IPv6 for IoT Networks

Adeel Baig
College of Computer and Information Systems (CCIS),
Al Yamamah University, Riyadh, Kingdom of Saudi Arabia.
a_baig@yu.edu.sa

***Abstract*— Internet of things (IoT) are growing immensely in the recent year. It is expected that by the year 2020, internet will have 50 billion devices connected to it. The main idea of IoT is that every object from our daily life will be connected to every other object and will be able to communicate via Internet. This opens a totally new challenge of adding new services for internet of things and adding new things to it. Without public IP addresses the capabilities of internet of things would be largely reduced. According to Internet Assigned Numbers Authority (IANA) IPv4 addresses were completely depleted in 2011. IPv6 was developed to overcome the shortage of addresses in IPv4. With the address space of 2^{128} it would be a better choice for IoT devices. Currently, the research on IoT devices and platforms is fragmented. There is a need for standardization of technology and the solutions offered. This paper highlights the challenges for IoT devices and possible ways for better address assignment. Our study makes use of the 6LowPAN, which was designed for low power wireless networks. We also present different approaches that can be used to connect and access IPv6 networks from within IPv4 networks.**

Keywords—IoT, IPv6, 6LowPAN, Tunnel Broker, CPE

I. INTRODUCTION

Internet of things is a growing paradigm in the modern internet technology. The basic theme of the concept is to connect various things around us to each other with an addressing scheme so that they can interact. During the last decade, the number of devices attached to internet has been growing exponentially. This has led to a new concept for the future internet known as Internet of Things (IoT). IPv4 could not support this large number of devices and is exhausted. IPv6 can support 2^{128} addresses, therefore, it can comfortably allow the billions of devices/objects connected to the internet in the future. IPv6 would not only provide a vast amount of unique addresses for IoT, but it would also provide other benefits like mobility, auto configuration feature, security and pure end to end communication[1].

The concept of IOT is the presence of smart devices/objects around us, which would be identified via tags and codes through a unique addressing scheme. These smart objects or things would communicate with each other using machine to machine (M2M) communication technique and would collaborate with each other to complete the tasks. These things could be the sensors, smart mobile phones, RFID (Radio-Frequency Identification) tags. These smart objects or devices would be small as well as highly confined. Due to their low capacity in terms of memory and low capability of computation, the communication among those smart devices would require new communication protocols like IPv6 Low Power Wireless Personal Area networks (6LoWPAN), defined by IETF [2].

The IoT will have a huge impact on the businesses, healthcare, domestics, industrial, logistics, transportation, manufacturing and several other fields [3]. These are the reasons due to which the US National Intelligence Council has considered IoT as one of the six "Disruptive Civil Technologies", which would have far greater potential impacts on the national power of US. The NIC has predicted that by the year 2025, the internet nodes would be residing in every aspect of the everyday life including food items/package, documents, papers, household furniture, kitchen items and many more things.

The rest of paper is organized as follows: IoT applications are discussed in section II. Related work is presented in section III. Key challenges are presented in section IV. IPv6 suitability is discussed in section V. Proposed solution, Implementation details and results are presented in section VI-VIII. Section IX concludes the paper.

II. INTERNET OF THINGS APPLICATIONS

The IoT offers a wide range of applications which would have a huge impact on the social life and environment. At the moment, several smart objects having primitive intelligence are linked to these environments which have improved the lives of the people. But these objects have not full-grown communication and collaboration with each other. By enabling these objects to collaborate and share information with each other would improve the way we communicate. Similarly, the IOT applications will bring quality and innovation in different domains as can be seen in Figure.1.

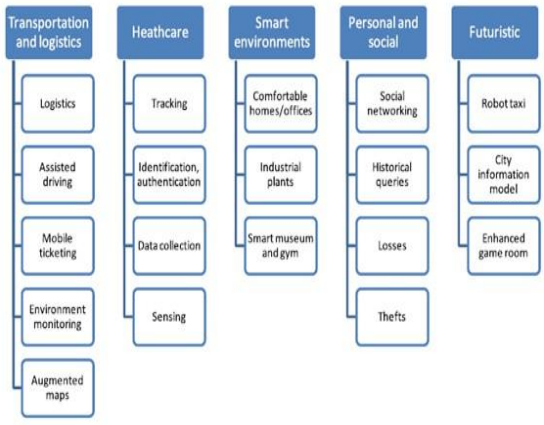

Figure 1 IoT Domains

In the transportation domain, the transportation vehicles like car, trains, buses, planes etc. are now being integrated with different sensors, actuators. The transportation vehicles are now having their own processing and computation power, which they utilize in accomplishing different tasks like finding optimal route to destination, informing the vehicle driver about better navigation, sending vital information to the traffic control areas to avoid congestion on the roads.

The benefits that IoT will bring in health care domain are tremendous. With the attachment of smart clinical devices/sensors with the patients, doctors and physicians can get access to the patient health data in real time as well as allow the doctors to get real time information regarding health indicators of their patients. IoT would allow the identification of the patients which would help the doctors to reduce patient's wrong diagnosis and treatment chances.

Additionally, IoT would bring a new concept of smart environments in the offices and homes. By attaching the sensors with the offices and household appliances, lives of the people would become more comfortable. The house temperature could be made to adopt with the change in the temperature and according to the users' preferences. The houses could be more secure with installment of monitoring sensors and alarms, and the household owner would have accessibility to data in real time. The household energy consumption could be monitored and controlled by the user automatically.

Also, there would be a huge impact on the industrial domain with the applications of industrial automation which could use the RFID deployments on several production parts [3]. This could enable the automation manufacturing of the products with reliability. Beside these realistic applications, there are several interesting futuristic possibilities that IoT could bring. Such as the concept of Robo taxi, smart city, Driverless cars, CIM (city information model) and gaming rooms with much more enhanced capabilities which could set the game levels and activity according to the continuously changing status of the player.

III. Related Work

During the last few decades, the research community of IoT has kept their focus on developing several application protocols which could empower the smart devices/objects which have constrained capabilities in terms of memory and computation power. Efforts have been made to make a common protocol for communication in the Internet of Things infrastructure. The main problem in this domain is the lack of resources for computation and communication as there will be different things with low communication power. Also, many different things globally will generate different types of data thus leading to different communication mechanisms. To overcome these issues there is a need for a common protocol for communication that should be light weight and support both type of networks i.e. IP and Non-IP based networks. Recently IETF Constrained RESTful Environments Working Group has introduced a protocol for resource-limited device, called Constrained Application Protocol (CoAP) [4]. However, CoRE-WG do not provide exact details about the communication between these devices. It does not say anything about no-IP networks or the mobility of objects. To enable machine-to-machine communication Machine Type Communications specifications are used [5]. Machine Type Communication (MTC) is a data communication that involves objects that do not require human interaction. MTC supports machine-to-machine applications.

Recently a new architecture was proposed with new protocol named TALP (Thing's Application level protocol) with TPS (Things Profile Server) to retrieve and identify other things attributes using TALP providing similar behavior like DNS and TIDS (Things Identification Service) for registering a node in TALP supported domain i.e. assigning GIDs [6].

TPS (Things Profile server) is used to obtain information on the types of supports and services that the protocol used by the thing. The profile of this thing is stored on the server corresponding TPS, and users can get by requesting the TPS server [6].

TALP (Things Application Level protocol) is used for translating of data; it allows communicating with the TIDS and TPS and supporting the multicast functionality. The general data function can share the messages of one user with other users. The TIDS/TSP use to enable the access to the domain name, IP address and the profile server to design and generate the Global ID for things. For the translation of addresses, comparison of header and the management of multicast function, TALP adaptor is used. By using these functionalities, the IoT architecture can provide the seamless and transparent communication between the things and users and also between things without knowing the underlying network (IP based Or Non-IP based).

In [7] the IoT6 architecture for IPv6 based service oriented architecture for internet of things was presented by the authors. The purpose of the architecture was interoperability among different technologies, information processing and interaction with cloud based services. The focus for IoT6 architecture is on modifying and enhancing the activities of different components and communication layer. The architecture was designed to facilitate devices with IPv6 addressing scheme and utilization of the DNS for the functionality of service and resource discovery and registration. DNS-SD is used for service discovery that worked on information system based on IPv6. A resource directory was replaced by multicast DNS which provide similar functionality by extending the IPv6 functions.

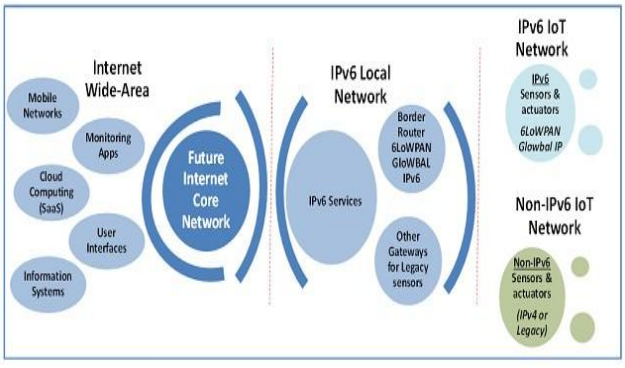

Figure 2 IoT6 Framework

Figure 2 shows the IoT6 architecture with different domains. The devices of the IoT present at the bottom of the architecture. There are two types of devices IoT complaint and legacy devices. The complaint devices are devices that are based on protocols like 6LowPAN.

A protocol named 6LoWPAN [2] specially made for small things with low computational power so that they can communicate easily. Since IoT devices are large in number and has limited computational power, we will discuss this solution in detail in section V.

IV. Key Challenges for Internet of Things

Despite the promise of bringing innovation and quality in different aspects of several domains and fields, IoT also brings key challenges with itself [8]. In IoT networks, integration of several different networks technologies and merging them into a common all-IP network is a serious challenge. As the number of devices attached to internet would be surely heterogeneous in their nature, so this poses another challenge of integration of such vast heterogeneous devices. Communication based on the IP protocol makes it reliable and easily scalable. Using IPv6 suits well for IoT networks as it guarantees the scalability requirements.

Initially, IoT was focused on the RFID technology due to its capability of uniquely identifying the objects/devices. But then as the technology starts evolving, the capabilities of RFID were not much metaphor by IoT and this started to begin a new research that the smart devices such as sensors, actuators and other smart devices/appliances connected to IoT would be more feasible option. Their connectivity could be done through IPv6 using protocols such as 6LoWPAN. Besides 6LoWPAN, several other technologies are being developed and researched. For example, Low Power Wi-Fi, Low Power Bluetooth, NFC (Near Field Communication), IEEE 802.15.4g. All the above-mentioned technologies are in fact the evolved technology of initial wireless sensor networks (WSN) and RFID. Beside the challenges of integration of several different technology networks and heterogeneous smart devices integration, another main challenge is to ensure the user confidentiality and privacy, data/ information integrity and several others security aspects, as can be seen in Figure.3

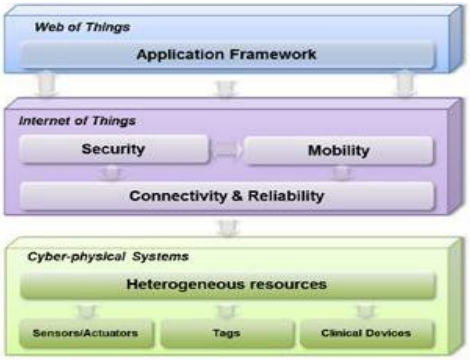

Figure 3 IoT Challenges

The third main challenge which IoT brings is the mobility support to the things connected to the internet.

V. Is IPv6 suitable for IoT?

As was discussed earlier, with the significant increase in IoT devices, the demand for more addresses is increasing. IoT devices have limited processing power and computation capabilities. IPv6 on the other hand requires extensive processing power as it adds extra bytes (20-40 Bytes at least) with each datagram that is transmitted. This is not efficient for small IoT devices that mostly transfer small amounts of data. Hence, using IPv6 native implementation will not be practical for IoT networks. An efficient protocol for low power devices was developed and is known as 6LoWPAN [6]. This main goal for this protocol is to provide IPv6 based wireless communication for low power devices. IP is the protocol that has always be considered for a local area or wide area network protocol. Using IP in IoT networks simplifies the connectivity and handles the addressing automatically. Moreover, it will be easier for the users to utilize the tools that are developed already for managing, configuring and debugging the networks. The administrators and developers don't have to learn new technologies as the network is entirely IP based. Another advantage of using IP is that there are number of protocols that are already developed and adapted for legacy sensor networks which run over IP.

To make 6LoWPAN work well for IoT networks, its complexity and overheads are significantly reduced. The 6LoWPAN can be used by a device a small memory of as low as 32k of flash memory. Beside the benefit of using immense address space and autoconfiguration of IPv6, 6LoWPAN uses compression to compress 40 bytes headers to just 4 bytes. As per the design 6LoWPAN defines four basic types of headers that are known as: Mesh header, Dispatch header, HCI header and Fragmentation header. In simplest cases only Dispatch header, HCI and the compressed IPv6 headers are necessary makes the size as 4 bytes. Additionally, to use these headers together, 6LowPAN uses stack of headers. Figure 5 shows the examples of the stacked headers.

Frame Hdr	Dispatch Hdr	HC1 Hdr	IPv6 compressed Hdr	UDP Hdr	Application Data

Point to Point Small Packet

Frame Hdr	Frag Hdr	Dispatch Hdr	IPv6 compressed Hdr	UDP Hdr	Application Data

Fragmented Packet Large Packet

Frame Hdr	Mesh Hdr	Dispatch Hdr	IPv6 compressed Hdr	UDP Hdr	Application Data

Mesh Transmitted Packet

Figure 5 Stacked headers example

Another major component of 6LoWPAN is the introduction of adaptation layer above the link-layer. Adaptation layer performs some important functions. The first major function of adaptation layer is that it compresses the TCP/IP header. The second main function which adaptation layer performs is that it handles the fragmentation and reassembly of packets. Another main function of adaptation layer is that it performs routing. It makes sure that border nodes of IoT network should route IP packets from outside into IoT network nodes and route inside packets to outside the network.

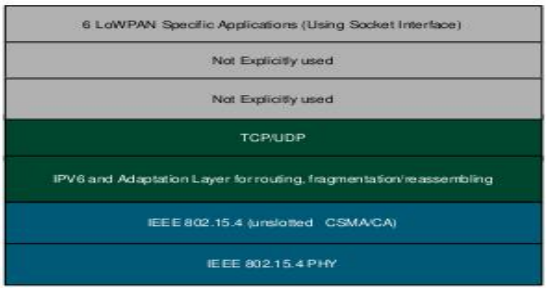

Figure 6 6LoWPAN stack

VI. Proposed Solution

The proliferation of IoT devices and shortage of IPv4 addresses has led us to propose a mechanism to connect IoT devices using IPv6. Shifting the Internet on IPv6 at once is not an easy task. At the same time, it is important to have both protocols in co-existence, because transition will continue for few years before IPv6 replaces IPv4 completely.

The home users, however, are unaware of this fact that they need to have IPv4 and IPv6 support on their home computers and IoT devices. Also, during this transition, all major companies will be shifting to IPv6. Users and many IoT devices should not be left behind during this transition. This marks as our motivation for working on creating a generalized solution for users and IoT devices.

To make a simple and automatic transition for home users and IoT devices, we propose an automatic Tunnel Broker mechanism and a dual stack CPE (Customer Premises Equipment) approach. In these days all IPv6 ready sites and domains can be accessed using tunneling mechanisms which are configured manually. These tunnels are difficult to configure and maintain for nontechnical home users, which are not aware of these complex configuration parameters. We develop a utility that can connect to a tunnel provider automatically. Additionally, we modified an open source firmware to make a dual stack firmware for the CPE. This will enable multiple users and devices to connect to the IPv6 Internet.

VII. Implementation

In this section we present possible ways of connecting IoT devices to IPv6 network using tunnel brokers and dual stack CPEs. These solutions can be used to simplify the connectivity of IoT devices to an IPv6 network. In another study, we present a detailed discussion on transition schemes from IPv4 to IPv6 in campus area networks [9].

IPv6 through Tunnel Broker:

Tunneling is a process of encapsulating IPv6 packets in IPv4 packets, so that they can go through the existing IPv4 network without facing any compatibility issues. Figure. 7 shows how encapsulation looks like. Although tunneling support is provided with dual stack hosts (i.e. PCs) and routers, but there is still manual configuration required to encapsulate IPv6 in IPv4. Again, this manual configuration is not an easy task for nontechnical home users.

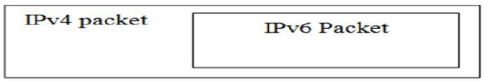

Figure 7 - Design Model

To automate the whole tunneling process IETF has proposed a solution named IPv6 Tunnel Broker in RFC-3053 [10]. Figure 8 shows the general design of Tunnel Broker model. Tunnel Broker is a server which entertains the users (Tunnel Clients) requests for tunnel creation with a dual stack router acting as a tunnel server. In our implementation of Tunnel Broker, tunnel server is a dual stack router (we named it IPv6-Router in our scenario) which is connected with IPv6 cloud through ISP-to-ISP globally routed IPv6-in-IPv4 tunnels. This IPv6-Router is also connected with organization's internal private network; through this link tunnel broker and eventually tunnel clients are connected to this router which acts as a tunnel server.

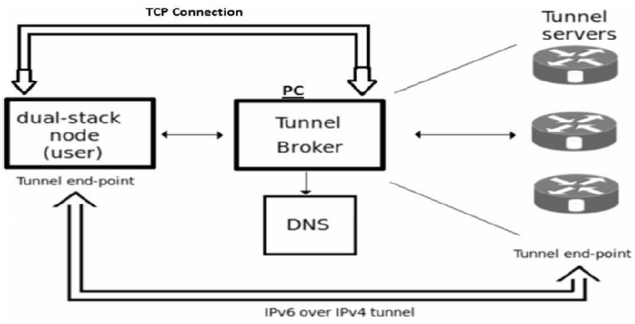

Figure 8 – Tunnel Broker Design

From a client's perspective the IPv6 access through Tunnel Broker is a four steps process, as shown in Figure 9.

Step 1: Tunnel Client (TC) connects to Tunnel Broker (TB) by establishing TCP connection with it, through an automated TC Utility.

Step 2: Tunnel Broker responds to the client with configuration parameters, required to configure client-side tunnel end point.

Step 3: Tunnel Broker establishes connection with Router to configure it remotely and automatically, according to the

client's tunnel parameters. This completes the client-to-router tunnel.

Step 4: When Tunnel Broker configures both ends of tunnel, an IPv6 connection is established between client and router

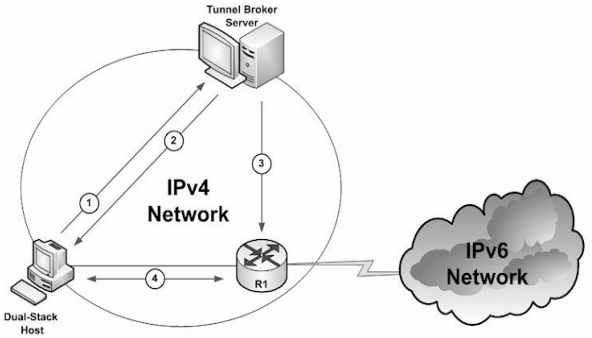

Figure 9 – Steps for IPv6 Connection Establishment

The proposed tunnel broker usage is better than the global tunnel brokers in a way that it is in a local network and provides minimum geographic distance connectivity to a user/IoT device which reduces the latency. We also control the server side and can modify the whole design according to requirements of users. We also use an efficient way of IPv6 address assignment to users i.e. we can accommodate all our users by just one /64 subnet of IPv6 address space.

IPv6 through CPE:

In the second approach we upgrade a CPE to act as a dual-stack router. In this way Users and IoT devices can communicate with the IPv6 cloud over the IPv4 infrastructure. This CPE is capable of encapsulating and decapsulating user requests for tunnel implementation.

After enabling the dual-stack mechanism in the operating system of the router, the second step in this module was the implementation of a tunneling techniques so that the home users and IoT devices can connect to IPv6 cloud. The CPE, in this case, acts like a Tunnel Broker that is connected to the IPv6 cloud, and controls all the connection parameters and authentication process.

VIII. Results

Figure 10 shows the output of an online IPv6 connectivity test. This test checks either the node is IPv6 enabled or not, if yes then it shows the global IPv6 with which we are connected to the IPv6 internet.

IX. CONCLUSION

This paper presents a discussion on IoT, its applications and challenges. To cater the address shortage for large number of IoT devices, we propose using IPv6 6LoWPAN. This protocol can be a best fit for low power devices and can provide the of using IPv6. We have also deployed IPv6-IoT connectivity by using a Tunnel Broker. This solution can be adopted for IPv6-IoT connectivity within universities, institutions, companies, enterprises or other organizations for research and testing purposes. This also emphasizes on the need of IPv6 in the near future when all the home appliances and embedded systems will be connected to the computer and internet converting everything and every place into a smart place.

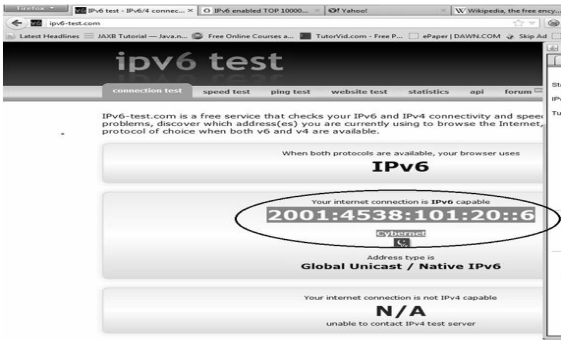

Figure 10-Online IPv6 Connectivity Test

X. References

[1] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460 (Draft Standard), Dec. 1998, updated by RFC 5095.

[2] M. Geoff "The 6LoWPAN architecture." Proceedings of the 4th workshop on Embedded networked sensors. ACM, 2007.

[3] Atzori, Luigi and Iera, Antonio and Morabito, Giacomo "The Internet of Things: A Survey" Journal of Computer and Networks, October 2010.

[4] Z. Shelby, B. Frank, and D. Sturek, "Constrained Application Protocol (CoAP),"Internet-Draft, IETF, May 2010, draft-shelbycorecoap01.txt

[5] ITU 3GPP MTC specification TS 22.368

[6] Suho Jeong, "Enabling Transparent Communication with Global ID for the Internet of Things" in 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing.

[7] Ziegler, Sébastien, et al. "IoT6–Moving to an IPv6-Based Future IoT." The Future Internet. Springer Berlin Heidelberg, 2013. 161-172.

[8] Antonio J Jara, Latif Ladid, Antonio Fernandez Gómez-Skarmeta, The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities, Journal of Wireless Mobile Networks. 2013

[9] Adeel Baig "IPv6 campus network deployment guidelines for DNS, Web server, Proxy server and Wi-Fi" IEEE Conference on Telecommunication Networks and Applications Conference (ITNAC), 2016.

[10] A. Durand, P. Fasano, I. Guardini, D. Lento, IPv6 Tunnel Broker (RFC-3053), 2001.

[11] DD-WRT Open source Linux Firmware https://www.dd-wrt.com/site/index