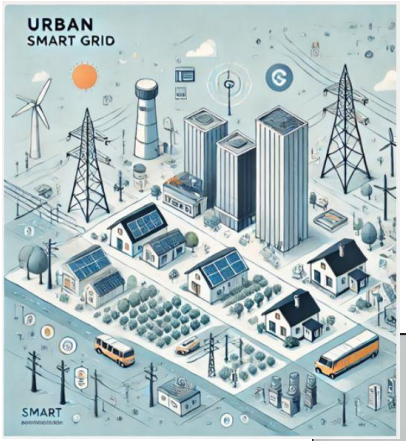
Large AMI systems – Architecture, Reliability, Security

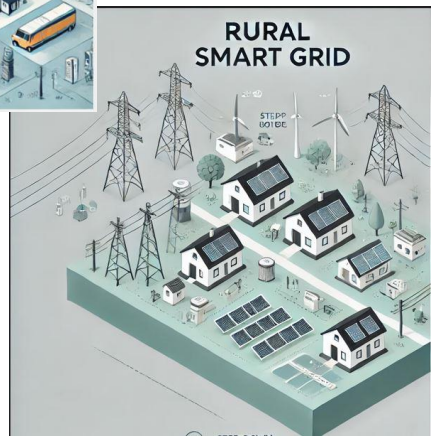
A semiconductor solutions provider's perspective

Chander Goel

Network technologies based on density

- Cellular technologies are better for Sparse Networks like rural or small urban settlements
  - No separate gateway required.
  - High Range and scalability
  - Low latency
  - Drawbacks - High on power, cost, congestion in dense networks
- Sub GHz Low Power RF like (WiSUN or proprietary mesh) are low cost alternative for Dense Networks in Urban Areas
  - Cost optimized and low power consuming
  - Mesh Networking with self healing
  - Free from interference due to frequency hopping
  - Drawbacks – Long Network Set up time, High Latency, Medium data rates





* AI Generated Graphic

Why same SLA for both type of networks?

Billing profile data for installed meters	hours after the midnight
3. On-Demand Remote reads of meters	
Collection of 7 days of interval energy data and the current total accumulated energy from a selected individual meter	From 90% of the meters in 2 minutes
4. Remote connect / disconnect	
Action to response for individual meter	Less than 3 mins
5. Updating of data on consumer portal/ app	
Updating of individual consumer data on portal/ app after receiving the data in MDM	Action performed for active on portal consumers within 5 minutes after receiving the data in MDM
6. Ping Response with acknowledgement/ response for selected meters	
For installed meters	Action performed at 99.9% of meters within [1] minute; and
For an individual meter	Action performed within 3 seconds
7. Meter loss and restoration of supply	
Receiving of alert for all affected AMI meters	Alert to be received within 3 minutes for 60% of meters
8. Meter Tamper Alerts	
Receiving of alert for an individual meter	Alert to be received within 3 minutes
9. Power Quality Alerts	
Receiving of alert for an individual meter	Alert to be received within 5 minutes

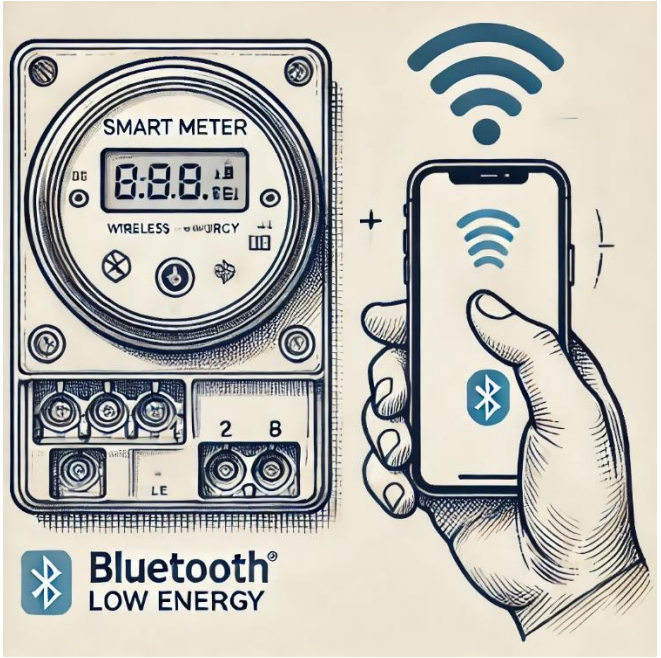
RF mesh networks like Wi-SUN typically have a longer joining time compared to cellular networks due to the following reasons:

- **Multi-Hop Network Discovery**: In Wi-SUN mesh networks, a new device must first scan for nearby neighbors and establish a multi-hop path to a gateway which involves - Finding the nearest parent node , Verifying link quality, Selecting the optimal routing path, Establishing multi-hop connectivity.
  - In contrast, a cellular device only needs to connect to the nearest base station, making the process faster.
- **Secure Authentication & Key Exchange**
  - Wi-SUN networks use public key infrastructure (PKI) for authentication, requiring secure key exchange between the device, neighbors, and gateway. This involves Certificate validation, Mutual authentication, Establishing encrypted communication.
  - Cellular networks rely on pre-provisioned SIM cards, which authenticate quickly with the mobile network.
- **Network Synchronization & Routing Setup**
  - Mesh networks require:
    - Time synchronization between nodes to coordinate transmissions.
    - Routing table construction for multi-hop data forwarding.
    - Cellular networks do not need complex time sync or routing protocols, making the connection process faster.
- **Self-Forming & Self-Healing Overhead**
  - Wi-SUN mesh is a self-forming, self-healing network, which means:
  - New nodes must find stable connections and integrate into the existing mesh.
  - Nodes constantly update routing tables, which adds overhead.
  - Cellular networks use a centralized infrastructure, eliminating the need for distributed routing updates.

Source: https://www.nsgm.gov.in/sites/default/files/AMISP_Contract_Final.pdf

Use Case for mandating BLE

- BLE can provide 1-to-1 direct access to the User Mobile phone or Utility Operator's Tablet. It is a good tool for commissioning, servicing and monitoring
- Experience tells that both Sub GHz RF as well as Cellular technologies may falter at some or the other point. BLE provides a reliable fail-safe connectivity especially for pre-payment operations.
- It can replace old way of plugging an optical reader.
- The present BLE SOC offerings from Semiconductor vendors like Texas Instruments are very cost optimized and thus add minimal cost
- The BLE technology and BLE SOCs consume ultra low power. They can remain active through small batteries during power outages.



* AI Generated Graphic

Security in AMI – A key feature of latest Sub GHz RF and BLE SOCs

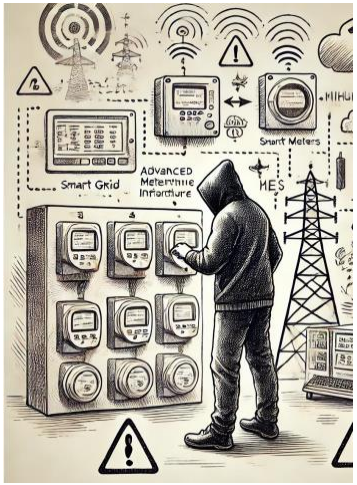
Security is AMI is of utmost importance to:

- **Prevent Cyber Attacks** – Blocks hacking, malware, and DoS threats.
- **Ensure Data Privacy** – Protects consumer energy data.
- **Stop Energy Theft** – Detects meter tampering and fraud.
- **Maintain Grid Stability** – Prevents disruptions from cyber threats.
- **Authenticate Devices** – Blocks unauthorized access.
- **Prevent Insider Threats** – Restricts unauthorized data access.
- **Avoid Service Disruptions** – Ensures reliable power distribution.

Snapshot from CC2755 Datasheet (TI's Latest BLE SOC)

Security enablers

- Global Platform SESIP (Security Evaluation Standard for IoT Platforms) Level 3 and Arm PSA (Platform Security Architecture) Level 3 Certification
- Hardware Security Module (HSM) with proprietary controller and dedicated memories supporting accelerated cryptographic operations and secure key storage:
  - AES (up to 256 bits) crypto accelerator
  - ECC (up to 521 bits), RSA (up to 3072 bits) public key accelerator
  - SHA-2 (up to 512 bits) accelerator
  - True random number generator
  - HSM firmware update support
- Separate AES 128bit crypto accelerator (LAES) for latency-critical link-layer crypto operations
- Secure boot and secure firmware updates
- Cortex®-M33 TrustZone-M, MPU, memory firewalls for software isolation
- Voltage glitch monitor (VGM)



* AI Generated Graphic

Questions