Sunbeam Institute of Information Technology
Pune and Karad

Module – Internet of Things (IoT)

Trainer - Devendra Dhande

Email – devendra.dhande@sunbeaminfo.com

LoRaWAN

- LoRa is a wireless modulation technique derived from **Chirp Spread Spectrum (CSS)** technology
- LoRa is ideal for applications that transmit small chunks of data with low bit rates.
- Data can be transmitted at a longer range compared to technologies like WiFi, Bluetooth or ZigBee.
- These features make LoRa well suited for sensors and actuators that operate in low power mode.

- LoRa can be operated on the license free **sub-gigahertz** bands, for example, 915 MHz, 868 MHz, and 433 MHz.
- It also can be operated on **2.4 GHz** to achieve higher data rates compared to sub-gigahertz bands

- LoRaWAN is a Media Access Control (MAC) layer protocol built on top of LoRa modulation
- The LoRaWAN protocol is developed and maintained by the LoRa Alliance.
- The first LoRaWAN specification was released in January 2015.
- LoRaWAN is suitable for transmitting small size payloads (like sensor data) over long distances

Why LoRaWAN?

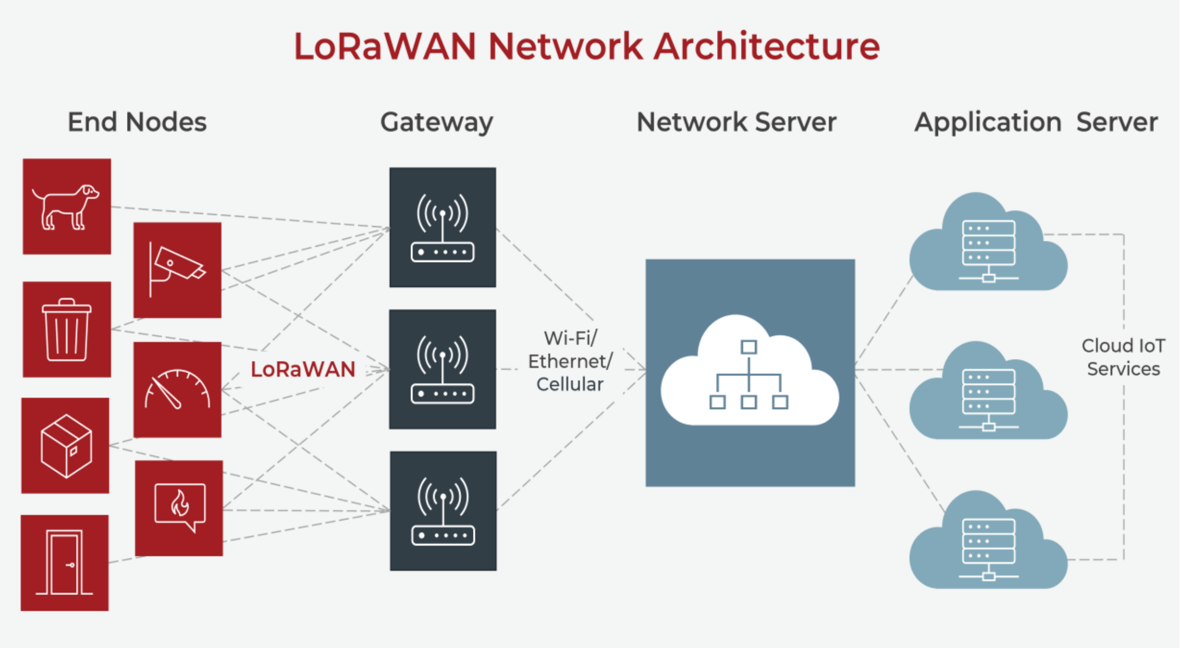
- **Ultra low power** - LoRaWAN end devices are optimized to operate in low power mode and can last up to 10 years on a single coin cell battery.
- **Long range** - LoRaWAN gateways can transmit and receive signals over a distance of over 10 kilometers in rural areas and up to 3 kilometers in dense urban areas.
- **Deep indoor penetration** - LoRaWAN networks can provide deep indoor coverage, and easily cover multi floor buildings.
- **License free spectrum** - You don’t have to pay expensive frequency spectrum license fees to deploy a LoRaWAN network.
- **Geolocation**- A LoRaWAN network can determine the location of end devices using triangulation without the need for GPS. A LoRa end device can be located if at least three gateways pick up its signal.
- **High capacity** - LoRaWAN Network Servers handle millions of messages from thousands of gateways.
- **Public and private deployments** - It is easy to deploy public and private LoRaWAN networks using the same hardware (gateways, end devices, antennas) and software (UDP packet forwarders, Basic Station software, LoRaWAN stacks for end devices).

Why LoRaWAN?

- **End-to-end security**- LoRaWAN ensures secure communication between the end device and the application server using AES-128 encryption.
- **Firmware updates over the air** - You can remotely update firmware (applications and the LoRaWAN stack) for a single end device or group of end devices.
- **Roaming**- LoRaWAN end devices can perform seamless handovers from one network to another.
- **Low cost** - Minimal infrastructure, low-cost end nodes and open source software.
- **Certification program**- The LoRa Alliance certification program certifies end devices and provides end-users with confidence that the devices are reliable and compliant with the LoRaWAN specification.
- **Ecosystem**- LoRaWAN has a very large ecosystem of device makers, gateway makers, antenna makers, network service providers, and application developers.

LoRaWAN Architecture

- LoRaWAN networks are deployed in a **star-of-stars** topology.
- A typical LoRaWAN network consists of the following elements.
  - **End Devices**
    - sensors or actuators send LoRa modulated wireless messages to the gateways or receive messages wirelessly back from the gateways. .
  - **Gateways**
    - receive messages from end devices and forward them to the Network Server.
  - **Network Server**
    - a piece of software running on a server that manages the entire network.
  - **Application servers**
    - a piece of software running on a server that is responsible for securely processing application data.



Use cases of LoRaWAN

- **Vaccine cold chain monitoring** - LoRaWAN sensors are used to ensure vaccines are kept at appropriate temperatures in transit.
- **Animal conservation** - Tracking sensors manage endangered species such as Black Rhinos and Amur Leopards.
- **Smart farms**- Real time insights into crop soil moisture and optimized irrigation schedule reduce water use up to 30%.
- **Water conservation**- Identification and faster repair of leaks in a city's water network.
- **Food safety**- Temperature monitoring ensures food quality maintenance.
- **Smart waste bins** - Waste bin level alerts sent to staff optimize the pickup schedule.
- **Smart bikes**- Bike trackers track bikes in remote areas and dense buildings.
- **Airport tracking** - GPS-free tracking monitors vehicles, personnel, and luggage.
- **Efficient workspaces** - Room occupancy, temperature, energy usage and parking availability monitoring.
- **LoRa in space** - Satellites to provide LoRaWAN-based coverage worldwide.

NB-IoT

- Narrowband IoT is wireless IoT protocol that uses Low Power Wide Area Network (LPWAN) technology.
- It was developed by the 3rd Generation Partnership Project (3GPP) for cellular wireless communication.
- This standard allows IoT devices to operate via carrier networks, within an existing Global System for Mobile (GSM), Long-Term Evolution (LTE) channels or independently
- NB-IoT boosts the coverage extension beyond what existing cellular technologies offer. To do that, NB-IoT offers transmission repetitions and different bandwidth allocation configurations in uplink transmission.
- It reduces the power consumption of connected devices while increasing system capacity and bandwidth efficiency, particularly in locations that aren't easily covered by traditional cellular technologies.
- The NB-IoT standard uses a small radio band of 200 kilohertz (kHz), specifically designed to support IoT use cases.

NB-IoT - Benefits

- **Ubiquitous coverage and connectivity**
  - supports massive number of devices by establishing NB-IoT networks which connects billions of nodes. Designed for extended coverage indoors, the lower complexity of the devices provides long-range connectivity and communication.
- **Bandwidth**
  - NB-IoT is designed with bandwidth efficiency in mind. It uses a small portion of the spectrum, meaning multiple NB-IoT networks can coexist in the same area without any interference.
- **Strong signals**
  - NB-IoT signal strengths are typically strong, designed to penetrate multiple layers of brick.
- **Low power consumption**
  - NB-IoT doesn't need to run a heavy operating system, such as Linux, or do a lot of signal processing, making it more power-efficient compared to other cellular technologies.
- **Low cost of devices**
  - Because it's easier to create devices with lower complexity, the devices cost significantly less.
- **Multiyear battery life**
  - The enhanced power consumption capability enables NB-IoT to support a multiyear battery life for devices.
- **Security**
  - NB-IoT is secured using methods such as data encryption, secure authentication and signaling protection.

NB-IoT - Applications

- Smart metering
- Energy savings
- Water conservation
- Supply chain management (SCM)
- Monitoring temperature levels or optimizing store layouts
- Smart cities
- Smart buildings
- Tracking
- Smart farming

IoT Security

- **Device Authentication & Identity Management**
  - Managing the identities of millions of connected devices in IoT is a complex task
  - Traditional security models like password-based authentication or centralised access management are often insufficient for IoT ecosystems
  - Each IoT device needs a unique identity that allows it to securely authenticate with other devices, networks, and cloud services.

  - **Solution**
    - *Device identity management* take advantage of digital certificates and cryptographic keys to ensure each device has a unique, verifiable identity.
    - Public Key Infrastructure (PKI) is a common approach, providing a hierarchical framework of certificates that authenticate devices.

IoT Security

- **Network Edge Security Considerations**
  - Edge devices often operate in less secure physical environments and face more frequent attempts at tampering or unauthorized access.
  - **Device Management**
    - Device Authority’s platform offers automated provisioning, onboarding, and status monitoring of devices.
    - This includes maintaining an inventory, monitoring device health, and enforcing security baselines across all devices.
  - **Data Encryption**
    - Data is sensitive, requiring encryption both in transit and at rest.
    - Protocols such as TLS 1.3 should be used for securing data in transit, while AES-256 is recommended for data at rest.
    - Device Authority enables end-to-end encryption management, ensuring that data remains protected even if intercepted.
  - **Access Control**
    - Implementing role-based access control (RBAC) and attribute-based access control (ABAC) provides flexibility in defining access policies.
    - Device Authority’s platform integrates these models, ensuring that only authorized entities can interact with specific devices or services.
  - **Threat Detection and Response**
    - anomaly detection and AI-driven analysis, can identify unusual behaviors indicative of an attack.

IoT Security

- **Data Integrity and IoT Data Encryption**
  - Protecting the integrity of data exchanged between IoT devices is critical
  - Data integrity is essential for preventing unauthorized modifications.
  - **Solution**
    - *IoT data encryption* is achieved through symmetric and asymmetric cryptographic methods.
    - Symmetric encryption like AES (Advanced Encryption Standard) is effective for encrypting large data streams.
    - Asymmetric encryption, using RSA or ECC (Elliptic Curve Cryptography), is typically used for key exchange due to its higher computational cost.
    - Device Authority’s platform automates the management of encryption keys, supporting protocols such as MQTT with TLS for secure device-to-cloud communication.
    - It also implements hashing techniques like SHA-256 to validate data integrity, ensuring that data remains unchanged during transit.

IoT Security

- **Protecting Sensitive Data in IoT**
  - Protecting data from exposure and ensuring compliance with data privacy regulations is essential.
  - **Data Encryption**
    - IoT devices should use end-to-end encryption standards like AES-256 for stored data and TLS/DTLS for data in transit.
  - **Access Control**
    - Strong multi-factor authentication (MFA) combined with RBAC can limit access to sensitive data.
    - This ensures that even if user credentials are compromised, access remains protected.
  - **Data Storage**
    - Encrypted databases and secure hardware modules like Trusted Platform Modules (TPMs) or Hardware Security Modules (HSMs) provide an added layer of security.
  - **Data Transmission**
    - Secure communication protocols like
      - CoAP over DTLS (Datagram Transport Layer Security)
      - MQTT over TLS
    - are essential for lightweight IoT communications, providing secure channels while keeping latency low.

IoT Security

- **Secure Firmware Updates for IoT Devices**
  - *Secure firmware updates for IoT* involve digitally signing firmware files before distribution.
  - Device Authority's platform supports over-the-air (OTA) updates, enabling businesses to push updates remotely.
  - It uses cryptographic signing mechanisms like RSA or ECC, which ensure that only authorised updates are applied.
  - Additionally, implementing rollback protection prevents devices from being downgraded to vulnerable firmware versions, maintaining the security integrity of each device.

- **Compliance with IoT Security Regulations**
  - *IoT compliance management* involves automating the adherence to regulatory standards.
  - Device Authority's platform offers built-in tools for data encryption, access management, and audit logging, helping businesses maintain compliance.

- **Scalability in IoT Security Solutions**
  - *Scalable IoT security solutions* involve using cloud-based security management tools that can dynamically adjust to changes in device counts and network configurations.
  - Device Authority's platform enables centralised policy management, where security settings can be applied consistently across all connected devices.

IoT Security

- **Edge Device Security Solutions**
    - more data is processed at the network’s edge rather than in centralised data centres. This shift introduces new security challenges
    - Solutions
        - **Trusted Execution Environments (TEEs)**:
            - TEEs provide a secure area on a processor, isolating sensitive operations from the rest of the device.
            - This is particularly useful for protecting cryptographic operations and sensitive computations from being exposed to malware.
        - **Zero Trust Architecture**:
            - Zero Trust principles require all devices and users to authenticate themselves even within internal networks.
            - This includes mutual TLS (mTLS) between edge devices and servers, ensuring that each communication channel is verified and encrypted.
        - **Tamper Detection**:
            - Using sensors to detect physical tampering can trigger alerts or even automatically wipe sensitive data if a device is physically compromised.

IoT Security Best Practices and Solutions

- **Secure Communication Protocols**
  - Use protocols like TLS and DTLS to protect data in transit.
- **Data Encryption**
  - Protect data at rest and in transit using strong encryption standards such as AES-256.
- **Secure Device Management**
  - Implement secure boot mechanisms and secure firmware updates to ensure that devices run only trusted software.
- **Regular Security Audits**
  - Conduct regular security audits and vulnerability assessments to identify and address potential security risks.
- **Intrusion Detection and Prevention**
  - to monitor network traffic and detect suspicious activities.
- **Authentication and Authorization**
  - Implement secure authentication and authorization mechanisms to control access to IoT devices and systems.
  - Multi-factor authentication (MFA) and role-based access control (RBAC) are effective methods to enhance security.

IoT Security Best Practices and Solutions

- **IoT Security Platforms**:
  - Comprehensive security solutions that provide end-to-end protection for IoT devices and systems.
  - These platforms often include features like encryption, authentication, and secure device management.
- **IoT Security Gateways**:
  - Devices that provide secure connectivity and data processing for IoT devices.
  - They act as intermediaries between IoT devices and the cloud, ensuring secure data transmission.
- **IoT Security Software**:
  - Software solutions that offer secure device management, encryption, and authentication mechanisms.
  - These tools help in managing and securing IoT devices throughout their lifecycle.
- **IoT Security Services**:
  - Services that provide security monitoring, incident response, and security consulting.
  - These services help businesses in maintaining a strong security posture and responding effectively to security incidents.

SUNBEAM

Thank you!!!

Devendra Dhande

devendra.dhande@sunbeaminfo.com