Managing IoT Devices with LwM2M

Jaime Jiménez
jaime.jimenez@ericsson.com
Ericsson
Jorvas, Finland

ABSTRACT

In this paper we provide an overview of the Lightweight Machine-to-Machine (LwM2M) protocol, a standard device and service management protocol built on top of CoAP for remote management and configuration of devices. We highlight its role in IoT device management and its use of key IETF standards such as CoAP, DTLS,and OSCORE. While network management protocols like SNMP, RESTCONF, and CORECONF focus on monitoring and configuring endpoints within the network, LwM2M extends these capabilities by managing the entire lifecycle of individual devices, including configuration, control, and maintenance. We also discuss LwM2M's architecture, data model and communication interfaces. Last, we also introduce recent advancements in the protocol.

KEYWORDS

Internet of Things, IoT, network management, device management, security, standards

IAB Next Era of Network Management Operations Workshop, December 2024, held online
.

Reference:

Jaime Jiménez. 2024. Managing IoT Devices with LwM2M. In *submissions to the IAB Next Era of Network Management Workshop*, 6 pages.

1 INTRODUCTION

The rapid evolution of network management protocols necessitates a reevaluation of existing technologies and their applicability to modern challenges. The Lightweight Machine-to-Machine (LwM2M) protocol [2], developed by the Open Mobile Alliance (OMA), is a key player in this domain, offering a standardized framework for managing Internet of Things (IoT) devices [1]. This paper explores the role of LwM2M in the context of the IAB workshop on the Next Era of Network Management Operations, focusing on its current deployments, challenges, and future potential.

The IAB "NEMOPS" workshop seeks contributions that critically assess the progress made since the 2002 IAB workshop, particularly in terms of network management protocols. This paper aims to present LwM2M, an management protocol that addresses the needs for managing IoT endpoints from the operational point of view of device and network management.

Our contribution is informed by the authors' extensive experience with IoT and contributions in the IoT domain both at IETF and in OMA. The rest of the document is organized as follows: The Introduction outlines LwM2M as a standardized framework for managing IoT devices, addressing current network management challenges. The LwM2M Protocol Overview details its architecture, focusing on communication between Clients, Servers, and Bootstrap Servers (see Figure 1). Recent advancements, including integrations with blockchain and industrial protocols, are discussed in LwM2M Extensions, the Conclusions summarize the main points of the paper.

LwM2M and IETF

The IETF has played a fundamental role in shaping the protocols that underpin LwM2M. IETF efforts have focused on adapting existing Internet and Web protocols to meet the needs of resource-constrained IoT devices [20].

LwM2M is built upon several key IETF standards. At the core is the *Constrained Application Protocol (CoAP)* [29], a lightweight RESTful protocol designed for constrained environments, providing the fundamental request/response model for LwM2M communications. *RFC 7959* [7] defines block-wise transfers in CoAP, allowing LwM2M to efficiently handle large payloads by breaking them into smaller blocks. The *LwM2M* protocol also leverages *RFC 7641* [14] for resource observation, enabling clients to subscribe to changes of resource state without continuous polling. For secure communications, LwM2M often relies on the *Datagram Transport Layer Security (DTLS)* as outlined in *RFC 6347* [26], ensuring encryption and integrity over the CoAP protocol. An alternative layer of security is provided by *Object Security for Constrained RESTful Environments (OSCORE)* [27], which offers end-to-end encryption and integrity protection directly at the application layer, making it suitable for scenarios where DTLS is not applicable. Lastly the *Constrained RESTful Environments (CoRE) Resource Directory (RD)* [4] facilitates resource registration of IoT endpoints. It does so by maintaining information about resources on other servers, the lookup interface, although present is not intended for applications but solely for management purposes.

LwM2M also supports additional transport protocols, such as IETF's *Hypertext Transfer Protocol (HTTP)*[12] and OASIS' *Message Queuing Telemetry Transport (MQTT)*[23], expanding its applicability across diverse network environments and use cases.

2 LWM2M PROTOCOL OVERVIEW

This section presents an overview of the LwM2M protocol, emphasizing its participating entities, data model, and communication interfaces.

Participating Entities

The LwM2M protocol defines three primary entities that form the backbone of its communication architecture:

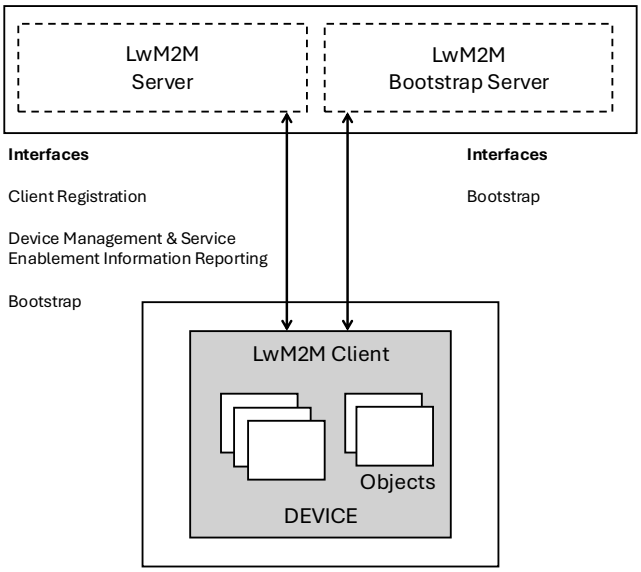

Figure 1: General LwM2M Architecture

- **LwM2M Client**: Typically a smart device, such as a light, smart meter, switch, or gateway, responsible for data collection and resource management at the device level. The client oversees the lifecycle of various objects residing in it and communicates with servers to transmit data and receive management instructions.
- **LwM2M Server**: Often referred to as the manager, this server manages multiple clients, aggregates their data, and issues configuration or maintenance commands. It is essential for controlling and coordinating client devices within an IoT ecosystem.
- **LwM2M Bootstrap Server**: This entity is responsible for the initial configuration of the LwM2M Client. Unlike other protocols, LwM2M includes a Bootstrap Server to streamline device setup, particularly when multiple servers are involved. During the bootstrap process, it provides the client with configuration details, such as security credentials and connection information, which can be pre-integrated into the device's software or dynamically supplied by the Bootstrap Server.

The introduction of the Bootstrap Server differentiates LwM2M from other IoT protocols. Before the client can

establish a connection to a server, it undergoes the bootstrap procedure to load initial configurations and key material. This feature is particularly advantageous in scenarios with multiple servers or when load balancing is required, as it allows for flexible and dynamic configuration.

LwM2M Data Model

The LwM2M protocol employs a structured, object-based data model to facilitate communication between clients and servers. In this model, each data entity is defined as an object, uniquely identified by an integer ID, as specified by the Open Mobile Alliance (OMA). These objects can represent various resources, such as sensors, actuators, or configuration settings.

Each object consists of multiple resources, which serve as the fundamental data points within the object. Resources are assigned integer IDs and are classified as either mandatory or optional, depending on the object's intended function being the mandatory ones used for interoperability purposes. An object can also have multiple instances, each with a unique instance ID, allowing for flexibility. For instance, a device with several sensors can represent each sensor as an instance of the same object, such as in a network of connected lightbulbs.

The LwM2M data model enables servers to access individual resources, instances, or entire objects using well-defined URI strings. The URI template approach follows the Web Linking and the IETF CoRE Link Format [28]. The format is as follows:

$$/< ObjectID > /< InstanceID > /< ResourceID >$$

In this structure, the instance or resource ID can be omitted if the request targets the entire object or a specific instance. This model provides a straightforward way to interact with data at different levels of granularity.

All objects are listed in the LwM2M Registry [25], categorized as either application-oriented (e.g., thermostats, lamps) or system-oriented (e.g., security, connectivity). Those for applications follow the same schema and come from the IP for Smart Objects (IPSO) [15] consortium which was integrated into OMA.

Communication Interfaces

LwM2M defines four primary communication interfaces that facilitate interactions between clients and servers, each serving distinct roles in the protocol's operation:

- **Bootstrap Interface**: This interface facilitates the initial setup by enabling the client to obtain necessary configurations and security credentials from the Bootstrap Server prior to connecting with an LwM2M Server. The process can be either automated or client-initiated.
- **Registration Interface**: After the bootstrap procedure, the client registers with the LwM2M Server through the Registration Interface. During registration, the client provides its endpoint name whcih together with the security credentials is used as identifier. To maintain its registration status, the client must periodically send updates. If these updates are not received within the agreed time, the client is considered de-registered and must re-initiate the registration process.
- **Device Management and Service Enablement Interface**: Once registered, the server can use this interface to perform various management tasks, such as reading and writing data or executing commands on the client. It allows the server to control the client's resources, adjusting settings or triggering actions as required.
- **Information Reporting Interface**: This interface enables the client to report changes in its status or resource values to the server, using the Observe function. The server can set up observation requests, prompting the client to notify it when certain resource values change or when predefined conditions are met. This capability is particularly useful for monitoring dynamic IoT environments where timely updates are crucial. LwM2M defines specific attributes to configure how frequently these notifications occur.

LwM2M has been integrated on most IoT OSs like FreeRTOS [13], Mbed [19], RIOT OS [6], Contiki-NG [9], and many others, with a strong focus on IoT device security [11].

LwM2M has also proven to be a preferred solution for managing cellular IoT (CIoT) devices [10] due to its low overhead and comprehensive management capabilities, particularly in environments where network efficiency, scalability, and efficient firmware updates are critical [32].

3 LWM2M EVOLUTION

LwM2M, though robust in its core functionalities, has advanced through various extensions and integrations. This section explores a subset of recent research developments that may inspire the future evolution of the standard.

Firstly, LwM2M has developed a Northbound Web API to simplify interaction with LwM2M systems by abstracting the protocol's complexities [3]. This API enables external applications to perform key operations such as tracking device registrations, executing management commands (e.g., read, write, delete), and subscribing to observations for real-time monitoring of device resources.

Outside OMA, several studies have concentrated on enhancing IoT security through the use of LwM2M. For instance, Muhammad et al. [21] investigated the use of ARIA cryptography within Hardware Secure Modules for both LwM2M and MQTT protocols. Similarly, Lanzieri et al. [18] proposed extensions to the LwM2M core specification to facilitate secure and authorized client-to-client communication, which is a limitation of the current standard.

Others have focused on interoperability between SDOs, Kim et al. [17] have designed and implemented a blockchain-based system that enables interworking between oneM2M [24] and LwM2M IoT systems. Their approach uses blockchain's immutable and distributed ledger properties for interoperability and security.

In the context of Industrial IoT (IIoT), Yaker et al. [31] introduced a novel edge Security Information and Event Management (SIEM) system for managing IoT flows within 5G private networks. Their approach incorporates LwM2M data events to manage and secure IoT data in a 5G environment. Similarly, Myoung et al. [22] addressed the integration of LwM2M with smart metering technologies, proposing a data interworking model between the Device Language Message Specification (DLMS) [5] used for managing smart meters and the LwM2M protocol.

Further efforts have been made to integrate LwM2M with industrial communication protocols. Karaagac et al. [16] explored the interoperability between LwM2M and the Open Platform Communications Unified Architecture (OPC UA), proposing a framework where OPC UA Servers can be virtualized as LwM2M Clients and vice versa. Similarly, Cavalcanti et al. [8] reviewed various machine-to-machine communication protocols within the context of Industry 4.0. A third example is based only on CoAP, Wang et al. [30], which proposed a CoAP-based OPC UA transmission scheme tailored for resource-constrained devices. These three papers aim to bridge the gap between IoT and industrial automation.

The evolution of LwM2M has also prompted considerations for enhancing its data model capabilities. While the current IPSO data model, utilizing the format */<ObjectID>/<InstanceID>/<ResourceID>*, is well-suited for constrained environments, it may fall short in addressing the needs of complex machines or network nodes with large, deeply nested configuration structures. This limitation suggests the potential for developing alternative data models that can accommodate more intricate configurations, thereby extending the LwM2M protocol's applicability to a broader range of devices.

The interoperability of LwM2M with hyperscalers is hindered by the lack of native CoAP support within these platforms. This limitation poses a challenge for vendors seeking to integrate LwM2M-based IoT solutions with HCS services. To overcome this obstacle, some vendors have devised methods to encapsulate CoAP messages within MQTT topics, although this solution is merely a workaround that may not fully address the efficiency needs of large-scale IoT deployments.

4 CONCLUSIONS

This paper provides an overview of the LwM2M protocol, detailing its core components, architecture, and integration with IETF standards. We explored its role in managing IoT devices, including its communication interfaces and data model, and discussed its adaptability through recent extensions. LwM2M continues to evolve as a key solution for IoT device management, offering scalability, security, and efficient operation, especially in constrained environments like Cellular IoT (CIoT). Future developments in interoperability and security enhancements will further strengthen its utility across diverse IoT applications.

5 ACKNOWLEDGMENTS

We would like to thank Ericsson for their support of this work. Special thanks to Jari Arkko, Carsten Bormann and Sándor Katona for their valuable review and feedback, which improved the quality of this paper.

REFERENCES

[1] Open Mobile Alliance. 2023. *Open Mobile Alliance Standards Development Organization.* https://omaspecworks.org/ Accessed: 2024-10-16.

[2] Open Mobile Alliance. 2024. *Lightweight Machine to Machine Technical Specification.* https://lwm2m.openmobilealliance.org/

[3] Open Mobile Alliance. 2024. LwM2M Northbound API. https://github.com/OpenMobileAlliance/lwm2m-northbound-api. Accessed: 2024-10-16.

[4] C. Amsüss, Z. Shelby, M. Koster, C. Bormann, and P. van der Stok. 2022. Constrained RESTful Environments (CoRE) Resource Directory. RFC 9176. https://datatracker.ietf.org/doc/html/rfc9176 Standards Track.

[5] DLMS User Association. 2020. *DLMS/COSEM: The Global Standard for Smart Metering and Energy Management.* DLMS User Association, Geneva, Switzerland. https://www.dlms.com/.

[6] Emmanuel Baccelli, Oliver Hahm, Mesut Gunes, Matthias Wahlisch, and Thomas C. Schmidt. 2015. RIOT OS: Towards an OS for the Internet of Things. *Proc. IEEE* 103, 4 (2015), 1–14.

[7] C. Bormann and Z. Shelby. 2016. Block-Wise Transfers in the Constrained Application Protocol (CoAP). https://www.rfc-editor.org/rfc/rfc7959.html

[8] Marcella Cavalcanti, Hugo Costelha, and Carlos Neves. 2023. Industry 4.0 Machine-to-Machine Communication Protocols and Architectures on the Shop Floor. (2023), 222–234.

[9] Adam Dunkels, Bjorn Gronvall, and Thiemo Voigt. 2004. Contiki - a Lightweight and Flexible Operating System for Tiny Networked Sensors. *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks* (2004), 455–462.

[10] Radim Dvorak, Lukas Jabloncik, Michal Mikulasek, Martin Stusek, Pavel Masek, Radek Mozny, Aleksandr Ometov, Petr Mlynek, Petr Cika, and Jiri Hosek. 2023. LWM2M for Cellular IoT: Protocol Implementation and Performance Evaluation. In *2023 15th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT).* 212–218. https://doi.org/10.1109/ICUMT61075.2023.10333286

[11] J Ellamathy. 2023. *Securing LwM2M with Mbed TLS in Contiki-NG.* diva-portal.org. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1751815 Query date: 2024-10-08 22:53:23.

[12] R. Fielding and J. Reschke. 2014. Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing. https://doi.org/10.17487/RFC7230

[13] FreeRTOS Community. 2023. FreeRTOS: Real-Time Operating System for Microcontrollers. https://www.freertos.org/. Accessed: 2024-10-16.

[14] K. Hartke. 2015. Observing Resources in the Constrained Application Protocol (CoAP). https://www.rfc-editor.org/rfc/rfc7641.html

[15] J. Jimenez, M. Koster, and H. Tschofenig. 2016. IPSO Smart Objects. Position paper for the IOT Semantic Interoperability Workshop. https://www.ietf.org/ietf-ftp/slides/slides-iotsiws-ipso-smart-objects-00.pdf Accessed: 2024-10-16.

[16] Abdulkadir Karaagac, Niels Verbeeck, and Jeroen Hoebeke. 2019. The Integration of LwM2M and OPC UA: An Interoperability Approach for Industrial IoT. (2019), 313–318. https://doi.org/10.1109/WF-IoT.2019.8767209

[17] Donggyu Kim, Uk Jo, Yohan Kim, Yustus Eko Eko, and Howon Kim. 2023. Design and implementation of a blockchain based interworking of oneM2M and LWM2M IoT systems. *Journal of Information Processing Systems* 19, 1 (2023), 89–97.

[18] Leandro Lanzieri, Peter Kietzmann, Thomas C. Schmidt, and Matthias Wählisch. 2022. Secure and Authorized Client-to-Client Communication for LwM2M. (2022), 158–170. https://doi.org/10.1109/IPSN54338.2022.00020

[19] Arm Ltd. n.d.. *Mbed OS.* https://os.mbed.com/ Accessed: 2024-10-16.

[20] Roberto Morabito and Jaime Jimenez. 2020. IETF Protocol Suite for the Internet of Things: Overview and Recent Advancements. *IEEE Communications Standards Magazine* 4, 2 (2020), 41–49. https://doi.org/10.1109/MCOMSTD.001.1900014

[21] I Muhammad, LAM Ari, and D Pratama. 2024. Next-Gen IoT Security: ARIA Cryptography within Hardware Secure Modules—A Comparative Analysis of MQTT and LwM2M Integration. *Proceedings of the Korea Society for Internet Information* (2024). https://koreascience.kr/article/CFKO202422572150314.page Query date: 2024-10-08.

[22] Nogil Myoung, Yoojin Kwon, Myunghye Park, and Changsoo Eun. 2023. Data Interworking Model and Analysis for Harmonization of Smart Metering Protocols in IoT-Based AMI System. *Sensors* 23, 6 (2023). https://doi.org/10.3390/s23062903

[23] OASIS. 2014. MQTT Version 3.1.1. https://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html

[24] oneM2M. 2023. oneM2M Technical Specification. https://www.onem2m.org/technical/onem2m-specifications.

[25] Open Mobile Alliance. [n. d.]. LwM2M Registry. https://github.com/OpenMobileAlliance/lwm2m-registry.

[26] E. Rescorla and N. Modadugu. 2012. Datagram Transport Layer Security Version 1.2. https://www.rfc-editor.org/rfc/rfc6347.html

[27] J. Selander, D. Palombini, F. Armknecht, G. Selander, and L. Seitz. 2019. Object Security for Constrained RESTful Environments (OSCORE). https://doi.org/10.17487/RFC8613

[28] Zach Shelby. 2012. Constrained RESTful Environments (CoRE) Link Format. RFC 6690. https://datatracker.ietf.org/doc/html/rfc6690

[29] Z. Shelby, K. Hartke, and C. Bormann. 2014. The Constrained Application Protocol (CoAP). https://www.rfc-editor.org/rfc/rfc7252.html

[30] Yi Wang, Chenggen Pu, Ping Wang, and Junrui Wu. 2020. A CoAP-based OPC UA Transmission Scheme for Resource-Constrained Devices. (2020), 6089–6093. https://doi.org/10.

1109/CAC51589.2020.9326995

[31] K Yaker, BA Salem, B Pierard, et al. 2024. A Novel EDGE SIEM for Industrial IoT Flows Within 5G Private Networks. *2024 Global ...* (2024). https://ieeexplore.ieee.org/abstract/document/10449912/ Query date: 2024-10-08 22:53:23.

[32] Koen Zandberg, Kaspar Schleiser, Francisco Acosta, Hannes Tschofenig, and Emmanuel Baccelli. 2019. Secure Firmware Updates for Constrained IoT Devices Using Open Standards: A Reality Check. *IEEE Access* 7 (2019), 71907–71920. https://doi.org/10.1109/ACCESS.2019.2919760