Request-Response Interaction Model in Constrained Networks

Izaz Ahmad Khan[1]*, Muhammad Safdar[2], Farman Ullah[3], Syed Roohullah Jan[4], Fazlullah Khan[5], Sabir Shah[6]

[1,2,3,6]Department of Computer Science, Bacha Khan University Charsadda, Khyber Pakhtunkhwa, Pakistan
[4,5]Department of Computer Science, Abdul Wali Khan University, Mardan, Khyber Pakhtunkhwa, Pakistan

ABSTRACT

Internet of things (IoT) is an important part of a new generation of technology that every object no matter things or human could be connected to Internet. There are many wireless protocols such as IEEE 802.11 Series, 802.15 Series and Zigbee for communication between devices. However, considering a lot of small devices are unable to communicate efficiently with constrained resources, Internet Engineering Task Force (IETF) has developed a lightweight protocol: Constrained Application Protocol (CoAP). In CoAP, the notion of "notifications" is introduced. A client can request a server that it wants to get notified when the value changes. The server then makes a note of the client request (if it supports observation). From there on, when a value changes at server side, it notifies all registered clients.

Keyword: -*Constrained Environment, IoT, Resource Observation, Request-Response Model .*

1. INTRODUCTION

Internet of Things (IoT) is represented as a global network which intelligently connects all the objects no matter devices,
systems or human, it is with self-configuring capabilities based on standard and interoperable protocols and formats [1-9]. Through smart sensing, identification technology and persuasive computing, IoT has been called the Third Wave in information industry following the computer and the Internet. There are hundreds of protocols supported by IoT. Of the many protocols, wireless protocols play an important role in IoT development. One latest protocol for application layer, i.e., CoAP, is nowadays famous among the research communities.

Constrained Application Protocol (CoAP) is a software protocol intended to be used in very simple electronics devices that allows them to communicate interactively over the Internet. It is particularly targeted for small low power sensors, switches, valves and similar components that need to be controlled or supervised remotely, through standard Internet networks. CoAP is an application layer protocol that is intended for use in resource-constrained internet devices, such as WSN nodes. CoAP is designed to easily translate to HTTP for simplified integration with the web, while also meeting specialized requirements such as multicast support, very low overhead, and simplicity. Multicast, low overhead, and simplicity are extremely important for Internet of Things (IoT) andMachine-to-Machine (M2M) devices, which tend to be deeply embedded [10-14] and have much less memory and power supply than traditional internet devices have. Therefore, efficiency is very important. CoAP can run on most devices that support UDP or a UDP analogue [15-23]. The rest of paper is organized as follows. In Section 2, the format of CoAP is provided. In Section 3, the request-response interaction model is given followed by conclusion in section 4.

2. COAP MESSAGE FORMAT

Knowing the internal details of the CoAP message format is best left for implementers of the CoAP protocol stack, however, you must have some understanding of the structure to truly appreciate the protocol. It will also help you make the right decisions. The CoAP message consists of a series of bytes, a four byte header that is mandatory, followed by a set of bytes that are optional. Therefore, the smallest size of a CoAP message is just 4 bytes. Figure 1 provides an overview of the CoAP message byte structure

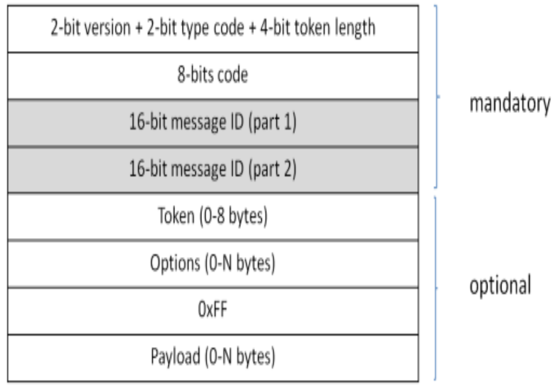

Fig -1: CoAP Message Byte Structure

The CoAP message is transmitted to the remote recipient over UDP. The byte ordering is in network byte order. The first 4 bytes that are mandatory contain the following pieces of information:

2.1 Byte 0

a. 2-bit version: The first two bits indicate the CoAP version number. As of now, only version 1 is supported.
b. 2-bit type code: The next two bits indicate the message type. This can take one of 4 values – CON, NON, ACK, RST
c. 4-bit token length: The next 4 bits indicate the length of the token value in bytes. Token is used to correlate messages. The length of token can be between 0-8 bytes. Other values are reserved

2.2 Byte 1

This contains the message code. The message code values can be GET, PUT, POST, NOT FOUND etc.

2.3Byte 2,3

The next two bytes together make up a 16-bit number. This is where the message ID is carried. This is an unsigned number.

After the first 4 bytes, based on the context, the message may contain additional bytes. It is recommended that we send a token with every message (especially in cases where correlation is required). Therefore, if the 0th byte indicates a token length value that is between 1 -8, then 5th byte onwards, we will have a token. For example, if last 4 bits of byte 0 in the 4-byte header have a value 5, then it indicates that this message contains a token whose value is 5-bytes long. Thus, byte number 4,5,6,7,8 that follow the 4-byte header (byte-0 to byte-3) will contain the token.

Following the token, there could be multiple options. Think of options as pieces of data that provide additional information about the message. If you compare with HTTP world, options are like request headers, however, there is one big difference. Unlike HTTP world, where you can add any arbitrary HTTP header, in CoAP, you are limited to what is defined. For new headers, you need to go through the process of submitting your recommendation for a review to IETF groups. Examples of options defined by CoAP are “Max-Age”, “Content-Format” and “ETag”. Once the options are complete, there is a separator marked by the presence of the value 0xFF. If this value is present, there must be at-least 1 -byte of payload data. The value 0xFF is followed by one or more bytes of payload data. This is where you can put any data that you want to transfer (like in previous examples, we put measured temperature value). The last point to note is that CoAP does not define an “End of Message” identifier. So, it’s pretty much left to the lower level implementations [24-30] to take care of when the message ends.

3. REQUEST-RESPONSE INTERACTION MODEL

The CoAP specification at the time of this writing was draft-18. In this draft, there is still some work to be done around clear set of rules that govern what is the response message type for a given request. While the CoAP specification will continued to get refined over a period of time, we have come up with simple guidelines as tabulated below in Table 1 to enable researchers decide what response to send back for a given request type [31-34].

Client Sends	Message Successfully Parsed and Understood By Server ?	Server Has all Information to Process the Request and can Successfully Process ?	Server Sends Message Type	Server Sends Message Code	Remarks
CON	YES	YES	ACK	One of success response codes (e.g. CONTENT)	Happy day scenario
CON	YES	NO	ACK	One of failed response codes (e.g.	URL path in request is wrong and
CON	NO	NO	RST	One of failed response codes (e.g. BAD OPTION)	e.g. Unknown option number
NON	YES	YES	-	-	No response sent back
NON	YES	YES	NON	One of success response codes (e.g. CONTENT)	Response sent back as NON message
NON	YES	NO	RST	One of failed response codes (e.g. NOT FOUND)	URL path in request is wrong and 4.04 not found is sent in RST
NON	NO	NO	RST	One of failed response codes (e.g. BAD	e.g. Unknown option number
NON	YES	YES	CON	One of request codes (e.g. PUT)	e.g. Previous NON request was for a data that requires confirmation from the sender on whether it reached the client or not

Table -1: Guidelines for Request and Response Messages

4. CONCLUSIONS

Internet of things (IoT) consists of resource-constrained sensor nodes at the core of each device. IoT is gaining momentum with inclusion of peculiar physical devices for the first time in the history. It was never imagined that a smart refigrator would have shopped automatically by placing order at a supermarket. The presence of resource-constrained sensor nodes require extremely lightweight interaction model for observing resources. Constrained Application protocol (CoAP) provides a similar interaction model to HTTP, however, the resources are observed in a very lightweight manner. This study present an overview of the resource observation in the context of IoT using CoAP protocol. We presented a guideline for matching requests with a corresponding matching response using four different message types.

5. REFERENCES

[1]. Khan. F., Bashir, F. (2012). Dual Head Clustering Scheme in Wireless Sensor Networks. in the IEEE International Conference on Emerging Technologies (pp. 1-8). Islamabad: IEEE Islamabad.

[2]. Syed Roohullah Jan, Farman Ullah, Hashim Ali, Fazlullah Khan, " Enhanced and Effective Learning through Mobile Learning an Insight into Students Perception of Mobile Learning at University Level", International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.674-681, March-April 2016. URL : http://ijsrset.com/IJSRSET1622209.php

[3]. Khan. F., Nakagawa. K. (2012). Cooperative Spectrum Sensing Techniques in Cognitive Radio Networks. in the Institute of Electronics, Information and Communication Engineers (IEICE), Japan , Vol -1, 2.

[4]. Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2015). A Dynamic Key Length Based Approach for Real-Time Security Verification of Big Sensing Data Stream. In Web Information Systems Engineering–WISE 2015 (pp. 93-108). Springer International Publishing.

[5]. M. A. Jan, P. Nanda, X. He, Z. Tan and R. P. Liu, "A robust authentication scheme for observing resources in the internet of things environment" in 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 205-211, 2014, IEEE.

[6]. Khan. F., Nakagawa, K. (2012). Performance Improvement in Cognitive Radio Sensor Networks. in the Institute of Electronics, Information and Communication Engineers (IEICE) , 8.

[7]. Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2015, August). DPBSV--An Efficient and Secure Scheme for Big Sensing Data Stream. InTrustcom/BigDataSE/ISPA, 2015 IEEE (Vol. 1, pp. 246-253). IEEE.

[8]. M. A. Jan, P. Nanda and X. He, "Energy Evaluation Model for an Improved Centralized Clustering Hierarchical Algorithm in WSN," in Wired/Wireless Internet Communication, Lecture Notes in Computer Science, pp. 154–167, Springer, Berlin, Germany, 2013.

[9]. Khan. F., Kamal, S. A. (2013). Fairness Improvement in long-chain Multi-hop Wireless Adhoc Networks. International Conference on Connected Vehicles & Expo (pp. 1-8). Las Vegas: IEEE Las Vegas, USA.

[10]. Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2016). A dynamic prime number based efficient security mechanism for big sensing data streams.Journal of Computer and System Sciences.

[11]. M. A. Jan, P. Nanda, X. He and R. P. Liu, "Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network", 2013 IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC & EUC), pp. 1400-1407, 2013.

[12]. Jabeen. Q., Khan. F., Khan, Shahzad, Jan. M. A., Khan. S.A (2016). Performance Improvement in Multihop Wireless Mobile Adhoc Networks. in the Journal Applied, Environmental, and Biological Sciences (JAEBS), Print ISSN: 2090-4274 Online ISSN: 2090-4215

[13]. Khan. F., Nakagawa, K. (2013). Comparative Study of Spectrum Sensing Techniques in Cognitive Radio Networks. in IEEE World Congress on Communication and Information Technologies (p. 8). Tunisia: IEEE Tunisia.

[14]. Puthal, D., Sahoo, B., & Sahoo, B. P. S. (2012). Effective Machine to Machine Communications in Smart Grid Networks. ARPN J. Syst. Softw.© 2009-2011 AJSS Journal, 2(1), 18-22.

[15]. Khan. F. (2014). Secure Communication and Routing Architecture in Wireless Sensor Networks. the 3rd Global Conference on Consumer Electronics (GCCE) (p. 4). Tokyo, Japan: IEEE Tokyo.

[16]. M. A. Jan, P. Nanda, X. He and R. P. Liu, "PASCCC: Priority-based application-specific congestion control clustering protocol" Computer Networks, Vol. 74, PP-92-102, 2014.

[17]. Khan. F. (2014). Throughput & Fairness Improvement in Mobile Ad hoc Networks. the 27th Annual Canadian Conference on Electrical and Computer Engineering (p. 6). Toronto, Canada: IEEE Toronto.

[18]. Mian Ahmad Jan and Muhammad Khan, "A Survey of Cluster-based Hierarchical Routing Protocols", in IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.3, April. 2013, pp.138-143.

[19]. Khan. S., Khan. F., (2015). Delay and Throughput Improvement in Wireless Sensor and Actor Networks. 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW) (pp. 1-8). Riyadh: IEEE Riyad Chapter.

[20]. Khan. Shahzad, Khan. F., Jabeen. Q., Arif F., Jan. M. A., Khan. S.A (2016). Performance Improvement in Wireless Sensor and Actor Networks. in the Journal Applied, Environmental, and Biological Sciences Print ISSN: 2090-4274 Online ISSN: 2090-4215

[21]. Puthal, D., & Sahoo, B. (2012). Secure Data Collection & Critical Data Transmission in Mobile Sink WSN: Secure and Energy efficient data collection technique.

[22]. Mian Ahmad Jan and Muhammad Khan, "Denial of Service Attacks and Their Countermeasures in WSN", in IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.3, April. 2013.

[23]. Qamar Jabeen, Fazlullah Khan, Muhammad Nouman Hayat, Haroon Khan, Syed Roohullah Jan, Farman Ullah, " A Survey : Embedded Systems Supporting By Different Operating Systems", International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.664-673, March-April 2016. URL : http://ijsrset.com/IJSRSET1622208.php

[24]. M. A. Jan, P. Nanda, X. He and R. P. Liu, "A Sybil Attack Detection Scheme for a Centralized Clustering-based Hierarchical Network" in Trustcom/BigDataSE/ISPA, Vol.1, PP-318-325, 2015, IEEE.

[25]. Jabeen. Q., Khan. F., Hayat, M.N., Khan, H., Jan., S.R., Ullah, F., (2016) A Survey : Embedded Systems Supporting By Different Operating Systems in the International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.664-673.

[26]. M. A. Jan, P. Nanda, X. He and R. P. Liu. 2016. A Lightweight Mutual Authentication Scheme for IoT Objects, IEEE Transactions on Dependable and Secure Computing (TDSC), "Submitted".

[27]. M. A. Jan, P. Nanda, X. He and R. P. Liu. 2016. A Sybil Attack Detection Scheme for a Forest Wildfire Monitoring Application, Elsevier Future Generation Computer Systems (FGCS), "Submitted".

[28]. M. A. Jan, M. Usman, P. Nanda and X. He. 2016. PAWN: A Payload-based mutual Authentication scheme for Wireless Sensor Networks, in 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-16), "accepted".

[29]. M. Usman, M. A. Jan and X. He. 2016. Cryptography-based Secure Data Storage and Sharing Using HEVC and Public Clouds, Elsevier Information sciences, "accepted".

[30]. Syed Roohullah Jan, Syed Tauhid Ullah Shah, Zia Ullah Johar, Yasin Shah, Fazlullah Khan, " An Innovative Approach to Investigate Various Software Testing Techniques and Strategies", International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.682-689, March-April 2016. URL : http://ijsrset.com/IJSRSET1622210.php

[31]. Khan. F., Khan. F., Jabeen. Q., Jan. S. R., Khan. S., (2016) Applications, Limitations, and Improvements in Visible Light Communication Systems in the VAWKUM Transaction on Computer Science Vol. 9, Iss.2, DOI: http://dx.doi.org/10.21015/vtcs.v9i2.398

[32]. Syed Roohullah Jan, Fazlullah Khan, Muhammad Tahir, Shahzad Khan., (2016) "Survey: Dealing Non-Functional Requirements At Architecture Level", VFAST Transactions on Software Engineering, (Accepted 2016)

[33]. M. A. Jan, "Energy-efficient routing and secure communication in wireless sensor networks," Ph.D. dissertation, 2016.

[34]. Syed Roohullah Jan, Faheem Dad, Nouman Amin, Abdul Hameed, Syed Saad Ali Shah, " Issues In Global Software Development (Communication, Coordination and Trust) - A Critical Review", International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.660-663, March-April 2016. URL : http://ijsrset.com/IJSRSET1622207.php