International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2221

(01/2010)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Service aspects: Service capabilities and service architecture

Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment

Recommendation ITU-T Y.2221

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Future networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.2221

Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment

Summary

Recommendation ITU-T Y.2221 provides a description and general characteristics of ubiquitous sensor network (USN) and USN applications and services. It also analyses the service requirements of USN applications and services, and specifies the extended or new NGN capability requirements based on the service requirements.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2221	2010-01-13	13

Keywords

NGN, sensor networks, ubiquitous sensor network (USN), USN applications and services, wireless sensor networks (WSNs).

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T Y.2221

Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment

1 Scope

This Recommendation, based on [ITU-T Y.2201], covers extensions and additions to NGN capabilities in order to support ubiquitous sensor network (USN) applications and services [b-ITU-T Y.Sup.7] 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] Recommendation ITU-T Q.1703 (2004), *Service and network capabilities framework of network aspects for systems beyond IMT-2000*.

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

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.

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

[ITU-T Y.2233] Recommendation ITU-T Y.2233 (2008), *Requirements and framework allowing accounting and charging capabilities in NGN*.

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

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1*.

[ITU-T Z.100] Recommendation ITU-T Z.100 (1999), *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.2201]: 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.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 sensor: An 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 interconnected 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 service: A set of functions and facilities offered to a user by a provider.

3.2.5 service description language: A language for the specification of event-driven systems, in particular telecommunication systems, and an object-oriented formal language intended for the specification of complex, event-driven, real-time, and interactive applications involving many concurrent activities that communicate using discrete signals.

3.2.6 ubiquitous sensor network (USN): A conceptual network built over existing physical networks which makes use of sensed data and provides knowledge services to anyone, anywhere and at anytime, and where the information is generated by using context awareness.

3.2.7 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.

3.2.8 USN gateway: A node which interconnects sensor networks with other networks.

3.2.9 USN middleware: A set of logical functions to support USN applications and services.

NOTE 1 – The functionalities of USN middleware include sensor network management and connectivity, event processing, sensor data mining, etc.

NOTE 2 – 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 and acronyms

This Recommendation uses the following abbreviations and acronyms:

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 Network
WCDMA	Wideband CDMA
WiMAX	Worldwide Interoperability for Microwave Access
WMN	Wireless Mesh Network
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor 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 Recommendation 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 3.2.6, is a conceptual network built over existing physical networks which makes use of sensed data and provides knowledge services to anyone, anywhere and at anytime, and where the information is generated by using context awareness.

USN utilizes wireline sensor networks and/or wireless sensor networks (WSNs). WSNs are 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. Up to now, WSNs were generally implemented as isolated networks. Simple design of applications and services based on isolated sensor networks is made by the capture and transmission of collected sensed data to designated application systems.

Such isolated, simple applications and services have been evolving over the years through deployment of networks, based upon advanced hardware and software technologies that provide network and service integration, data processing schemes enhanced by business logic and by data mining rules, context-awareness schemes, 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 and government.

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 or military field.

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 and directory services.

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

NOTE 1 – The details of physical sensor networks and USN middleware are out of scope of this Recommendation.

NOTE 2 – Figure 1 does not represent a functional architecture. The positioning of USN applications and services, USN middleware, NGN and sensor networks in this figure does not correspond to functional layering.

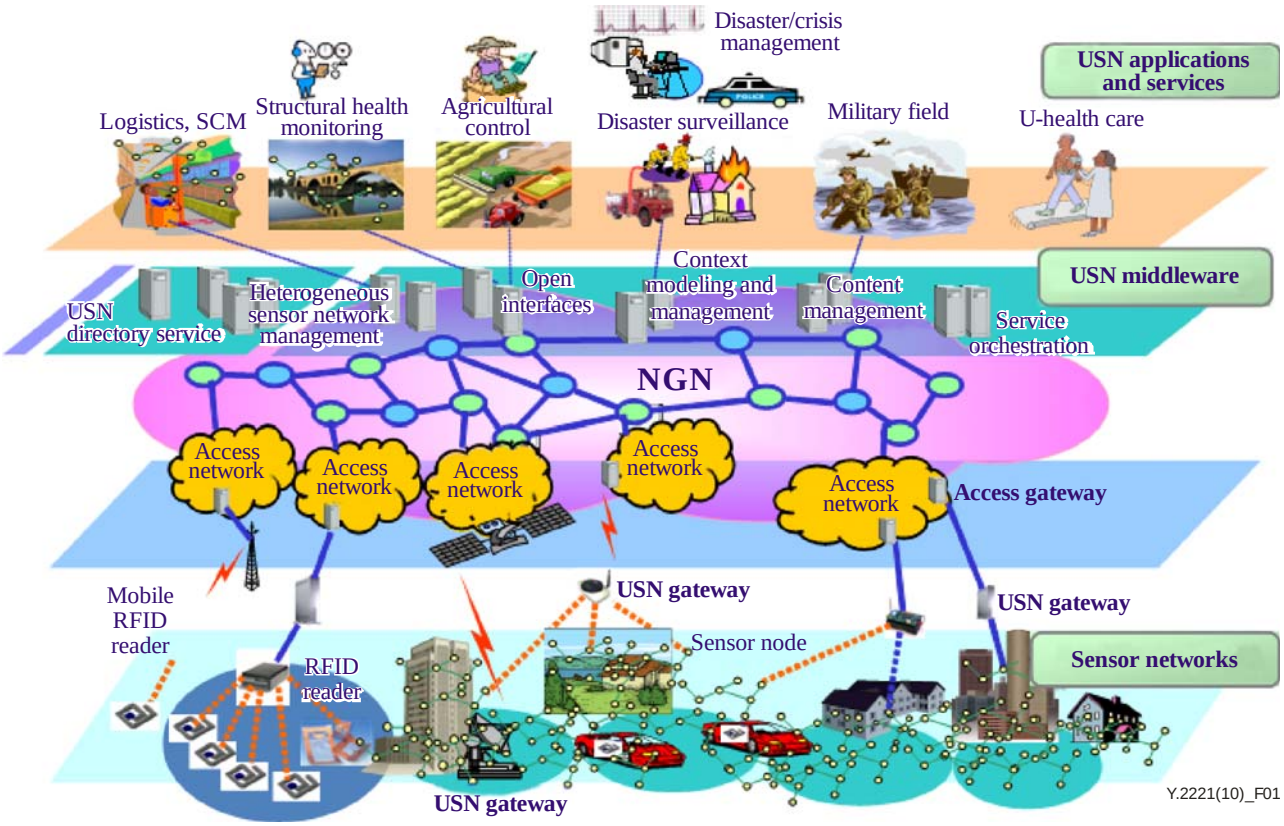


Figure 1 – An overview of USN with related technical areas

For the 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 3 – Sensor nodes generally have limited bandwidth, low processing power, and small memory size such as 32K.

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

– Dynamic network topology;

  NOTE 5 – Sensor networks often dynamically change the topologies due to the association and de-association of sensor nodes.

– High possibility of communication failures (e.g., due to low bandwidth or link failure);

– Heterogeneity of nodes;

  NOTE 6 – A USN application or service may be built using more than one sensor network, where sensor nodes use different PHY/MAC (e.g., [b-IEEE 802.15.4], [b-IEEE 802.15.3]) layers or operate differently in IP-based or non-IP based networks.

– Large scale of deployment;

  NOTE 7 – A USN application or service can be deployed on a wide geographical scale to monitor environmental conditions, for example of a river or a seashore.

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 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 coexist 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 networks include the case of a single sensor node directly connected to 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 lose its connectivity or its functionality despite the loss of a connection to a single node in the network due to link or hardware failure, which has a high probability of occurrence 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 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 the 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, and location information. 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. Unlike 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 and location. 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 as described in 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, 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 the service discovery for USN applications and services.

7.3.2 Service composition and coordination

It is useful to enable easy service creation by the 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 the creation of USN applications and services.

7.3.3 Interworking 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, interworking with service creation environments is recommended to be supported. Thus, USN applications and services have the following requirement on interworking with service creation environments:

1) It is recommended to support interworking with other service creation environments for the creation of USN applications and services.

7.4 Quality of service (QoS) support

7.4.1 Differentiated QoS 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 incident must be delivered in a timely and reliable way to the appropriate national disaster monitoring systems. As USN applications and services are supported over the 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 QoS 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 the IP. Although the underlying wired and/or wireless media access control manages the connectivity, connections between USN end-users and sensor networks are through the 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 the 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 the 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.
3) Location information is recommended to be trustworthy and so location discovery and management is recommended to be secure.

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 patient's doctor via a home-gateway when the patient 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 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 an 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 the creation of new services.

4) The security approaches for the support of USN applications and services are recommended to be consistent with the general approach for the security in NGN.

5) In addition to data security, the USN communication infrastructure is recommended to provide information transport security for protection against well-known passive and active attacks. Protocols for information transport are required to be resilient to attacks.

6) Depending on the specific USN application security requirements, means for intrusion detection are required.

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 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 Privacy

USNs allow for the remote collection of a huge volume of sensed data which in many cases are time-stamped and geo-located. The high volume from one hand and the possibility for remote collection from the other increase the potential damage that can be caused by unauthorized parties. Furthermore, the use of multi-hop based infrastructure may require the use of source, location and time for routing purposes, making thus this sensitive information available to intermediate relaying nodes.

In addition, knowing when and where events within a USN occur may compromise the security of the USN itself as well as the security of USN end-users (e.g., in building/home automation USN applications). For this reason, such information needs to be kept "private", i.e., can only be shared between trusted parties. Furthermore, in cases where the USN infrastructure is shared by different USN applications, there is the need for clearly keeping data "private" to each application (especially in operated USNs where a telecom operator may offer commercial services to business clients with conflicting interests).

Thus, USN applications and services have the following requirements:

1) There should be an option for privacy enhanced multi-hop routing mechanisms (information on originating node id, time and location should not be revealed – at least totally – to intermediate nodes).
2) There should be an operating option to de-correlate sensor activity patterns (revealing sensitive context information) from the ensuing communication traffic patterns.

7.11 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 sufficient if they are transmitted, at least once, within a certain period of time. 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 to 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 capabilities [ITU-T Y.2201] but require some extended and/or new capabilities. The capability requirements in this clause 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 capabilities

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

8.1.1 Network management

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

1) NGN is required to manage IP-based sensor networks including the case of a single node directly connected to the NGN.

2) NGN is required to manage non-IP based sensor networks.

3) 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 NGN. The following are additional requirements for the support of USN applications and services.

8.1.2.1 Service profile

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

1) 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, the following requirement is placed on NGN:

1) 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 NGN. The following are additional requirements for the support of USN applications and services.

8.1.3.1 Service registration and discovery

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

1) NGN open service environment (OSE) is required to support at least one standard USN service description language and its associated execution framework.

2) NGN is recommended to register and discover USN applications and services based on a standard set of USN service profiles.

3) NGN may support registration and discovery of sensor network devices (e.g., actuator, gateway) for USN applications and services.

8.1.3.2 Interworking with service creation environments

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

1) NGN OSE is required to support interworking 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

In addition to NGN QoS capabilities, the following requirements list those needed for the 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, the following additional requirements are placed on NGN:

1) NGN is required to support QoS capabilities to sustain the transaction volume caused by USN applications and services.

2) NGN is recommended to support QoS capabilities preventing from access concentration to a single resource (e.g., USN data repositories).

8.1.5 Privacy

Based on the privacy requirements in clause 7.10, the following additional requirements are placed on NGN:

1) NGN is required to provide protection of privacy-related information on relaying control and data packets of USN applications and services.

2) NGN is required to provide an optional operation to de-correlate activity patterns of sensor node and networks from the ensuing USN communication traffic patterns.

8.2 Requirements supported by existing NGN capabilities

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

8.2.1 Open service environment

8.2.1.1 Service composition and coordination

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

8.2.2 Quality of service

8.2.2.1 Differentiated quality of service and data prioritization

NGN 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 is supported by the existing capabilities of NGN [ITU-T Y.2201].

8.2.3 Connectivity

NGN provides connectivity capability. The connectivity requirement specified in clause 7.5 is supported by the existing connectivity capabilities of NGN [ITU-T Y.2201].

8.2.4 Location management

NGN 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 are supported by the existing location management capabilities of NGN [ITU-T Y.2201].

8.2.5 Mobility

NGN provides mobility support for the NGN. The mobility requirements specified in clause 7.7 are supported by the existing capabilities of the NGN Release 1 [ITU-T Q.1706].

8.2.6 Security

NGN provides security capabilities. The service requirements specified in clause 7.8 are supported by the existing security capabilities of NGN [ITU-T Y.2201] and [ITU-T Y.2701].

8.2.7 Identification, authentication and authorization

NGN provides identification, authentication and authorization capabilities. The service requirements specified in clause 7.9 are supported by the existing capabilities of NGN [ITU-T Y.2201] and [ITU-T Y.2702].

8.2.8 Accounting and charging

NGN provides accounting and charging capabilities. The service requirement specified in clause 7.11 is supported by the existing capabilities of NGN [ITU-T Y.2233].

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

The reference diagram of NGN capabilities for the 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 the 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.

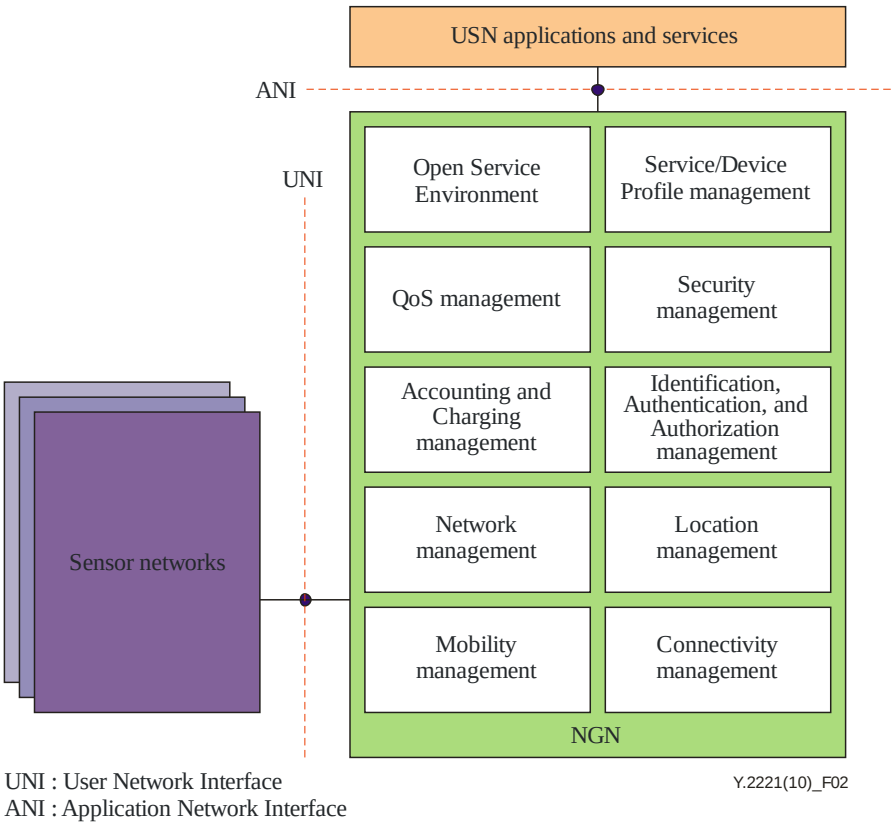


Figure 2 – Reference diagram of NGN capabilities for support of USN applications and services

10 Security considerations

Security is an important issue for USN applications and services. Different USN applications and services have different security requirements. USN applications and services require stringent security for the protection of sensed data. Service requirements on security and identification, authentication, and authority are described in clauses 7.8 and 7.9. NGN capability requirements on security are covered in [ITU-T Y.2201], [ITU-T Y.2701] and [ITU-T Y.2702], as stated in clauses 8.2.6 and 8.2.7.

Appendix I

Use-cases of USN applications and services

(This appendix does not form an integral part of this Recommendation)

Detailed analysis of USN applications and services is out of scope of this Recommendation, but some use-cases are listed in this appendix because they imply market needs and technical issues.

The USN applications and services can be grouped from the perspective of the market they serve, as follows:

– Automation, monitoring and control of manufacturing and industrial applications;
– Home automation;
– Agricultural monitoring;
– Monitoring and management of building and utility;
– Health care and medical research;
– Environment, pollution and disaster surveillance;
– Chemical, biological, radiological and nuclear (CBRN) sensor-based applications;
– Security;
– Military;
– Intelligent transportation management;
– Vehicle communication;
– Smart utility networks (e.g., smart metering for water, electricity, or gas); and
– Urban resource management (e.g., lightning, watering, or parking).

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

USN applications and services are numerous, and it is necessary to classify them according to varying business and technical factors. The following three examples show some use-cases of USN applications and services over the NGN.

I.1 Weather information service

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

The sensor nodes, gateways, or separate data gathering entities send the collected information to the servers of the service provider or the weather forecast centre that are connected to the NGN. The sensed data are periodically transferred and/or triggered by meteorological events. The servers of the centre estimate, integrate, and process the information.

The following provide examples of USN applications and services:

1) A fisherman in a seashore area wants to get the on-demand and alarm information of the wave conditions through his cell phone. He will subscribe to a USN service accessible through his cell phone.

2) A tourist who will go mountain hiking for a week wants to get the periodic and alarm information of the weather conditions of the mountain for the week. He or she will subscribe to a temporary weather service in the region.

3) A national disaster centre, which does not own sensor networks in a particular area, will subscribe to an on-demand USN service of a USN service provider, use the information to observe the natural phenomena of the area, and foresee an emergency situation.

USN service providers may manipulate the collected sensed data to suit the request of the USN end-users. The service provider uses NGN functions for support of USN applications and services that perform the data mining and event processing of the sensed data, the USN directory service, etc.

The sensed data are provided to the users in the following manner:

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

2) The sensed data are provided either on demand from the user, or on an event-by-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 the functions for USN applications and services and the corresponding sensor networks, it will process the service data and deliver them 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 service provider who owns the necessary functions, as shown in Figure I.2. The data are delivered via cellular networks, Mobile WiMAX networks, or other access networks.

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

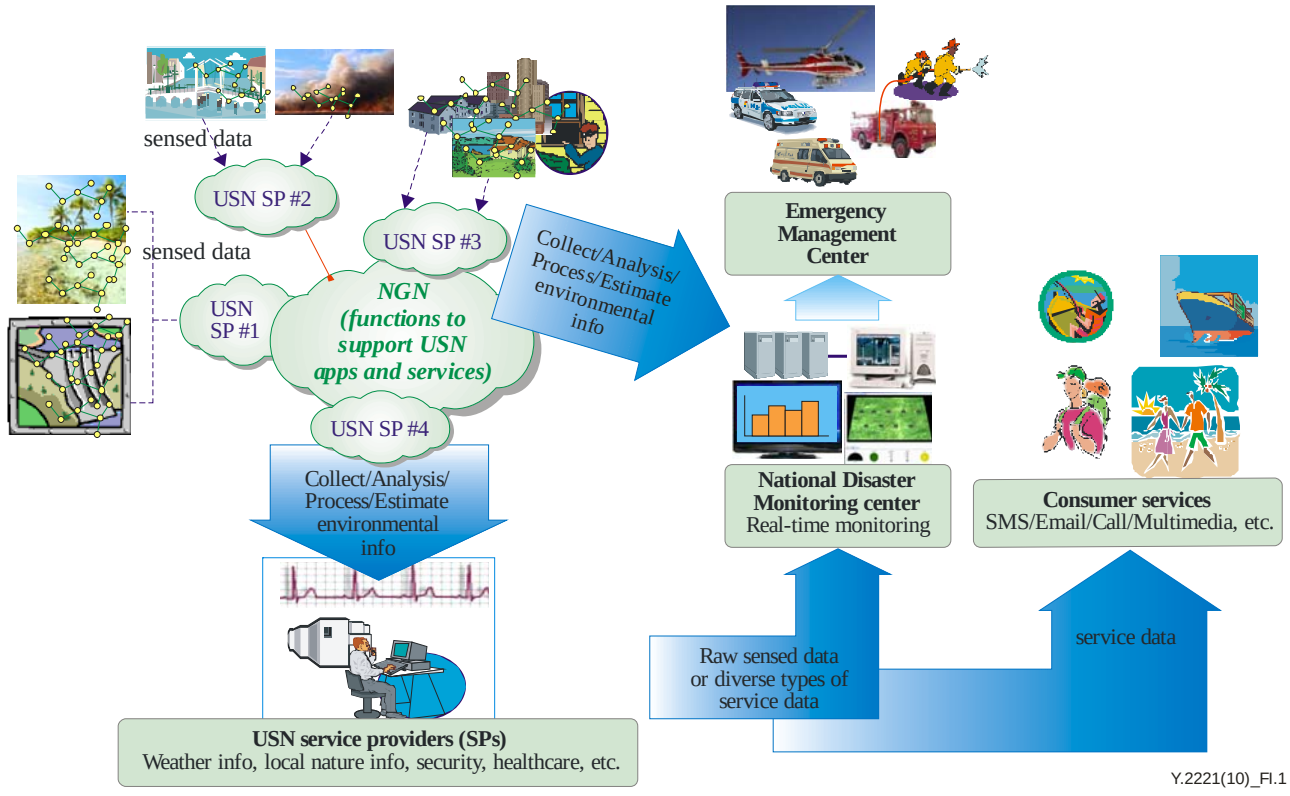
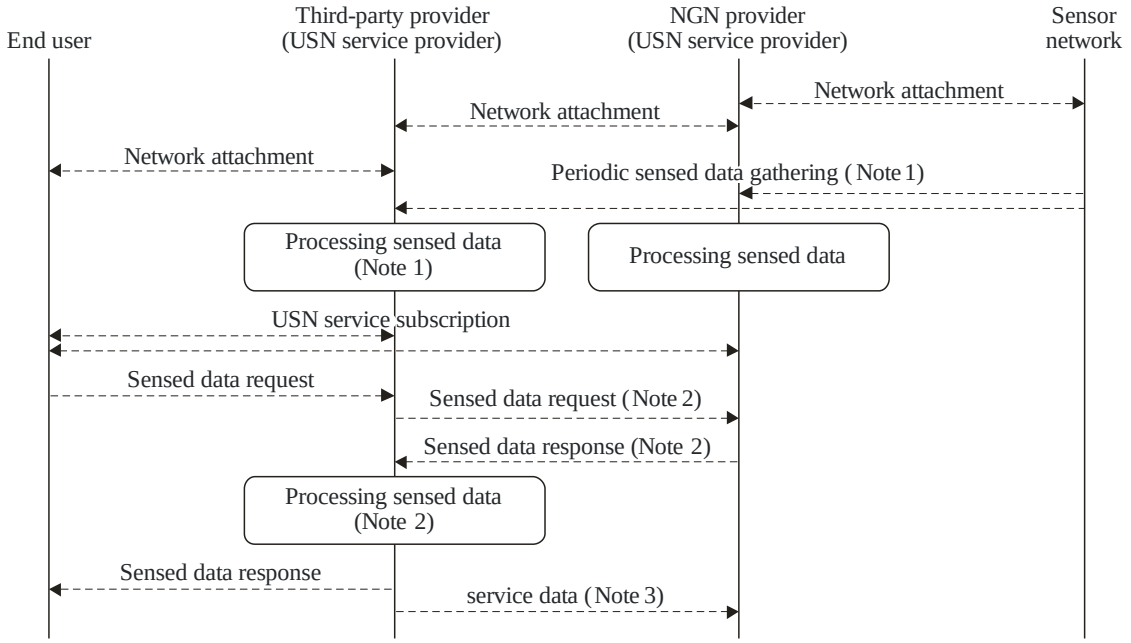


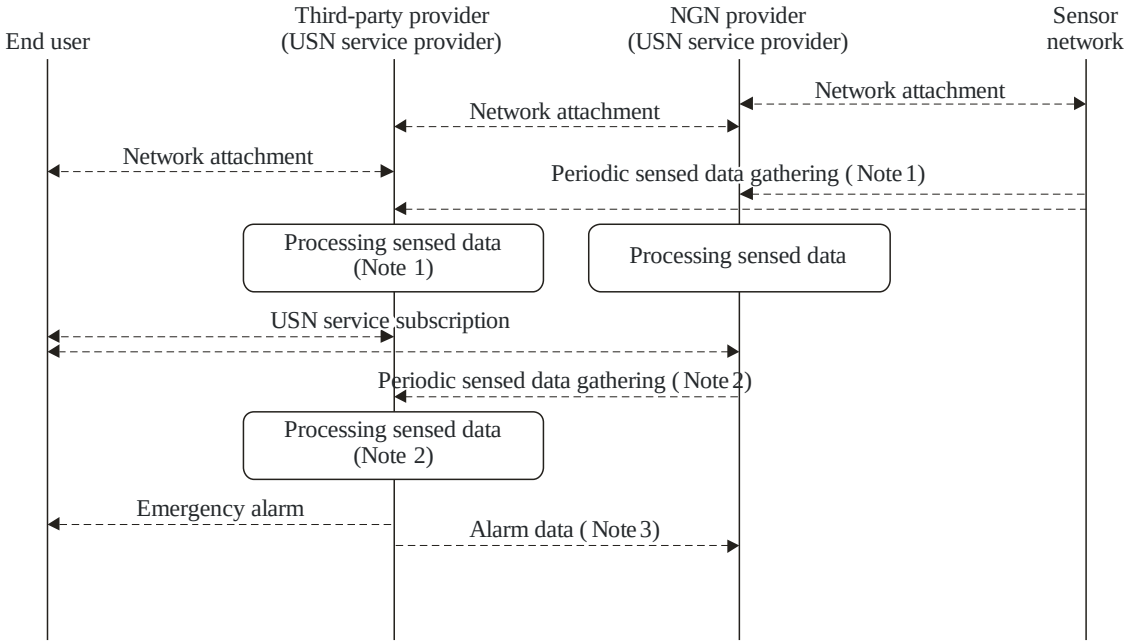
Figure I.1 – USN weather information service



NOTE 1 – If a third-party provider does not own sensor networks, periodic gathering and processing of sensed data on the flow are not necessary.
NOTE 2 – If necessary, the data request for sensed data can be transmitted to other USN service providers.
NOTE 3 – If necessary, a USN service provider sends service data, resulting in processing raw sensed data to other USN service providers.

Y.2221(10)_FI.2

Figure I.2 – Information flow of on-demand USN service



NOTE 1 – If a third-party provider does not own sensor networks, periodic gathering and processing of sensed data on the flow are not necessary.
NOTE 2 – If necessary, sensed data gathering can exist 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 providers.

Y.2221(10)_FI.3

Figure I.3 – Information flow of USN alarm service

I.2 Healthcare service

Another application scenario is that of a patient wearing medical equipment such as watches with attached pulse-measuring sensors, or glasses with attached temperature-measuring sensors, etc. Home network providers may provide a USN-service-enabled home gateway and be USN service providers. The sensors periodically gather medical data and send them to the USN service provider(s).

As Figure I.4 depicts, sensed data may be provided in the following examples:

1) A hospital can establish a business relationship with the USN service provider. The hospital system gets the sensed data either directly from the home gateway or through the service provider.
2) The family of the patient can subscribe to 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 an access gateway in a network-enabled car, bus, train, or subway, which may be connected via different types of access networks, e.g., WLAN, Mobile WiMAX, or cellular networks. The doctor obtains the information in the same way, using available communication networks.

Figures I.2 and I.3 cover the information flow of the USN healthcare services. Sensed data are sent to the service provider, and delivered to different USN end-users as diverse service data resulting from processing the raw sensed data.

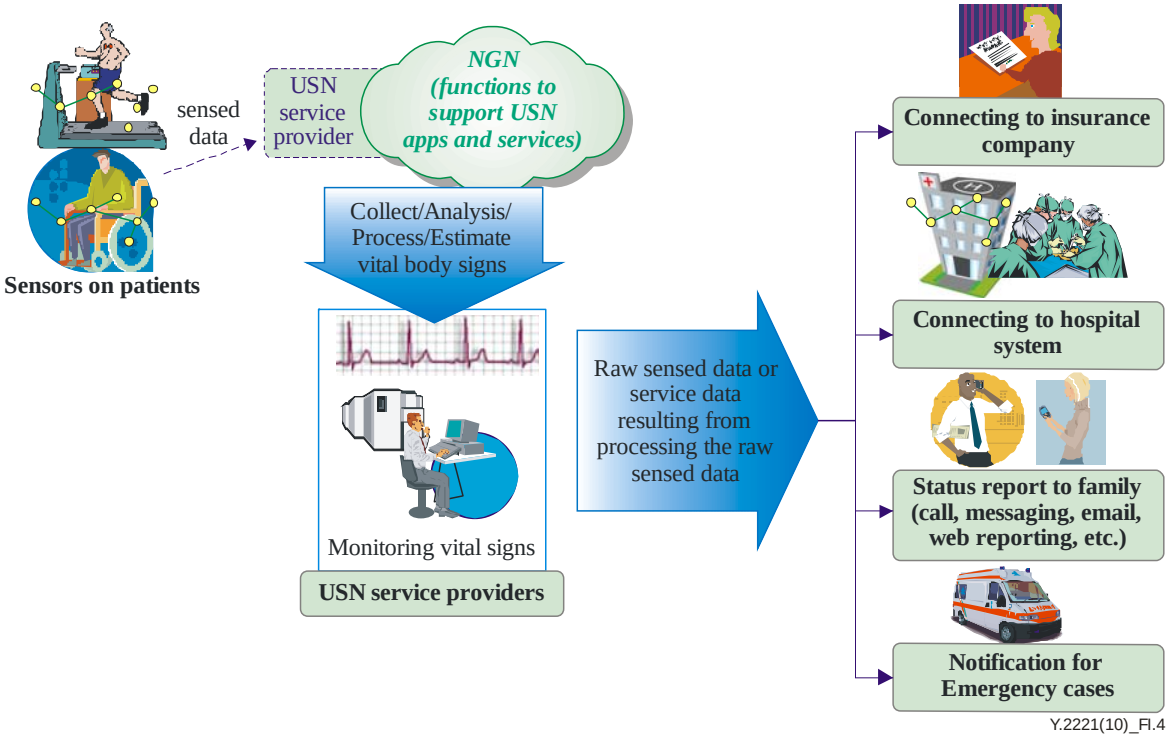


Figure I.4 – USN healthcare service

I.3 Environmental and situational information service using public transportation

Environmental and situational information is a useful source for specific mission-critical services and everyday value-added services. Moreover, information can be more valuable if it is provided regularly to a wide coverage area. Since it is not efficient to deploy static sensor networks for the city-wide target area, it is worthwhile to consider the adoption of a mobile solution (mobile sensor networks).

Environmental sensor nodes, video sensor nodes and location sensor nodes can form sensor networks on public transportation vehicles like buses or cabs. Environmental sensors include those which measure temperature, humidity, particulate air pollution, ozone, illumination, ultraviolet, etc., and video sensors include video cameras that collect video data on street or traffic situation. Environmental and video data can be collected together with location data using location sensor nodes that include GPS information. A gateway can be located in the vehicle where sensor nodes are installed and be connected to the NGN through various types of wireless access networks. As the vehicle moves, environmental and situational information is gathered along the route of the vehicle. Depending on the services, data collection rates can vary. Utilizing the information collected, a variety of services can be provided, as shown below:

– Traffic surveillance services for the operators of the intelligent transportation system (ITS).

– Environmental monitoring service for the administrators of the city environment.

– Traffic accident or crime inspection service.

Web-based environmental and situational information services can be provided for Internet users using mobile handheld devices, IPTV terminals or PCs. People who live or work near the route of the vehicle may be mostly interested in those services.

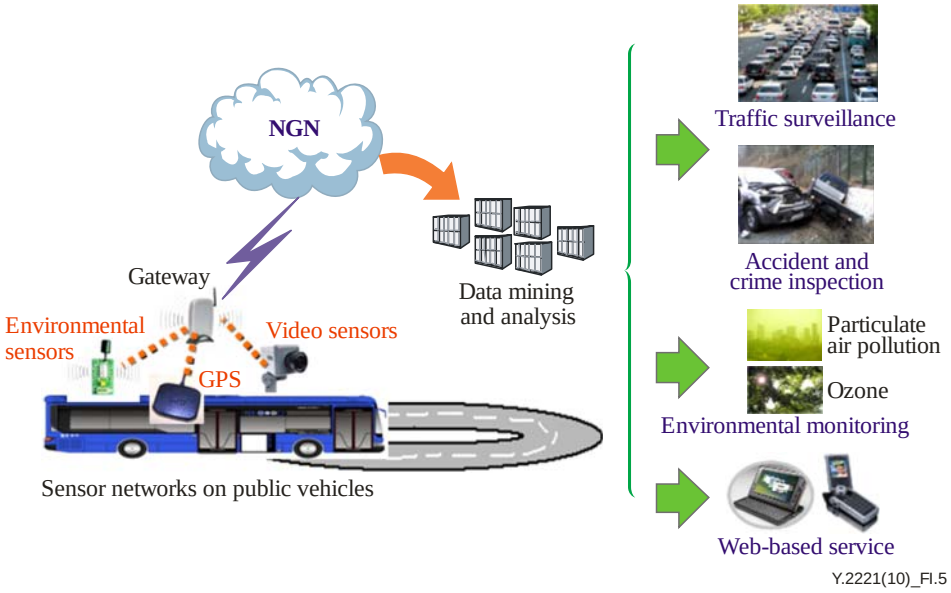


Figure I.5 – Mobile USN service of environmental and situational information monitoring

The above services can be provided in both passive and proactive ways. In a proactive service, the processing of the sensed data and recognition of some critical events is done by data mining and analysis systems that can notify the relevant USN end-users when an emergency situation happens. A passive service is just used by USN end-users for the monitoring of environmental and situational information: in this service, USN end-users detect critical events by themselves.

The following technical challenges need to be tackled:

– Sensor nodes should sense environmental data when the vehicles networked by sensor nodes are moving fast. Thus, the accuracy of the sensed data should consider the speed of the vehicle. Technologies for sensed data diagnostics 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

(This appendix does not form an integral part of this Recommendation)

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

II.1 Power conservation (sensors node)

In sensor networks, some devices are powered by mains power lines, but most are battery-operated (e.g., AA battery or IEC designated LR6 (alkaline), R6 (carbon-zinc), KR157/51 (nickel-cadmium), HR6 (nickel-metal-hydride), or FR6 (lithium-iron-disulfide)). 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 highly recommended to provide robust and energy efficient protocols to handle dynamic loss from battery deficit or mainly sleeping nodes.

II.2 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.

II.3 Addressing mechanisms

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 are recommended to support high 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.

II.4 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 words, they could have a global address such as an IP address, but have a special naming mechanism for the services. USN applications and services have the following ID design requirements:

1) In some applications and services, a 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, a geographical ID or a 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.

II.5 Sensor nodes mobility support

Sensor networks are likely to have a 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.

II.6 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 requirements are 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.

2) Design for power conservation should not compromise security, especially in USN applications with strong security requirements.

II.7 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.

   NOTE – Energy efficiency should not be considered in absolute terms (e.g., support of multi-path routing in case of USN application specific security and resilience requirements).

2) It is required to support routing schemes for sensor nodes in sleeping mode 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) are recommended to be supported for a large size of sensor networks.

II.8 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 tunnelling 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

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

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

[b-ITU-T Y.Sup.7] ITU-T Y-series Recommendations – Supplement 7 (2008), ITU-T Y.2000-series – *Supplement on NGN release 2 scope*.

[b-IEEE 802.15.3] IEEE 802.15.3 (2003), *Wireless medium access control (MAC) and physical layer (PHY) specifications for high rate wireless personal area networks (WPANs).*

[b-IEEE 802.15.4] IEEE 802.15.4 (2006), *Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs).*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2010