Empowered by Innovation NEC

3GPP's initial thoughts on *Machine to Machine communication*

Dr. Jörg Swetina
(joerg.swetina@nw.neclab.eu)

June 2008

History of M2M at 3GPP

a) Sept 2005: 3GPP SA1 starts a study on *" Facilitating Machine to Machine Communication in GSM and UMTS"*
   - ✓ finished in Rel-8 (2007) - TR 22.868

b) Sept. 2007: SA3 begins a study on *" Remote management of USIM application on M2M Equipment "*
   - ongoing

c) May 2008: a new work-item on *" Network Improvements for Machine-type Communications"* is agreed in 3GPP SA1.
   - Requirements will be based on the previous SA1 study, but aspects of (x)SIM are currently left out, waiting for input from GSMA, in consideration to the impact on the business models .

Related work:

- Sept 2006: workitem on *" Personal Network Management"*
  - Requirements done in 3GPP Rel-8, specification work continues into Rel-9.
- Sept 2006: workitem on *"eCall Data Transfer requirements"*

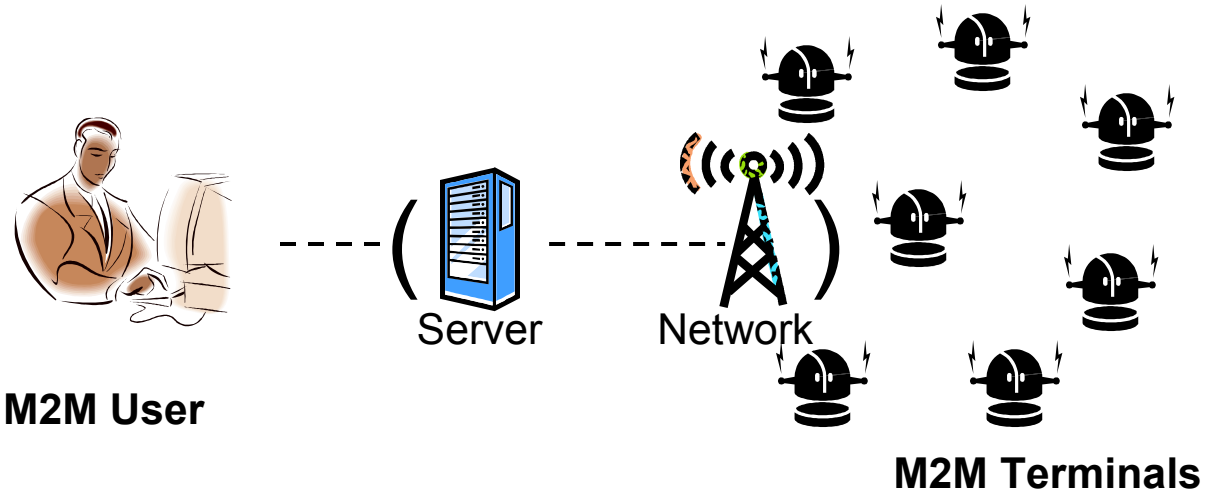
The 3GPP study in TR 22.868

"Enhancements to 3GPP systems to support machine to machine communication"

- Goals:
  - Investigate on improvements how 3GPP standards can be enhanced to provide network ***operators with lower operational costs*** when offering M2M services
  - Study how to ***lower the M2M users' effort*** associated with handling large M2M groups
  - Look at the ***trade-off between the effort and the benefits*** associated with the improvements
  - Identify potential ***requirements to facilitate improvements*** in M2M communication and the more efficient use of radio and network resources

Basic terms

- some definitions:
  - M2M Communication: a form of data communication between entities that do not necessarily need human interaction
  - M2M User: legal entity, i.e. company or person, that uses M2M terminals, usually the contractual partner for the operator
  - M2M Terminal: 3GPP terminal specifically adapted for M2M



Use cases

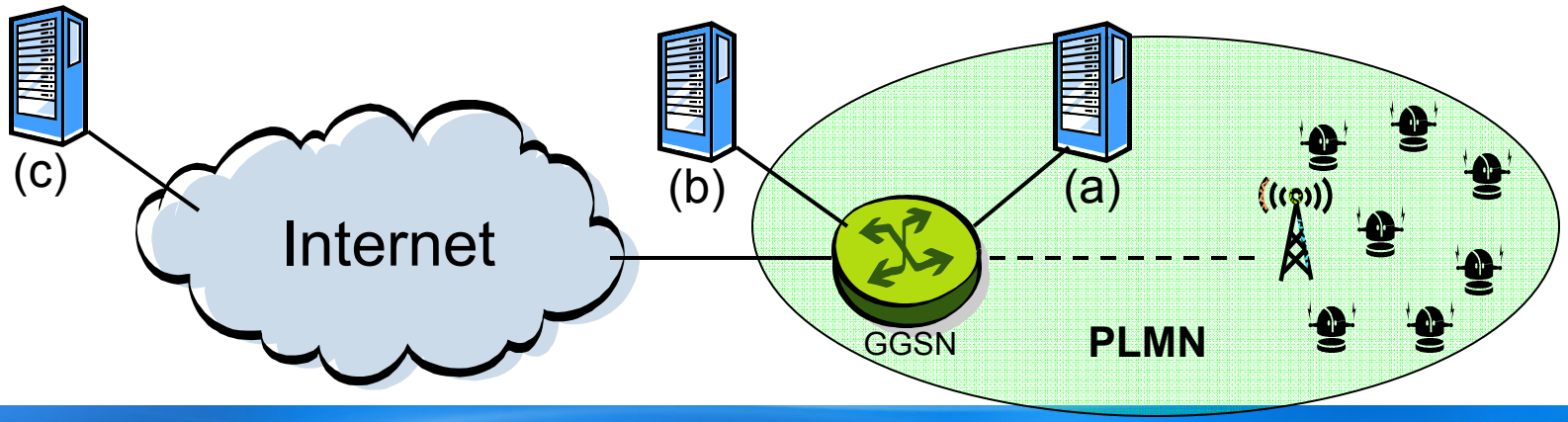
- Security, Tracking&Tracing, Payment, Health, Remote Maintenance/Control, Metering

  Examples:

  - "Pay as you drive" (car insurances base the premium on the usage of the car – exists in Italy, UK)
    => challenges: tampering, theft of UICC, fraud (e.g. deactivation)
  - "Tacking and theft detection" (e.g. for rental cars)
    => challenges: tampering/theft, long term reliability, possibility for the M2M user to change the subscription
  - Metering (e.g. remote metering of electricity consumption)
    => challenges: Metering device is usually untouched after installation for at least the next 8 years, low-volume and infrequent data transmissions, low (or no) mobility.

Communication scenarios

- 2 kinds of machines
  - Wireless modules (M2M terminals), connected via a RAN
  - Central servers
    a) within the operator (MNO) domain, giving the possibility for tight coupling to servers within MNO domain
    b) connected by a dedicated connection from GGSN (APN) to the server(s) and thus also routing and access control possibility at GGSN
    c) within general Internet, accessible via PDN (and ISP), i.e. without dedicated connection to the server(s)



Characteristics (topology) of data flows

- N:1 and N:M
  - Many wireless modules communicating with one (many) central server(s)
    - Currently prevailing commercial M2M operation mode
    - The machines are distinguishable from each other, i.e. outgoing messages (as seen by the central server) are not "broadcast"
    - For the first step, it is also considered sufficient that M2M communication is initiated by the M2M terminals only as most M2M scenarios run well with a pull type (by the M2M terminal) communication
    - Can be further restricted in that the group of M2M terminals belonging to one M2M user can communicate with one destination server only whose address is supplied by the network.
    - No single Tele-service or Bearer Service will satisfy all needs
- Peer-to-peer
  - [Many wireless modules communicating with each other (FFS)]

Issue 1: large numbers of terminals

- Operator perspective
  - Need for different subscription- and subscriber management (e.g. handling "N" terminals of a M2M user in one step)
  - save network signalling overhead (location update) for mobiles that are non-stationary and need not to be reachable i.e. use mobile originated traffic only (pull type).
  - mobility could be completely de-activated for e.g. mobiles that are stationary
- M2M User perspective
  - Tamper Save/Theft proof terminal including a UICC
  - change subscription out in the field e.g. after contract expiry without human intervention, (over the air) provisioning of USIM/ISIM parameters to a large number of M2M terminals
  - allocate the terminals at initial power up to a network operator without human intervention
- Personal Network Management (PNM) (TS 22.259) and Network Composition (NC) might also be applied to machine network management (MNM) communications.

Issue 2: Considerations on Charging

- traffic volume may vary by several orders of magnitude, e.g. from few bytes once a year to a few kilobytes every minute
  - Current charging mechanisms cause unnecessary overhead in creating at least 10 - 100 times longer CDRs than the payload for every few bytes transaction
  - Charging is considered sufficient to apply per group. Counters counting the traffic to and from the servers at the network boundary
- use of machine type subscription identifiers (e.g. always-on high security alarm systems, fixed location machines.)
  - Allows to differentiate machine to machine communications for optimised mobility management, call routing, security and charging purposes.
  - Allows to reduce administrative overhead at the operator (e.g. no need for Customer Care)

Issue 3: Considerations on Security

- Adaptation of Level of Security (balance between security provisions on the user side and those in the network)
  - A re-use and enhancement, where necessary, of the widespread GERAN/UTRAN technology for security for M2M communication seems promising (cost effective). Additional security should be on the application side by the M2M user.
- Security for unattended M2M devices (secure the UICC in such a way that it is not trivial to tamper with or steal)
  - theft or fraudulent modification of an M2M terminal may not be detected quickly. Related work exists in 3GPP TR 33.905 "Recommendations for Trusted Open Platforms"
  - the M2M ME and the system attached to it (or surrounding it, e.g. a vending machine) often represent a single functional entity. The interface between the M2M ME and its surroundings are security-relevant.
    It must be decided whether this interface is in scope or out of scope of 3GPP standardisation.

Issue 4: Addressing of M2M terminals

- Currently an IMSI is allways required to access a 3GPP network (CS, PS, IMS)
  - The limiting factor in addressing is the IMSI (only 9 or 10 digits are available for use within one network identified by a MNC)
  - Backwards compatible extension of the IMSI address range: Special MNC/MCC/MSIN, which are transparent to legacy systems, could trigger a further validation check of the M2M address part of the IMSI
- alternative addressing solutions based on IP addresses should be studied
  - authenticating the terminal by identifying only the group it belongs to (no individual authentication of M2M terminals)
  - Additionally, some identification of M2M terminals on application layer may be needed
  - However, there is a need be able to identify a rogue or misbehaving terminal and take it out of service

Summary: possible requirements (I)

- De-activation of mobility signalling for stationary terminals
- Optimised mobility signalling for low mobility and low activity terminals
- Possibility to instruct individual/group of terminal types e.g. static, low mobility, low activity terminals, not to perform any periodic location updates, and optionally location updates due to movement between LA/RAs.
- Possibility to instruct individual/groups of terminal types to perform a location update at a specific date and time
- Purging of subscriber data from VLR/SGSN for low activity / MO only terminals
- Tamper Save/Theft proof terminal including a UICC
- Possibility to change subscription out in the field e.g. after contract expiry without human intervention

Summary: possible requirements (II)

- Possibility to allocate the terminals at initial power up to a network operator without human intervention
- Re-use of PNM mechanisms for M2M communication
- Possibility to define groups and to have group counters to count the traffic to and from the servers at the network boundary
- Per group counters to count location update traffic
- Add a terminal type identifier to the subscription information to facilitate mobility management and charging
- Overcoming the limitations of the IMSI range by alternative addressing solutions
- To simplify terminals and networks and thus reduce costs the CS should not be impacted and preferably PS should be used.

Empowered by Innovation