coman
Internet-Draft
Intended status: Informational
Expires: August 9, 2013

B. Greevenbosch
K. Li
Huawei Technologies

February 5, 2013

Candidate Technologies for COMAN
draft-greevenbosch-coman-candidate-tech-00

Abstract

This draft identifies candidate technologies and considerations for the COMAN use cases and requirements.

Note

Discussion and suggestions for improvement are requested, and should be sent to coman@ietf.org.

Status of this Memo

Copyright Notice

Table of Contents

1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Introduction

In [I-D.ersue-constrained-mgmt], several use cases and associated requirements are defined for the management of constrained devices, in a possibly constrained network.

This document identifies possible technologies associated with the use cases and requirements.

In addition, this document includes several considerations associated with the requirements, that are relevant for choosing proper technologies.

The goal of this document is to identify what has been done, and what still needs to be done. Especially, it aims at establishing a clearer view of the scope and work in COMAN.

3. Identified candidate technologies for the requirements

3.1. OMA-LwM2M

OMA Lightweight M2M [OMA-LwM2M-TS] aims at providing an underlying layer agnostic protocol to allow M2M service enablement and management between the LwM2M Server and the LwM2M Client, which is placed in the resource constrained devices. The first version of enabler is currently being specified. The enabler provides a light and compact protocol and a flat data structure, and can satisfy various management requirements for constrained devices.

OMA-LwM2M has overlap with the following COMAN requirements:

- 4.2.002 Compact encoding of management data

- 4.4.001 Device status monitoring
- 4.4.002 Energy status monitoring
- 4.4.010 Logging
- 4.6.001 Security and access control
- 4.6.002 Authentication of managed devices
- 4.6.003 Access control on managed constrained devices
- 4.6.004 Access control on management systems
- 4.6.005 Support suitable security bootstrapping mechanisms
- 4.8.001 Software distribution (firmware update)

Because of the overlap and early stage of OMA-LwM2M, good coordination between COMAN and OMA-LwM2M is advisable.

3.2. OMA Device Management

OMA Device Management [OMA-DM] provides various functions for mobile device management. OMA-DM specifies and depends heavily on the SyncML language, which uses XML. The typical underlying transport protocol is HTTP. This makes OMA-DM in unaltered form infeasible for constrained devices. Especially, it violates the following requirements:

- 4.1.001 Support multiple device classes within a single network

- 4.2.002 Compact encoding of management data

Nevertheless, there is much overlap between OMA-DM functionality and COMAN requirements. As such, OMA-DM MAY be used as inspiration for the COMAN solution.

OMA-DM defines a general data model for management purpose, which is called a Management Object (MO). MOs are stored on the device and

can be manipulated by management actions carried over the OMA-DM protocol. For each management purpose, a specific MO has been defined. MOs relevant to the COMAN requirements include "FUMO" for firmware update requirements, "DiagMon MO" for diagnostic and monitoring requirements and the "Scheduling MO" for scheduling requirements. The various MOs are discussed in Section 3.2.1 and its subsections.

Apart from requirements covered by MOs, the following COMAN requirements intersect with the general OMA-DM functionality:

- 4.1.008 Network-wide configuration - Use broadcast capability from OMA-DM 1.3 - Sessionless specification.

3.2.1. OMA-DM Management Objects

3.2.1.1. OMA DiagMon MO

OMA DiagMon MO builds on and leverages the OMA DM v1.x protocol. It provides standard DM Management Objects and associated client-side and server-side behaviour necessary to conduct diagnostics and monitoring activities on mobile devices.

Requirements related to OMA DiagMon MO:

- 4.4.003 Monitoring of current and estimated device availability: can be achieved by DiagMon functions MO.
- 4.4.004 Network status monitoring: can be achieved by DiagMon functions MO.
- 4.4.009 Notifications: can be achieved by reporting functions in DiagMon MO.
- 4.4.011 Performance monitoring: can be achieved by DiagMon functions MO.
- 4.4.012 Fault detection monitoring: can be achieved by Trap MO.

- 4.4.013 Passive monitoring: can be achieved by Trap MO.

- 4.4.014 Reactive monitoring: can be achieved by Trap MO.

- 4.5.001 Self-management: device events can be captured by Trap MO, to achieve self-management.

- 4.5.002 Periodic self-management: device events can be captured by Trap MO periodically, to achieve self-management.

3.2.1.2. OMA Scheduling MO

The OMA-DM Scheduling MO enabler [OMA-Scheduling-MO] specifies the scheduling framework as well as its Management Objects that can be layered on top of OMA-DM v1.x, to seamlessly add the common scheduling capability to the OMA-DM based management infrastructure. With this capability, the OMA-DM system is able to schedule management operations on the device, and have them executed offline when the schedule - time-based or event-based - matches.

Requirements related to OMA Scheduling MO:

- 4.5.002 Periodic self-management: time-based scheduled task can achieve periodic self-management.

3.2.1.3. OMA-FUMO

OMA-FUMO provides information on management objects associated with firmware updates in OMA-DM based mobile devices and the behaviour associated with the processing of the management objects.

Requirements related to OMA-FUMO:

- 4.8.001 Software distribution: firmware update can be achieved by FUMO.

3.2.2. ACL mechanism in OMA-DM

OMA-DM [OMA-DM] defines the Access Control List (ACL) mechanism to control the access to the Management Objects. ACL is a property associated with the Management Object nodes, and is used to grant access permissions to the server identifiers.

Related requirements:

- 4.6.003 Access control on managed constrained devices

- 4.6.004 Access control on management systems
- 4.6.005 Support suitable security bootstrapping mechanisms

3.3. CoAP

The Constrained Application Protocol (CoAP) [I-D.ietf-core-coap] is defined by the IETF. It provides an application layer protocol especially designed for constrained devices. It is binary and easy to parse.

CoAP is especially suitable on top of IPv6 and UDP. However, other lower level protocols are possible too.

In addition, several drafts have been specified to target specific issues.

3.3.1. CoAP main specification

The following requirements are met by the CoAP main specification:

- 4.1.001 Support multiple device classes within a single network - the low complexity of CoAP allows usage in all device classes.
- 4.1.004 Minimise state maintained on constrained devices - CoAP has been designed to keep servers stateless.
- 4.1.007 Support for lossy and unreliable links - through the CoAP CON retransmission mechanism.
- 4.2.004 Mapping of management protocol interactions - CoAP provides HTTP/Coap Mapping.
- 4.2.007 Protocol extensibility - mainly provided by options mechanism.
- 4.3.004 Asynchronous transaction support - CoAP supports separate response and piggy-backed response.
- 4.4.012 Fault detection monitoring (partly) - CoAP pinging allows verification if a device is online.

3.3.2. CoAP capability discovery specifications

Various CoAP drafts cover different aspects of capability discovery.

- RFC 6690 [RFC6690] defines a link format, which provides information on resources a server is offering.

- The draft [I-D.greevenbosch-core-profile-description] allows signalling a CoAP server profile.

- The draft [I-D.shelby-core-resource-directory] allows acquiring information about resources from another server, called the "Resource Directory".

Related COMAN requirement:

- 4.3.003 Capability discovery

3.3.3. CoAP group communication

The informational CoAP group communication draft [I-D.ietf-core-groupcomm] discusses various aspects of group communication through IP multicast [RFC4604] in CoAP.

Related COMAN requirement:

- 4.8.002 Group-based provisioning

3.3.4. CoAP energy saving technology

The draft [I-D.rahman-core-sleepy] provides a mechanisms for sleepy devices. These mechanisms include informing an intermediate resource directory (defined in [I-D.shelby-core-resource-directory]) of its waking up or intent to fall asleep. Through these two drafts, clients can use the observe mechanism [I-D.ietf-core-observe] to be informed of whether a device is sleeping or active.

Related COMAN requirements:

- 4.1.005 Support devices that are not always online

- 4.7.005 Support of energy-optimized communication protocols

3.3.5. Congestion avoidance in CoAP

The considerations in this section relate to:

- 4.9.001 Congestion avoidance

- 4.9.003 Traffic delay schemes

The draft [I-D.bormann-core-cocoa] provides general background information about CoAP congestion control, and its challanges.

The draft [I-D.li-core-conditional-observe] defines a mechanism to

signal minimum time between CoAP observations.

The draft [I-D.greevenbosch-core-minimum-request-interval] defines a mechanism to restrict the speed in which a CoAP client sends requests to the CoAP server.

Other ways to delay the traffic in CoAP is by sending delayed ACKs. However, this has limitations as too much delay will lead to retransmits from the client side. In addition, this method requires the server to maintain bookkeeping of the delayed ACKs.

3.4. Cryptography considerations

4.6.001 Security and access control

4.6.002 Authentication of managed devices

- The raw public key as defined in [I-D.ietf-tls-oob-pubkey] can be used for establishing security and authentication.

- OCSP-lite as defined in [I-D.greevenbosch-tls-ocsp-lite] can be used for revocation checking of the raw public key.

4.6.005 Support suitable security bootstrapping mechanisms

- The draft [I-D.jennings-core-transitive-trust-enrollment] describes a system in which a Device is introduced to a Controller by a Introducer. In this draft, it is suggested that the Device symmetric key is coded as a QR code on the box, which can be read by the Controller, which may be a mobile phone with internet access.

4.6.006 Enable the authentication of a large number of devices at system start

- TBD

4.6.007 Select cryptographic algorithms that are efficient in both code space and execution time

- Candidates for asymmetric cryptography:
  - RSA
  - ECC

  Keysize TBD.

- Candidates for symmetric cryptography:
  - AES (keysize 128/192/256)

  Keysize TBD.

- Candidates for hashing:
  - SHA-1
  - SHA-256
  - SHA-512

4.6.008 Select cryptographic algorithms that are to be supported in hardware

- TBD

3.5. MANET

TBD.

Reference [RFC6130] for Neighbour Discovery, if it is sufficiently related to Neighbour Monitoring (4.4.007).

3.6. Other requirements and candidate technologies

4.1.003 Hierarchical management

4.1.005 Support devices that are not always online

- Mechanisms for devices that are not sleepy, but have unstable network connections (e.g. mobile devices) are needed.

4.1.006 Automatic re-synchronisation with eventual consistency

4.1.009 Distributed management

4.2.001 Enabling modular implementations of management protocols with a basic set of protocol primitives

4.2.005 Consistency of data models with the underlying information model

4.2.006 Loss-less mapping of management data models

4.3.001 Self-configuration capability

4.3.002 Enable peer configuration

4.3.003 Capability discovery

4.3.005 Network reconfiguration

4.3.006 Automatic reconfiguration of hierarchical networks

4.4.005 Network topology discovery

4.4.007 Neighbour-monitoring

4.4.008 Recovery

4.7.001 Management of energy resources

4.7.002 Support for layer 2 energy-aware protocols

- o IEEE 802.15.4 [IEEE-802.15.4] provides wireless low power communication on short distance.

4.7.003 Data models for energy management

4.7.004 Dying gasp

4.7.005 Support of energy-optimized communication protocols

- o 6LoWPAN [RFC4944] provides IPv6 functionality for IEEE 802.15.4 networks.

4.9.002 Redirect traffic

4.10.001 Scalable transport layer

4.10.002 Reliable unicast transport

4.10.003 Best-effort multicast

4.10.004 Secure message transport

4.11.001 Avoid complex application layer transactions requiring large application layer messages

4.11.002 Avoid reassembly of messages at multiple layers in the protocol stack

4. High level requirements that need to be observed continuously

4.1.001 Support multiple device classes within a single network

4.1.002 Management scalability

4.1.004 Minimise state maintained on constrained devices

4.1.007 Support for lossy and unreliable links

4.2.002 Compact encoding of management data

- o A binary format would be most compact.
- o TLV could be considered.
- o XML would be counter productive.
- o JSON may be counter productive.

4.2.003 Compression of management data or complete messages

- o When the messages are designed compact enough, compression will be unnecessary.

4.2.007 Protocol extensibility

5. Table of requirements and related technologies

The Table 1 summarises the requirements and related or possible candidate technologies.

Requirement number	Name	Associated technology
4.1.001	Support multiple device classes within a single network	[I-D.ietf-core-coap]
4.1.002	Management scalability	
4.1.003	Hierarchical management	
4.1.004	Minimise state maintained on constrained devices	[I-D.ietf-core-coap]
4.1.005	Support devices that are not always online	[I-D.rahman-core-sleepy], [I-D.shelby-core-resource-directory] ,[I-D.ietf-core-observe]
4.1.006	Automatic re-synchronisation with eventual consistency	
4.1.007	Support for lossy and unreliable links	[I-D.ietf-core-coap]
4.1.008	Network-wide configuration	[OMA-DM]
4.1.009	Distributed management	

4.2.001	Enabling modular implementations of management protocols with a basic set of protocol primitives	
4.2.002	Compact encoding of management data	[OMA-LwM2M-TS]
4.2.003	Compression of management data or complete messages	
4.2.004	Mapping of management protocol interactions	[I-D.ietf-core-coap]
4.2.005	Consistency of data models with the underlying information model	
4.2.006	Loss-less mapping of management data models	
4.2.007	Protocol extensibility	[I-D.ietf-core-coap]
4.3.001	Self-configuration capability	
4.3.002	Enable peer configuration	

4.3.003	Capability discovery	[RFC6690], [I-D.greevenbosch-core-profile-description], [I-D.shelby-core-resource-directory]
4.3.004	Asynchronous transaction support	[I-D.ietf-core-coap]
4.3.005	Network reconfiguration	
4.3.006	Automatic reconfiguration of hierarchical networks	
4.4.001	Device status monitoring	[OMA-LwM2M-TS]
4.4.002	Energy status monitoring	[OMA-LwM2M-TS]
4.4.003	Monitoring of current and estimated device availability	[OMA-DiagMon-MO]
4.4.004	Network status monitoring	[OMA-DiagMon-MO]
4.4.005	Network topology discovery	
4.4.006	Self-monitoring	[OMA-DiagMon-MO]
4.4.007	Neighbour-monit	[RFC6130]?

	oring	
4.4.008	Recovery	
4.4.009	Notifications	[OMA-DiagMon-MO]
4.4.010	Logging	[OMA-LwM2M-TS]

4.4.011	Performance monitoring	[OMA-DiagMon-MO]
4.4.012	Fault detection monitoring	[I-D.ietf-core-coap], [OMA-DiagMon-MO]
4.4.013	Passive monitoring	[OMA-DiagMon-MO]
4.4.014	Reactive monitoring	[OMA-DiagMon-MO]
4.5.001	Self-management	[OMA-DiagMon-MO]
4.5.002	Perodic self-management	[OMA-DiagMon-MO], [OMA-Scheduling-MO]
4.6.001	Security and access control	[OMA-LwM2M-TS], [I-D.ietf-tls-oob-pubkey], [I-D.greevenbosch-tls-ocsp-lite]
4.6.002	Authentication of managed devices	[OMA-LwM2M-TS], [I-D.ietf-tls-oob-pubkey], [I-D.greevenbosch-tls-ocsp-lite]
4.6.003	Access control on managed constrained devices	[OMA-LwM2M-TS], [OMA-DM]
4.6.004	Access control on management systems	[OMA-LwM2M-TS], [OMA-DM]

4.6.005	Support suitable security bootstrapping mechanisms	[OMA-LwM2M-TS], [OMA-DM], [I-D.jennings-core-transitive-trust-enrollment]
4.6.006	Enable the authentication of a large number of devices at system start	

4.6.007	Select cryptographic algorithms that are efficient in both code space and execution time	
4.6.008	Select cryptographic algorithms that are to be supported in hardware	
4.7.001	Management of energy resources	[IEEE-802.15.4], [I-D.rahman-core-sleepy],
4.7.002	Support for layer 2 energy-aware protocols	[IEEE-802.15.4]
4.7.003	Data models for energy	

	management		
4.7.004	Dying gasp		
4.7.005	Support of energy-optimize dcommunication protocols	[I-D.ietf-core-coap], [RFC4944], [I-D.rahman-core-sleepy], [I-D.ietf-core-observe], [I-D.shelby-core-resource-directory]	
4.8.001	Software distribution	[OMA-LwM2M-TS], [OMA-FUMO]	
4.8.002	Group-based provisioning	[I-D.ietf-core-groupcomm], [RFC4604]	
4.9.001	Congestion avoidance	[I-D.ietf-core-coap], [I-D.li-core-conditional-observe], [I-D.bormann-core-cocoa], [I-D.greevenbosch-core-minimum-request-interval]	

4.9.002	Redirect traffic		
4.9.003	Traffic delay schemes	[I-D.ietf-core-coap], [I-D.li-core-conditional-observe], [I-D.bormann-core-cocoa], [I-D.greevenbosch-core-minimum-request-interval]	
4.10.001	Scalable transport layer		
4.10.002	Reliable unicast transport		
4.10.003	Best-effort multicast		

4.10.004	Secure message transport	
4.11.001	Avoid complex application layer transactions requiring large application layer messages	
4.11.002	Avoid reassembly of messages at multiple layers in the protocol stack	

Table 1: Requirements and technologies

6. Conclusion and recommendations

In this document, we have identified possible technologies that can be used to realise the COMAN use cases. COMAN should reference relevant technologies where possible. In addition, this document points at technologies that are missing, and hence need standardisation. We recommend to do this standardisation in COMAN, and in addition write a document in COMAN that describes the overall system.

7. Security Considerations

TBD

8. IANA considerations

TBD

9. Acknowledgements

TBD.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

10.2. Informative References

[RFC4604] Holbrook, H., Cain, B., and B. Haberman, "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast", RFC 4604, August 2006.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.

[RFC6130] Clausen, T., Dearlove, C., and J. Dean, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 6130, April 2011.

[RFC6690] Shelby, Z., "Constrained RESTful Environments (CoRE) Link Format", RFC 6690, August 2012.

[I-D.ietf-core-coap] Shelby, Z., Hartke, K., Bormann, C., and B. Frank, "Constrained Application Protocol (CoAP)", draft-ietf-core-coap-10 (work in progress), March 2012.

[I-D.ietf-core-groupcomm] Rahman, A. and E. Dijk, "Group Communication for CoAP", draft-ietf-core-groupcomm-04 (work in progress, December 2012.

[I-D.ietf-core-observe]
Hartke, K., "Observing Resources in CoAP", draft-ietf-core-observe-07 (work in progress, October 2012.

[I-D.ietf-tls-oob-pubkey]
Wouters, P., Tschofenig, H., Gilmore, J., Weiler, S., and T. Kivinen, "Out-of-Band Public Key Validation for Transport Layer Security (TLS)", draft-ietf-tls-oob-pubkey-06 (work in progress), October 2012.

[I-D.bormann-core-cocoa]

Bormann, C., "CoAP Simple Congestion Control/Advanced", draft-bormann-core-cocoa-00 (work in progress), Augustus 2012.

[I-D.ersue-constrained-mgmt]
Ersue, M., Romascanu, D., and J. Schoenwaelder, "Management of Networks with Constrained Devices: Uses Cases and Requirements", draft-ersue-constrained-mgmt-02 (work in progress), October 2012.

[I-D.greevenbosch-core-minimum-request-interval]
Greevenbosch, B., "CoAP Minimum Request Interval", draft-greevenbosch-core-minimum-request-interval-00 (work in progress), September 2012.

[I-D.greevenbosch-core-profile-description]
Greevenbosch, B., Hoebeke, J., and I. Ishaq, "CoAP profile description format", draft-greevenbosch-core-profile-description-01 (work in progress), October 2012.

[I-D.greevenbosch-tls-ocsp-lite]
Greevenbosch, B., "OCSP-lite - Revocation of raw public keys", draft-greevenbosch-tls-ocsp-lite-00 (work in progress), December 2012.

[I-D.jennings-core-transitive-trust-enrollment]

Jennings, C., "Transitive Trust Enrollment for Constrained Devices", draft-jennings-core-transitive-trust-enrollment-01 (work in progress), October 2012.

[I-D.li-core-conditional-observe]
Li, S., Hoebeke, J., and A. Jara, "Conditional observe in CoAP", draft-li-core-conditional-observe-03 (work in progress), October 2012.

[I-D.rahman-core-sleepy]
Rahman, A., "Enhanced Sleepy Node Support for CoAP", draft-rahman-core-sleepy-01 (work in progress), October 2012.

[I-D.shelby-core-resource-directory]
Shelby, Z., Krco, S., and C. Bormann, "CoRE Resource Directory", draft-shelby-core-resource-directory-04 (work in progress), July 2012.

[IEEE-802.15.4]
IEEE Computer Society, "IEEE std. 802.15.4-2003", October 2003.

[OMA-DM] "OMA Device Management 1.3", OMA-ERP-DM-V1_3-20121213-C , December 2012.

[OMA-DiagMon-MO]
"OMA Diagnostics and Monitoring Management Object", OMA-ERP-DiagMon-V1_0-20120313-A , March 2012.

[OMA-FUMO]
"Firmware Update Management Object", OMA-TS-DM-FUMO-V1_0-20070209-A , February 2007.

[OMA-Scheduling-MO]
"OMA DM Scheduling Management Object", OMA-ERP-DM_Scheduling-V1_0-20110614-C , June 2011.

[OMA-LwM2M-TS]
"OMA Lightweight M2M", OMA-TS-LightweightM2M-V1_0-

20130123-D (work in progress), January 2013.

Authors' Addresses

Bert Greevenbosch
Huawei Technologies Co., Ltd.
Huawei Industrial Base
Bantian, Longgang District
Shenzhen 518129
P.R. China

Phone: +86-755-28979133
Email: bert.greevenbosch@huawei.com

Kepeng Li

Huawei Technologies Co., Ltd.
Huawei Industrial Base
Bantian, Longgang District
Shenzhen 518129
P.R. China

Phone: +86-755-28971807
Email: likepeng@huawei.com