Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14093
Date:	2009-09-29
Replaces:	
Document Type:	Liaison Organization Contribution
Document Title:	Liaison Statement from ITU-T SG 13 to ISO/IEC JTC 1/SC 6 on sensor networks security
Document Source:	ITU-T SG 13
Project Number:	
Document Status:	For your information.
Action ID:	FYI
Due Date:	
No. of Pages:	29

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)

Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;

Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

COM 13 – LS 76 – E

English only

Original: English

Question(s):	3/13	Mar del Plata, Argentina, 2-12 September 2009

Ref.: TD 82 (PLEN/13)

Source:	ITU-T SG 13 (Mar del Plata, Argentina, 2-12 September 2009
Title:	Reply to LS on sensor networks security

LIAISON STATEMENT

For action to:	
For comment to:	
For information to:	**ISO/IEC JTC1/SC6, copy ITU-T SG 16, JCA-NID, ISO/IEC JTC1/SC27, ISO/IEC JTC1/SGSN**
Approval:	**Agreed to at ITU-T SG 13 meeting**
Deadline:	

Contact:	Marco Carugi UK	Tel: +33-6-64047454 Email: marco.carugi@gmail.com

ITU-T SG13 thanks ISO/IEC JTC1/SC6/WG7 for your liaison statement regarding the development of SC6 N14015, ISO/IEC CD 29180 ("Security framework for sensor network").

It gives good insight to understand security issues in sensor networks and contains useful information for our future work in ITU-T SG13. ITU-T SG13 would therefore like to continue to be informed in the future about your progress on sensor network security related issues.

We also wish to inform you that Y.2221 (formerly Y.USN-Reqts) “Requirements for support of USN applications and services in the NGN environment”, has been consented at the September 2-12 2009 SG13 meeting.

We look forward to further collaboration.

Attachment: Y.2221 (formerly Y.USN-Reqts), TD 85 (PLEN/13)

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

STUDY GROUP 13

TD 85 (PLEN/13)

English only

Original: English

Question(s): 3/13 Mar del Plata, Argentina, 2-12 September 2009

TEMPORARY DOCUMENT

Source: Editor

Title: Output draft of Draft Recommendation Y.2221 (Y.USN-reqts), "Requirements for support of Ubiquitous Sensor Network (USN) applications and services in the NGN environment" – for consent

This document is the output draft of Y.USN-reqts, as agreed by the Q.3/13 meeting, Mar del Plata, Argentina, 02-12 September 2009. It is proposed for consent at this WP2/SG13 plenary meeting.

Requirements for support of Ubiquitous Sensor Network (USN) applications and services in the NGN environment

Summary

This Recommendation provides a description and general characteristics of Ubiquitous Sensor Network (USN) and USN applications and services. It also analyzes service requirements of USN applications and services, and specifies extended or new NGN capability requirements based on the service requirements.

Source and History

None

Keywords

Ubiquitous Sensor Network (USN), Sensor Networks, Wireless Sensor Networks (WSNs), NGN, USN applications and services

Table of Contents

Requirements for support of Ubiquitous Sensor Network (USN) applications and services in the NGN environment

1. Scope

This Recommendation, building upon [ITU-T Y.2201], covers extensions and additions to NGN Release 1 capabilities in order to support Ubiquitous Sensor Network (USN) applications and services [b-ITU-T Y.Sub7] in the NGN environment.

The scope of this Recommendation includes:

- Description and general characteristics of USN and USN applications and services;
- Service requirements to support USN applications and services;
- Requirements of extended or new NGN capabilities based on the service requirements.

The NGN functional architecture extensions for support of the identified extended or new NGN capabilities are out of scope of this Recommendation.

2. References

The following ITU-T Recommendations and other references contain provisions, which through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Q.1703] ITU-T Q.1703 (2004), *Service and network capabilities framework of network aspects for systems beyond IMT-2000*

[ITU-T Y.2012] ITU-T Recommendation Y.2012 (2006), *Functional requirements and architecture of the NGN*

[ITU-T Y.2201] ITU-T Recommendation Y.2201 (2006), *NGN Release 1 Requirements*

[ITU-T Y.2201Rev1] ITU-T Recommendation Y.2201 Rev1 (2009), *Requirements and capabilities for ITU-T NGN*

[ITU-T Y.2233] ITU-T Recommendation Y.2233 (2007), *Requirements and framework allowing accounting and charging capabilities in NGN*

[ITU-T Y.2234] ITU-T Recommendation Y.2234 (2008), *Open service environment capabilities for NGN*

[ITU-T Y.2801] ITU-T Recommendation Q.1706/Y.2801 (2006), *Mobility management requirements for NGN*

[ITU-T Z.100] ITU-T Recommendation (1999), *Formal description techniques (FDT) – Specification and Description Language (SDL)*

3. Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 context awareness [ITU-T Y.2201Rev1]: A capability to determine or influence a next action in telecommunication or process by referring to the status of relevant entities, which form a coherent environment as a context. .

3.1.2 network mobility [ITU-T Q.1703]: The ability of a network, where a set of fixed or mobile nodes are networked to each other, to change, as a unit, its point of attachment to the corresponding network upon the network's movement itself.

3.1.3 Open Service Environment capabilities [ITU-T Y.2234]: Capabilities provided by open service environment to enable enhanced and flexible service creation and provisioning based on the use of standards interfaces.

3.1.4 service [ITU-T Z.100]: A set of functions and facilities offered to a user by a provider.

3.2 Terms defined in this Recommendation

This Recommendation defines or uses the following terms:

3.2.1 sensor: Electronic device that senses a physical condition or chemical compound and delivers an electronic signal proportional to the observed characteristic

3.2.2 sensor network: A network comprised of inter-connected sensor nodes exchanging sensed data by wired or wireless communication.

3.2.3 sensor node: A device consisting of sensor(s) and optional actuator(s) with capabilities of sensed data processing and networking.

3.2.4 Ubiquitous Sensor Network (USN): A conceptual network built over existing physical networks which make use of sensed data and provide knowledge services to anyone, anywhere and at anytime, and where the information is generated by using context awareness.

3.2.5 USN end-user: An entity that uses the sensed data provided by USN applications and services. This end-user may be a system or a human

3.2.6 USN gateway: A node which interconnects sensor networks with other networks

3.2.7 USN middleware: A set of logical functions to support USN applications and services. The functionalities of USN middleware include sensor network management and connectivity, event processing, sensor data mining, etc.

NOTE - In the NGN environment, functions of the USN middleware may be provided by the NGN Open Service Environment (OSE) capabilities [ITU-T Y.2234] and/or by other NGN capabilities. However, some of the USN middleware functions (e.g. those for supporting interface to sensor networks) may not be provided by the NGN OSE capabilities or other NGN capabilities.

4. Abbreviations

This draft defines or uses the following terms:

CDMA Code Division Multiple Access

IP	Internet Protocol
ITS	Intelligent Transportation System
MAC	Media Access Control
MAN	Metropolitan Area Network
NGN	Next Generation Network
OSE	Open Service Environment
PHY	PHYsical layer
QoS	Quality of Service
USN	Ubiquitous Sensor Networks
WCDMA	Wideband CDMA
WiMAX	Worldwide Interoperability for Microwave Access
WMN	Wireless Mesh Network
WSN	Wireless Sensor Networks
WPAN	Wireless Personal Area Network

5. Conventions

In this Recommendation:

The keywords “is required to” indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords “is recommended” indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords “can optionally” and “may” indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor’s implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6. USN description and characteristics

Ubiquitous Sensor Network (USN), as defined in clause 3.2.4, is a conceptual network built over existing physical networks which make use of sensed data and provide knowledge services to anyone, anywhere and at anytime, and where the information is generated by using context awareness.

USN utilizes wire-line sensor networks and/or Wireless Sensor Networks (WSNs). WSNs, wireless networks consisting of interconnected and spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions (e.g., temperature, sound, vibration, pressure, motion or pollutants) at different locations, have been studied and implemented since long time as isolated networks. Simple design of applications and services based on isolated sensor networks is made by capture and transmission of collected sensed data to designated application systems.

Such isolated simple applications and services have been evolving with network evolution, network and service integration, data processing schemes enhanced by business logics and data mining rules, context awareness schemes, development of hardware and software technologies, etc. These technical developments enable the ability to build an intelligent information infrastructure of sensor networks connected to the existing network infrastructure. This information infrastructure has been called Ubiquitous Sensor Network (USN) opening wide possibilities for applications and services based on sensor networks to various customers such as human consumers, public organizations, enterprises, government, etc.

USN applications and services are created via the integration of sensor network applications and services into the network infrastructure. They are applied to everyday life in an invisible way as everything is virtually linked by pervasive networking between USN end-users (including machines and humans) and sensor networks, relayed through intermediate networking entities such as application servers, middleware entities, access network entities, and USN gateways. USN applications and services can be used in many civilian application areas such as industrial automation, home automation, agricultural monitoring, healthcare, environment, pollution and disaster surveillance, homeland security, military field, etc.

Support of USN applications and services may require some extensions and/or additions to core network architectures in order to cover the functional capability requirements extracted from USN applications and services. USN applications and services are provided through many network assisted functionalities such as context modelling and processing, orchestration of sensed information, data filtering, content management, open interface functions, network and software management, sensor profile management, directory services, etc.

Figure 1 shows an overview of USN with related technical areas including physical sensor networks, NGN, USN middleware and USN applications and services.

NOTE - The details of physical sensor networks and USN middleware are out of scope of this Recommendation.

NOTE - Figure 1 is not a functional figure. The positioning of USN applications and services, USN middleware, NGN and sensor networks in this figure does not correspond to functional layering.

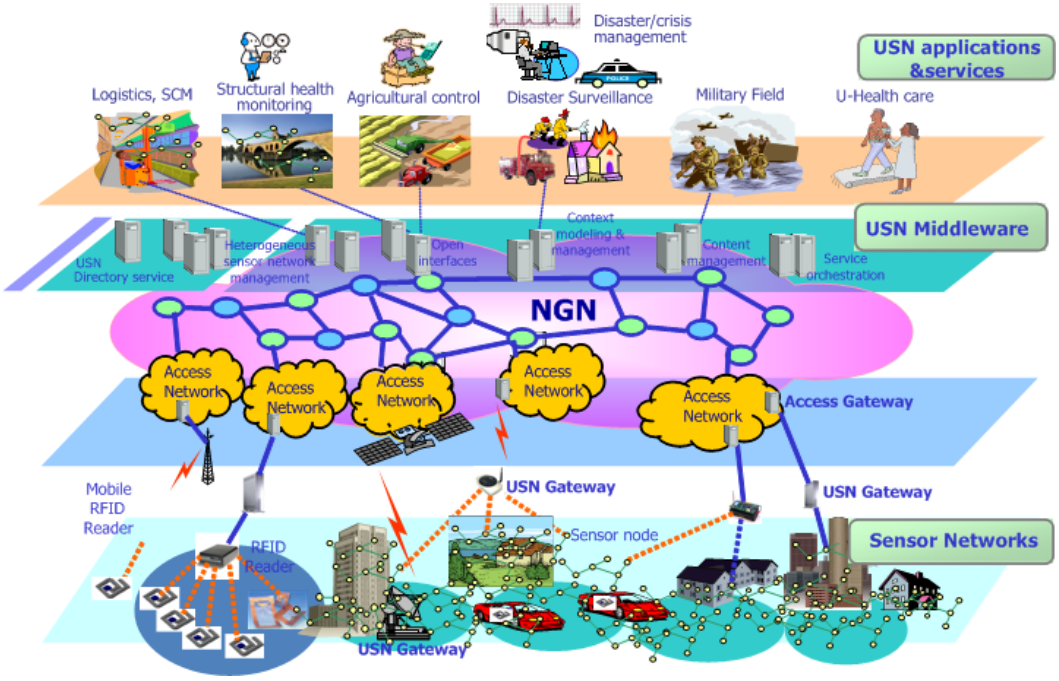

Figure 1 – An overview of USN with related technical areas

For support of USN applications and services, network and service functions have to be carefully designed to support the unique characteristics of sensor networks and their applications and services, including:

- Limited capabilities of sensor nodes;

  NOTE - sensor nodes generally have limited bandwidth, low processing power, small memory size such as 32K, etc.

- Limited power that sensor nodes can harvest or store;

- Harsh and dynamic environmental conditions which cause high possibility of node and link failure;

- Mobility support of sensor nodes, sensor networks and services;

  NOTE - Due to limited hardware capability, mobility capabilities may not be fully supported by a sensor node or a sensor network.

- Dynamic network topology;

  NOTE - sensor networks often dynamically change the topologies due to association and de-association of sensor nodes

- High possibility of communication failures (due to low bandwidth, link failure, etc.);

- Heterogeneity of nodes;

  NOTE – A USN application or service may be built using more than one sensor network where sensor nodes use different PHY/MAC or differently operate in IP or non-IP based

- Large scale of deployment.

  NOTE - A USN application or service can be deployed in geographical scale to monitor environmental conditions such as condition of river, seashore, etc.

These characteristics impact many technical areas of USN applications and services in NGN environment as described in clause 7.

7. Service requirements of USN applications and services

The following are service requirements of USN applications and services which impact the NGN capabilities. These requirements are used to fetch the required extensions to the set of NGN Release 1 capabilities.

NOTE - Appendix II provides requirements which do not directly impact the NGN capabilities. They are provided for informative purposes.

7.1. Sensor network management

IP based sensor networks and non-IP based sensor networks using various types of wired and/or wireless connection can co-exist in USN applications and services. Therefore, it is required to manage diverse types of sensor networks. Non-IP based sensor networks are often managed through their gateway. IP-based sensor network includes the case of a single sensor node directly connected to the NGN, while sensor networks are often managed as a set.

Configuration and reconfiguration of sensor networks may require different mechanisms than traditional network management as sensor networks are normally a group of nodes. A sensor

network must not loose its connectivity or its lifetime when a single node in the network has lost connection due to link or hardware failure which has high probability in sensor networks. Configuration and reconfiguration of a sensor network are used to support assurance of connectivity and lifetime management.

Thus, USN applications and services have the following requirements in order to be supported by various types of sensor networks:

1) It is required to manage IP based sensor networks including the case of a single node directly connected to the NGN.
2) It is required to manage non-IP based sensor networks.
3) It is required to support configuration and reconfiguration of sensor networks for assurance of connectivity and lifetime management.

7.2. Profile management

7.2.1 Service profile

In USN environments, a sensor network and its sensed data are utilized by several different applications and services, so sensed data are manipulated as different service data according to the different needs of applications and services. User demands also vary application by application and service by service.

USN service profile is a way to support the various characteristics and demands of sensed data usage. USN service profiles are composed by information sets of USN applications and services and may include service identifier, data types, service provider, location information, etc. Thus, USN applications and services have the following requirement:

1) It is recommended to use a standard set of USN service profiles to register and discover USN services.

7.2.2 Device profile

In USN applications and services, a device profile consisting of the information of sensor networks and/or sensor nodes can be optionally provided in conjunction with USN service profile. Unlikely traditional networks, only a group of sensor nodes provide meaningful data for general USN applications and services, while data from a single node are also meaningful in some other types of USN applications and services. As there are various types of sensors, sensor nodes and sensor networks, device profiles would help to manage the large number of heterogeneous nodes and networks. The information of device profiles may include sensor network identifier, device identifier, device types, capabilities, location, etc. Thus, USN applications and services have the following requirement:

1) It is optional to use device profiles containing sensor network related information.

7.3. Open Service Environment

7.3.1 Service registration and discovery

In order to discover USN applications and services, USN services should be registered beforehand. The association of an identifier of a sensor network and sensed data should be registered to service directories. As USN applications and services are very diverse, efficiency of registration and discovery may be increased by a standard set of service profiles (see clause 7.2). USN end-users

and applications should be able to discover the registered services by specifying one or more attributes.

For some USN applications and services, devices in sensor networks may need to be registered and discovered as well as USN services. If a device owner does not want to allow the device to be accessible by others, however, the device does not need to be registered or discovered. In order to provide device discovery, devices need to be registered with various attributes. USN end-users and applications may be able to discover the registered devices by specifying one or more attributes.

In addition, a USN service description language is required to be provided to support service registration and discovery.

Thus, USN applications and services have the following requirements on service registration and discovery:

1) It is required to support at least one USN service description language and its associated execution framework.
2) It is recommended to register and discover USN services based on a standard set of USN service profiles.
3) Registration and discovery of sensor network devices may be supported.
4) Context-awareness can be optionally supported in service discovery for USN applications and services.

7.3.2 Service composition and coordination

It is useful to enable easy service creation by reuse of existing resources and composition of services. Thus, USN applications and services have the following requirement to be supported on service composition and coordination:

1) It is recommended to support service composition and coordination for creation of USN applications and services.

7.3.3 Inter-working with service creation environments

New USN applications and services can be provided via integration with other services (e.g., integration with messaging service, or integration with other USN services). In order to support integration of USN applications and services with features of other service creation environments, inter-working with service creation environments is recommended to be supported. Thus, USN applications and services have the following requirement on inter-working with service creation environments:

1) It is recommended to support inter-working with other service creation environments for creation of USN applications and services

7.4. QoS support

7.4.1 Differentiated Quality of Service and data prioritization

USN mission-critical applications and services should be carefully managed. QoS may be a key technical issue in some scenarios. For example, emergency notification of a fire case must be delivered by time-critical and reliable way to national treasure monitoring systems. As USN applications and services are supported over existing network infrastructure, the emergency data are often carried over the network infrastructure to provide alarm notification. Thus, USN applications and services have the following requirement:

1) It is recommended to provide differentiated Quality of Service and data prioritization according to the specific USN service requirements.

7.4.2 Application traffic control

Besides the prioritization of certain types of data, efficient traffic and resource management for the sensed data may increase the Quality of Service of USN applications and services, as in general the application transaction volume due to USN applications and services is usually very high. The following requirements are placed on both infrastructure network and application/service provider's resources:

1) It is required to manage the transaction volume generated by USN applications and services.

2) It is recommended to be able to avoid access concentration to a single resource.

7.5. Connectivity

In IP based sensor networks, sensor nodes are networked using IP. Although the underlying wired and/or wireless media access control manages the connectivity, connections between USN end-users and sensor networks are through IP. In this type of sensor networks, it may be possible that a single sensor node is directly connected to the infrastructure networks without a USN gateway, however, USN gateways are normally used to interconnect sensor networks with infrastructure networks.

In non-IP based sensor networks, sensor nodes do not have IP addresses, and the connections between USN end-users and sensor networks are through USN gateways.

The different types of sensor networks have to able to connect to the infrastructure networks, so the following requirement applies:

1) It is required to support connectivity between sensor networks and infrastructure networks, regardless of the sensor network type, i.e. IP based or non-IP based and using various types of wired and/or wireless media connections. This includes the case in IP-based sensor networks of a single sensor node directly connected to the infrastructure networks.

7.6. Location-based service support

Location of sensor networks and/or individual sensor nodes needs to be maintained and managed in order to support context awareness with location information for USN applications and services. In addition, service and device discovery can be facilitated by usage of the location information. Thus, USN applications and services have the following requirements:

1) Location information of sensor networks is recommended to be registered for USN applications and services. Registration can be static or dynamic.

2) Location information of individual sensor node can be optionally registered for USN applications and services when the location information of a single sensor node is useful.

7.7. Mobility support

The challenge of achieving mobility in USN applications and services depends on the technologies used in the sensor networks. Existing IP mobility technologies can be adapted for IP based sensor networks. However, to port heavy IP mobile mechanisms into very low-power, low-rate sensor networks pose various challenging issues.

A typical USN application and service scenario illustrating mobility requirements can be found in the healthcare application domain. For instance, medical check-up data of a patient may be monitored via a sensor network. Several sensors may be attached to the patient, resulting in a body area sensor network. The sensors periodically gather the medical check-up data and send them to his/her doctor via a home-gateway when he/she is at home; while moving, the data can be sent via an access gateway in a network-enabled car, bus, train, or subway. Various cases of mobility may occur in such an application scenario.

The mobility scenarios for USN applications and services can be classified into three mobility cases:

- A sensor node moving within a sensor network, namely intra-sensor network mobility;
- A sensor node moving across multiple sensor networks, namely inter-sensor network mobility;
- A sensor network moving across infrastructure networks (e.g., across NGN and non-NGN), namely network mobility.

The first two cases can be managed by sensor network technologies which do not have impact on the infrastructure networks, unless there is a need for location tracking of a single sensor node. The last case requires support of existing mobility technologies of infrastructure networks. Thus, USN applications and services have the following requirements on mobility:

1) It is required to support network mobility when a sensor network moves across infrastructure networks.
2) Infrastructure networks are required to support intra-sensor network mobility and inter-sensor network mobility when location information of a moving sensor node is required to be traced.

7.8. Security

In general, USN applications and services require strong security, due to very sensitive sensed data. It has to be considered that tiny sensor nodes cannot provide all security features because they have lots of system limitations. Thus, the sensed data carried over infrastructure networks may not have strong encryption or security protection. Thus, USN applications and services have the following security requirements:

1) It is required to support key management schemes for USN applications and services.
2) It is recommended to support scalable key management schemes for USN applications and services operating with sensor networks of large size.
3) It is recommended to provide security for the aggregated data when sensed data from two or more applications and services are integrated in infrastructure networks for creation of new services.
4) The security approaches for support of USN applications and services are recommended to be consistent with the general approach for security in the NGN.

7.9. Identification, authentication and authorization

Network providers and USN service providers must verify the identification of users to access USN applications and services. There are various issues to be considered, such as protection against unauthorized use of network resources and unauthorized access to information flows and

applications, authentication of users which try to access to the NGN registration and discovery service for sensed data.

In USN applications and services, data can have different levels of authentication requirements. For example, in military systems, raw sensed data are as important as service data which are derived from raw sensed data by processing and manipulation from service providers or applications, while this may not be the case for other systems (e.g. hospital systems). Thus, USN service providers or NGN network providers should support authentication and authorization to use either raw or manipulated service data based on the service requirements. Thus, USN applications and services have the following requirements:

1) It is required to support identification, authentication and authorization of users to access USN applications and services based on the security level of service data.
2) It is required to support different levels of authentication for different types of data based on the requirements of USN applications and services.
3) The USN end-users can optionally identify and authenticate network providers and USN service providers.

7.10. Accounting and charging

There may be a number of sensor networks deployed inside a given geographical area. Some of them may be built within a single enterprise domain and some may be directly connected to access networks of a service provider domain. Different accounting and charging requirements might have to be addressed depending on the scenarios of USN applications and services. As an example, there are USN applications and services whose sensed data do not have to be continuously transmitted to the application systems, but it is enough they are transmitted once in a certain period. In these scenarios, the network connections may stay in an idle state for a long time. On the contrary, some other USN applications and services may continuously generate and transmit streaming data. These applications and services may require different accounting and charging policies. Thus, USN applications and services have the following requirement:

1) It is required to support different accounting and charging policies according the different data transaction types of USN applications and services.

8. NGN capability requirements for support of USN applications and services

USN applications and services use NGN Release 1 capabilities but require some extended and/or new capabilities. The capability requirements in this clause below are provided from a high level perspective and are not intended to constitute precise functional requirements for the NGN entities.

8.1 Requirements for extensions or additions to NGN Release 1 capabilities

Based on the service requirements described in clause 7 of this Recommendation, this clause specifies requirements for extensions or additions to the NGN Release 1 capabilities.

8.1.1 Network management

Based on the service requirements in clause 7.1 of this Recommendation, the following additional NGN management capabilities are placed on the NGN:

1) The NGN is required to manage IP based sensor networks including the case of a single node directly connected to the NGN.
2) The NGN is required to manage non-IP based sensor networks.
3) The NGN is required to support configuration and reconfiguration of sensor networks.

8.1.2 Profile management

[ITU-T Y.2201] provides requirements for user profile and device profile management in the NGN. The followings are additional requirements for support of USN applications and services.

8.1.2.1 Service profile

Based on the service requirement in clause 7.2.1 of this Recommendation, the following requirement is placed on the NGN:

1) The NGN is recommended to support a standard set of USN service profiles.

8.1.2.2 Device profile

Based on the service requirement in clause 7.2.2 of this Recommendation, the following requirement is placed on the NGN:

1) The NGN may support device profiles which contain sensor network related information sets.

8.1.3 Open Service Environment

[ITU-T Y.2234] defines the Open Service Environment (OSE) capabilities for the NGN. The followings are additional requirements for support of USN applications and services.

8.1.3.1 Service registration and discovery

Based on the service requirements in clause 7.3.1 of this Recommendation, the following requirements are placed on the NGN:

1) The NGN Open Service Environment (OSE) is required to support at least one standard USN service description language and its associated execution framework.
2) The NGN is recommended to register and discover USN applications and services based on a standard set of USN service profiles.
3) The NGN may support registration and discovery of sensor network devices (e.g. actuator, gateway) for USN applications and services.

8.1.3.2 Inter-working with service creation environments

Based on the service requirement in clause 7.3.3 of this Recommendation, the following requirement is placed on the NGN:

1) The NGN OSE is required to support inter-working of USN service creation capabilities with capabilities of other service creation environments as described in [ITU-T Y.2234].

8.1.4 Quality of Service

The NGN Release 1 defines Quality of Service capabilities for the NGN. The followings are additional requirements for support of USN applications and services.

8.1.4.1 Application traffic control

Based on the transaction and traffic-related requirements in clause 7.4.2 of this Recommendation, the following additional requirements are placed on the NGN:

1) The NGN is required to support QoS capabilities to sustain the transaction volume caused by USN applications and services.
2) The NGN is recommended to support QoS capabilities preventing from access concentration to a single resource (e.g. USN data repositories).

8.2 Requirements supported by existing NGN release 1 capabilities

Based on the service requirements in clause 7 of this Recommendation, this clause specifies requirements supported by existing NGN Release 1 capabilities.

8.2.1 Open Service Environment

8.2.1.1 Service composition and coordination

The NGN Release 1 provides service composition and coordination capabilities. The service composition and coordination requirement specified in clause 7.3.2 of this Recommendation is supported by existing capabilities [ITU-T Y.2234].

8.2.2 Quality of Service

8.2.2.1 Differentiated Quality of Service and data prioritization

The NGN Release 1 provides QoS supporting capabilities in terms of differentiated Quality of Service and data prioritization. The differentiated Quality of Service and data prioritization requirement specified in clause 7.4.1 of this Recommendation is supported by existing capabilities of the NGN Release 1.

8.2.3 Connectivity

The NGN Release 1 provides connectivity capability. The connectivity requirement specified in clause 7.5 of this Recommendation is supported by existing connectivity capabilities of the NGN Release 1.

8.2.4 Location management

The NGN Release 1 provides location management capability which determines and reports information regarding the location of users and devices within the NGN. The location management requirements specified in clause 7.6 of this Recommendation are supported by existing location management capabilities of the NGN Release 1.

8.2.5 Mobility

The NGN Release 1 provides mobility support for the NGN. The mobility requirements specified in clause 7.7 of this Recommendation are supported by existing capabilities of the NGN Release 1 [ITU-T Y.2801].

8.2.6 Security

The NGN Release 1 provides security capabilities. The service requirements specified in clause 7.8 of this Recommendation are supported by existing security capabilities of the NGN Release 1.

8.2.7 Identification, authentication and authorization

The NGN Release 1 provides Identification, Authentication and Authorization capabilities. The service requirements specified in clause 7.9 of this Recommendation are supported by existing capabilities of the NGN Release 1.

8.2.8 Accounting and charging

The NGN Release 1 provides accounting and charging capabilities. The service requirement specified in the clause 7.10 of this Recommendation is supported by existing capabilities of the NGN Release 1 [ITU-T Y.2233].

9. Reference diagram of NGN capabilities for support of USN applications and services

The reference diagram of NGN capabilities for support of USN applications and services is shown in Figure 2, based on the service requirements of USN applications and services described in clause 7 and the NGN capability requirements for support of USN applications and services described in clause 8. The functional capabilities in the figure show extended or new NGN capabilities as well as existing NGN capabilities to support USN applications and services. The related NGN architecture details are out of scope of this Recommendation.

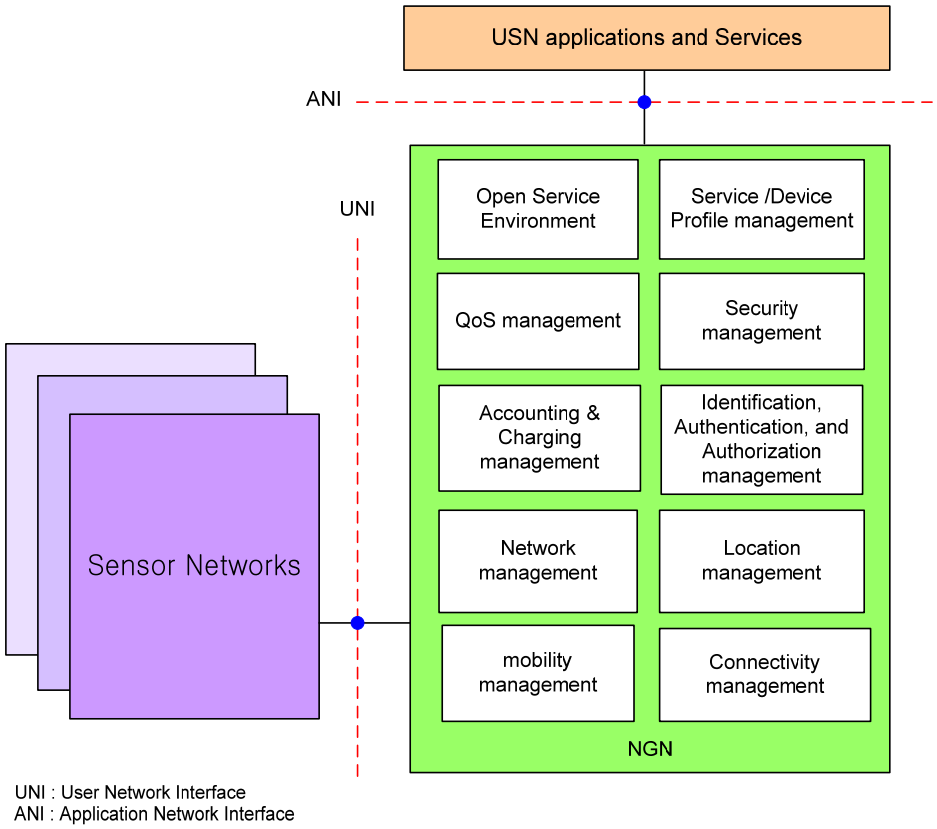

Figure 2 – Reference diagram of NGN capabilities for support of USN applications and services

Appendix I: Use cases of USN applications and services

(Appendix is not an integral part of this document)

Detail analysis of USN applications and services is out of scope of this document but some use cases are listed here because they imply market needs and technical issues.

The USN applications and services can be listed by different market field perspective as follows:

- Automation, monitoring and control of manufacturing & industrial applications;
- Home automation;
- Agricultural monitoring;
- Monitoring and management of building and utility;
- Health care & medical research;
- Environment, pollution & disaster surveillance;
- Chemical, biological, radiological and nuclear (CBRN) sensor based applications;
- Homeland security;
- Military;
- Intelligent transportation management; and,
- Vehicle communication.

The list is not complete, as USN applications and services are emerging markets and the applications and services constantly evolve.

USN applications and services are various and it is necessary to classify with various business and technical factors. However, the following three examples can show use-cases of USN applications and services over the NGN.

A. Weather Information service

One example of USN use-case connecting to the NGN is that of weather measuring sensors installed at the seashore, river, and local weather measuring points gathering meteorological data such as temperature changes, humidity changes, and precipitation. Figure I.1 shows the example. The sensor networks and necessary entities for USN applications and services such as directory servers can be installed by the 3rd party USN service providers or directly by national weather centre.

The sensor nodes, gateways, or separate data gathering entities send the gathered information to the servers of the service provider or the weather forecast centre which is connected to the NGN. The sensed data are periodically transferred and/or driven by event. The servers of the centre estimate, integrate, and process the information.

The following provides examples of USN applications and services:

1) A fisherman in a seashore area wants to get the on-demand and alarming information of the wave condition by his cell phone messages. He will subscribe a monthly paid USN service connected to his cell phone service.

2) A tourist who will hike a mountain for a week wants to get the periodic and alarming information of the nature condition on the mountain for the week. He will subscribe a temporary weather service for the region.

3) National disaster centre which does not own sensor networks on particular concerning area will subscribe a business on-demand USN service to a USN service provider, use the information to observe the natural phenomena of the area, and pre-detect emergency situation.

USN service providers may manipulate the collected sensed data to fit to the request from the USN end-users. The service provider uses functions on the NGN for support of USN applications and services which performs mining process and event process of the sensed data, USN directory service, etc.

The sensed data is provided to the users by the following example:

1) A user subscribes a USN weather information service to a service provider.

2) The sensed data is provided either by on-demand from the user or by an event-basis (alarm case).

3) When the user requests the sensed data, the request goes to the USN service provider. When the USN service provider owns functions for USN applications and services and the corresponding sensor networks, it will process service data and deliver it to the user. If the USN service provider is a third party service provider which does not own functions for USN applications and services and the corresponding sensor networks, it will request the necessary information to the other service provider who owns the necessary functions for USN applications and services as shown in Figure I.2. The data is delivered via Cellular Networks, Mobile WiMAX, or other access networks.

4) When the service provider detects emergency case, it will send an alarm to the USN end-users without request, as shown in Figure I.3.

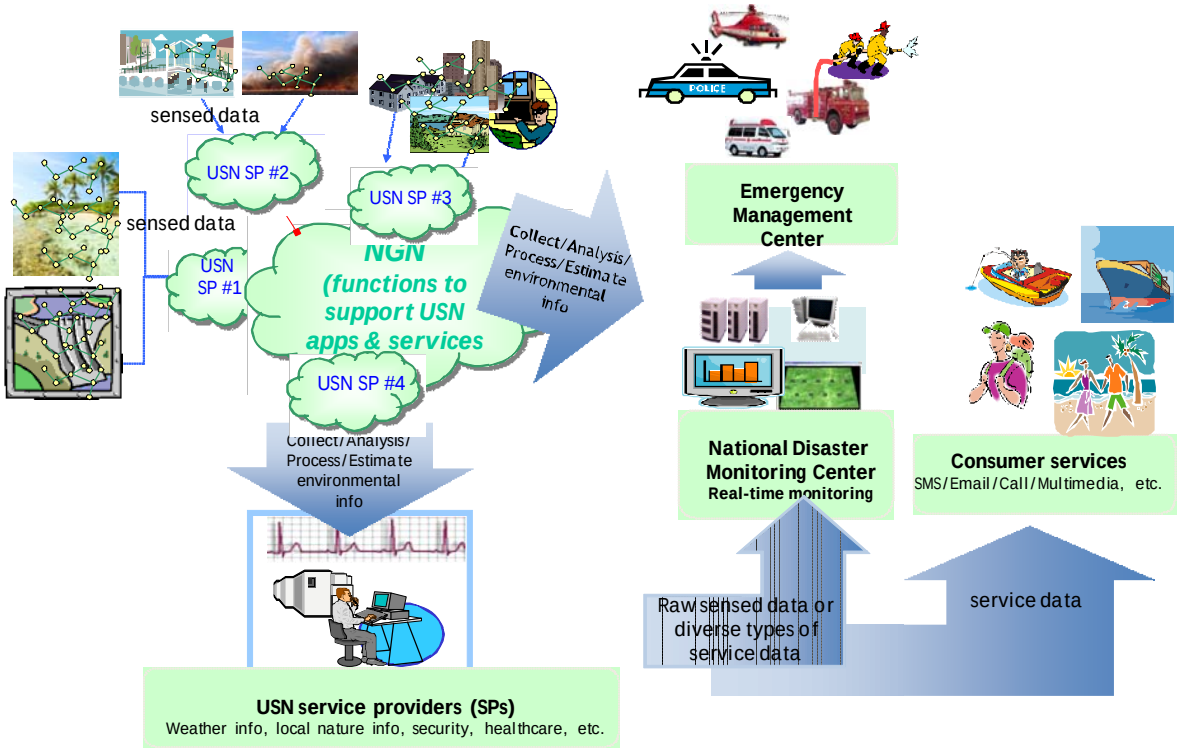

Figure I.1 - USN Weather information Service

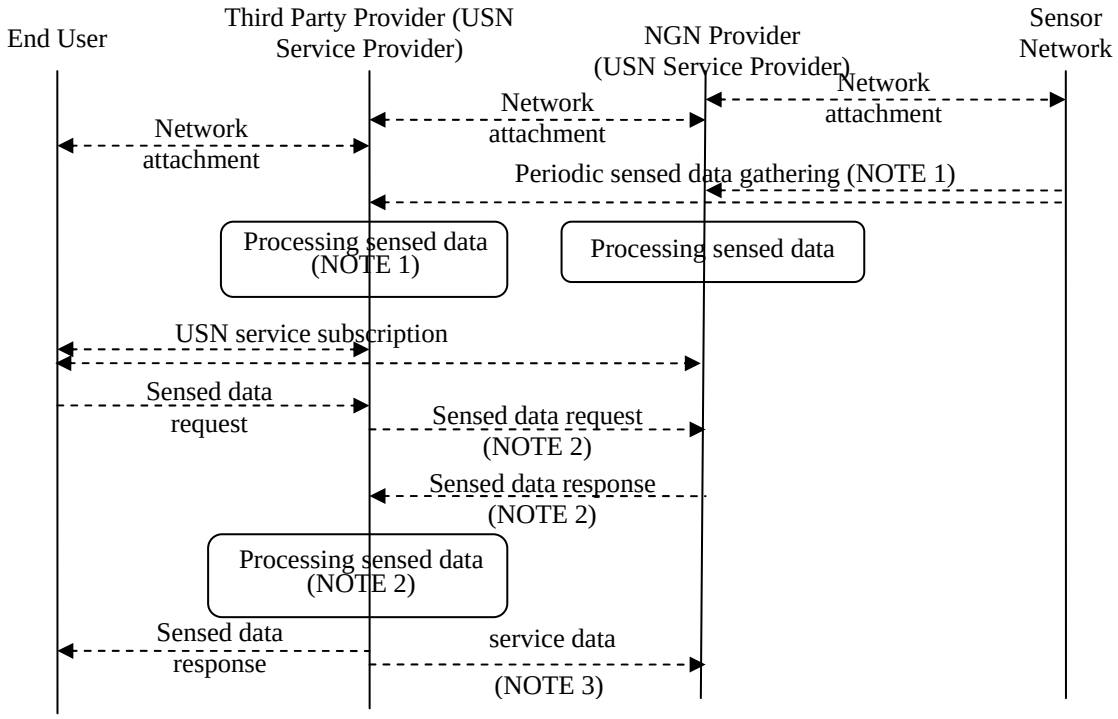

Figure I.1 - Information flow of on-demand USN service

NOTE 1 - If a third party provider does not own sensor networks, periodic sensed data gathering and processing sensed data on the flow are not necessary.

NOTE 2 - If necessary, data request for sensed data can be transmitted to the other USN service providers

NOTE 3 - If necessary, a USN service provider send service data resulting in processing raw sensed data to other USN service provider.

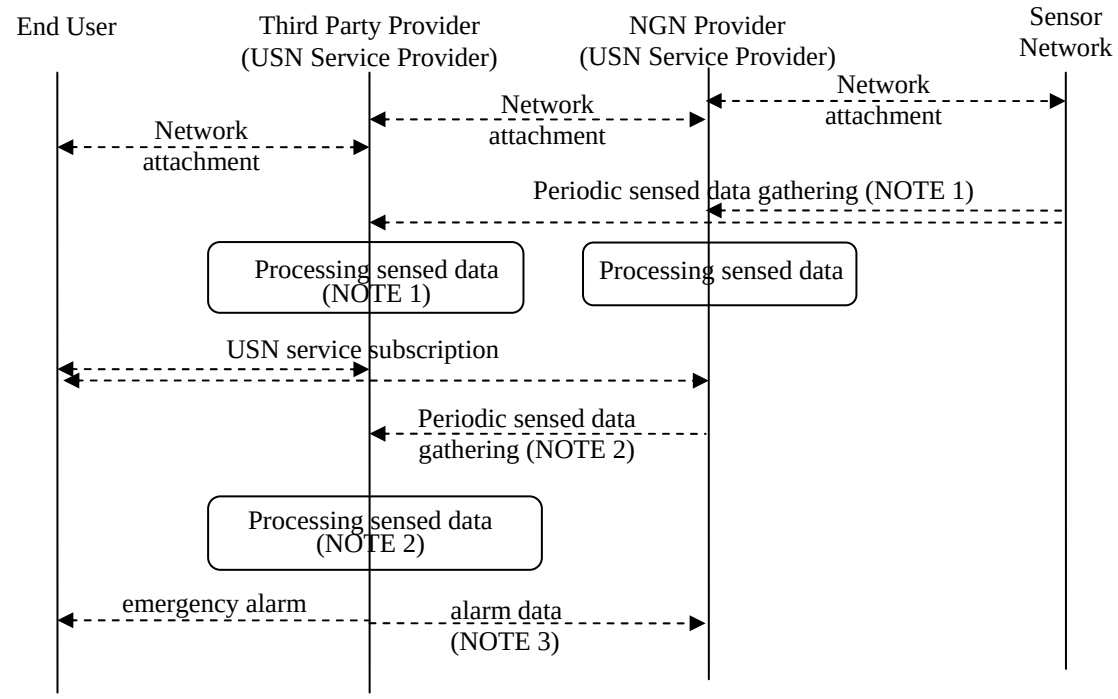

Figure I.2 - Information flow of USN alarming service

NOTE 1- If a third party provider does not own sensor networks, periodic sensed data gathering and processing sensed data on the flow are not necessary.

NOTE 2- If necessary, sensed data gathering can be existed whether periodically or on demand among USN service providers.

NOTE 3- If necessary, a USN service provider can send alarm data to other USN service provider.

B. Home healthcare service

Another application scenario is that a patient uses wearable medical equipments such as watches with an attached pulse measuring sensor or glasses with attached body temperature measuring sensors, etc. Home network providers can combine their modem with USN-service-enabled home gateway. The sensors periodically gather the medical check-up data and send them to the server of the service provider.

As Figure I.4 depicts, the sensed data are provided as following examples:

1) A hospital can make a business model together with the home USN service provider. The hospital system gets the sensed data via directly from the home-gateway or via the service provider.
2) The family of the patient can subscribe the service to get periodic status information of the patient. The service includes alarm notification in emergency cases.
3) The service will directly call the ambulance when it is necessary.

In an advanced scenario, the sensed data can be transferred even while the patient is moving. The data can be sent via access gateway in a network-enabled car, bus, train, or subway which is connected on WLAN, Mobile WiMAX, or Cellular Networks. The doctor obtains the information in the same way, using available communication networks.

Figure I.2 and I.3 cover the information flow of the USN home healthcare services. Sensed data goes to the service provider, and is delivered as diverse service data resulting in processing the raw sensed data.

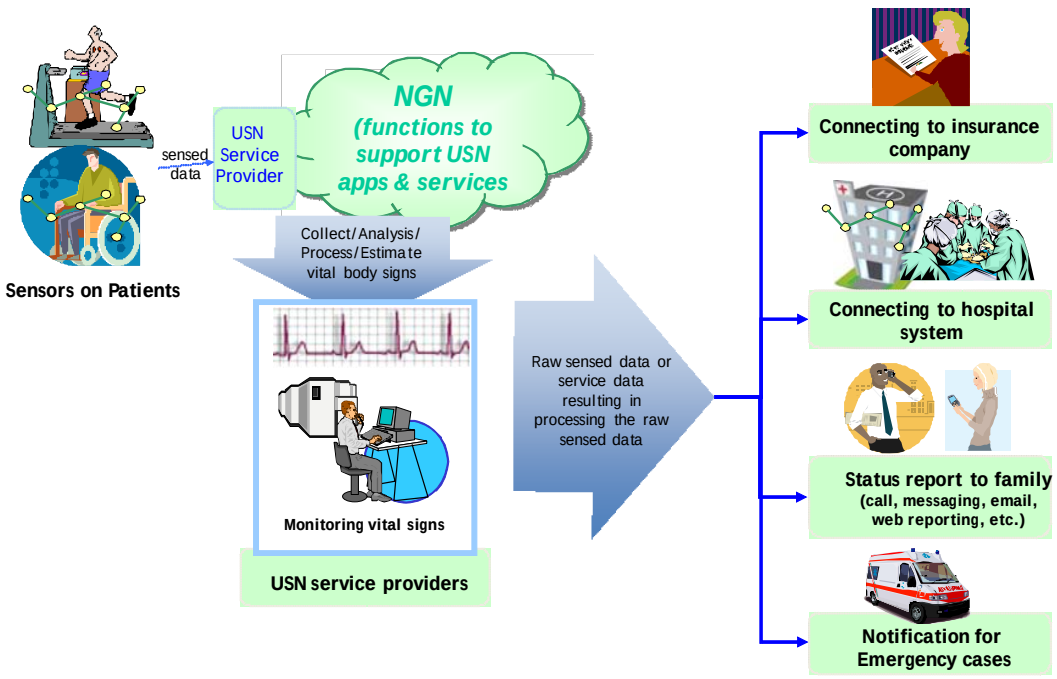

Figure I.3 - USN healthcare service

C. Environmental and situational information service using public transportation

Environmental and situational information is good resource for specific mission critical services and everyday value added services. Moreover, it can be more valuable information if it is provided regularly with quite wide interested area. Since it is not efficient to deploy static sensor networks for the city-wide target area, adoption of a mobile solution can be considered.

Environmental sensor nodes, video sensor nodes and location sensor nodes can be form sensor networks at public transportation vehicles like buses or caps. Environmental sensors include ones to measure temperature, humidity, yellow dust, ozone, illumination, ultraviolet, etc and video sensors include video cameras that collect video data on street or traffic situation. Those environmental and video data can be collected with location data using location sensor nodes which includes GPS. A gateway can be located at the vehicle where sensor nodes installed. The gateway is connected to the NGN through various wireless networks such as ones based on Mobile WiMAX, CDMA (WCDMA) based cellular networks, and MAN based wireless mesh networks. As the vehicle moves, environmental and situational information is gathered along the route of the vehicle. Depending on services, data collection rate can be various. Utilizing the information collected, a variety of services can be possible as below:

- Traffic surveillance services for operators of Intelligent Transportation System (ITS).
- Environmental monitoring service for administers of a city environment department.
- Traffic accident or crime investigation service.

Web based environmental and traffic information services can be provided for internet users using mobile handheld devices, IP TV terminal or PC. People who live or work near the route of the vehicle may be mostly interested in the services.

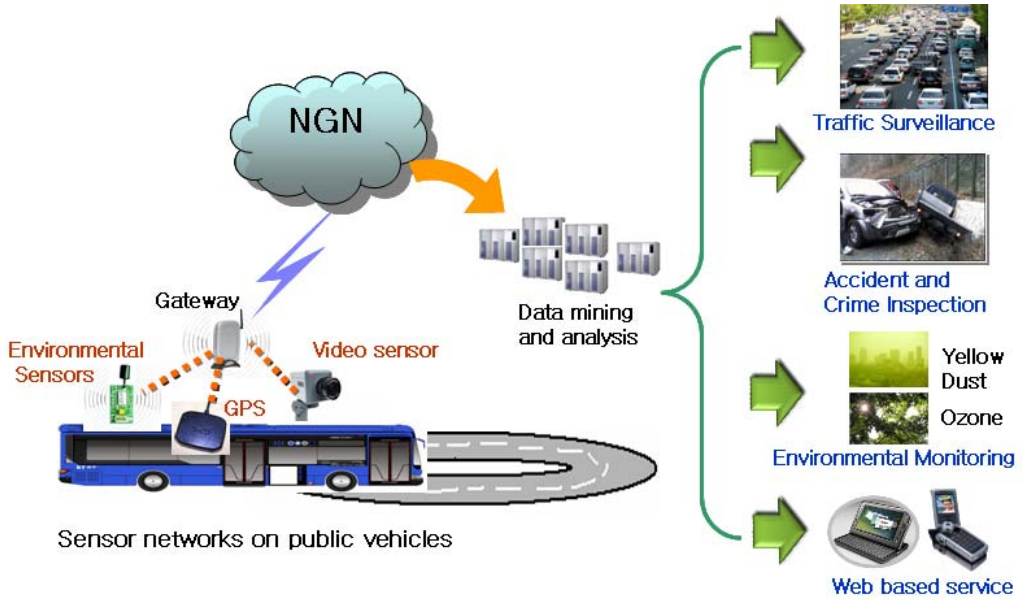

Figure I.5 – Mobile USN service to monitor environmental information

Above services might be provided in both passive and proactive methods. For proactive services, process of the sensed data and recognition of some critical events should be done by data mining and analysis systems that can notify to the relevant USN end-users when emergency situation

happens. Passive service is just used by USN end-users for monitoring of environment and situation. In this service, USN end-users detect critical events by themselves.

Technical challenges need to be tackled with are follows:

- Sensor nodes should sense environmental data when the vehicles networked by sensor nodes are moving fast. Thus, the accuracy of sensed data should be taken care of considering the speed of the vehicle. Technologies for sensed data diagnostic can be adopted.
- Strong video compression technologies are highly recommended because the video data volume can be huge due to continuous monitoring data.
- Networking between the sensor networks on the vehicle and the NGN should be reliable although the sensor networks move fast. Mobility support for the sensor networks must be provided.

Appendix II: Capability requirements for support of USN applications and services not directly affecting the NGN

(Appendix is not an integral part of this document)

Following requirements do not directly affect functional capabilities of the NGN but USN applications and services. The followings are on sensor network areas, not on access or core networks.

A. Power conservation (sensors node)

In sensor networks, some devices are mains-powered, but most are battery-operated and need to last several months to a few years with a single AA battery. In addition, sensor nodes have the characteristics of small devices, limited memory sizes, low processors, low bandwidth, high loss rates, etc. These characteristics lead to the following requirements:

1) It is required to provide small code size of network and transport layer protocols, application protocols and data.
2) Low protocol state is required to be supported; low memory usage, low protocol overhead, etc.
3) It is importantly recommended to provide robust and energy efficient protocols to handle dynamic loss from battery deficit or mainly sleeping nodes.

B. Network formation: auto-configuration and self-healing (sensor networks)

An important trait of sensor devices is their unreliability due to their limited system capabilities. It is predicted that user interaction and maintenance become impractical in such conditions, and auto-configuration and self-healing capabilities are useful to provide robustness of sensor networks. Thus, sensor networks have the following requirement:

1) Auto-configuration and self-healing are recommended to be supported for dynamically adaptive topologies.

C. Addressing mechanism

Some USN applications and services such as nature monitoring system, sensor networks will be comprised of significantly higher numbers of devices than counted in current networks. In addition, USN applications and services have Point to MultiPoint (P2MP) or MP to P traffic patterns, more than Point to Point (P2P) traffic. To support USN applications and services, the following addressing requirements are placed on sensor networks:

1) Address mechanisms is recommended to be enough scalability. IP addressing can be used as a global address mechanism for IP-based sensor networks, while local address mechanisms can be used within the stub networks in non-IP based sensor networks. When no global addresses are used in the sensor networks, it should be guaranteed that a local gateway can provide the connectivity to the sensor networks.
2) Efficient P2MP or MP2P communication is required to be supported. It can be provided either with a special address for multipoint or by efficient transport mechanisms.

D. ID design

As sensor networks are generally deployed as a stub network in many services, IDs for sensor nodes in the network may be allocated by a coordinator in the sensor network considering the applications

and service types. In other way, it could have global address like IP address, but have special naming mechanism for the services. USN applications and services have following ID design requirements:

1) In some applications and services, data-aware ID or naming mechanism is recommended. (e.g. temp_etri_x36y30, wind_etri_x36y30) Application functions should support to decode the ID with local or global addresses of the sensor nodes.

2) In some applications and services, geographical ID or naming mechanism is recommended. (e.g. temp_etri_x36y30, wind_etri_x36y30) Application functions should support to decode the ID with local or global addresses of the sensor nodes.

E. Sensor nodes mobility support

Sensor networks are likely to have certain degree of mobility. Due to the low performance characteristics of sensor nodes, the following requirement is placed on sensor networks:

1) Inter- and intra-mobility are required to be provided without extra protocol overhead in sensor nodes.

F. Secure control messages

Security threats within sensor networks may be different from existing threat models in other networks. E.g. bootstrapping and Neighbor discovery may be susceptible to threats. The following requirement is placed on sensor networks:

1) Control messages within sensor networks are required to be secure, in the way that security mechanism should not be overhead of low-powered sensor networks.

G. Lightweight Routing

As sensor networks have special requirements on energy saving and data-oriented communication, the following requirements are placed on sensor networks:

1) Energy efficient routing schemes are required to be supported.

2) It is required to support routing schemes for sensor nodes in sleeping mode at the most of the time.

3) It can optionally support data-aware routing schemes.

4) It is recommended to support efficient routing schemes for diverse data traffic patterns; MP2P, P2MP, and P2P.

Some USN applications and services are based on large scale sensor networks. To support high scalability, the following requirement is placed on sensor networks:

5) Scalable routing schemes (e.g. with reduced routing state) is recommended to be supported for large size of sensor networks.

H. Connectivity

Sensor networks, regardless of sensor network types are required to support connectivity to other networks (e.g. NGN or IP network). To support connectivity, the following requirements are placed on sensor networks:

1) IP based sensor networks can be connected to other IP based networks through IP routers. Protocol conversion or tunneling capability is required to be supported when the IP versions of the connected network and the sensor network are different.
2) Non-IP based sensor networks are required to be connected to other networks using gateways that support protocol conversion.
3) Scalability issues are recommended to be taken into account to support large scale sensor networks.

Bibliography

The following documents contain information that may be valuable to the reader of this Recommendation. They provide additional information about topics covered within this Recommendation, but are not essential for an understanding of this Recommendation.

ITU Recommendations

[b-ITU-T Y.2001] ITU-T Recommendation Y.2001 (2004), *General overview of NGN*

[b-ITU-T Y.2011] ITU-T Recommendation Y.2011 (2004), *General principles and general reference model for Next Generation Network*

[b-ITU-T Y.Sup7] ITU-T Supplement 7 for Y-series Recommendations (2008), *Supplement on NGN release 2 Scope*