International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.641

(02/2012)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Broadband, triple-play and advanced multimedia services – Ubiquitous sensor network applications and Internet of Things

SNMP-based sensor network management framework

Recommendation ITU-T H.641

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
Ubiquitous sensor network applications and Internet of Things	**H.640–H.649**
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T H.641

SNMP-based sensor network management framework

Summary

Recommendation ITU-T H.641 describes a sensor network management framework intended to provide integrated management functionalities for heterogeneous sensor networks using the simple network management protocol (SNMP).

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T H.641	2012-02-13	16

Keywords

Sensor network management framework, SNMP.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

Ubiquitous sensor network (USN) is a conceptual network built over existing physical networks that makes use of sensed data and provides knowledge services to anyone, anywhere and at any time, and where the information is generated by using context awareness [ITU-T Y.2221]. One of the basic infrastructures of USN is wireless sensor networks that monitor physical or environmental conditions. These sensor networks may use different MAC/PHY protocols and different transport protocols, they may have different sensor node identification schemes and may use different management protocols.

From the viewpoint of a sensor network management protocol, each sensor network may use different sensor network management protocols that are optimized for its MAC/PHY characteristics, transport layer characteristics and for each sensor network management information base (MIB). For example, an IEEE 802.15.4 based sensor network can deliver a 128 bytes frame at one time including 22 bytes of the IEEE 802.15.4 header. It means that a sensor network management protocol for an IEEE 802.15.4-based sensor network should be designed considering this frame size. The ZigBee sensor network based on IEEE 802.15.4 uses its own addressing scheme and defines its own MIB.

Currently, many new sensor networking technologies are under development and it is inevitable that optimized sensor networking technologies for a particular purpose will be deployed. This means that there will be many heterogeneous sensor networks.

From the viewpoint of network management, managing each heterogeneous sensor network with heterogeneous management protocols is impractical and an integrated management protocol for all heterogeneous sensor networks is needed.

The common management information protocol (CMIP) [ITU-T X.711] is widely used in network management systems. However, most TCP/IP devices only support SNMP. SNMP is favoured and strongly supported by vendors, and it has been successfully adapted to manage wired and wireless networks.

Due to the limited computing and communication power of sensor networks, the use of standard SNMP in sensor networks is either impractical or impossible.

Recommendation ITU-T H.641

SNMP-based sensor network management framework

1 Scope

This Recommendation provides an SNMP-based sensor network management framework. The primary purpose of this Recommendation is to describe the framework of integrated sensor network management which can be used to manage heterogeneous sensor networks. The scope of this Recommendation includes:

– overall architecture of framework

– functional entities of framework

– object identifier allocation for MIB

– object identifier translation between SNMP and sensor network management protocol.

2 References

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

[ITU-T Y.2221] Recommendation ITU-T Y.2221 (2010), *Requirements for support of Ubiquitous Sensor Network (USN) applications and services in the NGN environment*.

[ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN*.

[IETF RFC 3411] IETF RFC 3411 (2002), *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 context awareness [ITU-T Y.2201]: Context awareness is a capability to determine or influence a next action in telecommunication or process by referring to the status of relevant entities, which form a coherent environment as a context.

3.1.2 management information base [IETF RFC 3411]: A collection of managed objects, residing in a virtual information store.

3.1.3 sensor [ITU-T Y.2221]: An electronic device that senses a physical condition or chemical compound and delivers an electronic signal proportional to the observed characteristic.

3.1.4 sensor network [ITU-T Y.2221]: A network comprised of interconnected sensor nodes exchanging sensed data by wired or wireless communication.

3.1.5 sensor node [ITU-T Y.2221]: A device consisting of sensor(s) and optional actuator(s) with capabilities of sensed data processing and networking.

3.1.6 SNMP agent [IETF RFC 3411]: An SNMP entity containing one or more command responder and/or notification originator applications (along with their associated SNMP engine).

3.1.7 SNMP manager [IETF RFC 3411]: An SNMP entity containing one or more command generator and/or notification receiver applications (along with their associated SNMP engine).

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 sensor network management protocol agent: A sensor network management protocol entity containing one or more command responder and/or notification originator applications (along with their associated sensor network management protocol engine).

3.2.2 sensor network management protocol manager: A sensor network management protocol entity containing one or more command generator and/or notification receiver applications (along with their associated sensor network management protocol engine).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
AIB	Application support Information Base
ALG	Application Level Gateway
CMIP	Common Management Information Protocol
DST	Destination
ID	Identifier
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
MAC	Media Access Control
MIB	Management Information Base
NIB	Network Information Base
OID	Object Identifier
PAN	Personal Area Network
PDU	Protocol Data Unit
PHY	Physical layer
PIB	PAN Information Base
SDO	Standards Development Organization
SNMP	Simple Network Management Protocol
SRC	Source
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USN	Ubiquitous Sensor Network

5 Conventions

None.

6 Architecture of an SNMP-based sensor network management framework

Figure 1 illustrates the architecture of the SNMP-based sensor network management framework.

The architecture comprises a sensor network manager, sensor network gateway and sensor node. The sensor network manager resides in the TCP/IP network and manages sensor nodes or sensor networks through sensor network gateways.

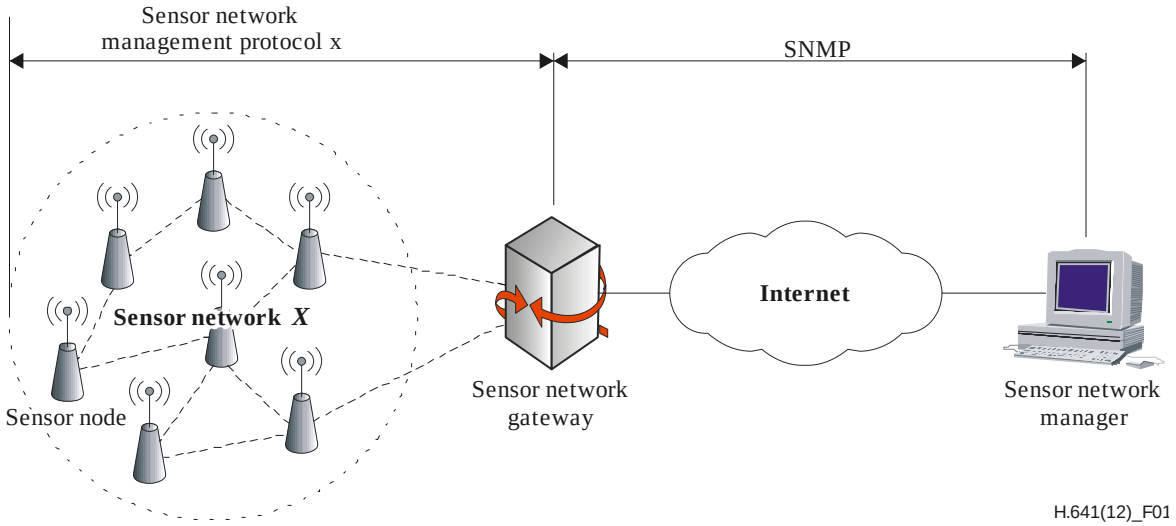

Figure 1 – Architecture of an SNMP-based sensor network management framework

A sensor network manager communicates with the sensor network gateway using standard SNMP over the IPv4 or IPv6.

A sensor network gateway communicates with sensor nodes using a sensor network specific management protocol. Specific sensor network management protocols for specific sensor networks are out of the scope of this Recommendation.

A sensor network gateway has dual network interfaces and performs MAC/PHY protocol translation, transport protocol translation, and management protocol translation between TCP/IP network and specific sensor networks if necessary. The translation of management protocol means translation between SNMP and sensor network specific management protocols. Protocol translations, other than management protocol translation, are out of the scope of this Recommendation.

7 Functional entities of SNMP-based sensor network management framework

Figure 2 illustrates the functional entities of an SNMP-based sensor network management framework.

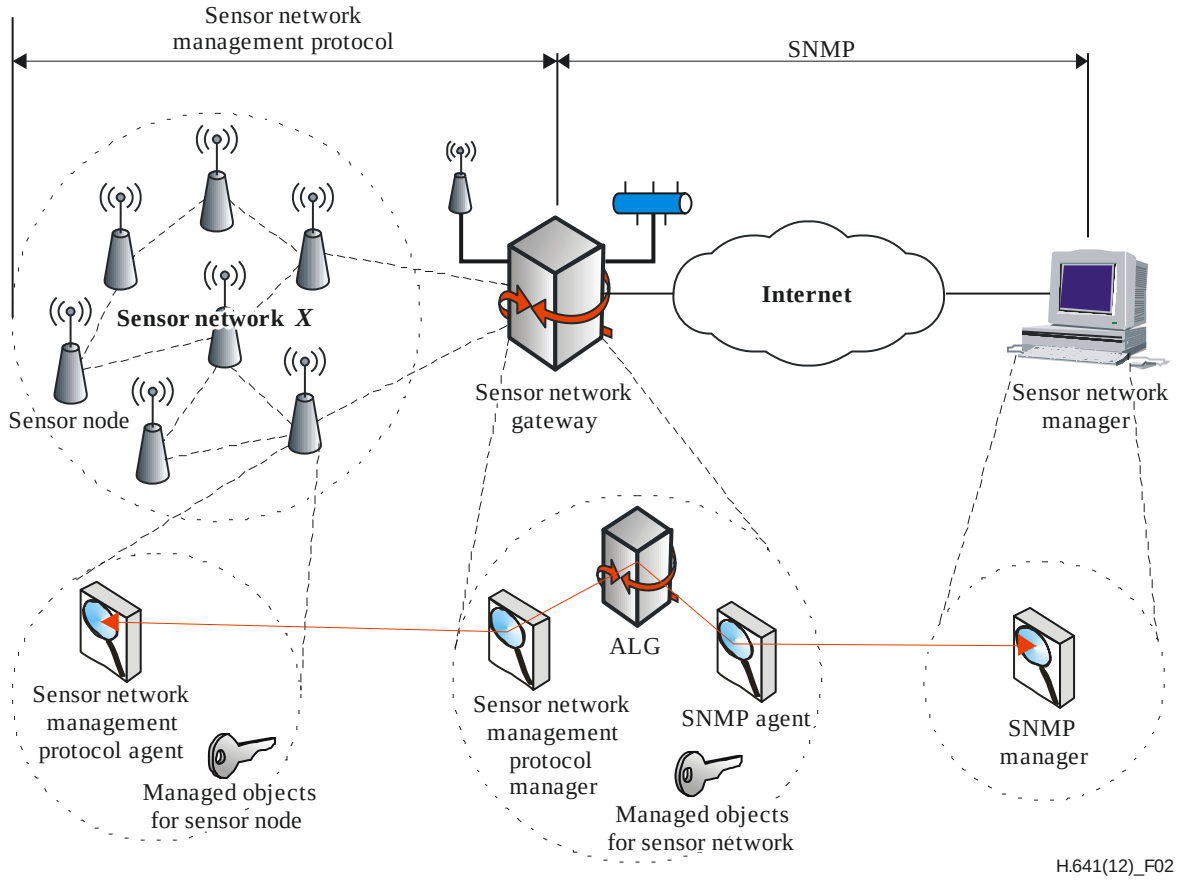

Figure 2 – Functional entities of an SNMP-based sensor network management framework

7.1 SNMP manager

An SNMP manager is a set of management applications that monitor and control network elements such as the sensor network gateway and sensor network elements such as sensor nodes. An SNMP manager uses standard SNMP. Because the sensor network gateway is a normal TCP/IP device, an SNMP manager can manage the sensor network gateway using standard SNMP.

7.2 SNMP agent

An SNMP agent is a set of software modules that reside in network elements. It collects and stores management information such as the number of error packets received by a network element. In this framework, the SNMP agent has two roles, a role as the standard SNMP agent for managing the sensor network gateway and another role of delivering SNMP commands to the application level gateway (ALG) and SNMP responses to the SNMP manager.

7.3 Sensor network management protocol manager

A sensor network management protocol manager is a set of management applications that monitor and control sensor network elements. It receives commands from an ALG and delivers these commands to the sensor network management protocol agent and receives responses from the sensor network management protocol agent and delivers these responses to the ALG.

7.4 Sensor network management protocol agent

A sensor network management protocol agent is a set of software modules that reside in sensor network elements. It collects and stores management information such as the number of error packets received by a sensor network element.

7.5 Application level gateway

An application level gateway is a set of software modules that perform protocol translation between the SNMP and the sensor network management protocol. A sensor network management protocol manager, a sensor network management protocol agent and an ALG may be implemented in one software module, or in separate ones.

7.6 Managed object for sensor network

A managed object for a sensor network is a characteristic of a sensor network that can be managed. The characteristic of a sensor network is mainly related to the whole sensor network (not just for each sensor node) such as the number of sensor nodes in a sensor network. This information is managed by the SNMP agent in a sensor network gateway (see clause 6).

7.7 Managed object for sensor node

A managed object for a sensor node is a characteristic of a sensor node that can be managed. This information is managed by a sensor network management protocol agent in each sensor node. The managed object for a sensor node should be defined by other SDOs developing standards for specific sensor network technology. For example, if the sensor network is a ZigBee sensor network, the managed objects for the sensor nodes could be a ZigBee network information base (NIB) and a ZigBee application support information base (AIB), which are described in [b-ZigBee Specification].

8 Operation of an SNMP-based sensor network management framework

8.1 Overview

Figure 3 illustrates the overall operation flow of an SNMP-based sensor network management framework.

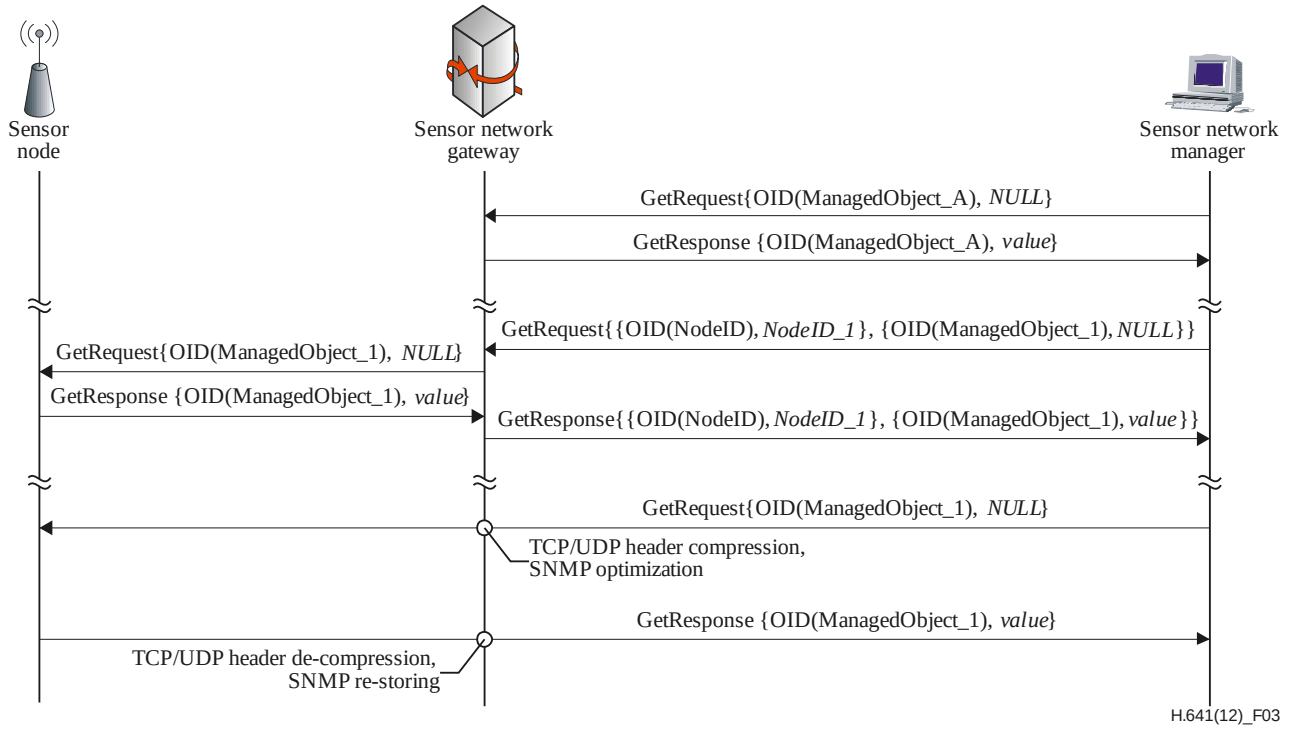

Figure 3 – Operation of an SNMP-based sensor network management framework

To manage a sensor node, a sensor network manager needs to send SNMP requests to a sensor network gateway.

When the SNMP agent receives an SNMP message from the sensor network manager, it should check the OID values in the first *VarBind*. If this OID does not begin with {itu-t(0) recommendation(0) h(8) h641(641)} (see Annex A), then it just performs a normal SNMP agent role as specified in [IETF RFC 3411].

If this OID begins with {itu-t(0) recommendation(0) h(8) h641(641)}, it passes the SNMP message to the ALG. In this message, the sensor node ID should be included as a *VarBind*. The ALG in the sensor network gateway converts this SNMP message to a sensor network management protocol message and sends it to a sensor node which is identified by a sensor node ID in *VarBind*. In this conversion process, the ALG removes the first *VarBind* from the *VarBindList*. The value of the first *VarBind* (sensor node ID) is used for the destination address in the sensor network protocol.

A sensor node management protocol agent replies back to the sensor network gateway using the sensor network management protocol. When the ALG in the sensor network gateway receives this message, the ALG converts this sensor network management protocol message to an SNMP message. In this conversion process, the sensor network gateway adds *VarBind* to the *VarBindList*. The value of this *VarBind* can be acquired from the source address of the received sensor network management protocol message or from a mapping table managed by the ALG in the sensor network gateway.

The ALG in the sensor network gateway also performs object identifiers (OIDs) conversion between the sensor network management protocol messages and SNMP messages (see clause 9 and Appendix I).

8.2 Application level gateway database

The sensor network gateway should maintain an ALG database. It is constructed with the information listed below for every SNMP message from the SNMP manager in order to perform protocol and OID translation between the SNMP and the sensor network management protocol.

– Request ID sequence number (generated by ALG)
– IP header (from SNMP message)
– UDP header (from SNMP message)
– Common SNMP header (from SNMP message)
– Get/set header (from SNMP message)
– Variable binding list (from SNMP message)

The sequence number shall be used as a primary key in this ALG database.

8.3 Translation from an SNMP to a sensor network management protocol message

Figure 4 shows the operational procedure of the sensor network gateway when it receives an SNMP message from an SNMP manager.

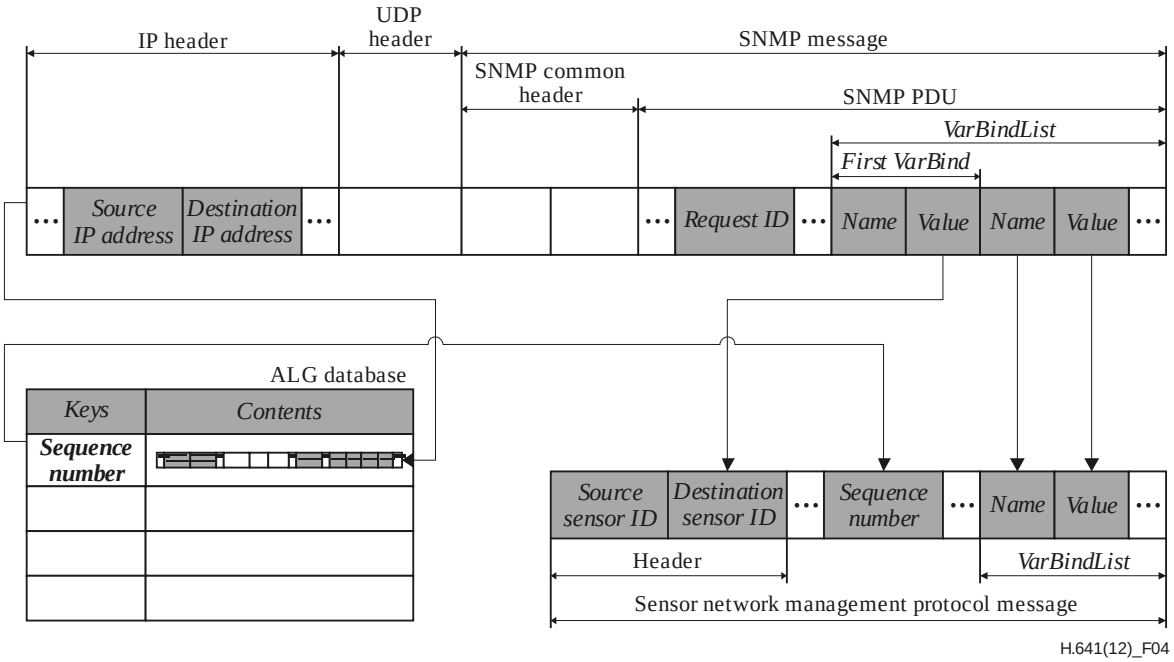

Figure 4 – Translation from an SNMP message to a sensor network management protocol message

When the sensor network gateway receives an SNMP message from an SNMP manager, it generates a sequence number to be used as the request ID in the sensor network management protocol message and records this sequence number and the whole message into an ALG database. Then it creates a sensor network management protocol message. It copies the sequence number in the ALG database into the sequence number field of the sensor network management protocol message. It copies the value of the first *VarBind* into the destination sensor ID field of the sensor network management protocol message. Then it copies the *VarBindList* except for the first one into the sensor network management protocol message. When it copies object identifiers in the *VarBindList*, base OID should be removed (see clause 9 and Appendix I).

The sensor network management protocol message should include a request ID field. If this field does not use the same format with an SNMP message, then the sensor network gateway also maintains mapping information between the request ID from the SNMP message and request ID from the sensor network management protocol message.

8.4 Translation from a sensor network management protocol to an SNMP message

Figure 5 shows the operational procedure of the sensor network gateway when it receives a sensor network management protocol message from a sensor network management protocol agent.

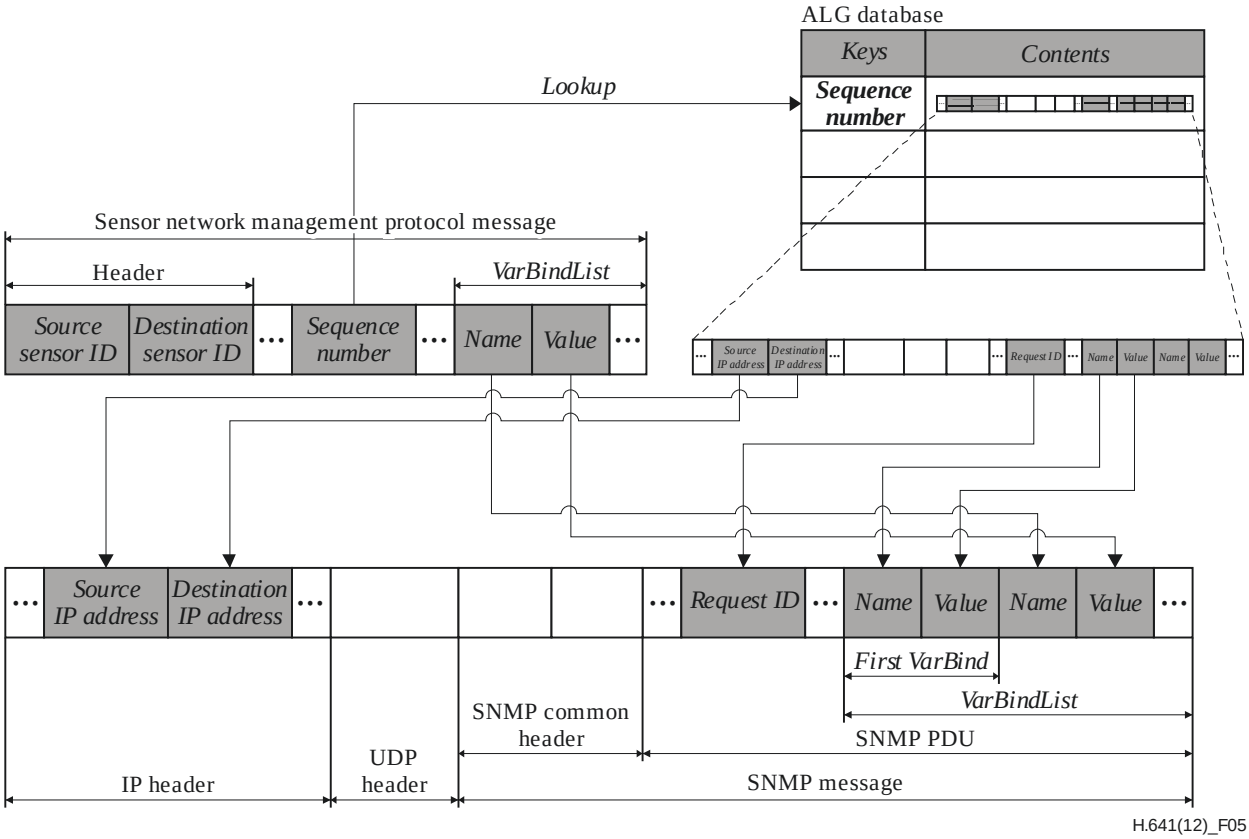

Figure 5 – Translation from a sensor network management protocol message to an SNMP message

When the sensor network gateway receives a sensor network management protocol message from a sensor node, it extracts the sequence number and looks up the original SNMP message from the ALG database. Then it creates a new SNMP message. It copies the destination IP address of the original SNMP message into the source IP address field. It then copies the source IP address of the original SNMP message into the destination IP address field. Then it copies the request ID and the first *VarBind*. It copies the *VarBindList* from the sensor network management protocol message into the *VarBindList* of the new SNMP message. When it copies the OID in the *VarBindList*, base OID should be added (see clause 9 and Appendix I).

8.5 Consideration of the sensor network gateway for supporting IP-based sensor networks

In case an IP-based sensor network is deployed (e.g. 6LoWPAN), the sensor network gateway (6LowPAN gateway) can be expected to inspect the data packets traversing the sensor network gateway. If the destination IP address of an IP header of an SNMP message is the IP address of the sensor node that resides under the sensor network gateway, the conversion of an SNMP message described in clause 8.3 is not needed. However, the sensor network gateway can perform TCP/UDP header compression and SNMP optimizations.

When the sensor network gateway receives an SNMP message that is bound for the sensor network manager, the sensor network gateway may perform TCP/UDP header de-compression and SNMP message re-storing if TCP/UDP header compression and SNMP optimizations are performed on the received SNMP message.

9 Object identifier allocation for MIB and object identifier translation between SNMP and sensor network management protocols

In SNMP, managed objects are identified by OIDs [b-ITU-T X.660] that are relatively long byte strings to be transferred on a sensor network. Considering the low data rate of sensor networks, relative OIDs are used in sensor network management protocols so as to identify managed objects relative to the base OID `{itu-t(0) recommendation(0) h(8) h641(641) sensor-network-mgt(2) n}` (see Annex A).

When a sensor network gateway translates an SNMP message into a sensor network management protocol message, the sensor network gateway can remove the base OID from the OID for MIB in *VarBind*. When a sensor network gateway translates a sensor network management protocol message into an SNMP message, the sensor network gateway inserts the base OID in front of the OID of the MIB in *VarBind* (see Appendix I).

Annex A

Object identifier assignments

(This annex forms an integral part of this Recommendation.)

Table A.1 lists the assignment of OIDs defined for use by this Recommendation.

Table A.1 – Object identifier assignments

Object Identifier Value	Description
{itu-t(0) recommendation(0) h(8) h641(641) sensor-network-mgt(2) ieee-802-15-4(1))}	This OID is used to indicate that the sensor network conforms to [b-IEEE 802.15.4]. Subsequent arcs of this node are identical to the identifiers of PHY and MAC PIB attributes defined in [b-IEEE 802.15.4].
{itu-t(0) recommendation(0) h(8) h641(641) sensor-network-mgt(2) zigbee(2)}	This OID is used to indicate that the sensor network conforms to [b-ZigBee Specification]. Subsequent arcs of this node are identical to the identifiers of the network layer information base, application layer information base and security-related application layer information base attributes defined in [b-ZigBee Specification].

Appendix I

Example of object identifier translation

(This annex forms an integral part of this Recommendation.)

Figure I.1 shows the translation of an OID in a sensor network gateway.

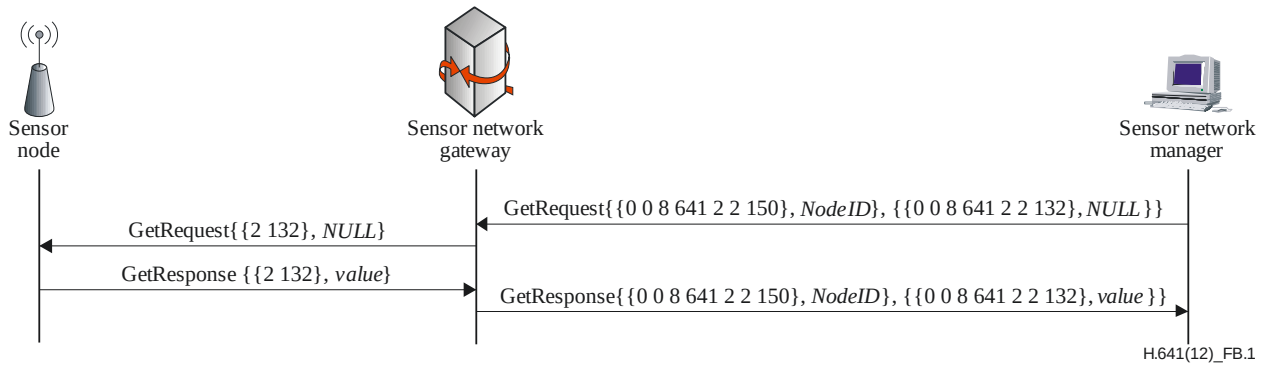

Figure I.1 – Example of object identifier translation

In Figure I.1, the sensor network is a ZigBee sensor network. When the sensor network manager wants to get the `nwkMaxChildren` of a ZigBee node, it sends a *GetRequest* message to the sensor network gateway with OID `{itu-t(0) recommendation(0) h(8) h641(641) sensor-network-mgt(2) zigbee(2) nwkMaxChildren(132)}` in a *VarBind*. When the sensor network gateway receives an SNMP message from the sensor network manager, it removes the base OID so as to create the relative OID `{zigbee(2) nwkMaxChildren(132)}` for the sensor network management protocol message.

NOTE – The OID `{itu-t(0) recommendation(0) h(8) h641(641) sensor-network-mgt(2) zigbee(2) nwkNetworkAddress(150)}` is allocated for nwkNetworkAddress of the ZigBee node and this is a 16-bit address used in a ZigBee network.

When the sensor network gateway receives a sensor network management protocol message from a sensor node, it inserts the base OID in front of the relative OID `{zigbee(2) nwkNetwork Address(150)}` so as to create the full OID `{itu-t(0) recommendation(0) h(8) h641(641) sensor-network-mgt(2) zigbee(2) nwkMaxChildren(132)}` for the sensor network management protocol message.

Bibliography

[b-ITU-T X.660] Recommendation ITU-T X.660 (2011) | ISO/IEC 9834-1:2012, *Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree.*

[b-ITU-T X.711] Recommendation ITU-T X.711 (1997) | ISO/IEC 9596-1:1997, *Information technology – Open Systems Interconnection – Common Management Information Protocol: Specification.*

[b-IEEE 802.15.4] IEEE 802.15.4 (2006), *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs).*

[b-ZigBee Specification] ZigBee Document 053474r17 (2008), *ZigBee Specification.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	**Audiovisual and multimedia systems**
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2012