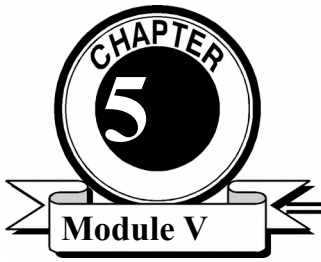

Mobility and Settings

Syllabus :

Introduction, localization, Mobility management, Localization and handover management, Technology considerations, Performance evaluation, Simulation setup, Performance results. Identification of IOT data formats. IPv6, identifiers and locators, tag etc.).

5.1 Introduction

- In the Internet of Things (IoT), each object, person, or entity features a virtual counterpart in internet. Beyond ubiquity, resilience, and other main features of IoT, there is a tendency to be accelerated regarding the mobility of devices, either being transported by humans (smart phones are an example) or by another carrier, or being mobile by itself, sort of a robot or a UAV.
- Therefore, it appears to be useful to consider state of the art of the mobile devices that these days are connected to Internet and within the future are going to be a major a part of the IoT, so as to underline which protocols, architectures, and technologies are going to be more useful. Mobile devices are also seen during a cloud computing environment; the result are often seen as Mobile Cloud Computing that's also interesting here, with a selected regard to IoT.
- Mobility in IoT consists of the following points :
    - Architectures and protocols for the mobile devices utilized in IoT
    - Device mobility is supported by Security Protocol
    - IoT involves Mobile Cloud Computing
    - Issues of Power Consumption related to the devices involved within the IoT
    - Enabling of technologies for the mobile devices in IoT
    - Optimization of network focused on mobility aspects
    - Mobility patterns supports machine learning applications
    - Green mobility, smart mobility, and e-mobility in IoT
    - Wearable devices
    - IoT includes M2M (Machine to Machine)

5.2 Localization

- With the rapid development of wireless technology, Internet and Internet of Things are to be envisioned to be the integral part of our day to day life. Localization-based services are among the foremost attractive applications associated with the IoT.
- They are actually, because of the deployment of networks of sensors, ready to collect and transmit data so as to determine the targets position. The localization systems are in two categories: device-based and device-free systems. In device-based techniques, localization is linked to the target, and localization is decided because of the cooperation with other deployed wireless devices. Whereas within the device free systems, the target doesn't include any wireless device consistent with the localization.
- Many localization algorithms and systems are developed for both indoor and outdoor environments by means of wireless sensor networks. To obtain higher accuracy localization, additional hardware equipments are utilized maximum of the localization solutions, this increases the cost and considerably limits the location-based applications. The Internet of Things (IoT) integrates many technologies, like Internet, Zigbee, Bluetooth, infrared, Wi-Fi, GPRS, 3G, etc, this enables different ways to get information about the location of various objects. Location-based service may be a primary service of the IoT, while localization accuracy may be a key issue.
- Originally, the concept of IoT was proposed by professor Ashton of MIT Auto-ID within the research of RFID in 1999. During research primary focus included RFID, to obtain the object information by browsing the Internet address or database entry to achieve recognition for objects.
- After that, the scope of IOT has been enlarged to several areas like environment surveillance, health care, smart home, logistics, and forest-fire prevention and so on. In 2005 ITU gave an Internet reports named “The Internet of Things”. In this reports some technologies for IOT as well as opportunity, challenges are acknowledged.
- In 2009, a report named “Internet of things, An action plan for Europe”, was drafted by European community in which they insisted on adopting a proactive approach so that they can play a leading role and people can reap the benefits of it.
- Many researchers has tremendous interest in IOT, and have made many creative achievements. Atzori has evaluated several integrated technologies and communication solutions, also has several concrete applications, like affect transportation, healthcare, smart environments and private and social domain.
- They proposed a practical architecture in IOT, which helped in providing environment monitoring and localization services. A communication protocol design approach was involved to construct network which can span several wireless radio networks of varying link-level characteristics was suggested by Silverajan and Harju.

- For IOT, a highly interoperable and lightweight event-based framework has been offered. Bolhi hold the opinion that IOT can help in beneficial of society and can offer new enhanced services and application and also economics and price issue while providing sensor based service.
- Khoo reviews some necessary issues and technology to enable RFID Technology successfully adopted in IOT application. Huircán and Cho used Zigbee protocol in WSNs for presenting examples of localization system which is suitable in IOT.
- In IOT, data acquisition and sensing usually using wireless sensor technology, thus concerning the localization issue can be referred to WSNs in some extent. In WSNs, many localization Algorithms are developed, which can be categorized into one among them as : range-based localization and range-free localization.
- **Range-based localization has two phases :** Ranging and position computation. In the initial phase it makes the use of some ranging methods such as TOA (Time of Arrival),TDOA (Time Difference of Arrival), AOA (Angle of Arrival) and RSSI (Received Signal Strength Indicator) this is used to obtain the distance between two nodes.
- With the information of reference node attached with RSSI, the blind node (refers the node or target)and calculate its own coordinate by using some mathematical methods, like Trilateration, Triangulation, and Maximum likelihood estimation.
- In TOA based localization system the synchronization between transmitting equipment and receiving equipment additional hardware is required; otherwise, this leads in resulting tremendous distance estimation error due to small timing error.
- In TDOA systems they call for expensive hardware as it shares similar drawbacks as in TOA systems. Moreover, TDOA employs ultrasound ranging technique, which requires density deployment as the transmission distance of ultrasound is merely 20-30 feet. AOA localization system can be considered as complementary technique for TOA and TDOA.
- Installing angle measuring equipments allows the nodes to estimate the distance according to relative angles. Therefore, it is not advised to be used in large scale sensor networks.
- On the contrary, majority of shortcomings mentioned above are overcome using RSSI technique. To translate signal strength into distance it utilizes some signal propagation models, either from theoretical or empirical. Thus, additional hardware are not required. However, this technique severely affects the accuracy of ranging estimate by the causes of multi-path fading, noise interference, and irregular signal propagation. Although there are many drawbacks, in this technique some special methods are used to alleviate this suffering and proper measures are taken to help in accuracy of localization which improves to meet requirements of most of the application systems. This can be achieved by employing regular deployment of node, region partition and localization refinement.
- In RSSI localization systems, by using received signal strength distance estimation is done between transmitter and receiver based-on some signal propagation model should be accomplished previously. The log-normal shadowing model is widely used propagation model and is expressed as :

$$Pr(d)[dBm] = Pr(d_0)[dBm] - 10\,n \log 10(d / d_0) + x\sigma\,[dBm] \quad \ldots(1)$$

- where d is the distance between transmitter and receiver, d0 denotes reference distance, Pr (d) denotes the power received, Pr (d 0) denotes the received power of the point with a reference distance d0, n denotes exponential attenuation factor to distance which is related to environment, and xσ represents Gaussian random variable which reflect the change of power when distance is fixed.
- The simplified shadowing model :

$$Pr(d)[dBm] = Pr(d_0)[dBm] - 10\,n\,lg(d / d_0) \quad \ldots(2)$$

- Usually, d0 is selected as 1 meter, so we have:

$$RSS[dBm] = Pr(d)[dBm] = A - 10\,n\,lg\,d \quad \ldots(3)$$

where A is the received signal power of receiver from a transmitter one meter away.

- Our system uses the CC2430 chip, which is system-on-chip solution for 2.4GHz IEEE 802.15.4/ Zigbee with the characteristics of low-power and low date rate (up to 250kbps). CC2430 has a build-in register called RSSI _ VAL for storing RSSI value, and the power value on RF pin is :

$$RSS = RSSI\_VAL + RSSI\_OFFSET\ [dBm] \quad \ldots(4)$$

- Empirically, the RSSI _ OFFSET can be assigned -45dBm.

5.2.1 Localization Scheme

- To provide more intelligent services it is hoped to get location information for many systems. For example, a mobile advertising business which needs to know the position of individuals for pushing services (discount shopping news), to seek out a nearest cafe consistent with current position, to trace somebody within the stadium.
- Some systems requires high precision positioning requirements, because the situation accuracy directly impacts the performance of entire application system. For instance , cargo tracking in large warehouse, wharf cargo scheduling, cargo location on crane tower.
- A localization method, consists of two phases : region partition and localization refinement. This method has a basic idea of dividing the target region into small grids by deploying sensor nodes regularly, and the nodes reside on the vertex of the grid.
- The grid during which the blind nodes current located are often easily determined by comparing their RSSI values. The shorter the distance, the larger the RSSI value is, and vice versa. During this, to satisfy the accuracy requirement by employing a trick algorithm determines grid position coordinates.
- The interactions between blind node and beacon nodes are described in Fig. 5.2.1, during which the beacon nodes accumulate RSSI values 8 times and return the average to blind node.

- In some systems it may carry to keep it up more times of accumulations, but this may affect the timeliness because two RSSI accumulations need a time spacing interval, and fewer RSSI accumulations will make the system easier subject to environmental impact. Therefore, selecting a good accumulation number and is also particularly important to the system performance.

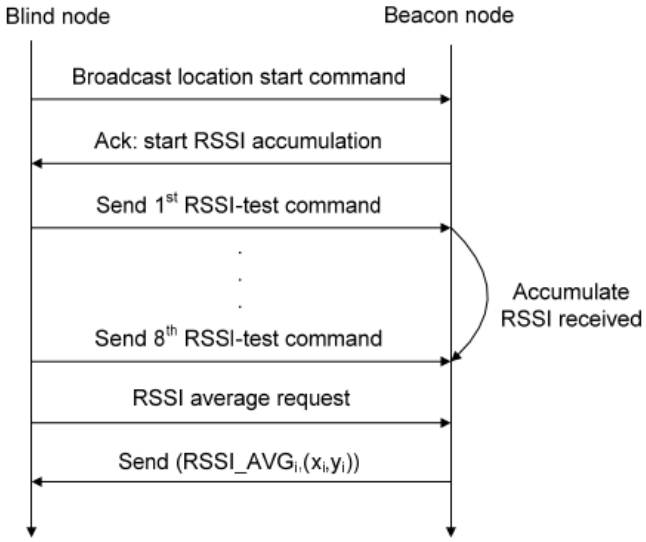

Fig. 5.2.1 : Interaction between blind node and beacon nodes to obtain RSSI values

- The overall flow chart of localization computation in blind node is shown in Fig. 5.2.2. For the blind node as well as beacon nodes, the localization process pseudo-code is shown below.

1. Algorithm 1 Blind node localization process algorithm

Broadcast location start command :

```
Wait for Ack;
IF receive Ack Then
For accumulate times=1:8
Do
Send RSSI-test command.
Wait 20 ms.
Send RSSI average value request command.
Temporarily store each beacon nodes' (RSSIi, (xi, yi)) (1<=i<=N)
IF (N>=4) Then
Select up to four groups.
IF four groups can form rectangle Then
Use formula (7) (8) to calculate (x, y).
Else
IF in four groups exist a large RSSI Then
Use last location to determine the direction θ.
Use RSSI value to get distance d.
Else
Calculate (x, y) in two groups by dividing the four groups.
```

Else
Return.

For beacon nodes the process is as follows:

2. Algorithm 2 beacon node localization process algorithm

Do
Wait for RSSI accumulation start command.
Send Ack to blind node to start RSSI test.
For each received RSSI-test from blink node Do
IF receive RSSI average request Then
Calculate the average value of accumulated RSSI and return to blind node.
Else
Accumulate RSSI value.
While the application is running.

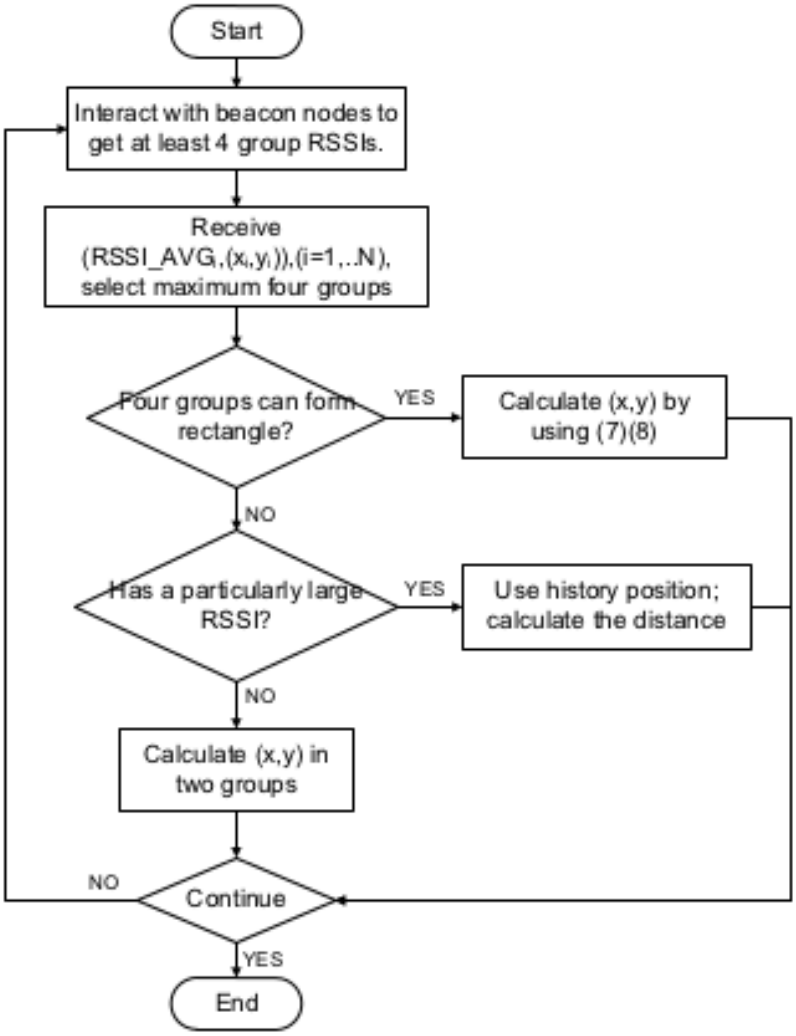

Fig. 5.2.2 : Blind node localization process flow chart

5.2.2 Elements of Localization Process

- Translation which means converting data from one form to another is a part of localization process. Other elements area as follows :
  - Availability of the product to target market
  - Accessibility of the product to other market by modification of content
  - Modification of design and layout in accordance with translated text.
  - Increasing efficiency for local requirements such as currency
  - Displaying dates, addresses and phone numbers in proper local formats
  - Considering rules and regulations of local areas
- Wireless sensor network is one of essential components in the IoT, in which it collects and processes the environmental data (e.g. temperature, humidity, and object movements) using hundreds of sensors in a node.
- The location information which is collected by sensor nodes is made available to base station (a.k.a., data center, sensor fusion, access point) responds and reacts to this environmental data.
- Fire alarm, energy transfer and emergency request are established on the data center, a way to identify the location information of all the nodes at the data center is of great importance are various actions in IOT.
- During this approach, i.e. localization at data center after the information is collected by data sensor node location information is then sent to the data center. Using the obtained distance information, data center constructs a map of sensor nodes.
- For performing localization process at the data center, it is necessary to provide pair wise distance information between each sensor pair. It has been observed that information regarding location can be found accurate only if, exact location of sensor nodes (also called anchor nodes) is provided.
- The localization process has Major problem that the data center does not have the enough information of the sensor nodes.
- Moreover, it is difficult to recover the original Euclidean distance matrix D from a subset of its entries because for the unknown entries there are many completion options.

5.3 Mobility Management

- Smart Mobility is a MaaS (Mobility as a Service) application that provides the information about the park and ride facilities, encouraging drivers to shift from private cars to sustainable transport modes, such as bus, car sharing and bike sharing, for being a part of their journey.
- Specifically, Smart Mobility aims in contributing to reducing traffic caused by private vehicles in the city apart from that helps the drivers in going towards low traffic areas by introducing real-time mobility information from various sources, using an ecosystem of IoT devices.

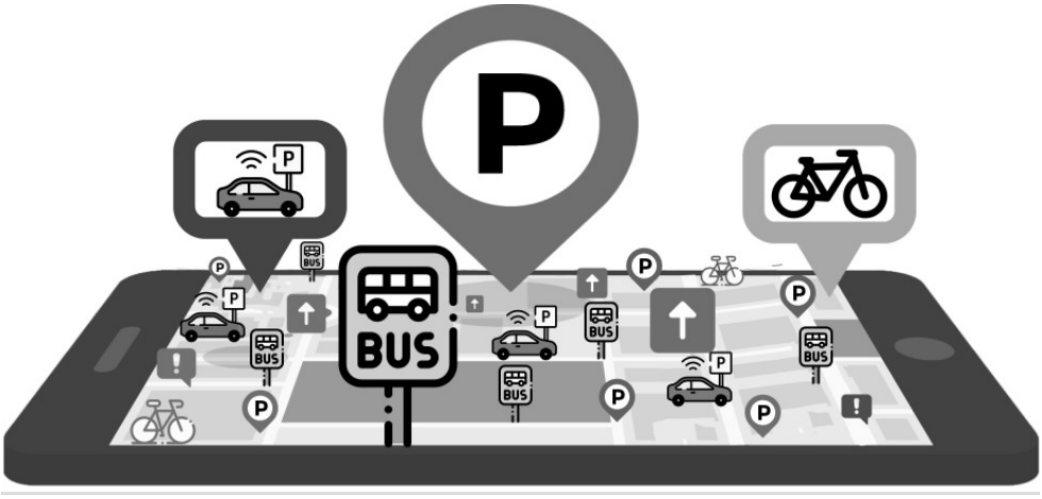

Fig. 5.3.1 : Smart mobility integrates sustainable transport modes

- In recent years, amount of connected devices has significantly grown in everyday life as a crucial part of the IoT. IOT has remarkable volume of devices. The IOT accentuates the connectivity between physical devices and data and also contributes the transportation systems supporting the vision of smart city.
- Smart cities, mostly, are enriched for more and more sophisticated services especially in terms of citizen's mobility. Multi-mobility integrates various modalities of transportation like private car, bus, car sharing, and bike sharing.
- The multimodal mobility has a growing popularity especially in urban centers with the problems recurring associated with the congestion, parking and lack of space. It is essential for the people to drive a car because it is an opportunity for autonomy.
- A driver going from sparsely populated areas to a relatively big or vast city may be motivated to park the private car and it becomes necessary to choose their alternative transportation options wisely.
- Therefore, issues varies and newly occurred issues are now related to finding a parking slot, catching the bus on time, or choosing an appropriate alternative.
- In the context of MaaS, that IoT acts as an enabler to integrate the private and public transport. Every element of Smart Mobility i.e., parking area, bus stop, car or bike sharing station are considered as an extremely sophisticated network due to miscellaneous connection of IoT devices, individually with its proprietary protocols, specifications, and characteristics.
- Consequently, it is necessary to handle such elements, which consists of both physical (commercial instruments, custom sensor boards etc.) and logical (other web platforms, open data services etc.) devices independently.

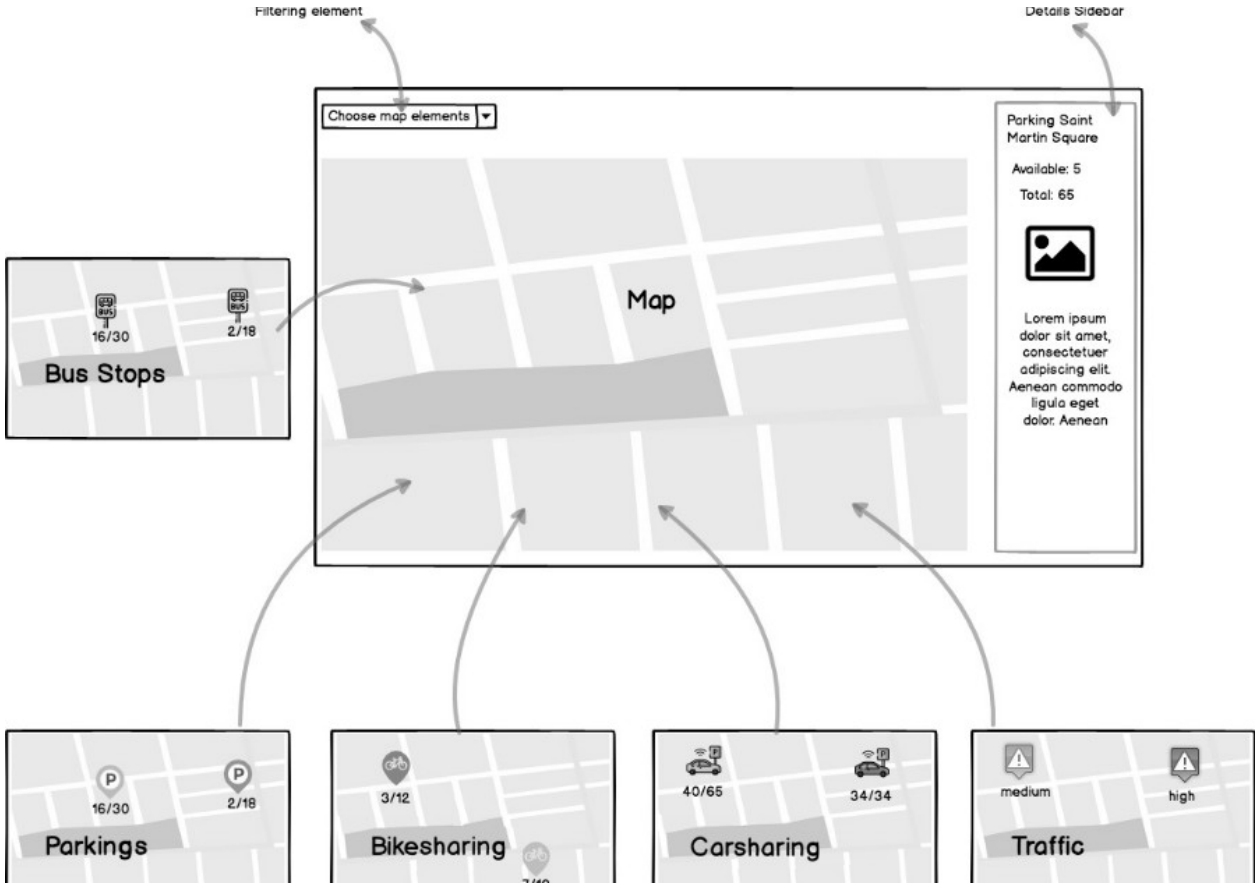

Fig. 5.3.2 : Smart mobility integrates physical and logical devices

- Smart Mobility is designed on top of a micro-service architecture especiallydesigned for the IoT, it is a collection of independently deployable and loosely coupled basic services.
- Micro-service executes its own process, communicates with lightweight mechanisms, such as HTTP resource API, and implements a definite feature. Smart-Mobility is CRS4 Micro-service Core for the IoT (CMC-IoT) uses the micro-service architecture.
- This helps to integrate various IoT devices and services. The services are composed of smaller entities, referred to as devices, this provides only a part of service functionality and has specific location within the city.
- Examples are bus stops, parking areas, and sharing stations among others. CMC-IoT extends CMC (CRS4 Micro-service Core) And implementing a general-purpose micro-service architecture is the fork of our first open source project.

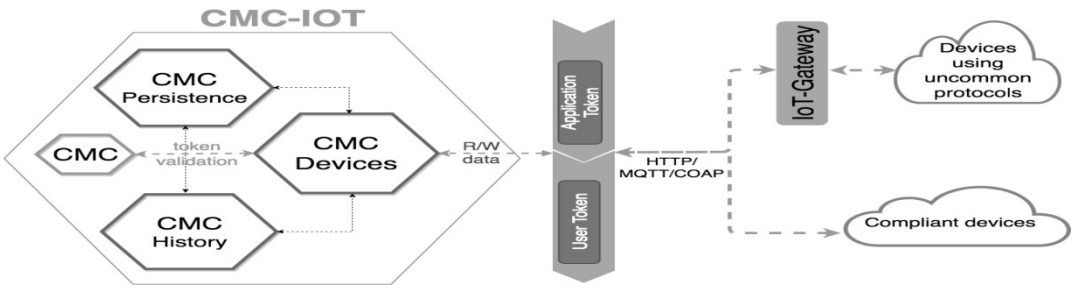

Fig. 5.3.3 : CMC-IoT, the CRS4's micro service architecture for the IoT

- Regardless of, the conventional and business-oriented MaaS platforms, such as UbiGo and myCicero, Smart Mobility does not provides any booking or payment services or any travel planner functionality.
- To the best of our knowledge, no application provides information regarding parking areas occupancy. Of course, drivers may be alerted regarding empty parking places either by displays on street signs or by looking at the map on the smartphone.
- Nevertheless, Smart Mobility focuses on parking areas providing firsthand information to the drivers trying to find parking and desiring to adopt an alternative transportation option, park and ride facilities.
- A real case study has been set up in the metropolitan area of Cagliari. Before entering the city center, the driver, using Smart Mobility, the drivers can check availability of parking spots within the monitored parking areas that are close to his/her position. Moreover, he or she does not have to drive around the city looking for a free parking spot. SmartMobility helps to view real-time traffic information on the main city roads.
- Once a parking lot has been identified and chosen, the user can check on the application the availability of mobility services around the parking area, such as bus stops and sharing services, and their reliability. So, he or she can choose the one most suitable as per his or her needs or walk to the final destination.

5.4 Localization and Handover Management

- Mobility and IoT are coming up with endless possibilities for your organization – for intelligent resource utilization – or it can be people or machines, strategic process optimizations to augmented customer experiences, there are several new values in the offing.
- And with strong links to Artificial Intelligence, Big Data, Machine Learning and Robotics, this ‘connected technology revolution’ has the potential to disrupt and force you to adapt new ways, and builds new business models – where human and machines correlate like never before. The quicker you realize and adapt, the faster you win in this digital age.
- However, following challenges may hamper the Mobility and IoT initiatives :
    - Designing a strategy against dynamic IoT and the evolving of Mobile landscape
    - Depending on legacy infrastructure that’s ill-equipped to handle a wide variety of sensors and controllers connecting myriad applications, products, services, vendors and customers
    - Managing network complexities, which is a costly and time-consuming effort
    - Lack of advanced data and analytics capabilities- a must to manage and harness insights from a wealth of data flow, continually and in real time
    - Addressing security concerns, which is critical for modern embedded, mobile, and IoT devices.

- Many businesses find answers for their IoT and Mobility needs and successfully get connected. They help them in their Augmented Reality (AR) and Virtual Reality (VR) journey. Mobility and IoT based Digital Services Practice stems out of to be proven expertise in designing, deploying, administering and managing the whole IoT / Mobility ecosystem.
- Handover management develops a wide range of solutions including :
  - Mobility Solutions
  - AR/VR solutions with 2D/3D technologies
  - Alexa, Wearables and Internet of Things (IoT)
  - Proximity and Location based solutions
  - Connected Fleet Management
  - Tele-Health
  - Digital Twins
  - Analytics

5.5 Technology Considerations

Table 5.5.1 : Classification and comparison of localization technique

Physical measurements		**Accuracy**	**Hardware cost**	**Computation cost**
Distance	RSS	Median	Low	Low
	TDoA	High	High	Low
Angle	AoA	High	High	Low
Area	Signal reference	Median	Median	Median
	Multi-reference	Median	Median	High
Hop-count	Perhop distance	Median	Low	Median

- The above Table 5.5.1 shows the Classification and comparison of localization technique.
- There are many other technologies competing with smart phones to achieve the same goal. The technology requires specific hardware, including infrared, ultrasound, RFID and Zig-bee, etc. They are mainly classified into three categories: Wi-Fi, Camera and Bluetooth.

5.5.1 Wi-Fi Based Localization

- In general, the Wi-Fi positioning system (WPS) is employed if the GPS becomes inadequate. It allows to locate a device (e.g., smartphone) using the detection of a Wi-Fi network. The

localization via Wi-Fi makes use of the known position of certain Wi-Fi networks in order to determine the position of a device connected to this network. Thus, the precision depends on the power of Wi-Fi access point.

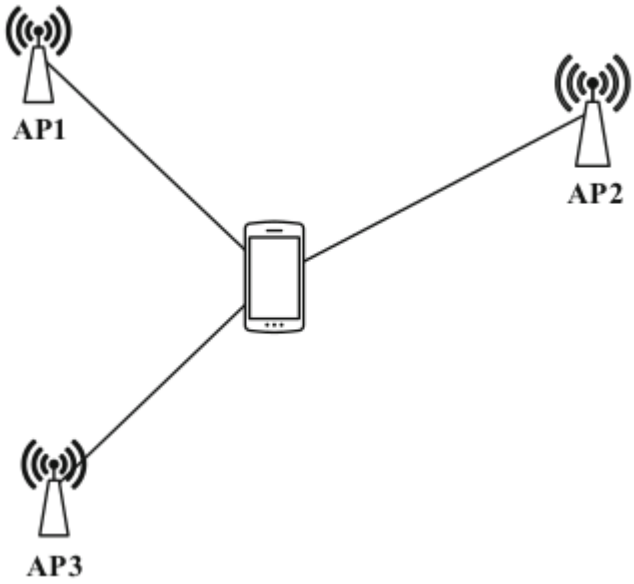

Fig. 5.5.1 : Localization based in Wi-Fi

5.5.2 Camera Based Localization

- Werner presents a localization system inside the building based on camera as the cameras are considered as the most important sensors of smart-phones and provide a computer vision for the localization.
- Although the positioning technique is designed to combine an image recognition system with a distance estimation algorithm to achieve the coordinates of the object to be located using the camera of a smart-phone, this system has a positioning error of 4.71 m.
- In order to reduce the increasing costs for the positioning system and to enhance its practicability, researchers have used the integrated sensors of smart-phones.
- In addition, there is another approach to localize integrated on a smart-phone which uses an optical camera and an orientation sensor. The authors use the fingerprint of the Wi-Fi signal based on the KWNN algorithm to determine the neighbors.
- Thereafter, an average weighted exponent algorithm with image functions is drawn out by the Scale-Invariant Functional Transformation (SIFT) and its orientation sensor. The output will consequently limit the random image choices for a mobile node on a smart-phone in order to refine the results according to a multithreaded mechanism. Figure 5.5.2 shows an example for localization based in camera of smart-phone.

Fig. 5.5.2 : Localization based on the camera of smartphone

5.5.3 Bluetooth Based Localization

- Bluetooth (standard IEEE 802.15), is a short-range data communication protocol. It uses a short distance radio technique to simplify connections between electronic devices.
- The position of a mobile device using this technology is considered as the same as the individual cell with which it communicates.
- However, the major disadvantage of such localization system is its accuracy that depends highly on the number of the installed cells and their sizes. Various localization systems have been tested using Bluetooth technology with very encouraging results.

5.5.4 Tag Based

- In this section, we present various localization methods using ultrasonic, infrared, RFID and UWB sensors. These approaches need specific hardware to realize the localization functionality based on tags. Figure 5.5.3 shows an example of localization based in tags.

Fig. 5.5.3 : Example of tag-based localization

1. UWB : Ultra Wide Band tags localization

- The Ultra Wide Band is a new type of wireless radio which is characterized by a large bandwidth respecting the central frequency of the emitted waves.
- There are two factors behind the UWB concept: relatively large bandwidth and relatively small center frequency. While the large bandwidth allows for precise time resolutions and in well-structured systems a better confidentiality, the low central frequency allows a better passage of the waves through different materials.

2. Ultrasonic tags localization

- The Ultrasonic technology is used to consider the objects position. The most ultrasound tracking systems are combined with another technology to get a distance estimation of the transmitter / receiver. The receiver successively receives the ultrasonic.
- Thereafter, it estimates their separating distance in function of the average speed of displacement. The emission of ultrasonic waves is generally directional which causes difficulties to lead precisely the transceiver.

3. RFID tags localization

- This technology permits remotely to identify, to track, and to know the characteristics of an object thanks to a radio-emitting tag linked or incorporated into the object itself.
- Therefore, the RFID technology allows reading tags even without a direct sight and can go through fine materials layers (paint, snow, etc.).
- The RFID tag is additionally composed of a chip connected to an antenna, encapsulated in a support and read by a reader that captures and transmits the data. Figure 5.5.4 shows an example of localization based in RFID tags.

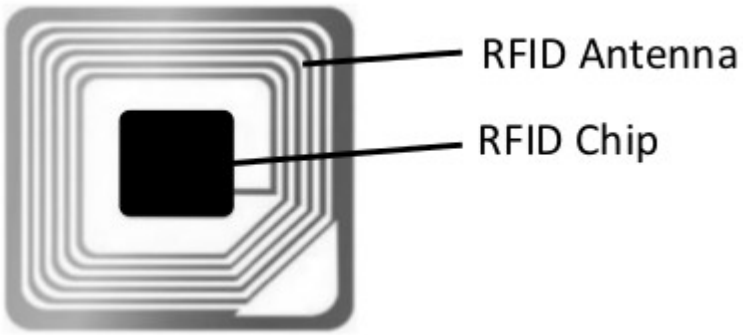

Fig. 5.5.4 : RFID tags

- Three main categories of RFID tags are: BRead-only^ (non-modifiable tags), Bread rewrite^ tags and Bwrite once, multiple read^ tags. In the last case, the chip has a blank memory area to write down a particular number specific to the user.
- However, this number can no longer be modified once it is written. Furthermore, there are two main families of RFID tags. The first family contains active tags connected to an onboard power source (battery, battery, etc.).

- Although active tags have a better range, their cost is higher and their lifetime is restricted. In the second family, the passive tags use the energy propagated at a short distance by the radio signal of the transmitter. Despite their lower cost and almost unlimited lifetime, tags require a significant amount of energy from the reader to operate.
- In localization approach tags in libraries or in warehouses are used to check the items localization. In this system, the RFID reader is always on the move to scan the tags and to determine their positions.
- The advantage of this approach is that it does not need to deploy tags or reference drives but use only a mobile RFID reader. Infrared Several localization systems employ infrared technology to determine the position of the targets.

5.6 Performance Evaluation

- Power management plays an important role in the good performance of wireless sensor networks. It can guarantee the basic levels of system performance, such as connectivity, delay and throughput, in the presence or absence of mobility.
- The energy utilization of sensor nodes, guaranteeing increasing the sensor network's life time in such energy constrained environments. Overuse of energy may cause many environmental and economic crises. Various IoT applications runs for years over batteries and reduce the overall energy consumption.

5.7 Simulation Setup

- Internet-of-Things (IoT) systems and networks are increasingly becoming large, complex, heterogeneous and pervasive. They integrate a large variety of physical devices (IoT devices and sensors) communicating through different networking connections (cellular, WiFi) spread across different architecture layers (cloud, fog, edge).
- That is, IoT systems are spanning both virtual and physical domains. The research process in IoT, starting with the idea formulation and culminating with real-world deployment, requires developing and validating initial proofs of concept and subsequent prototypes.
- Given the large scale and heterogeneity of IoT systems and networks, designing and testing IoT services are challenging tasks. Prototyping using a large number of hardware nodes may not be practical during the initial design phase.
- Similarly, benchmarking and setting up reproducible experiments are challenging undertaking tasks. Simulation-based approaches are significantly important for research benchmarking, designing, testing and experimenting IoT systems and networks.
- Simulation-based approaches offer significant benefits to researchers and practitioners, supporting and accelerating research and development of systems, applications and services. Simulation tools are generally important and necessary tools designed and developed to aid researchers in testing their hypothesis, benchmarking studies in a controlled environment and

easily reproducing results, conducting experiments with different workloads and resource provisioning scenarios, as well as testing systems performance.

- In the context of cloud computing, simulators have accelerated its research and development, as quantifying the performance of service provision in real cloud environments is challenging. In IoT systems and networks, simulation tools have also claimed their importance to fill the gap between conceptual research and proof-of-concept implementation.
- Despite the influx of research in IoT and the various simulations environments proposed so far, there is a general lack to the best of our knowledge of modelling and simulation environments to create a detailed representation of related networking and end-to-end IoT services.
- A novel self-contained platform for modelling and simulating end to end IoT services has been proposed with detailed representation of IoT systems and networking components, namely IoT NetSim.
- The main research objective is to assist researchers and practitioners in designing, validating and experimenting IoT systems and networks.
- To this extent, the proposed platform is designed as a multi-layered architecture, which allows modelling and simulating IoT systems with different structures, application models, IoT services and network connections.
- The modularity of the architecture allows modelling model systems with any combination of cloud, fog, edge, IoT components according to the system architecture and design. The extendable design supports modelling and testing bespoke IoT nodes and network types, as well as placement algorithms used in designing IoT systems.
- IoT NetSim platform contributes the research community with :
  (i) Detailed modeling of IoT nodes and sensors, includes the of mobility and power sources,
  (ii) Testing the IoT modeling and networking and covering various types of network connections used in IoT systems, and
  (iii) Modelling and simulation of IoT services and applications from the sensing data phase to data analysis in the cloud. The platform also supports modelling domain specific IoT applications and end-to-end services, as well as processing and testing the performance of IoT systems under varying dynamic workloads with different quality goals.
- The main objective of IoT Net Sim is simulating and modelling end-to-end IoT services with detailed representation of the associated connectivity and IoT paradigm. The design rationale of architecting IoT NetSim is a multi-layered modular architecture, which allows simulating and modelling various structures of IoT systems. For instance, a simple IoT system with a set of sensors connected to the cloud could be modelled with fine-grained details of the nodes.
- Meanwhile, a complex system with the sensors connected through edge and fog devices could also be modelled, allowing different topologies of networks. Following this design principle, the architecture of IoT NetSim is mainly consists of various layers for the Cloud, Fog, Edge, IoT, Application Model and Simulation Application, built on top of an event-based simulation engine.

- Fig. 5.7.1 shows the multi-layered architecture of IoT NetSim. The multi-layered modular architecture supports modelling various structures for IoT systems and networks, also extensions for further functionalities and placement algorithms.
- As shown in the figure, we have inherited the event-based simulation engine of Cloud Sim. The Cloud Sim simulation toolkit is one of the widely-used general purpose cloud simulation environments and the most sophisticated discrete event simulator for clouds.
- Cloud layer extends the Cloud Sim core simulation engine. Cloud Sim defines the core entities of a cloud environment, such as datacenters, hosts physical machines (PMs), virtual machines (VMs), applications or user requests (called cloudlets).
- A Data center is the resources provider simulating the infrastructure of the cloud (IaaS), which includes the hosts running virtual machines responsible for processing end-user requests (SaaS).
- Computational capacities of PMs and VMs (CPU unit) are defined by PE (Processing Element) in terms of million instructions per second (MIPS).
- Processing elements in a PM are shared among VMs and requests in a VM. The simulation also takes into account the memory, storage and energy consumption of different computational resources.
- A Data center Broker is responsible for the allocation of end-user requests to VMs. Once the simulation is started, the requests are scheduled for execution, and the cloud behaviour is simulated.
- The cloud layer covers the typical components of a cloud, including the physical resources (datacenters and their PMs), virtual resources (VMs), virtual services (VM services for end-user VMs provisioning) and end-user services (for running their service requests and cloudlets).
- Fog and Edge Layers These layers model fog- and edge-related components respectively, where simulations could include either, both, or neither according to the conducted experiments.
- The fog layer includes details of fog-enabled nodes, fog networks configurations and different types of network connections.
- The edge layer, similar to the fog layer, includes edge-enabled nodes and network edges. This layer also includes edge cloudlets, edge applications, and modules for basic and real-time data processing.
- IoT layer : This layer encompasses different types of IoT nodes, networks and services. IoT nodes include fixed and mobile sensors, link nodes, and gateway nodes. The power sources of each node are modelled in details to allow the simulation of real-time scenarios.
- Simulation Application : This is the topmost layer for setting up different policies and simulation parameters, including scheduling policies, service types, application models, networking configurations, and runtime workloads and scenarios.

- The multi-layered architecture allows implementing different functionalities of IoT nodes for processing and analysing data. For the networking in the different layers, details for data packets and network connection types are modelled for real-time scenarios of network loss and disconnection, as well as network traffic.
- The simulations results includes the quantitative measures of utility for simulating of an end-to-end IoT service across overall architectural layers. Researchers and practitioners, willing to design an IoT ecosystem and network or study the efficiency/ improvements of an existing one, would create instances of these layers with their design and IoT nodes to be used, along with network and applications configurations.

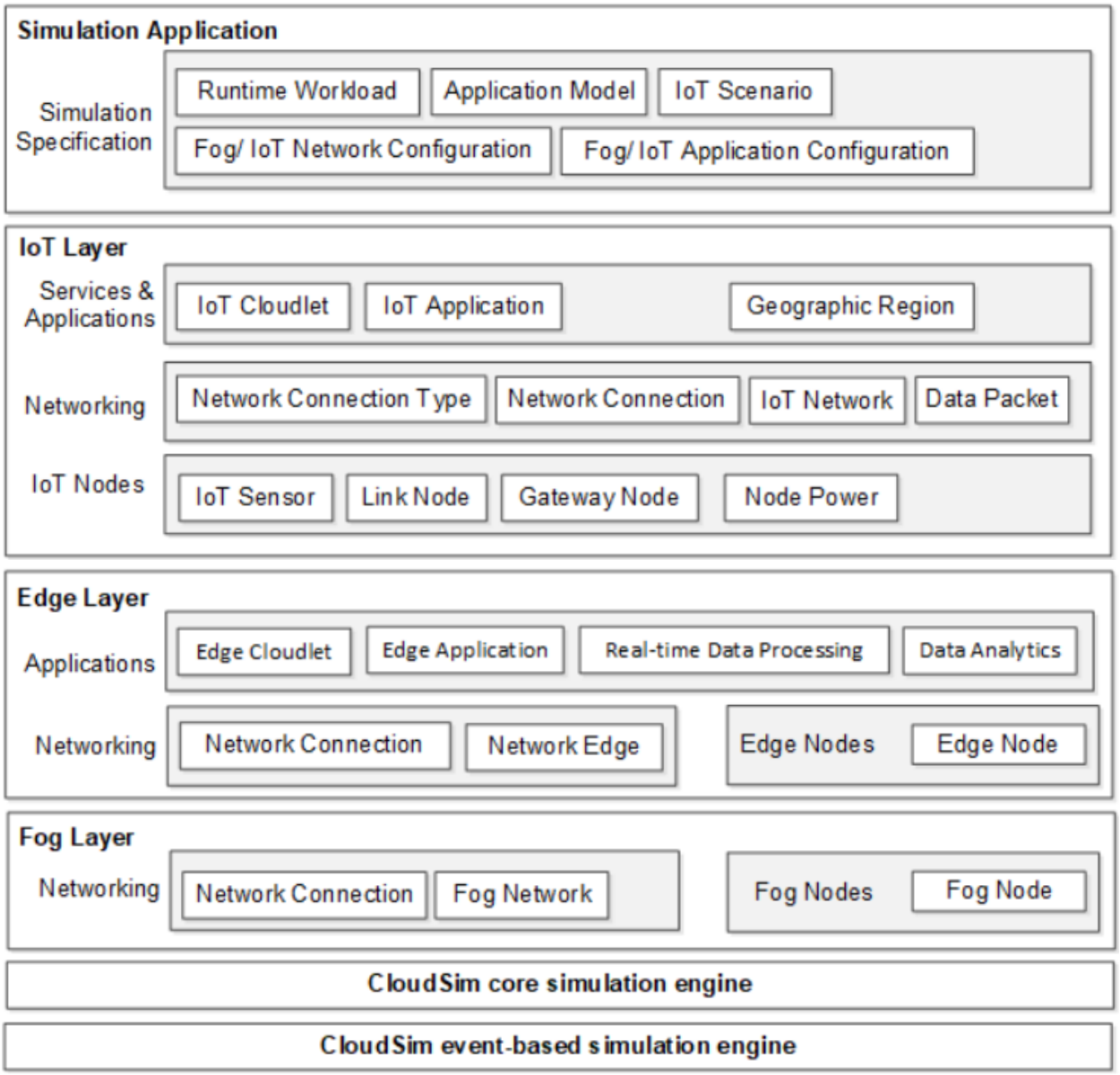

Fig. 5.7.1 : The Architecture of IoT NetSim

In more details, the design is composed of the following packages :

- Among the different layers of the architecture networking is a common package. Each connection type is modelled with signal type, range, capacity and power model.
- An instance of a network connection would inherit these properties from the type, with the strength of the current signal.
- This allows simulating real and hypothetical scenarios of network loss and disconnections. Data Packet and Data Stream simulate the data transferred with different sizes between different nodes.
- Node is shared among the IoT, Edge, Fog and Cloud layers. The package includes fine-grained properties that could be used for modelling and simulating IoT, edge and fog nodes.
- Properties including the power source, location, as well as geographic coverage. Configuring the location allows simulating different placement possibilities of IoT, edge and fog nodes, as well as their networks, enabling among other things the investigation of node placement algorithms.
- IoT encapsulates the components necessary for modelling and simulating an IoT ecosystem. It composes of :
  (i) IoT nodes for a general class.
  (ii) An interface for mobile nodes,
  (iii) A class for sensor nodes with communication functionalities,
  (iv) Link node class with functions for receiving and forwarding data, and
  (v) A gateway node class for nodes capable to aggregate, process and send data. Our implementation includes the basic functionalities of these components.
- Edge supports creating instances of edge devices with configurable computational and storage capacities, as well as configurable functions of data processing and sending data to either cloud or IoT nodes.
- Fog creates instances of configurable fog nodes and associated networking. A fog node could be any computing /storage device or micro-server. These devices inherit their computational configuration from the Physical Host of Cloud Sim and fine-grained properties from the Node package.
- Cloud (as the name implies) represents cloud infrastructure components. The IoT Datacenter is extended from the Cloud Sim Data center for including the functionalities of storing, analysing and processing data for IoT services.
- These functionalities could be either basic or real-time and could be further extended for complex data processing. The Hosts (physical machines) and VMs are extended for tracking energy consumption.
- IoT Cloudlets and Service Requests are tailored to support special types of IoT service requests, such as in-field enquiries and real-time alerts.

5.7.1 The Simulation Process

- The platform is a discrete-event simulation with the flow of events illustrated in Fig. 5.7.2. The simulation process could start either by an end-user submitting a service request to the cloud where the broker will schedule and provide adequate resources or by IoT sensors submitting regularly their sensing data by the scheduled reading interval. Reading data are received by link nodes, which in turn forward it to the gateway node.
- A gateway node aggregates data received and sends it to either the fog, edge or cloud according to the configured IoT system architecture.
- The cloud resources are for data storage, processing and analysis. If edge nodes are present in the architecture, they will forward the data to the cloud and/or process it.
- In case of having fog nodes only, their job will be to forward data according to the configured topology. Nodes could also perform as actuators to take actions according to the data received or the current state of the network.

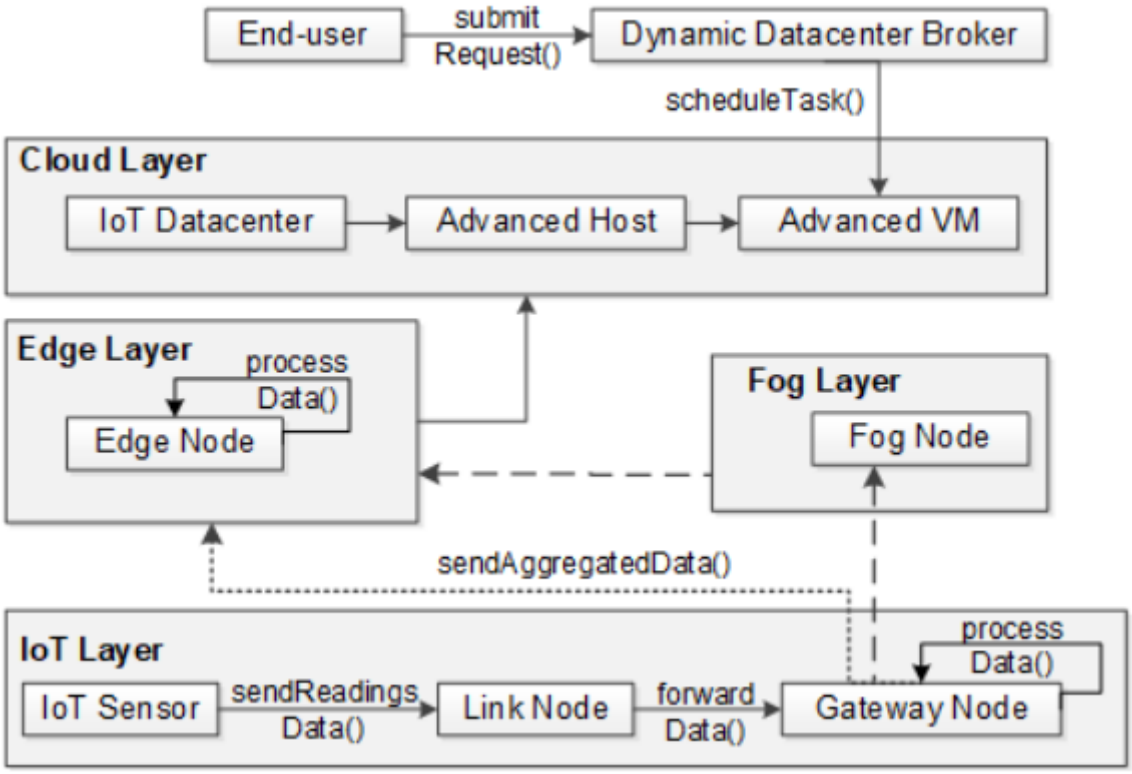

Fig. 5.7.2 : Simulation process in IoT NetSim

5.8 Performance Results

- The performance has been analyzed the state-of-the-art end-to-end security schemes in healthcare Internet of Things (IoT) systems. We should indentify the essential requirements of robust security solutions for healthcare IoT systems consists of :
  (i) Low-latency secure key generation approach using patient's Electrocardiogram (ECG) signals,

(ii) Efficient and secure authentication and authorization for healthcare IoT devices based on the certificate-based datagram Transport Layer Security (DTLS), and

(iii) Robust and secure mobility-enabled end-to-end communication based on DTLS session resumption. The performance of the state-of-the-art security solutions including in end-to-end security scheme is tested by developing a prototype healthcare IoT system. The prototype is made of a Panda board, a TI SmartRF06 board and WiSMotes. The Panda board alongside the CC2538 module acts as a smart gateway and therefore WisMotes act as medical sensor nodes. Based on the analysis, we found out that our solution has the most extensive set of performance features in comparison to related approaches found in the literature.

- The performance evaluation results show that compared to the existing approaches, the cryptographic key generation approach proposed in our end-to-end security scheme is on average 1.8 times faster than existing key generation approaches while being more energy-efficient.
- In addition, the scheme decreases the communication overhead by 26% and therefore the communication latency between smart gateways and end users by 16%. Our scheme is approximately 97% faster than the certificate based and 10% faster that symmetric key-based DTLS.
- Certificate based DTLS requires about 2.9 times more ROM and 2.2 times more RAM resources. On the other hand, the requirements of RAM and ROM our scheme are almost as low as in symmetric key-based DTLS.

5.9 Identification of IoT

- Identification is a crucial topic in Internet of Things (IoT). Beside identification of the things itself, various other entities are identified in IoT solutions.
- The various identification needs related various use cases and requirements. Furthermore, we glance for identifier standards, their applicability for the various identifier needs and discuss identifier allocation, registration, resolution, security, privacy and interoperability.
- Identification plays an important role for the Internet of Things (IoT). First discussions in AIOTI focused around the use of communication identifiers like IP addresses and mobile phone numbers in IoT.
- This was triggered by similar discussions in the Body of European Regulators for Electronic Communications (BEREC). However identification has a much wider scope and is relevant for many applications and entities in IoT.
- Beside identification for communication means this involves identification of the things, but example of services, users, data and locations. Various identification schemes had been already in existence, and are standardized, and are deployed in the market.

- To address the larger scope of identifiers in IoT, the AIOTI Working Group 03 (WG03) IoT Identifier taskforce was framed. The task force objectives are to provide a thorough analysis of the identification needs and related standardization for IoT, specifically :
  - Identifying the needs of IOT and evaluating related requirements;
  - Describing of identification standards and ongoing standardization work and elaborating their applicability for IoT.

5.9.1 Data Formats

- A great number of convenient standards exist on the level of communications in a local network, within a specific domain, or for a limited purpose like remote management of computers. However, at the instant of scripting this specification, we have not identified an appropriate standard that might address the higher-level requirements of the IoT.
- Such requirements are notably the necessity for any data sources (devices, machines, server-based systems, etc.) to be able to publish their available data and provide access to it in an easy and secure way, which includes the possibility to filter the data provided depending on the requester's identity, the context, etc.
- The O-DF (Open Data Format) can be used for publishing the available data using ordinary URL (Uniform Resource Locator) addresses. O-DF structures are also used for requesting and sending published data between systems, notably when used together with the O-MI standard (Open Messing interface).
- In the IoT, information about a product or a "Thing" is often distributed over various devices, systems, and organizations. The O-DF is meant to represent information about things during a standardized way that can be exchanged and understood in a universal way by all information systems that need to manage IoT-related data.
- A data format structure does not contain complete information about a particular thing. Information about the same thing may be available in several different data format structures.
- Object identifiers makes it possible to link the data of a single thing that might be located in different information systems. An object identifier is the only information that a data format structure that consists of particular thing.
- The access to data and visibility depends on the object identifier used, also on the identity of the requesting party, and on the context of the request. This is why the object identifier data structure is of great importance in any universal IoT standard.
- The O-DF using XML Schema is specified. It defines a simple and extensible ontology that allows the creation of information structures that are similar to those of objects and properties in object-oriented programming. It is generic enough to represent any object and information that is needed for information exchange in domains such as the IoT, lifecycle information management, etc.
- The O-DF is intended for expressing information about "any" identifiable object (products, services, humans, ...). How the information is communicating and is not a part of this standard.

- The communication media may be a file sent as an email attachment, on a USB stick, or any other media. O-DF content can also be sent using REST-based services, SOAP, Java Message Service (JMS), the O-MI, and other kinds of messaging protocols.
- The O-DF uses as a query and response format in such messaging; for instance, the O-MI specifies that a "*read*" request with an O-DF structure has responded to with the next level in the hierarchy shown in the figure above.
- As an example, a request with only an "*Objects*" element should return an O-DF response with the list of *Object* elements available, including at least compulsory attributes and sub-elements (notably at least one *id* element).

5.9.2 IPv6

- IPv6 is the next generation Internet Protocol (IP) standard intended to ultimately replace IPv4, this protocol still gives many Internet services today.
- Every mobile phone, computer and any other device connected to the Internet needs a numerical IP address so as to communicate with other devices. The original IP address scheme, called IPv4, is running out of addresses.
- IPv6 was developed by Internet Engineering Task Force (IETF) to deal with the problem of exhaustion in IPv4. IPv6 is 128-bits address having an address space of 2^128, which is larger than IPv4. IPv6 uses Colon-Hexa representation. There are 8 groups and every group represents 2 Bytes.
- In IPv6 representation, there are three different addressing methods :

1. Unicast
2. Multicast
3. Anycast

- **Unicast Address :** Unicast Address identifies a single network interface. A packet sent to unicast address is delivered to the interface identified by that address.
- **Multicast Address :** Multicast Address is used by multiple hosts, called as Group, acquires a multicast destination address. These hosts need not be geographically together. If any packet is sent to this multicast address, it will be distributed to all interfaces corresponding to that multicast address.
- **Anycast Address :** Anycast Address is assigned to a group of interfaces. Any packet sent to anycast address will be delivered to only one member interface (mostly nearest host possible).

Types of IPv6 address

We have 128 bits in IPv6 address but by looking at first few bits we can identify what sort of address it is.

Prefix	Allocation	Fraction of

		Address Space
0000 0000	Reserved	1/256
0000 0001	Unassigned (UA)	1/256
0000 001	Reserved for NSAP	1/128
0000 01	UA	1/64
0000 1	UA	1/32
0001	UA	1/16
001	Global Unicast	1/8
010	UA	1/8
011	UA	1/8

Note : In IPv6, all 0's and all1's is assigned to any host, there are no restriction like IPv4.

I. Provider based Unicast address

These addresses are used for global communication.

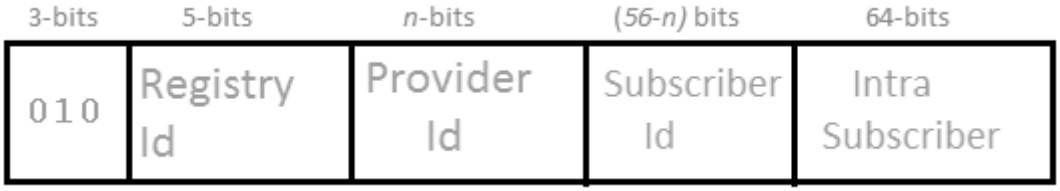

Fig. 5.9.1

The first 3 bits identifies its type.

1. Registry Id (5-bits) : Registry Id helps in identifying the region to which it belongs. Out of 32 (i.e. 2^5), only 4 Registry Id's are being used.

Registry Id	Registry
1000	Multi regional (IANA)

01000	RIPE NCC
11000	INTER NIC
00100	APNIC

2. **Provider Id :** Depending on the number of service providers, certain bits will be allocated to Provider Id field that operates under a region. This field is not fixed. Let's say if Provider Id = 10 bits then Subscriber Id is 56 – 10 = 46 bits.
3. **Subscriber Id :** After Provider Id is fixed, remaining can be used by ISP as normal IP address.

- **Intra Subscriber :** As per need of organization that is using the service this can be modified.

II. Geography based Unicast address

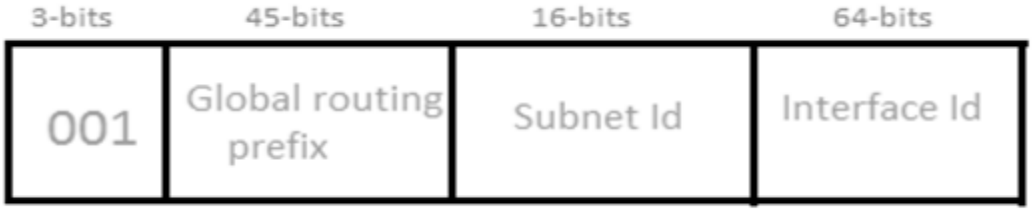

Fig. 5.9.2

- **Global routing prefix :** Global routing prefix contains all the details of Latitude and Longitude. As of now, it is not being used. In Geography based Unicast address routing will be based on location.
- **Interface Id :** In IPv6, we use the term Interface Id instead of using Host Id.

Internet Protocol version 6 (IPv6) Header

- IP version 6 is the latest version of Internet Protocol, which is preferred than IP version 4 in terms of complexity and efficiency. Let's look at the header of IP version 6 and understand how i different it is from IPv4 header.

IP version 6 Header Format

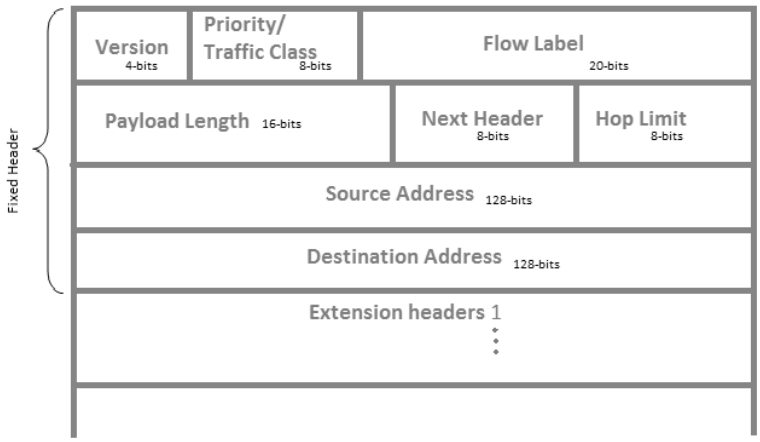

Fig. 5.9.3 : IP version 6 header format

- **Version (4-bits) :** Contains bit sequence 0110 indicating version of Internet Protocol.
- **Traffic Class (8-bits) :** The Traffic Class field indicates priority or class of IPv6 packet which is similar to the *Service Field* in IPv4 packet. It helps routers to handle the traffic based on priority of the packet.
- If congestion occurs in the router than the packets with the low priority will be discarded. As of now only 4-bits are being used (and remaining bits are under research), in which 0 to 7 are assigned to Congestion controlled traffic and 8 to 15 are assigned to Uncontrolled traffic.

5.9.3 Identifiers and Locators

- In any system of interacting components, identification of these components is needed in order to en-sure the correct composition and operation of the system.
- This applies to all lifecycle phases of a system from development to assembly, commissioning, operations, maintenance and even end of life. Especially just in case of flexible and dynamic interactions between system components identification plays a crucial role.
- Identifiers are used to provide identification. Generally, an identifier may be pattern to uniquely identify a single entity (instance identifier) or a class of entities (i.e. type identifier) within a specific context.
- Definition : An identifier helps in uniquely identifying the pattern of a single entity (instance identifier) or a class of entities (i.e. type identifier) within a specific context.
- Depending on the application and user need various types of identifiers are used.
- IoT is about interaction between users and things by electronic means through internet. Both things and user need to be identified in order to determine such interaction. Various other entities are involved within the interaction and are a part of an IoT system and identification is also additionally relevant for them. Figure 5.9.4 shows the different entities with the related identifiers in the IoT Domain Model of the AIOTI WG03 High Level Architecture.

- Different identification schemes exist already, and is standardized and deployed. This document-
  - Evaluating and Identifying of IoT needs;
  - Classification of different identification schemes;
  - Evaluating and categorizing related requirements;
  - Providing examples of identifier standards and elaborates their applicability for IoT;
  - Discussion on allocation, registration resolution of identifiers;
  - Consideration of security and privacy issues;
  - And discussion on interoperability of identifiers.

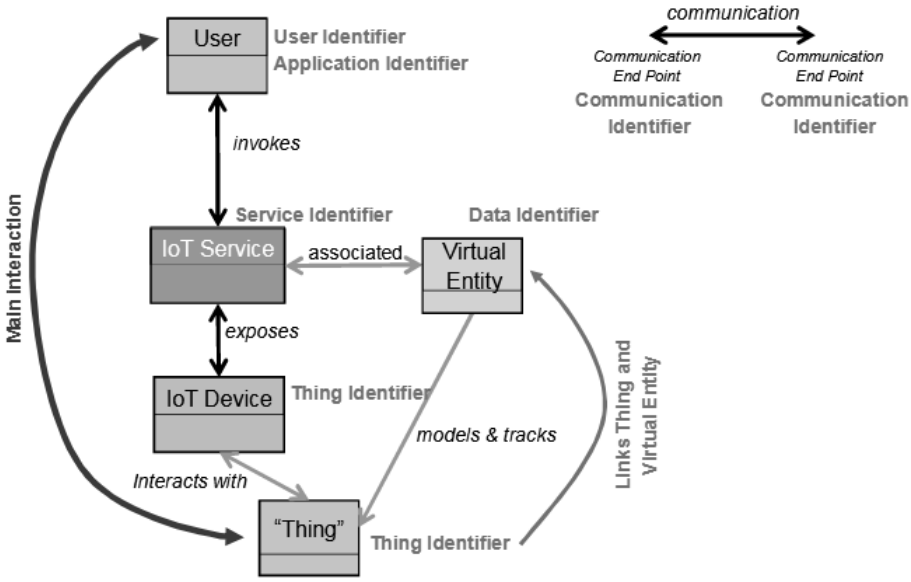

Fig. 5.9.4 : IoT Identifiers in the Domain Model of the AIOTI (Alliance of IoT Innovations) high level architecture

5.9.4 Tags

- Smart tags have given digital identities to several physical devices around us, connecting devices with applications wirelessly and making them an integral a part of the Internet-of-Things. They have the ability to help societies significantly resolve today's global challenges foreseen in areas like environment, energy, food production, healthcare and Iot more.
- Use of smart tags increases in areas like plants and warehouses because, they keep track on parameters of critical environment like humidity and temperature, log data for quality management and historical records, or are used as triggers for alarms or process management.
- Smart tags have three basic features which defines an IoT application: sensors; wireless connectivity and data analytics.

Here is brief workflow of Smart Tag :

- First, sensors like Motion sensors, Biosensors, environmental sensors perform data collection.

- Second, a combination of methods such as GPS (outdoor); Motion sensors; RF, geomagnetic, ultrasonic techniques help in indoor / outdoor tracking.
- Third, A microcontroller processes sensor signals for extraction and encryption of meaningful data.
- Four, a radio wirelessly transmits the data to the cloud or local applications on handheld device.
- AI, Deep and Machine learning techniques, Big data analysis and algorithm are applied to generate technical and business intelligence for the stakeholder.

- Due to their small size, smart tags heavily relay on efficient power management and state-of-the art power sources such as tiny rechargeable batteries even energy harvesting technologies.

() () ()