Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 9, Issue. 10, October 2020, pg.104 – 111

A Systematic Review on Open Networking Challenges in IoT Domain

Isha Padhy
Department of CSE, Chaitanya Bharathi Institute of Technology, Hyderabad
ishapadhy06@gmail.com

DOI: 10.47760/ijcsmc.2020.v09i10.013

Abstract: ***Internet of Things (IoT) is a versatile concept that aims to connect multiple physical devices to provide intelligent services to people in different work environment. Since IoT systems are built on hardware and communication technology, bringing devices to a software or application level to access logical information is a daunting task. This article introduces a review of all open source network related challenges. Here we focus on the big issues related to Big Data management, mobility issues, collaboration and power management issues that can be considered during the construction of any small IoT related projects. The main aim of the study is to show direction to researchers select specific challenges in IoT and opt suitable technologies for intelligent use.***

Keywords: Big Data, IoT, IoT Challenges, Broad Areas

INTRODUCTION

The concept of Internet of Things (IoT) is an idea to connect objects which can make life easier in some way. Smart items can be equipped with communication technology, actuators, sensors etc. Nowadays, IoT is gaining attention in many fields such as transportation, agriculture, industry, and health care. IoT data differs from other standard data collected by IoT systems in terms of signals during the data collection, including environment, noise, variability and fast growth. We therefore need to be very careful with the data received from these areas. Since 2004 many challenges have been addressed and solutions have been found but they still need to be improved in areas such as power management and Big Data. We have made progress in these areas as we have been provided with good sensors, contracts and security features. According to Sunil K Sonare, General Manager and Head - IT, Sadbhav Engineering Limited[14] , data and information are used for the purposes of first analysis and decision making. Various sensors are used to integrate IoT Solutions into various industries and to assist technical and business leaders with a view to improving design, product features, business growth etc. It requires such a switching technology that provides at any time a seamless connection between the sensors of a different home Internet of Things (IoT) devices.

The remaining paper is divided into four parts. The Section-2 describes background research. Section-3 describes the challenges in various fields of IoT and finally; Section 4 describes the end and scope of the future.

BACKGROUND

Background Study

Lack of standards and documentation can aid in idle activities with IoT devices. Low or cheap standard made and configured devices that have undesirable effects on communication services. In addition to the guidelines for manufacturers and manufacturers, they sometimes design products that work disruptively on the Internet [22]. The performance of all technologies requires a group of skilled people who have sufficient knowledge of network, hardware, software and that technology. And India is back to this point where workers think when technology is being distributed, they lose their jobs and there is no life for new technology. Therefore, they do not take action to rely on it. Therefore, every organization faces many problems during its phase of transition from legacy to IoT-enabled systems. Similarly, Scalability, Error tolerance and empowerment are also major challenges in India. Accenture of the Industrial Internet of Things confirms that 60 perc of companies have been involved in IoT projects and more than 30% in the first phase of deployment. It is also found that 69% Companies IoT Programs is working on reducing operating costs. Cisco survey says, 74% of organizations failed with their IoT systems. The reason is that there are many factors which involve human in the use of IoT, in addition to functional sensors and networks which are integrated elements of IoT. Yet not all devices contain advanced sensors and communication skills to communicate successfully and share information. Alternatively, alternative power sensors and safety standards built with inherited equipment may not be able to provide the same results. Working faster can include external sensors, but this is also a challenge because deciding which function and which part will contact and share information with the network is difficult. A report says, more than 20,00000 connected devices at the moment, and connecting all devices brings a lot of security risks and not just difficulties. Bringing a large number of connected devices to a single platform requires organization and system configuration that can identify and authenticate those devices.

The mobile satellite company Inmarsat has brought forward that 24% found connectivity problem as one of the major challenges towards use of IoT devices. Specifically, Logistics and Oil and Gas companies that involve remote operations expect strong communication network to collect data in critical situations and later for analysis. The signal quality collected and transmitted over Networks largely depends on the routers, LAN, MAN and WAN.

The current IoT network technology and integrated routing procedures were discussed. The provision of a fully based taxonomy is provided, while how network and operational agreements work to meet the latest IoT needs and applications is also demonstrated. The main focus is on the introduction of network proto schemes and processes.

Interactions, collaborations, and configuration issues with existing protocols are focused here depending on the latest developments of IPv6 [12]. IoT's development depends on present day communication technologies that includes Bluetooth technology, Zig-Bee, WiFi, and (LTE-A) Long-Term Evolution Advanced etc. To build an acceptable IoT system, is a challenge. The IoT structure and configuration is essential for providing newest interoperability for all sensory and object devices, which require a proprietary system. In addition, secured network and confidentiality raise significant issues [4]. Finally, effective and efficient data management systems, with a view to greening IoT systems [3]. These are few challenges that has to be addressed in the accepted form of communication technology. In paper [5], existing and emerging technology to support broadband IoT based (M2M) Machine-to-Machine networks was introduced, while [7] focused on IoT standards in the field of communication, services of (M2M) / IoT application areas. In [6] the authors gave an overview of empowering applications, protocols, technologies, and research efforts addressing various aspects of IoT network. In [8], an overview of the IETF protocol suite has been proposed to support IoT network of devices and applied area.

The Paper [15] introduces the IoT network layer and its challenges that partially and indirectly explored with other activities involving cases of IoT technology use or queuing efforts at various construction sites. In the literature, the term 'IoT technology' is often confused because it can be used to specify agreements from all building blocks of the IoT platform. We are in a society where an IoT user is able to use (RFID) which is termed as a radio-frequency identification, on cell phones to scan embedded RFID tags and download their privacy policy for use, using an interesting process called the privacy trainer [21]. Here, in case the downloaded privacy policy does not match the user's choices, the user may decide not to use the item. So, if a RFID reader attempts to read data from a user's mobile phone, the phone may review the privacy policy and request user's consent[21]. The other uses of the privacy trainer are to protect the user's private space (eg house or office). Such protection is achieved through the process of scanning unwanted or dangerous objects, such as nerves left in the home to perform surveillance without the consent of its owner (Radomirovic, 2010). Let's take an example, a user can find someone close to their place who would prefer same variety of songs without giving their current place and song choices to that user nearby.

LARGE FIELDS

Interaction

Communication is said to be the capability of two or more components to exchange information and use that information for analysis. As, IoT is able to connect everything that is visible, heterogeneity emerges in the image. The challenges we face here are frightening. The urgency of the IoT collaboration has been emphasized by both academics and the industry. Many industries are trying to address the challenges of IoT integration by setting common goals. Several attempts have been made to maintain standards while interoperating between IoT devices, networks, services and data formats managed by various sources. India and Russia have jointly implemented major IoT industrial projects.

Second, although there are many common processes designed for various IoT applications, a framework that complies with the rule of law is still needed in the market. Thirdly, the quality of the security parameters must be taken into account because outsiders may be able to access the data by interfering in or removing data during the transfer, in both cases the data should be protected. Confirmation regarding anonymity of author and user data in the event of Smart Homes should be maintained. Many major retailers offer their IoT infrastructure, social

media agreements, non-compliant standards, formats, and semantics that create a closed environment. The next big problem is the construction of pre-defined specifications of objects. It is loss for small companies to fund complex connectors of different platforms. From the point of view of developers, the incompatibility between IoT platforms results in syncing their application to a API with specific platform.

There are different network processes and technologies used to provide IoT communication interoperability. Such as, Universal Plug and Play (UPnP) and standard DLNA protocols are used for interaction between gateway and IoT devices.

IP-based methods integrate a complete TCP / IP stack into smart devices. The sensors and actuators are connected through the IP network to allow end-to-end communication between the network of sensors and the IP network. A key advantage of using the TCP / IP stack on nodes is, the translation of gateways and protocol are not required. But the authors of [6] argue that the entire set up of IP sensor network is not possible due to their block chain features.

IETF has established functional groups (WGs) in network infrastructure such as (ROLL) which is Routing Over Low Power and Lossy Networks, IPv6 over Low Power WPAN (6LoWPAN), UDP-based Constrained Application Protocol (CoAP), and Constrained Restful Environment (CRE) to solve the problem of connectivity. The former method, still uses the gates to switch between standard protocols used on the Internet and related protocols used in the sensor network, e.g. Pv6 to 6LoWPAN. Hence, due to the use of standard protocols, this method has no limitations of gate-based routes. The main advantage is that the gateway and sensor nodes do not have to come from the same source that enhances interoperability among heterogenous devices. Road safety challenges designed for IP are described in detail in [6]. However, there are many other methods [2] such as Software Defined Network (SDN), Network function virtualization, fog computing. The IPv6 over Networks of Resource-constrained Node (6Lo) group working in IETF develops a set of standards on transmitting IPv6 frames over data links [11] which are characterized by limited performance, memory resources, tight restrictions by government, code location, network bandwidth optimization and power consumption. A working group of 6Lo was formed to cover data links, apart from IEEE 802.15.4 and IEEE 802.15.4e covered by 6LowPAN and 6TiSCH. Some of these 6Lo-approved RFC specifications have been discussed [7] as IPv6 over 802.11ah, IPv6 over G.9959, IPv6 over Bluetooth Low Energy, IPv6 over NFC, IPv6 over MS / TP (6LoBAC), IPv6 over DECT.

Method	Health Care	Medical Imaging	Human Genetics	Speech Recognitio	Bio Informatics	NLP	e-governance
Classification	-	✔	-	✔	-	✔	✔
Clustering	✔	✔	✔	-	✔	-	✔
Association rule	✔	-	-	-	✔	--	✔
Prediction	-	-	-	-	-	-	-
Time series	-	✔	-	✔	-	-	✔

Fig.1. Different Machine Learning concepts

The fig 1. shows the application areas of big data mining functionalities, '✓' shows the support for an application, '-' denotes that the method may or may not support to an application[23].

Big Data Analytics (BDA)

BigData Analytics (BDA) involves large data analytics systems with a wide variety of data [13] that provide surprisingly duplicate patterns, unexpected hidden combinations, market trends, preferences of customer, and many other useful business information. As cost of storage is very high, the first challenge of the BDA is storage media and in speed of input and output. This is because the existing algorithms do not always respond properly when working with the actual data. The automation[12] of this process and the development of new algorithms for learning the machine to ensure consistency has been a major challenge in recent years. Access to information and representation of information is a major issue in big data which includes raised concerns such as authentication, administration, archiving, data retrieval. And now due to the increase in the size of Data the existing tools may not be effective in processing this data for meaningful information. The most important challenge for the BDA's strategy is its disability and safety. The purpose of visualization of data is to present data in a way that is suitable, using other photographic theory techniques. The graphical display links between the data and the appropriate description. However, online markets, such as Flipkart, Amazon or e-bay, have millions of users and more than that number of products they will sell each month, this generates a lot of data. Maintaining highly secretive information is a major problem for the BDA. The high risk towards information security can be improved through different authentication and encryption techniques [10].

The Data Collaboration aspect should be considered: The widespread popularity of IoT has made large data calculations a challenge due to the optimization and collection of data by various sensors in the IoT environment. Big IoT data analysis can be defined as steps in which various IoT data are explored [12] to reveal styles, abstract patterns and hidden relationships. The Companies and individuals can be benefitted by analysing large amounts of data and managing large amounts of information that can affect businesses [13]. So, IoT big data analytics aims to help business organizations and other organizations achieve a better understanding of data, and thus, make more efficient and informed decisions. Large data sets enable data miners and scientists to analyse large amounts of random data that can be used using traditional tools [11]. Also, big data analytics aims to quickly extract useful information using data mining techniques that may help in predictions, establish the newest trends, discover hidden patterns, and make decisions. [14]

Energy Management

The demand for IoT applications is increasing, whereas IoT devices continue to grow both in their numbers and requirements. So, smart city solutions ought to be able to harness energy efficiency and address the associated challenges. Energy management is taken into account to be the key to the conclusion of complicated energy systems in intelligent cities. Both academics and industry is trying to focus on handling power in smart cities. Fujitsu proposed a power management system for companies and introduced a smart architecture management system as a cloud service [7].

Home appliances are a great source of energy consumption. Energy management is key to customizing the use of energy at homes/residential buildings by managing the electrical equipments like lighting, cooling and heating systems.

Lightweight contracts: Simple means that a rule of thumb causes a lower downturn. IoT-enabled smart cities should use a variety of protocols to communicate. We can find several policies such as Message Queue Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), Extensible Messaging and Presence Protocol (XMPP), Advanced Message

Queue Protocol (AMQP), 6lowPAN, and -Universal Plug and Play (UPnP) IoT. MQTT and CoAP are the most popular procedures. The most used MQTT is a protocol that gets data from IoT devices and sends it to the servers. CoAP is designed for scaled down devices and web transfer networks. Every processes are designed for particular situations and applications in which it works well. In addition, regulatory reform is an important component of IoT building, which may require IoT devices from different manufacturers or use different protocols.

Planning: IoT-enabled smart city plans focus on efficient resource utilization aiming at reducing energy and electricity consumption. In this connection, the DSM is very important; refers to the use of domestic electricity by changing the load capacity of the system and thereby reducing costs. Overall, the DSM consists of two major functions: load transfer and energy conservation, where freight forwarding refers to the transfer of customer load from the highest levels. The electricity can be stored to provide space for other customers. Power Predicting Models: The types of power consumption forecasts in IoT enabled cities are very important. They refer to a variety of applications in intelligent cities, including traffic models, temperature and humidity speculation models etc. Here predictions using (NN) neural networks and Markov decision-making processes can be included. Using such models will not only reduce significant power consumption but will lead to benefits of many others.

Cloud-based Approach: Cloud computing can also be useful in designing computer storage services to provide much efficient solutions for smart cities powered by IoT. Specifically, the cloud-based approach helps manage large data centre flexibility and energy efficiency. Low Power Transceivers: The IoT devices in smart city applications operate with limited battery, low power design architecture is very important in dealing with power management in smart IoT enabled cities. Most importantly, the existing application terms for IoT devices are not in line with the idea of using power. The radio frequency cycle of IoT devices is critical to energy efficiency, and researchers are exploring ways to reduce the radio frequency function of IoT devices and finally achieve energy-saving power generation.

Multipath Energy Routing: The traditional technology of routing is no better adapted. In fact, the lack of responsiveness with respect to the difference in network changes makes them not much useful. And, energy conservation is a major concern in the design of routing protocols for ad hoc networks, as most of the mobile nodes operate with limited battery capacity, and the energy decrease of a node affects not only the node itself but also on the overall lifetime of network.

The all-proposed single-path routing schemes involves a process of discovering new path once a path failure is detected, this process causes delay and wastage of node resources. A multipath routing scheme can be used to maximize the lifetime of a network.

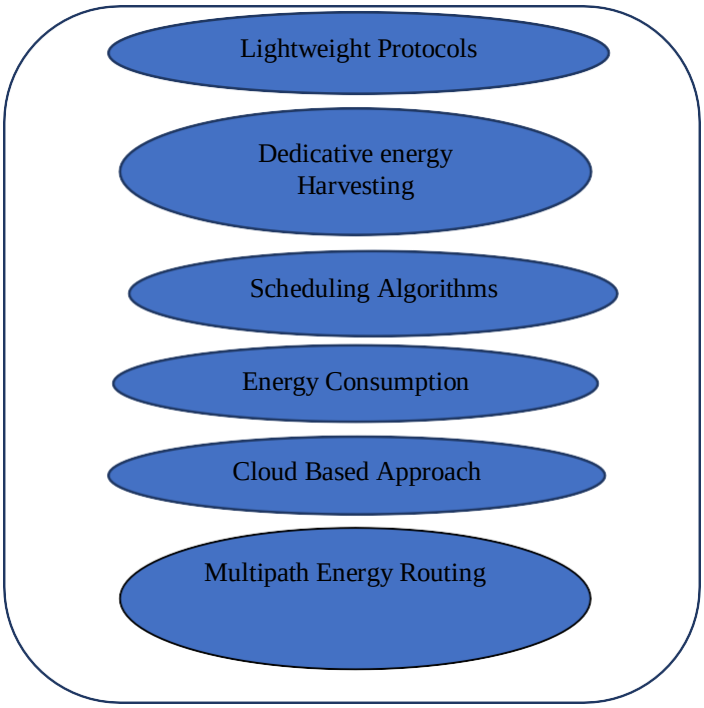

Fig.2. Solutions for IoT in smart cities for well managing the Energy

Fig2 Lists out few solutions for IoT-enabled smart cities with respect to efficient energy management. Some are described in this section.

CONCLUSION AND FUTURE WORK

A requirement of configuration, pre-defined precision design of the components, horizontal interaction with simple device integration is there. A scalability management protocol to support a large number of smart items is expected. There is a need for green technology for energy-efficient machines. In the future there will be many different solutions but we need to choose wisely based on the analysis made here. Genetic Algorithm and Deep Learning Algorithms can be used to analyse information acquired by intelligent applications. There is no other idea that there have been more attacks taking place against IoT, and it is far from new. With the rapid growth of technology and their development, cyber attackers are also more reliable and robust than ever in recent times. One of the biggest threats to AI is a strong AI attack. They attack many industries and one of them is the development of the mobile app. Another major problem and challenge with the Internet of Things is consumer perception. These days, consumers do not trust the security of their gadgets due to the increase in cyber-attacks. Voice recognition has been a growing technology for years now, and advances in accuracy have been impressive. Because processing voice data requires only an Internet connection and a microphone, many IoT devices may offer voice support. Bringing IoT technology to robots and public transport can lead to significant improvements in efficiency. One feature is required in the development of a smart city will be 5G technology, which makes bringing new devices to the network much easier than using the current communication infrastructure.

Our work was to focus on the latest areas where still challenges can be faced while dealing with networking of IoT devices. Expecting to overcome few of the listed out challenges we would be using appropriate methods to implement devices in a smart home and smart building.

References

[1]. C. C. Sobin1 "A Survey on Architecture, Protocols and Challenges in IoT", Springer Science Business Media, LLC, 2020

[2]. MahdaNoura, Mohammed Atiquzzaman & Martin Gaedke, "Interoperability in Internet of Things: Taxonomies and Open Challenges", SpringerLink Open Access, 2018

[3]. Radatz J, Geraci A, Katki F (1990) "IEEE standard glossary of software engineering terminology" IEEE Std 610121990(121990)

[4]. Anna Triantafyllou, Panagiotis Sarigiannidis,1 and Thomas D. Lagkas "Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends" Hindawi Wireless Communications and Mobile Computing Volume 2018, Article ID 5349894, 24 pages

[5]. Zuniga M, Krishnamachari B (2003) "Integrating future large-scale wireless sensor networks with the internet", USC Comptuer Sci Tech Rep

[6]. Fabián ConstanteNicolalde, Fernando Silva , Boris Herrera , and António Pereira "Big Data Analytics in IOT: Challenges, Open Research Issues and Tools" March 2018"Trends and Advances in Information Systems and Technologies (pp.775-788)

[7]. Chasaki D, Mansour C (2015) "Security challenges in the internet of things". Int. J. Space-Based Situated Comput. 5(3):141

[8]. J. Gantz and D. Reinsel, "Extracting value from chaos", IDC Iview, vol. 1142, pp. 1-12, Jun. 2011.

[9]. R. Mital, J. Coughlin and M. Canaday, "Using big data technologies and analytics to predict sensor anomalies", Proc. Adv. Maui Opt. Space Surveill. Technol. Conf., pp. 84, Sep. 2014.

[10]. N. Golchha, "Big data-the information revolution", Int. J. Adv. Res., vol. 1, pp. 791-794, 2015.

[11]. C.-W. Tsai, "Big data analytics: A survey", J. Big Data, vol. 2, no. 1, pp. 1-32, 2015.

[12]. P. Russom, "Big Data Analytics, 4th Quart. 2011.

[13]. Chi, Q., Yan, H., Zhang, C., Pang, Z., & Xu, L. D. (2014). A reconfigurable smart sensor interface for industrial WSN in IoT environment. IEEE Transactions on Industrial Informatics,2014, 1417–1425.Google Scholar

[14]. ValdiviesoCaraguay, A. L., Peral, A. B., Barona Lopez, L. I., & Garcia Villalba, L. J. (2014). "SDN—Evolution and opportunities in development of IoT application" International Journal of Distributed Sensor Networks, 10, 735142.

[15]. C.-W. Tsai, C.-F. Lai, and A. V. Vasilakos, "Future internet of things: open issues and challenges," Wireless Networks, vol. 20, no. 8, pp. 2201–2217, 2014.

[16]. D. Miorandi, S. Sicari, F. de Pellegrini, and I. Chlamtac, "Internet of things: vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.

[17]. O. Mavropoulos, H. Mouratidis, A. Fish, and E. Panaousis, "ASTo: a tool for security analysis of IoT systems," in Proceedings of the 15th IEEE/ACIS International Conference on Software Engineering Research, Management and Applications (SERA '17), pp. 395–400, June 2017.

[18]. R. Khan, S. U. Khan, and R. Zaheer, "Future internet: the internet of things architecture, possible applications and key challenges," in Proceedings of the 10th International Conference on Frontiers of Information Technology (FIT' 12), pp. 257–260, December 2012.

[19]. H. S. Dhillon, H. Huang, and H. Viswanathan, "Wide-area wireless communication challenges for the internet of things," IEEE Communications Magazine, vol. 55, no. 2, pp. 168–174, 2017.

[20]. V. Gazis, "A survey of standards for machine-to-machine and the internet of things," IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 482–511, 2017.

[21]. Qusay Idrees Sarhan, "Internet of things: a survey of challenges and issues" Int.J. Internet of Things and cyber-Assurance, Vol. 1, No. 1, 2018.

[22]. Er Pooja Yadav, Hemant Yadav "IoT: Challenges and Issues in Indian Perspective", 3rd IEEE International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU 2018), 24-25 February 2018, Bhimtal, Nainital.

[23]. Feng Chen, Pan Deng, Jiafu Wan, "Data Mining for the Internet of Things: Literature Review and Challenges" International Journal of Distributed Sensor Networks 2015(9):1-14, August 2015.

