M2M Communications

By

Z. Cihan TAYŞİ

IoT

- IoT
  - What is IoT
  - IoT vs. WSNs
  - IoT Elements
  - Problems in IoT
  - Research Topics

What is IoT

- The worldwide network of interconnected objects uniquely addressable based on standard communication protocols.
  - The RFID group
- 'Things' are active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information sensed about the environment, while reacting autonomously to the real/physical world events and influencing it by running processes that trigger actions and create services with or without direct human intervention.
  - Cluster of European research projects on the Internet of Things
- Uses information and communications technologies to make the critical infrastructure components and services of a city's administration, education, healthcare, public safety, real estate, transportation and utilities more aware, interactive and efficient.
  - Forrester Research

Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems, Volume 29, Issue 7, September 2013, Pages 1645-1660, ISSN 0167-739X, http://dx.doi.org/10.1016/j.future.2013.01.010.

What is IoT

- "Internet of Things semantically means a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols."
- Challenges include object unique addressing and the representation and storing of exchanged information.

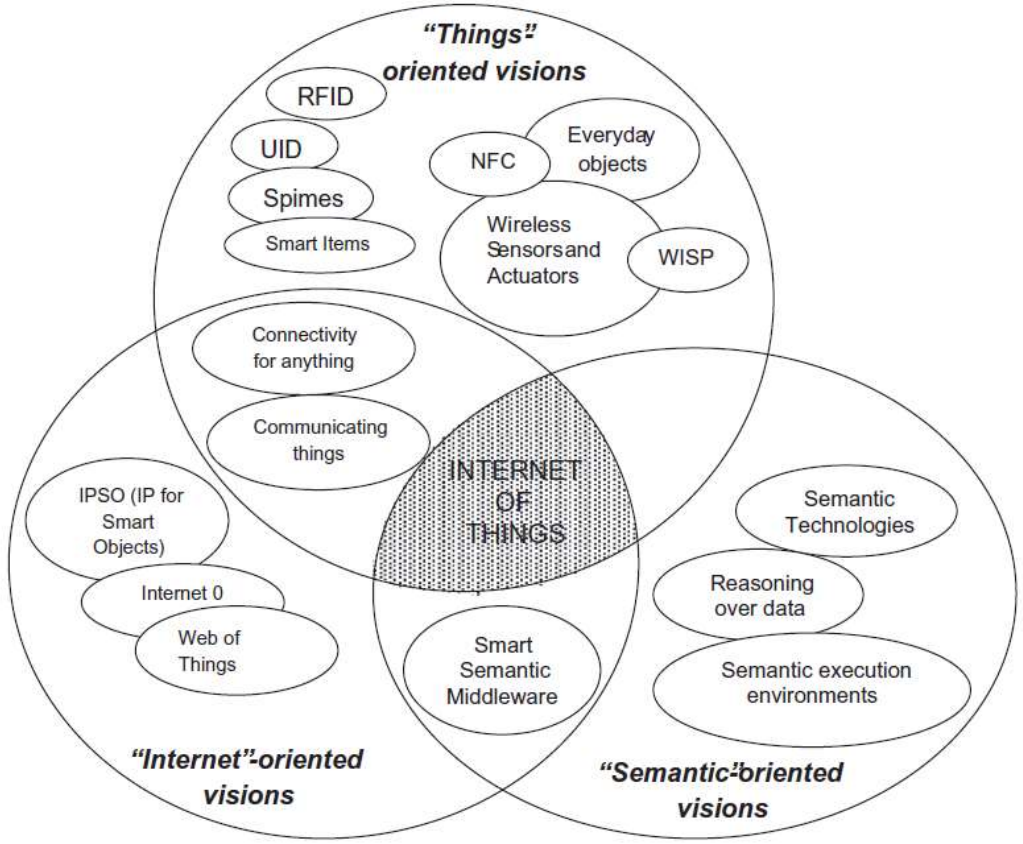


Fig. 1. "Internet of Things" paradigm as a result of the convergence of different visions.

IoT vs. WSN

- System
  - is platform: concurrent applications at endpoints
- Protocol
  - IP to endpoints
  - … on top of low resource networks
- Applications
  - use standard IP protocols
  - developed separately
- Management
  - IP management protocols
  - explicit, requires interfaces

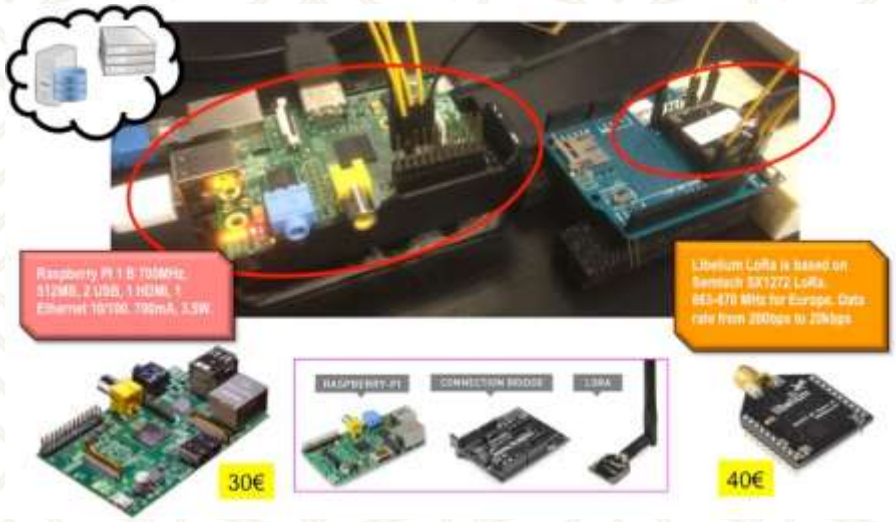
- System
  - is the application
- Protocol
  - application oriented
  - cross-layer optimization
- Applications
  - developed and optimized along with the entire system
- Management
  - implicit, part of the application

IoT Elements

- There are three IoT components which enables seamless ubicomp:
  - (a) Hardware
    - made up of sensors, actuators and embedded communication hardware
  - (b) Middleware
    - on demand storage and computing tools for data analytics
  - (c) Presentation
    - novel easy to understand visualization and interpretation tools which can be widely accessed on different platforms and which can be designed for different applications.

IoT Hardware

- Identification, sensing
  - Sensors
  - WSN nodes
  - RFID (passive, semi-passive and active)
- Communication
  - Wireless
  - 802.15.4 in most commercial WSNs already



Middleware

- Layers between the technology and the application.

- Some propose SOA (Service Oriented Architecture) approach for middleware
  - e.g., designed workflows of coordinated services which are associated with object actions.
  - Goal is complete, integrated approach.

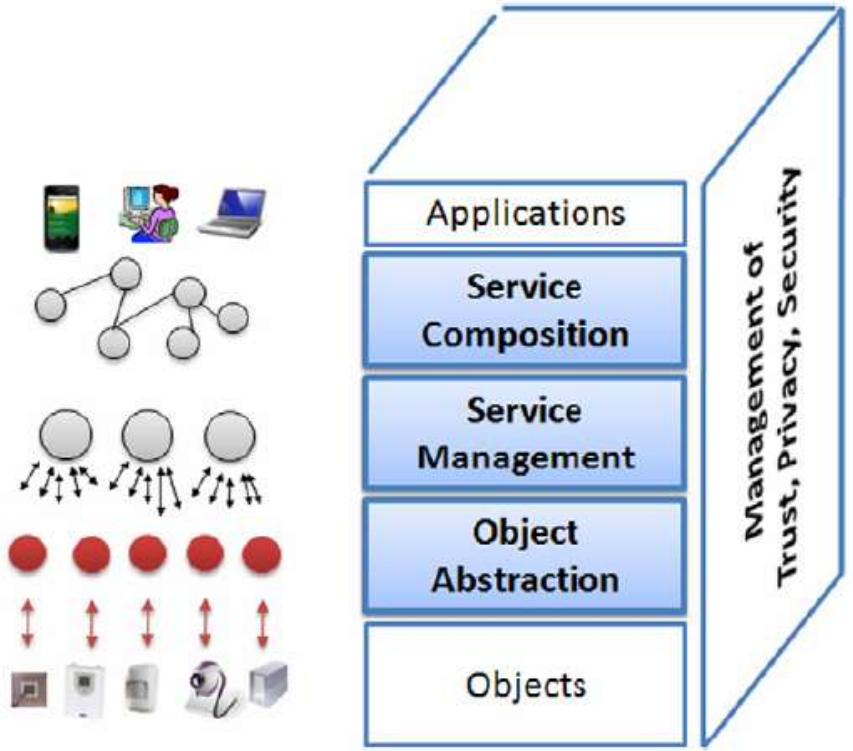


Fig. 2. SOA-based architecture for the IoT middleware.

Middleware Cont'd

- **Service composition**
  - Provides functionality for the composition of services offered by objects to build applications.
  - Workflow languages here such as Web Service Definition Language (WSDL).
- **Service management**
  - Basic set of services encompass:
    - Object dynamic discovery
    - Status monitoring
    - Service configuration
  - Functionalities related to QoS and lock management.

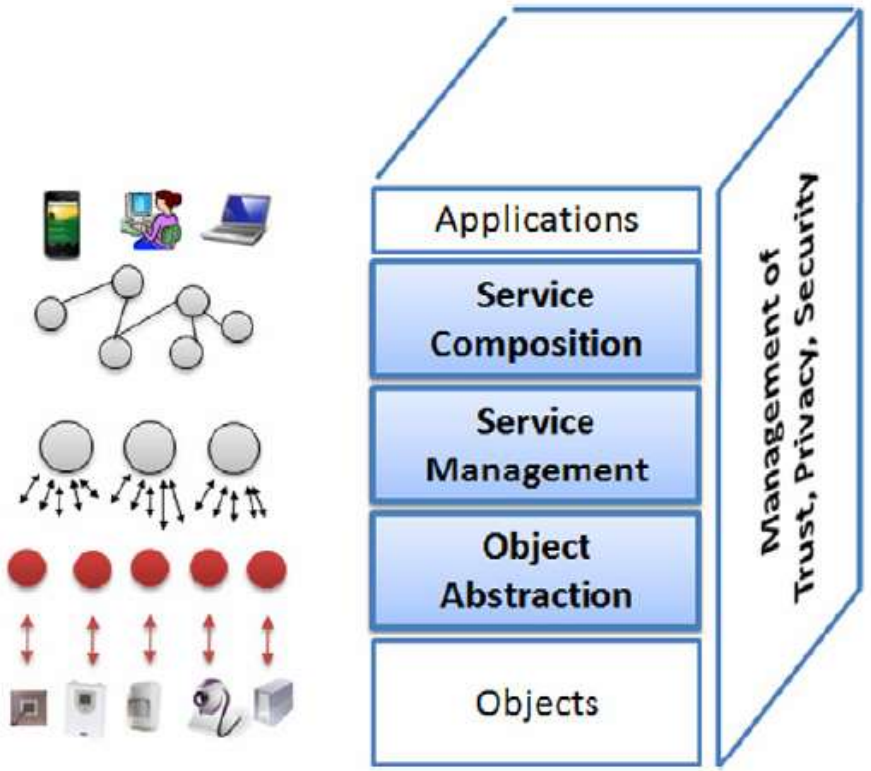


Fig. 2. SOA-based architecture for the IoT middleware.

Middleware Cont'd

- **Object Abstraction**
  - Need an abstraction layer to handle heterogeneous set of objects to harmonize the access with common language and procedures.
  - Speak of a wrapping layer to handle:
    - Web interface
    - Second interface converts service methods into device-specific commands for communicating with objects.
  - Some propose embedded stack in devices to provide wrapping function.
  - However, more often direction is for a proxy which uses socket style communication with device.

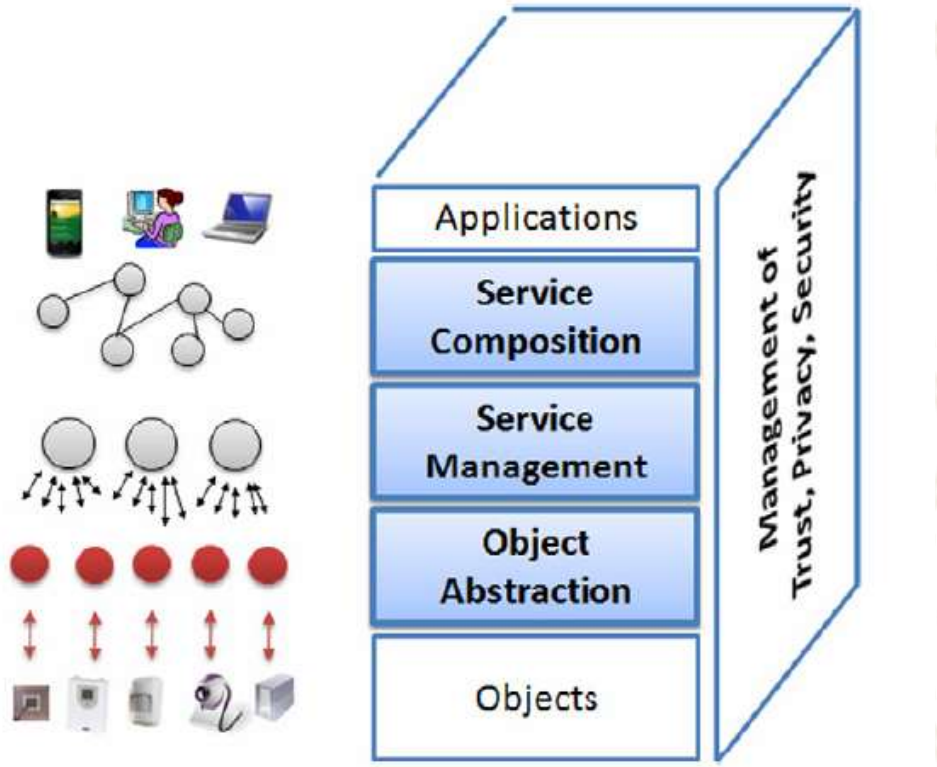


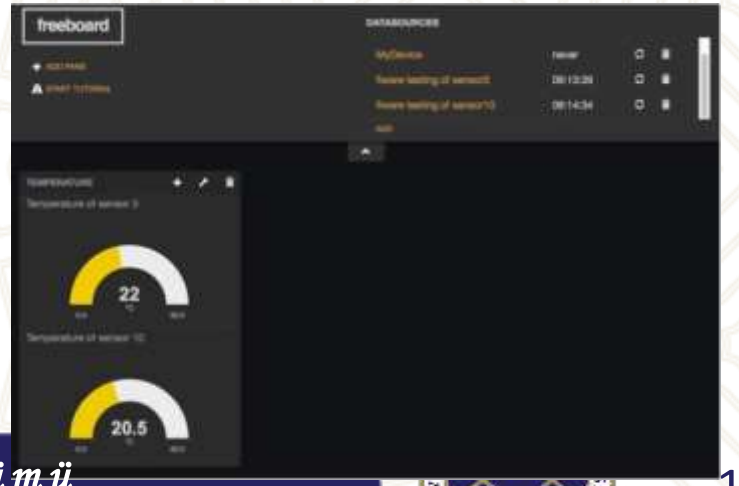
Fig. 2. SOA-based architecture for the IoT middleware.

Presentation

- The Internet of Things-generated data is growing twice as fast as social and computer-generated data,
  - it is extremely varied, noisy, time-sensitive and often confidential.
  - Complexity grows as billions of devices interact in a moving world.

- **Solution !?**

- Examples
  - Firebase, ThinkSpeak, Fiware
  - MS Azure IoT suite
  - IBM Watson



https://freeboard.io/board/h0vSv5

Research Areas for IoT

- Have you heard about Cognitive IoT !?

- Cognitive IoT is not explicitly programmed.
  - It learns from experiences with the environment and interactions with people.
  - It brings true machine learning to systems and processes so they can understand your goals,
  - then integrate and analyze the relevant data to help you achieve them.

References

- Carlos Pomalaza-Ráez, “Wireless Sensor Networks”, International Workshop on Wireless Ad Hoc Networks, May 31 – June 3, 2004
  - **http://www.ee.oulu.fi/~carlos/IWWAN_04_WSN_Tutorial.ppt**
- http://www.sciencedirect.com/science/article/pii/S1389128610001568
- http://www.ibm.com/smarterplanet/us/en/ibmwatson/
- https://www.fiware.org/

Machine-to-Machine (M2M) Communications

Outline

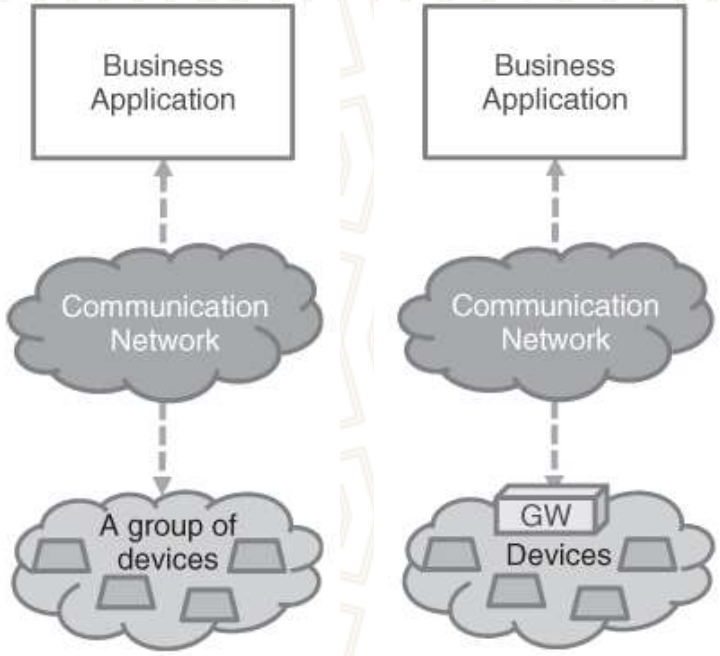
- **Introduction to M2M**
- **Bussiness of M2M,**
- **Early deployments**
- **M2M Requirements**
- **High-level Architectural Principles**

Definition of M2M

- Many attempts have been made to propose a single definition of the M(s) of the M2M acronym:
  - Machine-to-Machine, Machine-to-Mobile (or vice versa), Machine-to-Man, etc.
- Defining the complete “Machine-to-Machine” concept is not a simple task either!
  - the scope of M2M is, by nature, elastic, and the boundaries are not always clearly defined.
- The role of M2M is to establish the conditions that allow a device to (bidirectionally) exchange information with a business application via a communication network, so that the device and/or application can act as the basis for this information exchange.
  - M2M will often be a shortened synonym for M2M communications, which is itself a shortened acronym for M2(CN2)M: Machine-to-(Communication-Network-to-)Machine)

Definition of M2M Cont'd

- This description still does not fully characterize M2M.
  - For instance, a mobile phone interacting with a call center application is not seen as an M2M application because a human is in command.
  - In many cases, M2M involves a group of similar devices interacting with a single application.
    - **Ex :** Fleet management
  - In some cases, the devices in the group may not directly interact with the application, since they have imited capacities.
    - In such cases, the relationship is mediated by another device (e.g., a gateway) that enables some form of consolidation of the communication.
    - Smart metering



Definition of M2M Cont'd

- M2M area network
  - An M2M area network provides physical and MAC layer connectivity between different M2M devices connected to the same M2M area network, thus allowing M2M devices to gain access to a public network via a router or a gateway.
  - The term has been introduced by the European Telecommunication Standards Institute (ETSI).
- M2M's unique characteristic is largely due to the key role of the end-device.
  - Devices are not new in the world of information and communication technologies (ICT),
  - M2M market is seeing a new family of devices with very specific characteristics.

M2M Characteristics

- Multitude
  - more pressure on applications architectures, as well as on network load; creating scalability problems…
- Variety
  - A large variety of devices with extremely diverse requirements.
  - A major challenge to interoperability.
- Invisibility
  - the devices have to routinely deliver their service with very little or no human control.
- Criticality
  - Usage of life-critical systems places stringent requirements upon latency or reliability, which may challenge or exceed the capabilities of today's networks
- Intrusiveness
  - privacy concern of end users

Device Characteristics in M2M

- Limited in functionality
  - limited computational capabilities compared to a modern portable computer.
- Low powered
  - Although many M2M devices are connected to a power network, many of them have to be powered differently (often on batteries) for a variety of reasons.
- Embedded
  - Many devices are, and will be, deployed in systems with specific (hostile, secure) operating conditions that will make them difficult to change without a significant impact on the system itself.
  - Examples are systems embedded in buildings or in cars that are hard to replace (e.g., when they are soldered to the car engine, as is the case with some M2M devices)
- Here to stay

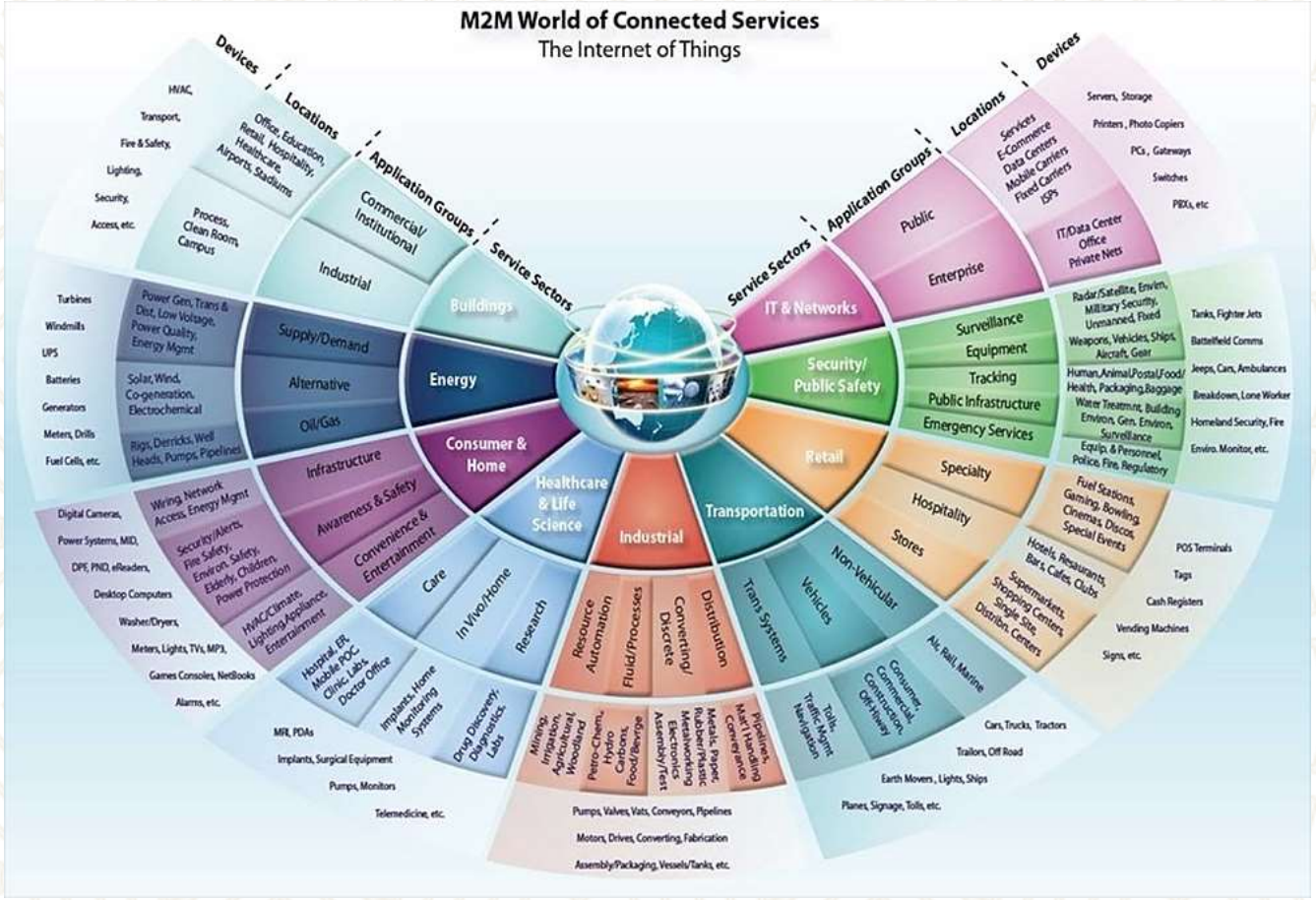
M2M vs. ICT Applications

- A separation between "regular" ICT applications versus M2M applications is to a large extent purely artificial since, in some cases, devices are able to operate both in "regular" and M2M modes.
- A classical example of this is Amazon's Kindle. Although it is a "regular" ICT device centered on both human-to-machine function (enabling eBooks) and interface (the eBook reader), it is also an M2M device in its role of providing an eBook to an end-user.
  - When the end-user has decided to buy an eBook and clicks to get it, the Kindle device enters M2M mode with a server and a network.
  - This is perfectly transparent to the end-user, thanks to a set of enablers, including the SIM card in the device, the secure identification of the device by the network, and the pre-provisioning of the device in the operator network

M2M vs. IoT

- M2M and IoT largely overlap but neither is a subset of the other and there are areas that are particularly specific to each
- IoT is dealing with Things or Objects that may not be in an M2M relationship with an ICT system.
  - An example of this is in the supermarket where radio-frequency identification (RFID) "tagged" objects are offered to the customer. These objects are "passive" and have no direct means with which to communicate "upstream" with the M2M application.
  - They can be "read" by an M2M scanner which will be able to consolidate the bill, as well as making additional purchase recommendations to the customer. From this perspective, the M2M scanner is the "end point" of the M2M relationship.
  - There are M2M relationships initiated by devices that are to be seen as direct human-machine interface extensions of a person (e.g., the above-mentioned end-user Kindle) rather than as Things (e.g., the end-user refrigerator).
- In the longer term, it is quite likely that the rather artificial distinctions, on the one hand, between traditional and M2M communication types and, on the other, between IoT and M2M domains will become further blurred with the advance of M2M and its ability to integrate more objects within existing systems.

Bussiness of M2M



- Illustration by Beecham Research

Bussiness of M2M Cont'd

- A vast quantity of documented use cases
  - some have never progressed past the drawing board
  - some have been subject to prototypes, early implementations and commercial deployments
  - **only a few** have led to the creation of significant business models!
- Despite progress in M2M Technologies, there are several challenges ;
  - fragmentation of solutions, network misalignment, security, privacy, service capabilities, certification, high-level frameworks, policy & goverment incentives, standards

Challenges

- **fragmentation of solutions**
  - In most cases, the solutions developed and implemented to date have been addressing specific vertical applications requirements in isolation from all others.
- **network misalignment**
- **security**
  - some of the most promising M2M applications (eHealth, Jet Smart Grids) are safety-critical and must be made robust against a large variety of security threats.
- **privacy**
  - To develop and resolve the sensitive issue of privacy, both regulation (an essential precondition) and standardization are required.

Challenges Cont'd

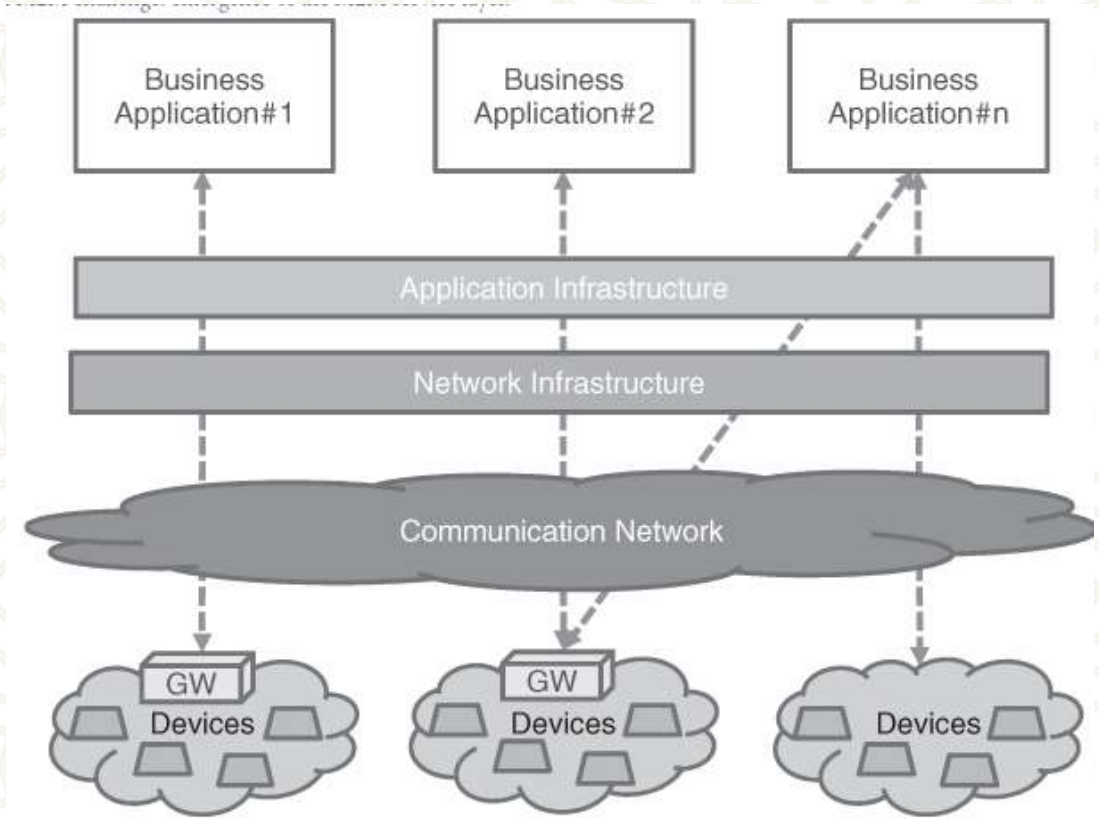
- **service capabilities**
  - In order to deal with the fragmented market, it is necessary to outline capabilities that can be reused across several applications.
  - The history of ICT networks shows that this always requires that some separation be made between different architectural layers.
  - In particular, separating applications from service capabilities (e.g., device management) and network capabilities (e.g., policy) will be key.
- **testing & certification**
  - A large number of M2M solutions will have to be developed outside of the traditional service silos, integrated with other M2M or traditional applications.
  - This will require a larger degree of interoperability and vendor compliance, which will in turn necessitate the organization of (interoperability) testing and certification of devices and equipment.
  - This will be the role of industry and/or standards organizations or forums.

Accelerators

- **high-level frameworks**
  - This refers to an emerging set of standards-based architectures, platforms, and technologies integrated in a way that allows for the development of "non-silo," future-proof applications. These frameworks allow, in particular, for economies of scale that will change the dynamics of M2M business models.
- **policy and government incentives**
  - Based on the realization that some M2M challenges may not be addressed by the industry alone, public authorities and governments have started to play an active role both in stimulating the investment by setting up ambitious incentive programs and in policy-making. This is, in turn, drives more investment in the wider M2M ecosystem, as well as creating more trust in the viability of the M2M industry.
- **standards**
  - A large number of credible industrial partners, large and small, from various industries have started to work together in order to create the new standards required to address M2M at the global system level.

High-Level M2M Frameworks

- Horizontal platforms
  - A coherent framework valid across a large variety of bussiness domains, networks and devices
  - A set of capabilities in the form of software modules that are offered to M2M applications



Policy & Goverment Incentives

- **Economic Incentives**
  - provide an attractive and stable framework that creates opportunities for investment in new projects
  - American Recovery and Reinvesment Act (ARRA) $27 billion to energy efficiency and renewable energy
  - 1511 Öncelikli araştırma alanları (1511-ENE-EVKN-2015-2)
    - Akıllı Binalarda Enerji Tasarrufu için Gerekli Gömülü Sistemlerin Geliştirilmesi
- **Regulation**
  - provides precise directions for the development of the set of standards applicable or to be enforced within a country or region
- **Funding**
  - funding of cooperative research and development projects,
  - 8th frame program of European Union

Which Standards for M2M ?!

- Data Models
- M2M Area Networks
- Access and Core Network Optimizations for M2M
- Horizontal Service Platforms and Related APIs
- Certification for M2M Modules and Terminals

Data Models

- explicitly determine the structure of data exchanged primarily between M2M applications but also with other entities within an M2M system.
- if the same data structures are used to store and access data, then different applications can exchange data in an interoperable fashion.
- Data models for M2M are application and business-logic specific.
- A data model built from scratch for a meter designed to provide reporting on consumption data to a utility application will not be useful for a sensor designed to report data on patient health monitoring.

M2M Area Networks

- The term M2M area network was used for the first time in the ETSI TS 102 690 Technical Specification.
- It is a generic term referring to any network technology providing physical and MAC layer connectivity between different M2M devices connected to the same M2M area network or allowing an M2M device to gain access to a public network via a router or a gateway.
  - Wireless Personal Area Network (W PAN) technologies such as IEEE 802.15.x, ZigBee, KNX, Bluetooth, etc. or local networks such as power-line communication (PLC), meter bus (M-BUS), Wireless M-BUS, etc.
  - While several M2M area networks are based on wireless RF technologies, other wireline-based technologies are also considered.
  - The most notable example beyond PLC is the G.hn family of standards, which has been designed with the aim of providing multiple profiles adapted for both multimedia/bandwidth-hungry applications and low-complexity/lower-bandwidth terminals.
  - ITU-T Study Group 15 initiated work known as G.hnem (home network energy management) to specify how G.hn can be used for Smart Grid applications such as advanced metering infrastructure (AMI)

M2M Area Networks Cont'd

- The Internet Engineering Task Force (IETF) has adopted the term **constrained devices** for devices that qualify for one or more of the below criteria.
  - low CPU, limited memory, low data rate, battery-operated, low power, low cost, small size (placing further constraints on the battery size).
- Constrained devices place new and challenging requirements on the communication protocols that are supported by the device.
  - it is often expected that battery-operated M2M devices will have a battery life of 10-15 years.
  - The only way this could be achieved is through self-switching the device into a "sleep mode" when there is no need to send or receive data.
  - Examples of IP-based communication protocol evolutions to cope with constrained devices include the work done in the IETF 6LoWPAN (IPv6 over low power and lossy networks) Working Group.
  - The 6LoWPAN WG group has defined encapsulation and header compression mechanisms that allow IPv6 packets to be sent and received over IEEE 802.15.4-based networks.
    - IEEE 802.15.4 maximum transfer unit (MTU) is limited to 127 bytes.
    - Taking into account frame overhead and optional security headers, very little is left for upper layers, that is, TCP/IP and application payload, unless protocol overhead is optimized.
    - In essence, the 6LowPAN work allows IP to be used all the way to constrained devices, a desirable feature to allow for an end-to-end IP-based communication.

Access and Core Network Optimizations for M2M

- In particular, cellular networks providing circuit-based services (namely voice or SMS) and data services have been optimized for personal communications.
  - After an initial deployment phase of M2M services, mostly driven by B2B applications such as telemetry or fleet management, cellular operators came to the conclusion that their networks need to become "M2M-enabled."
- Special nature of M2M traffic
  - Around 90% of the M2M devices across all applications are stationary.
  - In 3GPP and 3GPP2 wireless access, the network has procedures in place to track the location (cell or cell group) of the device.
  - For naturally stationary devices such as smart meters, constantly keeping track of the device location becomes cumbersome and consumes valuable radio resources on the air interface.
- Low volumes of data
  - As an example, a utility smart meter is required to generate meter data of around 200-500 bytes every hour (maybe slightly more frequently during peak hours).
  - In a cellular network, sending data requires the establishment of a data bearer within the access network, which means several handshake messages back and forth between the device and other entities in the access and core network (for access to radio resource, authentication/security procedures, acquiring IP address, enforcement of bearer QoS parameters, confirmation, etc.). Data bearer establishment and its teardown after use require more than 20 handshakes, **not including** the often-used TCP transport protocol's three-way handshake, acknowledgments, and connection release.

Access and Core Network Optimizations for M2M Cont'd

- New charging & billing models
  - As opposed to personal communications where charging and billing are performed for each device subscription, M2M often requires charging to be performed on a network application basis (the utility back-end application, the central fleet management application, etc.).
  - A concrete example would be to send a single network usage bill for all utility smart meters connected to a network operator, as opposed to a bill per connected smart meter.
  - Network operators and equipment vendors alike have initiated work on access and core network optimization for 3GPP and 3GPP2 cellular systems. However, since the resulting standards will take time before being deployed in operational networks, operators have adopted
- A two-step approach to cope with the growth of M2M traffic:
  - Step 1- Re-architect access and core networks so as to adapt better to the fundamental characteristics of M2M traffic while avoiding impacting the high-revenue services related to personal communications. Some of the considered scenarios include the deployment of dedicated equipment (home location register (HLR), gateway GPRS support node (GGSN)) and **traffic isolation**.
  - Step 2 - Progressively deploy new equipment, software upgrade, and network solutions that are optimized for M2M traffic types, based on the developing work on M2M standards in 3GPP and 3GPP2.

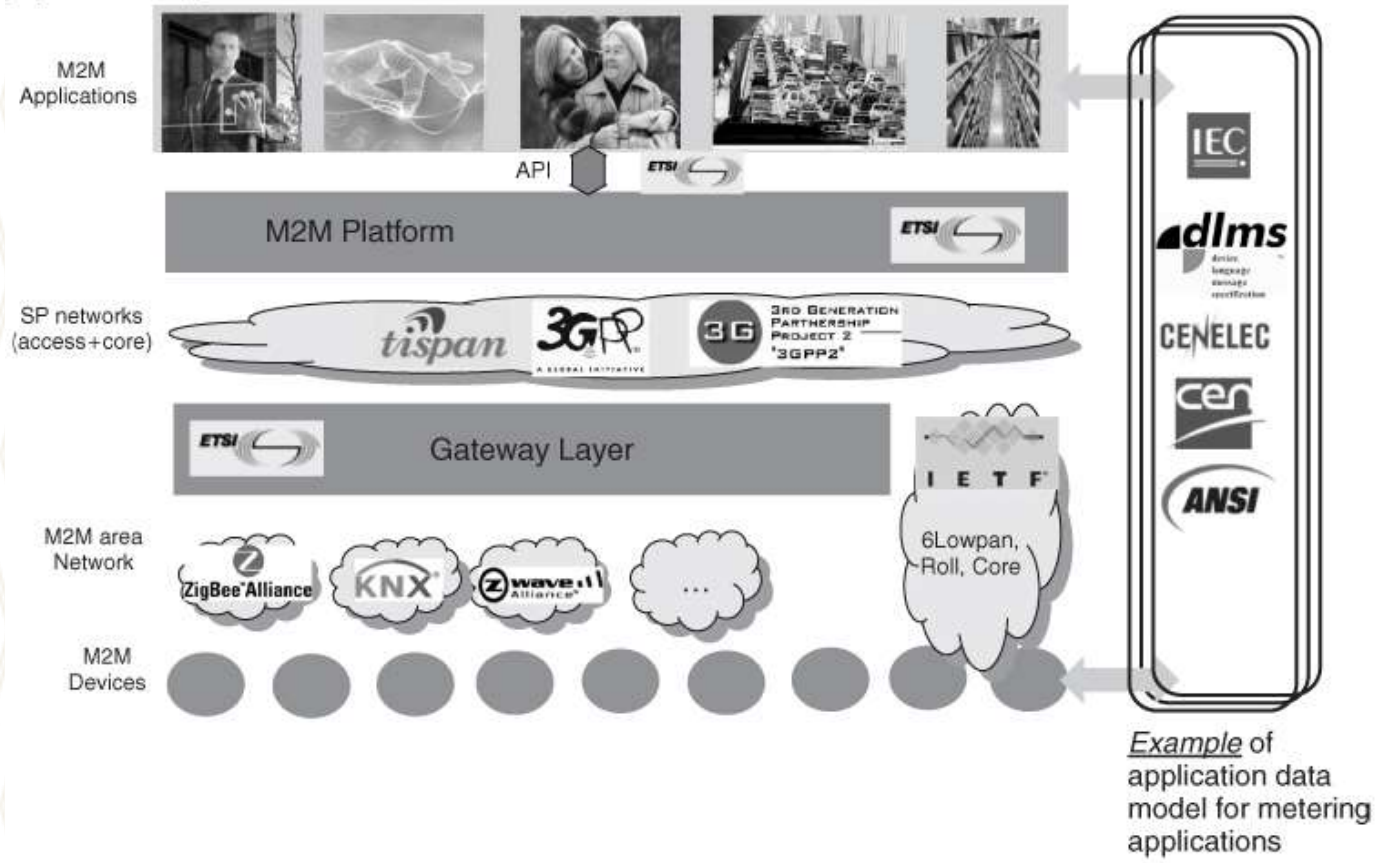
Horizontal Service Platforms and Related APIs

- As outlined above, the emergence of the next phase of M2M business will rely on the deployment of horizontal platforms implementing a set of service capabilities, that is, software modules that are exposed to the M2M applications in order to expedite their development, test, and deployment life cycles.
- Examples of service capabilities include
  - device activation, device monitoring, device localization, data storage, and Mediation to the horizontal platform (running the M2M service capabilities).
- Telecom operators have designed several API sets in the past, but their level of adoption and deployment has often suffered from lack of visibility and expertise within the IT and application developer community.
- Today, it is becoming increasingly clear that a successful Telecoms application enablement strategy mandates the use of IT-friendly APIs inspired by the Web 2.0 frame-work.
  - Representation state transfer (REST) based APIs using HTTP protocol are being specified by ETSI M2M.

Certification for M2M Modules and Terminals

- Certification refers to the confirmation of certain characteristics (usually based on a standard) of items of equipment.
- Generally, certification is provided by some form of external review, education, or assessment performed by an independent entity.
- It has become an important requirement for deploying an item of equipment (in particular, terminals) in operational environments.
- Certification can be divided into
  - mandatory regulatory certification
    - Ex : European Member States mandate the following certifications for 1912M modules, Ro1-1S, WEE/RAEE, and R&TTE directives which pertain respectively to reducing risks of hazardous substances, GSM radio spectrum, …
  - voluntary certification

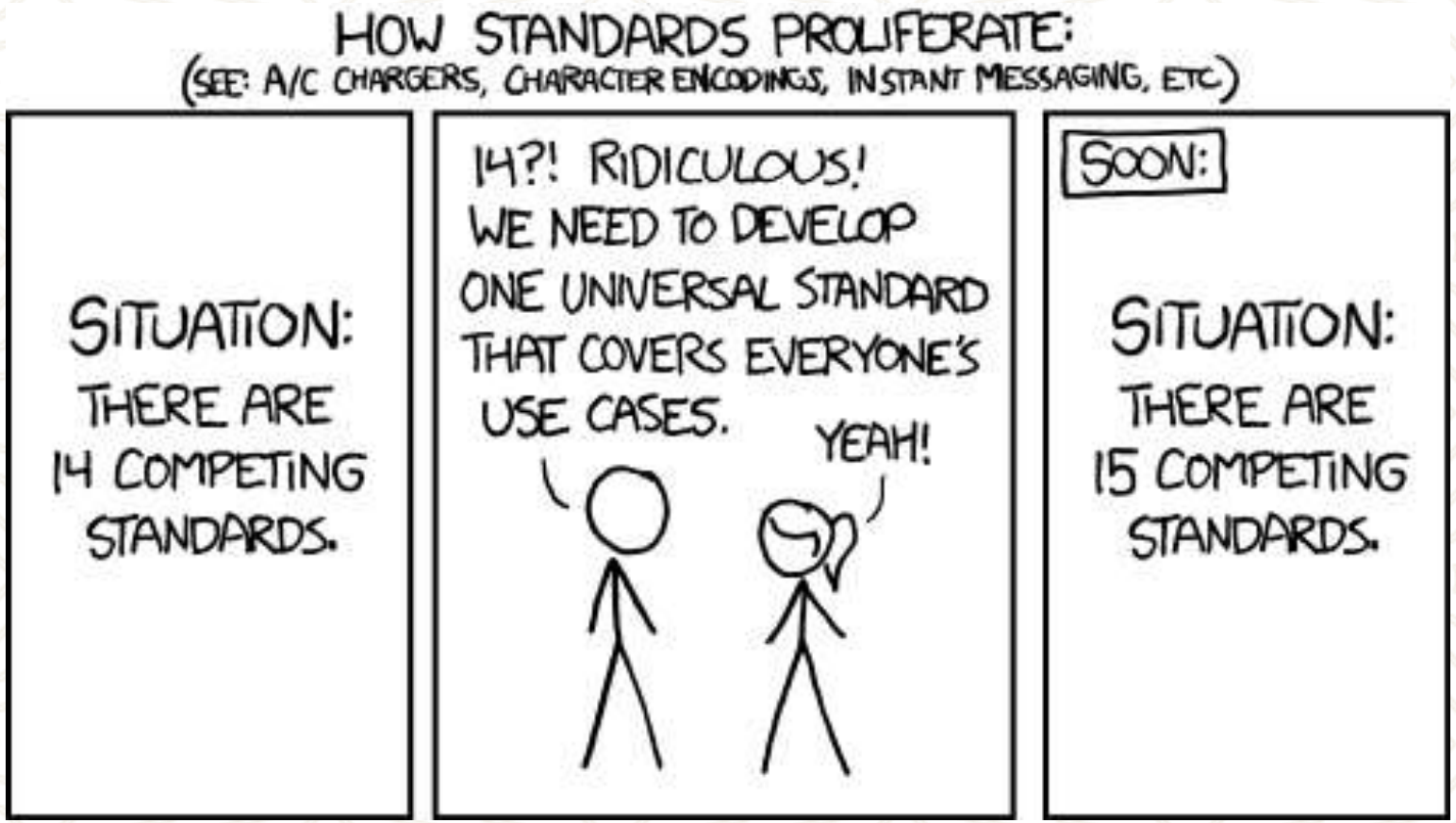
The Standards Organizations Ecosystem for M2M



Example of application data model for metering applications

- Zigbee Alliance
- KNX
- Home grid
- IETF protocol suite

M2M Area Networks



Outline

- Introduction to M2M
- Bussiness of M2M,
- Early deployments
- M2M Requirements
- High-level Architectural Principles

Business of M2M

- Market
  - Healthcare
  - Transportation
  - Energy
- Market Adoptation
  - Drivers & Barriers
- Value Chain
- Market Size Predictions
- Bussiness Models

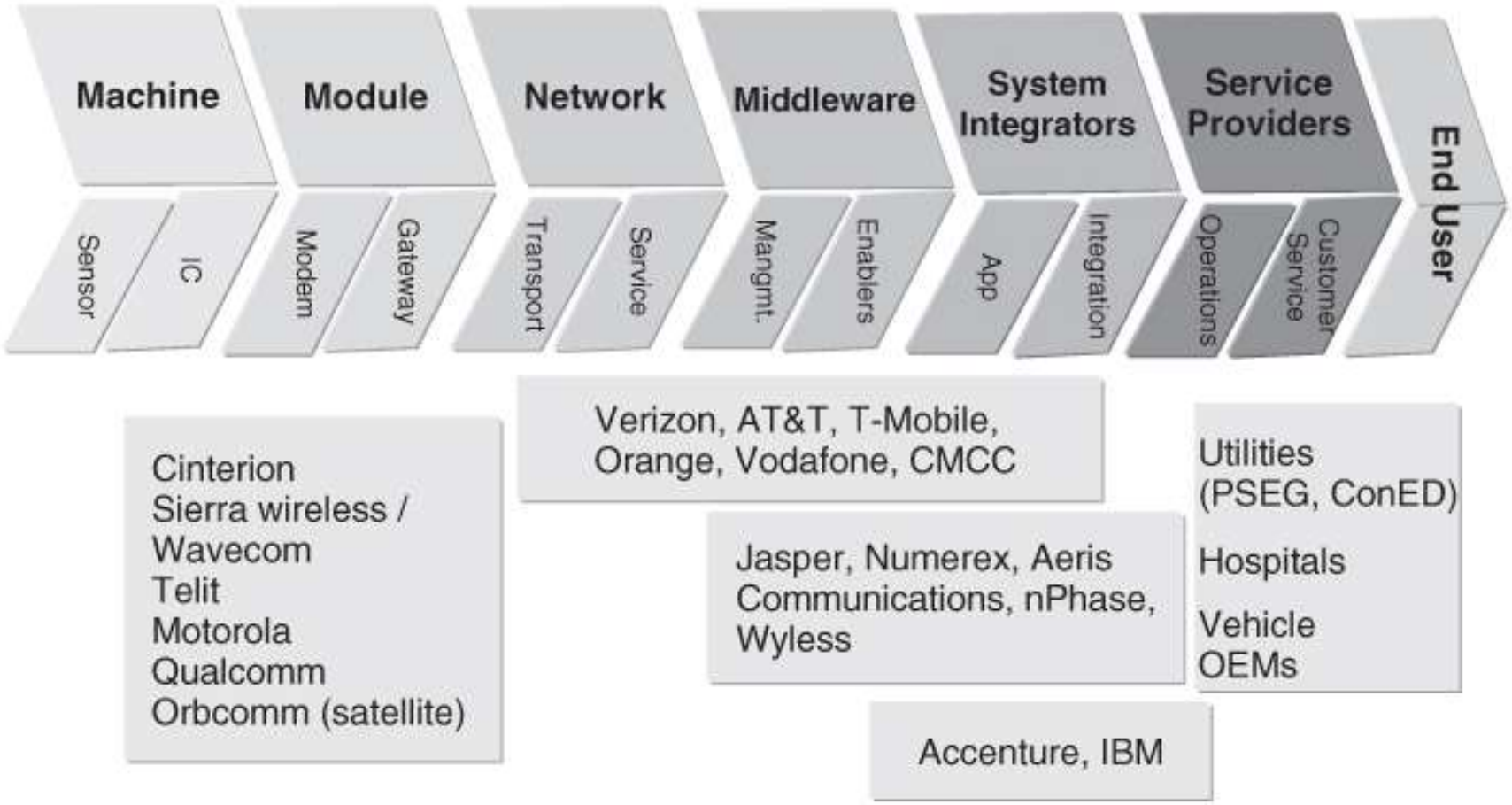
Market Adoptation

- Drivers
  - Diminishing prices for devices and communication costs
    - 20 cents to send a 140-byte SMS
    - 5 GB-per-month data plan for 50$
  - Widespread deployment of wireline and wireless IP networks
    - de facto standard for network communications
    - significantly simplies deployment and maintenance of devices and applications
  - Ubiquitous coverage provided by commercial networks
    - switching from private networks to commercial ones
  - Clear regulatory requirements and green technology investsments
    - goverments pushing for effeciencies in distribution and consumption of energy

Market Adoptation

- Barriers
  - Numerous incomplete standards leading market fragmentation
    - large number of standards addressing the same problems
    - ex : for short range communication; ZigBee, Zwave, Wireless HART, IETF 6LowPAN/ROLL
  - Global regulatory hurdles
    - different rules, different countries
  - Security & privacy
    - data collected from items that people own, and often in their homes!
  - Carrier portability
    - inability to **easily** switch operators
  - Network operator and company mismatch
    - guarantee availability of a specific technology for a long period of time (avergae life cycle of 15 years)
  - Technology challanges
    - device management, network scalability, device authentication, subscriber network and application policy, charging rules…

Value Chain

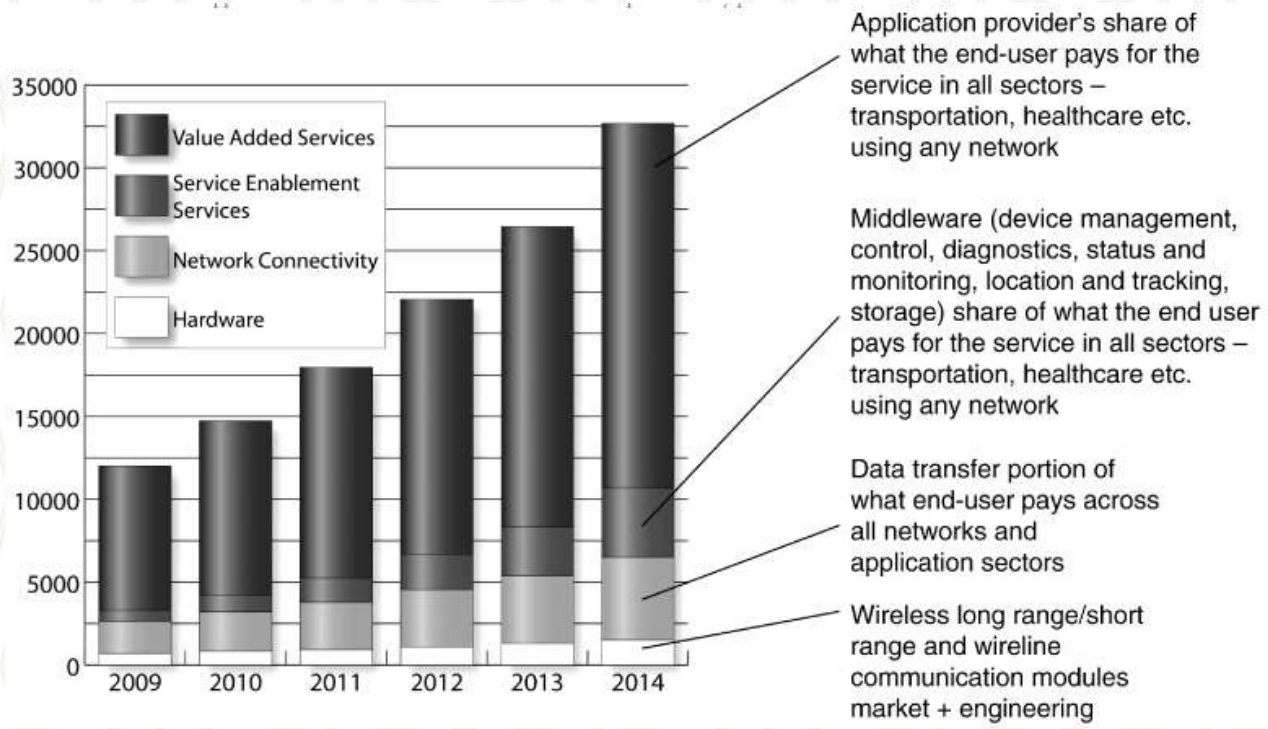

Machine
Module
Network
Middleware
System Integrators
Service Providers
End User
Sensor
IC
Modem
Gateway
Transport
Service
Mangmt.
Enablers
App
Integration
Operations
Customer Service
Cinterion
Sierra wireless / Wavecom
Telit
Motorola
Qualcomm
Orbcomm (satellite)
Verizon, AT&T, T-Mobile, Orange, Vodafone, CMCC
Jasper, Numerex, Aeris Communications, nPhase, Wyless
Accenture, IBM
Utilities (PSEG, ConED)
Hospitals
Vehicle OEMs

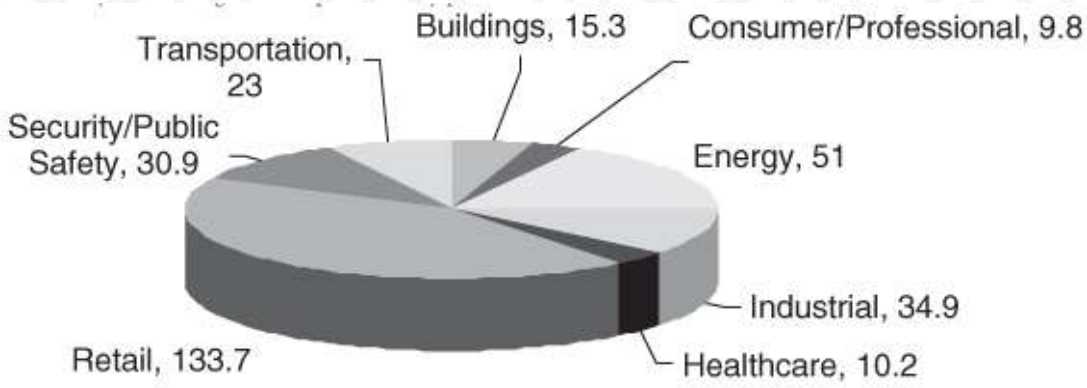
Value Chain

- Machine
  - machine is a car, in case of a connected car application,
  - includes sensory and actuation capability
- Communication
  - cellular modules, short range communication Technologies (Zigbee, Zwave)
  - In case of commercial networks, network operators or communication service providers
- Middleware
  - includes the bulk of the M2M service capabilities that are horizontal and applicable to many different applications
- System Integrators
- Application Service Providers

Market Size Projections

M2M revenues mapped to different actors of value chain

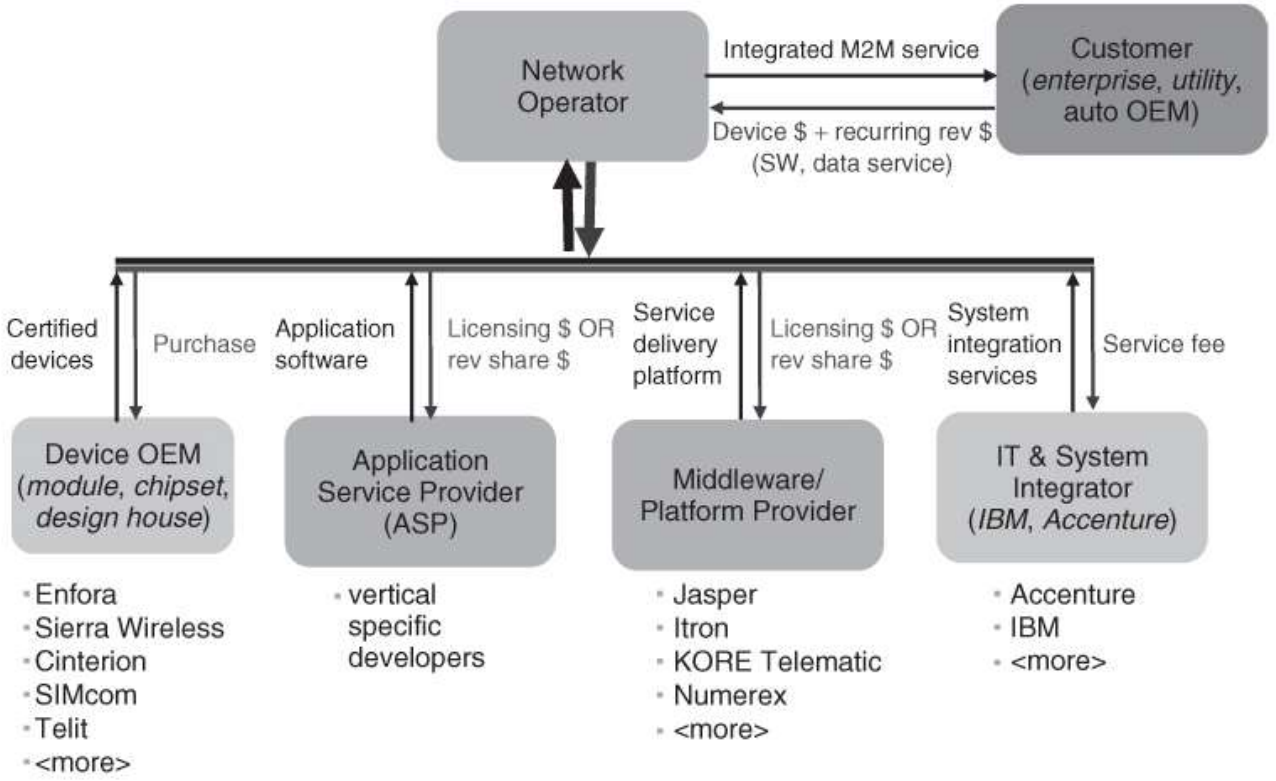




M2M market size by vertical segment

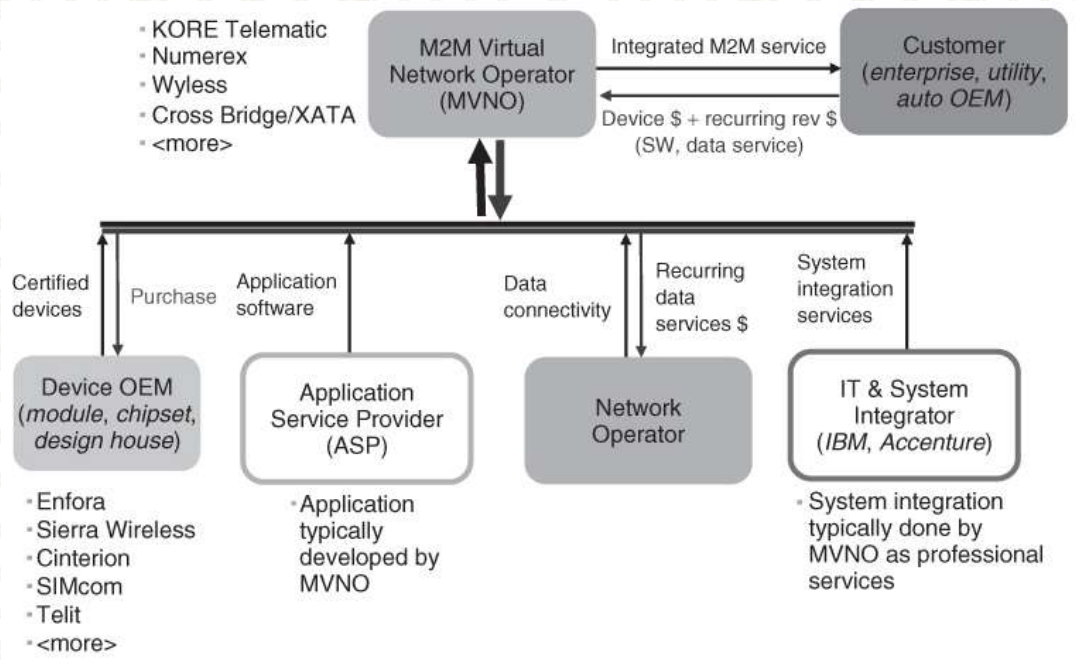
Bussiness Models

- Network Operator or CSP-Led Model
  - Communication Service Provider (CSP) plays the central role
  - CSP may also employ the services of system integrators



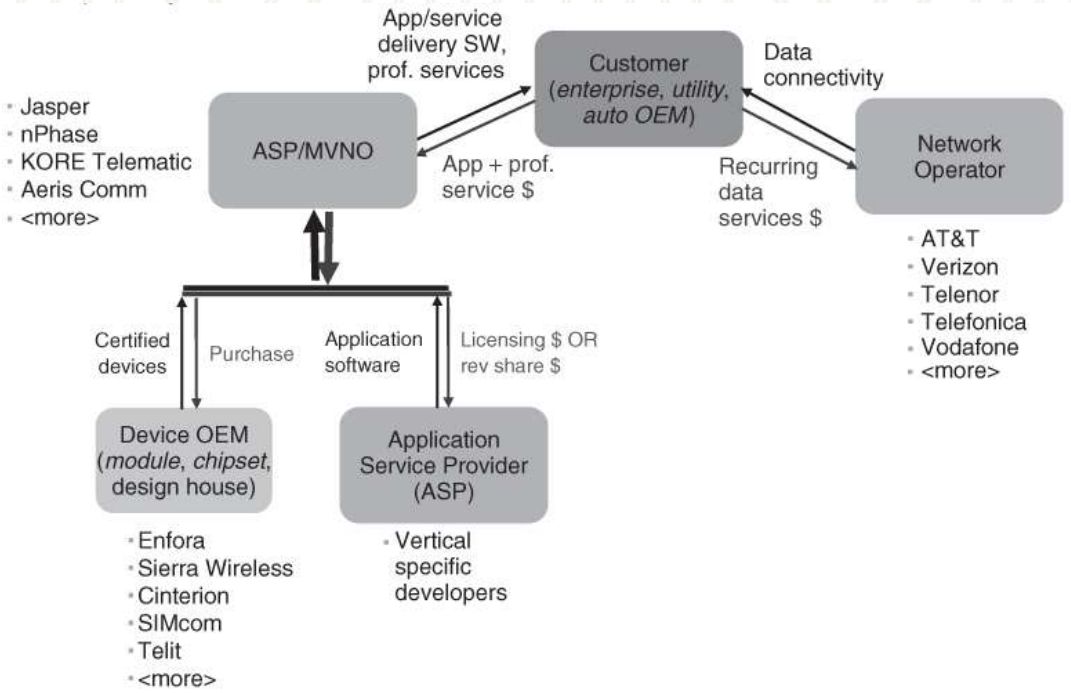
Bussiness Models Cont'd

- MVNO-Led Model
  - bandwidth agreements with specialist M2M mobile virtual network operators (MVNO)
  - MVNO plays the central role in M2M Ecosystem
  - MVNO may also offer application development



Bussiness Models Cont'd

- **Corporate Customer-Led Model**
  - company deploying large number of devices
  - negotiates with a selected network operator
  - employs a platform provider for MVNO
- **Example of Amazon Kindle**
  - integrated 3G module into kindle
  - bandwith agreements with AT&T



Outline

- Introduction to M2M
- Bussiness of M2M,
- Early deployments
- M2M Requirements
- High-level Architectural Principles

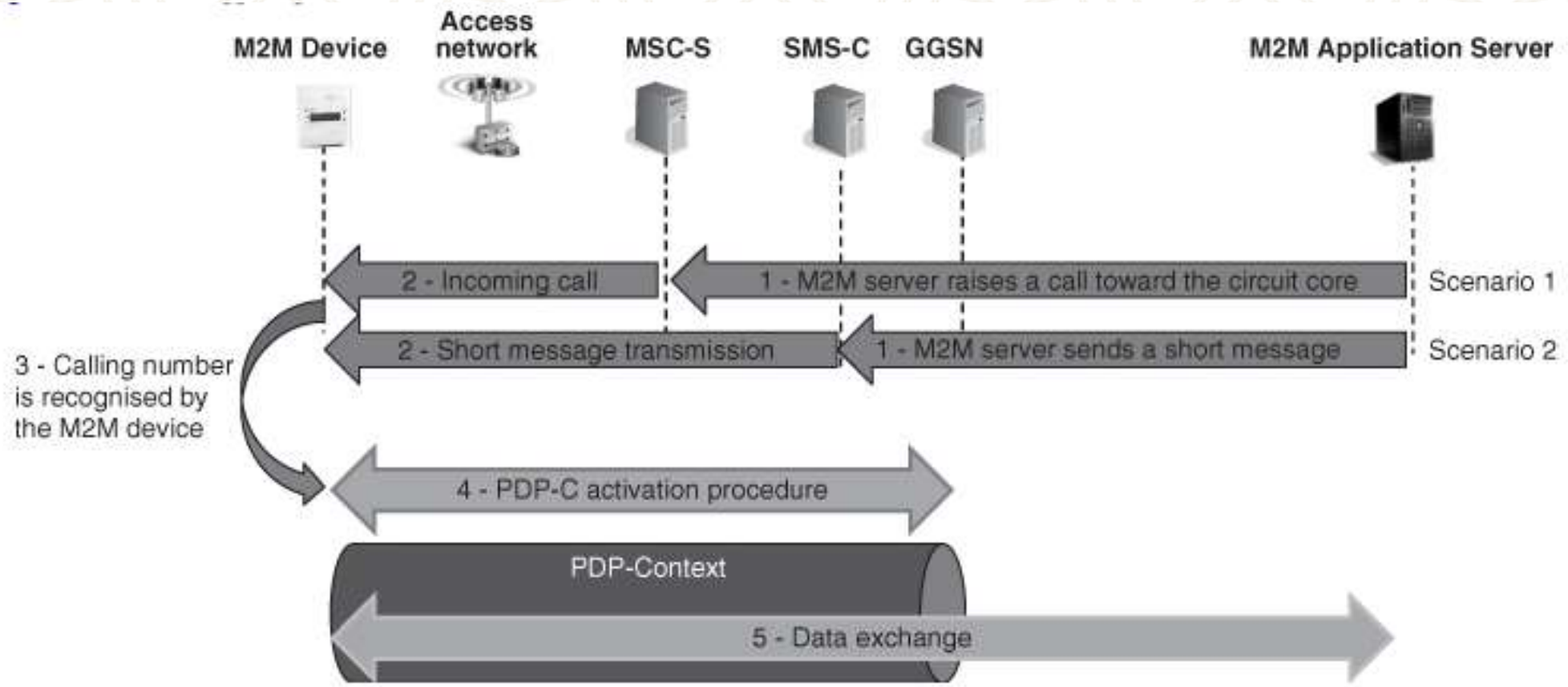
Early Deployments

- Introduction
- Examples
  - Vehicle tracking
  - Smart Telemetry
  - Healthcare monitoring
  - Surveillance and Security
- Conclusions

Early Deployments - Basic Setup

- Data collection and Exchange
  - Circuit Switched (CS) domain services such as SMS Circuit-Switched Data (CSD)
  - Packet-switched bearers
- Device triggering by the M2M server
  - sending a specific SMS to the device
  - an unanswered voice call
  - Network-requested PDP context activation (NRPCA)

Early Deployments - Basic Setup



Examples - Vehicle tracking

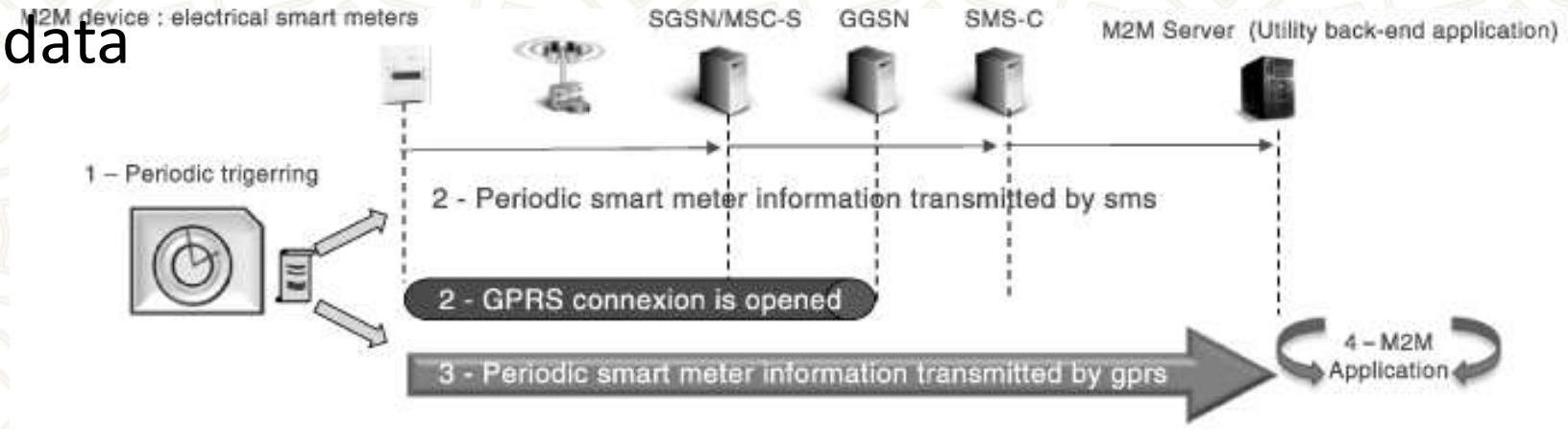
- Vehicle tracking based M2M applications
  - Fleet management
  - Pay-as-you-drive car insurance
- Howto extract location
  - GPS location
    - mandates the deployment of an antenna,
    - may not work under all conditions
  - network location
    - based on the base station cell that is serving a particular terminal
    - estimated based on the triangulation technique considering signal strengths measured base station cells

Examples - Vehicle tracking

- **Network Location**
  - **Step 1** : M2M Server requests the geo-location of the M2M device from location platform
  - **Step 2** : Geo-location platform polls the Home Location Registrar (HLR) in order to contact the MSC-S (Mobile Switching Center - Server) that controls the M2M device.
  - **Step 3-6** : Geo-location server requests the MSC-S to page all cells where the M2M device is potentially camped in order to provide 2G/3G cell-id information.
  - **Step 7** : Geo-location server translates cell-id into a geo-location position using preconfigured mapping tables.
  - **Step 8** : The geo-location information is then transmitted tothe M2M server over a pre-established VPN tunnel

Examples – Smart Telemetry

- Allows the real-time collection of various data from meters
  - temperature, energy consumption, pollution levels, and so on…
- M2M server may send urgent commands to smart meters
  - Gas tank level monitoring
- Periodic reporting of data
  - SMS solution
  - GPRS solution



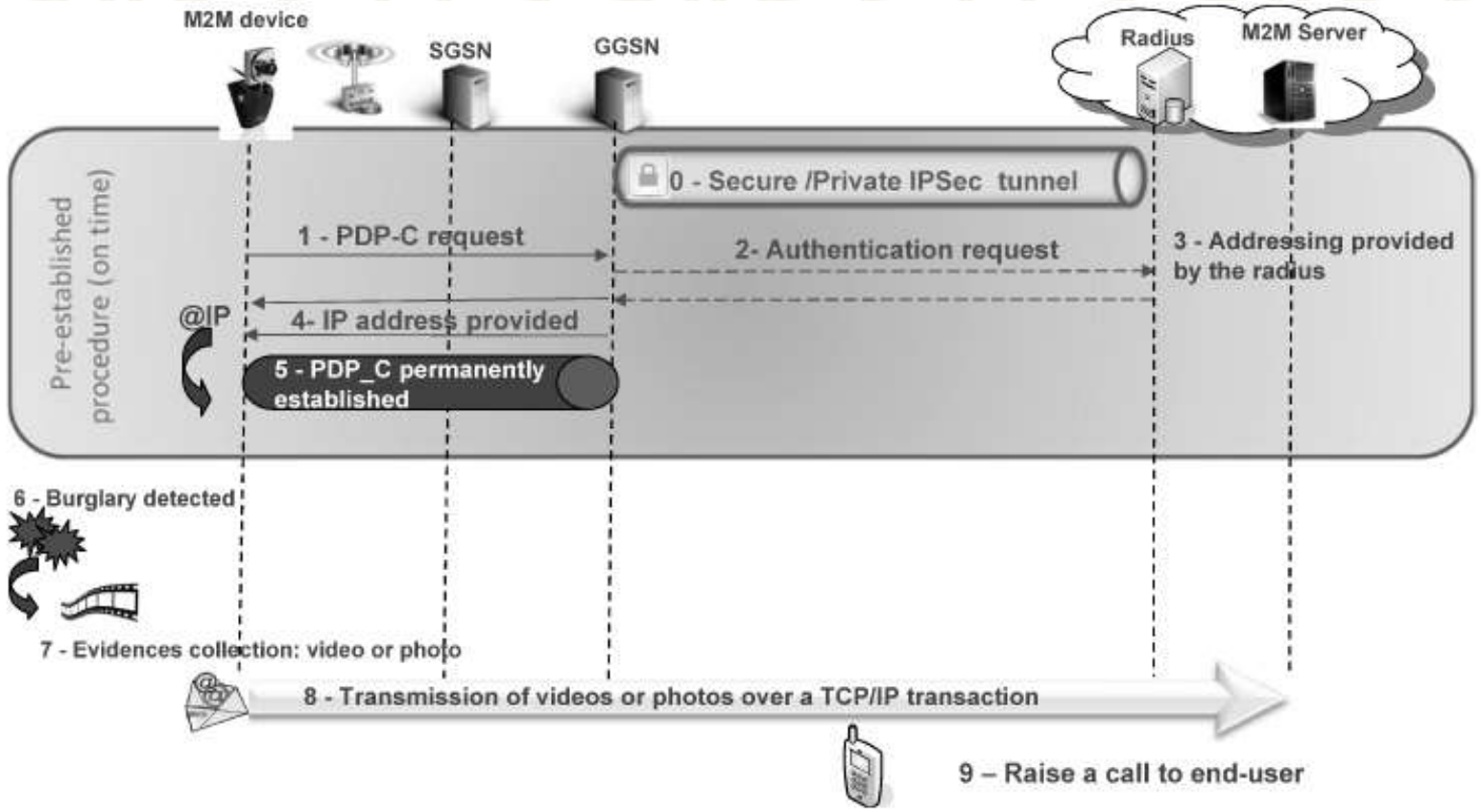
Examples – Healthcare Monitoring

- eHealth Applications
  - remote patient monitoring, healthy ageing personal fitness, disease management
- M2M devices are integrated into a wearable bracelet or a necklace
- Scenario
  - a single button to contact M2M server
  - M2M server recognizes the calling number and calls back the patients M2M device (charging & billing)
  - Patient is then assisted by an emergency medical technician
- Software updates ?
  - prioritize traffic by using **two** Mobile Station International Subscriber Directory Number (MSISDN)

Examples – Surveillance & Security

- Information exchanged
  - primarily alarm information
  - occasionally audio & low to medium resolution video signals
- Requires
  - low delay and high bandwidth (for still images & video)
  - authentication of M2M device is provided by M2M server (RADIUS)
  - IP address assignment of M2M device
  - IPSec tunnel to secure the privacy of the data that is exchanged between MNO and M2M server
- Otherwise!!
  - http://www.healthyfoodteam.com/parents-be-careful-a-3-year-old-child-said-that-someone-was-talking-to-him-at-night-and-what-his-mother-discovered-is-shocking/

Examples – Surveillance & Security



General Conclusions from Early Deployments

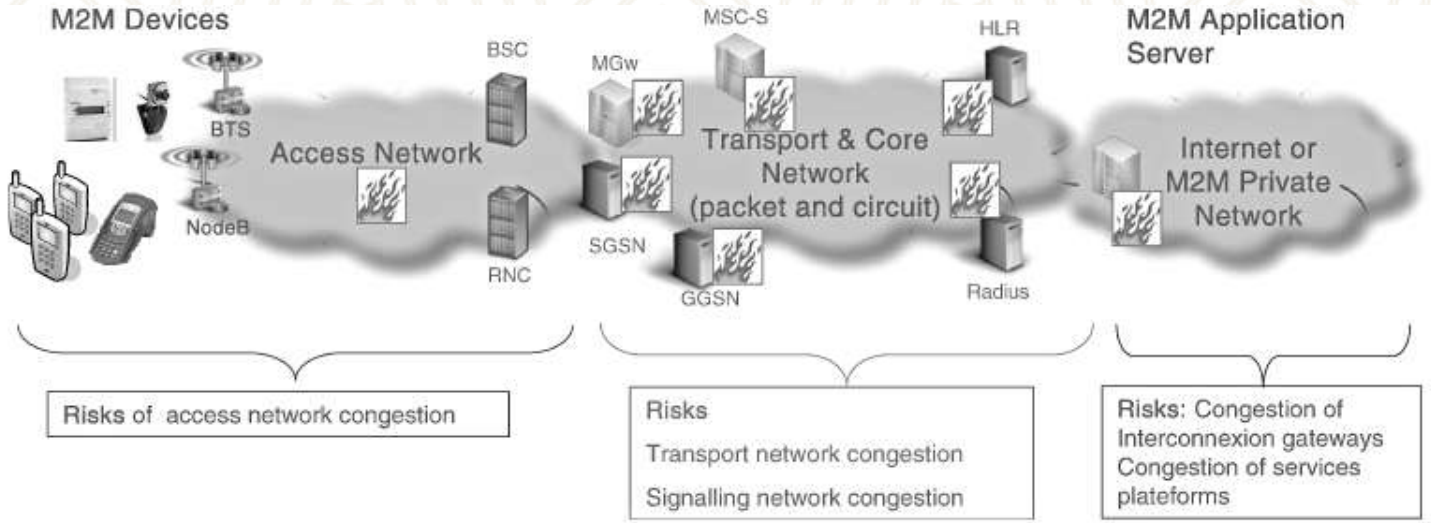
- End-to-end delay & interactivity requirements
- Data volumes
- Data Exchange frequency
- Server vs. client initiated communication
- Communication module capabilities

- **TODO : add table for this !!!**

Common Questions in Early M2M Deployments

- Congestion & Overload
  - synchronized
  - unpredictable
  - bursty
  - uncontrollable
- Shortage of identification and addressing resources
- Use of CS domain context for data-only services

Congestion & Overload



- Typically, congestion occurs when the M2M device requets the establishment of the PDP context
  - Due to abnormally high number of requests, the authentication server (RADIUS) start to overload early in the process
  - A regular human to human PDP connectivity request come to packet core network, authentication server is unable to reply and sends back a time-out failure response
  - The overload propagates back through the gateway GPRS support node (GGSN)
  - and consequently freezes the entire packet network in the latter stages…

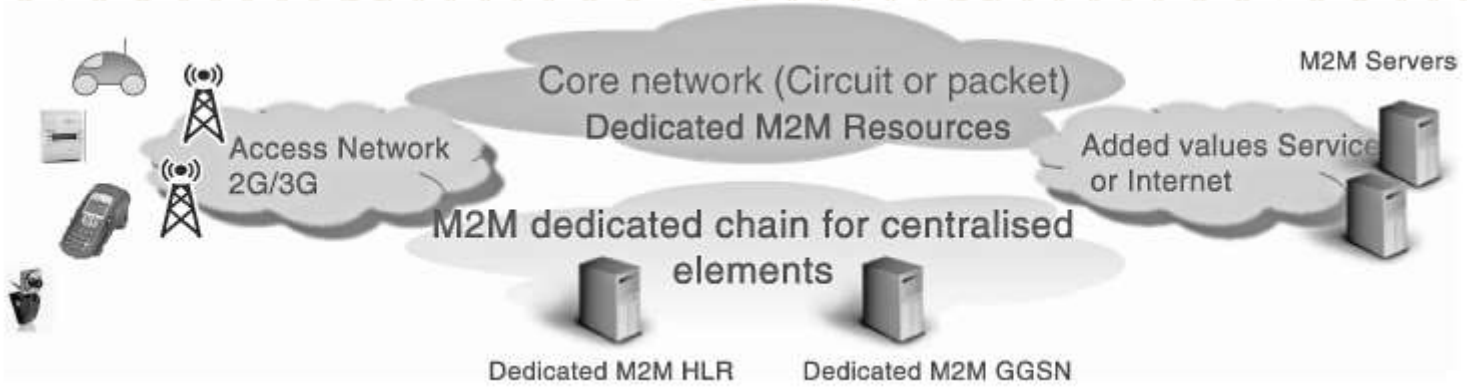
Shortage of Identification and Addressing Resources

- MSISDN
  - format specified in Recommendation E.164 of the ITU-T
  - Ex : France 200 million subscriptions / 65 million inhabitants
    - 06 XX XX XX XX – operator A
    - 07 XX XX XX XX – operator B
- IP
  - public addressing
  - private addressing
    - requires specific network setup; lease line, NAT, so on…

Possible Optimizations

- Traffic identification
  - optimizing an operational network to better handle M2M
  - providing M2M specific operational administration and maintenance functions
    - ex : disabling a set of devices in case of congestion
- Use of International Mobile Subscriber Indetity (IMSI) range
  - a specific range dedicated to M2M applications
  - another type of traffic classification

Possible Optimizations



- Dedicated core network central equipment
- HLR
  - is the central database that manages all subscriptions to the network.
  - together with use of a specific IMSI ranges for M2M allows all network requests to be routed to this particular HLR
- GGSN
  - provides gateway function to IP-based networks
  - this device can be optimized for M2M applications (small amount of traffic)

Possible Optimizations

- Specific set-up of core network elements
  - APN is a parameter of the GPRS that allows specific traffic routing toward IP networks
  - each subscription in HLR can be assigned to a specific APN that is activated upon establishment of a PDP context
- APN parameter setup
  - connection mode : permanent / non-permanent
  - IP addressing : public / private
  - timer session timeout : indicates a timeout after which a PDP context is released by the network

Cellular Networks

Outline

- Abbreviations & Who is who
- Introduction to GSM Networks
- Evolution of GSM networks
- Security in GSM Networks
- Attacks in GSM Networks

Abbreviations & Who is who

- GSM : Global System for Mobiles
- TDMA : Time Division Multiple Access
- CDMA : Code Division Multiple Access
- 3GPP : The 3rd Generation Partnership Project
- 3GPP2 : Third Generation Partnership Project 2
- GPRS : General Packet Radio Service
- EDGE : Enhanced Data rates for Global Evolution
- LTE : Long Term Evolution
- LTE-A : LTE Advanced
- RAN : Radio Access Network
- GERAN : GSM Edge Radio Access Network
- SIM : Subscriber Identity Module
- PLMN : Public Land Mobile Network
- UMB : Ultra Mobile Broadband

Abbreviations & Who is who

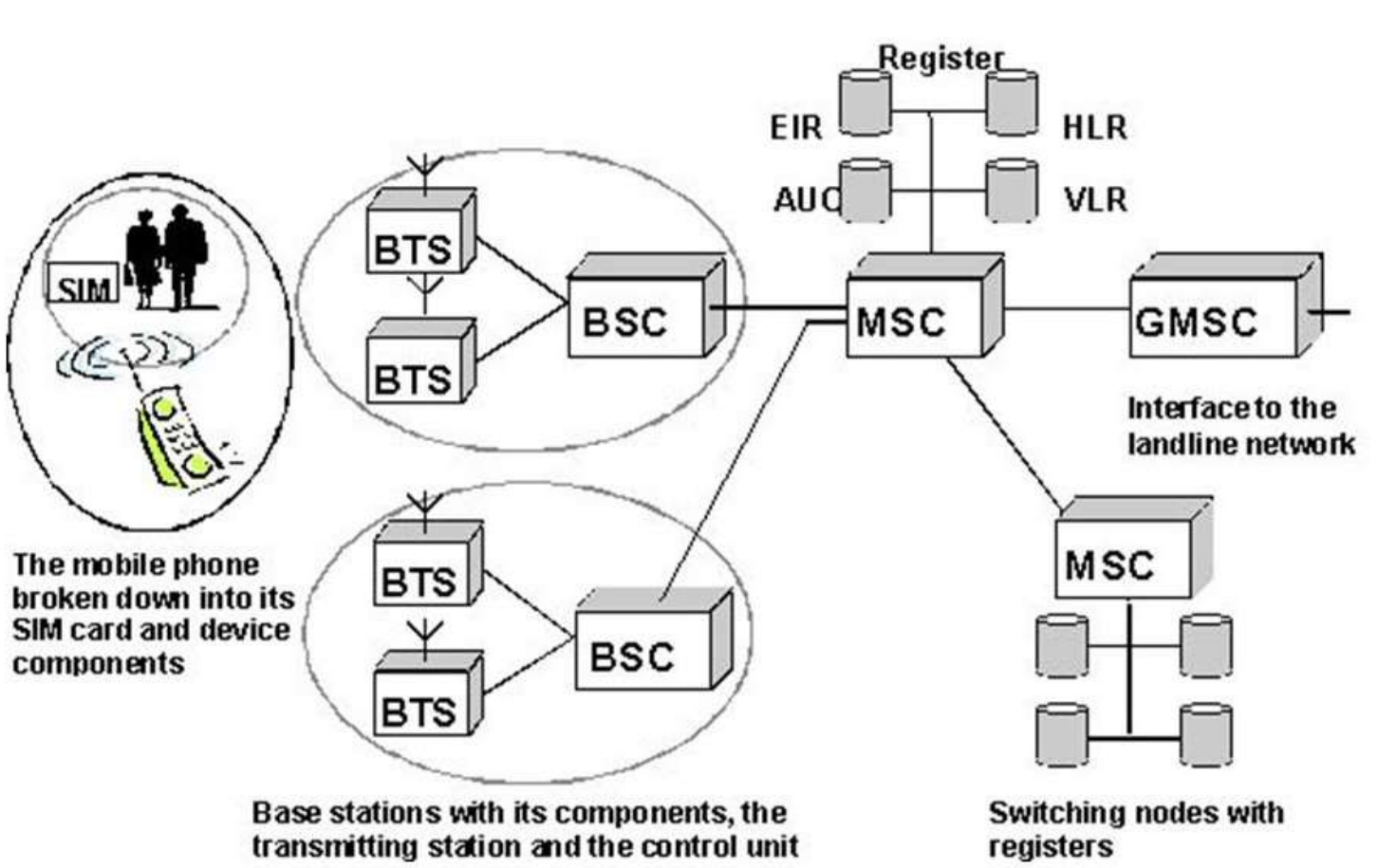
- UE : User Equipment
- ME : Mobile Equipment
- MS : Mobile Station
- BTS : Base Transceiver Station
- BSC : Base Station Controller
- MSC : Mobile Switching Center
- HLR : Home Location Register
- VLR : Visited Location Register
- EIR : Equipment Identity Register
- AuC : Authentication Centre

- 3GPP
  - The 3rd Generation Partnership Project unites 7 telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as “Organizational Partners” and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies.
- 3GPP2 :
  - 3GPP2 was born out of the International Telecommunication Union's (ITU) International Mobile Telecommunications "IMT-2000" initiative
  - UMB was a 3GPP2 project to develop a fourth-generation successor to CDMA2000. In November 2008, Qualcomm, UMB's lead sponsor, announced it was ending development of the technology, favoring LTE instead.

What is GSM

- 1982
  - Groupe Speciale Mobile (GSM) is formed by the Confederation of European Posts and Telecommunications (CEPT) to design a pan-European mobile technology.
- 1989
  - Groupe Speciale Mobile (transferred to an ETSI technical committee) defines the GSM standard as the internationally accepted digital cellular telephony standard.
- 1990
  - Phase 1 of the GSM specification released.
- 1991
  - Commercial launch of the GSM service!

GSM Architecture



GSM Architecture Cont'd

- SIM : Subscriber Identity Module
  - A3/8 algorithms, IMSI and Ki
- UE : User Equipment / ME : Mobile Equipment / MS : Mobile Station
  - contains A5 algorithm
- BTS : Base Transceiver Station
  - contains the radio transceivers and antennas that provide radio interface to and from the MS
- BSC : Base Station Controller
  - controls several BTS, manages radio resources for BTSs
  - handles call set-up, coordinates hand-overs
  - link between BTS and BSC is usually point to point microwave link

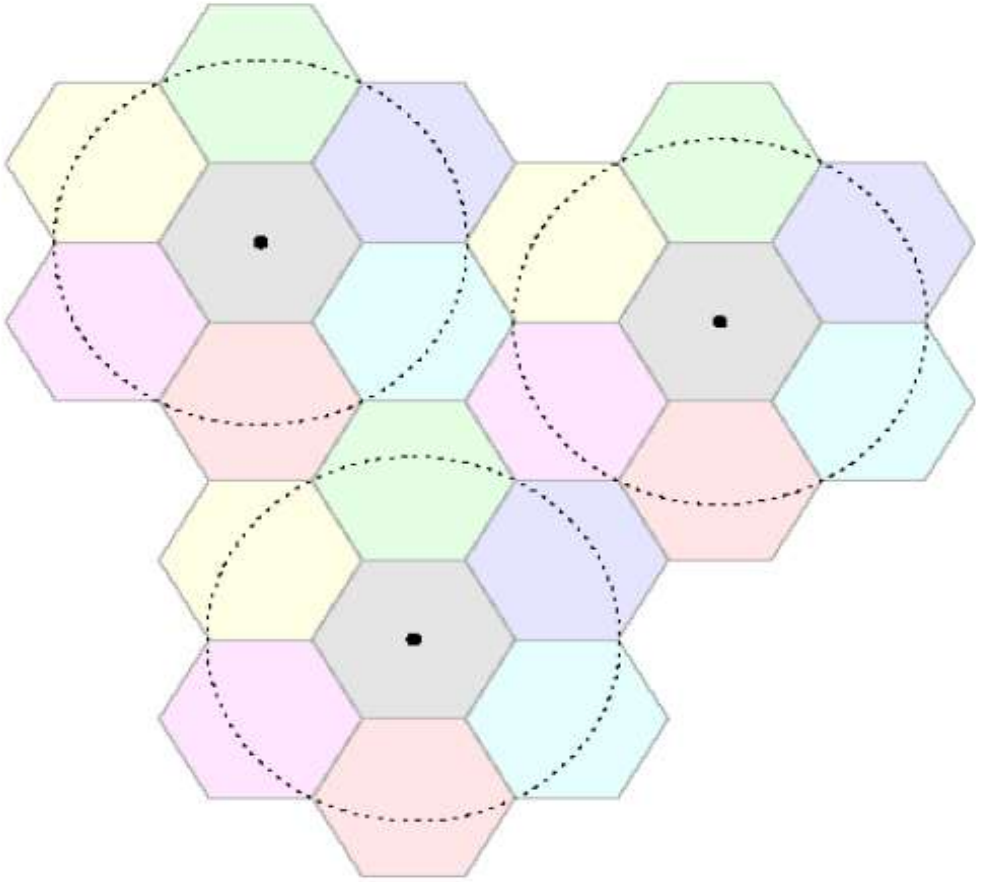
GSM Architecture Cont'd

- MSC : Mobile Switching Center
  - controls a large number of BSC
  - responsible of switching, authentication, registration, location updates, and so on...
  - inter MSC call hand-off
- EIR : Equipment Identity Register
  - a database that keeps tracks of handsets on the network using the IMEI
  - three lists; white, gray, and the black...
- HLR : Home Location Register
  - various identification numbers and addresses are stored, as well as authentication parameters.
  - The HLR database contains the master database of all the subscribers to a GSM PLMN.

GSM Architecture Cont'd

- VLR : Visiting Location Register
  - The VLR contains a copy of most of the data stored at the HLR.
  - It is, however, temporary data which exists for only as long as the subscriber is "active" in the particular area covered by the VLR
- AuC : Authentication Center
  - is a function in a GSM network used for the authentication a mobile subscriber that wants to be connected to the network.
  - contains A3/8 algorithms and Ki
  - can be co-located with HLR
- GMSC : Gateway Mobile Switching Centre
  - provides an interface to Public Swicthed Telephone Network (PSTN)

GSM network areas



- **Cell** is the basic service area; one BTS covers one cell. Each cell is given a Cell Global Identity (CGI), a number that uniquely identifies the cell.
- A group of cells form a **Location Area** (LA). This is the area that is paged when a subscriber gets an incoming call. Each LA is assigned a Location Area Identity (LAI). Each LA is served by one or more BSCs.
- The area covered by one MSC is called the **MSC/VLR service area**.
- The area covered by one network operator is called the **Public Land Mobile Network (PLMN)**. A PLMN can contain one or more MSCs.

Mobile Subscriber ISDN Number (MSISDN)

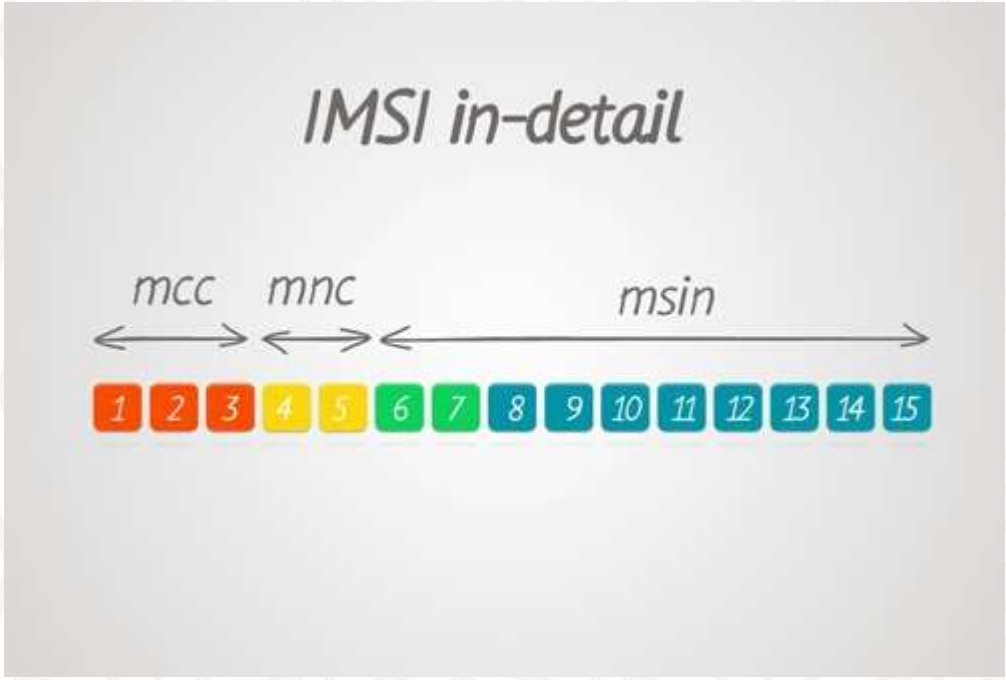
- The authentic telephone number of a mobile station is the Mobile Subscriber ISDN Number (MSISDN).

- Based on the SIM, a mobile station can have many MSISDNs, as each subscriber is assigned with a separate MSISDN to their SIM respectively

- **MSISDN format**
  - **Country Code (CC)** : Up to 3 decimal places.
  - **National Destination Code (NDC)** : Typically 2-3 decimal places.
  - **Subscriber Number (SN)** : Maximum 10 decimal places.

International Mobile Subscriber Identity (IMSI)

- This is a unique identifier that defines a subscriber in the wireless world, including the country and mobile network to which the subscriber belongs.
- It has the format MCC-MNC-MSIN.
  - MCC = Mobile Country Code (e.g. 286 for Turkey);
  - MNC = Mobile Network Code (e.g. 01 for Turkcell, 04 for Aycell),
  - MSIN = sequential serial number.
- All signaling and messaging in GSM and UMTS networks uses the IMSI as the primary identifier of a subscriber.
- The IMSI is one of the pieces of information stored on a SIM card.



http://mcclist.com/mobile-network-codes-country-codes.asp

International Mobile Station Equipment Identity (IMEI)

- IMEI looks more like a serial number which distinctively identifies a mobile station internationally.
- It is allocated by the equipment manufacturer and registered by the network operator, who stores it in the EIR
- By means of IMEI, one recognizes obsolete, stolen, or non-functional equipment.

- **Type Approval Code (TAC)**
  - 2 decimal places, centrally assigned.
- **Final Assembly Code (FAC)**
  - 6 decimal places, assigned by the manufacturer.
- **Serial Number (SNR)**
  - 6 decimal places, assigned by the manufacturer.
- **Spare (SP)**
  - 1 decimal place.
- After April 1, 2004, the Final Assembly Code ceased to exist and the Type Allocation Code increased to eight digits in length

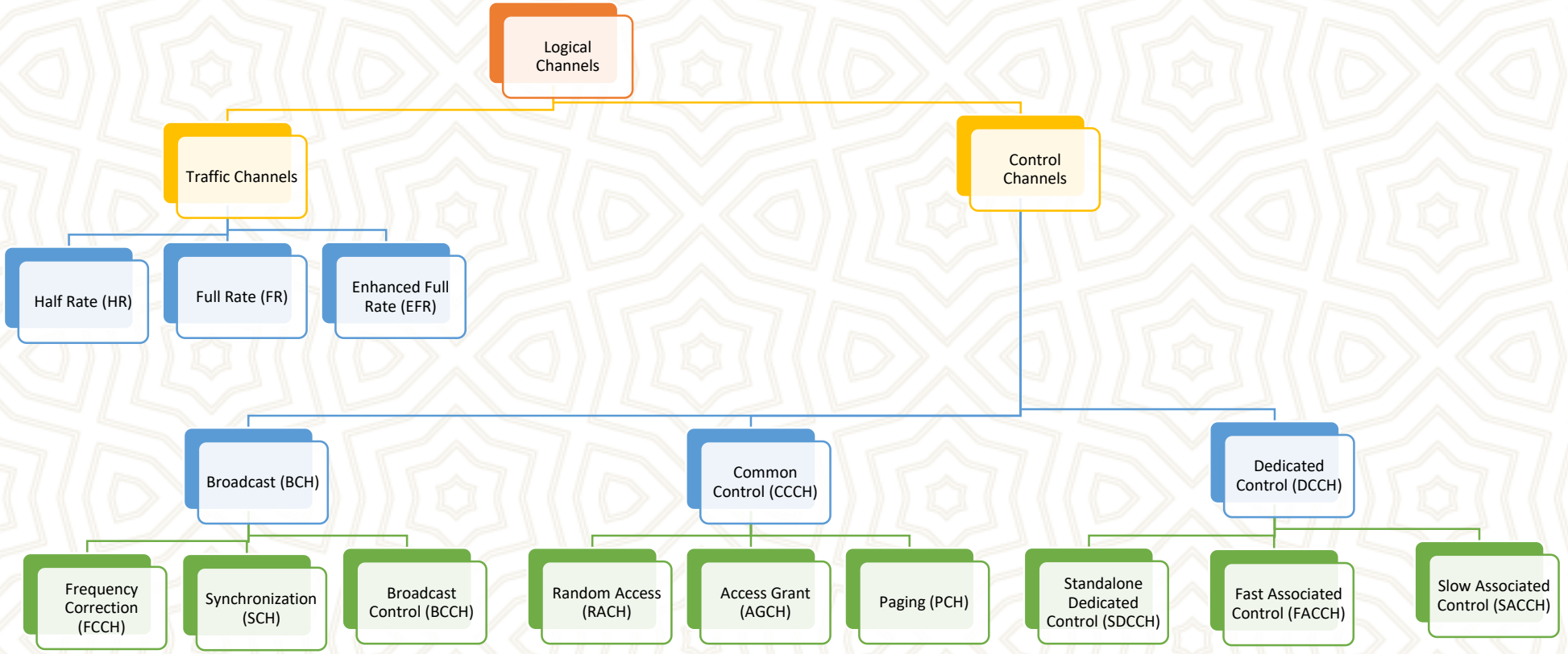
Integrated Circuit Card ID (ICCID)

- This is the identifier of the actual SIM card itself
  - an identifier for the SIM chip.
- ICCIDs are stored in the SIM cards and are also engraved or printed on the SIM card body during a process called personalization.
- It is possible to change the information contained on a SIM (including the IMSI), but the identify of the SIM itself remains the same.
- The number is composed of the following subparts:
- Issuer identification number (IIN) Maximum of seven digits:
  - Major industry identifier (MII), 2 fixed digits, 89 for telecommunication purposes.
  - Country code, 1–3 digits, as defined by ITU-T recommendation E.164.
  - Issuer identifier, 1–4 digits.
- Individual account identification
  - Its length is variable, but every number under one IIN will have the same length.
- Check digit
  - Single digit calculated from the other digits using the Luhn algorithm.

GSM Channels

- There are two main types of **GSM channels**
  - **physical channel** and **logical channel**.
  - Physical channel is specified by specific time slot/carrier frequency.
    - each physical channel(time slot at one particular ARFCN) will have either 26 Frame MF(Multi-frame) or 51 Frame MF structure.
  - Logical channel run over physical channel i.e. logical channels are time multiplexed on physical channels;
    - For example, every 26 TDMA frames a logical channel gets bandwidth in a physical channel.
    - logical channels are classified into traffic channel and control channel.
    - Traffic channel carry user data.
    - Control channels are interspersed with traffic channels in well specified ways.

GSM Channels Cont'd



GSM Channels

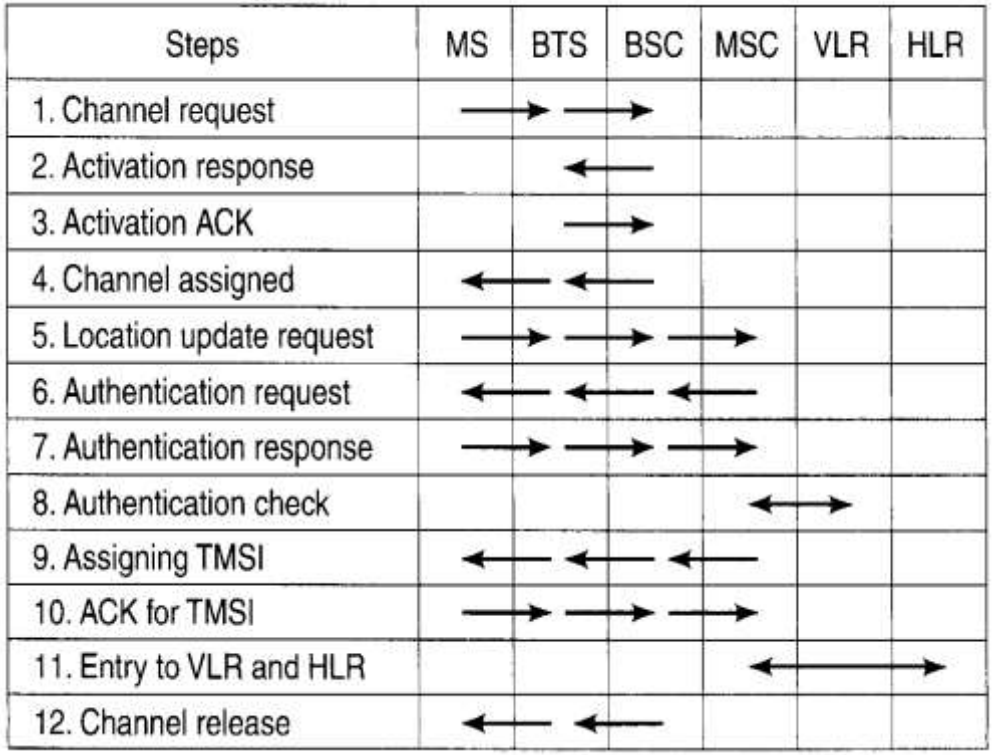
- **Category 1: Broadcast channels**
  - As the name suggests they are point-to-multipoint and downlink only channels.
  - **FCCH:** this is transmitted by BTS to MS. This helps MS tune its local oscillator to exact RF carrier frequency of the BTS cell.
  - **SCH:** synchronization channel, this carry BSIC(Base transceiver station identity code) and Frame number which helps MS tune to specific (Frequency,Ts) physical slot on TDMA frame in GSM network.
  - **BCCH:** Broadcast control channel, carry CGI,MNC,MCC which is received by MS. It is compared with SIM information, once verified, connection is established with the network.
- **Category 2: Common Control channels**
  - They are point-to-multipoint and downlink only channels except RACH which is used in uplink.
  - **PCH:** this channel sends information on downlink to alert called mobile phone.
  - **RACH:** is used in mobile originated call. When mobile wants to make a call, control information is sent on this channel.
  - **AGCH:** transmitted by BTS to MS once network approves request of mobile by RACH.
  - **CBCH:** used to carry the short message service cell broadcast.
- **Category 3: Dedicated Control channels**
  - They are bidirectional and point-to-point Channels.
  - **SDCCH:** is used for call setup.
  - **SACCH:** is used for control and supervisory signals associated with the traffic channels.
  - **FACCH:** is used for control requirements such as handoff/handovers.

GSM Attach

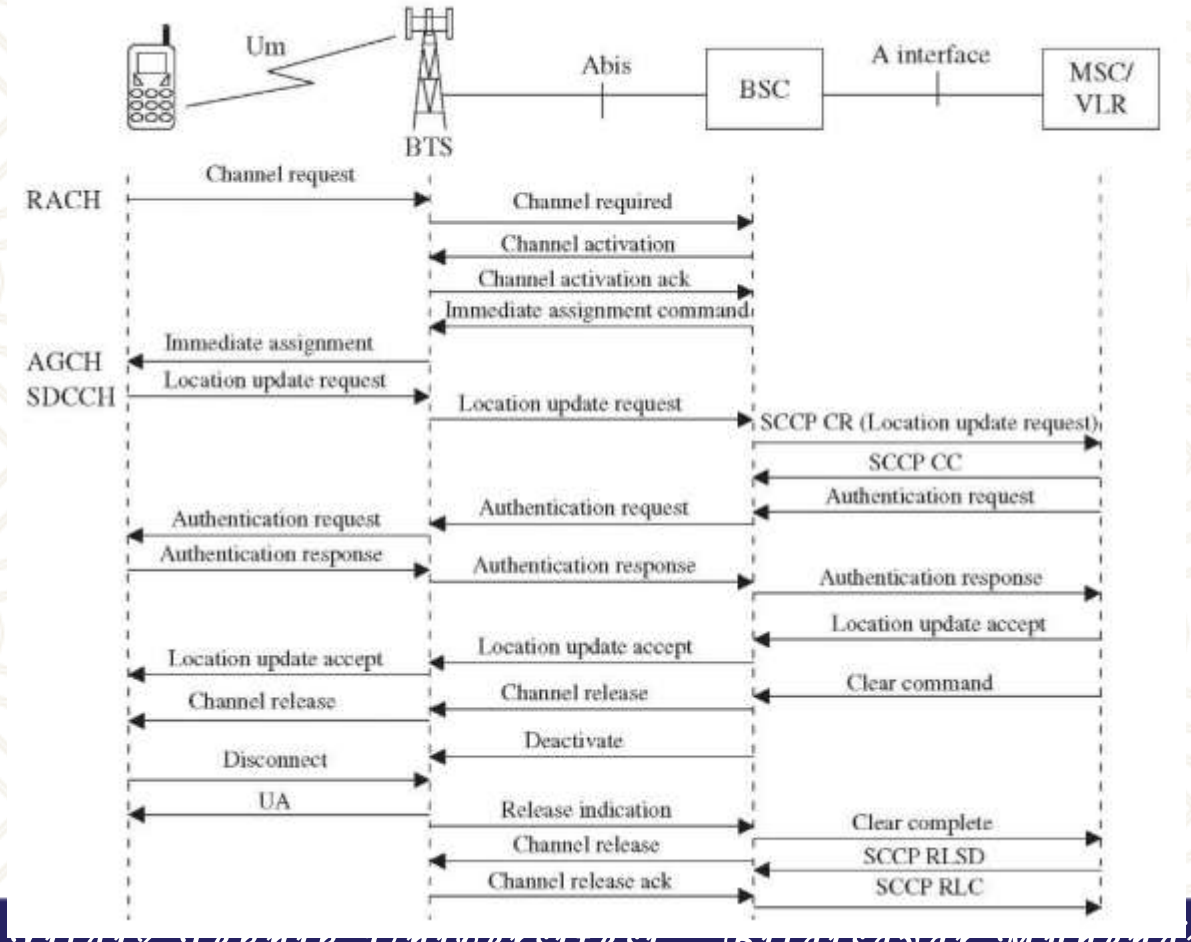
- GSM Attach/Detach or IMSI Attach/Detach is done only if you switch ON and switch OFF your cell phone…
- First synchronize with frequency (FCCH Channel) then time synchronization (SCH Channel) and then you start getting information about your network (BCCH Channel).
- The MSC/VLR is now set the flag as you are now attached…
- if you were there under this MSC/VLR before, what happens is that the state changes from the detach to attach.
- When MSC finds that the MS is new MS that is there is no any kind of entry for this particular MS in VLR then the MSC will ask HLR…
  - The HLR will forward the IMSI to the Authentication Center (AuC) and request authentication triplets.
  - The AuC generates the triplets and sends them along with the IMSI, back to the HLR.

GSM Attach Cont'd

- The HLR validates the IMSI by ensuring it is allowed on the network and is allowed subscriber services. It then forwards the IMSI and Triplets to the MSC/VLR.
- The MSC/VLR stores the SRES and the Kc and forwards the RAND to the BSS and orders the BSS to authenticate the MS.
- The BSS sends the MS an Authentication Request message. The only parameter sent in the message is the RAND.
- The MS uses the RAND to calculate the SRES and sends the SRES back to the BSS on the SDCCH in an Authentication Response. The BSS forwards the SRES up to the MSC/VLR.
- The MSC/VLR compares the SRES generated by the AuC with the SRES generated by the MS. If they match, then authentication is completed successfully.
- The MSC/VLR forwards the Kc for the MS to the BSS. **The Kc is NOT sent across the Air Interface to the MS**. The BSS stores the Kc and forwards the Set Cipher Mode command to the MS. The CIPH_MOD_CMD only tells the MS which encryption to use (A5/X), no other information is included.
- The MS immediately switches to cipher mode using the A5 encryption algorithm. All transmissions are now enciphered. It sends a Ciphering Mode Complete message to the BSS.
- The MSC/VLR sends a Location Updating Accept message to the BSS. It also generates a new TMSI for the MS. TMSI assignment is a function of the VLR. The BSS will either send the TMSI in the LOC_UPD_ACC message or it will send a separate TMSI Reallocation Command message. In both cases, since the Air Interface is now in cipher mode, the TMSI is not compromised.
- The MS sends a TMSI Reallocation Complete message up to the MSC/VLR.
- The BSS instructs the MS to go into idle mode by sending it a Channel Release message. The BSS then de-assigns the SDCCH.
- The MSC/VLR sends an Update Location message to the HLR. The HLR records which MSC/VLR the MS is currently in, so it knows which MSC to point to when it is queried for the location of the MS.



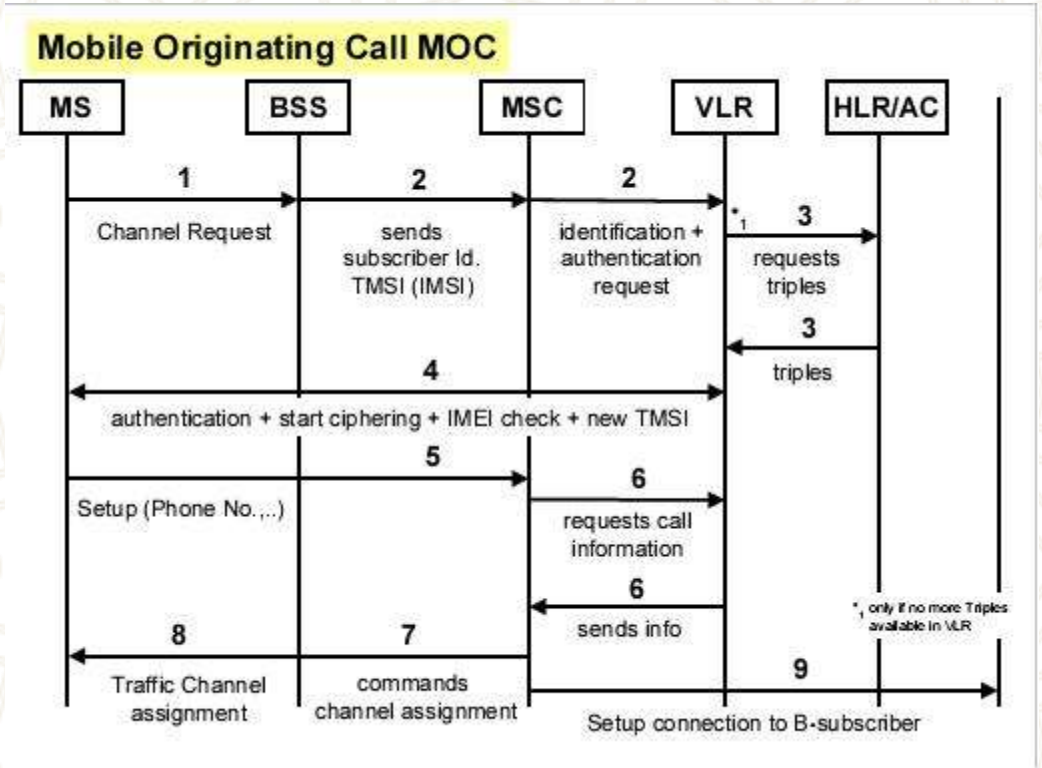
Location Update



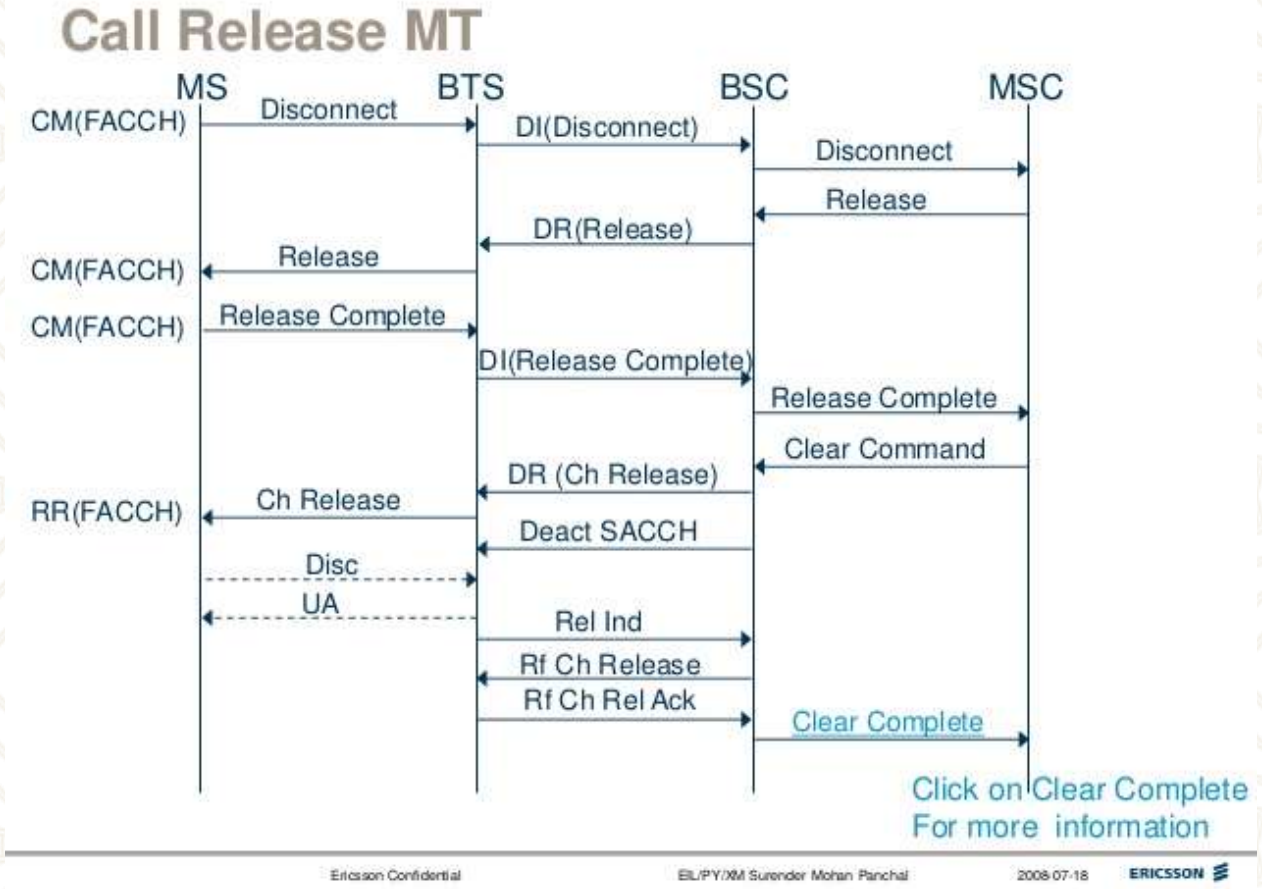
- There are three different location-updating scenarios.
  - **Attach/initial registration**, used when a mobile is turned on
  - **Normal/forced registration,** initiated when a mobile station moves to a new location area
  - **Periodic updates**, regular location updates on expiry of a timer. This is required to track those mobile stations the locations of which may be lost because of some reason.

Mobile Oriented Call

- The MS requests for the allocation of a dedicated signaling channel to perform the call setup.
- After allocation of a signaling channel the request for MOC call setup, included the TMSI (IMSI) and the last LAI, is forwarded to the VLR
- The VLR requests the AC via HLR for Triples (if necessary).
- The VLR initiates Authentication, Cipher start, IMEI check (optional) and TMSI Re-allocation (optional).
- If all this procedures have been successful, MS sends the Setup information (number of requested subscriber and detailed service description) to the MSC.
- The MSC requests the VLR to check from the subscriber data whether the requested service an number can be handled (or if there are restrictions which do not allow further proceeding of the call setup)
- If the VLR indicates that the call should be proceeded, the MSC commands the BSC to assign a Traffic Channel (i.e. resources for speech data transmission) to the MS
- The BSC assigns a Traffic Channel TCH to the MS
- The MSC sets up the connection to requested number (called party).

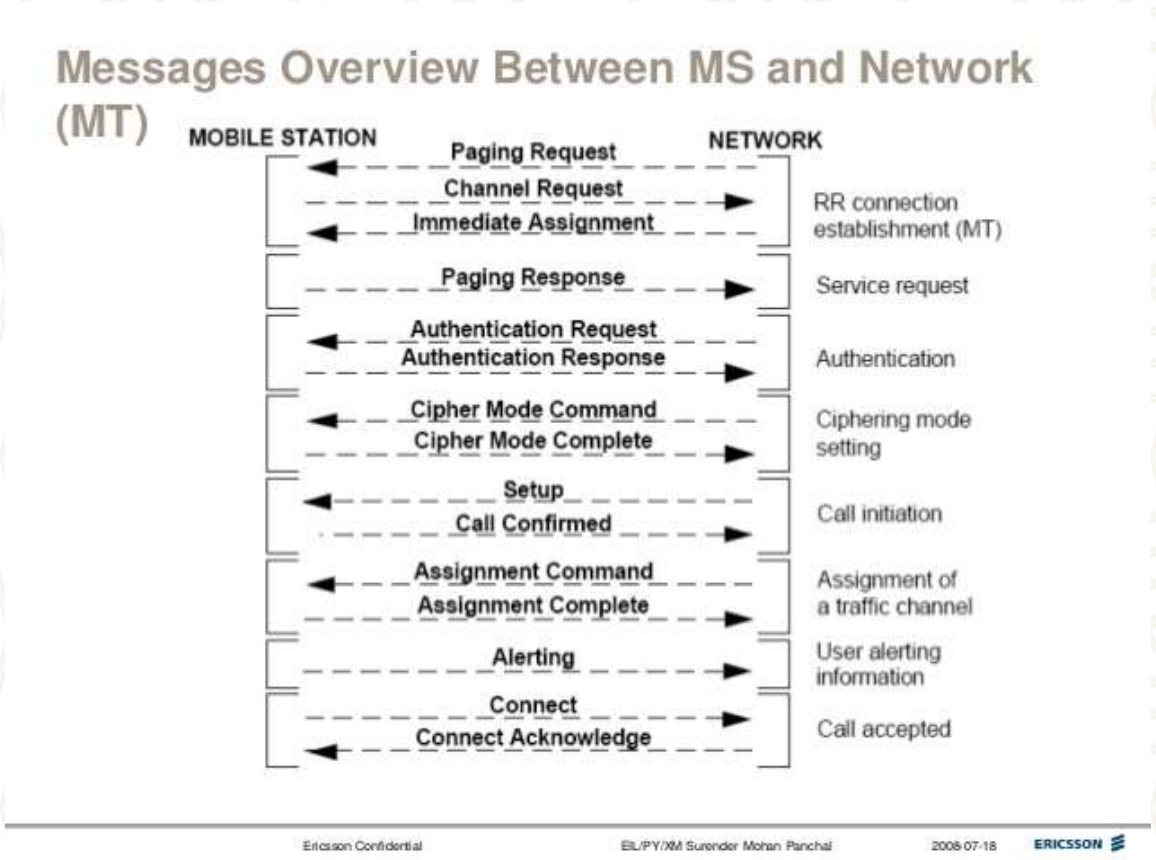


Call Release

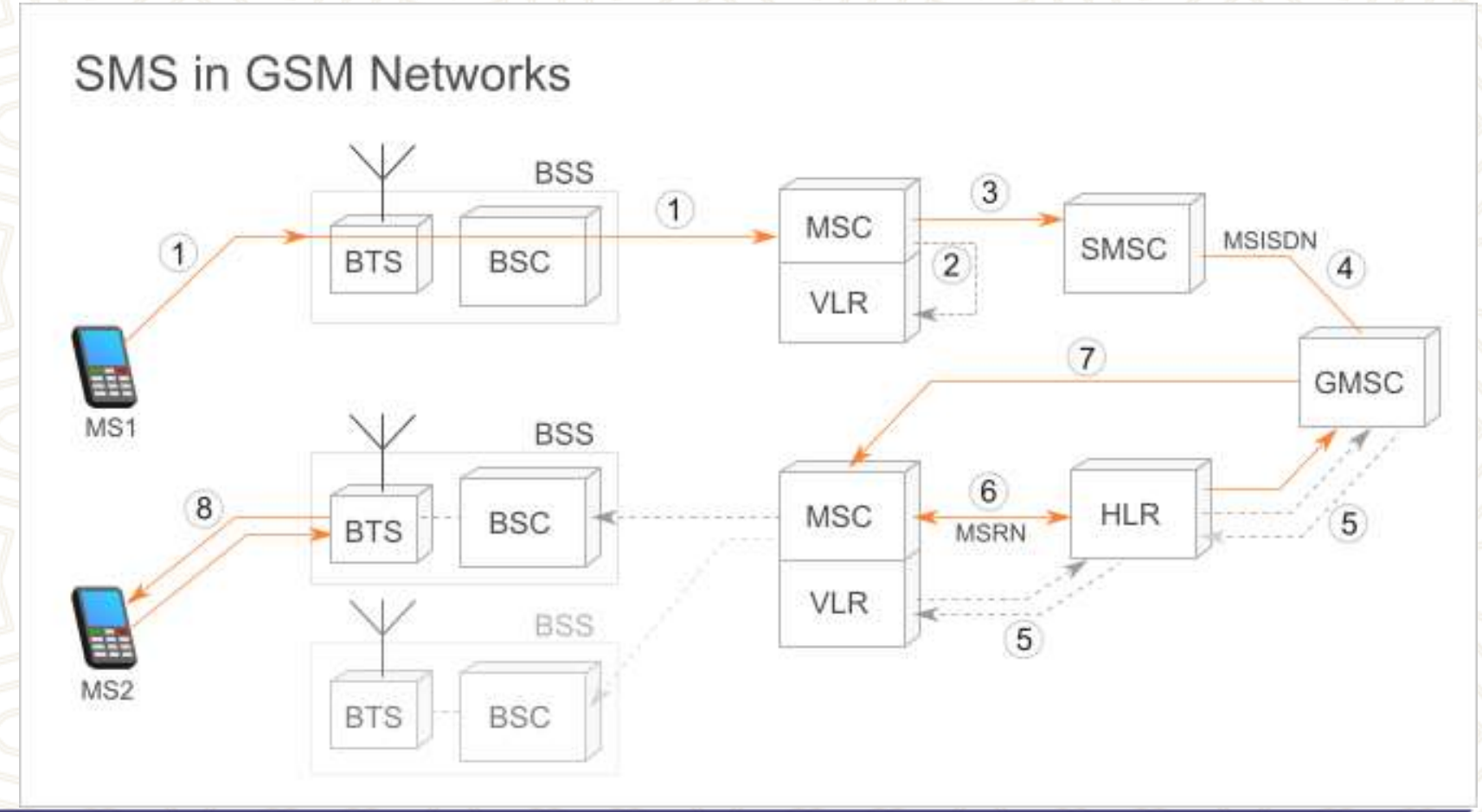


http://www.slideshare.net/gstoynov/gsmcallflow-39142890

Mobile Terminated Call



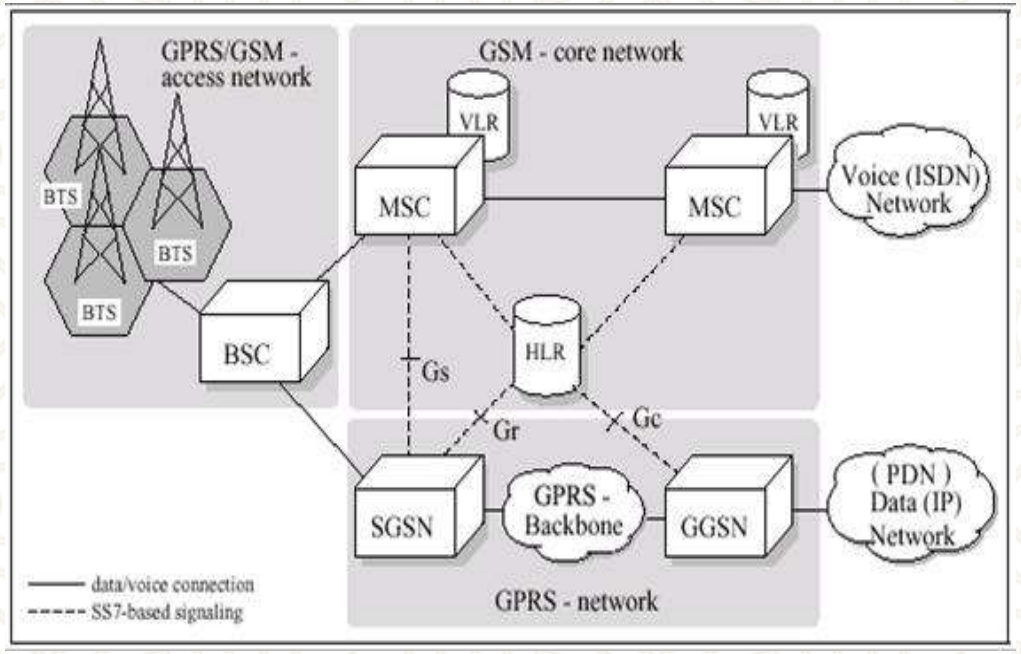
SMS Flow


SMS in GSM Networks
BSS
BTS
BSC
MS1
MS2
MSC
VLR
SMSC
GMSC
HLR
MSISDN
MSRN
1
2
3
4
5
6
7
8

Packet Domain

- GSM™ is a circuit-switched network;
  - ideal for the delivery of voice but with limitations for sending data.
- In 2000 the introduction of General Packet Radio Service (GPRS) added packet-switched functionality and ‘kick started’ the delivery of the Internet on mobile handsets.
  - in Release 97, GPRS typically reached speeds of 40Kbps in the downlink and 14Kbps in the uplink by aggregating GSM time slots into one bearer.
  - Enhancements in Releases R’98 and R’99 meant that GPRS could theoretically reach downlink speeds of up to 171Kbps.
- The next advance in GSM radio access technology was EDGE (Enhanced Data rates for Global Evolution) or Enhanced GRPS.
  - a new modulation technique yielding a three-fold increase in bit rate (8PSK replacing GMSK) and new channel coding for spectral efficiency,

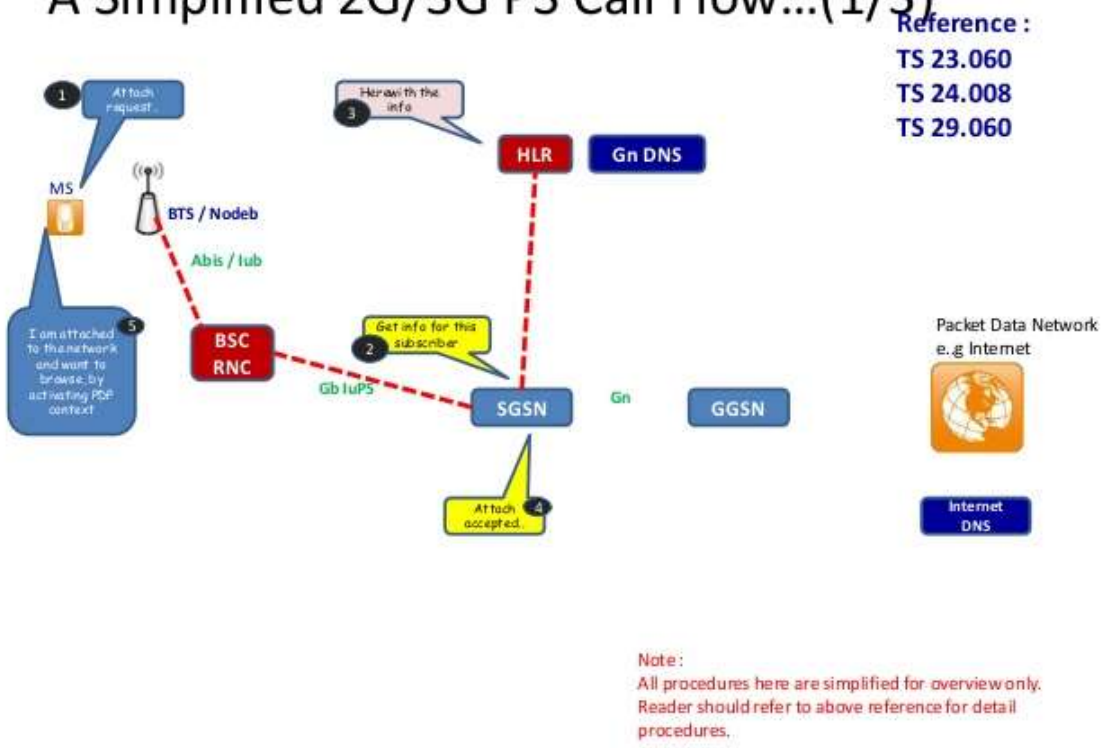
Packet Domain



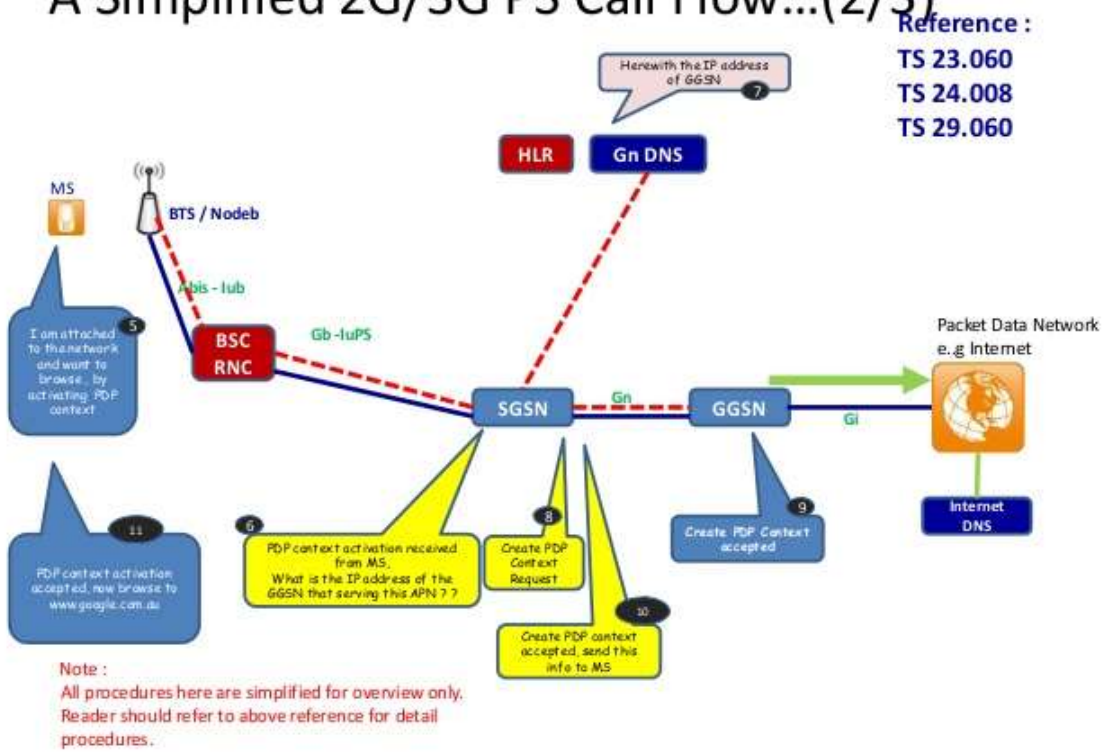
- *Serving GPRS Support Node (*SGSN)
  - authentication of GPRS mobiles
  - handles the registration of the mobile
  - takes care of its mobility management.
- Gateway GPRS Support Node (GGSN)
  - responsible for the interworking between the GPRS network and external packet switched networks, like the Internet and X.25 networks.
  - GGSN keeps a record of active mobile users and the SGSN the mobile users are attached to. It allocates IP addresses to mobile users and last but not least, the GGSN is responsible for the billing.

2G/3G PS Call Flow

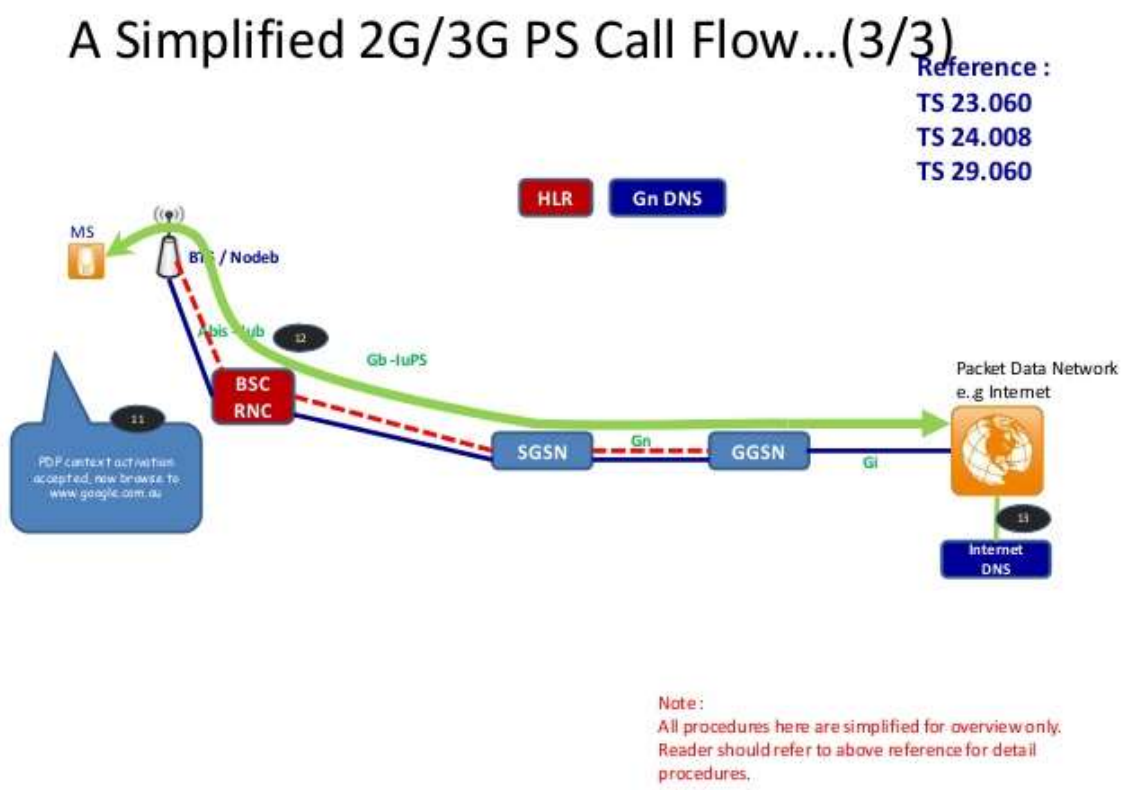
A Simplified 2G/3G PS Call Flow...(1/3)



A Simplified 2G/3G PS Call Flow...(2/3)

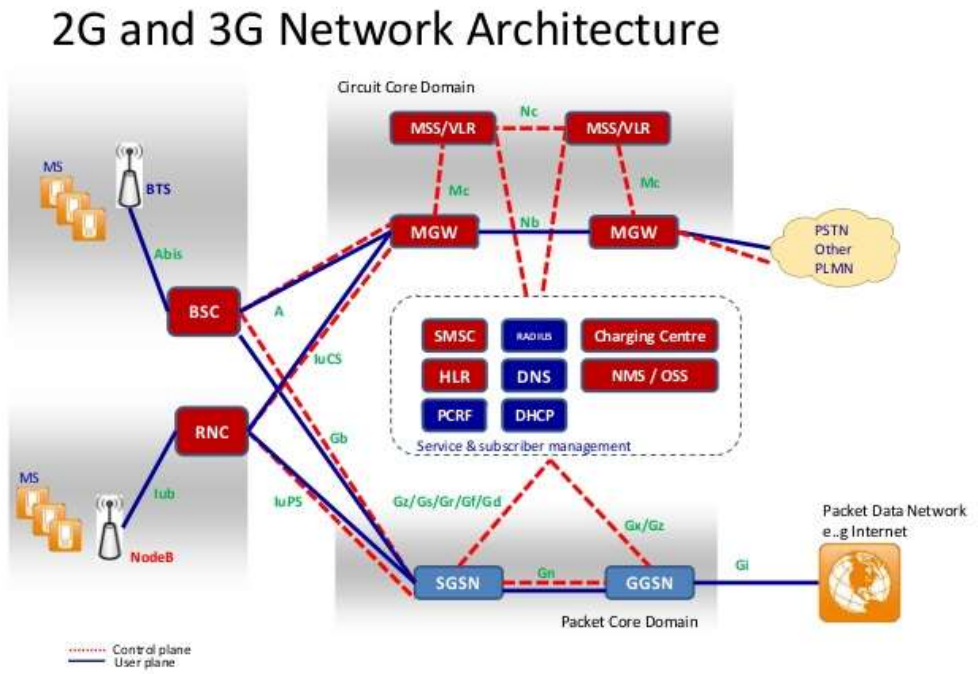


2G/3G PS Call Flow Cont'd



- Attach request (1)
  - Request sent to SGSN (2)
  - SGSN ask HLR for info (3)
  - Attach Accepted (4)
- Initiate PDP context (5)
  - activation received SGSN(6)
  - look up for IP address of the GGSN for that APN (7)
  - forward request to GGSN (8)
  - PDP context created (9)
  - send info to MS
- browse Internet (10)

Newer Technologies – 3G / UMTS

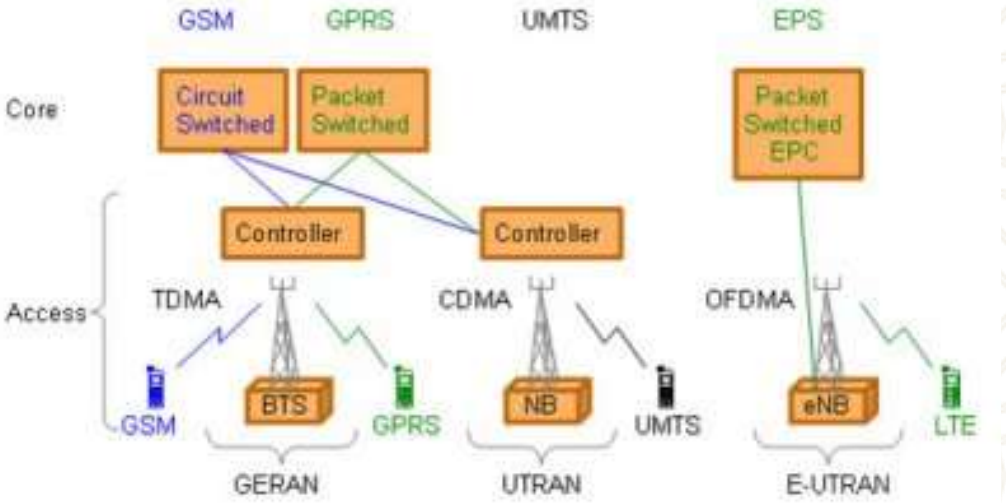


- Core Network is an evolution from the GSM core.
- Base Station Subsystem (BSS) become Radio Access Network (RAN)
  - BTS become NodeB
  - BSC become Radio Network Controller (RNC)

Universal Mobile Telecommunications System

- UMTS is an umbrella term for the third generation radio technologies developed within 3GPP.
  - optimizations in Radio Access Network (RAN)
  - more access-agnostic core network
- UMTS includes the original W-CDMA scheme using paired or unpaired 5 MHz wide channels in globally agreed bandwidth around 2 GHz,
  - though subsequently, further bandwidth has been allocated by the ITU on a regional basis.
  - Both Frequency Division Duplex (FDD) and Time Division Duplex (TDD) variants are supported.
  - W-CDMA was specified in Release 99 and Release 4 of the specifications. High Speed Packet Access (HSPA) was introduced in Releases 5 (Downlink) and 6 (Uplink).

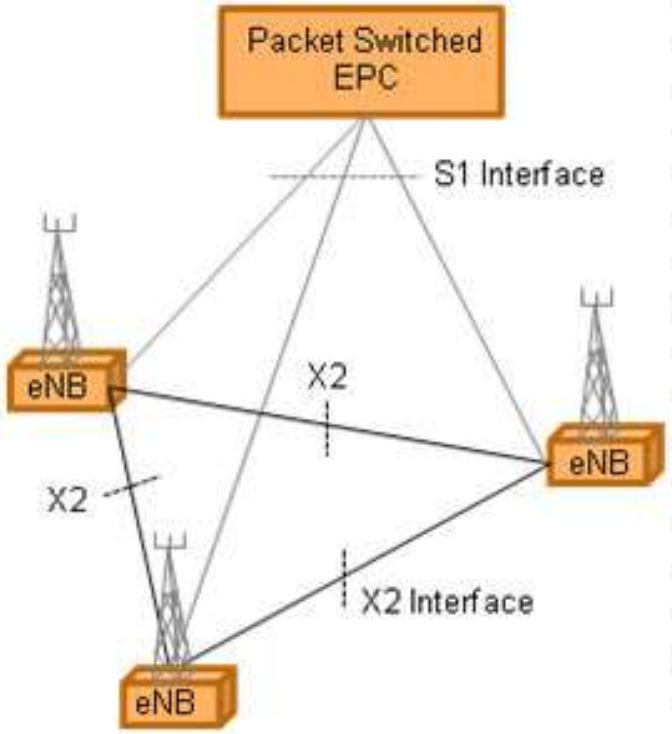
Long Term Evolution



- The Evolved Packet System (EPS) is purely IP based.
  - *Both real time services and datacom services will be carried by the IP protocol.*
  - *The IP address is allocated when the mobile is switched on and released when switched off.*

- LTE or the E-UTRAN (Evolved Universal Terrestrial Access Network), introduced in 3GPP R8.
  - it is the access part of the Evolved Packet System (EPS)
- A new access technology WCDMA (Wideband Code Division Multiple Access) was developed
- Incoming datacom services are therefore still relying upon the circuit switched core for paging.

Long Term Evolution (LTE)



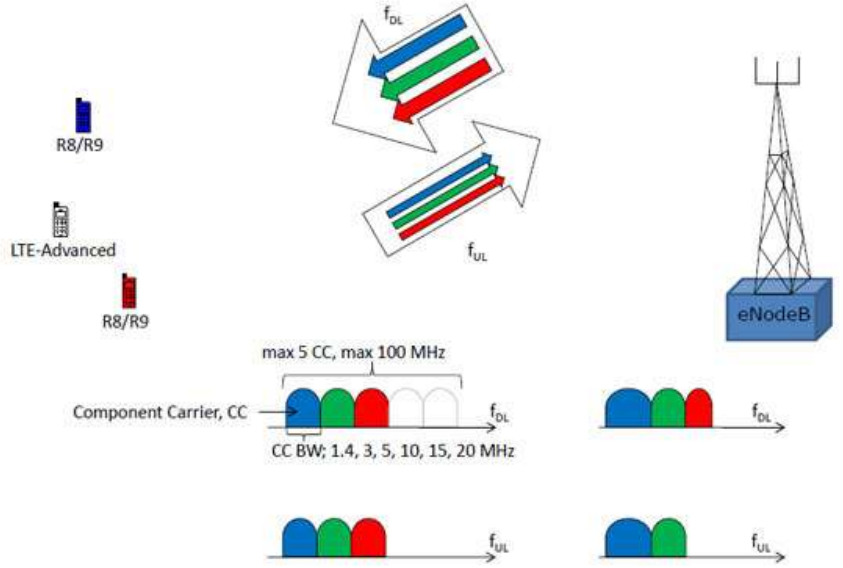
- The LTE access network is simply a network of base stations, evolved NodeB (eNB), generating a flat architecture.
- The eNBs are normally inter-connected via the X2-interface and towards the core network by the S1-interface.
  - to speed up the connection set-up and reduce the time required for a handover.
- MAC protocol layer, which is responsible for scheduling, is represented only in the UE and in the base station leading to fast communication and decisions between the eNB and the UE.
- In UMTS the MAC protocol, and scheduling, is located in the controller
  - when HSDPA was introduced an additional MAC sub-layer, responsible for HSPA scheduling was added in the NodeB.

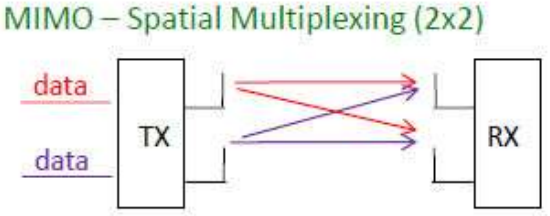
Long Term Evolution (LTE)

- The scheduler is a key component for the achievement of a fast adjusted and efficiently utilized radio resource. The Transmission Time Interval (TTI) is set to only 1 ms.
- During each TTI the eNB scheduler shall:
  - The UEs report their perceived radio quality, as an input to the scheduler to decide which Modulation and Coding scheme to use. The solution relies on rapid adaptation to channel variations, employing HARQ (Hybrid Automatic Repeat Request) with soft-combining and rate adaptation.
  - prioritize the QoS service requirements amongst the UEs.
    - delay sensitive real-time services
    - datacom services requiring high data peak rates.
  - inform the UEs of allocated radio resources.
    - The eNB schedules the UEs both on the downlink and on the uplink.
    - For each UE scheduled in a TTI the user data will be carried in a Transport Block (TB).
    - **The TB is delivered on a transport channel. In LTE the number of channels is decreased compare to UMTS.**

Long Term Evolution - Advanced

- Carrier Aggregation
  - the increase in bandwidth is provided through aggregation of R8/R9 carriers.
  - Carrier aggregation can be used for both FDD and TDD
- MIMO
  - Multiple Input Multiple Output
  - MIMO can be used when S/N is high
- Relay Nodes (RN)
  - are low power base stations that will provide enhanced coverage and capacity at cell edges, and hot-spot areas
  - it can also be used to connect to remote areas without fibre connection. The Relay Node is connected to the Donor eNB (DeNB) via a radio interface
- Coordinated Multi Point operation
  - introduced in R11





Security in GSM

- On air interface,
  - GSM uses encryption and TMSI instead of IMSI
- SIM is provided 4-8 digit PIN
  - validate the ownership of SIM
- 3 algorithms
  - A3 algorithm for authentication
  - A5 algorithm for encryption
  - A8 algorithm for encryption

GSM Attacks

- Crypto-attacks
  - main goal is to capture IMSI, Ki, Kc,
  - depends on weakness of COMP128 (implementation of A3/8)
  - **outcome can be used in DoS attacks**
- Denial Of Service (DoS) attacks
  - network design
    - smart network & dumb terminals
    - procedures computationally light for terminals, resource consuming for the network!
  - repeating procedures overload the network
    - several points to attack

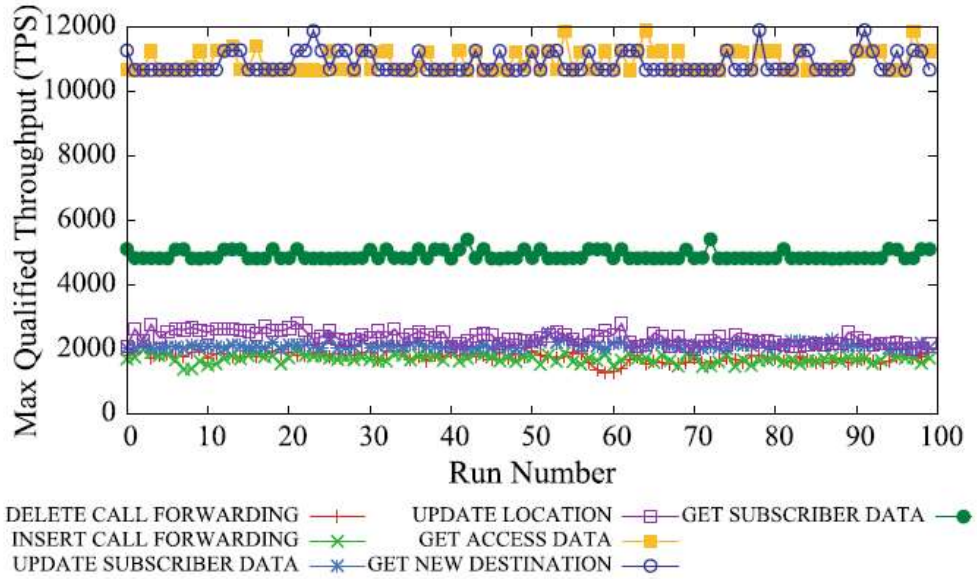
GSM DoS Attack #1*

- Remember “**attach to network**” procedure
- An unauthenticated device may force the core network to carry on computations that are **more resource consuming** than the request itself.
- Build a database of valid IMSIs
- Flood the network with attach requests each one carrying a different IMSI
  - network forwards these request to HLR/AuC
  - triggers the calculation of authentication information, since each IMSI is validated
  - authentication information passed to SGSN
  - SGSN submits challenge back to the mobile station

- *Khan, Muzammil, Attiq Ahmed, and Ahmad Raza Cheema. "Vulnerabilities of UMTS access domain security architecture." *Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008. SNPD'08. Ninth ACIS International Conference on*. IEEE, 2008.

GSM DoS Attack #2*

- Targeting HLR !
  - repeatedly injecting resource demanding transactions
- Which transaction !?
  - Transaction per Second (TPS)
  - **INSERT CALL FORWARDING**
- A botnet of authenticated devices
  - tested on simulation environment
  - disregards AuC calculations
  - 2500 TPS is enough to reduce HLR capabilities by 95%



- *Traynor, Patrick, et al. "On cellular botnets: measuring the impact of malicious devices on a cellular network core." *Proceedings of the 16th ACM conference on Computer and communications security*. ACM, 2009.

More to Read !!

- Khan, Muzammil, Attiq Ahmed, and Ahmad Raza Cheema. "Vulnerabilities of UMTS access domain security architecture." *Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008. SNPD'08. Ninth ACIS International Conference on*. IEEE, 2008
- Gobbo, Nicola, Alessio Merlo, and Mauro Migliardi. "A denial of service attack to GSM networks via attach procedure." *Security Engineering and Intelligence Informatics*. Springer Berlin Heidelberg, 2013. 361-376.
- Traynor, Patrick, et al. "On cellular botnets: measuring the impact of malicious devices on a cellular network core." *Proceedings of the 16th ACM conference on Computer and communications security*. ACM, 2009.
- http://www.ipt.etsi.org/iptlib/iptLib/BaseDocs/3GPP23.060.htm
- http://www.rfwireless-world.com/Terminology/GSM-combined-channel-configuration.html
- http://www.3gpp.org/technologies/keywords-acronyms/97-lte-advanced
- http://www.3gpp.org/technologies/keywords-acronyms/98-lte
- http://wiki.yatebts.com/index.php/GSM_Functionalities