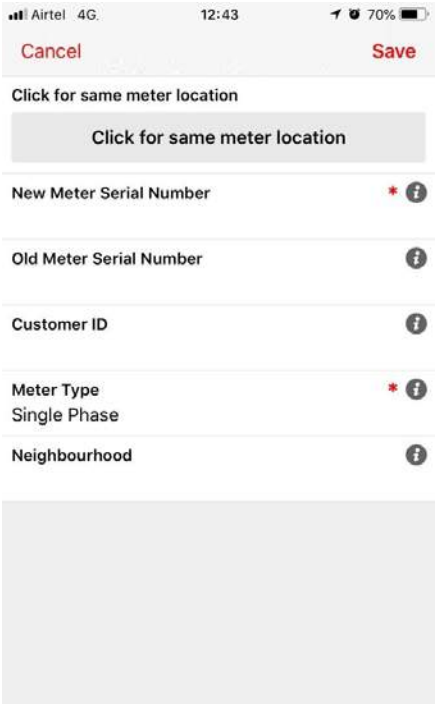
- Signal Jammer
  - Illegal BUT Always Local : No Large Scale attack !
- Unauthorized Joining Of Mesh Networks
  - AES128 Keys To Encrypt/Decrypt Radio Frames (RFCs)
  - More Standardization Required
- Concentrator Of Credentials : Major Security Risk
  - Any Device In the Field Can & Will Be Hacked !
  - Access Point (>500 device credentials) : Easy Target For Large Scale Attack
  - Passthrough Gateways : Nothing To Steal

Smart City Roll-Outs : How To Deploy Fast?

Work Flow For Installers : FULLY STREAMLINED…

1. Mount Meter with integrated Com Module
2. Power Up … Meter connects to RF mesh within Minutes - LED
3. Associate Meter & Customer – Installer App → MDM← HES
4. Record Location Information (GPS) – Installer mobile App
5. Move On To Next Meter !

Smart City Roll-Outs : Time Line



Smart City Roll-Outs : How To Scale ?

Rules To Roll Out Millions Of Devices :

- ❑Rule 1 : Manufacturing & Transportation At Scale
- ❑Rule 2 : Unique Certificates
- ❑Rule 3 : End-To-End Security
- ❑Rule 4 : No Complex Radio Planning Prior To Installation
- ❑Rule 5 : 100% Automatic Provisioning
  - ❑Communication Stack
  - ❑IoT Device Application (Metering Profiles , Capture Period , Firmware Version, etc.)
- ❑Automatic Operational Reports
  - ❑To Identify Problematic Devices

➔ Metering Data Available At Utility By End Of Day !

Thank You

Sylvain Vittecoq
CTO – CyanConnode

Sylvain.Vittecoq@CyanConnode.com