

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1312

(02/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services – Ubiquitous sensor
network security

Ubiquitous sensor network middleware security guidelines

Recommendation ITU-T X.1312

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

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

Recommendation ITU-T X.1312

Ubiquitous sensor network middleware security guidelines

Summary

Recommendation ITU-T X.1312 provides guidelines for ubiquitous sensor networks (USN) middleware security. It analyses security threats on USN middleware and defines security requirements.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1312	2011-02-13	17

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/>.

© ITU 2011

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
4	Abbreviations.....	2
5	Overview of USN middleware security.....	2
	5.1 USN middleware for applications	3
	5.2 USN middleware for sensor networks.....	4
	5.3 USN middleware system	4
6	Security threats to USN middleware	4
	6.1 System security threats	4
	6.2 Security threats on data	5
	6.3 Security threats on communication	6
7	Security requirements for USN middleware.....	7
	7.1 Security requirements for the system	7
	7.2 Security requirements for data.....	8
	7.3 Security requirements for communication	8
8	Guidelines for USN middleware security.....	9
	8.1 Middleware system security	10
	8.2 Access control	10
	8.3 Stored data protection.....	11
	8.4 Transmission/receipt data security	11
	8.5 Secure channel.....	12

Recommendation ITU-T X.1312

Ubiquitous sensor network middleware security guidelines

1 Scope

This Recommendation provides guidelines for USN middleware security and also covers the following:

- overview of USN middleware security;
- the functional model of USN middleware;
- security threats on USN middleware;
- security requirements for USN middleware;
- guidelines for USN middleware security.

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 F.744] Recommendation ITU-T F.744 (2009), *Service description and requirements for ubiquitous sensor network middleware*.
- [ITU-T X.1311] Recommendation ITU-T X.1311 (2011) | ISO/IEC 29180:2011, *Information technology – Security framework for ubiquitous sensor network*.
- [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 open application interface [ITU-T F.744]: An interface used by USN applications to access USN middleware.

3.1.2 processed data [ITU-T F.744]: Data that are processed from raw sensed data by sensor network or USN middleware.

3.1.3 sensed data [ITU-T F.744]: Data sensed by a sensor that is attached to a specific sensor node.

3.1.4 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.

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

3.1.6 sensor network common interface [ITU-T F.744]: An interface used between USN middleware and a sensor network/radio frequency identification (RFID) reader.

3.1.7 sensor network metadata [ITU-T F.744]: 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.

3.1.8 sensor network metadata directory service [ITU-T F.744]: A directory service that provides sensor network metadata.

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

3.1.10 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.

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

4 Abbreviations

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

DDoS Distributed Denial of Service

DoS Denial of Service

RFID Radio Frequency Identification

SN Sensor Network

USN Ubiquitous Sensor Network

WSN Wireless Sensor Network

5 Overview of USN middleware security

USN middleware is an intermediate entity that provides the functions commonly required by different types of USN applications and services. USN middleware receives requests from USN applications, and delivers those requests to the 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 the like [ITU-T F.744].

This means that all the data involved in USN services pass through USN middleware. For this reason, an attack on USN middleware can cause serious damage such as service disruption, misuse, system failure, and more.

In the USN service environment where 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 controls actuators. The USN middleware provides functions commonly required by different USN applications and services over the shared sensor networks [ITU-T F.744].

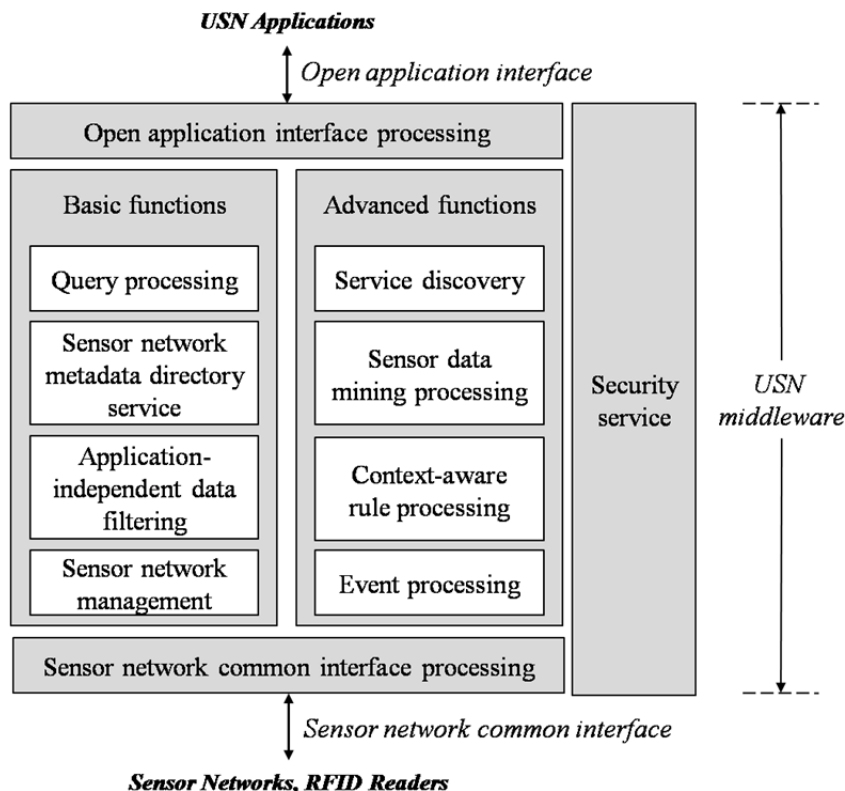


Figure 1 – Functional model of USN middleware

As shown in Figure 1, USN middleware provides five functions: open application interface processing, basic functions, advanced functions, sensor network common interface processing and security service. Of these functions, this Recommendation focuses on security service. Security service in USN middleware is approached from the following three perspectives.

5.1 USN middleware for applications

Applications use USN middleware to control sensor networks and collect sensing information from the sensor networks connected to the USN middleware. Applications send queries to USN middleware to acquire raw sensing value and/or processed information. Information is integrated and derived from raw sensing data from a (or multiple) sensor network(s). The USN middleware interprets application requests and sends requests to various sensor networks in ways that are comprehensible by each sensor network. Multiple applications can share the sensing information through USN middleware. USN middleware can provide raw sensing value from sensor networks. In addition, USN middleware integrates several raw sensing values from different sensor networks, and, even more, provides processed information from several sensing values and legacy data. Furthermore, USN middleware can derive processed information from raw sensing data, historical data and legacy data using mining technology, context-aware technology, and event processing technology.

An application can control sensor networks that are connected to USN middleware. The application may activate/deactivate some kinds of actuators, change the sensor network's topology, or even dynamically change applications running on a sensor node.

Usually, a sensor network is powered by batteries. Furthermore, the devices required for a sensor network, such as sensor node, sink node, and gateway, are not cheap. For this reason, applications have to manage sensor networks in a cost-effective way.

5.2 USN middleware for sensor networks

Sensor networks use USN middleware to provide sensing values to the applications. A sensor network provides its sensing value as response to a request, or without an explicit request. Usually, a sensor network is used for environmental surveillance.

From a USN middleware viewpoint, sensor networks are information providers. Sensing information flowing into USN middleware is flowing into several applications. Therefore, the authenticity of sensing information is very crucial to the USN middleware and the USN application.

5.3 USN middleware system

USN middleware is used to provide a logical link between a USN application and a sensor network, and plays a pivotal role in data processing for USN service. Also, it manages a variety of sensor networks and supports many USN applications. In this situation, if security challenges occur in USN middleware, serious damage will be caused, and confidence in the USN service will be lost. For this reason, USN middleware security should be considered as a design point of USN middleware and securely maintained.

6 Security threats to USN middleware

USN middleware is located between the USN application and the sensor network in the USN service model. It processes sensing data from the sensor network, and sends the processed information to the appropriate application. Therefore, attacks on USN middleware cause USN service disruption, misuse, system failure, and so on. The following clause examines USN middleware security threats by analysing potential attacks related to USN middleware.

USN middleware security threats can be divided into three groups according to the target: device, data and network.

6.1 System security threats

As stated earlier, USN middleware plays an important role in USN service. For this reason, if USN middleware is compromised by an attack, the USN service may be completely disrupted.

Accordingly, this clause defines security threats that can occur on USN middleware as a system.

6.1.1 Unauthorized USN middleware access

- Unauthorized USN middleware access by a USN application.

This security threat occurs when an unregistered USN application tries to access USN middleware. An attacker can use a USN application as a means of attack after the USN application is compromised by an initial attack. In this way, the attacker can compromise the sensor network or use it, because the USN application manages the sensor network via USN middleware.

- Unauthorized USN middleware access by a sensor network.
This security threat occurs when an unregistered sensor network tries to access USN middleware. An attacker can use a sensor network as a means of attack after the sensor network has been compromised by an initial attack. Through this approach, an attacker can illegally access USN middleware and cause confusion in the USN service, because the sensor network communicates with the USN middleware to transmit sensing data.
- Unauthorized USN middleware access by external entities.
This security threat occurs when an external entity tries to access the USN middleware directly. Through this means, an attacker may try to steal the data stored in USN middleware, disturb USN service provision, use resources illegally, etc.

6.1.2 DoS, DDoS attacks against USN middleware

This security threat occurs when a huge number of packets is transmitted from the USN application or sensor network to USN middleware, or when an attacker makes and sends a huge number of packets to the USN middleware to compromise the USN middleware system. This attack consumes large amounts of system resources. As a result, the USN service cannot be provided normally, causing monetary losses.

6.1.3 Malicious or abnormal traffic transfer to USN middleware

This security threat occurs when malicious or abnormal traffic is transmitted to the USN middleware. An attacker can send malicious data to USN middleware. This might be a malware such as a worm, virus, etc. Also, an attacker can confuse the USN middleware by sending abnormal traffic. These kinds of attacks compromise the USN middleware system.

6.1.4 Misuse and abuse of the USN middleware system

This security threat occurs when a USN middleware system administrator misunderstands the system and operates it incorrectly. The administrator may consume excessive system resources and cause it to function incorrectly. These kinds of security threats can lead to tremendous losses of resources, and threaten service availability.

6.1.5 Careless mistake

This security threat occurs when a USN middleware system administrator makes an error in handling the system's operation. It also can occur when the updated rules have not been applied to the USN middleware system, in the event that the system policy has been updated. These situations can cause a state of confusion in the USN service.

6.1.6 Cross-application breach of containment

In the context of a common USN service platform serving different USN applications for different users with potentially conflicting interests, it is desirable to ensure containment across applications so that an authorized middleware user for one application is not capable of gaining access to the USN resources of another application. The threat consists of an attacker gaining access to the resources of e.g., USN application #1 by first becoming an authorized user for USN application #2.

6.2 Security threats on data

Data passed through USN middleware are classified into sensitive information for service entity identification and authentication, sensing data for USN service providing, data for sensor network controlling, and all data stored in USN middleware.

This clause specifies the security threats that can occur in relation to each type of data.

6.2.1 Data leakage

- Sensitive information leakage.

Once a USN application or a sensor network attempts to access USN middleware, the USN middleware requests the authentication information of the USN application or sensor network for identification and authorization. In the middle of this process, sensitive information such as the ID/PW of the USN application and sensor network can be exposed.

- Control data leakage.

A USN application manages and controls sensor network via USN middleware. To do this, the USN application sends control data to the USN middleware and the USN middleware delivers the data to the sensor network. In this process, control data can be exposed.

- Sensing data leakage.

A sensor collects data for environment and situations, etc. The sensing data is then transmitted to USN middleware. In this process, the sensing data can be exposed.

- Leakage of data stored in USN middleware.

This security threat occurs when the data stored in USN middleware is exposed by carelessness or by an attack. Compromising USN middleware can cause a state of confusion in USN service, because USN middleware processes and stores the authentication information of USN applications and sensor network as well as the service data to provide the USN service.

6.2.2 Data forgery

- Sensitive information forgery.

This security threat occurs when an attacker disguises itself as a legal USN application or sensor network by modifying sensitive information, such as ID, PW, etc. Using this, the attacker tries to access USN middleware.

- Control data forgery.

This security threat occurs when an attacker modifies sensor network control data and gets permission to manage and control the sensor network. Through this process, the attacker can use the sensor network for another purpose or for an attack.

- Sensing data forgery.

This security threat occurs when an attacker modifies sensing data collected by sensor nodes. This causes the USN service to provide information based on the modified data.

- Forgery of data stored in USN middleware.

This security threat occurs when the data stored in USN middleware is modified. This can cause a state of confusion in the USN service, because the USN middleware processes all the data used in the USN service.

6.3 Security threats on communication

This clause specifies the security threats that can occur to communications.

6.3.1 Eavesdropping

- Eavesdropping on communications between a USN application and USN middleware.

An attacker can get USN service data by eavesdropping on communications between the USN application and USN middleware. The attacker can try another attack based on the derived information after analysing the data.

- Eavesdropping on communications between the sensor network and USN middleware.
An attacker can get USN service data by eavesdropping on communications between the USN middleware and the sensor network. After analysing the data, the attacker can try another attack based on the derived information.

6.3.2 Interruption

- Interruption of the communication between a USN application and USN middleware.
This security threat occurs when an attacker interrupts the communication between a USN application and USN middleware. This causes the USN service to not be provided normally by blocking authentication messages or sensing data request queries between the USN application and the USN middleware.
- Interruption of the communication between the sensor network and the USN middleware.
This security threat occurs when an attacker interrupts the communication between USN middleware and a sensor network. This prevents USN service from being provided normally by blocking authentication messages or sensing data transmission between USN middleware and the sensor network.

6.3.3 Hijacking

- Hijack packets sent between the USN application and USN middleware.
An attacker can hijack packets that are transmitted between the USN application and USN middleware. After analysing the packet, the attacker can try another attack targeting the USN application or USN middleware.
- Hijack packets sent between the sensor network and USN middleware.
An attacker can hijack packets that are transmitted between the sensor network and USN middleware. After analysing the packet, the attacker can try another attack targeting the USN application or USN middleware.

6.3.4 Jamming (wireless section)

If communication between the USN middleware and the sensor network is wireless, a jamming attack that causes a disturbance in the radio waves can occur due to the network's wireless communication property. This prevents the USN service from being provided normally.

7 Security requirements for USN middleware

This clause clarifies the security requirements for providing secure USN service, considering USN middleware security threats.

7.1 Security requirements for the system

The following are the security requirements for protecting against attacks to a USN middleware system.

7.1.1 Security requirements for unauthorized USN middleware access response

USN middleware is basically required to allow only authorized entities access to a USN middleware system.

In detail:

- It is required to allow only authorized USN applications access to the USN middleware system.
- It is required to allow only authorized sensor networks access to the USN middleware system.

- It is required to allow only authorized external entities access to the USN middleware system.

7.1.2 Security requirements for DoS and DDoS attack response

USN middleware is required to prevent DoS and DDoS attacks. It is required to enable service to be constantly maintained, even when the system has been attacked.

7.1.3 Security requirements for malicious and abnormal traffic influx response

USN middleware is required to prevent malicious or abnormal traffic attacks and to constantly enable USN service.

7.1.4 Security requirements for USN middleware system misuse and abuse response

USN middleware is required to design and manage the USN middleware system securely to prevent system misuse and abuse.

7.1.5 Security requirements for response to worker error

USN middleware is required to manage the USN middleware system securely in order to prevent mistakes arising from carelessness.

7.1.6 Security requirements for cross-application breach of containment response

USN middleware is required to allow only authorized users access to USN application resources.

7.2 Security requirements for data

The following are the security requirements for protecting data against attacks.

7.2.1 Security requirement for data leakage response

USN middleware is basically required to maintain the confidentiality of USN data.

In detail:

- It is required to treat sensitive information as confidential.
- It is required to treat control data as confidential.
- It is required to treat sensing data as confidential.
- It is required to treat the data stored in USN middleware as confidential.

7.2.2 Security requirements for data forgery response

USN middleware is basically required to maintain the integrity of USN data.

In detail:

- It is required to maintain the integrity of sensitive information.
- It is required to maintain the integrity of control data.
- It is required to maintain the integrity of sensing data.
- It is required to maintain the integrity of the data stored in USN middleware.

7.3 Security requirements for communication

The following are the security requirements for protecting against attacks during communication between USN middleware and a USN service entity.

7.3.1 Security requirements for eavesdropping response

USN middleware is basically required to keep communication between USN middleware and the USN service entity confidential.

In detail:

- It is required to keep communication between the USN application and USN middleware confidential.
- It is required to keep communication between USN middleware and the sensor network confidential.

7.3.2 Security requirements for interruption response

USN middleware is basically required to prevent an interruption in the communication between the USN middleware and the USN service entity, and to enable constant USN service.

In detail:

- It is required to prevent an interruption of communication between the USN application and USN middleware and to enable constant USN service.
- It is required to prevent an interruption of communication between the USN middleware and the sensor network, and to enable constant USN service.

7.3.3 Security requirements for hijacking response

USN middleware is basically required to prevent the hijacking of packets sent between USN middleware and the USN service entity, to avoid the exposure and analysis of such packets.

In detail:

- It is required to prevent the hijacking of packets sent between the USN application and the USN middleware, to avoid the exposure and analysis of such packets.
- It is required to prevent the hijacking of packets sent between the USN middleware and the sensor network, to avoid the exposure and analysis of such packets.

7.3.4 Security requirement for jamming response

The USN middleware system is required to protect against jamming attacks in wireless communications between the USN middleware and the sensor network and to enable constant USN service.

8 Guidelines for USN middleware security

This clause specifies the security functions that USN middleware should satisfy for a confidential USN service. Figure 2 shows the security functions of the USN middleware. Security service in USN middleware consists of middleware system security, access control, data protection, transmission/receipt data security and secure channel. Security guidelines are provided on the security functions in terms of security between an application and the middleware, between the middleware and the sensor network(s), and within the middleware itself.

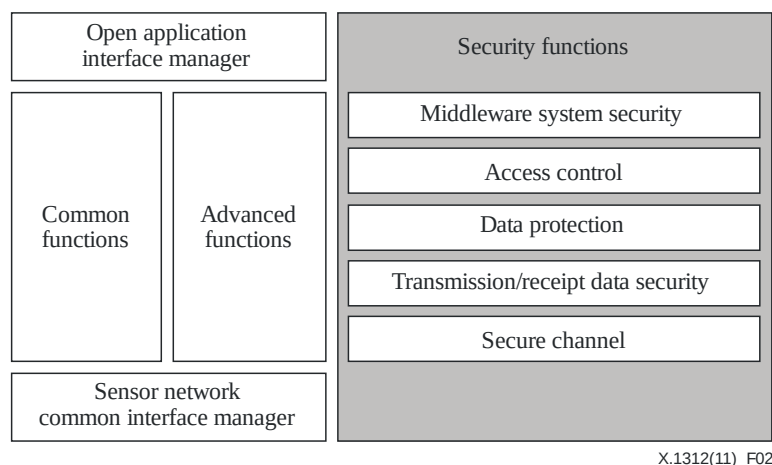


Figure 2 – Security functions for USN middleware

8.1 Middleware system security

The purpose of this function is to protect the middleware itself. USN middleware plays an important role in the USN environment. Hence, if USN middleware is compromised by a malicious person, it may cause a critical situation. But data delivered from sensor networks is untrustworthy data and may even contain malicious code. Queries transmitted from applications may also be malicious code aiming to compromise USN middleware. Accordingly, middleware system security is necessary to protect the middleware itself.

The following are the security guidelines for middleware system security:

- The USN middleware system is recommended to be designed securely.
- The USN middleware system shall not preclude support for unsecured protocols.
- The USN middleware system is recommended to support the capability of being updated periodically or at the request of the administrator of the middleware.
- The USN middleware system is recommended to support the capability to periodically test for the integrity of the middleware.
- The USN middleware system is recommended to support the capability to clean the USN middleware of all data before the USN middleware is discarded.
- The USN middleware system is recommended to support the capability to detect and block illegal formatted data.
- The USN middleware system is recommended to support the capability to detect and block malicious traffic.

8.2 Access control

The purpose of this function is to prevent unauthorized access from applications and sensor networks. It can be implemented with authentication for applications and sensor networks. In particular, authorization is also required for applications, as applications have different privileges for specific resources (e.g., sensed data, etc.).

The following are the security guidelines for access control:

- The USN middleware is recommended to support the capability to block the access of unregistered USN applications.
- The USN middleware is recommended to support the capability to block the access of unregistered sensor networks.
- The USN middleware is recommended to support the capability to assign different permissions of access to each USN application resource.

- The USN middleware is recommended to support the capability to manage the list of allowed access to sensor networks by USN applications.
 - For wired sensor networks, the USN middleware is recommended to support access control with the ID and authentication information of the sensor network.
 - For mobile sensor networks, the USN middleware is recommended to support access control with ID, authentication information and verified location information of the sensor network.
 - For ad-hoc sensor networks, the USN middleware is recommended to support access control with ID, authentication information, verified location information and network validation of the sensor network.
- The USN middleware is recommended to support the capability to authenticate and verify a sink node trying to access USN middleware.
 - If the sink node is wired, USN middleware is recommended to support the capability to determine whether the node is cloned or not, in addition to authentication.
 - If the sink node is mobile, USN middleware is recommended to support the capability to re-authenticate according to whether it is moving.
 - If the sink node is ad-hoc, USN middleware is recommended to support the capability to determine whether the node is alive or not, in addition to authentication and re-authentication.
- USN middleware is recommended to support the capability to allow access only by an authenticated administrator.

8.3 Stored data protection

This function is to ensure the confidentiality of data stored in USN middleware. The data may be authentication-related data for application and sensor networks, important sensed data, or the like.

The following are the security guidelines for data protection:

- The USN middleware is recommended to support the capability to keep ID and authentication information of sensor network securely through ID management and DB security.
- The USN middleware is recommended to support the capability to keep ID and authentication information of USN applications securely through ID management and DB security.
- The USN middleware is recommended to support the capability to keep sensing data securely through DB security.

8.4 Transmission/receipt data security

This function is to protect sensitive data, including authentication data such as passwords and the like, exchanged between applications and middleware and between sensor networks and middleware.

The following are the security guidelines for transmission/receipt data security:

- The USN middleware is recommended to support the capability to send and receive authentication data safely through encryption/decryption.
- The USN middleware is recommended to support the capability to determine whether the receipt data is forged or not through an integrity check.
- The USN middleware is recommended to support the capability to deliver sensing data to a USN application safely through encryption/decryption.

- The USN middleware is recommended to support the capability to determine whether the sensing data received from the USN application is forged or not through an integrity check.
- The USN middleware is recommended to support the capability to determine whether the sending data received from a sensor network is forged or not through an integrity check.

8.5 Secure channel

This function is to protect the communication channel between applications and middleware and between the sensor network and middleware.

The following are the security guidelines for a secure channel:

- The USN middleware is recommended to support the capability to maintain communication between the USN application and the USN middleware securely through methods of establishing a secure channel.
- The USN middleware is recommended to support the capability to securely maintain communications between the sensor network and the USN middleware through methods of establishing a secure channel.
- The USN middleware shall not preclude support for unsecured communication protocols between the USN application and the USN middleware.
- The USN middleware shall not preclude support for unsecured communication protocols between the sensor network and USN middleware.

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