****

**APT REPORT**

**on**

**MACHINE TO MACHINE   
COMMUNICATIONS APPLICATIONS AND DEVELOPMENTS**

**No. APT/AWG/REP-42**Edition: September 2013

**Adopted by**

**The 15th APT Wireless Group Meeting**

**27 – 30 August 2013  
Bangkok, Thailand  
*(Source: AWG15/OUT-20)***

**APT REPORT ON MACHINE TO MACHINE   
COMMUNICATIONS APPLICATIONS AND DEVELOPMENTS**

**1 Scope**

This report will promote and accelerate the M2M industry in Asia-Pacific area from following perspectives:

* Study applications of machine to machine (M2M) communications, including innovation, standardization and successful examples in this domain as well as the business model aspect.
* Identify any obstacle along with M2M industry development, and identify the issues that AWG is supposed to solve and launch the work. Responses to the AWG questionnaire should be considered in this study.

**2 Summary of AWG Questionnaire**

**2.1 Summary of the Received Feedback**

Based on the responses received until AWG-14, the responding participants of the questionnaire are:

1. China (People’s Republic of) (doc. AWG-10/INP-34).
2. The Republic of Korea (doc. AWG-11/INP-33).

The response from the republic of Korea is given by M2M project group (PG708) of Telecommunications Technology Association (TTA).

1. Japan (doc. AWG-14/INP-38)

**2.2 Market**

1. M2M applied industry and the respective scale

M2M applications have already been applied in the listed eleven industries in China, Korea, and Japan are as follows:

1. Transport
2. Smart Grid
3. Smart Metering
4. Consumer Electronics
5. E-Health
6. Agriculture
7. Logistics
8. Automation
9. Environment
10. Structure
11. Disaster Monitor

In Japan, the other M2M applications applied industries are Digital signage, Anticrime/Security, Public infrastructure management (Bridge, Road, Water Pipe, and River/Dam).

As for the respective scale of those industries, only Korea provided M2M applications and subscribers in another classification as illustrated in Figure 1.

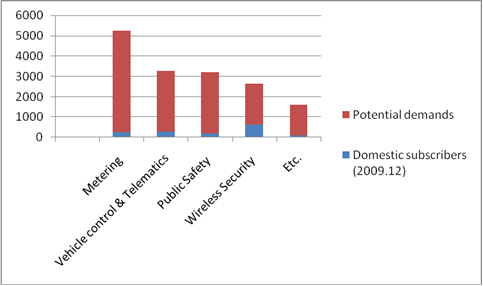


Figure 1 Major M2M Applications & Subscribers of Korea

(Unit: Thousand Subscribers) - Source: M2M/IoT Forum

1. The problems in deploying the M2M applications

China and Korea both identified inter-operability as a problem in deploying the M2M applications, besides, China added market/trade barrier and market entry into its problem list, and China also provided its considerations on this topic as the following:

* Need more research on key technologies
* Application scale is small and the business model is not so mature
* Challenge in privacy and security issues

Japan identified that the problems in deploying the M2M applications are as follows:

* Lack of attractiveness for market access due to fragment markets per industry (small cost-benefit performance, niche markets)
* Lack of market environments that enable M2M business players to provide services in a flexible way considering import/export circumstances as wireless device certifications and M2M related regulations are different per countries.

1. The prospective for the M2M applications

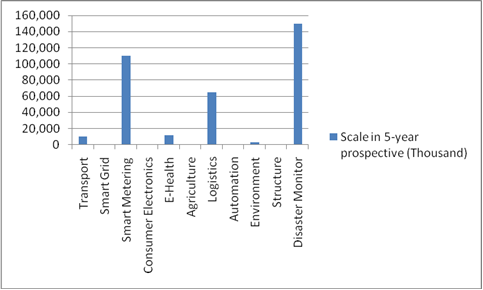


Figure 2 Five-year prospective for the M2M application in China

In the prediction of five-year prospective and ten-year prospective, all the listed eleven M2M applications are identified both in China and in Korea.

As for the respective scale of those industries, China provided the five-year forecast for the M2M applications in the listed eleven industries as illustrated in Figure 2, while Korea provided the ten-year result in another industry classification as shown in Figure 3.

In japan, M2M market is expected to be approximately 330 billion Yen in 2015 (including network, module, software and service) per ROA Holdings research.

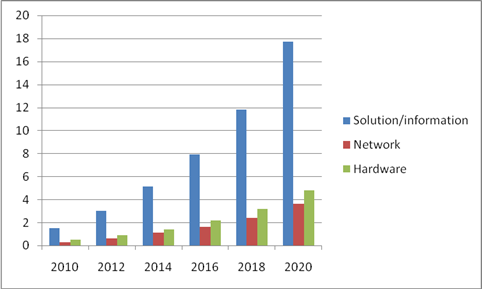


Figure 3 Ten-year forcast for M2M market prospective of Korea

(Unit: KRW) Source: IDATE, Beecham (2009)

**2.3 Policy and Regulation**

All of questions in this section are not applicable in input document from Japan.

1. National policy for M2M applications promotion

Chinese government released a decision on accelerating the development of new industries in 2010. The decision noted that the government should speed up the M2M development and application, and it pointed out that the M2M enterprises should be supported to expand market and to innovate commercial mode. Accordingly, some provinces and cities released its local policies, such as Chongqing and Wuxi. Particularly in Wuxi, a national innovation and demonstration area is under construction and some supporting policies are implemented including finance, land, taxation etc.

In October 2009, Korea Communications Commission (KCC) announced the basic plan for establishing M2M infrastructure until 2012. The major four strategies for M2M are as in the following:

* Establishment of M2M infrastructure in collaboration with Korea government and private sectors
* Efficient utilization of existing broadcasting and cellular network resources and facilitation of relevant law and legal issues for the emerging M2M services
* Promotion of trial M2M services to public sector, and its spreading to private sectors
* Supporting of relevant R&D projects including standardization and its promotion of market environments

In May 2010, KCC announced that M2M is one of the ten future strategic ICT services.

1. Telecommunication regulation for M2M applications facilitated

The question about telecommunication regulation for M2M applications facilitated is not applicable both in China and in Korea.

1. Specific frequency spectrum applicable to M2M applications

The question about specific frequency spectrum applicable to M2M applications is not applicable both in China and in Korea.

1. Regulation for M2M applications/ service deployment upon the existing infrastructure

The question about regulation for M2M applications/ service deployment upon the existing infrastructure is not applicable both in China and in Korea.

1. National policy promoting M2M applications in five to ten years

In the twelfth ‘Five-Year Program’ released by the Communist Party of China Central Committee in October 2010 mentioned M2M industry. It is said that the M2M development and application should be promoted. Ministry of Industry and Information (MII) released guidance on M2M industry development in 2011.

Meanwhile, the following table shows M2M vision of Korea from 2012 to 2015.

**Table 1 M2M vision of Korea**

|  |  |
| --- | --- |
| **Year** | **Goal** |
| 2012 | * Development of M2M open platform & Establishment of test bed * Start the demonstration service in metropolitan area |
| 2013 | * Finding the core technology & Standardization |
| 2014 | * Development of M2M based fundamental technology |
| 2015 | * Expansion of M2M demonstration project to the whole country * Preoccupancy of global market up to 30% |

Source: KCC (2011)

1. Telecommunication regulation facilitating M2M applications in five to ten years

In China, some technical standards are being developed by China Communications Standards Associations (CCSA), such as general technical requirements for mobile M2M business, the communication protocol requirements for mobile M2M business etc.

As a part of Korea government policies, O2N (Object to Object Intelligent Network) Forum was established in October 2009 under TTA, later on its name has been changed as M2M/IoT Forum to avoid any possible duplications on terminology. M2M/IoT Forum is trying to promote M2M business market in KOREA. In addition, TTA Standardization Coordination Committee approved the establishment of M2M Project Group (PG708) at Dec. 07. 2010. PG708 had a kick-off meeting on Feb. 14. 2011, and it is focusing on the scope of possible M2M services and its direction for domestic & international standardization.

TTA PG708 ToR (Terms of Reference)

* Development of M2M service requirements
* Standardization of M2M identification scheme and naming technology
* Standardization of M2M platform interface and interoperability.
* Standardization of M2M security technology
* Invigoration of domestic M2M market and standardization with collaborating M2M/IoT forum
* Collaboration with standardization activity of one M2M, 3GPP, ITU-T/R

**2.4 Technical**

1. Telecommunication techniques used for existing M2M applications

It is the telecommunication techniques are being used for existing M2M applications in China, Korea, and Japan, the details are shown in Tabel 2.

Table Telecommunication techniques used for existing M2M applications

|  |  |  |  |
| --- | --- | --- | --- |
|  | **China** | **Korea** | **Japan** |
| **Wired Line** | Yes | Yes | Yes |
| **GSM** | Yes | No | No |
| **EDGE** | Yes | No | No |
| **WCDMA** | Yes | Yes | Yes |
| **TD-SCDMA** | Yes | No | No |
| **CDMA** | Yes | Yes | Yes |
| **WiMAX** | No | Yes | Yes |
| **Satellite** | No | Yes | Yes |
| **UWB** | No | No | Yes |
| **Wi-Fi** | Yes | Yes | Yes |
| **Zigbee** | Yes | Yes | Yes |
| **Bluetooth** | Yes | Yes | Yes |
| **RFID** | Yes | Yes | Yes |

1. Major M2M applications coverage/deployment situation

Table 3 Major M2M Application Coverage/Deployment

|  |  |  |
| --- | --- | --- |
| **Content**  **Country** | **Wired**  **(In application penetration rate)** | **Wireless**  **(In land coverage rate)** |
| **China** | * A mixed mode with wireless mainly used in government level, i.e. * Security usage monitoring * Traffic monitoring both for real time traffic information and for traffic security | * Vehicle location reporting * Scheduling system used by Taxi/Bus companies * Remote monitoring application in environment * Traffic and agriculture |
| **Korea** | PLC, Ethernet | CDMA/WCDMA, WLAN, WiBro |
| **Japan** | Broadband service coverage is 56% (unit of household) in Dec. 2011. (Note that the number is not M2M specific.) | Coverage is 100% if mobile networks are used. |

1. Potential new radio technique considered to be used for future M2M applications

China: LTE and LTE-Advanced

Korea: LTE (4G), LTE-A

Japan: LTE, LTE-A

1. Technical problems in deploying the M2M applications

The lack of global M2M standard is the common concern between China and Korea, besides, the lack of experienced technical support team and some specific technical bottlenecks of industry application are other concerns in China, while the lack of proper access technology and inter-operability scheme are identified by Korea. Meanwhile, wireless/wired network overload due to simultaneous connection establishment/termination requests from large amount of M2M devices is technical problem facing by Japan.

1. Evaluation characteristics for M2M applications

Table Evaluation characteristics for M2M applications

|  |  |  |  |
| --- | --- | --- | --- |
|  | **China** | **Korea** | **Japan** |
| **Power Consumption** | Yes | Yes | Yes |
| **System Capacity** | Yes | Yes | Yes |
| **Coverage** | Yes | Yes | Yes |
| **Device Cost** | Yes | Yes | Yes |
| **Delay Response Time** | Yes | No | Yes |

China, Korea, and Japan identified power consumption, system capacity, coverage and device cost as the characteristics that can evaluate the M2M applications, in addition, China and Japan regarded delay or response time should be also considered.

**3 Introduction**

After organization restructuring and rebranding AWF to AWG (doc.AWF-9/OUT-03), the scope of work of Convergence Working Group that related to study on telecommunication broadcasting convergence was handled in the Task Group on Radiocommunication Convergence (TG-RC) within the Working Group on Service and Applications (WG-SA). The ToR of TG-RC is the as following:

* + To identify the wide range of current and future activities on the radiocommunication convergence technologies and also possible application scenarios including M2M;
  + To review survey on economic issues such as business model of convergence service; and
  + To review survey on regulatory issues to facilitate convergence service

Based on several input documents and presentations which were received and presented in the WG-SA, as well as some more other references, this document will illustrate the following aspects related to machine to machine communications applications and developments:

* Challenges and considerations for M2M Communications
* Specific considerations for security and privacy, and key vertical sector
* Special case of M2M Communication in Wireless Sensor Network

**4 Challenges for Machine to Machine Communications**

**4.1 Radio Access Network**

**RAN overloading**

RAN (Radio Access Network) overload is one of the challenges after more and more M2M communications occur. It is expected that the M2M communication would be at least two orders of magnitude higher than for H2H communications in future. When a large number of M2M devices are expected to be deployed in a specific area, the network including the uplink random access resource may be congested / overloaded due to mass concurrent data and signaling transmission. This may cause intolerable delays, packet loss or even service unavailability. Especially the H2H communications are affected greatly.

**4.2 Core Network**

**Signalling traffic flooding prevention**

The level of signaling traffic due to M2M connections is not currently a burden on cellular networks. However, it is one of the few technical areas directly related to core network performance that is cited as a concern by M2M industry participants. The concern rests on the expected future growth in the volume of M2M connections, and consequently, the growth in signaling traffic on the network. The fear is that with billions or tens of billions of M2M devices, the core network infrastructure will not be adequate.

Many terminal vendors have not given enough consideration to the mobile network, so the M2M devices may try to access to the network or establish the session repeatedly when some errors happens. So when the mobile network is overload, the mobility and session management requests from M2M devices shall be restricted in the following scenarios:

* Restricting the mobility management request from the M2M devices belongs to specific M2M user
* Restricting the session management request from the M2M devices belongs to specific M2M user
* Restricting the mobility management request from the low access priority M2M devices
* Preventing mass of the roaming M2M devices accessing to the local network simultaneity

**Small amount data transmission**

M2M devices with Small Data Transmission send or receive only small amounts of data. The exact amount that is considered to be small may differ per individual system improvement proposal. It is the amount of data where a specific system improvement proposal still provides its benefits. For today’s packet switch network, the data is transferred via the bearer, so the network shall first activate the Pbearer for the device before transferring packet data. For such small amount data transmission, it may be inefficient to transfer the data via the bearer as the amounts of the bearer activate signaling may great larger than the application data. So, the network shall transmit small amounts of data with very efficient resource. Considerations for solutions should include the small data upper limit and the frequency of small data transmissions that the solution is suitable for.

The SMS may be a potential solution for small data transmission, while the SMS still involves CS domain nodes which means the operators has to continue to invest the CS network. Besides, the SMS mechanism may consume much of SS7 signaling resource, and SMS mechanism relies on the unique MSISDN for each device which may not be satisfied as the lack of number resource.

**Diagnostics for Services Troubleshooting**

One of the fundamental shifts in the interaction between MNOs and MVNOs with their ASP customers has been the enabling of ASPs to self-provision, manage, and troubleshoot their active devices in the field. From the connectivity service provider perspective, this is far more efficient than having to manage these processes directly. Likewise, from the ASP perspective, this provides far greater granularity of control and ability to interact with end devices in the field than having to work through MNO/MVNO ―trouble tickets.

However, managing mobile network-attached devices is far more complicated than managing devices connected to the wireline network. These challenges range from bandwidth typically being scarcer on mobile networks to protocol issues between GSM and GRPS that can make a connection appear active because it has GSM connectivity even though the ability to send packets over GPRS is inoperable.

The ability to perform diagnostic analysis on the signaling and data traffic between the remote device and the server-side M2M application software is one important means to increase the capability of MNOs and MVNOs to provide a robust self-management platform for use by their ASP customers. For example, this gives the ability for the ASP to know if a device is inoperable due to coverage loss, because it was physically shut off, or if there is a particular malfunction with the device itself.

**Stateful Geo-redundancy for Session Recovery**

In order to keep the connectivity always available, there is a need to have mobile packet gateways that not only scale up to a large number of bearer activations – for example, in response to disaster recovery – but also to be able to shift those sessions over to a second mobile packet gateway in a stateful manner in case the first mobile packet gateway becomes non-operational.

Stateful IP packet session failover has the benefit of being able to keep the state of sessions active within the mobile packet gateway directly without having to flood the ASP’s RADIUS servers with a huge signaling storm and potential crash as a multitude of remote M2M devices try to connect. Fundamentally, as the context states are maintained directly in the M2M-optimized mobile packet gateway, this enables the ASP to work with more cost optimized server technology that does not need to support millions of activations simultaneously, as the mobile packet gateway takes on this burden in the context of geo-redundancy.

**Network-Initiated Data Session Activation for Increased Application Robustness**

Very large numbers of data-capable devices are coming onto mobile networks, both for M2M as well as traditional smartphone and PC connectivity. While M2M-optimized network elements can aid in managing extremely large numbers of PDP context activations, MNOs are still becoming more concerned about reducing idle time to make their networks more efficient. It is becoming increasingly common for MNOs to require idle devices (that is, remote devices that have an active packet data networking session in place (bearer) but that are not actually transmitting data) to drop their session after one to four hours of inactivity. This frees up network resources for other remote devices to activate bearers.

It is not too significant a burden for traditional smart phone and PC modem data users to have a context dropped if idle; if their session is idle, they are simply not using the service and can renew the bearer as soon as they need to be reconnected.

For M2M applications, decreasing idle time can be a significant burden since it is often the server based application software that needs to communicate with the remote device. Take, for instance, a new emergency firmware upgrade that needs to be immediately delivered to a set of remote devices. Given that with traditional mobile network functionality bearers cannot be initiated from the network side, that is, by the server based application software, ASPs have needed to rely on either rules-based embedded software on the remote device telling it to initiate a bearer at certain intervals or at certain specified events, or on SMS to cause the remote device to initiate a bearer.

The challenge with a rules based paradigm is that the remote device’s embedded set of rules may not lead it to initiate a bearer when the server-based application software would like it to do so, as in the case of the emergency firmware download described above. The challenge with SMS, wherein the server-based application software sends an SMS to the remote device, which is allowed under traditional mobile network functionality, is that SMS messaging is not always seen as reliable enough for some M2M applications; there is the possibility that the message is unacceptably delayed or never delivered at all.

There is a new capability emerging in mobile packet gateways to enable the ASP’s server-based application software to initiate a bearer with a remote device directly, called network initiated bearer. MNOs/MVNOs that provide this capability could enable ASPs to have a more robust capability to contact their remote devices while also addressing the MNO goal of minimizing idle bearers.

**5 General Considerations for Machine to Machine Communications**

**5.1 Radio Access Network**

**RAN overloading**

As for RAN overload including uplink random access resource congestion, several solutions may be used:

* Access Class Barring schemes

Separate Access Class(es) for M2M devices allows the network to separately control the access from M2M devices, in addition to access control for H2H devices. Depending on the granularity of the control needed among M2M devices, either one or several Access Classes can be introduced.

* Separate RACH resources for M2M

When M2M and H2H devices share the random access resource, they experience the same access collision probability. Separate random access resources can be provided for the H2H and M2M devices to avoid the collision by each other.

* Backoff scheme

The network can allocate backoff timer to M2M devices for them to delay their access attempts when the network is overloaded.

* Pull based scheme

MO (Mobile Originated) service would be initiated without network overload knowledge so that the network may be congested by large number of concurrent MO service. If the services are always initiated through MT (Mobile Terminated), the network would take the load information into account firstly and then decide whether to page the M2M device and establish the connection towards it. If the load won’t permit, the network would give up paging the device to avoid further load and congestion.

**5.2 Core Network**

**NAS level congestion control**

NAS level congestion control contains the functions: "APN based congestion control" and "General NAS level Mobility Management control". The use of the APN based congestion control is for avoiding and handling of mobility management and session management signaling congestion associated with M2M devices with a particular APN (belongs to certain M2M user).

The SGSN/MME may detect the NAS signaling congestion associated with the APN and start and stop performing the APN based congestion control based on criteria such as:

* + Maximum number of active bearers per APN
  + Maximum rate of Bearer activations per APN
  + One or multiple mobile packet gateway of an APN are not reachable or indicated congestion to the mobility management node
  + Maximum rate of mobility management signaling requests associated with the devices with a particular subscribed APN
  + Setting in network management

With General NAS level Mobility Management control, the mobility management node may also use the reject of NAS level Mobility Management signaling requests under general congestion conditions. E.g., when the resource of SGSN/MME is heavily occupied, the mobility management node executes general NAS level mobility management control. At the first phase, the SGSN/MME may first reject the NAS signaling request from the low access priority M2M device. The M2M device may be configured as low access priority, and containing such low access priority in the NAS level signaling.

In order to minimal the impacts which are brought to the local network by the roaming M2M devices, e.g., the M2M devices roaming to the local PLMN when HPLMN is failure and some following mechanisms may be used:

* UE configured to perform Attach with IMSI at PLMN change, in order to avoid signaling exchange between the PLMNs;
* UE configured with a long minimum periodic PLMN search time limit, in order to avoid the M2M devices reselect to the H PLMN even the HPLMN is still in failure status.
* UE configured for specific handling of the invalid USIM state, the "forbidden PLMN list", the "forbidden PLMNs for GPRS service list" remembers that the USIM is invalid and keeps the PLMN forbidden lists even if the UE is switched off and then switched on.

**Small amounts data transmission based on SMS (TR)**

The SMS could be used as the potential solution for small amounts data transmission. But the existing SMS mechanism is based on SS7 signaling, which is not efficient, the optimized SMS mechanism based on IP is recommend for small data transmission.

For GPRS, the SGSN has supported the SMS transmission, so, it is proposed that the Gd interface between the SGSN and GMSC based on IP, e.g., Diameter protocol. And the SMS transferred via the SGSN instead of MSC/VLR. In addition, this solution does not rely on the device has CS registration. So for the devices only have PS only subscription, the SGSN’s support of SMS transfer needs to be used.

For E-UTRAN, it is proposed to consider the provision of SMSoSGs by the SGSN. For UEs with SMS only the MME may select the SGs provided by an SGSN. Thereby PS only can be accomplished for UEs without voice/CSFB needs.

**Smart pipe (TR)**

The mobility management node has the mobility management and session management functions, so, the mobility management node could detect the M2M device’s MM/SM status. When some error happens, the mobility management node could report the error cause to the M2M SDP, e.g. attach failed cause or PDP activation failed cause. Besides, the mobility management node could also report the device’s location to the M2M SDP. The mobile packet gateway could detect the PDP status of the devices, so, the mobile packet gateway could report the device’s online/offline status to the M2M SDP.

**M2M device triggering (discussing)**

The M2M-optimized network elements can aid in managing extremely large numbers of PDP context activations, MNOs are still becoming more concerned about reducing idle time to make their networks more efficient. It is becoming increasingly common for MNOs to require idle devices to drop their session after one to four hours of inactivity. This frees up network resources for other remote devices to activate bearer s. When the server wants to send MT data to such device, the network should first trigger the device to initiate session establishment procedure.

Today’s solution is using SMS for device triggering, while, SMS mechanism may have some drawbacks, e.g., transmission inefficient, relying on the MSISDN/CS subscription. So, some optimized and general solution is recommended. The NAS level like NI bearer mechanism is recommended, the M2M SDP acts like a mobile packet gateway, which could trigger the mobility management node to send the NAS message to the device for triggering the device to initiate bearer activate procedure.

**6 Considerations for Security and Privacy**

**6.1 Threat Assessment**

**M2M group-based optimization:**

M2M devices can be grouped together for the control, management or charging facilities etc. to meet the need of operators. The network resource could be saved by using group based optimization when the number of M2M devices is large. The M2M devices within the same group can be in the same area and/or have the same M2M features attributed and/or belong to the same M2M user, which provides the flexibility to allocate a group. Moreover, each of the M2M devices is visible from the network perspective.

The devices connected to M2M Gateway Device can constitute a group. If each device adopts the existing method of authentication, the signaling load of the network will increase largely (especially when the group of devices access to the network almost at the same time). In order to avoid the signaling overload issue and achieve signaling optimization for M2M group, the M2M gateway can perform authentication on behalf of the devices connected to it.

An attacker can impersonate a M2M device belonging to a particular M2M group to get information. Therefore a mechanism should be provided to prevent such attacks.

For the case when M2M GW is not owned or controlled by the operator, there can be fraud as of M2M GW authorizing the network access to also illegitimate M2M devices. For example, session keys and perhaps M2M device identities can be cloned.

If the devices in the group access to the network almost at the same time, then the signaling load of the network will increase largely. In order to avoid the signaling overload issue and to achieve signaling optimization for M2M group, group based authentication is needed.

**Small Data Transmission:**

Using NAS for SMS transport was designed as a stop-gap solution with the goal of eventual deployment of IMS-based SMS. What is being proposed now will standardize overloading of NAS, strictly control protocol, with what is effectively UP content. Such content will be generated by potentially hundreds of millions devices, creating an environment for a DOS attack on MME.

There may be no pre-established NAS security context in transfer data via optimized SMS solution. Thus the small data transmission cannot be protected by valid security context and can be easily tampered or intercepted by the attacker. Sometimes small data is sensitive and important because it may be related to emergency event or commerce. Once it is tampered or intercepted, the consequence can be serious.

**Congestion Control:**

When requesting access to the mobile network, a UE shall provide its currently enabled indicators to the network. There exist security threats if the indicators are sent without any protection. The attackers can tamper with the low priority indicators to the normal state to let many M2M devices connect when the network setup congestion control mechanism. The problem is serious since nowadays congestion is the most urgent issue that operators face. Vise verse, if an attacker adds a fake low priority indicator in the request sent by normal UEs, the service of normal UEs (esp. some VIP users) is maliciously degraded.

**M2M trigger:**

**False network attack:** When a M2M device is in detached state, the attacker can impersonate a network to send a trigger indication to the M2M device. Although there are existing mechanisms in the current network to prevent a M2M device to connect to a false network, there is still an issue. M2M devices are different from UEs such that they may need to operate for a long time by using a single battery supply without recharging. False network triggering can awaken a M2M device and waste its power. So the false network attack is more serious for M2M devices compared to non-M2M communications and therefore we need to improve the network to deal with this security threat.

**Tamper attack:**

The trigger indication may contain the IP@ (or FQDN) and/or TCP (or UDP) port of the application server that the M2M device has to contact. If the IP@ (or FQDN) and/or TCP (or UDP) port of the application server is tampered by the attacker, the M2M device may establish the PDN connection to the wrong M2M server or be rejected by the M2M server. It will cause that M2M device is unable to communicate with the correct M2M server and it will also waste the M2M device's power consumption.

When the legacy SMS is used to trigger M2M devices, SMS spam could be exploited by the attackers to send fake trigger indication. Although the human holding a normal UE can make his own judgment, the fake trigger indication sent in SMS spam could be a serious attack on the unattended M2M devices and will lead to battery draining (particularly for the devices with limited power supply). Moreover the fake trigger indication sent in SMS will cause M2M devices trying to access the network and lead to the waste of network resources.

**6.2 Security and Privacy Considerations**

**M2M group-based optimization:**

The authentication between the device and the network can be divided into two parts and the M2M gateway acts as an authentication agent. The M2M gateway and the core network node authenticates with each other (e.g. AKA). The device and M2M gateway authenticates with each other. The M2M gateway should notify the result of the authentication between the device and the M2M gateway to the core network node. If the above two parts of authentication succeed, it can be considered the authentication between the device and the core network node is successful. According to the key which is generated in the M2M gateway and core network node authentication procedure, the M2M gateway can provide different session keys used between the devices and the network element.

**Small Data Transmission:**

If the M2M devices and the network delete the security context after the detach procedure, the small data transmission can not be protected by valid security context. The following method is proposed to avoid the above security issue. When M2M device detaches from the network, the network checks whether the M2M device is subscribed with M2M feature- small data transmission, i.e. the network entity checks the subscribed M2M features from the HSS and then determine whether the M2M device has the M2M feature -small data transmission according to it. If it has, the network stores the security context corresponding to this M2M device. The M2M device also stores the security context if it has small data transmission M2M feature. Then the M2M device and the network can use the stored security context as current security context and transfer small data which is protected by the current security context.

**Congestion Control:**

Current LTE mechanism should be used to protect M2M indicator and low priority indicator. If the UE has valid security context, the Attach Request and LAU/RAU/TAU request shall be integrity protected by the NAS-MAC.

**M2M trigger:**

**For offline M2M device:** If the M2M device is in detached state, the network should protect the trigger indication message by using the last security context stored in the network and the M2M Device.

**For online M2M device:** The current security mechanism (after the security mechanism is activated) can ensure trigger indication securely transferred.

**7 Machine to Machine Communication in Wireless Sensor Network**

**7.1 Background and Description of Wireless Sensor Network**

Sensing is a technique used to gather information about a physical object or process, including the occurrence of events (i.e., changes in state such as a drop in temperature or pressure). An object performing such a sensing task is called a sensor. Sensor can also be implemented as remote sensors, which imply that they do not need to physically touch the monitored object in order to gather information. From a technical perspective, a sensor can be described as a device that translates parameters or events in the physical world into signals that can be measured and analyzed. Other commonly term used is *transducer*, which is often used to describe a device that converts energy from one form into another. A sensor, then, is a type of transducer that converts energy in the physical world into electrical energy that can be passed to a computing system or controller. An example of the steps performed in a sensing (or data acquisition) task is shown in Figure 4.



**Figure 4 Data acquisition and actuation [Dargie- Poellabauer]**

Many wireless sensor networks also include actuators which allow them to directly control the physical world. For example, an actuator can be a valve controlling the flow of hot water, a motor that opens or closes a door or window, or a pump that controls the amount of fuel injected into an engine. Such a wireless sensor and actuator network (WSAN) takes commands from the processing device (controller) and transforms these commands into input signals for the actuator, which then interacts with a physical process, thereby forming a closed control loop.

**7.1.1 Wireless Sensor Network (WSN) Definition**

While many sensors connect to controllers and processing stations directly (e.g., using local area networks), an increasing number of sensors communicate the collected data wirelessly to a centralized processing station. This is important since many network applications require hundreds or thousands of sensor nodes, often deployed in remote and inaccessible areas. Therefore, a wireless sensor has not only a sensing component, but also on-board processing, communication, and storage capabilities. With these enhancements, a sensor node is often not only responsible for data collection, but also for in-network analysis, correlation, and fusion of its own sensor data and data from other sensor nodes. When many sensors cooperatively monitor large physical environments, they form a wireless sensor network (WSN). Sensor nodes communicate not only with each other but also with a base station (BS) using their wireless radios, allowing them to disseminate their sensor data to remote processing, visualization, analysis, and storage systems.

A WSN can be defined as a network of devices, denoted as nodes, which can sense the environment and communicate the information gathered from the monitored field (e.g., an area or volume) through wireless links. The data is forwarded, possibly via multiple hops, to a sink (sometimes denoted as controller or monitor) that can use it locally or is connected to other networks (e.g., the Internet) through a gateway. The nodes can be stationary or moving. They can be aware of their location or not. They can be homogeneous or not.

**7.1.2 WSN Node (mote) Main Components**

A practical wireless sensor node must consist of the following:

* A sensor (e.g. a light sensor)
* A signal converter (usually an analogue to digital converter)
* A processor and memory (minimum capability for minimum power drain)
* A network interface (wireless; either radio or optical)
* A suitable packaging solution (a reliability and cost driver)
* A power supply (or a method of harvesting power in situ, e.g. from vibration or light, etc)

An example of implementation of WSN node (called “mote”) can be seen in Figure 5. These sensors, when used as a network, form a mini weather station. The word “mote” derived from its dictionary definition, which is ‘speck of dust’ or similar. This describes the role of an individual sensor node very well; each is relatively small, like a speck of dust, but there are lots of specks of dust in the network.



Figure 5 Wireless Sensor Node (Mote)

**7.2 Sensing Technologies and WSN Challenges**

**7.2.1 Sensing Technologies**

A sensor is a transducer which produces a measurable response to an external stimulus of, say, a change in a physical condition such as temperature, moisture or electromagnetic field, or to a change in chemical concentration. The following sections highlight key sensor technologies that can find application in WSNs. As this is an actively evolving engineering field, these sensor technologies are intended as illustrative examples rather than an exhaustive list. Broadly speaking, sensors can be classified under different categories based on their fundamental scientific principles as follows:

* Mechanical Sensors
* Thermal sensors
* Optical sensors
* Chemical sensors

**7.2.2 WSN Challenges**

There are some challenges faced by WSN which are can be refer to design a reliable WSN systems, i.e.:

* Energy Efficiency
* Limited storage and computation
* Low bandwidth and high error rates
* Errors are common
  + Wireless communication
  + Noisy measurements
  + Possibility of node failure
* Scalability to a large number of sensor nodes
* Survivability in harsh environments
* Experiments are time- and space-intensive

**7.3 Technology Perspective of WSN**

**7.3.1 WSN Architecture**

Figure 6 describe the WSN architecture, which comprise of sensor subsystem, processor subsystem and communication subsystem. Each will be described later in next paragraphs.

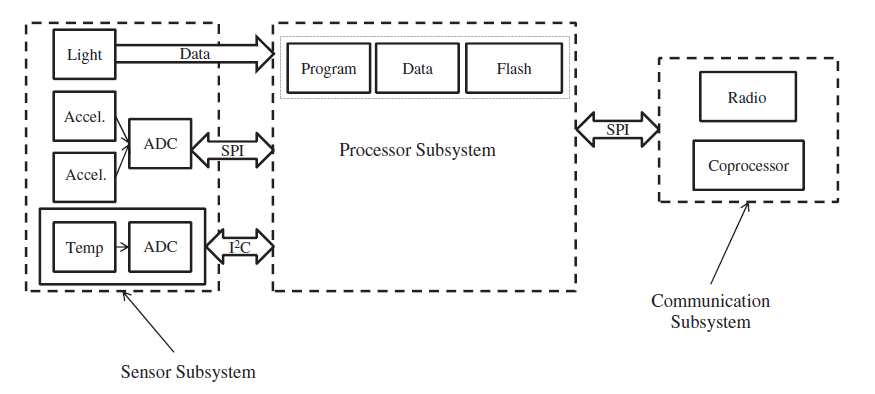


Figure WSN Architecture

The sensing subsystem integrates one or more physical sensors and provides one or more analog-to-digital converters as well as the multiplexing mechanism to share them. The sensors interface the virtual world with the physical world. the advent of microelectro mechanical systems (MEMS) has made sensing a ubiquitous process. Nowadays, there are a plethora of sensors that measure and quantify physical attributes at a cheap price. A physical sensor contains a transducer, a device that converts one form of energy into another form of energy, typically into an electrical energy (voltage). The output of this transducer is an analog signal having a continuous magnitude as a function of time. Therefore, an analog-to-digital converter is required to interface a sensing subsystem with a digital processor.

The processor subsystem brings together all the other subsystems and some additional peripherals. Its main purpose is to process (execute) instructions pertaining to sensing, communication, and self-organization. It consists of a processor chip, a nonvolatile memory (usually an internal flash memory) for storing program instructions, an active memory for temporarily storing the sensed data, and an internal clock, among other things.

Whereas a wide range of off-the-shelf processors are available for building a wireless sensor node, one has to make a careful choice, as it affects the cost, flexibility, performance, and energy consumption of the node. If the sensing task is well defined from the outset and does not change over time, a designer may choose either a field programmable gate array or a digital signal processor. These processors are very efficient in terms of their energy consumption; and for most simple sensing tasks, they are quite adequate.

In many practical cases, however, the sensing goal changes or a modification may be required. Moreover, the software that runs on the wireless sensor node may require occasional updates or remote debugging. Such tasks require a considerable amount of computation and processing space at runtime. In which case, special-purpose, energy-efficient processors are not suitable.

Most existing sensor nodes at present use microcontrollers. There are some justifications besides those just mentioned. WSNsare emerging technologies; and the research community is still active with research for developing energy-efficient communication protocols and signal processing algorithms. As this requires dynamic code installation and update, the microcontroller is the best option.

**7.3.2 WSN Positioning and Applications**

**7.3.2.1 WSN, RFID & M2M Positioning and Segmentation**

Within the range of wireless technology, the illustration of overlap position of WSN alongside RFID and Machine to Machine (M2M) Communication is shown in Figure 5.



Figure Illustration of WSN Comparison to RFID and M2M

The finite definition of wireless sensor and WSN from the perspective of application is not exact. Market analysts have broad view of these cases and produce reports based on different market segments. Current definitions also reflect to a degree the different historical development paths and differing industry segments and stakeholder groups. This is particularly true for RFID, a technology that has evolved as an industry segment over a relatively long period (15 years) compared to WSNs.

Wireless M2M covers applications involving longer range, remote monitoring and management of devices, and will typically adopt cellular or other wide-area data transfer technologies. Thus the examples of a remotely monitored vending machine and networked photocopier might employ GSM or 3G data connectivity to allow remote monitoring of machine status. The wireless node will typically be powered from the machine itself, supporting the higher transmission power requirements needed.

Automated Meter Reading (AMR) is an example of an application that has been in development for some time, driven particularly by players in the energy industry, with a corresponding specific set of requirements to meet those industries’ needs. However many of the characteristics of AMR systems are similar to those of WSNs, and AMR may be seen as a particular application of WSN technologies, but with aspects of M2M depending on the architecture of the back-end system. Key characteristics of M2M, WSN, and RFID are summaries in table 5.

Table Key Features of M2M, WSN, and RFID sensors/nodes

|  |  |
| --- | --- |
| **Wireless Technologies** | **Key Characteristics** |
| M2M | 1. longer range (order of 10m – 10km) 2. not power consumption critical 3. encompasses other technologies in some instances 4. processing capability and data storage 5. size/weight not over-riding factor in many applications |
| WSN | 1. short/medium range (order of 1m-1km) 2. very low power (battery, scavenged power) 3. two-way communications, point-to- multipoint or peer-to-peer 4. local processing capability 5. some data storage 6. typically small size, weight, typically environmentally rugged |
| Active RFID | 1. contains power supply 2. short range (0.1 – 10m) 3. very low power 4. two-way communications, normally point-to-point 5. some local processing capability 6. limited data storage 7. small size/weight, may be environmentally rugged |
| Passive RFID | 1. receives power via reader 2. near field (0.01 – 1m) 3. essentially one-way communications, point-to-point 4. limited or zero local processing 5. no local data storage 6. very small size/weight, robust packaging |

**7.3.2.2 Applications of WSN**

The applications can be divided in three categories:

1. Monitoring of objects.
2. Monitoring of an area.
3. Monitoring of both area and objects.

Some generic example of the Monitoring of objects categories, i.e.:

1. Structural Monitoring
2. Eco-physiology
3. Condition-based Maintenance
4. Medical Diagnostics
5. Urban terrain mapping

Some generic example of the Monitoring of an area objects categories, i.e:

1. Environmental and Habitat Monitoring
2. Precision Agriculture
3. Indoor Climate Control
4. Military Surveillance
5. Treaty Verification
6. Intelligent Alarms

Some generic example of the Monitoring Interactions between Objects and Space

1. Wildlife Habitats
2. Disaster Management
3. Emergency Response
4. Ubiquitous Computing
5. Asset Tracking
6. Health Care
7. Manufacturing Process Flows

**8 Specific Considerations for Key Vertical Sector**

**8.1 Automotive**

Nowadays, along with economic development, population growth, and increasing urbanization and motorization, the transportation system faces a lot of problems to be settled, such as increasing traffic accidents, traffic jam, air pollution, and fuel consumption. Automotive is an upgrade of general transportation system. With the cooperation of information and communication technologies, automotive aims to make the transportation system more efficiency, safety and also involve value added services to facilitate people on the road.

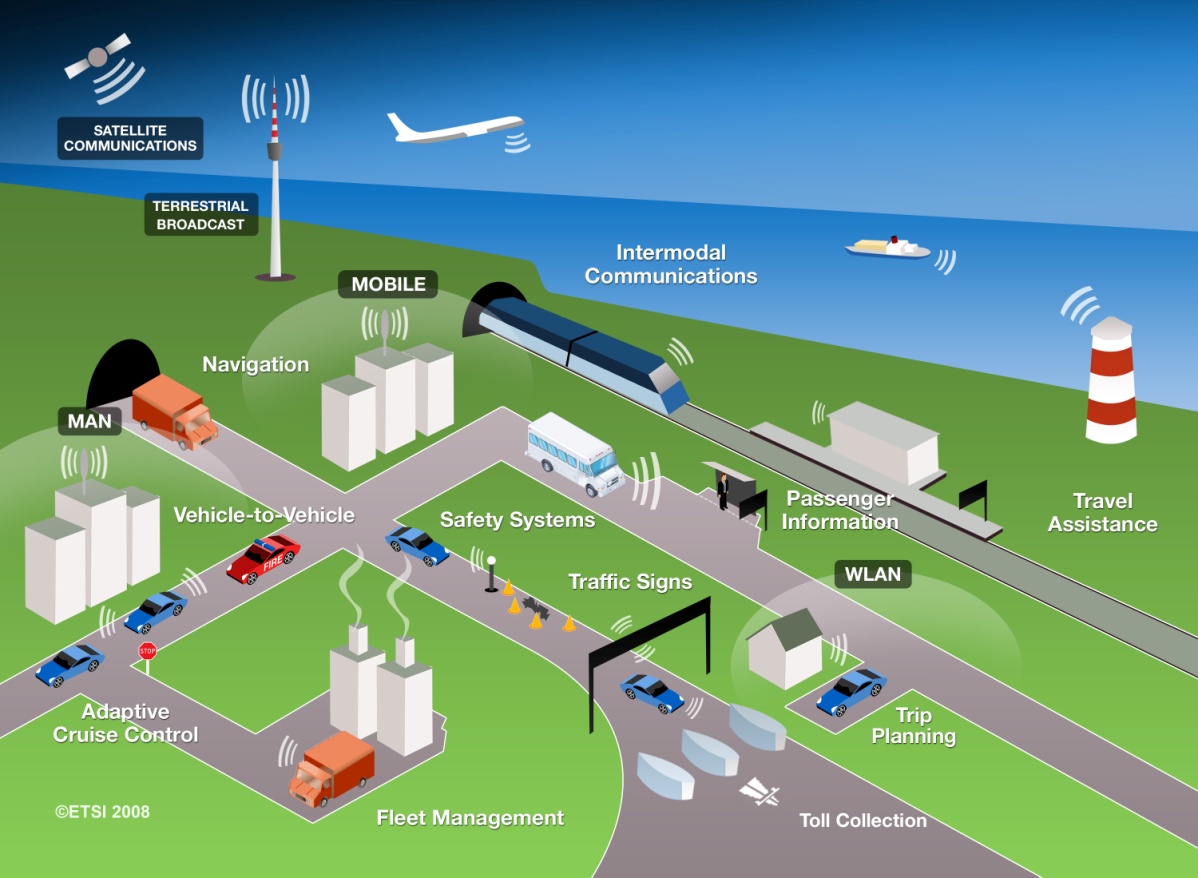


Figure Communication technologies and services

**8.1.1 Ecosystem Description**

This section will give general descriptions on the automotive ecosystem. There are several actors in automotive ecosystem which from the information network’s view are mainly around information collection, information transmission, and information processing. For information collection, the ecosystem actors include sensor, video/photo, GPS and radar related equipment manufacturers.

For information transmission, the ecosystem actors include wired/wireless network equipment manufacturers, user equipment manufacturers, vehicle communication equipment manufacturers, and operators. For information processing, the ecosystem actors include all types of chipset manufacturers, computer system manufacturers, software companies and storage equipment manufacturers. From the system point of view, integrators, vehicle manufacturers, national authorities, business customers and end customers play really significant roles that must also be involved in the automotive ecosystem.

The service stream of automotive system is illustrated in figure 9.



Figure Service stream in automotive system.

Potential automotive customers may roughly be divided into three groups. The different customer groups and the specific benefits gained from automotive system are illustrated in Figure 10.



Figure Customers in automotive ecosystem

The main payment, which is shared by the automotive infrastructure and service contributors, comes from all the benefits gainers, i.e. members in the three customer groups. For the broad range of possible actors in automotive system, the new operation mode and value distributed mode may be triggered.

**8.1.2 Representative Use Cases for the Automotive Sector**

Such as pre-trip and on-trip journey planning, travel information, and location-based services, email access, entertainment (like internet radio)The automotive sector will generally go through three stages as below:

The fist stage is the single navigation service which uses GPS and satellite communication, now we have basically actualized this stage. The second stage is to combine the mobile Internet with GPS, obtaining more abundant information and service, and therefore 3G or other wireless communications systems and intelligent traffic platform are all-important in this stage. The third stage is coordination of vehicle, road and passerby, achieving the implementation of safety pre-warning and traffic optimization etc. There are varieties of use cases for the automotive sector, which are mainly focused on three goals: efficiency, safety and value-added business. The following use cases are described mostly based on the second stage.

* 1. The driver or the passenger makes use of the traditional communication service, including voice, short message and internet access etc, to get available information or service. e.g, when emergency occurs, the driver calls the rescue center for the first aid. In another case, the information of entertainment or consultation such as weather forecast and news will be pushed and displayed in the screen of vehicle terminal.
  2. The driver may initiate an inquiry about the car position, route guidance and parking guidance etc, and then the intelligent traffic platform may return the real-time result displayed on the screen or via voice through the vehicle terminal. e.g, when arriving at the destination, the driver set up an inquiry of parking guidance and then the information such as position and current state of the nearest parking lot are transmitted and displayed in the screen.
  3. The driver may get real-time information of car condition or other needed via the sensors in the vehicle or by the intelligent platform, and then some decision such as travel security and car maintenance will be made. e.g, when traffic emergency occurs, information such as traffic control, traffic accident, severe weather condition are informed in the customized form such as short message, voice or video. In another case, data of car condition is collected and reported to the intelligent platform periodically and in sometime the driver are informed to maintain the car via the vehicle terminal.
  4. The vehicle may be monitored remotely and some action will be taken when needed. e.g, when the driver forgets the parking place, he may access the call center, and then the specified vehicle may be remotely operated to trumpet or start the double jumping light after identity authentication. In another case, when the unusual move of specified car are detected, the driver will be informed via short message.

The more detailed use cases are given in Table 6.

Table Use cases in the second stage of automotive system

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Service class | Use case | | | |
| Communication service | Basic call | Emergency call | Short message | Multimedia short message |
| Internet access | Video call |  |  |
| Road navigation | Basic information inquiry | Car position inquiry | Routing computing and lead | Road map updating |
| Real-time road condition navigation | Voice navigation | Parking guidance |  |
| Driving assistant | Car condition report | Car maintenance notice | Emergency traffic notice | Emergency rescue |
| Remote monitoring | Parking position remind | Remotely opening the door | Unusual move alarm remind |  |

**8.1.3 Solution Design Challenges**

Automotive is a regional specific sector. The traffic related activities, policies, infrastructure and road conditions are differentiated among different countries or regions，so it is difficult to find a single solution to coordinate all the differences. However, the use cases of automotive sector have proposed several different requirements for vehicle terminal and MNO’s network, so it is necessary to analyze the challenges for solution design in the perspective of ecosystem and technology, thereby providing reference to the application of M2M in the automotive sector.

* **Challenge1**: The complexity of ecosystem. Since many stakeholders from different industries are involved in the automotive sector, it is difficult to integrate industrial chain for the development of the automotive sector under the Internet of Things umbrella. The current situation is the lack of successful and effective cooperative mode between vehicle manufactures and MNOs, user quantity is inadequate due to the lack of killer applications, a long-term financing is still required to build a stable and sustainably profitable business model.
* **Challenge2**: The service based on location information. As a lot of applications of intelligent transport system need to utilize the vehicle’s location information to calculate travel time by locating current position, or provide the business and service information nearby, therefore the vehicle terminal in the network of vehicles should be able to acquire geographical location information periodically via GNSS interface, accordingly store and manage the information in order to support data transmission based on position trigger.
* **Challenge 3**: To support the connection of various passenger devices. As it is potential risk to use mobile phone when driving, and some European countries have issued a ban on it, the vehicle terminal should provide Bluetooth interface for the driver’s mobile phone to meet the needs of voice call. For other passenger’ s devices as MP3 player and PDA, the vehicle terminal should provide various communication interfaces such as Bluetooth, Zigbee, Wifi and USB in order to perform information sharing, multimedia entertainment, condition data query, etc.
* **Challenge 4**: Mass addresses of devices. The fast growing quantity of vehicles will have an impact on the limited address resource. Vehicle terminal is required to support IPv4 and recommended to support IPv6 packet delivery over ITS communication, demanding the minimum set of changes to the IPv6 stack.
* **Challenge5**: Qos guarantee with regard to different service. The data of networked vehicle includes high timeliness security service data and that of additional value-added entertainment service. The network used in automotive sector should be able to identify specific service information, thereby providing differentiated Qos level. Considering the high timeliness security service, network should assign a dedicated Channel and set a lower access waiting time to support it. Instead, network takes the best-effort strategy for the data of video and multimedia entertainment.
* **Challenge 6**: To support service continuity. Some services need steady access to the network, such as real-time navigation. Since the communication link keeps changing due to the mobility of vehicle, a seamless access to the infrastructure of the network can realize autonomously switches between the “best” available communication systems at the current time and location. Therefore, the vehicle terminal is required to have interfaces to one or more wide area networks such as GSM、UMTS and one or more vehicle area networks including short range radio communication.
* **Challenge 7**: Latency sensitive. Vehicle safety applications allow a certain degree of latency depending on safety services requirements and on the network characteristics. Safety applications such as ‘pre-crash warning’ or ‘lane changing assistance’ require real-time communication processing ability. To exchange this kind of emergency information and invoke safety critical controls for vehicle or alerting to the driver, a low latency communication within 35ms should be supported. However, some safety services, like emergency vehicle approaching notice can tolerate seconds of latency. Network is required to support a low latency communication to exchange emergent information within a certain period of time to guarantee the reliability of communicating with nearby vehicles.
* **Challenge 8**: The security issues. Highly attention should be attached to the security of vehicle network, it not only concerns of general network security, like personal information and privacy protection, but more importantly, it could be a threat to passenger’s life when the vehicle’s status data is modified deliberately or the vehicle is malicious manipulated by other people. Security of network of vehicles is a rather difficult issue due to complex technologies and sharing of sensitive information of a networked vehicle. Information of vehicles should be protected from any malicious use such as invoking of malfunction, abuse of private information, and so on. Therefore, network is required to keep safe through protocols and cryptographic mechanisms deployed in vehicle terminal and network elements.

**8.2 Consumer Electronics**

Consumer electronics is the electronic products designed for consumer’s work, entertainment, and ultimately to the purposes which consumers enjoy the convenience of life.It focues on electronic products include household appliances and portable electronic products. The household appliances used in the home with fixed characteristics, one is the video entertainment products such as television and home video game, the other is the smart home equipments such as air conditioners, washing machines, refrigerators. The portable electronic products which have mobile characteristics, such as mobile phones, PAD, electronic reader, digital photography products.In this section, we focused on the second category of consumer electronics, portable consumer electronics.

At present, the development of portable consumer electronics shows the trend of the core of video, mobile and wireless technologies. With the development of manufacturing process, the consumer electronics terminal functions is more powerful which has more  processing power ,display capabilities,  information receiving capacity.On one hand, it can display information from the Internet, radio, satellite, digital cameras and video cameras, phones and other sources. On the other hand, the volume of consumer electronic devices gets smaller and smaller, which is more portable. In addition, the rapidly growth of wireless technology makes consumer electronics, one-way information receiving and two-way information exchanges becomes more readily available.It also makes information content exchange between different consumer electronics more convenient, so that the same content can called on different terminals in different locations.

**8.2.1 Ecosystem Description**

In the portable consumer electronics the ecological system, there are four roles：terminal providers, content providers, network providers and the platform provides，each role provides the corresponding product or service.



Figure Portable consumer electronics ecological system

The terminal providers provides terminal product to consumers. Terminal product includes the following categories: Tablet PC, electronic reader, gaming devices, digital photography products, smart phones (which have the characteristics of the previous class of products). The role of the terminal providers is generally played by terminal manufacturers, the internal ecosystem of device manufacturers, including hardware manufacturers, operating software providers, integrators, and so on, which should not be included in this topic.

Content providers provided various forms of content, including video, text, games, pictures, voice which rely on the different types of terminals. Content providers are divided into commercial and individual consumers by the purposes of profit-driven, the former one provides all the content to the terminal for user to get profit (such as games, video, e-books), the latter is release of private information to the terminal (such as picture, text, voice).

Network provider is a bridge that connects various contents and the terminals. Network providers provide wide range wireless connectivity for global voice and data network such as 2G \ 3G \ WIFI, etc., to meet the requirement of this content-to-end mode. In this case, the network provider's role is mainly played by the telecom operators.

The platform is a carrier of content publishing, which faciliates the exchange of information between content provider and terminal.Various types of terminals can acquire the relative content through platform. Content providers can publish the related content on the platform and derive income. In general, platform is corresponding to the terminal, different platforms corresponding to different devices. Platform provider role has more diverse, there may be an independent platform provider, is also possible that by the terminal manufacturer, content providers, network providers to serve.

**8.2.2. Representative Use Cases for the Consumer Electronics Sector**

From the use of portable consumer electronics products, it includes reading and writing the text, viewing the video and pictures, playing games, making voice calls, photography.A Pad is the most common personal portable consumer electronics to meet the basic one or more of the above purposes, which includes PDA, handheld computer, and E-reader, mp4, electronic games with a certain processing power and network communications capabilities. It general has a certain size screen capable of displaying content information such as video, games, pictures, sounds, text. It can be connected through a wireless network platform (not necessarily the same platform) to get content acquire, transfer and publish. As a typical representative of the consumer electronics industry, the Pad has a good blend of the four roles of terminals, contents, platforms, networks. Some Pad terminal providers at the same time provide a platform, so that content providers can publish content, terminal user can access to content, such as app store of Apple's iPad; some terminal providers provide a platform bunding with telecom operators’s network, such as Amazon's the Kindle; some content providers provide platforms and terminals, such as the cloud bookstores and bambook of electronic reader.

From the bussiness model of the Pad, we can see that through wireless network connected to the platform to access content has become a mainstream model. Network providers wish to see that because there are more and more users use their wireless network services, however, it brings more wireless network challenges.

**8.2.3 Solution Design Implications**

The challenges the portable consumer electronics faced including the following:

The network connection brings challenges about battery life. More and more portable consumer electronics products are in the network connection status, which make terminal power decreased rapidly. Terminal size and weight is more and more light and thin, simply increasing the battery capacity becomes infeasible. How to optimize network connection, reducing the energy consumption of the terminal access, network switch, and online access is the key to improve battery efficiency.

Most of the portable consumer electronics products access network via WIFI, only a few products via telecom networks. WIFI resources do not specification like the telecom network resources, as the standardization of WIFI resources, the consumer electronics products which only support the WIFI Transfer Protocol will face the network access WIFI problem.

**8.3 M-Health**

Development of modern information communication technology is opening a new opportunity to improve access to healthcare, which facilitates the appearance of M-Health. From a health data oriented point of view, an M-Health application includes four essential parts, data collection, data transmitting, data processing and result feedback.

Firstly, in order to fulfill data collection, the patient or monitored person typically uses one or more sensor devices that record not only biological signs (such as blood pressure, body temperature, heart rate, weight, etc), but also activity information of his/her body(such as walking, running , disable status, etc). Secondly, data transmitting involves the use of a lot of wireless technologies, including both short range network technology (such as Bluetooth, Zigbee, etc) and wide area network technology (such as Second Generation, Third Generation, Long Term Evolution, etc). Thirdly, large amount of collected data is processed by a back-end entity, which may physically be a platform or an application server. Finally, medical professionals and/or patients can access to the analysis results and get some feedbacks.

**8.3.1 Ecosystem Description**

M-Health ecosystem is shown in the figure below. This figure points out some key roles and demonstrates their typical elements.



Figure Ecosystem of M-Health

* **End point provider**

It provides sensors and actuators. Sensors and actuators have to cope with severe limitations on form factor and battery consumption because of the impact on human body. Actuators may also convert digital electronic signals from the information networks into operations.

* **Device provider**

It provides two types of devices including terminals and gateways. Their functions are quite similar. The main difference between them is that a gateway usually acts as an anchor between short range networks and wide area networks, while a terminal only appears in a wide area network. Some devices used by mHealth belong to medical devices which must be compliance with medical device rules.

* **Network provider**

It provides public connectivity for transporting M-Health data. Furthermore, M-Health specific enhancements upon networks are become more attractive to cater new requirements, such as alarm messages always need to be delivered securely and quickly, location tracking needs to be supported, etc.

* **Platform provider**

It provides platform which is based on a set of capabilities in the form of software modules that are offered to the M-Health applications in order to accelerate their development, test, and deployment life cycles. Some examples of these modules are device management, conversion and storage of monitoring data, Business to Business (B2B) administration and so on.

* **Service provider**

It provides the M-Health service to their end users. It is mainly responsible for the daily operations of the M-Health service and is responsible for user assistance and billing, if applicable.

* **End user**

It is the recipient of health services, often labeled by its insurance status: insured or uninsured, privately or publicly insured etc. for the purposes of financial case management and clinical case management.

To be noted, some special roles also belong to M-Health ecosystem, such as regulator, insurance provider and Standardization Development Organization (SDO).

* **Regulator**

It develops laws and/or regulations and/or policies to ensure a secure, effective operation environment for M-Health ecosystem.

* **Insurance provider**

It provides financial support services against the risk of incurring medical expenses among individuals.

* **Standardization Development Organization**

It provides standards to comply, aiming to reduce cost and guarantee interoperability For example, some influential SDOs in M-Health sector are European Telecommunications Standards Institute (EIST), Continua Health Alliance (CHA), Health Level Seven (HL7), Integrating the Healthcare Enterprise (IHE), IEEE and so on.

**8.3.2 Representative Use Cases for the M-Health Sector**

According to different emergency level, M-Health can be classified into two types: general service and emergency service.

Use case 1: General service of M-Health



Figure General service of M-Health

1. A patient can obtain his biological signs (e.g., Electro Cardio Gram, temperature, blood glucose, blood pressure) through body-embedded sensor devices, wearable sensor devices, or sensor devices around him. Besides, motion information (e.g., walking, running, and disable status) of the user and other context information (e.g., monitoring time, position) may also be gathered by related devices.
2. Gathered information will be uploaded to an M-Health platform, by direct connection into the network or by wireless gateways between the network and the patient environment. If information collected through the short-range wireless network (such as Bluetooth, Zigbee, etc) is transmitted to a gateway, then it will be uploaded by the gateway through a wide area network (such as Second Generation, Third Generation, Long Term Evolution, etc).
3. An M-Health platform is responsible for data processing, addressing fragmentation of various Health Information systems, providing effective devices management and other service support functions (e.g., authentication, traffic control, and B2B administration). This platform can be provided by a network operator or a 3rd platform provider.
4. Care providers (e.g., clinicians, health care assistants, family members, fitness coaches) can have access to personal data of monitored patient via web/PC/mobile and make feedbacks about the patient’s health situation.
5. The patient himself can also have access to his personal data and review his feedbacks via web/PC/mobile.

Use case 2: Emergence service of M-Health

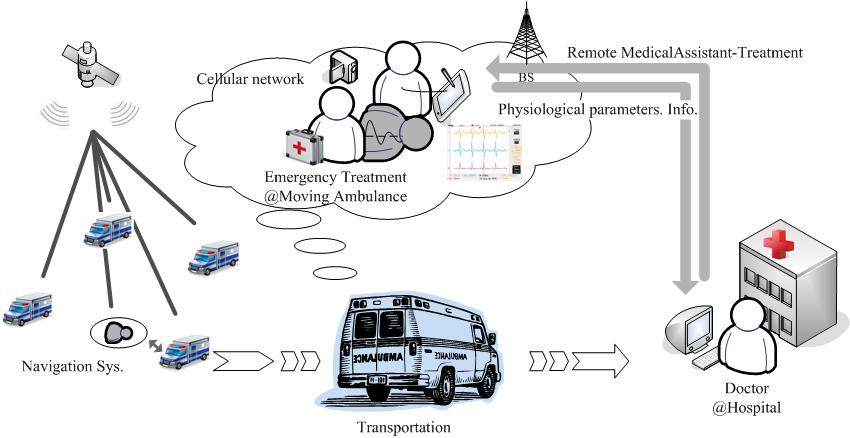


Figure Emergency Service of M-Health

Pre-hospital emergency medical service (PEMS), which is a kind of emergency services of M-Health, can be understood as an emergency medical treatment for patients injured by accidents or life-threatened disease from the onsite location to hospital; it can reduce the time and allay the costs of patient transportation significantly.

* 1. Ambulances install navigation system with positioning system, e.g., GPS, and wireless communication network, e.g., GPRS. By GPS satellite positioning system, emergency medical service center can know the locations of the patient and available ambulances and quickly send an ambulance which is the most nearby. At the same time, the navigation system can also show to the ambulance team the most effective path to the hospital.
  2. The emergency medical doctor should give an instant treatment according to the real-time physiological signals of the remote patients, such as ECG, heart rate, oxygen saturation, blood pressure, respiratory rate etc. Despite unstable environment of the moving ambulance, the physiological signal monitors must be transmitted in a guaranteed manner so that the doctor can collect the high quality vital signals. Besides, the communication terminals on the ambulance must resist the fast fading when vital signals are transmitted to the hospitals via mobile networks.
  3. Remote medical assistant-treatment makes possible for patients in ambulance needing special medical care to have face-to-face consultations with specialists that are situated in hospital or another far away medical institution. In other words, it enables the emergency medical doctor to send the medical sounds, images and video, captured using medical peripherals, to a doctor in hospital to be used to make a diagnosis for a patient.

**8.3.3 Embedded Module Requirements and Solution Design Implications**

For wider deployment of M-Health, there are still some significant challenges as follows:

Challenge 1: Privacy protection. Whenever patient information is exchanged, stored, or processed, the confidentiality of the data must be enforced and safeguarded by the M-Health applications. All exchanges of data between the M-Health partners must be performed in a way that prohibits any unwanted disclosure of data.

Challenge 2: Cost issues. While enjoying the benefits of M-Health, end users are not willing to afford high expense. M-Health services and devices must be cost-effective.

Challenge 3: Interoperability of heterogeneous systems. Before M-Health systems become fully-standardised, interoperability will be a big concern of ecosystem players, all of whom using different platforms and systems.

Challenge 4: Regulation considerations. Regulation, particularly medical device regulation, has also impacted the growth of the M-Health market. Solution vendors who do not follow the regulations should be kept out of the market as they would increase risks, in the end-to-end solution.

**8.4 Smart Metering**

Smart metering is the service in which the smart meters automatically report their energy consumption to the server (Fig 4). The smart meter may be the electrical meter, gas meter, water meter, heat meter or many other kinds of meters. Based on the reported data, people may have a detail analysis on the consumption behaviour so make a corresponding right action. So furthermore, the utility may initiate the load control to cut down the energy consumption. As people recognize the energy and natural resource shortage more and more clearly, smart metering becomes an important service and help people to manage the energy or natural resource better. There are now more than two hundred smart metering projects or announced plans around the world (Fig 5). Much more smart metering projects will start in the future. It is estimated there will be about 1 billion smart meters serving for the people around the world in the year of 2020 (Pike, 2011).

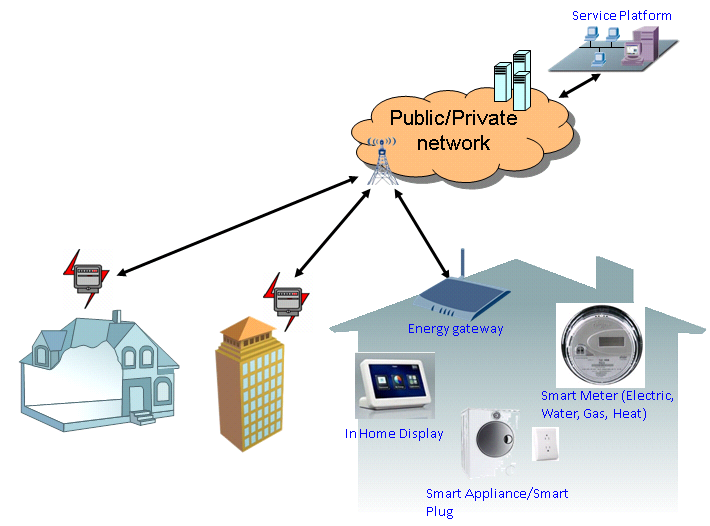


Figure 15 Smart metering system



Figure 16 Smart metering project (Google, 2012)

**8.4.1 Ecosystem Description**

The smart metering ecosystem contains several roles in the value chain. This section will give some descriptions and analysis on each role in the ecosystem. In the ecosystem, the utility and the end user lie in the two ends of the chain. The utility is the energy provider who is in charge of the energy generation, transmission and distribution. Some utilities may only focus on the energy transmission and distribution, and purchase energy from others like the electrical plants. The utility may get a few benefits from the smart metering. Firstly, it can cut down the manpower requirement because the automatic meter reading doesn’t require again specific persons to hand-write down the meter reading values home by home. Secondly, according to the analysis of the metering data, the utility can have further knowledge of each customer. The utility can forecast the energy consumption including the peak hour so that to accurately generate, transmit and distribute the energy. The extra investment for the peak load can be saved. Thirdly, the utility can even make a control on the energy usage. Load control and demand response can decrease the fluctuation of the energy consumption. Fourthly, the utility can provide better energy service for its customers. Besides increasing the reliability, the utility may provide more flexible tariffs for the customers, like the TOU tariff and block tariff.

While from the end user side, some benefits can be earned from the smart metering also. Firstly, the end user may have improved visibility of energy use. He may then change his living style a little in order to decrease the energy consumption. Secondly, the end user can reduce his cost on energy through selecting an appropriate tariff and schedule the energy usage well. Thirdly, the end user may acquire much convenience. He may purchase the energy through the prepayment.

The communication network is indispensable for smart metering. It may be set up and managed by the utility itself, or the third party telecom operator. There are several advantages to involve telecom operator into the ecosystem. Firstly, the telecom operators have much experience on the communication network setting up and operating. Secondly, the telecom operators may build a horizontal solution to decrease the cost on the communication network. Thirdly, the utility may get benefit from the telecom services by binding the smart metering and the telecom services together to make a new business model.

The telecom vendor which is in the ecosystem provides the communication network equipments. It mainly focuses on the WAN devices, sometimes including WAN terminal like home gateway. The telecom vendors may depend on the telecom operators or provide the equipments to the utilities if the latter build the communication network by themselves.

Metering devices vendor, unlike the telecom vendor, mainly focuses on the HAN and NAN devices, like the smart meters, in-home displays, and smart plugs etc. Some metering devices vendors may have had a lot of cooperation with the utilities since many years ago, even before the smart metering coming forth. They have much expert in the energy area.

Software vendor is also a very important role in the value chain. It may provide two kinds of software. One is oriented to the utility and the other is oriented to the home users. It’s important for the utility to manage the metering data. After collection of these data, storage, search, processing and analysis of these data are implemented by the metering data management (MDM) system. On the other hand, the home users may have the energy analysis software in their terminal like smart phone or in-home display, to show graphs and texts about the detail energy usage analysis.

System integration plays a special role in the ecosystem. It provides a total solution instead of a specific device or software. It may cooperate with different vendors and integrate their products into a whole smart metering system. Then the whole smart metering system can be provided to the utility.

White goods manufacturer can be involved in the ecosystem too. The smart metering system may extend to include the smart appliances like the smart refrigerators, smart air conditioners, and smart clothes washers etc. The energy management is a good selling point for the white goods, so the manufacturers can make their products more competitive. On the other hand, the home users can get benefits on more detail management on the home energy consumption.

**8.4.2 Representative Use Cases for the Smart Metering Sector**

In this section, some typical use cases of smart metering will be addressed. The first one is automatic meter reading, which is also the basic use case of smart metering. The smart meters periodically report their metering data to the MDM server. The report period is usually from several minutes to one month. It may be enough for the smart meter to report its data once a month for bill. A period up to several minutes helps for the accurate energy consumption analysis. In some cases, the server triggers the meter to report data, i.e. on-demand metering. The server may poll the meter very fast, saying once several seconds, in some special cases, in order to acquire enough data for diagnosis.

The utility can charge the energy consumption based on the meter reading. Various types of tariffs like TOU tariff or block tariff can be provided by the utility, because the utility can know much more accurate energy consumption information. TOU tariff provides several tiers in different time during a period like a day, while block tariff charge differently for the consumption sections belonging to different volume zone divided by some specific thresholds. These two policies can be combined together. But then it requires telling the detail charging related information like time and thresholds to the customers. The server can publish this information and also other public information like weather forecasting to the customers. Furthermore, prepayment can be done at home. The home user may select or change the tariff type, and finish the transaction of energy purchase through the in-home devices.

Another use case is load control and demand response. The server may send a load control command to the in-home devices, to solicit them to decrease their energy consumption or shut down voluntarily, or to force them to shut down. The in-home devices will then react to the load control request and send back a demand response to report the current status of the devices. Then the utility can have more control on the energy consumption to make the grid more reliable and be more flexible to adjust the energy supply. The load control may also bind with the charging policy. For example, during the peak consumption hours, the energy cost will be high, and the server sends load control request to the in-home devices. The devices can select to shut down or to keep the operation depending on whether the user cares about the excess peak hour fee. For better operation, devices and service management can also be provided by the smart metering. The smart metering devices will send warning messages to the server if specific events take place, such as the voltage become abnormal, or the communication is detected being interfered. And the smart meter may also provide the features for service management like supplier switching and connection on/off. The server sends a control command to the meter and the meter return a response after the corresponding action.

**8.4.3 Embedded Module Requirements and Solution Design Challenges**

There are a lot of requirements for smart metering on embedded module design. Some are even seemed a bit challenging. In this section, some of these challenges will be addressed.

The first one is the very large amount of devices. As mentioned above, the amount of smart meters will be about 1 billion in 2020. The amount of smart meters is comparable with the population. Furthermore, the meters are usually deployed in a concentrated way. And the meters more or less have concurrency on the communication sessions, saying the meters in one block may report the metering data nearly simultaneously. So lots of burden will be increased onto the current communication network. It’s meaningful to decrease the volume of data sent by each meter, and disperse the network accessing time of the meters.

The second challenge is the changeless position of the smart meters. This issue is severe if the smart metering system depends on the wireless communication. The wireless communication channel is always varied. So it’s very hard to ensure the channel is always good in a specific position. And some meters are even deployed in some places where it is not good for wireless communication. For example, a meter may be put inside a metal box or a cabinet which contains the metal components, the signal will be attenuated a lot across the box or cabinet. And some meters may be deployed in the basement or at the corner of a house, where the wireless signal is usually weak. Unlike the mobile phone services, in which the person can just walk to another position if he notices the signal is weak, in smart metering, the meter itself cannot move to another place. It’s necessary to consider the bad communication condition and increase the link budget.

The third challenge is the low power requirement. Some devices, like the gas meter and water meter, are hard to use the mains power. They operate with the batteries. Some other devices can operate with mains power. But it should be considered maintaining their communication at least for a while like two hours when the mains power is cut down by accident, so batteries as backup power will be used also for these devices. For the battery powered devices, it would be unacceptable to change or charge the battery once every month or several days. The low power feature should be considered for the communication mechanism, and the battery life should also be considered, to decrease the frequency of changing or charging the battery.

The fourth challenge is the security issue. The smart metering data contains some key information and need high security protection. It should be reconsidered whether the current security mechanism of WAN and HAN is enough for smart metering. The smart metering system relates to some stakeholders, such as the utility, the telecom operator and the home user. It should be ensured that each stakeholder is able to get their data but cannot get access to those of others. At the same time, the security mechanism should not add burden on the network infrastructure investment and so infrastructure sharing may be encouraged. Another point is the physical protection of the smart metering infrastructure. So theft detection and vandalism avoidance should be considered. And even if some smart metering devices are physical compromised; the security of other devices should not be hurt.

The fifth challenge is the industry level design. Unlike the personal devices such as mobile phones or PCs, the smart metering terminals require much on the reliability and size. The device can be used in some severe environments and have a long life such as 10 years. Due to the small size of the whole device, the space left for the communication module would not be very large. A compact modules arrangement should be considered well.

**8.5 Logistics**

Logistics is a whole process of planning, implementation and management. In this process, raw materials, semi-finished products and finished products are fully controlled by means of transportation, warehousing and distribution. The scope of the process is from original place of production to the consumption place of the production. The logistics services are provided in the cost-effective and more reliable manner with a high level of customer satisfaction.

The newborn IoT (Internet of Things) opens up a new era. Based on the Internet, it's a goods based global network, which makes real-time sharing of goods information possible with the help of RFID, EPC coding and wireless data communication technology. The ultimate objective is to build an open system with unified standard, intelligent tracking and managing capabilities. In this system, every goods could be identified and be communicated with the others.

With the capability of single goods tracking on the global basis, IoT improves the monitoring ability in every section of logistics service, facilitate the development of the logistic industry, and finally optimize the resources distribution for the whole society.

The main sections of IoT technology involved logistics activities are transportation, warehousing and distribution, as illustrated as the following:



Figure Logistics activities and services

Warehousing management sector:

* Goods safety ensured by warehouse environment monitoring using video camera and infrared alarm device.
* RFID based goods information acquisition system includes the RFID tagged goods tray and a fixed reading device. In the system, the information of the goods can be fast and automatically recorded. The information processing efficiency is improved by using the system.
* Barcode based goods information acquisition system includes bar-coding goods, handheld reading device. In the system, the information of the goods can be fast and automatically recorded. The information processing efficiency is improved by using the system.

Transportation management sector:

* Providing the trace of real-time transport tools for drivers and dispatchers by using the vehicle or ship based terminals to acquire basic parameters of vehicles and ships, the parameters include.
* Assigning dispatching orders through various channels like logistics information service platform, handheld mobile terminal or PC.

Distribution management sector：

* Using handheld mobile terminal to scan information in the business acceptance form, acquiring the information and state of goods through all kinds of identifications of goods.
* Taking photos and uploading acceptance information using handheld mobile terminal. The security and accuracy of the delivery are ensured for the whole service process.

**8.5.1 Ecosystem Description**

Logistics ecosystem includes the seller, buyer, a third party, system integrator, network operator. In the system, goods flow is realized through transportation, warehousing, distribution processes. Combining with other flows like information flow, business flow, cash flow, all the flows support the logistics activities from original place of production to the consumption place of the production for raw materials, semi-finished products and finished products.



Figure Logistics information and information flow in Logistics system

In Figure 18, information flow of goods is introduced. Logistics information consists of basic elements of logistics activities, which includes items, equipment and facilities and the operators. And logistics information service platform plays the role of information service provider for the seller, the buyer and a third party to information flow, as shown in Figure 19.



Figure Logistics Information Service Platform User and function

**8.5.2 Solution Design Challenges**

There is no unified goods identification mechanism, so that logistic related information can’t be shared between different roles in the whole ecosystem, consequently, it’s impossible to utilize the single solution for different enterprises. By comparison with current barcode technology, RFID has more cost and low usage rate.

**8.6 Personal Environment Service**

The vision behind the personal environment service is that of recreating a user’s customized living or working surroundings in accordance with user-defined settings and in response to the user’s mobility. Concepts such as ambient intelligence and home networks could be instrumental in realization of PES. Indeed, integration of elements of these technologies may attract industrial attention and support, which in turn may speed up the implementation and deployment of PES. Moreover, underlying technologies related to the above concepts are envisioned to play a key role in the realization of PES, including mobile communications supported by ubiquitous infrastructure and wireless personal area networks (Jongtaek & Haas, 2010)

PES is the one of the application services of M2M, as defined in ITU-R Recommendation M.1822 (Framework for services supported by IMT), that “The electric, electronic, and mechanical machine surrounding users can be automatically configured according to the pre-defined and/or self-growing user preference.” The conceptual architecture of PES is shown in the figure below.

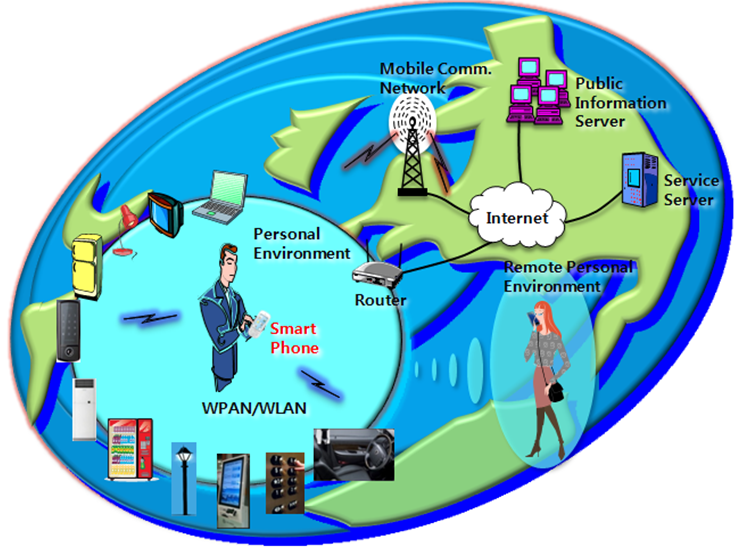


Figure 20 The conceptual architecture of PES

As the user moves in the living environment, the smart phone which includes short range radio communications device and personal preference profile recognizes the surrounding appliances and configures the functions to be optimized to the user, automatically and intelligently. Also the remote service server monitors the user behavior and recommends proper services to the user. So the user can feel safe and comfortable living environment which is upgraded continuously. This new M2M service paradigm could proliferate the business of smart phone and a lot of appliances, and even change the pattern of human life.

**9 References**

1. Research Pike, “Smart Meter Market Forecasts”, 2011
2. Smart Metering Project Google Map, http://maps.google.com/maps/ms? ie=UTF8&hl=en&msa=0&msid=115519311058367534348.0000011362ac6d7d21187&ll=53.956086,14.677734&spn=23.864566,77.519531&z=4&om=1
3. Jongtaek Oh and Zygmunt J. Haas, “Personal Environment Service Based on the Integration of Mobile Communications and Wireless Personal Area Networks,” IEEE Comm. Mag., vol.48, no.6, pp.66-72, June 2010.
4. Waltenegus Dargie, Christian Poellabauer, “Fundamentals of wireless sensor networks : theory and practice“,John Wiley & Sons Ltd., 2010
5. Steve Methley, Colin Forster, Colin Gratton, “Wireless Sensor Networks Final Report”, Plextek Limited, 2008
6. APT Wireless Group input document AWF-9/INP-17, AWF-9/OUT-08, AWG-10/INP-17, AWG-10/INP-34, AWG-11/INP-33, AWG-11/INP-43, AWG-11/INP-69, AWG-12/INP-56, AWG-12/INP-57, AWG-12/INP-58, AWG-12/INP-79, AWG-12/INP-97, AWG-13/INP-41, AWG-13/INP-78, AWG-14/INP-38.

\_\_\_\_\_\_\_\_\_\_\_\_