CoRE
Internet-Draft
Intended status: Informational
Expires: April 15, 2013

L. Wang
W. Wang
BUPT
L. Zhu
F. Yu
Huawei Technologies
October 12, 2012

CoAP Option Extensions: Profile and Sec-flag
draft-wang-core-profile-secflag-options-02

Abstract

This memo adds two Options for the Constrained Application Protocol (CoAP): Profile and Sec-flag. The Profile Option is indicating the identification of an application using CoAP. The Sec-flag Option complements the security considerations of CoAP.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 15, 2013.

Table of Contents

1. Introduction

CoAP is a specialized web transfer protocol for machine-to-machine applications such as smart energy and building automation using with constrained nodes and networks. This memo adds two new options for CoAP: Profile and Sec-flag.

The main purpose of the Profile Option is indicating the identification of an application using CoAP, by reading this option some intermediaries (e.g. proxy) and transport networks could distinguish different applications and do some differentiated processing.

The Sec-flag Option complements the security considerations, enabling NoSec pattern in a segment of the communication path between the client and server, by taking care of establishing and maintaining lower layer security instead of DTLS in these intermediate networks.

1.1. Terminology

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. Motivations

CoAP is a light-weight web protocol and can be used in constrained devices, fulfilling machine-to-machine requirements. Because of its features, more and more M2M applications MAY adopt CoAP.

2.1. Profile Option Extension

CoAP applications SHOULD use an operator's network as the transport bearer. Different machine-to-machine applications MAY have different Quality of Service (QoS) requirements in terms of required bit rates

as well as acceptable packet delays and packet loss rates. When application data is transmitted through the transport network, the network MAY need to identify different machine-to-machine services to do some differentiated processing, applying different control policies with subscriptions. Before applying control policies to applications, transport networks SHOULD identify them and distinguish each one from another referring to application identification, and then networks MAY apply different policies to different applications. Some intermediaries (e.g.CoAP proxy) MAY also would like to distinguish different applications and do some differentiated processing such as caching and forwarding application data in different priorities.

This memo describes the extensions to CoAP and is to provide expanding proposal(s) to fulfill the motivations and requirements, defining an additional Option for the Constrained Application Protocol (CoAP): Profile. The Profile Option is defined as the identification of CoAP applications. When CoAP messages are transmitted through the transport network, network entities MAY use some technologies to read the Option Value to identify the application, and then apply control policies with the subscription of application owner.

2.2. Sec-flag Option Extension

The transmission path between the client and server MAY consist of some segments: Network domain based on existing standards 3GPP, TISPAN, IETF, etc., and M2M Device and Gateway Domain based on existing standards and technologies like DLMS, CEN, CENELEC,PLT, Zigbee, M-BUS, KNX, etc. The application data MAY be transmitted through different networks between the client and server.

The basic CoAP protocol defines the DTLS binding. DTLS would add a per-datagram overhead and some initialization vectors. For some constrained networks and nodes, this is really expensive. And intermediate network domain MAY have some independent and reliable security standards (e.g. ZigBee standard). In some cases, CoAP could use these security standards instead of DTLS to avoid DTLS overhead in some intermediate networks.In these network domains DTLS may be disabled but be retained in other domains.

As an example, the ZigBee standard for sensor networks defines a

security architecture based on an online trust center and uses CCM* model to secure applications. This standard can fulfill the security requirements of CoAP. That is to say, CoAP applications could be secured by lower layer security, so in this network DTLS could be disabled to avoid DTLS datagram overhead. We just mark a security flag to indicate that CoAP data is secured by lower layer instead in this network domain and the overhead would be much less. And in the Transport Network domain we still establish DTLS security. Thus we MAY enable two different security patterns described in [I-D.ietf-core-coap] in different segments between the client and server.

The Sec-flag Option can be used to indicate the security information and ensure the integrality of the security mechanism.

3. Profile Option

3.1. Profile Option Definition

No.	C/E	Name	Format	Length	Default
2n	Elective	Profile	(see below)	4B	(none)

The Profile Option indicates the identification of CoAP applications. Transport network entities MAY use some technologies to read the Option Value and then apply corresponding treatment.

This option is "elective" and the Option Number is even. It MUST NOT occur more than once.

The detailed definitions and encoding SHOULD refer to the description of Option Format in [I-D.ietf-core-coap]. It is RECOMMENDED that the Option Value consists of Enterprise Number, Application ID and Priority.

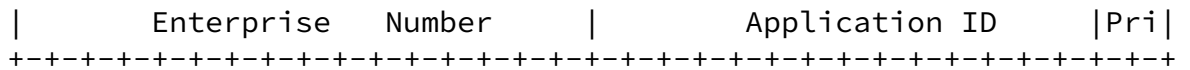

Figure 1: Option Value Format

As shown in Figure 1, Enterprise Number is the register number of application owners (e.g. traffic management agencies) in network operators. Application ID is the identification of the owner's application which subscribes transport and communication services from operators. Priority (Pri) indicates the priority of application data, data of the same application MAY has different priority (For some cost reasons, application owners MAY subscribe low priority for some application data).

The SDNV[RFC5050] encoding can be used.

We can distinguish different applications with a combination of Enterprise Number, Application ID and Priority.

3.1.1. Option Value Length

In actual usages, the number of CoAP application owners MAY be out of length range indicated by 2 bytes, the default length cannot fulfill requirements. Hence, we can define another Option Value Length: 5bytes.

In the initialization phase of CoAP message, the Option Value Length SHOULD be determined.

3.2. Using the Profile Option

The semantics of Option Value are defined by prior agreement between the application owners and network operators. Some encryption algorithms MAY be used. Network entities MAY also apply some validation policies when reading the Option Value.

CoAP application owners MAY realize functions through a M2M communication for some purposes (e.g. Meter readings) at their customer's premises. The Profile Option can be contained in the application message to indicate the identity.

When CoAP messages across transport network, network entities MAY use some technologies such as Deep Packet Inspection (DPI) to read the Profile Option Value and report it to policy control decision function entities. And then policy control decision function entities determine the policies applied to CoAP data as well as establishing dedicated bearers.

3.3. Example

In some M2M environments, the nodes access to Internet through 3GPP network.

This example (Figure 2) shows that mobile network is the bearer between two M2M end-points. These end-points MAY belong to an electric power company and this M2M application is a meter reading service. The profile option value of this application is 0x12111111.

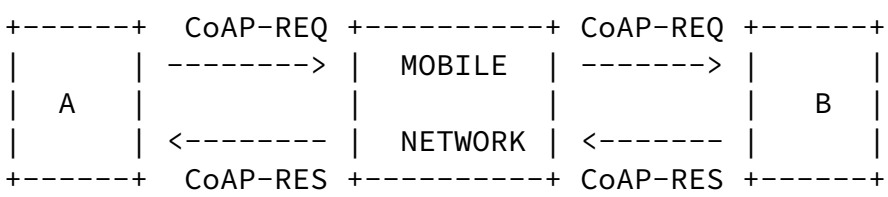

Figure 2 An example

The message flow is shown in Figure 3. At first the requester (server) sends a request which MAY be a device trigger that makes end devices return electricity records. The number of end devices is numerous and this triggering MAY happen in a preset period of time. All devices return their records at the approximately same time, and the data transmission volume is huge. Hence it is expected that the network SHOULD offer QoS guarantee (such as high bandwidth and

throughput) for the M2M application.

The requester SHOULD initial the Profile Option when sending a request. Network entities can read the Option Value and know that the application is a meter reading service belonging to a certain electricity company. And then specialized policies MUST be applied. The Profile option value MUST be echoed in the messages from recipients.

When the M2M application data comes into the network, network entities MUST provide corresponding policy control with subscriptions and MAY also establish dedicated bearers assign dedicated network resources to ensure the quality of transport and communication if necessary.

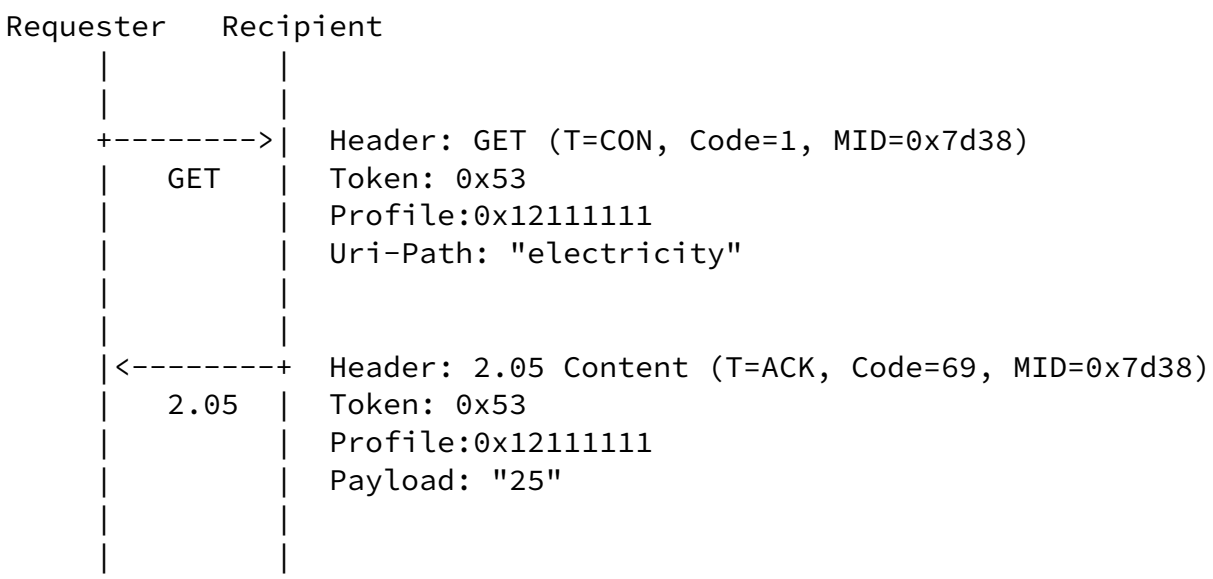

Figure 3 Profile Option in CoAP messages

4. Sec-flag Option

The Sec-flag Option complements the security considerations, enabling NoSec pattern in one or more segments of the communication path between the client and server.

4.1. Security Negotiation

Before establishing a security session between endpoints, the negotiation SHOULD be made. As shown in Figure 4, the basic model includes three actors: a client, a proxy and a server.

Client Proxy Server

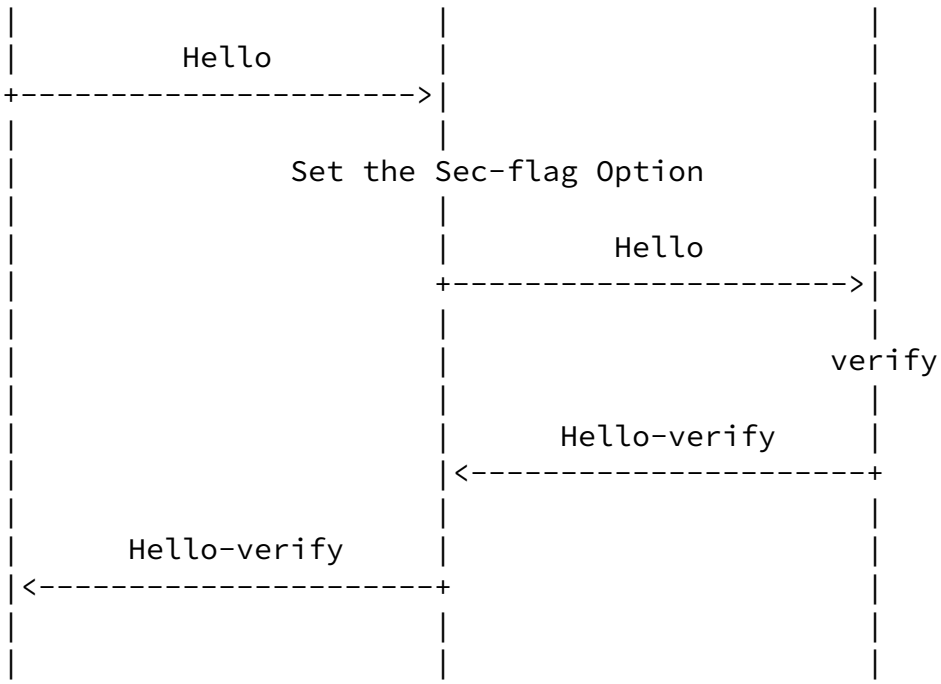

Figure 4 Basic model

(1) Lower security can secure CoAP application data

At first, the client sends to the server a hello message in which the Sec-flag Option with an empty value is included. The proxy is requested to forward the request or serve it, and return the response. If the network domain between the client and proxy could guarantee the lower layer security, the proxy SHOULD set the Sec-flag Option with a valid value and transfer the hello message to the server.

When the server receives the message, it MUST respond with a server hello-verify message. A response with the same valid option value as the value set in the proxy SHOULD be returned only if the server trusts the lower layer security between the client and proxy. If the server accepts the lower layer security, DTLS would be disabled between the client and proxy and then the proxy SHOULD make a DTLS handshake with the server to make up a DTLS security session. Otherwise, the DTLS handshake SHOULD be made between the client and server, that would be introduced in the following.

(2) Lower security cannot secure CoAP application data

When the server receives the Hello message, if the server does not trust the lower layer security between the client and proxy, the server would respond a hello-verify message containing an empty

Security option and an error code. Then the client would send DTLS handshake messages to the server and establish DTLS between the client and the server.

(3) There is no lower security between the client and M2M Gateway

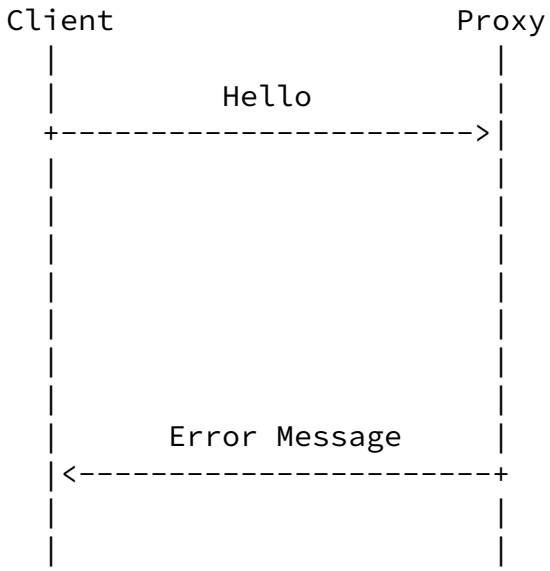

Figure 5 There is no lower security in the Device and Gateway Domain

If the network domain between the client and proxy could not guarantee lower layer security, the proxy SHOULD return an appropriate error response code with an empty Security Option as shown in Figure 5. Then the client would send DTLS handshake messages to the server and establish DTLS between the client and the server.

In all the situations, the client and the proxy also need initialize lower security mechanism, which MAY happen either before the Security Option negotiation or after it.

4.2. Using the Sec-flag Option in data transport

When the security negotiation is completed, a security session is established between the client and server.

The Sec-flag Option MUST be included in messages sent by the client and the value SHOULD be empty. When the proxy receives the message, it MUST set the Sec-flag Option with a valid value and transfer the message to the server. The Sec-flag Option indicates that the message comes from a reliable network domain and the server could

trust it. And then the server would respond the request. The same Sec-flag Option SHOULD be echoed in the response. When the response

comes to the proxy, the proxy reads the option and knows that the message SHOULD be secured by lower layer security.

4.3. Sec-flag Option Definition

No.	C/E	Name	Format	Length	Default
2n+1	Critical	Sec-flag	(see below)	1B	(empty)

The Sec-flag Option is used for indicating the lower layer security.

This option is "critical" and the Option Number is odd.

The detailed definitions and encoding SHOULD refer to the description of Option Format in [I-D.ietf-core-coap]. The value is made up of security indication.

The SDNV[RFC5050] encoding can be used.

4.4. System Overview

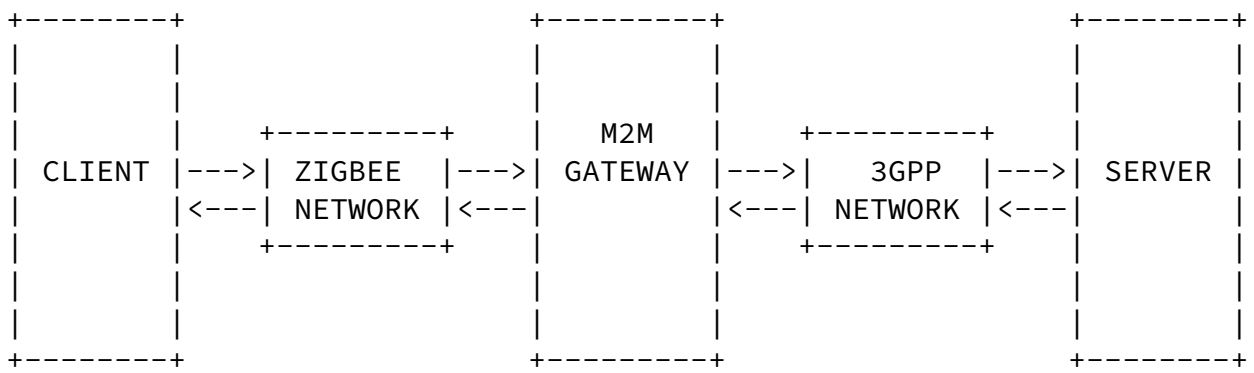

Figure 6 System overview of a usage scenario

As shown in Figure 6, the nodes access to Internet through 3GPP

network. DTLS is enabled between M2M Gateway and application server, and in Zigbee network DTLS is disabled and lower layer security secures CoAP applications. M2M Gateway, working as a "marker", sets the Sec-flag option to show that the data from Zigbee network domain is secured and reliable in the uplink and indicate that the data need low layer security and DTLS SHOULD be disabled in the Zigbee network domain in the downlink. As the intermediate gateway, M2M Gateway needs to transfer the data to each network and adapt the security standard to the other one. M2M Gateway also needs to check the

message. When a message from the end devices is received, the gateway checks whether the Sec-flag option is set by the end devices illegally (the default value SHOULD be empty). If the Sec-flag option is not empty, the gateway SHOULD drop it, else the gateway SHOULD set the valid value and transfer the message.

5. Security Considerations

To be defined.

6. IANA Considerations

The following entries are added to the CoAP Option Numbers registry:

Number	Name	Reference
2n	Profile	RFC XXXX
2n+1	Sec-flag	RFC XXXX

7. References

7.1. Normative Reference

[I-D.ietf-core-coap]
Shelby, Z., Hartke, K., Bormann, C., and B. Frank,

"Constrained Application Protocol (CoAP)", draft-ietf-core-coap-12 (work in progress), October 2012.

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

[RFC5050] Scott, K. and S. Burleigh, "Bundle Protocol Specification", RFC 5050, November 2007.

7.2. Informative References

[I-D.fossati-core-publish-monitor-options] Fossati, T., Giacomin, P., and S. Loreto, "Publish and Monitor Options for CoAP", draft-fossati-core-publish-monitor-options-01 (work in progress), March 2012.

Authors' Addresses

Lei Wang
Beijing University of Posts and Telecommunications
Xitucheng road 10
Haidian District, Beijing 100876
P. R. China

Email: wleiblue@163.com

Wendong Wang
Beijing University of Posts and Telecommunications
Xitucheng road 10
Haidian District, Beijing 100876
P. R. China

Email: wdwang@bupt.edu.cn

Lei Zhu
Huawei Technologies
Huawei Building, Q20 No.156 Beiqing Rd.Z-park
Haidian District, Beijing 100095
P. R. China

Email: lei.zhu@huawei.com

Fang Yu
Huawei Technologies
Huawei Building, Q20 No.156 Beiqing Rd.Z-park
Haidian District, Beijing 100095
P. R. China

Email: grace.yufang@huawei.com