“The Fairhair Alliance facilitates the Internet of Things for Commercial Buildings”

Workshop on IoT Semantic/Hypermedia Interoperability 2017

Teresa Zotti, Piotr Polak, Philips Lighting,
{teresa.zotti, piotr.polak}@philips.com
(High Tech Campus 7, 5656AE, Eindhoven, The Netherlands)

Abstract

In the last few years, an extremely intense and exciting wave of standardization in IETF (Internet Engineering Task Force) has made IPv6 communication possible on a variety of physical interfaces. These developments with the availability of new protocols such as Thread show that the IoT (Internet of Things) for resource constrained devices is becoming reality. Along with new ways of connecting devices and innovative communication protocols, the IoT comes with the promise to ease boot-strapping of devices and commissioning procedures, make maintenance cost-effective via real-time monitoring and to open the way to new business opportunities based on data analytics.
However, to be able to turn the IoT promises into reality the industry has to face two major challenges: interoperability and security.
This paper describes how Fairhair, an alliance of leading companies from the Lighting, Building Automation and IT industry proposes to solve these problems bridging today’s state-of-the-art technology to tomorrow’s needs.

1. Introduction

IoT applications require standard solutions which can communicate and interwork with each other and where sensor data can be discovered and shared across multiple players in the ecosystem. However, the need for horizontal integration is confronted with today’s highly fragmented market where a plethora of technologies, created to meet the needs of different industries, exists.

Furthermore, in a connected world which envisions data flowing across domains and which relies on multiple underlying networking technologies, security becomes a crucial aspect. The lack of a standard common approach to secure communication between devices, which is independent from the specific networking protocol in use, creates additional barriers.
The fear that thousands of internet-connected devices in close proximity can be compromised by malware created by hackers with unpredictable consequences is becoming more and more a key concern and is unavoidably hampering the adoption of IoT systems in commercial buildings.

Globally successful and established ecosystems such as BACnet, KNX and zigbee already count many millions of field devices deployed in today’s buildings and together give a relevant representation of the actual size of the lighting and building automation market. The major asset of these protocols resides in their mature data models, the fruit of years of contributions from many industry leaders. Preserving their models and limiting the impact on existing tooling and their application design paradigms is one of the aspects that needs to be considered while evolving towards IoT.

While the common challenges that these ecosystems are facing in their journey towards IoT are complex obstacles, at the same time they represent an incredible opportunity for the industry: breaking down existing barriers and bringing building domains closer to each other.

This opportunity is the foundation on which Fairhair, an alliance of leading companies from the Lighting, Building Automation, IT, and silicon industry[1] was built. The Fairhair Alliance's mission is to guide major lighting and building automation ecosystems such as BACnet, KNX and zigbee in their extensions towards IP-based connected systems, standardizing a common infrastructure and specifying all needed application services, ranging from security, discovery to network management.

Early in 2017, Fairhair has completed its first draft specification. This paper gives an overview of the main technical solutions specified by Fairhair.

2. Fairhair scope and key technology choices

Although the Fairhair specification does not prescribe any specific physical interface, it is particularly designed to work with resource-constrained interfaces. This becomes obvious when looking at the technology choices and the IP stack shown in Figure 1.

The Fairhair application framework sits on top of a generic User Datagram Protocol [2] (UDP)/IPv6 stack that provides a medium-independent means of data transport over wired or wireless physical interfaces.
At the transport layer, UDP is a natural choice for network applications such as lighting control applications in which latency is critical, guaranteeing a lower bandwidth overhead when compared for example to the Transmission Control Protocol (TCP).
To interface to the UDP/IPv6 stack, Fairhair uses services provided by the Constrained Application Protocol (CoAP) [3], designed by IETF for use with low-power and constrained networks.

In general, the work carried out in Fairhair builds upon specifications coming out of the IETF, tailoring existing RFCs to meet the requirements of the building automation industry, or driving new RFCs.

The core of Fairhair is represented by a set of mechanisms, such as network management, resource discovery and security which are independent from the specific application layer protocol in use. These services all operate on resources that are described according to common rules and interfaces defined by the Fairhair resource model.

A Representational State Transfer (REST) architectural style is used as interaction model for creating, reading, setting, and deleting data by means of standard CoAP methods (i.e., GET, PUT, POST, DELETE) [3].
The format chosen to encode the messages exchanged between devices is the Concise Binary Object Representation (CBOR) [4] which is based on the widely successful JSON (JavaScript Object Notation) format [5], specified in IETF. The usage of CBOR aims to reduce both code and message size thereby enabling faster processing of data.

[1] At the time of writing, Fairhair counts six Sponsor Members (Cisco, Lutron, Osram, Philips Lighting, Siemens and Silicon Labs) and five Regular Members (Trilux, KNX Association, NXP, Runtime Inc. and Zumtobel group). More information is available at https://www.fairhair-alliance.org/membership/fairhair-members.

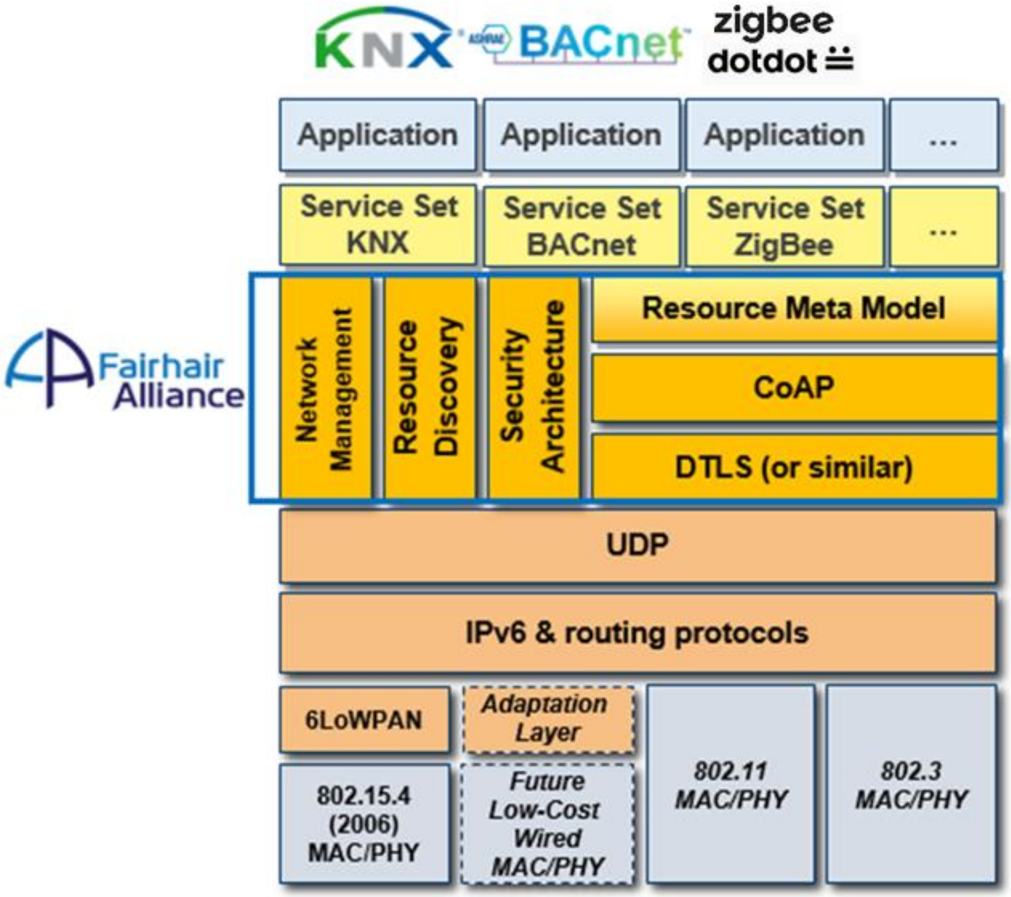

Figure 1- Fairhair technology stack

In smart buildings, where thousands of devices are deployed and installed, a mechanism which enables the discovery of devices and the resources they host is an essential step during commissioning as well as at run-time.
The need for seamless scalability from small, for example ten devices, to large (1000+ devices) networks and the ability to support battery-powered devices, are driving requirements for the Fairhair Resource Discovery.

The solution proposed is based on IETF CoAP discovery using Link Format [6] resource descriptions. Fairhair supports both a distributed discovery, usually via multicast queries to the "/.well-known/core" resource of devices, as well as unicast queries and registrations to a central resource directory [7].

The security architecture is based on state-of-the-art IT technology, appropriating the technology for wireless mesh networks. It builds on public key cryptography (IEEE 802.1ar) [8] supporting strong device identities. The protocol flow to bring devices automatically onto the network is based on the Autonomic Networking Integrated Model and Approach (ANIMA) [9]. Application layer security is based on DTLS [10] and adapts the well-known Transport Layer Security (TLS). Additional extensions are developed to secure group communication for example, as in COSE (CBOR Object Signing and Encryption) [11].

On top of the common application services defined by Fairhair, we find the ecosystem specific "service-set". It is here where the ecosystems like KNX, BACnet and zigbee position their core asset: their application layer protocol specifications with their specific commands and device representations. A concrete example of "service-set" is the zigbee Cluster Library (ZCL), a mature and very fine-grained specification of control functions and properties for luminaires, sensors, switches, etc.

3. Towards semantic interoperability: Fairhair standard metadata.

Smart devices can potentially generate a vast quantity of data, however the semantic of this data is often implicit or exposed in eco-system specific formats.

To make interpretation of data easier, some protocols nowadays already define ways of adding a notation to the data, the so-called metadata. Literally "data about data", metadata can be extremely useful to understand things such as the data types of a value for example binary, string, or integer, its resolution or even the engineering units used to represent it such as degrees Celsius or Fahrenheit for temperature data.

However, there will still be limited value in defining metadata if each application protocol chooses different formats and mechanisms to retrieve it.

As a first step to enhance semantic interoperability, Fairhair defines a standard list of metadata and promote its adoption by the relevant ecosystems.
Table 3-1 shows a subset of Fairhair metadata, with their standardized description and mnemonic.

Metadata	**Description**	**Mnemonic**
Base	The base data type of the data item (e.g. Boolean, unsigned integer)	**$base**
Unit	The engineering unit of the data item (e.g. meter, Celsius, Fahrenheit)	**$unit**
Min	The minimum value allowed for the data item.	**$min**
Max	The maximum value allowed for the data item.	**$max**
Access	The allowed methods of accessing the data item (i.e. readability, writability, etc.)	**$acc**

Table 3-1- Subset of Fairhair standard metadata

Metadata is accessible on demand (i.e. only if requested, e.g. by query parameter) by means of the same CoAP methods and RESTful interfaces used for data.
The list of standardized metadata is the result of a careful evaluation of common information that each protocol needs to expose. At the same time, to address those use cases not common to all applicable protocols, Fairhair allows to add more metadata, by providing guidelines which allow for ecosystem-specific metadata definitions, avoiding clashes with those ones proposed by Fairhair.

Fairhair achieves the next step towards semantic interoperability by standardizing primitive data types (e.g., boolean, string, integer), complex data types (e.g., array, list) and restrictions of values (e.g., range for numeric values, length for strings), their definition and a consistent encoding format of this information in CBOR.
In this way, each application protocol could annotate an ecosystem specific data value with additional information that is commonly interpreted.
For example, an ecosystem specific resource is enriched with a Fairhair metadata "$base" equal to "uint". Because of the use of the same agreed notation and format value, every protocol will properly parse and interpret "uint" as an unsigned integer without possibility of misinterpretation.

Table 3-2 shows Fairhair primitive datatypes and their corresponding CBOR representations.

Fairhair Data Type	**Description**	**Standard mnemonics** ($base=)	**CBOR Representation**
Null	No value. The data item has no value set.	null	CBOR null (major type 7, additional information 22)
Boolean	Boolean value (true/false)	bool	CBOR true (major type 7, additional information 21) CBOR false (major type 7, additional information 20)
Unsigned Integer	Represents unsigned integer values of different sizes.	uint	CBOR unsigned integer (major type 0)
Signed Integer	Represents signed integer values of different sizes.	int	CBOR unsigned integer (major type 0) or CBOR signed integer (major type 1), depending on the actual value
Half Float	Half precision floating point	float16	major type 7, additional information 25
Float	Single precision floating point	float32	major type 7, additional information 26
Double	Double precision floating point	float64	major type 7, additional information 27
String	Unicode character string	string	CBOR text string data item (major type 3)
Enumeration	Value from a set of assigned names	enum	CBOR unsigned integer data item (major type 0)

Bits	Set of flags identified by position	bits	CBOR byte string data item (major type 2)
Binary	Binary data, i.e. a sequence of octets	binary	CBOR byte string data item (major type 2)

Table 3-2- Fairhair primitive data types

The continuous and open dialogue with the involved ecosystems highlighted how the work done so far in Fairhair could become even more useful if standard metadata along with their definitions and format would be described in a machine-readable format. The creation of this machine-readable description represents work in progress in Fairhair. By accomplishing this task, it will be possible to discover the semantic of data in real-time and make the solution future-proof. Changes in the definition of the metadata across different software versions will be in fact reflected in their online descriptions, easing maintenance.

4. Conclusions

Fairhair defines a common IP based network infrastructure and connectivity, allowing integrating different BA and Lighting applications on a single network. The solution can be deployed on top of any IP network deployment independently form the underlying networking technologies.
Fairhair fosters:

- common syntactic understanding (CoAP, CBOR)
- common approaches to cross cutting issues, e.g. security and discovery
- framework/methods for adding semantic annotation, which will mainly be defined in the eco-systems.

The Fairhair Alliance is an open, global consortium, and welcomes all potential new members.

Companies, associations and universities can benefit from joining Fairhair by:

- Breaking down the traditional silos of independent building-automation and lighting-control systems in buildings.
- Co-creating specifications for a common network infrastructure.
- Defining requirements and validating related specifications to create an aligned, unified, IP-based solution.
- Co-creating draft specifications for the application protocol layer, for adoption by the respective ecosystems such as BACnet, KNX and zigbee.
- Getting access to specifications
- Participating in interoperability testing with other members.

Interested to join and contribute to Fairhair? Please contact the secretary general of Fairhair Alliance Ruud van Bokhorst, secretary-general@fairhair-alliance.org.

5. References

[1] Deering, Hinden, “Internet Protocol, Version 6 (IPv6) Specification”, RFC 2460, December 1998, https://tools.ietf.org/html/rfc2460

[2] Postel, “User Datagram Protocol”, RFC 768, 28th August 1980, https://tools.ietf.org/html/rfc768

[3] Shelby, Hartke, Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, June 2014, https://tools.ietf.org/html/rfc7252

[4] Bormann, Hoffman, Concise Binary Object Representation (CBOR), RFC 7049, October 2013, https://tools.ietf.org/html/rfc7049

[5] Bray, The JavaScript Object Notation (JSON) Data Interchange Format, RFC 7159, March 2014, https://tools.ietf.org/html/rfc7159

[6] Shelby, Constrained RESTful Environments (CoRE) Link Format, RFC 6690, August 2012, https://tools.ietf.org/html/rfc6690

[7] Shelby, Koster, Bormann, van der Stok, CoRE Resource Directory, https://tools.ietf.org/html/draft-ietf-core-resource-directory-10

[8] 802.1AR-2009 - IEEE Standard for Local and metropolitan area networks - Secure Device Identity, https://standards.ieee.org/findstds/standard/802.1AR-2009.html

[9] Pritikin, Richardson, Behringer, Bjarnason, Watsen, Bootstrapping Remote Secure Key Infrastructures (BRSKI)”, May 20177, https://tools.ietf.org/html/draft-ietf-anima-bootstrapping-keyinfra-06

[10] Rescorla, Modadugu, Datagram Transport Layer Security Version 1.2, RFC 6347, https://tools.ietf.org/html/rfc6347

[11] Schaad, Cellars, CBOR Object Signing and Encryption (COSE), May 2017, https://tools.ietf.org/html/draft-ietf-cose-msg-24