Egyptian Informatics Journal 20 (2019) 1–10

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Cloud based SDN and NFV architectures for IoT infrastructure

Mamdouh Alenezi [a,*], Khaled Almustafa [a], Khalim Amjad Meerja [b]

[a] Prince Sultan University, Saudi Arabia
[b] V R Siddhartha Engineering College, India

ARTICLE INFO

Article history:
Received 21 November 2017
Revised 27 February 2018
Accepted 24 March 2018
Available online 9 April 2018

Keywords:
Computer networks
Software defined networking (SDN)
Network function virtualization (NFV)
4G

ABSTRACT

Connected devices which are commonly known as Internet of Things (IoT) are increasing at an alarming pace. Network infrastructure has to accommodate all these devices by providing adequate connectivity and delivering application based services. Service providers have to invest more in network infrastructure to meet the growing needs. To address this issue, a new concept of infrastructure sharing among service providers has emerged to reduce excessive investment costs related to infrastructure deployment. For this reason new architectures based on network virtualization are emerging to provide network sharing, handle Big data explosion from IoT devices, and simplify management tasks. Two complementary architectures, software defined networking (SDN) and network function virtualization (NFV) are emerging to comprehensively address several networking issues. In this work, we introduce the most embraced virtualization concepts proposed by SDN and NFV architectures. We quantitatively evaluate hardware and energy cost savings with these two SDN and NFV architectures compared to the existing state-of-the-art network 4G hardware technologies.

1. Introduction

Connected devices on the Internet which are commonly known as Internet of Things (IoT) are increasing continuously at an alarming pace. There should be adequate network infrastructure facilities to handle the data explosion. One challenge is that IoT devices are globally distributed. The network infrastructure should be able to reach all these globally distributed devices. This is an enormous challenge and a huge investment in infrastructure by any single service provider. Since users are subscribed to many different service providers, and are globally distributed, it is impossible for each service provider to have its own separate network to serve its own subscribers. As new technology emerges, the hardware becomes quickly obsolete leading to huge recurring costs by each service provider [31,7].

A new sharable architecture is needed which is flexible to the changing demands of the subscribers of each service provider. This is particularly the case when the number of subscribers are changing for each of the service providers. The demand for the network resources will always be dynamically changing. Service providers will be able to borrow resources from the sharable network architecture and also relinquish those resources based on the demand of its subscribers. As a result, sharable architecture would ensure that adequate resources are allocated to the service providers based on their current needs, and plan to reserve resources for future predicted needs.

Another key issue is the network reconfiguration required in order to accommodate changing traffic characteristics such as bandwidth and delay requirements [10]. The security and service provisioning policies will keep on changing with time as new business applications are added to serve users on the network [1]. Packet handling policies have to be modified and high layer processing may have to be incorporated to newly added traffic [18]. As a result the location of the firewalls, load balancers, and other special purpose gateways have to be changed based on new policies. Such reconfiguration will be an issue in the shared network scenario when multiple service providers will be using a common network infrastructure. Because of all these concerns, isolation of network resources and strict confidentiality must be maintained between service providers. This will be made possible through

* Corresponding author.
E-mail addresses: malenezi@psu.edu.sa (M. Alenezi), klamustafa@psu.edu.sa (K. Almustafa), kmeerja@gmail.com (K.A. Meerja).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.eij.2018.03.004
1110-8665/

newly developing technologies based on software defined networks (SDN) and network function virtualization (NFV).

In this work, futuristic SDN and NFV architectures are discussed. Cost analysis is performed to analyze the benefits of such sharable SDN and NFV based network architectures.

2. Challenges for future networks

Technology usage and its forecasted demand is growing at a very rapid phase [4]. To catchup with the demand, research and innovation is continuously providing better and more efficient solutions in the field of data communication networks [13,36]. These new solutions are essential as previous existing solutions are quickly becoming obsolete [24,12]. It is not just because we have better understanding of the technology with passing of time, but predominantly because of growing concerns and new requirements. New users are constantly being added to the networks daily as well as new types of network services. Both added number of users and new kinds of services are demanding huge network resources and this demand is growing exponentially [11,22,9].

There has been a colossal increase in the number of connected devices, exceeding beyond what has been thought for the data communication networks, that it could to handle such huge number of devices at present and in the near future [17,16]. A clean slate solution is required for data communications network technology that can withstand explosive growth in terms of the number of devices that can be serviced through a single network solution. Such a solution has to also provision services to futuristic network based applications developed for future needs that may demand larger chunks of network resources. The network solution has to keep track of continuous movement of devices and users, make their data available readily for them within time according to their desired quality of service. The network solution has to be resilient by seamlessly fixing network breakdowns and other sort of failures through quick recovery mechanisms.

It is important to look at various factors that add cost to deploy networks to serve trillions of devices interconnected together to form Internet of Things (IoT) [33]. First of all, it must be noted that the end devices are very diverse in nature. Specialized network behavior and services are needed to operate these diverse IoT devices [20,19,35]. Each type of application needs a different network policy to treat its data traffic differently based on underlining confidentiality, integrity, and overall security. The previous trend was to build specialized network functionality in hardware to speedup network operations. These specialized network devices have to be carefully placed in the network depending on the different kinds of services offered by the network service providers.

It is prohibitively expensive for service providers to own site locations and network infrastructure over a large geographical region. It is easier and economical to lease network resources from other infrastructure providers in certain parts of the regions to provide services to their customers in those locations. With this necessity, comes a new requirement to share network resources among multiple service providers. These infrastructure providers must have the capability to provide network resources on required basis to network service providers through proper partitioning and isolation mechanisms.

The key solution to all these problems is network virtualization [5]. Through the concept of network virtualization, all the network elements will be programmable using a single standard user interface and can be controlled remotely from any of the chosen central locations. All network operations will be automated under the new framework as network elements are implemented completely in software. The role of a certain network element can be easily changed by redefining the network function of that element. The following sections discusses further on virtualization of network element functions.

3. Concept of network virtualization

The present network scenario and future envisaged virtual network scenarios are depicted in Fig. 1. First consider the present traditional network scenario. In this scenario, all these different devices are spread throughout the entire network. Since each device has fixed network functionality, the device location has to be carefully planned within the network. After some duration of time, if the network layout has to be changed to accommodate new requirements, these network devices have to be rearranged, reconnected, and then reconfigured individually. Since the control function of each device is embedded into it, each device presents a separate management interface that has to be accessed individually. Sometimes new devices have to be added and the old ones have to be discarded, wasting network infrastructure resources. All these reasons leads to higher infrastructure, operations, and management costs.

On the other hand, the idea of future network architectures that predominantly bring software virtualization in practice is shown in Fig. 1. It can be seen that most of the infrastructure is simply a bank of COTS servers and switches created as a hardware pool. These hardware pools can host many virtual network devices that have different functionalities. Virtual network functions created in software access underlying hardware through standard interface. This will allow a service provider to instantaneously create, delete, and modify network functions as needed on daily basis. This added flexibility allows hardware resources to be diverted to actual needs of service providers. Software programmability of virtual network devices, created on COTS based server pool, allows service providers to experiment new concepts without major service interruption. No considerable additional new infrastructure investment is needed to tryout new technologies. Network capacity can be upgraded by simply adding more COTS servers to the existing server pool. Virtual networks built on these software implemented network functions are highly flexible, easily allowing reconfigurations and addressing new network layouts. It is possible to have one single management interface and the complete network can be controlled from a single or multiple central locations. As a result, network operations and management is a very simple and cost effective affair compared to handling specialized hardware based networks.

3.1. Implementing network elements in software

The idea is based on the old preexisting original concept of implementing all sorts of network functions virtually in software using the same basic hardware resources. This concept is being revisited due to the current ability to manufacture cheap but powerful COTS hardware. Now, the virtual network functions created in software can consume any amount of hardware resources as required. Many virtual network functions can share a single physical hardware or a pool of hardware resources as shown in Fig. 2.

Fig. 2 shows a single COTS server along with proper forwarding hardware which is hosting many virtual network functions (VNF). Each VNF can be a server by itself, a router, a gateway, a load balancer, a proxy, or a firewall to name a few. Generally, more than one of these physical servers and forwarding units are bundled as hardware resources pool to host multiple VNFs. This is for addressing dynamically changing hardware resource requirement by individual VNF instances. This scenario is also shown in Fig. 2, where it is seen that many VNFs are sharing a pool of hardware resources.

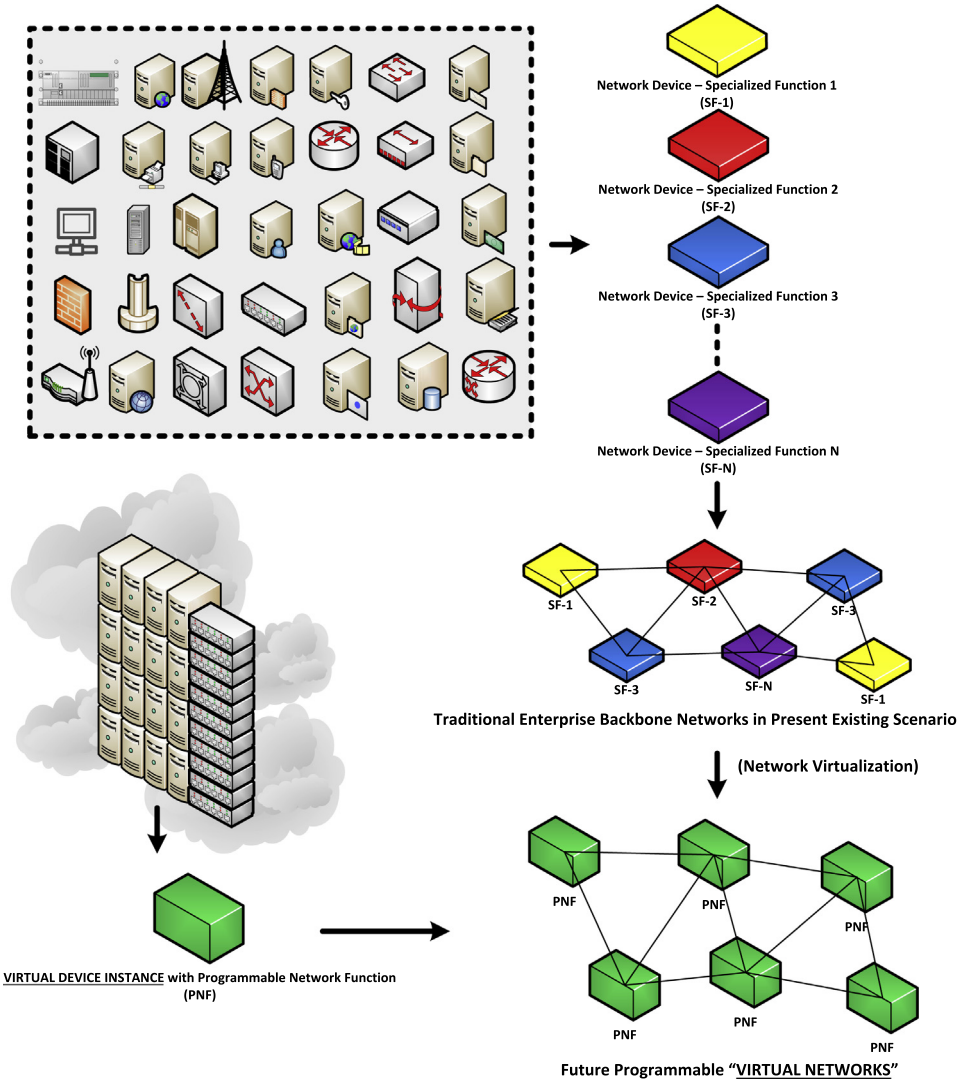


Fig. 1. Evolution of future "VIRTUAL NETWORKS" from existing specialized hardware based networks.

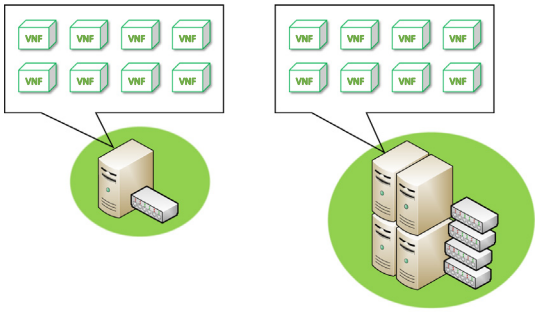


Fig. 2. Virtual network function realization in software.

It is absolutely necessary to clearly distinguish the role of infrastructure providers, network service providers, and network operators. Their relation with each other must be identified and should be relied on for a very long time. Because, when this changes, everything including the technological requirement changes. The business model developed to address market demand is the corner stone for the evolution, acceptance, growth and ultimate popularity of any typical kind of technology. The terminology used in this paper considers network operators as the end users of network services who depend on it for performing their core business operations. They are businesses such as application and content providers, academic and non-academic institutions, federal public and private services, and commercial and financial agencies.

Network operators rely on network functional resources that are purchased as a service from a third party as per on demand basis. By doing so, they will be relieved from having to invest and maintain their own network, upgrade it with time due to business expansion. They will instead focus on their core business and invest everything in it and avoid having to deal with continuous upfront costs involved in operating and upgrading their own private network infrastructure.

On the other extreme end, infrastructure providers will procure sites all around the geography and install network infrastructure in those locations. Their business is to offer their hardware to clients through means of highly resilient software based network hardware virtualization. They will offer raw computational, storage, and forwarding resources as fine tunable virtual hardware resources. The clients will be charged based only on their actual usage through a "pay as you go" billing scheme. Through hardware virtualization, the physical resources are shared among multiple

clients who are normally the intermediate network service providers.

The network service providers will play the role as intermediators between the actual hardware infrastructure providers and the end network operators who are the ultimate users of the network services for functioning of their main business. The network service providers, as can seen in Fig. 3, can remotely create and maintain numerous networks for their end clients using virtual hardware resources acquired form infrastructure provider. The network service providers will create VNFs and connect them to different networks that are either for public or private use. The network service providers themselves can be many who have purchased virtual hardware resources from the same infrastructure provider. They all might be competing with each other to maintain their lead in this business by attracting more network operators as their clients. For this reason, they come up with their own network policies, service quality agreements, and billing options to remain profitable in their business.

So the objective of future generation networks is to have the ability to remotely create, control, and manage networks of virtual resources which are interconnected VNFs created in software. The network topology can be changed without manual intervention. The capacity of VNFs can be increased or decreased based on the need. This eliminates the situation of over-provisioning or under-provisioning resources to certain client and thus be able to always maintain the service quality based on the contractual agreement.

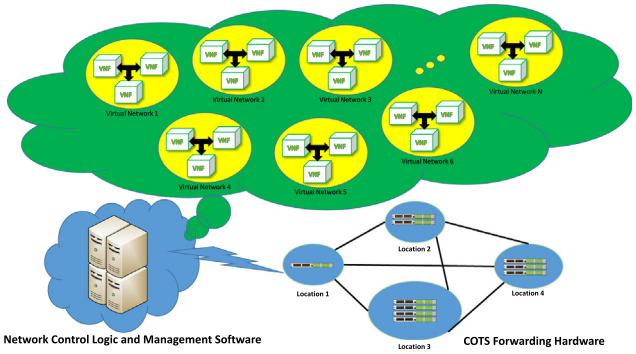


Fig. 3. Multiple virtual networks built using software implemented network element functions. The network control and management software in cloud performs the sharing of underlying COTS based forwarding hardware infrastructure, spread over various geographically separated locations.

Complex network policies can be implemented through fine grain network resource control and configuration. Network policies can be instantly applied and tested without any service interruption. New innovations in network technologies can be embraced in software easily without considerable investment.

To achieve the dream goal of futuristic capability networks portrayed in Fig. 3, the network architecture has to undergo complete transformation. A complete new architecture is needed to incorporate virtualization in physical hardware. Much of the theory can be borrowed from the existing knowledge and apply to current needs and network scenarios. Two profound approaches are used immensely to create a network element in software known as VNF. These two approaches are different but complementary and can be roughly be compared as shown in Fig. 4. The main difference in these approaches is that, one approach retains the control plane in the physical device. While the other approach separates the control function from the physical device so that the device only performs the data forwarding function or some other function for which it was built.

The architecture allows the control plane to be embedded in the physical device to acknowledge the practice that exists in current hardware manufacturing process. This is an intermediate solution instead of complete overhaul in the architecture. In this architecture, the physical hardware is covered with a layer of software that will manage the physical resources. This software layer will prevent applications from directly accessing physical device. This is known as virtualization software, which in this architecture is referred as hypervisor. There is another small piece of software layer that addresses cross-platform issues. These two layers together will provide the means for virtually provisioning the device resources. VNFs are created which these virtual resources that emulate the exact functionality of the desired network element. VNFs are nothing but specialized network functionality elements created virtually in software as a replacement for the specialized network hardware built for exactly the same purpose. VNFs created according to this architecture uses the logically available resources that are made available through the hypervisor. The capability of VNFs can be carefully tailored through proper provisioning of logically available slices of physical device resources.

The other major architecture under discussion suggests a complete overhaul to the current network device manufacturing process. It does not advocate leaving the control plane in the device. So, it removes the control plane from the hardware, thus encouraging manufacturing of general purpose network devices that does only data forwarding. There will be a separate software controller

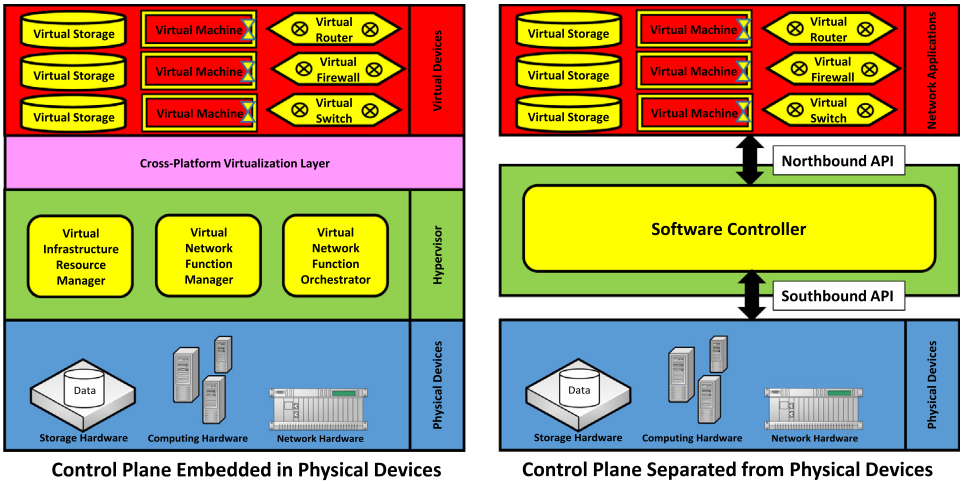


Fig. 4. Software implementation of virtual device resources.

that will be controlling all devices in the network. This is also known as network operating system. The software controller will interface with physical devices using southbound API. The software controller will provide a northbound API that is accessed by the network applications designed for specific network functionality. These network applications will create the required VNFs that are under the control of the software controller. Look at Fig. 4 for layer by layer comparison of the two architecture that are used to create network elements in software.

3.2. Using the cloud platform for implementing network functions in software

Cloud platform is an ideal network solution to provide various forms of services such as virtual hardware as service, virtual network functions and platform as a service, and finally the applications and software as service. The idea of having cloud networks is to be able to serve globally, have theoretically infinite capacity that is elastic to changing requirements, be highly resilient and secure, and to have the ability to provide metered service. The infrastructure providers will use the cloud environment to launch their virtual hardware resources as a service that is made available globally to its clients. The network service providers will use this global availability service to create virtual networks and VNFs for their clients who will be the actual network operators. The network service providers will build networks to their network operator clients who will use them to do their business. The network operators will be able to create applications and software services to their end users, who are the ultimate consumers of the network services. These network services could be accessing to Internet to participate in social networks, using certain piece of software in their home or office work, acquiring news and information, performing video conference, etc.

The requirements of future generation networks such as infrastructure resources pooling and sharing, service on demand, simple interface to encourage self-service, multiple graded service quality for broad network access, and many other desired features are inherently offered with the concept of cloud networks. This concept of cloud networks is realized through interconnection of distributed data centers with high bandwidth links. These data centers hosts huge number of server pools along with network related hardware that are readily available to perform virtualization. Because of the large scale deployment of the infrastructure, it will be economical to perform research and development to build more powerful software virtualization frameworks and constantly improve them over time. Since the predicted savings are huge under cloud networks, all the stakeholders are constantly looking into investing in this framework to further improve and expand the services using this model. The main advantage of cloud networks is that, they provide a huge potential where small investments have large impact in terms of improvement in the services offered in the global market. These cloud networks easily launch highly complex, scientifically related services such as grid computing and autonomic computing. On the other hand they also provide utility based computing to less sophisticated users.

Cloud networks are moving towards providing highly available network services of any kind ranging from infrastructure to the end user applications. Physical and logical network topologies are built to ensure adequate degree of redundancy and high availability. Network protocols are designed to ensure secure delivery of data to pertinent users without any compromise on confidentiality and authenticity. These network protocols have to deliver data within the time duration, not exceeding the maximum tolerable delay. In other words, full conformance to the service level agreements (SLA) has to be met under all circumstances. Each network user has a different requirement. Users requirement constantly change with time, and they are also not always fixed in number as they come and go depending on their needs. Cloud networks make use of software virtualization framework discussed before to offer multitenancy features to support multiple applications on the same hardware and software infrastructure. The challenging issue here is to properly share all the underlying resources. At the same time the framework used in the cloud should provide complete isolation between the multitenent applications. Addition of new applications should not degrade the performance of already existing applications. To that extent, the cloud network must be elastic to gracefully respond to changing load on the network.

One of the prime concerns of our networks today is scalability. Everyone is spending more time online, seeking higher data transfer rates, larger storage capacities, more computational power. This huge data cannot be handled properly in real-time without addition of new network infrastructure. Resources are expensive, consume lot of energy which is a burden on the environment. Technology has to rapidly catchup with the high demand which is now unstoppable under any circumstances. The solutions must be cheap, quickly deployable, and energy conservative. The data presented in these networks will be highly unstructured, semi-structured, and structured. Under any case, the data has to be manipulated to extract knowledge and information for daily living. The cloud networks adopting a proper software virtualization framework is the way ahead to address the scalability issues and to tackle the huge data generation. So, our main concern is how to efficiently tackle Big Data emerging from IoT devices and other forms of network users. The key lies in developing a highly scalable cloud based software virtualization framework.

3.3. Resource provisioning for big data handling

Many experts in industry related to information technology and data networks will immediately conclude that the obvious major sources of data in future would be IoT devices and social networks. When Big Data grows, the concern over its trustworthiness also increases. The data also has to be highly accessible through a simple query mechanism. This is a necessary because the success of any data analysis activity depends on the degree of data availability. If relevant data is readily available, quick and accurate decisions can be drawn from the analytical activity [21,29]. Decisions based on accurate data analysis will have profound effect on taking sound decisions to improve any business activity. Another major aspect is the speed with which the data can be transferred between relevant users so that they can quickly correlate data to jointly extract and exchange knowledge as well as information. By doing so, they will be able to come up with decisions in time and do not miss any major opportunities. This is crucial for any business to remain ahead of their counterparts.

The currently available storage technology using solid-state devices (SSDs) is very slow to fully embrace even the minimum requirements of Big Data Analysis that is needed today. The future is even more challenging and some intermediate storage solutions are required. This could be some solution that innovatively emulates a more faster distributed storage. This will be needed until a new radically different storage technology comes into marketplace [38,37]. It is envisaged that holographic storage technology will come to the rescue, but it is still at least a decade away from coming to mainstream usage. Added to this the data is stored in locations that are geographically far apart. Data from different regions must be fetched for analysis, which puts lot of stress on communication links connecting these remotely located storages.

Due to all these constraints, network resources have to be diverted beforehand and reserved for Big Data Analysis carried out by certain user [6]. The concept of time domain multiplexing can be used to cater the requirements of different clients who have

active periods during different timeframes. This will lessen the burden on the required network resources. Routing techniques can also be used to intelligently transfer data between the destination nodes in the network so that the overall consumption of the network resources in very minimal [30]. Thus optimal network scheduling and resource provisioning policies play crucial role to enhance the experience of Big Data Consumption [25]. Carefully designed quality of service provisioning mechanisms and traffic admission schemes are essential until there is a major boost in the network capacity in all forms. Network management strategies have to overcome the bottlenecks of read/write speeds of storage devices and data transfer rates of communication links.

IoT devices are dispersed all round different regions and very remote locations [27,23]. They are often located at a far distance, difficult to physically reach and can be accessed only through a highly unreliable wireless communication medium. Since IoT devices will many times be placed in hostile environments that are subjected to high levels of surrounding noise and interference, the quality of communication will be poor. Still data has to be extracted from such devices using energy efficient means. The data will be intermediately transmitted to data sinks that have better and more reliable communication links to the central processing locations [3]. Due to many limitations on the capacity of such sink nodes, appropriate data storage and forwarding mechanisms must be designed. Optimal policies have to be framed to decide on the location of data processing and storage. The decision to store the results of analysis or simply discarding them is also another issue to be looked into based on the time required to redo the analysis. The IoT network topology and its communication with the central cloud must be taken into account to have an efficient resource provisioning strategy for Big Data Handling [28].

4. Software defined network (SDN) based IoT architecture

In the new paradigm of software defined network (SDN) based virtualization, all the IoT network elements are simply forwarding devices without any intelligence instilled in them which can control and forward data traffic. These are simply COTS based equipment that receive commands from a separate software agent residing on remote servers. The entire network management and control operations reside in this software which is generally called SDN controller. The SDN controller is regarded as the brain of the entire network. The SDN controller resides on multiple physically distributed servers in a large cloud network. Besides residing on multiple servers, the SDN controller software behaves to logically control the network in a centralized manner. The control and management policies are seemed to be applied at the central location that reflects on the entire span of the network. This logical central control of the network will tremendously reduce the burden of network operators as it will avoid configuration errors across the network which is quite common in today's networks. Open and standard interfaces are developed between the data, control, and management planes that allows heterogeneous devices to connect to network without any effort. This is not possible with the current traditional networks where it is difficult to connect heterogeneous devices.

The three different planes namely data, control, and management planes in the SDN architecture are shown in Fig. 5. The data plane resides on the actual network hardware which are various COTS based IoT devices. The data plane is connected to the control plane through a southbound interface. The actual device virtualization takes place in the control plane residing in the SDN controller. Fig. 5 shows that the control plane in the SDN controller consists of a network hypervisor module for virtualization of the COTS based IoT devices. The SDN controller consists of both control and management planes as separate layers. These control and management planes communicate with each other using the northbound interface. The control plane also consists of the network operating system that controls the entire network as a single logical entity.

5. Network function virtualization (NFV) based IoT architecture

The conceptual diagram for network function virtualization (VNF) based architecture is shown in Fig. 5. Instead of a network hypervisor, this virtual layer in form of hypervisor is located on the device itself. The hypervisor creates virtual machines (VMs) on these physical hardware which is referred as virtual infrastructure in the conceptual diagram [26]. The virtual hardware can be accessed using an open standard API. The higher level programming languages can access these standard set of open APIs to create virtual network functions (VNFs). The VNFs can be created using a central software manager running on a separate server farm. The resources can be allocated and released on the fly using a software manager similar to software controller in SDN architecture [8]. On the otherhand, VNF enable devices can also be controlled using a central SDN controller so that both architectures can coexist and function together [32].

The three basic components of the VNF architecture are: **(a) Physical Hardware:** The hardware is any bare-metal machine that hosts resources such as CPU, Memory, and storage. **(b) Virtual Hypervisor Layer:** This virtual layer is the software layer that runs on the bare-metal hardware that manages the resources such as CPU power, memory, and storage capacity. **(c) Virtual Machine:** The guest virtual machine is a software that emulates the architecture and functionalities of the physical platform using a fraction of hardware resources. As a result, a particular physical hardware can host more than one VM. The maximum number of VMs that can be hosted on a physical hardware is dependant on the resources of the physical hardware and the amount of resources used by each VM [15].

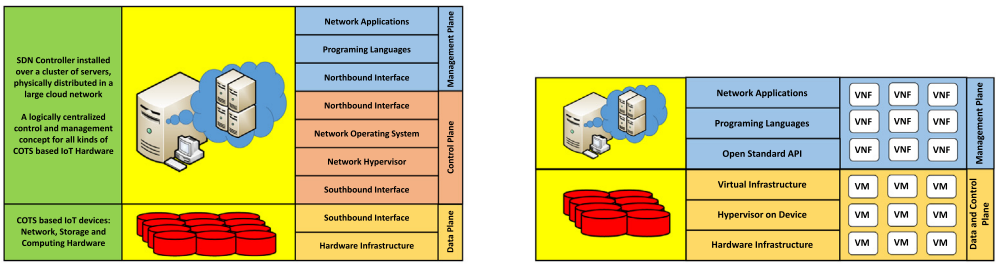
The key advantage of VNF and SDN architectures is that a general purpose COTS based servers can be incorporated in enterprize class networks for Big Data handling and computation. Even the physical layer processing of the cellular mobile networks can be implemented in these COTS servers [14]. This is a big step for telecommunication industry as it will transform the entire cellular network architecture. It will dramatically reduce the capital investment and reduce the energy consumption by resorting to cloud based data centers. However, it is yet to test the performance of such a network and only the future trials can be able to answer these questions through developing good test bed networks for active user trials. Multiple tenants will be able to share cloud based SDN and NFV architecture based virtualized network resources to improve profit margins and achieve reduced spending on infrastructure [34,12].

6. Cost analysis for SDN/NFV architecture over 4G infrastructure

The cost analysis in this section will provide comparison of the cost incurred for traditional 4G hardware networks and futuristic networks that make use of cloud enabled SDN/NFV based architecture.

6.1. Cost analysis: Baseline 4G network

Suppose that a central 4G router r_i will be able to handle k_i sessions and costs u_i dollars for a service provider i to procure it and configure in his own network ~~n~~. Let the shelf-life of the routers be x years, after which they have to be replaced. Suppose that there are m such service providers in the same business using their own



(a) SDN Architecture Kreutz et al. (2015) (b) NFV Architecture

Fig. 5. Architecture conceptual diagrams.

Table 1
Definition of input variables for 4G network.

Input variable	Description
$M = \{1, 2, \ldots, m\}$	Number of service providers
$V = \{1, 2, \ldots, c_m\}$	Number of customers of service provider m
$R = \{r_1, r_2, \ldots, r_m\}$	4G Router installed by service providers
$U = \{u_1, u_2, \ldots, u_m\}$	Unit cost of the 4G router installed by service provider
$k_i, i \in \{1, m\}$	Number of simultaneous sessions handled by router r_i
$k_v, v \in \{1, c_m\}$	Average number of sessions occupied by customer v
$e_i, i \in \{1, m\}$	Energy consumed by router r_i per day

kind of 4G central router r_i. Now suppose that each service provider m has total customers, say c_m. Each customer $v, v \in \{1, c_m\}$ uses on average k_v sessions. Suppose the average energy consumption of router r_i is e_i per day. All the input variables are summarized in Table 1.

The number of routers needed by service provider i to support all of its customers and the associated cost for x years is given by

$$n_i = (k_v/k_i) \times c_i \tag{1}$$
$$C_i = n_i \times u_i \tag{2}$$

where n_i is the number of routers needed and C_i is the cost incurred for service provider i for x years. The energy consumption for service provider i is given by E_i as follows

$$E_i = n_i \times e_i \tag{3}$$

Therefore the total cost of all m service providers for the period of x years is given by C as follows

$$C = \sum_{i=1}^{m} (n_i \times u_i) \tag{4}$$

Similarly, the total energy consumption per day is given by E as follows

$$E = \sum_{i=1}^{m} (n_i \times e_i) \tag{5}$$

6.2. Cost analysis: Network with SDN/NFV based architecture

Suppose that a SDN/NFV architecture based network offers a virtual machine (VM) that can handle $\widetilde{k}$ simultaneous sessions. Let the cost of leasing each of these VM per year is $\widetilde{u}$ dollars. The energy consumed by a VM per day is $\widetilde{e}$. Suppose that all m service providers use a common sharable SDN/NFV based network. Supposing that all other input variables for the service providers is the same, such as their number of customers and their behavior on the network, it can be seen that the number of VMs needed by service provider i to support all of its customers and the associated cost for x years is given by

$$\widetilde{n}_i = (k_v/\widetilde{k}) \times c_i \tag{6}$$
$$\widetilde{C}_i = \widetilde{n}_i \times \widetilde{u} \times x \tag{7}$$

where $\widetilde{n}_i$ is the number of VMs needed and $\widetilde{C}_i$ is the cost incurred for service provider i for x years. The energy consumption of the service provider i is denoted by $\widetilde{E}_i$, and is given by following equation.

$$\widetilde{E}_i = \widetilde{n}_i \times \widetilde{e} \tag{8}$$

For quantitative comparison, let

$$\widetilde{k} = \alpha_i \times k_i \tag{9}$$
$$\widetilde{u} \times x = \gamma_i \times u_i \tag{10}$$
$$\widetilde{e} = \beta_i \times e_i \tag{11}$$

The cost incurred by service provider i for using SDN/NFV based network for x years, expressed in terms of the cost of its 4G networks is given by $\widetilde{C}_i$ as follows

$$\widetilde{C}_i = \frac{\gamma_i}{\alpha_i} \times C_i \tag{12}$$

For the cost reduction under SDN/NFV architecture γ_i/α_i should be less than 1. If both VM and 4G router handle same number of sessions, the cost of VM should be lower than that of the 4G router cost. However, when a VM supports more sessions than the 4G router, there is more relaxation on VM cost. But it is expected by Industry experts that VMs will be more powerful and yet be less costly than 4G routers. The necessary and required condition is that $\alpha_i > \gamma_i$.

The percentage cost reduction for service provider i for using SDN/NFV architecture based shared network is given by the following expression, denoted by Γ_i.

$$\Gamma_i = \begin{cases} \frac{C_i - \widetilde{C}_i}{C_i} \times 100 \\ \frac{\alpha_i - \gamma_i}{\alpha_i} \times 100 \end{cases} \tag{13}$$

For energy consumption in SDN/NFV, it can be expressed in terms of 4G parameters as

$$\widetilde{E}_i = \frac{\beta_i}{\alpha_i} \times E_i \tag{14}$$

Next, the total cost of all m service providers for the period of x years is given by $\widetilde{C}$ as follows

$$\widetilde{C} = x \times \widetilde{u} \times \sum_{i=1}^{m} \widetilde{n}_i = C \times \frac{\sum_{i=1}^{m} \frac{n_i}{\alpha_i}}{\sum_{i=1}^{m} \frac{n_i}{\gamma_i}} \tag{15}$$

Similarly, the total energy consumption per day is given by $\widetilde{E}$ as follows

$$\widetilde{E} = \widetilde{e} \times \sum_{i=1}^{m} \widetilde{n}_i \tag{16}$$

The overall energy consumption in SDN/NFV based network expressed in terms of the energy consumption of 4G router based network is given as follows.

$$\widetilde{E} = E \times \frac{\sum_{i=1}^{m} \frac{n_i}{\alpha_i}}{\sum_{i=1}^{m} \frac{n_i}{\beta_i}} \tag{17}$$

6.3. Results

The cost and energy consumption comparison between two completely different technologies is undoubtedly very complex as it has to take many hardware specific aspects into consideration [2]. Empirical results will be more substantial to reveal the actual cost and energy consumption. However we are already aware from industrial experts that new COTs based server platforms have evolved to become more powerful to emulate the special purpose network hardware in terms of packet processing speeds and yet consume lesser power. So we take this information in the form of variable parameters to study the relative cost and energy consumptions between SDN/NFV networks and 4G networks as the above model has illustrated. This model will nevertheless provide insight on cost and energy savings as function of many different important factors.

One of the important metric is the number of sessions supported by a device. We refer a session is a constant piece of hardware resource used to serve a user. In general, a user may use more that one session on the device. This was reflected in our model presented before. In SDN/NFV based network, VMs are allocated for the service providers to serve the traffic of their customers. For this purpose, the VMs in the SDN/NFV based network are also described in terms of the number of sessions supported and the amount of energy they consume. Fig. 6 shows the variation of cost for a certain service provider i when using VMs of SDN/NFV network relative to the cost incurred while using 4G hardware. In our model and all the presented results, we assume that all customers have traffic all the time for an infinite time period. Though this assumption is not valid, it represents the worst case scenario, which will also eliminate the multiplexing gain from shared SDN/NFV network resources. Therefore the relative cost reduction is real and quantitative for the parameters of interest.

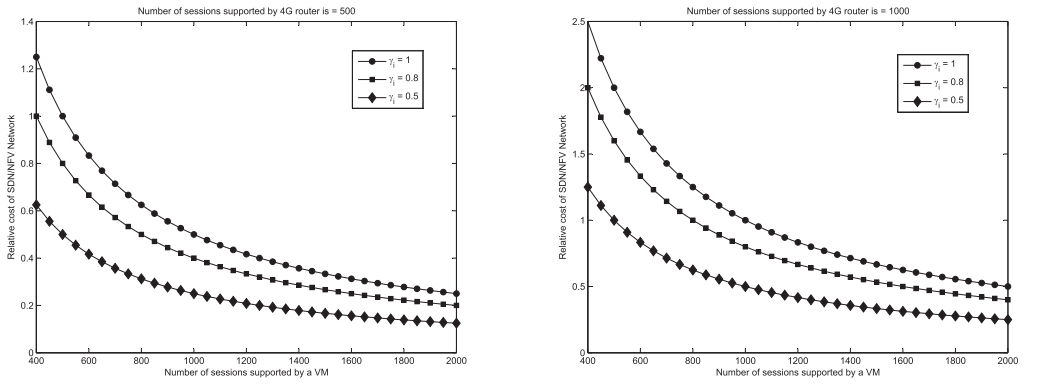
The relative cost and energy consumption reduction for service provider i in SDN/NFV network is a dependant on how powerful the VM is and at the same time how cost effective and energy efficient it is. For instance, Fig. 6 displays results for the case where the 4G router supports 500 sessions for instance. We vary the performance capacity of VM of SDN/NFV network by changing the number of sessions supported from 400 to 2000. As a worst case, we assumed that VM rent cost is same as buying a 4G router and maintaining it for its entire shelf-life. We obviously see that SDN/NFV network costs more if the VMs are not powerful enough. However, when VM start supporting more sessions than 4G router, the cost of SDN/NFV network falls down. When the actual cost of renting a VM is below the actual cost of owning a 4G router, the network cost for the service provider i is considerably lower. When VM are very powerful and supports 2000 sessions, the cost of renting VMs on SDN/NFV network falls considerably.

The SDN/NVF technology has to catchup with traditional specialized hardware technology, particularly when the 4G technology is more powerful. This is illustrated in Fig. 6, where the 4G router now supports 1000 sessions instead of 500 sessions as shown in the previous result. Thus we gradually increase the strength of 4G technology and see how that would effect the relative cost of sharing the SDN/NFV network. It is quite clear that unless the VMs have not shown real progress in strength and be economically viable, we will not witness the same amount of cost reduction while using the SDN/NFV technology. However, we still see that the relative cost of leasing the VMs in SDN/NFV network saves cost, quite substantially, for the service provider i. This would be the key to the success of the virtualization technology.

The cost reduction for SDN/NFV network in percentage is shown in Fig. 7 for cases where 4G router supports 500 and 1000 sessions respectively. It can be seen from these two results that between 40% and 80% cost reduction can be observed depending on the success of SDN/NFV technology in providing cheaper alternative and better processing power. The results have considered very nominal values for γ_i that are practically suitable. However as already mentioned, the cost is relative to the existing 4G hardware technology. It is assumed that 4G hardware is expensive compared to COTS hardware, which is true in the current existing scenarios. Enabling COTS servers to be more powerful with efficient virtualization software is another key factor in reducing cost of SDN/NFV networks. The feedback from experts from research and industry has a strong indication for higher savings in SDN/NFV technology. The energy savings from using the SDN/NFV network, for service provider i, is shown in Fig. 8.

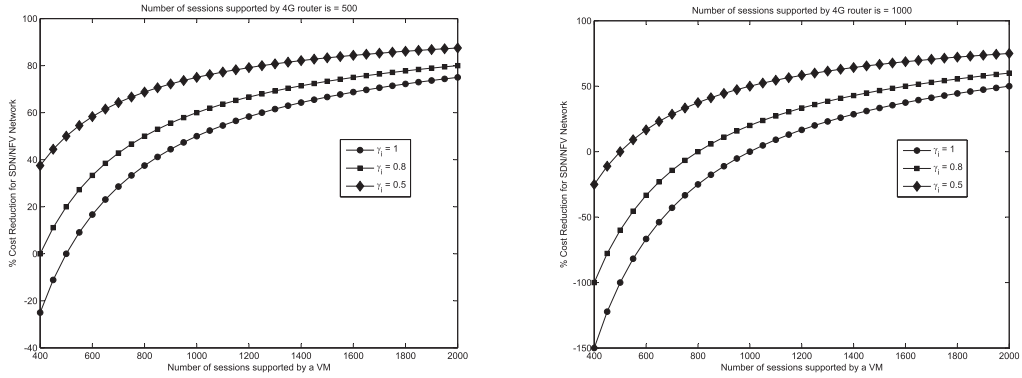
For the case of multiple service providers, we consider two scenarios, first with 3 service providers, and the second with 5 service providers. For the case of 3 service providers, $k_v = \{1, 2, 3\}$, $k_i = \{700, 800, 1000\}, \gamma_i = \{0.5, 0.6, 0.7\}$, and $c_i = \{1500, 2000, 2500\}$. For another network scenario consisting of 5 service providers,

- $k_v = \{1, 2, 3, 4, 5\}$
- $k_i = \{500, 600, 700, 800, 1000\}$



(a) The 4G router supports 500 sessions (b) The 4G router supports 1000 sessions

Fig. 6. Relative cost comparison of SDN/NFV VMs with respect to 4G network hardware for a single service provider i.



(a) The 4G router supports 500 sessions (b) The 4G router supports 1000 sessions

Fig. 7. Percentage cost reduction for using SDN/NFV VMs for a single service provider *i*.

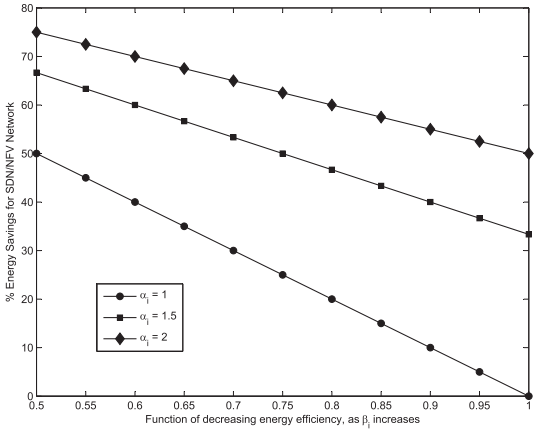


Fig. 8. Percentage energy savings for using SDN/NFV VMs for a single service provider *i*.

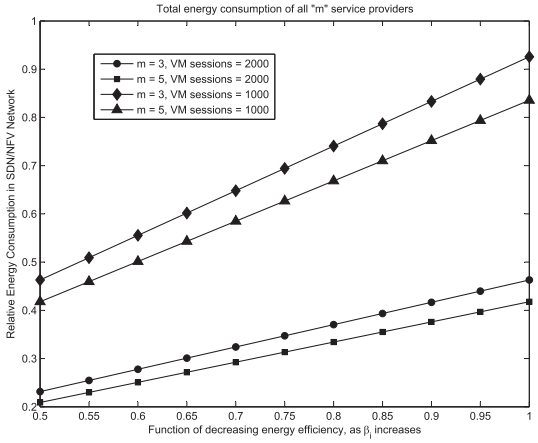


Fig. 10. Overall energy savings while using shared SDN/NFV network.

- $\gamma_i = \{0.3, 0.4, 0.5, 0.6, 0.7\}$
- $c_i = \{1500, 2000, 2500, 3000, 3000\}$

The total cost savings over all the service providers sharing the common SDN/NFV network is shown in Fig. 9. Similarly, the total energy savings over all the service providers, while using the SDN/NFV network is shown in Fig. 10. From these two results it can be seen that even when the SDN/NFV does not take multiplexing gain, it still provides substantial cost and energy savings. In our future work, we are interested in seeing how the opportunistic resource access and the multiplexing gains will provide more energy and cost savings in the shared SDN/NFV network.

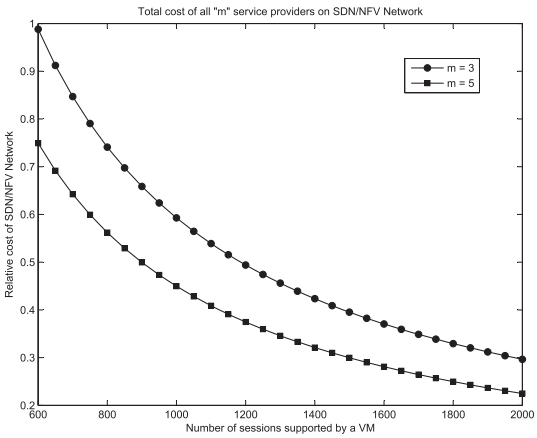


Fig. 9. The total cost over all service providers sharing SDN/NFV network.

7. Conclusion

The future network challenges and the role of virtualization in addressing all issues related to cloud based SDN and NFV technologies were discussed. Further, the concepts of virtualization were discussed along with the concepts from SDN and NFV frameworks. The necessity of cloud based data center networks is discussed from the view point of big data explosion and how the SDN/NFV based technology will likely handle the big data explosion over cloud networks. Furthermore, a cloud based SDN/NFV network was studied and a mathematical model is presented that compares the cost and energy consumption between the SDN/NFV network and a typical 4G network. All key metrics are taken as variable functions to study their effect on the overall cost and energy consumption in the SDN/NFV network. Adhering to the common assumptions in the literature, the proposed model investigates the relative cost and energy consumption for both single service provider and all the service providers in the system as a whole that are involved in SDN/NFV network sharing. By eliminating the possibility of any multiplexing gain, we have still found considerable cost reductions and energy savings in SDN/NFV based networks. The results have substantiated the claims of many gains achievable through successful deployment of networks based on software vir-

tualization. In our future work, we are interested in seeing how the opportunistic resource access and the multiplexing gains will provide more energy and cost savings in the shared SDN/NFV network.

Acknowledgments

This research is sponsored by King Abdulaziz City for Science and Technology (KACST).

References

[1] Alenezi M, Almustafa K, Hussein M. On virtualization and security-awareness performance analysis in 5G cellular networks. J Eng Sci Technol Rev 2018;11(1):199–207.
[2] Almustafa K, Alenezi M. Cost analysis of SDN/NFV architecture over 4G infrastructure. Proc Comput Sci 2017(113):130–7.
[3] Amendola S, Lodato R, Manzari S, Occhiuzzi C, Marrocco G. RFID technology for IoT-based personal healthcare in smart spaces. IEEE Internet Things J 2014;1(2):144–52.
[4] Ameur H, Khoukhi L, Esseghir M, Boulahia LM. Energy efficient networks: recent research and future challenges. Int J Wirel Mob Comput 2017;12(1):1–15.
[5] Banikazemi M, Olshefski D, Shaikh A, Tracey J, Wang G. Meridian: an SDN platform for cloud network services. IEEE Commun Mag 2013;51(2):120–7.
[6] Bello-Orgaz G, Jung JJ, Camacho D. Social big data: recent achievements and new challenges. Inform Fusion 2016;28:45–59.
[7] Callegati F, Cerroni W, Contoli C, Cardone R, Nocentini M, Manzalini A. SDN for dynamic NFV deployment. IEEE Commun Mag 2016;54(10):89–95.
[8] Choi Y, Lim Y. Optimization approach for resource allocation on cloud computing for IoT. Int J Distrib Sens Netw 2016:2016.
[9] Costa LR, Ramos GN, Drummond AC. Leveraging adaptive modulation with multi-hop routing in elastic optical networks. Comput Netw 2016;105:124–37.
[10] Dechene DJ, Shami A. Energy-aware resource allocation strategies for LTE uplink with synchronous HARQ constraints. IEEE Trans Mob Comput 2014;13(2):422–33.
[11] Demestichas P, Georgakopoulos A, Karvounas D, Tsagkaris K, Stavroulaki V, Lu J, et al. 5G on the horizon: key challenges for the radio-access network. IEEE Veh Technol Mag 2013;8(3):47–53.
[12] Duan Q, Ansari N, Toy M. Software-defined network virtualization: an architectural framework for integrating SDN and NFV for service provisioning in future networks. IEEE Netw 2016;30(5):10–6.
[13] Hamdaoui B, Alshammari T, Guizani M. Exploiting 4G mobile user cooperation for energy conservation: challenges and opportunities. IEEE Wirel Commun 2013;20(5):62–7.
[14] Han B, Gopalakrishnan V, Ji L, Lee S. Network function virtualization: challenges and opportunities for innovations. Commun Mag IEEE 2015;53(2):90–7.
[15] Hawilo H, Shami A, Mirahmadi M, Asal R. NFV: state of the art, challenges, and implementation in next generation mobile networks (vEPC). IEEE Netw 2014;28(6):18–26.
[16] Meerja KA, Ho P-H, Wu B. A novel approach for co-channel interference mitigation in femtocell networks. In: Proceedings of IEEE GLOBECOM 2011; 2011.
[17] Meerja KA, Ho P-H, Wu B, Yu H-F. Media access protocol for a coexisting cognitive femtocell network. Comput Netw 2013;57(15):2961–75.
[18] Meerja KA, Shami A, Refaey A. Hailing cloud empowered radio access networks. IEEE Wirel Commun 2015;22(1):122–9.
[19] Nitti M, Girau R, Atzori L. Trustworthiness management in the social internet of things. IEEE Trans Knowl Data Eng 2014;26(5):1253–66.
[20] Ortiz AM, Hussein D, Park S, Han SN, Crespi N. The cluster between internet of things and social networks: review and research challenges. IEEE Internet Things J 2014;1(3):206–15.
[21] Ranjan R. Streaming big data processing in datacenter clouds. IEEE Cloud Comput 2014;1(1):78–83.
[22] Saquib N, Hossain E, Kim DI. Fractional frequency reuse for interference management in LTE-advanced HETNETS. IEEE Wirel Commun 2013;20(2):113–22.
[23] Sheng Z, Yang S, Yu Y, Vasilakos AV, Mccann JA, Leung KK. A survey on the IETF protocol suite for the internet of things: standards, challenges, and opportunities. IEEE Wirel Commun 2013;20(6):91–8.
[24] Sivaraj R, Mohapatra P. Future radio access, Wi-Fi-LTE, LTE-advanced: the path to 5G. In: Fiber-wireless convergence in next-generation communication networks. Springer; 2017. p. 3–41.
[25] Spiess J, TJoens Y, Dragnea R, Spencer P, Philippart L. Using big data to improve customer experience and business performance. Bell Labs Tech J 2014;18(4):3–17.
[26] Sun S, Kadoch M, Gong L, Rong B. Integrating network function virtualization with SDR and SDN for 4G/5G networks. IEEE Netw 2015;29(3):54–9.
[27] Suto K, Nishiyama H, Kato N, Mizutani K, Akashi O, Takahara A. An overlay-based data mining architecture tolerant to physical network disruptions. IEEE Trans Emerg Top Comput 2014;2(3):. 292–30.
[28] Tao F, Cheng Y, Xu LD, Zhang L, Li BH. CCIOT-CMFG: cloud computing and internet of things-based cloud manufacturing service system. IEEE Trans Ind Inform 2014;10(2):1435–42.
[29] Tsai C-W, Lai C-F, Chiang M-C, Yang LT. Data mining for internet of things: a survey. IEEE Commun Surv Tutorials 2014;16(1):77–97 [First Quarter].
[30] Vilalta R, Mayoral A, Pubill D, Casellas R, Martínez R, Serra J, et al. End-to-end SDN orchestration of IoT services using an SDN/NFV-enabled edge node. In: Optical fiber communication conference; 2016. p. W2A-42.
[31] Wibowo FX, Gregory MA, Ahmed K, Gomez KM. Multi-domain software defined networking: research status and challenges. J Netw Comput Appl 2017.
[32] Wood T, Ramakrishnan K, Hwang J, Liu G, Zhang W. Toward a software-based network: integrating software defined networking and network function virtualization. IEEE Netw 2015;29(3):36–41.
[33] Xu LD, He W, Li S. Internet of things in industries: a survey. IEEE Trans Ind Inform 2014;10(4):2233–43.
[34] Yu R, Xue G, Kilari V, Zhang X. Network function virtualization in the multi-tenant cloud. IEEE Netw 2015;29(3):42–7.
[35] Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of things for smart cities. IEEE Internet Things J 2014;1(1):22–33.
[36] Zhang Y, Chen M. Cloud-based networking. In: Cloud based 5g wireless networks. Springer; 2016. p. 9–19.
[37] Zheng X, Martin P, Brohman K, Xu LD. Cloudqual: a quality model for cloud services. IEEE Trans Ind Inform 2014;10(2):1527–36.
[38] Zheng X, Martin P, Brohman K, Xu LD. Cloud service negotiation in internet of things environment: a mixed approach. IEEE Trans Ind Inform 2014;10(2):1506–15.