INTERNATIONAL STANDARD

ISO/IEC 29180

First edition
2012-12-01

Information technology — Telecommunications and information exchange between systems — Security framework for ubiquitous sensor networks

Technologies de l'information — Télécommunications et échange d'informations entre systèmes — Cadre de sécurité pour réseaux de capteurs ubiquitaires

Reference number
ISO/IEC 29180:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

CONTENTS

Page

1 Scope 1

2 Normative references 1

2.1 Identical Recommendations | International Standards 1

2.2 Paired Recommendations | International Standards equivalent in technical content 1

2.3 Additional references 1

3 Definitions 2

3.1 Terms defined elsewhere 2

3.2 Terms defined in this Recommendation | International Standard 2

4 Abbreviations 3

5 Conventions 4

6 Overview 4

7 Threats and security models for ubiquitous sensor networks 7

7.1 Threat models in sensor networks 7

7.2 Threat models in IP networks 10

7.3 Security model for USNs 10

8 General security dimensions for USN 10

9 Security dimensions and threats in ubiquitous sensor networks 11

9.1 Security dimensions and threats for the message exchange in sensor networks 11

9.2 Security dimension and threats for the message exchange in the IP network 14

10 Security techniques for ubiquitous sensor networks 14

10.1 Key management 14

10.2 Authenticated broadcast 15

10.3 Secure data aggregation 16

10.4 Data freshness 17

10.5 Tamper-resistant module 17

10.6 USN middleware security 17

10.7 IP network security 17

10.8 Sensor node authentication 18

10.9 Privacy protection in sensor networks 18

11 Specific security functional requirements for USN 18

11.1 Mandatory functional requirement 18

11.2 Recommended functional specifications 18

11.3 Optional functional specifications 18

Annex A – Key management in sensor networks 20

A.1 Threat time 20

A.2 Key management classes 20

A.3 Key schemes 21

Annex B – Authenticated broadcast in sensor networks: µTPC 23

B.1 Construction of µTPC 23

B.2 Construction of µTPCT 24

B.3 Authenticated broadcast 25

Annex C – Authentication mechanisms in sensor networks 26

C.1 XOR-based mechanism 26

C.2 Hash-based mechanism 27

C.3 Public key-based authentication 29

Annex D – Secure data aggregation in sensor networks 32

D.1 Elect aggregation node and supervisor 32

D.2 Implementation of supervisor functions 33

D.3 Upload supervising message 33

D.4 Determine the trust of aggregation nodes 33

Page
D.5 Send revocation message 33
Bibliography 34

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national 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 and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 29180 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*, in collaboration with ITU-T. The identical text is published as Rec. ITU-T X.1311 (02/2011).

Introduction

This Recommendation | International Standard describes the security threats to and security requirements of the ubiquitous sensor network. In addition, this Recommendation | International Standard categorizes the security technologies according to the security functions that satisfy the said security requirements and where the security technologies are applied in the security model of ubiquitous sensor networks. Finally, the security functional requirements and security technologies for the ubiquitous sensor networks are presented.

INTERNATIONAL STANDARD
RECOMMENDATION ITU-T

Information technology – Security framework for ubiquitous sensor networks

1 Scope

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

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

This Recommendation | International Standard describes the security threats to and security requirements of the ubiquitous sensor network. In addition, this Recommendation | International Standard categorizes the security technologies according to the security functions that satisfy the said security requirements and where the security technologies are applied in the security model of the USN. Finally, the security requirements and security technologies for the USN are presented.

2 Normative references

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

2.1 Identical Recommendations | International Standards

None.

2.2 Paired Recommendations | International Standards equivalent in technical content

- Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

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

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

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

2.3 Additional references

- Recommendation ITU-T H.235.0 (2005), *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems*.
- Recommendation ITU-T X.1111 (2007), *Framework of security technologies for home network*.
- Recommendation ITU-T X.1191 (2009), *Functional requirements and architecture for IPTV security aspects*.

- Recommendation ITU-T Y.2221 (2010), *Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment*.
- Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.
- FIPS PUB 140-2 (2001), *Security Requirements for Cryptographic Modules*.

3 Definitions

3.1 Terms defined elsewhere

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

3.1.1 Terms from FIPS PUB 140-2

a) key transport

b) tamper detection

c) tamper evidence

d) tamper response.

3.1.2 Terms from Rec. ITU-T Y.2221

a) sensor

b) sensor network

c) USN middleware

d) ubiquitous sensor network (USN).

3.1.3 Terms from Rec. ITU-T H.235.0

a) attack.

3.1.4 Terms from Rec. ITU-T X.1191

a) tamper-resistant.

3.1.5 Terms from Rec. ITU-T X.800 | ISO/IEC 7498-2

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

a) access control

b) authentication

c) authorization

d) confidentiality

e) data origin authentication

f) denial of service

g) digital signature

h) integrity

i) key

j) key management

k) peer-entity authentication

l) privacy

m) repudiation

n) security policy

o) threat.

3.2 Terms defined in this Recommendation | International Standard

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

3.2.1 aggregator node: Sensor node that performs the data aggregation function in a sensor network.

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

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

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

3.2.5 **group-wise key**: Refers to a key that is used to protect multicast communications among a set of sensor nodes over a shared wireless link.

3.2.6 **intrusion detection**: Process of monitoring the events occurring in a computer system or a network and analysing them for intrusions.

3.2.7 **key agreement**: A key establishment procedure (either manual or electronic) where the resultant key is a function of information by two or more participants, so that no party can predetermine the value of the key independently of the other party's contribution.

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

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

3.2.10 **resilience**: Ability to recover from security compromises or attacks.

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

3.2.12 **tamper-resistant module**: A device designed to make it difficult for attackers to gain access to sensitive information contained in the module.

4 Abbreviations

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

BNode	Broadcast Node
BS	Base Station
CDMA	Code Division Multiple Access
DDoS	Distributed Denial of Service
DoS	Denial of Service
ECDH	Elliptic Curve Diffie-Hellman
FP	Feature Parameters
GSM	Global System for Mobile Communications
HSDPA	High Speed Downlink Packet Access
ID	Identity
MAC	Medium Access Control; Message Authentication Code
NGN	Next-Generation Network
PHY	physical layer
RFID	Radio-Frequency IDentification
SN	Sensor Network
TPM	Trusted Platform Module
USN	Ubiquitous Sensor Network
WCDMA	Wideband CDMA
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WSN	Wireless Sensor Network

5 Conventions

In this Recommendation | International Standard:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation | International Standard 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 Recommendation | International Standard 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 this Recommendation | International Standard.

6 Overview

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

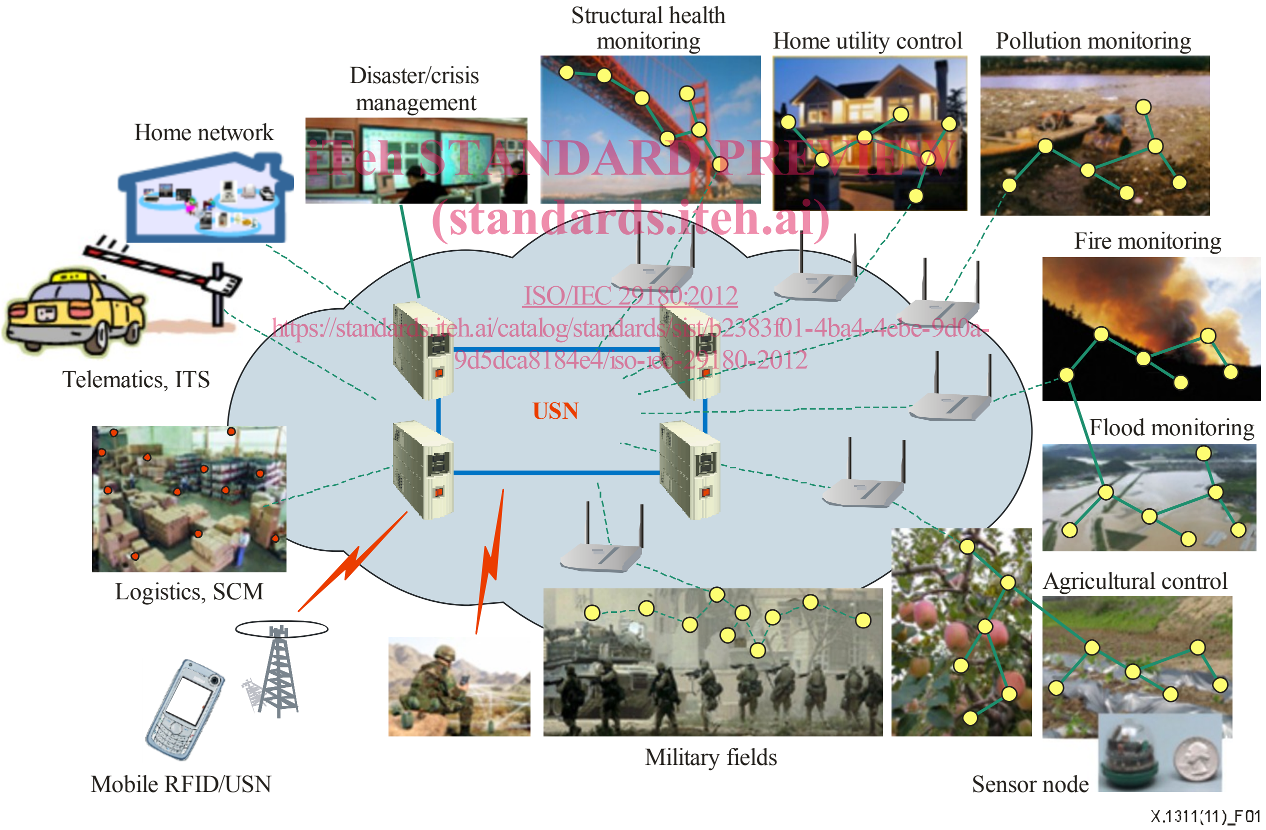

Figure 1 – Application areas for USN

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

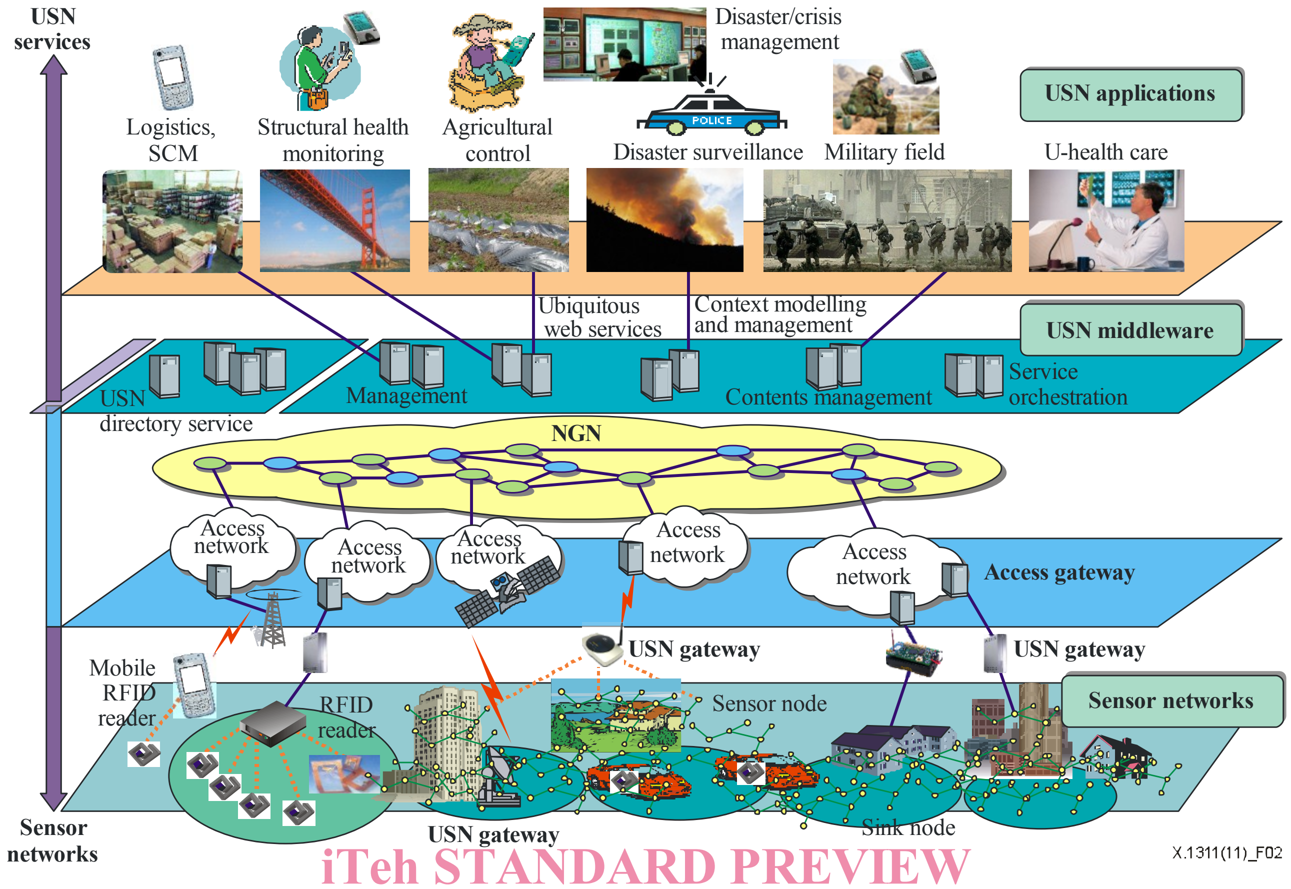

Figure 2 – Overall structure of USN

The sensor networking domain of USN usually corresponds to the sensor node (SN) but includes wire-line sensor networks as well. Thus, many kinds of wired and wireless networking technologies may be used according to the service characteristics and requirements. That is, sensor nodes use different PHY/MAC (e.g., IEEE 802.15.4) layers or operate differently in IP-based or non-IP based networks.

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

The security model for USN can be divided into 2 parts: one for the IP network and the other for the wireless sensor network. This Recommendation | International Standard seeks to develop the security model for the SN as well as the IP network.

The communication patterns within our SN fall into five categories:

- Node-to-base station communication, e.g., sensor readings or special alerts.
- Base station-to-node communication, e.g., specific requests.
- Communication between a base station to all sensor nodes, e.g., routing beacons, queries, or reprogramming of the entire sensor network.
- Node-to-node communications including communications among a defined cluster of sensor nodes, e.g., communications between a sensor node and all its neighbours.
- Communications between a base station and a group of nodes wherein the group is defined by nodes sharing a common property (e.g., location, software version, etc.).

The following assumptions can be made:

- 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, a gateway which interconnects sensor networks with other networks, may be part of a trusted computing environment.
- Communication is from base station to sensor, from sensor to base station, from sensor to its neighbours, and from node to node.

Therefore, how security technologies are integrated should be taken into account.

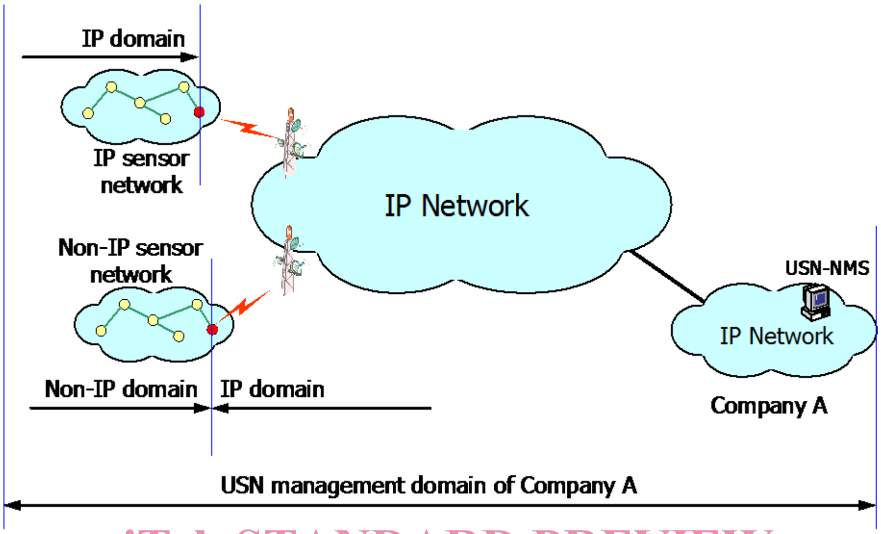

Figure 3 – USN network configuration

The following are the characteristics of the sensor network:

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

There are three components in the SN: the application server communicating with the sink node; the sink node called the base station, which interfaces the sensor network and the application server, and the collection of sensor nodes using wireless communication to communicate with each other. The sink may communicate with the application server via the Internet or a satellite. Security architecture in the IP-based network is very similar to that in Rec. ITU-T X.805 | ISO/IEC 18028-2. Therefore, this Recommendation | International Standard focuses on the security of the wireless sensor network (SN) consisting of a set of sensor nodes using wireless transmission.

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

- **Difficulty of using public key cryptosystems**: The limited computational power, memory size, and power supply make it very difficult to use a public key cryptosystem – such as Diffie-Hellman key agreement or RSA encryption and signature. Even though a specific sensor node may have enough resources to perform the very complex operations required for a public key cryptosystem, it may become vulnerable to a denial of service attack as described in clause 7.1.1.
- **Vulnerability of sensor nodes**: Since sensor nodes may be deployed in hostile locations, their security may be compromised. After obtaining physical access to the sensor node, the attacker is able to access sensitive information such as key information or sensed information. This attack can be prevented by using a tamper-resistant sensor node, which entails a high cost. Moreover, a large number of sensor nodes render the employment of the tamper-resistant sensor node very difficult since it may result in a

high-cost network. For some applications (e.g., military, safety-critical applications, etc.), however, the higher costs incurred in employing tamper-resistant sensor nodes may be acceptable.

- **Difficulty in obtaining post-deployment knowledge**: In most cases, the sensor nodes will be deployed in a randomly scattered manner; hence, the difficulty for the security protocol to know the location of neighbouring nodes.
- **Limited memory size, transmission power, and transmission bandwidth**: Since the memory in sensor nodes is limited, storing the unique keys used with other sensor nodes in the network is very difficult. Moreover, a typical sensor node has low capability in terms of transmission bandwidth and power to communicate with neighbour nodes.
- **Single point of failure of a base station**: In sensor networks, a base station is a gateway to communicate the sensed information to an application server through the IP-based core network. The security of the sensor network relies on that of the base station. Therefore, base stations could become an appealing target for various types of attack.

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

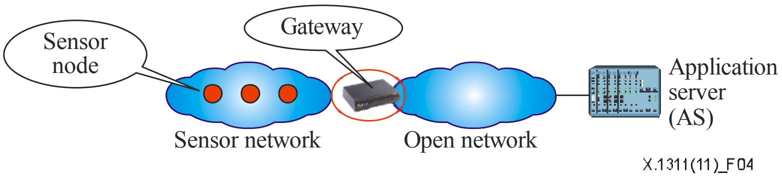

Figure 4 – General model of an end-to-end communication between a sensor node in the SN and an AS

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

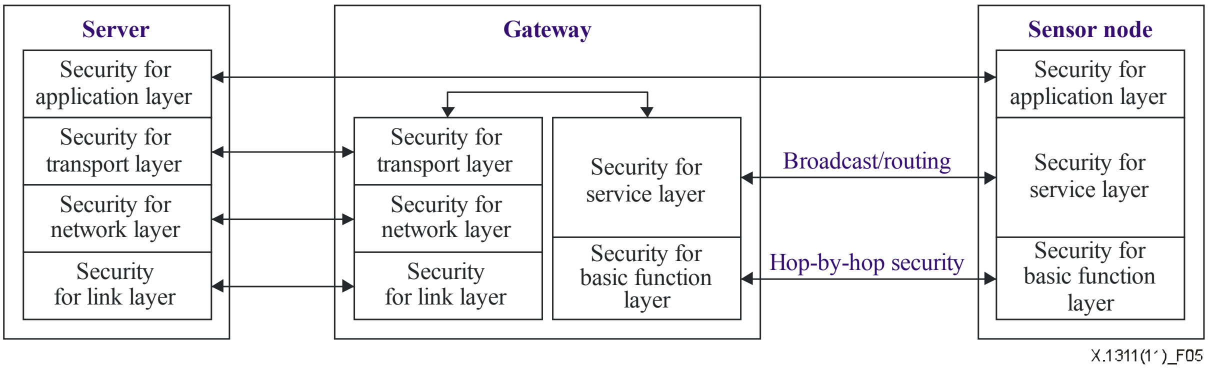
Server
Security for application layer
Security for transport layer
Security for network layer
Security for link layer
Gateway
Security for transport layer
Security for network layer
Security for link layer
Security for service layer
Security for basic function layer
Broadcast/routing
Hop-by-hop security
Sensor node
Security for application layer
Security for service layer
Security for basic function layer
X.1311(11)_F05

Figure 5 – Layers implementing security functions for USN

7 Threats and security models for ubiquitous sensor networks

The threats to USNs can be classified into threats to the IP network and threats to the SN.

7.1 Threat models in sensor networks

There are two types of attackers in the SN: a mote-type attacker and a laptop-type attacker. In the former, the attacker has a capability similar to the sensor node; it can have access to a few sensor nodes. An attacker with a mote-type device may be able to jam the radio link in its vicinity. In the latter, an attacker may have access to more powerful devices such as a laptop computer. An attacker with a laptop-type device may eavesdrop on the communication in the