INTERNATIONAL STANDARD

ISO/IEC 15149-4

First edition
2016-01-15

Information technology — Telecommunications and information exchange between systems — Magnetic field area network (MFAN) —

Part 4: Security Protocol for Authentication

Technologies de l'information — Téléinformatique — Réseau de zone de champ magnétique (MFAN)

Reference number
ISO/IEC 15149-4:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

This first edition of ISO/IEC 15149-4, together with ISO/IEC 15149-1, ISO/IEC 15149-2, and ISO/IEC 15149-3, cancels and replaces ISO/IEC 15149:2011, which has been technically revised.

ISO/IEC 15149 consists of the following parts, under the general title *Information technology — Telecommunications and information exchange between systems*:

— *Part 1: Air Interface*

— *Part 2: In-Band Control Protocol for Wireless Power Transfer*

— *Part 3: Relay Protocol for Extended Range*

— *Part 4: Security Protocol for Authentication*

Introduction

This part of ISO/IEC 15149 provides protocols for magnetic field area networks (MFAN). MFAN can support the service based on wireless communication and wireless power transfer in harsh environments. MFAN is composed of four protocols; air interface, in-band control protocol, relay protocol and security protocol for authentication.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning MFSec technology given in this part of ISO/IEC 15149.

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured the ISO and IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC.

Information on the declared patents may be obtained from:

Patent Holder: China IWNCOMM Co., Ltd.

Address: A201, QinFengGe, Xi'an Software Park, No. 68, Keji 2nd Road, Xi'an Hi-Tech Industrial Development Zone, Xi'an Shaanxi, P. R. China 710075

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

ISO (www.iso.org/patents) and IEC (http://patents.iec.ch) maintain on-line databases of patents relevant to their standards. Users are encouraged to consult the databases for the most up to date information concerning patents.

Information technology — Telecommunications and information exchange between systems — Magnetic field area network (MFAN) —

Part 4:
Security Protocol for Authentication

1 Scope

This part of ISO/IEC 15149 specifies security protocol for authentication in magnetic field networks.

2 Normative references

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

ISO/IEC 15149-1:2014, *Information technology — Telecommunications and information exchange between systems — Magnetic field area network (MFAN) — Part 1: Air Interface*

ISO/IEC 15149-3:2016, *Information technology — Telecommunications and information exchange between systems — Magnetic field area network (MFAN) — Part 3: Relay Protocol for Extended Range*

3 Terms and definitions

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

3.1
Magnetic Field Area Network
MFAN
wireless network that provides reliable communication in harsh environments using magnetic field

3.2
Magnetic Field Area Network – Coordinator
MFAN-C
device that manages the connection and release of nodes within the communication area and the sending and receiving time of data in an MFAN

3.3
Magnetic Field Area Network – Node
MFAN-N
A device except the coordinator that forms a network in an MFAN

4 Symbols and abbreviated terms

4.1 Symbols

$\oplus$ exclusive or

|| concatenation

O_n fixed value

+ binary addition

4.2 Abbreviated terms

AuRc Authentication Response Confirmation

AuRq Authentication Request

AuRs Authentication Reponse

MFSec MFAN Security

PSK Pre-Shared Key

RN Random Number

RNc Random Number generated by Coordinator

RNn Random Number generated by Node

SORNc Secret Output with Random Number computed by Coordinator

SORNn Secret Output with Random Number computed by Node

SRNc Secret Random Number generated by Coordinator

SRNn Secret Random Number generated by Node

SS Shared Secret

UID Unique Identifier

UID^C Unique Identifier of Coordinator

UID^N Unique Identifier of Node

5 Overview

MFAN, like some other networks, e.g. Wireless Sensor Networks, suffered from many specific network security threats. To countermeasure those threats, some security procedures should be deployed in such networks.

The security threats of networks, which are specified in the ITU-T X.800 and ITU-T X.805, are applicable to MFAN, as follows:

— Destruction of information and/or other resources

— Corruption or modification of information

— Disclosure of information

In addition, the specific threats to nodes such as sensor mode compromise, eavesdropping, privacy of sensed data, denial of service attack, and malicious use of commodity network are also applicable to MFAN.

The following security requirements specified in ITU-T X.805 could be applicable to MFAN:

— Data Confidentiality

— Data Authentication/identification

— Data Integrity

This part of ISO/IEC 15149 specifies an MFAN security (MFSec) protocol that uses the exclusive or operation for mutual authentication between MFAN-C and MFAN-N. See Annex A for security considerations of MFSec.

NOTE The exclusive or is extremely common as a component in complex ciphers. By itself, using a constant repeating key, a simple exclusive or crypto can trivially be broken using frequency analysis. If the content of any message can be guessed or otherwise known then the key can be revealed (the exclusive or crypto is vulnerable to a known-plaintext attack, since plaintext⊕ciphertext=key). Its primary advantage is that it is simple to implement, and that the exclusive or operation is computationally inexpensive. A simple repeating exclusive or crypto is therefore sometimes used for hiding information in cases where either no particular or light security is required.

6 Network elements

6.1 General

The security network elements of MFAN consist of time and physical elements.

6.2 Time element

Specified in ISO/IEC 15149-3:2016, 6.2.

6.3 Physical element

Specified in ISO/IEC 15149-3:2016, 6.3.

6.4 Address element

Specified in ISO/IEC 15149-3:2016, 6.4.

7 Network functions

7.1 General

The superframe of MFSec protocol consists of request, response and confirmation period. The authentication protocol requires that MFAN-C and MFAN-N shall have a PSK with 8-octet before they start the authentication procedure. How to generate and set a high quality PSK is out of the scope of this standard. The key update function is not supported in this international standard. Figure 1 shows the MFSec protocol message exchange.

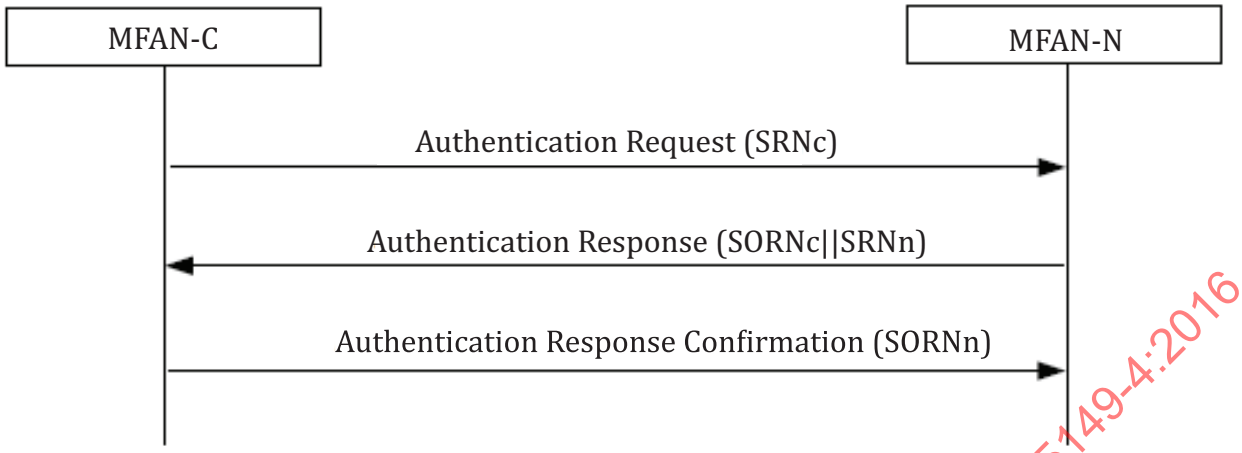

Figure 1 — MFSec protocol

7.2 Request period

During the request period, MFAN-C shall generate an 8-octet random number RNc, and compute SRNc = (RNc + UID^C + O_n) ⊕ PSK, where O_n is defined by a manufacturer. MFAN-C then sends AuRq packet to MFAN-Ns. O_n shall be 8-octet in length.

NOTE The recommendation of the value of O_n is 5555 5555 5555 5555 h.

7.3 Response period

During the response period, MFAN-N shall compute RNc = (SRNc ⊕ PSK) - UID^C - O_n, and SORNc = (PSK' + UID^C + O_n) ⊕ RNc', where, PSK' and RNc' means bit-wise rotate PSK and RNc left for n bits, respectively (n is the number of binary value 1 of RNc). Then MFAN-N shall generate an 8-octet random number RNn and compute SRNn = (RNn + UID^N + O_n) ⊕ PSK. MFAN-N sends AuRs packet to the MFAN-C.

When the MFAN-C receives AuRs packet from the MFAN-N, it shall compute the value of (SORNc ⊕ RNc') and (PSK' + UID^C + O_n), then compare the value of (PSK' + UID^C + O_n) with (SORNc ⊕ RNc'). If these two values are equivalent, then the authentication is successful, otherwise the authentication is failed.

7.4 Confirmation period

When the authentication procedure of MFAN-C is successful, MFAN-C shall compute RNn = (SRNn ⊕ PSK) - UID^N - O_n, and SORNn = (PSK' + UID^N + O_n) ⊕ RNn', where, RNn' means bit-wise rotate RNn left for n bits (n is the number of binary value 1 of RNn). MFAN-C sends AuRc packet to MFAN-N.

Finally, when MFAN-N receives AuRc packet from the MFAN-C, it shall compute the value of (SORNn ⊕ RNn') and (PSK' + UID^N + O_n), then compare the value of (PSK' + UID^N + O_n) with (SORNn ⊕ RNn'). If these two values are equivalent, then the authentication is successful, otherwise the authentication is failed.

7.5 Key generation

For the MFAN-N and MFAN-C that support secure communication or high layer secure application, a shared secret (SS) may be used and shall be established between the two nodes after the successful authentication procedure: SS= (UID^N + UID^C)⊕RNc⊕RNn⊕PSK. SS service is optional.

SS is used to derive additional keys used by MFAN and possibly other applications. The lifetime of SS should be expired after disconnection. A new SS should be established or updated by a new MFSec authentication procedure. The key derivation function is out of the scope of this standard.

8 Network status

8.1 General

In a security network of MFAN, MFAN-N may enter the active state of network authentication.

8.2 Network authentication

When MFAN-C sends the AuRq packet in the request period, MFAN-N probes the received packet and then if it is the AuRq packet for the desired MFAN, MFAN-N sends the AuRs packet to the MFAN-C in the response period. MFAN-C, having received the AuRs packet, transmits the AuRc packet to MFAN-N. The network authentication of MFAN-N is completed upon receiving the valid AuRc packet from MFAN-C.

9 MAC layer frame format

9.1 General

The MAC frame of MFAN consists of the frame header and the frame body. The frame header has information for data and the frame body has the data for transmissions between MFAN devices. See ISO/IEC 15149-1:2014, Clause 8.

9.2 Frame format

Specified in ISO/IEC 15149-1:2014, 8.2.

9.3 Frame type

Specified in ISO/IEC 15149-1:2014, 8.3.

9.4 Payload format

9.4.1 Request frame

9.4.1.1 Request code

Table 1 shows the values for request code for MFAN.

Table 1 — Request code

Category	Request code	Content	Remarks
Network	0x01	Association request	Request for association response to unjoined nodes
	0x02	Disassociation request	Request for disassociation response to joined nodes
	0x03	Association status request	Request for association status response to joined nodes
	0x04	Authentication request	Request for authentication to joined nodes
	0x05 – 0x0F	Reserved	-
Data	0x11	Data request	Request for data transmission to joined nodes
	0x12 – 0x1F	Reserved	-

Table 1 *(continued)*

Category	Request code	Content	Remarks
Configuration	0x21	Group ID set-up request	Request for group ID change to joined nodes
	0x22	Repeater set-up request	Request for repeater allocation among nodes
	0x23 – 0x2F	Reserved	-
Wireless Power Transfer	0x31	Power transfer request	Request for power transfer response to joined nodes
	0x32	Power transfer beacon request	Request for power transfer beacon to joined nodes
	0x33 – 0x3F	Reserved	-
Reserved	0x40 – 0xFF	Reserved	-

9.4.1.2 Request block

The request block of Authentication Request (AuRq) is illustrated in Figure 2. The first 8 octets are the UID of MFAN-C, the next 1 octet is the slot number, and the last 8 octets are SRNc.

Unit: Octet

8	1	8
UID_C	Slot number	SRNc

Figure 2 — Block format of authentication request

9.4.2 Response frame

9.4.2.1 Response code

Table 2 shows the values for response code for MFAN.

Table 2 — Response code

Category	Response code	Content	Remarks
Network	0x01	Association response	Transmission of node UID
	0x02	Disassociation response	Transmission of node UID
	0x03	Association status response	Transmission of node UID
	0x04	Authentication response	Transmission of node UID and security parameters
	0x05 – 0x0F	Reserved	-
Data	0x11	Data response	Transmission of requested data
	0x12 – 0x1F	Reserved	-

Table 2 *(continued)*

Category	Response code	Content	Remarks
Set-up	0x21	Group ID set-up response	Transmission of UID and group ID after changes in group ID
	0x22	Repeater set-up response	Transmission of UID and repeater number
	0x23 – 0x2F	Reserved	-
Wireless Power Transfer	0x31	Power transfer response	Transmission of requested data to receive wireless power transfer
	0X32 – 0x3F	Reserved	-
Reserved	0x40 – 0xFF	Reserved	-

9.4.2.2 Response block

The response block of Authentication Response (AuRs) is illustrated in Figure 3. The first 8 octets are the UID of MFAN-N, the next 1 octet is the slot number, the next 8 octets is SORNc, and the last 8 octets are SRNn.

Unit: Octet

8	1	8	8
UID^N	Slot number	SORNc	SRNn

Figure 3 — Block format of authentication response

9.4.3 Response confirmation frame

9.4.3.1 Response confirmation code

Table 3 shows the values for response confirmation code for MFAN.

Table 3 — Response confirmation code

Category	Reception confirmation code	Content	Remarks
Network	0x01	Association response confirmation	UID and assigned UID transmission of nodes
	0x02	Disassociation response confirmation	UID and UID transmission of nodes
	0x03	Association status response confirmation	UID transmission of nodes
	0x04	Authentication response confirmation	UID and security parameters transmission of nodes
	0x05 – 0x0F	Reserved	-
Data	0x11	Data response confirmation	Confirmation of data transmission to a joined node
	0x12 – 0x1F	Reserved	-
Set-up	0x21	Group ID set-up response confirmation	UID and group ID transmission after group ID changes
	0x22	Repeater set-up response confirmation	UID and repeater number transmission after repeater set-up
	0x23 – 0x2F	Reserved	-
Wireless Power Transfer	0x31	Power transfer response confirmation	Confirmation of power transfer response
	0x32	Power transfer execution command confirmation	Confirmation of power transfer execution command
	0x33	Power level request command confirmation	Confirmation of power transfer request command
	0x34 – 0x3F	Reserved	-
Reserved	0x41 – 0xFF	Reserved	-

9.4.3.2 Response confirmation block

The response confirmation block of Authentication Response Confirmation (AuRc) is illustrated in Figure 4. The first 8 octets are the UID of MFAN-C, the next 1 octet is the slot number, and the last 8 octets are SORNn.