International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 21 Issue 2 – APRIL 2016.

USING COAP PROTOCOL FOR RESOURCE OBSERVATION IN IOT

Syed Roohullah Jan[1], Fazlullah Khan*[1], Farman Ullah[2], Nazia Azim[1], Muhammad Tahir[1]

[1]*Department of Computer Science, Abdul Wali Khan University Mardan*
[2]*Department of Computer Science, Bacha Khan University, Charsadda*

***Abstract*--Technological growth has enabled the communication systems to move forward by enabling interaction among physical world objects without human interventions. A lot of work has already been done in the past to setup the Internet which makes sense to follow the lead and try to leverage the already existing infrastructure and build on top of it. To standardize a communication methodology for machines to independently exchange information with each other, keeping in mind that we want to build on and leverage existing knowledge and infrastructure. The Internet Engineering Task Force created a working group called Constrained RESTful Environment Group (or CoRE) group. This group was assigned the task to define a mechanism using which a large number of small, resource constrained, low power devices, an communicate over lossy networks. This group defined a set of specifications that is known today collectively as – Constrained Application Protocol or CoAP in short. The objective of this paper is to provide an overview of CoAP protocol and observing resource, similar to http, in the Internet of things (IoT) and wireless sensor networks (WSNs).**

Keywords: **Surveillance, Data Mining, Privacy, Security, Data Surveillance, Function Creep.**

I. INTRODUCTION

Constrained Application Protocol is a protocol at the application level that is designed to allow message exchange between resource-constrained devices over resource constrained networks such as WSN and IoT [1-7]. Resource constrained devices are small devices that lack the processing power, memory footprint and speed that we generally expect from our computing devices. These devices often are built using 8-bit microcontrollers or low-cost, general purpose 32-bit microcontrollers. Resource constrained networks are network stacks and configurations that do not have the full capabilities of TCP/IP stack and have lower transfer rates. CoAP runs over UDP and not TCP. 6LoWPAN is an example of such a constrained network configuration setup. CoAP provides an HTTP-like request and response paradigm where devices can interact by sending a request and receiving a response. Like the web, devices are addressed using IP address and port number. Access to services exposed by the

* corresponding author fazlullah@awkum.edu.pk device is via RESTful URIs. It's very much similar to HTTP, where method type (e.g. GET, PUT), response codes (e.g. 404, 500) and content-type are used to convey information. Given the protocol's close similarity to HTTP, it's obvious that it was designed for easy web integration.

CoAP does not replace HTTP, instead, it implements a small subset of widely accepted and implemented HTTP practices and optimizes them for M2M message exchange. Think of CoAP as a method to access and invoke RESTful services exposed by "Things" over a network. As an example, let's consider our temperature sensor installed in the conference room of our office as shown in figure below. The temperature sensor works like a "server" (Thing) which any CoAP based client (another Thing) can query to get the temperature.

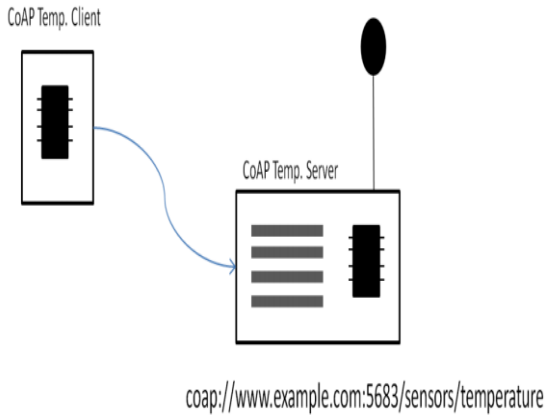

Figure 1. CoAP Client and Server

In the figure above, the server exposes the interface to query the temperature as a RESTful URL with the path as "sensors/temperature". By this time, you would have noticed the new scheme – coap. Instead of using http as the scheme, a new scheme called "coap" is introduced. There is also a secure version, just like https, you can use coaps. In the figure above, the full provides the scheme name, the DNS name, the port number and the path. Remember, the default port suggested for CoAP is 5683. Also remember, that the communication will use UDP and not TCP [22-29]. Therefore, the client needs to establish a UDP connection with the server, send a GET request to the server over the given URL path and get a response. Just like HTTP response, you can get a response in various formats (remember HTTP content-type?). The specification allows for various content formats, notable amongst them is JSON, XML and plain text. In the next section, we present the request/response interaction model for CoAP which is somewhat similar to HTTP; however, it uses extremely lightweight options, headers, metadata and tokens [8-11].

1. CoAP Request/Response Interaction Model

As stated before, CoAP is similar to HTTP. One party can send a request to the remote party [11-10], and the remote party may respond back. There are four kinds of message types defined by the specification:

1. CON – This represents a confirmable message. A confirmable message requires a response, either a positive acknowledgement or a negative acknowledgement. In case acknowledgement is not received, retransmissions are made until all attempts are exhausted. The retransmissions use a non-linear, exponential strategy between attempts.
2. NON – This represents a non-confirmable message. A non-confirmable request is used for unreliable transmission (like a request for a sensor measurement made in periodic basis. Even if one value is missed, there is not too much impact). Such a message is not generally acknowledged by the receiver, i.e., a server.
3. ACK – This represents an acknowledgement. It is sent to acknowledge a confirmable (CON) message.
4. RST – This represents a negative acknowledgement and means "Reset". It generally indicates, some kind of failure (like unable to parse received data)

A typical confirmable message exchange could look like as shown in Figure 2

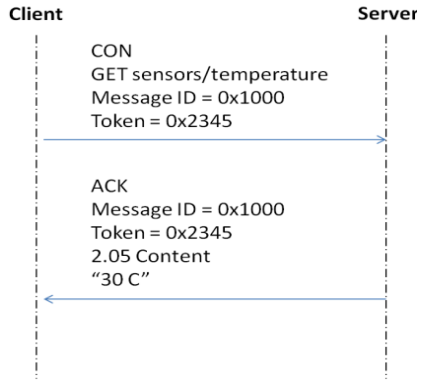

Figure 2. CON Message Exchange

The client sends a CON message to the server. The method type is GET, the path URL is "sensors/temperature". The message ID is a 16-bit number used to uniquely identify a message and help the server in duplicate detection [35-37]. Token is used to correlate messages. We will soon see an example of message correlation. Once the server gets the message, it measures the temperature and returns an acknowledgement. The acknowledgement contains the same message ID and the token that was received in the request [9-11]. Along with the acknowledgement, the message also contains the temperature data (in the above figure, its 30 C). Sending response data, along with the acknowledgement is also called "piggy-backed response". Finally, the response also has a message code, in this case it's "2.05 Content". These are very similar to HTTP status codes (there is a 4.04 message code to indicate not found, like the HTTP 404 not found status code) [20-26].

The previous example indicates a success, but sometimes CON message might result in failure. For example, if the path URL is incorrect, there is no way the server can serve the request. In HTTP world, if the URL is incorrect, we get a **404** as response code. In the same manner, in CoAP also, we get a "Not Found" response. Figure 3 indicates such a situation.

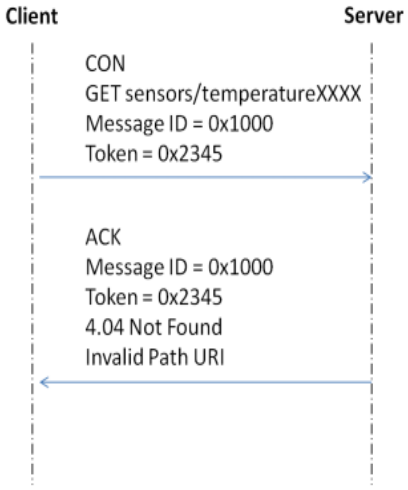

Figure 3. CON Message Exchange Failure

In the figure 3, the request is made to an unrecognized path URL"sensors/temperatureXXXX". Since there is no way server can handle that path, it acknowledges the receipt of the message, however, it sets the message code as **4.04** which means "not found". Additionally, implementations may add diagnostic message in the response payload, and in this example, the string "Invalid Path URL" was added as the diagnostic payload. Sometimes, the request is not mission critical and it's acceptable if some values are never received. Classic example is temperature sensing request for room cooling that continues 24 x 7. Even if some queries to the temperature server are lost there would hardly be an issue. In those cases, NON (or Non-Confirmable) requests are used. Figure 4 depicts such a scenario.

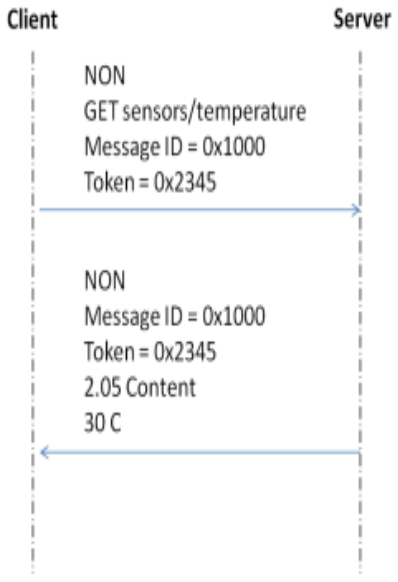

Figure 4. NON Message Exchange

The client sends a NON based GET request. The server also responds back with a NON message. In either

direction, the message may get lost, but unlike a CON message, no attempt will be made to retransmit the lost message. A new NON message will simply be sent by the client when it's due. Natural question to ask in this case would be what if NON message cannot be understood by the server (for example, the URL path is incorrect), will the server respond back? The specification states that a NON message, being non-confirmable, must not be acknowledged by the recipient. The recipient, at best, may send a RST (reset) message and must silently ignore. Therefore, if a NON message carries incorrect path, there is no guarantee that the sender will be informed of the error [28-34]. The sender may choose to re-transmit the message up to a limit, but the sender cannot expect a guaranteed response. Further information and details can be seen in [36-51].

II. CONCLUSION

CoAP is an extremely lightweight protocol for resource observation in Internet of Things. It is a lightweight version of HTTP, however, it cannot be used as an alternative to HTTP. In this paper, we presented various types of scenarios for resource observation using CoAP protocol. Also, different messages, i.e., CON, NON, ACK and RST are studied and analyzed. Furthermore, we gave an inside to the situation where we can use such messages.

REFERENCES

[1] Z. Shelby, K. Hartke, C. Bormann, "The constrained application protocol (CoAP)", 2014.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] K.Hartke, "Observing resources in coap", 2014.

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

[9] 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.

[10] O. Bergmann, K. T. Hillmann, S. Gerdes, A c oap- gateway for smart homes,
in: 2012 International Conference on Computing, Networking and Communications (ICNC), 2012, pp. 446–450.

[11] 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.

[12] 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.

[13] 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

[14] 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.

[15] 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.

[16] 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.

[17] M. Castro, A. J. Jara, A. F. Skarm eta, "Enabling end-to-end coap-based communications for the web of things", Journal of Network and Computer Applications (2014).

[18] Syed Roohullah Jan, Faheem Dad, Nouman Amin, Abdul Hameed, Syed Saad Ali Shah.(2016)." *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.

[19] Syed Roohullah Jan, Khan. F., Zaman. A., (2015) The Perception of students about Mobile Learning at University Level. in the khgresearch.org NO. CONTENTS PAGE NO Turkey, pp.97

[20] Khan. F., (2014). *Fairness and throughput improvement in mobile ad hoc networks.* the 27th Annual Canadian Conference on Electrical and Computer Engineering (p. 6). Toronto, Canada: IEEE Toronto.

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

[22] 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.

[23] 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

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

[25] 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.

[26] Jabeen. Q., Khan. F., Hayat, M.N., Khan, H., Jan., Syed Roohullah Jan, 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.

[27] Syed Roohullah Jan, Syed Tauhid Ullah Shah, Zia Ullah Johar, Yasin Shah, Khan. F., *"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.

[28] 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.

[29] L. Atzori, A. Iera, G. Morabito, *The internet of things: A survey*, Computer
networks 54 (2010) 2787–28 05.

[30] 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.

[31] 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.

[32] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (iot): A vision, architectural elements, and future dire ctions, Future

Generation
Computer Systems 29 (2013) 1645–1660

[33] 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.

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

[35] Khan. F., Khan. F., Jabeen. Q., Syed Roohullah Jan, Khan. S., (2016) *Applications, Limitations, and Improvements in Visible Light Communication Systems* in the VAWKUM Transaction on Computer Science Vol. 9, Iss.2.

[36] Azim. N., Majid. A., Khan. F., Tahir. M., Safdar. M., Jabeen. Q., (2016) Routing of Mobile Hosts in Adhoc Networks. in the International Journal of Emerging Technology in Computer Science and Electronics (in press)

[37] Azim. N., Qureshi. Y., Khan. F., Tahir. M., Syed Roohullah Jan, Majid. A., (2016) Offsite One Way Data Replication towards Improving Data Refresh Performance. in the International Journal of Computer Science and Telecommunications (in press)

[38] Azim. N., Majid. A., Khan. F., Tahir. M., Syed Roohullah Jan, (2016) People Factors in Agile Software Development and Project Management. in the International Journal of Emerging Technology in Computer Science and Electronics (in press)

[39] Azim. N., Khan. A., Khan. F., Syed Roohullah Jan, Tahir. M., Majid. A. (2016) Offsite 2-way Data Replication towards Improving Data Refresh Performance. in the International Journal of Engineering Technology and Applications (in press)

[40] Azim. N., Ahmad. I., Khan. F., Tahir. M., Majid. A., Syed Roohullah Jan, (2016) A New Robust Video Watermarking Technique Using H.264/AAC Codec Luma Components Based On DCT. in the International Journal of Advance Research and Innovative Ideas in Education (in press)

[41] Syed Roohullah Jan, Ullah. F., Khan. F., Azim. N, Tahir. M. (2016) Using CoAP protocol for Resource Observation in IoT. in the International Journal of Engineering Technology and Applications (in press)

[42] Syed Roohullah Jan, Ullah. F., Khan. F., Azim. N, Tahir. M,Safdar, Shahzad. (2016) Applications and Challenges Faced by Internet of Things- A Survey. in the International Journal of Emerging Technology in Computer Science and Electronics (in press)

[43] Tahir. M., Syed Roohullah Jan, Khan. F., Jabeen. Q., Azim. N., Ullah. F., (2016) EEC: Evaluation of Energy Consumption in Wireless Sensor Networks. in the International Journal of Engineering Technology and Applications (in press)

[44] Tahir. M., Syed Roohullah Jan, Azim. N., Khan. F., Khan. I. A., (2016) Recommender System on Structured Data. in the International Journal of Advance Research and Innovative Ideas in Education (in press)

[45] Tahir. M., Khan. F., Syed Roohullah Jan, Khan. I. A., Azim, N., (2016) Inter-Relationship between Energy Efficient Routing and Secure Communication in WSN. in the International Journal of Emerging Technology in Computer Science and Electronics (in press)

[46] Safdar. M., Khan. I. A., Khan. F., Syed Roohullah Jan, Ullah. F., (2016) Comparative study of routing protocols in Mobile adhoc networks. in the International Journal of Computer Science and Telecommunications (in press)

[47] Syed Roohullah Jan, Khan. F., Zaman. A., (2015) The Perception of students about Mobile Learning at University Level. in the khgresearch.org NO. CONTENTS PAGE NO Turkey, pp.97

[48] 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".

[49] 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".

[50] 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".

[51] 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".