Problem and possible approach of development and operation of Smart Objects

Shoichi Sakane
sakane@tanu.org

Abstract. This paper gives problems that would happen when the protocol stack for the Smart Objects is developed, and also gives some possible approaches.

1. Introduction

Smart Objects have the different feature from the node that has been used in the Internet. The smart objects have typically limited resource and constraints. For example, the power consumption is highly considerable, and the physical size of the device is typically very small. Furthermore, the characteristics of the network where the objects work are also unique, for example, the link is sometimes unstable, lossy, and the bandwidth is typically very low. There are four major areas to be solved in order to use the IP technology in the smart objects. 1) Adaptation layer for new medias. 2) Low power and resource consideration. 3) Resilient routing protocol. 4) Comprehensive and simple application protocol.

In five or six recent years, several new protocols are being standardized in each working group of IETF in order that the objects will work on it properly. However, no working group considers how to implement each protocol into a single smart object, how to configure it, and how to operate it. This paper describes the problem of the smart object in terms of implementation and operation. This paper proposes possible solutions though they have to be evaluated by the members, and have to be implemented for feasibility.

2. Problem

Problem-1: The specifications are not simple. For example, RPL[1] is constructed by six different drafts. The current draft of the RPL core specification becomes more than 150 pages. The Fig.1 shows the minimum protocol stack of the smart object without security. A red box means a new protocol that is being standardizing. A broken lined box means that the protocol is optional. A box with a triangle means the protocol is selective to the near box. The total number of pages of the new protocols is more than 500 pages when we choose CoAP[2]. Fig.2 shows the minimum protocol stack with security. A yellow box means a security protocol or a security function. When you implement all of them you have to additionally read more than 300 at least. After that, you have to decide which to implement or not. It causes complicated to implement the protocol, and the total of the stack size becomes larger. It is not suitable for the smart object. Furthermore, complicated specifications result hard to make sure of interoperability. As a result, it causes deployment to be delayed.

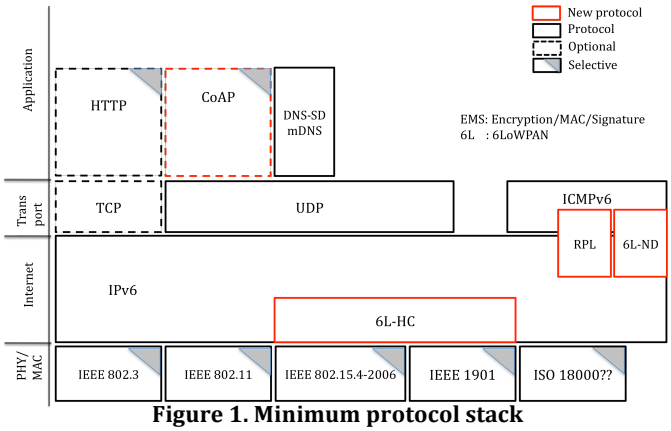

Figure 1. Minimum protocol stack

Problem-2: It is lack of a consideration of total operation that enables each security protocol. In Fig.2, each protocol is protected by each security mechanism. However, each security mechanism is defined by each protocol, or different specifications. It results same situation to the problem-1. The big problem is that some specifications just refer to the other specification. For example, DNSSEC[3] and SEND[4] are referred by DNS-SD[5] and 6L-ND[6] respectively. However, both protocols are tough to run on the smart device without simplification.

Problem-3: It is lack of a consideration of the device management protocol in order to configure, to monitor, to update the parameters of the device. It is assumed that many objects are to be managed. For example, there are 15,000 nodes for building automation. The operation needs to be considered such situation. No working group in IETF discusses such topics so far. CoAP could be used for this purpose. However, chicken-and-egg problem needs to be solved because the parameters of DTLS[7] are not configured when CoAP is used.

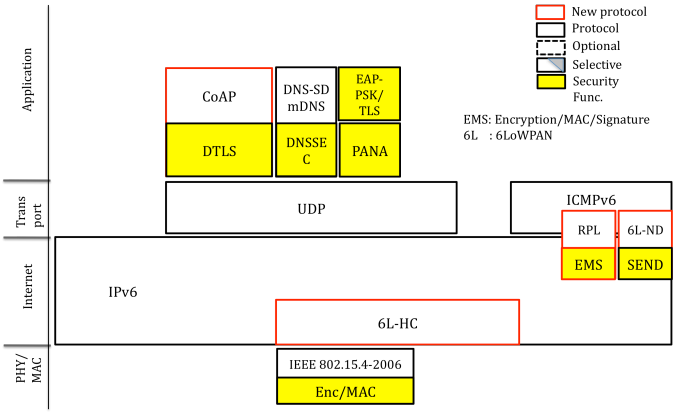

Figure 2. Mimimum implementation with security

3. Proposed approach

Implementation guideline must be useful for an implementor. It should be based on typical use cases so that an implementor could adopt it easily for his environment. It would help to reduce the number of variety of combination of the options in each protocol. The guideline should consider minimizing the implementation cost and the resource size. Operation guideline must be helpful for an operator. There are several parameters for each protocol. The guideline should include which parameters to be installed, how, and when before the device joins into a network. Lightweight Implementation Guideline (lwig) WG is forming to publish guidelines for the smart objects. This WG should consider above topic and should publish the guidelines. At the same time, those protocols in both Fig.1 and Fig.2 should have to be implemented for making sure whether the guideline is reasonable. Another approach is to hold several times of Interoperability testing that affects to increase mutual connectivity between each device. Certification program is also helpful.

4. Conclusion

The smart objects are going to be deployed rapidly, and they are connected into the Internet. In order to more accelerate the deployment and to make sure the interoperability, the implementation guidelines and the operation guideline are required. lwig WG should have to take account into it. At the same time, those protocols should have to be implemented to confirm the guideline is reasonable. Interoperability testing and certification program should be held periodically.

References

[1] T. Winter, P. Thubert, at el., "RPL: IPv6 Routing Protocol for Low power and Lossy Networks", draft-ietf-roll-rpl-18 in progress, February 4, 2011

[2] Z. Shelby, K. Hartke, C. Bormann, and B. Frank, "Constrained Application Protocol (CoAP)", draft-ietf-core-coap-04 in progress, January 24, 2011

[3] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "Resource Records for the DNS Security Extensions", RFC4034, March 2005

[4] J. Arkko, J. Kempf, B. Zill, and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005

[5] S. Cheshire, and M. Krochmal, "DNS-Based Service Discovery", draft-cheshire-dnsext-dns-sd-08.txt in progress, 12 January 2011

[6] Z. Shelby, S. Chakrabart, "Neighbor Discovery Optimization for Low-power and Lossy Networks", draft-ietf-6lowpan-nd-15 in progress, December 17, 2010

[7] E. Rescorla, and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 2006