ISO/IEC JTC 1 N 9070

2008-05-16

ISO/IEC JTC 1
Information Technology

Document Type:	**Other Document(Defined)**
Document Title:	**System Architecture and Standard Framework for Sensor Networks for consideration at the 1st SGSN Meeting, 26-27 June.**
Document Source:	**SGSN Convenor**
Reference:	
Document Status:	**This document is circulated to JTC 1 National Bodies for information**
Action ID:	**Information**
Due Date:	
No. of Pages:	**10**

Secretariat, ISO/IEC JTC 1, American National Standards Institute, 25 West 43rd Street, New York, NY 10036; Telephone: 1 212 642 4932; Facsimile: 1 212 840 2298; Email: lrajchel@ansi.org

ISO/IEC JTC 1
Study Group on Sensor Networks

Document Number:	SGSN N011
Date:	2008-05-15
Replace:	
Document Type:	National Body Contribution
Document Title:	System Architecture and Standard Framework for Sensor Networks
Document Source:	National Body of China
Document Status:	For consideration at the 1st SGSN Meeting, 26-27 June.
Action ID:	FYI
Due Date;	
No. of Pages:	9

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

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

System Architecture and Standard Framework for Sensor Networks

China NB

ISO/IEC JTC1/SGSN

This contribution suggests architecture and standard framework of sensor networks for SGSN.

Sensor networks consist of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. In addition to one or more sensor nodes, each node in sensor networks is typically equipped with a radio transceiver or other wireless communication devices, a microcontroller, and an energy source, usually a battery.

Sensor networks are the connection between physical world and mankind, which cannot be simply regarded as communication networks. It should mainly concentrate on sensory information processing and services. Sensor networks should be developed as an integrated information infrastructure, in which information aggregation and collaborative processing are key issues.

1. Architecture of Sensor Networks

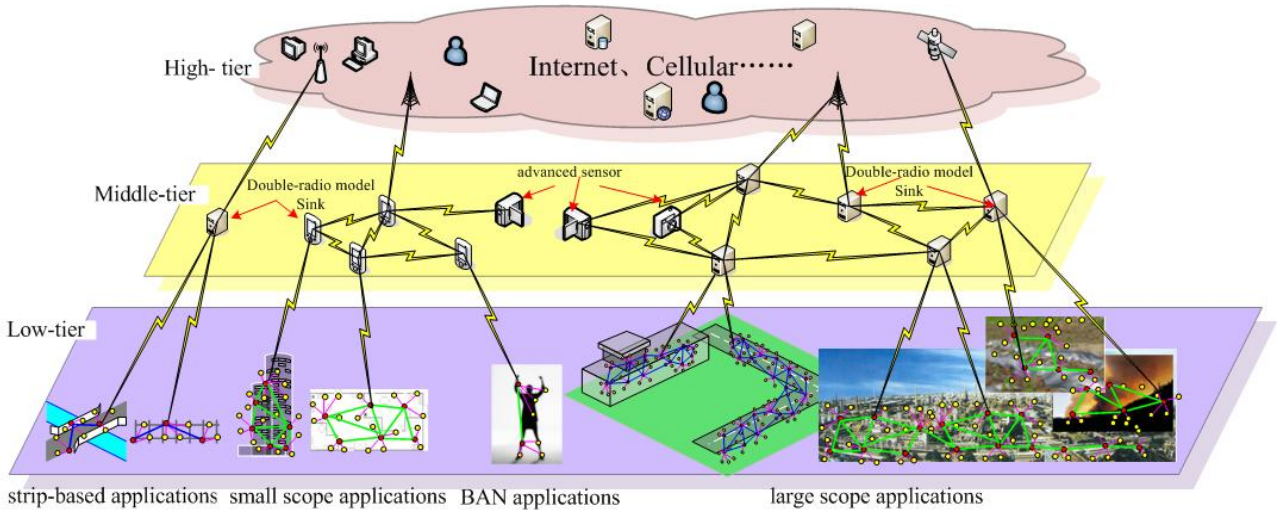

Figure 1 Architecture of Sensor Networks

As the key feature of sensor network applications, the diversity of sensors, data flow and QoS requires the system architecture be of compatibility, universality and scalability to meet the various requirements.

The prevailing studies on sensor networks focus on the solution of low data rate, short message burst, low network traffic and low device cost issues. ITU, ISO, IEEE and other standardization organizations have been working on the standards of

PHY/MAC layers, network protocol, identifier and sensor interfaces, however the completed solutions on various applications have not been found out.

I In sensor network applications, such as anti-intrusion, public security, and environment monitoring, various sensors have to work cooperatively, while the current solution like Zigbee cannot meet the requirements. For instance, with the concern on longevity and QoS requirements, the cooperative monitoring on the same target by the combination of video, vibration, sound and other sensors cannot be achieved by Zigbee.

Due to the network scale, node resource and heterogeneity, the sensor networks cannot always directly access to Internet or other communication systems without sink or gateway.

The main purposes of sensor networks are information sensing and processing. Thus, the information cooperative processing scheme in sensor networks must be considered in the architecture design.

As analyzed above, the three-tier architecture for sensor networks is proposed as showed in Figure 1.

The low-tier is primarily concerned on the solutions of various requirements of network interconnection of sensor nodes with lower data flow and longer life time, and data transmitting between sensor nodes and sinks with clustering and multi-hop. Several standards can be constituted to deal with speciality and commonality of applications.

The middle-tier sensor networks concern on the network interconnection of sinks, gateways and the sensor nodes with higher data flow and less resource constraints. It mainly serves as the solution for the information aggregation and larger range coverage in different applications.

The high-tier sensor networks take advantage of the existing networks to bear the applications of sensors networks and information services.

2. Standard Framework of Sensor Networks

Due to the diversity of sensor network applications, the trade-off between the speciality and universality should be carefully considered.

The standard framework of sensor networks can be divided into two parts: the fundamental platform standards and the application profiles. Based on the common characteristics and technology requirements for different sensor network applications, the fundamental platform standards consist of a series of standard function modules, including terms, interface, communication and information exchange, collaborative information processing, information services, security and testing. According to the speciality of specific applications, the application profiles are intended to describe various application modes, scenes, functions, node deployment and so on. It

customizes different function modules from the fundamental platform standards in order to establish a complete system. Figure 2 shows the standard framework of sensor networks.

Standard Framework of Sensor Networks

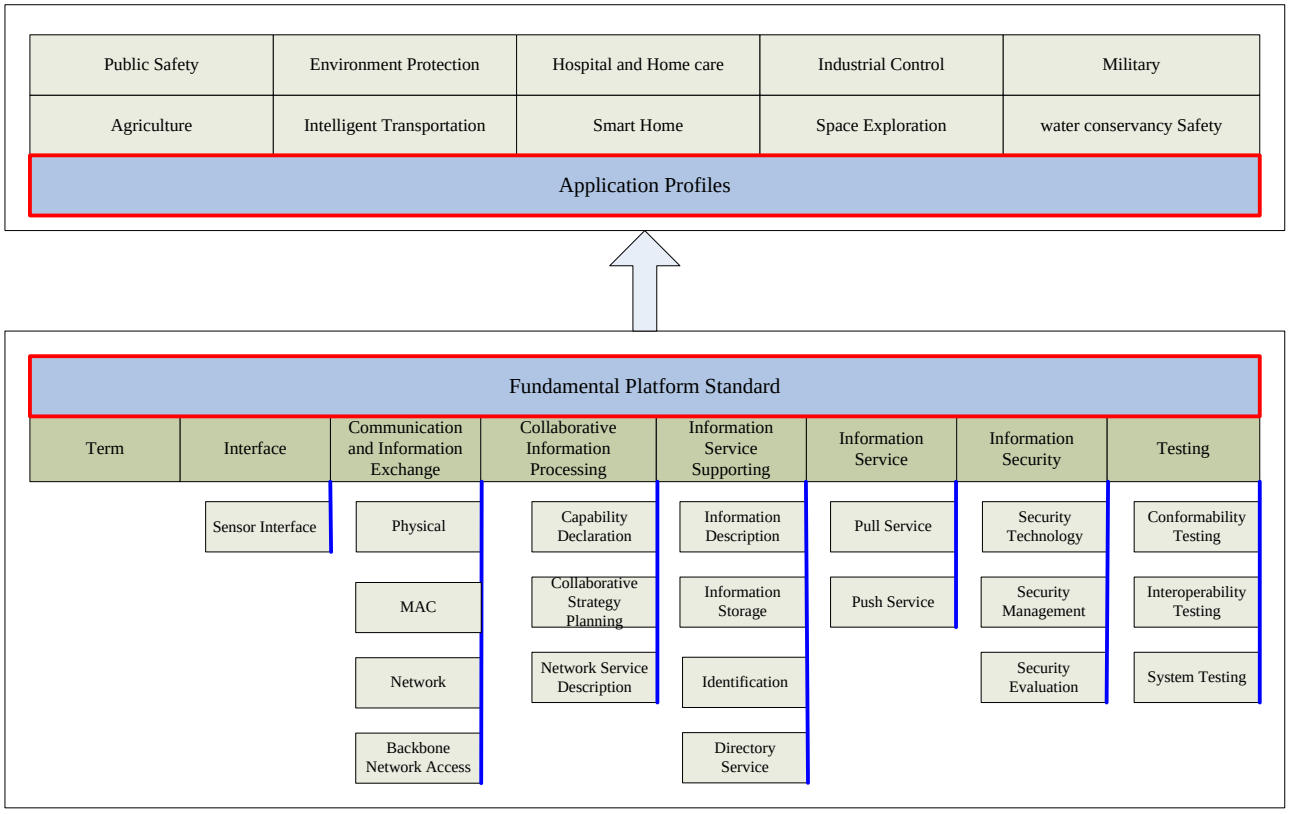

Figure 2 Standard Framework of Sensor Network

2.1 Fundamental Platform Standard

2.1.1 Terms:

The ambiguous key words in sensor networks require the discussion to give them the clear definition. This specification could be a part of ISO/IEC 2382 (Information Technology Vocabulary) serial standards.

2.1.2 Sensor Interface:

Due to the diversity interfaces of various sensors, the standards need to be developed to gather the information among sensors, including analog and digital sensors and some interface protocols. Many analog and digital interfaces are widely used, such as 4-20mA, 0-5V, SPI, RS232, and etc. At present, there exist some intelligent sensor interface protocols, such as IEEE1451.x protocols and OGC sensor Web interfaces.

2.1.3 Communication and information exchange:

From the viewpoint of network, standards for physical layer, MAC layer, network layer and access to backbone network should be established. Network protocols for sensor networks need to be self-organizing, self-configurable, robust, and scalable.

Physical Layer

Physical (PHY) layer is the fundament and infrastructure of the reliable and real-time data transmission in sensor networks. Upon the basis of three-tier system architecture, the PHY layer standards for low-tier and middle-tier should be designed to meet the requirements of various services and applications, respectively. The PHY layer of low-tier can provide short distance and low data rate transmission with ultra-low average power under various indoor and outdoor communication environments. The current standards like IEEE 802.15 series were not designed to support complicated applications like outdoor and mobile environment etc. While the PHY layer of middle-tier should satisfy the requirement of the longer distance and the higher data rate under complicated environments. Therefore, the PHY layer of sensor networks should be further considered.

MAC Layer

Sensor networks serve for diverse applications from low to high data rate. Medium access control (MAC) protocol plays a key role in determining channel capacity utilization, throughput, congestion, fairness, network delays and power consumption, etc. The low-tier and middle-tier MAC layer should emphasize on different network aspects.

Network Layer

Topology and routing are the main tasks of sensor networks. Time synchronization and localization also need to be considered.

Topology in sensor networks ensures network connectivity and efficiency, such as mesh, cluster, strip-based, etc. Efficient collaborative sensing among adjacent nodes should be considered in the design of the network layer protocol. Time synchronization and localization may be requested to support these requirements. Generally, the network layer needs to support efficient gathering, dissemination, and storage of network state information. The difference and interconnection between low-tier and middle-tier network layer must be taken into account.

Access to backbone network

The autonomous sensor networks generate contents to satisfy the needs of backbone network like Internet or mobile network, etc. The high-tier focuses on protocol translation from low-tier or middle-tier.

2.1.4 Collaborative Information Processing

The key difference between traditional telecommunication infrastructures and sensor network based information service system is that sensor network based information service system collects low-level sensory data, extracts application-specific information from these sensory data, and tries to obtain high-level knowledge about physical world. Usually both spatial and temporal information are essential to sensor network based information service system.

Sensor network based information service system can be conceptually clarified from two perspectives: information service user perspective and information service provider perspective. Information service user defines its requirements with task specification entity. Requirements may vary significantly in different application scenarios. In Information service provider perspective, information processing is the main concern in designing information service provider framework.

Indeed, information processing itself acts as network service user and can use data transmission service provided by network service provider.

Collaborative information processing (CIP) is one of the key issues in information service provider perspective for distributed sensor network based information service system. Integrated with other issues such as sensory information description, sensor identification and sensory information storage, CIP concerns on how to resource-efficiently fulfil dynamic tasks specified by information service users. Though different sensor network application scenarios normally require scenario-specific services, collaboration is an indispensable requirement for senor network based information service to handle constraints in energy, computing, storage and communication bandwidth. To information service provider, it also has to deal with technical challenges from issues such as task dynamics, measurement uncertainty, node mobility and environmental changing. Hence, collaborative information processing (CIP) is an essential standardization item to be considered in defining architectural framework for sensor network based on information service.

CIP can be modelled with three distinct entities, which is named as capability declaration entity (CDE), collaborative strategy planning entity (CSPE) and network service description entity (NSDE). Functional relationships among these entities are shown in figure 3.

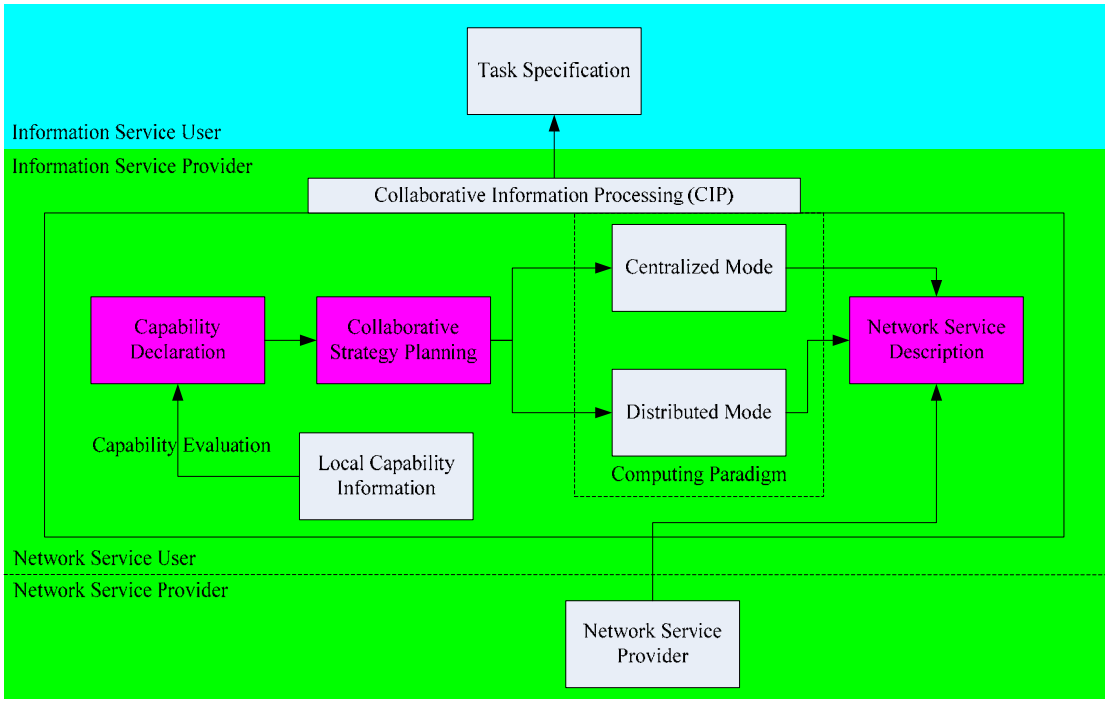

Figure 3 Collaborative Information Processing

Capability declaration entity (CDE) declares capabilities of one sensor node to other nodes. Capabilities include not only individual node information on sensing modality configuration, sensing range, residual energy, storage and communication bandwidth etc., they also include certain characteristic information of sensory data collected by individual sensor node. One of representative characteristics on sensory data is signal-to-noise ratio (SNR) value. In other words, one sensor node should qualify itself to be a CIP participant before any actual CIP procedure is triggered. CDE requires a preliminary local capability evaluation process which uses local capability information.

Collaborative strategy planning entity (CSPE) is the second and probably the most important entity in CIP. CSPE uses available information provided by CDE and forms global or regional maps or scopes on signal and information processing problems. With certain cost functions or utility measures, CSPE tries to find a resource-efficient solution to collaborative strategy planning

problem, with which the best information processing performance can be achieved at the same time. Two computing paradigms can be used in the implementation of resulting solution from CSPE. One is centralized computing paradigm; the other is distributed computing paradigm.
The interface entity between information service and network service is network service description entity (NSDE). NSDE defines languages or protocols and describes definitely what network service provider should do in order to fulfil information processing tasks.

2.1.5 Information Service Supporting

Information description

Several kinds of specific information communicated among the nodes in the sensor network should be defined and described exactly by the standards. The defined information is the basic requirement for the interoperability for the sensor network. The information could be described based on some existed description language or notation, such as ASN.1 (ISO/IEC 8824 and ISO/IEC 8825serial standards) and XML (W3C XML) specification.

Information Storage

The storage of sensor networks targets storage-constrained sensor network applications, in which the monitored data is typically stored in adaptable resolution fashion. This allows reclamation of some storage space when needed by reducing the quality of stored data while sacrificing some of the precision. Compression of sensor readings, correlation of sensor readings, and detection and cueing of events are three important areas in information storage.

Identifier

Some different kinds of identifiers should be defined by the specifications for sensor network, such as the sensor node identifier, sensor node type identifier, information identifier, information type identifier, application type identifier. The identifier could be specified based on the existed identifier standards, such as OID (ISO/IEC 9834 serial standards), URI (RFC 3986), URN(RFC 2141).

Directory

The information among the nodes in the sensor network should be assigned in the database by the suitable directory which is important for finding the information more easier. The directory specification for the sensor network could be based on Directory (ISO/IEC 9594 serial standards).

2.1.6 Information Service

Information Services provided by sensor networks can be basically classified into two classes: Pull service and Push service. Pull service refers to a top-down service mode in which service users proactively initialize requests while sensor networks provide related information and fulfil specified tasks in case of the requests. Typical Pull services include information query, data mining and information task assignment etc. In Push service, sensor networks either regularly or occasionally transmit environment and target information to service users and actuators according to a set of predefined conditions and rules. Pull service provides a down-top service, and event detection, target tracking and autonomous controlling are representative Pull service.

2.1.7 Security

Security is of extreme importance for many of the proposed applications of sensor networks.

Because of their unique properties, most notably limited resources and physical exposure of sensor nodes, sensor networks require a new type of security protocols. These protocols are tailored to the underlying system architecture, patterns of network traffic, and specific security requirements so that security-related resource consumption is minimized. Physical exposure of nodes, as well as the threat that their cryptographic secrets are potentially available to an adversary, demands that security protocols in sensor networks protect the integrity of the network even if cryptographic secrets are compromised.

Security technology

The security technologies of sensor networks mainly focus on distributed key management, security route protocols (such as DSDV, DSR, and SEAD), node cooperation and selfishness, malicious power consumption, and intrusion detection model.

Security management

Referring to standard IEC 17799, security management of sensor networks also meets following requirements: easy deployment and application, reducing manual operation, maximum battery life, using existed security technology of encryption and authentication, using existing security standards.

Security evaluation

It is helpful for the system owner to perform security evaluation to ensure the security of sensor network activities, before selecting the specific devices, analyzing security requirements, constructing, rebuilding and running sensor networks, connecting to Internet.

2.1.8 Testing

There are different kind of testing should be considered in sensor network, including Conformance testing, interoperability testing, and systems testing.

Conformance Testing

Conformance testing is to confirm the consistency of Implementation Under Test (IUT) and standard. The general approach is comparing actual and expected output of a black box test using a group of test case sequence under specific network condition. The existing test methods are ISO/IEC 9646 series.

Interoperability Testing

Interoperability testing is to confirm whether a required functionality is supported by the target equipment. The test is accomplished by evaluating the correctness of protocol standard specified interoperation between target implementation and the connected relative implementation under network interoperating environment. Interoperability testing provides important interconnection information, and is commonly used as testing between multiple manufacturers during R & D stage or the model selection test for system runners.

System Testing

System testing includes physical interconnection test, planning verification test, evaluation and test of reliability and usability, performance test, flow measurement and modelling of network systems, etc.

2.2 Application Profiles

Sensor network application profiles specify application domains. Each profile defines requirement descriptions and set of processing actions for each application. It can provide simplicity and reliability for the end user and consumer flexibility for products. For example, the application profile in subway station security monitoring network should define types of sensor deployed (explosive, poisonous gas, etc), mounting places, node quantity, information publish mode, function and parameter set, etc.