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
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.

Get me 2 beer babe!

Why is your status still single in M2M- SNS?!

Get him some beer and charge twice!

You guys breaking up or what?
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

JPY (Japan market)
Where can we use M2M?

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

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?

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

### 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
What can be used?

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

*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

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?

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

Strategic Direction: Avoid Duplication
Examples of Current M2M-related Standardization Work (1):
- 3GPP: [http://www.3gpp.org/ftp/Information/WORK_PLAN/Description/releases/IMTC_M2M_20100521.zip](http://www.3gpp.org/ftp/Information/WORK_PLAN/Description/releases/IMTC_M2M_20100521.zip)
- CCISA’s Ubiquitous Network Technical Committee: [http://www.ccsa.org.cn/english/show_article.php?article_id=cyx_e02046a2-7c02-5a7e-5f3c-4b544e4a3545](http://www.ccsa.org.cn/english/show_article.php?article_id=cyx_e02046a2-7c02-5a7e-5f3c-4b544e4a3545)
- ETSI General M2M Activities (TC M2M): [http://www.etsi.org/Application/Search?search=m2m](http://www.etsi.org/Application/Search?search=m2m)
- Open Mobile Alliance Device Management: [http://www.openmobilealliance.org](http://www.openmobilealliance.org)

Strategic Direction: Avoid Duplication
Examples of Current M2M-related Standardization Work (2):
- Wi-Fi Alliance certification programs (IEEE 802.11) [http://www.wi-fi.org](http://www.wi-fi.org)
- Bluetooth (IEEE 802.15.1) [https://www.bluetooth.org/ap](https://www.bluetooth.org/ap)
- Zigbee Alliance (IEEE 802.15.4) M2M-related solution
- WiMAX (IEEE 802.16) project planning committee [http://www.wimax.com](http://www.wimax.com)
- GS1 standardization work [http://www.gs1.org/](http://www.gs1.org/)
- Wavenis Open Standard Alliance: [http://www.wavenis-x.com](http://www.wavenis-x.com)
- Work within World Wide Web Consortium (W3C): [http://www.w3.org](http://www.w3.org)

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](http://www.comcare.org/VEDS.html)
  - ISO TC 204 - ITS: [http://www.iso.org/iso/iso204_technical_committee?commitid=54798](http://www.iso.org/iso/iso204_technical_committee?commitid=54798)
  - ITU and Standardization Activities for Intelligent Transport Systems [http://www.itu.int/dms_pubrec/itu-t/012/17250100000000020PDX.pdf](http://www.itu.int/dms_pubrec/itu-t/012/17250100000000020PDX.pdf)
- Smart Grid space
  - IEC TC 57 - Communication networks and systems for power utility automation: [http://www.iec.ch/cgi-bin/dg57g2_project_progress22.pl?searchnummber=335&iecpdno=515506&partan=1&submit=Submit](http://www.iec.ch/cgi-bin/dg57g2_project_progress22.pl?searchnummber=335&iecpdno=515506&partan=1&submit=Submit)
  - NG Smart Grid Interoperability Standards Project: [http://www.net.gov/standard/](http://www.net.gov/standard/)
- Healthcare space
  - Continua Health Alliance: [http://www.continuaalliance.org/index.html](http://www.continuaalliance.org/index.html)
- Home automation space

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
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

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

*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
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