ENHANCED COMMUNICATION PROTOCOL FOR ISO/IEEE 11073-20601

Alexandru EGNER[1], Florica MOLDOVEANU[2], Nicolae GOGA[3], Alin MOLDOVEANU[4], Victor ASAVEI[5], Anca MORAR[6]

ISO/IEEE 11073 (X73) has raised great interest from the research community since its announcement. X73 has several vulnerabilities that have to be addressed before reaching mainstream usage. This paper identifies an important feature the association mechanism lacks: the Manager should have the means of initiating the communication. The paper discusses the importance of this capability, highlighting several scenarios where the bidirectional initiation is required. The paper further presents the proposed solution, which is designed to be optional, in order to maintain backward compatibility. A complete scenario where the Manager initiates the association procedure is presented, with illustration of the exchanged messages. Finally, implementation guidelines are provided.

Keywords: ISO/IEEE 11073, Continua, Body Area Networks

1. Introduction

ISO/IEEE 11073 (X73) is a family of standards designed to facilitate the communication between mobile medical devices belonging to Body Area Networks (BAN). ISO/IEEE 11073-20601 *Application profile – Optimized Exchange Protocol* [1] defines the communication protocol for exchanging medical data.

Continua Health Alliance [7] is an organization that aggregates healthcare and technology companies with the aim of improving the quality of personal healthcare. Continua Health Alliance is one of the most important promoters of

[1] PhD student, Faculty of Automatic Control and Computer Science, University POLITEHNICA of Bucharest, Romania, e-mail: alexandru.egner@cs.pub.ro

[2] Prof., Faculty of Automatic Control and Computer Science, University POLITEHNICA of Bucharest, Romania, e-mail: florica moldoveanu@cs.pub.ro

[3] PhD student, University of Groningen, Netherlands / University POLITEHNICA of Bucharest, e-mail: n.goga@rug.nl

[4] Reader, Faculty of Automatic Control and Computer Science, University POLITEHNICA of Bucharest, Romania

[5] Lecturer, Faculty of Automatic Control and Computer Science, University POLITEHNICA of Bucharest, Romania

[6] Assistant, Faculty of Automatic Control and Computer Science, University POLITEHNICA of Bucharest, Romania

X73. Continua awards certifications to attest that the software or hardware meets the requirements of the Continua Design Guidelines and its underlying standards.

Even though X73 has been recently announced, it raised great attention from the research community. The research is mainly guided to a) the analysis of the plug-and-play interoperability between Body Area Network (BAN) entities [9], [10], [13], b) advantages and disadvantages of various communication channels used in OEP [12], [14], or c) assuring data security and privacy [5] [11], [13]. This paper focuses on a different aspect, namely on the association between the devices.

In the current version of the ISO/IEEE 11073-20601 protocol, the Agent is the only entity that is able to initiate the association procedure. A bidirectional association initiation refers to the fact that both the Agent and the Manager are able to initiate the *Association* procedure, an important feature that the communication protocol lacks. This represents an important limitation to the communication capabilities and affects the process of exchanging medical data and the way medical devices are configured and managed.

For instance, if the Agent is configured as a dialysis device, the correct configuration of this device is vital, and it should be done whenever the care personnel, represented by the Manager, needs to. The Manager should be enabled to change the Agent's configuration parameters, without having to wait for an association request from it.

The bidirectional association initiation is also required when the Manager needs to reestablish the association. This may happen in several situations: a) when the Manager recovers from a crash and needs to re-associate to the Agents, b) if the authentication procedure is changed and the Agents have to re-authenticate using another protocol, or c) if configurations such as the session length are changed.

This paper presents an enhancement to the ISO/IEEE 11073-20601 protocol, which enables the Manager to instantiate the *Association* procedure. The solution is proposed as an extension of the standard, in order to support interoperability between the mobile medical devices. The solution is designed to be optional. This way, backward compatibility with devices that use the current version of the standard is ensured.

The paper discusses the current state of communication between the medical devices and the enhancement proposal. Two different *Association* scenarios are identified and a solution is proposed for each of one. The paper also presents the standard-level enhancements, i.e. new terms defined in the ISO/IEEE 11073-10101 – Nomenclature [2], changes in the communication model, etc. and guidelines for implementing the enhancements.

In order to validate the solution, an extension for the OpenHealth Project from LibreSoft [8] was implemented. OpenHealth is an open source implementation of the ISO/IEEE 11073-20601 protocol, developed in Java following the Continua Design Guidelines.

2. Overview of the ISO/IEEE 11073-20601 communication protocol

2.1. The ISO/IEEE 11073 (X73) standard suite

X73 contains the following important standard specifications, as described in Fig. **2.1**:

- ISO/IEEE 11073-10101: *Nomenclature*, which defines the vocabulary of terms used in Medical Device Communication (MDC)
- ISO/IEEE 11073-10201: *Domain Information Model (DIM)*, which contains the definition for structuring information transferred between entities
- ISO/IEEE 11073-104zz: *Device Specialization*, which defines specific medical device specialization. For example, the device specialization for a Blood Pressure Monitor is ISO/IEEE 11073-10407, while the specialization for a Glucose Meter is ISO/IEEE 11073-10417
- **ISO/IEEE 11073-20601**: *Application Profile - Optimized Exchange Protocol*, which defines the communication protocol for exchanging medical data

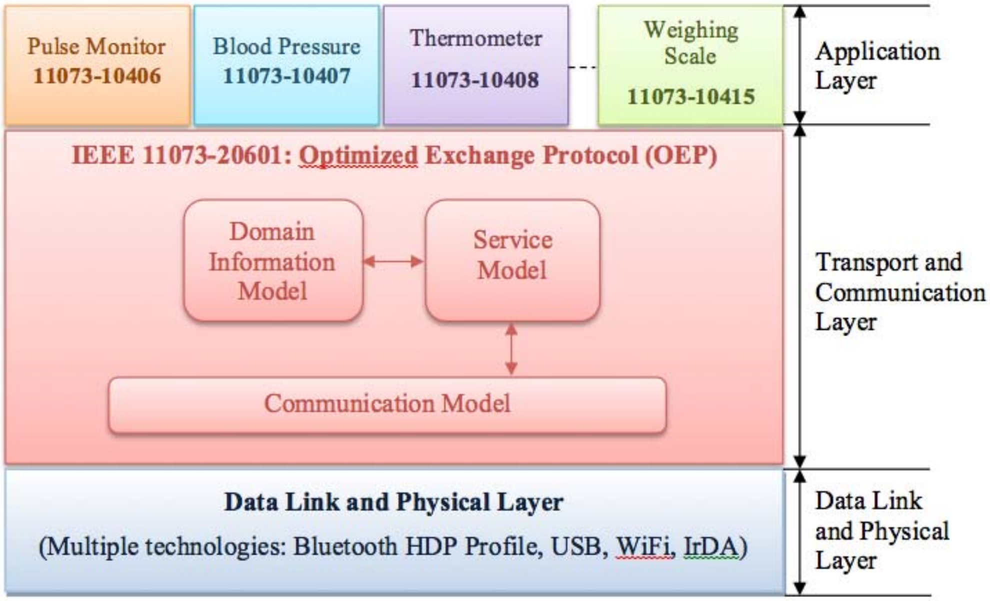

Pulse Monitor
11073-10406
Blood Pressure
11073-10407
Thermometer
11073-10408
Weighing Scale
11073-10415
Application Layer
IEEE 11073-20601: Optimized Exchange Protocol (OEP)
Domain Information Model
Service Model
Communication Model
Transport and Communication Layer
Data Link and Physical Layer
(Multiple technologies: Bluetooth HDP Profile, USB, WiFi, IrDA)
Data Link and Physical Layer

Fig. 2.1. The ISO/IEEE 11073 standard suite

For readability reasons, the standard "*ISO/IEEE 11073-20601: Application Profile – Optimized Exchange Protocol*" will be henceforth referred to as the ISO/IEEE 11073-20601 and the communication protocol defined within this standard will be referred to as the OEP (Optimized Exchange Protocol).

2.2. Entities involved in OEP

The ISO/IEEE 11073-20601 standard defines a point-to-point communication protocol between two entities, which are called Agent and Manager.

The *Agent* represents the device that collects personal health data directly from patients. It can be a thermometer, a blood pressure monitor, etc. In order to define the behavior of these heterogeneous devices, specific medical device specializations were defined: the ISO/IEEE 11073-104zz specializations.

The *Manager* represents the device that collects personal health data from the Agents. The Manager is represented by a local hosting device, which can be a smartphone, a notebook, a PC, etc.

2.3. Architecture of OEP

ISO/IEEE 11073-20601 [1] defines the means of creating abstract models for communicating personal health data between Agents and Managers over Body Area Networks (BAN). The standard definition consists of three main sections:

- The Domain Information Model (MDIB)
- The Service Model (CMDISE + ACSE)
- The Communication Model

These three sections describe the *data model*, the *operations* supported by the entities involved in the communication and the finite state machine describing the *communication process*, respectively. Fig. **2**.**2** shows the relationship between these components.

The standard was designed to provide means for short-distance communication, through the use of standardized wireless networks. The OEP protocol is flexible and lightweight. It can be implemented for different types of Agents, even for those with limited processing power and storage space.

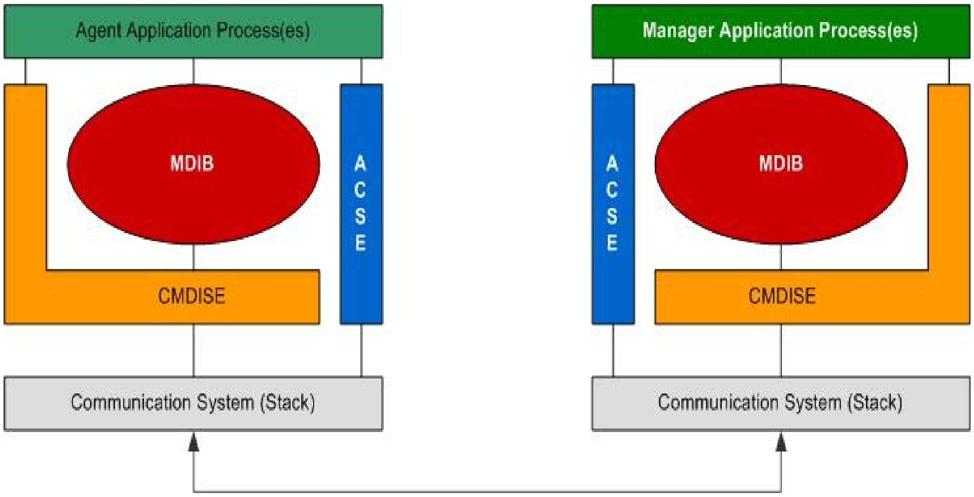

Agent Application Process(es)
MDIB
A C S E
CMDISE
Communication System (Stack)
Manager Application Process(es)
A C S E
MDIB
CMDISE
Communication System (Stack)

Fig. 2.2. Relationship model between Agents and Managers, as defined in OEP

2.4. Communication model of OEP

The OEP communication model supports a one-to-many topology. One Manager can communicate with one or more Agents over point-to-point connections. The communication model is defined by two finite state machines (FSM) that describe all the possible states the Agent and Manager may be in. Fig. **2**.**3** shows a simplified version of the state machine diagram that describes the communication between the Agent and the Manager (adaptation of the Agent's and Manager's state machine diagrams described in [1] – Fig. 10, pg. 57 and Fig. 11, pg. 60, respectively).

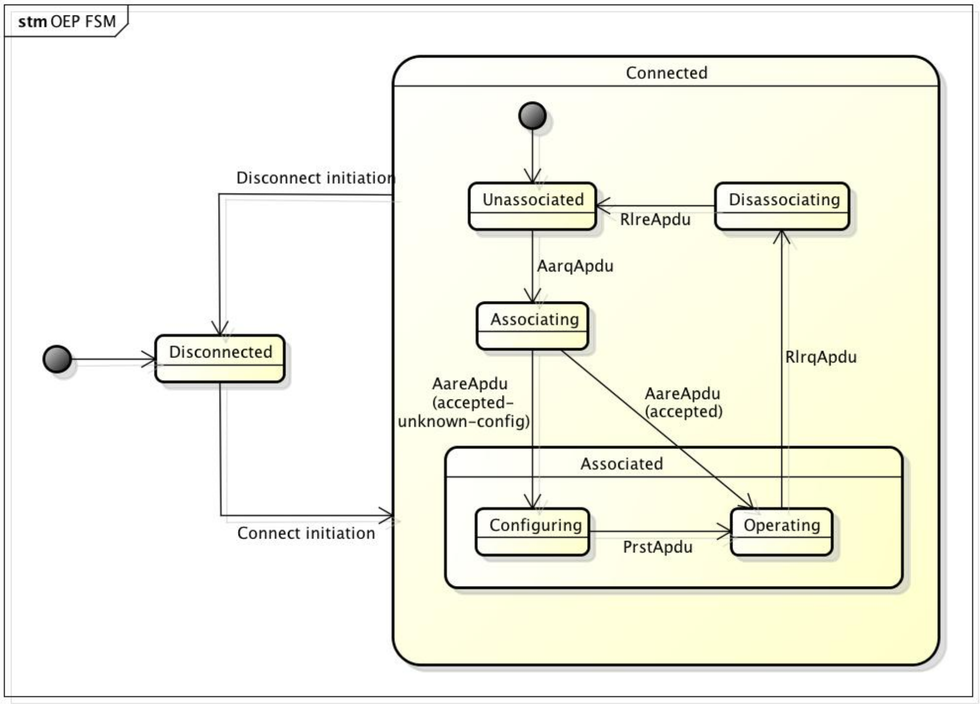


Fig. 2.3. Simplified communication state machine diagram

2.5. Configuration of OEP entities

The device configuration of an Agent is a set of objects and attributes that characterize that Agent. The device configuration is associated with a *dev-config-id* value. An Agent may own multiple device configurations, which may change in time. During the association procedure, however, the configuration cannot change. If the association with the Manager is already established, the Agent may change the configuration only by releasing the association first and then re-associating with the new desired configuration.

2.6. Association between OEP entities

The associating procedure allows the Agent and Manager to agree on a common data protocol and a common set of operating parameters. Both entities transit from the *Unassociated* state into the *Associating* state when the Agent decides to associate and sends an *Association Request* message.

Fig. **2.4** shows the sequence diagram of the associating procedure between the Agent and the Manager.

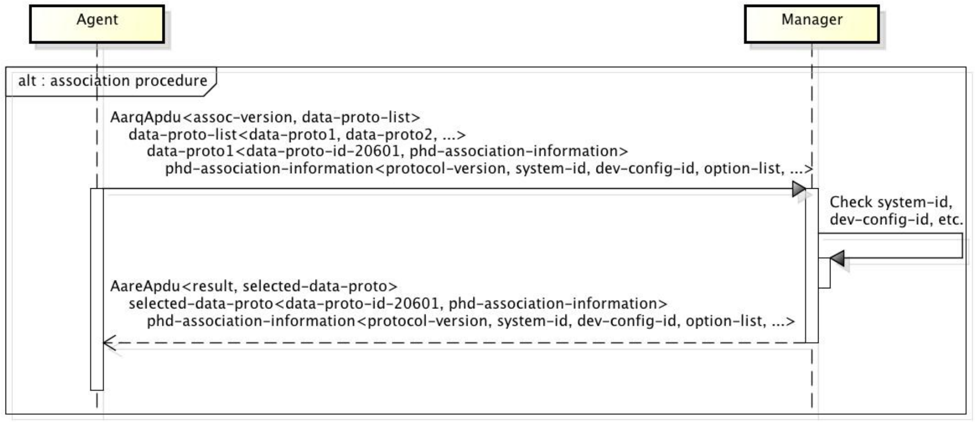

Agent
Manager
alt : association procedure
AarqApdu<assoc-version, data-proto-list>
data-proto-list<data-proto1, data-proto2, ...>
data-proto1<data-proto-id-20601, phd-association-information>
phd-association-information<protocol-version, system-id, dev-config-id, option-list, ...>
Check system-id,
dev-config-id, etc.
AareApdu<result, selected-data-proto>
selected-data-proto<data-proto-id-20601, phd-association-information>
phd-association-information<protocol-version, system-id, dev-config-id, option-list, ...>

Fig. 2.4. Error-free association procedure

There are two situations that may occur when the Agent initiates the association with the Manager:

- The Manager knows the Agent’s configuration
- The Manager does not know the Agent’s configuration

If the Manager already knows about the Agent’s configuration, the *result* field of the *AareApdu* message is set to *accepted*. This situation happens if a prior connection with the Manager had been established, or when the Agent has a standard configuration (i.e. a predefined configuration that is specified in a specialization standard). In this case, both entities transit into the *Operating* state.

If the Manager does not know the Agent’s configuration, the Manager informs the Agent that the association request is accepted, but that the configuration is unknown. The *result* field of the *AareApdu* message is set to *accepted-unknown-config*. In this case, both entities enter in the *Configuring* state.

2.7. ASN.1 and MDER

Abstract Syntax Notation One (ASN.1) [3] was chosen for representing all data types and exchange formats defined in OEP. ASN.1 is a standard notation used for describing rules and structures for information data.

Many communication protocols specifications define messages as binary values of sequences of octets. ASN.1 provides means of defining complex data types and messages without necessarily determining their binary representation. This notation is supplemented by the specification of one or more algorithms called *encoding rules*, which determine the value of the octets that carry the application semantics (called the transfer syntax).

ISO/IEEE 11073-20101:2004 [4] defines the medical device encoding rules (MDER) used in this standard.

3. Enhancing communication in ISO/IEEE 11073-20601

The current version of OEP does not support authentication. OEP passes the security responsibility to the implementer. However, different implementations of authentication procedures lead to incompatibilities and interoperability problems. In the authors' opinion, authentication guidelines should be at least provided, if not included in standard.

The authors' recent research [5] focused on designing an authentication procedure based on biometric keys, which can be integrated in an identity management system. The authentication is derived from the *mutual challenge-response* [6] authentication protocol. The exchanged authentication information is contained in the association messages, stored in an optional field named *optionList*. The proposed authentication is designed to be optional, to maintain backward compatibility with existing implementations of OEP. Thereby, two different scenarios can be distinguished, in terms of the bidirectional association initiation:

- Extending the association procedure for implementations that allow the authentication procedure
- Extending the association procedure for implementations that do not allow authentication (existing implementations of the ISO/IEEE version of the protocol)

3.1. Bidirectional association when authentication is required

This section proposes the extension of the association procedure for systems that employ authentication mechanisms. The method of authentication regarded here is the one considered in the recent research [5], i.e. *mutual challenge-response*. Fig. **3.1** describes the flow of messages exchanged between the Agent and the Manager when the Manager initiates the association procedure.

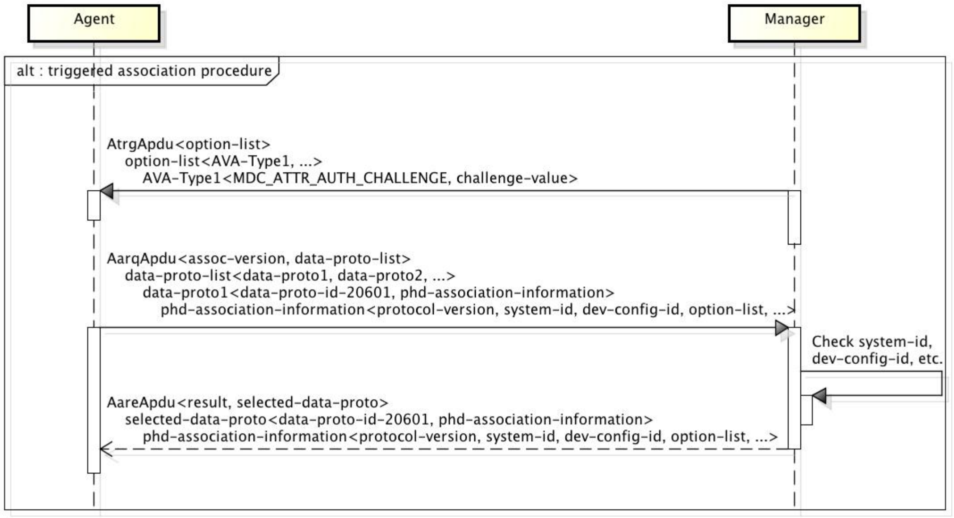

Agent
Manager
alt : triggered association procedure
AtrgApdu<option-list>
option-list<AVA-Type1, ...>
AVA-Type1<MDC_ATTR_AUTH_CHALLENGE, challenge-value>
AarqApdu<assoc-version, data-proto-list>
data-proto-list<data-proto1, data-proto2, ...>
data-proto1<data-proto-id-20601, phd-association-information>
phd-association-information<protocol-version, system-id, dev-config-id, option-list, ...>
Check system-id, dev-config-id, etc.
AareApdu<result, selected-data-proto>
selected-data-proto<data-proto-id-20601, phd-association-information>
phd-association-information<protocol-version, system-id, dev-config-id, option-list, ...>

Fig. 3.1. The message flow of an association procedure initiated by the Manager

The Manager initiates communication by triggering the Agent to request for association. The first message in Fig. **3.1** represents the trigger message. Existing association message types were used for describing the exchange of authentication information. In this case, however, existing association message types cannot be used to trigger the association. These types can only be used when the Agent and the Manager are in the *Associating* state. Since the Manager is in the *Unassociated* state when initiating the association, new type of message should be defined, to avoid ambiguous use of these messages.

Therefore, a new type of message named *AtrgApdu* is defined, which is detailed in section 4. This message is used by the Manager to trigger the Agent to request for association. To optimize the traffic flow, the *AtrgApdu* sent by the Manager should also contain the challenge, stored as the value of an *AVA-Type* attribute contained in the *optionList* field.

The second message represents the Agent's response to the triggered event received from the Manager. The *AarqApdu* message contains three important pieces of information:

- The *Association Request* triggered by the *AtrgApdu* message
- The response to the Manager's challenge
- The challenge for the Manager

The response to the Manager's challenge is the output of an irreversible function that takes two inputs: the challenge and the cryptographic key. A new *AVA-Type* attribute is created having the id set to *MDC_ATTR_AUTH_RESPONSE* and value set to the computed response. This attribute is stored in the *optionList* field contained in the *AarqApdu* message sent to the Manager.

The challenge sent by the Agent ensures that the authentication procedure is mutual. The Agent's challenge is generated identically to the one received from the Manager in the *AtrgApdu* message. This challenge is stored as the value of a new *AVA-Type* attribute that has the id set to *MDC_ATTR_AUTH_CHALLENGE*. This attribute is also added to *optionList*.

The third message represents the Manager's response to the *Association Request*. It also contains the authentication verdict and the response to the Agent's challenge. If the authentication succeeds, the outcome stored in the field *result* of the *AareApdu* message is usually set to either *accepted* or *accepted-unknown-config*, depending on the association information received from the Agent. If the authentication fails, the *result* is set to *rejected-authentication-required* and a new challenge is sent to the Agent.

The response to the Agent's challenge is determined identically to the one calculated by the Agent. A new *AVA-Type* attribute is created having the id set to *MDC_ATTR_AUTH_RESPONSE* and value set to the determined response. This attribute is stored in the *optionList* field of the *AareApdu* message.

If the *response* of the *AareApdu* message is *accepted*, the Agent enters in the *Operating* state. In this state the association is considered established, the configuration of the device is known, authentication is ensured and medical data can be transmitted.

3.2. Bidirectional association when authentication is not required

This section proposes the extension of the association procedure for systems that don't employ any authentication mechanism. The mechanism is similar to the one used when authentication is required. Fig. **3.1** depicts the association message flow.

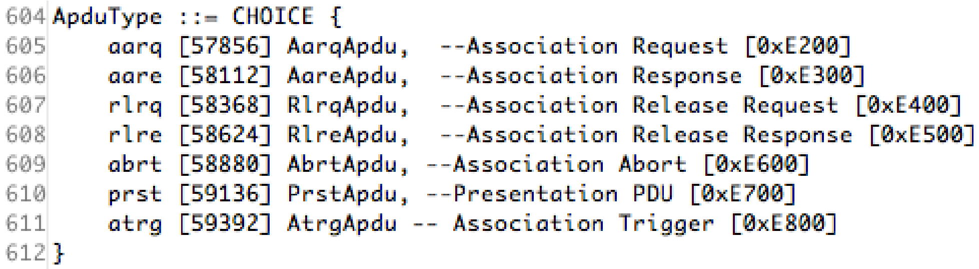
In this case, the trigger message sent from the Manager to the Agent does not encapsulate any authentication information, such as the challenge. The field *optionList* of the *AtrgApdu* message is empty.

The other two messages, i.e. *AarqApdu* and *AareApdu*, are identical to the ones used by the systems that implement the current specification of the protocol. The only extension of the protocol in this scenario is the *AtrgApdu* message, which represents just a trigger for the Agent to start the association phase.

4. The extended ASN.1 specification of OEP

This section presents the ASN.1 definitions of the terms introduced to support the bidirectional association initiation.

The first message depicted in Fig. **3.1**, i.e. *AtrgApdu*, is not defined in the ISO/IEEE version of the standard. A new ASN.1 message definition should be added to the specification, as shown in Fig. **4.1**.



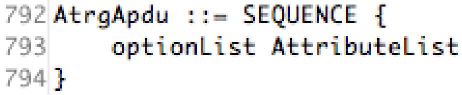
```
ApduType ::= CHOICE {
    aarq [57856] AarqApdu,  --Association Request [0xE200]
    aare [58112] AareApdu,  --Association Response [0xE300]
    rlrq [58368] RlrqApdu,  --Association Release Request [0xE400]
    rlre [58624] RlreApdu,  --Association Release Response [0xE500]
    abrt [58880] AbrtApdu, --Association Abort [0xE600]
    prst [59136] PrstApdu, --Presentation PDU [0xE700]
    atrg [59392] AtrgApdu -- Association Trigger [0xE800]
}
```

Fig. 4.1. Extended ASN.1 definition of *ApduType* with support for *AtrgApdu*

The *AtrgApdu* message has a clearly defined purpose, i.e. to determine the Agent to start the association procedure. This message is not intended to be a container for medical data, or configuration information. The only piece of information stored in the *AtrgApdu* message is the authentication challenge, which is used when systems employ an authentication procedure.

Therefore, the paper proposes that the *AtrgApdu* message type contains one optional field of type *AttributeList*, named *optionList*. *AttributeList* is a list of *AVA-Type* attributes, which are suitable containers for storing authentication information such as the challenge. *AVA-Type* attributes are adaptable to any changes regarding the challenge, such as its length, or type.

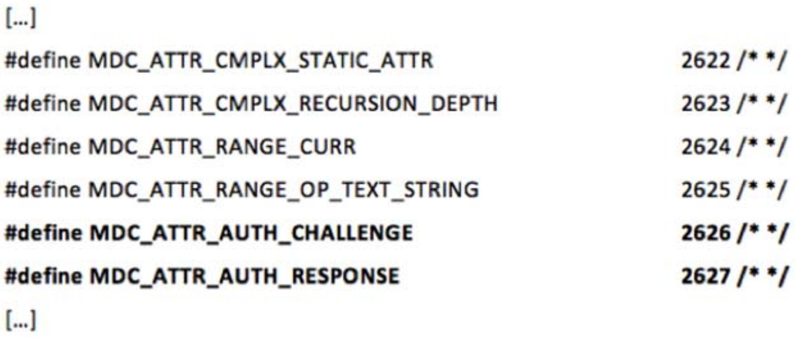
If there is no authentication procedure employed, the *optionList* should be left empty. Fig. **4.2** shows the ASN.1 definition of the *AtrgApdu* message.



```
AtrgApdu ::= SEQUENCE {
    optionList AttributeList
}
```

Fig. 4.2. ASN.1 definition of *AtrgApdu*

AVA-Type is a data type that specifies attribute objects characterized by *attribute-ids* and *attribute-values*. When instantiating new *AVA-Type* attributes, their *attribute-ids* must be set to values defined in the ISO/IEEE 11073-10101 – Nomenclature. Therefore, attributes used for storing authentication information should use two *attribute-ids*, i.e. *MDC_ATTR_AUTH_CHALLENGE* and *MDC_ATTR_AUTH_RESPONSE*. The definition of the two ids are added in the “Partition: ATTR/GROUP” section of the Nomenclature, as shown in Fig. **4.3**.



```
[...]
#define MDC_ATTR_CMPLX_STATIC_ATTR              2622 /* */
#define MDC_ATTR_CMPLX_RECURSION_DEPTH          2623 /* */
#define MDC_ATTR_RANGE_CURR                     2624 /* */
#define MDC_ATTR_RANGE_OP_TEXT_STRING           2625 /* */
#define MDC_ATTR_AUTH_CHALLENGE                 2626 /* */
#define MDC_ATTR_AUTH_RESPONSE                  2627 /* */
[...]
```

Fig. 4.3. ASN.1 definition of challenge and response attribute-ids

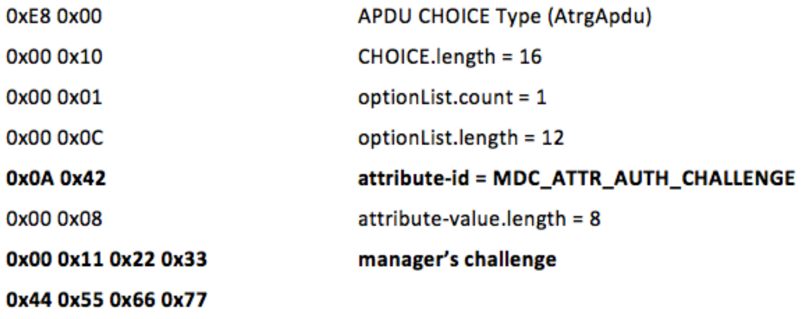
If no authentication is required, the *AtrgApdu* message contains an empty list of attributes. If authentication is required, the *AtrgApdu* contains a list that includes an *AVA-Type* attribute that has the *attribute-id* set to *MDC_ATTR_AUTH_CHALLENGE* and the *attribute-value* set to the value of the actual challenge. The extension of the protocol to allow the Manager to instantiate communication does not imply major changes in the standard. The behavior of the applications that implement the ISO/IEEE version of the protocol does not change and the new functionality can be easily implemented.

5. Illustration of association initiated by the Manager

The section highlights the contents of the messages exchanged in the association process. For this illustration, a scenario where the mutual challenge-response authentication is employed is considered. In this scenario, the challenge's length is 64 bits, and the response is 128 bits.

5.1. The association trigger

Fig. **5.1** describes the message sent by the Manager to initiate communication. This message corresponds to the first message depicted in Fig. **3.1**.

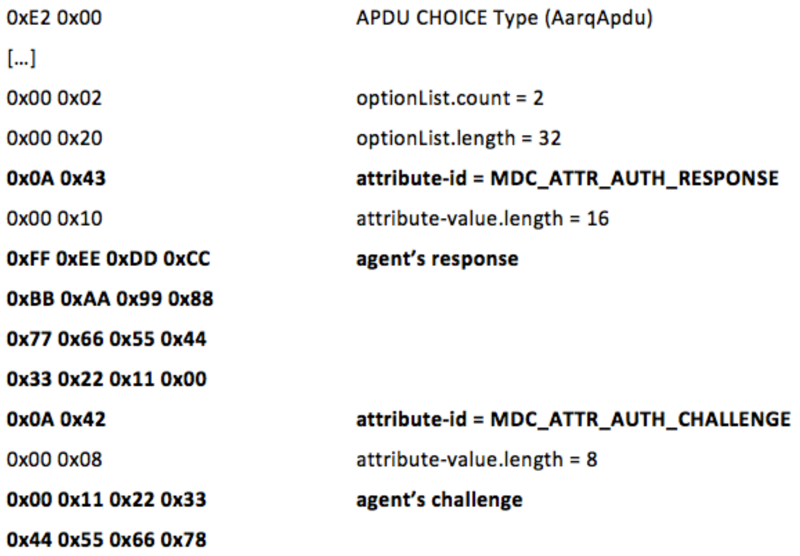


```
0xE8 0x00                    APDU CHOICE Type (AtrgApdu)
0x00 0x10                    CHOICE.length = 16
0x00 0x01                    optionList.count = 1
0x00 0x0C                    optionList.length = 12
0x0A 0x42                    attribute-id = MDC_ATTR_AUTH_CHALLENGE
0x00 0x08                    attribute-value.length = 8
0x00 0x11 0x22 0x33          manager's challenge
0x44 0x55 0x66 0x77
```

Fig. 5.1. Example of an *AtrgApdu* message

5.2. The association request

The *Association Request* contains the response to the Manager's challenge and its own challenge. This message, which corresponds to the second message presented in Fig. **3.1**, is detailed in Fig. **5.2**.



```
0xE2 0x00               APDU CHOICE Type (AarqApdu)
[…]
0x00 0x02               optionList.count = 2
0x00 0x20               optionList.length = 32
0x0A 0x43               attribute-id = MDC_ATTR_AUTH_RESPONSE
0x00 0x10               attribute-value.length = 16
0xFF 0xEE 0xDD 0xCC     agent's response
0xBB 0xAA 0x99 0x88
0x77 0x66 0x55 0x44
0x33 0x22 0x11 0x00
0x0A 0x42               attribute-id = MDC_ATTR_AUTH_CHALLENGE
0x00 0x08               attribute-value.length = 8
0x00 0x11 0x22 0x33     agent's challenge
0x44 0x55 0x66 0x78
```

Fig. 5.2. Example of an *AarqApdu* message triggered by the *AtrgApdu*

5.3. The association response

Since the authentication is mutual, the Manager must authenticate to the Agent, as well. The third message described in Fig. **3.1** represents the last step of the association process. This message contains the association outcome, the verdict to the Agent's authentication attempt, and the response to the Agent's challenge, if authentication succeeded. This message is constructed in a similar way to the messages presented in this section.

6. Conclusions

This paper presented a solution for an issue of the standard that has not gained research focus so far. The bidirectional initiation of the association procedure is an important OEP capability required in common real-world scenarios. Several scenarios were discussed to highlight the importance of this capability.

The paper presented the proposed solution that addresses the problem. Two different scenarios were identified: the current implementation of the standard (with no required authentication), and an extended implementation that employs a patient and device authentication mechanism. A solution was proposed for each of the two scenarios. The solution is designed to be optional. Therefore, backward compatibility with current implementations of the protocol is ensured.

In terms of the implementation, the paper offered guidelines such as how to extend the Nomenclature with the required terms, or how to define the association trigger ADPU. A complete real-world scenario was considered. The messages exchanged during the association procedure were detailed in the paper.

It is the authors' opinion that the extension is required in common scenarios encountered in laboratories or hospitals and should be included in the standard specification, in order to promote interoperability.

REFERENCES

[1] IEEE Engineering in Medicine and Biology Society, Health informatics—Personal health device communication Part 20601: Application profile—Optimized Exchange Protocol, New York, 2008.

[2] IEEE Engineering in Medicine and Biology Society, Health informatics — Point-of-care medical device communication — Part 10101: Nomenclature, First edit., 2004.

[3] International Telecomunication Union, "Abstract Syntax Notation One (ASN.1)." [Online]. Available: http://www.itu.int/ITU-T/asn1/index.html. [Accessed: 08-Sep-2012].

[4] IEEE Engineering in Medicine and Biology Society, Health informatics — Point-of-care medical device communication — Part 20101: Application profiles — Base standard, First edit., 2004.

[5] *A. Egner, A. Soceanu, and F. Moldoveanu*, "Managing Secure Authentication for Standard Mobile Medical Networks," in *Proceedings of IEEE ISCC*, 2012, Cappadocia, Turkey, pp. 390 – 393.

[6] *B. Forouzan*, Cryptography and Network Security, First edit. 2007, pp. 421 – 426.

[7] "Continua Health Alliance." [Online]. Available: http://www.continuaalliance.org/index.html. [Accessed: 08-Sep-2012].

[8] LibreSoft, "OpenHealth Project." [Online]. Available: http://libresoft.es/research/software/openhealth. [Accessed: 08-Sep-2012].

[9] *L. Schmitt, T. Falck, F. Wartena, and D. Simons*, "Towards Plug-and-Play Interoperability for Wireless Personal Telehealth Systems."

[10] *I. Martinez, P. Del Valle, P. Munoz, J. D. Trigo, J. Escayola, M. Martínez-Espronceda, A. Muñoz, L. Serrano, and J. Garcia*, "Interoperable and standard e-Health solution over Bluetooth," in 32nd Annual International Conference of the IEEE EMBS, 2010, pp. 2192–2195.

[11] *M. Petkovic*, "Remote patient monitoring: Information reliability challenges," in 9th International Conference on Telecommunication in Modern Satellite Cable and Broadcasting Services, 2009, pp. 295–301.

[12] *J. Noueihed, R. Diemer, S. Chakraborty, and S. Biala*, "Comparing Bluetooth HDP and SPP for Mobile Health Devices," in 2010 International Conference on Body Sensor Networks, 2010, pp. 222–227.

[13] *X. M. Zhang and N. Zhang*, "An Open, Secure and Flexible Platform Based on Internet of Things and Cloud Computing for Ambient Aiding Living and Telemedicine," in 2011 International Conference on Computer and Management (CAMAN), 2011, pp. 1–4.

[14] *M. Patel and J. W. J. Wang*, "Applications, challenges, and prospective in emerging body area networking technologies," Ieee Wireless Communications, **vol. 17**, no. 1, pp. 80–88, 2010.