SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po),
Coimbatore – 641 107

An Autonomous Institution

DEPARTMENT OF COMPUTER SCIENCE AND DESIGN

Course Code and Name : 19IT503 Internet of Things

Unit 3 – EVOLVING IoT STANDARDS & PROTOCOLS

Topic 1 – IETF IPv6 Routing Protocol for RPL Roll

IETF IPV6 Routing Protocol for RPL Roll

- IETF- Internet Engineering Task Force
- RPL- Routing Protocol for LLNs
  - LLNs- Low power and Lossy Networks
- ROLL- Routing Over Low power and Lossy networks

IETF IPV6 Routing Protocol for RPL Roll

- Low power and lossy networks (LLNs)
  - A class of networks in which both the routers and their interconnect are constrained.
  - LLN routers typically operate with constraints on processing power, memory, and energy (battery power)
  - their interconnects are characterized by high loss rates, low data rates, and instability. LLNs comprise a few dozen routers up to thousands of routers.
  - Supported traffic flows include
    - point-to-point (between devices inside the LLN),
    - point-to-multipoint (from a central control point to a subset of devices inside the LLN)
    - multipoint-to-point (from devices inside the LLN toward a central control point).
- The IPv6 Routing Protocol for LLNs (RPL) is proposed by the IETF to support multipoint-to-point traffic from devices inside the LLN toward a central control point, as well as point to-multipoint traffic from the central control point to the devices inside the LLN.

IETF IPV6 Routing Protocol for RPL Roll

- LLNs consist largely of constrained nodes
  - with limited processing power, memory, and sometimes energy when they are battery operated or energy scavenging.
- These routers are interconnected by lossy unstable links, resulting in relatively high packet loss rates and typically supporting only low data rates.
- Another characteristic of such networks is that the traffic patterns are not simply point-to-point, but in many cases point-to-multipoint or multipoint-to-point. Furthermore, such networks may potentially comprise up to thousands of nodes.
- To address these issues, the IETF ROLL Working Group has defined application-specific routing requirements for an LLN routing protocol; it has also specified the RPL.

IETF IPV6 Routing Protocol for RPL Roll

- Existing routing protocols include
  - OSPF/IS-IS (open shortest path first/ intermediate system to intermediate system),
  - OLSRv2 (optimized link state routing protocol version 2),
  - TBRPF (topology-based reverse path forwarding),
  - RIP (routing information protocol),
  - AODV (ad hoc on-demand distance vector),
  - DYMO (dynamic MANET on-demand),
  - DSR (dynamic source routing).
- Some of the metrics for IoT applications include the following:
  - Routing state memory space—limited memory resources of low power nodes;
  - Loss response—what happens in response to link failures;
  - Control cost—constraints on control traffic;
  - Link and node cost—link and node properties are considered when choosing routes.
- The existing protocols all fail one or more of these goals for IoT applications.

IETF IPV6 Routing Protocol for RPL Roll

- In order to be use of LLN application domains, RPL separates packet processing and forwarding from the routing optimization objective.
- Examples of such objectives include minimizing energy, minimizing latency, or satisfying constraints.
- Consistent with the layered architecture of IP, RPL does not rely on any particular features of a specific link layer technology.
- RPL is able to operate over a variety of different link layers.

IETF IPV6 Routing Protocol for RPL Roll

- RPL operations, require bidirectional links.
- LLN scenarios, communication links may exhibit asymmetric properties.
  - the reachability of a router needs to be verified before the router can be used as a parent.
- RPL expects an external mechanism to be triggered during the parent selection phase in order to verify link properties and neighbour reachability.
  - Neighbour unreachability detection (NUD) is a mechanism,
  - but alternates are possible, including bidirectional forwarding detection and hints from lower layers via layer 2 triggers.
- In general, a detection mechanism that is reactive to traffic is favored in order to minimize the cost of monitoring links that are not being used.

IETF IPV6 Routing Protocol for RPL Roll

- RPL also expects an external mechanism to access and transport some control information, referred to as the “RPL Packet Information,” in data packets.
  - The RPL packet information enables the association of a data packet with an RPL instance and the validation of RPL routing states.
- Example : IPv6 Hop-by-Hop RPL
  - The mechanism is required for all packets except when strict source routing is used which, by nature, prevents endless loops and alleviates the need for the RPL packet information.

IETF IPV6 Routing Protocol for RPL Roll

- RPL provides a mechanism to disseminate information over the dynamically formed network topology to operate autonomously.
- In some applications, RPL assembles topologies of routers that own independent prefixes.
  - A prefix that is owned by a router is advertised as “on-link.”
- RPL have the capability to bind a subnet together with a common prefix and to route within that subnet.
- RPL in particular, disseminate IPv6 neighbour discovery (ND) information prefix information option (PIO) and the route information option (RIO).

IETF IPV6 Routing Protocol for RPL Roll

- Some basic definitions in RPL are as follows :
  - Directed acyclic graph (DAG) is a directed graph with no cycles.
  - Destination-oriented DAG (DODAG) is a DAG rooted at a single destination.
- RPL defines optimization objective when forming paths toward roots based on one or more metrics.
  - Metrics may include both link properties (reliability, latency) and node properties (e.g., powered on not).

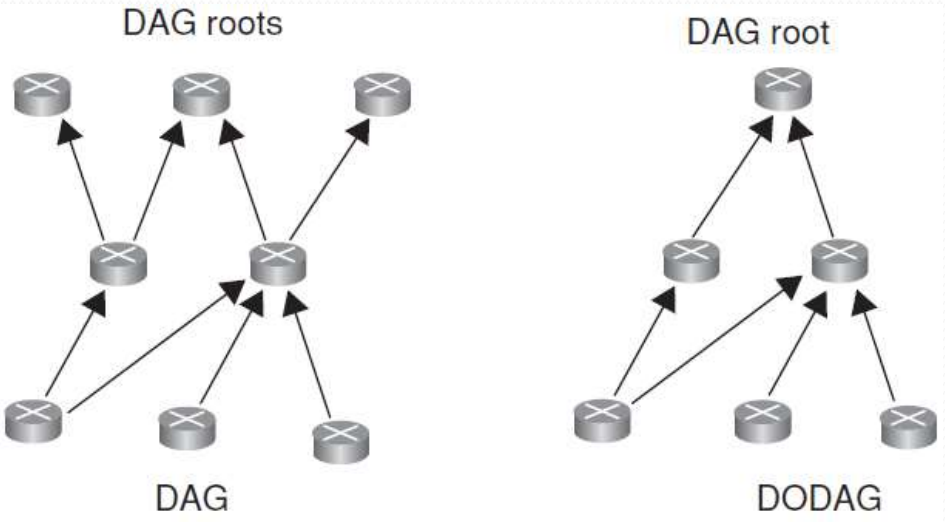
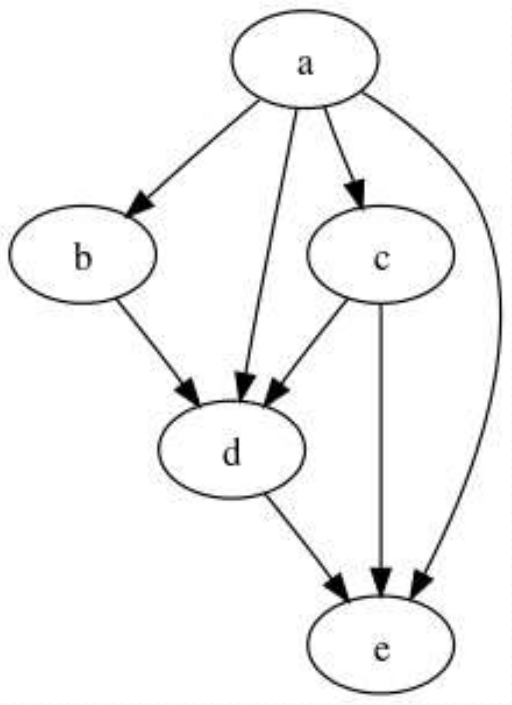
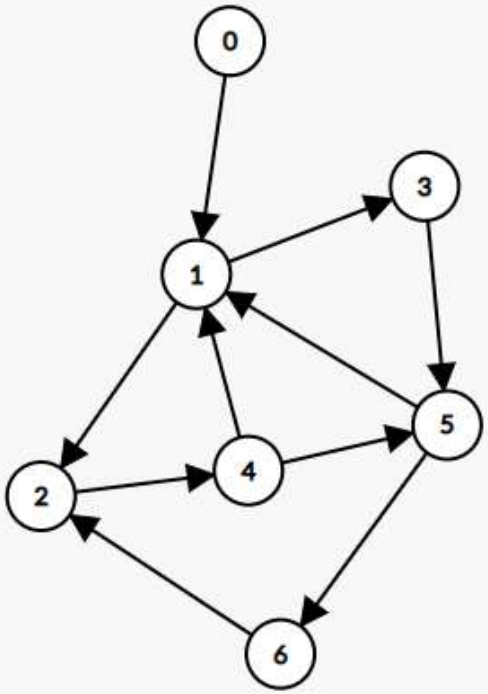


FIGURE 5.1 DAGs and DODAGs.

Example of a directed acyclic and cyclic graph



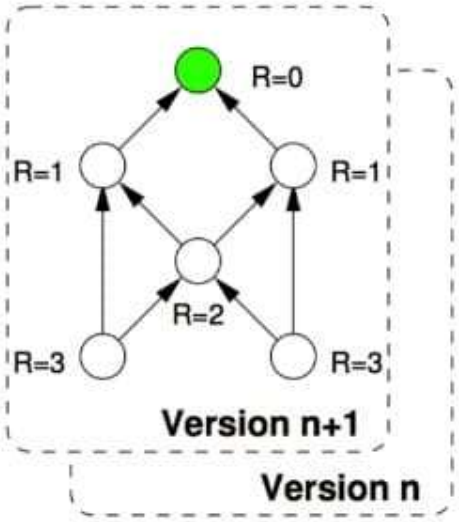
Directed Acyclic Graph



Directed cyclic Graph

DODAG Rank

RPL Rank



- A node's Rank defines the node's individual position relative to other nodes with respect to a DODAG root. The scope of Rank is a DODAG Version.

- Upward path is so common (mp2p)
- Downward path is optional mainly for p2p and p2mp

Upward—Rank decreases
Downward--- Rank increases

IETF IPV6 Routing Protocol for RPL Roll

- RPL defines a new ICMPv6 (Internet control message protocol version 6) message with three possible types:
  - DAG information object (DIO)—carries information that allows a node to discover an RPL instance, learn its configuration parameters, and select DODAG parents;
  - DAG information solicitation (DIS)—solicit a DODAG information object from an RPL node;
  - Destination advertisement object (DAO)—used to propagate destination information upward along the DODAG.

IETF IPV6 Routing Protocol for RPL Roll

- A node rank defines a node's relative position within a DODAG with respect to the DODAG root.
- DODAG construction proceeds as follows:
  - Nodes periodically send link-local multicast DIO messages;
  - Stability or detection of routing inconsistencies influence the rate of DIO messages;
  - Nodes listen for DIOs and use their information to join a new DODAG, or to maintain an existing DODAG;
  - Nodes may use a DIS message to solicit a DIO;
  - Based on information in the DIOs, the node chooses parents that minimize path cost to the DODAG root.
- RPL is optimized for many-to-one and one-to-many traffic patterns

IETF IPV6 Routing Protocol for RPL Roll

- IETF- Internet Engineering Task Force
- RPL- Routing Protocol for LLNs
  - LLNs- Low power and Lossy Networks
- ROLL- Routing Over Low power and Lossy networks

IETF IPV6 Routing Protocol for RPL Roll

- Low power and lossy networks (LLNs)
  - A class of networks in which both the routers and their interconnect are constrained.
  - LLN routers typically operate with constraints on processing power, memory, and energy (battery power)
  - their interconnects are characterized by high loss rates, low data rates, and instability. LLNs comprise a few dozen routers up to thousands of routers.
  - Supported traffic flows include
    - point-to-point (between devices inside the LLN),
    - point-to-multipoint (from a central control point to a subset of devices inside the LLN)
    - multipoint-to-point (from devices inside the LLN toward a central control point).
- The IPv6 Routing Protocol for LLNs (RPL) is proposed by the IETF to support multipoint-to-point traffic from devices inside the LLN toward a central control point, as well as point to-multipoint traffic from the central control point to the devices inside the LLN.

IETF IPV6 Routing Protocol for RPL Roll

- LLNs consist largely of constrained nodes
  - with limited processing power, memory, and sometimes energy when they are battery operated or energy scavenging.
- These routers are interconnected by lossy unstable links, resulting in relatively high packet loss rates and typically supporting only low data rates.
- Another characteristic of such networks is that the traffic patterns are not simply point-to-point, but in many cases point-to-multipoint or multipoint-to-point. Furthermore, such networks may potentially comprise up to thousands of nodes.
- To address these issues, the IETF ROLL Working Group has defined application-specific routing requirements for an LLN routing protocol; it has also specified the RPL.

IETF IPV6 Routing Protocol for RPL Roll

- Existing routing protocols include
  - OSPF/IS-IS (open shortest path first/ intermediate system to intermediate system),
  - OLSRv2 (optimized link state routing protocol version 2),
  - TBRPF (topology-based reverse path forwarding),
  - RIP (routing information protocol),
  - AODV (ad hoc on-demand distance vector),
  - DYMO (dynamic MANET on-demand),
  - DSR (dynamic source routing).
- Some of the metrics for IoT applications include the following:
  - Routing state memory space—limited memory resources of low power nodes;
  - Loss response—what happens in response to link failures;
  - Control cost—constraints on control traffic;
  - Link and node cost—link and node properties are considered when choosing routes.
- The existing protocols all fail one or more of these goals for IoT applications.

IETF IPV6 Routing Protocol for RPL Roll

- In order to be use of LLN application domains, RPL separates packet processing and forwarding from the routing optimization objective.
- Examples of such objectives include minimizing energy, minimizing latency, or satisfying constraints.
- Consistent with the layered architecture of IP, RPL does not rely on any particular features of a specific link layer technology.
- RPL is able to operate over a variety of different link layers.

IETF IPV6 Routing Protocol for RPL Roll

- RPL operations, require bidirectional links.
- LLN scenarios, communication links may exhibit asymmetric properties.
  - the reachability of a router needs to be verified before the router can be used as a parent.
- RPL expects an external mechanism to be triggered during the parent selection phase in order to verify link properties and neighbour reachability.
  - Neighbour unreachability detection (NUD) is a mechanism,
  - but alternates are possible, including bidirectional forwarding detection and hints from lower layers via layer 2 triggers.
- In general, a detection mechanism that is reactive to traffic is favored in order to minimize the cost of monitoring links that are not being used.

IETF IPV6 Routing Protocol for RPL Roll

- RPL also expects an external mechanism to access and transport some control information, referred to as the “RPL Packet Information,” in data packets.
  - The RPL packet information enables the association of a data packet with an RPL instance and the validation of RPL routing states.
- Example : IPv6 Hop-by-Hop RPL
  - The mechanism is required for all packets except when strict source routing is used which, by nature, prevents endless loops and alleviates the need for the RPL packet information.

IETF IPV6 Routing Protocol for RPL Roll

- RPL provides a mechanism to disseminate information over the dynamically formed network topology to operate autonomously.
- In some applications, RPL assembles topologies of routers that own independent prefixes.
  - A prefix that is owned by a router is advertised as “on-link.”
- RPL have the capability to bind a subnet together with a common prefix and to route within that subnet.
- RPL in particular, disseminate IPv6 neighbour discovery (ND) information prefix information option (PIO) and the route information option (RIO).

IETF IPV6 Routing Protocol for RPL Roll

- Some basic definitions in RPL are as follows :
  - Directed acyclic graph (DAG) is a directed graph with no cycles.
  - Destination-oriented DAG (DODAG) is a DAG rooted at a single destination.
- RPL defines optimization objective when forming paths toward roots based on one or more metrics.
  - Metrics may include both link properties (reliability, latency) and node properties (e.g., powered on not).

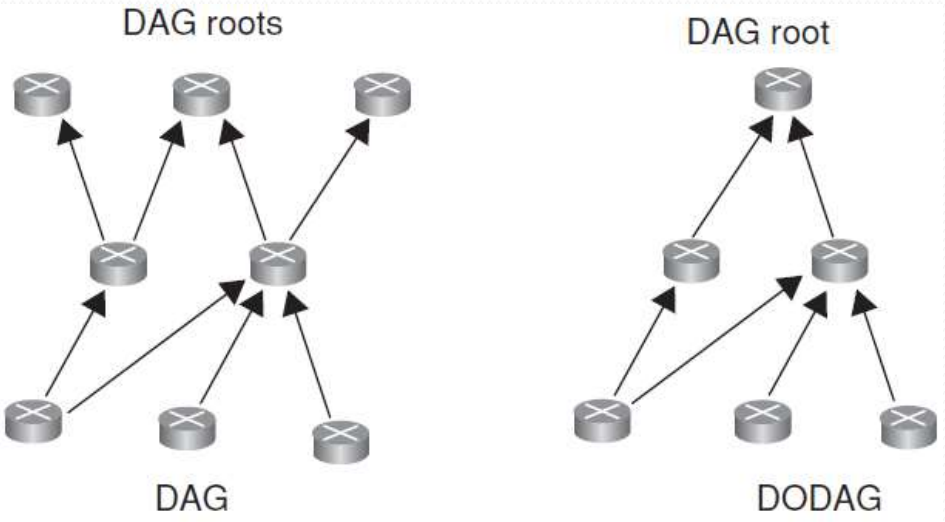
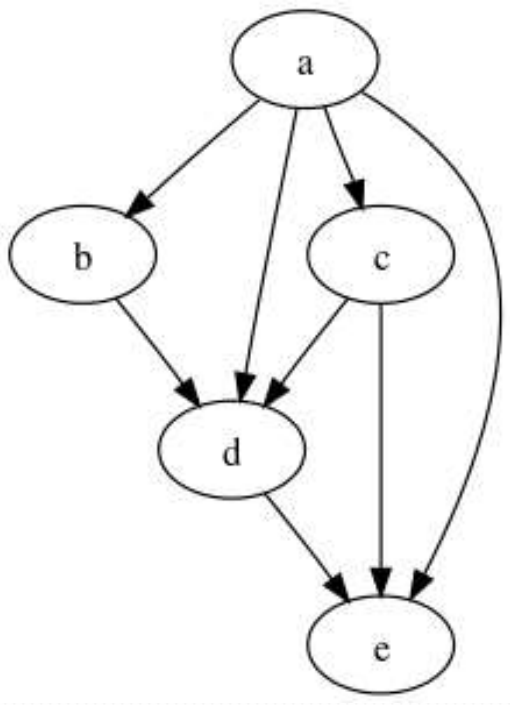
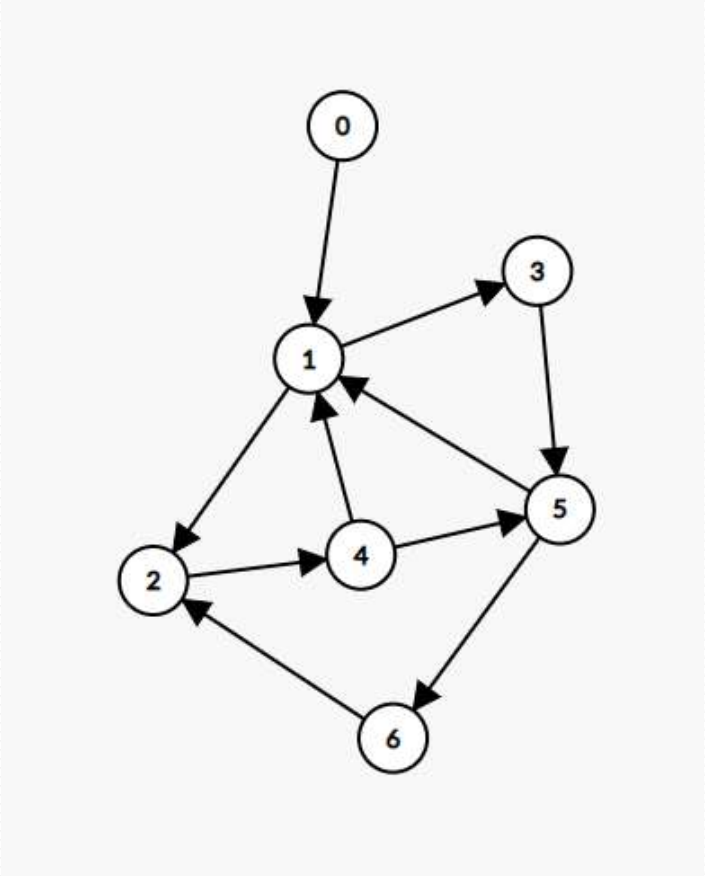


FIGURE 5.1 DAGs and DODAGs.

Example of a directed acyclic and cyclic graph



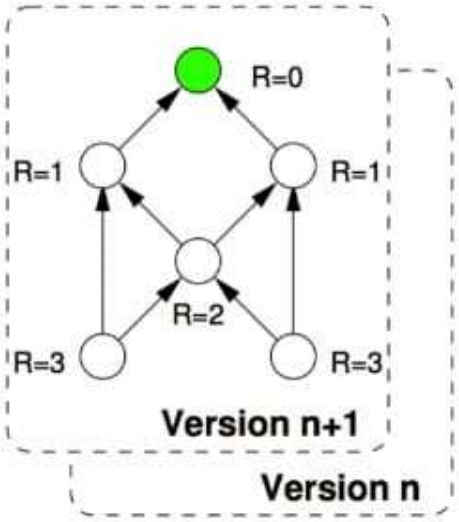
Directed Acyclic Graph



Directed cyclic Graph

DODAG Rank

RPL Rank



- A node's Rank defines the node's individual position relative to other nodes with respect to a DODAG root. The scope of Rank is a DODAG Version.

- Upward path is so common (mp2p)
- Downward path is optional mainly for p2p and p2mp

Upward—Rank decreases
Downward--- Rank increases

IETF IPV6 Routing Protocol for RPL Roll

- RPL defines a new ICMPv6 (Internet control message protocol version 6) message with three possible types:
  - DAG information object (DIO)—carries information that allows a node to discover an RPL instance, learn its configuration parameters, and select DODAG parents;
  - DAG information solicitation (DIS)—solicit a DODAG information object from an RPL node;
  - Destination advertisement object (DAO)—used to propagate destination information upward along the DODAG.

IETF IPV6 Routing Protocol for RPL Roll

- A node rank defines a node's relative position within a DODAG with respect to the DODAG root.
- DODAG construction proceeds as follows:
  - Nodes periodically send link-local multicast DIO messages;
  - Stability or detection of routing inconsistencies influence the rate of DIO messages;
  - Nodes listen for DIOs and use their information to join a new DODAG, or to maintain an existing DODAG;
  - Nodes may use a DIS message to solicit a DIO;
  - Based on information in the DIOs, the node chooses parents that minimize path cost to the DODAG root.
- RPL is optimized for many-to-one and one-to-many traffic patterns

Constrained Application Protocol (CoAP)

- Background
- Messaging Model
- Request/Response Model
- Intermediaries and Caching

Constrained Application Protocol (CoAP) Background

- CoAP is a simple application layer protocol targeted to simple electronic devices (e.g., IoT/M2M things) to allow them to communicate interactively over the Internet.
  - CoAP is designed for low power sensors (wireless sensor network [WSN] nodes and actuators.
- CoAP can be seen as a specialized web transfer protocol for use with constrained networks and nodes for M2M applications.
- CoAP operates with HTTP (hypertext transfer protocol) for basic support with the web

Constrained Application Protocol (CoAP) Background

- CoAP protocol are as follows:
  - (i) minimal complexity for the mapping with HTTP;
  - (ii) low header overhead and low parsing complexity;
  - (iii) support for the discovery of resources;
  - (iv) simple resource subscription process;
  - (v) simple caching based on max-age.

Constrained Application Protocol (CoAP) Background

- CoAP makes use of two message types, requests and responses, using a simple binary base header format.
  - Any bytes after the headers in the packet are considered the message body if any.
  - The length of the message body is implied by the datagram length.

Constrained Application Protocol (CoAP) Background

- The constrained nodes for which CoAP is targeted often have 8-bit microcontrollers with small amounts of ROM and RAM, while networks such as 6LoWPAN (IPv6 OVER LOWPOWER WPAN)
- CoAP provides a method/response interaction model between application end-points, supports built-in resource discovery, and includes key web concepts such as URIs (uniform resource identifiers) and content-types.
- CoAP easily translates to HTTP for integration with the web.

Constrained Application Protocol (CoAP) Background

- The use of Web Services (WS) on the Internet has become ubiquitous in most applications; it depends on the fundamental representational state transfer (REST) architecture of the web.

Constrained Application Protocol (CoAP) Background

- CoAP has the following main features:
  - Constrained web protocol fulfilling M2M requirements;
  - UDP (User datagram protocol) binding with optional reliability supporting unicast and multicast requests;
  - Asynchronous message exchanges;
  - Low header overhead and parsing complexity;
  - URI and content-type support;
  - Simple proxy and caching capabilities;
  - A stateless HTTP mapping, allowing proxies to be built providing access to CoAP resources via HTTP in a uniform way or for HTTP simple interfaces to be realized alternatively over CoAP
  - Security binding to datagram transport layer security (DTLS).

Constrained Application Protocol (CoAP) Background

- M2M interactions typically result in a CoAP implementation acting in both client and server roles (called an end-point).
- A CoAP request is equivalent to that of HTTP and is sent by a client to request an action (using a method code) on a resource (identified by a URI) on a server.
- The server then sends a response with a response code; this response may include a resource representation.
- Unlike HTTP, CoAP deals with these interchanges asynchronously over a datagram-oriented transport such as UDP. This is done logically using a layer of messages that supports optional reliability (with exponential back-off).
- CoAP defines four types of messages:
  - confirmable (CON), non-confirmable (NON), acknowledgement, reset;
- Method codes and response codes included in some of these messages make them carry requests or responses.
- The basic exchanges of the four types of messages are transparent to the request/response interactions.

Constrained Application Protocol (CoAP) Background

- CoAP logically as
  - using a two-layer approach,
  - a CoAP messaging layer used to deal with UDP (User Datagram Protocol)
  - the asynchronous nature of the interactions,
  - the request/response interactions using method and response codes

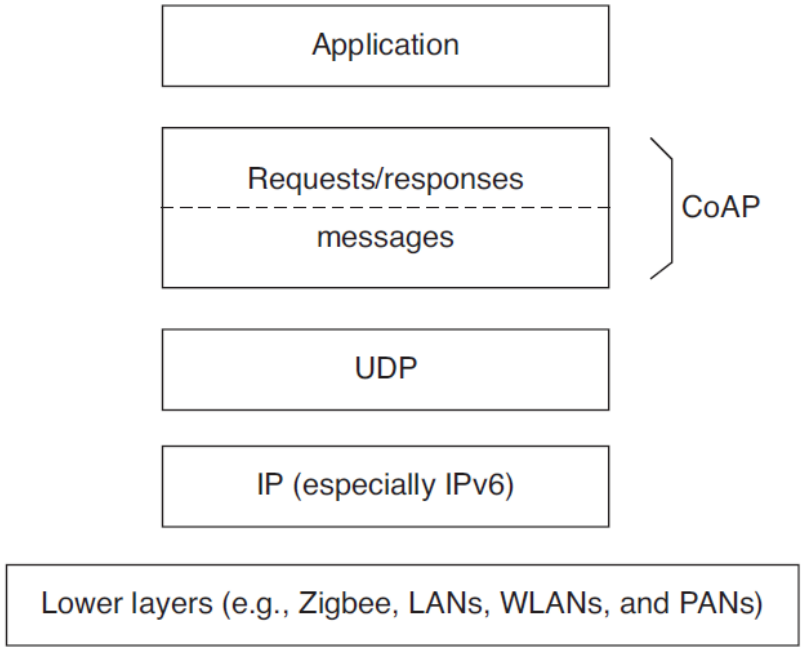


FIGURE 5.2 Abstract layering of CoAP.

Constrained Application Protocol (CoAP) Background

- CoAP is, however, a single protocol, with messaging and request/response just features of the CoAP header.
- Figure depicts the overall protocol stack that is being considered in the CoAP context.

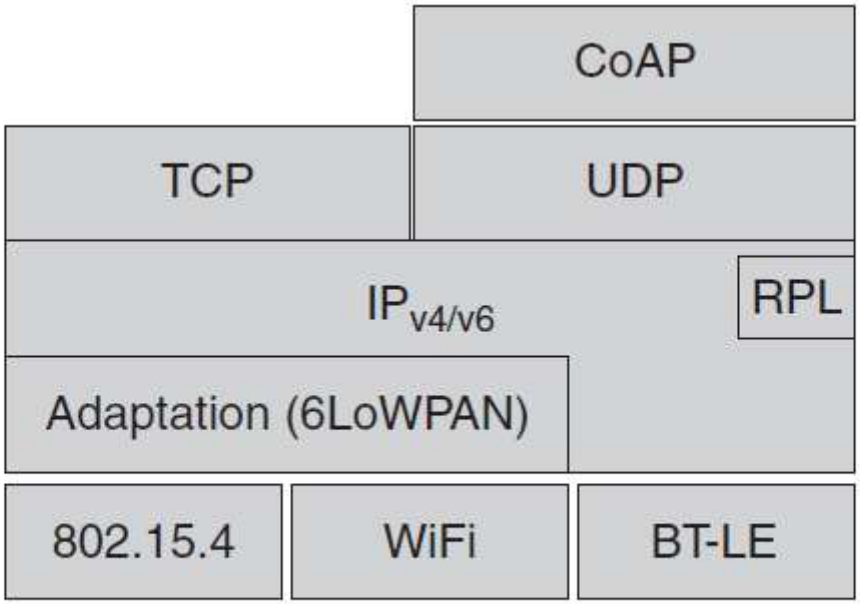


FIGURE 5.3 Overall protocol stack in CoAP's environment.

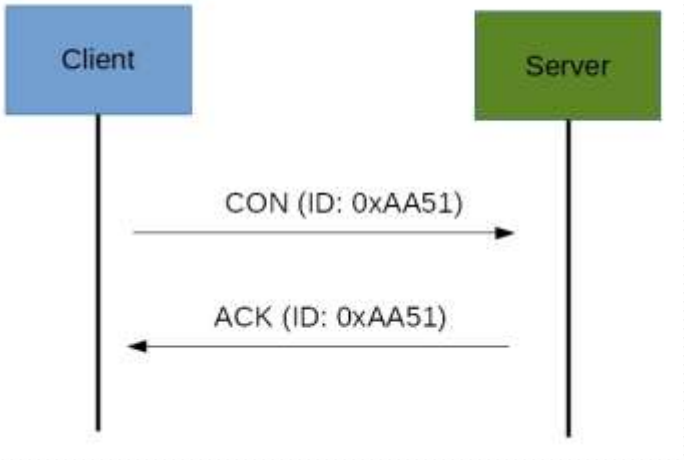
Constrained Application Protocol (CoAP) Messaging Model

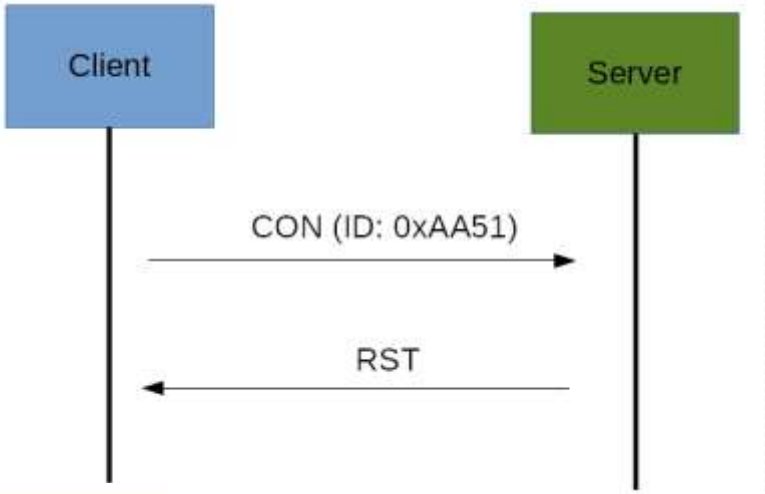
- The CoAP messaging model is based on the exchange of messages over UDP between end-points.
  - It uses a short fixed-length binary header (4 bytes) that may be followed by compact binary options and a payload.
  - This message format is shared by requests and responses.
  - Each CoAP message contains a message ID used to detect duplicates and for optional reliability.

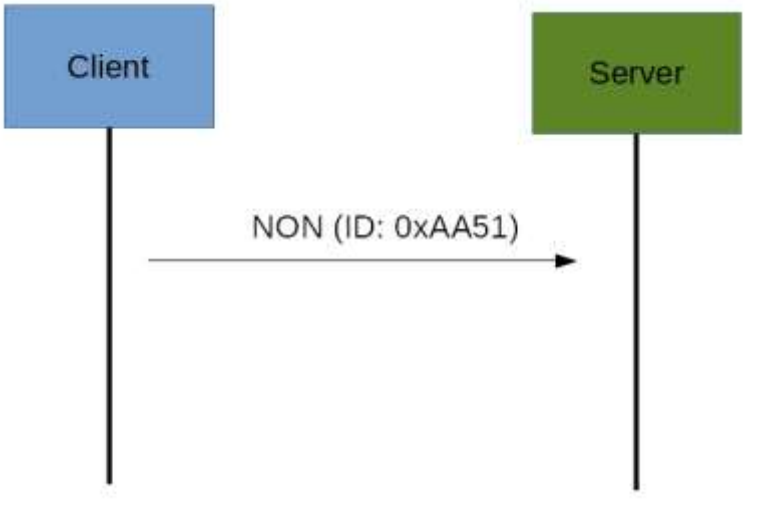
Constrained Application Protocol (CoAP) Messaging Model

- Reliability is provided by marking a message as CON.
- A CON message is retransmitted using a default timeout and exponential back-off between retransmissions, until the recipient sends an acknowledgement message (ACK) with the same message ID from the corresponding end-point.
- When a recipient is not able to process a CON message, it replies with a reset message (RST) instead of an ACK.
- A message that does not require reliable delivery, for example, each single measurement out of a stream of sensor data, can be sent as a NONmessage.
  - These are not acknowledged, but still have a message ID for duplicate detection.
  - When a recipient is not able to process a NON message, it may reply with an RST.
- Since CoAP is based on UDP, it also supports the use of multicast IP destination addresses, enabling multicast CoAP requests.

CON and NON


Client
Server
CON (ID: 0xAA51)
ACK (ID: 0xAA51)


Client
Server
CON (ID: 0xAA51)
RST


Client
Server
NON (ID: 0xAA51)

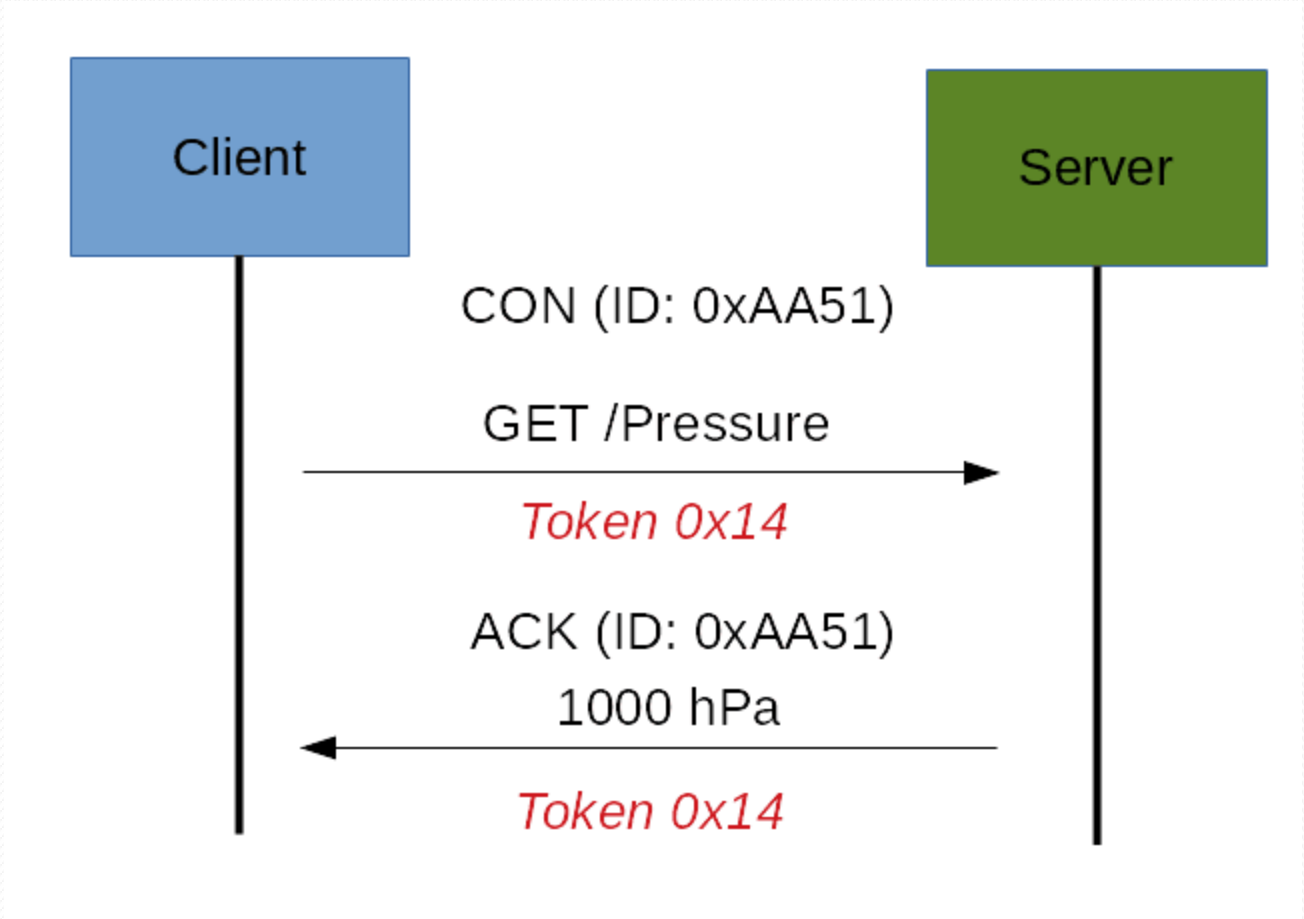
Constrained Application Protocol (CoAP) Request/Response Model

- CoAP messages, which include either a method code or response code, respectively.
- Optional (or default) request and response information, such as the URI (uniform resource identifier) and payload content-type, are carried as CoAP options.
- A token option is used to match responses to requests independent of the underlying messages.

Constrained Application Protocol (CoAP) Request/Response Model

- A request is carried in a CON (confirmable) or NON (non-confirmable) message, and if immediately available, the response to a request carried in a CON message is carried in the resulting ACK message. This is called a **piggy-backed response**.
- If the server is not able to respond immediately to a request carried in a CON message, it simply responds with an empty ACK message so that the client can stop retransmitting the request.
- When the response is ready, the server sends it in a new CON message (which then in turn needs to be acknowledged by the client). **This is called a separate response.**
- Likewise, if a request is sent in a NON message, then the response is usually sent using a new NON message, although the server may send a CON message.
- CoAP makes use of GET, PUT, POST, and DELETE methods in a similar manner to HTTP.

Request/Response Model



Constrained Application Protocol (CoAP) Intermediaries and Caching

- The protocol supports the caching of responses in order to efficiently fulfill requests.
- Simple caching is enabled using freshness and validity information carried with CoAP responses.
- A cache could be located in an end-point or an intermediary.

Constrained Application Protocol (CoAP) Intermediaries and Caching

- Proxying is useful in constrained networks for several reasons, including
  - (i) network traffic limiting,
  - (ii) to improve performance,
  - (iii) to access resources of sleeping devices,
  - (iv) for security reasons.
- The proxying of requests on behalf of another CoAP end-point is supported in the protocol.
- The URI of the resource to request is included in the request, while the destination IP address is set to the proxy.

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC)

- Approach
- Architectural Reference Model for MTC

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC)
Approach

- Current mobile networks are optimized for human-to-human (H2H) traffic and not for M2M/MTC interactions; hence, optimizations for MTC are advantageous.
- For example, one needs lower costs to reflect lower MTC ARPUs (average revenue per user); also, there is a need to support triggering.
- Hence, 3GPP has started work on M2Mspecification in 2010 for interoperable solutions, particularly in the 3G/4G/LTE context.

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC) Approach

TABLE 5.1 3GPP Specifications Related to MTC

3GPP Specifications	Specifications Associated with or Affected by MTC Work
22.011	Service accessibility
22.368	Service requirements for MTC; stage 1
23.008	Organization of subscriber data
23.012	Location management procedures
23.060	General packet radio service (GPRS); service description; stage 2
23.122	Non-access-stratum (NAS) functions related to mobile station (MS) in idle mode
23.203	Policy and charging control architecture
23.401	GPRS enhancements for evolved universal terrestrial radio access network (E-UTRAN) access
23.402	Architecture enhancements for non-3GPP accesses
23.888	System improvements for MTC
24.008	Mobile radio interface layer 3 specification; core network protocols; stage 3
24.301	NAS protocol for evolved packet system (EPS); stage 3
24.368	NAS configuration management object (MO)
25.331	Radio resource control (RRC); protocol specification
29.002	Mobile application part (MAP) specification
29.018	GPRS; serving GPRS support node (SGSN)—visitors location register (VLR); Gs interface layer 3 specification
29.060	GPRS; GPRS tunneling protocol (GTP) across the Gn and Gp interface
29.118	Mobility management entity (MME)—VLR SGs interface specification
29.274	3GPP EPS; evolved GTP for control plane (GTPv2-C); stage 3
29.275	Proxy mobile IPv6 (PMIPv6)-based mobility and tunneling protocols; stage 3
29.282	Mobile IPv6 vendor-specific option format and usage within 3GPP
31.102	Characteristics of the universal subscriber identity module (USIM) application
33.868	Security aspects of MTC
36.331	Evolved universal terrestrial radio access (E-UTRA); RRC; protocol specification
37.868	RAN improvements for MTC
43.868	GERAN improvements for MTC
44.018	Mobile radio interface layer 3 specification; RRC protocol
44.060	GPRS; MS–base station system (BSS) interface; radio link control/medium access control (RLC/MAC) protocol
45.002	Multiplexing and multiple access on the radio path

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC) Approach

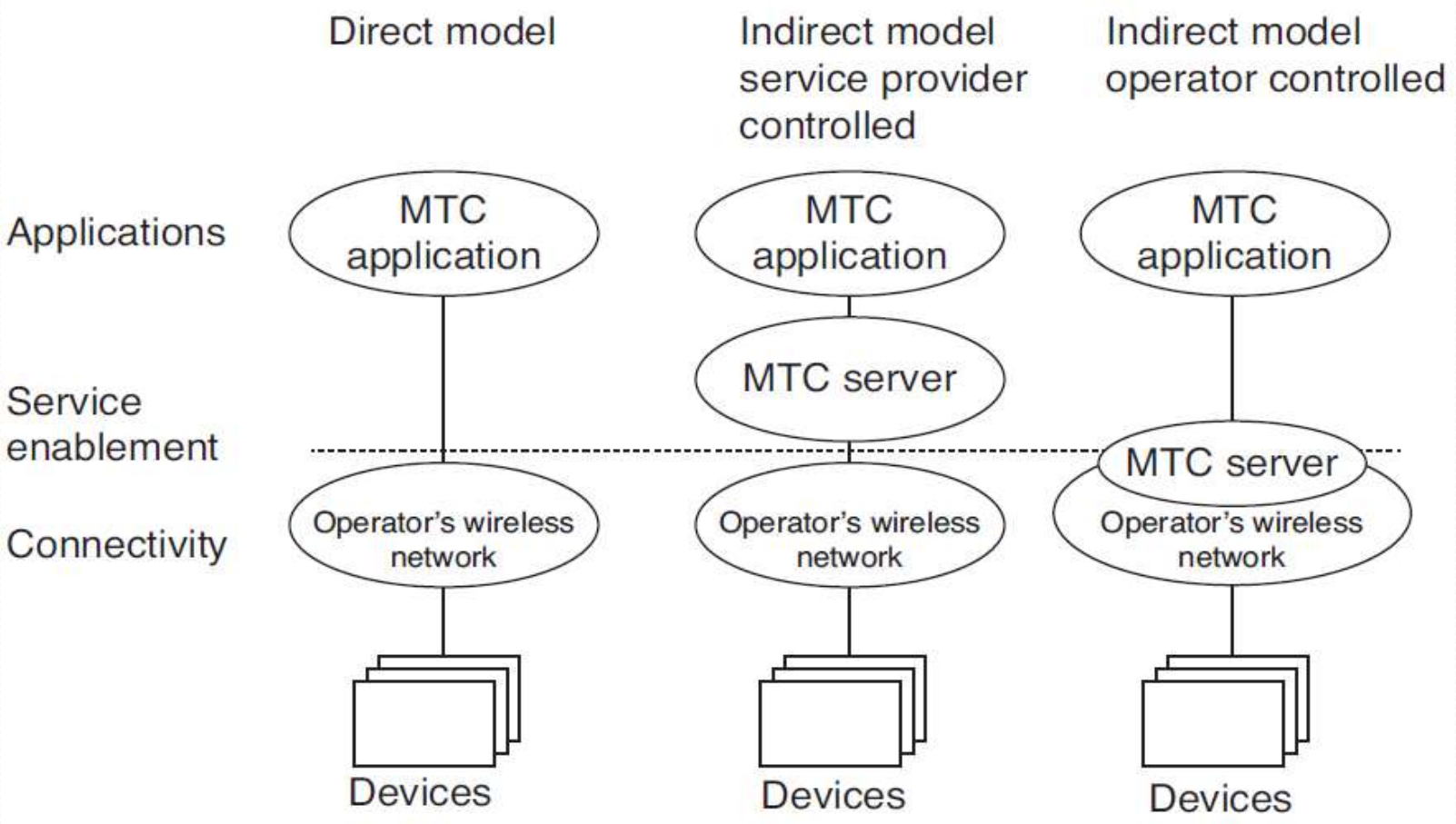
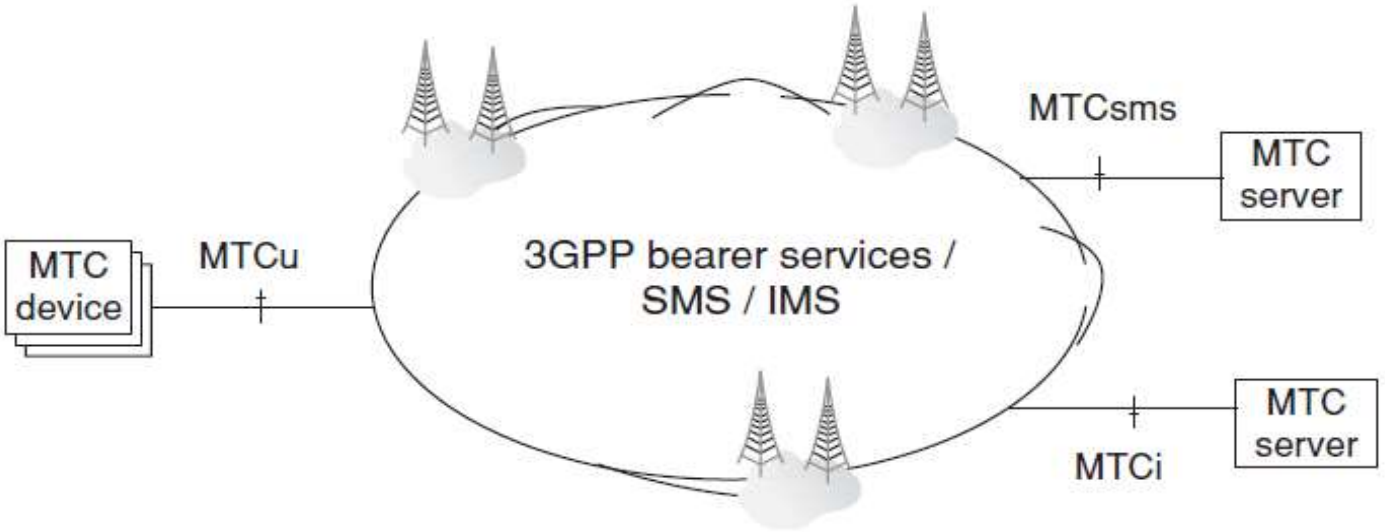


FIGURE 5.4 M2M in 3GPP—service models.

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC) Approach

- In architecture, the interfaces are as follows:
  - MTCu: provides MTC devices access to the 3GPP network for the transport of user traffic;
  - MTCi: the reference point for MTC server to connect the 3GPP network via 3GPP bearer service;
  - MTCsms: the reference point for MTC server to connect the 3GPP network via 3GPP SMS.



Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC) Approach

- The key document *3rd Generation Partnership Project Service Requirements for Machine Type Communications*—focused on
  - overload and congestion control,
  - extended access barring (EAB),
  - low priority access,
  - APN (access point name)-based congestion control,
  - downlink throttling.

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC)
Approach

- For MTC communication, the following communication scenarios are identified:
  - (i) MTC devices communicating with one or more MTC server;
  - (ii) MTC devices communicating with each other.

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC) Approach

- For MTC devices communicating with one or more MTC servers, the following use cases exist:
  - (a) MTC server controlled by the network operator; namely the MTC server is located in the operator domain. Here
    - The network operator offers API (e.g., Open Systems Architecture [OSA]) on its MTC server(s)
    - MTC user accesses MTC server(s) of the network operator via API
  - (b) MTC server not controlled by the network operator; namely MTC server is located outside the operator domain. Here
    - The network operator offers the network connectivity to the MTC server(s) located outside of the network operator domain

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC)
Approach

- MTC applications do not all have the same characteristics.
- This implies that not every system optimization is suitable for every MTC application.
- Therefore, MTC features are to provide structure for the different system optimization possibilities that can be invoked.

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC) Approach

- The following MTC features have been defined:
  - Low mobility
  - Time controlled
  - Time tolerant
  - Packet switched (PS) only (here the MTC feature PS only is intended for use with MTC devices that only require packet switched services)
  - Small data transmissions
  - Mobile originated only
  - Infrequent mobile terminated
  - MTC monitoring
  - Priority alarm
  - Secure connection
  - Location-specific trigger
  - Network provided destination for uplink data
  - Infrequent transmission

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC)
Architectural Reference Model for MTC

- *3rd Generation Partnership Project Service Requirements for Machine Type Communications* focuses on numbers and addressing, on improvements of device triggering, and on interfaces between MTC server and mobile network.
- Referring to Figure in next slide,

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC) Architectural Reference Model for MTC

MTC-IWF is a new interworking function between (external) MTC server and operator core network handling security, authorization, authentication, and charging.

MTCsp is a new control interface for interactions with MTC server

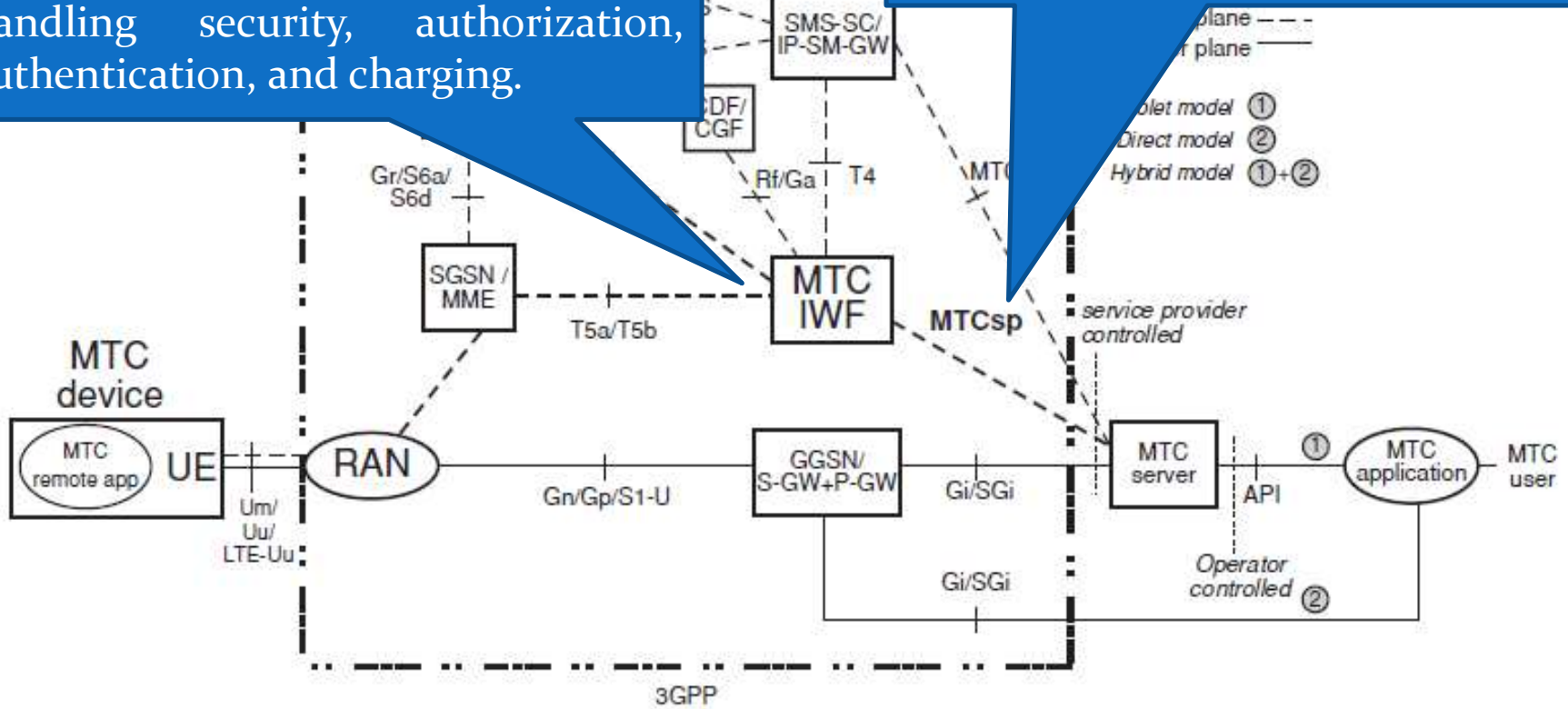


FIGURE 5.5 M2M in 3GPP—Architecture.

https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-015-0479-y/tables/4

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC)
Architectural Reference Model for MTC

- The end-to-end application, between the user equipment (UE) used for MTC and the MTC application, uses services provided by the 3GPP system, and optionally services provided by an MTC server.
- The 3GPP system provides transport and communication services (including 3GPP bearer services, IMS, and SMS) including various optimizations that can facilitate MTC.
- UE used for MTC connecting to the 3GPP network (UTRAN, E-UTRAN, GERAN, I-WLAN, and so on) via the Um/Uu/LTE-Uu interface.

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC)
Architectural Reference Model for MTC

- The architecture encompasses a number of models as follows:
  - Direct model —direct communication provided by the 3GPP operator: The MTC application connects directly to the operator network without the use of any MTC server;
  - Indirect model —MTC service provider controlled communication: The MTC server is an entity outside of the operator domain. The MTCsp and MTCsms are external interfaces (i.e., to a third-party M2M service provider);
  - Indirect model—3GPP operator controlled communication: The MTC server is an entity inside the operator domain. The MTCsp and MTCsms are internal to the public land mobile network (PLMN);
  - Hybrid model: The direct and indirect models are used simultaneously in the hybrid model, for example, connecting the user plane using the direct model and doing control plane signalling using the indirect model.

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC)
Architectural Reference Model for MTC

- In several countries, regulators have indicated that there are not enough (mobile) numbers available for M2M applications.
- 3GPP postulates that solutions will have to support 100× more M2M devices than devices for H2H communications.
- Proposed solutions include:
  - (i) mid-term solution: special M2M number ranges with longer telephone numbers (e.g., 14 digits);
  - (ii) long-term solution: no longer provide telephone numbers for M2M applications.

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC) Architectural Reference Model for MTC

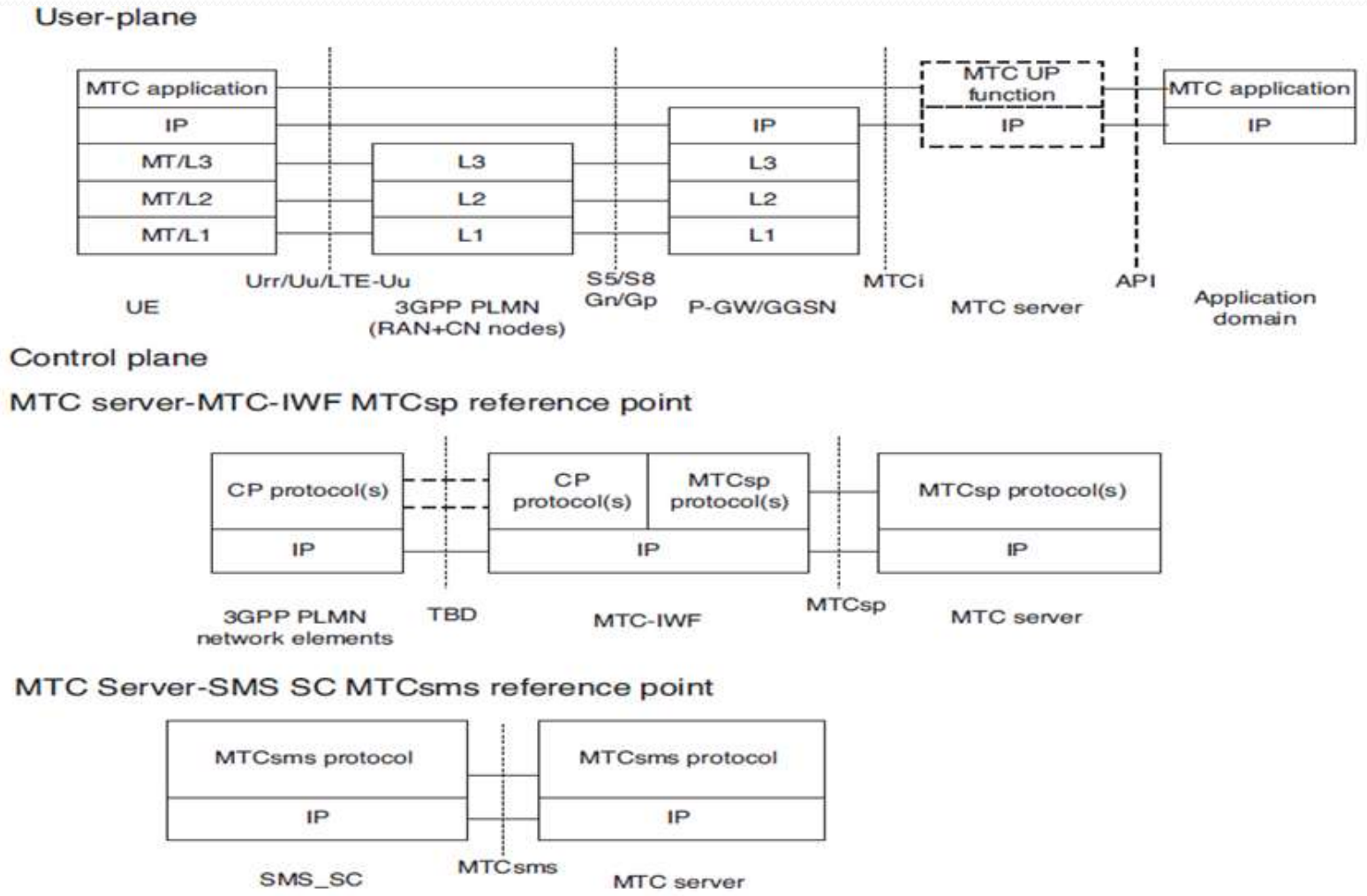


FIGURE 5.6 User and control plane stack for MTC architecture

CENELEC

- European Committee for Electrotechnical Standardization (CENELEC)
  - has adopted the transport profile of Siemens' distribution line carrier communication protocol (CX1) as a standardization proposal.
- The standard aims at supporting open and fault tolerant communication via powerline in intelligent power supply grids.
- As the basis for the transmission protocol, which uses the low voltage network as a communication channel for data of grid sensors and smart meters, the transport profile has been designed to ensure interoperability in accordance with EU Mandate M/441.

CENELEC

- CENELEC TC 13 was planning to forward the CX1 transport profile to TC 57 of the International Electrotechnical Commission (IEC).
- CX1 is already used to connect meters and other intelligent terminal devices in Siemens' SG metering systems, such as in the load switching devices that will replace household ripple control receivers.
- The systems collect energy consumption data and network information, which are then relayed to a control center for further processing.
- The communication protocol can handle any change in the physical communication parameters of a low voltage power supply grid, such as signal attenuation, noise, network disruption and signal coupling, as well as operational changes in network configuration.
- The protocol can also be integrated into existing IEC protocol-based network automation and energy management infrastructures.

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC)

- Approach
- Architectural Reference Model for MTC

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC)
Approach

- Current mobile networks are optimized for human-to-human (H2H) traffic and not for M2M/MTC interactions; hence, optimizations for MTC are advantageous.
- For example, one needs lower costs to reflect lower MTC ARPUs (average revenue per user); also, there is a need to support triggering.
- Hence, 3GPP has started work on M2Mspecification in 2010 for interoperable solutions, particularly in the 3G/4G/LTE context.

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC) Approach

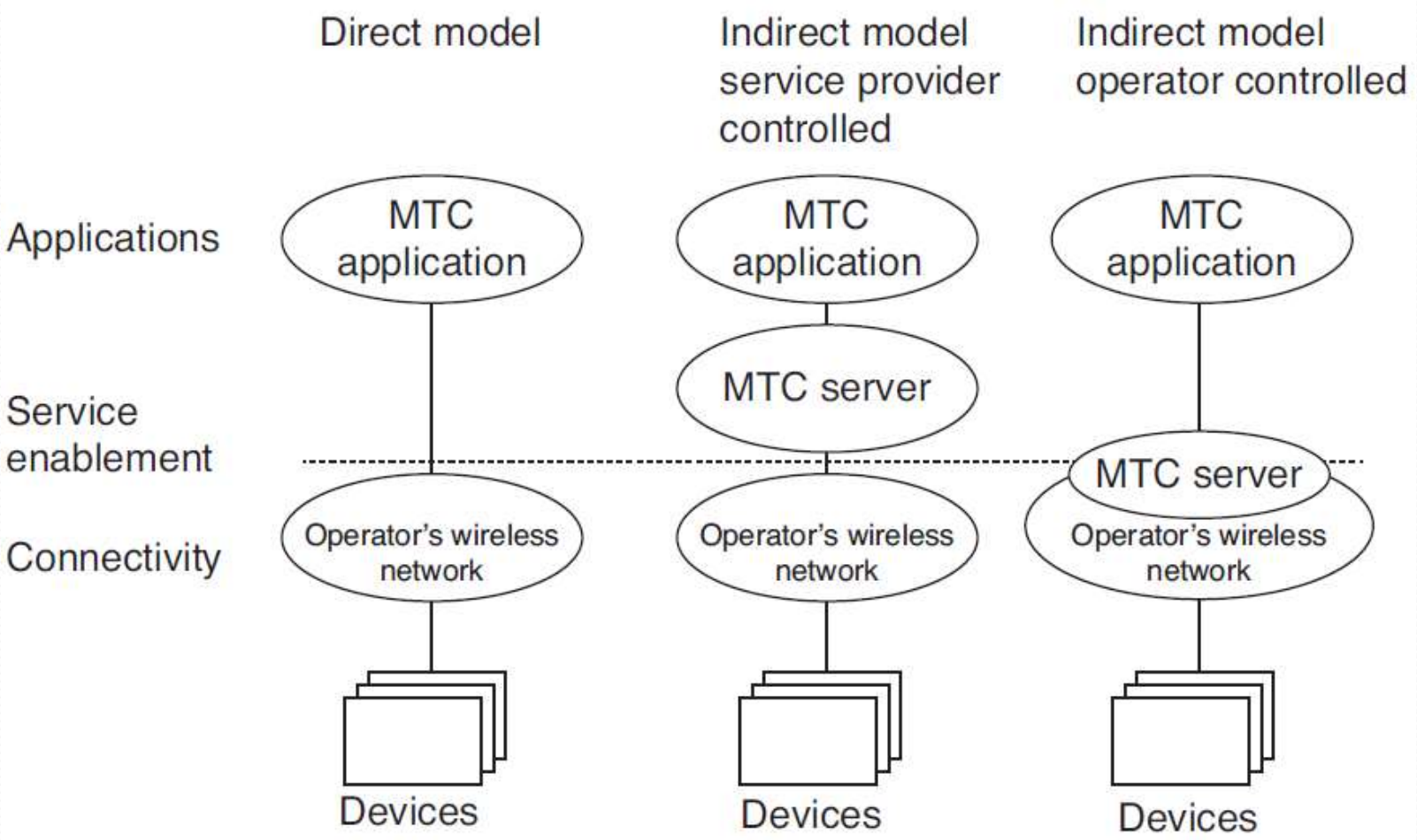
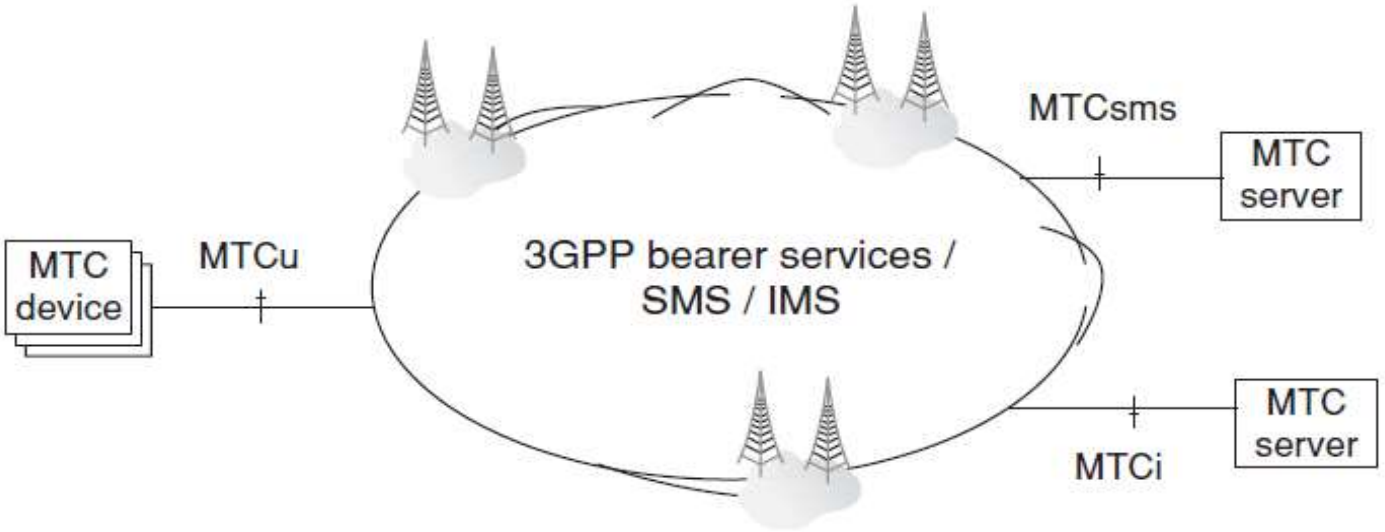


FIGURE 5.4 M2M in 3GPP—service models.

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC) Approach

- In architecture, the interfaces are as follows:
  - MTCu: provides MTC devices access to the 3GPP network for the transport of user traffic;
  - MTCi: the reference point for MTC server to connect the 3GPP network via 3GPP bearer service;
  - MTCsms: the reference point for MTC server to connect the 3GPP network via 3GPP SMS.



Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC) Approach

- The key document *3rd Generation Partnership Project Service Requirements for Machine Type Communications*—focused on
  - overload and congestion control,
  - extended access barring (EAB),
  - low priority access,
  - APN (access point name)-based congestion control,
  - downlink throttling.

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC)
Approach

- For MTC communication, the following communication scenarios are identified:
  - (i) MTC devices communicating with one or more MTC server;
  - (ii) MTC devices communicating with each other.

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC)
Approach

- For MTC devices communicating with one or more MTC servers, the following use cases exist:
  - (a) MTC server controlled by the network operator; namely the MTC server is located in the operator domain. Here
    - The network operator offers API (e.g., Open Systems Architecture [OSA]) on its MTC server(s)
    - MTC user accesses MTC server(s) of the network operator via API
  - (b) MTC server not controlled by the network operator; namely MTC server is located outside the operator domain. Here
    - The network operator offers the network connectivity to the MTC server(s) located outside of the network operator domain

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC)
Approach

- MTC applications do not all have the same characteristics.
- This implies that not every system optimization is suitable for every MTC application.
- Therefore, MTC features are to provide structure for the different system optimization possibilities that can be invoked.

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC) Approach

- The following MTC features have been defined:
  - Low mobility
  - Time controlled
  - Time tolerant
  - Packet switched (PS) only (here the MTC feature PS only is intended for use with MTC devices that only require packet switched services)
  - Small data transmissions
  - Mobile originated only
  - Infrequent mobile terminated
  - MTC monitoring
  - Priority alarm
  - Secure connection
  - Location-specific trigger
  - Network provided destination for uplink data
  - Infrequent transmission

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC)
Architectural Reference Model for MTC

- *3rd Generation Partnership Project Service Requirements for Machine Type Communications* focuses on numbers and addressing, on improvements of device triggering, and on interfaces between MTC server and mobile network.
- Referring to Figure in next slide,

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC) Architectural Reference Model for MTC

MTC-IWF is a new interworking function between (external) MTC server and operator core network handling security, authorization, authentication, and charging.

MTCsp is a new control interface for interactions with MTC server

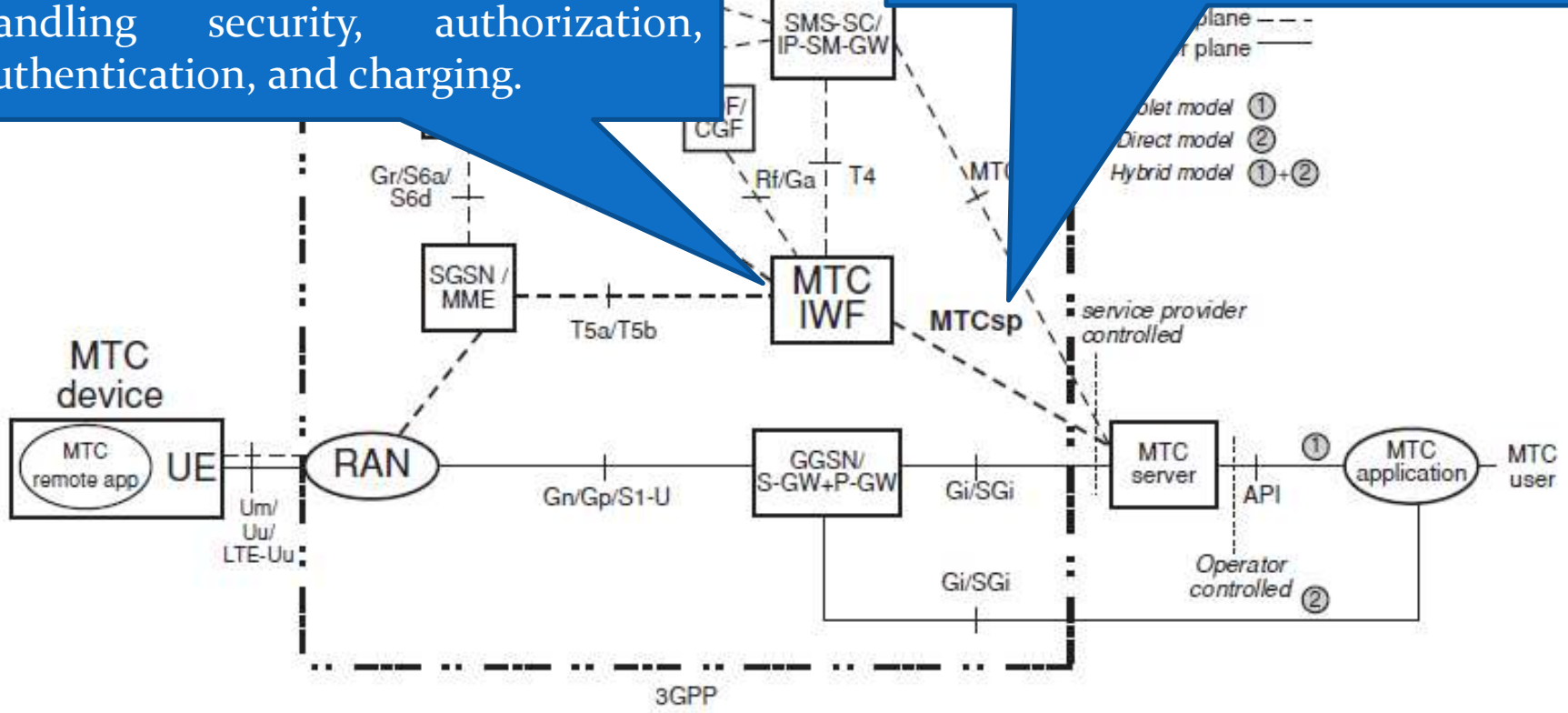


FIGURE 5.5 M2M in 3GPP—Architecture.

https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-015-0479-y/tables/4

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC)
Architectural Reference Model for MTC

- The end-to-end application, between the user equipment (UE) used for MTC and the MTC application, uses services provided by the 3GPP system, and optionally services provided by an MTC server.
- The 3GPP system provides transport and communication services (including 3GPP bearer services, IMS, and SMS) including various optimizations that can facilitate MTC.
- UE used for MTC connecting to the 3GPP network (UTRAN, E-UTRAN, GERAN, I-WLAN, and so on) via the Um/Uu/LTE-Uu interface.

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC)
Architectural Reference Model for MTC

- The architecture encompasses a number of models as follows:
  - Direct model —direct communication provided by the 3GPP operator: The MTC application connects directly to the operator network without the use of any MTC server;
  - Indirect model —MTC service provider controlled communication: The MTC server is an entity outside of the operator domain. The MTCsp and MTCsms are external interfaces (i.e., to a third-party M2M service provider);
  - Indirect model—3GPP operator controlled communication: The MTC server is an entity inside the operator domain. The MTCsp and MTCsms are internal to the public land mobile network (PLMN);
  - Hybrid model: The direct and indirect models are used simultaneously in the hybrid model, for example, connecting the user plane using the direct model and doing control plane signalling using the indirect model.

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC)
Architectural Reference Model for MTC

- In several countries, regulators have indicated that there are not enough (mobile) numbers available for M2M applications.
- 3GPP postulates that solutions will have to support 100× more M2M devices than devices for H2H communications.
- Proposed solutions include:
  - (i) mid-term solution: special M2M number ranges with longer telephone numbers (e.g., 14 digits);
  - (ii) long-term solution: no longer provide telephone numbers for M2M applications.

Third Generation Partnership Project Service Requirements for Machine Type Communications (MTC) Architectural Reference Model for MTC

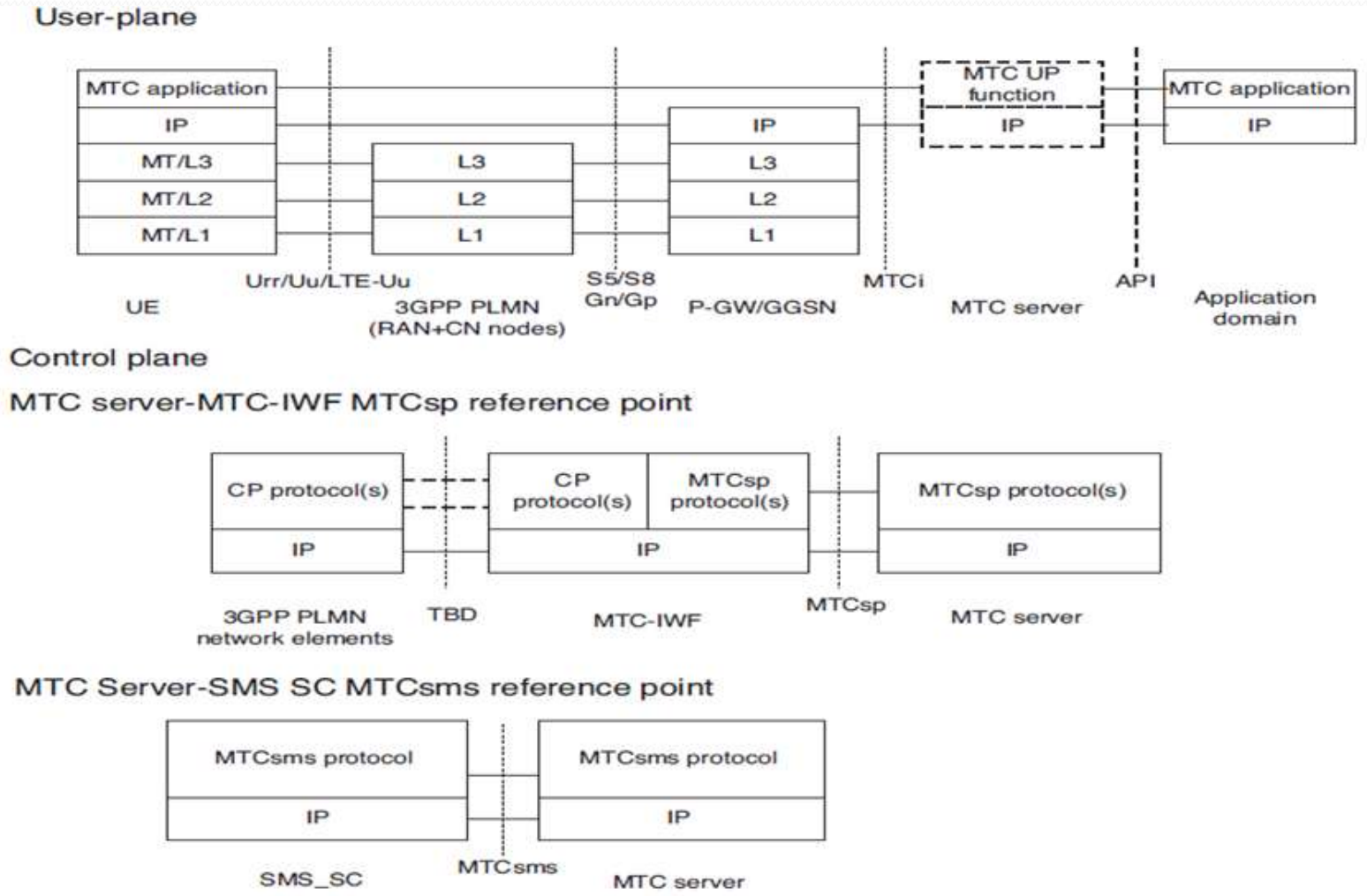


FIGURE 5.6 User and control plane stack for MTC architecture

CENELEC

- European Committee for Electrotechnical Standardization (CENELEC)
  - has adopted the transport profile of Siemens' distribution line carrier communication protocol (CX1) as a standardization proposal.
- The standard aims at supporting open and fault tolerant communication via powerline in intelligent power supply grids.
- As the basis for the transmission protocol, which uses the low voltage network as a communication channel for data of grid sensors and smart meters, the transport profile has been designed to ensure interoperability in accordance with EU Mandate M/441.

CENELEC

- CENELEC TC 13 was planning to forward the CX1 transport profile to TC 57 of the International Electrotechnical Commission (IEC).
- CX1 is already used to connect meters and other intelligent terminal devices in Siemens' SG metering systems, such as in the load switching devices that will replace household ripple control receivers.
- The systems collect energy consumption data and network information, which are then relayed to a control center for further processing.
- The communication protocol can handle any change in the physical communication parameters of a low voltage power supply grid, such as signal attenuation, noise, network disruption and signal coupling, as well as operational changes in network configuration.
- The protocol can also be integrated into existing IEC protocol-based network automation and energy management infrastructures.

6LoWPAN

IETF IPv6 OVER LOWPOWER WPAN (6LoWPAN)

•6LoWPAN is an IPv6 adaption layer for low power wireless PAN (LoWPAN).

•A link in a LoWPAN is characterized as lossy, low power, low bit-rate, short range, with many nodes saving energy with long sleep periods.

•6LoWPAN provides a means of carrying packet data in the form of IPv6 over IEEE 802.15.4 and other networks

•A LoWPAN is potentially composed of a large number of overlapping radio ranges works on 2.4 GHz

•It uses AES-128 link layer security for authentication and encryption and TLS

6LoWPAN

IETF IPv6 OVER LOWPOWER WPAN (6LoWPAN)

•6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks), is a low power wireless mesh network where every node has its own IPv6 address.

•This allows the node to connect directly with the Internet using open standards.

•It works great with open IP standard including TCP, UDP, HTTP, COAP, MATT and web-sockets.

•It offers end-to-end IP addressable nodes.

•There's no need for a gateway, only a router which can connect the 6LoWPAN network to IP.

•In a 6LowPAN network, leaf nodes can sleep for a long duration of time.

6LoWPAN

6LoWPAN Application Areas

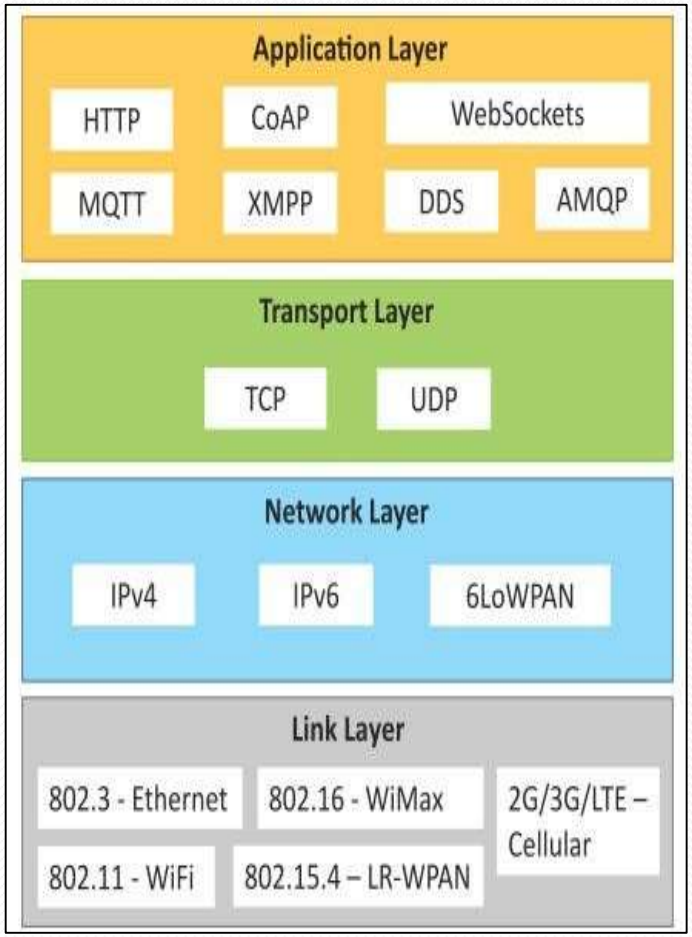
•Automation: There are enormous opportunities for 6LoWPAN to be used in many different areas of automation.

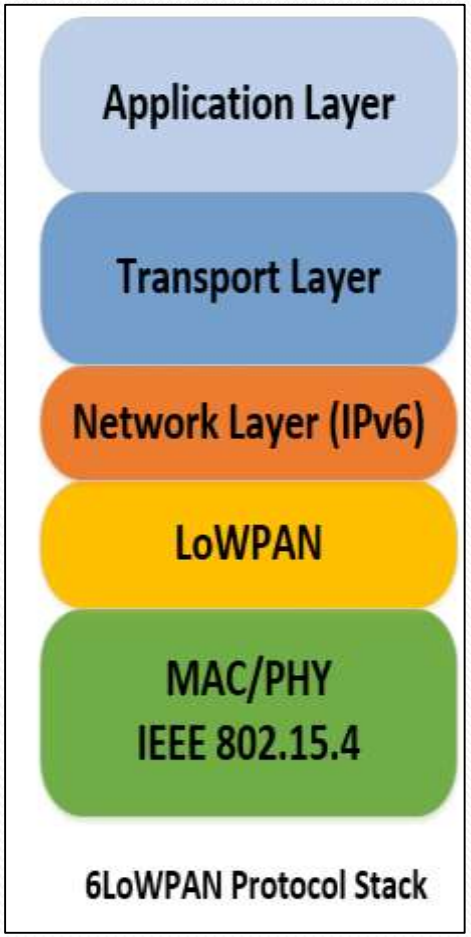
•Industrial monitoring: Industrial plants and automated factories provide a great opportunity for 6LoWPAN. Major savings can be made by using automation in every day practices. Additionally, 6LoWPAN can connect to the cloud which opens up many different areas for data monitoring and analysis.

•Smart Grid: Smart grids enable smart meters and other devices to build a micro mesh network. They are able to send data back to the grid operator's monitoring and billing system using the IPv6.

•Smart Home: By connecting your home IoT devices using IPv6, it is possible to gain distinct advantages over other IoT systems.

6LoWPAN-Protocol Stack





Conti….

- A LoWPAN is potentially composed of a large number of overlapping radio ranges. Although a given radio range has broadcast capabilities, the aggregation of these is a complex non-broadcast multiaccess (NBMA) structure with generally no LoWPAN-wide multicast capabilities.
- Link-local scope is in reality defined by reachability and radio strength.
- A LoWPAN to be made up of links with undetermined connectivity properties, along with the corresponding address model assumptions defined there in.

IP IN SMART OBJECTS (IPSO)

The IPSO Alliance is an advocate for IP-networked devices for use in energy, consumer, healthcare, and industrial applications.

The IPSO Alliance is a non-profit association of more than 60 members from leading technology, communications, and energy companies around the world.

The mission is to provide a foundation for industry growth through building stronger relationships, fostering awareness, providing education, promoting the industry, generating research, and creating a better understanding of IP and its role in connecting smart objects

IP IN SMART OBJECTS (IPSO)

GOALS

•Promote IP as the premier solution for access and communication for smart objects.

•Promote the use of IP in smart objects by developing and publishing white papers and case studies and providing updates on standards progress from associations like IETF, among others, and through other supporting marketing activities.

•Understand the industries and markets where smart objects can have an effective role in growth when connected using the Internet protocol.

•Organize interoperability tests that will allow members and interested parties to show that products and services using IP for smart objects can work together and meet industry standards for communication.

•Support IETF and other standards development organizations in the development of standards for IP for smart objects.

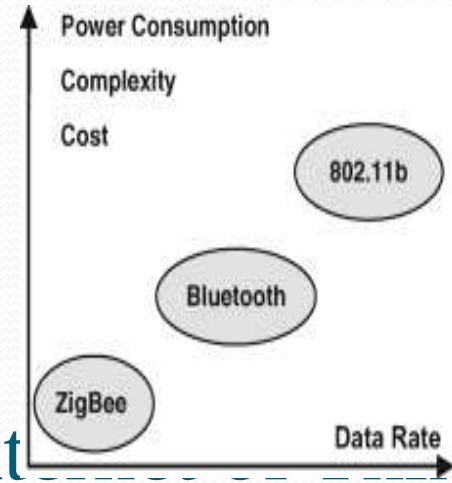
ZigBee

ZigBee
ZigBee is similar to Bluetooth and is majorly used in industrial settings.

It has some significant advantages in complex systems offering low-power operation, high security, robustness suitable for sensor networks in IoT applications.

The latest version of ZigBee is the recently launched 3.0, which is essentially the unification of the various ZigBee wireless standards into a single standard.

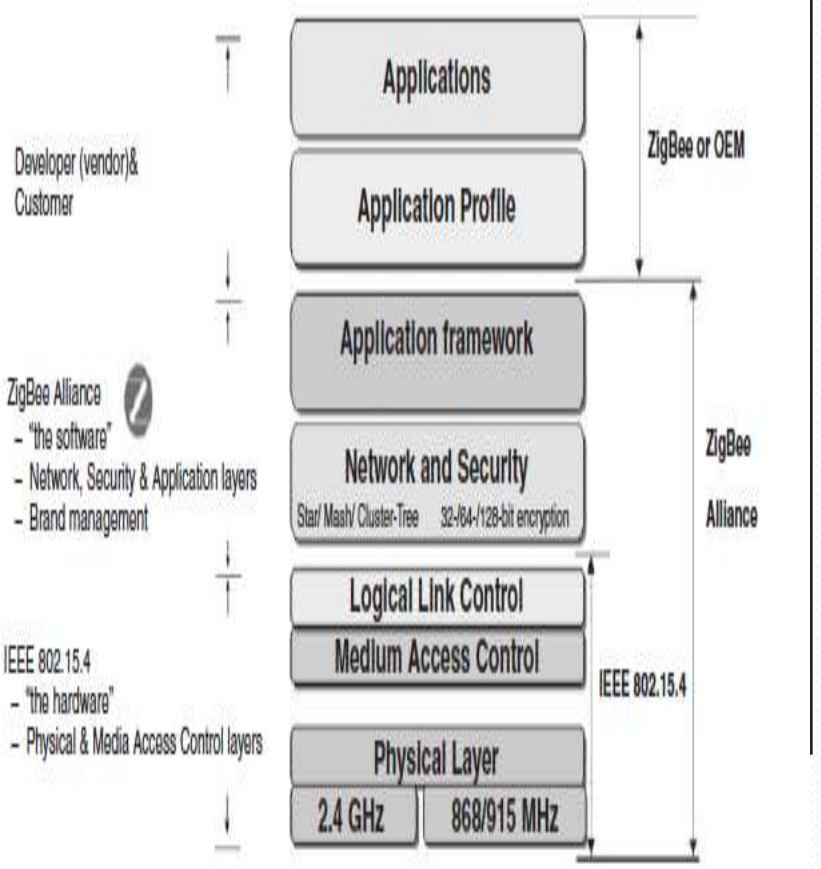
Standard- Zigbee 3.0 based on IEEE802.15.4
Frequencies- 2.4 Ghz
Range- Approx. 10-100m
Data Rates – 250 kbps



	Data Rate	Typical Range	Application Examples
ZigBee	20 to 250 Kbps	10–100 m	Wireless Sensor Networks
Bluetooth	1 to 3 Mbps	2–10 m	Wireless Headset Wireless Mouse
IEEE 802.11b	1 to 11 Mbps	30–100 m	Wireless Internet Connection

ZigBee

- ZigBee utilizes the globally available, license-free 2.4 GHz industrial, scientific, and medical (ISM) frequency band to provide low data rate wireless applications
- ZigBee networks support star, mesh, and cluster-tree topologies. These capabilities enable a network to have over 65,000 devices on a single wireless network.
- ZigBee offers low-latency communication
- ZigBee can create robust self-forming, self-healing wireless mesh network.
- The ZigBee mesh network connects sensors and controllers without being restricted by distance or range limitations
- It allows participating devices to communicate with one another and act as repeaters transferring data between devices



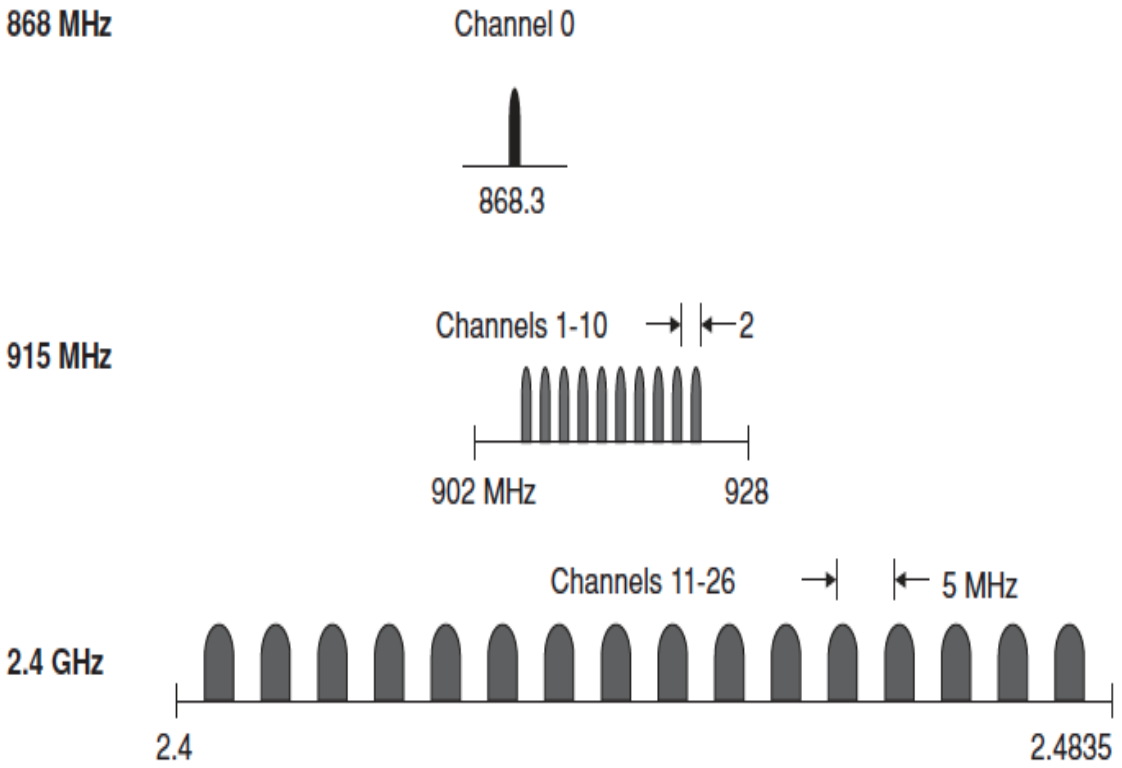
ZigBee

- ZigBee is available as two feature sets, ZigBee PRO and ZigBee.
- ZigBee PRO, the most widely used specification, is optimized for low-power consumption and to support large networks with thousands of devices
- ZigBee PRO adds some new application profiles such as automatic meter reading, commercial building automation, and home automation.
- ZigBee PRO networks have the ability to aggregate routes through the use of “many-to-one” routing
- The ZigBee 802.15.4 spec defines a maximum packet size of 128 octets; this packet size is optimal for short control messages.
- The ZigBee Alliance is a global ecosystem of 400+ companies in the M2M/IoT space developing standards and producing products for use in commercial building automation, consumer electronics, health care and fitness, home automation, energy management, retail management, and wireless telecommunications.

ZigBee

- The PHY layer of the reference model specifies the network interface components, their parameters, and their operation.
- To support the operation of the MAC layer, the PHYlayer includes a variety of features, such as receiver energy detection (RED), link quality indicator (LQI), and clear channel assessment (CCA).
- The MAC layer handles network association and disassociation. It also regulates access to the medium;
- The network layer provides the functionality required to support network routing capabilities, configuration and device discovery, association and disassociation, topology management, MAC layer management, and routing and security management. Three network topologies, namely star, mesh, and cluster tree, are supported.
- The application layer consists of the application support sublayer (APS), the ZigBee device object (ZDO), and the manufacturer-defined application objects. The responsibilitiesof the APS sublayer include maintaining tables for binding devices together,based on their services and their needs, and forwarding messages between bound devices

ZigBee



	COVERAGE	DATA RATE	CHANNELS
868 MHz	Europe	20 Kbps	1
915 MHz	Americas	40 Kbps	10
2.4 GHz ISM	Worldwide	250 Kbps	16

ZigBee

The design of the PHY layer is driven by the need for low-cost, power-effective PHY layer for cost sensitive, low data rate monitoring and control applications. Under IEEE 802.15.4, wireless links can operate in three unlicensed frequency bands.

- Direct sequence spread spectrum (DSSS) using binary phase shift keying (BPSK), operating in the 868 MHz at a data rate of 20 Kbps;
- DSSS using BPSK, operating in the 915 MHz at a data rate of 40 Kbps; and
- DSSS using offset quadrature phase shift keying (O-QPSK), operating in the 2.4 GHz at a data rate of 140 Kbps.

IEEE 802.15.4 defines four types of frames: beacon frames, MAC command frames, acknowledgement frames, and data frames

ZigBee

- Network and MAC layer consist of physical devices, namely a full function device (FFD) and a reduced function device (RFD).

- There are three categories of logical devices:
- Network coordinator : An FFD device responsible for network establishment and control.

- Router : An FFD device that supports the data routing functionality, including acting as an intermediate device to link different components of the network and forwarding message between remote devices across multihop paths.

- End Devices : An RFD device that contains (just) enough functionality to communicate with its parent node, namely the network coordinator or a router. An end device does not have the capability to relay data messages to other end devices.

- A PAN coordinator is the designated principal controller of the WPAN. Every network has exactly one PAN coordinator.

ZigBee

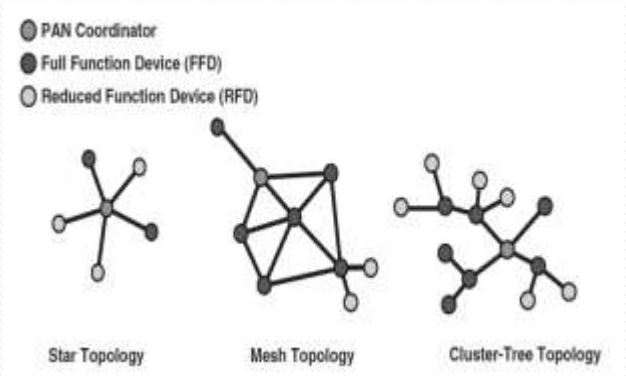
Based on these logical device types, a ZigBee WPAN can be organized into one of three possible topologies, namely a star, a mesh (peer-to-peer), or a cluster tree.

The star network topology supports a single coordinator, with up to 65,536 devices. In this topology configuration, one of the FFD-type devices assumes the role of network coordinator. All other devices act as end devices.

The mesh configuration allows path formation from any source device to any destination device,
using tree- and table-driven routing algorithms.

Cluster-tree networks enable a peer– peer network to be formed with a minimum of routing overhead, using multihop routing.

The cluster can be rather large, comprising up to 255 clusters of up to 254 nodes each, for a total of 64,770 nodes



ZigBee

Application Standards

- ZigBee Building Automation
- ZigBee Health Care
- ZigBee Home Automation
- ZigBee Input Device
- ZigBee Light Link
- ZigBee network devices (assist and expand ZigBee networks)
- ZigBee Remote Control (used for advanced RCs)
- ZigBee Retail Services (used for smarter shopping)
- ZigBee Smart Energy (SE) (used for home energy savings)
- ZigBee Telecom Services (used for value-added services)

Radio Frequency for Consumer Electronics (RF4CE)

- Radio Frequency for Consumer Electronics (RF4CE) is a protocol developed by a consortium that includes companies such as Freescale, Texas Instruments, OKI, Panasonic, Philips, Samsung, and Sony.
- It defines a standard specification for designing remote-control devices for the TV, VCR, and DVD.
- The RF4CE consortium merged with ZigBee to produce the ZigBee RF4CE standard. Whereas most remote controls currently are based on infrared (IR) technology that requires line of sight, RF4CE does not have that limitation.

Radio Frequency for Consumer Electronics (RF4CE)

- RF4CE protocol has been designed for simple, two-way device-to-device control applications that do not require the full-featured mesh networking capabilities offered by ZigBee 2007.

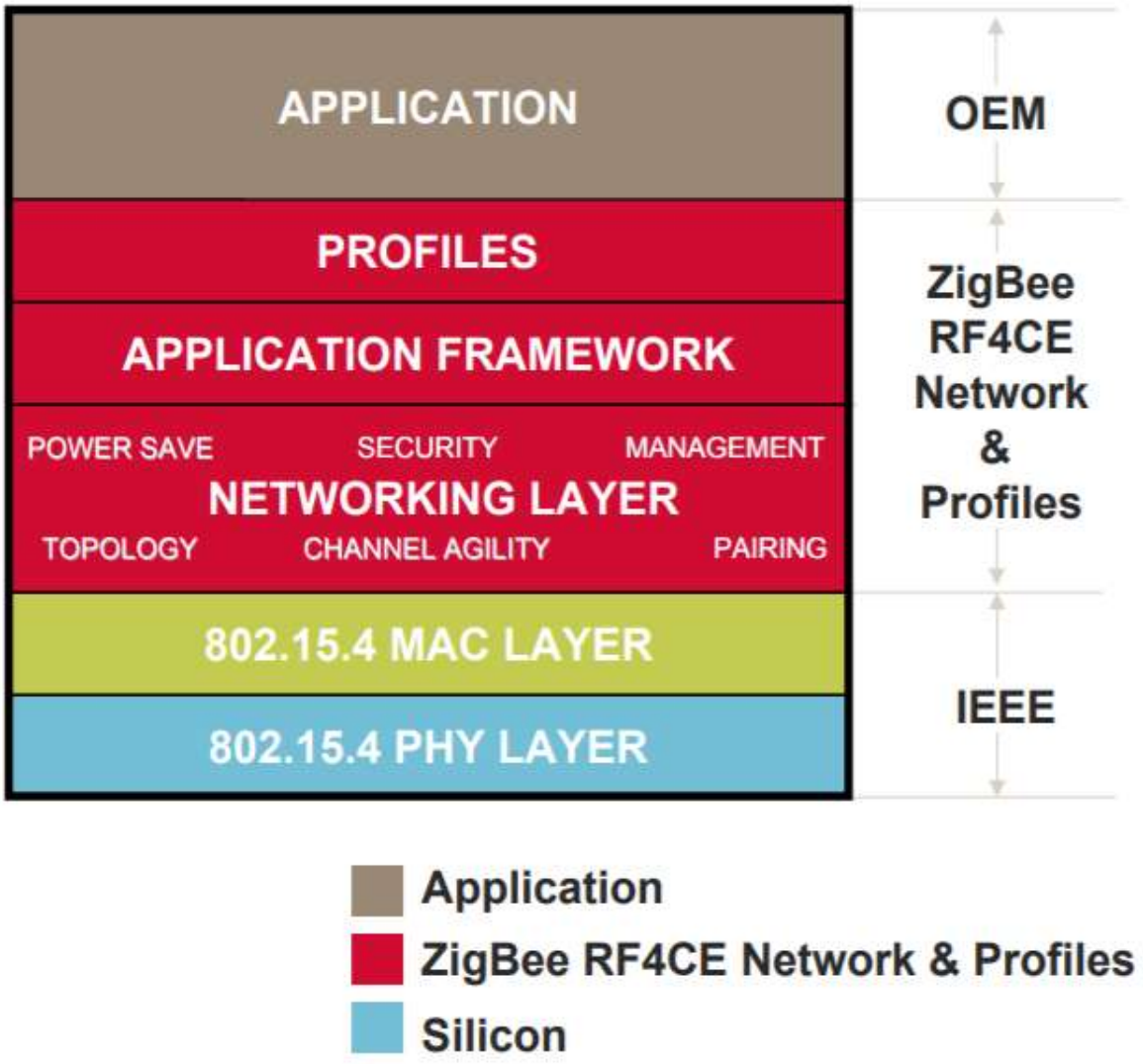
- ZigBee RF4CE offers lower memory size requirements, thereby enabling lower cost implementations

- RF4CE is based on ZigBee and was standardized in 2009 by four consumer electronics (CE) companies:
  - Sony,
  - Philips,
  - Panasonic, and
  - Samsung.

Radio Frequency for Consumer Electronics (RF4CE)

- The ZigBee RF4CE specification defines an RC network that defines a simple, robust, and low-cost communication network allowing wireless connectivity in applications for CE devices.
- The ZigBee RF4CE specification enhances the IEEE 802.15.4 standard by providing a simple networking layer and standard application layer that can be used to create a multivendor interoperable solution for use within the home.
- RF4CE's intended use is as a device RC system, for example for television settop boxes.
- The intention is that it overcomes the common problems associated with infrared (IR): interoperability, line-of-sight (LOS), and limited enhanced features.
- At least two-chip vendors supported RF4CE as of press time: Texas Instruments and Freescale Semiconductor, Inc.

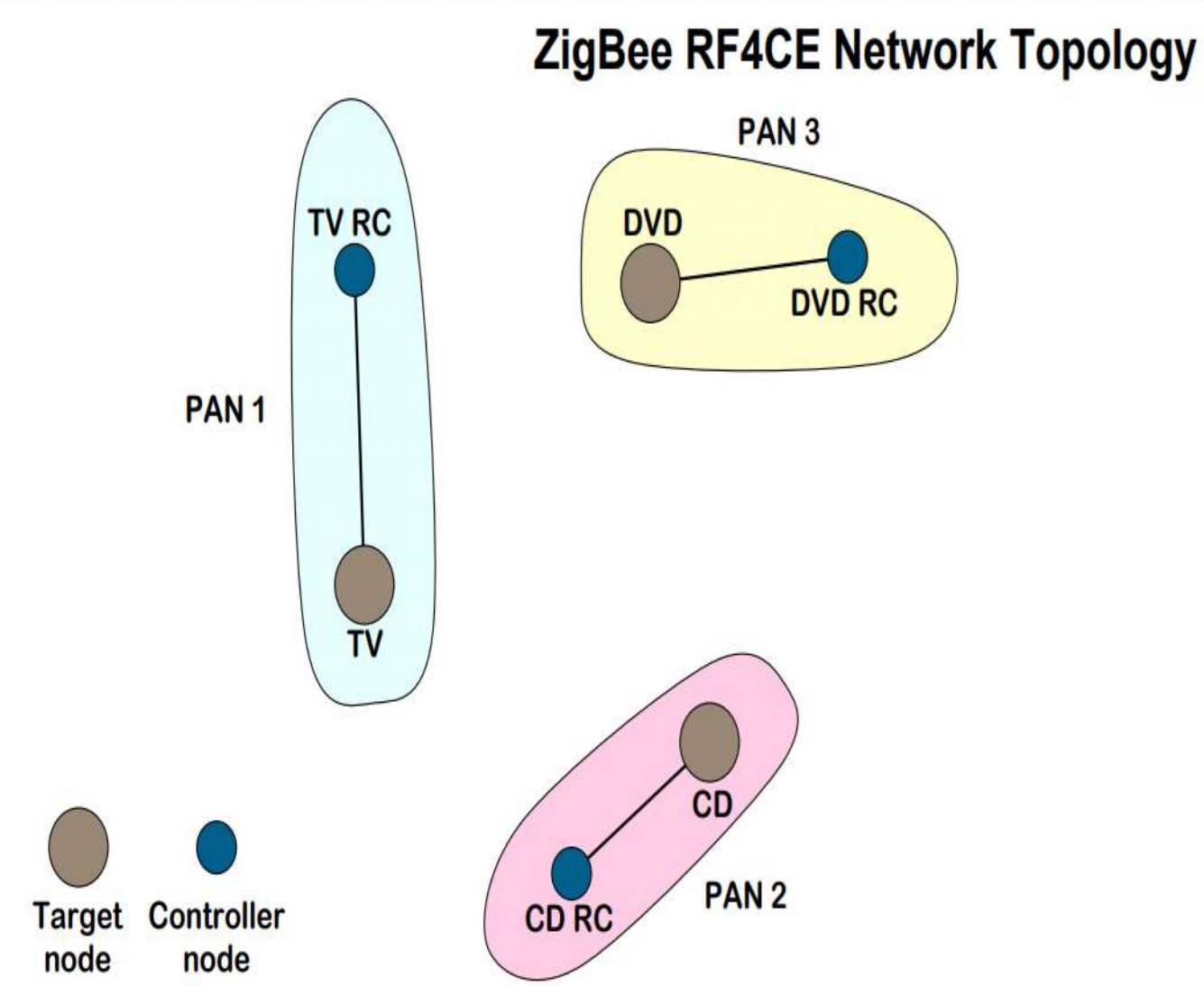
Architecture



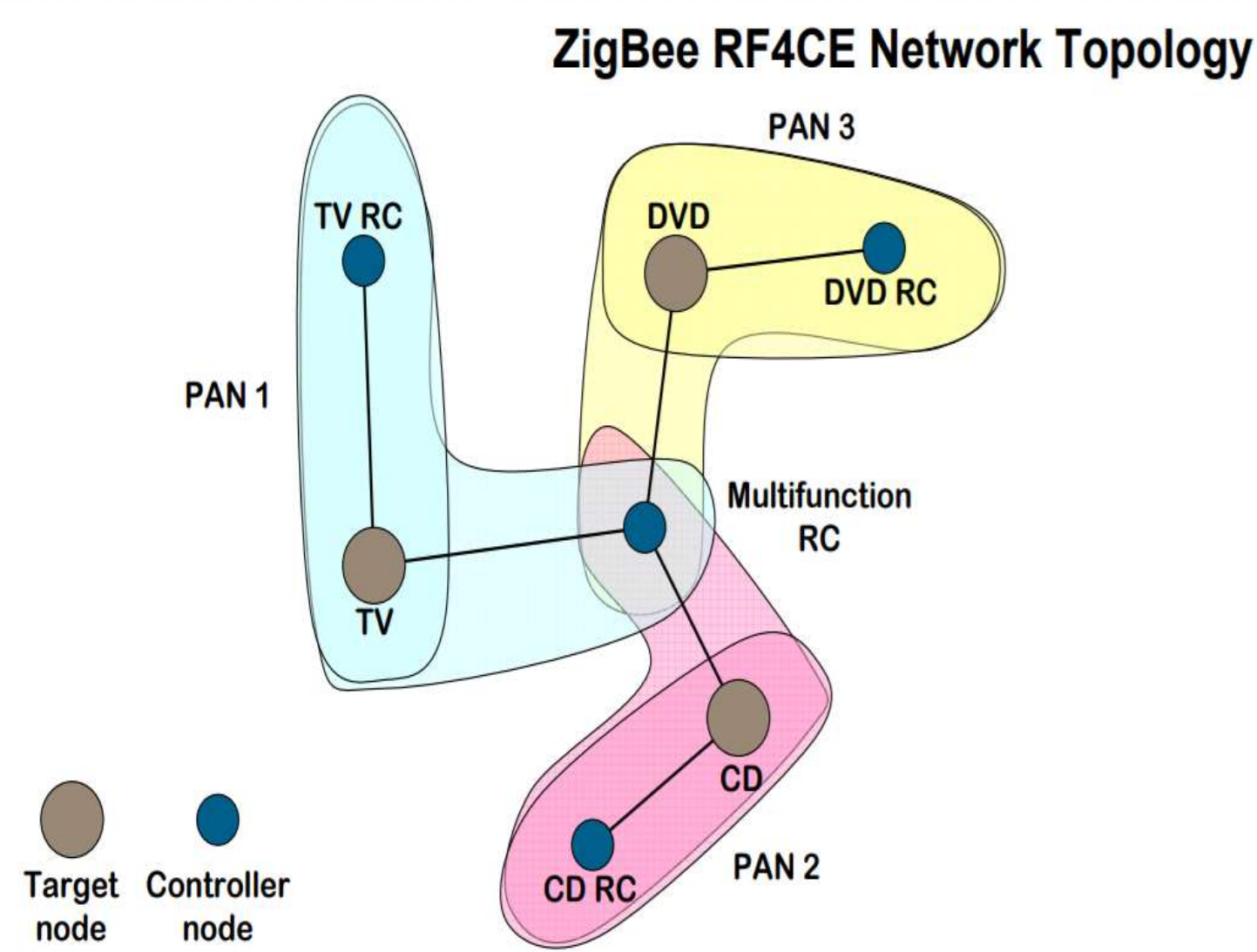
Architecture

- The ZigBee RF4CE specification is designed to be built on top of the IEEE 802.15.4 standard MAC and PHY layers. It provides networking functionality,
- while the ZigBee Remote Control and/or ZigBee Input Device can interface to the end-user application.
- Manufacturer specific extensions to standards can be defined by sending vendor-specific data frames within the standard.
- In addition, manufacturer specific profiles can also be defined.

Network Topology



Network Topology



Radio Frequency for Consumer Electronics (RF4CE)

Characteristics of ZigBee RF4CE include the following

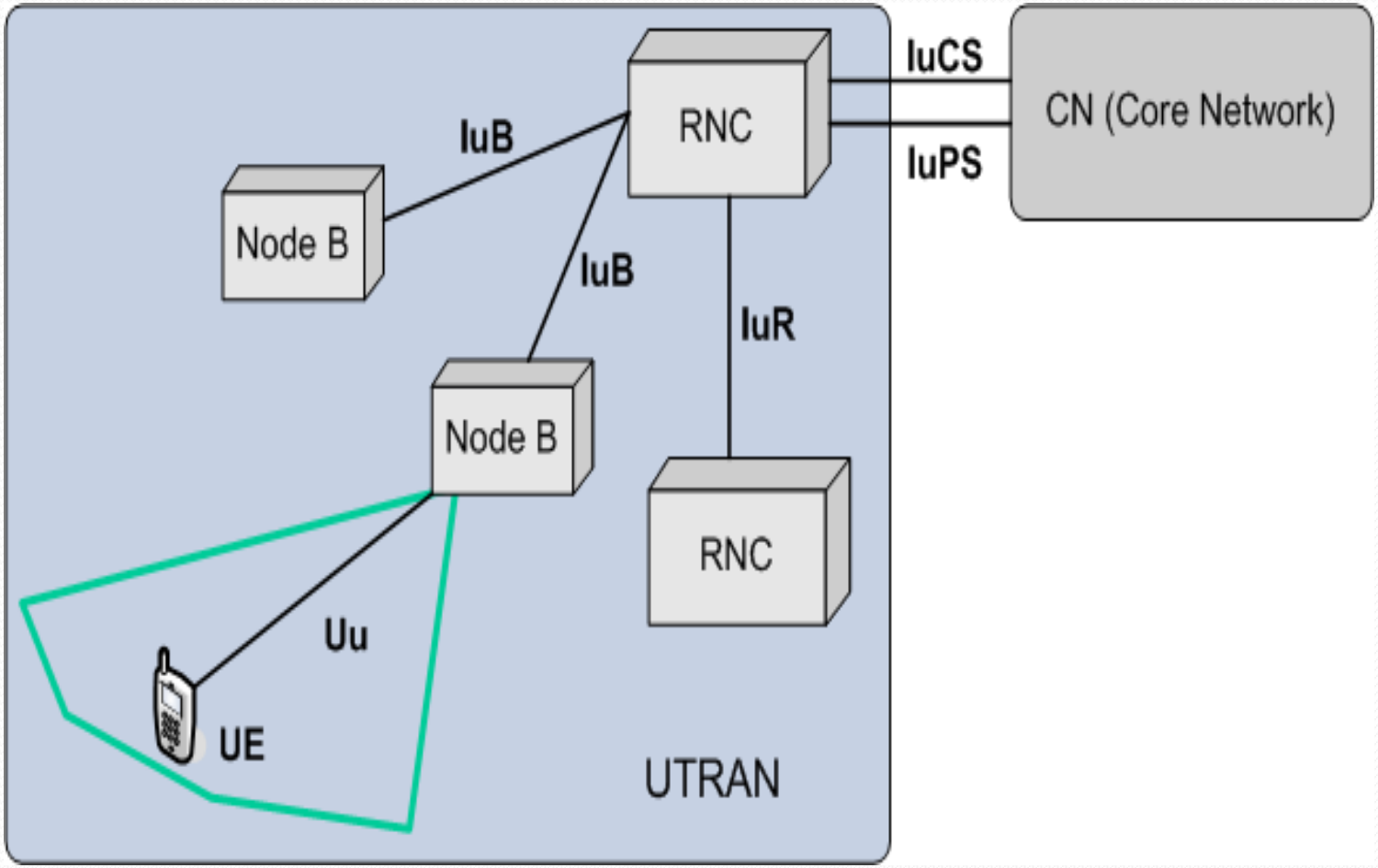
- Operation in the 2.4 GHz frequency band according to IEEE 802.15.4;
- Frequency agile solution operating over three channels;
- Incorporates power-saving mechanisms for all device classes;
- Discovery mechanism with full application confirmation;
- Pairing mechanism with full application confirmation;
- Multiple star topology with inter-PAN communication;
- Various transmission options including broadcast;
- Security key generation mechanism;
- Utilizes the industry standard AES-128 security scheme;
- Specifies a simple RC control profile for CE products;
- Support alliance-developed standards or manufacturer-specific profiles.

Cellular and Mobile Network Technologies for IoT/M2M

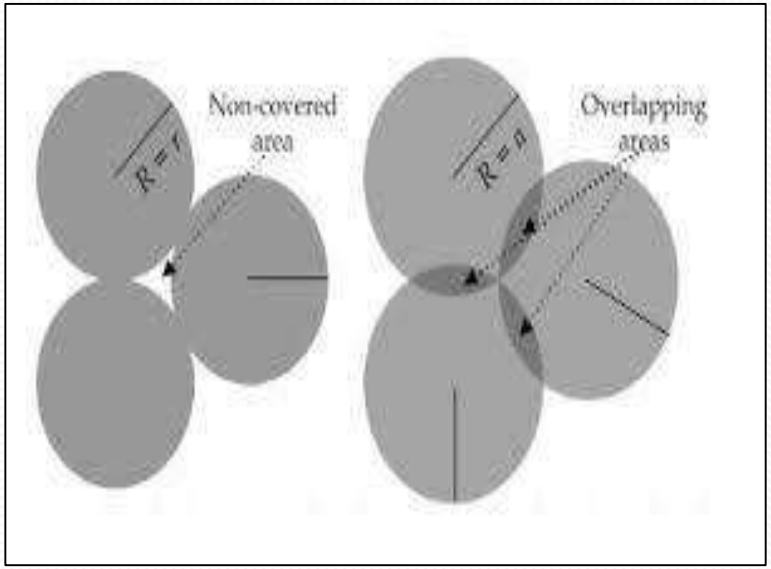
Universal Mobile Telecommunications System (UMTS)

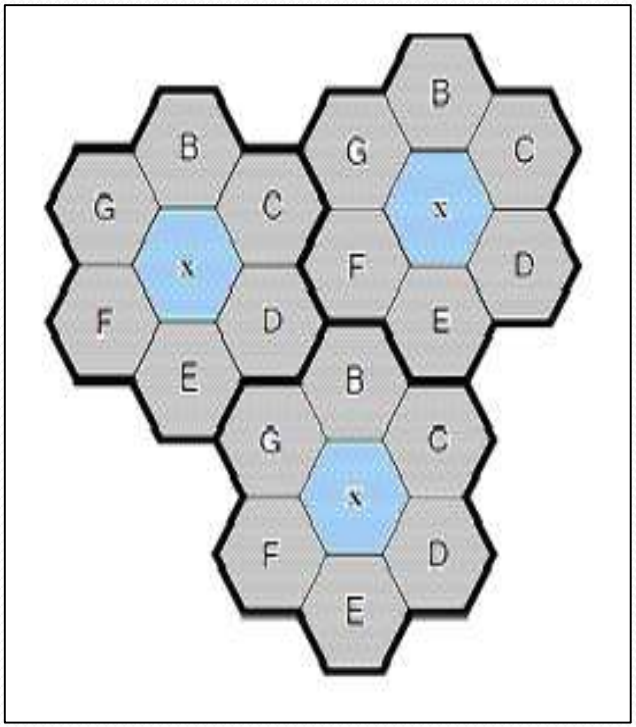
- UMTS is a 3G mobile cellular technology for networks supporting voice and data (IP) based on the GSM standard developed by the 3GPP (Third-Generation Partnership Project).
- UMTS is a component of the ITU IMT-2000 standard set and is functionally comparable with the CDMA2000 standard set for networks based on the competing cdmaOne technology.
- UMTS can carry many traffic types from real-time circuit switched to IP-based packet switched.
- Universal terrestrial radio access network (UTRAN) is a collective term for the NodeBs (base stations) and radio network controllers (RNC) that comprise the UMTS RAN.
- NodeB is the equivalent to the base transceiver station (BTS) concept used in GSM. The UTRAN allows connectivity between the UE and the CN

Cellular and Mobile Network Technologies for IoT/M2M

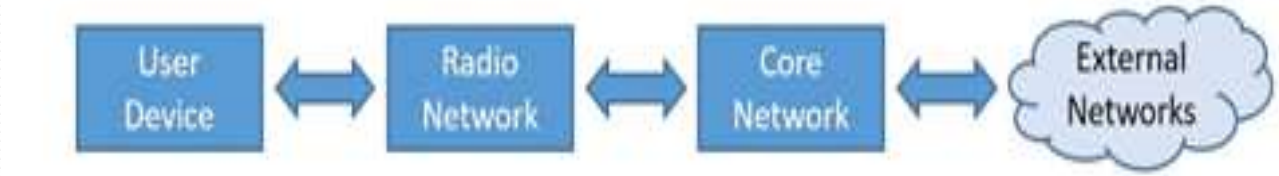


ACCESS POINT COVERAGE AREA



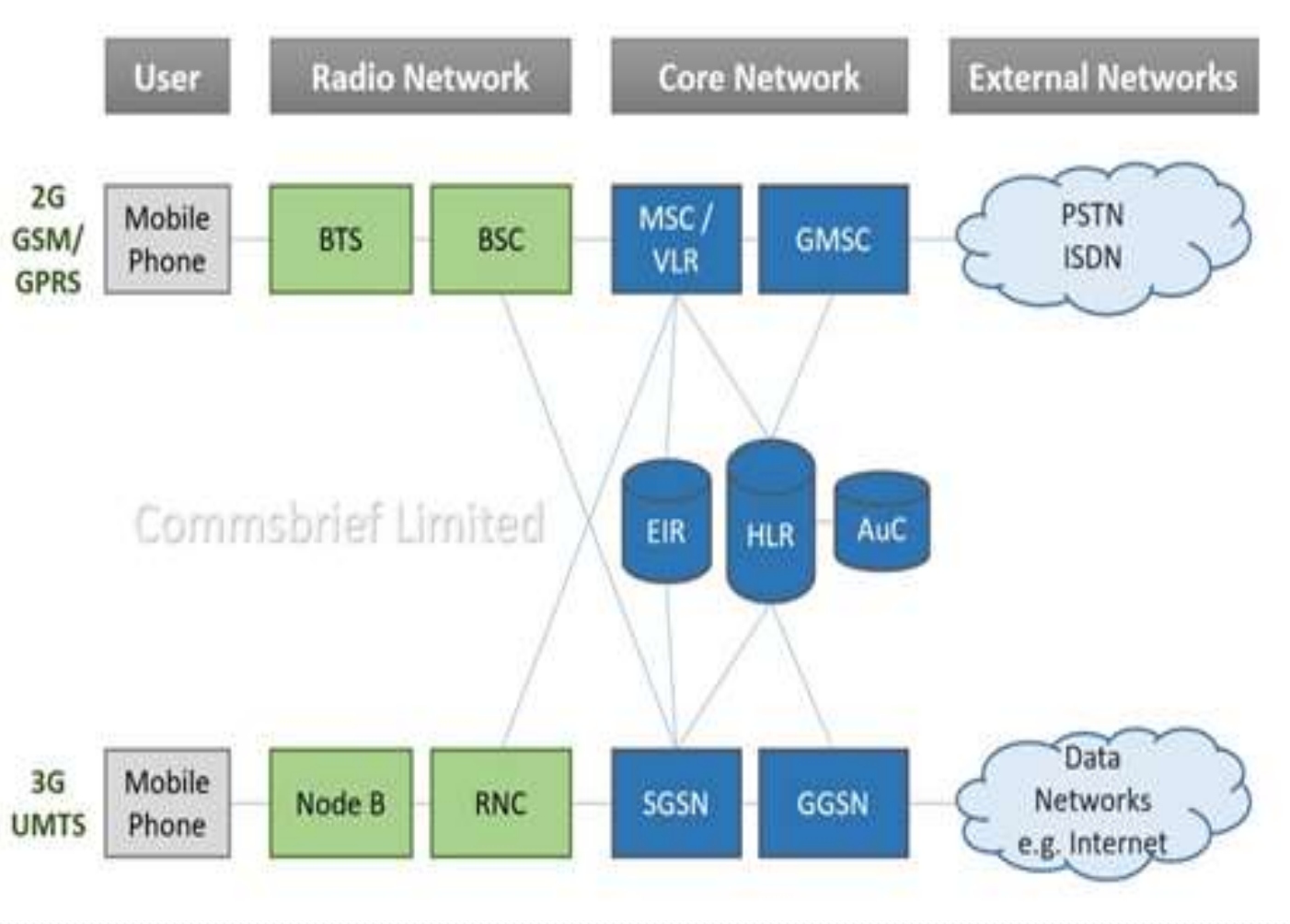


Cellular and Mobile Network Technologies for IoT/M2M

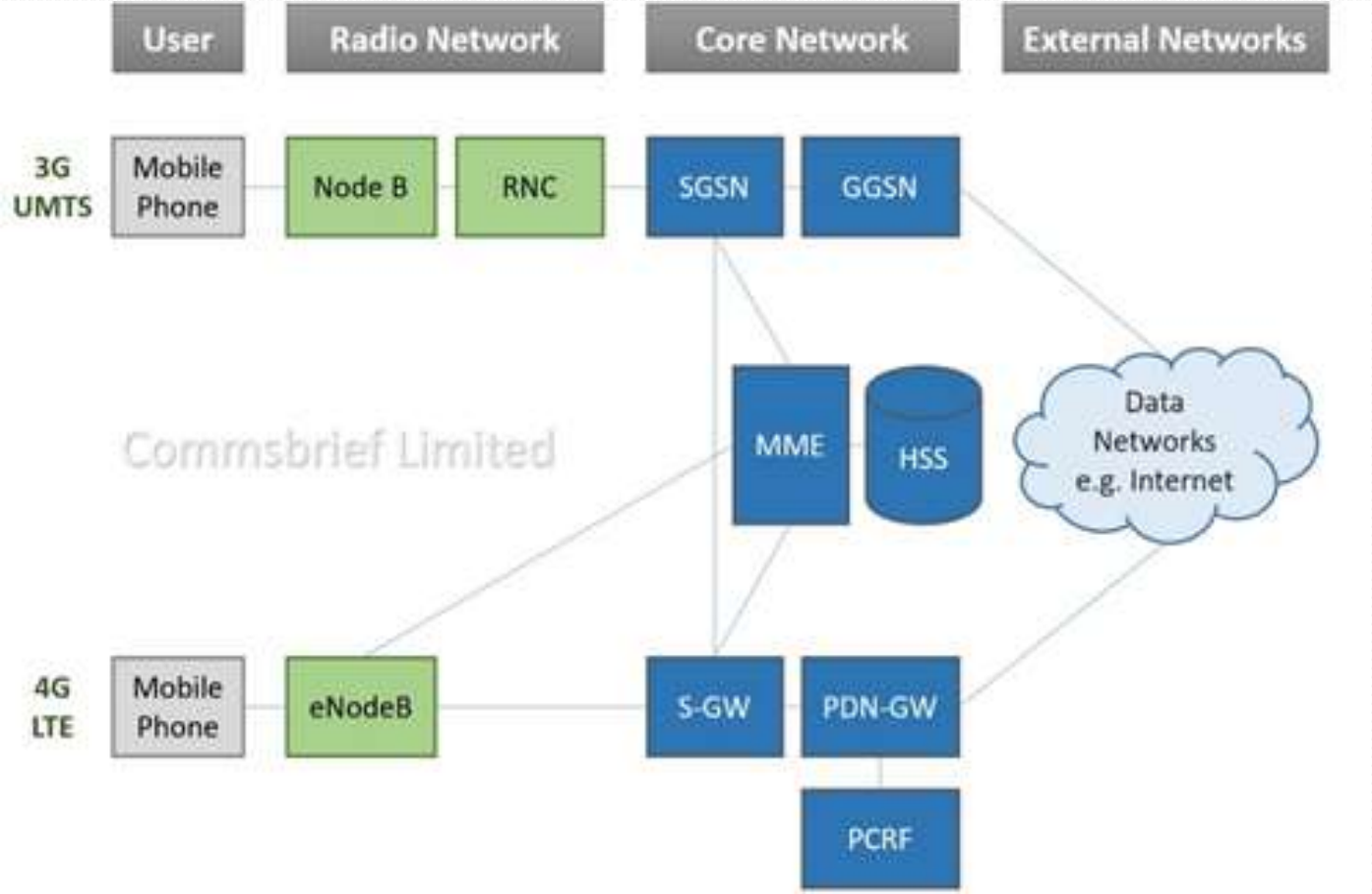


User Device	Radio Network	Core Network	External Networks
• Smartphones • Feature phones • Other SIM enabled devices	• BTS / Node B / eNodeB • BSC / RNC	• MSC / SGSN / S-GW • MME / VLR • HSS / HLR • GMSC / GGSN / PDN-GW	• PSTN • PLMN • Internet • Other

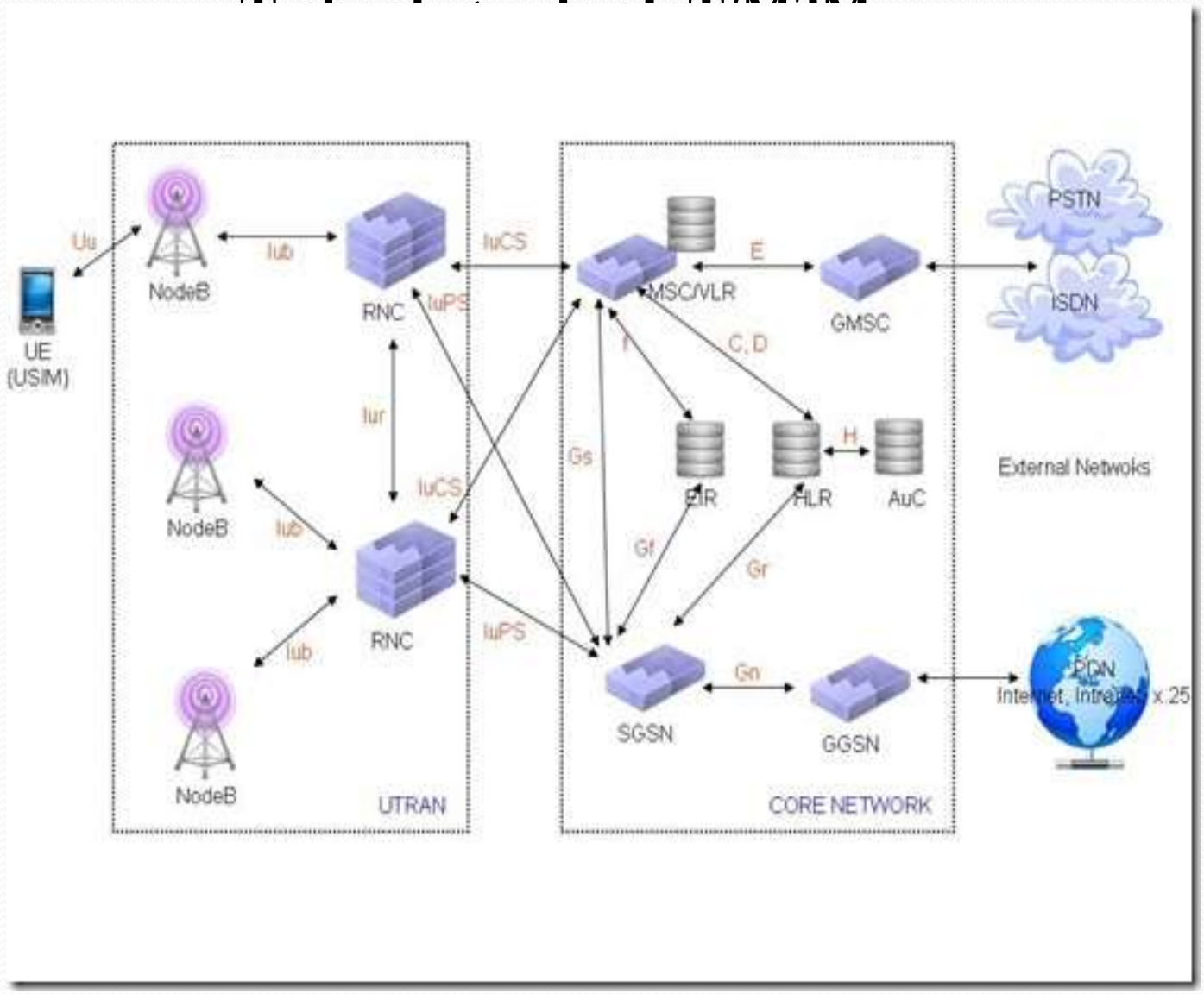
Cellular and Mobile Network Technologies for IoT/M2M



Cellular and Mobile Network Technologies for IoT/M2M



Cellular and Mobile Network



Cellular and Mobile Network Technologies for IoT/M2M

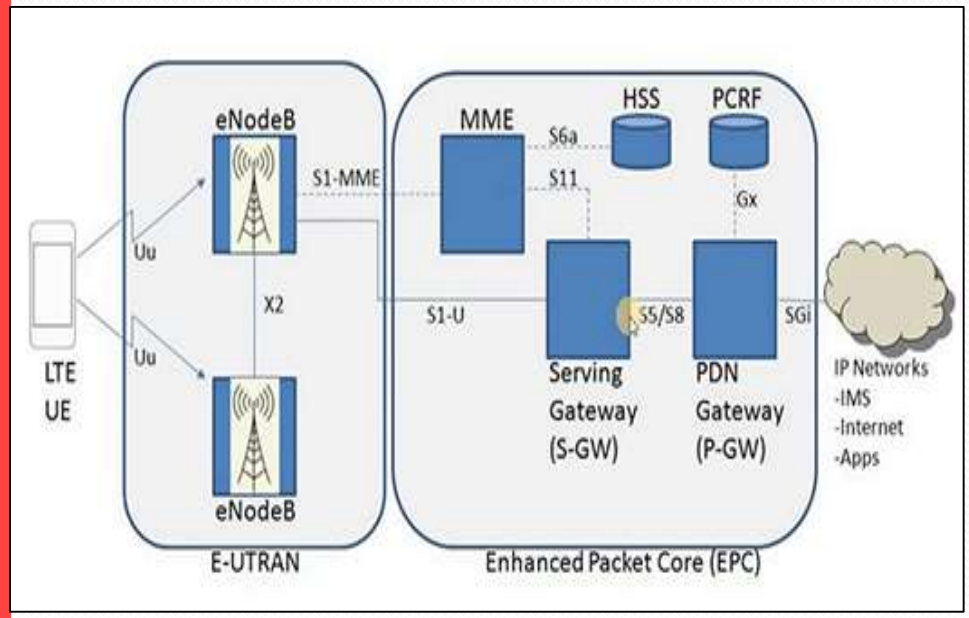
Long Term Evolution

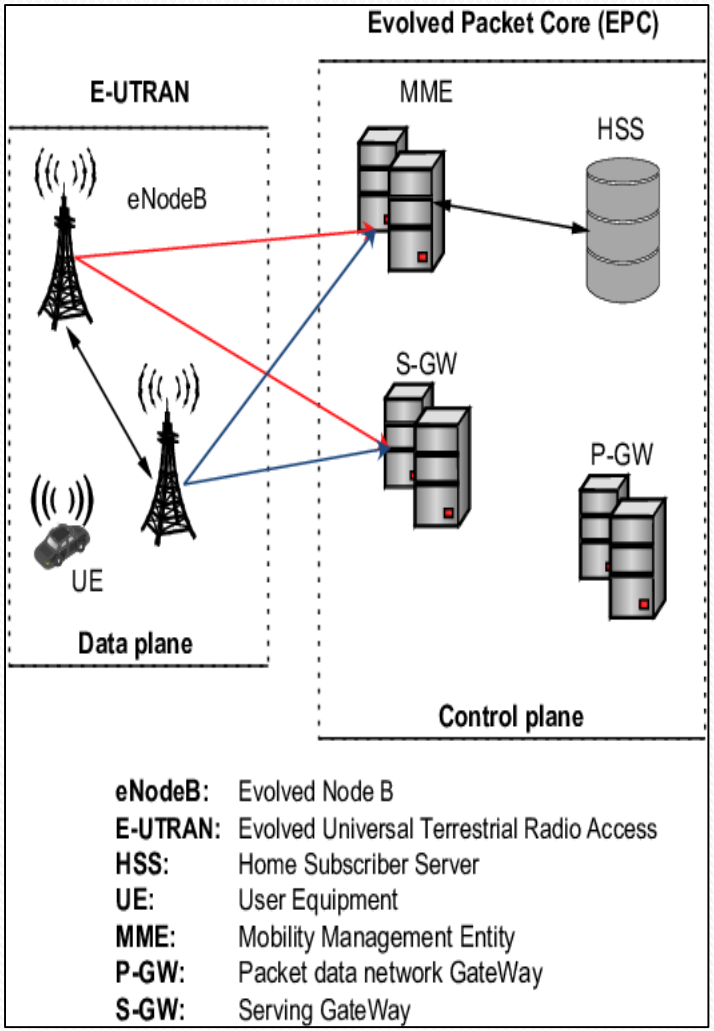
- LTE is the 3GPP initiative to evolve the UMTS technology toward a 4G.
- LTE can be viewed as an architecture framework and a set of ancillary mechanisms that aims at providing seamless IP connectivity between UE and the packet (IPv4, IPv6) data network without any disruption to the end-users' applications during mobility.
- In contrast to the circuit-switched model of previous-generation cellular systems, LTE has been designed to support only packet-switched services.
- System architecture evolution (SAE) is the corresponding evolution of the GPRS/3G packet CN evolution.
- The key element provided by LTE/SAE is the EPS (evolved packet system), that is, together LTE and SAE comprise the EPS.
- EPS provides the user with IP connectivity to a packet data network for accessing the Internet, as well as for supporting services such as streaming video.

Cellular and Mobile Network Technologies for IoT/M2M

The EPS consists of the:

- New air interface E-UTRAN (evolved UTRAN) and
- The evolved packet core (EPC) network





Cellular and Mobile Network Technologies for IoT/M2M

Cellular and Mobile Network Technologies for IoT/M2M

Core Network

- At a high level, the network is comprised of the CN (i.e., the EPC) and the access network E-UTRAN.

- While the CN consists of many logical nodes, the access network is comprised of essentially just one node, the evolvedNodeB (eNodeB), which connects to the UE.

- The CN is responsible for the overall control of the UE and establishment of the bearers.

The main logical nodes of the CN are:
(i) PDN gateway (P-GW);
(ii) serving gateway (S-GW); and
(iii) mobility management entity (MME).

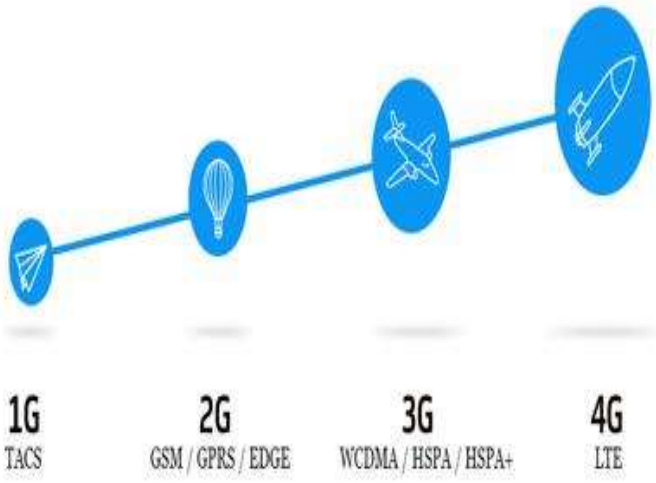
- In addition to these nodes, the CN also includes other logical nodes and functions such as the Home Subscriber Server (HSS) and the Policy Control and Charging Rules Function

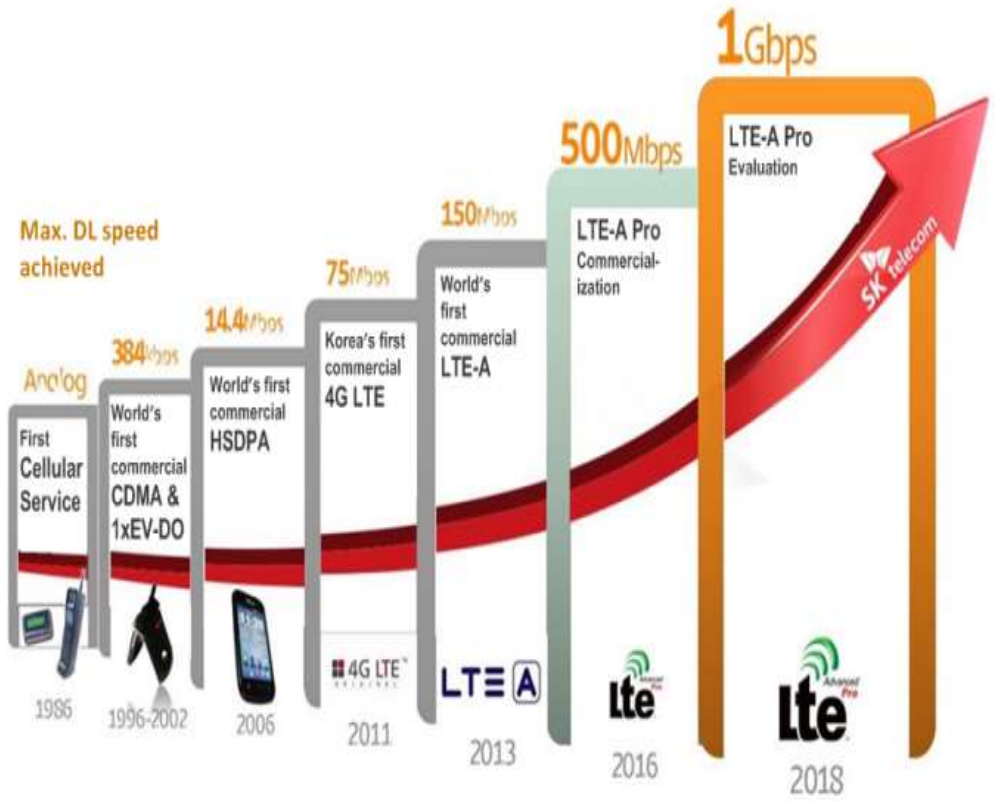
Cellular and Mobile Network Technologies for IoT/M2M

Evolution Paths to 4G/LTE
3GPP environments: GSM, GPRS, EDGE, WCDMA, HSPA

Network element evolution from 2G/3G to LTE includes the following upgrades in the provider network:

GERAN and UTRAN -> E-UTRAN
SGSN/PDSN-FA ->S-GW
GGSN/PDSN-HA ->PDN-GW
HLR/AAA ->HSS
VLR ->MME

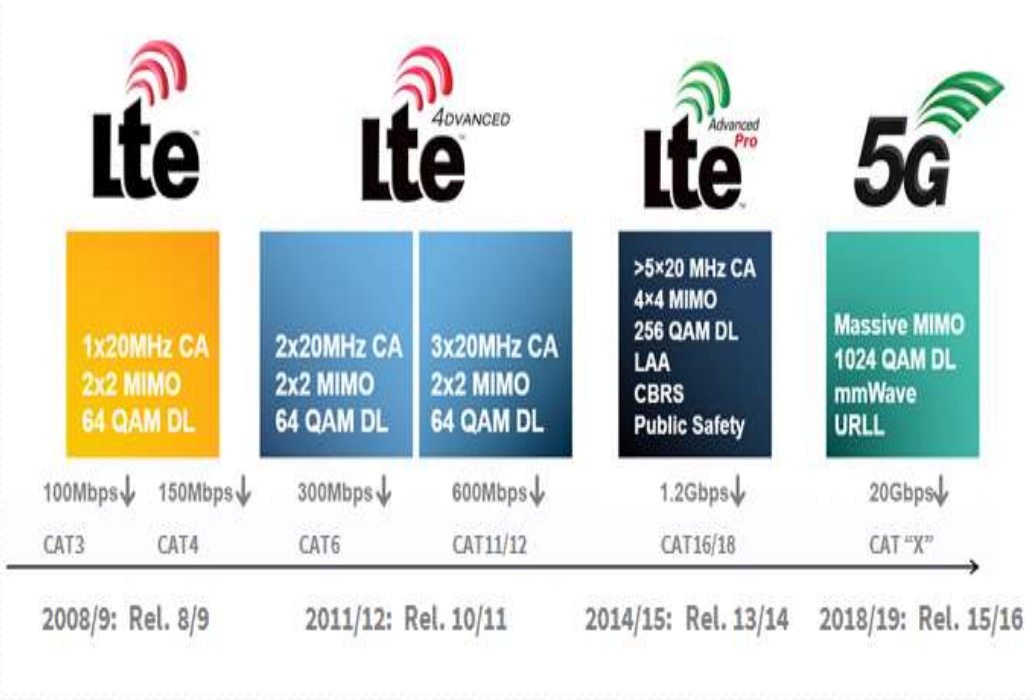




Cellular and Mobile Network Technologies for IoT/M2M

In principle, LTE promises the following benefits:

- Simplified network architecture (Flat IP based);
- Efficient interworking;
- Robust QoS framework;
- Common evolution for multiple technologies;
- Real-time, interactive, low-latency true broadband;
- Multisession data;
- End-to-end enhanced QoS management Policy control and management;
- High level of security.



Cellular and Mobile Network Technologies for IoT/M2M

Comparison	2G	3G	4G	5G
Introduced in year	1993	2001	2009	2018
Technology	GSM	WCDMA	LTE, WiMAX	MIMO, mm Waves
Access system	TDMA, CDMA	CDMA	CDMA	OFDM, BDMA
Switching type	Circuit switching for voice and packet switching for data	Packet switching except for air interference	Packet switching	Packet switching
Internet service	Narrowband	Broadband	Ultra broadband	Wireless World Wide Web
Bandwidth	25 MHz	25 MHz	100 MHz	30 GHz to 300 GHz
Advantage	Multimedia features (SMS, MMS), internet access and SIM introduced	High security, international roaming	Speed, high speed handoffs, global mobility	Extremely high speeds, low latency
Applications	Voice calls, short messages	Video conferencing, mobile TV, GPS	High speed applications, mobile TV, wearable devices	High resolution video streaming, remote control of vehicles, robots, and medical procedures

THANK YOU