IJCSC 0973-7391 Volume 7 • Number 2 March 2016 - Sept 2016 pp. 42-48 available online at www.csjournalss.com

Securing Application Layer Protocol For IOT

Dr. Gaurang Raval, Foram Suthar
Computer Science and Engineering(Networking Technologies), Ahmedabad, India.
gaurang.raval@nirmauni.ac.in, 14mcen27@nirmauni.ac.in

Abstract: IoT is a new concept or we can say that it is a new technology for a new generation. It enhances our daily life, using some tiny devices and sensor nodes which are connected to each other through Internet. Home appliances can be easily operated by IoT at any time, from anywhere. Secure communication between all devices is an important thing in IoT. The purpose of this paper is to provide security at Application layer protocol in IoT. We are going to the discussion about CoAP application layer protocol, DTLs security protocol and some related work done in security area on Internet of Things.
Keywords: IoT, CoAP, DTLs, Reed Solomon.

Introduction

The Internet of Things(IoT) is a rapidly growing technology which connects all devices using the internet. It is communication tool which works as a bridge between computer and human andalso between two computers. There are many application layer protocols available in IoT but one of the preferable protocol for IoT is CoAP .CoAP is basically used for M2M application and also for IoT based application.

The main difference between M2M and IoT is M2M is a machine to machine type technology and it is a subset of IoT.M2M technology provides communication between two network devices. It also performs some tasks without any manual interaction. Communication may happen over a wired or wireless network.For example synchronization process in your mobile. Mobile synch the data between cloud and mobile. After connecting your mobile to the internet it will automatically synch data. IoT is like a network of some tiny devices.For example Device senses the entry of a person into the room and based on his/her requirements,a device will turn on fan or lights. So IoT is not only M2M but it is the combination of M2H (machine to human),H2M (human to machine), M2M (machine to machine).

The main problem in IoT is security, during communication between two tiny nodes security is a must otherwise, any malicious node can attack during communication. The purpose of this paper is to provide security for IoT at the application layer. In this paper in the first section, we will see some brief introduction of application protocol CoAP. In the second section, we will see security protocol DTLs, in the third section, related work done on DTLs and in forth section implementation.

COAP (Constraint Application Layer Protocol)

CoAP is standard application layer protocol, used for constraint node and constraint network. Constraint node is a small or tiny device having limited CPU memory, power resources [1].Constraint network has a high packet error rate, low throughput of Kbits and lack of advance services such as IP multitasking, for example, 6LoWPAN.6LoWPAN is IPv 6 Low power personal area network, it is the combination of IPV6 and Personal area Network, which allows tiny devices to transmit the information wirelessly using Internet Protocol. CoAP is standard protocol same as client server where the client sent the request message to sever and server response it according to the request. CoAP is similar to stop-and-wait mechanism also called Block Wise Transfer [2]. There are four types of the message used in CoAP: (1) Confirmable (2) Non-Confirmable (3) ACK (4) Reset. The Request can be Confirmable and Non-Confirmable. This protocol supports Public / Subscriber mechanism in which publisher can publishes message without any knowledge of subscriber.That message will be categorized into different channels. A subscriber subscribes the message base on their interest. Layer architecture of CoAP is shown in Figure 1.

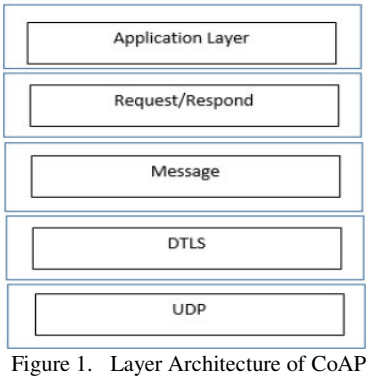

Figure 1. Layer Architecture of CoAP

DTLs (Datagram Transport Layer Security Protocol)

DTLs is one of the best transport layer protocol for user datagram. It is based on TLS, but TLS is used for connection oriented channel or reliable transport layer channels like web security or E-Mail.
The main two issue in TLS are

(1) TLs does not allow independent decryption of individual records. Because the integrity check depends on the sequence number and thus will fail.[3]
(2) The TLS handshake layer assumes that handshake messages are delivered reliably elseit will breakif those messages are lost [3].

Due to these two issues, we cannot apply TLS protocol for CoAP. So new protocol is developed by the researcher that is DTLs.DTLs only works for datagram protocol. For example, media streaming, internet telephony, online gaming application.
(A) Overview of DTLs

1. Packet Loss

   - DTLs use simple retransmission timer to handle packet loss.

   - The client will transmit "Hello" request to the server, start the timer and wait for a reply. If server message is lost or time is over than client will know that either hello message has been lost or verify request has been lost. The client has to retransmit the message.

2. Reordering

   - In DTLs, each handshake message is assigned a specific sequence number within that handshake only. When a peer receives a handshake message, it can quickly determine whether that is next message or not. If it is expected message then it will do further process. If the message is not expected message then it will push into the queue for future purpose.

3. Denial-of-Service

   - Two types of attacks occur in Datagram Security Protocol.

     (1) An attacker can consume excessive resources on the server by transmitting a series of handshake initiation requests.[3]

     (2) An attacker can use the server as an amplifier by sending connection initiation message with a forged source of the victim.[3]

   - DTLS solved attacks using stateless cookie techniques used by Photuris[3] and IKE[3] . The client sendsa hello message to the server. The server responds with "HelloVerify" message. This message contains a stateless cookie, which is generated by the technique of Photuris.The client retransmits"Hello" message with the cookie added. The server verifies the cookie and proceeds with the handshake only if it is valid.

Related Works

The internet of wireless things needs the power-efficient protocol, but existing protocol have typically been designed without power-efficiency. In [4] author used ContikiMAC protocol at radio duty cycle layer.Contiki/MAC is an efficient wake-up mechanism, which has 8 Hz wake-up frequency and 0.6% radio duty cycle [5].

Florian Junge introduced new security concept for Bootstrapping process [6]. They implemented security using shutter control mechanism, where sensor only communicates with the microcontroller. Microcontroller works as the heart for this mechanism. Because in Bootstrapping process nodes are vulnerable. Nodes do not have knowledge about the network and communication partners, so new nodes will be accidentally added to a neighbor network.

In [7] they developed one security framework for IoT "BlinkToSCoap".It is the combination of main three IoT protocol DTLS, CoAP, SiGLowPan.

Network Architecture

In Internet of Things, Reliability is an important factor. Erasure coding is standard practice for systems that store data reliably. For data reliability, the best coding technique is Reed-Solomon coding.It is an error correcting coding. It is able to detect and correct multiple symbols error. For Reed –Solomon coding simple, reliable and efficient java library is needed. Reed-Solomon code first divided the original file into six blocks during the encoding process, from which four equal blocks will be of original data and remaining two will be of theparity block. During decoding, the original file will be created using all six files. If any server will crash or file will be deleted by someone then, the original file will be reconstructed by reed Solomon code. Thus, reed Solomon code provides more reliability for IoT nodes.

In Figure: 1.2 IoT has 3 layers, where Reliability Layer is added on top ofthe upper layer of IoT.

(1) Application Layer: Standard CoAP protocol is used at the application layer. This layer provides communication between IoT nodes.

(2) Security Layer: Standard DTLs protocol is used at security layer. This layer provides secure communication between two nodes. In DTLs protocol mainly two types of process areoccurring.When data will betransferred from the client to server, thenfirstly data will be encodedand letter on it will be compressed by compression method. At the server side data will be first decompressed by compression method and then decoded.

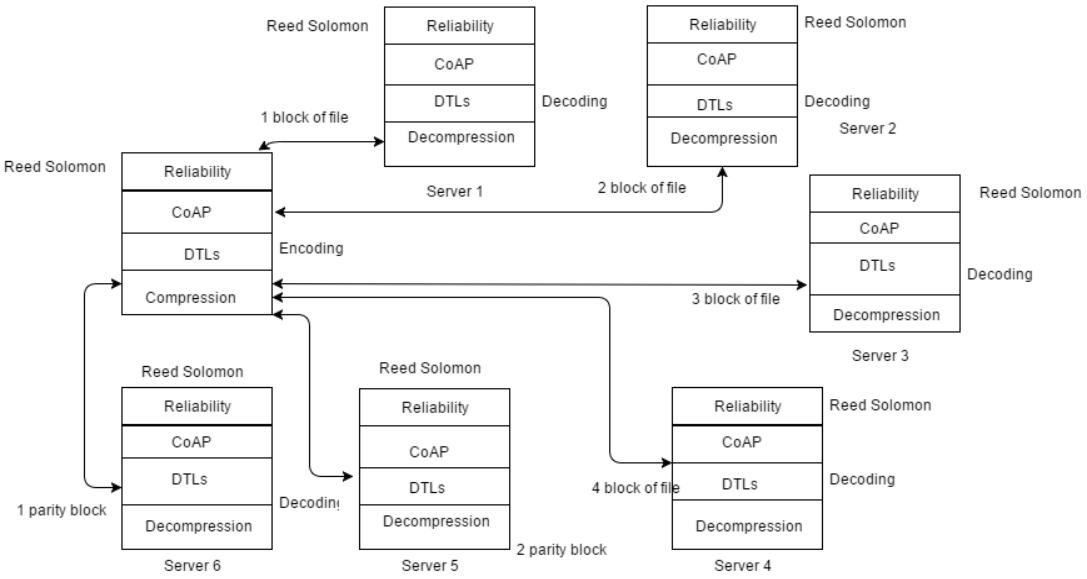

Figure 1.2 DTLs communication between one client and six server after adding reliability Layer on top of application layer of IoT

In Figure 1.2 one client communicates with six different servers. First, the one file will come through reliability layer. At reliability layer, Reed-Solomon will divide the original file into six different files. These six files will pass through the application layer. At the end, these files will pass through security layer. At security layer, each filewill be again encoded by encoding algorithm and then it will be compressed by compression method. After compressing the files the client sends these six different files to the different servers. First, four files are the equal division of original file, which will be sent to four different four servers (server1, server2, server3, server4). Remaining two files contain parity bits, which will be sent to server 5 and server 6 as shows in Figure 1.2.Each server receive the file and send "ACK" back to the client. At server side,each file will be decompressed by compression method and decoded at security layer. At reliability layer, file will be again decoded by Reed-Solomon code.

In future, one of the server will crash or files will be deleted at server side, then reed Solomon code will re-construct it using the parity bits. This thing increase reliability for IoT. In this architecture, only client and the server knows the communication process between them. No malicious node can interfere with communication. So, this model will increase the security in the network.

Results and Analysis

In Figure 1.2, architecture is implemented in Californium-Framework. Californium-Framework is open source project under Eclipse Technology. Californium provides an implementation of CoAP and is written in JAVA. Reed-Solomon also supports Californium-Framework environment. Figure 1.2 network is implemented using three compression techniques they are DEFAULT, LZ78,and LZ77.The performance of DEFAULT techniques is best as compare to LZ78 & LZ77 and performance of LZ78 is better than LZ77.

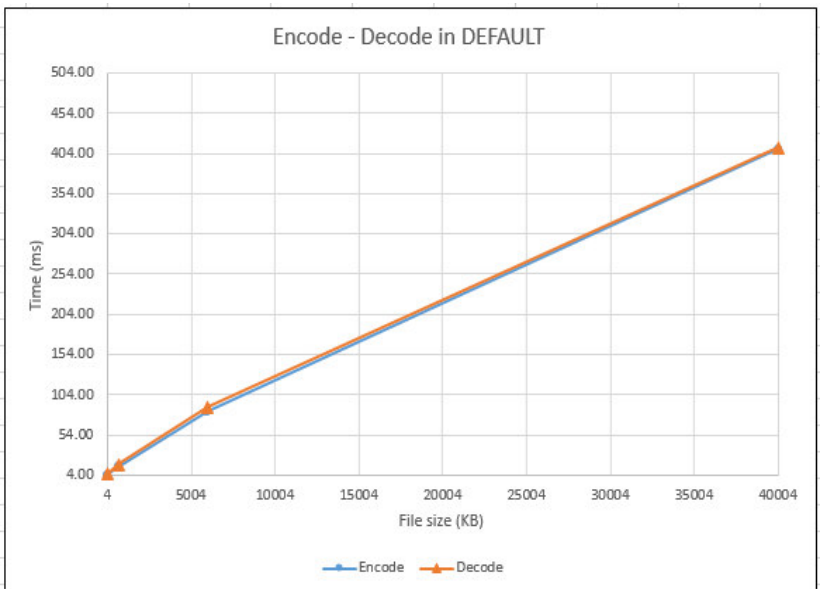

Figure 1.3 Encoding-Decoding using DEFAULT compression techniques in DTLs after sending 1 file.

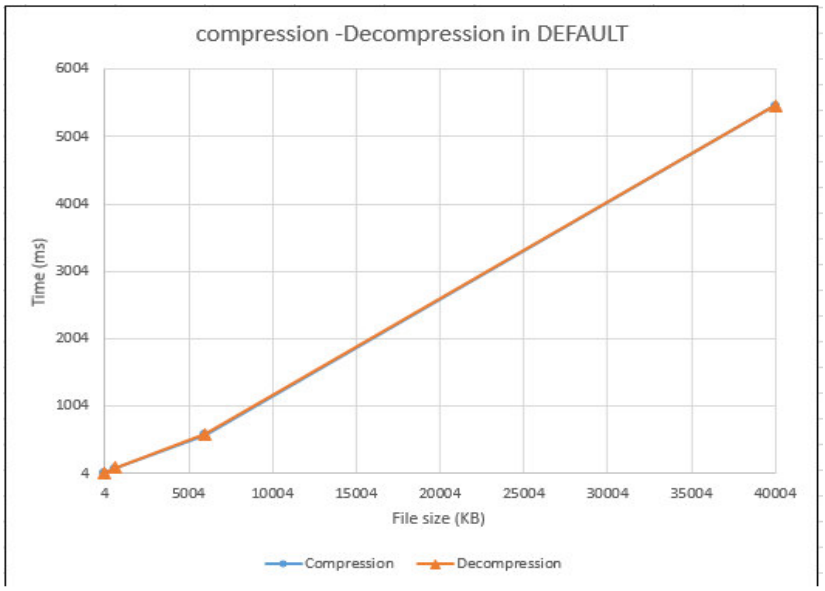

Figure 1.4 Compression-Decompression using DEFAULT compression techniques in DTLs after sending 1 file.

Figure 1.3 and Figure 1.4 shows filevs. Time graph of encoding - decoding and compression – decompression process for six different files (4kb, 660kb, 6000kb, and 40000kb).

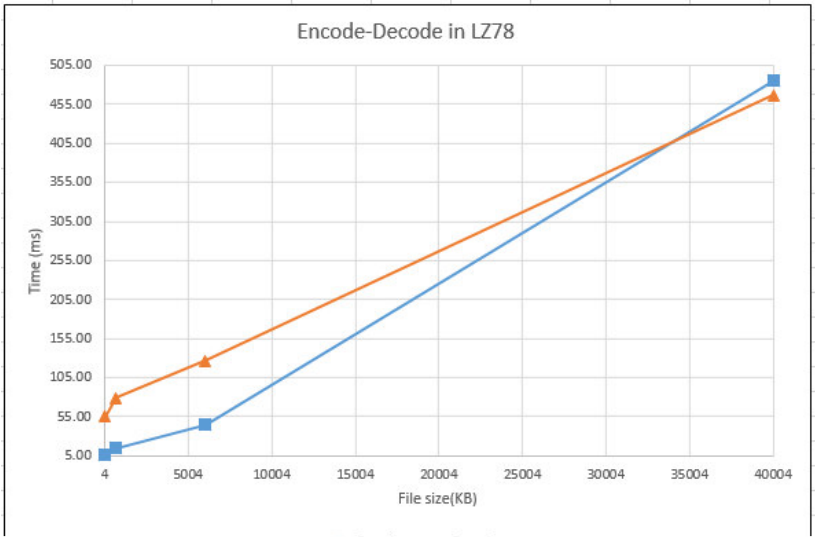

Figure 1.5 Encoding-Decoding using LZ78 compression techniques in DTLs after sending 1 file.

Figure 1.5 and Figure 1.6 shows the results of encoding – decoding and compression – decompression process using LZ78 algorithm. The LZ78 algorithm gives less performance as compare to DEFAULT but, gives better performance to LZ77. So, LZ78 requires more time to encode – decode and to compress-decompress the six files and then less time compared to LZ77.

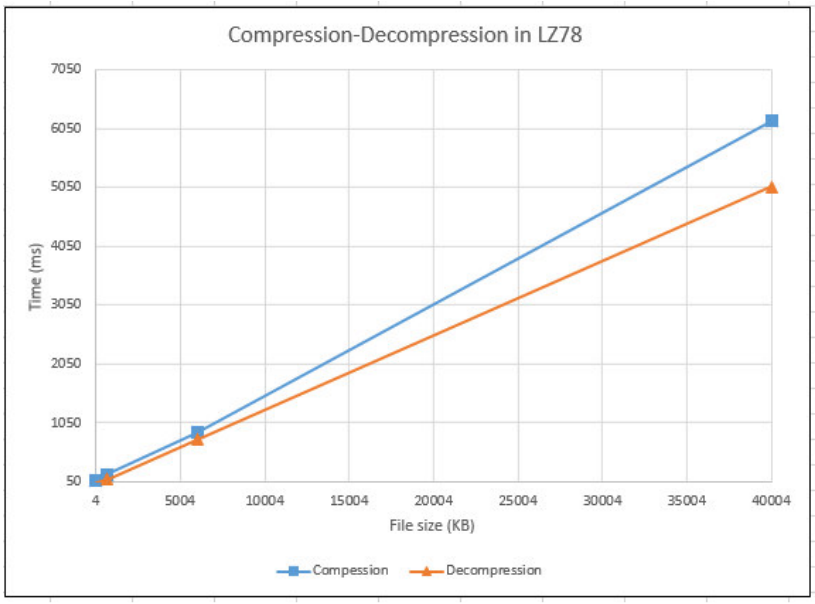

Figure 1.6 Compression-Decompression using LZ77 compression techniques in DTLs after sending 1 file.

Figure 1.7 and Figure 1.8 shows the results of encoding – decoding and compression – decompression process using LZ7 algorithm. The LZ77 algorithm gives less performance as compare to LZ78, so LZ77 required more time to encode – decode and to compress-decompress the six files.

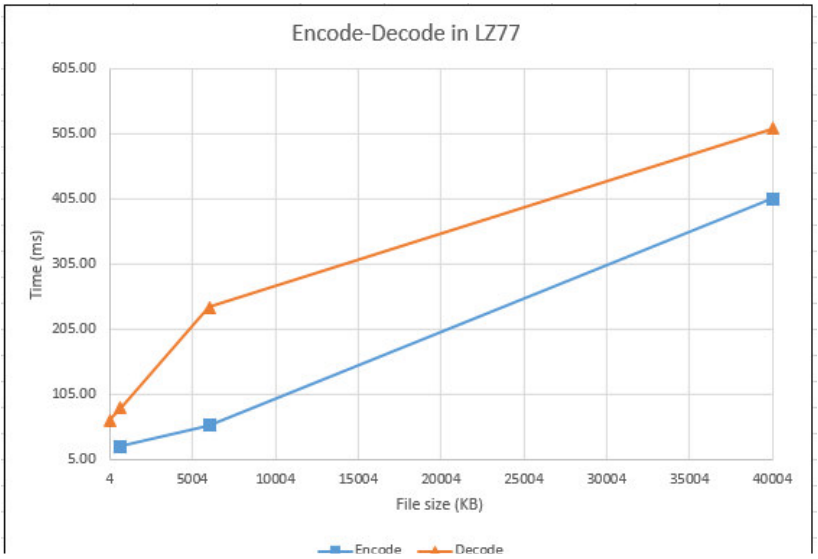

Figure 1.7 Encoding-Decoding using LZ77 compression techniques in DTLs after sending 1 file.

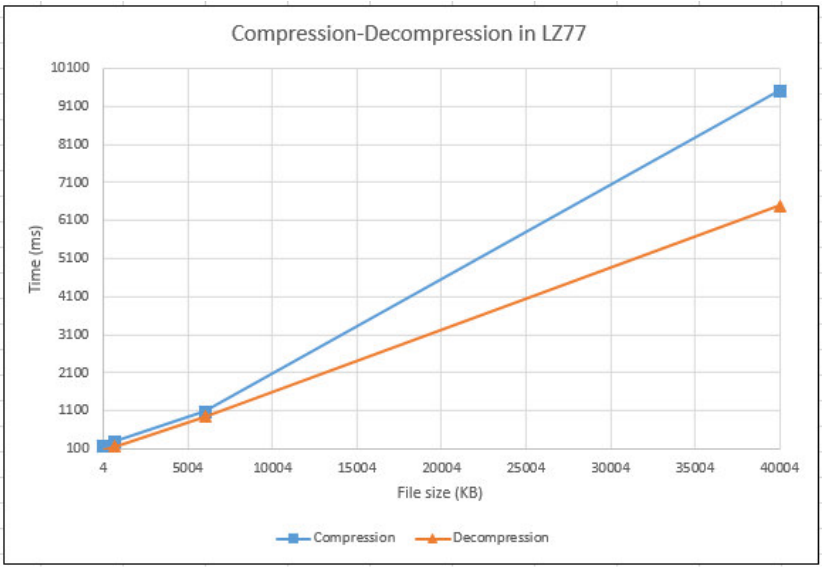

Figure 1.8 Compression-Decompression using LZ78 compression techniques in DTLs after sending 1 file.

Conclusion

With the help of Internet of Things helps one can monitor things likes fan, light, Ex. Sensor nodes are remotely connected tothe cloud and they send their data tothe cloud. At application layer, IoT uses CoAP protocol which is very useful for M2M communication. CoAP is basically used for constraining node. CoAP is designed reduced power consumption of IoT nodes. DTLs is used at security Layer, which provides secure communication. To improve the reliability of the network, Reed Solomon code is implemented on top of the IoT layer, which will increase the security during the communication between two IoT devices.

Future Work

Implementation of CoAP protocol allows us to docommunication betweenmachines to machine without any human interaction. Two IoT nodes are used for communication. For more reliability, Reed Solomon/CoAP model is created.In future, to improve more reliability six server nodes and one client node model may be implemented. So underlying network client sends the file to 6 different servers. Both,client and server, must implemente Reed-Solomon/CoAP. Reed-Solomon /CoAP model to reconstruct the original file if the file is deleted or server crash occur. To support this reliability across a dense network, torrent like indexing can be designed for this application which can help in locating the devices where the file or parity blocks may be stored.

References

[1]. Zach Shlby, Klaus Hatrke, and Carsten Bormann."The constrained application protocol(CoAP)". In: (2014).

[2]. C Bormann and Z Shelby. "Blockwise tranfers in COAP" . In: *draft-ietf-core-block-04 (work in progress)* (2011).

[3]. Eric rescorlaand Nagendra Modadugu. "Datagram transport layer security version 1.2". In: (2012).

[4]. Matthias Kovatsch, Simon Duquennoy, and Adam Dunkels."A low-power CoAP for Contiki". In: *Mobile Adhoc and Sensor Systems (MASS). 2011 IEEE 8th International Conference on.* IEEE. 2011,pp. 855-860.

[5]. Adam Dunkels et al. "The announcement ayer: Beacon coordination for the sensornet stack". In: *Wireless sensore networks*. Springer, 2011, pp. 211-226.

[6]. Olaf Bergmann et ai. "Secure bootstrapping of nodes in a CoAP netwrok". In: *Wireless Communications and Networking Conference Workshops (WCNCW), 2012 IEEE.* IEEE. 2012, pp. 220-225.

[7]. Giulio Peretti, Vishwas Lakkundi, and Michele Zorzi."BlinkToSCoAP: An End-to-End Security Framework for the Internet of Things". In: (2015).

[8]. J. W. Hui and D. E. Culler, "Ip is dead, long live ip for wireless sensor networks," in *Proceedings of the 6th ACM conference on Embedded network sensor systems,* pp.15-28, ACM, 2008.

[9]. J. Hui amd P. Thubert, "Compression format for ipv6 datagrams over ieee 802.15. 4-based networks," 2011.

[10]. S. Raza, D. Trabalza, and T. Voigt, "6lowpan compressed dtls for coap," in *Distributed Computig in Sensor Systems (DCOSS), 2012 IEEE 8th International Conference on,* pp. 287-289, IEEE, 2012.

[11]. M. Vucinic, B.Tourancheau, T. Watteyne, F. Rousseau, A. Duda, R. Guizzetti, and L. Damon, "Dtls performance in duty-cycled netwroks," in *Personal, Indoor, and Mobile Radio Communication(PIMRC), 2015 IEEE 26th Annual International Sumnosium on ,* pp. 1333-1338, IEEE, 2015.

[12]. T. Yashiro, S. Kobayashi, N. Koshizuka, and K. Sakamura, "An internet of things (iot) architecture for ambedded appliances," in *Humanitarian Technology Conference (R10-HTC), 2013 IEEE Region 10,* pp.314-319, IEEE, 2013.