Machine-to-Machine Communication: A 3GPP Security Perspective

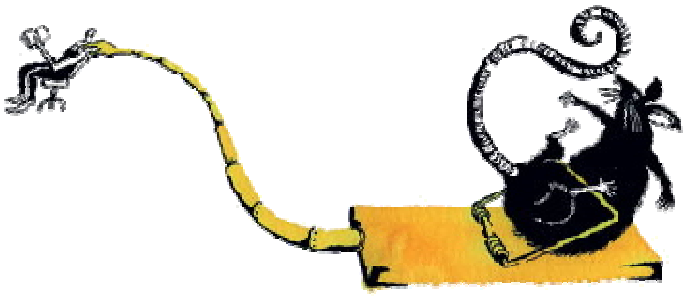
Company: NEC Corporation
Author: Anand R. Prasad
Contact information: anand@bq.jp.nec.com
Purpose: Discussion

Abstract

This presentation gives an introduction to M2M and standardization activities in 3GPP. The presentation concludes with thoughts on 3GPP M2M security activities and way forward for GISFI IoT work with the proposal to continue the mHealth standardization work.

Outline

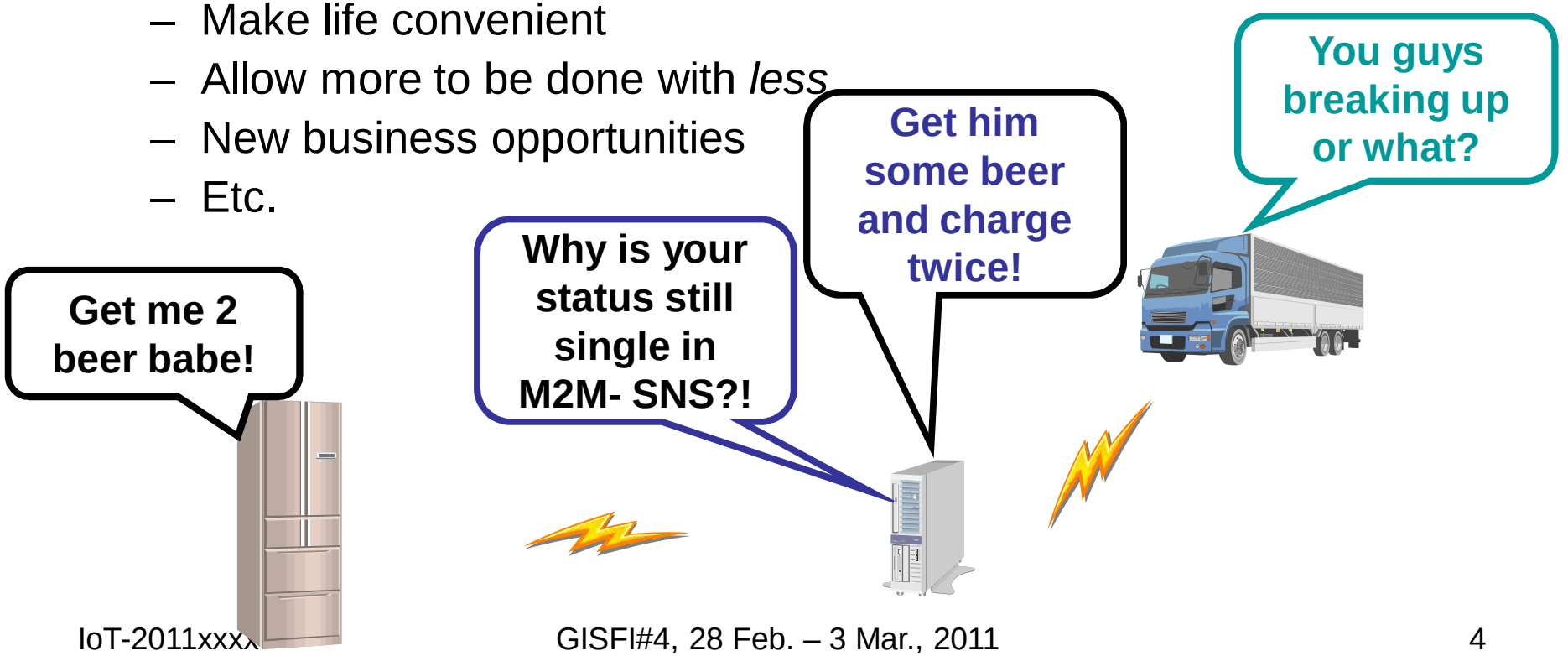
- Background and Introduction
- 3GPP activities on M2M
- Security study on 3GPP features
- Conclusions
- GISFI mHealth work time-plan



Figures source: The Economist, Wireless Incorporated, Apr. 26, 2007

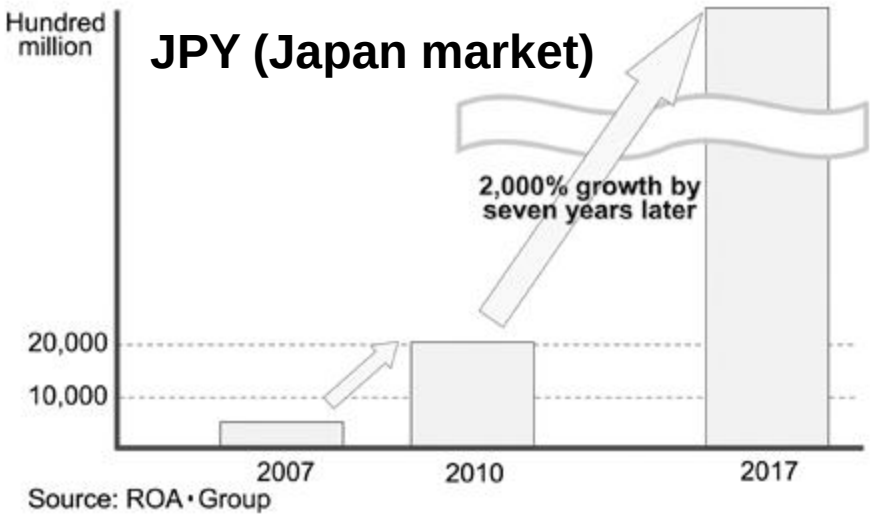
What are we talking about?

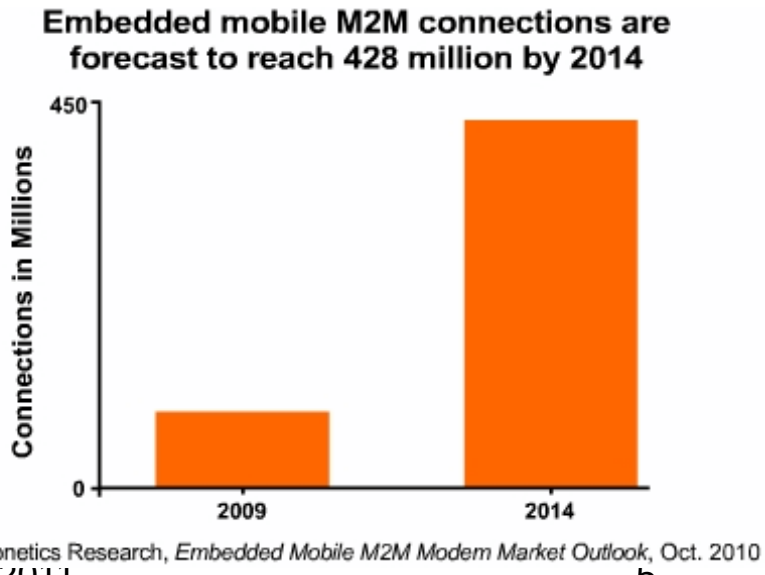
- Communication between machines without human intervention
- Why? Because there seems to be need of it
  - Make things cheaper
  - Make life convenient
  - Allow more to be done with *less*
  - New business opportunities
  - Etc.



M2M market?

- Mobile M2M market is mainly focused on fleet/asset management and some on smart metering
- GSM is the main technology in use
- Almost all major mobile operator worldwide is engaged in M2M business





© Infonetics Research, *Embedded Mobile M2M Modem Market Outlook*, Oct. 2010

Where can we use M2M?

- Farming
  - Irrigation
  - Fertilizer dosage
  - Pesticide dosage
- Healthcare
  - Monitoring
  - Health checks
  - Medication
- Vehicles
  - Accident
  - Charging
  - Traffic
  - In-vehicle comm.

Source: Monarchbearing.com / growingpower.org

Source: REVAi from Wikipedia

Several uses leading to large number of devices

Example: 600M houses with 3 utilities and 6 M2M devices = 5.4B M2M devices

What is needed? What it brings?

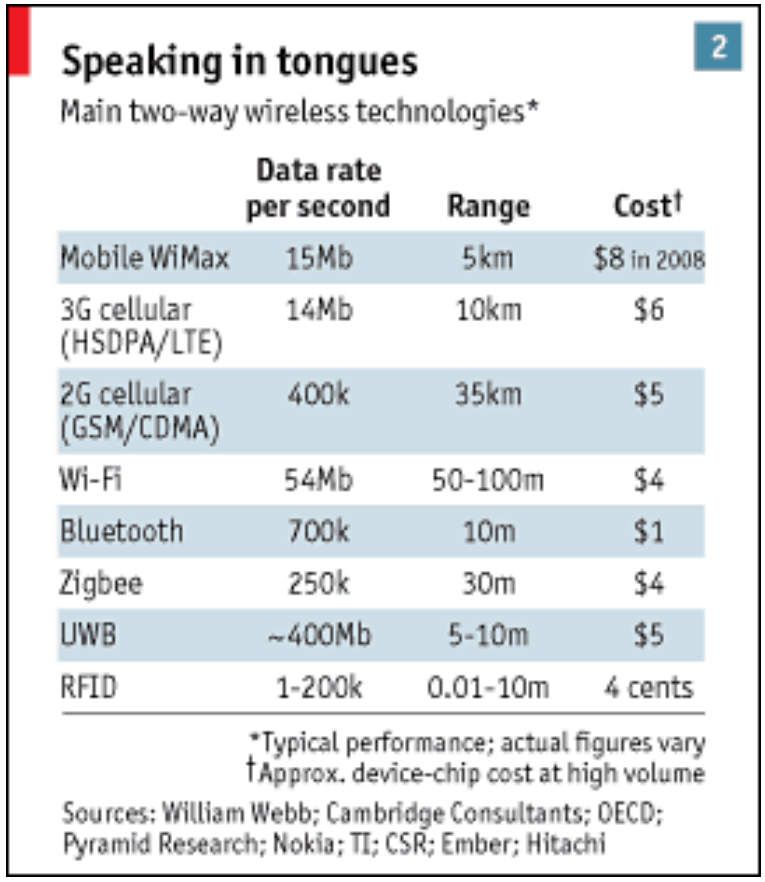
	Data-rate	Data-volume	Accuracy	Security	Cost	Time Sensitivity	Traffic Nature	Infrastructure and/or Ad-hoc	Always-on / connected
Healthcare	Low to High	Low to High	High	High	Low to High	High	Sporadic & Periodic	Both	Yes
Farming	Low	Low	Medium	Low	Low	Low to Medium	Sporadic & Periodic	Infrastructure	No
Vehicle	Low	Low	Medium to High	High	Low	High	Sporadic & Periodic	Both	Yes
Vending machine	Low	Low	Medium	Medium	Low	Low	Periodic	Infrastructure	No
Content mgt.	High	High	High	Low to High	Low	Low to Medium	Periodic	Infrastructure	No
Utilities	Low	Low	High	Medium	Low	Low	Periodic	Infrastructure	Yes
Home electronics	Low to High	Low to High	Medium	Medium	Low	Low to High	Continuous & Periodic	Both	Yes/No

Issues

- Heterogeneous radio access technologies needed
- Huge network load – predictable and unpredictable
- Varying requirements for Security and QoS – service differentiation needed
- Management complexities
- Deployment
- Compatibility – backward / forward?
- Robust solutions / products – usability, weather etc.
- Scalability

Varying requirements

What can be used?



Speaking in tongues 2

Main two-way wireless technologies*

	Data rate per second	Range	Cost†
Mobile WiMax	15Mb	5km	$8 in 2008
3G cellular (HSDPA/LTE)	14Mb	10km	$6
2G cellular (GSM/CDMA)	400k	35km	$5
Wi-Fi	54Mb	50-100m	$4
Bluetooth	700k	10m	$1
Zigbee	250k	30m	$4
UWB	~400Mb	5-10m	$5
RFID	1-200k	0.01-10m	4 cents

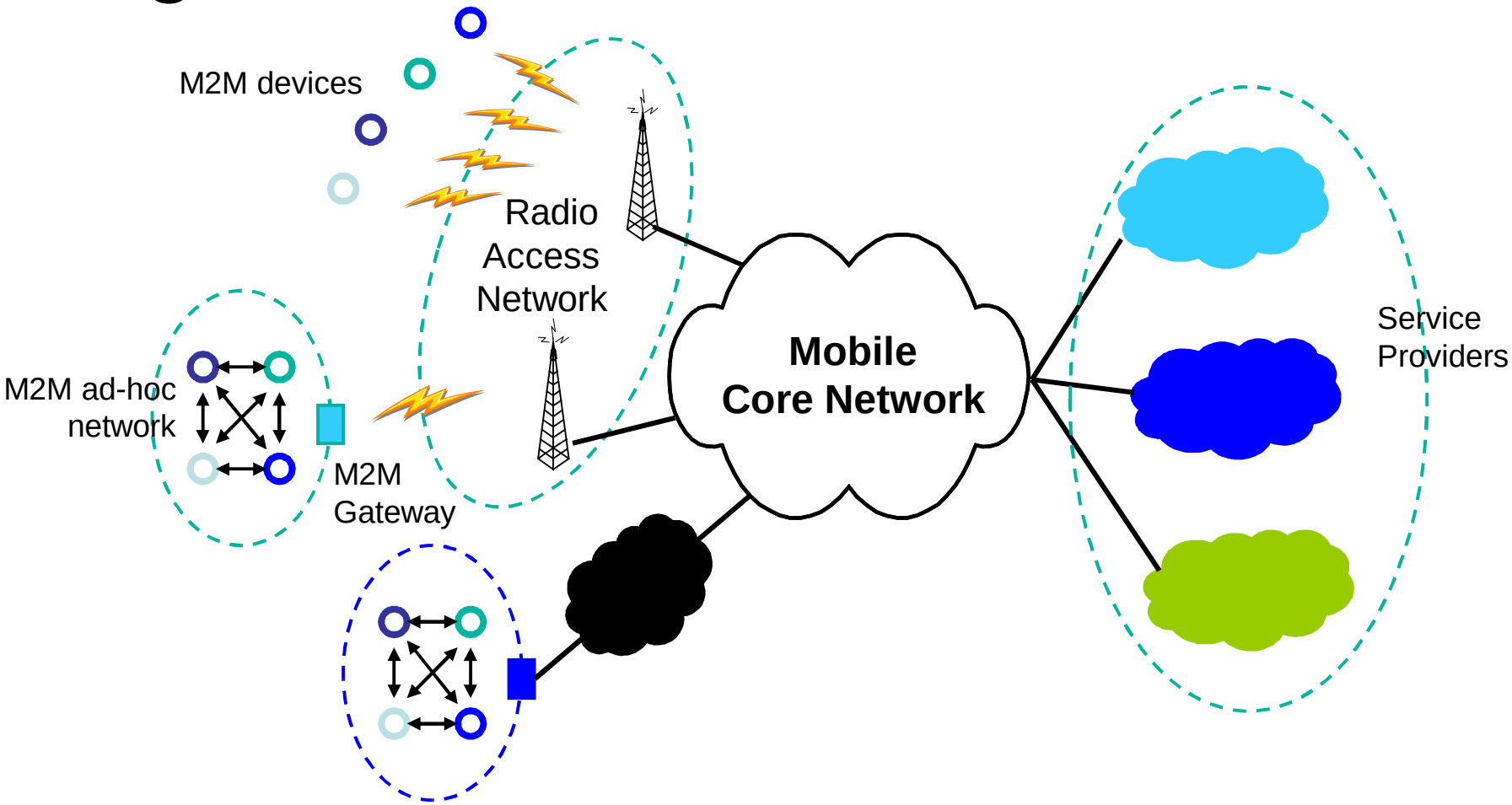
*Typical performance; actual figures vary
†Approx. device-chip cost at high volume

Sources: William Webb; Cambridge Consultants; OECD; Pyramid Research; Nokia; TI; CSR; Ember; Hitachi

Source: On the radio: Wireless takes many forms; Apr. 26, 2007, The Economist

Contradiction in features & requirements
Necessitates careful consideration of technology combination or Enhancement of existing technologies (can we enhance LTE to do it all)?

High level architecture?



Capacity consideration at all interfaces and network elements
Dense deployment of radio network – optimize from beginning
Varying security requirements

Business relations

Players (e.g., smart metering service)

- **Smart-card vendors**
- **Software and hardware vendors**
- **System integrators**
- **Network providers**: Mobile network operator (MNO)
- **Service transporters**: Mobile virtual network operator (MVNO)
- **Service owners**: Electricity company
- **Service providers**: M2M service provisioning company
- **Subscribers**: Land-lord of your rented apartment
- **Users**: Electricity meter in your apartment and you

Roles can change or merge
Creating dynamic business environment

Security is dependent on business and role of stakeholders

What are the standards doing?

Strategic Direction: Avoid Duplication

Examples of Current M2M-related Standardization Work (1):

- **3GPP** http://www.3gpp.org/ftp/Information/WORK_PLAN/Description_Releases/NIMTC_M2M_20100621.zip
- **3GPP2** TR50-20100617-004_ALU__LS 3GPP2 M2M Updates.ppt
- **CCSA's Ubiquitous Network Technical Committee** http://www.ccsa.org.cn/english/show_article.php?article_id=cyzx_a20c92a3-7c03-8a7e-5f3c-4b944cba3345
- **ETSI General M2M Activities (TC M2M)** http://www.etsi.org/Application/Search/?search=m2m
- **ETSI and Smart Card Platform work related to M2M** http://portal.etsi.org/scp/ActivityReport2009.asp
- **EU-funded project CASAGRAS** ('Coordination and support action for standardisation') http://cordis.europa.eu/search/index.cfm?fuseaction=
- **GISFI's Work on Specs for Standardized Framework on Internet** http://gisfi.org/pdf/IOT%20Work%20Plan.pdf
- **ITU Mobile Wireless Access Systems for sensors and/or actuators** Working parties 1a and 5D,ITU-T JCA-NID, ITU-T SG 16, ITU-T SG 17, and External orga providing telecommunications for a large number of ubiquitous sensors and/or actuators s service"
- **ITU-T Study Group 15 Optical transport networks and access netv** http://www.itu.int/ITU-T/studygroups/com15/index.asp
- **Open Mobile Alliance Device Management** http://www.openmobileal

Strategic Direction: Avoid Duplication

Examples of Current M2M-related Standardization Work (2):

- **GSMA Embedded Mobile Initiative** http://www.gsmwor work/mobile_broadband/embedded_mobile/
- **Wi-Fi Alliance certification programs (IEEE 802.11)** ht
- **Bluetooth (IEEE 802.15.1)** https://www.bluetooth.org/ap
- **Zigbee Alliance (IEEE 802.15.4) M2M-related solution**
- **WIMAX(IEEE 802.16) project planning committee** http
- **GS1 standardization work** http://www.gs1.org/
- **IETF's Constrained Restful Environments (core)** https
- **Wavenis Open Standard Alliance** http://www.wavenis-
- **Work within World Wide Web Consortium (W3C)** http:
- **European Usenet project** http://ercim-news.ercim.eu/er service-networks

Strategic Direction: Avoid Duplication

Examples of Current M2M-related Standardization Work (3):

- **Transportation space**
  - **Vehicular Emergency Data Set (VEDS):** http://www.comcare.org/VEDS.html
  - **ISO TC 204 - ITS -** http://www.iso.org/iso/iso_technical_committee?commid=54706
  - **ERTICO ITS Europe** http://www.ertico.com/
  - **ITU and Standardization Activities for Intelligent Transport Systems** http://www.itu.int/dms_pub/itu-t/oth/23/01/T230100000080002PDFE.pdf
- **Smart Grid space**
  - **IEC TC 57 - Communication networks and systems for power utility automation.** http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=sea22.p&search=iecnumber&header=IEC&pubno=61850&part=&se=&submit=Submit
  - **NIST Smart Grid Interoperability Standards Project** http://www.nist.gov/smartgrid/
  - **ETSI and Smart Grid** http://docbox.etsi.org/Workshop/2010/201006_SMARTGRIDS/ELLOUMI_M2M.ppt
  - **IEEE 802.15 Smart Utility Networks (SUN)** http://www.ieee802.org/15/pub/TG4g.html
- **Healthcare space**
  - **ISO TC 215** http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=54960
  - **HL7.org** http://www.hl7.org/implement/standards/ansiapproved.cfm
  - **Continua Health Alliance** http://www.continuaalliance.org/index.html
  - **ISO/IEEE 11073 Personal Health Data (PHD) Standards** http://en.wikipedia.org/wiki/ISO/IEEE_11073_Personal_Health_Data_%28PHD%29_Standards
- **Home automation space**
  - **ISO/IEC JTC 1/SC 25/WG 1 – Home Electronic System** http://hes-standards.org/

Lots of activities worldwide. In this presentation focus is on 3GPP specifically on security.

Source: J. Smith "Telecommunications Industry Association (TIA) TR-50 Engineering Committee Activities & Recommendations"; GSC-15, August 30 – September 2, 2010, Beijing, China.

3GPP Activities

- 3GPP SA1 (Services)
  - TS 22.368 with use cases and requirements completed in Rel. 10
  - Defines general requirements and specific MTC Features
  - New study items
    - Alternatives to the use of E.164 for MTC
    - Study on enhancements for MTC in 3GPP TR 22.888
- 3GPP SA2 (Architecture)
  - 3GPP TR 23.888 on key issues identified in SA1 and proposed solutions
- 3GPP SA3 (Security)
  - Completed (stalled) one study on remote provisioning and change of subscription in TR 33.812
  - TR 33.868 being prepare as SA2 work enhances
- 3GPP RAN groups
  - Study on RAN Improvements for MTC in 3GPP TR 37.868 on hold
  - New Work Item “RAN mechanisms to avoid CN overload due to MTC”
- 3GPP GERAN groups
  - Study on GERAN Improvements for MTC in 3GPP TR 43.868

3GPP activity is still at early stage
Focus is on all 3GPP solutions starting from GSM

Partially taken from: T. Norp, “Mobile Network Improvements for Machine Type Communications”, ETSI TC M2M Workshop, 19-20 October 2010

3GPP SA1 M2M Features 1/2

- Low mobility: Devices that do not move or move infrequently
  - Network changes mobility management procedures and defines frequency of location update
- Time controlled: Apps that send/receive at defined time interval
  - Network communicates granted time interval and duration. Any access outside granted period can be charged separately.
- Time tolerant: Devices that can delay data transfer
  - Network can restrict device network access that can also be location dependent
- Packet switched only: For devices that require PS only
  - Services with or without MSISDN and accessible from MTC server with or without MSISDN – current services use SMS thus MSISDN
- Small data transmission: For devices that send or receive small amount of data
  - Minimal network impact and small data definition is configurable per subscriber or based on MNO policy
- Mobile originated only
  - Network can reduce mobility management procedures and configure it to call time only
- Infrequent mobile terminated
  - Network will be able to reduce mobility management procedure per device

3GPP SA1 M2M Features 2/2

- MTC monitoring: Related to device events
  - System detects: not aligned behavior, change in point of attachment, UE-UICC association change and loss of connectivity
  - User can define which events to observe and what the network should do
- Priority alarm: Alarm set on specific events, e.g. theft
  - Alarm even if normal service not possible and precedence over other features
- Secure connection: Between device and server
  - Network makes it possible even for roaming device
- Location specific trigger: Trigger devices when in specific area
  - Network initiates trigger based on area information provided to it
- Network provided destination for uplink data: All data to a IP address
  - Network provides and uses a IP address for uplink communication
- Infrequent transmission: Send / receive data infrequently – long period
  - Connection only when transmission and then sleep
- Group based MTC features: Optimize group handling and group feature is valid for all members of the group
  - Network enforces maximum bit rate for send/receive – network sets policy
  - Network can broadcast messages to group – group based addressing

Features are from mobile network perspective

3GPP Features and Security Concerns

- Security issues for all features
  - Change feature in the device
    - Configuration change in the device
    - Modify message from the network to device
  - Change in conditions for specific feature
- Requirements
  - Authorization based on feature setting
  - Access control of communication based on authorization
  - Means to identify modification in device

These are high level security issues and requirements
Focus is from technology perspective

3GPP Features Security Issues & Requirements

Nr.	Feature	Issue	Requirement
1	**Low mobility**	Attack (modification etc.) on messages with (1) mobility management procedure information (2) location update frequency	(1) Integrity protect the message, optionally give confidentiality (2) Device verification and validation
2	**Time controlled**	(1) Attack on message with time and interval and (2) Force device to communicate in charging period	Same as 1 and (2) Authenticate network (3) Security for interface between service provider and mobile network
3	**Time tolerant**	(1) Incorrect time and location information to device (2) Incorrect location information to network	Same as 2
4	**Packet switched only**	Attack on identity	Secure identity provisioning and management
5	**Small data transmission**	Attack on configuration regarding small data	Same as 1
6	**Infrequent mobile terminated**	(1) Attack on mobility management procedure (2) Unnecessary data to device	(1) Integrity protect the message, optionally give confidentiality (2) Authentication of network (3) Security between network and SP
7	**MTC monitoring**	(1) Attack on conditions (2) Attack on network behaviour	Same as 1 and (2) Secure user based management interface
8	**Priority alarm**	(1) Attack on condition for alarm (2) Create condition	Mechanims in network and device to judge validity of condition
9	**Secure connection**		All standard LTE requirements should be taken in account
10	**Location specific trigger**	(1) Incorrect setting in device (2) Incorrect location information to network	Same as 1
11	**Network provided destination for uplink data**	Attack on message with destination IP address	Same as 1
12	**Infrequent transmission**	(1) Incorrect time information to device (2) Force device communication for longer time and frequent intervals	Same as1
13	**Group based MTC feature**	(1) All group relaed issues: rogue device joining; attack on device removal (2) Issues regarding key management (3) Issues regarding addressing	Same as 2 and provide group based security solution

We need to check whether these requirements are fulfilled by GSM, UMTS and EPS (SAE/LTE)

We must also study scenarios of importance and security for them

Conclusions

- M2M market is expected to be huge – with time this certainly will be true
- There are lot's of benefits from M2M for India
  - Farming: Irrigation, fertilizer, pesticides etc.
  - Management: Population and country size makes all sorts of management far more complex be it utilities, traffic or pollution
  - Traffic and vehicles
- Cost is of high concern – simple and cheap systems with simple identification and payment solution is needed
- Security study in 3GPP is on-going with specific consideration for the requirement on backward compatibility with current deployments
- Deployment and market based security study and solutions must be studied + standardized
- M2M can play a major role in Green ICT

Conclusions: GISFI Steps

mHealth

Agreed during GISFI#3, proposal made by A.R. Prasad, NEC Corporation and V.M. Wadhai, MIT Pune

,□Health-20100018.zip

Supporters added during GISFI#3: Mr. Dua, COAI; Prof. Prasad, I4CT; Mini Vasudevan, Ericsson; Arpan Pal, TCS; B. Hooli, Individual member

1. Requirements: From service providers (healthcare professionals, IMA, hospitals etc.) and mobile network operators
   Deliverable: Technical report on mHealth requirements
   Time required: 2 meeting cycles (GISFI#5 to GISFI#6)
2. Gap analysis: Study what is already out there in India and elsewhere. Identify gaps.
   Deliverable: Technical report on Gap analysis
   Time required: 2 meeting cycles (GISFI#5 to GISFI#6)
3. Solution development: Develop solution based on gaps and requirements or bring to other standardization bodies on behalf of GISFI
   Deliverables:
   a. Architecture specification
      Time required: 4 meeting cycles (GISFI#6 to GISFI#9)
   b. Detail protocol specification
      Time required: 4 meeting cycles (GISFI#8 to GISFI#11)

GISFI meetings

- GISFI#5: 20-22 June 2011 Hyderabad, India
- GISFI#6: 27-29 Sept., 2011
- GISFI#7: 5-7 December, 2011
- GISFI#8: March, 2012