I.J. Education and Management Engineering, **2017, 2, 20-29**
Published Online March 2017 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijeme.2017.02.03

Available online at http://www.mecs-press.net/ijeme

Protocols for Secure Internet of Things

Azka [a], S Revathi [b]

[a] *B S Abdur Rahman University, Vandalur, Chennai and 600048, India*
[b] *B S Abdur Rahman University, Vandalur, Chennai and 600048, India*

Abstract

Internet of Things has become a buzzword. It refers to networking of simplest mundane objects not just for human to machine or human to human interactions but for independent thing to thing interaction as well. Such interconnected or smart environment can do wonders but at the same time poses numerous threats to human lives. The ordinary and less powerful objects from day to day life are holding sensitive and private data from humans and trying to transport that through the insecure world of Internet. This new phase of Internet or Internet of Things (IoT) is yet in its infancy and does not have a security support mechanism of its own. The Internet and World Wide Web deal with interconnection of powerful devices like computers or smart phones and are well supported by standard Internet protocols ensuring optimum security and protection. The lightweight versions of the existing Internet protocols are backing the operations of IoT to a large extent but the security needs are not met completely as of yet. Many research organizations and individual researchers are working to make existing protocols and infrastructure applicable in IoT. This paper highlights the threats posed by uncontrolled proliferation of Internet of things and discusses major protocols that have been or that are being designed to overcome the security issues raised by Internet of things

Index Terms: Internet of Things (IoT), DTLS, COAP, IPSec, MQTT, SDN.

1. Introduction

The huge mobile network consisting of variety of smart devices has shrunk the world and indeed turned it into a global village. In next to no time new technology will wrap the world where ordinary devices with ubiquitous computing features and networking capabilities will become pervasive and make Internet of Things (IoT) a necessity. The Internet of Things is going to be the future of the Internet with all the usual things around us interacting with each other wirelessly, without our intervention, managing and coordinating their tasks, updating their firmware and making human lives easy. The Internet of Things does not just connect well equipped smart devices but appliances, automobiles, actuators, meters, sensors and numerous other things. This

Corresponding author. Tel.:
E-mail address:

extensive network of day to day objects represents the next generation of a hyper-connected world. The activities from kitchen and living room will be coordinated by microwaves, refrigerators or geysers communicating with clocks and door sensors. Inventory in factories will be managed by interactive machines and containers holding raw materials.

Such ecosystem where all animate and inanimate objects are interconnected leads to a global infrastructure relying on existing and evolving network communication protocols. Apropos object can be a thing, device or an entity embedded with necessary computational circuitry and equipped with limited storage and communication capabilities. The objects are of varying of capacities based on size and power (sensor, actuator, mobile phone, desktop, laptop, printer, car, fridge, oven, etc.). Such ecosystem where everything is connected generates a huge influx data and hence demands a massive well designed infrastructure. No doubt the Internet of Things (IoT) has been created with the purpose of improving quality of life, but this type of network in which people and things are interconnected in every aspect, sensitive and critical details about an individual are accessible to anyone via Internet. Internet of things is going to operate without boundaries and such uncontrolled network propagation is definitely going to raise issues related to verification and access control [2]. IoT are becoming very popular in every field and medical field is no exception; the patients are ready to implant actively connected things inside their bodies. Such wearable or eatable medical items are part of network of numerous devices operating from different locations. Such medical things have been created for improving health of the person but these can backfire and lay base for a fatal onslaught. The pervasiveness of Internet of Things and the craze of connecting one thing to every other thing in our lives are making an average person vulnerable to countless security threats. We are always applauded by a new technology and we work on the security concerns raised by it much later. In case of IoT the security measures cannot be delayed since this technology is not going to affect any material asset but it poses a direct threat to human lives if proper security measures are not enforced. The security issues raised by IoT are going to add to the already existing billion dollar industry working on Internet Security.

This paper is organized in five sections. The next section compares Internet of Things with the traditional Internet. The third and the fourth sections of the paper discuss the communication process in IoT devices and point out major protocols which are currently popular in the field of IoT.

2. Comparison between Internet and IoT

Internet has come a long way from ARPANET in 1960's with plenty of additional technologies like cognitive computing, cloud storage, file hosting systems, big data and others. Internet surfaced more than decades ago and took very less time to become the popular most technology of the world. The security challenges and the technologies to overcome those are evolving since the birth of internet. The standardization bodies like IETF, IEEE and W3C have been working in coordination to making Internet secure by standardizing many protocols [2]. The Internet of Things (IoT) is a dense network of interconnected items or things supporting different technologies. The IoT is constituted of variety of devices embedded with actuators, Radio Frequency Identification (RFID) tags, sensors or other similar miniature sensory chips.

All these communicating nodes in IoT vary in their capacity, performance, and size and working. Some of the devices in same IoT domain might be capable of carrying out complex operations while some may not be able to perform simple operations of their own [3]. Such devices also have limited capabilities when compared to high end devices seen in traditional Internet. The devices forming up IoT cannot be embedded with sophisticated circuitry or installed with software used in computers or smart devices of Internet and are hence termed as Constrained Nodes (CN). The operating system software used in conventional Internet devices and IoT also differ with respect to their processing power, memory requirements etc. With limited resources, computational power and available memory the IoT cannot afford to carry out communication the way computers or other smart devices are doing.

The security professionals are facing a big challenge in meshing the heterogeneous and constrained IoT devices with existing infrastructures and protocols. These need to be coordinated with conventional Internet

smoothly without any security compromise. The protocols currently operating at the physical level of interactive devices include proprietary non-IP solutions such as Bluetooth, IR, Zigbee, HART/ Wireless HART, Z-Wave, etc. These protocols work flawlessly only at a small scale and within a limited geographical area. Since IoT intends to connect the things at a large scale and covering a larger area, using IP-based solutions, hence IoT poses a risk of exposing ordinary things to the world of Internet and allowing them to interconnect with any other communicating node [4].

Currently the researchers are focused on adapting the standard IP protocols in the IoTs and this process has resulted in creation of many lightweight protocols suited for constrained devices of IoT. With the creation of IP equivalent protocols for the IoT, the IoT devices are able to communicate with other Internet devices both within their network and beyond that with lesser security threats. Making IoT devices as IP enabled can result in one huge giant technology in which Internet and IoT are combined together. Figure.1 depicts how Internet and Internet of Things are meshed together

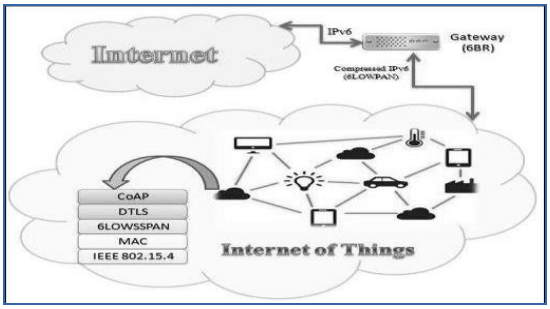

Fig.1. Internet and IoT interoperability

Nevertheless IPv6 address space of up to 3.4×1038 will accommodate as many as 4,000 addresses for every individual of the world; the added functionalities like automatic address configuration are also going to make scalability easier. In the process of securing IoT and making it compatible with Internet, IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) [5], Routing Over Low-power and Lossy networks (RPL) [6], Datagram Transport Layer Security (DTLS) [7], Constrained Application Protocol (CoAP) [8] have surfaced as approved lightweight variants to IPv6, IP Routing Protocols, TLS and HTTP respectively [9]. Such variants are making constrained IoT devices capable of using IPv6 and creating a smooth communication process between IoT and Internet domains. The devices in domain of IoT are connected to the services and devices in outside network through a gateway. An IP enabled scenario is put to practice for communication between the devices of different capacity working in different domains [10]. In spite of these standard protocol adaptations some security concerns still persist owing to large number of heterogeneous devices and limited resource availability of IoT.

3. Threats in IoT

The concept of security and protection covers variety of different areas. It aims at providing of security services that ensure confidentiality, integration, authentication, authorization, availability and non-repudiation. In traditional Internet, such security services are provided by methods of cryptography and require a complete key management mechanism.

In the context of the IoT, however, security is a major concern of current times. There are no well established security mechanisms for IoT yet and is vulnerable to countless attacks. In the context of the IoT, however, security is a major concern of current times. There are no well established security mechanisms for IoT yet and is vulnerable to countless attacks.

Since a huge number of addresses are required in IoT, IPv6 is the best possible option for addressing such

devices. Lighter version of IPv6 i.e. 6LoWPAN is preferred for IoT and it is vulnerable to the same set of attacks as IPv6, such as, IP spoofing, fragmentation attacks, reconnaissance, packet sniffing, neighbor discovery attacks, DDos attacks, rogue devices, man-in-the-middle attacks, and others. IoT joins the physical world with the digital world and hence increases the attack surface considerably [11]. The IoT has threat from various categories of attacks, some of which have been highlighted in Table 1: Solutions to these security threats are also suggested.

Table 1. Attacks on IoT Based on Different Component

Components Compromised	Attack Type	Protection Strategy
Attacks on data	Data leakage, loss/theft, authentication, sovereignty.	Secure communication, protection of stored data and securely shutting off the devices.
Attacks on availability	DDoS, Man in the middle.	Intrusion detection, monitoring of traffic and event reporting.
Attacks based on poor architecture	Wormhole attack, sinkhole attack, Selective forwarding attack, Witch attack	Tested trust model for IoT devices, communicating with other known, trusted entities.
Attacks on terminals	False User Identity Module (UIM), Script kiddies, Virus, Trapdoor.	Secure setup, configuration and booting of end devices.
Attacks on storage	Illegal Alteration , Disclosure of sensitive data	Proper authentication for data-in-rest, Firewalls

4. Secure Communication Process in IoT

Internet is also known as global network and it attained world wide popularity in lesser time period. Considering the security perspective of Internet, the security protocols and standards for carrying out sensitive and private activities online are rigorously reviewed and tested. The layer by layer security approach provided by TCP/IP forms the base of secure foundation of the Internet. Several other protocols like WAP and Wireles33s Transport Layer Security (WTLS) were created to enhance security features for mobile networks but they failed to make their place due to their shortcomings like WTLS did not ensure end-to-end security and all the date being transmitted was transparent to WAP gateway.

In contemporary times the protocols and technologies like HTTPS, SSL/TLS, IPSec, IDPS and Firewalls are making the online activities secure. A similar approach with comparable security technologies is need of hour for implementation of IoT in our lives.

Standardization groups as IEEE are working towards security issues of IoT and are in process of developing standards. Some of IEEE standards addressing security elements of traditional Internet are applicable to IoT as well. IEEE P1363 enables Asymmetric-Key cryptography, IEEE P1619 encrypts data on permanent and removable storage devices, IEEE P2600, resolves security concern of peripherals and IEEE 802.1AE and IEEE 802.1X ensure security in Media Access Control (MAC) [12]. Such standards have started resolving various security concerns of IoT but it will be naive to think that a standard will remove all cyber-attacks against IoT devices anytime soon. End users can rely on the devices that are standardized for provision of a required level of security and protection.

The development of smaller versions Internet protocols is underway for ensuring end to end security in the constrained IoT devices. Symmetric key algorithms or raw public key algorithms are most used in development of such variants because of their less memory requirements and lesser complexity. In fact many of the newly developed IoT specific standards presume that the keying material is fitted into the device during its manufacture and configuration. Although the symmetric keys would continue to be preferred because of their ease of implementation, researchers are also arguing that using certificates in lightweight security solutions can solve numerous issues where other methods have failed. The certificate based system has been regularized for security in World Wide Web and other related systems. Commonly used web browsers are pre configured with certificates. So if it becomes possible to enable the certificate based systems like X.509 on IoTs, huge amount

of effort and cost would be saved by making use of existing certificate infrastructure. The raw key algorithms can be replaced by public key infrastructure (PKI) and the compromised devices can be removed from the network by enabling certificate revocation list (CRL) feature on the certificate based system. This could be next step towards a more secure IoT ecosystem. However hurdles can be foreseen in implementing a full- fledged certificate system since IoT are limited by low processer power and available memory. The lightweight versions of protocols created for IoT have been highlighted in Table 2.

The working and coordination of IoT protocols and TCP/IP is shown in the following diagram. Figure 2.

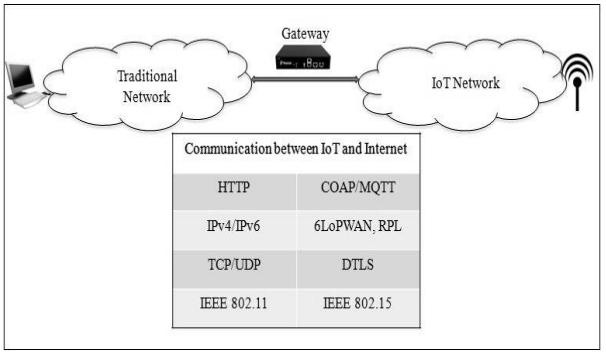

Fig.2. Layer wise Communication Process in IoT

As depicted in the Figure 1, the IoT network follows the set of protocols which are actually the lighter version of the Internet protocols. In order to communicate with the unconstrained devices the constrained devices takes services from a gateway. The gateway coordinates IoT and Internet communication by resolving IoT protocols to the corresponding Internet protocols. The mapping of TCP/IP layers from Internet of Things to Internet is depicted in following table. Table.2

Table 2. IoT Protocols and Corresponding Internet Protocols

TCP/IP Layers	**Protocols**	
	Internet Version	IoT Version
Physical Layer/ Data Link Layer	Ethernet, Wireless	IEEE 802.15.4 (ZigBee, Bluetooth, Wireless Hart)
Network Layer	IPv4, IPv6	6LoWPAN, RPL
Transport Layer	UDP, TCP	DTLS, UDP
Application Layer	HTTP, FTP, SMTP.	COAP, MQTT

The protocols for physical layer in Internet are Ethernet and Wireless while as for IoT the physical layer protocols like ZigBee, Bluetooth etc come under IEEE 802.15.4 standard. Likewise for network layer IoT has protocols like 6LoWPAN, *Routing Protocol* for Low power and Lossy Networks (RPL).

4.1. DTLS for Constrained Devices

The Datagram Transport Layer Security (DTLS) is a protocol devised for security of datagram communication approach in Internet. It was developed to meet security goals for unreliable packet delivery across the nodes in a network. Transport layer Security (TLS) is the base protocol for DTLS and both have same security features except that underlying protocol for TLS is Transport Control Protocol (TCP) and for DTLS it is User Datagram Protocol (UDP). The delays related to reliable protocols are not seen in DTLS but fragmentation and packet reassembly can create problems in DTLS approach if the packet length is not

managed. The DTLS works as a series of protocols starting with The Record protocol which keeps message limits by incrementing a unique sequence number for every sent message [13]. So in case the incoming message does not have the intended sequence number the connection is withdrawn. Next is the Handshake protocol of DTLS which is required for connection establishment and negotiation of the security parameters to be used in the session cryptographic and hashing algorithms, encoding or compression mechanism. The handshake is initiated by client and it sends a Hello message to the server. The Hello message contains the security parameters which Client can support and a random number. If some error occurs in the handshake process, necessary warnings and notifications are generated with the help of alert protocol [14].

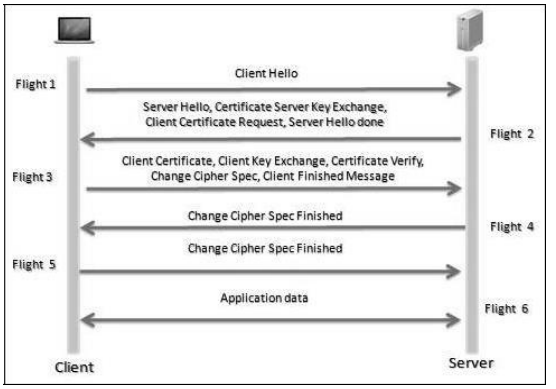

Fig.3. DTLS Handshake Protocols.

By reducing the handshake overhead in DTLS, certificate based DTLS can prove to be a successful mechanism for authentication in Web of Things. Ren é Hummen et al have proposed three methods to improve the DTLS handshakes and hence make them eligible for handling certificate based authentication [7]. Three design based methods have been proposed to reduce overheads caused by certificates in DTLS handshake. The first method checks for validation at the gateway which has been configured beforehand. Secondly the session's resumption method as an improvement for overheads and lastly a mechanism is proposed according to which the device owner performs the DTLS handshake on behalf of devices which have limited resources for certificate handling.

Thomas Kothmayr et al have proposed DTLS method to provide confidentiality, integrity and authentication for Web of Things with 2-way authentication. X.509 certificate based 2048-bit RSA public key infrastructure is used for full authentication during DTLS handshake. The memory requirement in the proposed method is within the available ROM/RAM of ordinary motes and the energy consumptions are also less approx 490 mJ. The ability to implement certificate based PKI and end to end secure authentication make DTLS a feasible security solution for the upcoming network miniature devices [15]. The above approach is suitable solution for IoTs except that implementation uses TinyOS which doesn't support real time processing and multi threading and it relies on hardware for storage of keys and their computation. Accommodating the same approach on a better operating system like Contiki can resolve the stated issue.

Table 3. DTLS Header Compressions [20]

Header	No	Compression	Overhead
	Compression		Saved
Record	104	40	62%
Handshake	96	24	75%
ClientHello	336	264	23%
ServerHello	304	264	14%

DTLS is most preferred choice for IoT devices and much work has been done to make DTLS suitable for devices with limited memory and processing capability. DTLS has been able to protect the unicast traffic of application layer. Multicasting is an important feature in IoT applications as it can support communication in a group of devices, so it would be an advantage if DTLS protects multicast traffic as well.

4.2. IPSEC for IoT

IPv6 comes with many added benefits when compared to Ipv4 and IPSec is one of them. IPSec is inherent in IPv6 and provides complete end to end security unlike IEEE 802.4.16 which provides hop to hop security. IPSec does not only provide confidentiality and message integrity but it also includes efficient key exchange mechanism and authentication by making use of the Authentication Header (AH) and Encapsulating Security Protocol (ESP) protocols. IPSec has been created for authenticating the nodes communicating with each other as well as for encrypting the packets exchanged between them. In contrast to transport layer security protocols that require application layer for implementation, IPSec works at network layer and makes security transparent to above layers [16]. Most of the IoT applications demand secure and safe data transfer between the things or from nodes to servers. The data captured by a health device connected to patient should travel securely through the network since the any compromise to integrity can prove fatal for the patient. Extending the IPSec features to 6LowPAN can enable the authentication and encryption in constrained devices in addition to relieving the burden of proxies and gateways between Internet and IoT domain. Implementing IPSec in IoT raises many concerns like packet overhead and cost of sending. So the original version of IPSec cannot be used in devices with limited capability. In this process of rendering IPSec services in low power devices some work has been done and lightweight variants for underlying IPSec protocols have been drafted. Two different modes i.e. tunnel mode and transport mode are supported by IPSec. The transport mode is preferred in case of 6LoWPAN since tunnel mode places a new header on the packet and hence adds to the overhead.

Raza et al have come up with a compressed lightweight IPSec design that acts as a replacement of IPSec for 6LoWPAN. The proposed variant provides both authentication of the nodes and the encryption of messaged by including both AH and ESP [17]. In IPSec protocol ESP extension produces encrypted packet from the clear message. Robust Header Compression (ROHC) compresses the overhead of the overhead of IP, UDP or Ipv6 of 40 to 60 bytes into 1 to 3 bytes with the help of compressor and a decompressor placed before and after that data transfer link respectively. Such compression mechanism which requires compression and decompression mechanism in the devices can prove to be complex to be implemented in IoT. In [18] T.Guggemos has suggested an ESP protocol for IoT devices called Diet-ESP. Diet-ESP provides the encryption of data and uses ROHC's U(Unidirectional) mode of operation. It can be said that Diet-ESP implements a plain and simplified ROHC framework without the need of whole framework.

Many other network layer solutions have also been provided which provide security at different layers to improve security IoT. For example a network layer approach using a SaaS mechanism can prove to be better because it does not require changing the entire communication protocols or mechanism. A database is maintained in the cloud to store the regulations for security to be implemented in IoT. This database is updatable in case some new weakness or vulnerability arises. The suggested method is quite naive when compared to the security models proposed for IoT so far and can prove to be a good security mechanism for IoT owing to its end to end security and simple API for query management.

4.3. Constrained Application Protocol (COAP)

An application layer protocol for resource constrained devices has been devised by the The Constrained RESTful Environments (CoRE) working group of the IETF. The protocol is known as Constrained Application Protocol (CoAP) and works the same way as HyperText Transfer Protocol (HTTP) works for application layer of traditional Internet. In CoAP the Uniform Resource Identifier (URI) is used to locate the host. As compared to HTTP, CoAP is simpler and has both reliable and unreliable forms of communication [19].

HTTP has all the features which are best suited for IoT but this protocol is based on TCP and hence too complex for constrained devices. In contrast to HTTP, CoAP is UDP based and implements Representation State Transfer (REST) architecture. In order to make communication reliable it employs retransmission mechanism. CoAP reduces the length to the datagram packet for reliable communications with minimum available resources. As in case of traditional Internet we make HTTP secure by using TLS(Transport layer Security) in the underlying layer, likewise when we use DTLS(Datagram Transport layer Security) in underlying layers of IoT devices CoAP will be secure.

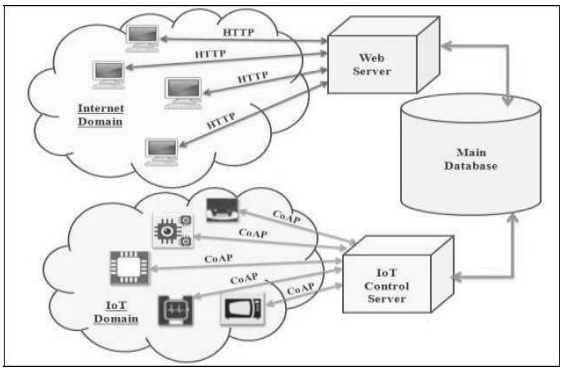

Fig.4. Interoperability of HTTP and CoAP for a Smart IoT Based Ecosystem.

CoAP is going to be mandatory application layer protocol for IoT devices. As already mentioned the underlying protocol for CoAP is DTLS, so the reductions of DTLS overhead is going to make CoAP implementation easier and promising. To this end authors in [20] have proposed reduction of DTLS overhead by compressing 6LoWPAN header. The DTLS header compression mechanism has also been presented for CoAP overhead reduction. The Header compression in DTLS avoids fragmentation and reassembly and hence makes it suitable for IoT environment. As HTTP and TLS after combining form HTTPS, similarly CoAP when combined with DTLS becomes CoAPS (Secure CoAP) or secure CoAP

4.4. Message Queuing Telemetry Transport (MQTT)

One more protocol that is gaining popularity for use in IoT is MQTT. It stands for Message Queuing Telemetry Transport (MQTT). It is a simple protocol that suits networks which are not reliable and have lesser bandwidth. MQTT is an open standard protocol built to meet the requirements of the devices with limited resources and is hence best suited for IoTs. It follows general client/server architecture with each sensor device as a client and server is known as broker in MQTT [21]. The message sending procedure is somewhat different in MQTT; the messages are separate blocks of data not known to the server /broker. Each message is sent to an address known as topic in MQTT. One client can be subscribed to one or many addresses or topics. In MQTT the topics are arranged in a top down fashion following a hierarchy. Privacy and confidentiality is maintained by username/ password authentication and SSL/TLS encryption respectively. In spite of such a promising usage in IoT, it has some limitations like each client has to support TCP. Also the addressing scheme for topics requires long names which are difficult to be used in constrained devices.

5. Conclusion

Ensuring all the security goals in Internet of things is indepensable now since IoTs are commonplace. In this paper we have highlighted many lightweight security protocols that are in process of being standardized for

Internet of Things. We also noted that DTLS is most preferred protocol for IoTs and forms base for the protocols pertaining to various layers of IoT communication. The symmetric approach is being replaced by lightweight versions of public key cryptography. We reviewed the IPSec protocol and its implementation progress in IoT devices. Several lighter versions of IPSec are ready to be used in IoTs and have been accepted as standards as well. The lightweight version of HTTP known as CoAP is the default application layer protocol for constrained devices and has been acclaimed for its services.

References

[1] R. Roman, J. Zhou, J. Lopez, "On the features and challenges of security and privacy in distributed internet of things", Computer Networks, Elsevier Vol. 57, pp. 2266–2279, 2014

[2] Sye Loong Keoh, Sandeep S. Kumar, and Hannes Tschofenig, "Securing the Internet of Things: A Standardization Perspective," *IEEE Internet of Things Journal*, vol. 1, no. 3, pp. 265-275, June 2014.

[3] Kim Thuat Nguyen, Maryline Laurent, Nouha Oualha, "Survey on secure communication protocols for the Internetof Things," Ad Hoc Networks Journal, vol. 32, pp. 17–31, 2015.

[4] Chakib Bekara, "Security Issues and Challenges for the IoT-based Smart Grid," Procedia Computer Science, vol. 34, pp.532 – 537, 2014

[5] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals," RFC 4919, Aug. 2007.

[6] T. Winter et al., "RPL: IPv6 routing protocol for low-power and lossynetworks," RFC 6550 (Proposed Standard), Mar. 2012.

[7] Z. Shelby, K. Hartke, and C. Bormann, "Constrained application protocol (CoAP)," draft-ietf-core-coap-18, IETF, 2013.

[8] René Hummen, Jan H. Ziegeldorf, Hossein Shafagh, Shahid Raza, Klaus Wehrle," Towards Viable Certificate-based Authenticationfor the Internet of Things," ACM 978-1-4503-2003, April 19, 2013

[9] Tobias Heer, Oscar Garcia-Morchon, René Hummen, Sye Loong Keoh, Sandeep S. Kumar, Klaus Wehrle, "Security Challenges in the IP-based Internet of Things," Wireless Pers Commun Journal, vol. 61, pp.527–542, 2011

[10] Z. Shelby, K. Hartke, and C. Bormann, "Constrained application protocol (CoAP)," draft-ietf-core-coap-18, IETF, 2013.

[11] http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html.

[12] http://www.standardsuniversity.org/e-magazine/march-2016/iot-security-news-and-further-reading/

[13] http://www.standardsuniversity.org/e-magazine/march-2016/iot-security-standards-paving-the-way-for-customer-confidence/

[14] Mukul Panwar, Ajay Kumar, "Security for IoT An effective DTLS with public certificates," IEEE-ICACEA, pp-163-166, March 2015.

[15] https://tools.ietf.org/html/rfc4347

[16] Thomas Kothmayr, Corinna Schmitt, Wen Hu, Michael Brünig, Georg Carle, "DTLS based security and two-way authentication for the Internet of Things," Ad Hoc Networks Journal vol. 11, pp. 2710–2723, 2013.

[17] https://tools.ietf.org/html/rfc4301

[18] Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, Dechao Qiu,"Security of the Internet of Things: perspectives and challenges" Wireless Networks, Springer, Vol-20,Issue-8, pp 2481-2501, November 2014.

[19] IETF, "Diet-IPsec (IPSECME) WG,"2014.

[20] http://www.cse.wustl.edu/~jain/cse574-14/ftp/coap

[21] Shahid Raza, Hossein Shafagh, Kasun Hewage, René Hummen, and Thiemo Voigt, "Lithe: Lightweight Secure CoAP for the Internet of Things," IEEE Sensors Journal, VOL. 13, NO. 10, pp. 3711- 3720,

October 2013.
[22] Jongmoon Park, Myung-Joon Lee, "A Smart Context Distribution Framework Based on a Messaging Service for the Internet of Things", Journal of Applied Mathematics, Hindawi, Vol-2014, Article ID 271817, 2014.

Authors' Profiles

Azka (born June 8, 1989) is a Research Scholar in B S Abdur Rahman University Vandalur, Chennai -600048, India. Her field of interest is Networks and Security and she is pursuing research in security of Internet of Things.

Dr. S. Revathi is an Associate Professor in B S Abdur Rahman University Vandalur, Chennai - 600048, India. She is taking courses like IoT, Network Security for the students Computer Science. Her field of interest is Networks and Security and Cryptography.

How to cite this paper: Azka, S Revathi,"Protocols for Secure Internet of Things", International Journal of Education and Management Engineering(IJEME), Vol.7, No.2, pp.20-29, 2017.DOI: 10.5815/ijeme.2017.02.03