# Predecessors of IoT

## Computing for Internet of Things

**Dr. Arijit Roy**

# Overview

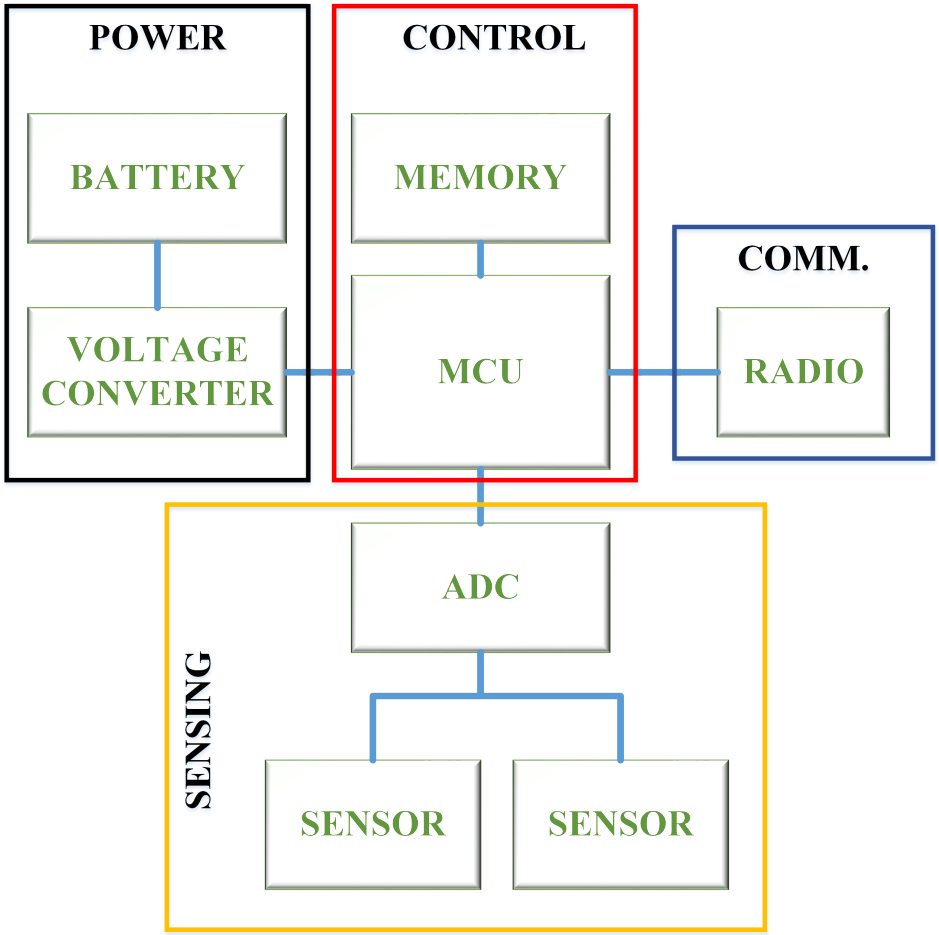
# Introduction

- A majority of the predecessor technologies before the IoT era were used separately for providing sensing, decision making, and automation tasks.
- The range of application domains of these technologies extended from regular domains like healthcare, agriculture, home monitoring, and others to specialized domains such as military and mining.
- Some of these precursor technologies still being used and often re-engineered for IoT are
  1. Wireless Sensor Networks (WSN)
  2. Machine to Machine (M2M) Communications
  3. Cyber-Physical Systems (CPS).
- All of these precursor paradigms have their distinct signatures and application scopes.

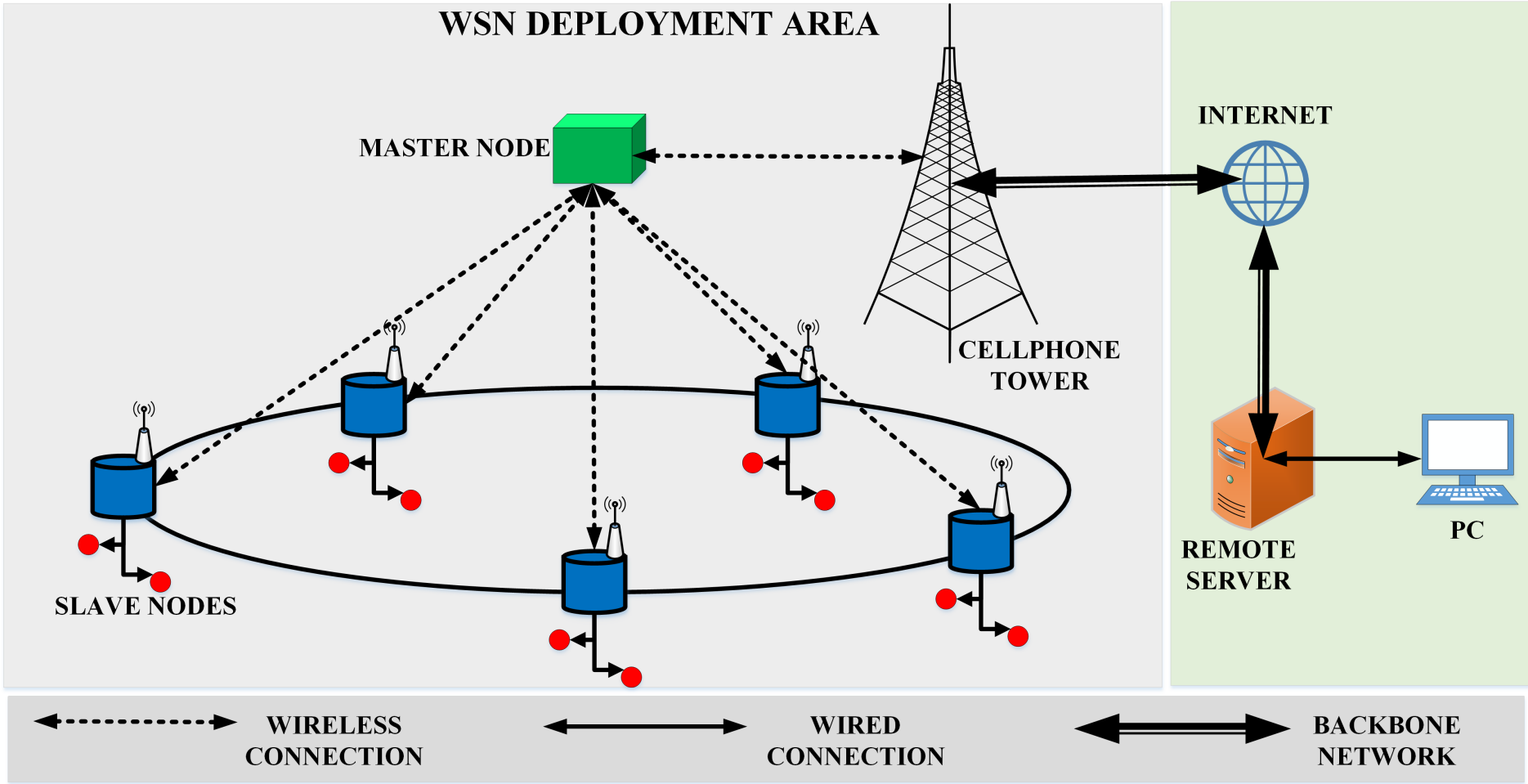
# Wireless Sensor Networks

- Wireless sensor networks (WSN), as the name suggests, is a networking paradigm making use of spatially distributed sensors for gathering information concerning the immediate environment of the sensors and collecting the information centrally.
- Here, the sensors are not standalone sensors but a combination of sensors, processors, and radio units – referred to as sensor nodes – sensing the environment and communicating the sensed data wirelessly to a remote location, which may or may not connect to a backbone network.
- The exact specifications of each of these blocks vary depending on the implementation requirements and the network architect's choice.

# Components of WSN



# WSN Architecture



# WSN Architecture

- WSNs mainly follow a system of communication known as master-slave architecture.
- In a master-slave architecture, a single aggregator node – the master – is responsible for collecting data from various sensor nodes under its dominion or range of operations.
- The sensor nodes under the range of the master node are referred to as slave nodes.
- Multiple slave nodes communicate to a master node using low-power short-range wireless radios such as Zigbee, Bluetooth, and WiFi for transferring their sensed data to a remote central server.
- Often, in popular WSN architectures, the master node connects the WSN to the Internet and acts as the gateway for the WSN.
- Upon collecting data from the slave nodes, the master node pushes the aggregated data to a remotely located central server using the Internet.

# WSN Features

The main distinguishing features of a WSN are as follows:

1. **Fault Tolerance**: The occurrence of faults in WSN nodes should not take down the whole WSN implementation, or hamper the transmission of data from non-faulty nodes to the central location.
2. **Scalability**: WSN implementations must have the feature of scalability associated with their architectures and deployments. In the event of a future increase or decrease of sensor node units, the WSN must support the scaling of the infrastructure without changing the whole implementation.

# WSN Features

1. **Long life time**: The lifetime or the energy replenishment cycle of WSNs must be long enough to make large-scale applications feasible. WSNs have been used for monitoring remote, harsh, and hard to access environments; wherein, it is not feasible to regularly replenish the energy source of the WSN nodes, which necessitates the need for long node lifetimes.
2. **Security**: The security of WSNs, if not considered, can easily compromise with the security of the whole system, right back to the central server. As WSNs are used for a wide range of applications, some of which are crucial, security is one aspect, which must be properly addressed to prevent intrusion and maintain the integrity of the data.

# WSN Features

1. **Programmability**: The programmability of WSNs is important as it ensures the robustness of these systems. WSNs deployed in one application area can be reused for other applications just as easily with the change in sensors and the backend programs associated with it. Moreover, programmability also helps in providing a means of adjusting the parameters of the system in the event of a scale-up or scale-down operation.
2. **Affordability**: As the WSNs generally require multiple units, typically in the range of tens or hundreds of WSN nodes, the cost of the nodes and its affordability is vastly responsible for the acceptability of the system. Except for some specialized domains such as the military and the industry, where the sensing requirements are quite high and that too in harsh and challenging conditions, the majority of WSN applications are regular.

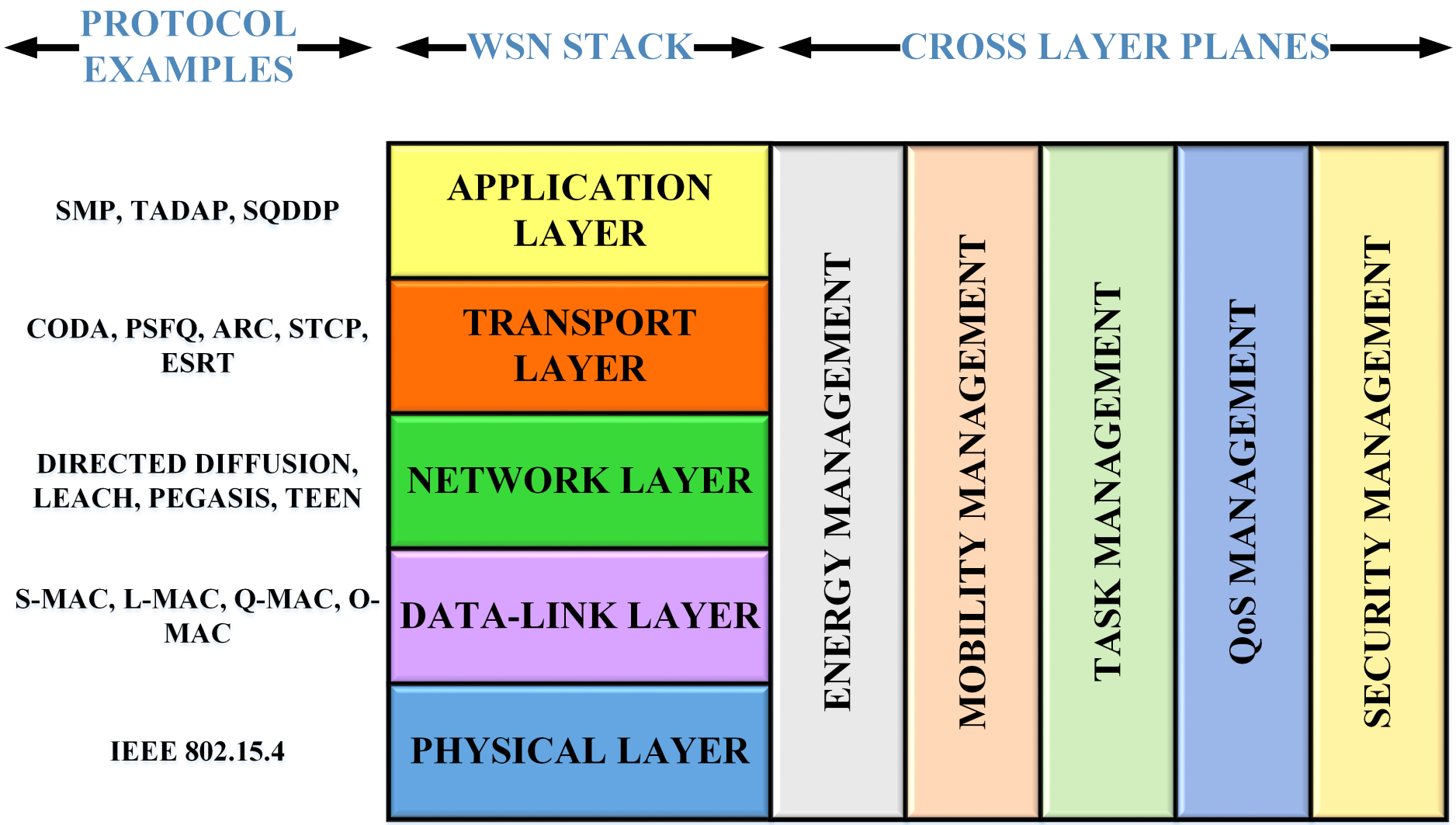
# WSN Features

1. **Heterogeneity**: The WSNs must support a wide number and types of sensors and solutions, thus enabling heterogeneity. In the absence of heterogeneity, WSN will tend to become very application-specific, which in turn would require major customizations even in the event of minor changes to the network or architecture.
2. **Mobility**: WSNs must support the notion of the mobility of nodes such that the nodes may be easily relocatable or mobile. Mobility would ensure the rapid deployability of WSN-based solutions in all environments types.

# Architectural Components of WSN

- WSNs similar to regular computer network paradigms may be explained in terms of a protocol stack, which is very similar to the ISO/OSI stack.
- However, instead of seven layers similar to the OSI model, the WSN stack is made up of five layers – 1) Physical, 2) Data Link, 3) Network, 4) Transport, and 5) Application layer.
- In addition to these five layers, the WSN stack further comprises of five cross planes concerned with management tasks such as 1) Power management plane, 2) Mobility management plane, 3) Task management plane, 4) QoS management plane, and 5) Security management plane.

# Architectural Components of WSN



# WSN Stack - Physical Layer

- The Physical layer, which is at the bottom of the stack and is responsible for enabling transmission of signals over a physical medium between multiple WSN nodes/units.
- In regular computer networks, the medium can be both wired as well as wireless, however in WSNs, the medium is strictly wireless.
- In WSNs, this layer is responsible for carrier frequency generation, carrier frequency selection, modulation/ demodulation, encryption/decryption, and signal detection.
- Typically, WSNs make use of the IEEE 802.15.4 standard for this layer, which is attributed to its low cost, low energy budget, low data rate, and small form factor.

# WSN Stack - Data Link & Network Layer

- The Data-link layer resides above the Physical layer.
- It is responsible for medium access control (MAC) functions such as multiplexing/ demultiplexing, framing of messages from the upper layer, frame detection, and error control.
- These functions help in ensuring the reliability of communication between the WSN nodes.
- In continuation, the Network Layer lies on top of the Data-link Layer.
- The primary function associated with this layer is the routing of packets.
- As routing is a demanding task and depends on many factors affecting the network elements (nodes, gateways, routers, switches, and servers), the choice of routing protocols dictates the power and memory requirements of the WSN elements such as the sensor nodes.

# WSN Stack - Transport & Application Layer

- The Transport Layer sits on top of the Network layer.
- This layer, in contrast to the Network layer, plays a crucial role in ensuring reliability and congestion control of the packets arriving and leaving from each WSN node.
- Protocol-based mechanisms for loss recognition and loss recovery are inherent to this layer.
- Typically, the protocols in this layer are either packet driven or event-driven.
- Finally, the Application Layer, which is responsible for traffic management and software interfaces, sits on top of all these previous four layers.
- The software interfaces are responsible for the conversion of data from various application domains of WSN into an acceptable format for transfer to the layer underneath this layer.

# WSN Stack - Cross-layer Management Planes

- The use of OSI-like stack for outlining the functionalities of WSN face limitations due to their specialized uses in areas requiring prolonged deployments with constrained energy and communication infrastructure, and mobility.
- Unlike regular computer networks, the use of OSI-like WSN stack does not fully describe the functionalities of WSN-based systems as because of its specialized nature, there is a strong correlation between the five WSN stack layers.
- Typically, solutions addressing WSN applications and functionalities make joint use of all the five layers.
- It is mainly because of this reason, the cross-layer management plane structure is more popularly accepted as a means of abstraction of WSN-based systems and solutions.

# WSN Types

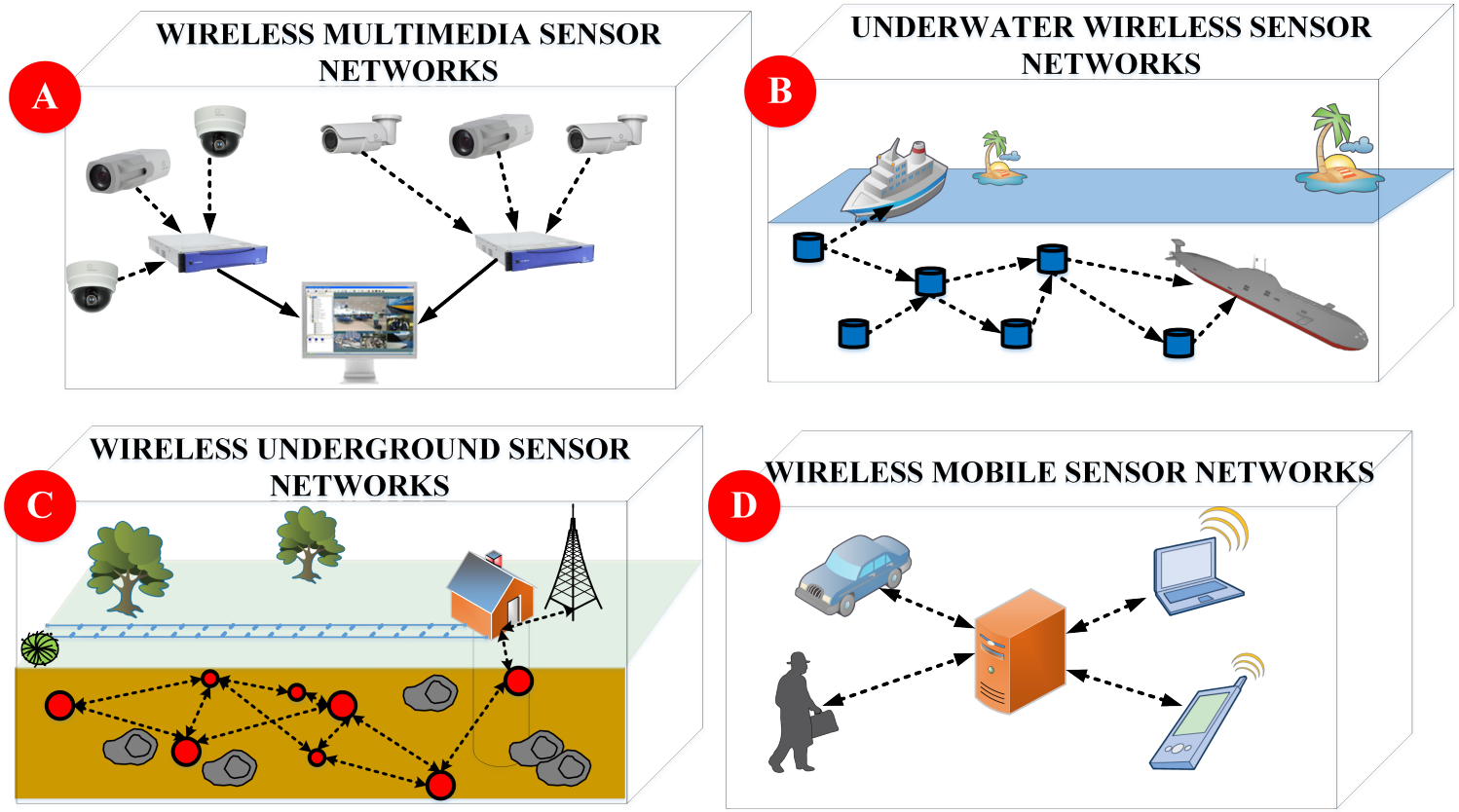



Figure: The various domains of implementation of WSNs signifying its types – A) WMSN, B) UWSN, C) WUSN, and D) MSN

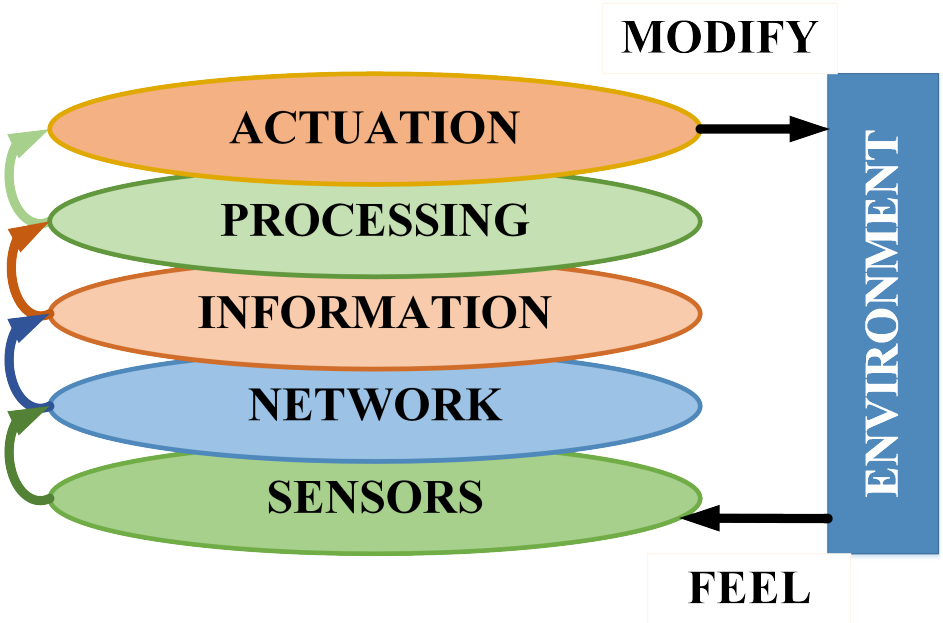
# Machine to Machine Communications

- The machine to machine (M2M) paradigm, as the name suggests, implies a system of communication between two or more machines/devices without human intervention.
- Some basic examples of M2M from our daily lives include:
  1. ATM machines signalling banks about the need for refilling them with cash
  2. Power line monitoring systems in a house alerting a generator set of possible power failures and switching to generator-based supply
  3. Vending machines updating stock of items in their inventory and alerting a remote inventory of the need to refill certain depleting items.

# M2M Ecosystem

- The task of any sensor network system (be it WSN, M2M, CPS, or IoT) is sensing of a physical environment and converting it into a tangible output in the form of numbers using sensors.
- This sensing is followed by the transfer of sensed data to a device or location using a network, which may be wired or wireless.
- The data collected at the remote device from various sensors – homogeneous or heterogeneous – is converted to usable information, which can be used to define the course of actions for individual scenarios.
- This information is processed to decide upon the most valid and optimum course of action, which must be undertaken to control the sensed environment desirably or as per requirements.
- Finally, actuators are put to work to modify or adjust the sensed environment.

# M2M Ecosystem



# M2M Characteristics

- The $3^{rd}$ Generation Partnership Project (3GPP), which is responsible for unification and benchmarking of telecommunication standards across seven different telecommunication standardization organizations, refers to M2M as Machine Type Communications (MTC).
- 3GPP highlights the following significant characteristics of M2M:
  1. Heterogeneous markets
  2. Low data footprint
  3. Low cost maintenance, and integration efforts
  4. A very large number of communicating devices without human intervention.

# Features of M2M

1. **Negligible mobility**: M2M devices are generally not mobile and may be considered majorly static. Even if the need for mobility arises, the displacement is generally minimal to acknowledge in terms of network signals and communication parameters.
2. **Time-restricted transmissions**: The data transmission between M2M devices/terminals are highly time-bound and restricted. The data transmission duration is generally pre-defined.
3. **Delay Tolerant**: The data transmission between M2M devices is not real-time. These connected systems are designed to be delay tolerant.
4. **Packet switched**: The M2M communication network is always packet-switched. The communication between the devices/terminals is in the form of packets with their respective headers, footers, and payloads.

# Features of M2M

1. **Small data footprint**: The data footprint of M2M devices is tiny. However, the frequency of transmission and reception of data between the devices is typically high.
2. **Event detection**: The M2M devices are designed to detect and monitor events only. These do not generally react physically or actuate in the occurrence of events.
3. **Low-power requirements**: very low power requirements characterize M2M systems. This makes then easily integrable with a variety of solutions ranging from industrial and commercial systems to even household systems.

# Features of M2M

# Architectural Components of M2M

- M2M being a complex paradigm is better understood if the components are grouped under the following two categories:
  1. M2M Networking model
  2. M2M Service Ecosystem
- The networking model approaches the prospective scopes and features of the M2M platform in terms of the networking components and their roles.
- The service ecosystem attempts to describe the M2M platform and interactions in terms of the various service providers, their roles and responsibilities.

# M2M Devices

- M2M devices are those entities, which are capable of responding to requests for data by means of replying through networked messages almost autonomously.
- The devices at the end of the network, which are tasked with sensing and actuation, also fall under this category.
- The mode of communication of these devices may be wired or wireless.
- These devices connect to a network through a gateway, or directly using a cellular operator's network.
- In the latter case, the responsibility of the device's Service Level Agreements (SLAs) and accountability lie with the cellular network provider.
- For the remaining cases, accountability and SLAs are undertaken by Internet Service Providers (ISPs).

# Low-end M2M Devices

1. This device type is typically cheap and has low capabilities such as auto-configuration, power saving, and data aggregation.
2. As these devices are generally static, energy-efficient, and simple, a highly dense deployment is needed to increase network lifetime and survivability.
3. Moreover, low-end devices are resource-constrained with no IP support and are generally used for environmental monitoring applications.

# Mid-end M2M Devices

1. These devices are more costly than low-end M2M devices as the devices may have mobility associated with them.
2. However, these devices are lesser complex and energy-efficient than high-end devices.
3. The presence of capabilities such as localization, intelligence, support for Quality of Service (QoS), traffic control, TCP/IP support, and power control make them lucrative for applications such as home networks, SCM, asset management, and industrial automation.

# High-end M2M Devices

1. These devices generally require low-density of deployment.
2. These devices are designed as such that they can handle multimedia data (video) with QoS requirements, even in mobile environments.
3. The mandatory inclusion of mobility as a feature of this device class makes them costly.
4. Generally, these device classes are applied to ITS and military or bio-medical applications.

# M2M Area Network

1. The M2M area network is comprised of multiple M2M devices, either communicating with one another or to a connected platform, which is remotely situated.
2. The local communication between the M2M devices upto the M2M gateway can be considered as the M2M area network.
3. It is also referred to as the *device domain*.
4. Some examples, which can be correlated to the functioning of M2M area networks include personal area networks (PANs) and local nodes in a Wireless Sensor Network (WSN).

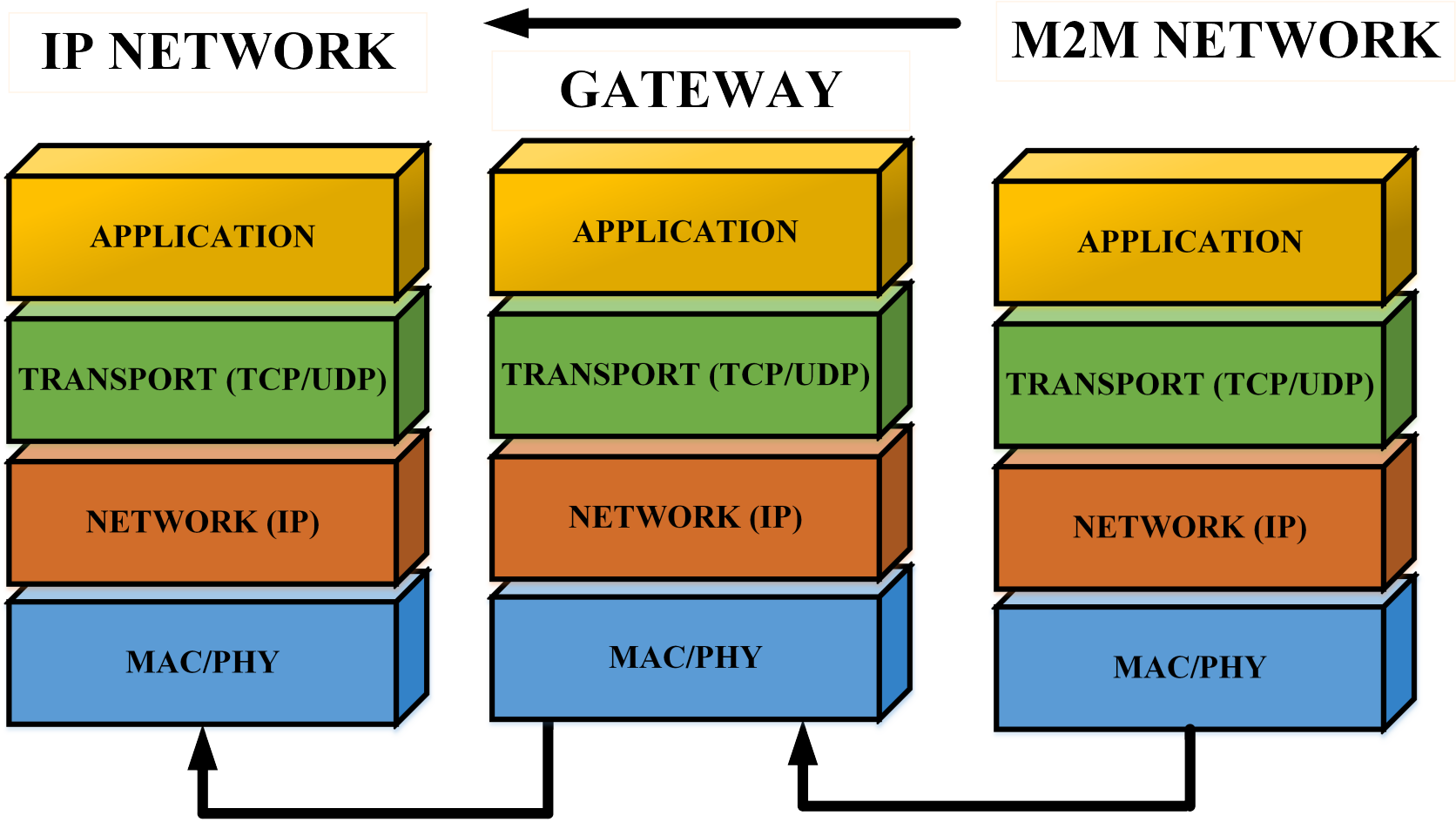
# M2M Gateway

1. It is responsible for enabling connectivity and communication between the M2M devices and a global communication channel such as the Internet.
2. The gateway is responsible for distinguishing data and control signals between the M2M platform to enable monitoring as well as maintenance of the M2M area network remotely.
3. The gateways must additionally ensure that the M2M devices can access an outside network, as well as the devices themselves can be accessed from an outside network.

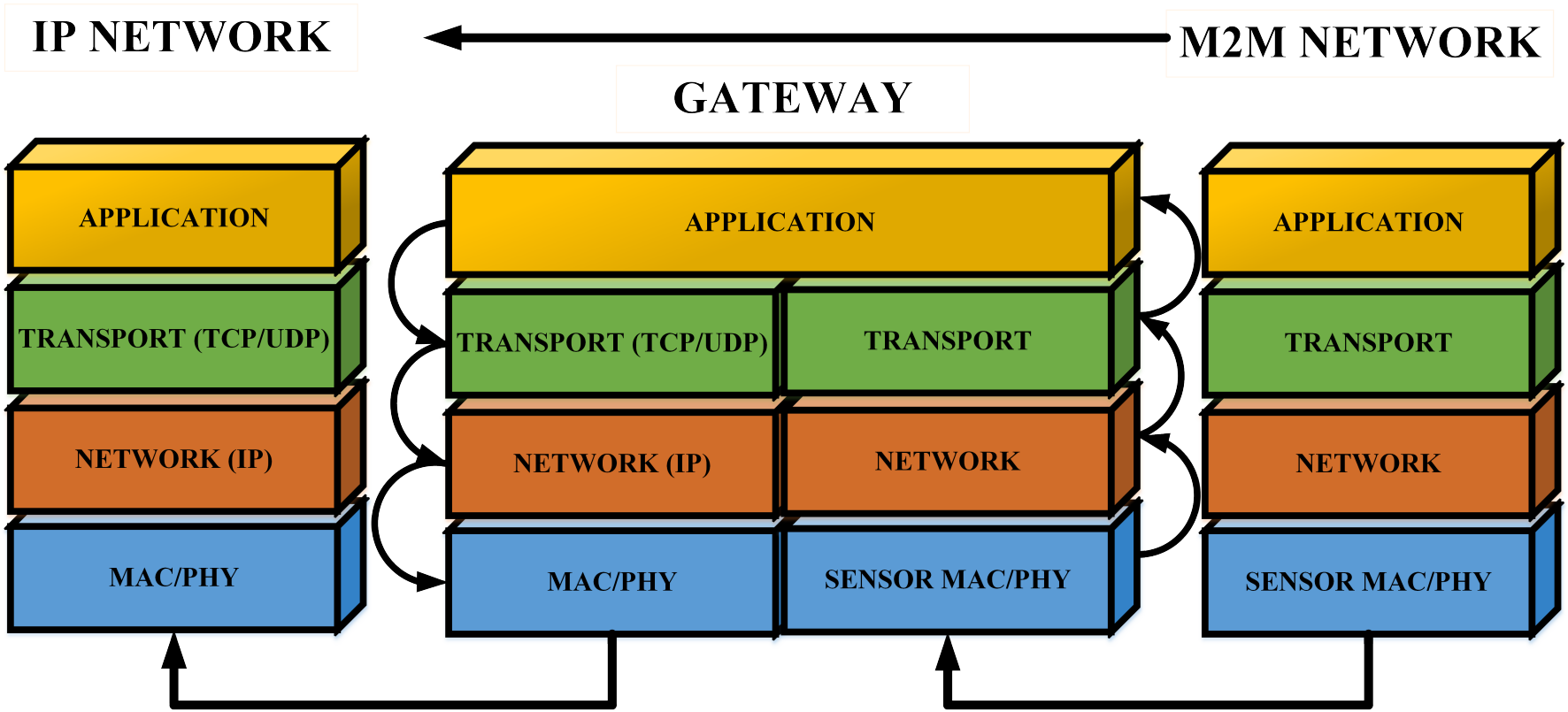
# M2M Communication Network

1. This is also referred to as the M2M network domain.
2. It consists of the communication technologies and paradigms for enabling connectivity and communication between M2M gateways and various applications.
3. Some M2M communication Network enablers include WLAN, WiMAX, LTE, and others.
4. These M2M networks can be distinguished as either
   - IP-based
   - Non-IP-based

# M2M communication over IP-based networks



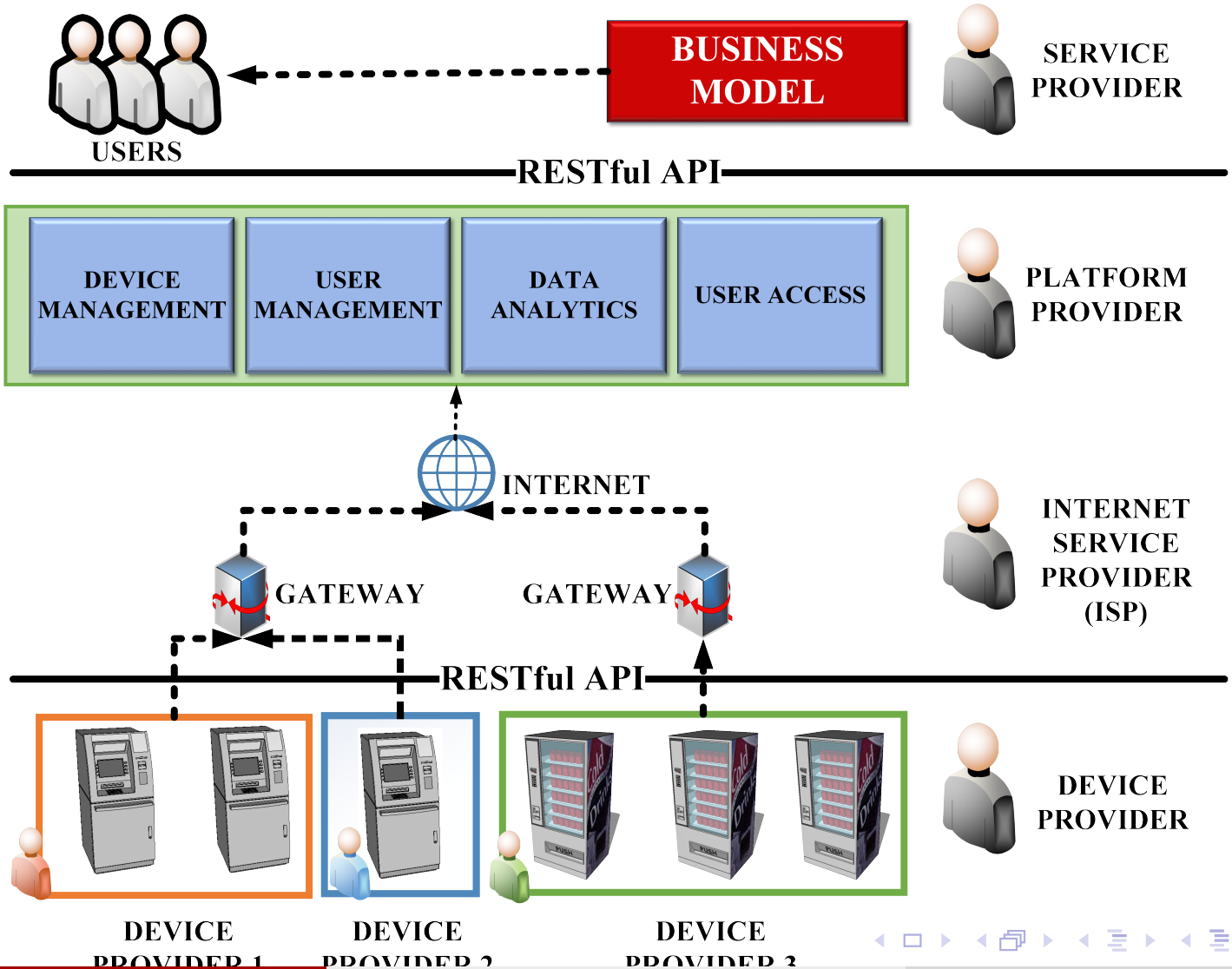
# M2M communication over non-IP-based networks



# M2M Service Ecosystem

- The M2M service ecosystem, unlike the networking model, classifies the various components of an M2M ecosystem based on the needs of service offerings from an M2M platform.
- The ecosystem can be broadly divided into four domains:
  1. M2M area networks
  2. Core network
  3. M2M service platform
  4. Stakeholders

# M2M Service Ecosystem



# M2M Area Networks

- This forms the base of the M2M ecosystem.
- The M2M area networks previously described in the M2M networking model is the same as this one.
- The constituent devices are classified as low-end, mid-end, and high-end based on their functionalities and ability to handle mobility.

# Core network

- The core networks form the crux of the communication infrastructure of M2M, and carries the bulk-load of traffic across the M2M network.
- The core network can be wired or wireless or both.
- Some of the conventional technologies associated with the core networks include WLAN, LTE, GSM, WiMAX, DSL, and others.

# M2M Service Platform - Device Management

1. Enables anytime and anywhere access between Internet-connected platforms and registered objects or devices connected.
2. During device registration, an object database is created from which information can be easily accessed by end-users such as managers, users, and services.
3. The main functions of this platform include the management of device profiles (location, device type, address, and description), authentication, authorization, and key management functionalities.
4. Additionally, it monitors device statuses, M2M area networks, and their interactions and controls.

# M2M Service Platform - User Management

1. Various service providers and device managers can maintain administrative privileges over the devices or networks under their jurisdiction through the platform's device monitoring and control.
2. User profiles and functionalities such as user registration, account modification, service charging, service inquiry, and other M2M services are provisioned and managed through this entity.
3. This platform also enables interoperability between the device managers, and provisions control services such as user access restrictions to devices, networks, or/and services.

# M2M Service Platform - Data and Analytics

1. Provides integrated services based on device-collected data and data-sets.
2. Heterogeneous data merging from various devices are used for creating new services.
3. This platform collects and controls processing and log data for management purposes.
4. These collected data on the devices is achieved in conjunction with the device management platform.
5. Connection management services by means of connecting with the appropriate network are provided for seamless services and are achieved by analyzing the log and data behavior of the registered devices and networks.

# M2M Service Platform - User Access

1. Provides a smartphone and web access environment to users.
2. These redirect to service providers who have a mapping of the registered devices, users, and the services subscribed.
3. Provisions for modifications to a device or user-specific mapping is also provided.

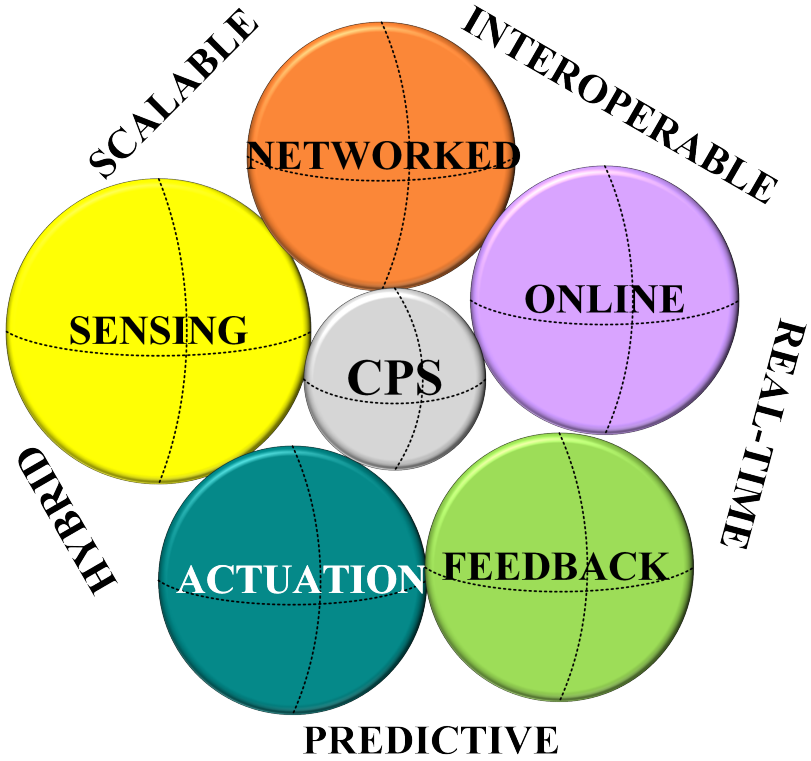
# Stakeholders

- The stakeholders in an M2M service ecosystem can be divided into five different types – Device providers, Internet Service Providers (ISPs), Platform providers, Service providers, and Service users.
- The functional jurisdiction of each of these five classes of stakeholders is well defined and devised in such a manner that they do not overlap and may be considered mutually exclusive in terms of their offerings.
- However, at the time of functioning, all these stakeholders have to work together to ensure the smooth functioning of the M2M service ecosystem.

# Cyber Physical Systems

- Cyber-Physical Systems (CPS) are Internet-based and networked monitoring and controlling systems, which are regulated and governed by feedback-based intelligent control algorithms.
- This is a highly interdisciplinary domain that involves expertise in lots of domains such as mechanical, electrical, computing, electronics, and many more.
- These are mainly designed to monitor and control physical world processes linked to businesses and industries.
- The most interesting aspect of CPS is the involvement of the concept of human-in-the-loop, which is an integral part of many CPS-based solutions.
- The striking difference of CPS from paradigms such as WSN and M2M is the inclusion of a compulsory feedback system.

# Overview of CPS



# Overview of CPS

- The sensing mechanism senses an environment. Various networked sensors simultaneously generate data for the environment, which is sent over the Internet to a processing cum controlling unit.
- Depending on the intelligent monitoring and control algorithms in the control unit, feedback is provided to the actuators controlling the state of the environment for which the sensed data was transmitted.
- The changes are again sensed and forwarded to the controller via the previously defined flow.
- The algorithms decide whether the desired state of the environment is achieved or not, and it keeps on sending adjusted feedbacks to the actuators until the desired state is achieved.

# Features of CPS - Real timeliness

1. The CPS depends on real-time communication, processing, and feedback to effectively provide control to the environment they are deployed.
2. For example, in a CPS-based industrial chemical concentration monitoring system, the real-timeliness of the process from sensing to feedback to actuation is crucial for maintaining the operations of the chemical manufacturing plant and prevention of disasters.

# Features of CPS - Intelligent

1. ntelligent and adaptive decision making is crucial for the maintenance of CPS-based functionalities.
2. In the event of random or sudden changes in the environment being controlled, this feature ensures effective control of the environment and effective coordination between the various dependent sub-processes and systems.
3. For example, in case of an electrical fault in a section of a smart-grid system, this feature would enable the re-routing of the electrical supply flow through other paths instead of bringing the whole system to a complete standstill.

# Features of CPS - Predictive

1. This feature enables the prediction of outputs and events based on past behavior under similar constraints and conditions.
2. The prediction of events enables the activation of precautionary measures to control the damage if the harmful event does occur.
3. For example, the trend of minor line disturbances and noise in a communication channel might lead to network data loss in a backhaul network.
4. This feature would help in the timely activation of preventive countermeasures to avoid network outage in case the network does start massively dropping packets.

# Features of CPS - Interoperable

1. The vast and massive deployment zones of CPS-based systems may include software as well as hardware from a variety of manufacturers.
2. This would lead to data, speed and format mismatch under normal circumstances, however CPS-based interoperability prevents this and enables systems from various vendors to work in sync with one another as a single system.
3. This feature also ensures that legacy systems already-in-place are not replaced but are added to the CPS infrastructure.

# Features of CPS - Heterogeneous

1. Heterogeneity in CPS-based systems may be in
   - Types of actuators, sensors, processors
   - Data formats being used
   - Sensing types, software, and application types
2. However, provisions are already present in CPS to accommodate these types of challenges.

# Features of CPS - Scalable

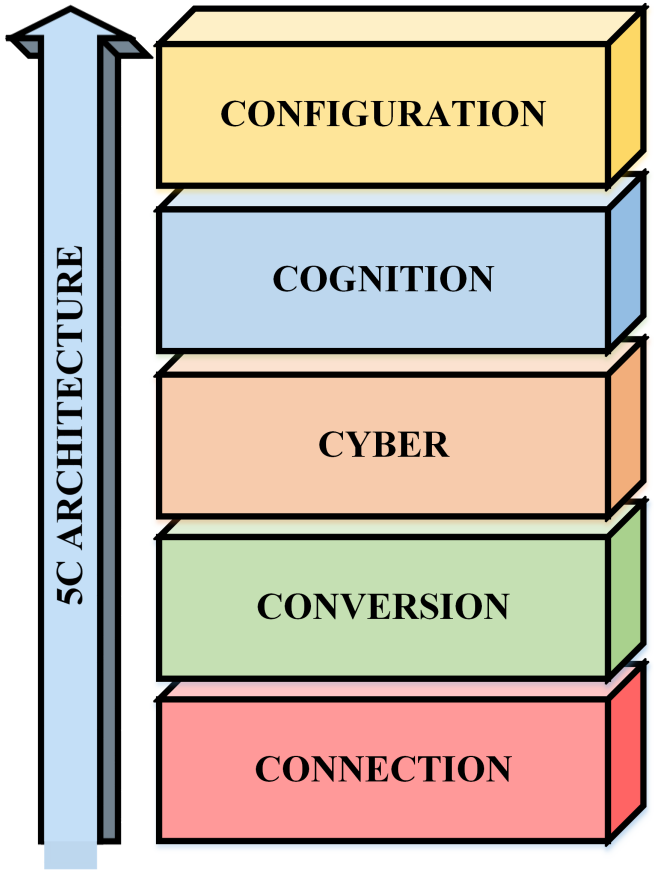
1. Scalability in CPS-based systems may be in terms of network bandwidth being required due to various sensing types (scalar or multimedia), number of sensors and actuators, size of deployment zones, and other factors.
2. CPS-systems should be able to handle such demands even after preliminary deployment.
3. For example, a smart building wants to incorporate human presence detectors to control the central cooling for the whole building.
4. Initially, conventional scalar sensors were deployed on all floors and corridors to monitor the approximate headcount of people in the building.
5. However, after some years, the building management upgrades the scalar sensors by replacing them with camera sensors.
6. The deployed CPS should be able to accommodate this upgrade without changing the whole system.

# Features of CPS - Secure

1. The security of CPS is crucial as almost all of the traffic flows through a network and eventually over the Internet.
2. Provisions should be in place to avoid unauthenticated use of the CPS and its hijacking by unscrupulous elements or even attacks, which may reduce the response of the system or eventually bring it down all-together.

# Architectural Components of CPS

The 5Cs – connection, conversion, cyber, cognition, and configuration – aptly describes the CPS control flow and functionalities.



# 5C's of CPS

## Connection

The sensed data from the base of the architecture should be accurate and reliable enough to actuate effectual feedback for the whole system. The sensed data from various sensor units should be collected in a hassle-free and organized manner. The best possible solution is the use of tether-free communication systems, which should be able to support plug-and-play features of these sensing units.

# 5C's of CPS

## Conversion

The collected data should be converted to a standard unified format. Post data standardization, usable information must be extracted from the sensed data. Data from various sensor types and sources need to be correlated to generate practical information from vastly multi-dimensional data. This data can be used to predict changes to the monitored environments, machinery malfunctions, and failures.

# 5C's of CPS

## Cyber

This acts as the central nodal point of data collection and the holistic analysis of the system under control of the CPS. Data from various machine networks, environments, systems, and processes arrive at this point. Detailed and advanced analytics on the obtained data is performed to gather statistical trends. These trends can be used to predict the future behavior of machine systems and processes. The prediction can be based on digital twins of the actual systems, comparative performance of a machine with other machines, and temporal and regression of machine health and performance.

# 5C's of CPS

## Cognition

This level is mainly responsible for the amalgamation of the collective health of the running systems and processes. The information is presented in the form of human-readable visualizations and trends. This helps in prioritizing actions and control of processes and systems under the purview of the CPS.

# 5C's of CPS

## Configuration

This stage is responsible for generating feedback for adjusting the environment being controlled. The feedback systems need to be highly adaptive, self-configuring, and resilient for effective control of the system as a whole.

# The End