

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1313

(10/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services – Ubiquitous sensor
network security

Security requirements for wireless sensor network routing

Recommendation ITU-T X.1313

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

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

Recommendation ITU-T X.1313

Security requirements for wireless sensor network routing

Summary

Recommendation ITU-T X.1313 provides the security requirements for wireless sensor network routing. It explains the general network topologies and routing protocols in ubiquitous sensor networks. In addition, this Recommendation analyses the security threats facing wireless sensor networks.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1313	2012-10-14	17

Keywords

Routing, security, USN, WSN.

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 not 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/>.

© ITU 2013

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	Characteristics of general network topologies and routing protocols on security considerations for wireless sensor networks (WSN).....	4
	6.1 General features of routing in the configuration of network topology.....	4
	6.2 General network topologies in the WSN.....	4
	6.3 Characteristics of routing protocols in WSN.....	5
7	Requirements for secure routing.....	7
	7.1 Requirements for sensor and base station	7
	7.2 Security requirements for the neighbour discovery procedure.....	7
	7.3 Security requirements for routing set-up and packet delivery.....	8
	7.4 Security dimensions and requirements for secure routing	8
	Appendix I – Overview of wireless sensor routing protocols.....	11
	I.1 Examples of existing routing protocols.....	11
	Bibliography.....	16

Recommendation ITU-T X.1313

Security requirements for wireless sensor network routing

1 Scope

Recommendation ITU-T X.1313 describes the security requirements for wireless sensor network routing and also covers the following:

- general network topologies and routing protocols for wireless sensor networks (WSN)
- security threats faced by WSN routing
- security requirements for WSN routing.

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 X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- [ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.
- [ITU-T X.1311] Recommendation ITU-T X.1311| ISO/IEC 29180:2011, *Information Technology — Security framework for ubiquitous sensor networks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [ITU-T X.800]: See data origin authentication and peer-entity authentication in [ITU-T X.800].

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

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

3.1.4 key [ITU-T X.800]: A sequence of symbols that controls the operation of encipherment and decipherment.

3.1.5 sensor [b-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.

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

3.1.7 threat [ITU-T X.800]: A potential violation of security.

3.1.8 ubiquitous sensor network (USN) [b-ITU-T Y.2221]: A conceptual network built over existing physical networks which makes use of sensed data and provides knowledge services to anyone, anywhere and at any time, and where information is generated by using context awareness.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 actuator: A receiving and transmitting for sensed data.

3.2.2 ad hoc on-demand distance vector (AODV): An on-demand routing protocol that discovers routes on an "as-needed" basis for wireless ad hoc networks and wireless sensor networks. AODV builds routes using a route request (RREQ) and a route reply (RREP) query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backward pointers to the source node in the route tables.

3.2.3 node integrity: The property wherein the node has not been altered or destroyed in an unauthorized manner.

3.2.4 routing: The process for establishing a communication association between the sensor nodes. Routing involves determining the path, and transporting information through the network.

3.2.5 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.

3.2.6 topology: The physical and logical arrangement of the elements of a sensor network. In a WSN, it is represented as a collection of sensor nodes and gateways, some of which are connected by wireless links.

3.2.7 wireless sensor network (WSN): A network that consists of a base station and a large number of sensor nodes with wireless transmission capability in the sensor networking domain of the USN.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

ACQUIRE	Active query forwarding In sensor networks
AES	Advanced Encryption Standard
AODV	Ad hoc On-demand Distance Vector
APTEEN	Adaptive Periodic Threshold-sensitive Energy-Efficient sensor Network protocol
BS	Base Station
CADR	Constrained Anisotropic Diffusion Routing
CDMA	Code Division Multiple Access
CH	Cluster Head
DAG	Directed Acyclic Graph
DAM	Distributed Aggregate Management
DC	Data-Centric
DODAG	Destination Oriented DAG
DoS	Denial of Service