Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14118
Date:	2009-10-26
Replaces:	
Document Type:	Liaison Organization Contribution
Document Title:	Liaison Statement from ITU-T SG 17 to ISO/IEC JTC 1/SC 6/WG 7 on the USN security
Document Source:	ITU-T SG 17
Project Number:	
Document Status:	For your information.
Action ID:	FYI
Due Date:	
No. of Pages:	33

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

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

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

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

COM 17 – LS 059 – E

English only

Original: English

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

Ref. : TD 0648

Source:	ITU-T SG 17 (Geneva, 16-25 September 2009)
Title:	USN security Recommendations

LIAISON STATEMENT

For action to:	
For comment to:	
For information to:	ISO/IEC JTC 1/SC 6/WG 7
Approval:	Agreed to at SG 17 meeting
Deadline:	

Contact:	Jonghyun Baek Rapporteur of Q.6/17	Tel: Fax: Email:	+82 2 405 5330 +82 2 405 5219 jhbaek@kisa.or.kr
Contact:	Yutaka Miyake Associate Rapporteur of Q.6/17	Tel: Fax: Email:	+81 49 278 7367 +81 49 278 7510 yu-miyake@kddi.com

ITU-T SG 17 thanks ISO/IEC JTC 1/SC6 /WG 7 for your interest in Question 6/17 activities on USN security.

We would like to provide information on the current activities on USN security Recommendations X.usnsec-2 (see Attachment 1) and X.usnsec-3 (see Attachment 2) as initial items for further collaboration.

We look forward for collaboration with ISO/IEC JTC 1/SC 6/WG 7. In addition, we would appreciate your comments or suggestions about these Recommendations.

Attachments: 2

1) X.usnsec-2, *USN middleware security guidelines* (TD 0578)
2) X.usnsec-3, *Secure routing mechanisms for wireless sensor network* (TD 0630)

____

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 Jae 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

~~***[Editor's note] There were some opinions that the draft Recommendation X.usnsec-2 needs to be specify the security threat to the Sensor Network dimension which cannot be addressed by existing methods and techniques from the PC or Internet world and provide specific solution to the software of the sensor nodes and to the wireless link in conjunction with the node hardware constraints and the apparent non-applicability of existing security approaches.***~~

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.

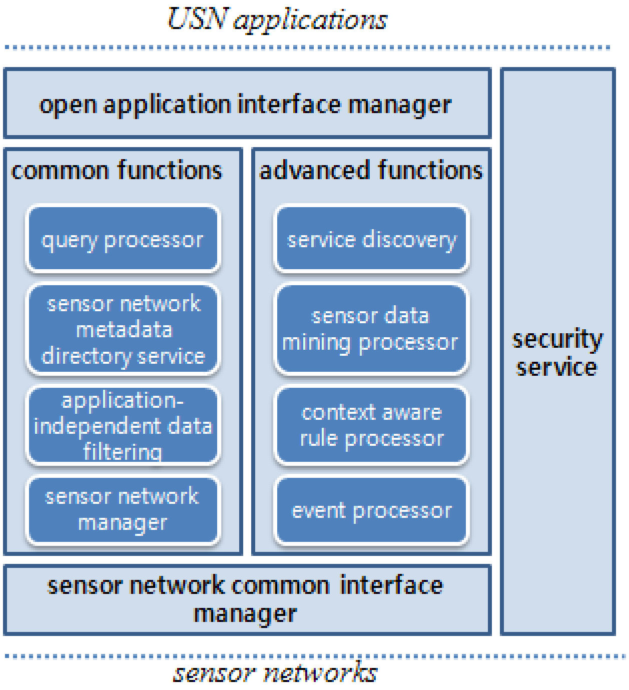

USN applications
open application interface manager
common functions
query processor
sensor network metadata directory service
application-independent data filtering
sensor network manager
advanced functions
service discovery
sensor data mining processor
context aware rule processor
event processor
sensor network common interface manager
security service
sensor networks

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.

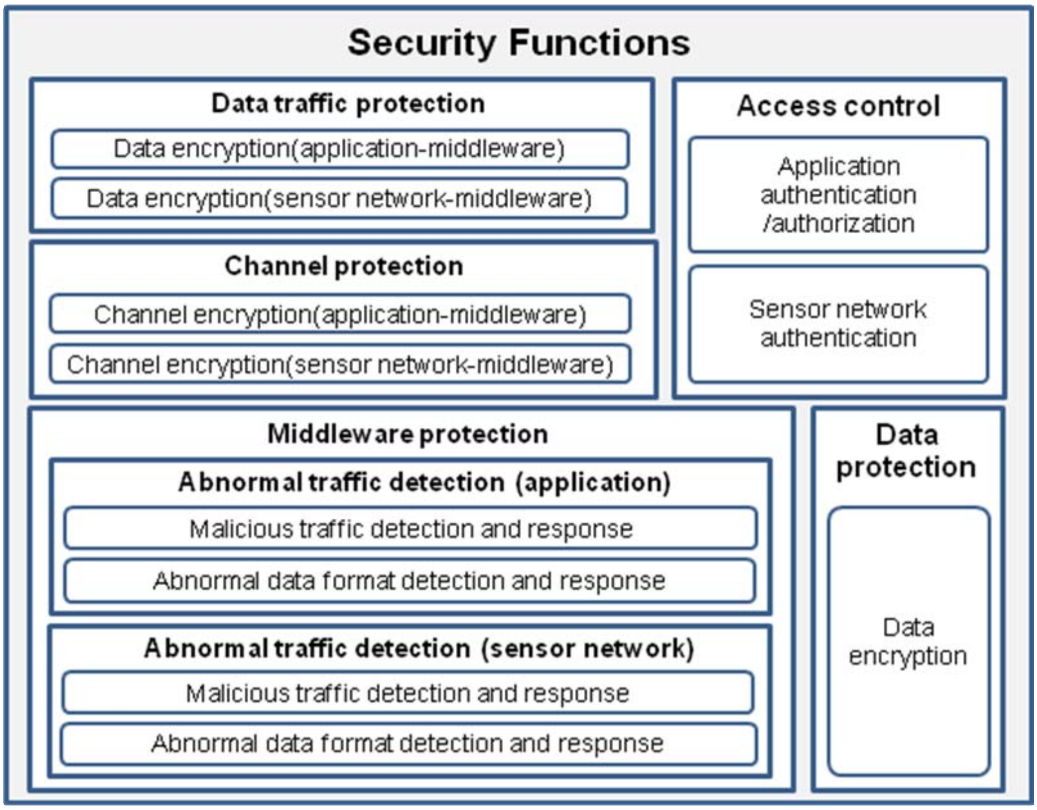
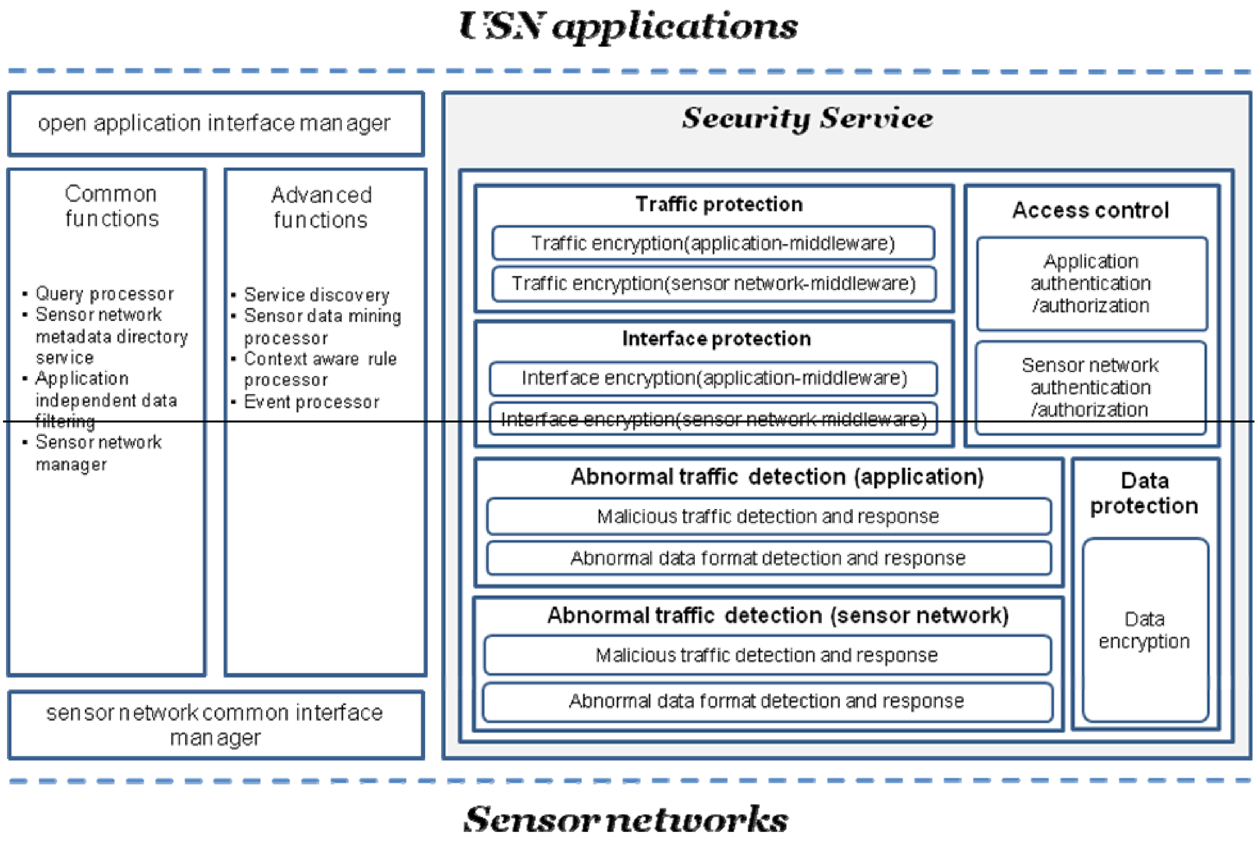

Security Functions
Data traffic protection
Data encryption(application-middleware)
Data encryption(sensor network-middleware)
Channel protection
Channel encryption(application-middleware)
Channel encryption(sensor network-middleware)
Access control
Application authentication /authorization
Sensor network authentication
Middleware protection
Abnormal traffic detection (application)
Malicious traffic detection and response
Abnormal data format detection and response
Abnormal traffic detection (sensor network)
Malicious traffic detection and response
Abnormal data format detection and response
Data protection
Data encryption

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.


USN applications
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
Security Service
Traffic protection
Traffic encryption(application-middleware)
Traffic encryption(sensor network-middleware)
Interface protection
Interface encryption(application-middleware)
Interface encryption(sensor network-middleware)
Access control
Application authentication /authorization
Sensor network authentication /authorization
Abnormal traffic detection (application)
Malicious traffic detection and response
Abnormal data format detection and response
Abnormal traffic detection (sensor network)
Malicious traffic detection and response
Abnormal data format detection and response
Data protection
Data encryption
Sensor networks

~~**Figure 2 – Security model of USN middleware**~~

~~1.1.~~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.

~~Middleware protection is to protect middleware against malicious traffic flowing into middleware or traffic that has an abnormal format.~~

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

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

~~1.2.~~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).

~~Access control is a means to protect middleware from unauthorized access. It can be implemented using an authentication and authorization mechanism.~~

The followings are the detailed components for access control.

- Application authentication/authorization
- Sensor network authentication~~/authorization~~

~~1.3.~~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.~~Data protection provides security for sensitive data, such as authentication information of applications and sensor networks stored in a middleware database. Even though the middleware system is compromised, it prevents a sensitive data leakage.~~

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

~~1.4.~~9.1.4. Data~~T~~ 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.~~Traffic protection provides a means to protect traffic from eavesdrop, traffic hijacking, traffic modification and so on. It can be implemented using an encryption.~~

The following are the detailed components for traffic protection.

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

~~1.5.~~9.1.5. ~~Interface~~ Channel protection

This function is to protect communication channel between application and middleware and between sensor network and middleware.~~Interface protection is to prevent interface against threats that can be happened by stealing a look the interface and taking abnormal activities. It can be implemented using an encryption for interface itself.~~

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.

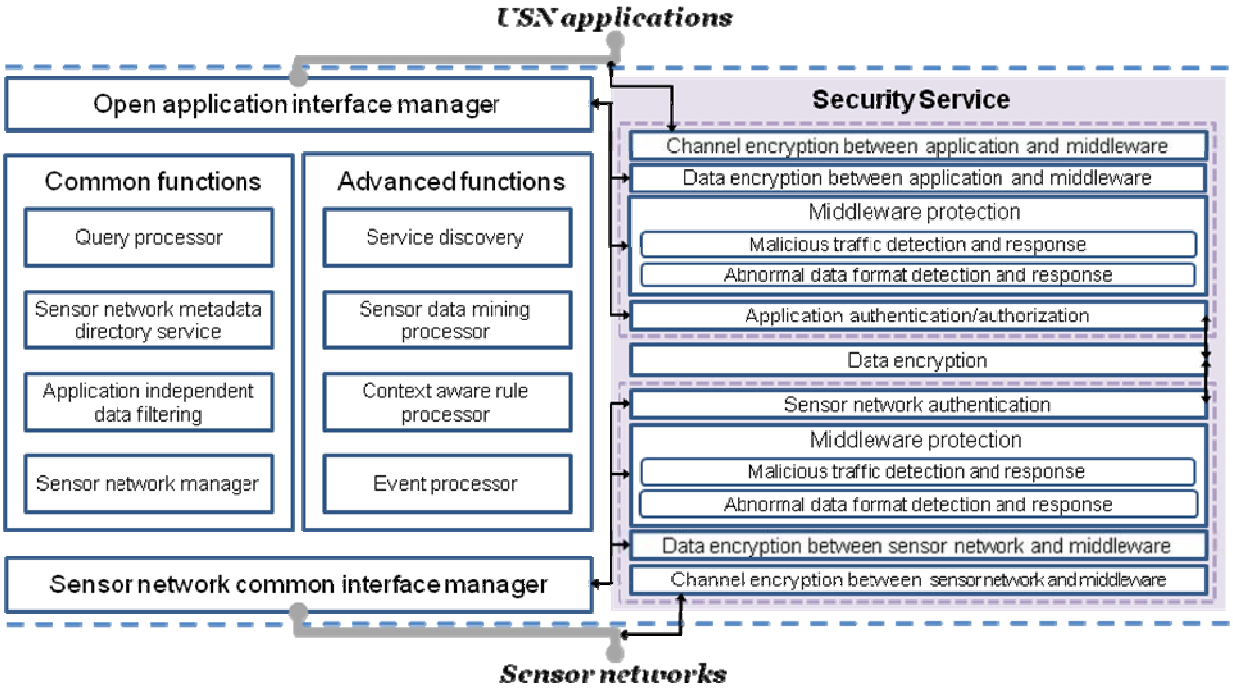

USN applications
Open application interface manager
Common functions
Query processor
Sensor network metadata directory service
Application independent data filtering
Sensor network manager
Advanced functions
Service discovery
Sensor data mining processor
Context aware rule processor
Event processor
Sensor network common interface manager
Security Service
Channel encryption between application and middleware
Data encryption between application and middleware
Middleware protection
Malicious traffic detection and response
Abnormal data format detection and response
Application authentication/authorization
Data encryption
Sensor network authentication
Middleware protection
Malicious traffic detection and response
Abnormal data format detection and response
Data encryption between sensor network and middleware
Channel encryption between sensor network and middleware
Sensor networks

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.

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

STUDY GROUP 17

TD 0630

English only

Original: English

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

TEMPORARY DOCUMENT

Source: Editors

Title: Draft Recommendation X.usnsec-3: Secure routing mechanisms for wireless sensor network

This is a revised text of draft Recommendation X.usnsec-3 based on C117, agreed on September Q.6/SG17 meeting. The changed parts are as follows:

- Change the sentence in clause 9 from "~ against attacks such as spoofed routing information, selective forwarding attack, Sybil attack, and so on" to "~ against attacks described in clause 8".
- Add several abbreviations into Clause 4(Abbreviations and acronyms) and edit several words in this draft recommendation.
- Change the titles of 9.1.5 and 9.2.5 to accord with other requirements in clause 9.1, and countermeasures in clause 9.2, respectively.
- Modify figures' captions in clause 9.2 since the figure related to each security requirement is one example for operating each countermeasure.

Contact:	Eunyoung Choi KISA Korea	Tel: +82-2-405-4706 Fax: +82-2-405-5319 Email: bluecey@kisa.or.kr
Contact:	Howon Kim Pusan University Korea (Republic of)	Tel: +82-51-510-1010 Fax: +82-51-517-2431 Email: howonkim@pusan.ac.kr
Contact:	Hyangjin Lee KISA Korea (Republic of)	Tel: +82-2-405-5446 Fax: +82-2-405-5219 Email: jiinii@kisa.or.kr
Contact:	Hyuncheol Jung KISA Korea (Republic of)	Tel: +82-2-405-5350 Fax: +82-2-405-5219 Email: hcjung@kisa.or.kr

Draft text of X.usnsec-3: Secure routing mechanisms for wireless sensor network

(September, 2009)

Summary

This Recommendation provides secure routing mechanisms for wireless sensor network in ubiquitous sensor network. It introduces general network topologies and routing protocols in ubiquitous sensor network. It describes security threats of wireless sensor network and provides countermeasures for secure routing in wireless sensor network.

Table of Contents

1 Scope

This recommendation provides secure routing mechanisms for wireless sensor network in ubiquitous sensor network. First, this recommendation reviews the architecture of USN. It introduces general network topologies and routing protocols in ubiquitous sensor network. It describes security threats of wireless sensor network and provides countermeasures for secure routing in wireless sensor network.

2 References

[TBD]

3 Terms and Definitions

This recommendation defines the following terms:

3.1 Terms defined elsewhere

The terms used herein shall be defined as follows.

3.1.1 **Authentication [ITU-T X.800]** : See data origin authentication and peer-entity authentication.

3.1.2 **Actuator[b-ISO/IEC SGSN N049] :** a device that changes a measureable physical property in response to an electrical signal.

3.1.3 **Confidentiality [ITU-T X.800]** : The property that information is not made available or disclosed to unauthorized entity.

3.1.4 **Data Integrity [ITU-T X.800]** : The property that data has not been altered or destroyed in an authorized manner.

3.1.5 **Key [ITU-T X.800]** : A sequence of symbols that controls the operation of encipherment and decipherment.

3.1.6 **Sensor[**b-ISO/IEC SGSN N049**]**: a device that generates an electrical signal which represents a measureable physical property.

3.1.7 **Sensor network** [b-ISO/IEC SGSN N049] **:** a collection of two a collection of two or more sensor-network nodes and one or more sensor-network controllers interacting with each other in a single network.

3.1.8 **Sensor-network controller**[b-ISO/IEC SGSN N049] **:** a processing system that can receive sensor data from sensor-network nodes, send electrical signals to actuators in sensor-network nodes, and send control signals to sensor-network nodes.

3.1.9 **Sensor-network node** [b-ISO/IEC SGSN N049]:a device that contains at least one sensor and zero or more actuators, with the capability of 1) using internal sensor data to control any actuators present, or 2) sending sensor data and receiving actuator commands over the network.

3.1.10 **Threat[ITU-T X.800] :** A potential violation of security.

3.1.11 **Ubiquitous Sensor Network(USN)** [X.usnsec-1] **:** a conceptual structured network which deliver sensed information and knowledge services to anyone at anywhere and anytime where the information and knowledge is developed by using context awareness. Or a sensor network which either covers a wide geographical area or supports several different applications, or both.

3.2 Terms defined in this recommendation

3.2.1 Wireless Sensor Network(WSN): In the sensor networking domain of USN , it is composed of a base station and a large number of the sensor nodes with the wireless transmission capability except for wire-line sensor networks.

3.2.2 Routing : It refers to a process to establish a communication association between the sensor nodes. Routing involves determining the path and transporting information through the network.

3.2.3 Topology : It refers to the physical and logical arrangement of the elements of sensor network. In WSN, it is represented as a collection of sensor nodes and gateways, some of which are connected by wireless links.

3.2.4 Ad hoc On-Demand Distance Vector (AODV): It is an on-demand routing protocol that discovers routes on an “as-needed” basis for wireless ad-hoc network and wireless sensor network. AODV builds routes using a route request(RREQ) and a route reply(RREP) query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backward pointers to the source node in the route tables.

3.3

[TBD**]**

4 Abbreviations and acronyms

This recommendation uses the following abbreviations:

USN-Ubiquitous Sensor Network

WSN-Wireless Sensor Network

SPIN - Sensor Protocols for Information via Negotiation

MAC - Message Authentication Code

DoS - Denial of Service

ID - Identity

5 Conventions

None

6 Overview of USN architecture

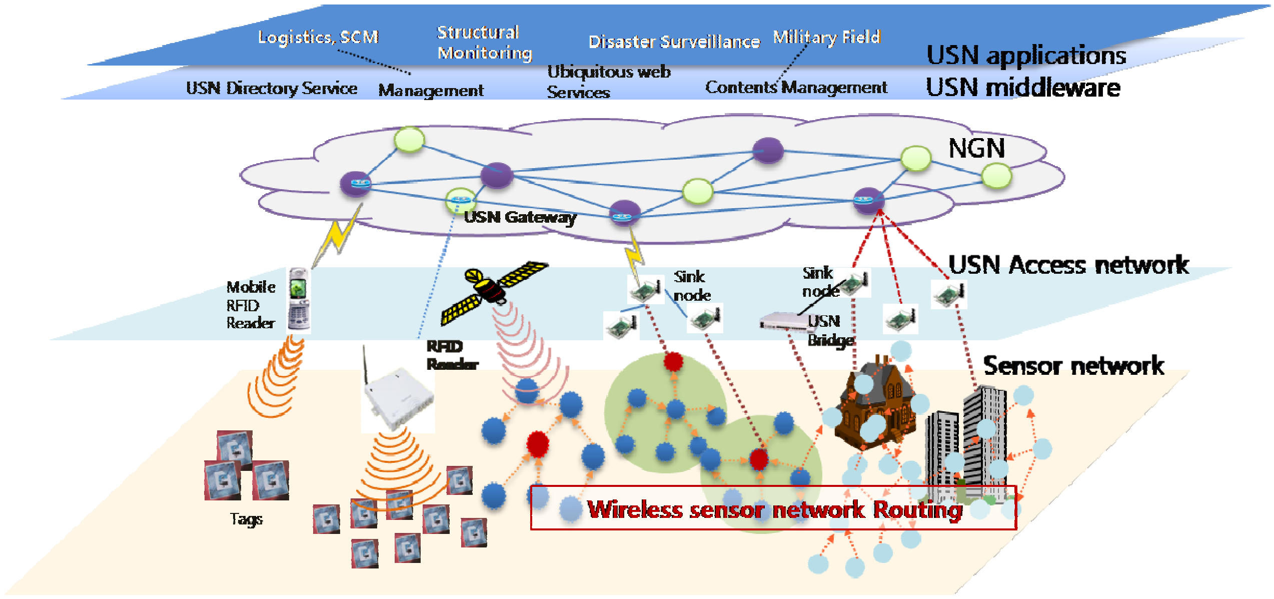


Figure 1 – Overall structure of USN

Figure 1 describes the overall structure of the USN. It is composed of five layers; Sensor Networking, USN Access Networking, Network Infrastructure, USN Middleware and USN Applications.

The sensor network part of the USN regarded that it consists of wire-line and wireless sensor networks. It can either be based on Internet Protocol (IP) or non-IP-based protocols. The 6LoWPAN (IPv6 based Low-power Wireless Personal Area Network) standard can be used to realize the IP sensor network. And for the non-IP platform, ZigBee, which is an implementation of the IEEE 802.15.4 standard for wireless personal area networks (WPAN), provides such a suite of communication protocols.

This recommendation deals with wireless sensor network of the sensor network and will assume the main components of WSN ; application server which communicate with sink node~~, sink node~~, called a base station, which interface sensor network and application server, and a collection of sensor nodes using the wireless communication to communicate with each other. The sink may communicate with application server via internet.

7 General network topologies and routing protocols for WSN

7.1 General network topologies in WSN

The WSN nodes are typically organized in one of three types of network topologies: star, tree and mesh topology. Figure 2 shows these three types of network topologies. In a star topology, each node is directly connected to a central node such as a gateway node. The nodes can communicate with all others by transmitting to, and receiving from, the central node. In a cluster tree network, each node connects to a node higher in the tree and then to the gateway, and data is routed from the leaf node to the gateway via several intermediate nodes, which compose the tree topology. In the tree topology network, a hierarchical routing scheme can be implemented. Finally, in mesh topology network, there are at least two nodes with two or more paths between them. This type of topology allows for most transmissions to be distributed and reliable due to its multiple paths even though it causes hardness and expensiveness to maintain the redundant connections between nodes.

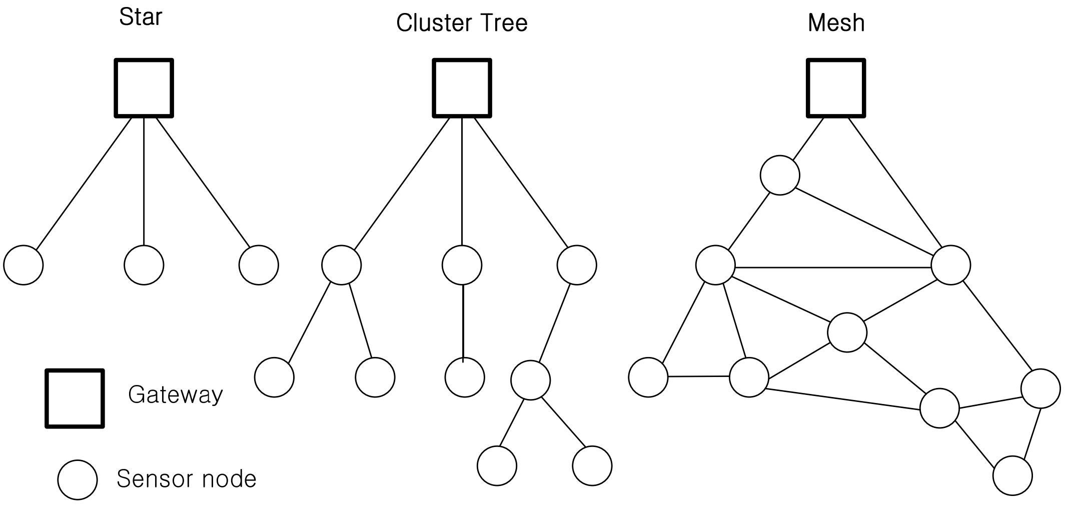


Figure 2 – General three network topologies for WSN

7.2 General routing protocols for WSN

Many mechanisms have been proposed for the routing for sensor networks. These routing mechanisms have taken into consideration the inherent features of sensor networks along with the application and topological requirements. The task of finding and maintaining routes in sensor networks with considering viewpoints of the energy consumption, the effectiveness of routing, the reliability of data and security is nontrivial one. Almost all of the routing mechanisms can be divided into flat-based routing, hierarchical-based routing, and location-based routing depending on the network structure.

In flat-based routing, all nodes are typically assigned equal roles or functionality. In hierarchical-based routing, however, nodes will play different roles in the network. In location-based routing, sensor nodes' positions are exploited to route data in the network. A routing protocol is considered adaptive if certain system parameters can be controlled in order to adapt to the current network conditions and available energy levels.

In the flat-based routing mechanism, it assume each node typically plays the same role and sensor nodes collaborate together to perform the sensing task. This routing mechanism basically assumes the densely deployed environment. Due to the large number of such nodes, it is not feasible to assign a global identifier to each node. This consideration has led to data centric routing, where the base station sends queries to certain regions and waits for data from the sensors located in the selected regions. The data centric routing such as SPIN and directed diffusion are typical examples for these routing mechanisms.

Hierarchical or cluster-based routing is usually used to perform energy-efficient routing in sensor networks. In a hierarchical architecture, higher energy nodes can be used to process and send the information while low energy nodes can be used to perform the sensing in the proximity of the target. This means that creation of clusters and assigning special tasks to cluster heads can greatly contribute to overall system scalability, lifetime, and energy efficiency.

In location based routing protocols, sensor nodes are addressed by means of their locations. The distance between neighbour nodes can be estimated on the basis of incoming signal strengths. Relative coordinates of neighbour nodes can be obtained by exchanging such information between neighbours. The location of nodes may be available by using GPS (Global Positioning System) or a proper location finding system such as RTLS(Real Time Locating Systems).

8 Security threats of WSN Routing

The security threats in wireless sensor network routing exist in the communication layers such as a physical layer, data-link layer, network layer, transport layer and application layer. This recommedation is mainly considering in the network layer, which is closely related to the routing operation. Also, since the routing is closely related to data link layer which is the underlying layer of a network layer, this recommendation considers security threats in data link layer and network layer. Others layers are not considered in this recommendation.

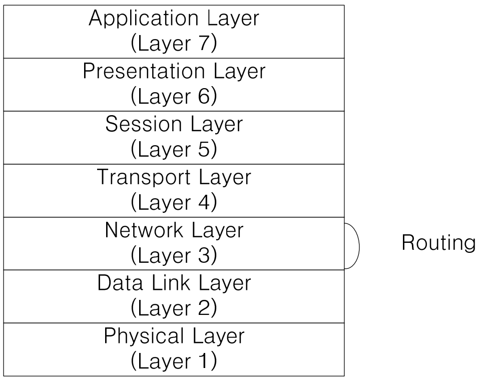

Application Layer (Layer 7)
Presentation Layer (Layer 6)
Session Layer (Layer 5)
Transport Layer (Layer 4)
Network Layer (Layer 3)
Data Link Layer (Layer 2)
Physical Layer (Layer 1)
Routing

Figure 3 – 7-layer OSI reference model

The radio jamming attack and tampering is an example of the physical layer attack. And the passive eavesdropping, link layer jamming attack, MAC spoofing attack, replay attack, collision attack, exhaustion attack, and unfairness attack is a kind of data link layer attacks.

The attacks on the network layer can be divided into control plane attacks and data plane attacks. Control plane attacks generally target the routing functionality of the network layer. The objective of the attacker is to make routes unavailable or force the network to choose sub-optimum routes. On the other hand, the data plane attacks affect the packet forwarding functionality of the network. The objective of the attacker is to cause the denial of service for the legitimate user by making user data undeliverable or injecting malicious data into the network.

In control plane attacks, there are several attacks such as a rushing attack, a wormhole attack, a sink-hole attack, a sybil attack. The eavesdropping attack is an example for data plane attack.

This recommedation deals with the attacks on network layer from the viewpoint of routing operation. The attacks on the network layer are classified into the following active three types of attacks on each steps that the routing scheme needs: (1) attacks on route discovery process, (2) attacks on route selection process, and (3) attacks after establishing routing paths.

8.1 Attacks on Route Discovery Process

For this type of attack, a malicious node attempts to prevent other legitimate nodes from establishing routing paths by sending fake routing information. To achieve the goal of this attack, for an on-demand routing protocol such as AODV, a malicious node can reply a non-existing route to the source or alter the addresses in an RREQ(Route Request) packet to spoof the destination. It can also modify an RREP packet to cause invalid route to the source. Moreover, the malicious node can send excessive route request messages to exhaust the network bandwidth. Examples contain a fake routing information, RREQ flood attack, and so on.

8.2 Attacks on Route Selection Process

The route selection attack attempts to increase the chance that malicious nodes are selected by other legitimate nodes as part of their routes. After establishing a route through itself, the attacker can overhear, modify or does other harmful actions on transmitted messages. The hello flood and sybil attack can be classified to this kind of attack. The sinkhole and wormhole attack use this kind of attack to complete their attacks. In hello flood attack, the malicious node broadcasts its hello message with high radio transmission power to cover a large range of network. Then the receiving nodes consider the malicious node as a neighbour node and then establish connection to the malicious node. It destroys the normal route selection mechanism based on the power strength of radio signal. In sybil attack, a malicious node spoofs its neighbour nodes by disguising itself as multiple different nodes by advertising multiple identities to its neighbours.

The objective of a sinkhole attack is to attract all neighbour nodes of the attacker to establish routes through the attacker, all traffic from a particular area will flow through the attacker, thus creating a sinkhole with the attacker. Sinkhole attacks typically work by making a malicious node look especially attractive to surrounding nodes with respect to the routing mechanism. For example, in the case that the neighbours are selected by the radio signal strength, the malicious node advertises high radio transmission power to attract surrounding nodes to select itself as neighbour nodes.

In wormhole attack, two distant malicious nodes utilize an out-of-bound channel to communicating the collected messages from one side (i.e., attacked region) to the other side (i.e., the gateway). To establish such a tunnelling channel, the malicious node on the side of an attacked region spoofs their neighbours to be a central node and the malicious node on the other side spoofs the gateway to be an neighbour node itself.

8.3 Attacks after Establishing Routing Paths

Once a source node establishes a route through a malicious node, the malicious node can unscrupulously drop the packets from the source or modify the contents of packets if proper countermeasure is not applied. Blackhole attack and selective forwarding attack can be classified to this kind of attack. Multi-hop communications must rely on the cooperation of participating nodes to forward the received messages. In a blackhole attack, malicious nodes violate such an assumption by dropping all received messages from the source to prevent these messages from being propagated any further. In selective forwarding attack, malicious node can refuse to forward certain packets and simply drop them, ensuring that they are not propagated any further. The sinkhole and wormhole attack can also be categorized into the attacks after establish routing paths.

9 Secure routing mechanisms for WSN Routing

This recommendation describes security requirements to establish secure routing against attacks ~~such as spoofed routing information, selective forwarding attack, Sybil attack, and so on~~ described in clause 8. It also proposes the countermeasures satisfying the security requirements.

9.1 Security requirements for wireless sensor network routing

Though the security technology of the routing mechanism in network layer of sensor networks are strongly dependent on the type and characteristics of the routing mechanism, there are common security requirements for secure and trustable routing.

In the route discovery process, the legitimate node should find the routing path based on the legitimate routing information. A malicious node can prevent other legitimate nodes from establishing routing paths by sending fake routing information. That is, the malicious node attacks the discovery process of a legitimate node. Moreover, a malicious node can send excessive route request messages to exhaust the network bandwidth. The former is to provide fake information to spoof the route discovery process, while the latter is to overly use the route discovery process. Both of them attempt to cause denial of service (DoS). To make a legitimate node can do the proper route discovery process, fake routing information from malicious node should be prevented. To do this, the authenticity of the routing information that is from a node should be provided.

In the route selection process, the malicious nodes can be selected by other legitimate nodes as part of their routes. After establishing a route through itself, the malicious node can overhear the transmitted messages or disrupt the correct routing of the wireless sensor network. To prevent the malicious nodes from being selected as a legitimate routing node, the other legitimate nodes should not be deceived by routing information from malicious node. For example, in hello flood attack, the malicious node sends its hello message which covers a large range of sensor. And the receiving nodes will be convinced that the malicious node as their neighbouring node.

After a routing path established, the malicious node can drop, eavesdrop, modify and other malicious behaviors anything it wants. In this stage, conventional security requirements such as confidentiality, integrity, authentication should be provided and proper malicious behavior detection scheme should be provided to detect the wormhole and sinkhole attack.

To prevent from security threats, wireless sensor netwrok must satisfy the security requirements as follow.

9.1.1 Confidentiality

A wireless sensor network is composed of a collection of wireless node. A node can communicate with other nodes within its limited transmission ran~~a~~ge. Thus, to facilitate communication between two nodes without a direct communication link, routing protocols have to be developed to support muti-hop communcation. To assure a source node of finding a route to its destination, most routing protocols try to invite all available nodes to participate in the routing mechanism. This provides a lot of opportunities for adversarys to establish invalide route by modifying route information or dropping route information delivered to other nodes. The sensor network can securely be maintained according as the routing protocols provide the confidentiality for routing information. However, since routing information are frequently updated according to status of surrounding neighbours, it may be diffcult to provide the confidentiality for routing information.

Also, a malicious adversary can attack legitimate nodes after establishing routing paths to eavesdrop and modify the transmitted messages between nodes. The communication data should not be leaked to malicious nodes. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess. The security requirement of confidentiality can be satisfied if sensor node applys the standard encryption algorithm such as AES to the payload or a proper part of a communication message which are routed on sensor networks.

9.1.2 Integrity

To detect if Route Reply (RREP) packets that are transferred for establishing a route from a source to destination is modified or not, routing protocols must provide integrity of the routing information transmitted between nodes.

The integrity means that the assurance of data received are exactly as sent by an authorized sensor node. That is, the communication data was not modified, inserted, deleted by malicious node. The integrity can be provided by applying a mode of operation of standard encryption algorithm and hash function to communication messages (command and sensed data) properly.

9.1.3 Authentication

Authentiation is necessary for many kinds of tasks in ubiquitous sensor network applications. For example, when a gateway injects a control command to a sensor node, the gateway should identify itself that it is an authorized gateway to sensor nodes and the control command is a legal command. That is, the gateway should provide appropriate proof of identity to the sensor nodes. Also, only verified sensor node can join to existing sensor network. The data authentication allows a receiver to verify that the data really was sent by the claimed sensor.

9.1.4 Data Freshness

Data freshness ensures that no old messages have been replayed. This requirement is important when shared-key encryption techniques are employed in sensor networks for providing the confidentiality on the communication messages among the sensor nodes. Typically shared keys to sen~~o~~sor nodes need to be changed over time. However, when the keys are changed, the malicious node can capture the key and replayed in future. For providing the anti-replay attack, a nonce, timestamps, or more elaborate solutions required to ensure the data freshness for sensor networks.

9.1.5 Intrusion detection functionality

Although wireless sensor networks satisfy security requirements such as confidentiality, integrity, authentication, the sensor networks may be vulnerable to several attacks such as wormhole and hello flood among routing attacks. For example, wormhole attack is hard to detect because the attacks do not inject abnormal volumes of traffic into the network. To enhance security related to wireless sensor network routing, an intrusion detection system or additional detection function for specific routing attacks will be provided in wireless sensor network.

[TBD]

9.2 Countermeasures for secure wireless sensor network routing

To avoid attacks on sensor networks, basic security requirements for USN should be satisfied. For example, to provide the confidentiality on the data communication between sensor nodes, wireless sensor nodes can use the link layer encryption with proper cryptographic algorithms such as AES. But most attacks such as sybil attack, sinkhole and wormhole attacks are not countered by encryption. In the followings, this recommendation provides countermeasures especially on the possible threats on wireless sensor network routing.

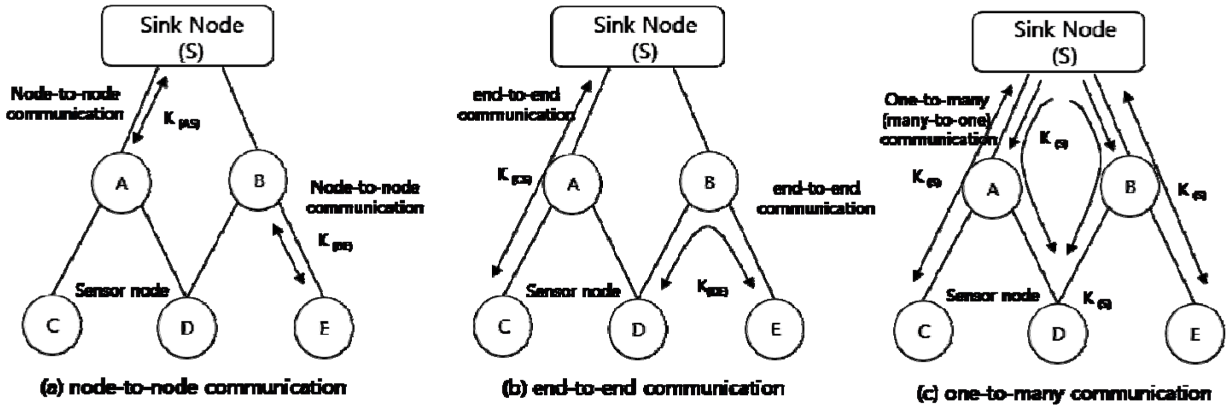
9.2.1 Confidentiality

The encryption can provide the node-to-node or end-to-end confidentiality between sensor nodes and a sink node(or base station)~~gateway~~. If an intermediate node wants to access the message body, then it can access the information with decrypting the encrypted packet body with proper secret information. The nodes which have no secre~~re~~t information can not access the encrypted packet body.

In wireless sensor network, the packet communication pattern of routing information can be categorized into three types such as node-to-node communication, end-to-end communication and one-to-many communication pattern.

Cosidering wireless sensor network, there are many methods to establish and manage keys which are shared between them : a single network-wide key which is preloaded into all the nodes, a pairwise key establishement method that each node shares a unique key with every other node, key distribution method that several keys are preloaded into each node and sensor nodes probablistically shares some key, and so on. Accoriding to communication parttern, secret keys are established between sensor nodes : Keys used in end-to-end or node-to-node communciation are induced by a secret key for one-to-many communication.

The node-to-node communication is occurred between neighbor nodes and the message body is encrypted/decrypted with the secrete information which are securely shared by two neighbor nodes. In Figure 4 (a), the secret information $K_{(AS)}$ is shared between communication counterparts, that is, the node and a sink node. Since the the end-to-end communication requires multihop communication to reach its destination, the secret information ($K_{(CS)}$ and $K_{(DE)}$ in Figure 4 (b) should be shared exclusively between the source and destination node. In one-to-many (or many-to-one) communication, the communicating correspondents should share the secret information ($K_{(S)}$ in Figure 4(c)) to correctly encrypt/decrypt the confidential routing information.



(a) node-to-node communication

(b) end-to-end communication

(c) one-to-many communication

Figure 4 – Example of ~~T~~three types of communication patterns

The routing packets of sensor networks usually have two types of packet format. One is the packet for data (information) transmission and the other is a control packet such as sending command or receiving acknowledgement. When the communicating nodes have the secret key information properly, the node can send and receive data and commands information confidentially by using standard encryption algorithm such as AES.

9.2.2 Integrity

The modified data payload and falsified control packet in routing information will spoil proper operations of the sensor network application. Consider an example of surveillance application. When a critical situation (intrusion event) occurs, the sensor node detects the event and then sends the information to a sink node. The malicious node easily falsifies the transferred event and then the surveillance system cannot operate properly. To detect the illegal modification of the routing information, sensor nodes can use the MAC(Message Authentication Code) to the data payload or control information. Similar to the way providing confidentiality into wireless sensor network, to compute MAC, sensor nodes newly share a secret key or use the shared key for the encryption.

In figure 5, a sink node shares keys $K_{(AS)}$ and $K_{(BS)}$ with nodes A and B, which may be pre-loaded on nodes deployment phase. Using key distribution protocol underlying two keys, two nodes can share a new key $K_{(AB)}$ and then can be used for MAC containing message(Msg).

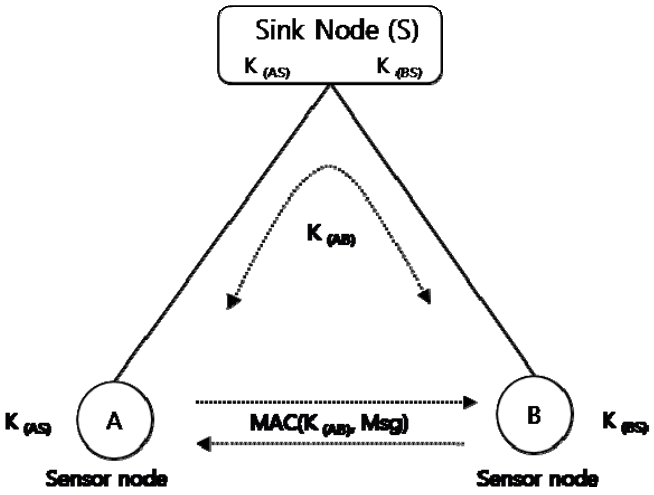


Figure 5– Example of ~~C~~communication way for integrity, authentication

<TBD>

9.2.3 Authentication

When sensor nodes use the authentication on the routing information, the fake routing information attack and RREQ (Route Request) flood attacks can be defensed.

In case of fake routing information attack, a malicious node is to provide fake routing information during its route discovery phase. It makes legitimate nodes esatablish invalid routes in sensor network or forward all network traffic to a specific node. Thus, sensed data of legitimate nodes cannot be transmitted to a sinknode or base station.

In case of RREQ flood attack, a malicious node can also reply a non-exsitng route to the source or alter the address in an RREQ packet to spoof the destination. To settle those attacks, nodes in the nework share keys to authentication their data packets and routing control messages such as RREQ and RREP. Thus, legitimate nodes can securely transmitted legitimate nodes in the network because the adversaries never modify or delete routing information transmitted between nodes ; they does not have the keys to authenticate its packets.

Similary, a hello flooding attack broadcasts localized hello messages to spoof themselves to their neighbors so that malicious nodes are selected by other legitimate nodes as part of their routes. To settle those threats, legitimate nodes should provide authenticity of the routing information using Message Authentication code (MAC) function based on shared keys between them.

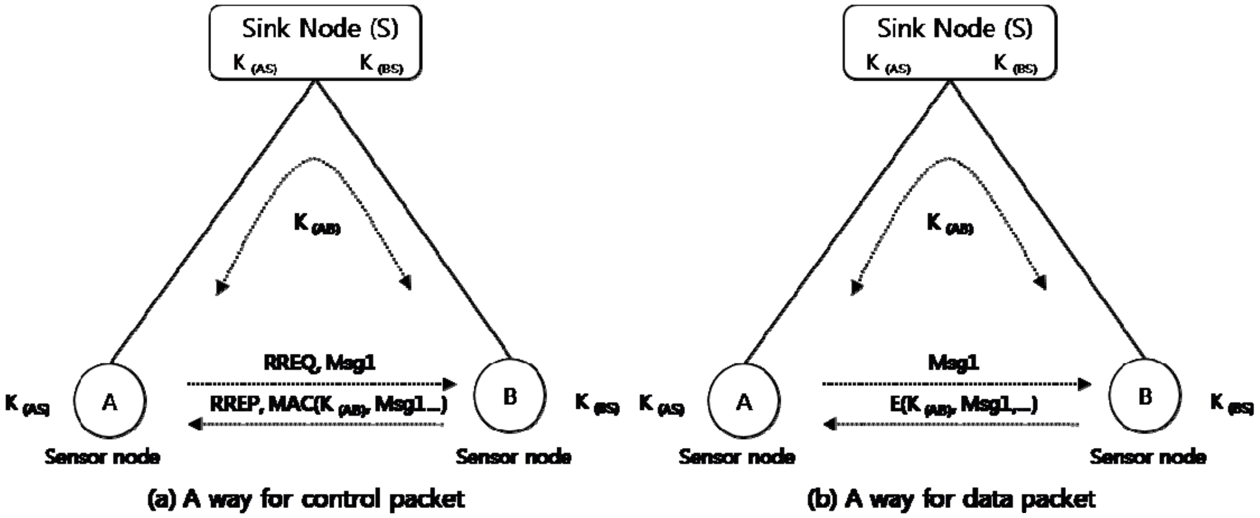
In case of the sybil attack, every nodes share a unique symmetric key with a trusted sink node , which may be applied cluster tree topologies and hierarchical(or cluster)-based routing mechanism. Two legitimate nodes can use a symmetric encryption verify each other’s identity and establish a new shared key using a pre-shared key and nonces. The new shared key is used for authenticated link between them. Thus they are assured of the authenticity of neighobrings identity.

In figure 5, if a message(Msg) is an identity (ID) of a node, wireless sensor network can provide authentication using MAC funcation.

<TBD>

9.2.4 Data Freshness

Data freshness is considered as an important problem when shared-key encryption techniques are employed in sensor networks for providing the confientiality on the communication messages. Thus, data freshness ensures that no old messages have been replayed. To settle this threat in wireless sensor network, sensor nodes can use a nonce, time-related counter, timestamps. For example, like figure 6 (a), sensor nodes shares a key $K_{(AB)}$ and a node request a RREQ packet to neighboring node with a nonce(Msg1), and then, a receiving node generates a MAC using the nonce ,Msg1 and sends RREP packet with the MAC. To ensure the freshness related to sensed data transmitted between nodes, the sensor node A sends a nonce, time-related counter and timestamps that is denoted as Msg1 like figure 6(b). If a sensor node use an encryption function providing the confidentiality. nodes encrypts the sensed data using the Msg1, and sends back encrypted data E($K_{(AB)}$, Msg1,..).



(a) A way for control packet

(b) A way for data packet

Figure 6– Example of communication way for data freshness

<TBD>

9.2.5 Intrusion detection functionality

Though prevention is safer than relying on detection, the preventive approaches are useless to some routing attacks such as a wormhole attack and selective forwarding. Therefore, proper detection and recovery mechanism should be provided to defeat some kinds of attacks.

Detection involves monitoring the real-time behavior of the sensor nodes. Once malicious behavior is detected, one can resort to recovery techniques to eliminate the malicious node and to restore correct routing functionality. The detection approach can guard against potentially unknown attacks, as long as we can distinguish anomalous behavior and correctly attribute it to a misbehaving entity. However, detecting the adversary node among the sensor nodes are known to be difficult.

The detection based security mechanisms at the routing level primarily address the issues of malicious and misbehaving nodes that are at the heart of almost all the attacks at the routing level.

This security mechanism identifies the anomalies in the routing messages to detect the routing attacks like wormhole and sinkhole attack. The detection based security mechanism consists of three functions, first, the detection mechanism collects data by monitoring some type of events. The second functional part of the detection mechanism is an analysis engine that processes the collected data. This part has special function that it can detect unusual or malicious signs in the data.The third functional part of the detection mechanism is a response, which is typically an alert to system administrators(or monitoring center). The system administrator (or monitoring center) is responsible for follow-up investigatoin of an event after receiving an alert signal.

9.2.5.1 Collection of the anomaly

The first part of the detection based security mechanism for routing attack is to collect the anomaly. The collection can be done by a centralized system or distributed monitoring sensor nodes. The monitoring center in a sensor network can collect the anomaly on the sensor networks by collecting information such as routing patterns, signal strengths, etc. Also the anomaly collection function can be implemented to each sensor node, and they can send the collected information to the monitoring center.

9.2.5.2 Analysis

The second part of the detection based security mechanism for routing attack is an analysis engine. Analysis can be done manually by monitoring the collected data, but automated analysis is much efficient. To make an automated analysis, the analysis engine has an intelligence to differentiate the normal behavior of routing and abnormal behavior of the routing mechanism.

Currently, there are two basic approaches to analysis: misuse detection and anomaly detection.
Misuse detection is also called signature-based detection because the idea is to represent every attack by a signature (pattern or rule of behavior). It is essentially a problem of matching the observed attack patterns to signatures. If a matching signature is found, that attack is detected.
A common implementation of misuse detection is an expert system. An expert system consists of a knowledge base containing descriptions of routing attack behavior based on past experiences and rules that allow matching of packets against the knowledge base. These rules are often structured as “if-then-else” statement.

9.2.5.3 Response

The third functional part of the detection based security mechanism for routing attack is the response. Detection of an intrusion must lead to some type of output.

The responses can be passive or active. The passive response is to log the abnormal behavior information and raise an alert signal to system administrators (or monitoring center). In this passive response, the highly trained system administrators are responsible for the judgement and reactions based on the alert signal. Active response is also possible. It attempts to limit the damage of an attack or stop the attack in progress. Damage can be mitigated by protecting the attack in progress or the specific target of the attack.

<TBD>