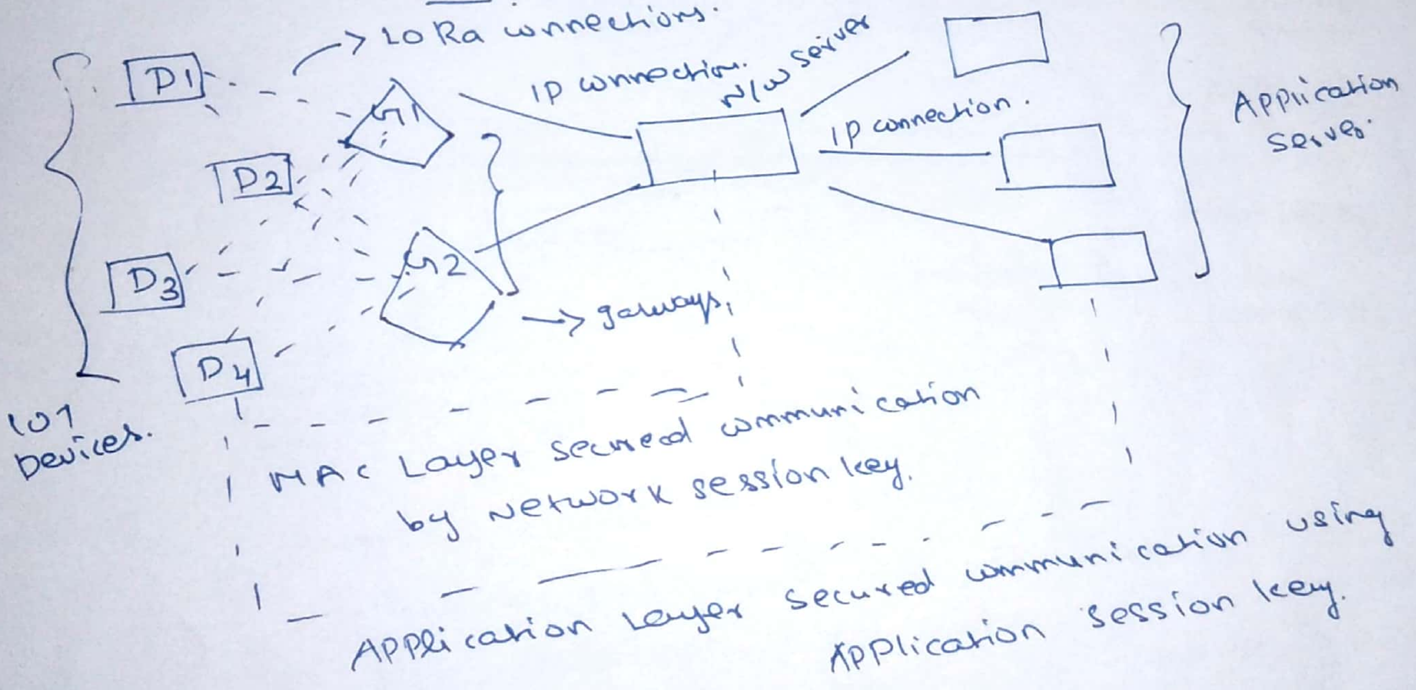
P191113
A. KAMIL KHAN

LoRa:

is Low Range, low data rate, low power wireless Platform technology.

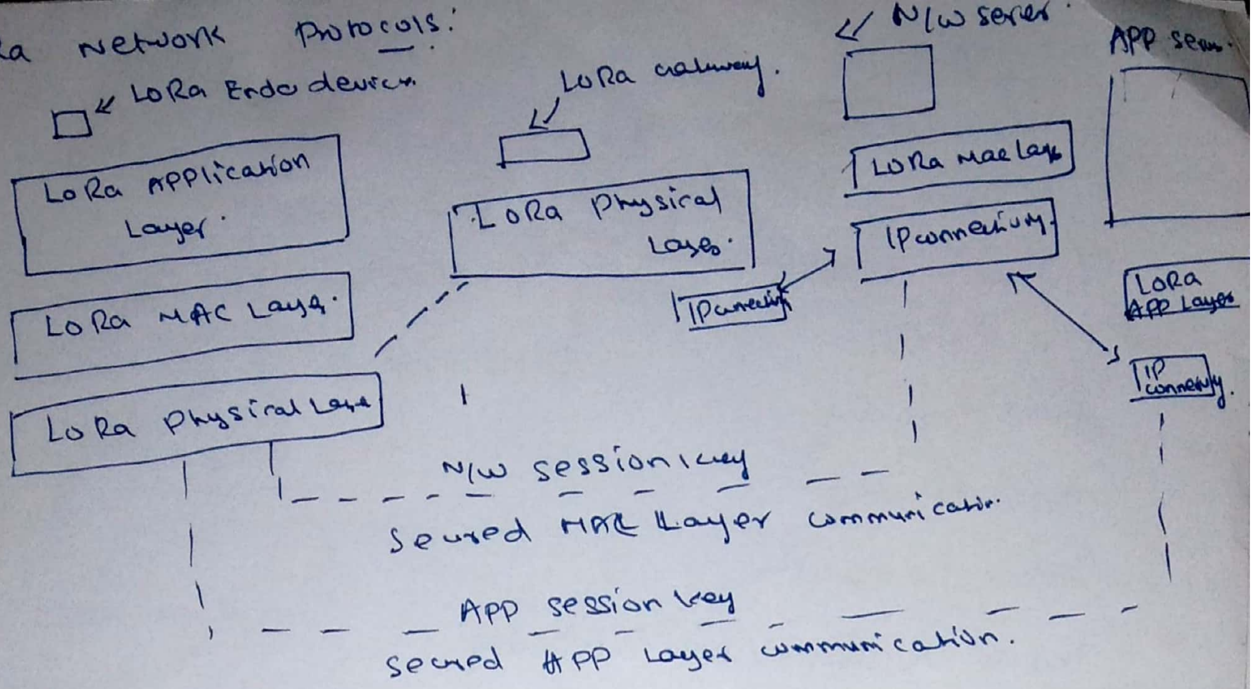
- used to build IOT networks.
- uses unlicensed radio spectrum in the Industrial scientific and Medical (ISM) bands.
- Enable communication between remote sensors and gateways.
- owned by a chip company called semtech.
- Semtech formed LoRa alliance which develops global standards.

LoRa N/w Architecture:

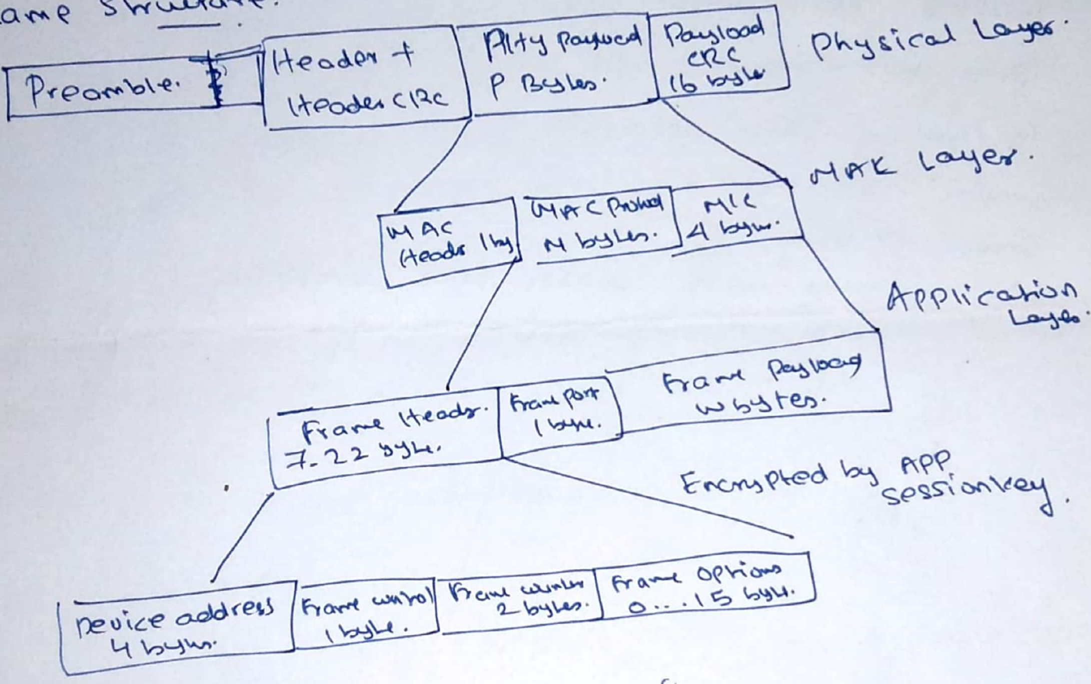

LoRa connections.
IP connection.
N/w server
IP connection.
Application server.
D1
D2
D3
D4
G1
G2
gateways.
IOT Devices.
MAC Layer secured communication by network session key.
Application layer secured communication using Application session key.

- star topology.
- end IOT Device can send message to multiple gateways.
- more than one gateway can receive messages.
- LoRa Radio access technology is used in communication between end device and gateways.
- gateways and network servers are connected via standard IP connections.

LoRa network Protocols:



Frame Structure:



Encryption - AES 128 Algorithm.

MIC Value - MAC Header and MAC Payload Portion is used ~~by join~~ to compute MIC value. with network session key (NwK_Skey). used to Prevent forgery of messages and authenticate end node.

Preamble - duration is 12.25 Ts.

only uplink frame contains Payload CRC.

MAC Header defines Protocol version and message type.

Frame Header - idenity device - 8 bits to idenity network.

frame counter for sequence numbering.

Frame options used to change data rate, transmission Power and connection

[illegible]

Applications:

Air Pollution Montioring.

Agriculture Processing.

Animal Tracking

Fire Detection

Fleet Tracking.

Home security

Indoor Air Quality.

Industrial Temperature monitoring.

Assets management.

Predictive maintainence

Radiation Leak detection.

Smart Lighting

Smart Parking

Waste management, water flow monitoring.

Security Mechanism:

Principle: use of standard, well-vetted Algorithms.
End to End Security.

Fundamental Properties: 1. Mutual Authentication, 2. Integrity Protection. 3. Confidentiality.

Mutual Authentication:

— only genuine and authorized devices are allowed to join genuine and authorized networks.

Integrity Protection:

origin authenticated, integrity protected, replay protected, encrypted. ensures that

- network traffic is not altered
- traffic coming from legitimate device
- not comprehensible to eaves droppers
- not captured and replayed by rogue actors.

Confidentiality: End to End encryption for app. payload between end-devices and application server.

Security Mechanism:

AES cryptographic methods, Each LoRa wan device is personalized with a unique 128 bit AES key and globally unique identifier. (EUI-64 based DevEUI) LoRa WAN networks are uniquely identified by a 24-bit globally unique identifier assigned by the LoRa alliance. EUI-64 identifiers require the assignor to have an organisationally unique identifier (OUI) from IEEE.

uses HTTPS and VPN for application security.

LoRa Vs LoRa WAN:

LoRa - is the signal and contains only phy layer protocol. Robust to noise and tra of

LoRa WAN - links the signal to the application. so it will contain the data transfer layer also. allows data to be sent to any connected devic in the cloud. Bidirectional where as LoRa is Unidirectional.

LORA uses more gateways where as LoRa WAN reduces the no of gatewa

SHVLBILL Summary Sharewise=&co=01&subcd=CA00000165&pTrFilter stno=2015151&pTrFilter sttype=N