Mobile IOT and its LoRa WAN applications

Anurag Chaturvedi
Electrical Engineering
Stony Brook University
New York City, New York, USA
anurag.chaturvedi@stonybrook.edu

ABSTRACT
The Internet of Things (IoT) is the communications paradigm that can provide the potential of ultimate communication. The IoT paradigm describes communication not only human to human (H2H) but also machine to machine (M2M) without the need of human interference. In this paper, We examine the features, advantages and also review the threats to Mobile IOT devices. Additionally, we focus on future IoT key enabling technologies like the new fifth generation (5G) networks and Semantic Web. Finally, we present main IoT application domains like smart cities, transportation, logistics, and healthcare.

Internet of Things (IoT) expansion led the market to find alternative communication technologies since existing protocols are insufficient in terms of coverage, energy consumption to fit IoT needs. Low Power Wide Area Networks (LPWAN) emerged as an alternative cost-effective communication technology for the IoT market. LoRaWAN is an open LPWAN standard developed by LoRa Alliance and has key features i.e., low energy consumption, long-range communication, builtin security, GPS-free positioning. In this paper, we will introduce LoRaWAN technology, the state of art studies in the literature and provide open opportunities.

1.INTRODUCTION

Cost-effective Internet connectivity is an essential issue for the low power embedded devices that are dedicated to a specific task. Conventional wireless communication technologies are insufficient when considered for coverage (communication range), energy consumption and cost. LPWAN aims to solve these problems which can scale and suitable for large-scale deployments for low power end devices. Low Power Wide Area Networks are supposed to operate at low data rates to have kilometer range coverage from dense urban to suburban regions. LoRaWAN, SigFox, NB-IoT, Weightless, and other sub-GHz communication technologies are successfully providing these functionalities, however, LoRaWAN took the attention of organizations, communities, and researchers and have become a popular LPWAN technology.

LPWANs have some common characteristic that distinguishes these technologies within traditional communication networks:

- Low power, the network and end devices should consume low energy.
- Communication, deployment and management cost is an essential issue since a large number of deployments are considered.
- From devices to the applications, the whole eco-system needs strong security mechanism.
- Built-in localization is a plus when indoor deployments are considered.
- Network deployment in dense urban areas leads radio networks to jam within same or adjacent channels. Robust (interference resistance) modulation is a must.
- •End of the day, nodes generate data and this has to be handled properly.

2. LoRa & LoRa WAN Technologies

LoRa is a RF modulation and corresponds to the physical layer in OSI reference model. Whereas LoRaWAN is a MAC layer standard which coordinates the medium.

2.1. Architecture

Network topology of the LoRaWAN is considered as star-of-stars and from the architectural point of view, the system has three main components

(i) network servers,
(ii) gateways (GWs) and
(iii) end nodes.

End nodes communicate with the network server (or data server) via GWs and Node-to-GW communication can be either LoRa or FSK modulation with different data rates and channels. Network servers manage the GWs through standard IP technology and data frames sent through end nodes, received by GWs and routed through the network server. An overview of the LoRaWAN architecture is presented in Figure.

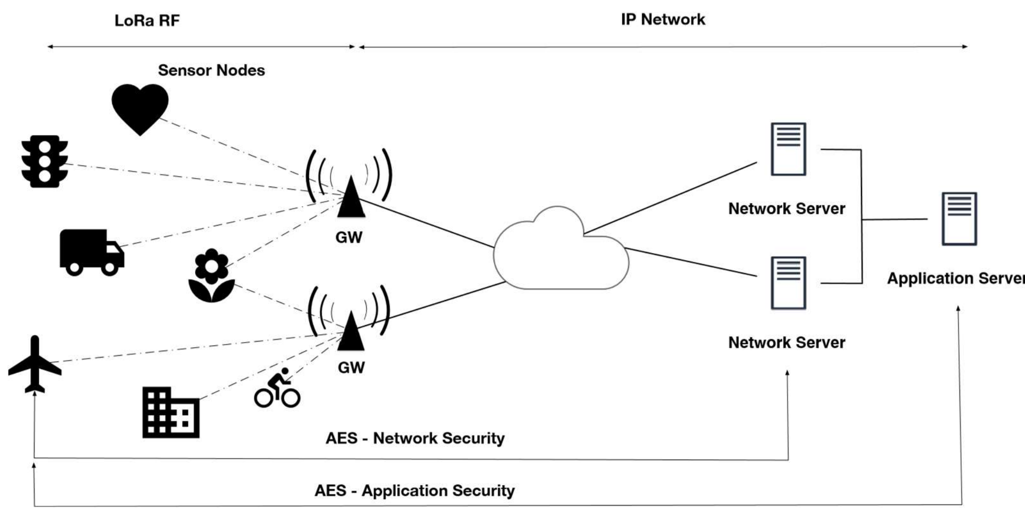


Figure 1 LoRa ARCHITECTURE

LoRaWAN is a MAC layer protocol and aims to solve management issues of the medium and network congestion. Any node using LoRaWAN protocol can benefit the following features provided by the standard;

- Channel management
- Energy efficiency
- Adaptive data rate
- Security
- GPS-Free geolocation

- **2.2 PROTOCOL:**

- OSI Reference Layers
- Layered network design provides seamless communication among different network elements. LoRaWAN layers can be mapped to OSI Reference for better understanding underlying technology as presented in Figure. Generic LoRaWAN network deployments consist of multiple end-nodes, one or more gateways and at least one network server to run a complete

network. LoRaWAN networks are distinguished with classical TCP/IP communication with GWs and end-nodes. Network servers are plain application services that operate over Transport Layer however, all MAC layer functionalities of the whole network are controlled by the Network Server.

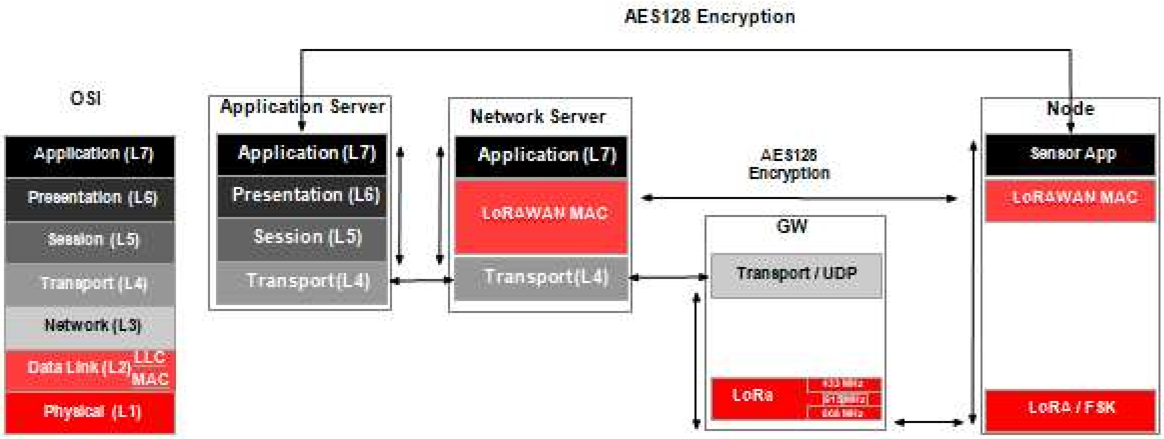


Figure 2 LoRa PROTOCOL

LoRa is a Physical layer technology that operates on L1, and the main function is to transmit

Application layer data to the medium. OSI reference L2 Data Link Layer matches with the LoRaWAN protocol, which defines secure medium access and end-node management strategies. Usually, end-nodes do one simple specific task to minimize energy consumption thus, end-nodes perform L1, L2, and L7 functionalities in OSI reference. GWs are the links between the end-node and the network server. Network Server is the main factor that controls the medium.

2.3 Physical Layer-LoRa

Long **Ra**nge (LoRa) is a physical layer technology introduced by Semtech and intellectual property rights of the modulation are held by the company.

LoRa modulation extends the traditional Spread Spectrum principles to reduce the amount of energy required to transmit bits over the channel. The Data Rate (DR) in attainable communication can be computed from the bandwidth BW (Hz), the Spreading Factor (SF), and the Coding Rate (CR).

The LoRa modulation has better performance than Frequency Hopping techniques in managing interferences. The modulation can tolerate interferences of arbitrary power levels up to 30% of the symbol length with less than 6 dB sensitivity degradation.

SF is the key variable that ensures the quality of service. When using the lower range of SF values, the data rate is very high and air time is low. The higher SFs extend the range but limit the Quality of Service. SFs from 7 to 12 allow orthogonal communications, i.e., different networks can speak simultaneously on the same frequency band without interfering. Table presents SF values against Chirps/Symbol and Demodulation SNR. SF LoRa modulation is based on the representation of each bit of information by multi-chirps information.

Spreading Factor	Chirps/Symbol	Demodulation SNR
7	128	−7.5 dB
8	256	−10 dB
9	512	−12.5 dB
10	1024	−15 dB
11	2048	−17.5 dB
12	4096	−20 dB

2.4 MAC Layer—LoRaWAN

LoRaWAN is a layer two protocol to provide LoRa end devices Adaptive Data Rate (ADR), Security, GPS-free Geolocation, Channel Access and Energy Saving functionalities. LoRaWAN is introduced by LoRa alliance. By version 1.1 LoRaWAN supports roaming and adds additional security features to Class B.

LoRa and other narrowband technologies have to be efficient that’s any overhead will cost more energy or latency. To overcome this problem LoRaWAN uses a quite simple channel management strategy to keep end devices to be cost-effective. LoRaWAN adopts pure Aloha with additional ACK mechanisms to simplify medium access control. MAC layer protocol defines one mandatory and two optional classes for different possible use cases and an overview of this class representations is presented in Figure 3.

2.5 Energy

LPWANs built on the communication range and energy efficiency, this has been investigated among other narrowband technologies. LoRaWAN Class A devices are designed to be the most energy efficient modes of the protocol. Since DL procedure is initiated by successful UL transmissions, end-nodes don’t require power during sleep mode for network operations. Class A devices intended to send a few packets (i.e., 3 packets per day), LoRa transceivers are not active frequently. Despite efficient protocol design, energy consumption highly depended on the hardware implementations.

Semtech SX1272/76 transceivers are the first market-ready chips that have been actively used LoRa end-node manufacturers. According to the datasheets, SX1276 has 100 mW constant RF output at +20 dBm and can have high sensitivity down to −148 dBm.

Class	Battery Consumption	Description

A	Most energy efficient	Must be supported by all the End-Nodes. DL after TX
B	Efficient with controlled DL	Slotted communication synchronized with beacon frames
C	Least efficient	Devices listen continuously. DL without latency.

Figure 3 ENERGY CONSUMPTION

2.6 Security

LoRaWAN has built-in security to protect network protocol and user data. Data through node-to-application and note-to-network-server are protected by AES 128 encryption by four components:

- DevAddr: a 32 bit device identifier.
- AppEUI: an Application unique identifier which as IEEE UI64 address space.
- NwkSKey: a Network session key used to encrypt end-device to network-server communication.
- AppSKey: an Application session key (AES-128 key) used to protect application specific data.

LoRaWAN supports two main end-device activation methods (i) Over-the-Air Activation (OTAA) and (ii) Activation by Personalization (ABP).

2.6.1. Over-the-Air Activation (OTAA)

End-devices require to join the network before the application specific data transmission stage.
End nodes initiate the activation process with an unencrypted Join Request, with AppEUI (8 octets), DevUI(8 octets) and a DevNonce (2 octets). DevNonce is a randomly generated and GW keeps tracks of these values for each end-node.

If the network server replies to the Join Request with a Join Accept, end-node is allowed to join the network. Unanswered messages yield that end-node cannot participate in the network.

Join Accept message contains; a random AppNonce (3 octets), Network Identifier—NetID (3 octets), an end-node address—DevAddr (4 octets), a delay RxDelay between TX and RX(1 octet), DL configuration parameters DLSettings (1 octet) and optional channel frequency list CFList.

Initial Join Request message sent from a node is unencrypted, however, the response message from Network Server (Join Accept message) is encrypted with AppKey. NwkSKey and AppSKey are calculated as follows:

$$NwkSKey = ases128\_encrypt(AppKey, 0x01|AppNonce|NetID|DevNonce|pad_{16})$$

$AppSKey = aes128\_encrypt(AppKey, 0x02 | AppNonce | NetID | DevNonce | pad_{16})$

2.6.2. Activation by Personalization (ABP)

In ABP mode, end-devices store DevAddr, NwkSKey, and AppSKey to eliminate Join Request/Join Response stages. These devices can directly communicate with the Network server with given keys. Storing and securing critical keys is a vital task, any hardware attack can compromise these keys and unwanted network access may occur. Also, ABP strictly binds end-nodes to the specific Network Server where these types of devices cannot benefit roaming features available since LoRaWAN v1.1.

3. APPLICATIONS

3.1 PAXCOUNTER using LoRa WAN

Paxcounter is a proof-of-concept device for metering passenger flows in real time. It counts how many mobile devices are around. This gives an estimation how many people are around. Paxcounter detects Wi-Fi and Bluetooth signals in the air, focusing on mobile devices by filtering vendor OUIs in the MAC address.

Intention of this project is to do this without intrusion in privacy: You don't need to track people owned devices, if you just want to count them. Therefore, Paxcounter does not persistently store MAC addresses and does no kind of fingerprinting the scanned devices.

Data is transferred to a server via a Lora WAN network, and/or a wired SPI slave interface. It can also be stored on a local SD-card.

3.1.2 SCANNING OF MAC ADDRESS AND WIFI HOTSPOTS

The Paxcounter code stores scanned MAC addresses in the device's RAM, and keeps it in RAM temporary for a configurable scan cycle time (2 seconds). After each scan cycle the collected MAC data is erased from RAM. MAC data never is transferred to the LoRaWAN network. No kind of tracking and no persistent storing of MAC data or timestamps on the device and no other kind of analytics than counting is implemented in this code. Wireless networks are not touched by this code, but MAC addresses from wireless devices as well within as not within wireless networks, regardless if encrypted or unencrypted, are made visible and scanned by this code. The same applies to Bluetooth MACs, if the bluetooth option in the code is enabled."

Automatic Beacon Monitoring is the key to scan the Wi-Fi MAC addresses and Wi-Fi Hotspots as stated above that the latest android versions allow and send continuous wi-fi signals in search of a Wi-Fi beacon. Thus, enabling us to correctly count the passengers.

3.1.3ACCESSING THE DATA

The data collected by the ESP8266 is sent to a cloud and can be accessed by any device with a internet connection. The data stored in the cloud is then collected by our LoRa nodes available.

3.1.4 DIFFERENT TYPES OF PAXCOUNTERS:

- DynaPCN 10-20 Automatic Passenger Counter

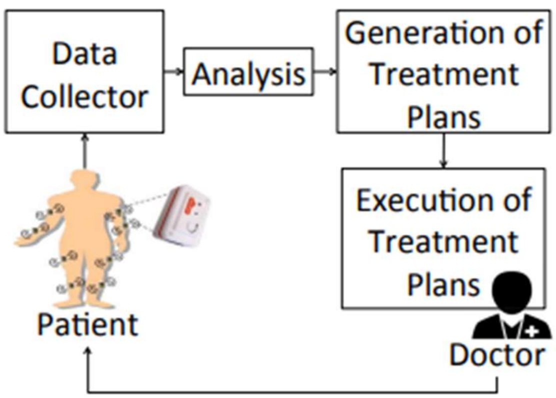
- Infrared Sensor based Automatic Passenger Counter
- Millimeter Wave Sensor based Automatic Passenger Counter
- Electronic Registering Farebox based Passenger Counter
- Weight Sensor based Passenger Counter.

PARAMETERS	ESP8266 Sensor	Dyna PCN Sensor	mm Wave Sensor	Electronic Registering Farebox	Weight Sensor
Cost	Low	High	High	High	High(Require more number of sensors)
Installation	Easy	Difficult (More Wires)	Difficult	Easy	Difficult (Disturbs the complete infrastructure)
Accuracy	High (97-99%)	High (95-99%)	High (97-99%)	Medium (70-85%)	Low (50-60%)
Man Power	Low	Low	Low	High	Low
Security	High	High	High	Low	Low
Maintenance	Once in a year	Daily Cleaning	Daily Cleaning	Daily Cleaning	Once in a month

3.2 Health Monitoring Device

- It consists of four main components. The first component is the "Data Collector" to gather data from different medical sensors.

- It sends collected health metrics to the second component of , the "Analysis" component. The latter is used to analyze health metrics and generate diagnosis reports.



- health data. The analysis results should be accurate and consistent to generate relevant diagnosis reports and adequate treatment plans.

- These are processed by the third component, the "Treatment Plans Generator", to generate adequate treatment plans.

- The generated plans are validated and executed by a medical expert via the fourth component, the "Treatment Plans Executor".

3.2.1 Challenges

- It is necessary to guarantee the privacy of patients' data and the security of links between the patient and his/her doctor.
- It is important to develop low-cost and low-power network protocols. Moreover, we need network protocols suitable for wide area communication.
- It is also mandatory to develop analysis approaches to efficiently and rapidly process collected

	Avg Range	Energy Consumption(mA)	Min Hardware Cost	Max Data Rate
LoRa	60 KM	Idle mode: 2.8 mA Continuous Receive Mode: 14.2 mA Send Mode: 38.9 mA	Transceiver: $10 Gateway: $250	50 kbps(Downlink) 50 kbps (Uplink)
GPRS	60 KM	Idle mode: 20 mA Continuous Receive Mode: 130 mA Send Mode: 2000 mA	Transceiver: $50 Gateway: $10000	85.6 kbps(Downlink) 14 kbps (Uplink)

4. Conclusion

The different types of available APC systems on the market have been shortly described; the applications show that the use of technologies to detect the location of the vehicle (AVL) is nowadays consolidated and evidently necessary to integrate the information coming from the APC systems.

Finally, no technology is better than the other ones in absolute terms: the final system performance depends on the objectives (i.e., the use of the collected data), on the size of the fleet of vehicles to be monitored, on the need of integration with other technologies and programs which are perhaps already activated within the public transport company, on the numerousness and sampling frequency required, on the type of vehicles and on other factors connected to the service to be dealt with.

You could say that LoRa is “You send few data but they will go further”.

This technology has great applications in reading sensors / meters for sending data over long distances.

You could say that the LoRa radios come from the factory with a frequency or band pre-defined in our case 915MHz, There are some radios that allow working in all bands, since the chip can make the change but the RC filters output the antenna are the drawback given that they are fixed values.

Maximum Distance LoRa:

Max 15-20Km suburban / outdoor, 2Km urban, depends on the quality of the Radio, line of sight, walls walls, etc.

Low RX current of 10.3 mA, 200 nA retention log, according to the RFM95 datasheet.

5. REFERENCES

1. A more complete and technological analysis had been published in "Dalla Chiara, Deflorio, Pinna (2010), "Automatic passenger counting and vehicle load monitoring/ Rilievo automatico dei passeggeri e del carico dei veicoli, Ingegneria Ferroviaria, Ingegneria Ferroviaria – Rome, February 2010", of which this article is a synthesis and updating.
   IBIS (I/O Buffer Information Specification), RS-485, RS-232 o J1708, Firewire, USB, HDMI (High-Definition Multimedia Interface), Light Peak; in some cases, or on some analysers of specific design, also with other interfaces or with additional switch outputs.
2. BOYLE D.K. (1998), "Synthesis of Transit Practice 29, Passenger Counting Technologies and Procedures", Transit Cooperative Research Program, 1998
3. PAVLIDIS I., FRITZ B., SYMOSEK P., PAPANIKOLOPOULOS N. P., MORELLAS V., SFARZO R. (1999), "Automatic Passenger Counting in the HOV Lane", Minnesota Department of Transportation, 1999.
4. T. O. Takpor and A. A. Atayero, "Integrating internet of things and ehealth solutions for students healthcare," in Proceedings of the World Congress on Engineering 2015 Vol I WCE 2015, July 2015, pp. 256– 268.
5. S. Zawoad and R. Hasan, "The enemy within: The emerging threats to healthcare from malicious mobile devices," CoRR, vol. abs/1210.2149, pp. 1–9, 2012.
6. IEEE, "IEEE standard for information technology– local and metropolitan area networks–part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low rate wireless personal area networks (wpans)," IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003), pp. 1–320, Sept 2006
7. H. D. Gadi, R. V. Murthy, R. S. M, and N. V, "Antennae Location Methodology for a Telecom Operator in India," CoRR, pp. 1–20, 2014
8. Mdhaffar, A., Chaari, T., Larbi, K., Jmaiel, M., & Freisleben, B. (2017, July). IoT-based health monitoring via LoRaWAN. In IEEE EUROCON 2017-17th international conference on smart technologies (pp. 519-524). IEEE.
9. Sethi, P., Sarangi, S. R. (2017). "Internet of Things: Architectures, Protocols, and Applications".
10. Hindawi Publishing Corporation. 1-25.
11. Kim, D. H., Lim, J. Y., Kim, J. D. (2016). "Low-Power, Long-Range, High-Data TransmissionUsing Wi-Fi and LoRa". 6th International Conference on IT Convergence and Security. 1-3.
12. Anand, P. (2015). "Towards Evolution of M2M into Internet of Things for Analytics". IEEE Recent Advances in Intelligent Computational Systems. 388-393.
13. Gupta, R., Gupta, R. (2016). "ABC of Internet of Things : Advancements, Benefits, Challenges,Enablers and Facilities of IoT". Symposium on Colossal Data Analysis and Networking. 1-5.

14. So, J., Kim, D., Kim, H., Lee, H., Park, S. (2016). “LoRaCloud: LoRa Platform on OpenStack”.2016 IEEE NetSoft Conference and Workshops. 431-434