Case Study of Data Exchange using Cross-Boundary Direct Interconnection between highly constrained Wireless Sensor Networks

Krongboon Singhanat\(^1\) and Kantida Panchareon\(^2\)*

\(^1\)Department of Electrical Engineering, Navaminda Kasatriyadhiraj Royal Air Force Academy, Bangkok, 10220, Thailand
\(^2\)Department of Electrical Engineering, Faculty of Engineering and Industrial Technology, Silpakorn University, Nakhon Pathom, 73000, Thailand

*Email: pancharoen_k@su.ac.th

Abstract. Internet of Things (IoT) connects multiple network entities together with different platforms and standards using the backbone network and Internet Protocol. However, some network interconnections may happen remotely at the edge of the network boundary between highly constrained platforms in absence of the connection with the backbone infrastructure. In this paper, we report the implementation of payload exchange between highly constrained multi-hop Wireless Sensor Networks (WSNs). The Constrained Application Protocol (CoAP) is accommodated by a native communication link using a payload fragmentation. The impacts of the hop distance and the fragmentation regarding the reliability and the latency are evaluated using a testbed showing less than 0.2 percent unsuccessful payload delivery.

1. Introduction

As the vision of IoT begins taking shape, many solutions have been emerged separately to support the diverse application. The interoperability between different hardware and distinctive network design is conventionally achieved by connecting each individual network with the Internet gateway using Internet Protocol [1]. However, in some cases, the communicating network entities may be deployed in a same spatial location which allows packet transfers between their physical platforms at the edge of the network under the authority consent [2], [3]. The concept of enabling interconnection has already been discussed by the previous works which report several benefits such as a data exchange, retrieving the lost segment and the extension of network lifetime via load distribution [2]–[5].

Enabling the connectivity between distinctive systems, the physical layer must be able to provide a mutual logical channel using the identical waveform for physical bit transfer. The link layer must adopt the mutual algorithm to access the common medium for timing the transmission and reception. Possible solutions on the link layer have been discussed by previous works [2], [3]. In the application layer, the payload format must be very compact and can be universally understood by all participants. The most well-known candidates for an application protocol in a constrained environment are MQTT (Message Queuing Telemetry Transport), AMQP (Advanced Message Queuing Protocol), XMPP (Extensible Messaging and Presence Protocol), and CoAP (Constrained Application Protocol) [6]. In comparison with all of them, CoAP consumes the least resources [7]. CoAP is proposed by IETF using the constrained RESTful architecture (CoRE) for application data exchange in the form of resource
access between client and server. Therefore, CoAP is mostly suitable for a constrained network which can be systematically integrated with HTTP REST for an elaborate system [7]. CoAP is designed and tested on top of IPv6 over Low-Power Personal Network (6LoWPAN) that can commonly be implemented on the up-to-date embedded platform. The 6LoWPAN standard is designed for IEEE 802.15.4 link layer with the goal to access every IoT device with IPv6 and requires at least 60-80 octets for payload accommodation [8]. However, a highly constrained WSN, deployed for sensing and report application, may possess a very compact frame size (less than 64 octets). Therefore, the network cannot directly support the 6LowPAN standard due to its insufficient maximum transmission unit (MTU). Nonetheless, forwarding application payload along the path with low-end devices may be used to provide an end-to-end communication for exchanging the data between neighbouring clusters or networks.

This work reports the implementation of the data exchange with a direct interconnection between highly constrained WSNs using CoAP on top of a native communication link on a testbed. The study assumes the scenario where neighbouring WSNs encounter each other and exchange the public resource. This paper is organized as follows: Section 2 elaborates the protocol design which allow the end-to-end exchange of CoAP messages on top of a customized link layer. In Section 3 the experiment setup is described. Section 4 discusses the results of the reliability measurement and end-to-end delay against the hop distance and degree of fragmentation.

2. Protocol Design
The main constraint in this design is the limitation on MTU which is imposed on hardware with low-computational performances. Therefore, the protocol design heavily focuses on the reduction of the frame space usage. The initial point of the protocol design considers the original convention and modifies the details to fit the design constraints.

2.1. Datagram Format
CoAP is originally designed on top of UDP (User Datagram Protocol). The format of the datagram is illustrated as follows.

![Figure 1. UDP Format](image)

![Figure 2. CoAP Message Format](image)

![Figure 3. Modified Local Datagram Format](image)

According to Figure 1, UDP header occupies 8 octets containing Source (SRC) port, Destination (DST) port, UDP datagram length and checksum. Since the CoAP message is relayed by a local native communication link, separated from the Internet, SRC/DST port can be omitted and automatically filled by the default port number 5683 specified by CoAP at the DST endpoint [6]. Figure 3 shows the datagram for carrying CoAP messages after the modification. The header fields of the CoAP message are literally defined by RFC7252 [6]. The modification results in the minimum header size of the modified datagram at 10 octets.
2.2. Fragmentation

Even though the framework for solving a limit frame size is recommended by Block-Wise Transfers RFC 7959 [8], it has a significant drawback. The block-wise transfer divides a CoAP message into blocks. However, each block must be separately requested causing excessive conversation. While these individual block requests can be handled by the systems recommended for 6LowPAN, the sheer number of block requests may pose a serious problem a bandwidth limited network. Therefore, the protocol design circumvents the drawback by using burst transmission of the message fragments which are reconstructed at the DST endpoint. Figure 4 illustrates the concept of the implemented fragmentation layer.

![Fragmentation Diagram](image)

**Figure 4.** Implementation of fragmentation of payload message by using transfer/reception session to fragment and reconstruct messages

The fragmentation header occupies one octet described by following format: \( \text{FRAGMENTATION} = (\text{FRAGMENT\_NUM} \ll 4) + \text{FRAGMENT\_COUNT} \). The reception process recognizes the total number of the message fragment from \( \text{FRAGMENT\_COUNT} \). The \( \text{FRAGMENT\_NUM} \) header specifies the order of the received fragment. Therefore, the maximum degree of fragmentation Since this design is directed to a highly constrained network, only one active session is permitted by default. The fragmentation knowingly introduces the exponential growth of the failed message reception \( P_{\text{failed}} = 1 - (1 - \text{PER})^n \), where \( \text{PER} \) is the probability of reception errors of the end-to-end packet transfer. To reduce \( P_{\text{failed}} \), the reception session sets a timeout counter proportionally to the total number of fragments at the point of the first fragment reception to selectively request the lost fragments. The reception session is regarded as unsuccessful after a pre-set number of attempts. This protocol design can moderately support resource discovery via web linking. The payload content can be further compressed in the CBOR format (Concise Binary Object Representation). However, the payload content is application dependent. Hence, it is outside the scope of this paper.

3. Experiment Setup

For the experiment, the scenario where two co-located WSNs with interoperable hardware detect each other and exchange the information of the public available resources via web linking. The protocol is tested in a testbed of 12 EZ430-RF2500 motes [10]. Figure 5 illustrated the experiment setup.

![Experiment Setup Diagram](image)

**Figure 5.** Experiment is set with co-located Network A and Network B accessing public resources via CoAP messages.
The experiment aims to study the effects of the fragmentation and hop distance which are the main key factors of message reception failures. Network A have been deployed in a sensing application in this local area. Later, Network B is deployed in the same Location. Each node periodically sends the sensing data packet to its own base station in which the application agent is programmed to exploit the sensing data. The EZ430-RF2500 mote is used for every sensor node in the experiment setup. However, Network A implements Low Power Polling Receiver-Initiated MAC protocol while Network B adopts Strobe Preamble Low Power Listening Sender-Initiated MAC Protocol. The end nodes (B6 and A6) at the edge of the network periodically exchange packets across a common channel. Exploiting this local connection, the application agent in the base station of each sensor network (emulated in the same PC for the sake of precise time measurements) accesses a useful resource provided by the neighbouring network using GET (0.01) request in the CoAP framework. The success rate is calculated every 10 messages and each measurement result is represented by 95-percent confidence interval of 10 samples. The end-to-end delay is represented by the 95-percentile of 1000 samples.

4. Experiment Results

4.1. Effects of Hop Distance

The number of hop distances is proportional to the network scale. The experiment varies the number of hop distances between the base station and the pairing node while measuring the collective network performances. The results are illustrated in Figure 6.

Figure 6. a) The measurement results show the success rate of the receptions of the resource exchange messages and periodical internal messages as the hop distance increases. b) The end-to-end delay and estimated data rate of the resource exchange messages as the hop distance increases.
The experiment shows the expected results. The link layer retransmits the packets until the packet buffer overflow forcing packet drops which is the only cause of packet losses. The resource exchange messages are always secured from the buffer overflow because the resource exchange message piggyback on the request and response in the form of CON messages in the CoAP framework which are prioritized. All packet drops are reflected in the reception failures of the periodic internal messages which are sent with a NON message in the CoAP framework. Additionally, the effect of carrying extra messages is relatively constant regardless of the hop distance as seen in the comparison between the cases of internal messages and the cases of internal messages with resource exchange. Most of the internal message failures are caused by the overflow due to the hop distance, not by the extra traffic from the resource exchange. That is because the extra traffic is limited to only one session. The effects of the hop distances on the end-to-end delay behaves as predicted. The travelling time proportionally increases with the hop distance approximately 3.5 seconds per hop.

The fragmentation is particularly introduced to solve the constraint of the physical frame space. The affordable payload size depends on the implementation. In this case study, we use EZ430-RF2500 motes. The physical frame size is limited by the memory buffer (Tx/Rx FIFO) at 32 bytes, therefore a message fragment can accommodate only 11 octets payload. The packet buffer size is set at 10 packets, therefore, the maximum number of fragments per session must be set at 5, since the communication partner may use the rest available space for send his traffic simultaneously. The distance between two base stations is 12 hops. According to Figure 7, the fragmentation can cause some reception failures. This situation happens in the rare chance that only CON messages are stacked in the packet buffer of a node in the forwarding route until triggering the buffer overflow. However,
the successful deliver rate in the case of 5 fragments is relatively reliable at 99.8 percent. In addition, the number of fragments does not introduce a sharp decline of the reliability and end-to-end delay because of the selective fragment request and message retransmission. Multiple fragment losses are corrected at the same time causing the slightly drop of performances instead of the exponential drops.

5. Conclusions
This paper reports the possibility of the data exchange with a local direct interconnection between neighbouring WSNs with highly constrained hardware. The CoAP framework is implement on top of a customized link layer. The protocol design heavily focuses on the compression of the datagram format to solve the frame space limitation. The fragmentation is introduced using burst transmissions and selective requests. The design is evaluated in a testbed of EZ430-RF2500 motes. The experiments show that the protocol offers a reliable data exchange up to 12 hop distances in the experimental conditions.

6. References
[1] P. Ray, “A survey on Internet of Things architectures,” J. King Saud Univ. - Comput. Inf. Sci., vol. 30, no. 3, pp. 291–319, 2018.
[2] K. Singhanat, N. R. Harris, and G. V. Merrett, “Experimental validation of opportunistic direct interconnection between different Wireless Sensor Networks,” in SAS 2016 - Sensors Applications Symposium, Proceedings, 2016, pp. 36–41.
[3] T. Jiang, G. V. Merrett, and N. R. Harris, “Opportunistic Direct Interconnection between Co-Located Wireless Sensor Networks,” in 2013 22nd International Conference on Computer Communication and Networks (ICCCN), 2013, pp. 1–5.
[4] T. Jiang, G. V. Merrett, and N. R. Harris, “Enabling opportunistic energy trading between overlapping energy harvesting wireless sensor networks,” in Proceedings of the 2nd International Workshop on Energy Neutral Sensing Systems - ENSys ’14, 2014, pp. 25–30.
[5] K. Singhanat, T. Jiang, G. V. Merrett, and N. R. Harris, “Empirical evaluation of OI-MAC: Direct interconnection between wireless sensor networks for collaborative monitoring,” in 2015 IEEE Sensors Applications Symposium (SAS), 2015, pp. 1–5.
[6] Z. Shelby, K. Hartke, and C. Bormann, “The Constrained Application Protocol (CoAP).” Internet Engineering Task Force (IETF), pp. 1–112, 2014.
[7] V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate2Nastase, “A Survey on Application Layer Protocols for the Internet of Things,” Trans. IoT Cloud Comput., 2015.
[8] C. Bormann, “Block-Wise Transfers in the Constrained Application Protocol (CoAP).” pp. 1–37, 2016.
[9] J. Postel, “User Datagram Protocol.” IETF, 1980.
[10] M. Morales and Z. Shivers, “Wireless sensor monitor using the eZ430-RF2500,” 2007.