International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

F.744

(12/2009)

SERIES F: NON-TELEPHONE TELECOMMUNICATION SERVICES

Audiovisual services

Service description and requirements for ubiquitous sensor network middleware

Recommendation ITU-T F.744

ITU-T F-SERIES RECOMMENDATIONS

NON-TELEPHONE TELECOMMUNICATION SERVICES

TELEGRAPH SERVICE	
Operating methods for the international public telegram service	F.1–F.19
The gentex network	F.20–F.29
Message switching	F.30–F.39
The international telemessage service	F.40–F.58
The international telex service	F.59–F.89
Statistics and publications on international telegraph services	F.90–F.99
Scheduled and leased communication services	F.100–F.104
Phototelegraph service	F.105–F.109
MOBILE SERVICE	
Mobile services and multidestination satellite services	F.110–F.159
TELEMATIC SERVICES	
Public facsimile service	F.160–F.199
Teletex service	F.200–F.299
Videotex service	F.300–F.349
General provisions for telematic services	F.350–F.399
MESSAGE HANDLING SERVICES	F.400–F.499
DIRECTORY SERVICES	F.500–F.549
DOCUMENT COMMUNICATION	
Document communication	F.550–F.579
Programming communication interfaces	F.580–F.599
DATA TRANSMISSION SERVICES	F.600–F.699
AUDIOVISUAL SERVICES	**F.700–F.799**
ISDN SERVICES	F.800–F.849
UNIVERSAL PERSONAL TELECOMMUNICATION	F.850–F.899
HUMAN FACTORS	F.900–F.999

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

Recommendation ITU-T F.744

Service description and requirements for ubiquitous sensor network middleware

Summary

The purpose of Recommendation ITU-T F.744 is to describe ubiquitous sensor network (USN) services and requirements for USN middleware. To provide various USN services easily and effectively, it is desirable to define an intermediate entity such as USN middleware for providing functions commonly required by various USN services. This Recommendation covers USN service description, USN middleware description, use cases of USN services using USN middleware, the functional model for USN middleware and requirements for USN middleware.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T F.744	2009-12-14	16

Keywords

Functional model, requirement, sensor network, USN middleware, USN services.

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 F.744

Service description and requirements for ubiquitous sensor network middleware

1 Scope

This Recommendation describes USN services and requirements for ubiquitous sensor network (USN) middleware. This Recommendation covers:

– description of the USN services;

– description of the USN middleware;

– use cases of USN services that use USN middleware;

– functional model of USN middleware;

– requirements for USN middleware to support functions commonly required by USN services.

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

[ITU-T Y.2221] Recommendation ITU-T Y.2221 (2010), *Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 context awareness [ITU-T Y.2201]: Context awareness is 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.

NOTE – This Recommendation also uses context-aware with same meaning of context awareness.

3.1.2 sensor [ITU-T Y.2221]: An electronic device that senses a physical condition or chemical compound and delivers an electronic signal proportional to the observed characteristic.

3.1.3 sensor network [ITU-T Y.2221]: A network comprised of inter-connected sensor nodes exchanging sensed data by wired or wireless communication.

3.1.4 sensor node [ITU-T Y.2221]: A device consisting of sensor(s) and optional actuator(s) with capabilities of sensed data processing and networking.

3.1.5 ubiquitous sensor network (USN) [ITU-T Y.2221]: 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.

3.1.6 USN middleware [ITU-T Y.2221]: A set of logical functions to support USN applications and services.

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

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 open application interface: An interface used by USN applications to access USN middleware.

3.2.2 processed data: Data that are processed from raw sensed data by sensor network or USN middleware.

3.2.3 sensed data: Data sensed by a sensor that is attached to a specific sensor node.

3.2.4 sensor network common interface: An interface used between USN middleware and a sensor network/radio frequency identification (RFID) reader.

3.2.5 sensor network metadata: Information about a sensor network, such as description of the sensor network, sensor node identifier, supported sensor type, the number of attached sensors for each sensor node, and the number of sensor nodes connected to the specific sensor network, etc.

3.2.6 sensor network metadata directory service: A directory service that provides sensor network metadata.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ECG Electrocardiogram

RFID Radio Frequency Identification

USN Ubiquitous Sensor Network

WSN Wireless Sensor Network

5 Conventions

None.

6 Description of USN services, USN middleware and use cases

6.1 Description of USN services

USN is a conceptual network built over existing physical networks that 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 wireline sensor networks and/or wireless sensor networks (WSNs). See [ITU-T Y.2221].

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; in homeland security, military field, etc., see [ITU-T Y.2221].

A USN service is a type of service that uses various sensors and/or actuators. In the USN services framework, communications take place between USN applications and sensor networks directly or via some intermediate entity.

Some USN applications and services use basic data processing to obtain the necessary data and others may use advanced data processing such as data mining, context-aware processing, and event processing. In addition, authentication of sensor network and confidentiality of sensed data are very important to protect the USN services from fraudulent data.

The functions of various USN applications and services can be summarized as follows:

– finding appropriate sensor networks to obtain sensed data;
– requesting raw sensed data and/or processed data;
– processing received sensed data;
– activating actuators;
– monitoring sensor network status;
– controlling sensor networks;
– authenticating sensor networks;
– providing appropriate services to users.

These functions are commonly required by many types of USN applications and services. Concerning complexity, scalability and cost-effectiveness, it would be beneficial to support functions by a separate entity rather than by each USN application and service.

6.2 Description of USN middleware

USN middleware is an intermediate entity that provides functions commonly required by different types of USN applications and services. USN middleware receives requests from USN applications and delivers those requests to appropriate sensor networks. Similarly, USN middleware receives sensed data or processed data from sensor networks and delivers them to appropriate USN applications. USN middleware can provide information processing functions such as query processing, context-aware processing, event processing, sensor network monitoring and so on.

6.3 Use cases of USN services

USN services use only sensor nodes or both sensor nodes and RFID readers. In some cases, USN services can activate actuators after processing the sensed data. Some other USN services monitor and/or control sensor networks.

USN services can be categorized into three groups, based on the above observations:

– using only sensed data including RFID tag data (e.g., healthcare applications);
– activating one or more actuators, based on the sensed data, including RFID tag data (e.g., cold chain management applications);
– monitoring and/or controlling sensor networks, including RFID readers (e.g., sensor network monitoring applications).

Use cases in this Recommendation show how USN services and USN middleware work together.

6.3.1 Healthcare applications

A healthcare application continuously monitors the location and the health status of the persons within the range of a sensor network in buildings, in order to handle possible emergencies. See Figure 1. Every resident wears a sensor node on his/her wrist, which looks like a wristwatch. The sensor node senses body temperature, pulse, momentum, and electrocardiogram (ECG) of the resident and then periodically transmits the sensed data to the USN application. A healthcare

application displays the current location and health condition of the resident based on the sensed data.

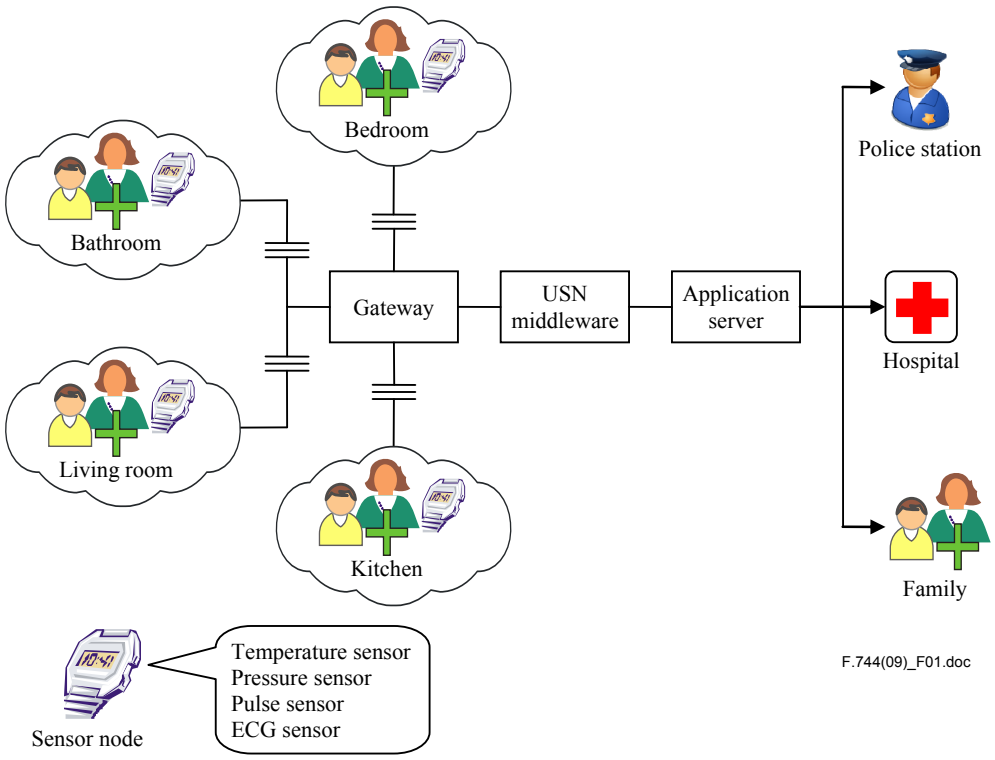

Figure 1 – Use case of a healthcare service

A healthcare application needs residents' medical histories and medical background to provide context-aware service for each resident. Based on the medical background, context-aware rules can be created. Context-aware rules take sensed data and residents' medical histories as inputs and issue emergency notifications when certain emergency conditions are met. Emergency notifications are delivered to the related authorities such as a hospital, a police station and the relatives or family to handle the situation appropriately. The steps are as follows:

Step 1: Managers or operators of a healthcare application should generate appropriate rules based on the medical background to process context-aware information. For services tailored to the individual, the rules need to take residents' medical histories as inputs.

Step 2: Each resident wears a sensor node on his/her wrist. After being turned on, each sensor node senses body temperature, pulse, momentum, and ECG and then periodically sends that sensed data to USN middleware.

Step 3: When a sensor network tries to connect to USN middleware, the USN middleware authenticates the connecting sensor network to protect itself against deceptive sensor networks.

Step 4: If a healthcare application tries to connect to USN middleware, the USN middleware needs to authenticate the connecting application.

Step 5: A healthcare application can utilize a sensor network metadata directory service to obtain the target sensor network metadata.

Step 6: A healthcare application registers appropriate rules to the USN middleware to obtain emergency notifications based on the rules and sensed data.

Step 7: USN middleware collects sensed data from the appropriate sensor networks, based on the requests of USN applications. USN middleware receives sensed data from sensor networks without any requests, if they periodically send sensed data.

Step 8: USN middleware processes sensed data based on the rules for context awareness and simultaneously provides sensed data to a healthcare application.

Step 9: A healthcare application displays current locations and the medical status of the residents on the screen using processed data and/or raw sensed data from USN middleware. The user can select which of the target residents to monitor in detail, then the healthcare application shows the detailed values on the screen.

Step 10: USN middleware generates an event to notify the application of an emergency if certain abnormal condition is detected. The application then alerts related parties such as a hospital and family.

Step 11: When a healthcare application is about to stop its service, it may request the USN middleware to no longer collect data from the sensor networks.

6.3.2 Cold chain management application

A cold chain management application uses RFID tag data and sensed data to monitor the condition of a delivery system. RFID tags are attached to each palette containing products to identify the objects on the palette. Sensor nodes and RFID readers are installed in delivery vehicles and storage buildings of distribution centres. Sensor nodes sense temperature, and send the data to a cold chain management application to report the current status of the delivery environment. If unusual conditions are detected, then a cold chain management application alerts operators to such unusual conditions. The steps are as follows:

Step 1: A cold chain management application generates appropriate rules based on each product management information to determine and then react to the abnormal conditions.

Step 2: Each sensor node equipped with sensors and RFID readers are attached to the delivery vehicles and storage buildings to sense temperature and to recognize the delivered items.

Step 3: Sensor networks/RFID readers are connected to USN middleware to provide sensed data/RFID tag data. When connected, USN middleware is required to authenticate the connecting sensor networks/RFID readers.

Step 4: When the application requires connection to USN middleware, the USN middleware authenticates the connecting application to protect itself from unauthorized application.

Step 5: A cold chain management application registers the context-aware rules in the USN middleware.

Step 6: A cold chain management application can utilize a sensor network metadata directory service to obtain the target sensor network metadata.

Step 7: A cold chain management application requests sensed data/RFID tag data to USN middleware. USN middleware in turn sends the requests to the target sensor networks and RFID readers to collect data.

Step 8: Sensor networks sense temperature and send the sensed data to USN middleware. At the same time, RFID readers collect RFID tag data and then send them as well.

Step 9: USN middleware collects and integrates the sensed data and RFID tag data to provide pairs of {RFID tag data, sensed data} to a cold chain management application. USN middleware filters redundant duplicate tag data to reduce the redundant RFID tag data. Moreover, sensed data aggregation may be performed.

Step 10: USN middleware tells the sensor networks to lower the temperature, if the rules are specified. Then the refrigerator (actuator within the sensor network) can be activated to decrease the temperature. Simultaneously, the event can be delivered to the application to notify the operators of the abnormal situation.

Step 11: A cold chain management application displays the current status of environment on the screen. RFID tag data may be converted into the product information and linked to other sensed data.

Step 12: A cold chain management application may request USN middleware not to collect data any more when a cold chain management application is about to stop its service.

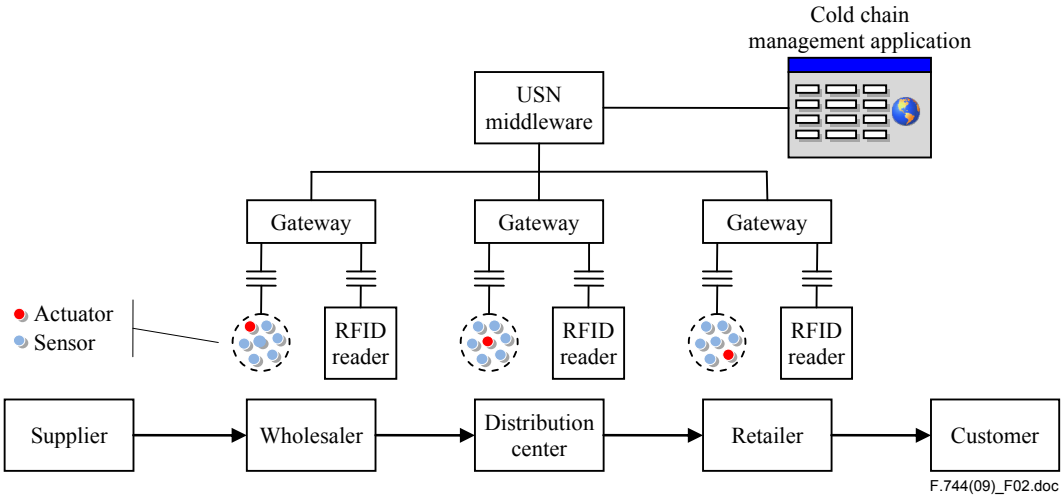

Figure 2 – Use case of a cold chain management service

6.3.3 Sensor network monitoring application

A sensor network monitoring application monitors the various sensor networks. The purpose of a sensor network monitoring application is to check and to control current state of sensor networks. See Figure 3.

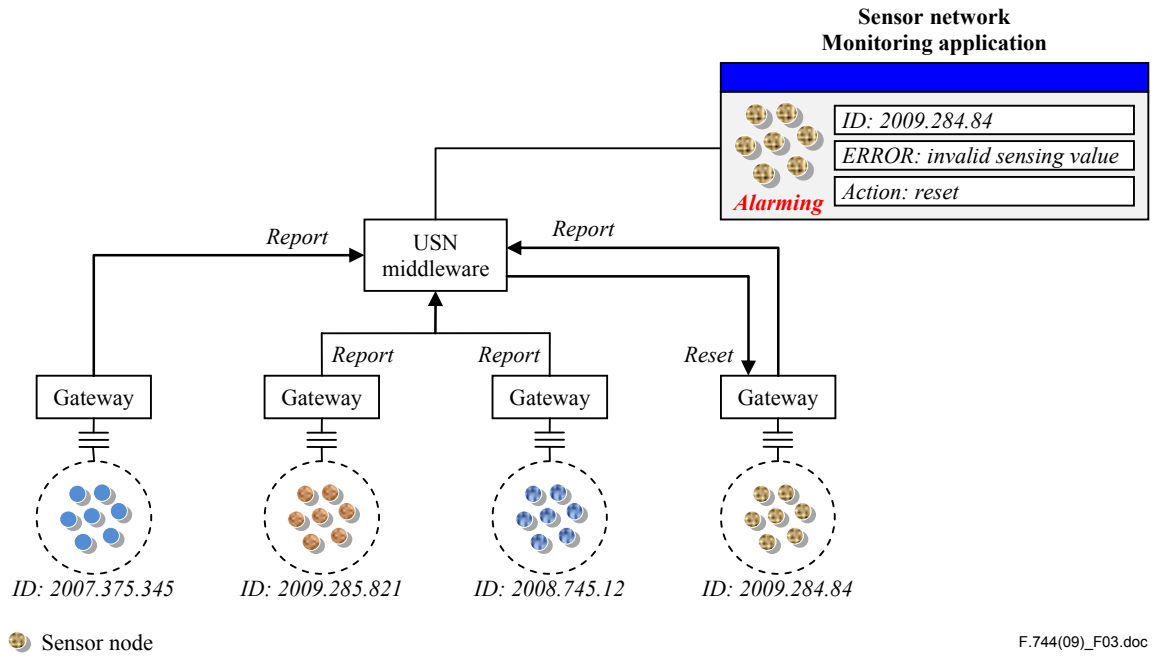

Figure 3 – Use case of a sensor network monitoring service

The sensor network should be associated with the appropriate authorization mechanism because sensor networks are shared by different applications. Therefore, only authorized applications or administrators should be permitted to control the sensor networks. The sensor network monitoring service operates as follows:

Step 1: A sensor network connects to USN middleware. The USN middleware is required to authenticate the connecting sensor network.

Step 2: A sensor network monitoring application connects to the USN middleware to monitor the sensor networks. The USN middleware is required to authenticate the connecting application.

Step 3: A sensor network monitoring application may monitor all the sensor networks that are connected to USN middleware at the same time, or may monitor specific sensor networks. A sensor network monitoring application may refer to the sensor network metadata directory service to determine target sensor networks.

Step 4: A sensor network monitoring application requests USN middleware to collect monitoring information from target sensor networks.

Step 5: USN middleware sends monitoring requests to the sensor networks for collecting monitoring information.

Step 6: Sensor networks send current information to USN middleware for monitoring.

Step 7: USN middleware collects monitoring information from the sensor networks and sends them to a sensor network monitoring application.

Step 8: A sensor network monitoring application displays the current status of target sensor networks on the screen.

Step 9: If a sensor network monitoring application detects abnormal conditions, it may request USN middleware to reset the sensor network.

Step 10: USN middleware sends the reset request to the target sensor network.

Step 11: USN middleware receives the reset result and sends the result to a sensor network monitoring application.

7 Functional model of USN middleware

In the USN service environment where the USN middleware works there are three main elements: the USN application, the USN middleware and the sensor network. In this environment, the USN application utilizes the sensed data and/or activates some actuators, and the sensor network produces sensed data and control actuators. The USN middleware provides functions commonly required by different USN applications and services over the shared sensor networks.

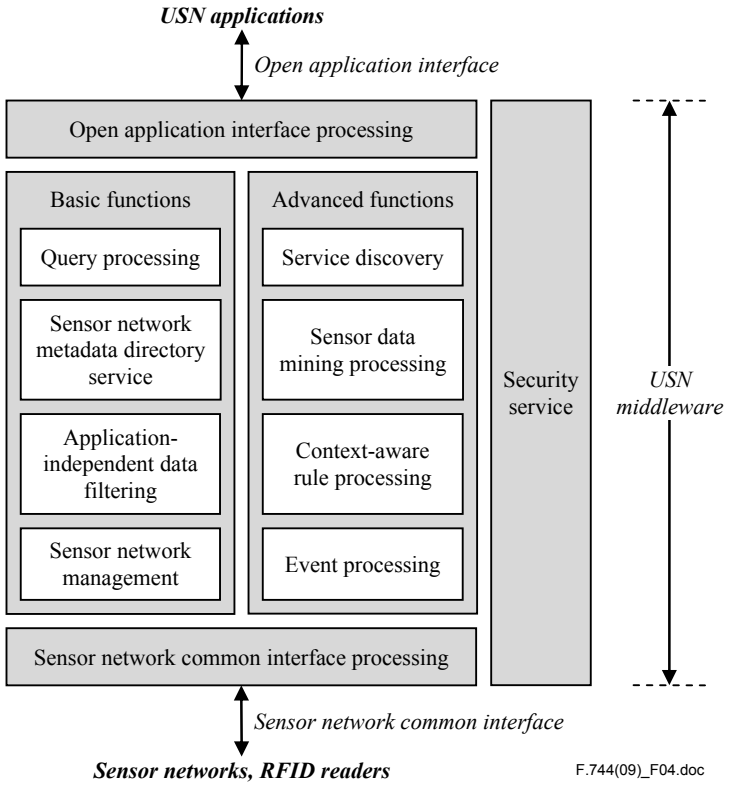

Figure 4 – Functional model of USN middleware

As shown in Figure 4, USN middleware provides functions for USN applications such as data query processing, sensor data mining processing, event processing, sensor network metadata directory service, data filtering, context-aware rule processing and sensor network management. In addition, USN middleware may provide a service discovery function for USN applications. USN applications refer to service discovery to retrieve functions provided by USN middleware and other USN services. In summary, USN middleware may provide five functions: open application interface processing, basic functions, advanced functions, sensor network common interface processing and security service.

7.1 Open application interface processing

An open application interface processing provides the following functions for USN applications and services:

– application interface for applications to access USN middleware;

– authentication, authorization and channel protection functions by cooperating with a security service.

7.2 Basic functions

USN middleware provides basic functions that can be used by most USN applications, as follows:

– Sensor network metadata directory service:
  - registration and retrieval of USN metadata.

– Application-independent data filtering:
  - sensed data validation regarding associated measurement units, data types and value ranges;
  - RFID tag data filtering (duplicate reduction).

– Sensor network management:
  - management of sensor networks including sensor network gateways and RFID readers;
  - software upgrade of sensor node;
  - topology (connectivity) management.

  NOTE – Software upgrade of sensor node and topology management can be provided optionally by sensor network management.

– Query processing:
  - query scheduling for multiple USN applications and multiple sensor networks;
  - query routing to designated sensor nodes;
  - application-dependent RFID tag data filtering;
  - application-dependent sensed data filtering;
  - sensed data aggregation and integration based on an application policy.

7.3 Advanced functions

Advanced functions are the functions that provide service discovery and processed information to applications by using basic functions if necessary. Advanced functions provide the following functions for USN applications and services:

– Sensor data mining processing:
  - detecting outlier, analysing patterns and predicting some events.

– Event processing:
  - generation of events based on raw sensed data or context-aware rule processing;
  - processing of events such as alerting applications and necessary authorities.

– Context-aware rule processing:
  - processing application-dependent context-aware rules on the collected sensed data.

– Service discovery:
  - registration and discovery of USN middleware services;
  - registration and discovery of USN services.

7.4 Sensor network common interface processing

A sensor network common interface processing provides the following functions for USN applications and services:

– sensor network common interface processing;

– authentication and channel protection functions by cooperating with a security service.

7.5 Security service

The security service provides the following functions for protecting USN middleware:

– access control for protecting USN middleware from malicious attacks;

– secure channel for protecting information exchanged between USN middleware and applications/sensor networks;

– secure channel for protecting information exchanged within USN middleware if USN middleware functions are distributed over the networks.

8 Requirements for USN middleware

According to the functional model, the requirements for USN middleware are defined in terms of interfaces, functions and security.

8.1 Interface requirements

– A standardized interface between the USN middleware and heterogeneous sensor networks is required to be provided.

– A standardized interface for applications to access USN middleware is required to be provided.

8.2 Functional requirements

– It is required to support sensor network metadata management.

– It is required to provide sensor network metadata directory service for obtaining sensor network information.

– It is required to provide appropriate data filtering functions such as redundant RFID tag data filtering and sensed data validation for removing unnecessary or erroneous data.

– It is required to provide sensor network monitoring and control function to effectively utilize sensor network.

– It is required to support explicit request-reply query processing mode (pull-mode) and implicit request-reply query processing mode (push-mode). An implicit request-reply query processing means providing sensed data to USN application without any explicit request.

– It is recommended to provide a sensor data mining function.

– It is recommended to provide event generating and processing functions.

– It is recommended to provide a context-aware rule processing function for supporting decision making of USN applications.

– It is recommended to provide service registration and discovery functions including both, USN services and USN middleware services.

8.3 Security requirements

USN middleware is required to provide the appropriate access control mechanisms to protect the sensed data from malicious applications and corrupted sensor networks. Before access to USN middleware, each application is required to register its profile to the USN middleware. Based on the registered application profiles, each application is authenticated and authorized to use USN middleware functions and sensor networks. The application profile may include application description, security information, policy, etc. USN middleware is required to provide security on sensed data and to control data against malicious attacks. In addition, USN middleware is required to authenticate the connecting sensor networks to prevent corruption of sensed data. It is recommended to provide a secure channel to protect the sensed data between the USN middleware and sensor networks.

NOTE – Detailed security requirements for USN middleware are out of scope of this Recommendation.

Bibliography

[b-ITU-T F.700] Recommendation ITU-T F.700 (2000), *Framework Recommendation for multimedia services.*

[b-ITU-T F.701] Recommendation ITU-T F.701 (2000), *Guideline Recommendation for identifying multimedia service requirements.*

[b-ITU-T F.741] Recommendation ITU-T F.741 (2005), *Service description and requirements for audiovisual on-demand services.*

[b-ITU-T F.742] Recommendation ITU-T F.742 (2005), *Service description and requirements for distance learning services.*

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