International Journal of Engineering & Technology, 7 (2.7) (2018) 77-83

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Strategies to handle heterogeneity prevalent within an IOT based network

T. Pavithra[1]*, J. K. R. Sastry [2]

[1]Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, AP, India-522502
[2] Department of ECSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, AP, India-522502
**Corresponding author E-mail: 999pavi000@kluniversity.in*

Abstract

One of the most important features of an IOT network is heterogeneity among the devices, subnets, communication systems, data storage and retrieval. IOT can be conceived to be in existence in hierarchal structure having situated in many layers. In each of the layer there is an element of heterogeneity. The heterogeneity is more severe in the layer which deals with real connect and communication.
In this paper different strategies are explored for handling heterogeneity among communication protocols that are used for effecting communication among devices, cluster of devices and the alike

Keywords*: IOT; Communications Systems; Heterogeneity; Protocols*

1. Introduction

Internet of things (IOT) is the most ought technologies these days. IOT has come into force due to invention small and powerful device, mobile communication, wireless communication, Micro computing, machine to machine communication etc. there have been many applications that needs establishment of an IOT. The applications are quite diverse and of the application include home automation, space navigation, atmospheric management etc. Billons of $s are being spent of the development and implementation of IOT based networks [Gartner 15].
IOT networks are built using small devices that are not computers, high computing platforms and many networking systems that must use internet as one of the means for communication for making the information flow to remote storage system such as cloud computing.
The devices on IOT are expected to be smart, self-configurable, and dynamic and act intelligently. The devices on IOT are expected to communicate and collaborate with each other so that quick implementations / decisions can be taken to save a critical situation. The devices on the network more active compared to the devices on conventional network. Many technologies are in use when it comes to IOT which generally include ubiquitous communication, light communication, use of internet protocols. Use of these technologies together makes IOT more versatile for use to develop different types of applications
Effecting communication among the IOT devices is a challenge. The need for standards and appropriate communication protocols needs not be emphasized. The most difficult thing is the ability to establish communications among the devices that follow different communication standards and protocols.

Different communication happens across various layers of IOT networks. The most important layer is the interconnect layer in which the hardware devices gets connected. At each of the interconnect a communication standard is followed which defines various kinds of layers that include MAC, Network and session layer. Many organizations (IEEE, IETF, and ITU) have released standards that should be used for implementing protocols that can be used in different layers of the standards. Many protocols are released that work in the same layer. The standard used for developing protocol greatly varies. Therefore protocol conversions would become necessary when devices with different protocols even in the same layer needs to communicate with each other. This paper thus concentrates on the protocol conversion and the strategy for achieving the same.

2. Literature survey

With a high prominence on IoT applications of how academics and companies of all kinds are leveraging wireless sensors, connectivity platforms and data to change the course of evolution and create new strategic opportunities to improve the lives of people all over the world. With the constant evolution of new technology in mobile broadband, Micro computing, Machine to Machine communication etc., have contributed to the development of IOT. According to the Hype-cycle of Gartner [17], IOT stands at the top of the cycle, which conveys that large amount of industrial funds, are invested over IOT. A much more raise of funds in IOT industry is expected over the coming years, which implies the importance of IOT across variable domains.
A number of protocols and topologies handle different phases of standardizing IOT as detailed by Tara Salman [3]. All the wireless sensors are integrated together with the help of certain standards and incorporated to a network. One of which is IETF (Internet Engineering Task Force), a protocol suite for accessing applications and services for WSN's proposed by Sheng [14]. In this IP-based internet dominated network world, several security issues will arise leading to the development of security protocols in order to enable the seamless connectivity of devices. Granjal [8] proposed a survey on existing security protocols and their characteristics along with the strategies and open challenges.

Any communication protocol follows certain standards in layers. These layers are discussed in detail in various papers by different authors, including the protocols used with respect to each layer and the type of network involved in the communication. Karagiannis [18] and K. Malar [10] discussed on application layer protocols, thrashing out few standard protocols based on reliability, security and energy consumption aspects. A detailed insight of IOT technologies and protocols are proposed by Fuqaha [7] and X. Che [2]. Different aspects of IOT relating to the trends involving protocols and enabling technologies which finally constitute to improve the quality of life are discussed.

Detailed explanation to physical and MAC layer features are discussed by M. Park [11]. With the advent of technology, more and more use cases are being used for different digital devices like mobiles, laptops, digital TV's, tablets supporting higher throughput and high data rates. IEEE 802.11ah with a support of wide range of applications are proposed with PHY parameters and MAC protocols with low frame overhead and low power consumption, for optimization of sensors and IOT applications. This IEEE802.11ah standard discussed by M. Park [11] consists of the following features: Synchronization frame, efficient bidirectional packet exchange, Short MAC frame, Null data packet, Increase sleep time.

The protocol used in data link layer is Wireless HART was proposed by A. Kim [19], operating on the top of PHY layer adopting TDMA in MAC layer. It offers reliability of data which is encrypted and transmitted to ensure the security of data. Wireless HART architecture consists of the following features: Network manager, security manager, a gateway as a medium between wireless and wired network, field devices, access points, routers and adapters. With the use of these characteristics, peer to peer security mechanisms are employed to secure the data from source to destination. For more emphasis on security, a novel solution is developed by S. Raza [13] which integrates Wireless HART at the network level rather at the device level.

Other protocols used in data link layer like Bluetooth low energy is discussed by C. Gomez[20] and J. Decuir[21], in which BLE is widely used for low range transmission and monitoring. Various parameters involving BLE are discussed which contribute to low latency and fast communication. Basically Bluetooth smart is a protocol used for communication between PHY and MAC layers. It follows master slave architecture supporting two types of frames: 1. Advertising frame 2. Data frames. Dedicated lines are used for advertising the channel with the use of slave devices and the connection is established once the master node senses the slave device. After the connection is established, master node specifies the scheduling sequence and waking cycle to the slave. The advantage of using Bluetooth low energy is that, nodes will be awake only when they are communicating and once the communication is complete, they go to sleep mode in order to save power.

Zigbee smart energy is a long range communication protocol supporting low data rates with low power consumption used in data link layer. It supports full mesh network including the following features: high security, scalability and efficient performance.

Another communication protocol that operates in data link layer for supporting IOT requirements is DASH7. As per O.Cetinkaya [5] due to the limited energy resources, the need for energy conservation has become compulsory and to achieve it DASH7 is introduced which implements a better architecture compared to Zigbee to reduce the limitations of power applications. In this master slave architecture, many features are supported which includes: Filtering, Addressing, and Frame formats. Other protocols like, Home plug, LTE-A, G.9959 are used. An approach for Machine to Machine communication through LTE-A protocol is discussed by M. Hasan [9] which supports IOT applications in cellular networks. It is highly scalable, low cost protocol which uses orthogonal frequency division multi access to communicate with MAC layer.

LoRaWAN is another communication protocol for low power and low cost networks. It supports high scalability, low power and bidirectional with an energy harvesting scheme to enable future needs of IOT applications. Another such communication protocol which enables low power and low cost communication is Weightless, developed by I. Poole [22] and designed for ultra-narrow frequency band.

S.Bush [23] discussed on DECT, a Universal European standard for cordless phones to enhance the support over congestion and interference by the use of a dedicated channel. In the improvised version of DECT i.e., DECT/ULE, both Frequency division multiple access and Time division multiple access are used.

A number of protocols are available for Network layer depending on whether it is used for routing purpose or for encapsulation purpose. Routing Protocol for low power and lossy networks is widely used for network layer routing. The extension for RPL protocol is CORPL (cognitive RPL) explained by A. Aijaz [4] and Xiaoni Wang [1] designed for cognitive networks with an efficient forwarding mechanism between the nodes. For the practical realization of IOT, machine to machine communication should be efficiently organized with the support of cognitive radio technology which plays a crucial role in today's radio technology.

Another such network layer routing protocol is Channel-Aware Routing Protocol (CARP), detailed in Z.Zhou [15] which effectively works for underwater communication. Due to its light weight packet feature, IOT applications uses CARP considering the link quality. The disadvantage of using CARP is, it doesn't allow the data to be reused. To overcome this, E-CARP is developed which allows sink node to save the previous sensory data. By this the reusability can be improved and the packet overhead can be reduced exponentially.

For securing the data, Network layer encapsulation protocols are used. There are several protocols covered under this category. 6LoWPAN is commonly used protocol that efficiently encapsulates the data into small packets. The header length should not exceed 128 bytes and is provided with compression techniques to reduce transmission overhead. Along with this there are other protocols like 6TiSCH proposed by D.Dujovne [6], which uses slotted channel hoping method; thereby the problem of interference can be avoided as the operations to be performed are scheduled in time-slots.

The other protocols covered in this network encapsulation layer are: 6Lo for the networks of resource constrained node, G9959 protocol covering higher layer security mechanism. These protocol standards still pose the limitation of interoperability due to the high level of diversity in protocols. However, most of the IOT applications are implemented in interoperable standard with the help of session layer protocols. Some of these protocols are discussed here.

V. Karagiannis [18] and D.Locke [24] suggested that MQTT protocol is well suited for IOT keeping in mind the issues related to reliability, security and energy consumption. It provides one to many communications and reduced packet overhead. The major concern of IOT applications is security of devices which the available protocols are unable to satisfy. To address this problem, a new protocol is developed by M. Singh [16] as an extension of MQTT which is called secure version of MQTT (SMQTT). In this protocol, one message is encrypted and is published to several other nodes which are made possible using broadcast encryption method.

Another session layer protocol to achieve significant packet overhead and low power consumption is through Constrained Application Protocol (CoAP) discussed by V. Karagiannis [18]. This protocol helps in usage of RESTful (Representation State Transfer) services to meet the power limitations and to interface with standard HTTP protocol.

XMPP (Extensible Messaging and Presence Protocol) proposed by V. Karagiannis [18] is a rarely used session layer protocol designed for extensive messaging and chatting purposes. This is not suitable for Machine to Machine communication due to heavy overload. Hence, it is hardly used in IOT applications.

3. Investigations and findings

3.1. Hierarchical Structure for communication within IOT

An IOT system as such comprises of services (Energy, health, entertainment, education, transportation), Applications and Software (SDN, Web services, clouds, grids), Analytics (Data Mining, machine learning, Analytics), Integrations (sensor data, GIS data), Interconnection between the devices that implements different protocols and communication standards, acquisition of data through sensors, cameras, smart phones, GPS systems etc. IOT systems are quite frequently being used for implementing different applications that include home automation, health management, smart cities etc. Out of these aspects communication among the devices is most complicated.

The communication standard used for effecting communication among the IOT devices generally comprises of three layers which include session, network and data link layer into which physical layer and MAC layer is incorporated. The protocols used in each of the layer and sub-layer are depicted in the Table 1.

It can be seen from the above table that IOT devices can use different protocols in each of the communication layer which are developed using different communication standards. The protocols differs in many ways making it difficult for the devices with different communication protocol to communicate leading to implementation of different strategies using which communication between heterogeneous devices can be effected.

3.2. Protocol conversion strategies

Most compelling issue when it comes to IOT is the ability to communicate among heterogeneous devices. Protocol conversions have to be undertaken leading to addition of more layers, hardware or software which some time lead to such an overhead that may affect response time, throughput and may even lead to heavy cost escalation. The strategies used must be efficient and reduce the overhead as much as possible. Some of the possible strategies that can be adapted are detailed in the below section.

3.3. Adding Abstract layer over a pair of communication standards

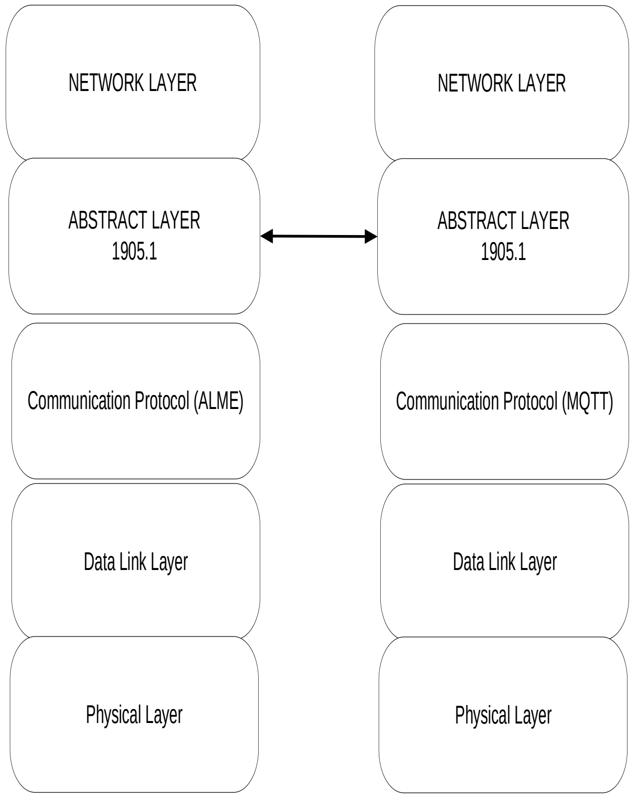

Figure 1: Handling heterogeneity through Abstract Layer

Table 1: communication system for IOT system

Layer	Sub Layer	Protocols used	Security protocols used	Communication standards used
Session		MQTT, SMQTT, Core, DDS, AMQP, XMPP, CoAP	TCG, Otah 2.0, Smack,	IEEE IETF ITU
Network	***Encapsulation***	6LoWPAN, 6TiSCH, 6Lo		
	Routing	RPL, CORPl, CARP		
Data	***MAC***	IEEE 802.15.4, 802.11G, 802.15		
	PHY	Wi-Fi, Bluetooth, ZigBee, 3G, NFC		

One of the strategies to tackle heterogeneity among communication protocols is to introduce an abstraction layer on top of the data link layer. Abstract layer is open standard that can be known to every person developing protocols related software. The abstract layer as such can be developed through a standard such as 1905.1. Two heterogeneous protocols can be made to communicate through an abstract layer. Transmitting protocol converts the data to be communication into abstract format. The receiving protocol reads the data transmitted through the open standard protocol and concerts the same to the local protocol which actually processes the received data. The communication structure for such a strategy is shown in Figure 1.

This strategy while it is quite simple is also cumbersome as many abstract standards are required to support all possible protocol heterogeneities. 1905.1 just support two communication standards.

3.3.1. Implementing native conversions within protocols

Within Every device and within every communication layer several protocols can be implemented and the protocol needed for communicating with a device using its native protocol can be selected at run time. A selector is a piece of software that can be made stay in layer variable dynamic selection of the protocol is required. Since protocols on both sides of the communication are same effective communication can be undertaken. Figure 2 shows such an implementation

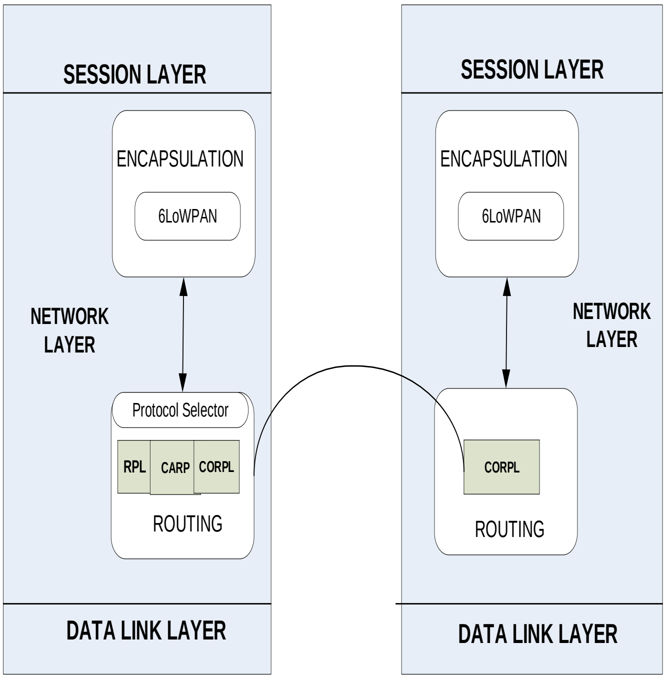

Figure 2: Native Protocol Selectors

Alternatively a single protocol can be provided with the intelligence to find exact protocol using which communication can be held. The Native protocol can be extended to incorporate required to convert the native protocol to the destination protocol with which communication can be held. This kind of an arrangement is shown in Figure 3

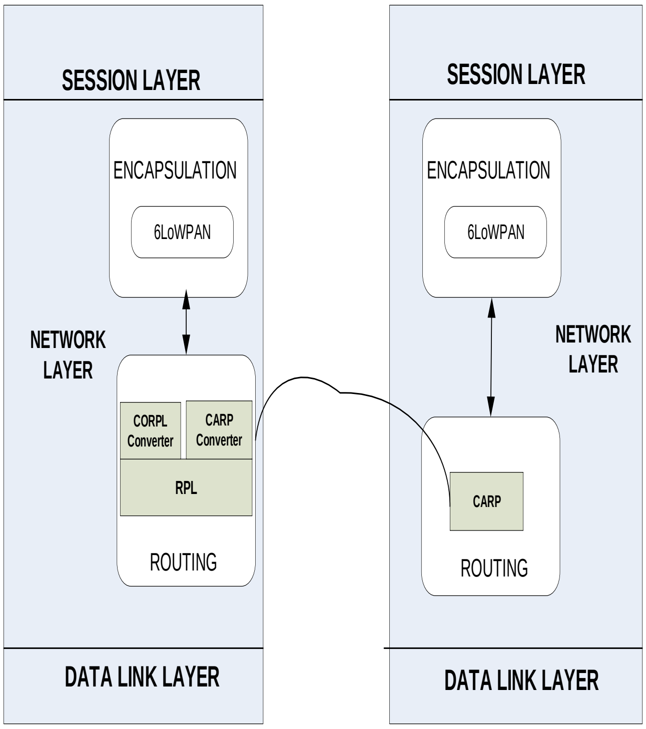

Figure 3: Native Protocol Converters

3.3.2. Hardware based Protocol converters at device levels

At another strategy is to develop a communication board that is capable of converting any standard protocol to fixed protocol and then use the same for communication. Communication board on the receiving side convert fixed protocol to standard protocol as required. Figure 4 shows such a strategy. This kind of implementation is quite complicated and becomes limited when few protocols conversions are implemented within the communication board.

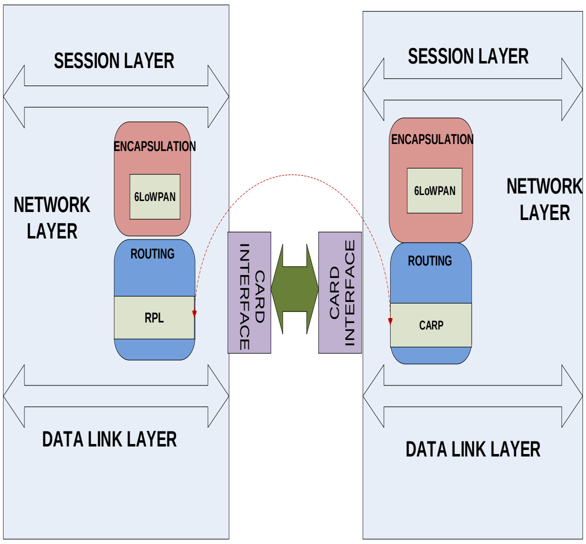

Figure 4: Hardware based protocol conversion

3.3.3. Gateway based conversion

Most of the IOTs are built around gateways which either hardware based or software based or both based implementation generally situated in the second layer of the IOT based system. Gateways are primarily developed for implementing the conversions required so as to bridge adjacent layers of an IOT based system. Gateways are designed in such a way that they have the support of communicating with different communication protocols. It is an additional overlay layer provided on the top of standard layers.
The gateway is a bridge that helps effecting communication with two devices that follow different protocols. Figure 5show the way a gateway connects two devices that follow different protocols. This kind of a strategy adds on to more layers making the system of communication more complicated and also leads to communication delays.

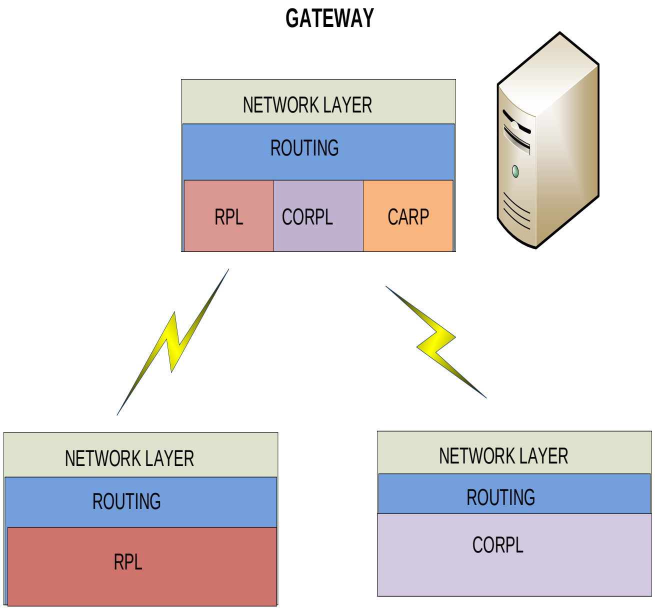

Figure 5: Protocol conversions through Gateways

3.3.4. Signal Composers and converters

One yet another strategy is to develop a converter that is capable of receiving any radio or wired signal without much worrying about the protocol used for transmitting signals as a consequence of communication between the devices connected on to the Internet. The signal composing and converting device will be able to receive any radio signal and the software filters will be able to separate the signal into different category that include Wi-Fi, ZigBee, Bluetooth etc., and forward the filtered signals into the related and appropriate interface. Even the wired signals can also be separated into RJ45, RS232C, RS485, I2C, CAN and USB and then trigger the connection to the related wired connection. This appears to be versatile solution. Figure 6 shows the signal composing and conversion scheme.

3.4. Comparative Analysis

Comparison of above mentioned strategies based different criteria that include need for additional hardware, need for additional software, response time, throughput, scalability, availability, context awareness, dynamic configurability, and fault tolerance is shown in Table **2**. From the table it can be seen that each strategy has merits and demerits. The strategy that deals with signal composers and converters appears to be more viable solution.

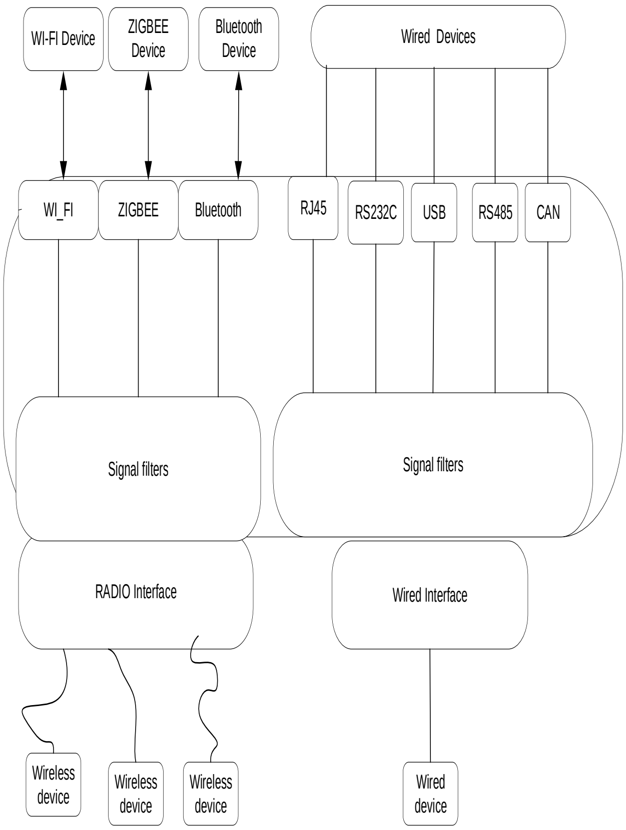

Figure 6: Signal composers and converters

4. Conclusions

Several modes of communication are to be supported within the ambit of IOT based networks. Many types of devices are used within IOT networks. It is possible that heterogeneity exists among the devices from the point of communication protocols built into the devices. Communication among the devices has to be effected considering varied protocols and communication standards. Effecting communication among the devices that support varied and heterogeneous protocols and standards is the most important issues that must be dealt with to make the use of IOT for implementing different types of applications. An elaboration of different strategies is required and deep learning of the same must be in place. This paper elaborated different strategies that one can adopt to deal with heterogeneous communication.

Table 2: Comparison protocol conversion strategies

Serial number	Strategy	Need for additional Hardware	Need additional software	Response time	Through put	Scalability	Availability	Context awareness	Dynamic Configurability	Fault Tolerance
1.	***Adding Abstract layer over a pair of communication standards***	X	Y	Poor	poor	Poor	Good	Poor	Poor	Poor
2.	***Implementing native conversions within protocols***	X	Y	Good	Aver age	Aver age	Good	Good	Good	Good
3.	***Hardware based Protocol converters at device levels***	Y	N	Good	Good	poor	Good	Good	Good	Poor
4.	***Gateway based protocol conversion***	Y	Y	Good	Good	Aver age	Good	Good	Good	Poor
5.	***Signal Composers and converters***	Y	Y	Good	Excel lent	Excel lent	Good	Good	Excel lent	Excel lent

References

[1] Xiaoni Wang, "Resource-aware clustering based routing protocol in the Internet of Things," *4th International Conference on Awareness Science and Technology*, Seoul, Korea (South), 2012, pp. 20-25.

[2] X. Che and S. Maag, "A Passive Testing Approach for Protocols in Internet of Things," 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, Beijing, 2013, pp. 678-684.

[3] Tara Salman, "Networking Protocols and Standards for Internet of Things", http://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot/index.html

[4] A. Aijaz and A. H. Aghvami, "Cognitive Machine-to-Machine Communications for Internet-of-Things: A Protocol Stack Perspective," in *IEEE Internet of Things Journal*, vol. 2, no. 2, pp. 103-112, April 2015.

[5] O. Cetinkaya and O. B. Akan, "A DASH7-based power metering system," *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, Las Vegas, NV, 2015, pp. 406-411.

[6] D. Dujovne, T. Watteyne, X. Vilajosana and P. Thubert, "6TiSCH: deterministic IP-enabled industrial internet (of things)," in *IEEE Communications Magazine*, vol. 52, no. 12, pp. 36-41, December 2014.

[7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, Fourthquarter 2015.

[8] J. Granjal, E. Monteiro and J. Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294-1312, thirdquarter 2015.

[9] M. Hasan, E. Hossain and D. Niyato, "Random access for machine-to-machine communication in LTE-advanced networks: issues and approaches," in *IEEE Communications Magazine*, vol. 51, no. 6, pp. 86-93, June 2013.

[10] K. Malar and N. Kamaraj, "Development of smart transducers with IEEE 1451.4 standard for Industrial automation," *2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies*, Ramanathapuram, 2014, pp. 111-114.

[11] M. Park, "IEEE 802.11ah: sub-1-GHz license-exempt operation for the internet of things," in *IEEE Communications Magazine*, vol. 53, no. 9, pp. 145-151, September 2015.

[12] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT," *2015 International Conference on Pervasive Computing (ICPC)*, Pune, 2015, pp. 1-6.

[13] S. Raza and T. Voigt, "Interconnecting WirelessHART and legacy HART networks," *2010 6th IEEE International Conference on Distributed Computing in Sensor Systems Workshops (DCOSSW)*, Santa Barbara, CA, 2010, pp. 1-8.

[14] Z. Sheng, S. Yang, Y. Yu, A. V. Vasilakos, J. A. Mccann and K. K. Leung, "A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities," in *IEEE Wireless Communications*, vol. 20, no. 6, pp. 91-98, December 2013.

[15] Z. Zhou, B. Yao, R. Xing, L. Shu and S. Bu, "E-CARP: An Energy Efficient Routing Protocol for UWSNs in the Internet of Underwater Things," in *IEEE Sensors Journal*, vol. 16, no. 11, pp. 4072-4082, June1, 2016.

[16] M. Singh, M. A. Rajan, V. L. Shivraj and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)," *2015 Fifth International Conference on Communication Systems and Network Technologies*, Gwalior, 2015, pp. 746-751.

[17] Gartner, "Gartner's 2014 hype cycle for emerging technologies maps the journey to digital business", 2014.

[18] M. B. Yassein, M. Q. Shatnawi and D. Al-zoubi, "Application layer protocols for the Internet of Things: A survey," *2016 International Conference on Engineering & MIS (ICEMIS)*, Agadir, 2016, pp. 1-4.

[19] A. N. Kim, F. Hekland, S. Petersen and P. Doyle, "When HART goes wireless: Understanding and implementing the WirelessHART standard," *2008 IEEE International Conference*

on Emerging Technologies and Factory Automation, Hamburg, 2008, pp. 899-907.

[20] C. Gomez, J. Oller, and J. Paradells website "Overview and evaluation of Bluetooth low energy: An emerging low-power wireless technology", http://www.mdpi.com/1424-8220/12/9/11734, 2012, Vol 12, Issue 9, pp.11734-11753.

[21] J. Decuir,"Bluetooth 4.0: Low Energy" Presentation slides, https://californiaconsultants.org/wp-content/uploads/2014/05/CNSV-1205-Decuir.pdf.

[22] I. Poole,"Weightless wireless - M2M white space communications-tutorial", http://www.radio-electronics.com/info/wireless/weightless-m2m-white-space-wireless-communications/basics-overview.php, 2014.

[23] S.Bush,"DECT/ULE connects homes for IoT" Electronics weekly, https://www.electronicsweekly.com/news/design/communications/dect-ule-connects-homes-iot-2015-09.

[24] D. Locke,"MQ telemetry transport (MQTT) v3. 1 protocol specification", IBM Developer Works Technical Library, https://www.ibm.com/developerworks/webservices/library/ws-mqtt/index.html, 2010.