Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N13935
Date:	2009-04-29
Replaces:	
Document Type:	Outgoing Liaison Statement
Document Title:	Liaison statement from JTC 1/SC 6 to JTC 1/SGSN
Document Source:	Proxy liaison representative from SC 6 to SGSN
Project Number:	
Document Status:	For your information.
Action ID:	FYI
Due Date:	
No. of Pages:	44

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

Reply to Liaison Statement from JTC 1 SGSN to JTC 1 SC 6

ISO/IEC JTC 1/SC 6

This is reply to Liaison Statement from JTC 1 SGSN to JTC 1 SC 6 (N13897).

Current works of SC 6 on sensor network:

There are two ongoing works on sensor network in SC6. In last Montreux meeting November 2008, SC6 has established new projects which are ISO/IEC 29180 and ISO/IEC 29182.

ISO/IEC 29180

ISO/IEC 29180 for "Security framework for sensor networks" is a common text project with ITU-T Q.6/17 which develops [X.usnsec-1] for "Security framework for USN". This standard describes security threats and security requirements to sensor network. In addition, this standard categorizes security technologies by security functions that satisfy above security requirements and by the place to which the security technologies are applied in the security model of sensor network. SC6 approved advance authorization for a CD ballot on ISO/IEC 29180 from WG7 interim meeting in February 2009. [X.usnsec-1] is expected to reach consent in September at the meeting 2009 and to be published as an ITU-T Recommendation in 2009. See attachment 1.

ISO/IEC 29182

ISO/IEC 29182 for "Reference architecture for sensor network applications and services" was started from November 2008. This standard specifies the reference architecture for sensor network applications and service and covers the following in network and transport layer:

- Requirements analysis of sensor network applications and services
- Identification of the network functionalities required by different sensor network applications
- Reference architecture for sensor networks functionalities supporting various sensor network applications and services
- Specification of interfaces for sensor network functionalities supporting sensor networks

The first WD was released to SC6 in March 2009 and will be discussed in Tokyo meeting, June 2009. See attachment 2.

Future works of SC6 on sensor network:

Sensor network applications and services are emerging at the moment. Their situational and context-aware information and knowledge will add more values and can provide more business opportunities to sensor-integrated applications and services which could be established in manufacturing and industrial fields; military; health care; environmental control and utility use management; civil engineering; precision agriculture; transportation; and so on.

So sensor networks and relevant applications/services have many technical issues to be considered.

Liaison statement from SGSN shows standardization areas which are possible to SC 6. They can be summarized as bellows;

- Requirement analysis
- Reference architecture
- Sensor Interfaces
- Data type and data interface
- Communication
- Mobility support
- Network management
- Information service supporting
- Quality of Service (QoS)
- Middleware
- Security & Privacy

In addition to ISO/IEC 29180 and ISO/IED 29182, SC6 considers that following work items are urgent and should be started as new projects as soon as possible;

- Requirements Analysis
  - Requirements analysis is a starting point to extract service features and required functions from various sensor network applications and services. Sensor network applications have the vertical market characteristics and many functional capability requirements may be clarified by analyzing sensor network applications and services. Therefore the following studies should be done:
    - → Analysis of sensor network application models and scenarios;
    - → Analysis of service requirements and functional capability requirements in terms of PHY/MAC, sensor networking aspects, inter-networking aspects, and application layer issues; and
    - → Analysis of further development and relevant standardization items.
- Reference architecture
  - This is on-going work item as ISO/IEC 29182 under SC 6 / WG 7
- Application profiling
  - Application profiling specifications are required. Since sensor network applications have vertical market characteristics and each sensor network application may have unique requirements, a type of sensor network applications and services needs an application profile to define service features, processing functions, interface procedures, operation attributes, attribute values, etc.
  - Convergence of services will require sensor node to interact with various service environments such as multimedia. Application profiling should consider sensor

network services that can support cooperative services with other service infrastructures.

- Wireless sensor network PHY/MAC
  - IEEE 802.15 focuses on the development of consensus standards for Personal Area Networks or short distance wireless networks. These WPANs address wireless networking of portable and mobile computing devices such as PCs, Personal Digital Assistants (PDAs), peripherals, cellular phones, pagers, and consumer electronics; allowing these devices to communicate and interoperate with one another.
    IEEE 802.15 alternatives have been adopted widely for wireless sensor networking technologies. But they had lack of considerations on outdoor sensor network applications which have different operation conditions such as difficulty in maintenances, long-chained network in tunnels or brigdes, interference by moving cars on the street and seasonal changes in mountains, etc.
  - Thus, other alternatives may have to be developed to support outdoor sensor network applications. SC 6 is required to tackle this new challenge.
    - → ISO/IEC 29157 is an alternative PHY/MAC that can support sensor network applications and multimedia applications. See attachment 3.
- Non-IP sensor networking
  - Wired sensor networks have fewer limitations in terms of power, bandwidth, etc. than wireless sensor networks. So they can be established based on IP. But wireless sensor networks have more limitations and IP-based wireless sensor networking might not provide many benefits compared to non-IP wireless sensor networking.
  - ZigBee is a typical non-IP wireless sensor networking and application platform based on IEEE 802.15.4. TinyOS is just a tiny operating system software for sensor nodes but can enable a wireless sensor network based on IEEE 802.15.4 with adopting multi-hop routing capability, management functions and various open-source application modules. That is, TinyOS can support another wireless sensor networking capability. Proprietary sensor networking technologies also are possible and can be adopted into the sensor networks market. AMR (Automatic Meter Reading) is not far from a sensor network application.
    What kinds of non-IP sensor networks can be established and how they are maintained and inter-worked with IP and telco networks and application systems need to be clarified to pursue impacts on telecommunication network infrastructure.
  - SC 6 will be able to develop its own standards package for a solution of non-IP sensor networking and application systems and moreover it is required to consider how to integrate various non-IP solutions and interwork each other.
- IP sensor networking
  - The IP-based sensor network can be an alternative because it can provide a few better benefits such as the End-to-End communication capability, mobility support, robust network management, reuse of existing IP network resources, etc.
    IETF 6LoWPAN WG covers only IPv6-based wireless networking issues. But, it is said that IPv4 could be an alternative since IPv4 could provide enough payload size in some sensor network applications while IPv6 couldn’t support it due to much bigger header size.

  - Moreover implementation profiles for IP networking standards and application- and service-perspective issues such as directory service, application profiling, middleware functions, etc. should be taken into account.

- Routing
  - As sensor networks have specific requirements on energy saving, data-oriented communication, sensor network-dedicated routing protocols may be required such as energy efficient routing scheme and data-aware routing scheme
  - Reducing transmission distance into one half using Ad-hoc relay makes transmission powers lessen into one eighth. This guarantees that overall power consumptions are decreased even if relay sensor node is applied which increases power consumption in double. Therefore it is necessary to develop MAC supporting Ad-hoc relay.
- Data delivery/distribution
  - Sometimes wireless communication protocol used in sensor network can raise data loss problem for many reasons such as congestion, RF interference, multi-path and Routing problem.
  - Because sensor data may be time critical to most sensor network applications, it is necessary to develop reliable and real-time sensor data delivery/distribution protocols to overcome data loss problems.
- Mobility support
  - Sensor networks can be involved with four mobility issues: a sensor node moves within a sensor network scope, called an intra-network mobility; a sensor node moves across multiple sensor networks, called an inter-network mobility; a sensor network itself moves across other sensor networks, called a network mobility; and a sensor network service moves across other service domains, called a service mobility.
  - A typical example of these mobility cases can be found at hospitals. Several sensors might be attached to a patient, resulting in a body area sensor network, and he might be moved to several medical examination rooms. Various mobility cases might occur herein. How those requirements are satisfied will depend on sensor networking technologies. That is, IP-based sensor networks can be helped by existing IP mobility technologies which have been developed at IETF. But non-IP based sensor networks have lack of studies yet on various mobility issues.
  - SC 6 can evolve existing IP mobility technologies to be tailored to fit requirements of sensor networks and has to develop mobility-supporting protocols for non-IP based sensor networks.
  -
- Network management
  - A sensor network may be built in IP-based and non-IP-based ways. Each type may build its own management architecture based on a specific management protocol. For example, ZigBee networks are established without IP, but 6LoWPAN networks are based on IP, especially IPv6. There two different management schemes such as ZigBee Network Layer Management and SNMP are applied each to them.
  - This issue will include a sensor node identification scheme because a unique identifier needs to be assigned to each sensor node for management purposes.

- QoS
  - Mission-critical applications and services among them should be carefully managed. QoS will be a key technical issue. So, non-IP- and IP-based sensor networks should exploit how to support QoS control capabilities. Existing QoS mechanisms haven't take into account sensor network requirements. A new protocol solution for QoS may be needed or existing solutions may be modified and/or extended.
- Directory service
  - So far, there are two directory service issues in sensor network. First, a globally unique identifier might be assigned to every sensor node for management or other purposes. So every association between identifiers and relevant information should be maintained by a directory service. The other is related to information service directory.
  - SC 6 is interested to study these two directory service issues.
- Middleware functions
  - A set of relevant standards need to be developed for middleware functions such as sensor information gathering, filtering by various policies and rules, data comparison and analysis, data mining, context modelling language, context-awareness processing, context-aware decision and estimation, integrated management of sensor information, service integration, and so on.
  - SC 6 considers this topic as an urgent standard work item.
- Security of sensor network applications and services
  - This is on-going work item as ISO/IEC 29180 under SC 6 / WG 7

Attachment 1

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

STUDY GROUP 17

TD 0162

English only

Original: English

Question(s): 6/17 Geneva, 11-20 February 2009

TEMPORARY DOCUMENT

Source: Editors of X.usnsec-1

Title: Proposed second draft text of Recommendation X.usnsec-1 : Security framework for ubiquitous sensor network

Abstract

In February 2009 SG17 meeting, the contribution C052 was presented and discussed in Q.6/17 meeting. This TD is output result to reflect the comments in the meeting and the comments in TD 0022 from ITU-T SG13. The meeting approved this TD to be its second draft text.

The modifications to C052 were made as follows;

- The “WSN” is replaced by “SN” and the “wireless sensor network” is replaced by “sensor network” in whole draft;
- The “capabilities” is replaced by “requirement”, accordingly, the word “capability” is deleted from all requirement items in clause 11;
- To reflect the first comment in TD22, one communication pattern, i.e., communications among a cluster of defined sensor nodes, is added in clause 6;
- To reflect the second comment in TD22, the normative reference of Y.2701 is added;
- To reflect the third comment in TD22, final sentence in paragraph 3.2.1 was deleted and the definition on credential which is an improved version to X.800 developed by Q.15/13 was used;
- To reflect the fourth comment in TD22, the first two requirements in clause 11.1 are updated;
- To reflect the fifth comment in TD22, the fifth requirement in clause 11.1 was updated;

ITU-T draft Recommendation X.usnsec-1

Security framework for ubiquitous sensor network

Summary

This draft Recommendation describes security threats and security requirements to the Ubiquitous Sensor Network. In addition, this draft Recommendation categorizes security technologies by security functions that satisfy above 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 requirements and security technologies are presented for the Ubiquitous Sensor Network.

Keywords

Security framework for Ubiquitous Sensor Network, Sensor Node Compromise, Secure Data Aggregation, Pair-wise key establishment, Group-wise key, Authenticated Broadcast Message

Content

1 Scope

Recent advancement of wireless based communication technology and electronics makes the low-cost, low power sensor network feasible. Basically USN consists of two parts: sensor network being composed of a large number of sensor nodes and the application server controlling the sensor node in the sensor network or collecting 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 at anywhere and anytime, where the information and knowledge is developed by using context awareness with detecting, storing, processing and integrating situational and environmental information gathered from sensor tags and/or sensor nodes affixed to anything. Since there are many threats in transferring the information in USN, appropriate security mechanisms are needed to protect against those threats in USN.

This draft Recommendation describes security threats and security requirements to the Ubiquitous Sensor Network. In addition, this draft Recommendation categorizes security technologies by security functions that satisfy above 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 requirements and security technologies are presented for the Ubiquitous Sensor Network.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is published regularly. A reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.800]	ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems*
[ITU-T X.805]	ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*
[ITU-T X.1111]	ITU-T Recommendation X.1111 (2007), *Framework for security technologies for home network*
[ITU-T Y.2701]	ITU-T Recommendation Y.2701 (2007), *Security Requirements for NGN Release 1*

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms 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 Authentication [ITU-T X.800]: See Data Origin Authentication and Peer-Entity Authentication.

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

3.1.4 **Actuator**[]: a device that changes a measureable physical property in response to an electrical signal.

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

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

3.1.7 **Data Origin Authentication [ITU-T X.800]:** The corroboration that the source of data received is as claimed.

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

3.1.9 **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.

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

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

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

3.1.13 **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.

3.1.14 **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.

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

3.1.16 **Sensor[ ]**: a device that generates an electrical signal which represents a measureable physical property.

3.1.17 **Sensor network**[]: a collection of two or more sensor-network nodes and one or more sensor-network controllers interacting with each other in a single network.

3.1.18 **Sensor-network controller**[]:a processing system that can receive sensor data from sensor-network nodes, send electrical signals to actuators in sensor-network nodes, and send control signals to sensor-network nodes.

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

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

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

Editors' note: the definition is from the Y.USN-reqts, the ongoing work in SG13. contributions are invited to enhance the definition (e.g. context awareness, anyone at anywhere and anytime)

3.1.22 USN middleware: The common application platform to support various functions on behalf of various USN applications and services to control heterogeneous sensor networks, provide basic query processing, and provide high-level integrated services(context-aware processing, event processing, sensor data mining, integrated sensor data processing)

Editors' Note: the definition is from the F.usn-mw, the ongoing work in SG16. Contributions are invited to enhance the definition

3.2 Terms defined in this Recommendation

This document defines the following terms:

3.2.1 Bootstrapping: It refers to a process to establish a security association between the sensor nodes which may have been initialized with key information, enabling the sensor node to securely communicate with other sensor node after deployment of sensor nodes.

3.2.2 Credentials: It refers to an identifiable object that can be used to authenticate the claimant is what it claims to be and authorize the claimant's access rights.

3.2.3 Group-wise key: It refers to a key which is used to protect a multicast communications among a set of sensor nodes over a shared wireless link.

3.2.4 Pair-wise key: It refers to a key which is used to protect unicast communication between a pair of sensor nodes over a single wireless link.

3.2.5 Secure data aggregation: It refers to an in-network process which is performed on the aggregator node to securely transfer the aggregation value to sink node 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, then aggregator calculate the encrypted aggregator results by 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.

4 Abbreviations and acronyms

This contribution uses the following abbreviations:

DDoS – Distributed Denial of Service

USN – Ubiquitous Sensor Network

SN–Sensor Network

5 Conventions

In this Recommendation:

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 describes the major USN's application areas which include home network application, pollution monitoring, fire monitoring, and flood monitoring.

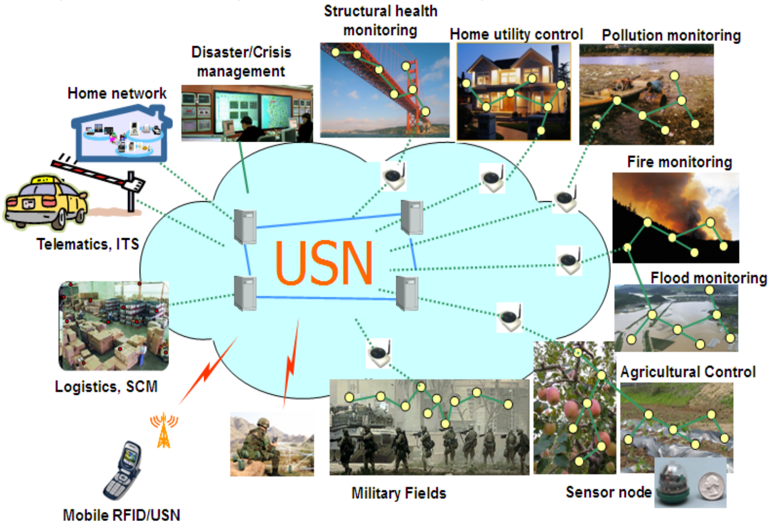

Figure 1 – Application area for USN

The Figure 2 describes the overall structure of USN. Based on this basic structure, the security model should be defined for USN security.

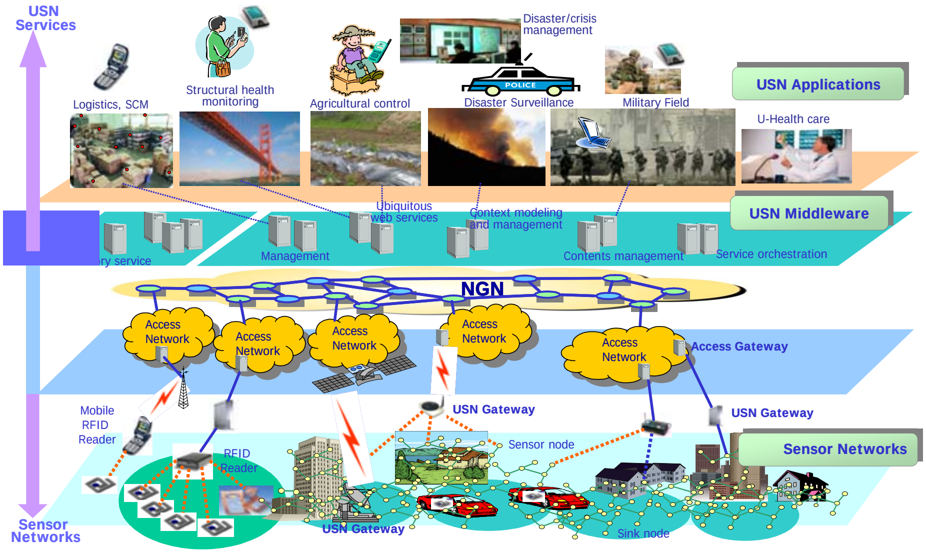

Figure 2 – Overall structure of USN

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

Sensor networks are not isolated but connected usually 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, WiBro, etc. The core networks are NGN, Internet, etc. USN might require some extensions and/or additions to core network architectures in order to cover new functional capability requirements extracted from USN applications and services. The USN middleware will be comprised 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 those 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 IP network and the other for Wireless Sensor network. However, since there is no security model for wireless sensor network studied by ITU-T, this Recommendation intends to develop the security model for SN as well as IP network.

The communication patterns within our SN fall into three categories:

- Node to base station communication, e.g. sensor readings or special alerts.
- Base station to node communication, e.g. specific requests.
- Base station to all nodes, e.g. routing beacons, queries or reprogramming of entire sensor network.
- Communications among a defined cluster of sensor nodes, e.g. communications between

a sensor node and all its neighbors.

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.
- The communication paradigm is either base station to sensor or sensor to base station.

So how such network managements are integrated should be taken into account.

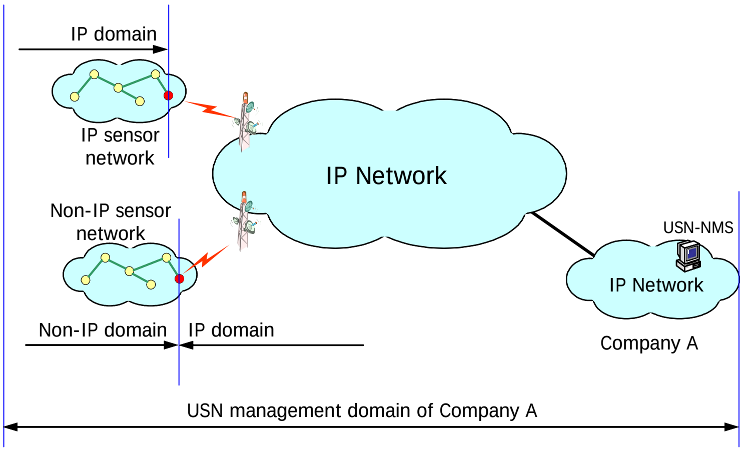

Figure 3 – A USN network configuration

The characteristics of the sensor network are as follows;

- The sensor network consists of a lot of sensor nodes interconnected by wireless medium.
- The sensor nodes are deployed densely in a wide area.
- The sensor nodes are vulnerable to failure.
- The communication from BS to sensor node would be broadcast type or point-to-point type.
- Sensor nod has a limited power, computational capacity, and memory.
- Sensor node may not have a global identification.

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

To communicate information between the sensor nodes, a secure association between each sensor nod needs to be established before the secure communication between them can be carried out. However, the following characteristics of the sensor network make the design of secure communication very difficult;

- **Infeasible to use the public key cryptosystems**: The limited computational power, memory size, and power supply make it very difficult to use the public key cryptosystem, such as Diffie-Hellman key agreement or RSA encryption and signature. Even though the sensor node has the resource to perform the very complex operation of public key cryptosystem, it cause a vulnerability to denial of service attack.

- **Vulnerability to sensor node compromise**: Since the sensor nodes may be deployed in very hostile positions, it causes the vulnerability to sensor nodes. When the attacker obtains the sensor node, he/she is able to access to sensitive information, such as key information or sensed information. This attack can be prevented by using tamper-resistant sensor node which results in high-cost sensor node. However, a large number of sensor node makes it very difficult to employ the tamper-resistant sensor node since it cause very high-cost network.
- **Difficulty to obtain the after-deployment knowledge**: In most cases, the sensor nodes will be deployed in a random scattering manner. Therefore, it is difficult for the security protocol to know the location knowledge of the neighbour node.
- **Limited memory size, limited transmission power, and limited transmission bandwidth**: Since there are limited memories in each sensor node, it is very difficult to store unique keys with each other sensor nodes in the network. In addition, typical sensor node has low capability of transmission bandwidth and power to communicate with neighbour 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. Hence a base station is a source of trust, tempting to invite various attacks of the attackers on the base station.

7 Threats model for USN

The threats for USN are composed of two parts: one for IP network and the other for SN.

7.1 Threats model in SN

There are two types of attackers in the SN; mote-type attacker and laptop-type attacker. In the former case, the attacker has a capability similar to the sensor node and can have access to few sensor nodes. An attacker with mote-type device might able to jam the radio link in its vicinity of attacker. In the latter case, attacker may have access to more powerful devices like laptop computer. An attacker with laptop-type device may eavesdrop on the communication in the sensor network, have a high-bandwidth, low-latency communications channel, and can jam the entire sensor network using high power transmitter. There are two types of threats for SN; general threats and routing-related threats. The threats in the SN are applied to the communication between the base station and sensor node, and nodes as described in clause 7.1, and the routing-related threats are applied to the routing message exchange as described in clause 7.2.

7.1.1 General threats in SN

[ITU-T X.800] and [ITU-T X.805] identify the following security threats to the networks, and which are also security threats that are 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; and

- Interruption of services.

In addition to them, there are a lot of sensor node specific threats like sensor mode compromise, eavesdropping, privacy of sensed data, denial of service attack, and malicious use of commodity network were identified.[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, making it impractical to monitor and protect each individual sensor from either physical or logical attack. The networks may be dispersed over a large area, further exposing them to attackers who capture and reprogram 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—for example, 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 make it challenging to reprogram captured sensor nodes. However, making nodes robust to tampering is not economically viable. We must therefore assume that an attacker can compromise a subset of the sensor nodes. Hence, 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 on resource limited hardware will require lightweight security protocols. Further, all communications and data-processing protocols used in sensor networks must be made *resilient*—that is, 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 might be able to monitor the light and temperature readings of sensor networks inside the house, thus revealing detailed information about the occupants' personal daily activities. Encrypting sensor node communications partly solves eavesdropping problems but requires a robust key exchange and distribution scheme. The scheme must be simple for the network owner to execute and 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 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, where each sensor node stores only encryption keys shared with its immediate neighbors. In this case, adversary control of a communication node eliminates encryption's effectiveness for any communications 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 are 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. Efficient discovery of the best disjoint paths to use for such an operation is another research challenge.
- **Privacy of sensed data:** Sensor networks are tools for collecting information, and 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 that gains access to both the indoor and outdoor sensors of a home may be able to isolate internal noise from external noise and thus extract details about the inhabitants' private activities. The main privacy problem, however, is not that sensor networks enable the collection of information that would otherwise be impossible. In fact, much information from sensor networks could probably be collected through direct site surveillance. Rather, sensor networks aggravate the privacy problem because they make large volumes of information easily available through remote access. Hence, 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 is accessible only to trusted parties is an essential step toward achieving privacy. Data encryption and access control is one approach. Another 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 sensed individuals. A system stores the sensed data in an anonymized database, removing the 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—for example, 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 exhaustion in sensor nodes—for example, by sending a sustained series of useless communications that the targeted nodes will expend energy processing and may also forward to other nodes. More insidious attacks can occur from inside the sensor network if attackers can compromise the sensor nodes. For example, 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 counteract jamming attacks. Proper authentication can prevent injected messages from being accepted by the network. However, the protocols involved must be efficient so that they themselves do not become targets for an energy exhaustion attack. For example, using signatures based on asymmetric cryptography can provide message authentication. However, 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 commodity networks:** The proliferation of sensor networks will inevitably extend to criminals who can use them for illegal purposes. For example, thieves can spread sensors on the grounds of a private home to detect the inhabitants' presence. If the sensors are small enough, they can also plant them on computers and cell phones to extract private information and passwords. With widespread use, the cost and availability barriers that discourage such attacks will drop. Sensor detectors offer one possible defense against such attacks. A detector must be able not only to detect the presence of potentially hostile wireless communications within an area that may have significant levels of radio interference but also to differentiate between the transmissions of authorized and unauthorized sensor networks and other devices. Such technologies might not prevent unauthorized parties from deploying sensor networks in sensitive areas, but they would make it more costly, thus alleviating the problem somewhat.

7.1.2 Routing-specific threats

[Editor's Note] It is required to be harmonized with X.usnsec-2.

[ITU-T X.800] and [ITU-T X.805] identifies five threats that are applicable to routing-related message exchange in SN. In addition to them, there are seven threats against the routing messages which are exchanged between the sensor nodes.

- **Spoofed, altered, replayed routing information:** The attacker is able to spoof, alter, reply the routing information resulting creating routing loop, attracting network traffic, extending source routing, and increasing end-to-end latency.
- **Selective forwarding:** It refers to an attack in which a compromised node by an attacker may refuse to forward certain messages and drop them, stopping propagating any further.
- **Sinkhole attack**: It refers to attack in which the attacker attracts all the traffic from a particular area through compromised node.
- **Sybil attacks**: It refers to attack in which 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 the wormhole attack, an adversary tunnels messages received in one part over a low latency link and replays then in a different part. Wormhole attacks will involve two distinct malicious nodes colluding to understate their distance from each other by replaying packet along an out-of-band channel available only to the attacks.
- **HELLO flood attacks**: It refers to the attack in which a laptop-type attacker broadcasts the HELLO packets convincing every node in the network that an adversary was its neighbor.
- **Acknowledgement spoofing**: In acknowledgement spoofing, an adversary can spoof link layer acknowledgement for “overheard” packet addressed to neighboring node convincing the sender that a weak link is strong or a dead or disabled node is alive.

7.2 Threats model in IP network

The threats model developed in ITU-T X.805 can be applied to the IP network. Therefore, details can be omitted.

8 Security requirements for USN

To countermeasure the above threats in both SN and IP network, the following security requirements in ITU-T X.805 can be 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 secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality.
- **Data Authentication:** 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 sensor node duty cycle).

At the same time, an adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from the correct source. Informally, *data authentication* allows a receiver to verify that the data really was sent by the claimed sender. In the two-party communication case, data authentication can be achieved through a purely symmetric mechanism: The sender and the receiver share a secret key to compute a message authentication code (MAC) of all communicated data. When a message with a correct MAC arrives, the receiver knows that it must have been sent by the sender. This style of authentication cannot be applied to a broadcast setting, without placing 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 insecure: Any one of the receivers knows the MAC key, and hence could impersonate the sender and forge messages to other receivers. Hence, we need an asymmetric mechanism to achieve authenticated broadcast. One of our contributions is to construct authenticated broadcast from symmetric primitives only, and introduce asymmetry with delayed key disclosure and one-way function key chains.

- **Data Integrity:** In communication, *data integrity* ensures the receiver that the received data is not altered in transit by an adversary.
- **Access control**[ITU-T X.805] Access control ensure that only authorized user or entity is allowed to gain access to information, resource, or services.
- **Non-repudiation**[ITU-T X.805] Non-repudiation ensure that no entity or user can not deny the activities in the network done by themselves.
- **Communication security**[ITU-T X.805] Communication security ensure that the information only flows from source to destination.
- **Availability**[ITU-T X.805] Availability ensure that information, service, and application are available to legitimate users any time.
- **Privacy**[ITU-T X.805] Privacy ensure that identifier of user or entities and network usage is kept secret.

9 Security requirements and threats in USN

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

9.1 Security requirement and threats for the message exchange in SN

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

Table 1 lists the Security requirements and describes mapping of Security Dimensions to 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 designate that a particular security threat is opposed by a corresponding security dimension.

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 requirements and describes mapping of Security Dimensions to sensor node specific threats for the message exchange between the nodes: the letter 'Y' in a cell formed by the intersection of the table's columns and rows designate that a particular security threat is opposed by a corresponding security dimension.

Table 2: Security requirements to sensor node specific threats

Security requirements	Sensor node specific threats				
	Sensor node compromise	Privacy of sensed data	DoS	Malicious commodity network	Replay attack
Access control					
Authentication			Y		Y
Non-repudiation					
Confidentiality		Y		Y	
Communication Security	Y				
Data Integrity					
Availability			Y		
Privacy					

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

Table 3 lists the Security Dimensions and describes mapping of Security requirements to security threats against the broadcast message by 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 designate that a particular security threat is opposed by a corresponding security dimension.

Table 3: security requirements 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	

9.1.3 Security requirement and threats for the routing message exchange

[Editor’s Note] It is required to be harmonized with X.usnsec-2.

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 are composed of sybil attack, HELLO flood attack, wormhole and sink hole attack, selective forwarding attack, and DoS attack. Table 4 lists the Security Dimensions and describes mapping of Security requirements to security threats of the routing message exchange launched by insider attack: the letter 'Y' in a cell formed by the intersection of the table's columns and rows designate that a particular security threat is opposed by a corresponding security dimension.

Table 4: Mapping of security dimensions to security threats for the insider attack

Security requrements	Security threat					
	Sybil attack	HELLO flood	Wormhole and sinkhole	Selective forwarding	DoS	Acknowledgement spoofing
Access control	Y	Y	Y	Y		
Message Authentication		Y				
Identification Authentication	Y	Y	Y	Y		
Non-repudiation						
Confidentiality			Y	Y		
Communication Security			Y	Y		
Data Integrity	Y	Y				
Availability						
Privacy			Y	Y		

Table 5 lists the Security Dimensions and describes mapping of Security requirements to security threats of the routing message exchange launched by outsider attack: the letter 'Y' in a cell formed by the intersection of the table's columns and rows designate that a particular security threat is opposed by a corresponding security dimension.

Table 5: Mapping of security dimensions to security threats for the outsider attack

Security dimension	**Security threat**					
	Sybil attack	**HELLO flood**	**Wormhole and sinkhole**	**Selective forwarding**	**DoS**	**Acknowledgement spoofing**
Access control				Y		
Message Authentication						
Identification Authentication	Y	Y	Y	Y		
Non-repudiation						
Confidentiality			Y	Y		
Communication Security			Y	Y		
Data Integrity		Y				
Availability						
Privacy			Y	Y		

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

The security threats and security requirements developed in ITU-T X.805 can directly be applied for the secure message exchange through the IP network. Therefore, details about them can be omitted.

10 Security technologies for USN

10.1 Key management

It refers to the generation, distribution, sharing, rekeying, and revocation of cryptographic keys for data confidentiality service, data integrity, data freshness, and data authentication in the SN. The security of key management forms a foundation of security of other security services. In sensor network, it is very important to share or distribute a pair-wise key between the sensor nodes and a group-wise key among a set of sensor nodes. It is sometimes called a 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 pair-wise key between the sensor nodes or group-wise key among the sensor nodes. The typical example of this scheme is Kerboros. However, 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 pair-wise key or group-wise key in the sensor network. The typical algorithm of public key algorithm includes Diffie-Hellman key agreement algorithm and RSA key transport algorithm. However, this scheme can not 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. That is, it is not assumed that a priori knowledge about the exact location of sensor node is not known prior to deployment. This scheme has a low communication overhead. In addition, it is resilient to node compromise and does not rely on the trust of base station. Therefore, this scheme is very suitable to wireless sensor network.

There are a number of key pre-distribution schemes that do not assume to have a knowledge of deployment of sensor node. The simple scheme is master key based pre-distribution scheme. 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 pair-wise key by exchanging the random nonces. This scheme does not provide desirable resilience to node compromise since if a node is compromised, the entire sensor network is compromised. The second scheme is called pair-wise key pre-distribution scheme. This scheme is to let each sensor node have N-1 secret pair-wise keys, each of which is only known 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 gives a perfect resilience against the node compromise since a compromised node does not affect security of any other node. However, it gives no scalability since adding new nodes to the existing sensor node is impossible since the existing node does not have a new pair-wise key. In addition, this scheme is not practical since the memory size is limited when the number of sensor node is very large. The third scheme is a random key pre-distribution scheme. In this scheme, the subset of keys from large key pool are stored before deployment of sensor node, two nodes find a common key, and use that common key as shared session key between the two sensor nodes.

The requirements of key management in a sensor network should be as follows;

- **Scalable key management**; The key management scheme should support a large sensor network. In addition, it should be flexible when there is a substantial increase of sensor nodes even after deployment of sensor node.
- **Efficiency of memory size, processing capability, and communication overhead required for key management**: The key management scheme should have efficient storage complexity, i.e. minimum memory size to sore the key in the sensor node, a efficient computation complexity required to establish the key, a efficient communication overhead, i.e. the number of message exchanged during key generation process.
- **High pair-wise key establishment**: The key management scheme should have a high probability that two sensor nodes establish the common key and key material.
- **Resilience against node compromise**: The key management scheme should have a capability to resistant against node compromise. Compromise of security credential should not reveal least information about security of other link in the sensor network, that is, higher resilience indicates lower number of compromised links.

The detail on key management is described in ANNEX A.

10.2 Authenticated Broadcast Message

A broadcast message is targeted to all sensor nodes. A broadcast message authentication scheme allows any targeted nodes to verify the authenticity of the broadcasted messages. Two kinds of techniques can be used to achieve it according to the type of cryptographic algorithm. In case of public key cryptography, digital signature can be used. However, if symmetric cryptography is used, it is necessary to append to the data the verifiable authentication data (i.e., message authentication code) based on the multiple shared secret between the sink node and sensor node. Due to the properties of sensor network, the broadcast authentication method is preferred to one-to-one authentication.

There is a typical scheme to achieve broadcast authentication in sensor networks. The uTESLA protocol [b-SPINS] is the simplified version of TESLA (Timed Efficient Stream Loss-tolerant

Authentication)[b-TESLA]. It basically uses a delayed disclosure of symmetric key. It is assumed that the base station and the sensor nodes are loosely time-synchronized. 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 at which 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, which has been generated by a one-way function. In order 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.

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 has been many related work proposed to address these security issues.

The secure data aggregation refers to an in-network process which is performed on the aggregator node to securely transfer the aggregation value to 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, then aggregator calculate the encrypted aggregator results by 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 a capability to aggregate data than individual value from all sensors. By aggregating data, it is possible to reduce the amount of data which needs to be transmitted from one sensor to other sensor. The secure data aggregation can be applied to the sensors that are deployed in a hierarchical structure.

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

- Hop-by-hop encrypted data aggregation: The operation is based on the hop-by-hop encryption between the neighbor sensor nodes. It is assumed that each pair of neighbor sensor nodes shares a common secret key. The sensed values are encrypted by many sensor nodes. All encrypted values collected are decrypted by the intermediate aggregator nodes. The intermediate aggregator nodes then obtain the aggregated value and encrypt the aggregated value again. This process is repeated until they are reached to sink node. Finally, the sink node obtains the total aggregated value.
- End-to-end encrypted data aggregation: The operation is based the end-to-end encryption between the many sensor nodes and one sink node. It is assumed that common secret is shared between the many sensor nodes and a sink node. The sensing nodes encrypt the sensed values and forward them to intermediate aggregator nodes. The intermediate aggregator nodes 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.

It is known that the framework for end-to-end encrypted data aggregation has higher computation cost on the sensor nodes, but achieves stronger security, in comparison with the framework for hop-by-hop encrypted data aggregation.

10.4 Data Freshness

Given that all sensor networks stream some forms of time varying measurements, it is not enough to guarantee confidentiality and authentication; we also must ensure each message is *fresh*. Informally, data freshness implies that the data is recent, and it 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, while strong freshness is useful for time synchronization

10.5 Tamper Resistant Module

The best well-known technique to protect against the sensor node compromise is to use the tamper-resistant module in sensor node. If each sensor node is equipped with a tamper-resistant module, it may be possible to protect the storage of sensitive data e.g. key data, resulting in the damage following the capture of sensor nodes. The other possible technique to protect against the 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. Therefore, the first option will be limited to applications that are critical enough to be more expensive. If sensor nodes cannot be tamper-resistant, the latter should be implemented to gain probability security.

10.6 USN Middleware security

Enormous amount of data collected at the sensor network is securely stored, managed and analysed by USN middleware, and USN middleware delivers data to appropriate application through secure channel. As USN middleware communicates with sensor networks or applications over the IP network, USN middleware should consider existing security threats on the IP network. And in order to ensure secure communications against various threats, such as spoofing, sniffing, message modifications, DDoS, etc., security techniques like encryption/decryption, authentication, authorization and access control are considered and applied. Furthermore, encryption/decryption function for data stored in USN middleware is also needed because USN middleware sometimes stores very important and valuable data which cause big problem when they are revealed. Security technique to ensure availability of USN middleware is considered as well.

10.7 IP Network Security

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

11 Specific Security Requirements for USN

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

11.1 Mandatory Requirements

- The key management scheme of SN is required to support the key pre-distribution scheme described in clause 10.1.
- The key management is required to support both an pair-wise key establishment and group-wise key establishment.

- The SN is required to authenticate broadcast messages from a base station to all the sensor nodes.
- The SN is required to support secure routing protocol with message authentication, ID authentication, and data integrity.
- The base station in SN is required to support the countering mechanisms to mitigate the effects of DoS attacks from both wireless interface and wired interface.
- The USN is required to support USN middleware security.
- [Editor Note: Further requirements will be developed]

11.2 Recommended Requirements

- The SN is recommended to support a secure end-to-end encrypted data aggregation scheme.
- The SN is recommended to support the data freshness.
- [Editor Note: Further requirements will be developed]

11.3 Optional Requirements

- The sensor node or base station can optionally to provide secure data aggregation.
- The sensor node can optionally to have tamper –resistant module for protecting credentials, sensed data, or any confidential data.

[Editor Note: Further requirements will be developed]

ANNEX A: Key management in Sensor Networks

A.1 **Threat Time**

Once deployed, in order to ensure key’s security, nodes establish a pair-wise key in a short time so that it is crucial whether the phase of key setup is exposed to an adversary or not 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 before key setup. This adversary can analyze communication between nodes or get the physical access to node during key setup. This adversary is regarded as strong and intensive. It means the application requiring a high security level must design a key scheme as assuming a prepared adversary.

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

A.2 Key Management classes

By above two criterion, two 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 not any other threat like node capture all along 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, 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 the communications when nodes are deployed and, after key establishment, he is prepared for all attacks including node capture.

A.2.4 Class 4

An active adversary always waits for node deployment. It means that eavesdropping and node capture happen already in the phase that nodes are deployed. This class, considering the strongest adversaries, is a general assumption but requires an expensive cost.

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

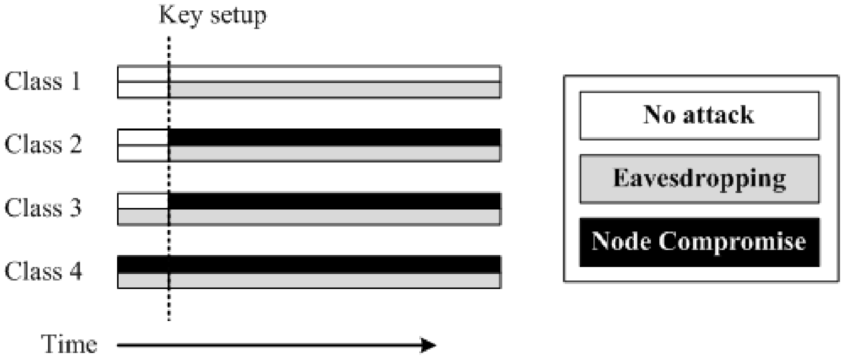

Figure A-1. Key Management Classes

A.3 Key Schemes

A.3.1 Key Management Mechanisms

A.3.1.1 PAIR-WISE KEY PRE-DISTRIBUTION

A pair-wise key between a pair of nodes is directly stored, pre-distributed, in each node before node deployment (hereafter Pair-wise key scheme). Since each node in this scheme stores its pairwise keys, it has perfect resilience against node capture which means even if a node is captured, the keys of non-captured nodes are never compromised. However, scalability is limited because network scale depends on the memory of node where potential keys are stored.

A.3.1.2 MASTER KEY BASED PRE-DISTRIBUTION

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

A.3.1.3 BASE STATION PARTICIPATION

`SPINS' is included in this mechanism. In SPINS, each node is given its shared key with the base station. The base station directly transmits a pair-wise key respectively encrypted with each node's shared key. In other words, the base station intermediates in key setup. This scheme supports not only full connection but also perfect resilience. However, it is not scalable because of the terrible 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. This mechanism results from the concept all the nodes in the entire networks are connected with the 0.9997 probability- almost fully connected- if the probability each node can establish a pair-wise key with its neighbour nodes is 0.33. A key ring is stored in each node before deployment (a key ring *k* is randomly selected from key pool *P* which is randomly selected from huge key space). A common key in both key rings of a pair of nodes is used as their pair-wise key. It guarantees enough resilience even though not perfect resilience, because the probability of breaking communication link is *k/P*. Moreover, it supports the large scale networks. The representative scheme is `EG scheme'. Its variants are proposed like a combination of the EG scheme and the Blundo scheme and a combination of the EG scheme and the Blom scheme which significantly enhance the security.

A.3.1.5 NO KEY PRE-DISTRIBUTION

This mechanism is considering the reality of sensor networks. If an adversary does not know where and when nodes are deployed, it is difficult to launch active attack at an early phase. It can be a good trade-off to improve efficiency instead of a little node loss due to attacks during key setup. `Key infection' is a representative scheme. In Key infection, key setup is completed in a relatively short time through a few transmissions. The advantage in this mechanism is the base station does not take part in a key setup so that it consumes relatively less energy. Unlike the pre-distribution schemes above, it need not load potential keys into a node, which results in the low cost of network organization. However, it is only strong when an adversary does not observe communication during key setup and it cannot add nodes since a pair-wise key is established through exchanged data during key setup.

A.4 Key Management Schemes in Class 1

[Editor’s note] Key schemes will be shown in class 1.

A.4.1 Key Management Schemes in Class 2

[Editor’s note] Key schemes will be shown in class 2.

A.4.2 Key Management Schemes in Class 3

[Editor’s note] Key schemes will be shown in class 3.

A.4.3 Key Management Schemes in Class 4

[Editor’s note] Key schemes will be shown in class 4.

Bibliography

- [b-ITU-T C22] ITU-T TSAG – C 22 – E, A preliminary study on the Ubiquitous Sensor Network, Feb. 2007.
- [b-Y.USN-reqts] Draft Recommendation Y.USN-reqts, "Requirements for support of ubiquitous sensor network (USN) applications and services in NGN environment" (NGN-GSI, 12-22 May 2008).
- [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*
- [b-Karlof] C. Karlrof, D. Wagner, *Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures*
- [b-Akildiz] I.F.Akildiz, W.Su, Y. Sankarasubramaniam, and E.Cayirci, *A Survey on Sensor Networks*
- [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.

____

Attachment 2

Reference number of working document: **ISO/IEC JTC 1/SC 31 N 000**

Date: 2009-02-14

Reference number of document: **ISO/IEC 29182**

Committee identification: ISO/IEC JTC 1/SC 6/WG 7

Secretariat: XXXX

Information technology — Telecommunications and information exchange between systems — Reference architecture for sensor network applications and services

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International standard
Document subtype: if applicable
Document stage: (20) Preparation
Document language: E

Copyright notice

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 6, *Telecommunications and information exchange between systems,* Working group 7, *Network and transport layers,* prepared ISO/IEC 29182

Introduction

To be added

Information technology — Telecommunications and information exchange between systems — Reference architecture for sensor network applications and services

1 Scope

This International Standard specifies the reference architecture for sensor network applications and service and covers the following in network and transport layer:

- Requirements analysis of sensor network applications and services
- Identification of the network functionalities required by different sensor network applications
- Reference architecture for sensor networks functionalities supporting various sensor network applications and services
- Specification of interfaces for sensor network functionalities supporting sensor networks

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC JTC1 SGSN N049, *Technical Document of ISO/IEC JTC 1 Study Group on Sensor Networks (SGSN)*

ITU-T Draft Recommendation Y.USN-reqts, *Requirements for support of Ubiquitous Sensor Network (USN) applications and services in NGN environment (01. 2009)*

To be added

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

[Editor’s Note] The following terms and definitions refers to ISO/IEC JTC1 SGSN TD049 and ITU-T Y.101 “Global Information Infrastructure terminology: Terms and definitions” and ITU-T JCA-NID “Draft for the terms and definitions relevant to the USN scope of ITU-T JCA-NID”.

3.1

Actuator
A device that performs a physical response caused by an input signal.

3.2

Sensor

A device that observes phenomenon/phenomena, measures physical property and quantity of the observation, and converts the measurement into a signal.

Note:

- Signal can be electrical, chemical, or other types of sensor responses.
- Signal can be represented by 1-D, 2-D, 3-D, or higher dimensional data.

3.3

Sensor Node
A device that consists of at least one sensor and zero or more actuators, and processing and networking capabilities using wired or wireless means.

3.4

Sensor Network
A system of spatially distributed sensor nodes interacting with each other and, depending on applications, interacting with other infrastructure in order to acquire, process, transfer, and provide information extracted from the physical world.

3.5

Sensor Network Applications
A structured set of capabilities, which provide value-added functionality supported by one or more services such as, home utility monitoring and control, industrial automation, infrastructure and environment monitoring, weather and disaster condition monitoring and emergency alert.

[Editor's Note] The definition of Sensor Network Applications refers to ISO/IEC JTC1 SGSN TD049 and ITU-T Y.101 "Global Information Infrastructure terminology: Terms and definitions".

3.5

Sensor Network Device
The sensor network device is sensor node or sensor network gateway.

3.6

Sensor Network Gateway
The sensor network gateway represents the bridge between the sensor network itself and the backend system. Therefore, it has to provide wired/wireless interface(s) to other sensor nodes as well as a wired (e.g., Ethernet) or wireless (e.g., mobile Ethernet via WLAN, UMTS or SatCom) interface to existing IT infrastructures.

3.7

Sensor Network Services
A structure set of capabilities offered by the sensor nodes or sensor networks to support sensor network applications.

[Editor's Note] The definition of Sensor Network Services refers to ISO/IEC JTC1 SGSN TD049 and ITU-T Y.101 "Global Information Infrastructure terminology: Terms and definitions".

4 Symbols (and abbreviated terms)

To be added

5 Requirements of sensor network applications and services

Sensor network applications and services have specific characteristics with different service requirements and functional requirements from each other. However characteristics of sensor network applications and services can be distinguished into basic service model and advanced service model from the way of application model, operation process, operation domain and type of user.

5.1 Classification of service model

5.1.1 Basic service model

A basic service model has following characteristics:

Table 1 — Features of basic service model

Features	Type	Description
Application model	Pre-defined	Sensor networks are installed for specific and static purposes such as structures monitoring, street light control, agriculture monitoring and management, surveillance, facilities management, etc.
Operation process	Straightforward	Straight forward process progresses into sensing, transmitting, processing and provisioning. Sensor nodes and resulting sensor networks detect physical status; they transmit sensor data to backend application systems; the application systems collect sensor data and perform data processing functions; and the application systems produce value-added information contents and services.
Operation domain	Single	Sensor data are captured, transmitted, processed and delivered within a single operation domain.
Type of user	Dedicated	Value-added data are provided to dedicated users: owner and partners.

5.1.2 Advanced service model

An advances service model can be considered as a service infrastructure and has following characteristics:

Table 2 — Features of advanced service model

Features	Type	Description

Application model	Dynamic	Services depend on the usage of users who anybody can be. It is very difficult to fix application features and relevant functions statically in advance. For weather information services as an example: – Fishermen may request on-demand and periodic weather information for fishing; – Tourists may request periodic and alarming information of the nature condition for a week, a few days, or a month by a service subscription; – National disaster center may request the whole weather information to observe the natural phenomena of an area and detect emergency situations; etc.
Operation process	Elaborated	Transmitting, processing and provisioning step have additional functions as follows: – Various sensor networks may be integrated and sensor data may be acquired via other sensor networks by business contracts; – Due to dynamic service models, a variety of application functions have to be involved such as filtering, analyzing, context processing, data mining, decision making, forecasting, integration, exporting, etc.; and – Since anybody can be information user and information contents cannot be pre-defined, sensor data may be delivered in different forms such as text, audio, voice, image, etc. according to information users.
Operation domain	Multiple	Multiple business domains are incorporated by business partnerships.
Type of user	Dedicated and arbitrary	Services are provided to consumers as well as business partners: – Pre-defined users by contracts or agreements result in B2B-type sensor network services; and – Consumers by service subscription result in B2C-type sensor network services.

5.2 Analysis of service requirements

The following are service requirements for sensor network applications and services and these requirements are based on clause 5.1. These requirements are used to define functional requirements of sensor network reference architecture.

To be added or modified

[Editor’s Note] This clause gives analysis of service requirements based on service model. This clause refers to ITU-T [Y.USN-reqts], “Requirements for support of Ubiquitous Sensor Network (USN) applications and services in NGN environment”. These requirements lead to functional requirements defined in clause 6 and 7.

5.2.1 Connectivity

There are many types of sensor networks, such as IP-based, non IP-based, wired or wireless sensor networks. In IP-based sensor networks, every sensor node is capable for IP networking. Although the underlying wired or wireless media access control is tightly managing the connectivity of sensor nodes, connection between end user and a sensor network is through IP. In this sensor network type, it may happen that a single sensor node may directly connect to the backend network without a gateway, although normal scenario would use gateway to interconnect sensor networks and access networks.

In non IP based sensor networks, sensor nodes do not have IP address, and the connection between end user and a sensor node is through sensor network gateways. The gateways interconnect sensor networks and access networks.

Therefore it is required to support connectivity between sensor networks and the backend network, regardless of sensor network type, i.e. IP based or non-IP based, wired or wireless sensor networks.

5.2.2 Sensor network management

IP based sensor networks and non-IP based sensor networks, and wired and wireless sensor networks can co-exist. Application level gateways or overlay IP networks can be used for the connectivity between sensor networks and the backend network, and the diverse types of sensor networks need to be managed.

5.2.3 Service registration and discovery

In order to discover the sensor network services, they should be registered beforehand. The association of senor network and sensor data should be registered to service registry. The registered services are needed to be discovered by applications or end-users.

5.2.4 Mobility support

The challenge of achieving mobility in sensor applications and services depends on the technologies used in the sensor networking. Existing IP mobility technologies can be adapted for IP-based sensor networks.

An example sensor network application scenario illustrating mobility requirements can be found in the healthcare application. For instance, a patient’s medical check-up data may be monitored via a sensor network: several sensors may be attached to the patient, resulting in a body area sensor network. The sensors periodically gather the medical check-up data and send them to his/her doctor via a home-gateway when he/she is at home; while moving, the data can be sent via an access gateway in a network-enabled car, bus, train, or subway. Various cases of mobility may occur in such an application scenario.

5.2.5 QoS support

Mission-critical applications and services should be carefully managed. QoS may be a key technical issue in some scenarios. For example, emergency notification of fire in national treasure monitoring system must be delivered by time-critical and reliable way.

5.2.6 Security

In general, sensor network services highly require strong security, as the sensed data are very sensitive. There are various security issues which need consideration, such as protection against unauthorized use of network resources and unauthorized access to information and authentication of users.

6 Overview of the reference architecture of sensor network

[Editor's Note] In this clause, overview of the reference architecture and descriptions on components of the reference architecture will be given.

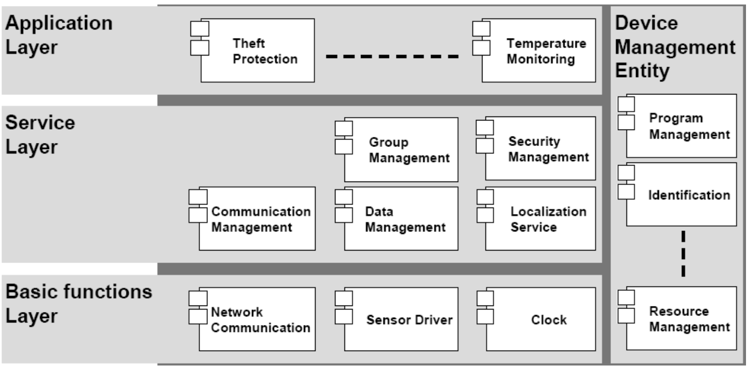

Figure 1 — Overview of the reference architecture *(just for reference and will be modified)*

[Editor's Note] Figure-1 is taken from ISO/IEC JTC1 SGSN N049 as a reference. This figure SHOULD be modified in this document. Contributions are required.

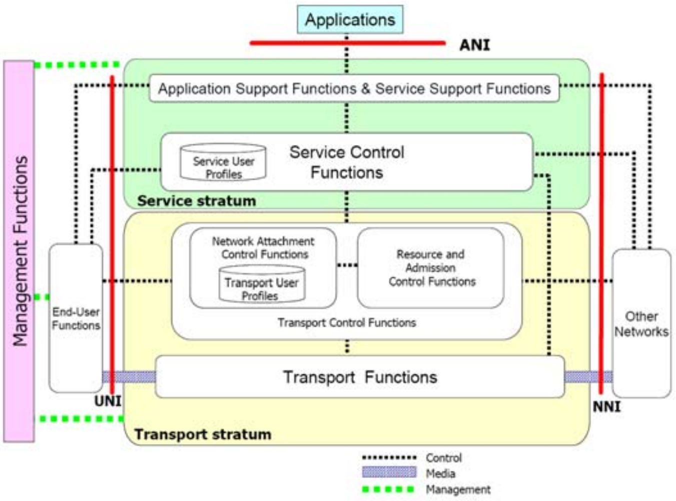

Figure 1-1 — NGN architecture overview *(just for reference and will be deleted)*

[Editor's Note] Figure 1-1 comes from ITU-T Y.2012, Next Generation Networks – Frameworks and functional architecture models – Functional requirements and architecture of the NGN of Release 1 as a reference. Overview of sensor network reference architecture may be given in the form of Figure 1-1.

6.1 TBD

[Editor’s Note] This clause will give descriptions on the overview of the reference architecture and the functionalities of components of the reference architecture based on service requirements defined in clause 5.2.

7 Generalized sensor network functional architecture

This clause explains the generalized functional architecture for the sensor network and defines the generalized functional entities. This architecture can be applied to general applications and services of sensor network. Also this architecture is technology-independent, therefore this architecture can be customized to respond to specific contexts in terms of the applications and services offered and the technologies used.

7.1 Sensor Network Functional Entities (FE)

In general, an FE is characterized by functions identified as sufficiently unique with respect to other FEs. In the case of the generalized sensor network architecture, the functional entities, called SN FEs, are to be understood as generic FEs to allow for their possible instantiation in more specific technology-oriented contexts. It is therefore possible that when SN FEs are instantiated, they can be used and can behave in a slightly different manner depending on the context. For example, this may lead to the case where at a given reference point (between the same SN FEs), the interface and the associated protocols are different depending on the instantiation. This means that interfaces, as well as protocol descriptions, can only be provided on the basis of a specific instantiation of the generalized functional architecture.

[Editor's Note] In this clause, Sensor Network Functional Entities (FE) will be given and the following is taken from ITU-T Y.2012, Next Generation Networks – Frameworks and functional architecture models – Functional requirements and architecture of the NGN of Release 1. The original sentences have NGN instead of sensor network or SN.

7.2 Generalized functional architecture

[Editor's Note] This clause will give generalized functional architecture showing all FEs and their relationships. Contributions are required.

Figure 2 — Sensor network generalized functional architecture *(To be defined)*

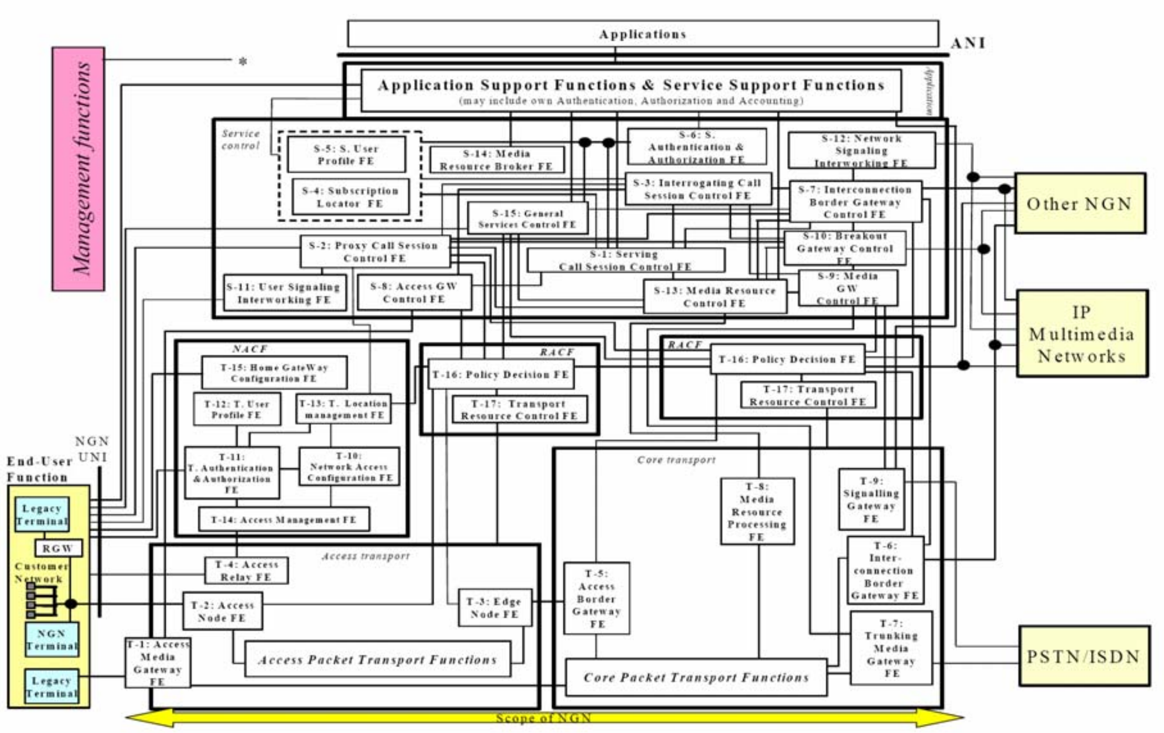
Management functions
*
Applications
ANI
Application Support Functions & Service Support Functions
(may include own Authentication, Authorization and Accounting)
Applications
Service control
S-5: S. User Profile FE
S-4: Subscription Locator FE
S-14: Media Resource Broker FE
S-6: S. Authentication & Authorization FE
S-12: Network Signaling Interworking FE
S-3: Interrogating Call Session Control FE
S-7: Interconnection Border Gateway Control FE
S-15: General Services Control FE
S-2: Proxy Call Session Control FE
S-1: Serving Call Session Control FE
S-10: Breakout Gateway Control FE
S-9: Media GW Control FE
S-11: User Signaling Interworking FE
S-8: Access GW Control FE
S-13: Media Resource Control FE
Other NGN
IP Multimedia Networks
NACF
T-15: Home GateWay Configuration FE
T-12: T. User Profile FE
T-13: T. Location management FE
T-11: T. Authentication & Authorization FE
T-10: Network Access Configuration FE
T-14: Access Management FE
RACF
T-16: Policy Decision FE
T-17: Transport Resource Control FE
RACF
T-16: Policy Decision FE
T-17: Transport Resource Control FE
NGN UNI
End-User Function
Legacy Terminal
RGW
Customer Network
NGN Terminal
Legacy Terminal
Access transport
T-4: Access Relay FE
T-2: Access Node FE
T-3: Edge Node FE
T-1: Access Media Gateway FE
Access Packet Transport Functions
Core transport
T-8: Media Resource Processing FE
T-9: Signalling Gateway FE
T-5: Access Border Gateway FE
T-6: Inter-connection Border Gateway FE
T-7: Trunking Media Gateway FE
Core Packet Transport Functions
PSTN/ISDN
Scope of NGN

Figure 2-2 — NGN generalized functional architecture *(just for reference and will be deleted)*

[Editor's Note] For reference to generalized functional architecture, Figure 2-2 is taken from ITU-T Y.2012. Figure2-2 is derived from Figure 1-1. As shown in Figure 2-2, functional entities are placed in each function block defined in Figure 1-1.

In this WD, Figure 1 - Overview of the reference architecture should be extended to Figure 2 - Sensor Network generalized functional architecture in the similar form of Figure 2-2.

7.3 Functional entity descriptions

This clause describes each FE.

7.3.1 Basic function layer FEs

[Editor's Note] The title of this clause and following clauses should be changed according to Figure 1 and 2.

7.3.1.1 Network Communication FE (NC-FE)

[Editor's Note] This clause describes the functionalities and interfaces with other FE (if required) of each FE. The following is example of NGN generalized functional architecture.

> *The access media gateway functional entity (AMG-FE) provides interworking between the packet based transport used in the NGN and analogue lines or ISDN access.*
>
> *a) It provides bi-directional media processing functions for user plane traffic between PSTN/ISDN and the NGN under the control of the AGC-FE.*

b) It provides adequate transfer functions for PSTN/ISDN user call control signalling to the AGC-FE for processing.

c) It optionally supports payload processing functions (e.g., codecs and echo cancellers).

d) It optionally provides the TDM/IP interworking function to support ISDN emulation service in cases where an ISDN unrestricted bearer is needed.

7.3.1.2 … FE

7.3.1.3 … FE

7.3.2 Service layer FEs

[Editor's Note] The title of this clause and following clauses should be changed according to Figure 1 and 2.

7.3.2.1 … FE

7.3.2.2 … FE

7.3.2.3 … FE

7.3.3 Applications layer FEs

[Editor's Note] The title of this clause and following clauses should be changed according to Figure 1 and 2.

7.3.3.1 … FE

7.3.3.2 … FE

7.3.3.3 … FE

7.3.4 … FEs

[Editor's Note] The title of this clause and following clauses should be changed according to Figure 1 and 2.

7.3.3.1 … FE

7.3.3.2 … FE

7.3.3.3 … FE

Bibliography

[1] ISO/IEC Directives, Part 2, *Rules for the structure and drafting of International Standards*, 2001

[2]

[Editor’s Note] To be added

Reference number of working document: **ISO/IEC JTC1 SC 06 N 000**

Date: 2008-11-05

Reference number of document: **ISO/CD 29157**

Committee identification: ISO/IEC JTC1 SC6 WG1

Secretariat: KATS

Information technology— Telecommunications and information exchange between systems — PHY/MAC specifications for short-range wireless low-rate applications in ISM band

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International standard
Document subtype: if applicable
Document stage: (20) Preparation
Document language: E

Contents

Page

Figure of Contents

Table of Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

Introduction

This international standard is applicable to various low-power, low-data-rate, short-range applications such as voice, data, and control. It enables multi-channel, one-to-multipoint communications. The unified simple protocol facilitates its use in implementing such application devices.

This international standard is based upon the synchronisation between structural data formats. The network synchronisation is maintained by the beacon signal from the master. The synchronised transmission and reception resolves the near-far problem that arises in the wireless environments. The standard also incorporates the sounding and the frequency hopping techniques to avoid collision with other possible existing services and to provide with multiple independent communication channels.

Information technology— Telecommunications and information exchange between systems — PHY/MAC specifications for short-range wireless low-rate applications in ISM band

1 Scope

This international standard specifies the PHY characteristics and MAC procedures used for short-range, low-data-rate, wireless communications with very low latency and point-to-multipoint connection capability.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

TBA

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
Pico-net
A small operational range for wireless transmissions within about 10 meters in radius from the user or his/her devices.

3.2
Group
Devices interoperable within a Pico-net, with their usage of the same group code separating them from other devices in different groups.

3.3
Master/slave
All devices within a group use the same group code and remain synchronized with each other centring on the master. Except for the master, all the devices within the given group serve as slaves; any slaves may take the role of master if the master disappears.

3.4
Scan
The master within a group regularly transmits synchronising signals; slaves are operated in accordance with synchronizing signals sent by the master. Therefore, the slaves need to search for their master, and this searching process is called ‘scan.’

3.5
Middleframe
A middleframe is the basic unit of frame operation, consisting of one control frame and one or more payload frames; sixteen middleframes constitute a superframe.

3.6
Superframe

Sixteen middleframes constitute a superframe. The superframe is the overall operational unit of pico-net MAC operations.

3.7
Scan code
A scan code is a 7-bit seed to generate one of the 127 gold codes. A scan code has a value between 1 and 127.

3.8
Open code
A code used for broadcasting.

3.9
Closed code
A code that is used only to a specific communication group or purpose.

3.10
Group code
A code to discriminate communication groups. Either an open or closed code may be applied.

3.11
Security code
A code that is applied to message data to enhance security or privacy of communications. Either an open or closed code may be applied.

4 Abbreviated terms

The following acronyms are used in this document.

BF	beacon frame
DME	device management entity
FBF	fast beacon frame
ISM	industrial, scientific, and medical
MAC	medium access control
MACF	MCF acknowledge control frame
MCF	master control frame
MLME	MAC sublayer management entity
MLME-SAP	MAC sublayer management entity-service access point
MPDU	MAC protocol data unit
MSDU	MAC service data unit
PD-SAP	PHY data service access point
PDU	protocol data unit
PF	payload frame
PHY	physical layer
PLME	physical layer management entity

PLME-SAP	physical layer management entity-service access point
PPDU PHY	protocol data unit
PSDU PHY	service data unit
RACF RCF	acknowledge control frame
RCF	request control frame
RSSI	received signal strength indication
SAP	service access point
SDU	service data unit

5 Overview

There may be many applications in the ISM band. Such applications that require a short-range wireless communication channel can be listed as follows in the order of data rates; video, audio, voice, control, sensor, and so on. A different platform for a different application may be an ineffective way in light of cost, time-to-market, compatibility, etc. Among many solutions is to provide a single platform which is capable of accommodating all these applications with the least overhead.

This standard is intended to provide a unified yet efficient and versatile platform for low-power, low-data-rate, short-range wireless communication applications. It is possible to accommodate diverse services of different nature in a single platform.

For mobile applications, low power consumption is one of the most important factors. To save power, data rate should be traded-off. The standard aims for applications of 1 Mbps or less. To minimise implementation effort, it assumes the use of off-the-shelf RF components for the ISM band.

The standard makes use of frequency hopping, time-division multiple access, and time/frequency hybrid diversity. Frequency hopping is adopted to render immunity to the channel variations and to provide independent simultaneous communication channels. Time-division multiple access provides us with the control of interference of strong adjacent signals which otherwise should be avoided using an elaborate manipulation. The diversity technology is the means to maintain quality-of-service in the ISM band where channel fading is of serious concern.

The devices in a pico-net are either a master or a slave. In a pico-net, there exists only one single master which transmits a beacon signal to which all the other devices (slaves) are synchronised. The beacon signal contains the time synchronization information and the frequency hopping pattern table. The frequency hopping pattern table contains the 16 best frequencies which are selected by sounding algorithms (see 7.4.5).

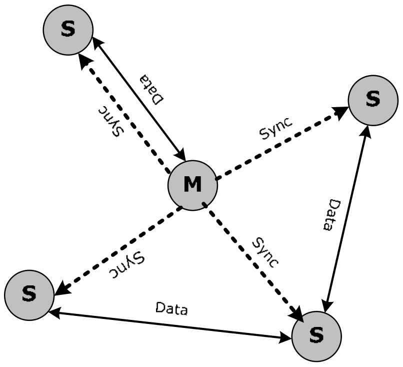

Figure 1 — A group communication example.

At start-up, the master checks the frequency channels and selects the best 16 channels out of 80 to form a table of sixteen orthogonal frequency hopping patterns (see 8.4.2). Each frequency hopping pattern corresponds to a channel. The master assigns a communication channel (or channels) using the MCF (Master Control Frame) to be described below (see 7.4). Within each communication channel which is specified by a unique frequency-hopping pattern, the devices communicate with each other using time-division multiple access without any other intervention of the master.

A pico-net may have up to sixteen independent simultaneous communication channels. Within each communication channel, point-to-multipoint communication (broadcasting) is possible not to mention one-to-one communications. Moreover, each device may switch to a communication channel other than the current one if permitted by the master. Figure 1 shows an example of group communication in a pico-net. The master (M) transmits a beacon signal and is communicating only with one slave (S). The other slaves are communicating with another via other channels independently of the master.

Data are encased into the well-tailored standard units of a frame, a middleframe, and a superframe (see 8.3). Figure 2 shows the relationship between these units. These data formats are synchronised to the master beacon signal. To accommodate different applications in a single framework, this standard fixes the length of protocol frames to 16 ms which gives a permissible level of latency in most applications. A middleframe consists of frames. Sixteen middleframes constitute a superframe.

A frame is categorised into one of the seven kinds depending on its use: (1) a beacon frame (BF), (2) a fast beacon frame (FBF), (3) a request control frame (RCF), (4) a master control frame (MCF), (5) an RCF acknowledge control frame (RACF), (6) an MCF acknowledge control frame (MACF), and (7) a payload frame (PF). All the frames except the payload frame (PF) are control frames. All the frames have an identical format consisting of Lock Time, Preamble, Header, Message, and EoF Delimiter (see 8.2). Header is used to identify the kind of the frame. The message field is used to convey information and data necessary for communications (see 7.1-7.7).

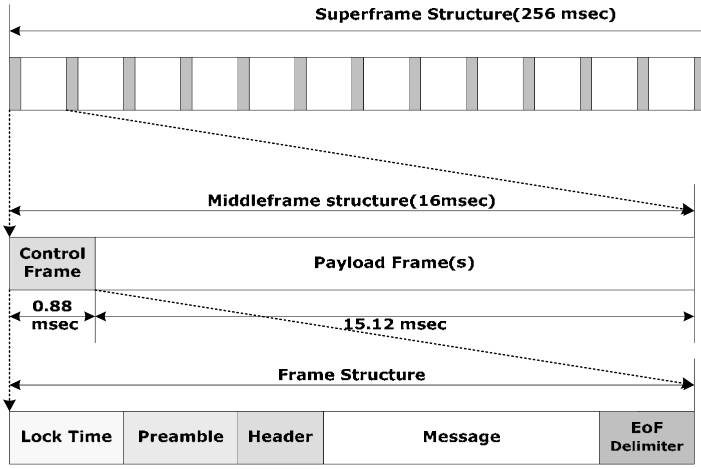

Figure 2 — Data formats: a frame, a middleframe, and a superframe.

A middleframe consists of one control frame and one or more payload frames (PF's). The middleframe starts with a control frame whose length is fixed to 0.88 ms. The length of the middleframe is fixed to 16 ms. The length of the payload frames varies depending on applications. The maximum number of payload frames within a middleframe is eighteen. Carrier frequencies hop in accordance with the middleframes.

A superframe consists of sixteen middleframes and is of 256 ms. The superframes have two modes: the normal mode and the fast synchronisation mode (see 8.3.2). The fast synchronisation mode is used for robust synchronisation. In the fast synchronisation mode, a frame called 'fast beacon frame (FBF)' is used instead of 'beacon frame (BF)'. Two modes may be interchangeably adopted by the unit of a superframe.

For security reasons, the preamble in the frame uses Gold codes for group identification. The message field data are also encrypted with security codes (see 9.3.2).

The MAC/PHY services and primitives will be defined and described in Section 6.

This standard uses the 2.4 GHz band and offers two classes of power transmission levels. Class one is up to 100 mW and class two is up to 10 mW. As a modulation scheme, the standard uses (G)FSK (see 9).

6 Interlayer service specification

This clause defines the interface between the MAC and PHY layers, and between the MAC layer and the upper layer.

6.1 Overview

Both MAC and PHY layers conceptually have management entities, called the MLME (MAC Layer Management Entity) and the PLME (PHY Layer Management Entity) respectively. These entities provide a service interfaces for the layer management functions.

The PHY provides data and management services through two SAPs (Service Access Points). The PHY data services are provided through the PD-SAP (PHY Data SAP), and PHY management services are provided through the PLME-SAP. The DME-PLME_SAP is equivalent to MLME-PLME-SAP except that it operates through DME rather than MLME.

The MAC provides data and management services through two SAPs (Service Access Points). The MAC data services are provided through the MAC-SAP, and MAC management services are provided through the MLME-SAP.

In order to provide correct MAC operation, each device must possess a DME (Device Management Entity). The DME is a layer-independent entity and act under the direction of a higher-level management application. Figure below depicts the relationships between the various management entities.

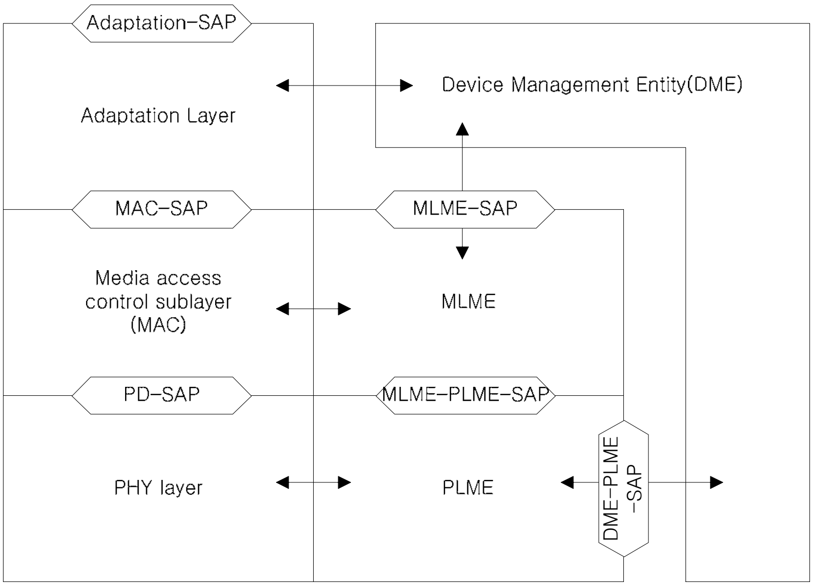

Figure 3 — The protocol model used in this standard

6.2 General format of management primitives

Each sublayer's specific management information is organized into the relevant Management information base (MIB). Corresponding to the MIB of the PAN, the LAN/MAN contains the Management Information Base (MIB) that operates according to the Simple Network Management Protocol (SNMP). However, since management within Network is restricted to an individual network (i.e. one network does not interfere in the management of another) the MIB is used to define the specifications of each sublayer.

MLME and PLME are assumed to have a MIB for each sublayer, and the management primitives of the MIB are exchanged by means of management SAPs. The manager can "GET" or "SET" the value of the MIB attribute via the primitives. The "SET" request primitive can also trigger certain actions within the relevant layer.

A "GET" or "SET" primitive may be expressed in the form of a request accompanying a confirm primitive. Such primitives have the prefix MLME or PLME depending on whether the point of exchange is the MAC SAP or the PHY SAP. DME utilizes the services provided by MLME through the MLME SAP.

In Table 1, "XX" stands for "MLME" or "PLME", and the parameters of the primitives are defined in Table 2.

Table 1 — General management primitive overview

Name	Request	Confirm
XX-GET	6.2.1	6.2.2
XX-SET	6.2.3	6.2.4

Table 2 — MLME/PLME general management primitive parameters

Name	Type	Valid range	Description
MIBattribute	Octet string	Any MIB attribute	MIB attribute name
MIBvalue	Variable		MIB value
ResultCode	Enumeration	SUCCESS, INVALID_MIB_ATTRIBUTE, READ_ONLY_MIB_ATTRIBUTE, WRITE_ONLY_MIB_ATTRIBUTE	Result of MLME or PLME request

6.2.1 MLME-GET.request and PLME-GET.request

This primitive requests information about the relevant MAC MIB or PHY MIB. The semantics of these primitives are as follows.

```
XX-GET.request   (
                 MIBattribute
                 )
```

The primitive parameters are defined in Table 2.

6.2.1.1 When generated

DME and MLME (in the case of a PLME-GET.request) create these primitives to retrieve information from the MAC or PHY MIB.

6.2.1.2 Effect of receipt

The relevant management entity fetches the requested MIB attribute from the database and returns the value as the result of XX-GET.confirm.

6.2.2 MLME-GET.confirm and PLME-GET.confirm

This primitive returns the result of an information request to the relevant MAC MIB or PHY MIB. The semantics of these primitives are as follows.

```
XX-GET.confirm    (
                  Status,
                  MIBattribute,
                  MIBattributevalue
                  )
```

The primitive parameters are defined in Table 2.

6.2.2.1 When generated

DME or MLME (in the case of a PLME-GET.confirm) creates these primitives in response to an XX-GET.request.

6.2.2.2 Effect of receipt

If the status is SUCCESS, these primitives return the value of the relevant MIB attribute, otherwise they return the error code in the status field. Valid error status values include INVALID_MIB_ATTRIBUTE and WRITE_ONLY_MIB_ATTRIBUTE.

6.2.3 MLME-SET.request and PLME-SET.request

These primitives attempt to set the value of the relevant MAC MIB or PHY MIB attribute to the specified parameter. The semantics of these primitives is as follows.

```
XX-SET.request    (
                  MIBattribute,
                  MIBattributevalue
                  )
```

The primitive parameters are defined in Table 2.

6.2.3.1 When generated

These primitives are created when DME or MLME (in the case of PLME-SET.request) tries to set the relevant MAC/PHY MIB attribute.

6.2.3.2 Effect of receipt

The relevant management entity tries to alter the value of the MIB attribute in the database. If the MIB is a reference to certain actions, this is interpreted as a request to execute the action. The management entity that receives this command responds by returning the result through a call to XX-SET.confirm.

6.2.4 MLME-SET.confirm and MLME-SET.confirm

This primitive returns the result of the attempt to set the MAC MIB or PHY MIB attribute. The semantics of this primitive are as follows.

```
XX-SET.confirm    (
                  Status,
                  MIBattribute
                  )
```

The primitive parameters are defined in Table 2.

6.2.4.1 When generated

DME or MLME (in the case of PLME-SET.confirm) create this primitive in order to respond to the XX-SET.request.

6.2.4.1 Effect of receipt

If the Status is SUCCESS, this means that the MIB attribute was set to the requested value. Otherwise, the Status field shows the error description. If the specified MIB attribute refers to a certain action, the primitive represents the success or failure of the execution of that action. Possible error status values include INVALID_MIB_ATTRIBUTE and READ_ONLY_MIB_ATTRIBUTE.

6.3 MLME-SAP

In this subclause, the services that MLME provides to DME are defined. These definitions are conceptual and do not specify a certain implementation or external interface.

The MLME SAP primitive generally follows the format of an ACTION.confirm in response to an ACTION.request. The ACTION.indication is used to inform DME of events from other stations. DME uses the services provided by MLME through MLME SAP, and those primitives are outlined in Table 3.

Table 3 — MLME primitive summary

Name	Request	Indication	Response	Confirm
MLME-GET	6.3.1			6.3.2
MLME-MASTER-START	6.3.3			6.3.4
MLME-RESET	6.3.5			6.3.6
MLME-SCAN	6.3.7			6.3.8
MLME-SET	6.3.9			6.3.10

Table 4 — MLME-SAP parameters

Name	Type	Valid range	Description
MIBAttribute	Enumeration		Desired physical layer MIB attribute
MIBStatus	Enumeration	SUCCESS, INVALID_ATTRIBUTE,	Result of request for MIB attribute information

		INVALID_VALUE	
MIBAttributeValue	Various	Attribute specific	Desired physical layer MIB attribute value
ResetResult Code	Enumeration	SUCCESS, FAILED	Response to reset request
ScanNumber	integer	0 ~ 65535	Scan duration is ScanNumber * 256 ms
ScanStartFreq	integer	0 ~ 3	Scan start frequency. Scan frequency round as 0 -> 1 -> 2 -> 3-> 0 (0 : freq 0, 1 : freq 26, 2 : freq 52, 3 : freq 78)
ScanResult Code	integer	SUCCESS, FAILED, INVALID_VALUE	Return Scan result code
MasterStart ResultCode	integer	SUCCESS, FAILED, INVALID_VALUE	Return Master-Start result code

6.3.1 MLME-GET.request

This primitive requests Information about a MAC sublayer MIB attribute.

6.3.1.1 Definition of service primitives

The semantics of this primitive are:

MLME-GET.request (
MIBAttribute
)

Table 4 define the parameter of this primitive.

6.3.1.2 When generated

This occurs by DME to obtain information from the MAC sublayer MIB of MLME..

6.3.1.3 Effect of receipt

The receipt of the MLME-GET.request primitive by the MAC sublayer entity extracts the requested MIB attribute from the database and sends the results through a MLME-GET.confirm primitive.

6.3.2 MLME-GET.confirm

This primitive report result of the requested information from the MAC sublayer MIB.

6.3.2.1 Definition of service primitives

The semantics of this primitive are:

MLME-GET.confirm (
MIBstatus,
MIBAttribute,

MIBAttributeValue

)

Table 4 define the parameter of this primitive.

6.3.2.2 When generated

MLME generates this as a response to a MLME-GET.request primitive and sends it to DME.

6.3.2.3 Effect of receipt

If the state parameter is SUCCESS the requested MAC sublayer MIB value is sent, otherwise an error is indicated.

6.3.3 MLME-MASTER-START.request

This primitive requests the process of creating a new network.

6.3.3.1 Definition of service primitives

The semantics of this primitive are:

```
MLME-MASTER-START.request        (
                                  MIBstatus,
                                  MIBAttribute,
                                  MIBAttributeValue
                                  )
```

Table 4 define the parameter of this primitive.

6.3.3.2 When generated

This primitive is generated by the next higher layer and issued to its MLME to create a new network.

6.3.3.3 Effect of recipt

This primitive initiate the piconet described in 7.1. The MLME subsequently issues an MLME-MASTER-START.confirm that reflects the results of the creation procedure.

6.3.4 MLME-MASTER-START.confirm

This primitive reports the results of a piconet creation.

6.3.4.1 Definition of service primitives

The semantics of this primitive are:

```
MLME-MASTER-START.confirm        (
                                  MasterStartResultCode
                                  )
```

Table 4 define the parameter of this primitive.

6.3.4.2 When generated

This primitive is generated by the MLME as a result of an MLME-MASTER-START.request.

6.3.4.3 Effect of recipt

MLME reports the result of the creation process of network. A ResultCode of SUCCESS indicates that the station is now the master.

6.3.5 MLME-RESET.request

This primitive requests a reset of the MAC sublayer.

6.3.5.1 Definition of service primitives

The semantics of this primitive are:

```
MLME-RESET.request    (
                        )
```

This primitive has no parameters.

6.3.5.2 When generated

This is generated whenever a MAC sublayer reset is requested.

6.3.5.3 Effect of receipt

The MAC sublayer resets all transceiver state machines to their initial states.

6.3.6 MLME-RESET.confirm

This primitive reports result of reset the MAC sublayer.

6.3.6.1 Definition of service primitives

The semantics of this primitive are:

```
MLME-RESET.confirm    (
                        ResetResultCode
                        )
```

Table 4 define the parameter of this primitive.

6.3.6.2 When generated

MLME generates this as the result of a MLME-RESET.request.

6.3.6.3 Effect of recipt

DME or Adaptation layer is notified of the result of the reset.

6.3.7 MLME-SCAN.request

This primitive define how a device can determine the presence or absence of PANs in a communications channel.

All devices shall provide an interface for these scan primitives.

6.3.7.1 Definition of service primitives

The semantics of this primitive are:

MLME-SCAN.request (

ScanNumber,

ScanStartFreq

)

Table 4 define the parameter of this primitive.

6.3.7.2 When generated

This primitive is generated by the next higher layer and issued to its MLME to initiate a channel scan to search for master device activity within the POS of the device.

6.3.7.3 Effect of receipt

When MLME receives this primitive from DME, it executes a manual SCAN of the channels in the Channel List. When this SCAN is completed, MLME responds to DME with the result of the SCAN through a call to MLME-SCAN.confirm.

6.3.8 MLME-SCAN.confirm

This primitive and its parameters are collected during the SCAN and sent back upon the completion of the SCAN.

6.3.8.1 Definition of service primitives

The semantics of this primitive are:

MLME-SCAN.confirm (

ScanResultCode

)

Table 4 define the parameter of this primitive.

6.3.8.2 When generated

This message is sent to DME when MLME completes the requested SCAN or when the parameters of MLME-request are incorrect.

6.3.8.3 Effect of receipt

On receipt of the MLME-SCAN.confirm primitive, The DME is notified of the results of the scan procedure. If the requested scan was successful, the status parameter will be set to SUCCESS. Otherwise, the status parameter indicates the error.

6.3.9 MLME-SET.request

This primitive request to set the MAC sublayer MIB attribute to the specified value.

6.3.9.1 Definition of service primitives

The semantics of this primitive are:

MLME-SET.request (

MIBAttribute,

MIBAttributeValue

)

Table 4 define the parameter of this primitive.

6.3.9.2 When generated

This occurs by DME to set the MAC sublayer MIB attribute to the specified value and sends it to MLME.

6.3.9.3 Effect of receipt

The receipt of the MLME-SET.request primitive by the MAC sublayer entity attempts to store the specified MAC sublayer MIB attribute in the database and reports the result through a MLME-SET.confirm primitive.

6.3.10 MLME-SET.confirm

This primitive reports result of the attempt to set the MAC sublayer MIB attribute to the specified value.

6.3.10.1 Definition of service primitives

The semantics of this primitive are:

```
MLME-SET.confirm        (
                       MIBstatus,
                       MIBAttribute
                       )
```

Table 4 define the parameter of this primitive.

6.3.10.2 When generated

MLME sends this to Adaptation layer as the response to the MLME-SET.request primitive.

6.3.10.3 Effect of receipt

If the state value is SUCCESS it means the MIB attribute was set as requested, otherwise an error is indicated if the MIB attribute was unable to be set for some reason.

6.4 MAC-SAP

The MAC SAP is the logical interface between the MAC and the higher adaptation layer. This logical interface incorporates a set of primitives and their definitions. These primitives and definitions are described conceptually here, but through this the process of the parameters exchanged between the MAC and adaptation layer can be understood. Table 5 lists the primitives supported by the MAC-SAP. These primitives are discussed in the subclauses referenced in the table.

Table 5 — MAC-SAP primitive summary

Name	Request	Confirm	Indication	Response
MAC-DATA	6.4.1	6.4.2	6.4.3	

Table 6 — MAC-SAP parameters

Name	Type	Valid range	Description
SourceID	integer		Target DEVID of MLME request
DestinationID	integer		DEVID initiating the MLME

			request
Length	Unsigned Short Integer	0-65535	MSDU length
data	variable length Octet	-	Data portion of MSDU
ResultCode	Enumeration	SUCCESS, INVALID_MIB_ATTRIBUTE	Result of MAC request

6.4.1 MAC-DATA.request

This primitive initiates the data transfer from one MAC entity to another MAC entity or entities.

6.4.1.1 Definition of service primitives

The semantics of this primitive are:

```
MAC-DATA.request        (
                        SourceID,
                        DestinationID,
                        Length,
                        Data
                        )
```

Table 6 define the parameter of this primitive.

6.4.1.2 When generated

This occurs when the adaptation layer entity requests transmission of a MSDU(i.e. APDU) to the MAC sublayer entity.

6.4.1.3 Effect of recipt

When this primitive is received, the MAC formats the MSDU according to the input parameters and sends it to the PHY-SAP; then the MSDU passes through the wireless media and is sent to the peer MAC entity. When the MAC sublayer entity has completed the sending, it will issue the MAC-DATA.confirm primitive with a status of SUCCESS.

6.4.2 MAC-DATA.confirm

This primitive confirm that the Adaptation layer entity has sent a MSDU (APDU) to another Adaptation layer entity.

6.4.2.1 Definition of service primitives

The semantics of this primitive are:

```
MAC-DATA.confirm        (
                        SourceID,
                        DestinationID,
                        ResultCode
                        )
```

Table 6 define the parameter of this primitive.

6.4.2.2 When generated

The MAC sublayer entity sends this primitive to the Adaptation layer entity as a response to the MAC-DATA.request primitive when the requested MSDU is transmitted.

6.4.2.3 Effect of receipt

On receipt of the MAC-DATA.confirm primitive, the Adaption layer entity is notified of the result of its request to transmit. If the transmission attempt was successful, the status parameter is set to SUCCESS.

6.4.3 MAC-DATA.indication

This primitive indicates to the adaptation layer that a MSDU has been received.

6.4.3.1 Definition of service primitives

The semantics of this primitive are:

```
MAC-DATA.indication    (
                       SourceID,
                       DestinationID,
                       Length,
                       Data
                       )
```

Table 6 define the parameter of this primitive.

6.4.3.2 When generated

This occurs when MSDU received by the MAC has been successfully processed.

6.4.3.3 Effect of receipt

The receipt of the MAC-DATA.indication primitive, the adaptation layer is notified of the arrival of an APDU(i.e. MSDU) across the MAC data service.

6.5 PLME-SAP

The PHY layer management object service access points (MLME-PLME-SAP) enable the operational language between MLME and PLME. Additional physical layer management object service access points (DME-PLME-SAP) enable the operational language between DME and PLME, and this interface is equivalent to the MLME-PLME-SAP interface. Table 7 defines the primitives supported by PLME-SAP. Table 8 lays out the individual parameters.

Table 7 — PLME-SAP primitive summary

Name	Request	Confirm	Indication	Response
PLME-GET	6.6.1	6.6.2		
PLME-SET	6.6.3	6.6.4		
PLME-RESET	6.6.5	6.6.6		

Table 8 — PLME-SAP parameters

Name	Type	Valid range	Description
MIBAttribute	Enumeration		Desired physical layer MIB attribute
MIBStatus	Enumeration	SUCCESS, INVALID_ATTRIBUTE, INVALID_VALUE	Result of request for MIB attribute information
MIBAttributeValue	Various	Attribute specific	Desired physical layer MIB attribute value
ResetResult Code	Enumeration	SUCCESS, FAILED	Response to reset request

6.5.1 PLME-GET.request

This primitive requests Information about a PHY layer MIB attribute.

6.5.1.1 Definition of service primitives

The semantics of this primitive are:

PLME-GET.request (
MIBAttribute
)

Table 8 define the parameter of this primitive.

6.5.1.2 When generated

This occurs by DME to obtain information from the PHY layer MIB of PLME..

6.5.1.3 Effect of receipt

The receipt of the PLME-GET.request primitive by the PHY entity extracts the requested MIB attribute from the database and sends the results through a PLME-GET.confirm primitive.

6.5.2 PLME-GET.confirm

This primitive report result of the requested information from the PHY layer MIB.

6.5.2.1 Definition of service primitives

The semantics of this primitive are:

PLME-GET.confirm (
MIBstatus,
MIBAttribute,
MIBAttributeValue
)

Table 8 define the parameter of this primitive.

6.5.2.2 When generated

PLME generates this as a response to a PLME-GET.request primitive and sends it to DME.

6.5.2.3 Effect of recipt

If the state parameter is SUCCESS the requested PHY layer MIB value is sent, otherwise an error is indicated.

6.5.3 PLME-SET.request

This primitive request to set the PHY layer MIB attribute to the specified value.

6.5.3.1 Definition of service primitives

The semantics of this primitive are:

```
PLME-SET.request        (
                    MIBAttribute,
                    MIBAttributeValue
                    )
```

Table 8 define the parameter of this primitive.

6.5.3.2 When generated

This occurs by DME to set the PHY layer MIB attribute to the specified value and sends it to PLME.

6.5.3.3 Effect of receipt

The receipt of the PLME-SET.request primitive by the PHY entity attempts to store the specified PHY layer MIB attribute in the database and reports the result through a PLME-SET.confirm primitive.

6.5.4 PLME-SET.confirm

This primitive reports result of the attempt to set the PHY layer MIB attribute to the specified value.

6.5.4.1 Definition of service primitives

The semantics of this primitive are:

```
PLME-SET.confirm        (
                    MIBstatus,
                    MIBAttribute
                    )
```

Table 8 define the parameter of this primitive.

6.5.4.2 When generated

PLME sends this to DME as the response to the PLME-SET.request primitive.

6.5.4.3 Effect of receipt

If the state value is SUCCESS it means the MIB attribute was set as requested, otherwise an error is indicated if the MIB attribute was unable to be set for some reason.

6.5.5 PLME-RESET.request

This primitive requests a reset of the PHY layer.

6.5.5.1 Definition of service primitives

The semantics of this primitive are:

```
PLME-RESET.request    (
                        )
```

This primitive has no parameters.

6.5.5.2 When generated

This is generated whenever a PHY layer reset is requested.

6.5.5.3 Effect of receipt

The PHY layer resets all transceiver state machines to their initial states.

6.5.6 PLME-RESET.confirm

This primitive reports result of reset the PHY layer.

6.5.6.1 Definition of service primitives

The semantics of this primitive are:

```
PLME-RESET.confirm    (
                        ResetResultCode
                        )
```

Table 8 define the parameter of this primitive.

6.5.6.2 When generated

PLME generates this as the result of a PLME-RESET.request.

6.5.6.3 Effect of receipt

DME or MLME is notified of the result of the reset.

6.6 PD-SAP

The PD-SAP supports the transmission of MPDUs between peer MAC sublayer entities. Table 9 lists the primitives supported by the PD-SAP. These primitives are discussed in the subclauses referenced in the table.

Table 9 — PD-SAP primitives

Name	Request	Confirm	Indication	Response
PD-DATA	5.6.1	5.6.2	5.6.3	

Table 10 — PD-SAP parameters

Name	Type	Valid range	Description
psduLength	Unsigned Short Integer	≤ aMaxPHYPacketSize	The number of octets contained in the PSDU received by the PHY entity.
psdu	Set of octets	-	The set of octets forming the PSDU received by the PHY entity.
status	Enumeration	SUCCESS (EoF)	The result of the request to transmit a packet.
rssi	Integer		RSSI Value

6.6.1 PD-DATA.request

This primitive requests the transmission of a MPDU from the MAC sublayer to the local PHY entity.

6.6.1.1 Definition of service primitives

The semantics of this primitive are:

```
PD-DATA.request  (
                        psduLength,
                        psdu
                        )
```

Table 10 define the parameter of this primitive.

6.6.1.2 When generated

This occurs when the MAC sublayer entity requests transmission of a MPDU to the PHY layer entity.

6.6.1.3 Effect of receipt

The receipt of the PD-DATA.request primitive by the PHY entity will cause the transmission of the supplied PSDU. When the PHY entity has completed the transmission, it will issue the PD-DATA.confirm primitive with a status of SUCCESS.

6.6.2 PD-DATA.confirm

This primitive confirm that the MAC sublayer entity has sent a MPDU (PSDU) to another MAC sublayer entity.

6.6.2.1 Definition of service primitives

The semantics of this primitive are:

```
PD-DATA.confirm  (
                        status
                        )
```

Table 10 define the parameter of this primitive.

6.6.2.2 When generated

The PHY layer entity sends this primitive to the MAC sublayer entity as a response to the PD-DATA.request primitive when the requested PSDU is transmitted.

6.6.2.3 Effect of receipt

On receipt of the PD-DATA.confirm primitive, the MAC sublayer entity is notified of the result of its request to transmit. If the transmission attempt was successful, the status parameter is set to SUCCESS.

6.6.3 PD-DATA.indication

This primitive indicates the received PSDU from PHY layer to the MAC sublayer entity.

6.6.3.1 Definition of service primitives

The semantics of this primitive are:

```
PD-DATA.indication      (
                      psduLength,
                      psdu
                      rssi
                      )
```

Table 10 define the parameter of this primitive.

6.6.3.2 When generated

This occurs when the PHY layer sends the received PSDU to the MAC sublayer entity.

6.6.3.3 Effect of recipt

The receipt of the PD-DATA.indication primitive, the MAC sublayer is notified of the arrival of an MPDU across the PHY data service.

7 MAC PDU format

This clause specifies the formats of the MAC PDU (MPDU).

MAC frame is consists of one control frame and more than one payload frame. Control frame is categorized into one of the six kinds depending on its use: (1) beacon frame (BF), (2) fast beacon frame (FBP), (3) request control frame (RCF), (4) master control frame (MCF), (5) RCF acknowledge control frame (RACF), and (6) MCF acknowledge control frame (MACF).

Figure 4 shows the relationship between MPDU and PPDU in a frame structure.

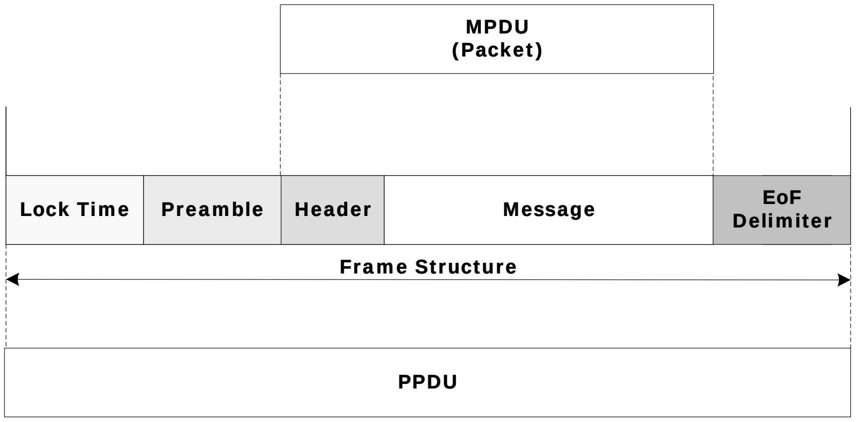

Figure 4 — MPDU in Frame structure

The format of each control frame is described in 7.1 through 7.6. The format of payload frame is described in 7.7.

7.1 MPDU of Beacon Frame (BF)

BFs are used to maintain synchronization. There are two BFs during a single normal superframe. The master sends information used for synchronization, and the slave adjusts synchronization for BFs.

MPDU format of BF is as shown in Figure 5.

7.1.1 Open flag (OF, 2 bits)

Provides open flag information. This is a flag that displays whether an open code is applied to the current frame. It comprises of a GCOF used for displaying whether the group code is applied and a SCOF used for displaying whether the security code is applied. When the GCOF is 1, this means that an open group code has been applied. When it is 0, a closed group code has been applied. When the SCOF is 1, this means that an open security code has been applied. When it is 0, a closed security code has been applied.

7.1.2 MAC version (6 bits)

Provides information about the MAC Version, and has a value between 0x00 to 0x3F.

7.1.3 Address mode (ADDM, 2 bits)

Provides information about whether a MAC address exists. The ADDM comprises of a bit used for displaying whether a source MAC address exists and another bit used for displaying the destination MAC address.

7.1.4 PHY version (6 bits)

Provides information about the PHY Version, and has a value between 0x00 to 0x3F.

7.1.5 Frame type (8 bits)

The Frame Type is a field used for displaying the BF Type.

7.1.6 Superframe mode control (SFMC, 2 bits)

The Superframe Mode Control (SFMC) is a field used for selecting a mode of the superframe. It comprises of the current superframe mode (CSFM) and the next superframe mode (NSFM). That CSFM is 1 means the current superframe is a normal superframe. When it is 0, the current superframe is a fast synchronization superframe. That NSFM is 1 means the next superframe is a normal superframe. When it is 0, the current superframe is a fast synchronization superframe.

7.1.7 Upper layer frame size (ULPS, 6 bits)

This field provides information on the size of the data from the upper layer.

7.1.8 Source MAC address (64 bits)

This field provides the MAC address of the master which is sending BFs.

7.1.9 Superframe counter (SFC, 4 bits)

This field provides information on the superframe counter. The value circulates from 0 to 15.

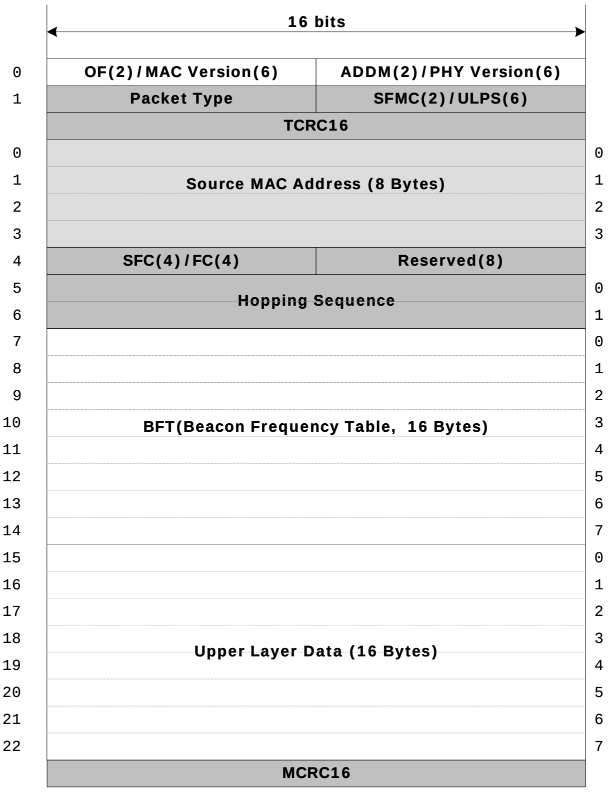

Figure 5 — MPDU format of Beacon Frame

7.1.10 Middleframe counter (FC, 4 bits)

This field provides information on the middleframe counter. The value circulates from 0 to 15.

7.1.11 Hopping sequence (32 bits)

This field provides the hopping sequence of the frequencies that were chosen for communication.

7.1.12 BF frequency table (BFFT, 16 bytes)

This field provides information on the sequence of the frequencies used for the partial band hopping. BFFT contains a table of 16 frequencies being used for communication.

7.1.13 Upper layer data (16 bytes)

This field is used for transmission of the data from the upper layer.

7.2 MPDU of Fast Beacon Frame (FBF)

This field is used for initial fast synchronization. There are 16 FBFs in a single fast synchronization superframe. The master sends information for synchronization in the FBFs, and the slaves are synchronised using these FBFs.

MPDU format of FBF is shown in Figure 6.

7.2.1 Open flag (OF, 2 bits)

This field provides information on whether an open code is applied to the current middleframe. This field comprises of GCOF which is used to indicate whether a group code is applied and SCOF which is used to indicate whether a security code is applied. That GCOF is 1 means an open group code has been applied. When it is 0, a closed group code has been applied. That SCOF is 1 means an open security code has been applied. When it is 0, a closed security code has been applied.

7.2.2 MAC version (6 bits)

This field provides information on the MAC Version, and has a value between 0x00 to 0x3F.

7.2.3 Address mode (ADDM, 2 bits)

This field provides information on whether MAC addresses exist. The ADDM comprises of two bits: one bit is used to indicate whether a source MAC address exists and the other bit is used to indicate whether a destination MAC address exists. One means an address exists.

7.2.4 PHY version (6 bits)

This field provides information on the PHY Version, and has a value between 0x00 to 0x3F.

7.2.5 Frame type (8 bits)

This field is used to indicate the type of the current frame.

7.2.6 Superframe mode control (SFMC, 2 bits)

This field is used to select the mode of the superframe. It comprises of the current superframe mode (CSFM) and the next superframe mode (NSFM). That CSFM is 1 means the current superframe is a normal superframe. When it is 0, the current superframe is a fast synchronization superframe. That NSFM is 1 means the next superframe is a normal superframe. When it is 0, the next superframe is a fast synchronization superframe.

7.2.7 Upper layer frame size (ULPS, 6 bits)

This field provides information on the size of the data from the upper layer.

7.2.8 Source MAC address (64 bits)

This field provides the MAC address of the master which is sending BFs.

7.2.9 Superframe counter (SFC, 4 bits)

This field provides information on the superframe counter. The value circulates from 0 to 15.

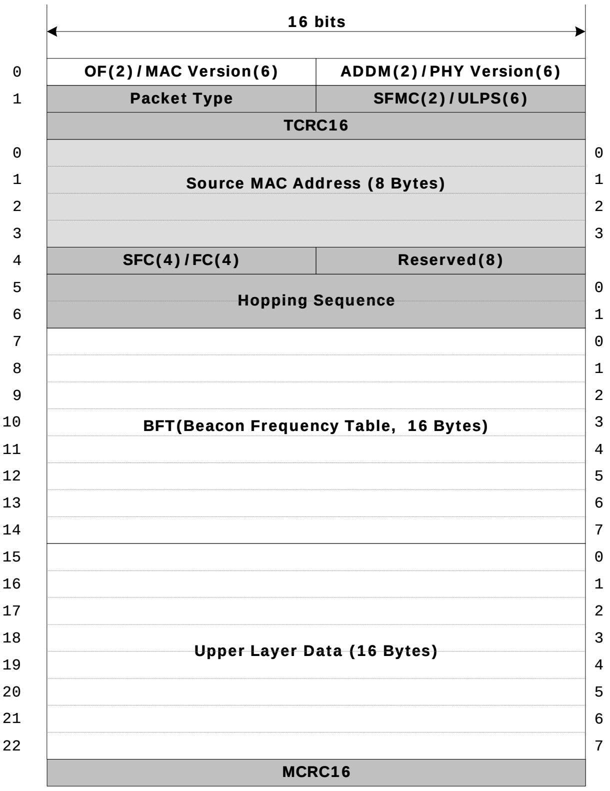

Figure 6 — MPDU format of Fast Beacon Frame (FBF)

7.2.10 Middleframe counter (SC, 4 bits)

This field provides information on the middleframe counter. The value circulates from 0 to 15.

7.2.11 Hopping sequence (32 bits)

This field provides the hopping sequence of the frequencies that were chosen for communication.

7.2.12 BF frequency table (BFFT, 16 bytes)

This field provides information on the sequence of the frequencies used for the partial band hopping. BFFT contains a table of 16 frequencies being used for communication.

7.2.13 Upper layer data (16 Bytes)

This field is used for transmission of the data from the upper layer.

7.3 MPDU of Request Control Frame (RCF)

RCFs are used to exchange control information between devices. In response to RCF, Acknowledge Control Frame of RCF (RACF) is issued. The RCF is used for multiple simultaneous communications among devices in a group. When two or more devices initiate communications at the same time, there may be collision. To ensure reliability of control information, the random back off must be implemented when collision occurs. All the handsets must be able to send and receive information. When not sending information, handsets must be able to receive information.

MPDU format of RCF is shown in Figure 7.

7.3.1 Open flag (OF, 2 bits)

This field provides information on whether an open code is applied to the current middleframe. It comprises of GCOF which is used to indicate whether a group code is applied and SCOF which is used to indicate whether a security code is applied. That GCOF is 1 means an open group code has been applied. When it is 0, a closed group code has been applied. That SCOF is 1 means an open security code has been applied. When it is 0, a closed security code has been applied.

7.3.2 MAC version (6 bits)

This field provides information on the MAC Version, and has a value between 0x00 to 0x3F.

7.3.3 Address mode (ADDM, 2 bits)

This field provides information on whether MAC addresses exist. The ADDM comprises of two bits: one bit is used to indicate whether a source MAC address exists and the other bit is used to indicate whether a destination MAC address exists.

7.3.4 PHY version (6 bits)

This field provides information on the PHY Version, and has a value between 0x00 to 0x3F.

7.3.5 Frame type (8 bits)

This field is used to indicate the type of the current frame.

7.3.6 Upper Layer Frame Size (ULPS, 6 bits)

This field provides information on the size of the data from the upper layer.

7.3.7 Source MAC Address (64 bits)

This field provides the MAC address of the master which is sending RCFs.

7.3.8 Destination MAC Address (64 bits)

This field provides the MAC address of the device which is to receive RCFs.

7.3.9 Upper Layer Data

This field is used for transmission of the data from the upper layer.

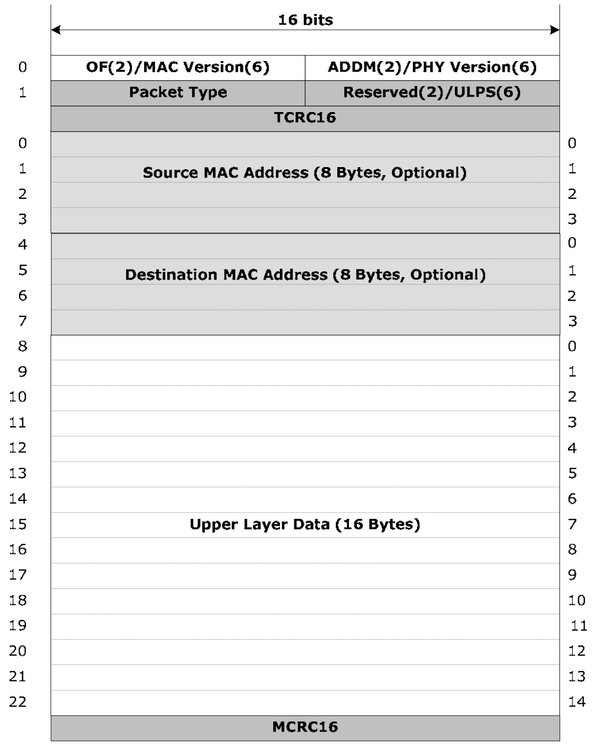

Figure 7 — MPDU format of RCF

7.4 MPDU of Master Control Frame (MCF)

MCFs are used by the master in a group to send control information to slaves. The master can send control information up to 8 devices by using a single MCF. Slave devices may respond to MCF using the frames called MACF (MCF acknowledgement control frame). MACFs are issued by the responding slaves as controlled by MCFs in a manner to avoid collision. Each responding slave takes up a different MACF slot.

MPDU format of MCF is shown in Figure 8.

7.4.1 Open flag (OF, 2 bits)

This field provides information on whether an open code is applied to the current middleframe. It comprises of GCOF which is used to indicate whether a group code is applied and SCOF which is used to indicate whether a security code is applied. That GCOF is 1 means an open group code has been applied. When it is 0, a closed group code has been applied. That SCOF is 1 means an open security code has been applied. When it is 0, a closed security code has been applied.

7.4.2 MAC version (6 bits)

This field provides information on the MAC Version, and has a value between 0x00 to 0x3F.

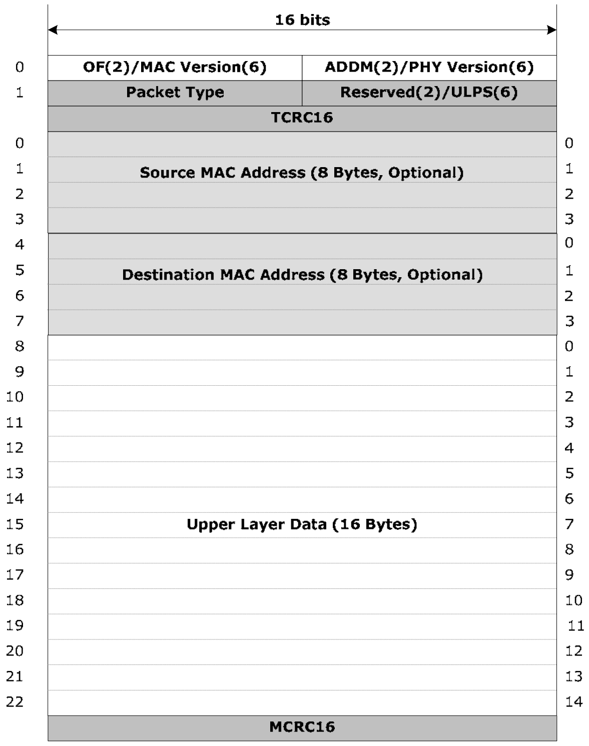

Figure 8 — MPDU format of MCF

7.4.3 Address mode (ADDM, 2 bits)

This field provides information on whether MAC addresses exist. The ADDM comprises of two bits: one bit is used to indicate whether a source MAC address exists and the other bit is used to indicate whether a destination MAC address exists.

7.4.4 PHY version (6 bits)

This field provides information on the PHY Version, and has a value between 0x00 to 0x3F.

7.4.5 Frame type (8 bits)

This field is used to indicate the type of the current frame.

7.4.6 Upper Layer Frame Size (ULPS, 6 bits)

This field provides information on the size of the data from the upper layer.

7.4.7 Source MAC Address (64 bits)

This field provides the MAC address of the master which is sending MCFs.

7.4.8 Destination MAC Address (64 bits)

This field provides the MAC address of the device which is to receive MCFs.

7.4.9 Upper Layer Data

This field is used for transmission of the data from the upper layer.

7.5 MPDU of RCF Acknowledge Control Frame (RACF)

A device receiving RCFs sends RACFs in response. The device that sent RCFs receives RACFs as an acknowledgement. RACFs are control frames that can be sent to both the master and the slave devices. After sending RCF, when a RACF response is not received as is necessary, RCF may be resent after backing off in random superframe units.

MPDU format of RACF is identical to that of RCF except for the Frame Type field.

7.6 MPDU of MCF Acknowledge Control Frame (MACF)

MACFs are issued by the slaves that need to acknowledge the reception of MCFs. The master checks MACFs to verify responses from the slaves with respect to MCFs.

MPDU format of MACF is identical to that of MCF except for the Frame Type field.

7.7 MPDU of Payload Frame (PF)

Payload frames are used to transmit data from upper layers. The number of payload frames may vary depending on the requirement of upper layers. The number may be from one to eighteen.

The MPDU format of PF is shown in Figure 9.

7.7.1 Open flag (OF, 2 bits)

This field provides information on whether an open code is applied to the current middleframe. It comprises of GCOF which is used to indicate whether a group code is applied and SCOF which is used to indicate whether a security code is applied. That GCOF is 1 means an open group code has been applied. When it is 0, a closed group code has been applied. That SCOF is 1 means an open security code has been applied. When it is 0, a closed security code has been applied.

7.7.2 MAC version (6 bits)

This field provides information on the MAC Version, and has a value between 0x00 to 0x3F.

7.7.3 Address Mode (ADDM, 2 bits)

This field provides information on whether MAC addresses exist. The ADDM comprises of two bits: one bit is used to indicate whether a source MAC address exists and the other bit is used to indicate whether a destination MAC address exists.

7.7.4 PHY Version (6 bits)

This field provides information on the PHY Version, and has a value between 0x00 to 0x3F.

7.7.5 Frame Type (8 bits)

This field is used to indicate the type of the current frame.

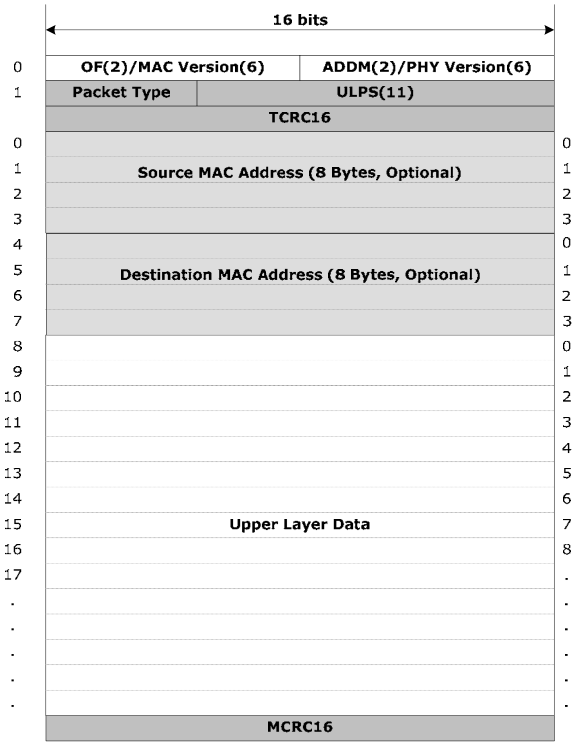

Figure 9 — MPDU format of PF

7.7.6 Upper Layer Frame Size (ULPS, 6 bits)

This field provides information on the size of the data from the upper layer.

7.7.7 Source MAC Address (64 bits)

This field provides the MAC address of the master which is sending PFs.

7.7.8 Destination MAC Address (64 bits)

This field provides the MAC address of device which is to receive PFs.

7.7.9 Upper Layer Data

This field is used for transmission of the data from the upper layer.

8 MAC functional description

This clause describes the functions of the MAC layer.

8.1 General description

In communications in a pico-net, it is required to keep the devices within the pico-net synchronized. For this purpose, in a pico-net, one device must operate as a mater, which sends synchronizing signals periodically, and the other devices operate as slaves in accordance with the synchronizing signals from the master.

Figure 10 shows a pico-net with only two terminals. One terminal must serve as a master while the other as a slave. The master regularly transmits synchronizing signals to which the slave is synchronized. Communications between the two terminals are based on this synchronization.

Figure 11 shows a pico-net with more than two devices. One device must serve as a master while the others as slaves. All the devices must be synchronized to the master's synchronizing signals. Communications between any two or more devices are carried out based on this synchronization with no further master's intervention. The master transmits synchronizing signals only to maintain the synchronization within the network. Communications between slaves are practiced directly without the master's relaying the communications.

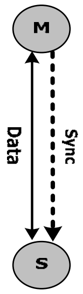

Figure 10 — A pico-net with only two devices.

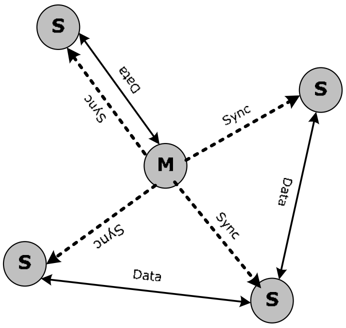

Figure 11 — A pico-net with more than two terminals

8.2 System state diagram

The master/slave operations can be expressed as a finite state machine with 10-phase states. Any device is in one of the ten states. The description of the ten states is summarised in Table 11.

Table 11 — Description of states

State	Description
Not initialized	A state before initialization.
Initialized	A state after initialization is completed; the master and slaves are determined.
Normal master sync.	A state where the device is serving as the master of the normal network cycle.
Fast master sync.	A state where the device is serving as the master of the fast synchronization network cycle.
Scanning	A state where the device is under synchronization with the master.
Normal slave sync.	A state where the device is serving as a slave in the normal superframe after synchronization with the master.
Fast slave sync.	A state where the device is serving as a slave in the fast synchronization superframe after synchronization with the master.
Passive sounding	A state where the master conducts passive sounding.
Master static sounding	A state where the master conducts static sounding.
Slave static sounding	A state where the slave conducts static sounding

Figure 12 shows the state-transition diagram. The solid line and the dotted line represent the paths of the state changes of the master and the slaves, respectively.

The network operation begins with initialisation. The initialisation starts when more than two devices within the communication range are first turned on.

When the initialisation starts, the master performs the initialisation process, regardless of whatever state it has been in. After initialization is completed, the master stays in the ‘initialised’ state. The master in the ‘initialised’ state can shift into the ‘passive sounding’ or ‘normal/fast master sync’ state.

Passive Sounding is a state where frequencies are selected by measuring the signal level at each frequency. The master may choose to put itself into the ‘passive sounding’ state if needed.

After shifting into the ‘normal/fast master sync’ state, the master sends synchronising signals. In these states, the master can communicate with the slaves synchronised with the synchronising signals. In the ‘master sync’ states, the master can shift into the ‘static sounding’ state where frequencies can be selected via special communication between the master and the slaves. In the ‘static sounding’ state, normal communications between the master and the slaves cannot be practiced. The ‘static sounding’ state can be selected by the user whenever needed.

After initialization with the master, the slaves are forced into the ‘initialised’ state. The slaves are forced into initialisation process once initialisation process is initiated, regardless of whatever state they have been in. The slaves synchronises with the master in the ‘scanning’ state after initialization. With the synchronisation information from the master, the slaves synchronise with the master and shift into the ‘normal/fast slave sync’ state. When the synchronisation information is not obtained, the slaves are again put into the ‘initialized’ state. After the slaves are synchronised with the master and put into the ‘normal/fast slave sync’ state, the slaves

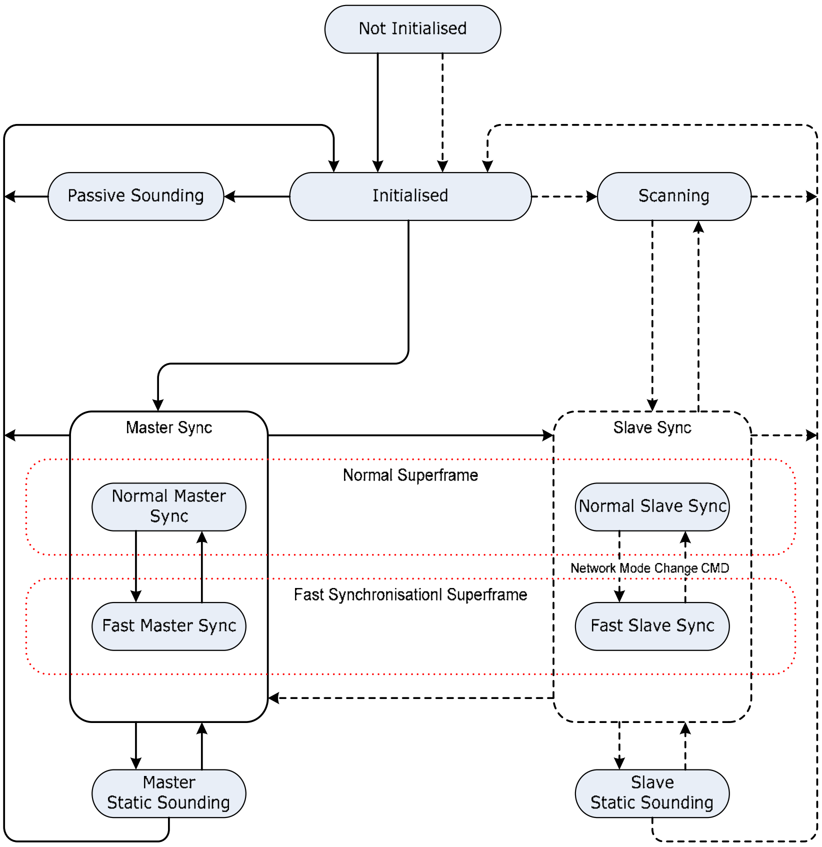

Figure 12 — State transition diagram

can communicate with the master. When a static sounding is requested from the master, the slaves shift into the ‘static sounding’ state to conduct static sounding.

8.3 Protocol structure

Figure 13 shows the hierarchical structure of the protocol. The protocol is structured based on the superframes of 256 msec each, which again consists of 16 middleframes of 16msec each. A middleframe consists of one control frame and one or more payload frames.

The middleframe is the most basic unit structure. The state of each middleframe can be set independently of the others.

The number of payload frames is determined based on the communication type (data, voice, control, etc). However, it is required to maintain the length of superframes equal for synchronised communication. The synchronisation between devices is possible only if the lengths of all superframes are equal. The synchronised communications minimize the frequency interference between devices of different services by controlling the transmission and reception based on time slots.

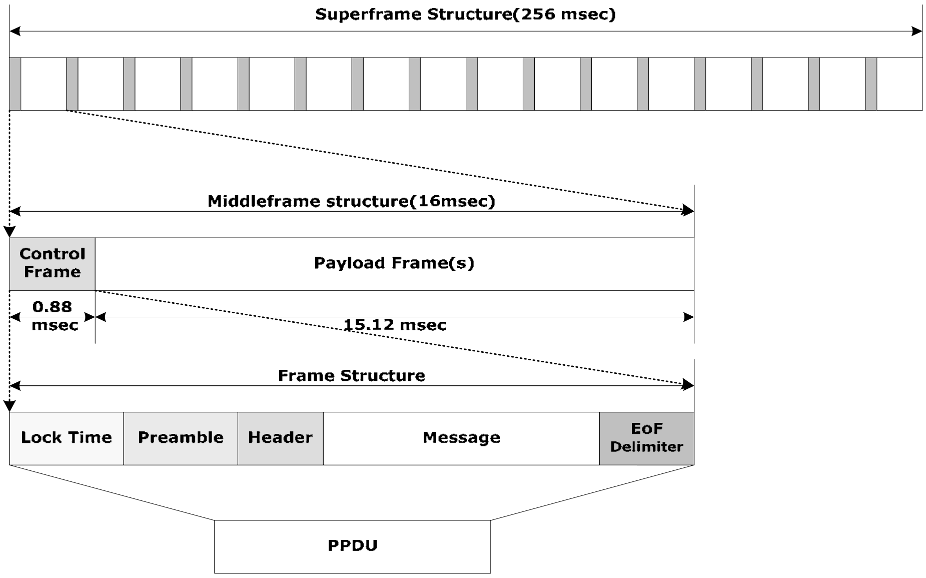

Figure 13 — The protocol structure

8.3.1 Middleframe structure

Figure 14 shows the structure of the middleframe. A middleframe consists of one control frame and one or more payload frames. The length of the control frame is fixed at 880 µsec. The number and length of payload frame within a middleframe can be set as needed. The upper layers may have various data rates depending on the number and length of the payload frames. When high data rate is needed, the number of payload frames can be reduced to lower overhead. However, transmission delay due to buffering increases in proportion to the length of middleframe. The number of payload frames must be between 1 and 18. The total length of all payload frames should be 15.12 msec.

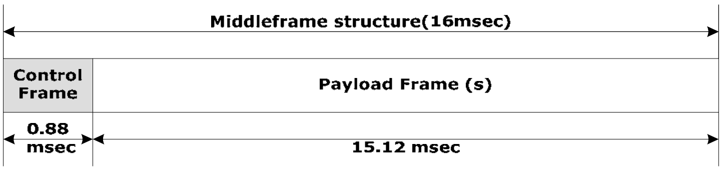

Figure 14 — Middleframe structure

8.3.2 Superframe structure

The length of a single superframe is 256 msec; the superframe consists of 16 frames. Within a superframe are 16 control frames with a length of 0.88 msec. Overall, 14.08 msec is assigned to control frames and the rest 241.92 msec to payload frame(s). Each control frame has its own unique function as described in section 7. There are two types of superframe: a normal superframe and a fast synchronization superframe.

8.3.2.1 Normal superframe

Figure 15 shows the structure of a normal superframe. There are 16 control frames in a normal superframe: two are beacon frames (BF), one is a request control frame (RCF) used when slaves send request information to the master, one is a master control frame (MCF) used when the master sends control information to the slaves, one is allocated for response to RCF, eight for response to MCF, and the remaining three are reserved.

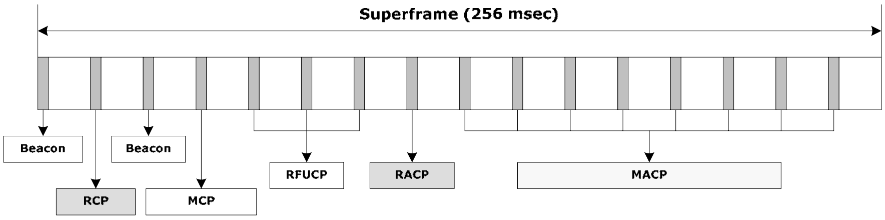

Figure 15 — Structure of a normal superframe

8.3.2.2 Fast synchronisation superframe

Figure 16 shows the structure of a fast synchronisation superframe. For a fast synchronisation, a fast synchronisation superframe is adopted. All control frames in the fast synchronisation superframe are used for synchronisation. These control frames used for synchronisation are called fast beacon frames (FBFs).

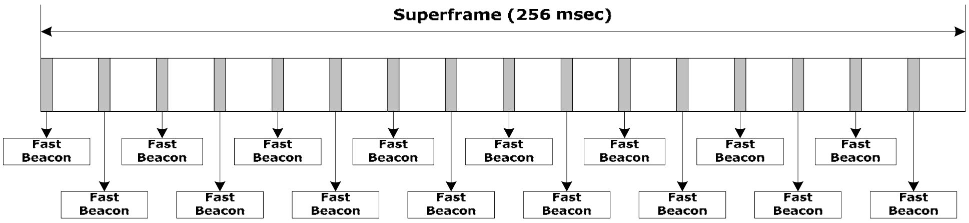

Figure 16 — Structure of a fast synchronisation superframe

8.3.2.3 Shift between superframes

For a normal operation, the normal superframe repeats itself. For a fast synchronisation, alternation between a normal superframe and a fast synchronization superframe is practiced. Figure 17 illustrates the operation of the fast synchronisation.

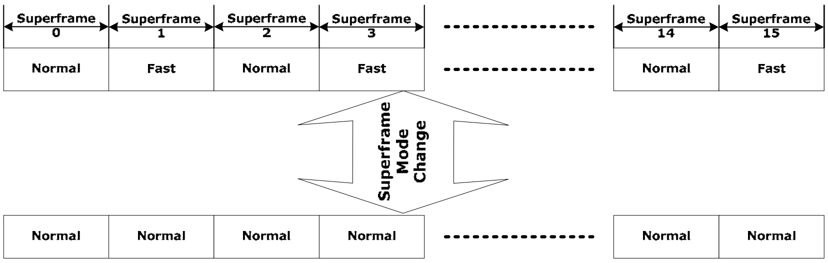

Figure 17 — Superframe mode alternation

8.3.2.4 Middleframe counter and superframe counter

Numbers are assigned to the frames and superframes to maintain the structure. The counters are in the message field of the frame. A number ‘0’ is assigned to the first middleframe in a superframe. The number increases by one in the frames that follow. A number ‘15’ is assigned to the last middleframe in the superframe. Likewise, a number is assigned to each superframe, which repeats itself with a period of 16. The number starts with 0 and ends with 15. Figure 18, 19 shows the middleframe and superframe counters, respectively.

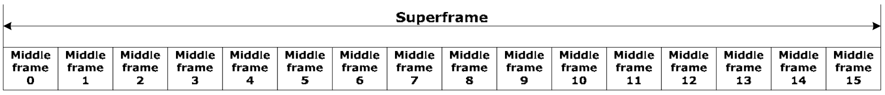

Figure 18 — Middleframe counter

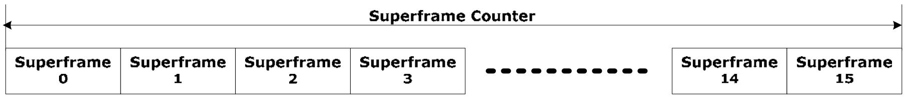

Figure 19 — Superframe counter

8.4 Frequency Operation

8.4.1 Frequency hopping control

The protocol carries out communication according to the frequency hopping table. The hopping sequence of the frequencies is in a random order out of the chosen best sixteen frequencies. The random sequence is generated by a hopping sequence generator which works as described below.

Figure 20 shows a hopping sequence generator. The generator uses 32 bit shift register to generate a maximal pseudo random sequence. The feedback tabs are [31, 21, 1, 0]. Output values are generated for every single middleframe (in every 16 msec). The sequence repeats itself every $(2^{32} - 1) \times 16$ msec.

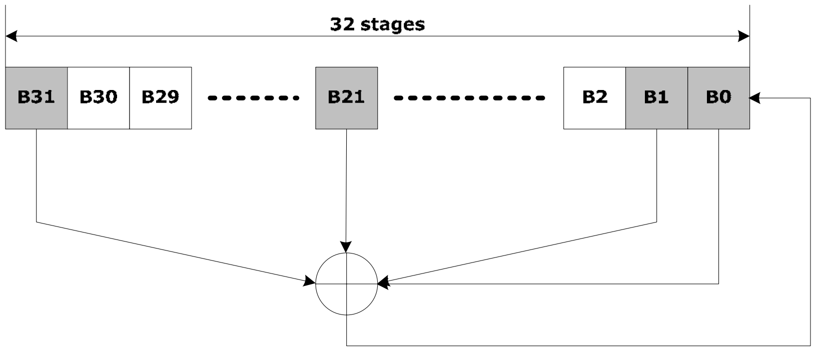

Figure 20 — The hopping sequence generator

8.4.2 Frame Frequency Mapping

This section describes how the outcomes of the hopping sequence generator are mapped to the frequencies.

The 32-bit value of every state of the hopping sequence generator is divided by 16, and the residue is taken. An offset value between 0 and 15 is added to the residue, and the resulting value is again divided by 16 and its residue is taken. The resulting values are used as the indices of the frequency hopping table. Figure 21 illustrates the frame frequency mapping scheme.

The offset values are added to provide more independent frequency channels. A different offset value means a different communication channel. All control frames use ‘0’ as the offset value.

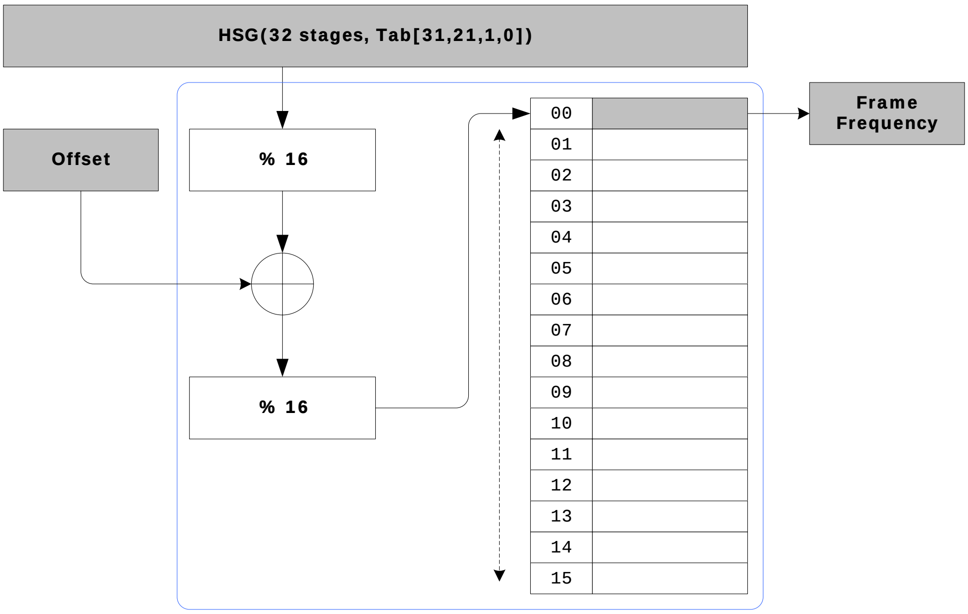

Figure 21 — Frame frequency mapping scheme

8.4.3 Frequency Diversity and Time Diversity

In the frequency band of 2.4 GHz, the communication channels are very vulnerable to fading. To maintain the communication quality, diversity techniques are adopted. Time diversity can be achieved through a multiple transmission of identical frames in the same middleframe. On the other hand, the frequencies hop frame by frame by varying the offset values of the frequency hopping sequence generator. Though the hopping sequence generator creates a new value by the unit of middleframe, a different offset value is applied to each payload frame in order to make the identical payload frames within the middleframe have different frequencies. In this way, frequency and time diversity are achieved simultaneously.

8.4.4 Orthogonal Frequency Offset

For payload and control frames, their frequencies change according to the hopping sequence determined by the hopping sequence generator. Except for the RCF, control frames avoid collision as only one device is allowed to transmit at a time. However, when a need of multiple simultaneous independent communication channels in a pico-net arises, collision is inevitable unless means to avoid it is not devised. In other words, to allow multiple simultaneous independent communications, means to assign a different frequency to each communication group should be devised. The multiple simultaneous communications are made possible by assigning a different offset value in the hopping sequence generator to each communication group.

8.4.5 Frequency Selection

The master uses sounding techniques to initialise the contents of the frequency hopping table with the best 16 frequencies free of interference from the surroundings. Even in the midst of operation, the master updates the table through passive and static sounding techniques. The renewed frequency table is transmitted regularly to the slaves via beacon frames (BFs) so that the identical frequency tables can be maintained within the same group in the pico-net.

8.4.5.1 Passive sounding

Passive sounding is a technique in which the master scans all through the frequency band and selects the best 16 frequencies. It is done in the initialization process to compose the hopping frequency table. Passive sounding requires a RSSI signal from the RF receiver circuit that indicate the level of each frequency.

The procedure of passive sounding is as follows:

1. RSSI is checked for 80 frequencies.

2. The above process is performed *N* times and the worst value is chosen for each frequency. The RSSI values are sorted in ascending order and the best 16 frequencies are selected.

3. The hopping frequency table is filled out with the selected 16 frequencies.

The time unit for the measurement of the channel is the middleframe. Figure 22 shows the time unit for channel measurement. The structure shown is just to compare with that of the middleframe. The length of each measurement time unit is 640 μsec. 80 sounding units constitute one cycle to measure the RSSI of the 80 frequencies. While passive sounding is being performed, control and payload frames cannot be used.

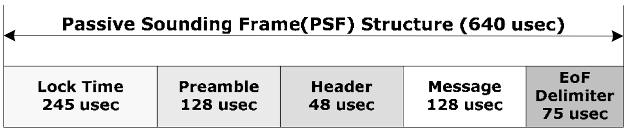

Figure 22 — Middleframe structure of passive sounding

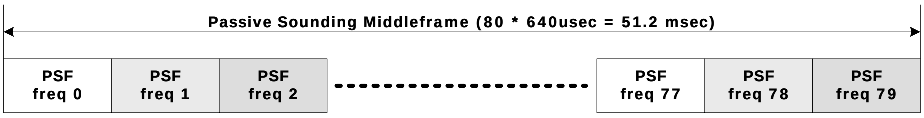

Figure 23 — One cycle of passive sounding frames

8.4.5.2 Static sounding

In static sounding, the master and the slaves cooperate to check the condition of the frequency band and select the 16 best frequencies. Static sounding is used when passive sounding cannot be adopted due to the lack of function in the RF receiver circuit that measures the RSSI. It is also used when a more accurate channel estimation is needed.

Figure 24 illustrates how static sounding is performed. In response to the control signal from the master, the slaves transmit static sounding signals of known bit pattern in the message field. The master estimates the channel by measuring the bit errors of the known bit pattern. The number of bit errors is called the static sounding value (SSV) and used as the measure of channel quality.

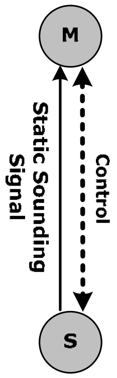

Figure 24 — Illustration of static sounding

The procedure of static sounding is as follows:

1.The master receives the static sounding signals for 80 channel frequencies transmitted by the slaves.

2.The SSV is measured for each of the 80 frequencies.

3.The above process is performed *N* times and the worst value is chosen for each frequency. The values are sorted in ascending order, and the best 16 frequencies are selected.

4.The hopping frequency table is filled out with the selected 16 frequencies.

The structure of the static sounding frame is shown in Figure 25. The structure is similar to that of a normal frame, that is, it consists of lock time, preamble, header, message and EoF. The length of a static sounding middleframe is 945 µsec.

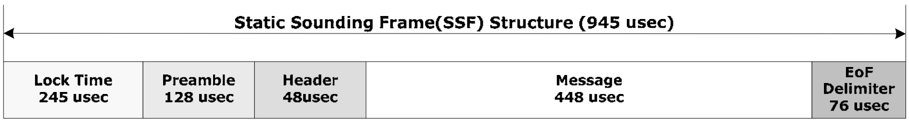

Figure 25 — Middleframe structure of static sounding

Figure 26 shows how the SSVs are measured.

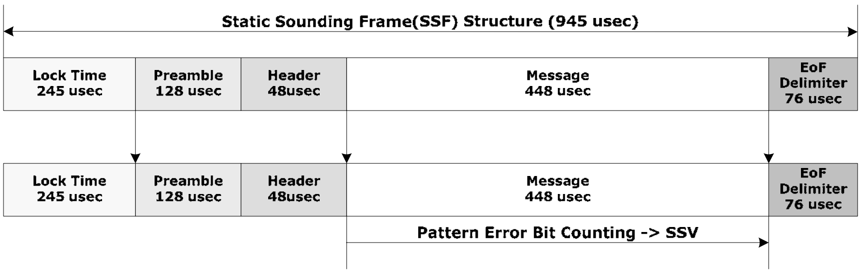

Figure 26 — Static sounding value

As shown in Figure 27, static sounding is performed preserving the superframe-like structure. 16 static sounding frames constitute a static sounding superframe. The control frames may be used as usual but the payload frames are used only for sounding. Therefore, usual communications cannot be practiced during the static sounding period.

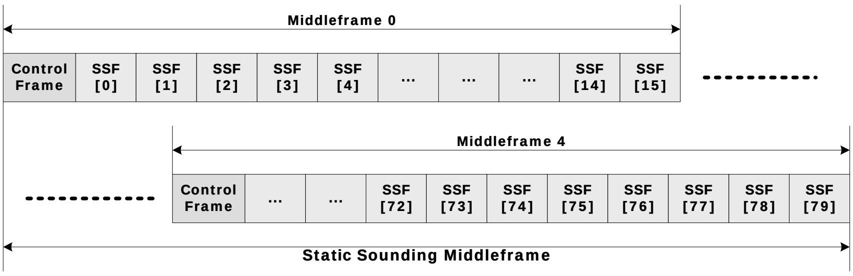

Figure 27 — The structure of the static sounding superframe

9 PHY specification

9.1 General requirements

9.1.1 Operating frequency range

The PHY layer is designed to support the adaptive frequency hopping technology in the 2.4 GHz Industrial Scientific Medical (ISM) band. Using sounding techniques, the best 16 out of all frequencies available are selected to form a frequency table, and the frequency hopping method is used with these frequencies.

The frequency band is between 2,400 MHz and 2,483.5 MHz; a total of 80 frequency channels are available. The channel frequencies are determined as shown below. The RF channel space is 1 MHz, and the number of channel, *k*, is decided in order.

Frequency range	RF channels
2.400-2.4835 GHz	f = 2402 + kMHz, k = 0, …, 79

Two guard bands are placed at the edges of the frequency band as shown below.

Lower guard band	Upper guard band
2MHz	2.5 MHz

9.1.2 Frequency assignment

Frequencies are assigned by the unit of middleframe as described in section 8.4. For diversity's sake, payload frames may be repeated and assigned different frequencies by varying the offset value in the hopping sequence generator.

9.1.3 Frequency synthesizer stabilisation time

The frequency of the signal generated from frequency synthesizer must stabilise within the lock time as defined in section 9.2.1. After the lock time, the transmitter should not have any problems in delivering messages within the frame.

9.1.4 Frequency synthesizer turn off time

The frequency synthesizer must be turned off completely within EOF (end of frame) as defined in verse 8.4.5.

9.2 PHY protocol data unit (PPDU) format

Figure 28 shows the structure of a frame which consists of lock time, preamble, header, message and EoF. The frame starts with lock time, which is necessary for the stabilisation of the frequency synthesiser. The lock time is followed by preamble, which is for synchronization, and then header and message. The header field is used for discrimination of frames and the message field is where data are loaded. At the end of the frame comes the 'end of frame' (EoF) field which indicates the end of the frame and spares time to prepare for next frame. Table 12 summarises the use of each field in the frame. Detailed description is given below.

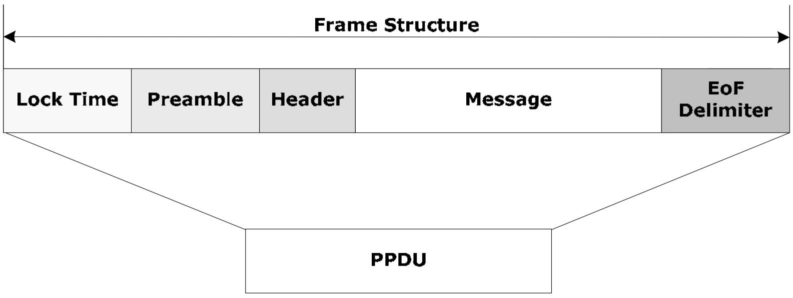

Figure 28 — PHY Protocol Data Unit (PPDU) format

Table 12 — The use of the fields in a frame.

Field	Use
Lock time	Time for stabilisation of RF frequency synthesiser.
Preamble	Coded symbols for synchronization
Header	Designation of frame types (e.g. emergency communications); special control signals
Message	Data
EoF	Indication of the end of a frame; RF circuit stabilisation

9.2.1 Lock time

Since shifting of frequencies and transmission/reception modes are practiced by the unit of frame, ‘lock time’ is required for the RF circuit to stabilise from frame to frame. Data transmission and reception are forbidden during lock time. When in the transmission mode, modem sends the alternating bits of 0 and 1 to the RF circuit during lock time; when in the reception mode, modem ignores the data.

9.2.2 Preamble (128 bits)

Preamble is a field for transmitting symbols for synchronization. The length of the preamble is 128 µsec. The 128-bit preamble is formed by adding "0" to a 127-bit gold code which is generated by a 7-bit scan code. Figure 29 shows one example of a gold-code generator.

9.2.3 Header (48 bits)

Header is a field to indicate the use of the frame. This field clarifies the use of the frame, which cannot be identified only with the preamble. It can also be used for open broadcasting channels or auxiliary signals. The length of a header is fixed to 32 bits; the CRC (cyclic redundancy code) of 16 bits is applied to the header.

메모 **[C. Eun1]:** Detailed description needed.

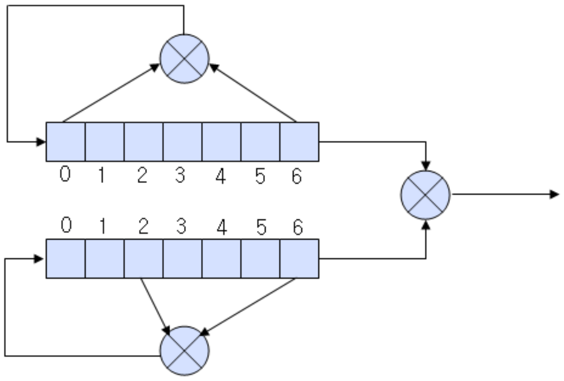

Figure 29 — An example of Gold code generators

9.2.4 Message

Message is a field where user data are loaded. CRC may be applied if needed. The length of the message field is fixed for control frames, but variable for payload frames. For payload frames, the length can be set by the unit of 8 μsec, up to 18 units.

9.2.5 EoF delimiter

EoF is a field to indicate the end of a frame. It is also used for stabilisation of the RF circuit and the modem which alternate transmission and reception modes from frame to frame. The duration of EoF may be set by the unit of 1 μsec.

9.3 Modulation and Codes

9.3.1 Modulation

9.3.1.1 Modulation Scheme

A binary GFSK or FSK is used for modulation. If transmitting antenna of directional gain greater than 0 dBi are used, the applicable paragraphs in EN 300 328, EN 301 489-17and FCC part 15 shall be compensated for.

9.3.1.2 Symbol Rate

Symbol rate is 1Msps.

9.3.2 Codes

9.3.2.1 Scan code

A scan code is 7-bit seed to generate a preamble for synchronisation. The 128-bit gold code (127 gold code with one 0 padded) generated by a scan code used as a preamble of the middleframe. Communications are possible only when the scan codes of the receiver and the transmitter are identical. A scan code has a value between 1 and 127.

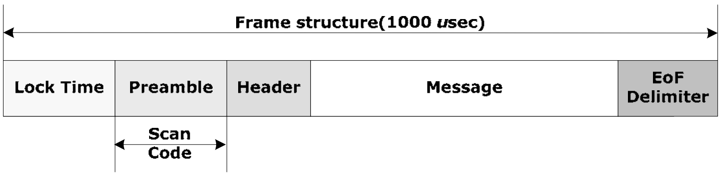

Figure 30 — Scan code

9.3.2.1 Security code

A security code is used for data transmission/reception. The security code is 2^{16} bits long and multiplied to the message field. Communications are possible only when the phases of the security codes of the receiver and the transmitter are identical.

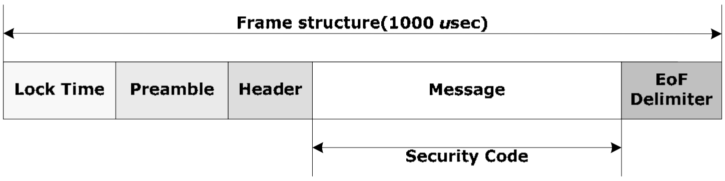

Figure 31 — Security code

9.3.2.1 Group code

A group code is used for data transmission/reception for group communications. It is 2^{64} bits long and multiplied to the message field. Communications are possible only when the group codes of the receivers and the transmitters in a group are identical.

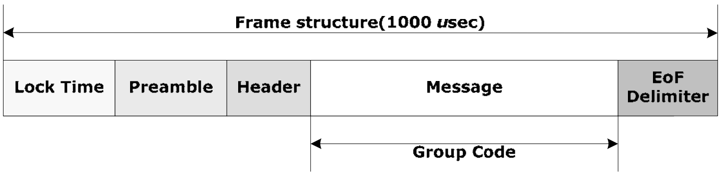

Figure 32 — Group code

9.4 Transmitter specification

The transmitter specification should be satisfied with International regulations and national laws regulate the use of radio receivers and transmitters. SRDs (Short Range Devices) for license free operation are allowed to operate in the 2.45 GHz bands worldwide. The most important regulations are EN 300 440 and EN 300 328 (Europe), FCC CFR47 part 15.247 and 15.249 (USA), and ARIB STD-T66 (Japan).

9.4.1 Pulse shaping filter

The Modulation is GFSK (Gaussian Frequency Shift Keying) with a bandwidth - bit period product BT=0.5. The Modulation index shall be between 0.28 and 0.35. A binary ‘one’ shall be represented by a positive frequency deviation, and a binary ‘zero’ shall be represented by a negative frequency deviation. The symbol timing shall be less than ±20 ppm.

In addition, the minimum frequency deviation shall never be smaller than 115 kHz. The data transmitted has a symbol rate of 1 Ms/s.

The zero crossing error is the time difference between the ideal symbol period and the measured crossing time. This shall be less than ±1/8 of a symbol period.

9.4.2 Transmitter power spectrum mask

This clause is to be determined.