Applications and Challenges Faced by Internet of Things - A Survey

Pir Amad Ali Shah[1], Masood Habib[2(✉)], Taimur Sajjad[2], Muhammad Umar[2], and Muhammad Babar[3(✉)]

[1] Department of Computer Science, University of South Asia, Lahore, Pakistan
amad.ali@usa.edu.pk
[2] Department of Computer Science,
Comsats Institute of IT Sahiwal, Sahiwal, Pakistan
{masoodhabib, taimursajjad, mumar}@ciitsahiwal.edu.pk
[3] National University of Sciences and Technology, Islamabad, Pakistan
babarkhan666@hotmail.com

Abstract. The Internet of Things (IoT) is a concept which expands the extent of internet by integrating a physical object to discover them into contributing bodies. This novel idea allows a physical gadget to embody itself in the digital world. There are a bunch of conjectures and opportunistic future of the IoT devices. However, most of them are vendor specific and requires a cohesive standard, which delivers their flawless assimilation and interoperable operations. Another key issue is the need of highly secure features in these devices and their equivalent products. Majority of these devices are resource constrained and not able to sustain computationally intricate and resource overwhelming secure algorithms. In this paper, we present a survey of various applications which have been made possible by IoT. Furthermore, the challenges faced by these networks.

Keywords: Internet of things · IETF · CoRE · CoAP

1 Introduction

Twenty first century has revolutionized the world of technology. Size of internet has been increasing rapidly with integration of miniaturized embedded devices into the internet world. Automation systems, personal gadgets, smart grid, cell phones and many other devices collaborate with each other and share valuable information about physical world. Internet is moving from traditional workstation and laptops to small embedded devices. We are moving from internet to Internet of Things (IoT) [1] by incorporating a sheer number of physical devices into internet. These objects contain miniature sensor nodes at their core which inherits all the limitations of Wireless Sensor Networks. IoT extends internet beyond personal computers, work stations to the world of physical objects. A broad range of appliances are now connecting to internet and provides valuable information. In internet, humans are the main source of generating information ranging from sending emails, capturing videos to messaging and browsing are some to mention. However, in IoT of the future, there will be millions and trillions of smart objects which will collect information, process it and communicate it. IoT

J. Ferreira and M. Alam (Eds.): Future 5V 2016, LNICST 185, pp. 182–188, 2017.
DOI: 10.1007/978-3-319-51207-5_18

relies of a set of distinct technologies which collaborate with each other. The major technologies behind this vision of IoT are Identification, sensing, embedded processing and communication are some to mention [2]. Radio Frequency Identification (RFID) tags are attached to physical world objects which contain data about those objects. These small tags are not capable to sense the environment but have the ability to collect data about a product. Internet of Things would not have been possible without them as they provide each object a unique identification to be recognized on the internet. On the other hand, sensor networks are capable to sense the environment based on unique identification provided by RFID tags and can also monitor their location, energy and other parameters. Once data is being sensed, partial processing take place at each object which is further transmitted for various operations to extract valuable information from it.

The Internet Engineering Task Force (IETF) shaped a working group called Constrained RESTful Environment Group (CoRE) group. This group was given the job to define a method to use a large number of tiny, resource limited, low-power devices, that can exchange information over lossy- networks. This group described a set of regulations that is termed as Constrained Application Protocol (CoAP) [3]. CoAP is an application-layer protocol that is created to permit information exchange between resource-limited gadgets over resource limited networks [4]. Resource limited devices are tiny devices which have low processing power, memory, and speed. These devices mostly manufactured with 8-bit microcontrollers. CoAP protocol runs over UDP and cannot use TCP. IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) is an example of such a constrained network configuration setup [5]. CoAP has similar to HTTP-like request and response paradigm where devices can interact by sending a request and receiving a response. CoAP is very similar to HTTP; it is evident that it has been intended for easy web integration. CoAP does not replace HTTP; instead, it implements a small subset of widely accepted and implemented HTTP practices and optimizes them for M2 M message exchange. Think of CoAP as a method to access and invoke REST fu l services exposed by “Things” over a network [6]. Some good survey and research on intelligent transportation and its application in Internet of Things can be studied [12–14].

In this paper, we discuss the applications of IoT and the wide range of challenges faced by these networks. The applications of IoT are restricted by various challenges faced by these networks at various layers. The rest of the paper is organized as follows. In Sect. 2, potential applications are discussed. In Sect. 3, various challenges faced by these networks are discussed. Finally, the paper is concluded and future research directions are provided in Sect. 4.

2 Applications of Inter of Things

The IoT allows us to use technology to improve our reassure, efficiency utilizes our energies, and easily performs the tasks that utilize our home and work life and give us greater control over our lives. Here, we discuss various applications of an IoT.

2.1 Connected Home

A connected home can mean dissimilar things to different people, but it is basically a home with one or more gadgets linked together so that the homeowner can organize, modify and check their environment. If the IoT is basically helping our lives comfortable and easier and more linked, then the connotations for a truly Connected Home are game-changing.

2.2 Wearable

This technology covers a verity of devices that monitors, record, and give response on you/your environment. In other words, wearable are divided in two categories:

2.2.1 Fitness and Environment

Fitness ribbons and wristwatches are capable to monitor and send data based on your daily activities such step counting, heart rate and temperature.

2.2.2 Health

These wearable devices can monitor vital health factors such as O_2 saturation, heart beat etc, and can transmit any information outside of a planned range to the patient and to his doctor.

2.3 Industrial IoT

The IoT has thoughtful solution to automate an industry with wireless and infrastructure-less connectivity using sensor networks, M2 M communications, and conventional industrial automation can be made efficient and more effective.

2.4 Smart Grid

A smart grid is collection of internet capable devices that could measures power/energy, water or natural gas utilization of a town/building. With smart grid we can save labor cost as well as actual and accurate information and demands of the users.

2.5 Transportation

CoAP protocol is used for tracking the vehicle by fetching the GPS coordinates of the vehicle position at a specific point of time. It monitors the speed of the vehicle by fetching the reading of the accelerometer of the vehicle. A simple symmetric handshaking for various states of the vehicle (Fast moving, slow moving and Rest) is investigated. The overhead incurred during the communication and handshaking is quiet low which suits the requirement of energy constrained devices.

These are just a subset of applications. There are many other applications of IoT. The scope and nature of IoT provides a wide range of opportunities for various

applications. Currently, a wide range of research is being conducted to investigate the applications of CoAP and various other IoT protocols for physical objects of daily life.

3 Challenges Faced by Inter of Things

Internet of Things consists of a bunch of physical devices connected with each other. The devices themselves are resource-rich; however, they will not be able to communicate with each other in absence of sensor nodes. The presence of sensor nodes at the core of each physical device makes the device intelligent and enables it to identity itself in the digital world. These sensor nodes are resource-constrained and as a result classify the device as resource-constrained as well [7]. Resource-constrained devices vary from one another in term of space code, RAM and other specifications which affects their capabilities to support HTTP protocol. Resource-constrained devices having 10 KBytes of RAM and about 100 Kbytes of ROM are not capable to support HTTP (Class 1 devices) while those having 50 Kbytes of RAM and around 250 Kbytes of ROM support HTTP (Class 2 devices) [9]. However, HTTP requires considerable amount of code space and ROM along with high energy in processing, so Class 1 devices refrain from adapting HTTP. As a result, extremely lightweight protocols such as CoAP need to be developed to make them feasible for IoT. The protocols need to adjust the battery power of each object so that they can operate for months and years for as little as 1 W.

Another challenging issue for IoT is interoperability [8]. As IoT incorporate a series of devices, hence, interoperability between various devices is a serious issue. Most of these objects have their own underlying hardware and software platforms and as a result, they are not able to communicate with each other. As a result, a common and unified standard for various technologies is required. The use of such a standard will provide seaming-less operations.

The devices require a scalable application layer for interoperable communication. Moreover, a common programming model is required, which will enable programmers to focus only on application development rather than the hassle of worrying about underlying platform architecture. In [15], the authors proposed an innovative solution to cope with these challenges by curbing the installation of application code on the embedded systems. Rather, they suggest that application code should run on the cloud and only firmware and network stack will be nested in the core of each embedded device. Running applications on cloud will serve two major purposes: ample memory space availability on the nodes and most importantly, developer will not have to worry about the hardware architecture [8]. The latter will help to develop applications on cloud which will enhances communication between heterogeneous nodes irrespective of any programming language. RESTful operations will be performed on the nodes to communicate with the hardware and perform various operations. Cloud operation will enhances communication between nodes from different manufacturers and will provide an interoperable communication between them. Now a NetDuino board will not require a custom protocol to communicate with TMote or Berkeley mote as everything is running on the code. Only Firmware and RESTful operations (PUT, DELETE, GET, and POST) will all that be implemented on the node. Application code is shifted to

cloud. In-network data processing consume considerable amount of a node resources, these operation will also need to be shifted to a powerful devices in order to ease the burden on these nodes [2].

The Quality of Service (QoS) provisioning in an IoT framework is another challenging issue which needs to be addressed. To provide QoS, two parameters are of high importance: Reliability and Timely delivery of data. Reliability is provided by transmitting CON messages (message type in CoAP) which need to be acknowledged. When a sender transmits a CON message to the server for resource observation (resources such as temperature etc. resides on a server), it waits for an acknowledgement by using Stop-and-Wait retransmission algorithm. In Resource observation, timeliness is maintained by using "Observe" option. This option enables the subscriber/listener to sequence the notification.

In resource observation, an observer registers itself with a resource residing on a server [10]. The subject (server) notify each observer when the state of the resource changes. This reduces the number of transmission flowing in the network which in turn improves the efficiency, reliability, energy consumption, bandwidth utilization and other QoS metrics of the network. Resource observation provides reliability by exchanging CON messages which need to be acknowledged. As far as timeline requirement is concerned, the Observe option helps the observers in sequencing the resources. Though, this option helps the subscribers/observers to check the validity of the notifications. However, it does not guarantee timely delivery of notification (carrying resources) to the observers. This will have severe consequences in real time application where a minor delay in notification will make it useless [11].

The presence of diverse range of devices at the core of IoT poses various security threats. Integrating everyday objects into the internet require various communication models. This requirement is likely to add some very ingenious and innovative malicious models [16]. It is of utmost importance that such models should be prevented or at least mitigating options should be in place to tackle their undesirable effects. To develop a secure solution in the internet of things context is much more difficult due to varying and unpredictable nature of objects, many of whom are to be connected for the first time in the internet. It is very important to understand the characteristics and features of things and underlying embedded technologies to combat various malicious models. Existing security and lightweight cryptographic algorithms are to be assessed and adapted in the internet of things environment. However, such profiling of these protocols and algorithms might not necessarily comply with their domain of applications and might results in undesirable outcomes. Any protocol or algorithm has their intended domain of applications and specification. Modification of protocol features might deviate from its original use of intend as many internet-based protocols were not designed for internet of things objects. Recent work can found in [10].

Heterogeneity plays a vital role in infrastructure protection. Highly constrained sensor nodes scattered in a battle field require a robust communication channel to communicate with cellular and wireless devices like Smartphone. Cryptographic algorithms are required to secure communication between these entities. However, due to battery power nature of these devices, the algorithms need to be computationally simple and fast efficient. AES algorithm might suit a small subset of IoT devices; however, they might not be suitable for extremely constrained RFID tags. Symmetric

algorithms are the best options rather than asymmetric algorithms as they are computationally simple and suit these tags etc [9, 10]. IoT devices need to use the existing internet standards to communicate with each other. However, all of them are not resource oriented. Hence existing security protocols need to be adapted and modified. In short, the challenges faced by IoT are summarized as follows:

- Sensing a complex environment: Innovative ways to sense and deliver information from the physical world to the cloud
- Connectivity: Variety of wired and wireless connectivity standards are required to enable different applications needs.
- Power is critical: Many IoT applications need to run for years over batteries and reduce the overall energy consumption.
- Security is Vita l: Protecting user's privacy and manufacturers IP, detecting and blocking malicious activities.
- IoT is complex: IoT application development needs to be easy for all developers, not just to exports.
- Cloud is important: IoT applications require end-to-end solutions including cloud services.

4 Conclusion

Internet of things incorporates a wide range of devices. The presence of miniature sensor nodes at the core of each device provides seamless and interoperable communication. Although, a wide range of applications exist, however, communication is still at risk in these applications. These networks face various challenges which need to be addressed in order to broaden the scope of IoT. These networks have the potential to enable communication between devices, which were not previously connected with the internet.

References

1. Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010)
2. Usman, M.J., Zhang, X., Chiroma, H., Abubakar, A., Gital, A.Y.: A framework for realizing universal standardization for internet of things. J. Ind. Intell. Inf. **2** (2014)
3. Understanding Constrained Application Protocol Using CoAPSharp Library (2014). www.coapsharp.com
4. Jan, M.A., Nanda, P., He, X.: Energy evaluation model for an improved centralized clustering hierarchical algorithm in WSN. In: Tsaoussidis, V., Kassler, Andreas, J., Koucheryavy, Y., Mellouk, A. (eds.) WWIC 2013. LNCS, vol. 7889, pp. 154–167. Springer, Heidelberg (2013). doi:10.1007/978-3-642-38401-1_12
5. Jabeen, Q., Khan, F., Khan, S., Jan, M.A.: Performance improvement in multihop wireless mobile adhoc networks. J. Appl. Environ. Biol. Sci. (JAEBS) Int. J. Eng. Trends Appl. (IJETA) **3**(2) (2016)

6. Shelby, Z., Bormann, C.: 6LoWPAN: The Wireless Embedded Internet, vol. 43. Wiley, Hoboken (2011)
7. Kovatsch, M.: Firm firmware and apps for the internet of things. In: Proceedings of the 2nd Workshop on Software Engineering for Sensor Network Applications, pp. 61–62. ACM (2011)
8. Puthal, D., Nepal, S., Ranjan, R., Chen, J.: DPBSV–an efficient and secure scheme for big sensing data stream. In: 2015 IEEE on Trustcom/BigDataSE/ISPA, vol. 1, pp. 246–253. IEEE, August 2015
9. Puthal, D., Nepal, S., Ranjan, R., Chen, J.: A dynamic key length based approach for real-time security verification of big sensing data stream. In: Wang, J., Cellary, W., Wang, D., Wang, H., Chen, S.-C., Li, T., Zhang, Y. (eds.) WISE 2015. LNCS, vol. 9419, pp. 93–108. Springer, Heidelberg (2015). doi:10.1007/978-3-319-26187-4_7
10. Jan, M.A., Nanda, P., He, X., Liu, R.P.: A lightweight mutual authentication scheme for IoT objects. IEEE Trans. Dependable Secure Comput. (TDSC) (submitted, 2016)
11. Puthal, D., Nepal, S., Ranjan, R., Chen, J.: A dynamic prime number based efficient security mechanism for big sensing data streams. J. Comput. Syst. Sci. **83**, 22–42 (2016)
12. Jan, M.A., Nanda, P., Usman, M., He, X.: PAWN: a payload-based mutual authentication scheme for wireless sensor networks. 15th Int. J. Eng. Trends Appl. (IJETA) **3**(2) (2016)
13. Alam, M., Ferreira, J., Fonseca, J.: Introduction to intelligent transportation systems. In: Alam, M., Ferreira, J., Fonseca, J. (eds.) Intelligent Transportation Systems. SSDC, vol. 52, pp. 1–17. Springer, Heidelberg (2016). doi:10.1007/978-3-319-28183-4_1
14. Alam, M., Albano, M., Radwan, A., Rodriguez, J.: CANDi for energy saving and facilitating short-range. Trans. Emerg. Telecommun. Technol. **26**, 861–875 (2013). doi:10.1002/ett.2763. ISSN 2161-3915
15. Alam, M., Trapps, P., Mumtaz, S., Rodriguez, J.: Context-aware cooperative testbed for energy analysis in beyond 4G networks. Telecommun. Syst. J. **62**, 1–20 (2016). doi:10.1007/s11235-016-0171-5. Online ISSN 1572-9451
16. Explore What's Possible with the Internet of Things. http://www.silabs.com/solutions/iot.html