SNS COLLEGE OF TECHNOLOGY

Coimbatore–35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF MECHANICAL ENGINEERING
19MEB204 IoT FOR PRODUCTION SYSTEM

TOPIC – M2M Communication

M2M

- Machine-to-machine, or M2M, is a broad label that can be used to describe any technology that enables networked devices to exchange information and perform actions without the manual assistance of humans.

- The main purpose of machine-to-machine technology is to tap into sensor data and transmit it to a network.

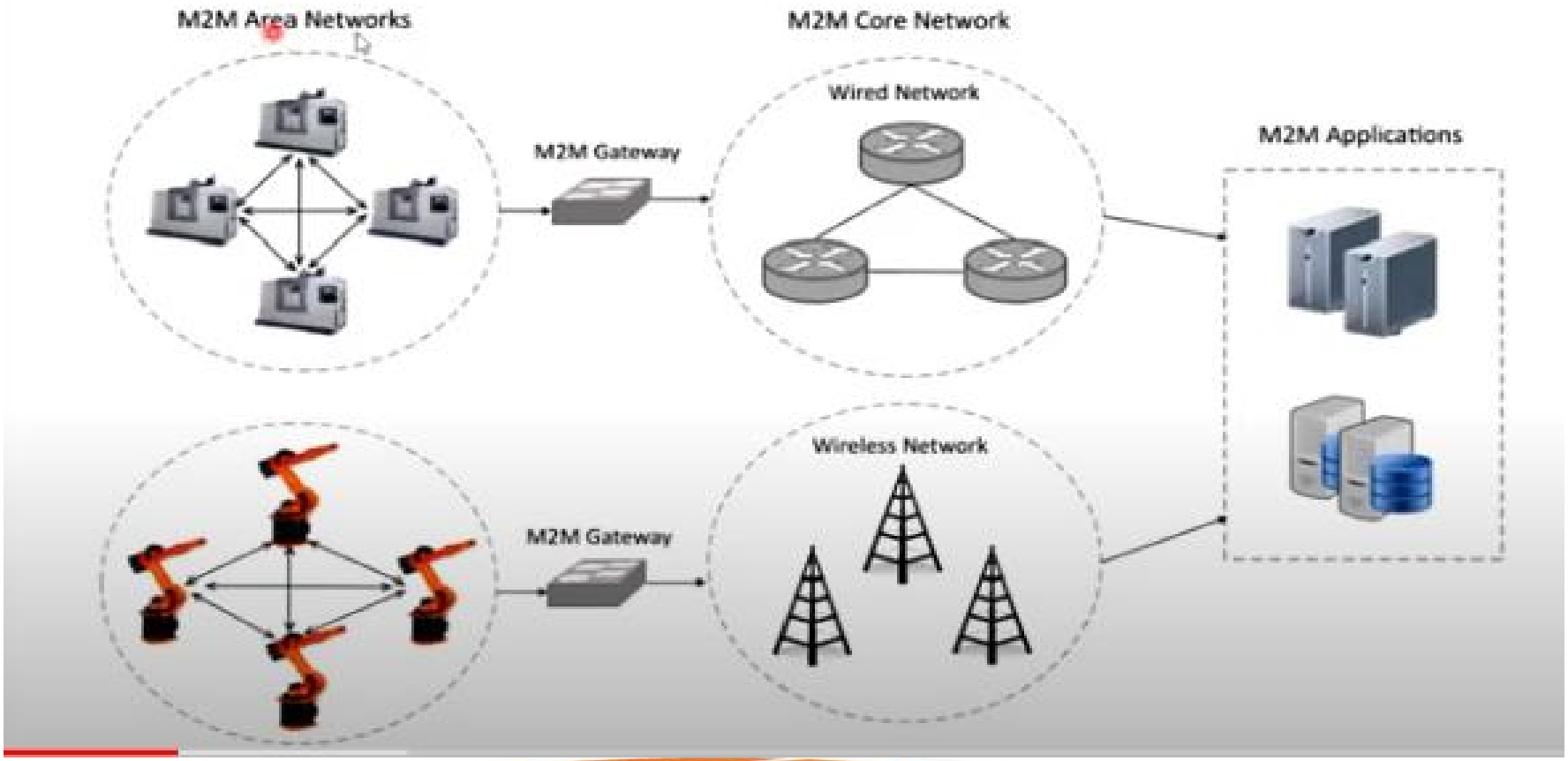
Key features of M2M

- Some of the key features of M2M communication system are given below:
- **Low Mobility :** M2M Devices do not move, move infrequently, or move only within a certain region
- **Time Controlled :** Send or receive data only at certain pre-defined periods
- **Time Tolerant :** Data transfer can be delayed
- **Packet Switched :** Network operator to provide packet switched service with or without an MSISDN
- **Online small Data Transmissions:** MTC Devices frequently send or receive small amounts of data.

- **Monitoring:** Not intend to prevent theft or vandalism but provide functionality to detect the events
- **Low Power Consumption :** To improve the ability of the system to efficiently service M2M applications
- **Location Specific Trigger :** Intending to trigger M2M device in a particular area

e.g. wake up the device

Architecture and components of M2M



Architecture and components of M2M

- **M2M Device:** Device capable of replying to request for data contained within those devices or capable of transmitting data autonomously.
- Sensors and communication devices are the endpoints of M2M applications.
- Generally, devices can connect directly to an operator's network, or they will probably interconnect using WPAN technologies such as ZigBee or Bluetooth.
- Backhaul to an operator's network is than achieved via gateways that encapsulate and manage all devices. Consequently, addressing and identifying, e.g., routing, of the devices relies heavily on the gateways. Devices that connect via gateways are normally outside the operator's responsibility but belong to M2M applications that are provided by service or application providers.

Architecture and components of M2M

- Sensors and devices that connect directly into an operator's network (via embedded SIM, TPM and radio stack or fixed line access) are endpoints of the network.
- Thus, the responsibility in terms of accountability, SLAs etc., lies within the network operator (or virtual network operator).
- This holds true especially with respect to TPM where it is necessary to ensure that the module is really that reliable and well protected.

- **M2M Area Network (Device Domain):** Provide connectivity between M2M Devices and M2M Gateways, e.g. personal area network.

- **M2M Gateway:** Equipment that uses M2M capabilities to ensure M2M Devices inter-working and interconnection to the communication network.
- Gateways and routers are the endpoints of the operator's network in scenarios where sensors and M2M devices do not connect directly to the network.
- Thus, the task of gateways and routers are twofold.
- Firstly, they have to ensure that the devices of the capillary network may be reached from outside and vice versa.
- These functions are addressed by the access enablers, such as identification, addressing, accounting etc., from the operator's platform and have to be supported at the gateway's side as well.

- Thus, platform and gateway form a distributed system, where generic and abstract capabilities are implemented on the gateway's side.
- Consequently, there will be a control flow between gateway and operator's platform that has to be distinguished from the data channel that is to transfer M2M application data.
- Secondly, there may be the need to map bulky internet protocols to their lightweight counterpart in low-power sensor networks. However, the latter application might lose its relevance since there are implementations of IPv6 for sensor networks available, that allow an all-IP approach.

- **M2M Communication Networks (Network Domain):** It covers the
- communications between the M2M Gateway(s) and M2M application(s), e.g. xDSL, LTE, WiMAX, and WLAN.

- **M2M Applications:** It contains the middleware layer where data goes through various application services and is used by the specific business-processing engines.
- M2M applications will be based on the infrastructural assets (e.g., access enablers) that are provided by the operator. Applications may either target at end users, such as user of a specific M2M solution, or at other application providers to offer more refined building blocks by which they can build more sophisticated M2M solutions and services. e.g. customer care functionality, elaborate billing functions, etc.
- Those services, or service enablers, may be designed and offered by an application provider, but they might be offered by the operator via the operator platform itself.

Requirements for M2M

- Some of the general requirements for the M2M System, as specified by ETSI, are
- given below.

- **M2M Application communication principles:**
- The M2M system shall be able to allow communication between M2M Applications in the Network and Applications Domain, and the M2M Device or M2M Gateway, by using multiple communication means, **e.g. SMS, GPRS and IP Access**.
- Also a Connected Object may be able to communicate in a peer-to-peer manner with **any other Connected Object**.
- The M2M System should abstract the underlying network structure including **any network addressing mechanism** used,
- e.g. in case of an IP based network the session establishment shall be possible when IP static or dynamic addressing is used.

- **Message Delivery for sleeping devices:**
- The M2M System shall be able to **manage communication towards a sleeping device.**

- **Delivery modes :** The M2M System shall **support anycast, unicast, multicast and broadcast communication modes.**
- Whenever possible a global broadcast should be replaced by a multicast or anycast in order to minimize the load on the communication network

- **Message transmission scheduling:**
- The M2M System shall be able to **manage the scheduling of network** access and of messaging.
- It shall be aware of the scheduling delay tolerance of the M2M Application.

- **Message communication path selection:**
- The M2M System shall be able to optimize communication paths, based on policies such as network cost, delays or transmission failures when other communication paths exist.

- **Communication with devices behind a M2M gateway:**
- **The** M2M System should be able to communicate with Devices behind a M2M gateway.

- **Communication failure notification:**
- M2M Applications, requesting reliable delivery of a message, shall be notified of any failures to deliver the message.

- **Scalability:**
- The M2M System shall be scalable in terms of number of Connected Objects.

- **Abstraction of technologies heterogeneity:**
- The M2M Gateway may be capable of interfacing to various M2M Area Network technologies.

- **M2M Service Capabilities discovery and registration:**
- The M2M System shall support mechanisms to allow M2M Applications to discover M2M Service Capabilities offered to them. Additionally the M2M Device and M2M Gateway shall support mechanisms to allow the registration of its M2M Service Capabilities to the M2M system.

- **M2M Trusted Application:**
- The M2M Core may handle service request responses for trusted M2M Applications by allowing streamlined authentication procedures for these applications. The M2M system may support trusted applications that are applications pre-validated by the M2M Core.

- **Mobility:**
- If the underlying network supports seamless mobility and roaming, the M2M System shall be able to use such mechanisms.

- **Communications integrity:**
- The M2M System shall be able to support mechanisms to assure communications integrity for M2M services.

- **Device/Gateway integrity check:**
- The M2M System shall support M2M Device and M2M Gateway integrity check.

- **Continuous connectivity:**
- The M2M System shall support continuous connectivity, for M2M applications requesting the same M2M service on a regular and continuous basis.
- This continuous connectivity may be de-activated upon request of the Application or by an internal mechanism in the M2M Core.

- **Confirm:**
- The M2M System shall support mechanisms to confirm messages. A message may be unconfirmed, confirmed or transaction controlled.

- **Priority:**
- The M2M System shall support the management of priority levels of the services and communications services. Ongoing communications may be interrupted in order to serve a flow with higher priority (i.e. pre-emption).

- **Logging:** Messaging and transactions requiring non-repudiation shall be capable of being logged. Important events (e.g. received information from the M2M Device or M2M Gateway is faulty, unsuccessful installation attempt from the M2M Device or M2M Gateway, service not operating, etc.) may be logged together with diagnostic information. Logs shall be retrievable upon request.

- **Anonymity:** The M2M System shall be able to support Anonymity. If anonymity is requested by an M2M Application from the M2M Device side and the request is accepted by the network, the network infrastructure will hide the identity and the location of the requestor, subject to regulatory requirements.

- **Time Stamp:** The M2M System shall be able to support accurate and secure and trusted time stamping. M2M Devices and M2M Gateways may support accurate and secure and trusted time stamping.

- **Device/Gateway failure robustness:** After a non-destructive failure, e.g. after a power supply outage, a M2M Device or Gateway should immediately return in a full operating state autonomously, after performing the appropriate initialization
- e.g. integrity check if supported.

- **Radio transmission activity indication and control:**
- The radio transmitting parts (e.g. GSM/GPRS) of the M2M Device/Gateway should be able to provide (if required by particular applications e.g. eHealth) a real-time indication of radio transmission activity to the application on the M2M Device/Gateway, and may be instructed real-time by the application on the M2M Device/Gateway to suspend/resume the radio transmission activity.

Applications of M2M

The applications of M2M cover many areas and the areas in which M2M is currently used are given below:

a. Security : Surveillances, Alarm systems, Access control, Car/driver security

b. Tracking & Tracing : Fleet Management, Order Management, Pay as you drive, Asset Tracking, Navigation, Traffic information, Road tolling, Traffic optimization/steering

c. Payment : Point of sales, Vending machines, Gaming machines

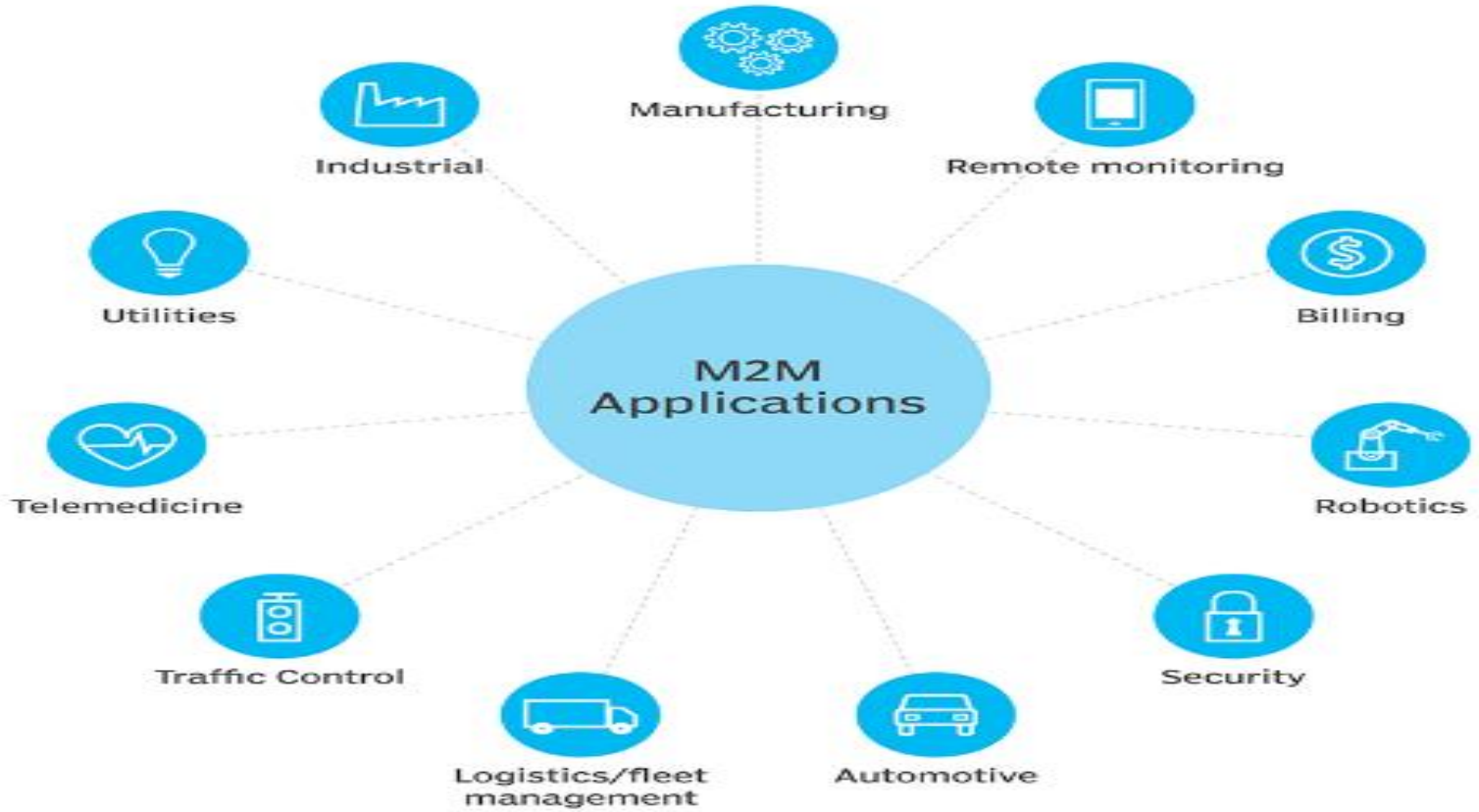
f. Metering : Power, Gas, Water, Heating, Grid control, Industrial metering

g. Manufacturing : Production chain monitoring and automation

h. Facility Management : Home / building / campus automation

d. Health : Monitoring vital signs, Supporting the aged or handicapped, Web Access Telemedicine points, Remote diagnostics

e. Remote Maintenance/Control : Sensors, Lighting, Pumps, Valves, Elevator control, Vending machine control, Vehicle diagnostics


M2M Applications
Manufacturing
Industrial
Remote monitoring
Utilities
Billing
Telemedicine
Robotics
Traffic Control
Security
Logistics/fleet management
Automotive

Difference between IoT and M2M

- 1. Internet of Things :
- IOT is known as the Internet of Things where things are said to be the communicating devices that can interact with each other using a communication media. Usually every day some new devices are being integrated which uses IoT devices for its function. These devices use various sensors and actuators for sending and receiving data over the internet. It is an ecosystem where the devices share data through a communication media known as the internet.
- Smart Home
- Connected cars
- Agriculture and Retail
- Smart cities
- Healthcare
- Poultry and Farming

Difference between IoT and M2M

- 2. Machine to Machine :
- This is commonly known as Machine to machine communication. It is a concept where two or more than two machines communicate with each other without human interaction using a wired or wireless mechanism. M2M is an technology that helps the devices to connect between devices without using internet. M2M communications offer several applications such as security, tracking and tracing, manufacturing and facility management.
- Warehouse Management Systems (WMS)
- Supply Chain Management (SCM)
- Harvesting energy like oil and gas
- Customer billing like smart meters
- Traffic control
- telemedicine
- Remote monitoring

Difference between IoT and M2M

M2M versus the IoT	
M2M	**IoT**
M2M is about direct communication between machines.	The IoT is about sensors automation and Internet platform.
It supports point-to-point communication.	It supports cloud communication.
Devices do not necessarily rely on an Internet connection.	Devices rely on an Internet connection.
M2M is mostly hardware-based technology.	The IoT is both hardware- and software-based technology.
Machines normally communicate with a single machine at a time.	Many users can access at one time over the Internet.
A device can be connected through mobile or other network.	Data delivery depends on the Internet protocol (IP) network.

PARAMETERS	M2M	IOT
Abbreviation for	Machine to Machine	Internet of Things
Philosophy	M2M is Concept where two or more machines can communicate with each other and carry out certain functions without human intervention. Some degree of intelligence can be observed in M2M model.	IOT is an ecosystem of connected devices (via Internet) where the devices have ability to collect and transfer data over a network automatically without human intervention. IOT helps objects to interact with internal and/or external environment which in turn control the decision making.
Connection Type	Point to Point	Through IP Network using various Communication types
Communication protocols	Old proprietary protocols and communication techniques	Internet protocols used commonly
Value Chain	Linear	Multi-sided
Focus Area	For monitoring and control of 1 or few infrastructure/assets.	To address everyday needs of humans.
Sharing of collected data	Data collected is not shared with other applications	Data is shared with other applications (like weather forecasts, social media etc.) improve end user experience
Device dependency	Devices usually don't rely over Internet connection	Devices usually rely over Internet connection
Device in scope	Limited devices in scope	Large number of device sin scope
Scalability	Less scalable than IOT	More scalable due to cloud based architecture
Example	Remote monitoring, fleet control	Smart Cities, smart agriculture etc.
Business Type	B2B	B2B and B2C
Technology Integration	Vertical	Vertical and Horizontal
Open APIs	Not supported	Supported
Related terms	Sensors , Data and Information	End users, devices, wearables, Cloud and Big Data

THANKS!