INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

STUDY GROUP 17

TD 0578

English only

Original: English

Question(s): 6/17 Geneva, 16-25 September 2009

TEMPORARY DOCUMENT

Source: Editors

Title: Draft Recommendation X.usnsec-2 : USN middleware security guidelines

Summary

This document is an output text of ITU-T draft Recommendation X.usnsec-2, agreed at the ITU-T Q.6/17 meeting in September 2009.

Contact:	Mi Yeon Yoon KISA Korea	Tel: +82 2 405 5311 Fax: +82 2 405 5219 Email: myyoon@kisa.or.kr
Contact:	Nam Je Park ETRI Korea	Tel: +82 42 860 5426 Fax: +82 42 860 5611 Email: namjepark@etri.re.kr
Contact:	Mi Joo Kim KISA Korea	Tel: +82 2 405 5307 Fax: +82 2 405 5219 Email: mijoo.kim@kisa.or.kr

Contents

Summary

This Recommendation aims to provide guidelines for USN middleware security. This Recommendation analyzes security threats on USN middleware, defines security requirements, and develops the guidelines for USN middleware security.

X.usnsec-2, Ubiquitous sensor network (USN) middleware security guidelines

1. Scope

This draft Recommendation describes provides guidelines for USN middleware security, this draft Recommendation covers as follows;

- Overview of USN middleware security
- Functional model of USN middleware
- Security threats on USN middleware
- Requirements for USN middleware security
- Guidelines for USN middleware security by technical means

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.usn-mw] ITU-T draft Recommendation F.usn-mw, *Service description and requirements for USN middleware.*

[Editor's note] Draft Recommendation X.usnsec-2 is referred to F.usn-mw that describes functional models of USN middleware. F.usn-mw is developed under Q.25/16. Therefore, if development of F.usn-mw is finished, the Recommendation number will be inserted instead of the draft Recommendation acronym.

[TBD]

3. Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application profile [ITU-T F.usn-mw]: Registered information of an application at USN middleware. It includes application identifier, application description, security information, accessible function list provided by USN middleware, etc.

3.1.2 open application interface [ITU-T F.usn-mw]: Interface used by USN applications to access USN middleware. This interface is web service-based interface and is required to be standardized for interoperability.

3.1.3 processed data [ITU-T F.usn-mw]: Data which are processed in sensor network or USN middleware from raw sensor data.

3.1.4 sensed data [ITU-T F.usn-mw]: Data sensed by a sensor which is attached to a certain sensor node.

[Editor's Note] According to F.usn-mw, there are some arguments for expression about sensed data. So, the expression may be changed according to the result of JCA-NID activities.

3.1.5 sensor network [ITU-T F.usn-mw]: The network which is comprised of various kinds of sensor nodes, which are equipped with sensor-compatible device(s) and actuator(s). It includes wireless sensor network, wired sensor network, and RFID reader.

3.1.6 sensor network common interface [ITU-T F.usn-mw]: Interface used between USN middleware and sensor network. This interface is required to be standardized for interoperability.

3.1.7 sensor network metadata [ITU-T F.usn-mw]: Metadata of heterogeneous sensor network. It includes sensor network identifier, description of a 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.usn-mw]: Directory service which provides sensor network metadata.

3.1.9 USN middleware [ITU-T F.usn-mw]: The common application platform to support various functions on behalf of various USN applications and services. It controls heterogeneous sensor networks, provides basic query processing, and provides high-level integrated services (context-aware processing, event processing, sensor data mining, integrated sensor data processing).

3.1.10 USN service[ITU-T F.usn-mw]: Service which uses various sensor data obtained from sensor networks.

[Editor's Note] If development of F.usn-mw is finished, the Recommendation number will be inserted instead of the draft Recommendation acronym.

[TBD]

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

[TBD]

4. Abbreviations

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

RFID Radio Frequency Identifier

SN Sensor Network

USN Ubiquitous Sensor Network

WSN Wireless Sensor Network

[TBD]

5. Overview of USN middleware security

The document classifies the USN middleware into two groups. One is USN application or administrator (consumer). Simply, The document calls it as an application. Application uses USN middleware to control USN infrastructure and acquire sensing information (raw sensing information or processed sensing information). The other group of users is USN infrastructure such as

wireless/wired sensor network, RFID, mobile RFID, and IP-USN, etc. Simply, call them as a sensor network.

5.1 USN middleware for application

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 which are 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 each sensor network comprehensible ways. 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 provide 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.

Application can control sensor networks which are connected to USN middleware. Application may activate/deactivate some kinds of actuators, change sensor network topology, or even change application running on sensor node dynamically.

Usually, sensor network is powered by battery. And the devices such as sensor node, sink node, gateway are not cheap yet. Therefore, applications have to manage sensor network in a cost-effective way.

5.2 USN middleware for Sensor Networks

Sensor networks use USN middleware to provide sensing values to the applications. Sensor network provides its sensing value as response to the request or without explicit request. Usually, sensor network is used for environmental surveillance. For example, Sensor Web[7] led by NASA JPL(Jet Propulsion Laboratory), has been used to implement a global surveillance program to study volcanos. Sensor network senses environmental parameters such as temperature, humidity, pressure, etc. The way of sensing is usually periodic with some specific interval and lifetime. Often it responds just one time on receiving the request from application. ETRI USN middleware classify the queries into 4 groups. They are Instant Query, Continuous Query, Instant Query with Condition and Continuous Query with Condition. “Instant Query”means sensor network responds only one time at receiving the request from application. “Continuous Query”means the query such as “get temperature every 30 minutes during 30 days.” “Instant Query with Condition”means a kind of Instant Query restricting the response. For example, “get temperature if sensed temperature is over 30^{o}C.” “Continuous Query with Condition”means a kind of Continuous Query restricting the response. For example, “get temperature every 30 minutes during 30 days if sensed temperature is over 30^{o}C.”

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

6. Functional model of USN middleware

Figure 1 shows a functional mode of USN middleware. This functional model is defined in [ITU-T F.usn-mw]. According to the functional model, USN middleware consists of open application

interface manager, common functions (query processor, sensor network metadata directory service, application-independent data filtering, sensor network manager), advanced functions (service discovery, sensor data mining processor, context aware rule processor, event processor), sensor network common interface manager, and security service. This draft Recommendation gives a detailed security functions for the security service.

[Editor's note] If development of F.usn-mw is finished, the Recommendation number will be inserted instead of the draft Recommendation acronym.

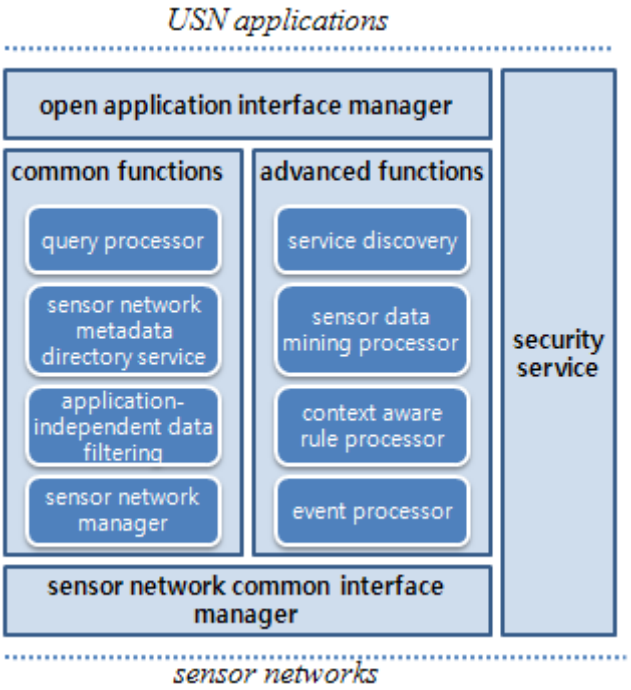

Figure 1 - Functional model of USN middleware

7. Security threats on USN middleware

USN middleware is located between USN application and Sensor Network in the USN service model. It processes sensing data from sensor network and sends the processed information to appropriate application. Therefore, attacks on USN middleware cause USN service disrupt, misuse, system failure, and so on. This clause provides USN middleware security threats by analyzing potential attacks relating to USN middleware.

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

7.1 Device-related security threats

Device-related security threats mean that attacks of application, sensor over the sensor network and middleware itself. There is close correlation among application, middleware, and sensor network. Hence, if the one object is attacked, and so it cannot operate normally, USN service cannot be provided normally.

Attacks on device are divided into three kinds; application, middleware, sensor.

Application manages sensor network by sending command to sensor network through middleware. Using this, attacker can disrupt sensor network and cause malfunction of sensor network by attacking application.

Security threats related to application are as follows.

- Buffer overflow
- SQL injection
- Brute force attack
- Dictionary attack
- Unauthorized access to administrator interface

USN middleware can be compromised by middleware system failure or attack, if that were to occur, USN system might be fall into utter confusion.

Also, the software used in sensor is generally designed for detecting something that is the natural function, except the security function. Because sensor typically has limited memory and bandwidth and low computing capability. Using this, attacker attacks to sensor and it can make sensor compromised. Also, sensor uses battery as a power source. Using this, attacker can make sensor stop working by exhausting a battery.

In addition, it is well known that the following attacks can be happened in sensor network, according to many research report and papers.

- Bogus routing information
- Sybil attack
- Selective forwarding
- Sinkhole attack
- Blackhole
- Hello flood attack, etc.

If sensor attack was happened and attacker manufactured data, sensor might send the manufactured data to USN middleware. It can cause a system failure.

7.2 Data-related security threats

Data-related security threats means that USN middleware is received unreliable data from application or sensor network or the data stored in USN middleware is leaked and modified illegally. Data collected, processed and forwarded by USN middleware are very important, because USN services are provided base on the basis of the data. Also, the data stored in USN middleware may use to manage application, sensor network and USN middleware itself. Hence, illegal changing for middleware management data can violate availability of USN service and cause critical effects on the system operation.

Data-related security threats are divided into two kinds of data; the data to USN middleware from application or sensor network and the data stored in USN middleware itself.

Forged data and wrong command message to USN middleware from application can cause system failure and compromise middleware system.

Forged data and wrong sensing value to USN middleware from sensor network can cause system failure and compromise middleware system.

Also, there are many kinds of security threats relating to data stored in USN middleware, such as a sensitive data leakage and illegal modification.

7.3 Network-related security threats

Network related security threats means that communication between two entities is attacked. There are two kinds of communication in USN service model. One is communication between application and USN middleware and another is communication between USN middleware and sensor network. Attacker can collect and modify communication data by attacking communications. Especially, in case the communication between two entities is supposed that it is a wireless communication, the data packet is transferred via the air interface. It can cause that the data packet is opened to everybody and analyzed. It is possible for unauthorized people to acquire data collected in sensor network that authorized users only can access. Also, attacker can modify data packets and insert malicious code, while the data packets are transmitted toward the USN middleware. It causes an USN system failure and has a bad influence upon the USN service.

Ultimately, attacks against the communication channel make data packet leakage and modification possible.

The followings are the general security threat happened over the network.

- Information Gathering
- Sniffing
- Spoofing
- Session Hijacking
- Denial of Service

8. Requirements for USN middleware security

This clause clarifies security requirements for providing secure USN service, based on above USN middleware security threats.

[Editor's Note] There was a discussion on the level of description for requirements. It is required to specify more detailed requirements including specific countermeasure method. Further contributions are required.

8.1 Device

The followings are the security requirements for preventing attacks against device.

- It is required to design middleware system safety, install security modules, manage a system and supply a means of controlling access to middleware system.
- It is required to design sensor software safety, install security modules, manage a system and supply a means of controlling access to software.
- It is required to design application safety, install security modules, manage a system and supply a means of controlling access to application.

8.2 Data

The followings are the security requirements for preventing attacks against data.

- It is required to detect and prevent for malicious data flow into USN middleware.
- It is required to detect and prevent for irregular data that is against the data format rule.

- It is required to verify data integrity.
- It is required to protect the sensitive data in case of data store.

8.3 Network

The followings are the security requirements for preventing attacks against network.

- It is required to protect communication channel among entities.
- It is required to verify transferring data integrity.

9. Security guidelines for USN middleware by technical means

9.1. Security Function for USN middleware

Figure 2 shows security functions that USN middleware should be satisfied for confidential USN service. Security functions can be divided into five sub-functions which are data traffic protection, channel protection, access control, data protection, and middleware protection.

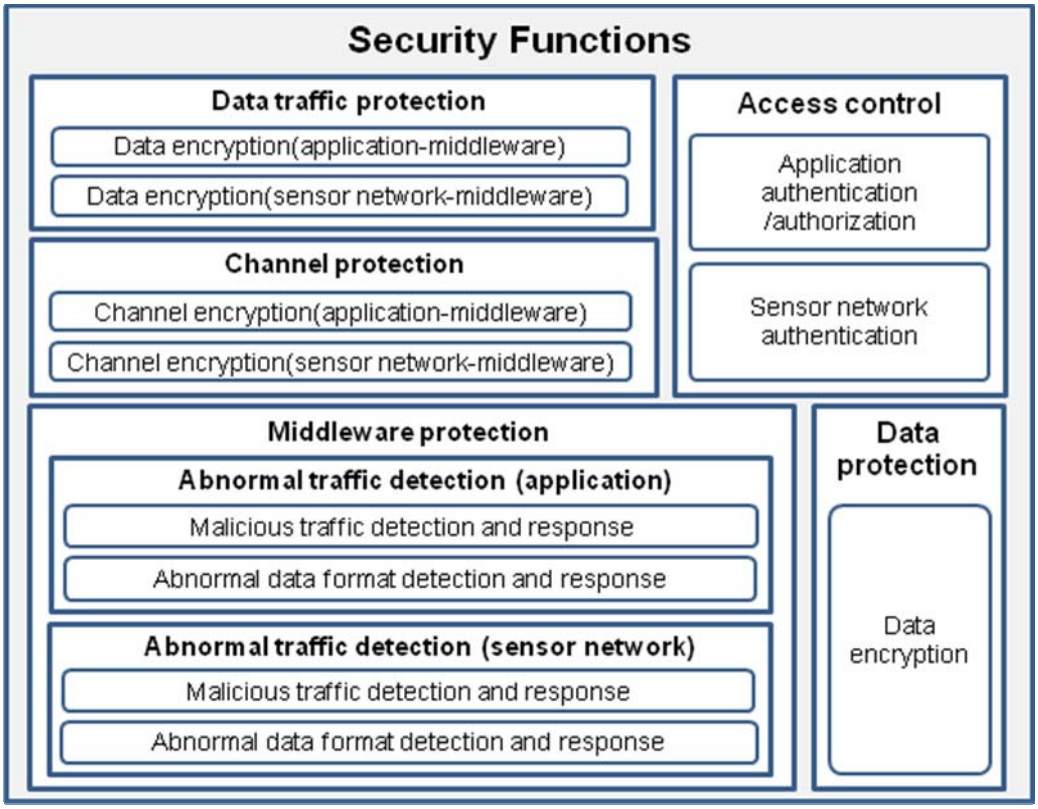

Figure 2 - Security functions for USN middleware security

Figure 2 shows the security model of USN middleware. Security service in USN middleware consists of Middleware protection, access control, traffic protection, interface protection and data protection.

9.1.1. Middleware protection

This function is to protect middleware itself. USN middleware plays an important role in USN environment. Hence, if USN middleware is compromised by malicious person, it may be cause a critical situation. But data delivered from sensor networks is untrusted data and even it may be

contained malicious code. Query transmitted from applications may be also malicious code aiming to compromise USN middleware. So, middleware protection is necessary to protect itself. This can be implemented with abnormal traffic detection.

To protect a middleware, the following detailed components are needed.

- Abnormal data format detection and response
- Malicious traffic detection and response

9.1.2. Access control

This function is to prevent unauthorized access from application and sensor network. It can be implemented with authentication for application and sensor network. Especially, authorization is also required for application. Because application have different privileges for specific resource(e.g., sensed data, etc).

The followings are the detailed components for access control.

- Application authentication/authorization
- Sensor network authentication

9.1.3. Data protection

This function is to ensure confidentiality for date stored in USN middleware. The data may be authentication-related data for application and sensor network, and important sensed data, and so on.

As a detailed component for data protection, encryption for data stored in middleware is needed.

9.1.4. Data traffic protection

This function is to protect sensitive data, which is like authentication data such as password and so on, exchanged between application and middleware and between sensor network and middleware.

The following are the detailed components for traffic protection.

- Data encryption between application and middleware
- Data encryption between sensor network and middleware

9.1.5. Channel protection

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

To protect an interface, the following detailed components are needed.

- Interface encryption between application and middleware
- Interface encryption between sensor network and middleware

9.2. USN middleware security model

Security functions described in sub-section 9.1 are operated as follows. Many of security functions are related to both of interface managers. Because most attacks targeting USN middleware are attempted at connection point.

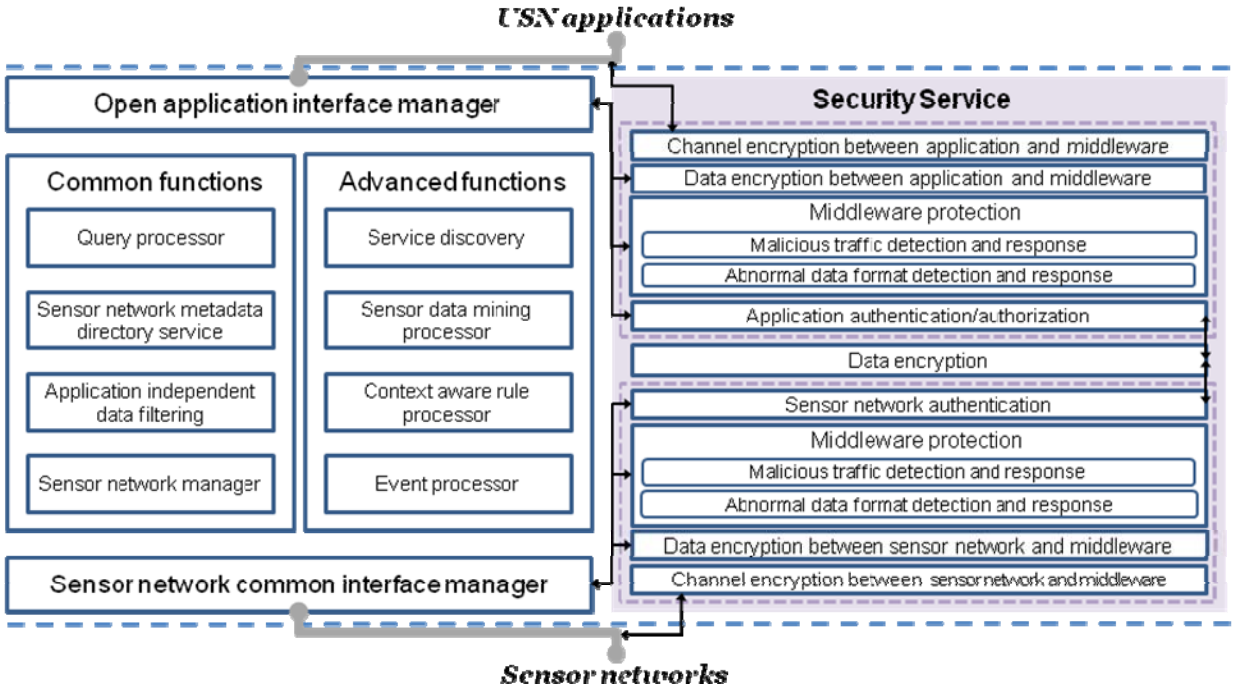

Figure 3 – Security model of USN middleware and its relationship

Channel encryption between application and middleware is applied on communication channel between USN application and open application interface manager. This function satisfies confidentiality for the traffic exchanged between USN application and middleware, and preventing from eavesdropping.

Data encryption between application and middleware is applied to sensitive data exchanged between USN application and open application interface manager. This function protects sensitive data via encryption. So, even malicious person achieves or hijacks traffic exchanged over communication channel, they cannot find original data. By doing this, data confidentiality is guaranteed.

Middleware protection is applied to open application interface manager and sensor network common interface manager. Procedure of middleware protection applied to open application interface manager is same with middleware protection function applied to sensor network common interface manager. But they check traffic or data transmitted from application and sensor network, based on different data format criteria. Because application data and sensor network data have different forms which fit one's application or sensor network.

Application authentication/authorization is applied to open application interface manager. This function is to avoid that untrusted applications access to middleware illegally. In addition, even though illegal access is happened, it is not able to change anything on middleware configuration and to access sensitive data stored at middleware database. For avoiding this situation, authorization function should be provided.

Data encryption is applied to database which stores sensitive data. Sensitive data contains data used for authentication and authorization. So this function is performed with application authentication/authorization function and sensor network authentication function.

Sensor network authentication is applied to sensor network common interface manager. This function is to avoid that untrusted sensor networks access to middleware illegally.

Data encryption between sensor network and middleware is applied to sensitive data exchanges between sensor network and sensor network common interface manager. This function protects

sensitive data via encryption. So, even malicious person achieves or hijacks traffic exchanged over communication channel, they cannot find original data. By doing this, data confidentiality is guaranteed.

Channel encryption between sensor network and middleware is applied to communication channel between sensor network and sensor network common interface manager. This function satisfies confidentiality for the traffic exchanged between sensor network and middleware, and preventing from eavesdropping.

9.3. Relationship between security threat and security function

The following table shows the relationship between security threats described in clause 2 and proposed security functions.

[Editor's Note] There was a discussion on the table showing relationship between security threats and security functions. It needs to be detailed to represent relationship between security threats and specific security mechanisms. Further contributions are required.

			Data traffic protection	Channel protection	Middleware protection	Access Control	Data protection
Device	Unauthorized MW access by App.					X	
	Unauthorized MW access					X	
	Unauthorized MW access by SN					X	
Data	Data transmission by App.	Sensitive data leakage	X				
		Abnormal traffic transmission			X		
		Malicious traffic transmission			X		
	Data transmission by SN	Sensitive data leakage	X				
		Abnormal traffic transmission			X		
		Malicious traffic transmission			X		
	Leakage of data stored in MW						X
Network	Eavesdropping communication APP.-MW			X			
	Eavesdropping communication SN-MW			X			

Table 1 – Relationship between security threats and security functions

Unauthorized application and sensor network access to USN middleware could be prevented with access control measures, such as authentication and authorization. Using this, USN middleware can protect itself from illegal accesses. There are three types of security threats relating to Data. Two of them are cases which data is transmitted by application and sensor network. In those cases, they have three kinds of data-related security threats which are sensitive data leakage, abnormal traffic transmission and malicious traffic transmission. Sensitive data leakage could be prevented with data traffic protection measures like an encryption for sensitive data. And abnormal traffic transmission and malicious traffic transmission could be handled with middleware protection means, such as abnormal data format detection and malicious traffic detection, etc. Security threat relating to data stored in USN middleware could be prevented with data protection function which has a data encryption function. Finally, eavesdropping on communication between application and USN middleware and communication between sensor network and USN middleware could be solved with channel protection which provides encryption for communication channel.

_____