IOP Conf. Series: Materials Science and Engineering **260** (2017) 012033 doi:10.1088/1757-899X/260/1/012033

Network Function Virtualization (NFV) based architecture to address connectivity, interoperability and manageability challenges in Internet of Things (IoT)

Shariq Haseeb, Aisha Hassan A. Hashim, Othman O. Khalifa and Ahmad Faris Ismail

1 Kulliyyah of Engineering, International Islamic University Malaysia, Jalan Gombak, 53100 Kuala Lumpur, Selangor, Malaysia

shariqkhan1@yahoo.com

Abstract. IoT aims to interconnect sensors and actuators built into devices (also known as Things) in order for them to share data and control each other to improve existing processes for making people's life better. IoT aims to connect between all physical devices like fridges, cars, utilities, buildings and cities so that they can take advantage of small pieces of information collected by each one of these devices and derive more complex decisions. However, these devices are heterogeneous in nature because of various vendor support, connectivity options and protocol suit. Heterogeneity of such devices makes it difficult for them to leverage on each other's capabilities in the traditional IoT architecture. This paper highlights the effects of heterogeneity challenges on connectivity, interoperability, management in greater details. It also surveys some of the existing solutions adopted in the core network to solve the challenges of massive IoT deployments. Finally, the paper proposes a new architecture based on NFV to address the problems.

1. Introduction

IoT is an extension of traditional computer based Internet model to a geographically distributed, heterogeneous and constrained model of connected things. The "things" in IoT can be computers, sensors, actuators and software systems that possess communication ability. The aim of IoT is to eliminate as much as possible, erroneous human roles by automating much of the communication and actuation process [1]. Most useful IoT applications aim to provide value to people by utilizing and combining data received from various IoT systems connected to the Internet rather than single isolated sensor network.

Typical IoT architecture consists of complex systems that perform various functions ranging from sensors that collect information about the environment, tracking people, tracking things, collecting physiological measurements, collecting machine data and stores them in IoT backend with or without the help of a gateway. IoT backend is responsible for fusing these data with the help of automated business logic found in process automation to provide feedback to actuators or application. The actuators and applications automate tasks for the benefit of people and processes. The aim of IoT is to eliminate as much as possible, erroneous human roles by automating much of the communication and processes [1].

The typical IoT architecture assumes that all devices are able to interoperate and communicate with the backend which is typically cloud based. However, this is not always true because there are too many device vendors with proprietary communication stack [2], too many communication layer protocols [2], constrained nature [3] of IoT device and too many application layer interfaces [2,3]. This heterogeneity leads to isolated vertical solutions that never communicate with other systems for exchanging valuable information thus, not allowing the true potential of IoT. Moreover, it is virtually impossible to manage a large number of heterogeneous IoT devices.

There is a dire need to manage these unprecedented challenges that were not anticipated when Internet protocol was first adopted globally. The sheer amount of predicted IoT devices entering the digital world, with vast array of technologies incorporated into them, are going to be a challenge the existing architecture at every layer from connectivity to network protocols to session protocols to application protocols and network management protocols. Moreover, successful IoT deployment would also need to resolve the traditional network security challenges like End-to-End Security, Data Security, Device Identity, Personal Data Protection, Access Control and Distributed Denial of Service attack. On top of the traditional challenges, IoT devices would also face Authorization, Authentication, Integrity and Confidentiality challenges because of the constrained computation and power on the devices [4].

This paper highlights some of the existing challenges and the efforts being made by the research community to resolve these challenges. It further introduces the concepts of NFV and proposes a new architecture based on NFV to tackle these challenges. The remainder of this paper is organized into section for existing IoT architecture, connectivity challenges, interoperability challenges, management challenges, NFV concepts and NFV inspired IoT architecture.

2. Typical IoT architecture

A typical IoT architecture is shown in figure 1 [5] which, consists of two types of IoT devices with either sensing capability, actuating capability or both capabilities built into them. These IoT devices could also connect directly to the IoT backend if they are IP capable or could connect to the backend with the help of an IoT gateway.

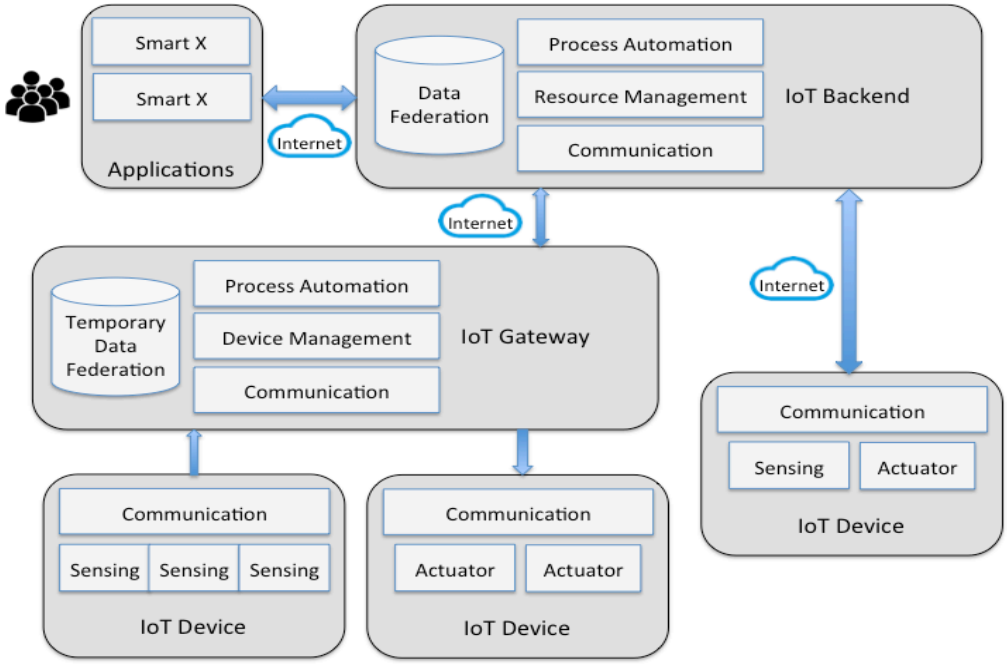

Figure 1. Typical IoT architecture

A typical gateway is meant to store, translate and forward data to the IoT backend system. Some of the more complex gateways perform proprietary device management for the IoT devices that they are serving. Furthermore, some fog [5] enabled IoT gateways also perform process automation before forwarding the processed data to the cloud backend for storage and further processing.

The cloud based IoT backend basically has the function of a large data store for analytics and process automation for actuation. Applications then communicate with the cloud backend to consume data for providing value to the users.

The entire IoT architecture, is designed to aid data flow from sensors to applications. However, the fundamental flaw in the architecture is that it offers a set of interfaces for IoT devices to push data to the backend. If the IoT device is not capable of communicating with the back end then they are unable to take advantage of the existing data on the backend. Furthermore, the IoT backend does not facilitate device to device communication, device discovery, device reachability and network management. The IoT backend is also limited by the capabilities of the physical IoT device and has no mechanism to overcome that. Further limitations are highlighted in the next sections of this paper.

3. Connectivity challenges in IoT

Connectivity is the fundamental component of IoT because transport of data from one IoT device or system to another depends very much on where they are able to connect with each other or not. Difference in connectivity protocols can be studied at various layers of the communication stack.

3.1. Physical layer

Deployment if IoT solutions depends largely on the availability and cost of the physical hardware that operates on the allowed frequency band in the country of deployment. Since the cost of IoT deployment depends largely on the mass production ability of a particular sensor/actuator, it is necessary to have some form of agreement on the allocated license frequency band for IoT. Different worldwide regulatory bodies define the frequency spectrum in different countries. For example, Federal Communications Commission (FCC) regulates radio transmissions for US and Conference of Postal and Telecommunications Administration (CEFT) for Europe. It is not an easy task to come up with a common licensed band for IoT since government auctions are used worldwide to sell spectrum bands to operators. [3] This leads to the first interoperability problem in IoT where devices manufactured for one country may not work in another.

Table 1. Worldwide ISM bands [3]

Region	Bands
America	315/433/915MHz and 2.4GHz
Europe	433/868MHz and 2.4GHz
Africa	433MHz and 2.4GHz
East Asia	315/426/950MHz and 2.4GHz
South Asia	315/433/470/780MHz and 2.4GHz
South East Asia	433/915MHz and 2.4GHz
Australia	433/915MHz and 2.4GHz

Many of the vendors have already started manufacturing IoT products on the ISM bands to work around the license spectrum issues. However, ISM bands are also not the same around the world. Table 1 [3] summarizes the available ISM bands in different parts of the world. From the table, it can be observed that the popular bands for deploying IoT solutions are 433MHz, 868MHz, 915MHz and 2.4GHz.

3.2. MAC layer

Presence of multiple vendor solutions and low-power communication technologies are the main cause of concern at the MAC layer. Different vendors have their preference on the MAC layer technologies for various reasons such as team capability, cost, ease of use etc. Various technology options at the data link layer include wired LAN, Wi-Fi, Bluetooth, ZigBee, 6LoWPAN, proprietary Sub-1GHz protocols, Power Line Communication (PLC), Fieldbus and many others. Moreover, many of the MAC protocols have already been enhanced to cater for better battery life. For example, Bluetooth has been modified to Bluetooth Low Energy (BLE) and Wi-Fi has been modified to Low-power Wi-Fi to suite the IoT power requirement [4].

Most standardization bodies are spending excessive amount of time trying to address heterogeneity at the MAC layer [4]. However, the implementation of some of these technology spans over different layers of the OSI model and makes it difficult to come to a consensus. Furthermore, standards are simply recommendations and not certification so the vendors have a choice to comply, partially comply or not to comply with the standards.

The research community is exploring cross layer protocols such has 6LoWPAN to unify the MAC and IP layer for communication [4]. However, 6LoWPAN requires the IoT devices to host computation and storage capability and that increase the cost of IoT device.

3.3. Network layer

In order to exchange information with each other, IoT devices need to be connected to the Internet or have a mechanism to push data to the Internet. Hence, they need to support the TCP/IP protocol suite that is too bulky and not cost effective for the IoT device. The Internet Engineering Task Force (IETF) has several recommendations for low powered IoT stacks that will be discussed next.

One of the biggest challenges of using reduced TCP/IP in IoT is Maximum Transmission Unit (MTU) size. IoT devices operate with much smaller MTU of about 127 bytes compared to computers, which typically assumes a minimum MTU of 1500 bytes. IPv6 specifications further complicate the situation because they include two design decisions that cause problems for small-MTU links. Firstly, fixed 40-byte header length adds too much overheads for IoT devices that produce small packets with little data. Secondly, IPv6 specifies the network to support a minimum MTU of 1280 bytes and this is unrealistic for constrained devices. The rationale behind fixed-header length is to improve protocol-processing speed and minimum MTU of 1280 bytes is to avoid in-network fragmentation. The proposed solution to this is to introduce padding and then header compression, however, padding introduces unnecessary overheads and header compression requires the nodes to have high computation and hence, higher cost of manufacturing [4].

Typical IP protocol is designed for Firstly, multi-access link, where multiple nodes are connected to the same access network and secondly, point-to-point links where there are only two nodes on a single link. However, in most IoT deployments, there is a need for mesh network where a collection of layer-2 links is joined without a presence of a layer-3 routing device. This poses a problem for legacy protocols such as Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP), Neighbor Discovery and many routing protocols as they depend on link scoped multicast, which does not work over mesh networks. Researchers are developing new intra-subnet routing protocol but these protocols are energy hungry and affect the lifetime of the IoT devices [4].

Multicast protocol is at the core of IP protocol. However, multicasting in IoT network requires the constrained IoT devices to forward packets for other nodes, thus reducing the lifespan of the battery. Furthermore, many IoT devices are designed to enter into sleeping state after transmission and are unable to process multicast packets. The solution to this problem is to redesign the IP protocol to operate only on unicast. However, devices that operate on full-IP protocol will note be able to communicate on unicast based IP protocol [4].

Traditional mesh routing protocols also need to be modified for use in IoT networks because they are designed to flood the network while IoT networks don't perform well under those scenarios. There

are already some proposals at IETF 802.15.5 standards to support link-layer routing for mesh networks [4].

The current IP mobility protocols are also not suitable for IoT use cases because firstly, they impose too many message exchanges for establishing mobility that affects the battery life of the IoT devices and secondly, and IoT device may not have the full mobile IP stack deployed on them as they are memory and CPU constrained [6]. The research community is considering many variations of the network-based mobility schemes. One such scheme is Sensor Proxy Mobile IPv6 (SPMIPv6) which introduces few components such as Sensor Local Mobility Anchor (SLMA) and Sensor Mobility Access Gateway (SMAG). SLMA could be a high-end computer as it resides in traditional network while SMAG could be one of the IoT nodes that have higher resource compared to the other nodes in the Network [7,8]. Inter-MARIO and LoWMob are yet other protocols for mobility management in IoT. They are designed with the make-before-break concept in mind where several static nodes in the IoT network known as partner nodes serve as access points for the MN and preconfigure future partner nodes before the MN moves to those networks [7]. However, To-date mobility in IoT is still a research focus area as the existing schemes are a mere adoption of existing mobility concepts in IPv4 and IPv6 which require the nodes that are involved in the mobility process to have high computational and power resources.

3.4. Transport layer

Transport layer in the Internet provides congestion control, guaranteed and in-order delivery of packets. These provisions are effectively used by the TCP protocol. However, TCP is not suited for IoT applications as IoT devices offer a varying traffic pattern due to their limitations. For example, firstly, due to the energy conservation requirements, IoT devices usually go into sleep mode after transmission or receiving the packet, making it difficult to maintain the communication and acknowledgement channels. Secondly, IoT devices send/receive only small amounts of data and TCP handshakes impose too much overheads for the devices. Thirdly, IoT applications have low latency requirements and TCP has too much delay in setting up communication. Finally, IoT applications operate in lossy domain, so in-order delivery and retransmission would block the communication until all previous packets have been successfully delivered. [4]

Some of the IoT protocols like ZigBee still maintain support for TCP, while the rest of the protocols like BACnet and CoAP have proposed to build TCP like transport functionality in the application layer and use UDP as the transport protocol.

4. Interoperability challenges in IoT

Heterogeneity in IoT solutions leads to Interoperability problems between IoT systems. Without interoperability, IoT deployments will be isolate to their use case and the data generated by one system can be consumed by other systems. Interoperability issues happen due to multi-vendor solutions and presence of legacy sensor network based solutions that have been deployed before the concepts of IoT was introduced.

4.1. Multi-Vendor problem

Standardization bodies only offer best practices for IoT. These recommendations only serve as guidelines for bodies that offer certification for IoT products. The certification bodes often adopt just a portion of the standards. Four well known bodies that manage certification programs today to ensure heterogeneous interoperability between IoT devices are Wi-Fi Alliance for wireless LAN technology, Bluetooth Special Interest Group (SIG) for Bluetooth enabled devices, ZigBee Alliance for ZigBee compatible devices and LoRa alliance for wide area IoT devices [3].

However, the problem lies in the fact that these certifications drive up the cost of IoT deployment and many vendors choose not to conform to the standards so that they can keep the cost down and offer value added services that can give them edge over their competitors.

4.2. Legacy solutions

Many vendors and solution providers have been offering closed loop vertical solutions like building management, home automation, vehicle tracking, personnel tracking, etc. The problem with these solutions is that they were never designed to connect to the Internet so their data is contained within their domain. The challenge faced today by IoT because of these solutions is that firstly, it is too expensive to upgrade these systems to take advantage of IoT and secondly, the data models deployed in these systems are based on old database technology like relational databases, which may not conform to the concepts of non-relational Big Databases. This gives opportunity to the research community to develop IoT middleware that can translate between legacy systems and newer IoT system. The middleware employs the concept of protocol translation and offers node resource discovery so that IoT systems can take advantage of the legacy systems [8].

5. Management challenges in IoT

Network management is the biggest challenge in large-scale network deployments. In IoT networks, this is an even bigger problem due to the sheer number of IoT devices. Traditional management protocols for remote control, monitoring and maintenance such as Simple Network Management Protocol (SNMP) will not work with IoT devices because they are too demanding in terms of computation, storage and networking resources. Moreover, they need the IoT devices to support the IP protocol stack [8,10].

Table 2. Management issues

Management issue	Description
Configuration Management	• How to setup IoT device one at a time and in batches • IoT device ownership • IoT device to single and multiple application relationship • Network connectivity • Asynchronous Transaction support • Network re-configurability
IoT Device Control	• Turning IoT device on and off • Disconnecting IoT device from network • Waking up and sending IoT devices to sleep
Monitoring	• Determining the status of IoT devices. To know if they are running, listening, down, sleeping etc. • Network status monitoring • Network topology discovery • Notification • IoT device logs

IoT Device maintenance	• Detecting network failure • Detecting Device failure • Over the air software update • Patch updates • Protocol version update
IoT Device Performance	• Monitoring network performance • Monitoring IoT device QoS
Security and Privacy	• Authorization of IoT devices • Authentication of IoT devices • Access control of IoT devices • Security bootstrapping mechanisms • IoT device ownership • IoT device to application authorization
IoT Device Energy Management	• Management of energy resource • Energy level management • Estimated lifespan before battery change

Table 2 summaries all the management issues in IoT that are being considered by researchers in this field. Each area in the first column is further described in the second column. Only when all of these issues are resolved, IoT would become manageable and would require lesser human intervention [11,12,13].

6. Concepts of NFV

NFV has been popularized by the telecommunication companies (Telcos), who have been suffering from the interoperability problems in their core networks. In 2012, more than 20 worlds' largest Telcos formed the Industry Specification Group (ISG) within the European Telecommunications Standard (ETSI) device a mechanism to virtualize their propriety core network hardware. It was aimed at addressing the operational challenges, high costs of managing closed and proprietary appliances and heterogeneity of device.

Heterogeneity is telco networks results in following issues [14]:

- Fixed Configuration: the telco hardware is configured with fixed IP locations that remain unchanged for years resulting in very rigid resource allocation.
- Manual management: configuration and management of telco equipment requires movement of physical staff and can be done one at a time. Hence, it's difficult to implement a common centralized policy.
- Rapid growth of IP end points: Telcos offer Internet access to large number of users and this is expanding as the consumer base grows. Hence its difficult if no central provisioning is established.
- Network endpoint mobility: networks are fixed and too rigid to move around so requirements for mobility takes long time to reconfigure the network for different scenarios.
- Elasticity: there is no mechanism to upgrade and downgrade a physical hardware based on demand so the networks have to be over provisioned.
- Multi-tenancy: usually one end-point equipment is configured for a single tenant and dynamic or multiple tenant is impossible on vendor define hardware as vendors always wants Telcos to buy more hardware.

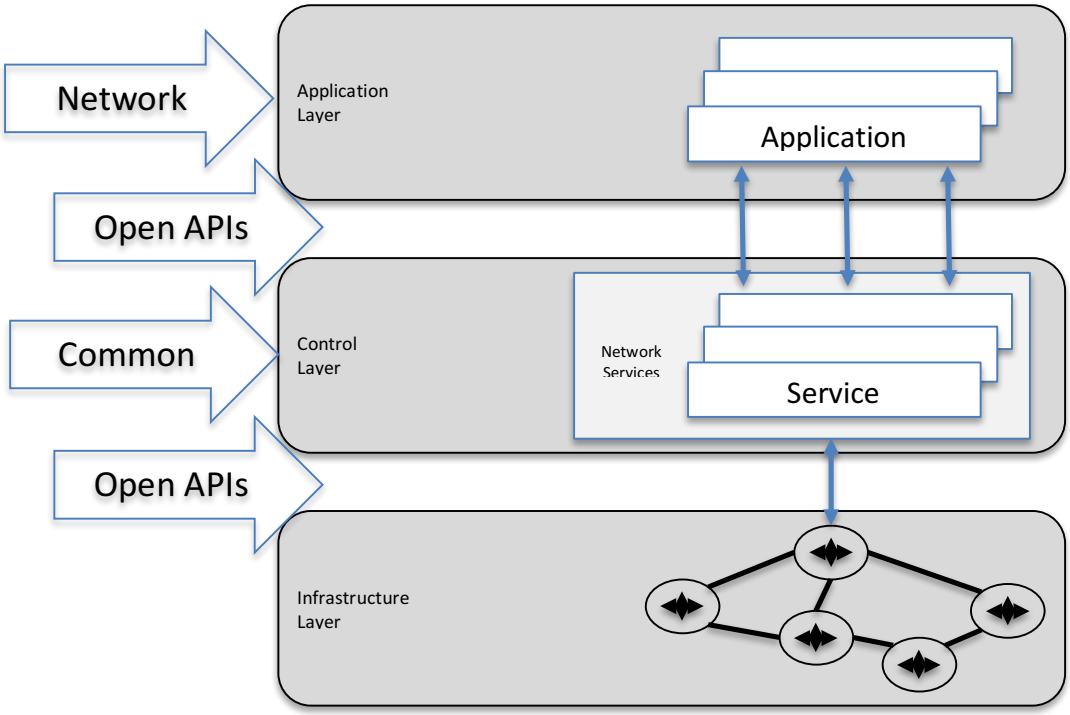

Figure 2. Typical NFV Architecture

In order to solve all these interoperability and management issues, ETSI has proposed a new architecture shown in figure 2 [15]. In this new architecture, Telco equipment (infrastructure layer) has been changed to dumb switches with only packet forwarding capabilities. Control layer has been separated from the hardware in order to enable centralized policy and dynamic resource allocation based on the need. Finally, application layer has been moved to the cloud to have virtually unlimited resources. This application layer could function as a firewall, DNS, load balance etc. and then communicates via software APIs to the control and infrastructure layer. Resulting in the entire core network to operate as a software that is independent of the limitations of the hardware and vendor specific protocols [16].

IoT today faces similar problems as Telcos did with their core network equipment and the NFV route seems like the best option for them. We have been inspired by this approach to solve the problem cause by heterogeneous devices in IoT. Our proposed architecture for virtualizing IoT devices is discussed in the next section.

7. Proposed IoT Architecture

Our proposed IoT architecture leverages on the existing architecture and the lessons learned from the NFV architecture. The new architecture is shown in figure 3 where, the IoT device could simply be a dumb device with purely a communication interface coupled with sensing or actuating capabilities. They could either directly connect to the IoT backend of connect with the help of an IoT Gateway. The IoT gateways would also be lightweight because they only need to maintain a device registry to know the IoT devices connected to it. The gateways also need to host two communication stacks for connecting to the IoT devices and the IoT backend.

The real change has to be made on the IoT backend that has to host more capabilities than the traditional IoT backend. The IoT backend would reside on the cloud to take advantage of the virtually unlimited resources available in the cloud infrastructure. The IoT backed would need to allow device virtualization where each dumb IoT device would be represented by a virtual IoT device. The virtual

IoT device will emulate the physical device capabilities but would be represented as a software code in the IoT backed. The important parameters of an IoT device that need to be emulated are as follows:

- Device ID: a unique device ID to identify it on the IoT backend. This is could follow the standard MAC address or an incremental email address format.
- IoT Device IP (Optional): this is the IP address of the IoT device in its current network.
- Gateway ID (Optional): a unique gateway ID to identify it on the IoT backend. This is could follow the standard MAC address or an incremental email address format.
- Gateway IP (Optional): this is the IP address of the gateway in its current network.
- CPU Utilization: the CPU utilization of the IoT device as a data stream to the IoT backend.
- Memory Utilization: the memory utilization of the IoT device as a data stream to the IoT backend.
- Battery Level: the battery utilization of the IoT device as a data stream to the IoT backend.
- Data Stream: type of data that the IoT device is generating.
- Service Stream: types of services offered by the IoT device.
- Status Stream: current status of the IoT device that could be online, offline, asleep etc.
- Location (optional): longitude and latitude of the IoT device.

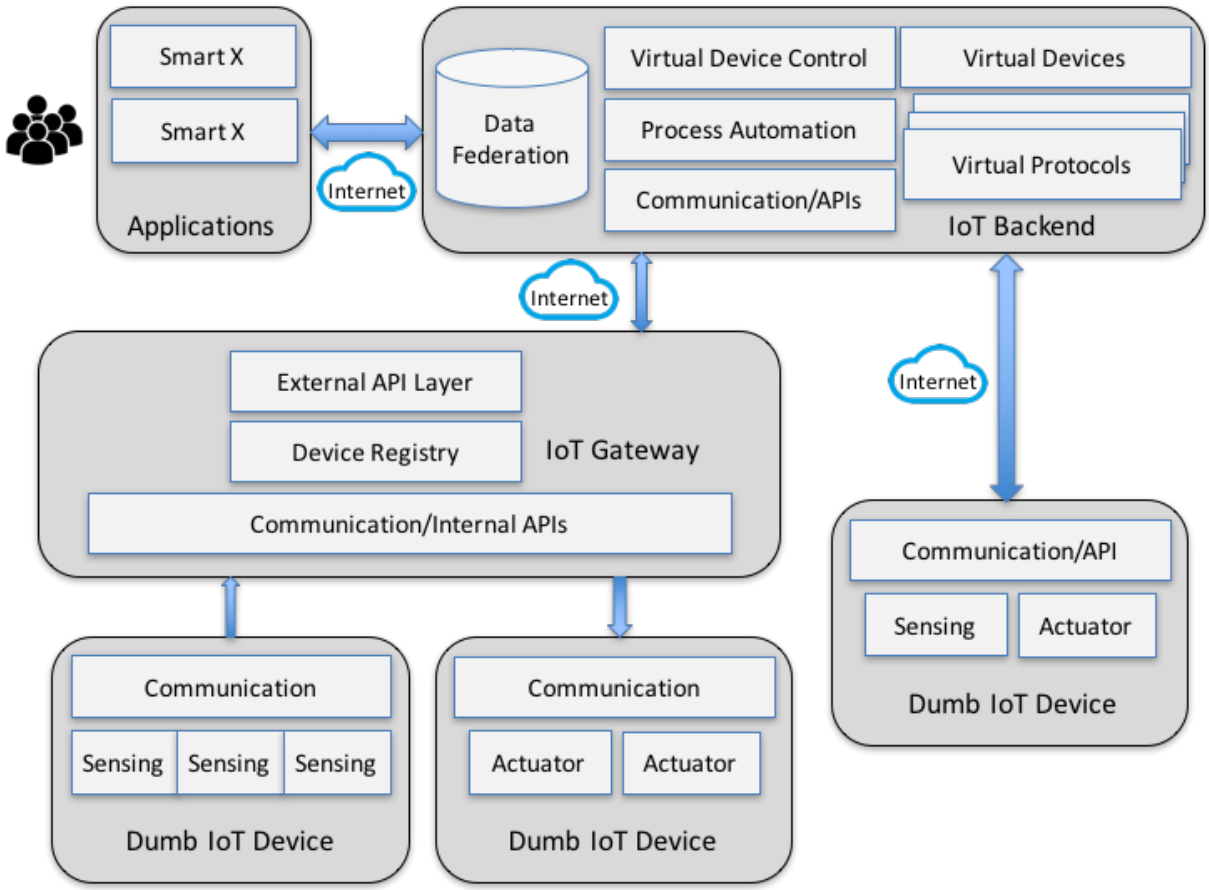

Figure 3. Proposed IoT Architecture

With the help of these parameters, a virtual IoT device can be created in the IoT backend. The IoT backend would need the status updates from the IoT devices either periodically or in real-time to maintain the device.

Once a device has been virtualized, it is no longer constrained to the physical limitations and vendor specific restrictions. The IoT backend can group the virtual devices into virtual networks by assigning IP protocols suite to the virtual devices. An IP capable virtual device can than take advantage of more complex protocols like Domain Name Service based Service Discovery, Constrained Application Protocol (COAP) for application layer protocol and Reachability Protocol (REAP) for device status discover in order to achieve IoT device interoperability. Simple Network Management Protocol Version 3 (SNMPv3) can also be used to manage large number for virtual IoT devices.

8. Conclusion

Internet designed for unconstrained devices with large amount of computation power. It was never designed for IoT, however the demand for IoT has forced the research community to retrofit the existing protocols into IoT and develop the IoT architecture. The existing IoT architecture suffers from connectivity, interoperability, manageability challenges due to the heterogeneous nature of the devices that are controlled by vendors. The Telcos faced similar heterogeneity problem in their core networks and are resorting to NFV for solving their problems. In this paper, we proposed a new architecture for IoT that has been inspired by concepts of NFV in order to tackle the problems in IoT. Future work for this architecture is to simulate the operations of the architecture and demonstrate it with a testbed.

References

[1] 811106755049Elkhodr M, Shahrestani S and Cheung H 2016 The Internet of Things : New Interoperability, Management and Security Challenges *Int. J. Netw. Secur. Its Appl.* 8 85–102

[2] Sutaria R and Govindachari R 2013 Making sense of interoperability: Protocols and Standardization initiatives in IOT *2nd International Workshop on Computing and Networking for Internet of Things (CoMNet-IoT) held in conjunction with 14th International Conference on Distributed Computing and Networking (ICDCN 2013)* pp 2–5

[3] Reiter G 2014 *Wireless connectivity for the Internet of Things. Europe, 433, 868MHz*

[4] Shang W, Yu Y, Zhang L and Droms R 2016 *Challenges in IoT Networking via TCP/IP Architecture* vol 8

[5] 5' Constant N, Borthakur D, Abtahi M, Dubey H and Mankodiya K 2017 Fog-Assisted wIoT: A Smart Fog Gateway for End-to-End Analytics in Wearable Internet of Things

[6] Silva R, Silva J and Boavida F 2014 Mobility in wireless sensor networks–Survey and proposal *Comput. Commun.*

[7] Sinniah G R, Suryady Z, Sarwar U and Hoey T K 2013 Node Mobility Scheme for IP and Non-IP Wireless Personal Area Network Nodes using 6LoWPAN *SENSORCOMM 2013 Seventh Int. Conf. Sens. Technol. Appl.* 83–9

[8] Richards T and Srivastav V 2014 Enabling communication of non-IP device in an IP-based infrastructure *US Pat. 8,837,485*

[9] Silva R, Silva J and Boavida F 2014 Mobility in wireless sensor networks–Survey and proposal *Comput. Commun.*

[10] Sheng Z, Yang S, Yu Y and Vasilakos A 2013 A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities *IEEE Wirel.*

[11] Marotta M A, Both C B, Rochol J, Granville L Z and Tarouco L M R 2015 Evaluating management architectures for Internet of Things devices *IFIP Wirel. Days* 2015–Janua

[12] Vasilomanolakis E, Daubert J, Luthra M, Gazis V, Wiesmaier A and Kikiras P 2016 On the Security and Privacy of Internet of Things Architectures and Systems *Proceedings - 2015 International Workshop on Secure Internet of Things, SIoT 2015* pp 49–57

[13] Sutaria R and Govindachari R 2013 Making sense of interoperability: Protocols and Standardization initiatives in IOT *2nd International Workshop on Computing and Networking for Internet of Things (CoMNet-IoT) held in conjunction with 14th International*

Conference on Distributed Computing and Networking (ICDCN 2013) pp 2–5
[14] Bernardos C J, Rahman A, Zuniga J C, Contreras L M and Aranda P 2016 *Network Virtualization Research Challenges (Research Report No.03)*
[15] Malcolm B, Nigel D, Rob D, Paul D, Steve F, Dave H, Mandar J and Kam L 2014 *SDN Architecture*
[16] Shin M K, Nam K, Pack S, Lee S and Krishnan R 2016 *Verification of NFV Services : Problem Statement and Challenges (Research Report No.02)*