ISO/IEC JTC 1/WG 7
Working Group on Sensor Networks

Document Number:	N103
Date:	2010-10-08
Replace:	
Document Type:	Liaison Organization Contribution
Document Title:	Liaison Statement from JTC 1/SC 6 to JTC 1/WG 7
Document Source:	JTC 1/SC 6
Document Status:	For your information.
Action ID:	FYI
Due Date:	
No. of Pages:	43

ISO/IEC JTC 1/WG 7 Convenor:

Dr. Yongjin Kim, Modacom Co., Ltd (Email: cap@modacom.co.kr)

ISO/IEC JTC 1/WG 7 Secretariat:

Ms. Jooran Lee, Korean Standards Association (Email: jooran@kisi.or.kr)

Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14453
Date:	2010-10-06
Replaces:	
Document Type:	Outgoing Liaison Statement
Document Title:	Liaison statement from JTC 1/SC 6/WG 7 to JTC 1/WG 7 for Collaboration on Sensor Networks
Document Source:	SC 6/WG 7 London meeting
Project Number:	
Document Status:	As per the SC 6 London resolution 6.7.10, this document is sent to JTC 1/WG 7.
Action ID:	FYI
Due Date:	
No. of Pages:	2
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	

Title: Liaison statement to JTC 1/WG 7 for Collaboration on Sensor Networks

Source: JTC 1/SC 6/WG 7 Meeting (27 September – 1 October 2010)

Contact: Shin-Gak Kang (Convenor of SC 6/WG 7)

For: Information

Deadline: None

JTC 1/SC 6/WG 7 thanks JTC 1/WG 7 for sending its liaison statements N024(JTC 1/WG 7) and N079(JTC 1/WG 7) for close collaboration on Sensor Networks related issues.
SC 6/WG 7 noted the current status and achievements on Sensor Networks at the recent meetings of JTC 1/WG 7.

SC 6/WG 7 would like to be kept informed of progress on standardization works in JTC 1/WG 7 on sensor networks.

Regarding the ISO/IEC 29180, Security framework for sensor networks which is a common text standard with ITU-T are in the FCD ballot processing after collaboration meeting with ITU-T Q.6/17 in April 2010. The FCD ballot resolution and further progression will be taken place at the next collaborative meeting with ITU-T Q.6/17 in December 2010 in Geneva. Also, it is planned to Consent in ITU-T SG 17 meeting in December 2010 upon successful completion of FCD ballot. Pre-authorization on FDIS ballot processing has been approved by SC 6 in September 2010, upon successful completion of Last Call in ITU-T SG 17.

The FCD ballot text for ITU-T X.usnsec-1 | ISO/IEC 29180 is attached for your consideration.

SC 6/WG 7 would like to keep close collaboration with JTC 1/WG 7 on sensor networks.
We would like to inform that SC 6 appointed Mr. S.G. Yoo (Korea) as a Liaison Representative to JTC 1/WG 7 for further collaboration.

Attachment: SC6 N14354: Text for FCD ballot, ISO/IEC 29180, Security framework for ubiquitous sensor network

Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14354
Date:	2010-08-02
Replaces:	
Document Type:	Text for FCD ballot
Document Title:	Text for FCD ballot, ISO/IEC 29180, Security framework for ubiquitous sensor network
Document Source:	Project Editor
Project Number:	
Document Status:	SC 6 NBs are requested to ballot on e-balloting system of SC 6 website (www.iso.org/jtc1/sc6) no later than 2010-12-02.
Action ID:	LB
Due Date:	2010-12-02
No. of Pages:	40

Title: **A text for FCD ballot on ISO/IEC CD 29180: Security framework for ubiquitous sensor network**

Status:

This is a text for FCD ballot on ISO/IEC 29180, Security for ubiquitous sensor network. This document had been developed by the joint meeting of JTC 1/SC 7/WG 7 and ITU-T Q.15/11 in April 2010 and editorial update has been completed through the correspondence.

It is requested to initiate FCD ballot in JTC 1 according to Resolution 6.7.10 of SC 6 Barcelona meeting in January 2010, which is "Advance Authorization for an FCD Ballot on Sensor Network Security".

It is planned for Consent at the ITU-T SG 17 upon successful completion of FCD ballot in JTC 1.

INTERNATIONAL TELECOMMUNICATION UNION

STUDY GROUP 17

**TELECOMMUNICATION
STANDARDIZATION SECTOR**

TD 1073

STUDY PERIOD 2009-2012

English only

Original: English

Question(s):	6/17	Geneva, 8-17 December 2010

TEMPORARY DOCUMENT

Source:	Editors
Title:	A text for FCD ballot on ITU-T X.usnsec-1	ISO/IEC CD 29180: Security framework for ubiquitous sensor network

Summary

This document is the updated text of TD 942, 5th revised text on ITU-T X.usnsec-1 | ISO/IEC CD 29180, and will be used as text for FCD ballot in ISO/IEC SC6.

Introduction

This draft Recommendation | International Standard describes the security threats to and security requirements of the Ubiquitous Sensor Network. In addition, this draft Recommendation categorizes the security technologies according to the security functions that satisfy said security requirements and by the place to which the security technologies are applied in the security model of the Ubiquitous Sensor Network. Finally, the security functional requirements and security technologies for the Ubiquitous Sensor Network are presented.

Keywords

Security framework for Ubiquitous Sensor Network, Sensor Node Compromise, Secure Data Aggregation, Pairwise key establishment, Groupwise key, Authenticated Broadcast Message, Node-to-node authentication

Contents

ITU-T RECOMMENDATION X.usnsec-1
INTERNATIONAL STANDARD ISO/IEC CD 29180

Information technology – Security framework for the ubiquitous sensor network

1   Scope

The recent advancement of wireless-based communication technology and electronics has facilitated the implementation of a low-cost, low-power sensor network. Basically, a Ubiquitous Sensor Network (USN) consists of three parts: a sensor network consisting of a large number of sensor nodes, a base station (also known as gateway) interfacing between the sensor networks and an application server, and the application server controlling the sensor node in the sensor network or collecting the sensed information from the sensor nodes in the sensor network.

USN can be an intelligent information infrastructure of advanced e-Life society, which delivers user-oriented information and provides knowledge services to anyone anytime, anywhere and wherein information and knowledge are developed using context awareness by detecting, storing, processing, and integrating the situational and environmental information gathered from sensor tags and/or sensor nodes affixed to anything. Since there are many security and privacy threats in transferring and storing information in USN, appropriate security mechanisms are needed to protect against those threats in USN.

This draft Recommendation describes the security threats to and security requirements of the Ubiquitous Sensor Network. In addition, this draft Recommendation categorizes the security technologies according to the security functions that satisfy said security requirements and by the place to which the security technologies are applied in the security model of USN. Finally, the security requirements and security technologies for USN are presented.

2   Normative references

The Recommendations and International Standards listed below contain provisions constituting those of this Recommendation | International Standard through referencing in this text. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of ITU maintains a list of currently valid ITU-T Recommendations.

2.1   Identical Recommendations | International Standards

2.2   Paired Recommendations | International Standards equivalent in technical content

[CCITT X.800]   Recommendation CCITT X.800 (1991), *Security architecture for Open Systems*

                              ISO 7498-2:1989, Information processing systems – Open Systems Interconnection – *Basic Reference Model – Part 2: Security Architecture*

[ITU-T X.805]   Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*

ISO/IEC 18028-2:2006, Information technology — Security techniques — *IT Network security –– Part 2: Network security architecture*

2.3 Additional references

[ITU-T X.1111]   Recommendation ITU-T X.1111 (2007), *Framework for security technologies for home network*

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

3 Definitions

For purposes of this Recommendation | International Standard, the following definitions apply:

3.1 Terms defined elsewhere

This Recommendation | International Standard uses the following terms, which are defined elsewhere:

3.1.1   **Access control** [ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2   **Attack** [ITU-T H.235]: The activities undertaken to bypass or exploit deficiencies in a system's security mechanisms. By a direct attack on a system they exploit deficiencies in the underlying algorithms, principles, or properties of a security mechanism. Indirect attacks are performed when they bypass the mechanism, or when they make the system use the mechanism incorrectly.

3.1.3   **Authentication** [ITU-T X.800]: See Data Origin Authentication and Peer-Entity Authentication.

3.1.4   **Authorization** [ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

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

3.1.6   **Accessibility** [ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.7   **Confidentiality** [ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.8   **Data origin authentication** [ITU-T X.800]: The corroboration that the source of data received is as claimed.

3.1.9   **Denial of Service** [ITU-T X.800]: The prevention of authorized access to resources or the delaying of time-critical operations.

3.1.10   **Digital signature** [ITU-T X.800]: Data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

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

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

3.1.13 **Key agreement**[b-FIPS PUB 140-3]:: a key establishment procedure (either manual or electronic) where the resultant key is a function of information by two or more participants, so that no party can predetermine the value of the key independently of the other party's contribution.

3.1.14 **Key transport**[b-FIPS PUB 140-3]: secure transport of cryptographic keys (CSPs) from one cryptographic entity to another entity.

3.1.15 **Key Management** [ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

3.1.16 **Privacy** [ITU-T X.800]: The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

3.1.17 **peer-entity authentication** [ITU-T X.800]: The corroboration that a peer entity in an association is the one claimed.

3.1.18 **Repudiation** [ITU-T X.800]: Denial by one of the entities involved in a communication of having participated in all or part of the communication.

3.1.19 **Security policy** [ITU-T X.800]: The set of criteria for the provision of security services.

3.1.20 **Sensor**[Y.2221]: Electronic device that senses a physical condition or chemical compound and delivers an electronic signal proportional to the observed characteristic.

3.1.21 **Sensor network**[Y.2221]: A network comprised of inter-connected sensor nodes exchanging sensed data by wired or wireless communication

3.1.22 **Tamper detection**[b-FIPS PUB 140-3]: the automatic determination by a cryptographic module that an attempt has been made to compromise the physical security of the module.

3.1.23 **Tamper evidence**[b-FIPS PUB 140-3]: the external indication that an attempt has been made to compromise the physical security of a cryptographic module. (The evidence of the tamper attempt should be observable by an operator subsequent to the attempt.)

3.1.24 T**amper-resistant** [ITU-T X.1191]**:** Resistance to tampering by either the personal users/ attackers of a product, package, or system with physical/software access to it. Resistance to make it difficult for attackers to gain access to sensitive information contained in the module

3.1.25 **Tamper response**[b-FIPS PUB 140-3]: the automatic action taken by a cryptographic module when a tamper attempt has been detected.

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

3.1.27 **Ubiquitous Sensor Networks (USN)** [b-ITU-T Y.2221]: A conceptual network built over existing physical networks which make use of sensed data and provide knowledge services to anyone, anywhere and at anytime, and where the information is generated by using context awareness.

3.1.28 **USN middleware**[b-ITU-T F.744]: An application platform used to support common functions required by various USN applications and services.

3.2   Terms defined in this Recommendation | International Standard

This document defines the following terms:

3.2.1 **Aggregator node**: Sensor node that performs the data aggregation function in a sensor network

3.2.2 **Bootstrapping:** Refers to a process performed in a secure context prior to the deployment of the sensor node to establish a security association between the sensor nodes that may have been initialized with credentials, enabling a sensor node to communicate securely with other sensor nodes after their deployment

3.2.3 **Credentials:** Set of security-related information consisting of keys, keying materials, and cryptographic algorithm-related parameters permitting successful interaction with a security system

3.2.4 **Data aggregation: I**n-network process that transfers the aggregation value to the sink node by combining the sensed values sent by a number of sensor nodes into concise digest

3.2.5 **Groupwise Key**: Refers to a key that is used to protect multicast communications among a set of sensor nodes over a shared wireless link

3.2.6 **Key establishment**: Process by which cryptographic keys are securely established among sensor nodes using key transport and/or key agreement procedures

3.2.7 **Intrusion detection**: Process of monitoring the events occurring in a computer system or a network and analyzing them for intrusions

3.2.8 **Pair-wise key:** It refers to a key that is used to protect unicast communication between a pair of sensor nodes over a single wireless link

3.2.9 **Resilience:** Ability to recover from security compromises or attacks

3.2.10 **Secure data aggregation:** Data aggregation that ensures the integrity of the results in the presence of a small number of malicious aggregation nodes that may be attempting to influence the result.

3.2.11 **Tamper-resistant module:** a device designed to make it difficult for attackers to gain access to sensitive information contained in the module

4   Abbreviations

This draft Recommendation uses the following abbreviations:

CDMA	Code Division Multiple Access
DDoS	Distributed Denial of Service
DoS	Denial of Service
GSM	Global System for Mobile Communications
HSDPA	High Speed Downlink Packet Access
ID	Identity
IEEE	Institute of Electrical and Electronics Engineers
MAC	Medium Access Control
NGN	Next-Generation Network
PHY	physical layer
RFID	Radio-Frequency IDentification
USN	Ubiquitous Sensor Network
SN	Sensor Network
WiMAX	Worldwide Interoperability for Microwave Access

WLAN   Wireless Local Area Network

5   Conventions

In this Recommendation | International Standard:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**is prohibited from**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6   Security Model for USN

Figure 1 shows the major USN's application areas including home network application, pollution monitoring, fire monitoring, telemetry applications for utility companies (electricity, gas, water, etc.), urban resource monitoring/management applications (e.g., smart city infrastructure), and flood monitoring.
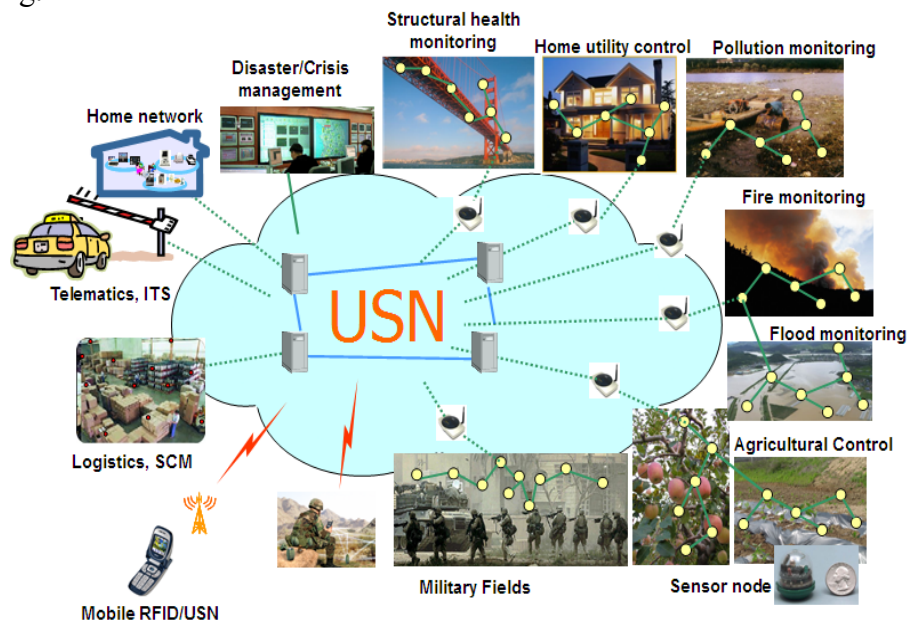

Figure 1 – Application area for USN

Figure 2 describes the overall structure of USN. Based on such basic structure, the security model should be defined for USN security.
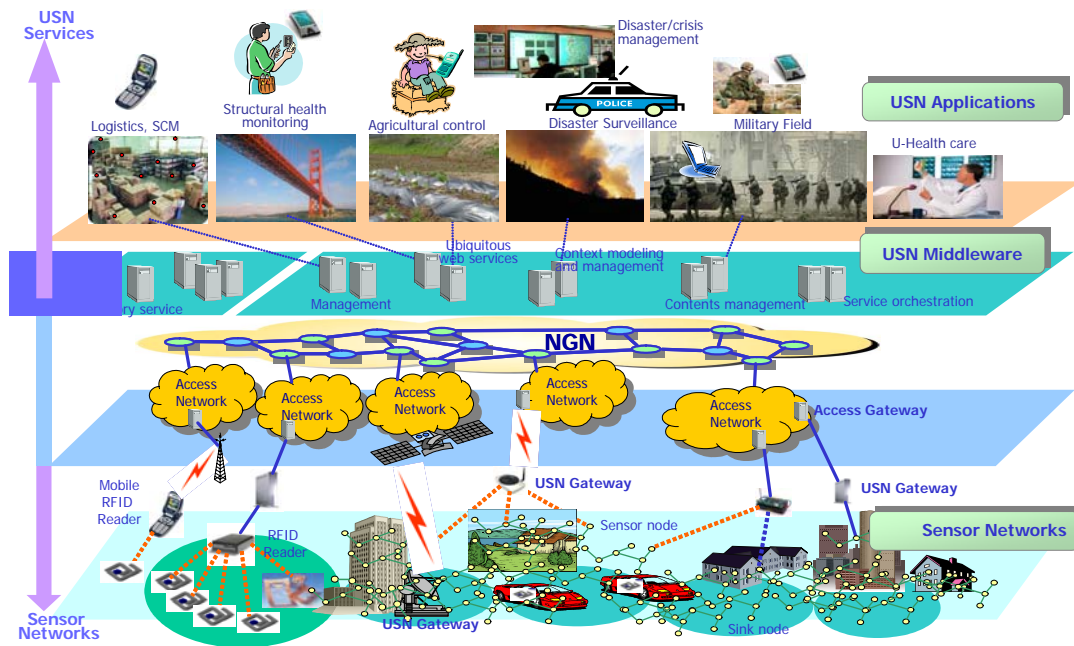
Figure 2 – Overall structure of USN

The sensor networking domain of USN usually corresponds to SN but includes wire-line sensor networks as well. Thus, many kinds of wired and wireless networking technologies may be used according to the service characteristics and requirements. The following are examples: RS-422, 423, 485, PLC (Power Line Communication), CAN (Controller Area Network), Ethernet, N-RFID, Bluetooth, WLAN, IEEE 802.15.4, etc., wherein leaf sensor devices may be sensor tags and/or sensor nodes.

Sensor networks are not isolated but are usually connected to customer networks via various access networks and core networks as shown in Figure 2. The access networking domain corresponds to many access networking technologies such as xDSL, HFC, PLC, satellite, GPRS, CDMA, GSM, HSDPA, WiMax, etc. Core networks include NGN, Internet, etc. USN may require some extensions and/or additions to core network architectures to cover new functional capability requirements extracted from USN applications and services. For instance, home security monitoring application requires some application-specific functional capability specifications. The USN middleware will consist of many software functionalities such as context models and processing, sensory information gathering, data filtering, contents management, Web Services functions, network and software management, sensor profile management, directory services, interworking gateways, etc. Based on all these functions, USN applications and services can be established and provided to customers as well as enterprises, organizations, and government.

The security model for USN can be divided into 2 parts: one for the IP network and the other for the Wireless Sensor network. Since there is no security model for the wireless sensor network studied by ITU-T, however, this Recommendation seeks to develop the security model for SN as well as IP network.

The communication patterns within our SN fall into five categories:

- Node-to-base station communication, e.g., sensor readings or special alerts

- Base station-to-node communication, e.g., specific requests

- Communication between a base station to all sensor nodes, e.g., routing beacons, queries, or reprogramming of the entire sensor network

- Node-to-node communications including communications among a defined cluster of

sensor nodes, e.g., communications between a sensor node and all its neighbors

- Communications between a base station and a group of nodes wherein the group is defined by nodes sharing a common property (e.g., location, software version, etc.)

We make the following assumptions:

- The base station is computationally robust, having the requisite processor speed, memory, and power to support the cryptographic and routing requirements of the sensor network. The base station is part of a trusted computing environment.

- Communication is from base station to sensor, from sensor to base station, from sensor to its neighbors, and from node to node.

Therefore, how such forms of network management are integrated should be taken into account.
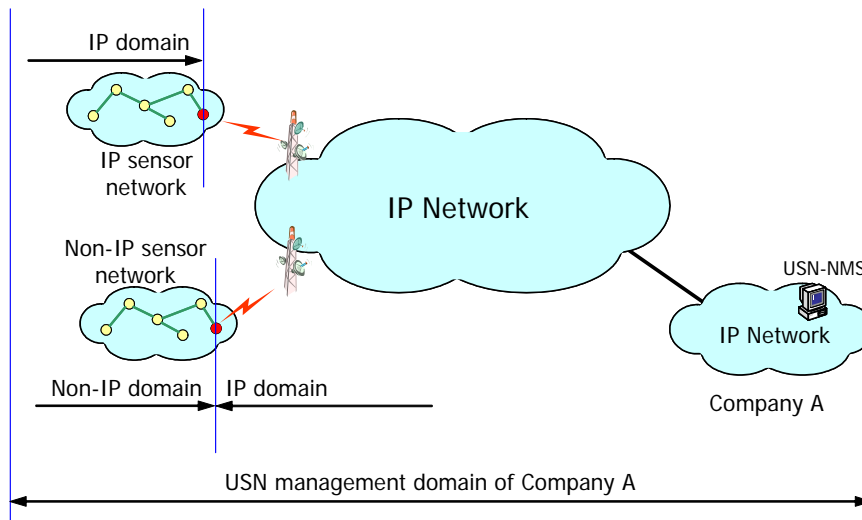

Figure 3 – USN network configuration

The following are the characteristics of the sensor network:

- The sensor network consists of a lot of sensor nodes interconnected by wireless medium.

- Sensor nodes are deployed densely in a wide area or a hostile context.

- Sensor nodes are vulnerable to failure.

- The communication from BS to sensor node would be of the broadcast type or point-to-point type.

- A sensor node has limited power, computational capacity, and memory.

- A sensor node may not have global identification.

There are three components in SN: application server communicating with sink node; sink node called base station, which interfaces the sensor network and application server, and; collection of sensor nodes using wireless communication to communicate with each other. The sink may communicate with the application server via Internet or Satellite. Security in the IP-based network is very similar to that in ITU-T X.805. Therefore, this draft Recommendation focuses on the security of the wireless sensor network (SN) consisting of a set of sensor nodes using wireless transmission.

To communicate information between sensor nodes, secure association between sensor nodes needs to be established before secure communication between them can be realized. Note, however, that the following characteristics of the sensor network make the design of secure communication very difficult:

- **Infeasibility of using public key cryptosystems**: The limited computational power, memory size, and power supply make using the public key cryptosystem -- such as Diffie-Hellman key agreement or RSA encryption and signature -- very difficult. Even though a specific sensor node may have enough resources to perform the very complex operations required for a public key cryptosystem, it becomes vulnerable to a denial of service attack as described in Section 7.1.1.

- **Vulnerability to sensor node compromise**: Since sensor nodes may be deployed in hostile locations, it results in vulnerability of sensor node compromise. After obtaining the sensor node, the attacker is able to access sensitive information such as key information or sensed information. This attack can be prevented by using tamper-resistant sensor node, which entails high cost. Moreover, a large number of sensor nodes make employing the tamper-resistant sensor node very difficult since it may result in a high-cost network. For some applications (e.g., military, safety-critical applications, etc.), however, the higher costs incurred in employing the tamper-resistant sensor node may be acceptable.

- **Difficulty in obtaining post-deployment knowledge**: In most cases, the sensor nodes will be deployed in a randomly scattered manner; hence the difficulty for the security protocol to know the location knowledge of the neighbor node.

- **Limited memory size, transmission power, and transmission bandwidth**: Since there are limited memories in each sensor node, storing unique keys with other sensor nodes in the network is very difficult. Moreover, a typical sensor node has low capability in terms of transmission bandwidth and power to communicate with neighbor nodes.

- **Single point of failure of a base station**: In a sensor network, a base station is a gateway to communicate the sensed information with an application server through the IP-based core network. The trust of the sensor network relies on that of the base station. Therefore, a base station is a source of trust, inviting various attacks by attackers on the base station.

Figure 4 presents a general model of an end-to-end communication between a sensor node in SN and an AS. There may be cases wherein the application server resides in the Gateway.
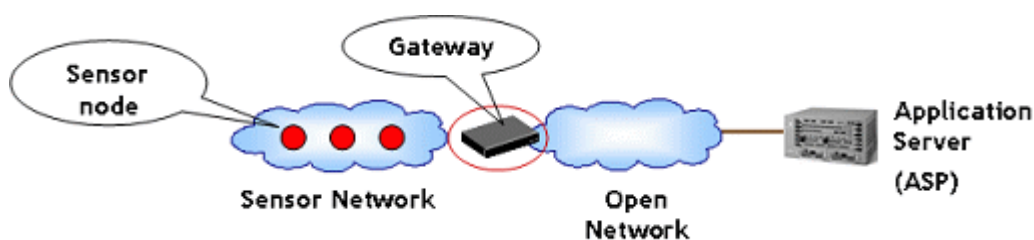

Figure 4 – General model of an end-to-end communication between a sensor node in SN and an AS

The security model for USN is shown in Figure 5. The basic security layer corresponding to MAC or link layer is responsible for link-by-link data transfer between sensor nodes or between the sensor node and a gateway. The service layer corresponding to the network layer is responsible for network data transfer between sensor nodes and between a sensor node and a gateway. Typical examples of the service layer include the broadcast message transfer from the gateway to the sensor node and vice versa. The security of the service layer and the basic function layer should implement the security functions described in Section 10, corresponding to the network layer and link layer security, respectively. Note that for some applications, the security function for application resides in a gateway rather than in an application server.
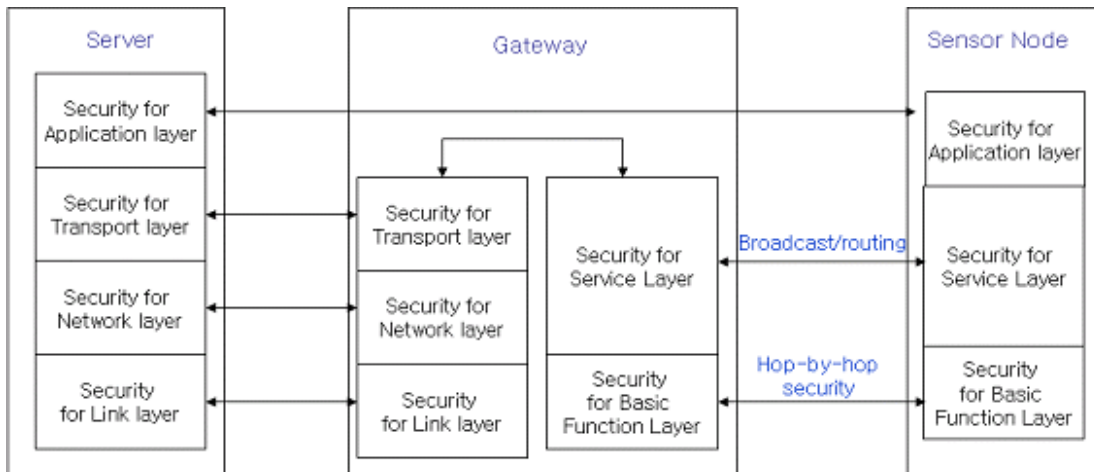
Figure 5 -- Security model for USN

7 Threats Model for USN

The threats to USN consist of two parts: those to the IP network and those to SN.

7.1 Threats model in SN

There are two types of attackers in SN; a mote-type attacker and a laptop-type attacker. In the former, the attacker has capability similar to the sensor node; it can have access to a few sensor nodes. An attacker with a mote-type device may be able to jam the radio link in its vicinity. In the latter, an attacker may have access to more powerful devices such as a laptop computer. An attacker with a laptop-type device may eavesdrop on the communication in the sensor network and have high-bandwidth, low-latency communications channel; it can also jam the entire sensor network using a high-power transmitter. There are two types of threats for SN: general threats and routing-related threats. The threats in SN are applied to the communication between the base station and sensor node and between nodes as described in Clause 6.1, and routing-related threats, to the routing message exchange as described in Clause 6.2.

7.1.1 General threats in SN

[ITU-T X.800] and [ITU-T X.805] cite the following security threats to the networks (note that these are also security threats applicable to SN):

- Destruction of information and/or other resources
- Corruption or modification of information
- Theft, removal, or loss of information and/or other resources
- Disclosure of information
- Interruption of services

In addition to these, there are a lot of sensor node-specific threats such as sensor mode compromise, eavesdropping, privacy of sensed data, denial of service attack, and malicious use of commodity network [b-Chan].

- **Sensor node compromise:** We expect sensor networks to consist of hundreds or thousands of sensor nodes. Each node represents a potential point of attack, rendering the monitoring and protection of each individual sensor from either physical or logical attack impractical. The networks may be dispersed over a large area, further exposing them to attackers capturing and reprogramming individual sensor nodes. Attackers can also obtain their own commodity sensor nodes and induce the network to accept them as legitimate nodes, or they can claim multiple identities for an altered node. Once in control of a few nodes inside the

network, the adversary can then mount a variety of attacks such as the falsification of sensor data, extraction of private sensed information from sensor network readings, and denial of service. Addressing the problem of sensor node compromise requires technological solutions. For example, cheap tamper-resistant hardware could pose a challenge to reprogramming the captured sensor nodes. Still, making nodes robust to tampering is not economically viable. Therefore, we should assume that an attacker can compromise a subset of the sensor nodes. As such, at the software level, sensor networks need new capabilities to ensure secure operation even in the presence of a small number of malicious network nodes. *Node-to-node authentication* is one basic building block for enabling network nodes to prove their identity to each other. *Node revocation* can then exclude malicious nodes. Achieving these goals given resource-limited hardware will require lightweight security protocols. Furthermore, all communications and data-processing protocols used in sensor networks must be made *resilient*, i.e., be able to function at high effectiveness even with a small number of malicious nodes. For example, routing protocols must be resilient against compromised nodes that behave maliciously.

- **Eavesdropping:** In wireless sensor network communications, an adversary can gain access to private information by monitoring transmissions between nodes. For example, a few wireless receivers placed outside a house may be able to monitor the light and temperature readings of sensor networks inside the house; thus revealing detailed information on the occupants' personal daily activities. Encrypting sensor node communications partly solves eavesdropping problems but requires robust key exchange and distribution scheme. The scheme must be simple for the network owner to execute and be feasible for the limited sensor node hardware to implement. It must also maintain secrecy in the rest of the network when an adversary compromises a few sensor nodes and exposes their secret keys. Ideally, these schemes would also allow the revocation of known exposed keys and rekeying of sensor nodes. The large number of communicating nodes makes end-to-end encryption usually impractical since sensor node hardware can rarely store a large number of unique encryption keys. Instead, sensor network designers may choose hop-by-hop encryption wherein each sensor node stores only encryption keys shared with its immediate neighbors. In this case, adversary control of a communication node eliminates the encryption's effectiveness for any communication directed through the compromised node. This situation could be exacerbated if an adversary manipulates the routing infrastructure to send many communications through a malicious node. More robust routing protocols serve as one solution to this problem. Another solution is *multipath routing*, which routes parts of a message over multiple disjoint paths and reassembles them at the destination. Multipath routing may enhance USN's resilience to attacks or compromises. The efficient discovery of the best disjoint paths to use for such an operation poses another research challenge. Note that this threat happens in the fixed core network and has relevance to privacy infringement in a sensor network.

- **Secrecy of sensed data:** Sensor networks are tools for collecting information; an adversary can gain access to sensitive information either by accessing stored sensor data or by querying or eavesdropping on the network. Adversaries can use even seemingly innocuous data to derive sensitive information if they know how to correlate multiple sensor inputs. For example, an adversary gaining access to both indoor and outdoor sensors of a home may be able to isolate internal noise from external noise and consequently extract details of the inhabitants' private activities. Still, the fact that sensor networks enable the collection of information that would otherwise be impossible is not the main privacy problem. In fact, a lot of information from sensor networks could probably be collected through direct site surveillance. Actually, sensor networks exacerbate the privacy problem because they make large volumes of information easily available through remote access. Thus, adversaries need not be physically present to maintain surveillance. They can gather information in a low-risk,

anonymous manner. Remote access also allows a single adversary to monitor multiple sites simultaneously. Ensuring that sensed information stays within the sensor network and remains accessible only to trusted parties is an essential step to ensuring privacy. Data encryption and access control serve as one approach. Another way is to restrict the network's ability to gather data at a detail level that could compromise privacy. For example, a sensor network might anonymize data by reporting only aggregate temperatures over a wide area or approximate locations of the sensed individuals. A system stores the sensed data in an anonymized database, removing details that an adversary might find useful. Another approach is to process queries in the sensor network in a distributed manner so that no single node can observe the query results in their entirety. This approach guards against potential system abuse by compromised malicious nodes.

- **DoS attacks:** As safety-critical applications use more sensor networks, the potential damage of operational disruptions becomes significant. Defending against denial-of-service attacks -- which aim to destroy network functionality rather than subverting it or using the sensed information -- is extremely difficult. DoS attacks can occur at the physical layer, e.g., via radio jamming. They can also involve malicious transmissions into the network to interfere with sensor network protocols or physically destroy central network nodes. Attackers can induce battery discharge in sensor nodes — for example, by sending a sustained series of useless communications that make the targeted nodes expend energy in processing such and forward them to other nodes as well. More insidious attacks can occur from inside the sensor network if attackers can compromise the sensor nodes. For instance, they could create routing loops that will eventually exhaust all nodes in the loop. Potential defenses against denial-of service attacks are as varied as the attacks themselves. Techniques such as spread-spectrum communication or frequency hopping can counter jamming attacks. Proper authentication can also prevent injected messages from being accepted by the network. Note, however, that the protocols involved must be efficient so that they themselves do not become targets of an energy exhaustion attack. For example, using signatures based on asymmetric cryptography can provide message authentication. Still, the creation and verification of asymmetric signatures are highly computationally intensive, and attackers that can induce a large number of these operations can mount an effective energy-exhaustion attack.

- **Malicious use of commodity networks:** The proliferation of sensor networks will inevitably extend to criminals who can use them for illegal purposes. For example, thieves can hack home automation sensors or even simply eavesdrop on their activity to gain private information on the presence, location, etc., of the owners and act accordingly. If the sensors are small enough, they can also be planted on computers and cell phones to extract private information and passwords. Such widespread use will lower the cost and availability barriers that are supposed to discourage such attacks. Sensor detectors offer one possible defense against such attacks. A detector must not only be able to detect the presence of potentially hostile wireless communications within an area that may have significant levels of radio interference but also be able to differentiate between the transmissions of authorized and unauthorized sensor networks and other devices. Although such technologies may not prevent unauthorized parties from deploying sensor networks in sensitive areas, they would make such costlier; thus alleviating the problem somehow.

7.1.2   Routing-specific threats

[ITU-T X.800] and [ITU-T X.805] identify five threats that are applicable to routing-related message exchange in SN. In addition to these, seven threats are identified in [b-Karlof] with regard to the routing messages exchanged between sensor nodes.

- **Spoofed, altered, replayed routing information:** The attacker is able to spoof, alter, and

replay the routing information, enabling creating a routing loop, attracting network traffic, extending source routing, and increasing end-to-end latency.

- **Selective forwarding:** It refers to the attack wherein a compromised node by an attacker may refuse to forward certain messages and drop them, stopping further propagation.

- **Sinkhole attack**: It pertains to the attack wherein the attacker attracts all the traffic from a particular area through a compromised node.

- **Sybil attacks**: It refers to the attack wherein a single node presents multiple identities to other nodes in the network, convincing every node that an adversary exists in more than one place at once.

- **Wormhole attacks**: In a wormhole attack, an adversary tunnels messages received in one part over a low-latency link and replays them in a different part. Wormhole attacks will involve two distinct malicious nodes colluding to understate their distance from each other by replaying the packet along an out-of-band channel available only to the attackers.

- **HELLO flood attacks**: It pertains to the attack wherein a laptop-type attacker broadcasts HELLO packets convincing every node in the network that the adversary is its neighbor.

- **Acknowledgment spoofing**: In acknowledgment spoofing, an adversary can spoof link layer acknowledgment for "overheard" packet addressed to the neighboring node, convincing the sender that a weak link is strong or a dead or a disabled node is alive.

Note that simple attacks exploiting any of the threats described above may even be used in combination to create more complex attacks (e.g., combination of Sybil and Sinkhole or Wormhole).

7.2   Threats model in the IP network

The threats model developed in [ITU-T X.805] can be applied to the IP network. Therefore, refer to [ITU-T X.805] for the details of the threats.

8   General Security Dimensions for USN

Dimension is a set of security measures designed to address a particular aspect of network security to protect against all major security threats; it is not limited to the network but extends to applications and end user information as well.

To counter the aforesaid threats in both SN and IP networks, the following security dimensions in [ITU-T X.805] are applicable:

- **Data Confidentiality:** A sensor network should not leak sensor readings to neighboring networks. In many applications (e.g., key distribution), nodes communicate highly sensitive data. The standard approach for keeping sensitive data confidential is to encrypt the data with a secret key that only the intended receivers possess; thus ensuring confidentiality.

- **Data Authentication/Identification:** Message authentication is important for many applications in sensor networks. Within the building sensor network, authentication is necessary for many administrative tasks (e.g., network reprogramming or controlling the sensor node duty cycle). At the same time, an adversary can easily inject messages; thus, the receiver needs to make sure that the data used in any decision-making process originates with the correct source. Informally, *data authentication* allows a receiver to verify that the data was really sent by the sender claiming to be such. Identification aims at proving the identity of the entity or sensor node. In the two-party communication case, data authentication can be realized through a purely symmetric mechanism: the sender and the receiver share a secret key to compute the message authentication code (MAC) of all

communicated data. When a message with a correct MAC arrives, the receiver knows that it is sent by the sender. This style of authentication cannot be applied to a broadcast setting without making much stronger trust assumptions on the network nodes. If one sender wants to send authentic data to mutually untrusted receivers, using a symmetric MAC is unsecure; since any one of the receivers knows the MAC key, he/she could consequently impersonate the sender and forge messages to other receivers. Therefore, we need an asymmetric mechanism to enable authenticated broadcast. One of methods is to construct authenticated broadcast from symmetric primitives only and introduce asymmetry with delayed key disclosure and one-way function key chains. Authentication mechanisms are mainly used to validate the legitimacy of the node so that its legitimacy and credibility are ensured.

- **Data Integrity:** In communication, *data integrity* assures the receiver that the received data is not altered in transit by an adversary.

- **Access Control:** Access control ensures that only the authorized user or entity is allowed to gain access to information, resource, or services.

- **Non-repudiation:** Non-repudiation ensures that the entity or user cannot deny the activities in the network he/she has done.

- **Communication Security:** Communication security ensures that the information only flows from the source to the destination.

- **Availability:** Availability ensures that information, service, and application are available to legitimate users anytime.

- **Privacy:** Privacy ensures that the identifier of the user or entities and network usage is kept confidential.

In addition to the security dimensions described above, a dimension for "Resilience to Attacks" through the appropriate design of PHY/MAC/Routing protocols should be added for the SN part only.

- **Resilient to attacks**: This refers to any of the measures for recovering from various attacks against USN. It ensures that USN is able to recover from attacks so that it is capable of detecting/remaining resilient to various attacks through the appropriate design of PHY/MAC/Routing protocols. Resilience to attacks include resiliency against compromised nodes, resiliency against eavesdropping on routing information, etc.

9   Security Dimensions and Threats in USN

Message exchange in SN can be grouped into three types: message exchange between nodes, message exchange between a base station and a node, and; message exchange for routing–related message.

9.1   Security dimensions and threats for the message exchange in SN

9.1.1   Security dimensions and threats for the message exchange between sensor nodes

Table 1 lists the security requirements and describes the relationship between the security dimensions and the security threats identified in ITU-T X.805: the letter "Y" in a cell formed by the intersection of the table's columns and rows suggests that a particular security threat is opposed by the corresponding security dimensions.

Table 1: Mapping of security dimensions to security threats

Security dimension	Security threat

	Destruction of information or other resources	Corruption or modification of information	Theft, removal, or loss of information and other resources	Disclosure of information	Interruption of services
Access control	Y	Y	Y	Y	
Authentication			Y	Y	
Non-repudiation	Y	Y	Y	Y	Y
Confidentiality			Y	Y	
Communication security			Y	Y	
Data integrity	Y	Y			
Availability	Y				Y
Privacy				Y	

Table 2 lists the security dimensions and describes the relationship between security dimensions and sensor node-specific threats for the message exchange between nodes or information stored in sensor node; the letter "Y" in a cell formed by the intersection of the table's columns and rows suggests that a particular security threat is opposed by the corresponding security dimension. For example, the threat of sensor node compromise could be addressed by employing physical access control to limit access to the resource of the sensor to the authorized user or entity only, using node-to-node authentication to prove one's identity to the other and vice versa, using data processing and communication protocol resilient to a small number of compromised sensor nodes, and/or employing routing protocols resilient to compromised nodes that behave maliciously. The threat of privacy infringement of sensed data could be addressed by employing data encryption and access control resulting in the protection of sensed data accessible to the authorized node only, processing sensed data transfer in a distributed manner so that no single node observes the sensed data, and/or selecting a secure routing path for transferring the sensed data. The threat of Denial-of-Service attacks could be addressed by employing the proper authentication of sensed data and designing the security protocol involved to be resilient to DoS attack and/or spread-spectrum communication technology to counter any jamming attack.

Table 2: Security dimensions to sensor node-specific threats

Security dimensions	Sensor node-specific threats			
	Sensor node compromise	Secrecy of sensed data	DoS	Malicious use of commodity network
Access control	Y	Y		Y
Authentication	Y		Y	Y
Non-repudiation				—
Confidentiality		Y		Y
Communication security	Y	Y		
Data integrity				
Availability			Y	

Security dimensions	Sensor node-specific threats			
	Sensor node compromise	Secrecy of sensed data	DoS	Malicious use of commodity network
Privacy		Y		Y
Resilient to attacks	Y	Y	Y	Y

9.1.2 Security dimension and threats for the broadcast message from a base station to all sensor nodes

Table 3 lists the security dimensions and describes the relationship between the security dimensions and the security threats against the broadcast message transmitted from a base station to all the sensor nodes: the letter "Y" in a cell formed by the intersection of the table's columns and rows suggests that a particular security threat is opposed by the corresponding security dimension.

Table 3: Security dimensions to security threats against broadcast message

Security dimension	Security threats against broadcast message from a base station to all nodes				
	Destruction of information	Corruption or modification of information	Theft, removal, or loss of information	Disclosure of information	Interruption of services, DoS
Access control	Y	Y	Y	Y	
Authentication		Y	Y	Y	
Non-repudiation	Y		Y		Y
Confidentiality			Y	Y	
Communication security			Y	Y	
Data integrity	Y	Y			
Availability	Y				Y
Privacy				Y	
Resilient to attacks	Y	Y	Y	Y	Y

9.1.3 Security dimension and threats for the routing message exchange

The threats can be classified into two categories: insider attacks and outsider attacks. Insider attacks can be launched by the insider, i.e., the attacker has knowledge of the sensitive information stored in the sensor node, i.e., key information for the secure channel. Insider attacks include Sybil attack, HELLO flood attack, wormhole and sink hole attack, selective forwarding attack, and DoS attack. Table 4 lists the security dimensions and describes the relationship between the security dimensions and the security threats of the routing message exchange launched by an insider attack: the letter "Y" in a cell formed by the intersection of the table's columns and rows designates that a particular security threat is opposed by the corresponding security dimension. The insider is able to compromise the sensor node, i.e., an authorized participant in the sensor node performs malicious activities, as well as launch active attacks including passive attack. Insider attacks may be launched from either compromised sensor nodes running malicious code or adversaries who have stolen the key material, code, and data from legitimate sensor nodes. The insider is able to attack SN by spoofing or injecting bogus routing information, creating sink holes, selectively forwarding packets, using Sybil attack, and broadcasting HELLO floods. Link layer security mechanisms using a globally shared key may be inefficient in the presence of insider attacks or compromised nodes.

For example, the Sybil attack can be addressed by using routing message authentication and encryption utilizing the resulting key as the outcome of a third-party key distribution scheme such as Needham-Schroeder and by limiting the number of neighbors that a node is allowed to have.

Table 4: Mapping of security dimensions to security threats of an insider attack

Security requirements	Security threat					
	Sybil attack	HELLO flood	Sinkhole	Selective forwarding	Worm hole	Acknowle dgment spoofing
Access control						
Message authentication	Y	Y				
Identification	Y	Y				
Non-repudiation						
Confidentiality	Y					
Communication security						
Data integrity						
Availability						
Privacy			Y		Y	
Resilient technology	Y (third-party key distribu tion)	Y (third-party key distributi on)	Y (tight time synchronizat ion)	Y (multipath)	Y (tight time synchroniz ation)	Y (third-party key distribution)

Table 5 lists the security dimensions and describes the relationships between the security dimensions and the security threats of the routing message exchange launched by an outsider: the letter "Y" in a cell formed by the intersection of the table's columns and rows suggests that a particular security threat is opposed by the corresponding security dimension. The outsider is able to launch only active attacks and passive attack; the attacker has no special access to the sensor network. Most outsider attacks against the sensor network routing protocol can be prevented by simple link layer encryption and authentication using a globally shared key. The Sybil attack is no longer relevant because nodes will not accept a single identity of the adversary. Therefore, for example, the Sybil attack can be addressed by verifying the identity of the sensor node or by using message authentication or through confidentiality. Selective forwarding and sinkhole attack may be impossible because the adversary is prevented from joining the topology. Link layer acknowledgment should be protected by employing message authentication. Multipath routing can be used to counter selective forwarding attacks. Messages routed over n paths are protected against selective forwarding attacks involving up to n compromised nodes.

Table 5: Mapping of security dimensions to security threats from the outsider

Security dimension	Security threat					
	Sybil attack	HELLO flood	Sinkhole	Selective forwarding	Worm hole	Acknowle dgment spoofing
Access control				Y		

Security dimension	Security threat					
	Sybil attack	HELLO flood	Sinkhole	Selective forwarding	Worm hole	Acknowledgment spoofing
Message authentication	Y	Y				Y
Identification	Y	Y				Y
Non-repudiation						
Confidentiality	Y	Y				Y
Communication security				Y		
Data integrity		Y				
Availability						
Privacy			Y	Y	Y	
Resilient technology	Y (TRM)	Y	Y (Multipath)	Y	(Multipath) Y	Y

9.2 Security dimension and threats for the message exchange in the IP network

The security threats and security dimensions developed in ITU-T X.805 can directly be applied to a secure message exchange through the IP network. Therefore, refer to [ITU-T X.805] for related details.

10 Security Technologies for USN

10.1 Key management

Key management refers to the generation, distribution, sharing, rekeying, and revocation of cryptographic keys for the data confidentiality service, data integrity, data freshness, and data authentication in SN. The security of key management forms the foundation of security of other security services. In the sensor network, sharing or distributing a pairwise key between the sensor nodes and a groupwise key among a set of sensor nodes is very important. It is sometimes called key agreement scheme.

In general, there are three types of key agreement: trusted server scheme, self-enforcing scheme, and key pre-distribution scheme. The trusted server scheme uses the central trusted server to share the pairwise key between the sensor nodes or the groupwise key among the sensor nodes. A typical example of this scheme is Kerboros. Note, however, that this type of scheme is not adequate for the sensor network since there is no trusted infrastructure in the sensor network. The self-enforcing scheme uses the public key algorithm to share the pairwise key or groupwise key in the sensor network. Typical algorithms of the public key algorithm include the Diffie-Hellman key agreement algorithm and RSA key transport algorithm. Note, however, that this scheme cannot be employed in the sensor network due to the limited memory and computational complexity of the sensor node. The key pre-distribution scheme pre-distributes the key information among all sensor nodes prior to deployment. The deployment of most sensor nodes is random. In other words, a priori knowledge as to the exact location of the sensor node is assumed to be unknown prior to deployment. This scheme has low communication overhead. In addition, it is resilient to node compromise, and it does not rely on the trust of the base station. Therefore, this scheme is very suitable for the wireless sensor network.

There are a number of key pre-distribution schemes that do not assume to have knowledge of deployment of the sensor node. The simple scheme is a master key-based pre-distribution one. In this scheme, all nodes have a single common master key that is pre-deployed to each sensor node. Any two nodes use this global master key to obtain the common pairwise key by exchanging random nonces. This scheme does not provide desirable resilience to node compromise since the entire sensor network is compromised if a node is compromised. The second scheme is called pairwise key pre-distribution scheme. This scheme is designed to let each sensor node have N-1 secret pairwise keys each of which is known only to this sensor node and one of the other N-1 sensor nodes where N is the total number of sensor nodes in the network. This scheme renders perfect resilience against node compromise since a compromised node does not affect the security of any other node. Nonetheless, it lacks scalability since adding new nodes to the existing sensor node is impossible owing to the absence of a new pairwise key in the existing node. In addition, this scheme is not practical since the memory size is limited when the number of sensor nodes is very large. The third scheme is the random key pre-distribution scheme. In this scheme, the subset of keys from a large key pool is stored prior to the deployment of sensor node; two nodes find a common key and use it as shared session key between them.

In the random key schemes presented so far, however, while each node can verify that some of its neighbors have certain secret keys, and that they are consequently legitimate nodes, no node can authenticate the identity of a neighbor that it is communicating with.

The following are the capabilities of key management in a sensor network :
- Key management supports node-to-node authentication.
- **Scalable key management**: The key management scheme supports a large sensor network. In addition, it should be flexible when there is a substantial increase in sensor nodes even after the deployment of sensor node.
- **Efficiency of memory size, processing capability, and communication overhead required for key management**: The key management scheme has efficient storage complexity, i.e., minimum memory size to store the key in the sensor node, efficient computation complexity required to establish the key, efficient communication overhead, i.e., number of messages exchanged during the key generation process.
- **High pairwise key establishment**: In the key management scheme, the two sensor nodes have high probability of establishing the common key and key material.
- **Resilience against node compromise:** The key management scheme has capability to resist node compromise. A compromised security credential should not reveal even the minimum information on the security of other links in the sensor network, i.e., higher resilience means lower number of compromised links. Note that resilience should not be limited to key management issues but should be applied to all sensor nodes. A typical example includes resilience against eavesdropping on routing information. Details of key management are described in ANNEX A.

10.2   Authenticated broadcast

This is important since broadcasts are used in many applications in sensor networks. For example, routing tree construction, network query, software updates, time synchronization, and network management all rely on broadcast. Due to the nature of wireless communication in sensor networks, however, attackers can easily inject malicious data or alter the content of legitimate messages during multihop forwarding. Sensor networks applications need authentication mechanisms to ensure that data from a valid source will not be altered during transmission. Broadcast authentication is one of the most important security primitives in sensor networks.

A broadcast message targets all sensor nodes. A broadcast message authentication scheme allows any targeted node to verify the authenticity of the broadcast messages. Two kinds of techniques can be used to achieve such according to the type of cryptographic algorithm. In the case of public key

cryptography, a digital signature can be used. If symmetric cryptography is used, there is a need to append to the data the verifiable authentication data (i.e., message authentication code) based on the multiple shared secret between the base station (sink node) and sensor node. Due to the properties of the sensor network, the broadcast authentication method is preferred in broadcast message authentication based on symmetric cryptography.

There is a typical scheme for enabling broadcast authentication in sensor networks, called TESLA (Timed Efficient Stream Loss-tolerant Authentication) [b-RFC4082, b-TESLA]. TESLA supports delayed per-packet data authentication and integrity checking. The key idea is the delayed disclosure of symmetric keys. The delayed key disclosure results in authentication delay. TESLA has the following properties: low computation overhead for the generation and verification of authentication information; low communication overhead; limited buffering required for the sender and the receiver; high robustness to packet loss; scales to a large number of receivers, and; protects receivers from denial of service. TESLA makes the following assumptions:

- The base station and the sensor node should be loosely time-synchronized.

- TESLA should be bootstrapped at session setup through a regular data authentication system.

As the simplified version of TESLA, µTESLA protocol [b-SPINS] basically uses the delayed disclosure of symmetric key. The base station and the sensor nodes are assumed to be time-synchronized loosely. The operation is as follows: the base station computes MAC on the packet with the key that is secret at that point of time. When a node receives a packet, it can confirm that the base station has not yet disclosed the corresponding MAC key according to its loosely synchronized clock and time when the keys are to be disclosed. The node stores the packet in its buffer. When the MAC keys are to be disclosed, the base station broadcasts the MAC keys to all sensor nodes. The sensor node can verify the authenticity of the broadcast message by using the disclosed MAC keys and MAC data stored in the buffer. Each MAC key is a member of a key chain that has been generated by a one-way function. For the base station to generate this key chain, the base station chooses the last key K_n of the key chain randomly and applies the one-way hash function H repeatedly to compute all other keys: $K_i = H(K_{i+1})$, i = 1, …, n-1. The sensor node, which shares K1 with the base station, can verify the correctness of the key and use the disclosed MAC keys and MAC data stored in the buffer to authenticate the packet stored in the buffer. The following are the differences between TESLA and µTESLA:

- TESLA authenticates the initial packet with a digital signature, which is too expensive for our sensor nodes. uTESLA uses only symmetric mechanisms.

- Disclosing a key in each packet requires too much energy for sending and receiving. uTESLA discloses the key once per epoch.

- Storing a one-way key chain in a sensor node is expensive. uTESLA restricts the number of authenticated senders.

The following are the capabilities of authenticated broadcast in a sensor network:

- **Resistance to node compromise:** Since tamper-proof hardware will unlikely be deployed on sensor motes in the near future, secure sensor network protocols need to be resilient against compromised nodes. In addition, being resilient to attacks necessitates the avoidance of single points of failure. For instance, a base station is a single point of failure. Tamper-proof base stations should be combined with multipath routing (even through access points) so that base station security failures may be less compromising.

- **Low computation overhead:** Sensor nodes have limited computation resources; thus, an ideal protocol would have low computation overhead for both sender and receiver.

- **Low communication overhead:** Energy is an extremely scarce resource in sensor nodes. In particular, radio communication consumes the greatest amount of energy. Thus,

protocols with high communication overhead are avoided, if possible.

- **Robustness to packet loss:** Reliable message delivery is the property of a network wherein valid messages are not dropped.
- **Immediate authentication:** Depending on the application, authentication delay may influence the design of the sensor network protocol. For time-critical messages such as fire alarms, the receiver would most likely need to authenticate the message immediately. Note, however, that authentication delay is typically acceptable for non-time-critical messages.
- **Messages sent at irregular times:** Some applications send synchronous messages at regular and predictable times, while others are not. In some situations, sending messages asynchronously (e.g., presence detector) should be avoided to prevent the creation of covert channels. In other cases, having synchronous (i.e., periodic) communication activity should be avoided to prevent security threats due to the predictability of network communication behavior.

μTPC is another improved version of TESLA. The details of μTPC for Authenticated Broadcast in Sensor Networks are described in ANNEX B.

10.3   Secure data aggregation

Data aggregation is a widely used technique in wireless sensor networks.

The security issues, data confidentiality, and integrity in data aggregation become vital when the sensor network is deployed in a hostile environment. There have been many related works proposed to address these security issues.

Secure data aggregation refers to an in-network process performed on the aggregator node to transfer securely the aggregation value to the sink node (i.e., a base station) by combining the sensed values sent by a number of sensor nodes. In this scheme, each sensor node sends an encrypted sensed value to the aggregator, which then calculates the encrypted aggregator results using aggregation functions such as summing function, average function, median function, and maximum value or minimum value; the sink node obtains the aggregation value by decrypting the encrypted aggregator results.

Therefore, it is more useful for the base station or a sensor node to have the capability to aggregate data than the individual value from all sensors. By aggregating data, reducing the amount of data that needs to be transmitted from one sensor to another sensor can be reduced. Secure data aggregation can be applied to sensors deployed in a hierarchical structure.

There are two kinds of secure aggregation methods: hop-by-hop encrypted data aggregation and end-to-end encrypted data aggregation.

- **Hop-by-hop encrypted data aggregation**: The operation is based on hop-by-hop encryption between neighbor sensor nodes. Each pair of neighbor sensor nodes is assumed to share a common secret key. The sensed values are encrypted by many sensor nodes. All encrypted values collected are decrypted by the intermediate aggregator nodes, which then obtain and re-encrypt the aggregated value. This process is repeated up to the sink node. Finally, the sink node obtains the total aggregated value.

- **End-to-end encrypted data aggregation**: The operation is based on the end-to-end encryption between many sensor nodes and one sink node. A common secret is assumed to be shared between many sensor nodes and a sink node. The sensing nodes encrypt the sensed values and forward them to intermediate aggregator nodes, which only collect them, perform some cryptographic operation on the aggregated values, and forward them since they do not have decryption keys. Finally, the sink node decrypts many encrypted aggregated results.

The framework for end-to-end encrypted data aggregation is known to incur higher computation cost on the sensor nodes but achieves stronger security compared with the framework for hop-by-hop encrypted data aggregation.

10.4   Data freshness

Since all sensor networks stream some forms of time-varying measurements, guaranteeing confidentiality and authentication is not enough; we must also ensure that each message is *fresh*. Informally, data freshness implies that the data is recent and ensures that no adversary replayed old messages. We identify two types of freshness: weak freshness, which provides partial message ordering but carries no delay information, and; strong freshness, which provides a total order on a request-response pair and allows for delay estimation. Weak freshness is required by sensor measurements, whereas strong freshness is useful for time synchronization.

10.5   Tamper-resistant module

The best well-known technique to protect against sensor node compromise is to use the tamper-resistant module in the sensor node. If each sensor node is equipped with a tamper-resistant module, protecting the storage of sensitive data, e.g., key data, may be possible, otherwise triggering damage in case of capture of sensor nodes. Another possible technique in protecting against a compromised sensor node is to limit the amount of information obtained by the attacker after reading data from the captured sensor nodes. The former is more expensive than the latter, however. Therefore, the first option will be limited to applications that are critical enough to require the more expensive option. If sensor nodes cannot be tamper-resistant, the latter should be implemented to gain probability security. The Cryptographic Module [b-FIPS PUB 140-3] is an example of a tamper-resistant module that ensures sensitive data without storage damage.

10.6   USN middleware security

An enormous amount of data collected in the sensor network are securely stored, managed, and analyzed by USN middleware, which delivers data to the appropriate application through a secure channel. Since it communicates with sensor networks or applications over the IP network, USN middleware should consider the existing security threats on the IP network. To ensure secure communications against various threats such as spoofing, sniffing, message modifications, DDoS, etc., security dimensions such as encryption/decryption, authentication, authorization, and access control are considered and applied. Furthermore, the encryption/decryption function for data stored in USN middleware is needed because USN middleware sometimes stores very important and valuable data that cause a big problem when they are revealed. The security technique to ensure the availability of USN middleware is considered as well. The Cryptographic Module [b-FIPS PUB 140-3] can be considered as a security module for USN middleware.

10.7   IP network security

The IP network security technologies in ITU-T X.805 can directly be applied to secure message exchange through the IP network. Therefore, related details can be omitted.

10.8   Sensor node authentication

The mechanisms for sensor node authentication are mainly used to validate the legitimacy of the equipment when it enters the network to ensure that equipment in the network are legitimate and credible. Details of authentication mechanisms for the sensor node are described in Annex C.

10.9   Privacy protection in sensor network

Data encryption and access control are typical approaches for ensuring privacy preservation in a sensor network. Another approach is to limit the network capability to collect the sensed data at a

detail level that could release the privacy of the individuals concerned. For example, the sensor network might report the aggregate temperature over a large area instead of a small area. Sensed data should be stored securely in a sensor node by applying access control mechanisms to them. Another approach is to process the query in a distributed manner so that a single or a small number of sensor nodes cannot obtain the query results, which might result in the compromise of privacy.

11 Specific Security Functional Requirements for USN

This clause specifies the various levels of security requirements that pertain individually or collectively to USN security.

11.1 Mandatory functional requirement

- SN is required to support the data integrity and message authenticity of sensed data.

- The key management scheme in SN is required to support the key pre-distribution scheme described in clause 10.1.

- Key management is required to support both pairwise key establishment and groupwise key establishment.

- SN is required to authenticate broadcast messages from a base station to all the sensor nodes and vice versa.

- SN is required to support secure routing protocols with message authentication, ID authentication, data freshness, and data integrity.

- SN is required to support the capability to be resilient against various attacks.

- The base station in SN is required to support the capability to mitigate the effects of DoS attacks from both wireless interface and wired interface.

- USN is required to support USN middleware security as described in Section 10.6.

- SN is required to support authentication/identification of the node by other nodes.

11.2 Recommended functional specifications

- SN is recommended to support a secure end-to-end encrypted data aggregation scheme.

- SN is recommended to support data freshness for sensed data.

- SN is recommended to support the confidentiality of sensed data.

- Key management is recommended to support pairwise key establishment based on ID-based authentication. An example of this authentication is described in ANNEX C.

- USN is recommended to support the mechanism for ensuring the privacy of sensed data.

- The base station is recommended to support tamper resistance to avoid a single point of failure.

11.3 Optional functional specifications

- The sensor node or base station can optionally provide a secure hop-by-hop data aggregation scheme.

- The sensor node can optionally have tamper–resistant module for protecting credentials, sensed data, or other confidential data.

- The sensor node can optionally have tamper detection, tamper evidence, or tamper response.

- SN can optionally have the capability to mitigate DoS attacks against the sensor node.

- SN can optionally have the capability to access multiple or randomly selected base stations to mitigate large-scale security threats due to single point of failure effects.

- SN can optionally have the capability to mask asynchronous activity into synchronous messaging.

- SN can optionally have the capability to provide multipath and/or randomized route selection to enhance resilience to attacks.

- The base station in the sensor network can optionally have the capability of intrusion detection.

- SN can optionally have the capability to be configured to provide privacy protection.

ANNEX A

Key Management in Sensor Networks

(This annex forms an integral part of this Recommendation | International Standard)

A.1   Threat Time

Once deployed, nodes establish a pairwise key in a short time to ensure the key's security. Therefore, whether the phase of key setup is exposed to an adversary or not is crucial because sensitive information such as random number or identity information of node is open during this phase. An adversary may get ready to attack in advance even before key setup. This adversary can analyze communication between nodes or obtain physical access to the node during key setup. This adversary is regarded as strong and intensive. This means that an application requiring a high security level must design a key scheme assuming a prepared adversary.

On the other hand, to make an application more flexible and usable, a key management scheme with low security level can be taken. In this case, an attack is possible after a key is established. It is hard for an adversary who does not know the deployed time and who is unable to access the deployed place to try an attack during key setup. This is a very real case despite the loose attack. On the application where loose or no attacks during key setup are launched, designing a key scheme is reasonable to improve efficiency and scalability with only loose security.

A.2   Key Management Classes

Based on the two criteria above, i.e., threats and threat time, 4 key management classes are defined.

A.2.1   Class 1

This class assumes that an adversary can eavesdrop after key setup. There is no other threat such as node capture throughout the network life. Thus, this class considers the weakest adversary.

A.2.1   Class 2

This class assumes that an adversary can eavesdrop or capture and reprogram nodes for node compromise after key setup. In other words, during key setup, there are no threats in place, and eavesdropping hardly exists. After key setup, however, an adversary is capable of eavesdropping or obtaining secret information through node capture.

A.2.3   Class 3

This class assumes that an adversary can eavesdrop on the communications when nodes are deployed; after key establishment, the adversary is prepared for all attacks including node capture.

A.2.4   Class 4

An active adversary always waits for node deployment. This means that eavesdropping and node capture already take place in the phase wherein nodes are deployed. Considering the strongest adversaries, this class is a general assumption but incurs high cost.

Generally, an adversary able to attack including executing node capture is considered to have enough ability to eavesdrop on transmitted data. Accordingly, other classes need not be considered: the case wherein node compromise is always possible but eavesdropping is practical only after key setup, and; the case wherein all attacks except eavesdropping are possible only after key setup. Moreover, the higher a class level is, the stronger an adversary. If a key scheme in a higher class is secure, it is also secure in a lower class. The key scheme classes are shown in Figure 1.
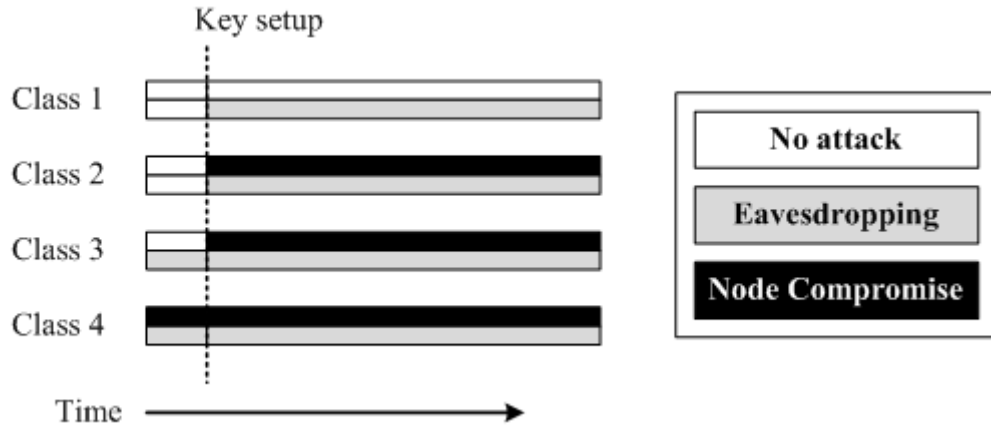
Figure A-1. Key Management Classes

A.3 Key Schemes

A.3.1 Key Management Mechanisms

A.3.1.1 PAIRWISE KEY PRE-DISTRIBUTION

A pairwise key between a pair of nodes is directly stored and pre-distributed in each node prior to node deployment ("pairwise key scheme"). Since each node in this scheme stores its pairwise keys, it has perfect resilience against node capture; in other words, even if a node is captured, the keys of non-captured nodes are never compromised. Note, however, that scalability is limited because the network scale depends on the memory of the node where potential keys are stored.

A.3.1.2 MASTER KEY-BASED PRE-DISTRIBUTION

A pairwise key is derived from both a random number exchanged between each node and a single master key pre-distributed into each node ("master key scheme"). It results in great key connectivity and requires little memory. Nonetheless, resilience is very low since all pairwise keys can be compromised when the master key is exposed to an adversary. Unlike the Master key scheme, which does not erase a master key after key setup, a master key is erased completely after a pairwise key is established. Although resilience is improved by erasing the master key of the deployed nodes, the risk of compromising a master key during node addition remains since the added nodes store a master key.

A.3.1.3 BASE STATION PARTICIPATION

"SPINS" falls under this mechanism[b-SPINS]. In SPINS, each node is given its shared key with the base station, also known as a gateway. The base station directly transmits a pairwise key encrypted with each node's shared key. In other words, the base station mediates in key setup. This scheme supports not only full connection but also perfect resilience. Still, it is not scalable because of the immense traffic volume resulting from intermediation.

A.3.1.4 PROBABILISTIC KEY PRE-DISTRIBUTION

For large networks, a probabilistic method is more efficient than a deterministic method. For instance, this mechanism is based on the concept that all the nodes in all networks are connected with a 0.9997 probability -- almost fully connected -- if the probability that each node can establish a pairwise key with its neighbor nodes is 0.33. A key ring is stored in each node prior to deployment (key ring k is randomly selected from key pool P, which is randomly selected from a huge key space). A common key in both key rings of a pair of nodes is used as their pairwise key. It

guarantees enough resilience -- albeit an imperfect one -- because the probability of breaking the communication link is *k/P*. Moreover, it supports large-scale networks.

A.3.1.5 NO KEY PRE-DISTRIBUTION

This mechanism considers the reality of sensor networks. If an adversary does not know where and when nodes are deployed, launching an active attack at an early phase is difficult. Improving efficiency instead of opting for minimal node loss can be a good trade-off due to attacks during key setup. In this scheme, key setup is completed in a relatively short time through a few transmissions. As an advantage of this mechanism, the base station does not take part in key setup; hence the relatively less energy consumed. Unlike the pre-distribution schemes above, it does not need to load potential keys into a node, thereby incurring low cost in terms of network organization. Note, however, that it is only strong when an adversary does not observe communication during key setup; it cannot add nodes since a pairwise key is established through the exchanged data during key setup.

A.3.1.6 PROBABILISTIC PAIRWISE KEY PRE-DISTRIBUTION

The probabilistic pairwise keys scheme is a modification of the pairwise key scheme based on the observation that not all n-1 keys need to be stored in the node's key ring to have a connected random graph with high probability. Formula allows us to calculate the smallest probability p of any two nodes connected such that the entire graph is connected with high probability c. To achieve this probability p in a network with n nodes, each node needs to store only a random set of np pairwise keys instead of exhaustively storing all n-1s. The use of pairwise keys instead of purely random keys chosen from a given pool can give us node-to-node authentication properties if each node holding key k also stores the identity (ID) of the other node, which also holds k. Thus, if k is used to create a secure link with another node, both nodes are certain of the identity of each other since no other nodes can hold k.

ANNEX B

Authenticated Broadcast in SN (Sensor Networks): µTPC

(This annex does not form an integral part of this Recommendation | International Standard)

B.1 Construction of µTPC

A major problem in scaling up µTESLA is how to distribute and authenticate the initial µTESLA parameters (µTP) including the key chain commitments, starting time, duration of each time interval, etc. The multilevel µTESLA uses high-level µTESLA instances to authenticate the parameters of low-level ones; it inherits the authentication delay introduced by µTESLA during the distribution of those parameters. As a consequence of such authentication delay, an attacker can launch DoS attacks to disrupt the distribution of the initial µTESLA parameters. Moreover, a multilevel µTESLA cannot handle a large number of senders. The tree-based µTESLA protocol uses the Merkle Tree mechanism to distribute µTP. Using the certificate from the Merkle tree, receiver nodes can authenticate µTP immediately; thus resisting DoS attacks. Note, however, that the cost of Tree-based µTESLA is too high. The µTPCT-based broadcast authentication protocol constructs µTPC (µTP one-way Chain) to distribute and authenticate µTP. It can resist DoS attacks but incurs low cost.

In sensor networks with multiple BNodes, BNode (Broadcast Node) may have different characteristics considering the task to be performed. The life cycle, broadcasting frequency, and real-time requirement of BNode are called Feature Parameters or FP for short. BS (Base Station) will construct µTP based on the FP of BNode. For example, for the BNode with short life cycle, high broadcasting frequency, and strict real-time requirement, BS will construct a special µTP containing short key disclosure lag and fewer µTESLA instances with short time interval. FP can be expanded if necessary.

µTPC consists of µTP and One-way Chain. After FP is determined, BS will first divide the lifetime of BNode into N time intervals with length of T_N such that the duration of T_N (e.g., 30 minutes) is suitable for running µTESLA instance on BNode and sensor nodes efficiently. Based on the broadcasting frequency and real-time requirement of BNode, BS will divide T_N into n time interval with length of T_n. Based on N and n, BS uses pseudo-random function F to generate N µTESLA key chains that are linked together. First, BS generates the last key $K_{N,n}$ of the N-th µTESLA key chain randomly. Afterward, using hash function H (e.g., SHA-1), BS generates the rest of the keys of the N-th µTESLA key chain according to $K_{N,i}=H(K_{N,i+1})$. For the $(i-1)$-th µTESLA key chain, BS generates the last key by performing a pseudo random function on the first key (key next to the commitment) of the i-th µTESLA key chain, and then generates the rest of the keys of the $(i-1)$-th µTESLA key chain by performing H on its last key. This way, BS generates all µTESLA key chains up to the last one. Figure B-1 shows the construction of µTESLA key chains.

After all µTESLA key chains are generated, for BNode j, BS will assign different keys to different time intervals T_n. Accordingly, there will be N µTESLA instances. Whereas the initial parameter of the ith µTESLA instance is $\mu TP_i=\{T_s \parallel K_{i,0} \parallel T_i \parallel T_{int} \parallel d\}$ where T_s denotes the current time, $K_{i,0}$ denotes the commitment, T_i refers to the starting time, T_{int} denotes the synchronization interval, and d refers to the disclosure lag of the key. After all µTPs are determined, BS generates a value U_N randomly, and then computes each U value by $U_{i-1}= H(U_i \parallel \mu TP_{i-1})$ up to U_0 where " $\parallel$ " denotes message concatenation. Finally, BS constructs µTPC that includes N µTPs. Figure B-2 shows an example of the construction of µTPC.
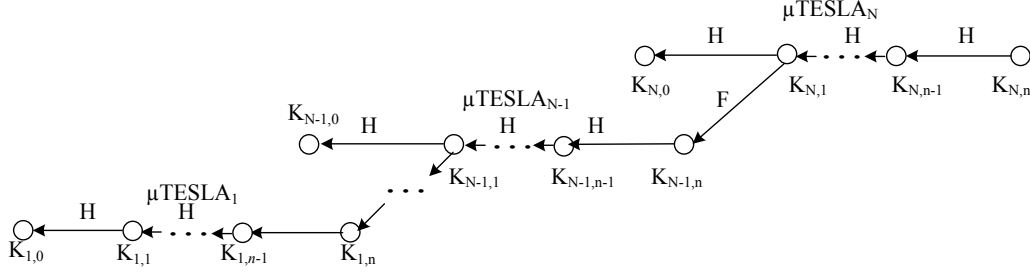
Figure B-1. Construction of µTESLA key chains of µTPC wherein each $K_{i,n}$ is derived from $K_{i+1,1}$ using pseudo random function F.
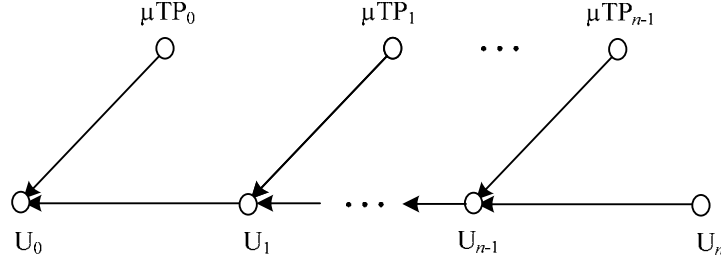

Figure B-2. Construction of µTPC where $U_i = H(U_{i+1}\|µTP_i)$.

B.2 Construction of µTPCT

Suppose m BNodes exist in sensor networks. For convenience, we assume $m = 2^k$ where k is an integer. Prior to deployment, BS pre-computes m µTPCs each of which is assigned a unique, integer-value ID between 1 and m. For purposes of presentation, we denote the j-th U value of i-th µTPC as $U_{i,j}$, j-th µTP as $µTP_{i,j}$, and i-th initial parameter (including $U_{i,0}$, ID_i) of µTPC as S_i. BS then computes $K_i = H(S_i)$ for all $i \in \{1,...,m\}$. Afterward, it constructs a Merkle tree using $\{K_1,...,K_m\}$ as leaf nodes. Each non-leaf node is computed by applying H to the concatenation of its children nodes. We call such Merkle tree as µTPCT (µTPC merkle hash Tree). Figure B-3 shows µTPCT with eight µTPCs, where $K_{12} = H(K_1 \| K_2)$, $K_{14} = H(K_{12} \| K_{34})$, $K_{18} = H(K_{14} \| K_{58})$, etc.
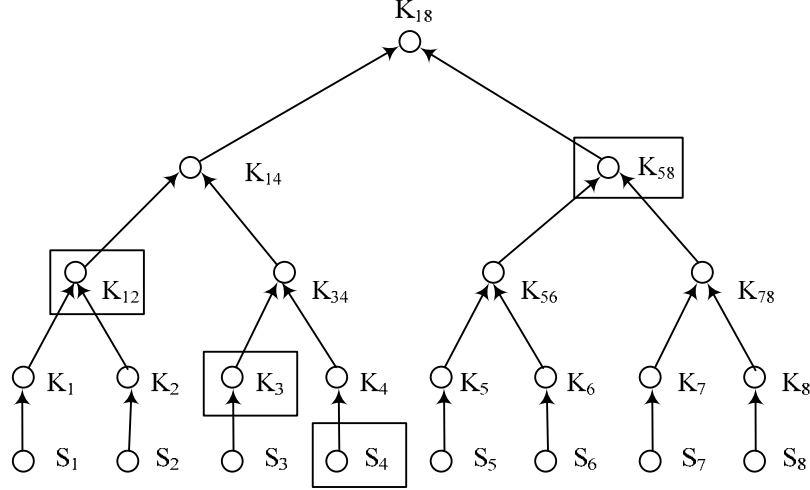
Figure B-3. µTPCT tree with 8 leaf nodes; the nodes in the boxes constitute the certificate of S_4 called PCert$_4$.

BS also constructs a parameter certificate for each µTPC instance. The certificate for the i-th µTPC instance consists of S_i as well as the values corresponding to the siblings of the nodes on the path from the i-th leaf node to the root of µTPCT. For example, the parameter certificate for the 4th µTPC instance in Figure B-3 is $PCert_4 = \{S_4, K_3, K_{12}, K_{58}\}$. For each BNode, which will use a given µTPC instance, BS distributes µTPC and corresponding parameter certificate to it. BS also pre-distributes the root of µTPCT to all potential receivers of broadcast messages.

Before the construction of µTPCT, if there are similar parts in all µTPs of some µTPCs, take the same parts of µTP together with the initial parameter of µTPC as leaf nodes to construct µTPCT. For example, if disclosure lag d and synchronization intervals T_{int} in all µTPs of μTPC_i are the same, take T_{int}, d together with the initial parameter of μTPC_i as leaf nodes to construct µTPCT. Accordingly, the same parts of µTP will be distributed together with the certificate of µTPC only once. In the process of µTP distribution, BNode needs to distribute the discrepant part only. This way, substantive communication cost will be saved.

B.3 Authenticated broadcast

The performance of authenticated broadcast protocol can be divided into the following five phases:

B.3.1 Protocol initialization

Prior to the deployment of sensor networks, BS builds µTinst (denotes the µTESLA instance), µTPC, and µTPCT according to the quantity and FP of all BNodes. Afterward, it distributes root R of µTPCT to RNode (Receiving Node).

B.3.2 Request for µTPC.

Before joining sensor networks, BNode sends request BREQ, which includes BNode's FP to BS. Afterward, BS searches for the compatible µTPC (e.g., μTPC_4 shown in Figure 3) according to the FP of BNode. Together with certificate $PCert_4$ and K_{gen} (denotes the generated key of the µTESLA key chain) of all µTinsts, BS sends µTPC back to BNode.

B.3.3 Authenticate BNode.

Before broadcasting, BNode publishes its certificate $PCert_4$ to all RNodes to prove its legitimacy. RNode uses R and equation $H(H(H(H(S_4) \| K_3) \| K_{12}) \| K_{58})=K_{18}$ to verify the validity of $PCert_4$. If it succeeds, RNode saves µTPC's initial parameter $U_{4,0}$, ID_4 in $PCert_4$ as well as the same parts of µTP in µTPC.

B.3.4 Distribute µTP.

After successful authentication, BNode creates the first µTESLA key chain according to K_{gen} of the first µTinst using hash function H. Afterward, BNode broadcasts $U_{4,1}$ and $\mu TP_{4,0}$ to RNodes. According to $U_{4,0}=H(U_{4,1} \| \mu TP_{4,0})$, RNode verifies the legitimacy of $\mu TP_{4,0}$. If it succeeds, RNode saves $U_{4,1}$ and $\mu TP_{4,0}$; otherwise, it is discarded. BNode then broadcasts $U_{4,2}$ successively. At the same time, BNode uses the 2nd K_{gen} to generate a second µTESLA key chain. After receiving $U_{4,2}$, RNode saves it and deletes $U_{4,0}$. To assure the reliability of the distribution, BNode will broadcast U repeatedly.

B.3.5 Authenticate broadcast message.

Once RNode gains $\mu TP_{4,0}$, based on $\mu Tinst_{4,0}$, RNode can authenticate all broadcast messages from BNode. Therefore, a broadcast authentication channel is created between RNode and BNode. When $2*T_{int}$ remains before the end of the life cycle of $\mu Tinst_{4,0}$ in the processing of broadcast authentication, the protocol will proceed to performing phase 4 subsequently. In other words, BNode broadcasts $\mu TP_{4,1}$. RNode verifies $\mu TP_{4,1}$ using $U_{4,1}=H(U_{4,2} \| \mu TP_{4,1})$. If it succeeds, RNode saves $\mu TP_{4,1}$; otherwise, it is discarded. Note that the protocol makes sure RNode can continue to authenticate the broadcast message of BNode in the life cycle of $\mu Tinst_{4,1}$. The later procedure of the protocol will repeat phase 5 until the end of the life of BNode.

ANNEX C

Authentication Mechanisms in Sensor Networks

(This annex does not form an integral part of this Recommendation | International Standard)
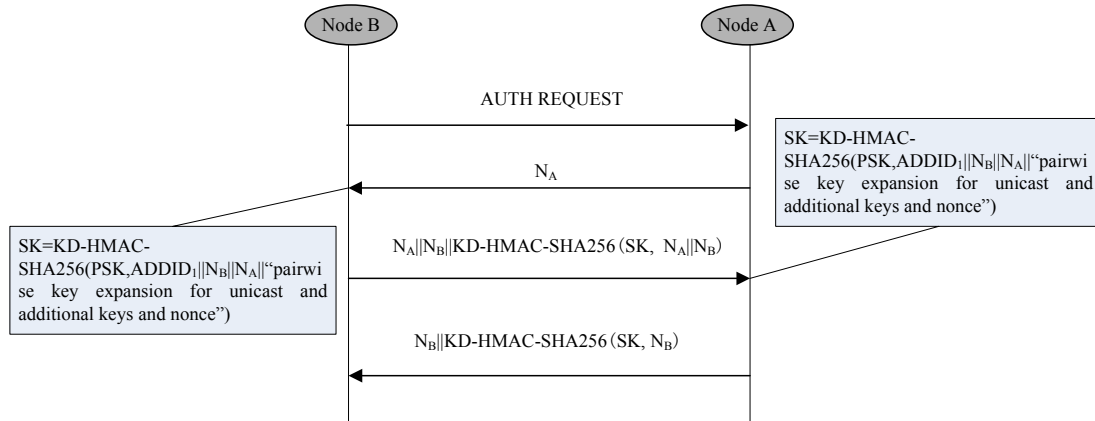
C.1 Preshared Key-based authentication

Figure C-1. Preshared Key authentication procedure

In the text below, PSK denotes the preshared key between A and B; "ADDID$_x$" is the concatenation of A's address and B's address. The mechanism is performed as follows:

Step 1: B sends an "AUTH REQUEST" message to A to start the authentication procedure.

Step 2: After receiving the message, A generates nonce N_A and sends it to B.

Step 3: B generates nonce N_B and calculates session key SK=KD-HMAC-SHA256(PSK,ADDID$_1$||N$_B$||N$_A$||"pairwise key expansion for unicast and additional keys and nonce") and message authentication code MAC$_1$=KD-HMAC-SHA256(SK, N$_B$||N$_A$), and then sends MAC$_1$,N$_B$ and N$_A$ to A.

Step 4: A checks N_A first, and then calculates SK=KD-HMAC-SHA256(PSK, ADDID$_2$||N$_B$||N$_A$||"pairwise key expansion for unicast and additional keys and nonce") and MAC$_2$=KD-HMAC-SHA256(SK, N$_B$||N$_A$). If MAC$_1$= MAC$_2$, A sends MAC$_3$=KD-HMAC-SHA256(SK,N$_B$) and N$_B$ to B.
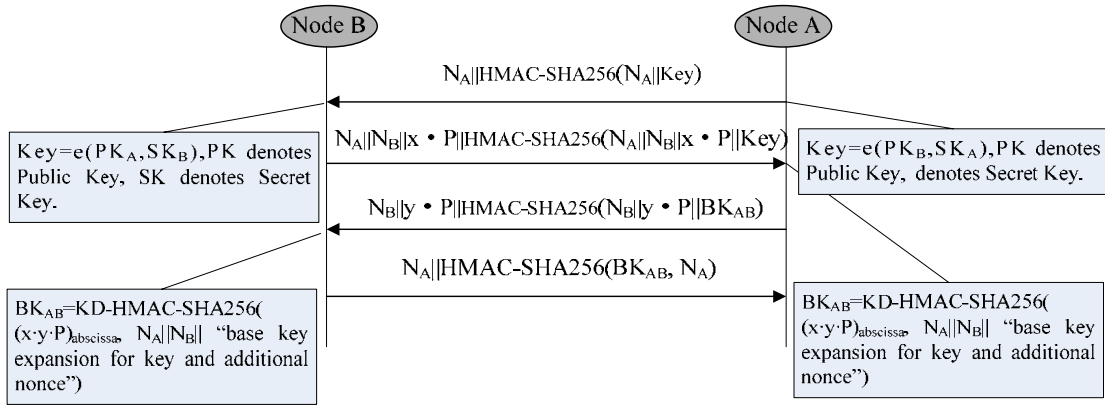
C.2 ID-based authentication (1)

Figure C-2. ID-based authentication procedure (1)
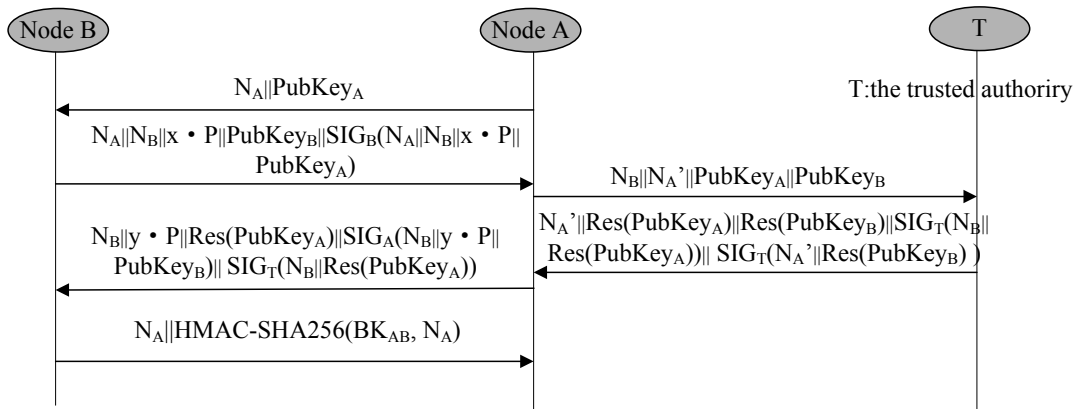
C.3 ID-based authentication (2)

Figure C-3. ID-based authentication procedure (2)

In the text below, $PubKey_X$ denotes the public key of X. SIG_X refers to the signature of X. Res ($PubKey_X$) denotes the result of verification of $PubKey_X$. The mechanism is performed as follows:

Step 1: A generates random number N_A and sends $N_A||PubKey_A$ to B.

Step 2: B generates temporal secret key x and temporal public key x·P for ECDH, and then sends $N_A||N_B||x·P||PubKey_B||SIG_B(N_A||N_B||x·P||PubKey_A)$ to A.

Step 3: After receiving the message from B, A generates another random number N_A' and sends $N_B||N_A'||PubKey_A||PubKey_B$ to T.

Step 4: Upon receiving the message from A, T inspects the validity of $PubKey_A$ and $PubKey_B$ and sends $N_A'||Res(PubKey_A)||Res(PubKey_B)||SIG_T(N_B||Res(PubKey_A))||SIG_T(N_A'||Res(PubKey_B))$ to A.

Step 5: After receiving the message from T, A verifies N_A' first followed by

$SIG_T(N_A'||Res(PubKey_B))$ by checking if N_A' agrees with the one sent to T. Afterward, A generates temporal secret key y and temporal public key y·P for ECDH, calculates BK_{AB}=KD-HMAC-

SHA256$((x \cdot y \cdot P)$abscissa and NA||NB|| "base key expansion for key and additional nonce"), and sends N_B||$y \cdot P$||Res(PubKey$_A$)||SIG$_A$(N_B||$y \cdot P$||PubKey$_B$)|| SIG$_T$(N_B||Res(PubKey$_A$)) to B.

Step 6: B verifies N_B first, then verifies SIG$_T$(N_B||Res(PubKey$_A$)) and SIG$_A$(N_B||$y \cdot P$||PubKey$_B$) by checking N_A and N_B, respectively. Afterward, B calculates Base Key BK$_{AB}$=KD-HMAC-SHA256$((x \cdot y \cdot P)$abscissa and NA||NB|| "base key expansion for key and additional nonce"). Based on BK$_{AB}$, B calculates MAC= KD-HMAC-SHA256(BK$_{AB}$, N_A), and then sends it with N_A to A. A verifies MAC from B based on BK$_{AB}$.

ANNEX D

Bibliography

(This annex does not form an integral part of this Recommendation| International Standard)

- [b-Y.2221] Draft Recommendation Y.USN-reqts, "Requirements for support of ubiquitous sensor network (USN) applications and services in NGN environment" January 2010.

- [b-SPINS] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, SPINS: *Security Protocols for Sensor Networks*

- [b-Chan] Haowen Chan and Adrian Perrig, *Security and Privacy in Sensor Networks.*Compuer, pp/99-101, October 2003.

- [b-Karlof] C. Karlrof, D. Wagner, *Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,* Elsevier, pp.293-315, 2003.

- [b-Akildiz] I.F.Akildiz, W.Su, Y. Sankarasubramaniam, and E.Cayirci, *A Survey on Sensor Networks*, IEEE, pp.102-114, August, 2002.

- [b-TESLA] A.Perrig, R.Canetti, J.D.Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in proceeding of IEEE symposium on Security and Privacy, Berkeley, CA, USA, 2000, pp.56-73.

- [b-ISO/IEC SGSN N049]   Technical Document of ISO/IEC JTC 1 Study Group on Sensor Networks (SGSN)

- [b- RFC 4082] A. Perrig, D. Song, R. Canetti, J. D. Tygar and B. Briscoe, "Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction," IETF RFC 4082, June 2005.

- [b-FIPS PUB 140-3] Revised Draft on FIPS PUB 140-3, Security Requirements for Cryptographic Modules, USA NIST, September 2009

- [b-ITU-T F.744]   Service description and requirements for ubiquitous sensor network middleware, December 2009

_____